内閣府政策統括官（経済安全保障担当）御中

令和６年度経済安全保障に関する国内外の研究開発動向等に係る調査研究

最終成果報告書

令和７年３月

株式会社エヌ・ティ・ティ・データ経営研究所

目次

1. エグゼクティブサマリ（要約）

本事業では、日本において研究セキュリティ・インテグリティを確保したオープンな研究環境を確立するとともに、今後重視して研究開発投資を行うべき技術領域を明らかにすることを目的として、「諸外国における研究セキュリティ・インテグリティの確保に係る政策動向」「国内外における先端技術の研究開発動向」について調査を実施した。

諸外国における研究セキュリティ・インテグリティの確保に係る政策動向にあたっては、まずオープンな研究環境を確立するための研究セキュリティ・インテグリティの確保に資する施策の観点から、①リスクに晒されている研究領域の特定と情報共有、②デュー・ディリジェンスの実施・リスクのある活動の領域の特定、③リスク軽減策の３つの調査テーマを設定したうえで調査対象国における各調査テーマの取り組みやリスト、ガイドライン等を公開情報から抽出し、詳細調査を実施した。

国内外における先端技術の研究開発動向の調査にあたっては、まず日本にとって経済安全保障上の重要性の観点から①宇宙分野、②サイバー分野、③海洋分野、④バイオ分野の 4 分野を設定したうえで、各分野において各国で実施されている主要な研究開発プログラム等から研究開発の潮流を把握し、潮流に沿って現在の学術・研究論文の公表状況等を調査・整理した。

最終的に、上記調査について結果を総合して分析を行った結果、以下のような結果を得た。

【諸外国における研究セキュリティ・インテグリティの確保に係る政策動向】

- テーマ１：リスクに晒されている研究領域の特定と情報共有
  - 机上調査の結果、諸外国では、科学技術政策上の重点分野の形成や、省庁間の調整、政府支援施策の根拠として、政府機関や研究コミュニティに情報を提供する事例が多く見られた
  - また、各研究領域に内在する経済・安全保障上のリスクへの対処については、関係機関への情報提供にとどまるものもある一方、研究セキュリティやインテグリティに関するデュー・ディリジェンスやスクリーニング基準の策定に活用されるリストも確認された

- テーマ２：デュー・ディリジェンスの実施・リスクのある活動の領域の特定
  - 机上調査の結果、諸外国では、資金提供機関が研究開発実施主体に必要な情報の開示を指示し、その情報に基づいてリスク評価を行うケースと、資金提供機関が研究開発実施主体（申請者）にデュー・ディリジェンスの実施を指示し、その結果を受け取った上で最終的なリスク評価や資金提供の可否を判断するケースが存在することが確認された。後者のケースでは、特にカナダの NSGRP におけるデュー・ディリジェンスのガイダンスなどで、具体的な作業手順まで示されていることが確認された
  - また、デュー・ディリジェンスの確認観点として、申請者の研究活動自体が持つリスク、共同研究のパートナー組織や申請者の組織内職員に関わる利益相反や責務相反のリスクなどが挙げられた

・ テーマ３：リスク軽減策
  - 机上調査では、米国の NSF 研究セキュリティトレーニングや英国、EU、豪州の取り組みについて、デュー・ディリジェンス結果との明示的な関連性は確認できなかったものの、これらは研究セキュリティ・インテグリティ上の脅威やリスクを示し、大学や研究機関に対してインフラ面・人的側面・組織的側面のリスク軽減策の実施をガイドラインとして推奨していることが分かった
  - 一方、カナダでは、NSGRP が適用される研究開発プログラムにおいてデュー・ディリジェンスを実施し、その結果に基づいてリスク軽減計画を策定・実施することが求められており、デュー・ディリジェンスの結果とリスク軽減策が連動している点で、他国との違いが確認された

【国内外における先端技術の研究開発動向】

・ 宇宙分野
  - 将来の通信インフラの重要な技術となる可能性や、スペースデブリ等の現状のインフラに対する脅威を防止することが可能となる技術等の経済安全保障上の重要性があり、既存の支援対象技術（特定重要技術）に該当しないこと等を考慮し、技術領域を調査・整理した。

・ サイバー分野
  - 従来のサイバー攻撃対処において共通の課題となっていた事項を解決することが期待され、また近年研究開発も多く実施されており、サイバー空間の活用が今後更に不可欠になると見込まれる状況等から経済安全保障の観点からもより一層重要性が増していくと判断した技術領域を調査・整理した。

・ 海洋分野
  - 現在 K プログラム等では支援対象となっておらず、無人探査やセンシング等にも関連する経済安全保障の観点からも重要となる技術領域を調査・整理した。

・ バイオ分野
  - 主に個別化医療、食料安全保障、バイオものづくりに関連した技術の研究開発が多く、ゲノムに関連する研究開発など、近年、日本の中で注目されているような技術領域を調査・整理した。

2. 調査の背景・目的

各国において経済安全保障の確保に関する各種政策、特に先端的な重要技術の研究開発の促進やその成果の活用に向けて鎬を削っているところ、中・長期的に我が国が国際社会で確固たる地位を確保し続けるためには、諸外国における取組状況に係る情報を更新し続けるとともに、こと研究開発においては日進月歩で進展・変化の早い先端技術分野に係る開発動向を適時把握することが肝要である。このような国内外の動向を明らかにすることにより、「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」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、本調査研究を行うこととする。

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、前項に示した目的を達成するために本業務においては、本作業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、計画の作成及び実施管理を行い（仕様書 6.(1)）、国外における経済安全保障の確保に向けた政策動向に関する調査研究（同 6.(2)）、及び国内外における先端的な重要技術の研究開発動向に関する調査研究（同 6.(3)）を実施し、最終的な検討結果を調査研究報告書として取り纏め作成する（同 6.(4)）。それにより、経済安全保障推進法に基づく特定重要技術の効率的な開発支援を推進することを本業務のスコープとする（図 3.1-1）。

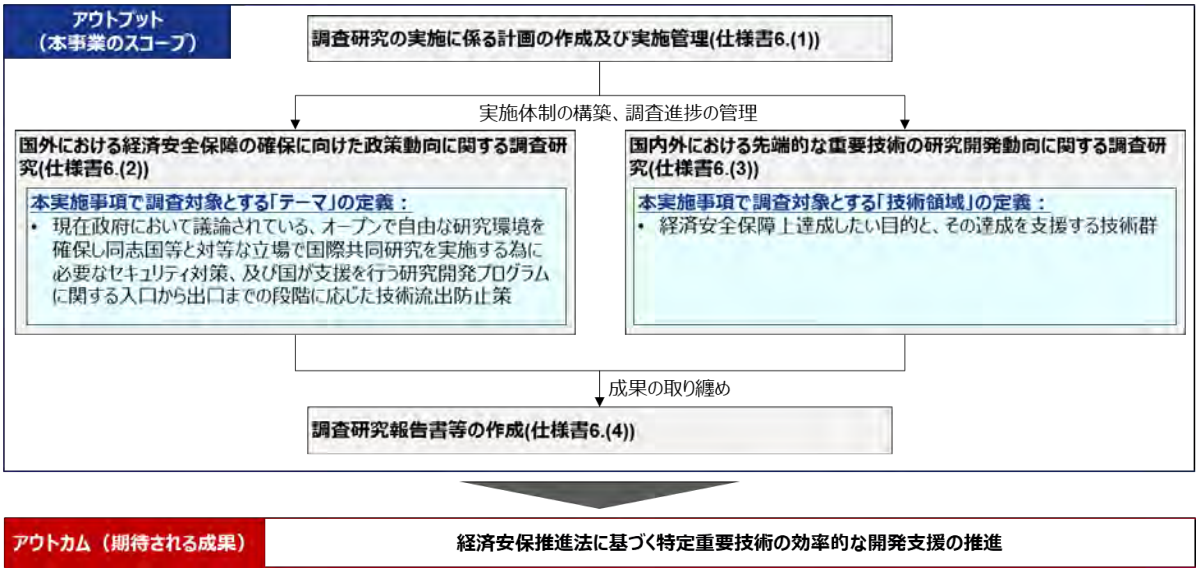


図 3.1-1　本事業実施の全体像

3.2 調査方法

3.2.1　国外における経済安全保障の確保に向けた政策動向に関する調査研究

（1）全体実施方針

本項においては、国外における経済安全保障の確保に向けた政策動向、特に先端的な重要技術の研究開発に係るリスクマネジメントやリスク低減対策等についての調査・整理を行う。

調査対象国については日本との経済・安全保障上の価値観の共有や、地域的な網羅性等の観点から、仕様書にも記載のある米国、英国に加え、カナダ、EU、豪州、韓国を調査対象とする。

調査を実施するテーマについては、G7 及び同志国による「経済安全保障法制に関する有識者会議」の議論結果（オープンで自由な研究環境を確保し、同志国等と対等な立場で国際

共同研究を実施する為に必要なセキュリティ対策、及び国が支援を行う研究開発プログラムに関する入口から出口までの段階に応じた技術流出防止策の検討が必要）を踏まえ、現在、日本が研究セキュリティ・インテグリティについて求められている対策を基点に、以下の 3 テーマとする（表 3.2-1）。

表 3.2-1　調査テーマ

テーマ	調査内容
テーマ１：リスクに晒されている研究領域の特定と情報共有	国にとって経済安全保障上、外国の影響力の行使に晒される等のリスクを有している研究領域を分析・特定し、その研究開発に係る研究コミュニティ、政府機関等へリスク情報を共有して対策を促す取り組みについて調査する
テーマ２：デュー・ディリジェンスの実施・リスクのある活動の領域の特定	政府からの資金提供支援の決定時に透明性と関連情報の開示を求める、懸念のある国・機関のリストを参照する等してデュー・ディリジェンスを実施して、リスクのある活動領域を明らかにする取り組みについて調査する
テーマ３：リスク軽減策	政府・資金提供機関等の方針やデュー・ディリジェンスの結果に基づいて実施される、組織レベルもしくはプロジェクトレベルでの電子的･物理的な情報へのアクセス制御や知財管理等の対策について調査する

また、3 つのテーマに加え、各国で近年研究機関の内部者・研究パートナー等による情報漏洩が各国の研究セキュリティやインテグリティ対策において重要な前提となっていることが考えられることから、近年発生した主要な情報漏洩事案を調査する。

以降、各テーマの実施方針及び実施項目・方法について記載する

（2）各調査テーマの実施方針及び実施項目・方法

1）テーマ１：リスクに晒されている研究領域の特定と情報共有

a）実施方針

テーマ 1 では、国にとって経済安全保障上、外国の影響力の行使に晒される等のリスクを有している研究領域を分析・特定し、その研究開発に係る研究コミュニティ、政府機関等へリスク情報を共有して対策を促す取り組みについて調査を実施する。

また、リスク管理のみならず、当該研究領域の研究開発を促進する取り組みについても調査するとともに、リスクを有している研究領域の分析・特定と各国の学術・研究領域の体系的な整理区分との関連性についても調査を実施する。

実施手順としては、まず調査単位となる取り組みを定義したうえで各国の主要な取り組みを抽出し、当該取り組みの詳細調査を実施する。その後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、その傾向やテーマ 2、テーマ 3 への活用動向について明らかにする。

b）実施項目・方法

① 各国の主要な取り組みの抽出

調査対象国におけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を公開情報から抽出する。抽出する対象の定義については表 3.2-2 の通り。

表 3.2-2 テーマ 1 における抽出対象の定義

抽出対象	定義
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	✓ 調査対象国における、国にとって経済安全保障上重要な研究領域の分析・特定に係る政策的な取り組み、及びそれによって特定された研究領域のリスト
学術・研究領域の体系的な整理区分	✓ 調査対象国において、研究開発予算の配分や教育の統計等の基礎となる学術・研究領域の体系的な整理区分・分類基準

② 詳細調査

抽出した取り組み、リストについて**①概要（名称、所管、策定時期、背景・目的、関係機関）、②リストの構成、③活用方法**を公開情報等から整理する。

2）テーマ 2：デュー・ディリジェンスの実施・リスクのある活動の領域の特定

a）実施方針

テーマ 2 では、政府からの研究開発に対する資金提供支援時に透明性と関連情報の開示・確認を求めるデュー・ディリジェンスの取り組みについて調査を実施する。

実施手順としては、まず調査単位となる取り組みを定義したうえで各国の主要な取り組みを抽出し、当該取り組みの詳細調査を実施する。

b）実施項目・方法

① 各国の主要な取り組みの抽出

まず、調査対象国における研究セキュリティ・インテグリティを確保するためのデュー・ディリジェンスに係る政策動向に関するマクロ調査を実施したうえで、政府からの研究開発に対する資金提供支援時に透明性と関連情報の開示・確認を求めるデュー・ディリジェンスの取り組みを公開情報から抽出する。抽出する対象の定義については表 3.2-3 の通り。

表 3.2-3 テーマ 2 における抽出対象の定義

✓ 政府による研究開発への資金提供支援時や、研究機関・研究者によるパートナーシップの締結時等に、支援対象機関・研究者等に関連情報の開示を求める、公開情報の確認を行う等により、当該機関・研究者の自律性を脅かす可能性のある構造や態勢、外国政府・軍隊・治安機関等との関係、透明性の欠如等のリスクを分析する取り組み
✓ 中でも、機密情報や秘匿された研究に関するものではなく、オープンな研究環境における取組を対象とする

また、抽出するデュー・ディリジェンスの取り組みについては、**政府、資金提供機関、研究開発実施主体**がそれぞれ実施主体であるものを整理する。

② 詳細調査

抽出した取り組みについて、**①概要（名称、所管、公表時期、背景・目的、デュー・ディリジェンスの実施主体、デュー・ディリジェンスの対象、デュー・ディリジェンスの実施タイミング）、②デュー・ディリジェンスの実施手法（実施プロセス、確認観点、参照している情報ソース）**を公開情報等から整理する。

3）テーマ 3：リスク軽減策

a）実施方針

テーマ 3 では、テーマ 2 で調査したデュー・ディリジェンスを実施した結果明らかとなったリスクに基づいて、政府・資金提供機関が研究開発実施主体に対して求めるリスク軽減策について調査を実施する。

実施手順としては、まず調査単位となる取り組みを定義したうえで各国の主要な取り組みを抽出し、当該取り組みの詳細調査を実施する。

b）実施項目・方法

① 各国の主要な取り組みの抽出

調査対象国におけるデュー・ディリジェンスを実施した結果明らかとなったリスクに基づいて、政府・資金提供機関が研究開発実施主体に対して求めるリスク軽減策を公開情報から抽出する。抽出する対象の定義については表 3.2-4 の通り。

他方、リスク軽減策がデュー・ディリジェンスによるリスク評価結果と関係するのか、及び資金提供機関が研究開発実施主体に課すリスク軽減策なのかが机上調査で判別できない場合は、デュー・ディリジェンス施策や所掌機関等のリスク軽減策を調査する。

表 3.2-4 テーマ 3 における抽出対象の定義

テーマ 2 で明らかにした政府・資金提供機関等の方針やデュー・ディリジェンスの結果に基づいて、政府・資金提供機関が研究開発実施主体に対して求めるインフラ・人・資金提供面のリスクを軽減する対策 特に段階的なリスク対応に関するもの

② 詳細調査

抽出した取り組みについて、**①概要（リスク軽減策の根拠となる取り組み等、背景・目的、リスク軽減策の指示主体、リスク軽減策の実施主体、リスク軽減策を実施するタイミング）、②リスク軽減策の内容（インフラ（デジタル・物理）面のリスク軽減策、人的リスク軽減策、組織的リスク軽減策）**を公開情報等から整理する。

4）情報漏洩事案の調査

a）実施方針

各国で近年研究機関の内部者・研究パートナー等による情報漏洩が各国の研究セキュリティやインテグリティ対策において重要な前提となっていることが考えられることから、各国で近年発生した主要な情報漏洩事案について調査・整理を実施する。

実施手順としては、まず調査対象とする事案を定義のうえ、公開情報を基にリストアップする。その後、過去に発生した情報漏洩事案を、各国で現在取り組まれている対策によって防ぎえたか、という観点から分析を行うため、各事案の発生状況について詳細調査を実施する。

b）実施項目・方法

① 各国の事案のリストアップ

日本及び調査対象国における、近年発生した研究機関における情報漏洩事案を公開情報から調査・整理する。その際、研究セキュリティ・インテグリティの確保に向けて各国において対策が講じられている、研究機関の内部者やパートナー機関を通じて発生した情報漏洩事案を対象とする。リストアップする事案の定義については表 3.2-5 の通り。

表 3.2-5 情報漏洩事案の調査において対象とする事案の定義

✓ 日本及び調査対象国で 2020 年以降、国立研究機関、大学、民間研究所等において、機関内の人員及びパートナー機関を通じて発生した技術情報等の漏洩事案（未遂及びリスクの発覚含む）
✓ ハッキングやランサムウェアによる被害ではなく、利益相反・責務相反、汚職や賄賂、外国からの圧力などによって「人」を通じて発生した情報漏洩を対象とする

② 詳細調査

リストアップした事案の中で、公開情報が充実しており、事件の詳細を把握することが可能な事案を絞り込み、その**①発生時期、②情報漏洩者の氏名・国籍・所属、③漏洩先・漏洩手段の類型・具体的手段、④事案の概要・なぜ起きたか、⑤事案の及ぼした影響**について詳細調査を実施したうえで、テーマ 3 までで調査した各国の対策によって事案を防ぎえたか、という観点から整理・分析を実施する。

3.2.2 国内外における先端的な重要技術の研究開発動向に関する調査研究

（1）実施方針

本項においては、宇宙分野、サイバー分野、海洋分野、バイオ分野において経済安全保障の観点から重要となる技術領域における先端的な重要技術の研究開発動向について、論文・特許等の公開情報に基づく調査・分析を行う。

調査対象国としては、日本に加え、経済安全保障の観点から価値観を共有する米国、英国EU 等を中心に調査を実施する。調査では、対象国の各分野における研究開発機関のプロジェクトや、各国で発表されている研究論文を対象に、その内容を整理する。整理した研究開発プロジェクトや論文の内容を基に、経済安全保障上の重要性や既存の支援対象技術（特定重要技術）などの要素を考慮し、各分野における技術領域を調査・整理する。

（2）実施項目・方法

1）技術領域の調査・整理

技術領域の調査・整理のために、まず各分野（宇宙、サイバー、海洋、バイオ）に関して研究開発を実施している各国の主要な機関・研究所の研究開発プロジェクトや各国で発表されている論文・特許等の調査を実施し、その研究目的、対象となる技術等について整理を実施する。整理した研究開発プロジェクト・論文について、経済安全保障上の重要性及び既存支援対象技術（特定重要技術）等を考慮しつつ、技術領域を調査・整理する。

（技術調査・整理の観点）
・　技術内容から経済安全保障上の重要性が高いと判断されること
・　国内外で当該技術領域に関する研究が多く実施されていること
・　既存の支援対象技術（特定重要技術）に該当しないこと

4. 調査結果

4.1 国外における経済安全保障の確保に向けた政策動向に関する調査研究

4.1 項における各調査テーマの調査先機関については Appendix I を参照。

4.1.1 テーマ１：リスクに晒されている研究領域の特定と情報共有

（1）米国

公開情報を基に、米国におけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を抽出した（表 4.1-1）。

表 4.1-1　詳細調査を行う取り組み・リスト

抽出対象	取り組み・リストの名称
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	Critical and emerging Technologies（CETs）
学術・研究領域の体系的な整理区分	CIP Codes

以下に表 4.1-1 に掲載した取り組み・リストについての詳細調査結果を示す。

1）Critical and emerging Technologies（CETs）[1]

■　所管

- 国立科学技術会議(the National Science and Technology Council: NSTC)
- 科学技術政策局（the Office of Science and Technology Policy: OSTP）
- 重要技術と新興技術に関するファストトラックアクション委員会(the Fast Track Action Subcommittee on Critical and Emerging Technologies)

■　策定（更新）時期

2020 年公表　その後 2022 年、2024 年に更新

■　背景・目的

CETs は、トランプ政権時 2017 年の国家安全保障戦略（NSS）に基づき 2020 年に公表された「重要・新興技術のための国家戦略」において特定された 20 分野の重要・新興技術（CETs）が基になっており、その後 2022 年 2 月、2024 年 2 月にリストが更新された。

CETs は①米国民の安全の保護、②経済的繁栄と機会の拡大、③民主的価値の実現・擁護の 3 つの米国の国家安全保障上の利益を拡大させる可能性のある技術とされており、2024 年に更新されたバージョンでは 18 の技術分野が特定されている

[1] https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf

■　関係機関

「CET リストを作成するために、科学技術政策局（OSTP）は、国家安全保障会議（NSC）との連携の下、国家科学技術会議（NSTC）を通じて、省庁間の広範な審議プロセスを進行した」という旨の記載があり、具体的な審議プロセスは明らかでないが「18 の省庁および大統領府から、主要な専門家が参加した」とあり、これは重要技術と新興技術に関するファストトラックアクション委員会に参加している以下のメンバーのことと思われる。

農務省、商務省 、国防総省 、エネルギー省、保健福祉省、国土安全保障省、内務省、司法省、国務省、運輸省、米国航空宇宙局、国家科学財団、国家安全保障局、国家安全保障会議スタッフ、国家宇宙会議スタッフ、国家情報長官事務所、行政管理予算局、科学技術政策局

■　リストの構成

CETs は 2024 年現在 AI、バイオテクノロジー、量子、半導体等の 18 分野が特定されており、各分野にはその範囲をより詳細に説明するためのサブフィールドが含まれている（図 4.1-1）。

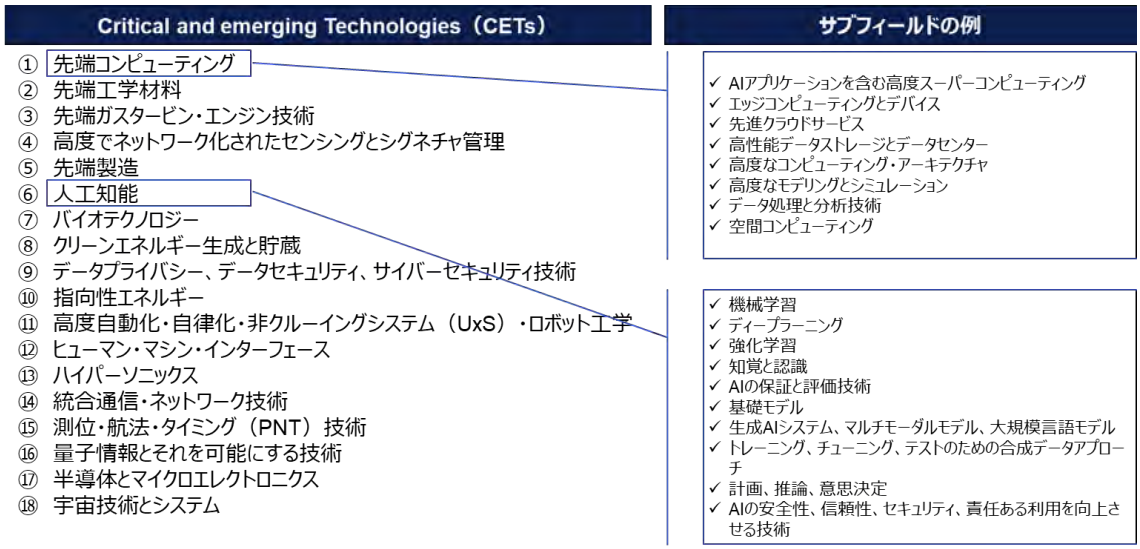


図 4.1-1　CETs リストの構成

■　活用方法

CETs は、政府機関や研究コミュニティ等にとって技術競争・国家安全保障上の重要技術に関する情報リソースとして活用されることが前提となっているものの、一部で以下のように機密情報の不正流用や悪用から研究を保護するための参考とできる旨も記載されている。

＜CETs におけるリストの活用方法に関する記載＞

✓ CET リストは、戦略文書ではないが、**米国の技術競争力と国家安全保障に関する政府全体、および各省庁固有の取り組みに役立つ情報を提供**することができる。

✓ また、このリストは、**CET とその構成分野の優先順位を決める今後の取り組み**に役立つ可能性がある。しかし、このリストは**政策立案や資金調達における優先順位を示したリストではない**。その代わり、このリストは以下のような目的で利用されるべきである。

① 米国の技術的リーダーシップを促進するための将来の取り組みに情報を提供する
② 同盟国やパートナーと協力して共通の技術的優位性を促進・維持する
③ 社会に具体的な利益をもたらし、民主的価値観に沿った CET を開発・設計・管理・利用する
④ 米国の安全保障に対する脅威に対応する米国政府の対策を開発するため。

✓ 国家安全保障を支援する技術の研究開発、国際的な人材の獲得競争、**機密技術の不正流用や悪用からの保護などのイニシアティブを開発する際**に、各省庁はこの CET リストを参考にすることができる。

2）CIP Codes[2]

CIP Code は米国、カナダにおける高等教育分野の分類であり、米国 NCES（国立教育統計センター）によって開発された。NCES の高等教育に関する統計データである IPEDS（統合高等教育データシステム）などに活用されている。

区分は「農業、農業経営、関連化学」「天然資源と保護」「建築及び関連サービス」など、最も大きな区分で 60 種となっている（図 4.1-2）。

図 4.1-2　CIP Code の区分例

[2] https://nces.ed.gov/ipeds/cipcode/browse.aspx?y=55

（2）カナダ

公開情報を基に、カナダにおけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を抽出した（表 4.1-2）。

表 4.1-2　詳細調査を行う取り組み・リスト

抽出対象	取り組み・リストの名称
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	✓ Sensitive Technology Research Areas（STRA） ✓ Emerging Technology Trend Cards
学術・研究領域の体系的な整理区分	カナダ研究開発分類（CRDC）

以下に表 4.1-2 に掲載した取り組み・リストについての詳細調査結果を示す。

1）Sensitive Technology Research Areas（STRA）[3,4]

■　所管

政府 HP や本文では特に所管主体は明示されていないが、公表は科学・産業大臣、保健大臣、公安・民主的制度・政府間問題大臣の連名によってなされている

■　策定（公表）時期

2024 年 1 月公表

■　背景・目的

2023 年に発出された、連邦政府による「カナダの研究保護に関する声明」に基づき、カナダの研究・機関・知的財産を保護するための政策検討の結果、カナダの連邦助成評議会であるカナダ衛生研究所(CIHR)、カナダ自然科学工学研究評議会(NSERC)、カナダ社会科学人文科学研究評議会(SSHRC)、及びカナダイノベーション財団(CFI)、関係する連邦省庁等との緊密な協議により、「機微技術研究と懸念される提携に関する方針（Policy on Sensitive Technology Research and Affiliations of Concern：STRAC ポリシー）」が政策文書として発出された。

そして STRAC ポリシーの中に、11 のセンシティブテクノロジー研究分野(STRA)のリストと、103 の指定研究機関(NRO)のリストが含まれており、連邦政府機関(CIHR、NSERC、SSHRC)およびカナダイノベーション財団(CFI)に提出されたすべての助成金申請に適用されることとなっている。STRA リストは、研究者が連邦政府から機密性の高い研究分野を推進する研究に対する資金提供を受ける際に、NRO リストとともに参照して資金提供を受けることが可能か判断する目的で公開された。

---

[3] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern

[4] https://research.mcmaster.ca/home/support-for-researchers/research-security/policy-on-sensitive-technology-research-and-affiliations-of-concern-strac/

■　関係機関

STRA を含む政策文書である STRAC には、策定にあたってカナダの研究コミュニティである連邦助成評議会（CIHR、NSERC、SSHRC）、カナダ革新財団（CFI）、カナダ外務省（GAC）科学・経済開発省（ISED）、カナダ政府大学ワーキンググループなどが関与したと述べられている。大学ワーキンググループには、上記の機関の他、カナダ安全保障情報局、カナダ公安などが含まれる。

■　リストの構成

STRA は、「カナダにとって重要だが、カナダの技術的優位性を不正に流用してカナダに損害を与えようとする外国政府、政府支援団体、非政府団体の関心を引く可能性のある先進技術と新興技術」とされ、先端デジタルインフラ技術、先端エネルギー技術等の 11 のハイレベル技術カテゴリと、その下のサブカテゴリ及び補足文から構成されている（図 4.1-3、表 4.1-3）。

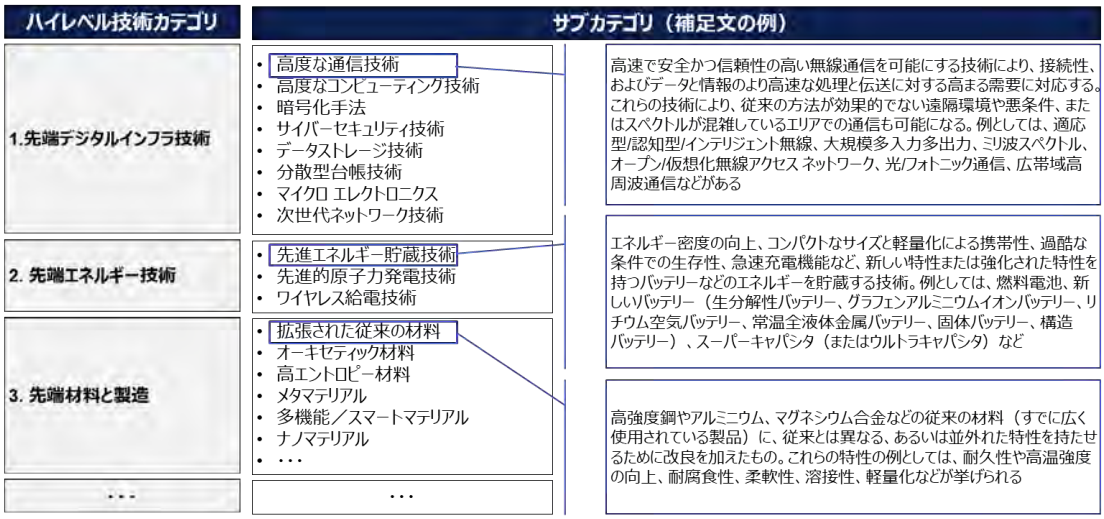


図 4.1-3　STRA の構成イメージ

表 4.1-3　STRA の一覧

ハイレベル技術カテゴリ	サブカテゴリー
1.先端デジタルインフラ技術	✓　高度な通信技術 ✓　高度なコンピューティング技術 ✓　暗号化手法 ✓　サイバーセキュリティ技術 ✓　データストレージ技術 ✓　分散型台帳技術 ✓　マイクロ エレクトロニクス ✓　次世代ネットワーク技術
2. 先端エネルギー技術	✓　先進エネルギー貯蔵技術 ✓　先進的原子力発電技術 ✓　ワイヤレス給電技術

ハイレベル技術カテゴリ	サブカテゴリー
3. 先端材料と製造	＜先端材料＞ ✓ 拡張された従来の材料 ✓ オーキセティック材料 ✓ 高エントロピー材料 ✓ メタマテリアル ✓ 多機能／スマートマテリアル ✓ ナノマテリアル ✓ アディティブマニュファクチャリング用粉末材料 ✓ 超伝導材料 ✓ 2 次元(2D)マテリアル ＜先進製造＞ ✓ アディティブ・マニュファクチャリング（3D プリンティング） ✓ 先端半導体製造 ✓ 重要材料製造 ✓ 4 次元(4D)プリント ✓ ナノマニュファクチャリング ✓ 2 次元(2D)材料製造
4.高度なセンシングと監視	✓ 高度な生体認証技術 ✓ 高度なレーダー技術 ✓ 原子干渉計センサー ✓ クロスキューセンサー ✓ 電界センサー ✓ イメージングおよび光学デバイスとセンサー ✓ 磁場センサー（または磁力計） ✓ マイクロ（またはナノ）電気機械システム（M/NEMS） ✓ 位置、ナビゲーション、タイミング（PNT）技術 ✓ サイドスキャンソナー ✓ 合成開口ソナー（SAS） ✓ 水中（無線）センサーネットワーク
5.高度な武器	✓ 軍隊、場合によっては法執行機関が防衛や国家安全保障の目的で使用している新兵器または改良兵器。材料、製造、推進、エネルギーなどの技術の進歩により、指向性エネルギー兵器や極超音速兵器などの兵器が現実に近づき、ナノテクノロジー、合成生物学、人工知能、センシング技術などにより、生物兵器や化学兵器、自律型兵器などの既存の兵器が強化された ✓ （サブカテゴリはなく、補足文のみ）

ハイレベル技術カテゴリ	サブカテゴリー
6. 航空宇宙・宇宙・衛星技術	✓ 先進的な風洞 ✓ 軌道上整備、組立、製造システム ✓ ペイロード ✓ 推進技術 ✓ 衛星 ✓ 宇宙ベースの測位、ナビゲーション、タイミング技術 ✓ 宇宙ステーション ✓ ゼロエミッション/燃料航空機
7. 人工知能とビッグデータ技術	✓ AI チップセット ✓ コンピュータービジョン ✓ データサイエンスとビッグデータ技術 ✓ デジタルツイン技術 ✓ 機械学習（ML） ✓ 自然言語処理
8. ヒューマンマシンインテグレーション	✓ ブレインコンピューターインターフェース ✓ 外骨格 ✓ 神経補綴/サイバネティック装置 ✓ 仮想現実/拡張現実/複合現実 ✓ ウェアラブルニューロテクノロジー
9. ライフサイエンステクノロジー	＜バイオテクノロジー＞ ✓ バイオ製造 ✓ ゲノム配列解析と遺伝子工学 ✓ プロテオミクス ✓ 合成生物学 ＜医療・ヘルスケア技術＞ ✓ 化学、生物、放射線、核（CBRN）医療対策 ✓ 遺伝子治療 ✓ ナノ医療 ✓ 組織工学と再生医療
10. 量子科学技術	✓ 量子通信 ✓ 量子コンピューティング ✓ 量子材料 ✓ 量子センシング ✓ 量子ソフトウェア
11. ロボティクス・自律システム	✓ 分子（またはナノ）ロボット ✓ （半）自律型/無人航空機/地上車両/海洋車両 ✓ サービスロボット ✓ 宇宙ロボット

■　活用方法

STRA は連邦助成評議会および CFI（カナダイノベーション財団）に提出されるすべての助成金申請に適用され、STRA のサブカテゴリに該当する研究プロジェクトは、従事する研究者が指定研究機関(NRO)に所属する、もしくは NRO からの支援を受けている場合申請対象外となる（図 4.1-4）。

図 4.1-4　連邦助成評議会および CFI に助成金を申請する際の STRA に関する判断基準 [5]

なお、STRAC ポリシーの対象となるか否かは当該研究プロジェクトが「STRA を発展・進歩させるのか」が判断基準であり、以下のように研究内容に STRA に該当する技術を含むとしても単純に対象となるわけではない [6]。

＜プロジェクトの進展に応じて STRAC ポリシーの対象となる例＞

例①：ある社会科学プロジェクトにおいてデータを整理するために人工知能（AI）を使用している場合

→STRA には人工知能関連技術が含まれるが、単純にその技術を使用・適用しているのみであれば、STRAC ポリシーの対象とはならない

例②プロジェクトの進展によって人工知能技術が進歩を遂げることがある場合

→これは STRA を発展・進歩する内容が含まれるため、STRAC ポリシーの対象となり、資金提供機関に対して報告する必要がある

実際にカナダの主要な資金提供機関である自然科学工学研究評議会(NSERC)の助成金プログラムの公募情報では、掲載されている「Alliance grants Terms and conditions of award（アライアンス補助金利用規約）」に STRAC ポリシーを遵守しなければならないことや、NSERC の承認なく研究活動を継続できない旨が記載されている [7,8]。

---

[5] https://research.mcmaster.ca/home/support-for-researchers/research-security/policy-on-sensitive-technology-research-and-affiliations-of-concern-strac/（STRAC について解説しているマクマスター大学 Web ページ）

[6] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/frequently-asked-questions-faq-policy-sensitive-technology-research-and-affiliations-concern

[7] https://www.nserc-crsng.gc.ca/Innovate-Innover/AllianceCatalyst-CatalyseurAlliance_eng.asp#note1

[8] https://www.nserc-crsng.gc.ca/_doc/alliance/TC-Alliance_e.pdf

＜NSERC の助成金プログラムの規約における STRA 適用に関する記載＞
20. 本補助金による活動に関与するすべての研究チームメンバーは、STRAC ポリシーに関する三機関ガイダンスに従い、本補助金の期間中、**「機密技術研究および懸念される提携に関するポリシー（STRAC ポリシー）」を遵守しなければならない**。

21. あなたは、「機微技術研究および懸念される提携に関する方針（Policy on Sensitive Technology Research and Affiliations of Concern）」に従った遵守の**証明書の提出が必要となるような研究内容の変更があった場合、NSERC および所属機関の職員に報告**する。**NSERC の承認が得られるまで、これらの研究活動を進めない**ものとする。

22. あなたの研究がリスト化された機微（センシティブ）技術研究分野を推進することを目的としていると特定されたため、1 つ以上の STRAC ポリシー証明書が NSERC に提供された場合：
国家安全保障の評価および STRAC ポリシーの遵守を目的として、**STRAC ポリシー証明書に記載されたすべての情報がカナダ政府の省庁で共有される**ことに同意する。
あなたは、NSERC および貴殿の所属機関の職員に、**機密技術研究および懸念される提携に関するポリシーの遵守に関する証明書の提出を必要とする可能性のある研究チームの構成の変更について報告**する。NSERC の承認が得られるまで、本助成金による研究活動を続行しないこと。

2）Emerging Technology Trend Cards[9]

■ 所管
・ カナダ国防省（DND）
・ カナダ軍（CAF）

■ 策定（公表）時期
2024 年 5 月（技術の特定自体は、2011 年から DRDC において実施されている、興の科学技術を特定し、防衛、公共の安全、国家安全保障への影響を評価する「科学技術予測およびリスク評価プログラム」で行われている）

■ 背景・目的
Emerging Technology Trend Cards は、特に民間と軍事の両方の用途を持つ新興技術に関して、セキュリティに対するリスクを最小限に抑えながら、研究者が科学と研究をより透明で包括的、持続可能で協力的なものにするために役立てるものとして、国防省（DND）の科学技術組織であるカナダ国防研究開発局（DRDC）が国立研究会議（NRC）と提携して策定された。
トレンドカードは、防衛と国家安全保障に特に焦点を当てた新興技術に関する背景情報を研究コミュニティに提供し、認識を高めることを目的としている。

[9] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/emerging-technology-trend-cards

ただし「トレンドカードは、カナダ政府の機密研究分野のリスト（恐らく STRA の事を指していると思われる）へ研究セキュリティのデュー・ディリジェンスの目的で追加または置き換えるものではない」としている。

■ 関係機関

・ カナダ国防省（DND）-カナダ国防研究開発局（DRDC）
・ カナダ軍（CAF）
・ 国立研究会議（NRC）

■ リストの構成

2024 年 5 月更新時点では 10 の新興技術が特定され、それらを可能とする技術及び関係するステークホルダーの動向、当該技術の与えるインパクトなどの背景情報が提供されている（表 4.1-4）。

表 4.1-4 現在のトレンドカードの一覧（2024 年 5 月時点）

新興技術	トレンドカードの概要
見通し外通信とアプリケーション	見通し外（BLOS）とは、無線通信システムの範囲を制限を超えて拡張する技術またはシステムを指す。用途には、無人航空機（UAV）の BLOS 制御、地平線上のターゲットを視認できるレーダー、自然災害救助に使用されるアドホック通信ネットワークなどがある
寒冷気候用衣料の素材と生理学的モニタリング	体温管理と寒冷による傷害からの保護のため、有機ハイドロゲル、イオンゲル、相変化材料などの新素材の進歩により、寒冷地用繊維製品やウェアラブル製品が改良されている
極超音速兵器への対抗手段	極超音速兵器への対抗策の研究には、高出力レーザーやマイクロ波兵器、レールガン、極超音速迎撃機のほか、衛星ナビゲーション信号の受信機や飛行面のコントローラーなどの重要なサブシステムを混乱、過負荷、または無効化するサイバー攻撃などの「ソフトキル」兵器が含まれる
指向性エネルギー兵器	指向性エネルギー兵器（DEW）は、運動エネルギーではなく、電磁気または粒子技術からの集中エネルギーを使用して、ターゲットを劣化または破壊する
寒冷地におけるエネルギー生成と貯蔵	北部および遠隔地のコミュニティは化石燃料に大きく依存しており、一次エネルギーの 70 ～ 80% はディーゼルによって生成されているため、クリーン エネルギーの生成と貯蔵に関する研究が求められている
軍の女性の健康に関する研究	女性は男性に比して特有の身体的および精神的健康問題のリスクがあることから、女性軍人の健康（MWH）に関する研究によって予防および治療ケアを提供し、女性軍人を保護するためのエビデンスに基づく実践の開発を支援する鍵となる
人員シールド	軍の人員には直接的および間接的な火災、即席爆発物、化学兵器および生物兵器、放射線、その他の脅威があり、次世代

新興技術	トレンドカードの概要
	の防護装備は複数の技術と改良された設計に依存している
測位、ナビゲーション、タイミング技術	GPS は偶発的または意図的な干渉に対して脆弱であり、屋内、地下、水中などの特定の場所では一般的に利用できない。そのため、GPS に依存しないソリューションによって将来の民間および軍事プラットフォームの回復力を確保する必要がある
宇宙技術	宇宙を利用したアプリケーションの範囲は、通信やナビゲーションから地球観測、天気予報、セキュリティや諜報活動、正確なタイミングや位置決めを必要とするアプリケーションまで多岐にわたる。しかし、宇宙ゴミ、スペクトルの混雑、通信妨害、複雑なガバナンスにより、宇宙での活動能力が脅かされる可能性がある
水中探知	水中探知技術は、海底インフラの位置特定と監視、海底地形のマッピング、水生生物多様性の研究、潜水艦やその他の物体の識別と追跡などの軍事作戦の支援など、幅広い用途がある

■ 活用方法

トレンドカードは「研究セキュリティのデュー・ディリジェンスの目的で、政府の機密研究分野のリストに追加または置き換えるものではない」とされ、STRA のような活用方法は想定されていないと思われる。

しかし「デュアルユースの新興テクノロジに関して、セキュリティに対するリスクを最小限に抑える」ことに役立てるという記載もあるため、研究コミュニティに対して当該技術がデュアルユースである（リスクがある）ことを周知する意図もあるものと想定される。

3）カナダ研究開発分類（CRDC）

CRDC は連邦政府助成機関とカナダ統計局がカナダの研究開発に関連するデータを収集および配布するために使用される標準分類であり、活動の種類（TOA）、研究分野（FOR）、および社会経済的目的（SEO）の 3 つの主要な区分で構成されている（表 4.1-5）。

表 4.1-5 CRDC の構成

区分	概要
活動の種類（TOA）	① 基礎研究：特定の応用や使用を目的とせずに、現象や観察可能な事実の根底にある基礎に関する新しい知識を主に獲得するために行われる実験的および理論的な研究 ② 応用研究：特定の実用的な目的または目標に向け新しい知識を得るために行われる独自の研究 ③ 実験的開発：研究と実践経験から得られた知識を活用し、新たな製品、材料、ポリシー、行動、展望、または新たなプロセス、システム、サービスを生み出すこと、もしくはそれらの改善
研究分野（FOR）	FOR は以下のようなレベルで研究分野を分類しており、一番下のレベル

<table>
<tr><td></td><td>で 1663 に区分される

<table><tr><th>レベル</th><th>レベル名</th><th>レベルの例</th><th>数</th></tr><tr><td>1</td><td>区分（Division）</td><td>RDF10：自然科学</td><td>6</td></tr><tr><td>2</td><td>グループ（Group）</td><td>RDF101：数学と統計</td><td>43</td></tr><tr><td>3</td><td>クラス（Class）</td><td>RDF10101：純粋数学</td><td>168</td></tr><tr><td>4</td><td>サブクラス（Subclass）</td><td>RDF1010101：代数</td><td>1663</td></tr></table></td></tr>
<tr><td>社会経済的目的（SEO）</td><td>SEO は以下のようなレベルで研究開発活動の目的を分類している

<table><tr><th>レベル</th><th>レベル名</th><th>レベルの例</th><th>数</th></tr><tr><td>1</td><td>区分（Division）</td><td>RDS101：地球の探査と開発</td><td>12</td></tr><tr><td>2</td><td>グループ（Group）</td><td>RD10101：鉱物探査</td><td>85</td></tr></table></td></tr>
</table>

その中でも、研究分野の分類である FOR は、最も大きなレベルの区分（Division）で、RDF10：自然科学、RDF20-21：エンジニアリングとテクノロジー、RDF30：医療、健康、生命工学、RDF40：農学及び獣医学、RDF50：社会科学、RDF60：人文科学と芸術　の 6 分類で構成されている（図 4.1-5）。

区分	グループ	クラス	サブクラス
RDF10：自然科学	RDF101：数学と統計	RDF10101：純粋数学	• RDF1010101：代数 • RDF1010102：数論 • ・・・
		RDF10102：応用数学	• RDF1010201：近似理論と漸近法 • RDF1010202：応用数学における積分方程式 • ・・・
		RD10103：統計	• RDF1010301：一般的な統計手法 • RDF1010302：生物統計学的手法 • ・・・
	RDF102：コンピュータと情報科学	RDF10201：人工知能（AI）	• RDF1020101：適応型エージェント • ・・・
		・・・	• ・・・
	・・・	・・・	• ・・・

図 4.1-5　FOR の構成イメージ

（3）英国

公開情報を基に、英国におけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を抽出した（表 4.1-6）。

表 4.1-6　詳細調査を行う取り組み・リスト

抽出対象	取り組み・リストの名称
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	The UK Science and Technology Framework-five critical technologies
学術・研究領域の体系的な整理区分	Research of Excellence Framework（REF）

以下に表 4.1-6 に掲載した取り組み・リストについての詳細調査結果を示す。

1）The UK Science and Technology Framework-five critical technologies[10]

■　所管

DSIT（科学・イノベーション・技術省）

■　策定（公表）時期

2023 年公表、2024 年 2 月更新

■　背景・目的

The UK Science and Technology Framework は、2023 年に公開された政策文書であり、科学技術に係る資金調達と政策が、産業界、政府、学界等の科学技術コミュニティをどのように支援し、促進するかの長期的なビジョンを示すものであり、10 のストランド（重点事項）で整理されている。

その中で、ストランドの 1 つである「重要技術の開発と展開」では、英国にとっての five critical technologies（5 大重要技術）を指定している。

5 大重要技術自体は、英国政府が発行する包括的な政策文書で、国家安全保障、防衛、開発、外交政策に対する戦略的アプローチを示すものである統合レビュー（Integrated review）に基づいているとされ、2023 年に更新された統合レビューでは「5 大重要技術（AI、工学生物学、未来の通信、半導体、量子技術）は、戦略的優位性を築き、成長の機会を創出し、既存の英国の強みを生かす能力を理由に選ばれた」とされている。

The UK Science and Technology Framework では、各技術に対して既に実行している政策と、今後実施予定の政策の概要が示されている。

[10] https://www.gov.uk/government/publications/uk-science-and-technology-framework/the-uk-science-and-technology-framework-update-on-progress-9-february-2024#developing-and-deploying-critical-technologies

■　関係機関

5 大重要技術を示す The UK Science and Technology Framework のストランドの 1 つである「重要技術の開発と展開」の所管は、DSIT（科学・イノベーション・技術省）となっている。

■　リストの構成

5 大重要技術は英国の戦略的優位性を築き、成長の機会を創出し、既存の英国の強みを生かす能力を理由に選定されたとされ、現在は AI、エンジニアリング生物学、未来の通信、半導体、量子技術が対象となっている（表 4.1-7）。

表 4.1-7　5 大重要技術の区分

技術	当該技術に関する説明
人工知能（AI）	2022 年後半以降の商用 AI 技術の進歩は、世界中で機会と課題をもたらしている。グローバルコラボレーションの最前線に立つ英国は、安全で革新的な AI の開発と使用を活用し、実現するための取り組みを推進するため、2023 年 11 月に初のグローバル AI セーフティサミットを主催した 国家 AI 戦略の実施により、 AI 公共部門のイノベーションへのアプローチと英国の AI ガバナンスへのより広範なアプローチの中心にイノベーションが置かれる
エンジニアリング生物学	エンジニアリング生物学とは、生物学から派生した製品やサービスの設計、スケーリング、商品化であり、これによりセクターを変革したり、既存の製品をより持続可能な方法で生産したりすることができる エンジニアリング生物学は、健康、農業、化学、材料、エネルギーの分野で進歩を促進する機会を提供する。エンジニアリング生物学の応用例としては、食品廃棄物から生産される新しいバイオ燃料、ファッション業界における有害な化学染料の生物学的代替品、新しい治療薬などがある
未来の通信	次世代の通信技術は、デジタル社会、公共サービス、経済のほぼすべての側面を支え、AI や量子など他の重要な技術も可能にするものである（その他技術そのものに関する説明はないが、6G を含む次世代ネットワークに言及している）
半導体	半導体はあらゆる電子機器の中核部品であり、英国の経済、国家安全保障、現代の生活様式を支えている。また、AI や量子技術など他の技術の進歩にも不可欠であり、科学技術における我が国の幅広い戦略的優位性の基礎となっている
量子技術	量子技術は、英国経済、社会、そして地球を守る方法に多大な利益をもたらすと期待されている。 今日、英国には、新製品や新薬の開発につながる量子コンピューターアプリケーション、腫瘍のより正確で迅速な診断を可能にする量子強化画像装置、脳をスキャンして地下インフラを検知するためのより感度の高い量子センサー、より高速で効率的な情報転送を可能にする量子通信ネットワークがある

■　活用方法

5 大重要技術は The UK Science and Technology Framework において科学技術政策上の重点分野を形成しており、今後の政府施策の根拠となっているが、内在するリスクの特定や研究セキュリティに活用するような記載は現状確認できない（表 4.1-8）。

表 4.1-8　5 大重要技術に係る政府施策の例

技術	これまで実施した施策	今後実施する施策
人工知能（AI）	✓ AI の最先端における基礎的な安全性研究を行う世界初の AI Safety Institute（AISI）を設立 ✓ UKRI から AI ハブへの 8,000 万ポンドの資金提供を発表	✓ AISI による AI ガバナンス支援の取り組み ✓ 規制当局の AI 能力を強化するための 1,000 万ポンドのパッケージの開始
エンジニアリング生物学	✓ エンジニアリング生物学の課題と機会についての、産業界からの意見募集 ✓ 「生物学工学に関する国家ビジョン」を発表し、今後 10 年間で生物学工学に 20 億ポンドを投資	✓ エンジニアリング生物学規制当局ネットワークを通じて、ネットワークと連携してサンドボックスを提供
未来の通信	✓ 2023 年 4 月に野心的なワイヤレス インフラストラクチャ戦略を発表 ✓ 英国の 6G ビジョンを公表	✓ UKRI 未来通信技術ミッション基金プロジェクトを開始
半導体	✓ 政府の国家半導体戦略を発表し、2023 年から 2025 年にかけて最大 2 億ポンド、今後 10 年間で最大 10 億ポンドの投資	✓ UKRI を通じて、半導体技術に関する複数のイノベーション ナレッジ センターに 2,100 万ポンドの投資
量子技術	✓ 国家量子戦略を発表し、2024 年から 10 年間で 25 億ポンドを投資し、さらに少なくとも 10 億ポンドの民間投資を生み出す	✓ 2024 年から 2029 年にかけて、UKRI を通じて最大 1 億ポンドの投資を受ける企業を発表し、研究拠点を開発

2）Research of Excellence Framework（REF）[11]

REF は英国の高等教育機関の研究評価を行い、公的資金の配分を決定するための評価を行う取り組みであり、評価単位（UoA)を使用して研究分野を分類しており、現在実施中の REF 2029 では、4 つのメインパネルと 34 のサブパネルで構成されている（表 4.1-9)。

表 4.1-9　REF における評価単位（UoA)による研究分野の分類

メインパネル	サブパネル
メインパネル A - 医学、健康、生命科学	①　臨床医学 ②　公衆衛生、保健サービス、プライマリケア ③　医療関連職種、歯科、看護、薬学 ④　心理学、精神医学、神経科学 ⑤　生物科学 ⑥　農業、食品、獣医学
メインパネル B - 物理科学、工学、数学	①　地球システムと環境科学 ②　化学 ③　物理 ④　数学科学 ⑤　コンピュータサイエンスと情報科学 ⑥　エンジニアリング
メインパネル C - 社会科学	①　建築、建築環境、計画 ②　地理学と環境学 ③　考古学 ④　経済学と計量経済学 ⑤　ビジネスと経営学 ⑥　法 ⑦　政治学と国際学 ⑧　社会福祉と社会政策 ⑨　社会学 ⑩　人類学と開発研究 ⑪　教育 ⑫　スポーツと運動科学、レジャーと観光
メインパネル D - 芸術と人文科学	①　地域研究 ②　現代言語と言語学 ③　英語言語と文学 ④　歴史 ⑤　クラシック ⑥　哲学 ⑦　神学と宗教学 ⑧　芸術とデザイン：歴史、実践、理論 ⑨　音楽、演劇、ダンス、舞台芸術、映画・スクリーン研究 ⑩　コミュニケーション、文化・メディア研究、図書館・情報管理

[11] https://2029.ref.ac.uk/

（4）EU

公開情報を基に、EU におけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を抽出した（表 4.1-10）。

表 4.1-10　詳細調査を行う取り組み・リスト

抽出対象	取り組み・リストの名称
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	Critical Technology Areas
学術・研究領域の体系的な整理区分	CERIF

以下に表 4.1-10 に掲載した取り組み・リストについての詳細調査結果を示す。

1）Critical Technology Areas[12]

■　所管

欧州委員会

■　策定（公表）時期

2023 年 10 月公表

■　背景・目的

欧州委員会は、2023 年 6 月に初の包括的な経済安全保障戦略を公表した。その中で、2023 年 10 月に重要な技術（Critical Technology Areas）10 分野に関してリスク評価を行う勧告を発表。さらに、最も重要で差し迫ったリスクとして 4 つの技術を特定、2023 年末までに委員会は加盟国と共に集団的リスク評価を実施すべきと勧告した。

リスク低減策については、現時点では具体的には決定しておらず、リスク評価後に加盟国と協議すると述べるにとどめた。（2024 年春にリスク評価の結果新たな低減策を講じる可能性があるとしていたが、調査時点では確認できない）

■　関係機関

・　欧州機関

・　加盟国の所管機関

■　リストの構成

重要な技術（Critical Technology Areas）10 分野のうち、さらに、最も重要で差し迫ったリスクとして 4 つの技術を特定している（表 4.1-11）。

[12] https://www.jetro.go.jp/biznews/2023/10/997ead20af218775.html

表 4.1-11　Critical Technology Areas で特定された 10 分野

区分	技術	詳細
最も厳重な対応を要し、差し迫ったリスクを有する可能性が高い技術	先端半導体技術	マイクロエレクトロニクス、フォトニクス、高周波チップ、半導体製造装置
	人工知能（AI）技術	ハイパフォーマンス コンピューティング、クラウドおよびエッジ コンピューティング、データ分析、コンピューター ビジョン、言語処理、オブジェクト認識
	量子技術	量子コンピューティング、量子暗号、量子通信、量子センシング、レーダー
	バイオ技術	遺伝子組み換え技術、新しいゲノム技術、遺伝子駆動、合成生物学
その他の重要技術	先端接続性、ナビゲーション、デジタル技術	―
	先端センサー技術	―
	宇宙、推進技術	―
	エネルギー技術	―
	ロボット工学、自律システム	―
	先端材料、製造、リサイクル技術	―

■　活用方法

欧州委員会は、リスク低減策については現時点では具体的には決定しておらず、リスク評価後に加盟国と協議すると述べるにとどめられている（2024 年春にリスク評価の結果低減策を講じる可能性があるとしていたが、調査時点では確認できない）。

2）CERIF[13,14]

CERIF は 1988 年に開発された、欧州の研究プロジェクトに関する情報データベースに共通して使用できるデータフォーマットであり、研究分野の分類スキームを有している。

最も大きな分類で人文学、社会科学、自然科学・数学、バイオ医療科学、技術科学の 5 分類からなる（図 4.1-6）。

[13] https://cordis.europa.eu/article/id/8260-cerif-common-european-research-information-format

[14] https://www.aris-rs.si/en/gradivo/sifranti/inc/CERIF.pdf

HUMANITIES H 000	Social Sciences S 000
H100 Documentation, information, library science, archivistics	S100 History and philosophy of the social sciences
H105 Bibliography	S110 Juridical sciences
H110 Paleography, bibliology, epigraphy, papyrology	S111 Administrative law
Philosophy H 001	S112 Human rights
H120 Systematic philosophy, ethics, aesthetics, metaphysics, epistemology, ideology	S114 Comparative law
H125 Philosophical anthropology	S115 Philosophy and theory of law
H130 History of philosophy	S120 Environmental law
H135 Phenomenology	S121 Juvenile law
H140 Philosophical logic	S122 Media law
H150 Philosophy of special sciences	S123 Informatics law
H155 Moral science	S124 Patents, copyrights, trademarks
Theology H 002	S130 Civil law: persons, family, marriage contract, successions, gifts, property, obligations, guarantees
H160 General, systematic and practical Christian theology	S136 Transportation law
H165 Canon law	S137 Insurance law
H170 Bible	S140 Public law
H180 History of the Christian church	S141 Fiscal law
H190 Non-Christian religions	S142 Judicial law
History and Arts H 003	S143 Social law
H200 Theory of history	S144 Industrial and commercial law
H210 Ancient history	S145 Notarial law
H220 Medieval history	S146 Labour law
H230 Modern history (up to circa 1800)	S148 Constitutional law
H240 Contemporary history (circa 1800 to 1914)	S149 Criminal law, criminal proceedings
H250 Contemporary history (since 1914)	S150 International private and public law
H260 History of science	S151 Aerial, maritime and space law
H270 Social and economic history	S155 European law
H271 Political history	S160 Criminology
H280 Local and regional history, historical geography since the Middle Ages	S170 Political and administrative sciences
H290 Colonial history	S175 Polemology
H300 History of law	

図 4.1-6　CERIF における共通研究分類スキームの例

（5）豪州

公開情報を基に、豪州におけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を抽出した（表 4.1-12）。

表 4.1-12　詳細調査を行う取り組み・リスト

抽出対象	取り組み・リストの名称
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	List of Critical Technologies in the National Interest
学術・研究領域の体系的な整理区分	オーストラリア・ニュージーランド標準研究分類（ANZSRC）

以下に表 4.1-12 に掲載した取り組み・リストについての詳細調査結果を示す。

1）List of Critical Technologies in the National Interest[15,16,17,18]

■　所管

産業科学資源省（DISR）：クリティカル・テクノロジーハブ

■　策定（公表）時期

2021 年公表、2023 年 5 月更新

■　背景・目的

List of Critical Technologies in the National Interest は、2021 年 11 月に首相・内閣府（PM&C）から公表された「重要技術のための青写真と行動計画（Blueprint and Action Plan for Critical Technologies）」に含まれる重要技術のリストである。

その後、首相・内閣府で当計画を所管していたクリティカル・テクノロジー政策調整室は、2022 年 7 月にクリティカル・テクノロジーハブとして産業科学資源省に移管され、2023 年 5 月に「国益にかかわる重要技術リスト（List of Critical Technologies in the National Interest）」及び「重要技術に関する声明（Critical Technologies Statement）」として発出された。

重要技術（Critical Technology）とは、「経済的繁栄、国家安全保障、社会的結束といった豪州の国益に影響を与える可能性のある技術」であるとしており、現在は AI、量子、バイオテクノロジー等の 7 分野と、その詳細（技術やアプリケーションの例）が特定されている。リストは、政府による重点的な投資領域として活用されている一方で、知的財産の盗難等のリスクにも言及している。

---

15 https://www.pmc.gov.au/news/launch-blueprint-and-action-plan-critical-technologies

16 https://webarchive.nla.gov.au/awa/20221209151937/https://www.industry.gov.au/publications/action-plan-critical-technologies

17 https://www.industry.gov.au/publications/list-critical-technologies-national-interest

18 https://www.industry.gov.au/publications/critical-technologies-statement

■ 関係機関

・ 産業科学資源省（DISR）：クリティカル・テクノロジーハブ（2022 年 7 月に首相・内閣府（PM&C）より移管）

・ 首相・内閣府（PM&C）（当初の計画を公表）

■ リストの構成

現在は AI、量子、バイオテクノロジー等の 7 分野とその詳細（技術やアプリケーションの例）が記載されているが、詳細はあくまで当該分野における技術やアプリケーションの例であり、網羅的なものではないとしている（表 4.1-13）。

表 4.1-13 List of Critical Technologies in the National Interest の構成

技術分野	詳細（技術やアプリケーションの例）
高度な製造および材料技術	✓ 3D プリントを含む付加製造 ✓ 重要な鉱物の抽出と処理 ✓ 先進複合材料 ✓ 高仕様の加工プロセス ✓ 半導体および高度な集積回路の設計と製造
AI テクノロジー	✓ ニューラルネットワークやディープラーニングを含む機械学習 ✓ AI アルゴリズムとハードウェアアクセラレータ ✓ 音声とテキストの認識、分析、生成を含む自然言語処理
高度な情報通信技術	✓ 高度なデータ分析 ✓ 高度な光通信 ✓ 5G や 6G を含む高度な無線周波数通信 ✓ 高性能コンピューティング ✓ 保護的なサイバーセキュリティ技術 ✓ 仮想世界
量子技術	✓ 量子コンピューティング ✓ 耐量子暗号 ✓ 量子通信 ✓ 量子センサー
自律システム、ロボット工学、ポジショニング、タイミング、センシング	✓ 高度なロボット工学 ✓ 自律システム運用技術 ✓ ドローン、群集ロボット、協働ロボット ✓ 高度な画像技術 ✓ 高度なセンサー技術 ✓ 衛星および測位技術 ✓ 推進、極超音速、誘導システムなどの高度な航空宇宙技術 ✓ 潜水艦の推進や廃棄物管理を含む核技術

技術分野	詳細（技術やアプリケーションの例）
バイオテクノロジー	✓ 合成生物学（生物学的製造を含む） ✓ 神経工学と脳コンピュータインターフェース ✓ ゲノムと遺伝子の配列解析と分析 ✓ ワクチンと医療対策 ✓ 核、抗ウイルス、抗生物質を含む新薬
クリーンエネルギー生成および貯蔵技術	✓ 排出削減技術 ✓ 高度なエネルギー貯蔵技術 ✓ 指向性エネルギー技術 ✓ 大規模再生可能エネルギー発電 ✓ バイオ燃料を含む低排出代替燃料 ✓ 小規模分散型エネルギーハーベスティング

■ 活用方法

リスト及び併せて公表された「重要な技術に関する声明」では、「重要技術セキュリティ対策を提供する」旨が記載されているのみであり、具体的な活用方法は確認できていない。

しかし、政府の主要な資金提供機関である豪州研究会議（ARC）は、「重要技術に該当する研究の助成申請にはリスク要因の検討を行う」旨述べており、デュー・ディリジェンスの対象となる研究分野のリストとしても活用されていると想定される[19,20]。

＜ARC の HP における重要技術への言及＞

- ✓ ARC は、NCGP やその他のプログラムを通じた資金申請に関連する可能性のある主なリスクを特定する。
- ✓ 申請において**「重要技術の青写真」*1 に概説されている技術が特定された場合**、ARC は**他のリスクが存在する可能性があるかどうかを検討する**。リスク要因には次のものが含まれる。
  - ・ 現在または最近の外国からの財政支援、教育、研究関連の活動。
  - ・ 現在または最近、外国人材育成プログラムに参加しているか、外国の大学に対する義務を負っているか
  - ・ 外国政府、軍隊、警察、諜報機関との現在または最近の関係
  - ・ オーストラリアが制裁を課している政権、個人、または組織との最近の関係
- ✓ 評価では、申請書に提供された情報と研究者の RMS プロファイル*2 が考慮される。外務貿易省（DFAT）の制裁制度や統合リストなどのオープンソース情報も考慮される。

*1：「重要技術の青写真」は、List of Critical Technologies in the National Interest の前身である、2020 年に公表された「重要技術のための青写真と行動計画（Blueprint and Action Plan for Critical Technologies）」のことを指す

*2：RMS プロファイルとは、ARC の行う資金提供プログラムにおいて申請、評価やプロセス管理に使用される研究管理システム（RMS)における研究者の情報である

[19] https://www.arc.gov.au/funding-research/research-security

[20] https://www.arc.gov.au/manage-your-grant/research-management-system-rms-information

2）オーストラリア・ニュージーランド標準研究分類 (ANZSRC)[21]

オーストラリアおよびニュージーランド標準研究分類（ANZSRC）は、オーストラリアとニュージーランドにおける研究および実験開発（R&D）統計の測定と分析に使用するための標準分類であり、CRDC と同様に活動の種類（TOA）、研究分野（FOR）、および社会経済的目的（SEO）の 3 つの主要な区分で構成されている（表 4.1-14）。

ANZSRC とカナダの CRDC には共通した構成要素が見られるが、これは OECD のフラスカティ・マニュアルを参考としているためと思われる。

フラスカティ・マニュアルは経済協力開発機構（OECD）が策定した、研究開発（R&D）に関するデータ収集と報告のための国際的な標準ガイドラインであり、1963 年に初版が発行された以降、科学技術政策の立案や R&D 活動の統計収集における世界的な基準となっている[22]。

表 4.1-14　ANZSRC の構成

<table>
<tr><th>区分</th><th>概要</th></tr>
<tr><td>活動の種類（TOA）</td><td>① 純粋な基礎研究：長期的な経済的・社会的利益を追求することなく、また、その成果を実用的な問題に応用したり、応用を担当する部門に移転したりする努力をすることなく、知識の発展のために行われる基礎研究
② 戦略的基礎研究 : 実用的な発見を期待して、特定の広範な分野に向けられた新しい知識を獲得するために行われる実験的・理論的研究
③ 応用研究：特定の実用的な目的または目標に向け新しい知識を得るために行われる独自の研究
④ 実験的開発：研究と実践経験から得られた知識を活用し、新たな製品、材料、ポリシー、行動、展望、または新たなプロセス、システム、サービスを生み出すこと、もしくはそれらの改善</td></tr>
<tr><td>研究分野（FOR）</td><td>FOR は以下のようなレベルで研究分野を分類しており、一番下のレベルで 1732 に区分される

<table>
<tr><th>レベル</th><th>レベル名</th><th>レベルの例</th><th>数</th></tr>
<tr><td>1</td><td>区分（Division）</td><td>31：生物科学</td><td>23</td></tr>
<tr><td>2</td><td>グループ（Group）</td><td>3103：エコロジー</td><td>190</td></tr>
<tr><td>3</td><td>分野（Field）</td><td>310301：行動生態学</td><td>1732</td></tr>
</table>
</td></tr>
<tr><td>社会経済的目的（SEO）</td><td>SEO は以下のようなレベルで研究開発活動の目的を分類している

<table>
<tr><th>レベル</th><th>レベル名</th><th>レベルの例</th><th>数</th></tr>
<tr><td>1</td><td>区分（Division）</td><td>20：健康</td><td>19</td></tr>
<tr><td>2</td><td>グループ（Group）</td><td>2003：健康及びサポートサービスの提供</td><td>256</td></tr>
<tr><td>3</td><td>目的（Objective）</td><td>200307：看護</td><td>822</td></tr>
</table>
</td></tr>
</table>

[21] https://www.abs.gov.au/statistics/classifications/australian-and-new-zealand-standard-research-classification-anzsrc/latest-release

[22] https://www.oecd.org/en/publications/frascati-manual-2015_9789264239012-en.html

（6）韓国

公開情報を基に、韓国におけるリスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト、及び学術・研究領域の体系的な整理区分を抽出した（表 4.1-15）。

表 4.1-15　詳細調査を行う取り組み・リスト

抽出対象	取り組み・リストの名称
リスクに晒されている研究領域の特定・情報共有に係る取り組み・リスト	国家戦略技術 [23]
学術・研究領域の体系的な整理区分	国家科学技術標準分類体系

以下に表 4.1-15 に掲載した取り組み・リストについての詳細調査結果を示す。

1）国家戦略技術 [24]

■　所管

科学技術情報通信部（MSIT）

■　策定（公表）時期

2024 年 1 月（根拠法の施行は 2023 年 9 月）

■　背景・目的

国家戦略技術は「国家戦略技術育成に関する特別法」を根拠として定められる技術分野である。同法は、国家的に重要性が高い国家戦略技術を育成して未来新産業の発展を促進し、科学技術主権を確立することにより、国民経済発展と国家安全保障に貢献することを目的として制定された。

国家戦略技術とは、外交・安全保障側面の戦略的重要性が認められ、国民経済及び関連産業に及ぼす影響が大きく、新技術・新産業創出など未来革新の基盤となる技術とされており、当該技術分野に関する研究開発事業は「国家戦略技術研究開発事業」として政府により資金配分がなされる。

同法では、国家戦略技術の情報保護及びセキュリティの施策についても規定されている。

■　関係機関

- 科学技術情報通信部（MSIT）
- 国家戦略技術育成に関する特別法では、国家戦略技術を研究・管理・保有したり、関連事業を運営する者（技術育成主体）として、以下のような機関が指定されている。

---

[23] 韓国政府による英語のプレスリリースでは Critical and Emerging Technologies（重要新興技術）と記載されている場合があるが、根拠文書では국가전략기술（国家戦略技術）となっている

[24] https://www.law.go.kr/LSW/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%A4%91%EC%9A%94+%EC%B2%A8%EB%8B%A8%EA%B8%B0%EC%88%A0+%EA%B0%9C%EB%B0%9C%EC%9D%84+%EC%9C%84%ED%95%9C+%ED%8A%B9%EB%B3%84%EB%B2%95#J27:0

✓ 「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」により設立された科学技術分野政府出資研究機関 ✓ 「特定研究機関育成法」 第 2 条による特定研究機関 ✓ 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 ✓ 「高等教育法」 第 2 条による学校、同法 第 29 条による大学院及び同法 第 30 条による大学院大学　等

■　リストの構成

国家戦略技術は、科学技術情報通信部長官が関係中央行政機関の長と協議した後、科学技術諮問会議の審議を経て指定されることとなっており、現在は半導体、二次電池、次世代原子力、バイオテクノロジー等の計 12 分野 50 技術が指定されている（表 4.1-16）。

表 4.1-16　国家戦略技術の区分

分野	技術
1) 半導体・ディスプレイ	(1) 完全統合型抵抗変化メモリ(ReRAM) (2) 高性能・低電力 AI 半導体 (3) 先端パッケージング (4) 電源管理集積回路(PMIC) (5) 次世代高性能センサー (6) 無機ディスプレイ (7) 自由形状(Free-form)ディスプレイ (8) 半導体・ディスプレイの材料・部品・装置
2) 二次電池	(9) リチウムイオン電池・そのコア部品 (10) 次世代二次電池部品・セル (11) 二次電池のモジュール・システム (12) 二次電池のリユース・リサイクル
3) 先端モビリティ	(13) 自動運転 (14) 都市航空交通(UAM) (15) 電気・水素自動車
4) 次世代原子力	(16) 小型モジュール炉(SMR) (17) 先進的原子力システム・廃棄物管理
5) 先端バイオテクノロジー	(18) 合成生物学 (19) 遺伝子・細胞治療 (20) 感染症のワクチン・治療薬 (21) 健康データの分析・利用

6）航空宇宙・海洋技術	(22) 段階的燃焼サイクルを用いた大規模エンジン (23) 宇宙観測・センシング (24) 月面着陸・探査 (25) 航空機の先端ガスタービン・エンジン・部品 (26) 海洋資源探査
7）水素	(27) 電気分解による水素製造 (28) 水素貯蔵・輸送 (29) 水素燃料電池・エネルギー生産
8）サイバーセキュリティ	(30) データ・AI セキュリティ (31) デジタル上の弱点の分析・対応(サプライチェーンセキュリティ) (32) ネットワーク・クラウドセキュリティ (33) 産業工程向けの仮想コンバージェンスセキュリティ
9）AI	(34) 先端学習・AI インフラ (35) 先端 AI モデリング・意思決定(認知・判断・推論) (36) 産業用途・イノベーションのための AI (37) 安全で信頼に値する AI

■ 活用方法

国家戦略技術は、「国家戦略技術育成に関する特別法」に定められている国による研究開発事業の実施や、その保護・育成に係る諸施策の対象となり、事業におけるセキュリティの強化や情報提供を研究開発実施主体等に求めることとなっている（表 4.1-17）。

表 4.1-17 国家戦略技術に対して実施される施策の例

国家戦略技術の開発・育成に関する施策	国家戦略技術の技術情報の保護に関する施策
✓ 国家戦略技術の開発･育成に関する研究開発プログラムを「国家戦略技術研究開発事業」として指定し、資金提供を実施 ✓ 国家戦略技術の開発・移転・拡散及び産業活性化等のために国内外の標準化に関連した支援活動等の実施 ✓ 国家および地方自治体による、国家戦略技術分野の人材養成及び確保等に関する施策の実施 等	**【セキュリティの強化】** 政府機関の支援によって国家戦略技術を開発する資金提供プログラムである「国家戦略技術研究開発課題」は、「国家研究開発革新法」 第 21 条第 2 項による「セキュリティ課題」（技術情報が流出した場合の技術・財産・国家安全保障的なリスクの高いプログラム）に指定することができ、より厳しいセキュリティ管理措置を研究開発実施主体に対して課すことができる **【情報提供】** 国家戦略技術の関連事業を運営する主体である「技術育成主体」は、政府から情報提供を求められた場合、以下の情報を提供しなければならない（施行令 26 条） ✓ 参加人材に関する情報 ✓ 研究成果 ✓ 国家戦略技術の開発・取得・維持・活用・処分と直接的な関連性がある経営情報

2）国家科学技術標準分類体系

国家科学技術標準分類体系は、科学技術基本法第 27 条を法的根拠とする科学技術の分類であり、科学技術情報通信部及びその専門機関である国家科学技術評価企画院が所管している。科学技術関連情報・人材・研究開発事業等を効率的に管理するために作成されたとされる（図 4.1-7）。

最も大きな分類 NA　数学、NB　物理学等は計 22 分類となっている。

大分類	細目
NA 数学 (Mathematics)	NA01 代数学（Algebra） NA02 解析学（Analysis） NA03 位相数学(Topology) NA04 幾何学（Geometry） NA05 応用数学 (Applied Mathematics) NA06 離散数学/情報数学 (Discrete / Information Mathematics)· NA07 統計理論 (Statistical Theory) NA08 統計方法論·計算(Statistical Methodology · Computing) . . .
NB 物理学（Physics）	NB01 素粒子物理学/場の理論 (Particle Physics / Field Theory) NB02 統計物理(Statistical Physics) NB03 原子核物理学(Nuclear Physics) NB04 流体·プラズマ物理学(Fluid · Plasma Physics) NB05 光学·量子電子学（Optics·Quantum Electronics） NB06 凝集系物質学（Condensed Matter Physics） . . .

大分類	細目
ND 地球科学 (Earth Science (Earth/Atmosphere/Marine/Astronomy))	ND01 地質科学（Geological Science） ND02 地球物理学(Geophysics) ND03 地球化学(Geochemistry) ND04 大気科学（Atmospheric Science） ND05 気象学（Meteorological science ） ND06 気候科学 (Climate Science) ND07 自然災害分析/予測 (Nature Disaster Analysis / Forecast) ND08 海洋科学（Marine Sciences） . . .
LA ライフサイエンス（Life Science）	LA01 分子細胞生物学（Molecular Cell Biology） LA02 遺伝学·ゲノミクス(Genetics · Genomics) LA03 発生/神経生物学 (Developmental/Neuronal Biology) LA04 免疫学/生理学 (Immunology / Physiology) LA05 分類/生態学/環境生物学 (Phylogenetics / Ecology / Environmentalbiology) . . .

図 4.1-7　国家科学技術標準分類体系における研究分野の分類の例

4.1.2 テーマ 2：デュー・ディリジェンスの実施・リスクのある活動の領域の特定

（1）米国

米国においては、NSPM-33（米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」が 2021 年に発出され、連邦政府の資金提供を受けた研究開発の研究インテグリティ・セキュリティの保護のための国家的対応の指示がなされた。

NSPM-33 の中では研究開発体制に大きな影響を与える個人の潜在的な利益相反および責務相反に関連する情報の開示要件を強化・標準化するとされ、翌 2021 年には 2021 年国防権限法（NDAA 2021）の成立により、すべての連邦研究機関（資金配分機関）が申請プロセスの一環として現在及び未決（pending）の支援についての情報開示を研究者から求めること等が義務付けられた。

そして 2022 年には NSPM-33 実施ガイダンスが発出され、米国政府の省庁・資金提供機関が、NSPM-33 に対応するための取り組みにおいて適用されるべき一般的な指導事項が示された。

上記政策動向を踏まえ公開情報を基に、米国において政府、資金提供機関、研究開発実施主体によって実施されている研究セキュリティ・インテグリティに係るデュー・ディリジェンスの取り組み・ガイドライン等を抽出した（表 4.1-18）。

表 4.1-18　詳細調査を行う取り組み・ガイドライン

取り組み主体	デュー・ディリジェンスに係る取り組み・ガイドライン
政府	NSPM-33 実施ガイダンス
資金提供機関	・ CFIP（対外国干渉プログラム） ・ TRUST ・ NIH Dicision Matrix
研究開発実施主体	ヒューストン大学における取り組み

以下に表 4.1-18 に掲載した取り組み・ガイドラインについての詳細調査結果を示す。

1）NSPM-33 実施ガイダンス

■ 概要

NSPM-33 実装ガイダンスは、米国政府の支援する研究開発事業の参加者に対して情報の開示を要求し、利益相反・責務相反の有無を判断する標準的な方針とプロセスを確立することを目的としており、その中でテーマ 2 では「1.情報開示の要件と標準化」を主に対象として調査した[25]（表 4.1-19）。

[25] https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

表 4.1-19　NSPM-33 実施ガイダンスの概要

項目	概要
所管	NSTC（研究環境に関する NSTC 合同委員会 - 研究セキュリティ小委員会）
公表（更新）時期	2022 年 1 月公表
背景・目的	・ 2021 年に NSPM-33 が発出され、政府の支援する研究開発を外国の干渉から保護するための行動として、研究資金を提供する連邦省庁の長等に対する要求事項が指示された ・ その中で、政府の支援する研究開発事業の参加者に対して情報の開示を要求し、利益相反・責務相反の有無を判断する方針とプロセスを確立することが求められた ・ 本文所の目的は NSPM - 33 の実施に関する指針を連邦省庁に対して提供することであり、各機関が適用すべき一般的なガイダンス（general guidance）と、NSPM-33 で取り上げられた 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の結果、4. 情報の共有、5. 研究セキュリティプログラム）におけるより詳細なガイダンスを提供している ・ テーマ 2 の調査では「1.情報開示の要件と標準化」を主な対象としている
デュー・ディリジェンス[26]の実施主体	・ 米国政府の資金提供機関
デュー・ディリジェンスの対象	・ 連邦政府が資金を提供する研究開発事業への参加者（研究開発実施主体）
デュー・ディリジェンスの実施タイミング	・ 研究開発事業への申請時、助成決定後

■　実施プロセス

NSPM-33 実施ガイダンスの「1.情報開示の要件と標準化」は、資金提供機関が資金提供プログラムへの参加を希望する者に対して開示要件（誰が何を開示するか、除外事由等）とプロセス（更新、訂正、証明、裏付け文書の提供など：詳細は資金提供機関が定める）を示すものであり、デュー・ディリジェンスを実施するプロセスは定めてはいない。

■　確認観点

NSPM-33 実施ガイダンスでは、研究開発事業における参加者の役割（ティア）に応じて、全ての研究機関に求める開示すべき情報として所属団体・雇用、役職・任命、外国政府の人材リクルートプログラム、支援の状況が挙げられている（表 4.1-20）。

[26] NSPM-33 及び実装ガイダンスでは、情報開示（disclosure）という用語を用いており、デュー・ディリジェンスという表現は用いていない

表 4.1-20　参加者の役割に応じ全ての研究機関に開示を求める情報の種類

開示すべき情報 / 参加者の役割	所属団体／雇用	役職／任命	外国政府主催の人材リクルート・プログラム	現在もしくは申請中の支援／その他サポート
ティア 1 ・　研究責任者及びその他の上級／主要職員 ・　プログラム役員 ・　学内研究者*2	Y	Y	Y	Y
ティア 2 ・　査読者 ・　諮問委員会／メンバーパネル	Y	Y	Y	N

また、ティア 1 の個人が開示すべき活動の情報として、個人情報及び職務上の情報の開示に関する詳細、及びプロジェクトに関して開示すべき情報が定められている（表 4.1-21、表 4.1-22）。

表 4.1-21　ティア 1 の個人が開示すべき活動の情報①

開示すべき活動の種類	略歴	現在及び保留中／その他の支援	年次プロジェクト報告書	受賞後の情報提供条件
個人情報				
専門職としての準備（教育学位など）	✓			
所属団体	✓			
報酬の有無を問わず、また常勤、非常勤、自発的であるか否かを問わず、学術的、専門的、または組織的な任命	✓			
個人の任命から外れる有償のコンサルティング		✓	✓	✓
研究資金情報				
現在および保留中の支援： 現在進行中の研究開発プロジェクト：現在検討中のすべての研究開発プロジェクト。また、その支援が直接的な金銭的拠出であるか、現物拠出（オフィス／研究室のスペース、設備、備品、従業員など）であるかにかかわらず、現在検討中のすべての研究開発プロジェクト。		✓	✓	✓

開示すべき活動の種類	略歴	現在及び保留中／その他の支援	年次プロジェクト報告書	受賞後の情報提供条件
研究資金情報				
外国政府が後援する人材採用プログラムを含む、外国政府、団体、または事業体が後援するプログラムへの現在または申請中の参加または申請	✓ （適切な配置は契約に依存する場合がある）			
提案中のプロジェクト／提案に使用することを目的としない現物寄付		✓	✓	✓
自機関以外から資金提供を受けている客員研究員		✓	✓	✓
所属機関以外から資金提供を受けている学生およびポスドク研究者		✓	✓	✓
時間的拘束を伴う研究活動を行うために、所属機関以外の組織から支援/支払いを受けた旅費		✓	✓	✓
開示された情報が正確、最新かつ完全であることの本人による証明書		✓	✓	✓

表 4.1-22　ティア 1 の個人が開示すべき活動の情報②

開示すべき活動の種類	設備その他リソース	その他
プロジェクト情報		
研究活動を支援する現物寄付（提案中のプロジェクト／提案に使用されるもの	✓	
プライベート・エクイティ、ベンチャー、その他資本による資金調達		✓
裏付け資料（契約書、助成金、その他の契約書など）		✓

■　参照している情報ソース

前記のとおり、デュー・ディリジェンスを実施するプロセスを定めているものではないため、デュー・ディリジェンスに使用する公開情報等の情報ソースは確認できなかった。

2）CFIP（対外国干渉プログラム）[27]

CFIP は DARPA の研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を支援するために、外国からの不当な影響を防止するためのプログラムであり、DARPA の助成金の授与前（Pre-Award）に重点を置いて申請者のリスク評価を実施するものである（表 4.1-23）。

表 4.1-23　CFIP の概要

項目	概要
所管	DARPA（国防高等研究計画局）
公表（更新）時期	2021 年 9 月公表
背景・目的	・　CFIP は、DARPA の研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を支援するために、外国からの不当な影響を防止するためのプログラムである ・　SF-424＊1 で提供された情報や公的に入手可能な情報を利用してリスクを評価して、提案者に対し、「低」から「非常に高い」までのリスク評価を実施する ・　主に助成金の授与前（Pre-Award）に重点を置き、助成後（Post-Award）には運用されないことや、研究の制限や拒否を目的とせず、スポンサー機関に利益相反や責務の相反リスクの緩和策を講じる機会を提供するとしている
デュー・ディリジェンス[28]の実施主体	・　DARPA CFIP チーム（CFIP チームは、DARPA の MSO - SID（ミッションサービスオフィスのセキュリティ及びインテリジェンス局）のアナリスト 2 名で構成され、革新的自動化ツールを活用して、審査プロセスをサポートし、リスク緩和レビューを実施するとされている）
デュー・ディリジェンスの対象	・　基礎研究助成金または協力契約交渉に選ばれた提案者（特にシニア／主要研究者）
デュー・ディリジェンスの実施タイミング	・　助成金の授与前の審査時

■　実施プロセス

CFIP は NSPM-33 と同様に、研究者によるデュー・ディリジェンスの実施プロセスを示すものではないが、DARPA 内部における CFIP レビュー結果に基づくリスク評価レビュープロセスを公開している（図 4.1-8）。

---

[27] https://www.darpa.mil/work-with-us/contrct-management

[28] NSPM-33 及び実装ガイダンスでは、情報開示（disclosure）という用語を用いており、デュー・ディリジェンスという表現は用いていない

リスク評価レビュープロセスでは、まず契約管理オフィス（CMO）はリスク評価を開示し、大学に緩和策を交渉する機会を提供し、大学が緩和策を採用しない場合、または緩和策がリスクレベルを下げるのに失敗した場合、科学審査担当者（SRO）が助成推薦を DARPA 副所長に送付して副所長がリスクを受け入れるか否かを判断こととなる。

そして副所長がリスクを受け入れられないと判断して、SRO が緩和策が不十分である、または代替の主要研究者が適切でないと判断した場合、助成は授与されず、リスクが受け入れられた場合は、リスク緩和計画が提供され、主要研究者が変更される。

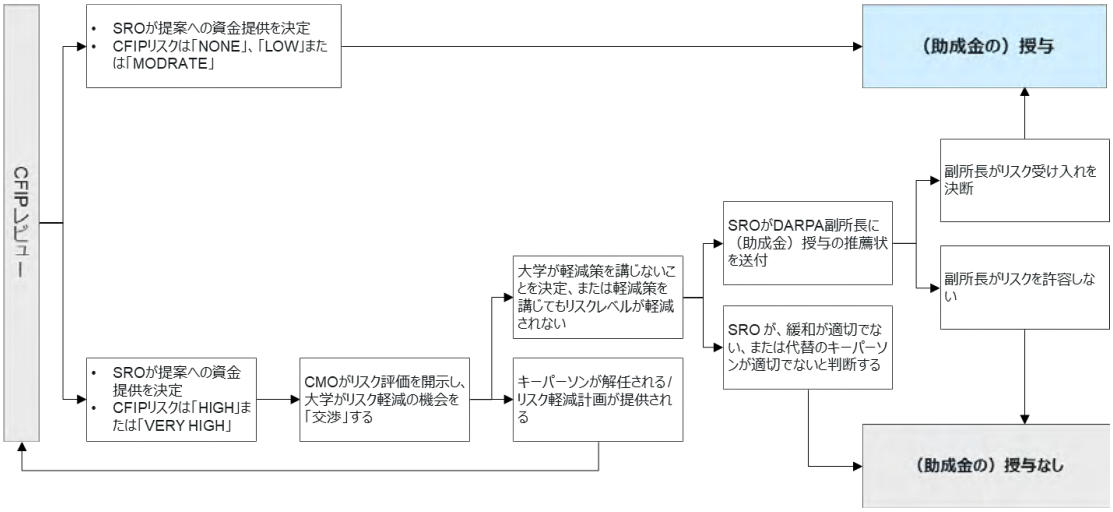


図 4.1-8　CFIP のリスク評価レビュープロセス

■　確認観点

CFIP では、①外国タレントプログラムへの参加、②制限対象リスト（Denied Entity Lists）に掲載された機関や個人との関係、③外国政府または外国政府関連機関からの資金提供、④高リスクな外国政府またはその関連機関との関係 の 4 要因をもって不当な外国の影響に関連する利益相反・責務相反リスクを評価するとして、各要因のリスクレベルの指標を公開している（表 4.1-24）。

表 4.1-24　各要因のリスクレベルの指標

リスクレベル・要因	外国タレントプログラムへの参加	制限対象リスト（Denied Entity Lists）に掲載された機関や個人との関係	外国政府または外国政府関連機関からの資金提供	高リスクな外国政府またはその関連機関との関係
VERY HIGH	戦略的競合国または米国の技術を不正移転の標的としてきた歴史を持つ国（CWHTUST）の政府が運営する外国人材プログラムに積極的(継続的)に参加していることを示す指標	米国政府によって特定された拒否された企業または人物リスト、またはEO13959、またはそれに続く同様の発行物に記載されている企業と、積極的（継続的）に提携していることを示す指標	戦略的競合相手または CWHTUST の外国政府または外国政府関連事業体から積極的（継続的）に直接資金提供を受けていることを示す指標	リスクの高い外国政府、または外国政府関連の機関や団体と積極的(継続的)に提携 していることを示す指標
HIGH	戦略的競合相手または CWHTUST の政府が運営する外国人人材育成プログラムに過去に参加したことがあるが、そのプログラムとの職業的関係が継続していることを示す指標	米国政府が特定した拒否企業・人物リスト、EO13959、またはそれに続く類似の発行物に記載されている企業と、過去に提携していた、または最近（**過去 4 年以内**）に複数回提携していたことを示す指標	外国政府、または戦略的競合相手や CWHTUST の外国政府関連事業体から直接資金提供を受けている履歴／パターンの指標	高リスクの外国政府、または外国政府関連の機関や団体と、複数の活発な(継続的な)直接的関係 が ある ことを示す指標
MODERATE	CWHTUST と技術共有協定を結んでいる米国の同盟国政府が運営する外国人材プログラムに積極的(継続的)に参加していることを示す指標	米国政府が拒否した企業リストまたは EO13959、あるいはそれに続く類似の発行物で特定された企業と、過去に複数の関連があったことを示す指標	戦略的競合相手または CWHTUST の外国政府または外国政府関連団体から、過去に継続的でない散発的な資金提供を受けたことを示す指標	リスクの高い外国政府、または外国政府関連の機関や団体と過去に何度も直接的な関わりがあったことを示す指標
LOW	外国人タレント・プログラムに参加していない	米国政府が特定した拒否企業・人物リスト、EO13959 またはそれに続く類似の発行物に記載されている企業と、過去または現在、関連 4 または所属していることを示す指標はない	戦略的競合相手または CWHTUST の外国政府または外国政府関連団体から過去に資金提供を受けていたことを示す指標はない	高リスクの外国政府、または外国政府関連の機関や団体と の関連性または提携を示す指標はない

■　参照している情報ソース

CFIP におけるリスク評価の実施者はあくまで SF-424 で提供された情報と公開情報を基にリスク評価を実施するとしているが、リスクレベルの指標において特定の国家主体や組織を識別する基準を参照している（表 4.1-25）。

表 4.1-25　CFIP のリスクレベルの指標において参照されている基準

参照されている基準	概要
制限対象リスト（Denied Entity Lists）[29]	米国商務省などで公開している、米国輸出管理規則（EAR）に基づく輸出特権が拒否された個人および団体や、 対象品目の一部または全部の受け取りを禁止されている外国の当事者（Entity List）のことと想定される
戦略的共同国（strategic competitor）・CWHTUST（country with a history of targeting US technologies for unauthorized transfer：米国の技術を不正移転の標的にしてきた歴史を持つ国）[30]	米国が国家安全保障戦略などの公式文書で使用する用語であり、中国やロシア、イラン、北朝鮮など、米国の経済的、軍事的、技術的な優位性に挑戦し、国際秩序に影響を及ぼす可能性のある国々を指す
EO 13959（大統領令第 13959 号）[31]	2020 年に署名された大統領令 13959 号「Addressing the Threat from Securities Investments That Finance Communist Chinese Military Companies（中国共産党の軍事企業を資金援助する証券投資に対処する）」において、米国の証券投資を利用して軍事力を強化することを防ぐための措置をとるため、中国共産党と関連する企業として指定された機関

[29] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern

[30] https://researchcompliance.caltech.edu/international_collaboration/federal-agency-requirements/dod_compliance#:~:text=A2%3A%20The%20most%20commonly%20recognized,techniques%2C%20and%20procedures%20vary%20greatly

[31] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/

3）TRUST

TRUST（Trusted Research Using Safeguards and Transparency：安全策と透明性による信頼できる研究）は、NSF の支援する研究提案や進行中のプロジェクトに関する情報開示等の要件の不順守、国家安全保障に対する潜在的なリスクを評価するための意思決定ツリーアプローチである[32、33]（表 4.1-26）。

表 4.1-26　TRUST の概要

項目	概要
所管	NSF（国立科学財団）OSRSSP（研究セキュリティ戦略およびポリシー担当長官室）
公表（更新）時期	2024 年 6 月公表
背景・目的	・ NSF は、2022 年 CHIPS 及び科学法に基づき、CUI（管理された非機密または機密情報）へのアクセスを伴う可能性のある研究分野の特定とアクセス許可への注意を指示されていたほか、2023 会計年度歳出報告書において国防長官および国家情報長官と協力し、外国の軍事作戦に影響を与える可能性のある NSF 資金によるオープンソース研究機能のリストを作成することを指示されたことなどを受け、新たな研究セキュリティ強化の枠組みを開発していた ・ TRUST は NSF の支援する研究提案や進行中のプロジェクトに関する情報開示等の要件の不順守、国家安全保障に対する潜在的なリスクを評価するための意思決定ツリーアプローチとされている ・ TRUST は以下の 3 つの評価観点を踏んでいくプロセスとなっている ① 外国政府に関連した現在の任命及び役職 ② 非開示の情報 ③ 研究の潜在的な国家安全保障への考慮事項
デュー・ディリジェンスの実施主体	・ NSF　OCRSSP、研究セキュリティレビューチーム
デュー・ディリジェンスの対象	・ NSF の資金提供する研究開発プログラムへの申請者、参加者
デュー・ディリジェンスの実施タイミング	・ NSF の支援への提案時（プレスの文章から、必要に応じ進行中のプロジェクトも含むと想定される）

[32] https://nsf-gov-resources.nsf.gov/files/NSF%20OCRSSP%20TRUST%20Policy%20Memo.pdf

[33] https://new.nsf.gov/news/nsf-enhances-research-security-new-trust-proposal

■　実施プロセス

TRUST は、まずプログラムの該当性を確認したのち、前記の 3 つの確認観点について OCRSSP 及び研究セキュリティレビューチームの確認を受け、リスク軽減策の実施要否が判断されることとなっている（図 4.1-9）。

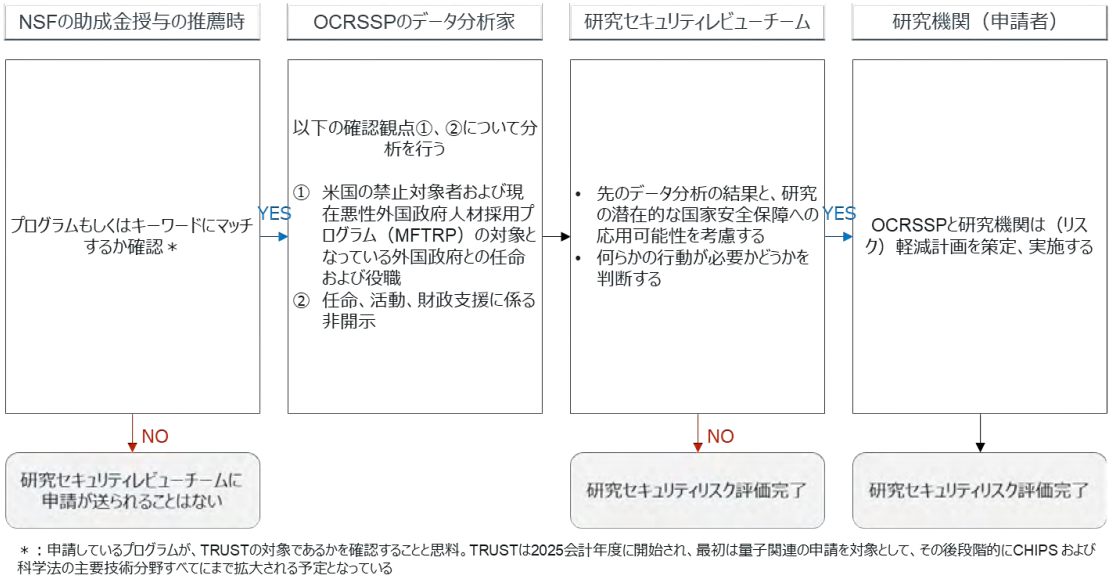


図 4.1-9　TRUST の実施プロセス [34,35]

■　確認観点

TRUST は、下記の①外国政府に関連した現在の任命及び役職、②任命、活動、財政支援に係る非開示情報、③研究の国家安全保障への潜在的な予測可能な用途　の 3 つの確認観点があり、それらが前述の NSF 内での分析・評価のプロセスにもなっている。

【TRUST の確認観点】

① 米国の禁止対象者および現在悪性外国政府人材採用プログラム（MFTRP）の対象となっている外国政府との任命および役職
- 米国商務省産業安全保障局のエンティティリスト、大統領令（EO）14032 またはそれに代わる EO の付属文書
- 2021 年度国防権限法（NDAA）第 1260H 条
- 2019 年度国防権限法（NDAA）第 1286 条（改正済み）

→OCRSSP は、（申請者の）上級職員が現在、米国の禁止対象者との雇用契約や役職を有しておらず、また、現在、悪意のある外国人人材採用プログラムの当事者ではないことを確認することとなっている

② 任命、活動、財政支援に係る非開示＊

→NSPM33 実施計画が発表された時点（2022 年 1 月）から非開示情報が精査されることとなっている

③ 研究の国家安全保障への潜在的な予測可能な用途

[34] https://nsf-gov-resources.nsf.gov/files/NSF%20OCRSSP%20TRUST%20Policy%20Memo.pdf

[35] https://cra.org/govaffairs/blog/2024/06/nsf-research-security-trust-framework/

■　参照している情報ソース

TRUST は、デュー・ディリジェンスの実施にあたり公開情報のデータベースや検索ツール等は参照していないが、確認観点から法令に規定されるエンティティリスト、外国人材採用プログラムをスクリーニングの対象としていることが確認できる[36,37,38]（表 4.1-27）。

表 4.1-27　TRUST の確認観点で参照されている法令・規則の概要

参照されている法令・規則	概要
米国商務省産業安全保障局のエンティティリスト	輸出管理規則（EAR）に指定されている、特定の品目の輸出、再輸出、および/または移転（米国内）に関する特定のライセンス要件の対象となる特定の外国人（企業、研究機関、政府および民間組織、個人、およびその他の種類の法人を含む）の名前のリスト
大統領令（EO）14032	米国人が中国の特定の企業に対して証券投資を行うことを禁止するものです。具体的には、中国の軍事産業や監視技術産業と関係があると米国政府が特定した企業への投資が対象となる
2021 年度国防権限法（NDAA）第 1260H 条	米国防総省の公開している、米国内で直接的または間接的に活動している中国人民解放軍（PLA）と関連のある企業のリスト
2019 年度国防権限法（NDAA）第 1286 条	米国防総省の公開している知的財産の窃盗、スパイ活動、軍や諜報機関とのつながり、あるいは米国の国益に脅威となる悪質な外国人人材募集プログラムの運営に関与している中国とロシアの学術機関のリスト

[36] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

[37] https://www.defense.gov/News/Releases/release/article/2645126/dod-releases-list-of-chinese-military-companies-in-accordance-with-section-1260/

[38] https://basicresearch.defense.gov/Portals/61/Documents/Research%20Security/1286%20List.pdf?ver=nEagju7uAK3DCdfMt9yZGg%3D%3D

4）NIH Dicision Matrix

■　概要

NIH Decision Matrix は、NIH の助成金における潜在的な外国の干渉を評価する意思決定ツリーとして作成されたものであり、その公開によって NIH に助成金を申請する研究者の外国干渉リスクに対する理解を促すとされている。

Decision Matrix 自体は、NSPM-33 等の国の上位指針に準拠する NIH 助成金ポリシーステートメント（NIHGPS）など、既存の NIH の外国干渉に関する申し立ての処理手順に含まれるものである[39]（表 4.1-28）。

表 4.1-28　NIH Dicision Matrix の概要

項目	概要
所管	NIH（National Institutes of Health：国立衛生研究所）
公表（更新）時期	2024 年 8 月
背景・目的	・ NIH Decision Matrix は、NIH 助成金における潜在的な外国の干渉を評価する方法に沿った意思決定ツリーとして作成されたものであり、その公開によって研究者の外国干渉リスクに対する理解を促すと述べている ・ Decision Matrix 自体は、NSPM-33 の実施ガイダンスなど国の上位指針に準拠する NIH 助成金ポリシーステートメント（GPS）など、既存の NIH の外国干渉に関する申し立ての処理手順に含まれ、それを強化するものとして位置づけられている ・ 文書中では、NIH が外国干渉の可能性があるとして問題視している行動の種類（リスク要因）と、それに対する評価レベルの区分について説明されている
デュー・ディリジェンスの実施主体	・ NIH（NIH 研究所もしくはセンター、NIH 外部研究オフィス（OER）のスタッフ）
デュー・ディリジェンスの対象	・ NIH の助成金を活用する機関・研究者
デュー・ディリジェンスの実施タイミング	・ 助成金の申請時／及び既に交付された助成金

■　実施プロセス

NIH の外国干渉に関する申し立ての処理では、情報開示や通報などによって懸念事項を検知したのち、それが NIH の助成金に関係する場合は情報開示のリマインドがなされ、その後事前の情報開示や承諾を順守していなかった度合いに応じて主任研究者の交代や助成金の保留といった措置が講じられることとなっており、このプロセスの中に Decision Matrix も含まれているものと想定される[40]。

[39] https://nexus.od.nih.gov/all/2024/08/15/new-decision-matrix-further-clarifies-nih-processes-for-handling-allegations-of-foreign-interference/

[40] https://grants.nih.gov/policy-and-compliance/policy-topics/foreign-interference/handling-allegations

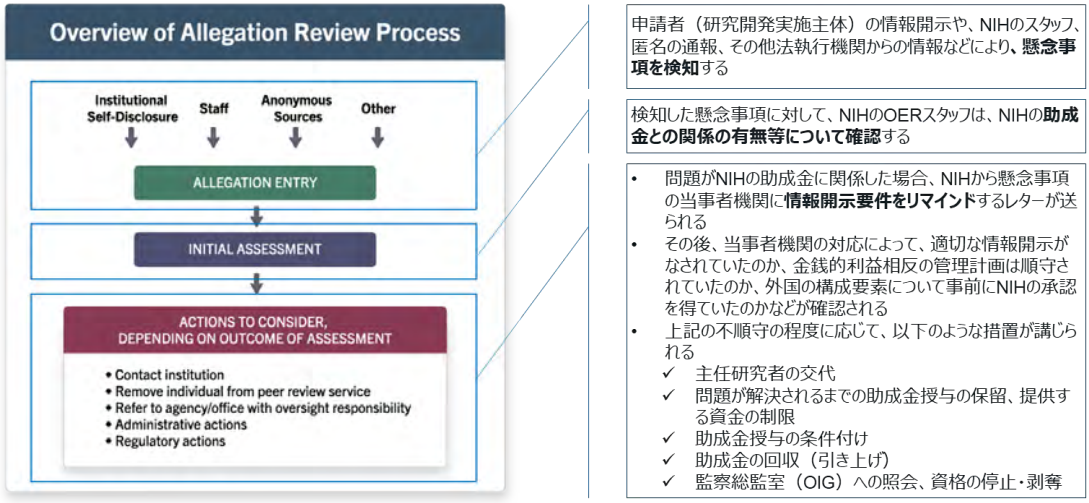


図 4.1-10　NIH における外国干渉の申し立て処理プロセスのイメージ

■　確認観点

NIH は助成金を活用する上級/主要職員に対して、研究支援のすべての出所、外国の構成要素[41]、および金銭的利益相反の開示を義務付けている。

そのうえで Decision Matrix では、①外国人材採用プログラム、②海外からの資金調達、③外国の機関または団体との提携関係　の 3 つをリスク要因として挙げ、それらに該当する事実に対する評価レベルを 4 段階に区分している（表 4.1-29）。

[41] 構成要素（Component）：米国国外で実施される NIH プロジェクトに関する実質的な作業を伴う国際協力やその他の活動を指すとされる

表 4.1-29　NIH Dicision Matrix のリスク要因と評価レベル

要因 / 評価	要因①：外国人材採用プログラム	要因②：海外からの資金調達	要因③：外国の機関または団体との提携関係
緩和策が必要 (required)	2022 年の CHIPS および科学法第 10638 条(4)(A)(i)~(ix)の基準のいずれかに該当する、悪意のある外国人材採用プログラム（MFTRP）への積極的な（継続中の）参加の兆候（自動的に失格）	懸念外国（FCOC）または FCOC 関連事業体からの未開示または不完全開示の実行中（継続中）の資金調達の指標	懸念外国（FCOC）に所在する、または懸念外国と関係のある機関または事業体との、非公表または不完全な公表の活動（進行中）の提携を示す指標
緩和策が推奨 (recommended) される	過去 5 年以内：2022 年のチップおよび科学法第 10638 条(4)(A)(i)~(ix)項の基準に該当する悪質な外国人材採用プログラム（MFTRP）への過去の参加の指標。 または外国人材採用プログラム（FTRP）への未開示または不完全開示の活動(継続中)参加の指標で、2022 年 CHIPS および科学法第 10638 条(4)(A)(i)~(ix)の基準を満たすもの	過去 5 年以内：懸念外国（FCOC）または FCOC 関連事業体からの過去の資金提供について、非開示または不完全開示の指標 または懸念外国（FCOC）または FCOC 関連事業体ではない外国国または外国事業体からの非開示または不完全開示の活動中（継続中）の資金提供の指標	過去 5 年以内：懸念される外国（FCOC）に所在する、または懸念される外国と関連のある機関または団体との、非公開または不完全な公開の過去の所属の指標 または懸念される外国ではない外国に所在する、または懸念される外国と関連のある機関または団体との、非公開または不完全な公開の活動中の（継続中の）所属の指標
緩和策が提示 (suggested) される	過去 5 年以内:2022 年 CHIPS および科学法第 10638 条(4)(A)(i)~(ix)項に該当する、外国人材採用プログラム（FTRP）への過去の参加について、非公開または不完全な開示が行われた場合の指標	過去 5 年以内：懸念外国（FCOC）または FCOC 関連事業体ではない外国国または外国事業体からの過去の資金調達について、非開示または不完全開示の指標	過去 5 年以内：懸念外国（FCOC）以外の外国に所在する機関または団体との過去の所属関係について、非開示または不完全開示の指標
緩和策は不要 (No needed)	悪意のある外国人材採用プログラム（MFTRP）への現在または過去（5 年以内）の参加を示す兆候がないこと、および、2022 年の CHIPS および科学法第 10638 条(4)(A)(i)~(ix)の基準のいずれかに該当する外国人材採用プログラム（FTRP）への現在または過去（5 年以内）の参加について、非開示または不完全開示の兆候がないこと	外国または外国の事業体からの現在または過去（5 年以内）の資金提供について、未開示または不完全開示の指標はないこと	外国にある機関または団体との現在または過去（5 年以内）の所属関係について、未開示または不完全な開示の兆候がないこと

■　参照している情報ソース

Decision Matrix は特定のデータベースや検索ツールを参照しているものではないが、Decision Matrix において法令に規定されるエンティティリスト、外国人材採用プログラムをリスク評価の要因としていることが確認できる（表 4.1-30）。

表 4.1-30　NIH Decision Matrix で参照されている法令・規則等

参照されている法令・規則	概要
2022 年 CHIPS および科学法第 10638 条(4)(A)(i)~(ix)における外国人材採用プログラム 悪意のある外国人材採用プログラム	・ 2022 年 CHIPS および科学法で規定される、以下の定義に該当するプログラム： ・ 外国人材採用プログラム（FTRP）　： ・ 現金、研究資金を含む現物支給、将来の報酬の約束、無料の海外旅行、少額でない価値の物品、敬称、キャリアアップの機会、または外国のあらゆるレベル（国、州、または地方）またはその指定機関、または外国に拠点を置く、外国から資金提供を受けている、または外国と提携している団体（外国が直接後援しているかどうかは問わない）が個人に直接提供するその他の種類の報酬または対価を含むプログラム、役職、または活動 ・ 悪意のある外国人材採用プログラム（MFTRP）： ・ 外国人材採用プログラムの中でも、対象となる個人が、取り決め、契約、またはその他の文書に直接的または間接的に記載されているかどうかにかかわらず、以下のような事項を求められるもの ✓ 米国の事業体の諸州する成果や非公開情報の譲渡 ✓ 当該プログラムに参加する研究者の募集が義務付けされる ✓ 特別な場合を除き当該プログラムの契約を解除できない ✓ 連邦政府に対し当該プログラムへの参加を非開示にするよう要求される　等
懸念外国（FCOC）	・ 米国国務省が米国にとって脅威であると判断した国であり、この用語は米国の法律および立法で使用される ・ 中華人民共和国、朝鮮民主主義人民共和国、ロシア連邦、イラン・イスラム共和国、または国務省が懸念国と判定したその他の国をいう

5）ヒューストン大学における取り組み

ヒューストン大学は、研究セキュリティの側面で公式 HP おいて、連邦及び州の法令・規則に則る旨を述べており、研究セキュリティのリソースが整備されている。

そこから、少なくとも NSPM-33 及び The Chips & Science Act of 2022 に準拠した体制がとられているものと考えられる。

■　実施プロセス

大学は政府の要件を監視し、それに応じてポリシーと手順とポリシーを変更するとあったことから、NSPM と同様のプロセスを踏んでいるものと思われる。[42]

その他、ヒューストン大学では、利益相反（Conflict of Interest, COI）のチェックプロセスが「ヒューストン大学の研究における利益相反に関する方針 [43]」で示されており、そこでは、認証完了、FCOI 認証レビュー、COI 委員会、FCOI の管理、金融利益の変更/更新、渡航に関する開示というプロセスを踏んでいる。

各ステップでの対応事項は以下の通り

①証明書記載：審査対象者は、「研究または機関の責任に関連する可能性のある」重要な財務的利益（SFI）を開示する。

②FCOI 認証レビュー：COI オフィスによる証憑と研究者のオンライントレーニング受講状況確認。

③COI 委員会：すべての開示は利益相反委員会（COIC）で検討され、研究の設計、実施、または報告に偏りがあるとみなされる可能性のある矛盾が存在するかどうかが判断される。

④FCOI の管理：金銭的利益が大きく、研究と矛盾する可能性がある場合には、研究活動の設計、実施、報告を偏見や客観性の低下から守るための保護措置を確実に講じるための管理計画が必要。COI 委員会は提出された管理計画を審査。

⑤金融利益の変更/更新：研究者は年に 1 回に利益相反証明書を提出する必要がある。重要な金銭的利益のステータスの変更または重要な金銭的利益の追加があった場合は、更新された証明書および/または新しい証明書と開示を 30 日以内に提出する必要がある。

⑥渡航に関する開示：PHS または DOE の資金提供を受けているプロジェクトに参加しており、第三者機関（非営利団体を含む）が旅費を後援している場合は、払い戻しを受けた旅費または後援を受けた旅費をすべて開示する必要がある。

■　確認観点

NSPM-33 に準拠していることから、同規則の確認観点は利益相反の確認の際含まれる。また、悪質な外国人人材採用プログラム（METRP）については、The Chips & Science Act of 2022 にも準拠しており [44]、同規則の確認観点は悪質な外国人材採用プログラム確の際に含まれる。さらに、Texas Executive Order GA-48 も準拠しており、同規則の確認観点は渡航や国外機関との共同研究の際に役立つとしている。

---

[42] https://uh.edu/research/research-security/nspm-33/

[43] https://uh.edu/research/compliance/coi/

[44] https://uh.edu/research/research-security/malign-foreign-talent-recruitment-program/

■　参照している情報ソース

NSPM-33 や The Chips & Science Act of 2022 に準拠していることから、同様の開示内容及び、外国人材採用プログラムなどを参照していると想定される。

（2）カナダ

カナダではISED（イノベーション・科学経済開発省）が中心となり、研究セキュリティのためのデュー・ディリジェンスに係る取り組みを進められてきた。

2021年にNational Security Guidelines for Research Partnerships（NSGRP）が公表され、研究パートナーシップにおける国家安全保障リスクに対処するため、連邦研究パートナーシップ資金プログラムにおけるデュー・ディリジェンスの実施を求められることとなった。

2022 年には、Conducting Open Source Due Diligence for Safeguarding Research partnership が公表され、研究パートナーシップにおいて研究者が公開情報を用いて自らの研究活動やパートナー組織のリスクを評価するオープンソース・デュー・ディリジェンスの具体的な実施手法のガイダンスの提供がなされた。

上記政策動向を踏まえ公開情報を基に、米国において政府、資金提供機関、研究開発実施主体によって実施されている研究セキュリティ・インテグリティに係るデュー・ディリジェンスの取り組み・ガイドライン等を抽出した（表 4.1-31）。

表 4.1-31　詳細調査を行う取り組み・ガイドライン

取り組み主体	デュー・ディリジェンスに係る取り組み・ガイドライン
政府	National Security Guidelines for Research Partnerships（NSGRP）におけるデュー・ディリジェンス
資金提供機関	NESRC、CIHR、SSHRC における取組
研究開発実施主体	マギル大学における取り組み

以下に表 4.1-31 に掲載した取り組み・ガイドラインについての詳細調査結果を示す。

1）National Security Guidelines for Research Partnerships（NSGRP）におけるデュー・ディリジェンス [45]

■　概要

NSGRP は、カナダにおける研究パートナーシップの開発、評価、資金提供に国家安全保障上の考慮事項を組み込むことを目的としたガイドラインであり、全ての研究者が活用することを推奨しているが、特に連邦政府の資金提供機関の実施する特定のプログラムに適用される。研究内容自体の潜在的なリスクと、パートナーの持つリスクの両方を特定する活動をデュー・ディリジェンスと呼称している点が特徴的である（表 4.1-32）。

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

表 4.1-32　NSGRP におけるディリジェンスの概要

項目	概要
所管	ISED（イノベーション・科学経済開発省）
公表（更新）時期	2021 年公表
背景・目的	NSGRP は、カナダにおける研究パートナーシップの開発、評価、資金提供に国家安全保障上の考慮事項を組み込むことを目的としたガイドラインであり、基本原則、リスクとは何かの解説、リスクの特定・緩和方法について解説している NSGRP におけるデュー・ディリジェンスは研究分野（何に取り組んでいるか）とパートナー（誰と取り組むか）の側面があり、そのうえで、リスクの高い研究分野の一部として STRAC ポリシー（前回テーマ 1 で報告）と、パートナーを調査する手法として OSDD のガイドラインなど他の文書と参照関係にある
デュー・ディリジェンスの実施主体	・ カナダにおけるあらゆる研究者（推奨） ・ 関連する連邦研究パートナーシップ資金提供の機会に申請する研究者
デュー・ディリジェンスの対象	・ 研究者自身の研究内容 ・ 連携する研究パートナー
デュー・ディリジェンスの実施タイミング	・ あらゆる研究機会（推奨） ・ 関連する連邦研究パートナーシップ資金提供の機会への申請時

NSGRP は、主要な連邦政府資金提供機関である NSERC、CIHR、SSHRC の 3 機関の特定の資金提供プログラムに適用されており、公募資料を読んでリスク評価シートの必要性の判断を求めている（表 4.1-33　NSGRP が適用されるプログラム（NSERC の HP より））[46]。

NSGRP が適用されるプログラムは「連邦研究パートナーシップ資金プログラム」とされており（明確な定義は確認できず）、パートナーシップと名の付く助成金プログラムには、複数のセクターや機関との連携が申請者に求められることが多い。その他研究分野等によって適用対象が区分されているかについては、「NSGRP と STRAC ポリシーは補完的な別個のものである」とされていることから、少なくとも研究分野によって対象は区分していないと思料される。

表 4.1-33　NSGRP が適用されるプログラム（NSERC の HP より）

資金提供機関	適用されるプログラム
NSERC（カナダ自然科学・工学研究会議）	資金提供機会に関する文献に記載されている、特別募集や共同資金提供機会を含む提携助成金
CIHR（カナダ保健研究所）	2024 年秋から公募が開始される研究プログラム
SSHRC（社会科学・人文科学研究会議）	カナダバイオメディカル研究基金（ステージ 2）

[46] https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp#a3

■　実施プロセス

NSGRP におけるデュー・ディリジェンスでは、カナダ政府の連邦研究パートナーシップ資金提供において、申請にあたり研究開発実施主体（申請者）が自身の研究活動やパートナー組織に関するリスクを分析するデュー・ディリジェンスを行い、その後その結果をもって資金提供機関がリスクの評価・資金提供の可否を判断することとなっている[47]。

以下に、それぞれの実施プロセスを記載する。

・　研究開発実施主体（申請者）の実施するデュー・ディリジェンスのプロセス

リスク評価フォームを記入するためのオープンソース・デュー・ディリジェンス実施のガイダンスとして、NSGRP は別文書の「Conducting Open Source Due Diligence for Safeguarding Research Partnerships（以下、ガイダンス）」を参照している[48]。

ガイダンスでは、大きく「ベースライン・リスクの理解」「初期検索戦略の立案・実行」「調査結果に基づく意思決定」「結果の記録・文書化・説明」を結節としたプロセスが組まれている（図 4.1-11）。

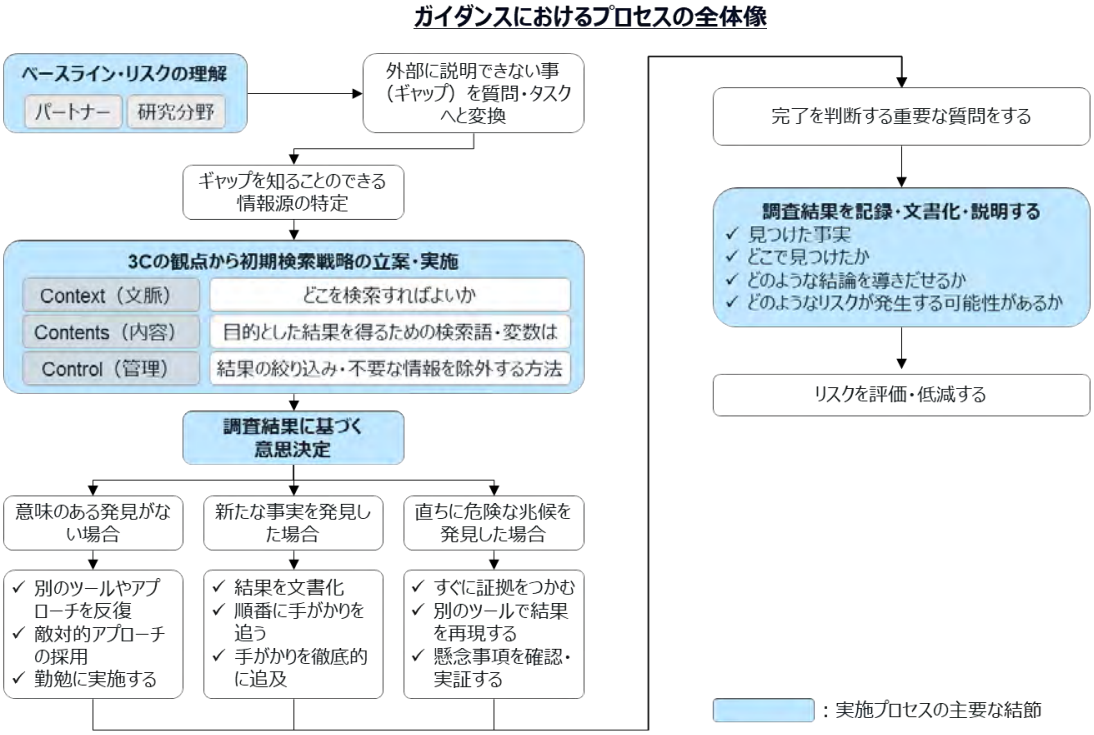


図 4.1-11　ガイダンスにおけるプロセスの全体像

まず、研究プロジェクトとパートナーに関するベースラインリスクを理解することから

[47] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process

[48] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-conducting-open-source-due-diligence/conducting-open-source-due-diligence-safeguarding-research-partnerships

始め、次いで当該研究パートナーシップについて知っていることを外部と話し合うことで、知識のギャップを特定し、曖昧さや仮定を浮き彫りにすることから始める。

＜ベースラインリスク＞
ベースラインリスクについて、明確な定義がなされているわけではないが、以下のような事項であるとガイドライン本文から推察される

- 研究プロジェクト：一部の研究領域はほかの研究領域より機密性が高い。NSGRP の AnnexA には、カナダ政府が機密性が高いとみなす研究領域のリストがある（輸出規制やデュアルユース技術など。STRA も含まれる）
- パートナー：CSIS（カナダ安全保障情報局）の公開する学術研究者から知的財産を盗んだ経歴を持つ特定の国、地域に関する情報など Safe guarding your research ポータルにある情報

＜外部と話し合うべきこと＞
次いで、当該研究パートナーシップについて知っていることを外部に伝えることで、知識のギャップを特定し、曖昧さや仮定を浮き彫りにする。以下のような基本的な質問に答え、話あうとよいとしている。

- このパートナーシップはどのようにして生まれたのですか?
- あなたのパートナーはあなたの研究への興味について何と言っていますか?
- パートナーの他の研究投資やパートナーシップについて、すでに何を知っていますか?
- パートナーの評判や履歴に関するあなた自身の個人的な理解から何がわかりますか?
- パートナーシップを妨げる可能性のある明らかな利益相反や義務の衝突はありますか?

そして上記のような話し合い・質問によって、自身が当該研究・パートナーシップについて知らない・説明できないこと（ギャップ）を特定し、ギャップを質問のレベルまで形を変え、質問をタスク（具体的に実施すべき事項）に変え、それを知ることのできる情報源を特定する（表 4.1-34）。

ギャップを質問に変換するにあたり最低限含めるべき質問として、以下のような質問は最低限含めるべきであるとしている。

- パートナー組織が外国政府の影響、干渉、または統制を受ける可能性がある兆候はありますか?
- ートナー組織に透明性の欠如や非倫理的な行為があり、提案された研究プロジェクトに影響を及ぼす可能性があることを示唆する兆候はありますか?
- パートナー組織の研究プロジェクトに関与する個人に、不正な知識移転につながるような利益相反や関係がある兆候はありますか?
- この研究プロジェクトの結果として、パートナー組織が、機密データを保管するインフラストラクチャを含む、研究機関のカナダの施設、ネットワーク、またはキャンパス内の資産にアクセスする、またはアクセスできる可能性があるという兆候はありますか?

表 4.1-34　特定すべき情報源の例

情報源	使用事例
企業記録	・　法人の所有者と株主を特定する ・　親会社と子会社を特定する
企業ウェブサイト	・　パートナーシップや投資に関するプレスリリースを確認する ・　他の情報源と照らし合わせてパートナーの経歴の詳細を確認する
学術および賞のデータベース	・　パートナーが資金提供している他のプロジェクトを特定し、その優先事項や他の協力者を理解する
知的財産および特許データベース	・　カナダで生まれたが外国のパートナーが所有している特許やその他の知的財産を特定する
制裁	・　研究パートナーがカナダ、米国、国連、その他の制裁機関によって制裁を受けていないことを確認する
規制対象品目およびエンドユーザーリスト	・　研究パートナーが自国の軍事および安全保障に研究を転用するリスクが高いと評価されていないことを確認する
法律データベース	・　パートナーがあなたの研究分野に関連する民事訴訟や刑事訴訟に関与していないことを確認する。

質問をタスクレベルに落とし込めたならば、「Context」「Contents」「Control」の 3 つの C の観点から初期の検索戦略を立て、実行・記録する（図 4.1-12）。

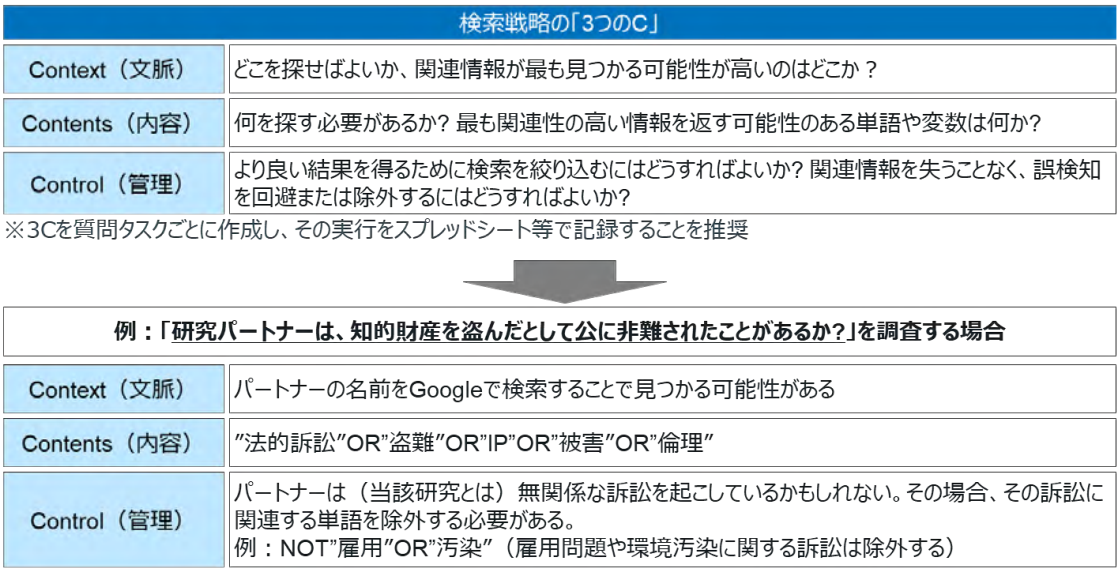


図 4.1-12　検索戦略の「3 つの C」とその例

その後 3 つの C の観点で計画した調査を実行する過程で、調査結果に基づき継続して意

思決定を行い、自身で作業を終了させるための判断を実施する（図 4.1-13）。

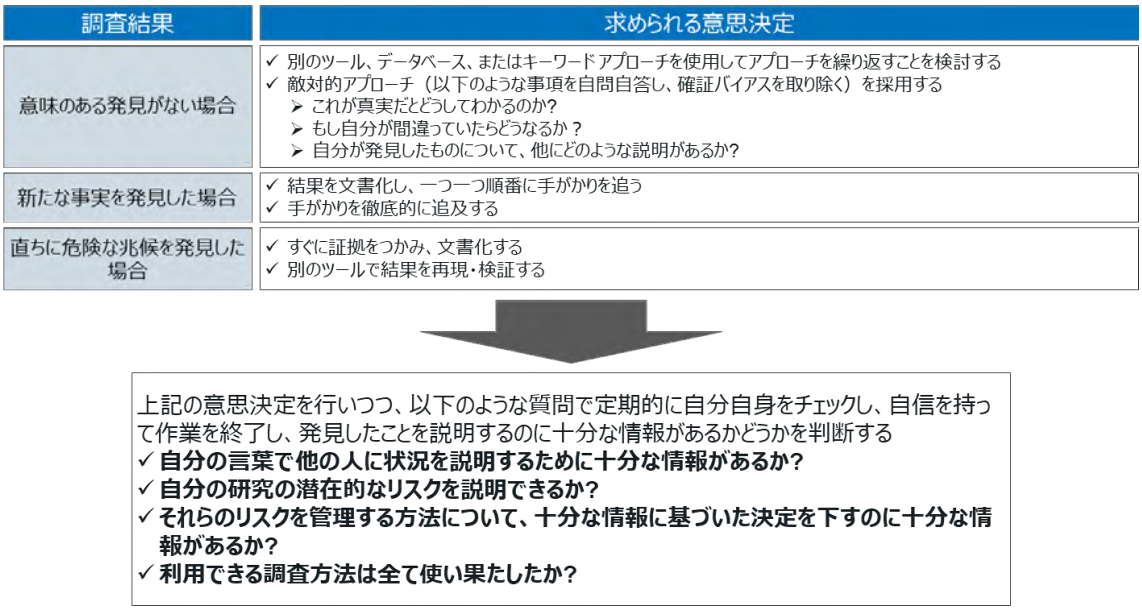


図 4.1-13　結果に応じた意思決定及び作業終了の判断

最後に、デュー・ディリジェンスを行った結果を以下のような質問に答えることのできるレベルまで文書化する。

＜デュー・ディリジェンスの結果を文書化するための質問＞
- ✓ どのような証拠を、どのようにして見つけたのか?
- ✓ 証拠はどこで見つけたのか? 信頼できる情報源から得たものか? 可能な場合は他の情報源で検証したか?
- ✓ 発見したことからどのような論理的な結論を導き出せるか?
- ✓ 自分の研究分野についての知識とパートナーについての発見に基づくと、パートナーシップにはどのようなリスクが生じる可能性があるか?

・　資金提供機関のリスクの評価・資金提供の可否判断のプロセス

上記のデュー・ディリジェンスの結果を基に、NSGRP が適用される資金提供プログラムでは、申請にあたり研究者は「リスク評価フォーム」を記入・提出することが求められる申請は、助成機関によるチェックと、必要に応じた安全保障部門のチェックを通じて資金提供の可否が判断されることとなっている[49]。

まず研究者は、オープンソース・デュー・ディリジェンスを実施して、リスク評価フォームを記入・提出する。リスク評価フォームは研究内容自体に関するリスク（重要な分野や機微技術分野との関連）とパートナーに関するリスク（外国の影響や干渉）の側面があり、それらを調べるために輸出管理リストや STRA（テーマ 1 を参照）、前記のガイダンスを参照している。

次いでリスク評価フォームは助成機関に審査され、フォーム上のすべての質問と構成要

[49] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process

素が申請者によって完了しているかどうかが確認される。この際、NSGRP や各機関のガイダンスに基づいたオープンソース情報に基づく検証評価が実施される。

リスクの可能性がある、またはリスクが特定された申請は助成機関の内部リスク評価委員会に送られ、国家安全保障部門および機関による追加の評価とアドバイスが必要かどうかを判断されることとなっており、必要と判断された場合、カナダ公安省に照会される。その際、リスク評価はメリット評価（研究の実施能力等に係る評価と思われる）とは分離され、カナダ公安省への照会はメリット評価の合格が確認されたのちに実施される。

助成機関から申請書を受け取ると、カナダ公安省は最初の審査を行い、国家安全保障評価を主導するセキュリティ機関（カナダ公安省、カナダ安全保障情報局、または通信安全保障局のいずれか）を決定し、各機関が権限と任務に基づき評価を実施する。

最終的に助成機関は、カナダ公安省から受け取った国家安全保障評価とアドバイスを、メリット評価の結果と併せて考慮し、各申請に対する助成決定を下すこととなっている。

資金提供が拒否された場合、申請者には助成期間と研究安全保障センターの代表者と面談を受ける機会がある。資金提供が決定された場合は、リスク評価シート記載のリスク軽減計画に追加の条件として、さらなるリスク軽減措置が国家安全保障部門から要求される場合がある。

■　確認観点

NSGRP の確認観点としては、研究開発実施主体（申請者）がデュー・ディリジェンスの結果に基づき資金提供機関に申請するリスク評価フォームの確認事項が挙げられる[50]。

リスク評価フォームは、大きく分けて研究内容自体の潜在的なリスクと、パートナーの持つリスクの２つの確認観点があり、それぞれの質問に対し「はい/いいえ/不明」の３つで回答することが求められ、回答ごとに使用したリソースと調査結果、リスク軽減計画を提示することが求められる（表 4.1-35）。

[50] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships/national-security-guidelines-research-partnerships-risk-assessment-form

表 4.1-35　リスク評価フォームの構成

セクション 1：研究内容の理解	
質問 1.1	**重要鉱物リスト**に掲載されている重要鉱物（重要鉱物サプライチェーンを含む）に関連する研究分野で活動しているか？
質問 1.2	**重要インフラに関する国家戦略**の重要インフラ部門の 1 つに分類される研究分野で活動しているか?
質問 1.3	この研究プロジェクトでは、**機密情報となる可能性のある個人データ**の使用が含まれるか?
質問 1.4	この研究プロジェクトには、**機密情報となる可能性のある大規模なデータセット**の開発または使用が含まれるか？
質問 1.5	**輸出入許可法（EIPA）の輸出管理リスト(ECL)**に記載されている商品または技術に関連する研究分野で活動しているか?
質問 1.6	NSGRP の AnnexA のリストにある**機密またはデュアルユースと見なされる可能性のある研究分野**で活動しているか? （上記質問の観点に加え、**STRA などが該当**する）
セクション 2：パートナー組織を知る	
質問 2.1	パートナー組織が**外国政府の影響、干渉、または統制**を受ける可能性がある兆候はあるか?
質問 2.2	パートナー組織に**透明性の欠如や非倫理的な行為**があり、提案された研究プロジェクトに影響を及ぼす可能性があることを示唆する兆候（詐欺、賄賂、スパイ活動、汚職、知的財産・特許の侵害、違法行為等）はあるか?
質問 2.3	パートナー組織の研究プロジェクトに関与する個人に、**不正な知識移転につながるような利益相反や関係**があることを示す兆候はあるか?
質問 2.4	この研究プロジェクトの結果として、パートナー組織が、機密データを保管するインフラストラクチャを含む、研究機関のカナダの**施設、ネットワーク、またはキャンパス内の資産にアクセスする、またはアクセスできる可能性**があるという兆候はあるか?

セクション 3：リスクの特定	
	・ 「自分の研究を知る」および「自分のパートナー組織を知る」セクションで提供した「はい」または「わからない」の回答ごとに、使用した**リソースと収集した主な調査結果**を説明すること ・ デューデリジェンス プロセス中に確認された懸念事項のうち、このフォームの前のセクションでは取り上げられていないものを挙げることもできる
セクション 4: リスク軽減計画	
	・ **リスク軽減計画を提示**すること。質問に答えて、特定したすべてのリスク要因に対処する必要がある ・ リスク軽減計画には、次のような事項が含まれるが、これらに限定されない ✓ プロジェクトが受けたその他の関連する審査プロセスの説明（例：研究プロジェクトを通じて収集された個人データがどのように保護されるかに焦点を当てた研究倫理委員会の審査） ✓ 研究セキュリティ意識を高め、研究チーム全体の能力を構築する ✓ パートナー組織の目的がパートナーシップの目的と一致していることを確認する ✓ 健全なサイバーセキュリティとデータ管理の実践の確保 ✓ 研究成果の利用目的に関する合意

■　参照している情報ソース

参照している情報ソースとしては、前記ガイドラインにおいてデュー・ディリジェンスに活用できる情報ソースの例がガイダンスの AnnexA、B に列挙されており、主に企業情報、学術、知的財産・特許、制裁、輸出規制等に関連した情報ソースが確認できる（表 4.1-36）。

表 4.1-36　ガイダンスの参照している情報ソース

区分	情報ソース	説明	無料/有料の別
企業情報	電子文書分析検索システム (SEDAR) - カナダ証券監督者	カナダの公開企業および証券管理人に関するさまざまな文書を含む、企業が提出した公開証券文書および情報のデータベース	無料
	電子データ収集、分析、検索 (EDGAR)	米国の株式公開企業の文書のデータベース	無料
	欧州電子司法ポータル - 企業を探す	EU 諸国の国家企業登録簿のデータベース	無料
	オープンコーポレート	世界最大の企業データベース。140 の管轄区域と約 2 億社の企業を網羅している	無料
	企業検索	120 か国以上をカバーする企業登録の統合ディレクトリ。国別に閲覧できる	無料
	海外登録	英国政府が提供する、世界のビジネス登録の概要	無料
	カナダ統計局 - 企業間の所有権	カナダにおける企業の所有権と「誰が何を所有しているか」に関する信頼できる包括的な情報源	無料
	カナダ法人データベース	連邦政府に登録されている企業を検索して、誰が関与しているかを確認できる 企業がカナダに登録されているかどうかを検索したり、企業名を確認したりするために使用できる	無料
	カナダの企業登録	アルバータ州、ブリティッシュ コロンビア州、マニトバ州、オンタリオ州、ケベック州、サスカチュワン州の連邦および州に登録されている企業を検索できる。	無料
各州の登記簿	アルバータ州法人登記所	有料でアルバータ州の法人登記所から記録を請求できる	有料
	ブリティッシュコロンビア州法人登記所	州に登録された法人を検索できる。アカウントの作成が必要	無料
	ニューブランズウィック州法人登記所	州に登録されている法人を検索できる。結果は無料で確認できるが、詳細は有料	無料と有料
	ニューファンドランド会社登記所オンライン (CADO)	州に登録されている法人を検索できる。アカウントを作成しなくても、結果と詳細は無料で利用できる	無料
	ノバスコシア州株式会社登録局	州に登録されている法人を検索できる。アカウントを作成しなくても、結果と詳細は無料で利用できる	無料

区分	情報ソース	説明	無料/有料の別
	オンタリオ eCore	州に登録された法人を検索できる。アカウントの作成が必要で、料金がかかる	無料
	プリンスエドワード島のビジネス検索	州に登録されている法人を検索できる。アカウントを作成しなくても、結果と詳細は無料で利用できる	無料
	ケベック州登録企業検索	州に登録されている法人を検索できる。アカウントを作成しなくても、結果と詳細は無料で利用できる	無料
	サスカチュワン州法人登記所	州に登録されている法人を検索できる。アカウントの作成が必要で、料金がかかる場合がある	有料
	ノースウエスト準州法人登記所	州に登録されている法人を検索できる。結果は無料で確認できる。詳細はアカウント作成時および有料で利用可能	無料と有料
	ヌナブト準州の企業記録	Corporate.Registries@gov.nu.ca まで問い合わせが必要	手数料がかかる場合あり
	ユーコン法人登記所	州に登録されている法人を検索できる。結果は無料で確認できる。詳細はアカウント作成時および有料で利用可能	無料と有料
学術及び採択・交付結果	IEEE Explore	エンジニアリング、コンピューター サイエンス、電気通信、電力、その他のエンジニアリング分野に関連する研究文書の概要。結果は無料だが、ダウンロードにはサブスクリプションが必要	無料と有料
	Web of Science	科学文献および引用データへのアクセスを提供するデータベースの有料コンパイル	有料
	Scopus	キュレーションとピアレビューに重点を置いた抄録および引用エンジン。基本検索（「プレビュー」）にはアカウントが必要。詳細検索にはサブスクリプションが必要	無料と有料
	Google Scholar	より包括的で自動化されたインデックス作成アプローチを備えた要約および引用エンジン。より幅広い結果リストが生成されるが、精度は低くなる可能性がある。	無料
	Dimensions.AI	Google Scholar に似た学術研究の抄録および引用検索エンジンだが、リンクと関係性に重点を置いている。記録は、資金提供データ、機関のサポート、ポリシー文書によってコンテキスト化されている	無料
	Cognit	カナダの研究機関のプロジェクト、施設、知的財産を含む研究データベースの概要。Cognit は、NSERC/CIHR/SSHRC/CFI データベースの統合検索を提供	無料
	CFI 研究施設ナビゲーター	大学、カレッジ、病院、カナダ連邦政府の研究施設のデータベース	無料

区分	情報ソース	説明	無料/有料の別
	NSERC 賞データベース	カナダ自然科学技術評議会が提供する採択・交付結果のデータベース	無料
	CIHR 賞データベース	カナダ保健研究機構が提供する採択・交付結果のデータベース	無料
	SSHRC 賞データベース	カナダ社会科学人文科学研究評議会が提供する採択・交付結果のデータベース	無料
知的財産・特許	カナダ知的財産データベース	カナダ政府の商標、特許、著作権、工業デザイン、その他の商品およびサービスのデータベース	無料
	Google Patent	全世界をカバーする特許検索エンジン。Google Scholar および Google ブックスの文書や文献を含めるオプションがある	無料
	Espacenet	欧州特許庁が提供する、世界規模でカバーする特許検索エンジン。検索とフィルタリングを高度に制御できる	無料
	Patentscope	世界知的所有権機関（WIPO）が提供する、世界規模をカバーする特許検索エンジン。Espacenet よりもレコード数は少ないが、分析機能は充実している	無料
制裁・エンドユーザーリスト	統合カナダ自治制裁リスト	カナダ政府による特定のカナダ制裁の対象となる個人および団体の公式リスト。検索およびフィルタリングが可能	無料
	米国外国資産管理局(OFAC)制裁リスト	米国政府の公式制裁リスト。検索およびフィルタリング可能	無料
	制裁エクスプローラー	米国 (OFAC)、欧州連合、国連の制裁を網羅する制裁検索エンジン。個人、組織、航空機、船舶が含まれる	無料
	米国統合スクリーニングリスト	米国政府が特定の品目の輸出、再輸出、または移転を制限している当事者のリスト	無料
法務・起訴・事件記録	CanLII	カナダの民事および刑事裁判の判例と関連文書の統合検索エンジン	無料
	WorldLII	カナダを含む世界 123 の管轄区域の法的判決およびその他の法的文書の統合データベース	無料
	FBI プレスリリース	FBI 事件に関連する起訴状、告訴、答弁を検索できるデータベース。場所、カテゴリ、日付でフィルタリングできる	無料
	米国司法省のプレスリリース	米国連邦訴訟に関連する起訴状、告訴、答弁を検索できるデータベース。場所、カテゴリ、日付でフィルタリングできる	無料

区分	情報ソース	説明	無料/有料の別
その他ニュースやアーカイブ記事	Google ニュース	ニュースソースの統合および検索エンジン。メディア報道とプレスリリースの両方の優れた情報源となる	無料
	OCCRP アレフ	調査ジャーナリストによって収集され、ジャーナリストのために作成されたデータと情報のアーカイブ。ジャーナリストによって発見されたさまざまな文書とデータにアクセスできる	無料
	インターネットアーカイブ	アクティブではなくなった Web サイトやライブ サイトの古いバージョンなど、Web サイトのキャッシュ バージョンにアクセスできる。削除された企業 Web サイトのセクションを確認するのに役立つ	無料
	ドメインビッグデータ	ドメイン レジストリや IP 範囲などの技術的な Web サイト データへの統合アクセス。Web サイトとドメインを確立するための WHOIS レコードも含まれる	無料
商用データベース	Comply Advantage	個人および企業のリアルタイムのリスク データベースを提供します。制裁および重要な公的地位にある人物（PEP）に関する情報が含まれます。また、不利な情報やメディアも含まれる	有料
	Dun & Bradstreet Onboard	統合されたコンプライアンス データ、世界的な制裁リストへのアクセス、および詳細な企業連携分析を提供し、あらゆるビジネス関係を特定するためのツール	有料
	Kharon ClearView	個人または団体が制裁対象または貿易制限対象者と関連しているかどうかを確認するための検索ツール	有料
	Refinitiv World-Check Risk intelligence	個人または団体がマネーロンダリング、テロ資金供与、贈収賄、汚職などの活動に関与しているかどうかを確認するための検索ツール	有料
	Strider Shield	IP 盗難や国家による人材募集に関与する当事者の特定に特化した検索ツール。社内顧客システムと統合するように設計されている	有料

2）NESRC、CIHR、SSHRC における取組

カナダの主要な資金提供機関である NESRC、CIHR、SSHRC は、特定の資金提供プログラムにおいて NSGRP のリスク評価レビュープロセスを適用する旨を「NSGRP に関する三機関ガイダンス」で述べており、実際に CIHR の公募ページでは、必要提出書類の補足文書として「リスク評価フォーム」が記載されていることが確認できる[51]（図 4.1-14）。

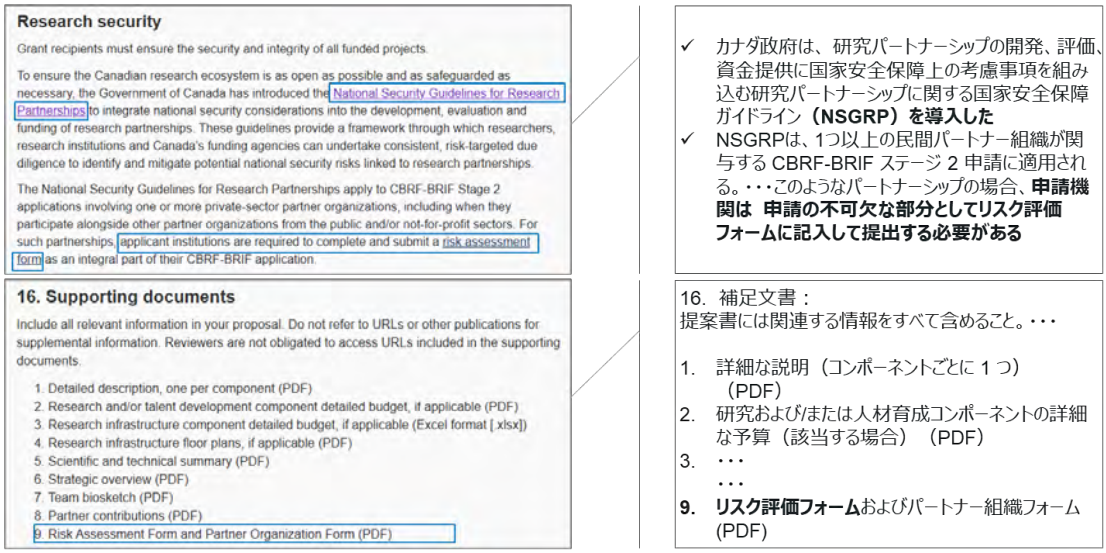


図 4.1-14　CIHR の公募ページにおける NSGRP への言及

[51] https://www.sshrc-crsh.gc.ca/funding-financement/cbrf-frbc/stage2-etape2/competition-concours/overview-eng.aspx

3）マギル大学における取り組み

■　概要

マギル大学は、研究セキュリティの側面で公式 HP において、カナダ政府の NSGRP に則る旨を述べており、研究セキュリティのリソースが整備されている。

そこから、少なくとも NSGRP に準拠した体制がとられているものと考えられる。

■　実施プロセス

NSGRP に準拠するとの記載があることから、同様のプロセスを踏襲しているものと思われる。

その他、マギル大学では、機密技術研究分野（sensitive technology research areas :STRA）に係る NSERC、SSHRC、および CIHR の助成金に申請する際のプロセスを解説しており、そこでは①研究助成金が STRA に当てはまるかどうかの確認②証明書フォームの記載というプロセスを踏んでいる。加えて、図において Tri-Council（カナダの主要 3 研究助成機関：NSERC、SSHRC、および CIHR）への研究助成金申請の際に、セキュリティやパートナー関係の要件を満たしているかを確認するプロセスについて解説している（図 4.1-15　Tri-Council への研究助成金申請における確認プロセス）。[52]

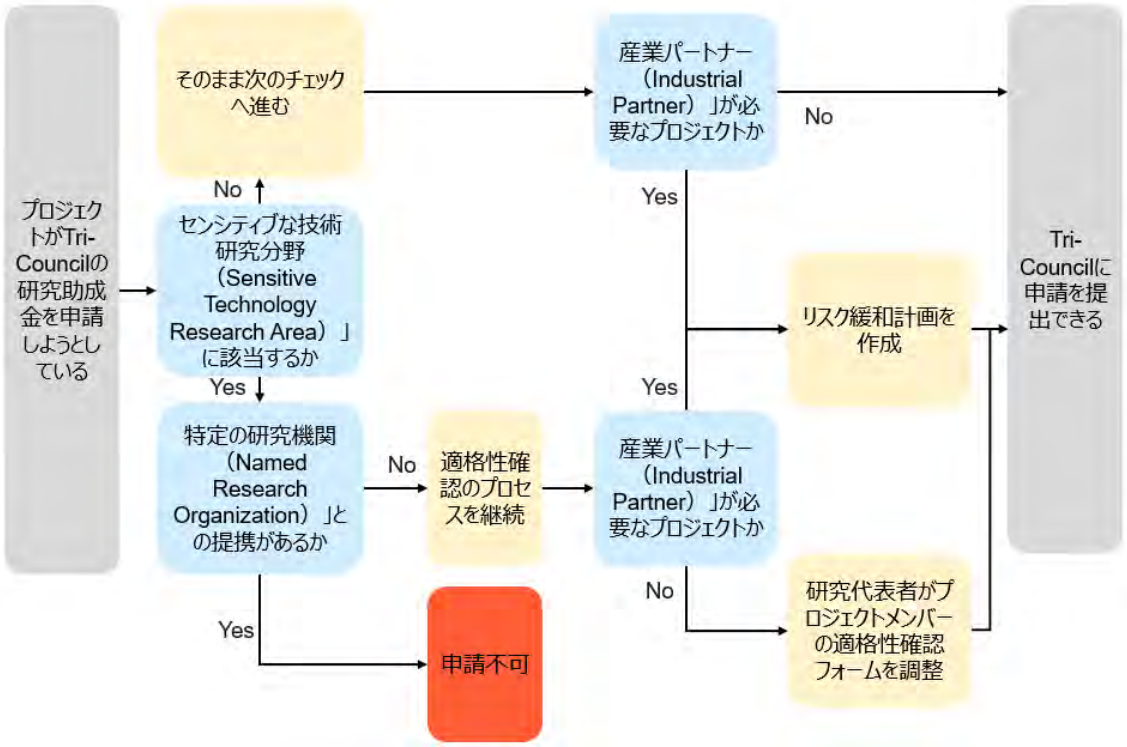


図 4.1-15　Tri-Council への研究助成金申請における確認プロセス

[52] https://www.mcgill.ca/research/research/researchsecurity

また、利益相反の開示プロセスについても図で解説しており（図 4.1-16　利益相反の開示プロセス）、①COI の開示②直属の上司に報告③研究関連か否かの確認、研究関連である場合は④研究イノベーション担当に連絡、研究関連でない場合は④‘学部長への報告⑤’学部長、副学部長に報告、というプロセスを踏むこととなっている。[53]

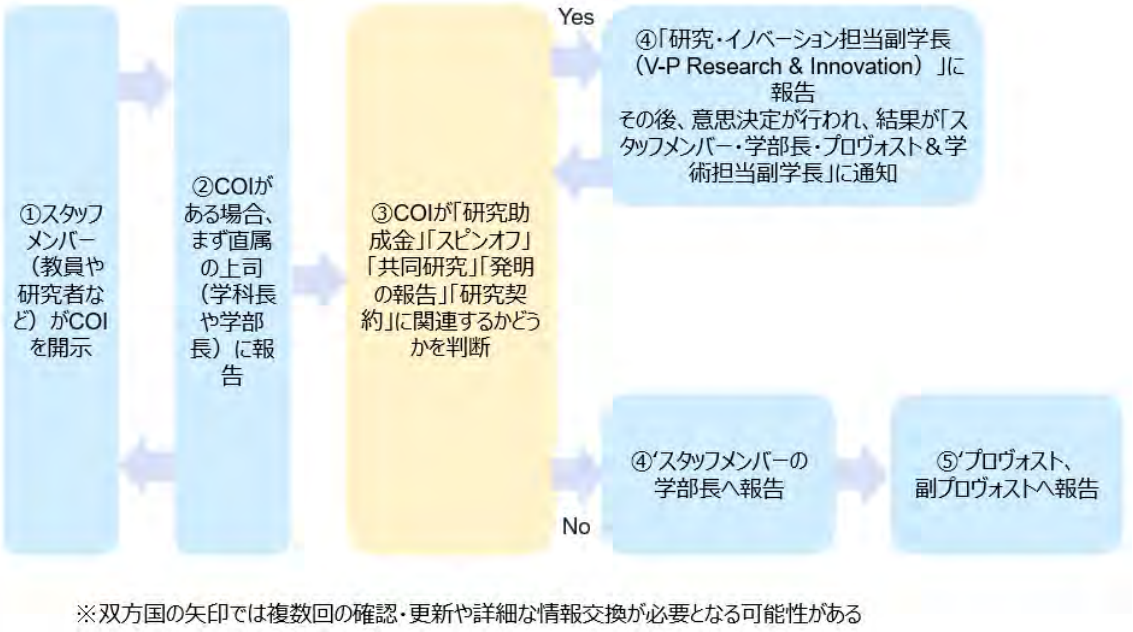


図 4.1-16　利益相反の開示プロセス

■　確認観点

NSGRP に準拠していることから、同規則の確認観点はマギル大学でも含まれているものと想定される。

また、マギル大学から STRA に係る NSERC、SSHRC、および CIHR の助成金に申請する際は、Sensitive Technology Research Areas list の確認を推奨している。

■　参照している情報ソース

NSGRP や NSERC、SSHRC、および CIHR に準拠していることから、同様の開示内容などを参照していると想定される。また、Sensitive Technology Research Areas list も情報ソースとして活用している。

[53] https://www.mcgill.ca/apo/forms/conflict-interest-reporting

（3）英国

英国では、2019 年以前に政府の外務委員会等で、中国をはじめとする外国勢力による大学への影響が問題視され、特に中国企業との連携が潜在的なリスクとして取り上げられ、国際的な研究協力が盛んに展開する一方、アカデミアや産業界が行う研究活動を通じた技術流出により、国家安全保障に重大なリスクを与えることが政府の安全保障部門に認識されてきた[54]。

それにより、2019 年に敵対的な行為者による干渉等も含め、英国の研究開発における知的財産、機密研究、人々、インフラを潜在的な盗難、操作、搾取から保護することを目的としてガイダンスやアドバイスの提供を実施するイニシアティブとして Trusted Research が開始され、以降 Trusted Research が中心となり、研究セキュリティ・インテグリティやデュー・ディリジェンスに関する取り組みが進められている。

そして Trusted Research の流れを受け、2021 年には英国政府の主要な政府資金提供機関である UKRI が、資金提供を受ける組織に期待されることを示す原則として Trusted Research and Innovation Principle を公開した。

上記政策動向を踏まえ公開情報を基に、英国において政府、資金提供機関、研究開発実施主体によって実施されている研究セキュリティ・インテグリティに係るデュー・ディリジェンスの取り組み・ガイドライン等を抽出した（表 4.1-37）。

表 4.1-37　詳細調査を行う取り組み・ガイドライン

取り組み主体	デュー・ディリジェンスに係る取り組み・ガイドライン
政府	Trusted Research ガイダンス群
資金提供機関	Due diligence guidance and supporting documents
研究開発実施主体	オックスフォード大学における取り組み

以下に表 4.1-37 に掲載した取り組み・ガイドラインについての詳細調査結果を示す。

1）Trusted Research ガイダンス群

■　概要

Trusted Research は、敵対的な行為者による干渉等も含め、英国の研究開発における知的財産、機密研究、人々、インフラを潜在的な盗難、操作、搾取から保護することを目的としてガイダンスやアドバイスの提供を実施するイニシアティブである[55]（表 4.1-38）。

NPSA の HP で Trusted Research のガイダンスが公開されており、特にデュー・ディリジェンスに関する内容を含んでいた学術界向けガイダンス、コラボレーションチェックリストを中心に調査を実施した。

[54] https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/109.pdf

[55] https://www.npsa.gov.uk/trusted-research

表 4.1-38　Trusted Research の概要

項目	概要
所管	・　NPSA（国家保護安全局（開始当時は CPNI）） ・　NCSC（国家サイバーセキュリティセンダー）
公表（更新）時期	2019 年開始
背景・目的	・　Trusted Research は、国際的な研究開発が活発に行われる中で、学術界・産業界の行う研究活動を通じた技術流出により、国家安全保障上のリスクが高まっている背景を踏まえ、NPSA（開始当初は CPNI）、NCSC が主体となって開始されたイニシアティブである ・　Trusted Research は、敵対的な行為者による干渉等も含め、英国の研究開発における知的財産、機密研究、人々、インフラを潜在的な盗難、操作、搾取から保護することを目的としてガイダンスやアドバイスの提供を実施するものである ・　テーマ 2 では、ガイダンスの中からオープンソース・デュー・ディリジェンスの実施に関連する情報が掲載されていた以下の資料を中心に調査した ✓　学術界向けガイダンス [56] ✓　コラボレーションチェックリスト [57]：
デュー・ディリジェンスの実施主体	・　大学の研究者、大学職員（学術界向けガイダンス、コラボレーションチェックリスト）
デュー・ディリジェンスの対象	・　研究パートナー、資金提供パートナー、自身の研究（学術界向けガイダンス）
デュー・ディリジェンスの実施タイミング	・　新たな研究や資金提供の協力を検討する際にデュー・ディリジェンスを実施することが推奨されている（学術界向けガイダンス）

■　実施プロセス

Trusted Research のガイダンス群では、確認観点や情報ソースについては記載されているものの、具体的なデュー・ディリジェンスの実施手順やプロセスについては確認できなかった。

■　確認観点

「学術界向けガイダンス」では、パートナーとの研究の適合性、法的な枠組み、自身の研究の有するリスク・ターゲットにされる可能性等について公開情報の収集を行うことを推奨している（表 4.1-39）。

表 4.1-39　学術界向けガイダンスにおける確認観点

確認観点	確認内容

[56] https://www.npsa.gov.uk/trusted-research-academia

[57] https://www.npsa.gov.uk/security-campaigns/trusted-research

パートナーとの研究の適合性(倫理的または国家安全保障上の懸念)	・ 組織、機関、団体に関して、懸念の原因となるような公開情報はあるか? ・ その情報を考慮すると、あなたが取り組む予定の研究分野で彼らと協力することで、より広範な応用や予期しない結果が生じる可能性があるか? ・ 研究パートナーが拠点を置く国の自由度と法の状態について、どのような情報が入手可能か? ・ 以下のようなリソースは、その判断に役立つ ✓ 米国輸出管理団体リスト ✓ 国連制裁リスト ✓ 国の汚職指数 ✓ 輸出に対する貿易制限 ✓ 人間の自由指数 ✓ 世界正義プロジェクト法の支配指数
法的な枠組み	以下のような法的な枠組みについて確認する必要がある ・ 輸出管理：あなたの研究は輸出管理の対象か ・ （外国の）法制：外国のパートナーが運用する可能性のある法的枠組みは何か、影響はあるか ・ GDPR：データと情報保護に責任を負うこと ・ 技術移転オフィス：技術移転を検討する場合、TTO（技術移転オフィス）にアドバイスを求めること ・ 国家安全保障投資法：2022 年に成立した NSI 法を順守すること
自身の研究の有するリスク・ターゲットにされる可能性	・ あなたの研究の応用に関して、倫理的または道徳的な懸念は潜在的にあるか? ・ あなたの研究は国内監視や弾圧など、英国と異なる倫理基準を持つ他国の活動を支援するために使用される可能性があるか? ・ あなたの研究は敵対的な国家軍に利益をもたらすか、あるいは他の国家主体に提供される可能性があるか? ・ あなたの研究には、軍事と非軍事の両方の用途があるか? ・ 研究のいずれかが英国または他の国の輸出許可規制の対象となる可能性はあるか? ・ 機密データや個人を特定できる情報を保護する必要があるか? これには、遺伝情報や医療情報、人口データセット、個人の詳細、商用テストデータなどが含まれる場合がある。 ・ あなたの研究は、あなたやあなたの組織が利益を得たいと思うような、将来的に商業化または特許取得可能な成果をもたらす可能性があるか?

また、「コラボレーションチェックリスト」においても、同様に研究自体の持つリスク、パートナー機関・パートナーシップの持つリスク、法的なリスク等について考慮するよう述

べられている（表 4.1-40）。

表 4.1-40　コラボレーションチェックリストにおける確認観点のイメージ

確認観点	確認内容
1.研究上の考察	・　研究はセンシティブか ・　研究はデュアルユースか ・　研究の応用先に倫理的・道徳的な懸念はあるか ・　第三者が研究を活用して英国の国家安全保障を損なう可能性はあるか ・　機密データや個人情報を扱うか
2.パートナーに関する考慮	・　パートナーは英国と民主主義的価値観・倫理基準が異なる国に所在、もしくは出身か ・　パートナーはオープンサイエンスに取り組んでいるか ・　独立性や自律性を損なう構造や関係はないか ・　軍・警察、治安機関との関係はあるか　等
3.法的考察	・　法的な制約（DPA、GDPR、ATAS 等）はあるか ・　輸出規制の対象となる要素はあるか、エンドユーザーリストにあるパートナーは含まれていないか ・　NSI 法の 17 分野に該当する研究はないか　等
4.制度上の配慮	・　大学の方針による制約はないか ・　この研究を行うために組織内でエスカレーションの必要はないか ・　外部機関（RCAT、ECJU 等）の意見を必要とする複雑な検討はあるか
5.評判への配慮	・　パートナーはなぜあなたと研究をしたいのか、その理由は明確か ・　パートナーはあなたの機関と価値観の一致しない団体に出資・連携していないか ・　パートナーは民事・刑事訴訟に巻き込まれているか ・　パートナーに透明性の欠如はないか ・　パートナーは国際的な規範から逸脱していないか
6.契約上の考慮事項	・　パートナーとの提携を進めることで、既存のパートナー等との間に利益相反は生じないか、 ・　パートナーとの提携を進めることで、既存の契約に違反しないか　等
7.知的財産に関する考慮事項	・　既存の知的財産を保護する必要はないか ・　パートナーは知的財産の侵害等で訴えられたことはないか ・　パートナーやその上位機関、政府などが、あなたの研究分野で知的財産を蓄積していないか ・　パートナーはあなたの知的財産を危険にさらす現地法の下で行動していないか　等
8.戦略的考慮事項	・　その協力は、英国に強みがある分野の能力や、国家安全保障を低下させないか ・　その協力は、あなたにパートナーへの財政的な依存を生み出さないか ・　あなたの研究は、外国の潜在的な悪意ある能力を強化しないか

■　参照している情報ソース

学術界向けガイダンスでは、パートナーとの研究の適合性、及び法的な枠組みの観点から

利用可能な公開情報や相談窓口のリソースを提供している（表 4.1-41）。

表 4.1-41　学術界向けガイダンスの提供している情報ソース

確認観点	細目	情報ソース
パートナーとの研究の適合性	—	・ 米国輸出管理団体リスト ・ 国連制裁リスト ・ 国の汚職指数 ・ 輸出に対する貿易制限 ・ 人間の自由指数 ・ 世界正義プロジェクト法の支配指数
法的枠組み（コンプライアンス）	輸出規制	・ 英国の戦略的輸出管理ガイダンスでは、英国の輸出管理に関する規制枠組みと、輸出ライセンスが必要になる可能性がある状況について詳しく説明している ・ 学術研究に適用される輸出規制 ・ 軍事技術または軍民両用技術の輸出：定義と範囲 ・ 英国の輸出ライセンス システムである SPIRE のツールとサービス。以下のものが含まれる ✓ 輸出したい品目が輸出規制の対象になっているかどうかを確認するための商品およびオープン一般輸出ライセンス（OGEL）チェッカー ツール。 ✓ エンド ユーザー アドバイス サービスでは、商品のエンド ユーザーが輸出ライセンスを必要とするかどうかを確認する。 ・ GOV.UK の武器禁輸、貿易制裁、その他の貿易制限の対象となる国のリスト。 ・ GOV.UK 軍事関連品目に適用される最終使用規制のリスト
	武器禁輸	米国から供給されたものを使用するかどうかは慎重に検討する必要がある。その場合、米国の輸出管理法の対象となる可能性もある。具体的には、次のとおり ・ ITAR（米国国際武器取引規則） ・ EAR（輸出管理規則）
	外国の法域におけるコンプライアンス	知的財産庁（IPO）は、他の国での知的財産の保護に関するアドバイスを提供している
	研究の出版と保護（特許申請）	・ 国家安全保障や公共の安全に悪影響を及ぼす技術 ・ 特許申請に対する国家安全保障チェック
	GDPR	ICO の Web サイト

2）Due diligence guidance and supporting documents[58,59]

Due diligence guidance and supporting documents は、UKRI の資金を活用する機関を含む、英国のあらゆる研究機関に向けて作成されたデュー・ディリジェンスのガイダンスであり、外国機関と契約する際のデュー・ディリジェンスプロセスを設定するためのガイドと質問票で構成されている（表 4.1-42、表 4.1-43）。

表 4.1-42　Due diligence guidance and supporting documents の概要

項目	概要
所管	UKRI
公表（更新）時期	2022 年 10 月公表
背景・目的	・Due diligence guidance and supporting documents は、UKRI から海外の研究機関と提携して研究や博士課程のトレーニングを実施する際のデュー･ディリジェンス要件に関する情報を提供するためにまとめられたものである ・本ガイド自体は「厳格な規則の規定を目的とするものではなく、研究機関が自らのリスク許容度や実施する研究やトレーニングの種類に応じた独自のポリシーとプロセスを開発できるようにすること」を目的としている一方で、UKRI の助成金の利用に関する規程である RGC 2.6/TGC 2.5 には「プロジェクト実施のために第三者を利用する場合、適切なデュー・ディリジェンスを実施すること」＊と示されているため、その際本ガイドが参照される可能性はあると考えられる ＊RGC2.6 には「UKRI International Due Diligence Guidance を参照」とあるが、現在リンク先は利用できなかった
デュー・ディリジェンスの実施主体	・UKRI（ガイドライン中に、UKRI が同等の質問票を用いている旨が記載されている） ・UKRI の資金を活用する機関：本ガイドは、UKRI の助成金およびトレーニング助成金の条件に関する規定である RGC 2.6/TGC 2.5 に根拠があることから、UKRI の資金を活用する機関は本ガイドを用いたデュー･ディリジェンスの実施主体であると考えられる ・英国のあらゆる組織：一方で、本ガイドには「あらゆる組織がデュー･ディリジェンスプロセスを設定する為に役立つ」とも記載されているため､英国で海外機関と提携する広範な組織に向けて作成されていると考えられる
デュー・ディリジェンスの対象	・英国の組織と連携する海外の機関、英国内の組織
デュー・ディリジェンスの実施タイミング	・UKRI への助成金の申請時 ・英国のあらゆる組織が海外機関と提携する際

[58] https://www.ukri.org/publications/due-diligence-guidance-and-supporting-documents/

[59] https://www.ukri.org/wp-content/uploads/2020/10/UKRI-201020-full-economic-costing-grant-terms-and-conditions-March-2020.pdf

表 4.1-43　Due diligence guidance and supporting documents の構成

構成	内容
①Due diligence: guidance for research organisations（研究機関向けのデュー・ディリジェンスガイダンス）	・あらゆる組織がデュー・ディリジェンスプロセスを設定するために役立つガイド
②Due diligence questionnaire (simplified) （デュー・ディリジェンス質問票（簡易版））	・資金調達のリスクが低い場合に使用される標準的なデュー・ディリジェンス質問票の簡易版 ・①には「先進国の研究集約型大学に対してデュー・ディリジェンスを実施する際に使用する」と記載されている
③Due diligence questionnaire (standard) （デュー・ディリジェンス質問票（標準））	・汚職認識指数に記載されている高リスクの分野でデュー・ディリジェンスを実施するときに使用される
④Due diligence questionnaire (enhanced) （デュー・ディリジェンス質問票（強化版））	・紛争が活発な領域では、標準的なデュー・ディリジェンスフォームに加えて使用される ・①には「資金が違法目的に使用されるリスクが高い場合やテロ活動のリスクが高い場合（FCDO（外務・英連邦・開発省）ウェブサイト参照 [60]）に、標準的なデュー・ディリジェンス質問票に加えて使用する」と記載されている

■　実施プロセス

Due diligence guidance and supporting documents におけるデュー・ディリジェンスプロセスは、ステップを 5 つに分け、契約の締結前～研究開発開始後に至るまで、実施すべきチェックや整備すべき組織体制について解説している（表 4.1-44）。

[60] 強化版の質問票を使用すべき「資金が違法目的使用やテロ活動のリスクが高い場合」について、FCDO では財務省と連携して、マネーロンダリングおよびテロ資金供与規制に基づき特定の国を「高リスク第三国」（High Risk Third Country：HRTC）として指定して、強化された顧客デュー・ディリジェンスを適用することを義務付けている https://www.gov.uk/government/publications/money-laundering-advisory-notice-high-risk-third-countries--2/money-laundering-advisory-notice-high-risk-third-countries--2

表 4.1-44　Due diligence guidance and supporting documents のデュー・ディリジェンスプロセス

ステップ	実施内容
ステップ１	・海外の研究機関との協力を検討する場合、研究者や指導員に速やかに知らせる ・組織内外での海外共同研究の経験者への相談、オンライン検索の実行、相手組織の拠点を置く国の汚職指数の確認、英国及び国連の制裁リスト、FCDO（外務・英連邦・開発省）サイトの確認、Dunn and Bradstreet（有料サービス）等の利用 ・ステップ１で重大な懸念事項が見つかった際は、別組織との連携を検討する
ステップ２	・協力先機関を決定した後は、質問票を活用してより詳細なチェックを実施する ✓ UKRI では先進国の研究集約型大学に対してデュー・ディリジェンスを実施する際に「デュー・ディリジェンス質問票（簡易版）」を使用している ✓ 資金が違法目的に使用されるリスクが高い場合やテロ活動のリスクが高い場合（FCDO ウェブサイトを参照）は「デュー・ディリジェンス質問票（標準）」に加えて「デュー・ディリジェンス質問票（強化版）」も使用する
ステップ３	・デュー・ディリジェンスで収集した情報は、組織内で最も適切である利害関係のない人々により確認される必要がある（エスカレーションルートのある研究室や財務スタッフなどが初期の段階では当たることがある） ・このプロセスで重大な問題が明らかになった場合、主導する研究機関は、リスクの進行/軽減に関する決定を、組織内で必要なレベルの権限を持つ関係者が行う必要がある（例：英国の複数の研究機関では、研究室、財務、助成金ホルダーのスタッフで構成される委員会で決定）
ステップ４	・デュー・ディリジェンスは、資金が提供されてからも続ける必要がある ・研究機関は、請求書/購入証明/進捗報告書の受領についてなど、海外の組織への資金送金に関するポリシーとプロセスを用意する
ステップ５	・財務チェックを行う：資金が交付目的のために使用され、請求された支出が助成金の条件に準拠していることを保証するために、UKRI は主導する組織が下請業者から請求された支出のチェックを実施することを期待している

■　確認観点

標準・簡易版の質問票では、相手組織に対してガバナンス体制やポリシー・プロセスの整備状況、過去の不正行為の有無や対処状況、下請業者の存在、実行能力について確認しており、強化版の質問票では、主に FCDO の求める要件として、テロリズム対策法に係る情報開示の可否等について確認している（表 4.1-45、表 4.1-46）。

表 4.1-45　質問票の内容（標準・簡易版）

確認観点	簡易版（Simplified）	標準（Standard）
組織ガバナンス	・　組織名、登録住所、所在国、法的地位 ・　他組織との提携関係、法務責任者の氏名等	簡易版に加え以下の内容 ・　公式／非公式を問わない他組織との提携関係 ・　研究関連事項に関する主要な連絡先
ポリシー・プロセス	以下の事項に関する管理状況、ポリシーの整備状況 ・　詐欺、賄賂、内部告発、旅費や付帯費用の管理、社会的弱者への保護、リスク管理、研究公正性・不正行為、データ及びサイバーセキュリティ	簡易版に加え以下の内容 ・　利益相反、健康と安全、倫理、スタッフ採用プロセス、財務手続き、個人情報・機密データの保護・管理、必要資材の調達
不正行為に関するリスク対応	・　過去 3 年間の研究資金に関する不正行為の疑いの有無、あった場合はその金額・処分状況 ・　過去 3 年間の研究不正行為の疑いの有無、あった場合はその処分状況	簡易版に加え以下の内容 ・　過去 3 年間の研究協力者からのクレーム・紛争、資金の返済、過失による研究の中断の有無、あった場合その詳細 ・　プロジェクトに影響を及ぼす可能性のある法的訴訟の有無 ・　上級職員による詐欺、不正、汚職の有無 ・　追加情報を要求できる連絡先
下請の管理	・　協力者や下請業者はいるか ・　いる場合、その組織に対して実施したチェックの詳細、組織への財務/支払いの管理方法の詳細	簡易版と同じ
実行能力	・　助成金の管理に使用する財務システム ・　期間中のプロジェクトに関する全取引リストの提出可否 ・　兼業スタッフの従事時間管理方法 ・　内部監査機能の海、実施方法等	簡易版に加え以下の内容 ・　助成金管理の能力：プロジェクトの財務独立性、スタッフの勤務時間の証明方法　等 ・　財務能力：外国為替リスクの管理方法、過去 3 年以内の内部・外部監査の受検の有無、保険加入の有無　等
プロジェクトガバナンス	・　簡易版には無し	・　プロジェクト特有のガバナンス体制、連絡先、第三者の受け取る金額の詳細、主要人物の家族との利益相反可能性　等

表 4.1-46　質問票の内容（強化版（Enhanced））

確認観点	内容
FCDO ポリシー	・ FCDO ポリシーでは、サプライヤー（対象事業者）は関連するテロ資金対策法に基づく義務を認識する必要がある ・ サプライヤーは、テロ対策法（Counter Terrorism legislation）に加えて、制裁規制にも準拠する必要があり、英国の制裁体制下での政府関係者/組織に対する国連制裁および英国の制裁（資産凍結）を回避するためのアドバイスを求める必要がある
	・ 英国法、主に 2000 年テロリズム法（Terrorism Act 2000）のテロ資金提供に関する sections 15-18 では、テロ目的で使用される、またはその可能性があると合理的に疑う理由がある場合に資金または財産を提供することは違法とされている。section 19 では、テロ資金提供を含むテロ行為に関する情報を開示しないことは違法とされている。
	・ プロジェクトに携わるスタッフは、制裁対象組織（またはその他のテロ組織）とは一切関係がないことを保証できるか
デュー・ディリジェンスチェック	・ リスク管理ポリシーは整備されているか ・ 整備されていない場合は、下流のパートナーがテロ資金供与のリスクを管理する方法を示すこと
	・ テロ資金供与を含む詐欺や金融犯罪の疑いがすべて報告されるための報告機能を備えた報告ポリシーはあるか
	・ パートナーは資金（税金やその他の賦課金を含む）を渡すつもりがあるか ・ 該当する場合は、報告とチェックに含まれるようにすること。ハマスやその他のテロ組織に資金が渡らないように、下流パートナーもチェックを行っていることを示す必要がある
	・ 下流パートナーの採用、選定、評価のための堅牢で透明性の高いシステムがあることを確認するための詳細を記入すること。これには下流パートナーと従業員を制裁リストに照らして審査することを含めることができる

■　参照している情報ソース

ガイダンスで参照される情報ソースとしては、非政府機関や政府機関の Web サイト、民間の情報サービスなどを参照して、主にデュー・ディリジェンス対象組織が拠点を置く国における汚職や違法な取引のリスク等を分析することを推奨している（表 4.1-47）。

表 4.1-47　Due diligence guidance and supporting documents で参照される情報ソース

名称	種別	概要	デュー・ディリジェンスでの活用
Corruption Perceptions Index（腐敗指数インデックス）	民間	・ 非政府組織トランスペアレンシー・インターナショナルの運営する、世界各地の公務員と政治家の、汚職に関する評価指数	・ ステップ 1 において、対象組織の拠点を置く国の汚職指数の確認に活用できるとしている
FCDO Web サイト	政府機関	・ FCDO（外務・英連邦・開発オフィス ）の Web サイト	・ ステップ 1 において対象国の組織との契約に係るリスクの判断に活用できるとしている ・ ステップ 2 において、金が違法目的に使用されるリスクが高い場合やテロ活動のリスクが高いケースの判断に活用できるとしている
英国および国連の制裁リスト	政府機関	・ 英国のマネーロンダリング防止法に基づく制裁リストや、国連安保理の制裁対象リスト等を指すと想定される（明確に URL 等は指定されていない）	・ FCDO の Web サイトと併せて、対象国の組織との契約に係るリスクの判断に活用できるとしている
Dunn and Bradstreet	民間	・ ビジネスに関する商用のデータベース・分析サービスを提供する米国企業のサービス ・ 制裁や監視リスト、メディア、訴訟、先取特権、破産などのデータを組み合わせてベンダー評価に活用できる（有料）	・ ステップ 1 において、「重要な公的地位を有する者（PEP）＊」の特定に活用できるとしている

3）オックスフォード大学における取り組み

オックスフォード大学は、QS 世界大学ランキングにおいて世界 3 位に位置づけられており、研究セキュリティの側面では、公式ホームページにおいて、Trusted Research を参照している。[61]そのため、Trusted Research に準拠した体制がとられているものと考えられる。

■ 実施プロセス

Trusted Research に準拠するとの記載があることから、同様のプロセスを踏んでいるものと思われる。

■ 確認観点

Trusted Research に準拠していることから、同規則の確認観点は利益相反の確認等の際含まれる。

■ 参照している情報ソース

Trusted Research のリソースである、同様の開示内容及び、国連制裁リストや国の汚職シスなどを参照している。[62]

[61] https://researchsupport.admin.ox.ac.uk/trusted-research

[62] https://researchsupport.admin.ox.ac.uk/trusted-research

（4）EU

EU では、2021 年 5 月に、変化する世界情勢における国際協力に向けた政策文書として「研究とイノベーションにおけるグローバルアプローチ」を公表し、その中で EU の研究機関や高等教育機関を標的とした外国の干渉に対処するためのガイドラインを提示する予定であると述べられた。そして 2022 年 1 月には、言及されたガイドラインとして、EU 内の大学や研究機関が外国との協力においてリスクを防止するために推奨される行動を提示する「研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書」が公表された[63,64]。

また、2024 年 1 月には、「欧州経済安全保障の進展：５つの新たなイニシアティブの導入」と題する 5 つのイニシアティブを含む政策文書が発表され、その中で「研究セキュリティ向上のための EU 指針」が提案され、同指針は 5 月に採択された。同指針では、今後研究機関に対してパートナー組織へのデュー・ディリジェンスの実施支援のためのリソースやツールを開発するとしていることから、より具体的なガイダンスが今後提供されるものと想定されている[65,66,67]。

上記政策動向を踏まえ公開情報を基に、EU において政府、資金提供機関、研究開発実施主体によって実施されている研究セキュリティ・インテグリティに係るデュー・ディリジェンスの取り組み・ガイドライン等を抽出した（表 4.1-48）。

表 4.1-48　詳細調査を行う取り組み・ガイドライン

取り組み主体	デュー・ディリジェンスに係る取り組み・ガイドライン
政府	研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書
資金提供機関	・　DFG 勧告 ・　BMBF のポジションペーパー（補足）
研究開発実施主体	ミュンヘン工科大学における取り組み

以下に表 4.1-48 に掲載した取り組み・ガイドラインについての詳細調査結果を示す。

63 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A252%3AFIN

64 https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2465

65 https://www.eu.emb-japan.go.jp/files/100726114.pdf

66 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363

67 https://www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/?DocumentNumber=9097%2F24

1）研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書

■　概要

「研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書（Tackling R&I foreign interference staff working document）」は、欧州委員会　研究イノベーション総局（DG-RTD）から発出された、EU 内の大学や研究機関が外国との協力においてリスクを防止するために推奨される行動を提示するものである[68]（表 4.1-49）。

表 4.1-49　研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書の概要

項目	概要
所管	欧州委員会　研究イノベーション総局（DG-RTD）
公表（更新）時期	2022 年 1 月
背景・目的	・　本作業文書は、EU 外の主体との協力において不当な影響から身を守ろうとしている大学や研究機関を支援するためのツールキットとして策定されたものである ・　価値観、ガバナンス、パートナーシップ、サイバーセキュリティの 4 つのテーマを中心に構成されており、各トピック領域ごとに具体的な行動勧告が提示されている。大学や研究機関は、これらを使用して、第三国による望ましくない影響から身を守るための対策を策定することができるが、規制的な拘束力はなく、必ずしも網羅的ではないとしている
デュー・ディリジェンスの実施主体	・　EU 内の大学や研究機関
デュー・ディリジェンスの対象	・　EU 外の主体
デュー・ディリジェンスの実施タイミング	・　パートナーシップにおける契約の準備段階

作業文書の中では、価値観、ガバナンス、パートナーシップ、サイバーセキュリティの 4 つのテーマにおいてとることが望ましいリスク緩和策が説明されている。テーマ 2 では、「パートナーシップ」のテーマにおいて推奨されているデュー・ディリジェンスについて記載する（表 4.1-50）。

[68] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-publishes-toolkit-help-mitigate-foreign-interference-research-and-innovation-2022-01-18_en

表 4.1-50　4 テーマにおける推奨される行動の例

テーマ	大項目	緩和策の例
価値観	①学問の自由が危機に瀕している国やパートナー機関の特定	・ 学問の自由指数を参考にする ・ パートナーの教育・研究・制度の調査、評価を行う
	②自組織の脆弱性評価を実施する	・ 外部アクターとの依存関係を確認する
	③個人・組織レベルの学問の自由と高潔さへのコミットメントを強化する	・ 研修の提供 ・ 学問の自由・インテグリティを教育のコアカリキュラムに組み込む
	④抑圧的な環境にあるパートナーとの協力を継続する	・ 非自由主義的な環境にある学生や同僚、組織を疎外しない ・ 倫理手続きの見直し
ガバナンス	①海外からの干渉に対する行動規範を公表する	・ 外国干渉の特定、内部告発者の保護などの手順を含める
	②外国干渉委員会の設置	・ 既存の組織に外国干渉委員会を組み込む
パートナーシップ	①リスクマネジメントを実施するための一般的な前提条件を策定する	・ 輸出管理法や外国直接投資に対する知識を深める ・ パートナーシップに潜在するリスクへの認識を組織内で広める
	②強固なパートナーシップ協定の策定手順を確立する	・ **デュー・ディリジェンスの実施**
サイバーセキュリティ	①サイバーセキュリティリスクに対する認識を高める	・ データ保護技術に対するトレーニングを実施する ・ サイバーハイジーンに関する教育・訓練の実施
	②外国からの妨害行為者によるサイバーセキュリティ攻撃を検知・防止する	・ OSINT 調査を定期的に設定・実行、アラートを立てる ・ サイバーセキュリティ認定機器を調達する
	③外国の干渉によるサイバーセキュリティ攻撃に対応し、そこから回復する	・ 教訓を共有し、ブラックリストやレピュテーションシステムを更新 ・ インシデント対応計画を策定する

■　実施プロセス

スタッフ作業文書は、パートナーシップの締結において確認しておくべきリスクや組織として整備するデュー・ディリジェンスの仕組みを推奨しているものの、デュー・ディリジェンス自体の実施プロセスは示していない。

■　確認観点

作業文書では、デュー・ディリジェンスにおいてパートナー機関の関心事項や活動状況、政府当局や軍事機関との関係性、輸出管理や外国投資規制等の関連法規の適用といった情報を収集することを推奨している。

【作業文書において収集することが推奨されている情報】

- パートナー機関の所属国におけるセキュリティ全般、データ共有、研究倫理、知的財産保護などに関する法律や規則。当該研究プロジェクトは現地法の対象となるか？また、それはパートナーシップにどのような影響を及ぼすか？
  - ✓　（潜在的な）商業活動や関心を含む、パートナー機関の活動や関心事項
  - ✓　パートナー機関・研究者の軍事機関や企業との関係、怪しい活動への関与など。言語の専門家を関与させて現地語で情報収集を行うことを推奨
  - ✓　パートナー機関と政府当局との関係：地方政府からの独立性など
  - ✓　パートナー機関の意思決定構造、手順
  - ✓　国境を越えた協力関係や、欧州の規範や価値観の遵守に関するパートナー機関の実績。過去に関与した外国干渉の事例を含む
  - ✓　透明性のレベル、研究倫理と学問の自由の遵守を保証する手続きを含む、学術的誠実さへのコミットメント
- 加えて、関係する研究者は以下を考慮すべきである：
  - ✓　研究成果がデュアルユース技術に使用される可能性や、経済的、安全保障的、社会的利益の強化を目的とした EU または国の政策に沿わない目的に使用される可能性
  - ✓　プロジェクトへの欧州デュアルユース規則 821/202153、EU のデュアルユース管理リストの年次改正、対応する各国の輸出管理法、関連する欧州委員会の勧告、外国直接投資審査規則などの関連規則の適用
  - ✓　プロジェクトの計画について、高等教育機関/研究・職業教育機関の中央レベルまたは特定の委員会に報告または提示する必要があるかどうか
  - ✓　教育における連携の場合：カリキュラムは、質および学術的誠実性の観点から、機関（自身）の要件を満たしているか。

■　参照している情報ソース

作業文書では使用が推奨されるデータベースや検索ツールなどは示されていないが、大学・研究機関が確認すべき EU の関連規則等を示している（表 4.1-51）。

表 4.1-51　作業文書において参照されている関連規則

規則名称	概要
欧州議会および理事会の 2021 年 5 月 20 日付規則（EU）2021/821、デュアルユース物品の輸出、仲介、技術支援、通過および移転の統制に関する連合体制の設立	軍民両用品目の輸出、仲介、技術支援、輸送、移転を管理する EU 体制を確立するための規則
毎年改正される EU のデュアルユース管理リスト（最新 2020/1749）を含む委任法令	EU のデュアルユースの規制リストは、国際的な不拡散体制で合意された変更を反映するために、委任法令を通じて毎年更新されている
規則 428/2009 に基づくデュアルユース貿易管理のための内部コンプライアンスプログラムに関する欧州委員会勧告 2019/1318	デュアルユース貿易管理のための内部コンプライアンスプログラム（ICP）を確立するためのガイダンスを提供する勧告
EU への外国直接投資のスクリーニングの枠組みを定める欧州議会および理事会による 2019 年 3 月 19 日付規則(EU)2019/452	EU の安全と公共秩序を保護するために、EU への外国直接投資（FDI）を審査するための枠組みを確立するための規則
EU による特定の第三国を対象とする制限措置、特定の第三国における制裁対象の自然人および法人、事業体、団体のリスト	EU は特定の外交政策および安全保障上の目的を達成するために、特定の第三国、団体、個人を対象とした武器禁輸や資産凍結、渡航禁止等の制限措置（制裁）を課している

2）DFG 勧告（国際協力におけるリスクへの対処）

■　概要

ドイツの主要な資金提供機関である DFG（Forschungsgemeinschaft：ドイツ研究振興協会）は国際研究協力においてパートナー組織について考慮すべき事項を勧告しており、今後 DFG の資金提供における審査や意思決定プログラムにも組み込まれる可能性があると述べている（表 4.1-52）。

表 4.1-52　DFG 勧告の概要

項目	概要
所管	DFG（Forschungsgemeinschaft：ドイツ研究振興協会）
公表（更新）時期	2023 年 9 月採択
背景・目的	・ 2023 年 9 月に政府系の資金提供機関である DFG は国際研究協力に関する勧告を発行し、申請者にもその内容の慣行を期待すると述べた ・ 勧告では研究者が国際的なパートナーとのプロジェクトに申請する前に自問すべき推奨事項を提供しており、今後 DFG の審査や意思決定プロセスにも含まれる可能性があるとして、現在は DFG の提案作成ガイドライン 4.1.5 章「リスクと利益の検討における、安全保障に関連する可能性のある側面（「懸念されるデュアルユース研究」）の説明」を参照するように述べられている

	・ 勧告中では言及されていないが、勧告の詳細事項として欧州委員会の「研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書」を参照していることから、影響を受けているものと思料される
デュー・ディリジェンスの実施主体	・ DFG への助成金を申請する研究者
デュー・ディリジェンスの対象	・ パートナー機関
デュー・ディリジェンスの実施タイミング	・ ―（今後、DFG の申請プロセスに組み込まれる予定）

■ 実施プロセス

勧告では、後述の研究者へ確認を推奨する観点を示しているが、デュー・ディリジェンスの実施プロセスまでは示していない。

■ 確認観点

DFG 勧告では、研究者が国際的なパートナーとの協同プロジェクトに申請する前に自問すべき事項を、研究対象と研究契約の観点から提示している（表 4.1-53）。

表 4.1-53 DFG 勧告が研究者へ推奨している質問

観点	自問すべき事項
研究対象	・ 研究分野においてパートナー国への依存はあるか？その場合、それはどのようなものか？代替の協力パートナーは存在するか? ・ 得られた結果や生成された知識が第三者によって悪用される可能性はあるか? ・ パートナーはプロジェクトを超えた目標を追求しているか?結果はどのような目的で使用される可能性があるか?
研究契約	・ パートナー機関は軍事目的または類似の目的で研究を行っているか? ・ 協力国の政治情勢を考慮すると、研究データや研究活動から得た経験を体系的に収集することは考えられ、あるいは期待できるか? ・ プロジェクト参加者の権利と義務、および共同プロジェクトの実施に関する書面による合意の締結を妨げる状況はあるか? ・ 書面による合意には法的効力がないと考えられる理由はあるか? ・ 例えば、プロジェクト成果の公表に関して、学問の自由が制限される可能性はあるか？

■ 参照している情報ソース

勧告及び現在の DFG の提案作成ガイドラインでは、使用が推奨されるデータベースや検索ツールなどは示されていないが、確認すべき EU、ドイツの関連規則等を示している[69]（表 4.1-54）。

[69] https://www.dfg.de/resource/blob/168314/9c1a931f2b58c0ec2ccfa7023fb687c7/54-01-en-data.pdf

表 4.1-54　DFG の提案作成ガイドライン

観点	自問すべき事項
戦争兵器管理法（Kriegswaffenkontrollgesetz）	ドイツ国内での軍事目的の兵器の開発・製造・取扱い・移転などを管理し、国際平和および安全保障を維持することを目的として、「戦争兵器」として定義したものの製造、取得、販売、輸出入、譲渡、または保管するには、連邦政府（原則として連邦経済省が主管）からの許可を必要とするもの
EC 規則第 428/2009 号	デュアルユース品目の輸出管理について EU 全体で共通の枠組みを定めるためのもの
外国貿易・支払法（Außenwirtschaftsgesetz） 外国貿易・支払条例（Außenwirtschaftsverordnung）	ドイツにおける外国貿易（輸出入・サービス取引・資本取引など）全般を規律する基本法であり、国家安全保障や対外政策上の理由から貿易を規制・監視する権限を連邦政府に付与するもの

3）BMBF のポジションペーパー

ドイツ連邦教育研究省は、2024 年 3 月に研究セキュリティを強化するための 3 つの目標と今後の施策検討内容を述べたポジションペーパーを発出した。具体的な要領が示されているわけではないが、ポジションペーパーの中でデュー・ディリジェンスに相当する内容の施策検討の可能性についても述べられている。

ポジションペーパーは、世界がロシアのウクライナ侵攻や多極化、サイバー脅威、中国を中心とした体制の台頭といったツァイテンヴェンデ（Zeitenwende : 歴史の転換点）にあるという認識のもと、学問の自由と安全保障政策の利害を結びつける戦略的なアプローチの第一歩として BMBF から発出されたものである。

ポジションペーパーでは、BMBF が研究セキュリティを強化するための 3 つの目標と今後の施策検討内容を述べている（表 4.1-55）。

表 4.1-55　ポジションペーパーにおける施策検討内容

目標①：利用可能な手段、構造、手順の効率性と有効性を高める：自主規制の強化と専門化を進める	
1	時代の転換を踏まえた科学界の自主規制手段の再検討と、必要に応じた修正
	・　安全保障関連研究合同委員会（GA）や安全保障関連研究倫理委員会（KEFs)による多面的な課題への対処が必要 ・　近い将来、既存規制のレビュープロセスを経て、**機関横断的な手続きやプロセスを試行・導入**する（例：大学と研究機関が輸出管理について協力するなど） ・　レビューの場としては、ドイツ科学団体連合（DFG）などが考えられる
目標②：知識と意識の強化	
2	研究セキュリティに関する共通ガイドラインの策定
	・　研究セキュリティに関連する問題や手続きに関する科学界の感度を高め、自己規制を強化するため、BMBF は科学界が**研究セキュリティに関する共通のガイドラインを策定**することを支援する ・　検討するガイドラインの例は以下： ✓　**デュアルユース関連性についての研究者の義務検討のためのガイドライン。異なる TRL や研究分野に対し段階的なルールシステムが有用かどうか検討** ✓　**ドイツの大学／科学機関と国際的パートナーとの協力に関するガイドライン** ✓　**科学機関の全職員を対象とした、外部スタッフとの取引における秘密保持義務、特にデータセキュリティに関するガイドライン** ✓　**各機関と治安当局、入国管理局などとの協力のためのガイドライン** ✓　**リスクに応じて研究情報・データへのデジタルおよび物理的なアクセスを、知る必要性に基づいて管理するための下位ドライン**
3	研究の安全性に関する疑問に対する情報基盤の改善、クリアリングハウスの必要性の検討
	・　全ての研究者と機関が研究セキュリティに関する関連情報や背景知識に可能な限りアクセスできるようにする ・　例えば、**研究セキュリティの問題を扱う中央情報プラットフォーム**がリスクが疑われる／リスクの高いケースのデータベースやその他情報を収集するなど ・　一つのモデルとして、オーストラリア戦略政策研究所（ASPI）が開発した**「Chinese Defense University Tracker」**などが考えられる。 ・　さらに、科学、省庁、安全保障機関の間のインターフェイスとして機能する**中央クリアリングハウス**の必要性を、科学界とともに検討する必要がある ・　中央コンプライアンス相談室のような機関の設立も検討される

目標②：知識と意識の強化	
4	機密技術の特定、連邦政府にとって特に関心のある研究分野の定義
	・ 欧州委員会が発表したEUの経済安全保障にとって重要な技術分野のリスト（ 2023 年 10 月 3 日 付 C(2023) 6689final の付属文書）等を踏まえて、ドイツ経済の主要部門にとって、**潜在的なデュアルユース性**や**卓越した重要性**などの理由で**関心を集める機密技術のリスト**が、連邦政府によって作成される
5	情報機関による情報収集に対する科学システムの耐性を強化
	・ 特に人的情報源やデジタル（通信）インフラの侵害・監視を通じた**外国の諜報機関による情報収集に対する科学システムのレジリエンスを向上**させる ・ この目的のために、**科学界の責任者やスタッフの啓発**が必要
6	科学機関依存関係に関する透明性の創出
	・ 公的研究機関や大学の責任主体は、海外（第三者）からの**資金提供や、その結果生じる依存状態について把握**しておく必要がある ・ この目的のため、第三国からの資金提供は、関連性が一定の基準を超える場合に開示されることになっている
目標③：民間研究と軍事研究の相乗効果の活用	
7	時代の転換期における民事条項の妥当性についての考察
	・ **軍事研究と民生研究のより良い統合の可能性**について、各州およびドイツ科学団体連合（AFG）、ドイツ学長会議 （HRK）との協議プロセスで検討される
8	民間研究と軍事研究の協力強化
	・ 研究セキュリティとドイツの研究能力に関連する知識をより広範な基盤に置き、学際的・横断的な協力を強化するために、**民間と軍の研究機関の交流と協力を強化**する ・ このために、BMBF はすべての関係省庁に対し、民間研究機関と軍研究機関との共同プロジェクトにどの程度重点を置くことができるかを検討するよう要請する

4）ミュンヘン工科大学における取り組み

■　概要

ミュンヘン工科大学（TUM）は、2022 年 11 月に学問の自由を維持しながら国際協力におけるリスクを管理するための方針として「TUM グローバルエンゲージメント原則：強靭な国際関係の構築」を策定した。

当該文書では、ドイツ学長会議の勧告や欧州委員会の「研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書」についても参照しており、国レベルおよび EU レベルの推奨事項に沿って、研究セキュリティ・インテグリティの確保に努めていることが確認できる[70]。

■　実施プロセス

「TUM グローバルエンゲージメント原則：強靭な国際関係の構築」は、TUM における国際協力のリスク管理方針や、TUM の研究者に対する質問事項などを整理しているが、具体的なデュー・ディリジェンスの実施プロセスについては確認できなかった。

■　確認観点

「TUM グローバルエンゲージメント原則：強靭な国際関係の構築」では、網羅的な基準やチェックリストではないとしつつ、国際協力におけるリスク管理を支援するための以下のような質問を列挙している。

【TUM グローバルエンゲージメント原則：強靭な国際関係の構築における質問事項】

1. パートナー機関とその機関が活動する特定の状況（安全性、政治的干渉、資金源など）について十分な知識がありますか？
2. 国際的なパートナーは、TUM の目的と共通した学術的および制度的目的を持っていますか？
3. あなたのパートナーシップは、あなたのユニット、学校での同様の活動に関連していますか？協力の可能性とリスクの評価を裏付けるものは何ですか？あなたの国際貢献に貢献してくれる同僚は誰ですか？
4. パートナー機関と TUM の両方において、パートナーシップの下で学問の自由をどのように守るかについて疑念はありますか？
5. 他のローカルまたは国際的な利害関係者との関係に影響を与える可能性のある力関係や不均衡を認識していますか?それともパートナー機関とコラボレーションパートナーの機関としての自主性でしょうか？
6. あなたのパートナーは気づいていますか TUM の研究行動規範？
7. あなたのコラボレーションには、それぞれ輸出管理と二重使用に関連する可能性のある機密性の高いトピックが含まれていますか？
8. 関連する制裁リストの事前協議によって、国際協力が制限されたカテゴリーに該当しないことを確認しましたか？
9. 研究協力への資金提供はどのように組織されていますか？また、そのような資金への公平なアクセスに関して潜在的な不均衡をどのように評価していますか？
10. 共同で生成された研究データと結果へのアクセスをどのように評価していますか？制限が予想される場合、レッドラインをどのように定義しますか？

[70] https://www.international.tum.de/fileadmin/w00bwe/www/Das_TUM_G_A_Office/TUM_Global_Engagement_Principles.pdf#:~:text=TUM%20Global%20Engagement%20Principles%20Building,Resilient%20International%20Relationships%20November%202022

■　参照している情報ソース

「TUM グローバルエンゲージメント原則：強靭な国際関係の構築」は、TUM における国際協力のリスク管理方針や、TUM の研究者に対する質問事項などを整理しているが、具体的なデュー・ディリジェンスの情報ソースについては確認できなかった。

（5）豪州

豪州における研究セキュリティ・インテグリティの確保やデュー・ディリジェンスに関する政策は、中国を念頭に置いた外国からの不当な干渉に対抗することを目的として展開されている[71]。

2017 年頃までの中国企業とのダーウィン港の賃貸契約や、親中の上院議員の中国からの献金の発覚等により、中国からの干渉に対する危機感が強まったことで ASIO（オーストラリア保安情報機構）長官が中国を念頭に大学への外国政府の干渉を警告した。

そのような中、豪州の大学に対する外国からの不当な影響力に対抗するため、政府と大学・研究機関で協働する大学対外干渉タスクフォース（UFIT）が 2019 年 8 月に設立され、同年 11 月には「オーストラリアの大学分野における外国の干渉に対抗するためのガイドライン」が公表された。

そして 2022 年には政府の情報・安全保障に関する議会合同委員会（PJCIS）は高等教育・研究セクターに影響を及ぼす国家安全保障上のリスクに関する調査を 2020 年に開始、2022 年には報告書を政府に提出し、それに基づき大学へ UFIT を通じた積極的な透明性に係る活動の実施等 27 の勧告を行った。

上記政策動向を踏まえ公開情報を基に、豪州において政府、資金提供機関、研究開発実施主体によって実施されている研究セキュリティ・インテグリティに係るデュー・ディリジェンスの取り組み・ガイドライン等を抽出した（表 4.1-56）。

表 4.1-56　詳細調査を行う取り組み・ガイドライン

取り組み主体	デュー・ディリジェンスに係る取り組み・ガイドライン
政府	豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン
資金提供機関	ARC（豪州研究会議）の取り組み
研究開発実施主体	ニューサウスウェールズ大学における取り組み

以下に表 4.1-56 に掲載した取り組み・ガイドラインについての詳細調査結果を示す。

1）豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン[72]

■　概要

1）豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン（以下、ガイドライン）は、豪州の大学セクターにおける外国の干渉に対するレジリエンスを高めるために、大学等による外国干渉リスクの管理・対処に役立つように UFIT によって開発され、ガイドライン本文及びそれをサポートするガイダンス資料から構成されている。

研究活動、外国のパートナー及び自組織の職員・学生等を対象としている点が特徴的である（表 4.1-57）。

[71] https://www.mof.go.jp/public_relations/finance/202203/202203h.html

[72] https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector

表 4.1-57　豪州の大学セクターにおける外国の干渉に対抗するためのガイドラインの概要

項目	概要
所管	大学対外干渉タスクフォース（UFIT）
公表（更新）時期	2019 年公表、2021 年更新
背景・目的	・　本ガイドラインは、大学セクターにおける外国の干渉に対するレジリエンスを高めるために、リスクの管理・対処に役立つように開発された ・　ガイドラインは、豪州の大学が既に実施しているリスク管理ポリシーとセキュリティ慣行を基盤として、意思決定者が外国の干渉によるリスクを評価できるように設計された ・　ガイドラインは、大学・研究機関がリスク管理を実施する上で重要なテーマを以下の 4 項目から解説しているほか、ガイドライン（PDF）をサポートするガイダンス資料（Web 上で公開）とともに参照される ①　ガバナンスとリスクのフレームワーク ②　コミュニケーション、教育及び知識共有 ③　デューディリジェンスやリスク評価、リスクマネジメント ④　サイバーセキュリティ
デュー・ディリジェンスの実施主体	・　豪州の大学や学術機関（特に意思決定者）
デュー・ディリジェンスの対象	・　外国からの干渉を受けるリスクのある研究活動、パートナー、大学職員、研究生
デュー・ディリジェンスの実施タイミング	・　（本ガイドラインは、既存の大学のポリシーに合わせて参照するように記載されていることから、大学が外国とかかわりのある研究活動を実施する際などが想定される）

ガイドラインは本文及びそれをサポートするケーススタディやツール等のガイダンス資料から構成されており、テーマ 2 の調査では、特に本文「3. デュー・ディリジェンス、リスク評価及び管理」とその補足ガイダンス資料、及びテンプレートとツールの「ファクトシート - オープンソース情報」「デュー・ディリジェンス支援フレームワーク」といったデュー・ディリジェンスの実施に関係する内容を中心に調査・整理を実施した（図 4.1-17）。

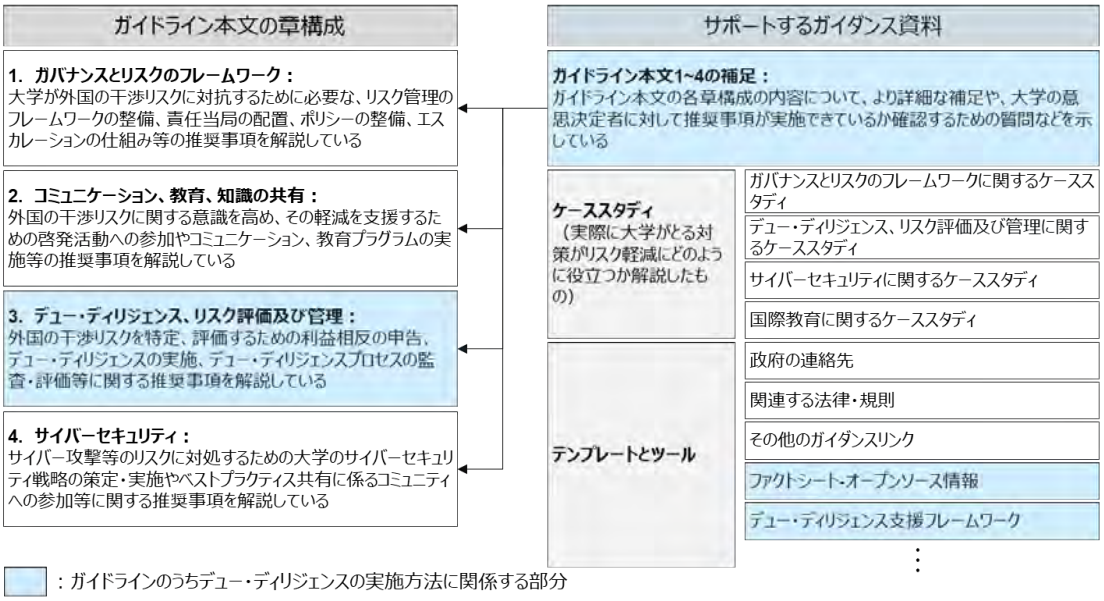


図 4.1-17　ガイドラインの構成

■　実施プロセス

ガイダンスではデュー・ディリジェンスの具体的な実施プロセスは示されていないが、大学が役立てることを想定したプロセスマップである「デュー・ディリジェンス支援フレームワーク」が提供されており、パートナーと技術の両側面のリスクと、法的な義務や補完的制度を確認するプロセスが求められていることが確認できる[73]（図 4.1-18）。

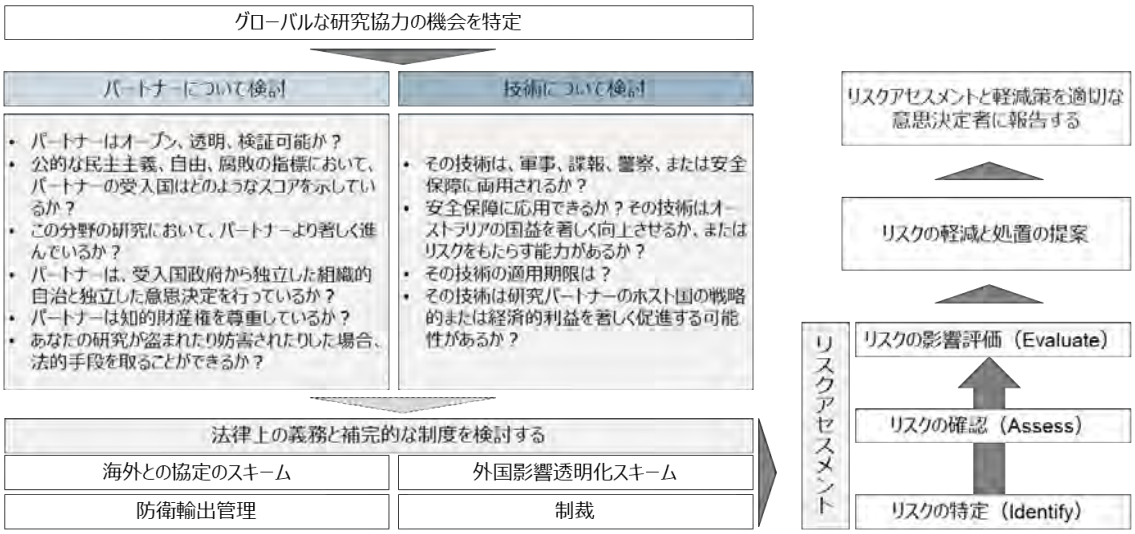


図 4.1-18　デュー・ディリジェンス支援フレームワークのプロセス

[73] https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/templates-and-tools

■　確認観点

ガイドライン本文では、自組織の教職員・パートナーに関する身上事項、技術・研究の持つポテンシャル等のデュー・ディリジェンスの確認観点を以下のように示している。

＜ガイドライン本文「3.　デューデリジェンス、リスク評価および管理」の記載概要＞

3.1　大学は、外国の干渉を受けるリスクがある教職員に対し、外国との提携、関係性、金銭的利益の特定を含む利益相反の申告を義務づける

3.2　大学は、意思決定者に外国の干渉リスクを知らせるためにデュー・ディリジェンスを実施する

3.2.1　大学は、パートナーおよび職員に対してデュー・ディリジェンスを実施する

潜在的なパートナーや職員をさらに評価し理解するための追加チェックの観点として、以下を含めることができる

- 所有権構造と管理
- 支配権
- 事業登録
- 背景
- 役員および取締役
- 法的問題の履歴
- IP 権に関する問題
- 提案された研究分野におけるパートナーの相対的な順位（提案された研究分野をリードしているのは誰か？）

3.2.2　大学は、技術および/または研究のポテンシャルを評価する

技術や研究の潜在的な使用とリスクを評価するための追加チェックの観点として、以下を含めることができる

- 技術または研究の潜在的な用途（新技術では明らかになるまでに何年もかかる場合があり、研究中に明らかになる場合もあることに留意する）
- 例えば、オーストラリアが世界をリードする立場であるなど、研究が魅力的な標的となる可能性
- 技術の成熟度
- 潜在的な商業価値
- 技術分野がオーストラリアの防衛戦略物資（DSGL）に含まれており、オーストラリア国外への物理的な輸出または電子供給が規制されているかどうか
- 自主的な制裁やその他の関連する法的枠組みなどの追加のコンプライアンスチェック
- 市場とサプライチェーンの多様性または競争力に及ぼす可能性のある影響
- 研究プロジェクトの過程で特定技術の機密レベルを変更することを含め、かかる評価は複雑になる可能性がある。政府部門とセキュリティ機関は、大学にこの活動のための支援を提供する

3.3　大学は、デューデリジェンスに包括的なアプローチを適用する（デュー・ディリジェンスを強化するための専門家への連絡等）

3.4　大学は、デュー・ディリジェンスプロセスの承認、監査、および継続的な評価を実施する

■　参照している情報ソース

ガイダンス資料における補足では、デュー・ディリジェンスを実施する上での参考サイトや、対象となる技術や研究分野を評価するための他のリソース等を参照しており、デュー・ディリジェンスの実施の参考となるツールのほか、輸出規制や国益上の重要技術、制裁制度などの情報ソースを示している（表 4.1-58）。

表 4.1-58　ガイダンス資料における参照リソース

大学がデュー・デリジェンスを実施する上で役立つリソースや参考サイト	
ASIO デュー・ディリジェンス インテグリティ ツール	ASIO（保安情報機構）の提供するツールと思われるが、ASIO アウトリーチチームへの問い合わせたが、回答が得られていない
外国影響透明性制度（FITS）	2018 年に制定された外国影響透明化制度法に基づき、個人または法人は、外国の主体に代わって特定の活動（ロビー活動、政治献金等）を行う場合、この制度に基づいて活動や外国・自組織を登録する必要があり、そのデータベースが整備されている
DFAT 統合リスト	豪州の制裁法でリストされているすべての個人および団体のリスト
防衛輸出管理（DEC）	防衛または国家安全保障を最終用途とする、豪州の防衛産業によって輸出される防衛特化型またはデュアルユースの物品またはサービスについて説明している
デュー・ディリジェンス支援フレームワーク	ガイドラインの「テンプレートとツール」に含まれる、デュー・ディリジェンスを実施する際に参考となるプロセスマップ
ファクトシート - オープンソース情報	ガイドラインの「テンプレートとツール」に含まれる、オープンソース情報からデュー・ディリジェンスを行う参考となる資料
技術と研究を評価するためのリソース	
防衛戦略物資リスト（DSGL）自己評価ツール	豪州の輸出管理上の記載対象となる DSGL 品目のリストや、その自己評価のためのヘルプツールが整備されている
外務貿易省 － オーストラリア制裁局 HP	国連及び豪州の制裁制度に基づいて、制裁の対象国や制裁対象商品・サービスについて説明している
重要な技術のサプライ チェーンの原則	政府の策定した「重要技術のサプライチェーン原則」に基づき、セキュリティ・バイデザイン、透明性、自律性と完全性の観点から確保すべき原則を示したもの
首相官邸：重要技術の保護と促進	豪州にとっての重要技術と保護の促進に係る政策の方針を示した文書
重要技術の青写真	豪州の国営上重要な技術分野を示したもの ※テーマ 1 において報告した List of Critical Technologies in the National Interest の前身

2）ARC（豪州研究会議）の取り組み

政府の主要な資金提供機関である ARC（豪州研究会議）は、「重要技術に該当する研究の助成申請にはリスク要因の検討を行う」旨述べており、デュー・ディリジェンスの対象となる研究分野のリストとしてもテーマ 1 で調査した List of Critical Technologies in the National Interest は活用されていると思料される [74,75]。

＜ARC（豪州研究会議）HP における重要技術への言及＞

- ARC は、NCGP やその他のプログラムを通じた資金申請に関連する可能性のある主なリスクを特定する。
- 申請において「重要技術の青写真」[76]に概説されている技術が特定された場合、ARC は他のリスクが存在する可能性があるかどうかを検討する。リスク要因には次のものが含まれる。
- 現在または最近の外国からの財政支援、教育、研究関連の活動。
- 現在または最近、外国人材育成プログラムに参加しているか、外国の大学に対する義務を負っているか
- 外国政府、軍隊、警察、諜報機関との現在または最近の関係
- オーストラリアが制裁を課している政権、個人、または組織との最近の関係
- 評価では、申請書に提供された情報と研究者の RMS プロファイル [77]が考慮される。外務貿易省（DFAT）の制裁制度や統合リストなどのオープンソース情報も考慮される。

また、ARC は豪州政府の国家競争的助成金プログラム（NCGP)等の申請において対外国干渉（CFI）評価プロセスを定めており、UFIT のガイドラインに基づいて大学がデュー・ディリジェンスを行った結果に基づき、安全保障機関への追加調査などを行っている [78]（図 4.1-19）。

---

[74] https://www.arc.gov.au/funding-research/research-security

[75] https://www.arc.gov.au/manage-your-grant/research-management-system-rms-information

[76] 「重要技術の青写真」は、List of Critical Technologies in the National Interest の前身である、2020 年に公表された「重要技術のための青写真と行動計画（Blueprint and Action Plan for Critical Technologies)」のことを指す

[77] RMS プロファイルとは、ARC の行う資金提供プログラムにおいて申請、評価やプロセス管理に使用される研究管理システム（RMS)における研究者の情報である

[78] https://www.arc.gov.au/sites/default/files/2023-12/ARC%20Countering%20Foreign%20Interference%20Framework.pdf

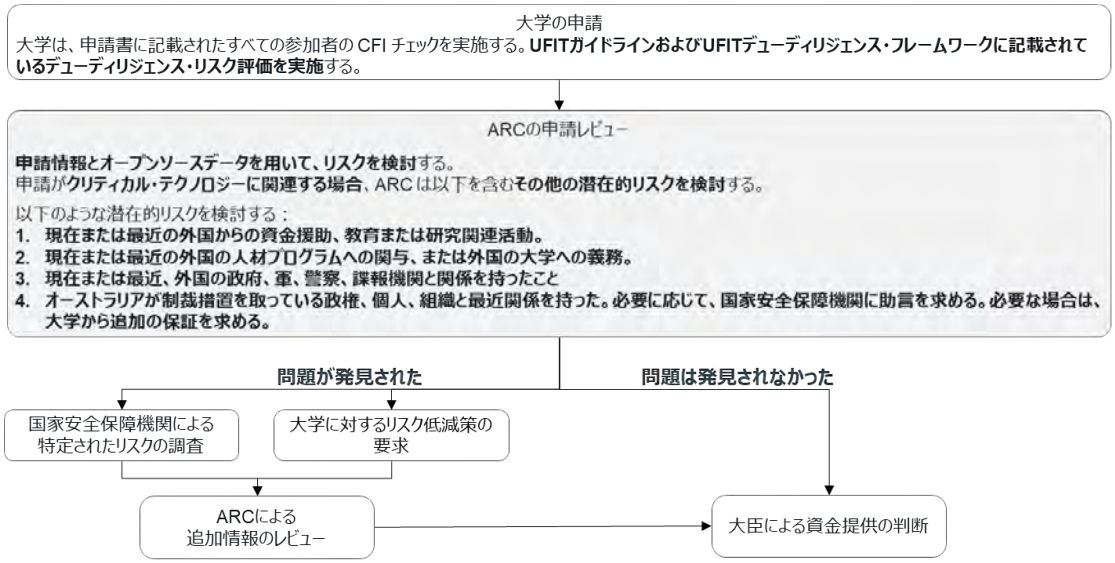


図 4.1-19　ARC の CFI 評価プロセス

3）ニューサウスウェールズ大学における取り組み

■　概要

ユーサウスウェールズ大学（UNSW）は、海外の研究パートナーとの共同研究や協力における潜在的なリスクに対処するため、政府の「豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン」への準拠を表明するとともに、UNSW 独自の取り組みとして「外国干渉に対抗するためのフレームワーク（Framework to counter foreign interference)」を導入している[79]。

当該フレームワークは、情報開示の義務化、中央レジストリの整備など８つのアクションで構成されるとしている（表 4.1-59)。

表 4.1-59 外国干渉に対抗するためのフレームワークにおける８つのアクション

1.情報開示の義務	利益相反の可能性、および／または海外との関係に関して、年次およびリアルタイムの情報開示が全スタッフに義務付けられる（このプロセスは現在進行中である）
2.中央レジストリ	利益相反や外資系企業との関係を照合、評価、報告するための中央登録簿（の整備）
3.外部リスク評価	UNSW を独立した外部機関が審査し、外国干渉リスクを評価する
4.ポリシーの見直し	利益相反に関する方針など、UNSW の主要な方針を見直し、改訂することで、政府の要求事項への準拠を含め、目的に合ったものとし高いレベルの内部透明性と説明責任を提供する
5.諮問委員会	外国干渉諮問委員会が設置され外国干渉に関するあらゆる事柄について全学的な対応と調整を行う
6.大学内の能力を高める	特別顧問が任命され、国家安全保障に関する助言を行い、各国の防衛・安全保障に関するコミュニケーションを行う 外国からの干渉リスクに関する助言を提供し、新たな脅威に対応し、UFIT ガイドラインへのさらなる対応力を構築する
7.国家安全保障機関との継続的な関与	国家安全保障機関と定期的に関わり、提案されている、あるいは進行中の国際的な関与について話し合い、あらゆるリスクに関連する助言を受け、発生したリスクに対処する方法について助言を求める
8.さらなる検討と協議	UNSW は、様々な関係者からの意見や感想を求めている

■　実施プロセス

UFIT ガイドラインへの準拠を表明していることから、UNSW におけるデュー・ディリジェンスの実施プロセスについても当該ガイドラインに準拠するものと想定される。

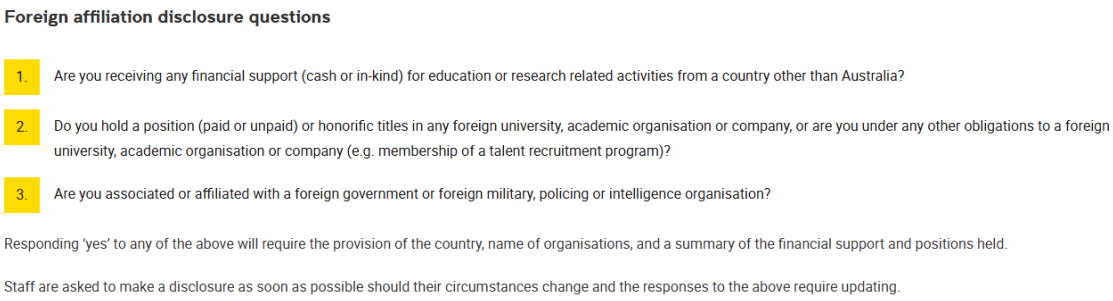
また、UNSW 独自の取り組みの中では、UNSW 内部のポータルシステムである MyUNSW を通じて、海外の大学、公的資金による研究機関、外国政府などの外国の団体と従業員との間に存在する提携関係やつながりの開示を義務付けている。

[79] https://www.unsw.edu.au/content/dam/pdfs/planning-assurance/2022-05-planning-assurance/UNSW%20Framework%20to%20Counter%20Foreign%20Interference.pdf

■　確認観点

UFIT ガイドラインへの準拠を表明していることから、UNSW におけるデュー・ディリジェンスの確認観点についても当該ガイドラインに準拠するものと想定される。

実際に、UNSW 職員を対象とした情報開示が必要な観点については、UFIT ガイドラインから抜粋した質問事項を公式 HP に掲載している（図 4.1-20）。



Foreign affiliation disclosure questions

1. Are you receiving any financial support (cash or in-kind) for education or research related activities from a country other than Australia?
2. Do you hold a position (paid or unpaid) or honorific titles in any foreign university, academic organisation or company, or are you under any other obligations to a foreign university, academic organisation or company (e.g. membership of a talent recruitment program)?
3. Are you associated or affiliated with a foreign government or foreign military, policing or intelligence organisation?

Responding 'yes' to any of the above will require the provision of the country, name of organisations, and a summary of the financial support and positions held.

Staff are asked to make a disclosure as soon as possible should their circumstances change and the responses to the above require updating.

図 4.1-20　UNSW の情報開示制度における質問事項

■　参照している情報ソース

UFIT ガイドラインへの準拠を表明していることから、UNSW におけるデュー・ディリジェンスの情報ソースについても当該ガイドラインに準拠するものと想定される。

UNSW の公式 HP では、共同研究に当たって留意すべき外国の主体について、国連安全保障理事会の制裁とオーストラリアの自主制裁制度を参照している。

（6）韓国

韓国では、2022 年に米国の NSPM-33 や英国の Trusted Research、豪州の UFIT などの取り組みの流れを受けて、研究におけるセキュリティ管理に関する課題を議論するための現場専門家と政府（科学技術情報通信部等）との議論や意見収集が実施された[80]。

その後 2023 年には、米国、日本、英国、豪州等の研究セキュリティの政策動向や事例を調査した「国際研究協力時の研究試算流出防止のための主要国の政策事例集」が発行されたのち、研究者が外国から得ている利益情報の管理や、汎省庁研究セキュリティ規程の体系化、研究課題のセキュリティ等級の細分化、専門家の育成支援などの施策を含む「信頼される研究エコシステム構築のための研究セキュリティ体制内実化方策（案）」が決議された[81,82]。

そして、2024 年 2 月に研究者の利益相反を防ぐために、政府の資金提供プログラムである「国家研究開発課題」の研究責任者が国外から受けている行政的・財政的支援や、労務・諮問などで対価を受けている内容を中央行政機関の長に報告する「国外受益情報報告制度」が施行された[83]。

上記政策動向を踏まえ公開情報を基に、韓国において政府、資金提供機関、研究開発実施主体によって実施されている研究セキュリティ・インテグリティに係るデュー・ディリジェンスの取り組み・ガイドライン等を抽出した（表 4.1-60）。

表 4.1-60　詳細調査を行う取り組み・ガイドライン

取り組み主体	デュー・ディリジェンスに係る取り組み・ガイドライン
政府	国外受益情報報告制度
資金提供機関	資金提供機関における国外受益情報報告制度の適用
研究開発実施主体	ソウル大学における取り組み

1）国外受益情報報告制度

■　概要

国外受益情報報告制度（국외수 혜정보 보고제도）は、国家研究開発課題を遂行する研究責任者が国外からの支援または支援予定事項を資金提供基幹に対して開示することで、利益相反を防止することを目的とした制度である[84]（表 4.1-61）。

[80] https://www.bioin.or.kr/board.do?bid=agenda&cmd=view&num=322601&utm

[81] https://www.iitp.kr/kr/1/business/rules/view.it

[82] https://www.kistep.re.kr/board.es?mid=a10306010000&bid=0031&list_no=93392&act=view

[83] https://www.pacst.go.kr/jsp/council/councilArchiveView.jsp?archive_id=1115&cpage=2&utm

[84] https://www.iitp.kr/kr/1/business/rules/view.it

表 4.1-61　国外受益情報報告制度の概要

項目	概要
所管	科学技術情報通信部
公表（更新）時期	2024 年 2 月施行
背景・目的	・　2022 年から科学技術情報通信部を主体として実施された研究セキュリティ強化のための各種政策検討の中で、米国、日本、英国、豪州などの政策における研究者の利益相反を防止するための情報公開制度を受けて 2023 年の「信頼される研究エコシステム構築のための研究セキュリティ体制内実化方策（案）」において国外受益情報報告制度の設立に言及された ・　国家研究開発課題を遂行する研究責任者が国外からの支援または支援予定事項を開示することで、利益相反を防止することを目的としている ・　諸外国が研究開発プログラムへの申請時に報告義務を設けていることに対し、国家研究開発課題の契約（협약）時に報告を実施させることや、報告項目を最小化することによって研究者の負担を緩和するとしている
デュー・ディリジェンス[85]の実施主体	・　各部（省庁）、専門機関（省庁の研究開発事業運営を効率化するための下部組織）
デュー・ディリジェンスの対象	・　国家研究開発課題の研究責任者
デュー・ディリジェンスの実施タイミング	・　国家研究開発課題の契約時

■　実施プロセス

国外受益情報報告制度は部（省庁）や専門機関（省庁の研究開発事業運営を効率化するための下部組織であり、資金提供機関も含む）が国家研究開発事業へ参加する者に対して開示要件を示すものであり、デュー・ディリジェンスを実施するプロセスを定めてはいない。

報告時期は他国が申請時に設定しているのに対して、契約時に義務付けていることが特徴的であり、故意または重過失によって未報告・虚偽報告のあった場合や虚偽・不正な方法で研究開発課題を遂行した場合に制裁金の賦課や参加制限が課される。

■　確認観点

国家研究開発課題を遂行する主管研究開発機関の研究責任者および共同・委託研究開発機関の責任者が受けている外国政府・機関・団体等からの財政的・行政的な支援や対価の受け取りが報告対象となっている（表 4.1-62）。

[85] 国外受益情報報告制度においてデュー・ディリジェンスという言葉は使用されていない

表 4.1-62　国外受益情報報告制度の対象・報告事項

対象者		国家研究開発課題を遂行する下記の者 主管研究開発機関の研究責任者 共同・委託研究開発機関の責任者
報告事項の定義		外国政府・機関・団体等から財政的・行政的（研究課題・人材・装備・施設）　支援及び講義・諮問・兼職などで対価[86]を受けることが対象となる
報告事項の詳細	支援・支給元	支援や対価を当人に提供する外国の政府・機関・団体等
	支援・支給理由	支援や対価の提供される理由 （講演の実施、外国事業への参加　等）
	支援・支給期間	支援や対価を当人に提供する期間
	支援・支給内容	支援や対価の内容 （例：計●●万ドル、博士級●名の派遣　等）
	研究開発課題との関連性	参加する研究開発課題と支援との関連性

■　参照している情報ソース

制度で情報ソースとなるのは研究開発事業に参加する責任者の開示した情報であり、公開情報などを参照している事実は現状確認できなかった。

研究機関は、所管省庁などから求められた場合は事実を検証するための資料を提供することとなっている。

2）資金提供機関における国外受益情報報告制度の適用

韓国の資金提供機関では、国外受益情報報告制度が既に施行されており、研究開発プログラムの管理や情報の集約、資金提供の申請・審査を行うプラットフォームである IRIS においても当該制度についての情報入力方法が整備されていることが確認できる[87]（図 4.1-21）。

[86] 同一機関から年間 5,000 ドル以上の金銭・有価証券・交通・宿泊等の提供を受けた場合

[87] https://medicine.yonsei.ac.kr/research/project/notice.do?mode=view&articleNo=122084&title=%5BIRIS%5D+%EA%B5%AD%EC%99%B8%EC%88%98%ED%98%9C%EC%A0%95%EB%B3%B4+%EB%B3%B4%EA%B3%A0+%EB%A7%A4%EB%89%B4%EC%96%BC

図 4.1-21　IRIS の研究者情報画面における国外受益情報の入力

3）ソウル大学における取り組み

ソウル大学においても、国外受益情報報告制度の施行にあたって、ソウル大学内の研究責任者等を対象として、その根拠法である国家研究開発革新法の改正内容及び制度対応に必要な事項について説明会を開催するとともに、政府作成のマニュアルを配布するなどして、制度の周知を図っている [88]

[88] https://science.snu.ac.kr/research/support/data?md=v&bbsidx=4934#:~:text=%E2%97%8B%20,%EC%9D%B4%EC%83%81%EC%9D%98%20%EA%B8%88%EC%A0%84%C2%B7%EC%9C%A0%EA%B0%80%EC%A6%9D%EA%B6%8C%C2%B7%EA%B5%90%ED%86%B5%C2%B7%EC%88%99%EB%B0%95%20%EB%93%B1%EC%9D%84%20%EC%A0%9C%EA%B3%B5%EB%B0%9B%EC%9D%80%20%EA%B2%BD%EC%9A%B0

4.1.3 テーマ 3：リスク軽減策

（1）米国

1）NSF 研究セキュリティトレーニング

■ 概要

NSF では、研究機関の研究者や管理者に対して、研究セキュリティ上の脅威・リスクを理解させ、それから澪守るための方法を学ぶためのオンライントレーニングを提供している。テーマ 3 では、トレーニングモジュール「3. リスクの管理と軽減」の内容について調査した[89,90]（表 4.1-63）。

表 4.1-63 NSF 研究セキュリティトレーニングの概要

項目	概要
リスク軽減策の根拠となる取り組み等	研究セキュリティトレーニング（Research Security Training）
背景・目的	・ 本トレーニングモジュールは、NSF が NIH、エネルギー省、国防総省と提携して提供しているオンライントレーニングプログラムである ・ トレーニングでは、政府の研究資金の受領者に、世界的な研究エコシステムに対するリスクと脅威に関する情報、およびこれらのリスクから保護するために必要な知識とツールを提供するとしている ・ トレーニングモジュールは、以下の 4 つに分かれ、「3. リスクの管理と軽減」では、国際共同研究や専門活動の種類、関連する潜在的リスク、およびそのようなリスクを管理および軽減するための戦略とベストプラクティスを特定する方法を学ぶためのコンテンツが提供されていることから、本調査ではモジュール 3 の内容について整理した ・ 研究セキュリティとは何か？ ・ （情報）開示 ・ リスクの管理と軽減 ・ 国際協力
リスク軽減策の指示主体	・ NSF（規制ではなく、ガイダンスとして実施を推奨するもの）
リスク軽減策の実施主体	・ 研究機関の研究者や管理者
リスク軽減策を実施するタイミング	・ ―（規制ではなく、ガイダンスとして実施を推奨するもの）

本トレーニングはオンライン上で研究者・管理者を対象とした授業形式のコンテンツが動画及び音声によって進行するため、その内容やトランスクリプトを参考に NTT データ経営研究所にて内容を整理した（図 4.1-22）。

89 https://www.nsf.gov/research-security#policies

90 https://www.nsf.gov/research-security/training#frequently-asked-questions-f02

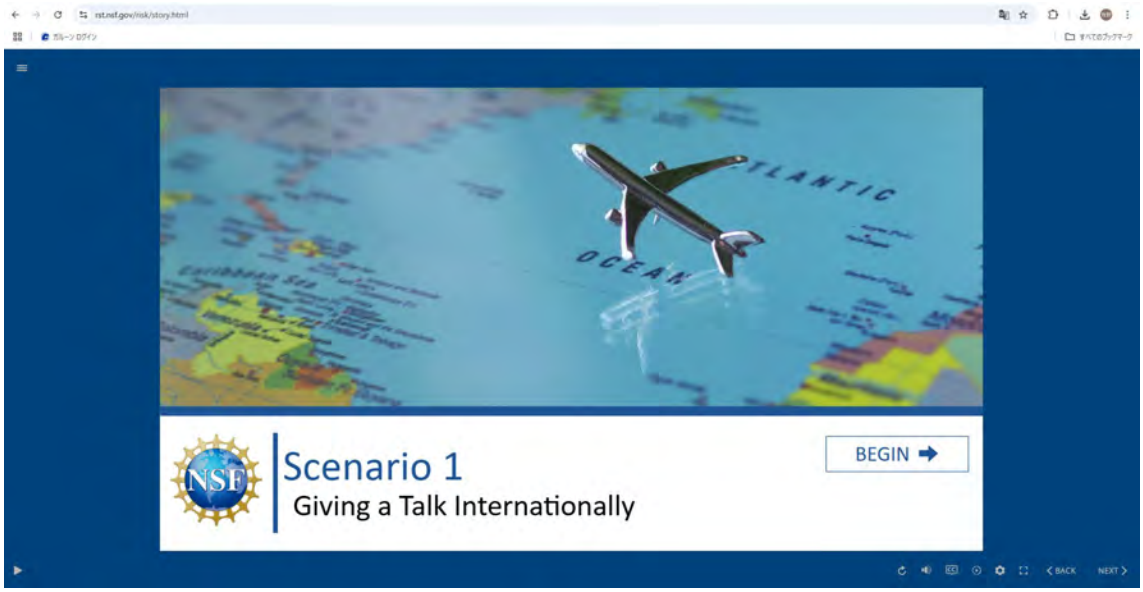


図 4.1-22　トレーニングモジュールの起動画面

■　インフラ面のリスク軽減策

インフラ面のリスク軽減策では、海外渡航中のデバイスからのデータ盗難への対策や、物理的・電子的な物資、情報を輸送する際の安全規制や輸出規制の確認、制限された技術設備や情報へのアクセス制御などが挙げられていた（表 4.1-64）。

表 4.1-64　研究セキュリティトレーニングにおけるインフラ面のリスク軽減策

リスク	対策
【データの盗難】 海外渡航中などは、自分のデバイスに他人が勝手にアクセスする可能性があることを想定する必要がある **【出荷に関する安全規制や記録要件の違反】** 生物学的物質、化学物質、放射性物質を輸送する場合、特別な梱包、マーキング、ラベリングが必要になる **【米国、仕向国の輸出管理規制への違反】** 電子的にデータを共有することも輸出とみなされることや、植物や動物を送る場合に仕向国の輸入許可が必要となる可能性がある **【制限された技術設備や情報の不適切な扱い】** 研究室や学内の他の場所で、制限された技術機器や情報を扱っている場合、適切なセキュリティ保護が行われているか確認する必要がある	**【渡航先やデータの種類に適したセキュリティ対策】** 渡航先やデータの種類に適したセキュリティ対策を講じ、スポンサーから許可を得るまでは、データを他人と共有しないようにする **【出荷に関する安全規制や記録要件の確認】** 物理的な物資の輸送に関しても、適切な梱包やラベリングを要するものか確認する **【輸出管理規制を確認し、電子的な共有にも留意】** 米国、仕向国における輸出規制を事前に確認し、電子的なデータも輸出に該当することを認識する **【制限された技術設備や情報の保護】** 訪問学生など、立場によって必要な情報のみへのアクセス管理や、設備のセキュリティ保護施策が適切になされているかを確認する必要がある

■　人的リスク軽減策

人的側面では、共同研究先メンバーの入国制限等に関するスクリーニングや、外国のプログラム参加に際しての悪意ある外国人材採用プログラム該当性の確認、風評被害を防ぐための外国との関与の早期開示などが挙げられていた（表 4.1-65）。

表 4.1-65　研究セキュリティトレーニングにおける人的リスク軽減策

リスク	対策
【コラボレーションメンバーの身上】 共同研究先のメンバーが米国の入国制限などに該当した場合、法令違反となる可能性がある **【外国人人材採用プログラムへの参加】** 悪意ある外国人人材採用プログラムに参加してしまった場合、研究セキュリティ・インテグリティ上の問題が生起する **【未公表の関与による風評被害】** （外国機関等との）未公表の関与が発覚した場合、個人や組織が風評被害を被る可能性がある	**【共同研究者のスクリーニング】** 共同研究に新たなメンバーが加入した場合などは、米国の入国制限リストに記載されていないかどうか追加のスクリーニングを要請する **【契約条件や要求事項の確認】** 海外赴任に同意する前に、その条件を十分に理解し、そのプログラムは悪意のある外国人人材採用プログラム出ないか、所属機関への助言を求めるなどする **【早期の開示・適切な管理】** 自己の関与する事項や外国との関係については、早期に開示し、適切な管理を行う

■　組織的リスク軽減策

研究セキュリティトレーニングは、研究者や研究機関の管理者といった個人を対象としたコンテンツが中心であったため、組織的なガバナンス等についての言及はあまり見られなかった。

2）NIH 助成金ポリシーステートメント（NIHGPS）

■　概要

NIH 助成金ポリシーステートメント（NIHGPS）は、NIH 助成金交付の条件となる要件を申請者に対して提供するためのガイドラインであり、テーマ 2 にて記載した Dicision Matrix についても、NIHGPS に基づいて実施されるものである[91]（表 4.1-66）。

表 4.1-66　NIHGPS の概要

項目	概要
リスク軽減策の根拠となる取り組み等	NIH 助成金ポリシーステートメント（NIHGPS：NIH Grants Policy Statement）
背景・目的	・ NIH 助成金ポリシーステートメント（NIHGPS）は、NIH 助成金交付の条件となる要件を申請者に対して提供するためのガイドラインである ・ NIHGPS では、NIH の支援する研究開発プログラムにおける機密データや情報の保護、利益相反に関する情報開示と管理など、リスク軽減策に相当する内容も含まれている
リスク軽減策の指示主体	・ NIH
リスク軽減策の実施主体	・ NIH の支援する研究開発プログラムへの申請者
リスク軽減策を実施するタイミング	・ 研究開発プログラムへの申請時、及び実施中

■　インフラ面のリスク軽減策

NIHGPS では、助成金の受領者は、連邦政府資金による研究を適切に管理する一環として、機密データおよび秘密情報を保護する重大な責任を負い、機密個人情報の不注意による開示、公開、紛失を防ぐためにあらゆる合理的かつ適切な措置を講じる必要があるとして以下のような情報管理策を要求している。

【NIHGPS 2.3.12　研究で使用される機密データと情報の保護】
- NIH は、NIH 支援研究または研究参加者に関する個人を特定できる機密情報をポータブル電子デバイスに保存しないよう勧告している
- ポータブル電子デバイスを使用する必要がある場合は、データと情報を保護するために暗号化する必要がある
- これらのデバイスには、ラップトップ、タブレット、モバイル デバイス、CD、ディスク ドライブ、フラッシュ ドライブなどが含まれる
- 研究者および機関は、パスワード保護などの適切なアクセス制御やその他の手段によって、個人を特定できる情報へのアクセスを制限する必要がある
- 研究データは、受領者のシステムのセキュリティがわかっていて、送信者がそれを満足できる場合にのみ送信する必要がある

[91] https://grants.nih.gov/grants/policy/nihgps/HTML5/introduction.htm

■　人的・組織的リスク軽減策

テーマ 2 において、Dicision Matrix 及び外国干渉に関する申し立て処理プロセスとして記載したように、NIH は助成金を活用する上級/主要職員に対して、研究支援のすべての出所、外国の構成要素 、および金銭的利益相反（FCOI）の開示を義務付けている。

そして、NIH が申請者の機関に FCOI が存在すると判断した場合、年次 FCOI レポートを提出し、NIH に報告することを NIHGPS で求めている。

初期提出の FCOI レポートには、以下の情報が含めるように求められる。

【NIHGPS　4.1.10 金銭的利益相反】

機関（NIH）が FCOI が存在すると判断した場合、機関は eRA Commons FCOI モジュールを使用して初期および年次 FCOI レポートを提出し、NIH に報告する必要がある。初期 FCOI レポートには、次の情報が含まれる。

- 助成金が複数 PI モデルに基づいて授与される場合は、助成金番号と PD/PI（プログラムディレクター／主任研究者）、または PD/PI への連絡先
- FCOI を記載した研究者の名前 (PD/PI と異なる場合)。
- 研究者が FCOI を持つ団体の名称
- FCOI の性質（例：コンサルティング料、謝礼、有償著作者、株式持分、知的財産権および利益、および旅費の償還またはスポンサー付き旅費）
- 金融利益の価値 $0-4,999、$5,000-9,999、$10,000-19,999、$20,000-100,000 の間の金額は $20,000 単位、$100,000 を超える金額は $50,000 単位、または価値を容易に決定できないという記述
- 金銭的利益が NIH の資金提供を受けた研究とどのように関係しているか、また、金銭的利益がそのような研究と矛盾すると機関が判断した根拠の説明
- 機関の管理計画の主要要素には以下が含まれる
  - ①　研究プロジェクトにおける利益相反のある研究者の役割と主な義務。
  - ②　管理計画の条件
  - ③　研究プロジェクトの客観性を保つために管理計画がどのように設計されているか
  - ④　研究者による管理計画への同意の確認
  - ⑤　治験責任医師の遵守を確実にするために管理計画をどのように監視するか
  - ⑥　必要に応じてその他の情報

（2）カナダ

1）NSGRP におけるリスク軽減策

■　概要

テーマ 2 で調査した NSGRP の適用される資金提供プログラムでは、助成金の申請にあたり申請者はリスク評価フォームを記入・提出する必要があり、その際特定したリスクを軽減するためのリスク軽減計画の提出・実施が求められ、また追加の軽減策を求めることもあるとされている[92]（表 4.1-67）。

表 4.1-67　NSGRP におけるリスク軽減策の概要

項目	概要
リスク軽減策の根拠となる取り組み等	National Security Guidelines for Research Partnerships（NSGRP）：研究パートナーシップに関する国家安全保障ガイドライン
背景・目的	・ NSGRP が適用される資金提供プログラム（連邦研究パートナーシップ資金プログラム）では、申請にあたり研究者はデュー・ディリジェンスを実施して「リスク評価フォーム」を記入・提出することが求められる ・ リスク評価フォームには、リスク確認に関する質問に対して回答するとともに、リスク軽減計画の提出を求められ、追加の条件として、さらなるリスク軽減措置が国家安全保障部門から要求される場合がある ・ NSGRP などと同じくカナダ政府の「Safeguarding Your Research」ポータルサイトでは、リスク軽減計画を立てるための参考情報を提供している
リスク軽減策の指示主体	・ NSERC、CIHR、SSHRC 等の資金提供機関 ・ カナダ公安省、カナダ安全保障情報局、または通信安全保障局（追加のリスク軽減措置の要求）
リスク軽減策の実施主体	・ NSGRP が適用される資金提供プログラムへの申請者
リスク軽減策を実施するタイミング	・ NSGRP が適用される資金提供プログラムへの申請が受理され、資金提供が決定されたのち、プロジェクト期間中に実施することとなっている

NSGRP などと同じく、カナダ政府の「Safeguarding Your Research」ポータルサイトでは、リスク軽減計画を申請者が立てるための参考情報が提供されており、テーマ 3 の調査では各参考情報をインフラ面、人的側面、組織的側面に分けて整理した。

[92] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process

■　インフラ面のリスク軽減策

インフラ面では、自組織及びパートナー組織における教育の実施、サイバーセキュリティ対策の慣行、国内外への移動におけるデバイスの管理といったリスク軽減策を推奨している（表 4.1-68）。

表 4.1-68　インフラ面のリスク軽減策の参考情報

リスク軽減策の例	内容
すべてのチーム メンバーがサイバーハイジーンおよびデータ管理のトレーニングを完了していることを確認する	適切なトレーニング オプションについて、最高情報責任者（CIO）または組織内で強力なサイバーハイジーンおよびデータ管理プラクティスの維持に責任を持つ担当者と話し合う
研究の完全性を適切に保護するために必要なデータ管理とサイバーセキュリティ対策が、すべてのパートナー間で実施されているかどうかを評価する	実施されているポリシーと実践について、所属機関と相談して連携すること。社内の研究と IT サービスも関与する必要があります。**カナダ公安省**と**カナダサイバーセキュリティセンター**は、リソースとベストプラクティスを提供している
異なるサイバーセキュリティとデータ管理の実践に重点を置き、研究データを保護するための相互に受け入れられるアプローチを決定する	・　研究データや結果などのコア資産の保護に役立つため、組織のセキュリティ体制が強固であることを確認する。組織のインフラストラクチャとビジネス プロセス内で、研究方法、技術、結果への不正アクセスにつながる可能性のある脆弱性の領域を特定することを推奨 ・　既存の相違点について考えるときは、「研究トピックとデータの機密性を考慮すると、侵害に関連するリスクレベルはどの程度で、侵害が発生する可能性はどの程度か」と自問することを推奨
プロジェクト期間中に仕事上または個人的な海外旅行が予想される場合は、デバイス管理のプロトコルに同意する	カナダ国内外への旅行が必要な場合に研究を保護する方法の詳細については、**「大学の研究者およびスタッフ向けの旅行セキュリティガイド」を参照**している

また、研究開発プロジェクト期間中の海外移動の際のデバイス管理等の面から、同じく「Safeguarding Your Research」ポータルサイト上の「大学の研究者と職員のための旅行安全ガイド」を参照しており、研究者の海外渡航における想定されるリスク要因とその軽減策を示している[93]（表 4.1-69）。

[93] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/mitigating-your-research-security-risks/how-can-you-protect-your-research-during-travel

表 4.1-69　研究者の海外渡航の際のリスク要因とその軽減策

項目	リスク要因	軽減策のヒント
1.カナダの研究者が関心を集め、危険にさらされる	・　研究者自身の研究分野（STEM、進行テクノロジーや軍事関連など）が悪意ある行為者の関心を引く ・　間接的に所属機関やカナダ政府の情報にアクセスするために研究者が標的にされる ・　カナダとの地理的･経済的近接性から米国の機関や情報へのアクセスのために標的にされる ・　渡航先によっては危険な国がある ・　注目度の高い一団に同行する等の場合、外国政府や関係者の標的となり得る	・　研究分野、間接的なパートナー、特に機密性の高い分野における米国の研究へのアクセスなどにより、渡航に関連するリスクのレベルを評価する ・　渡航計画を立て、大学内の適切な担当者へ相談する ・　カナダ政府の渡航勧告ウェブサイトを参照する ・　travel.gc.ca で旅行を登録する　等
2.個人プロフィール	・　研究やソーシャルメディアのプロフィールには、研究者の詳細な情報が記載されている可能性がある ・　ビザや渡航の申請は、上記のプロフィールと結び付けて評価される可能性がある ・　研究者の生体認証データが収集され、管轄区域を越えて保存および共有される可能性がある ・　国境警備官は、渡航目的に関する情報を収集、記録、送信するに際して、標的となる研究者に追加の質問や検査（入国前の二次審査）をする可能性がある	・　渡航前に研究やソーシャルメディアのプロフィールを確認して、必要に応じ露出を制限する ・　旅行申請やビザで提供する情報は、必要な情報のみに限定し、個人情報や職業上の詳細情報の追加は控える ・　国境警備隊員に提供する情報は、必要なものだけに限定する。二次審査を要求された場合、不適切な尋問等には領事のサービスを受けることができる

項目	リスク要因	軽減策のヒント
3. 研究へのアクセス方法（人・物理・サイバーを介した悪意ある行為者の試み）		
3-A. 人と人のつながり	・ **誘因：**他の研究者や学生、ビジネスマンが無害な会話に見せかけ、研究の事を聞き出してくる ・ **育成：**他の研究者や学生、ビジネスマンが情報を引き出すために人間関係を構築してくる ・ タクシー運転手、ウェイター、バーテンダー等が情報を収集してくる ・ 脅迫目的での性的な罠	・ 渡航中は警戒を怠らず、現地外国人との新しい関係や繋がりに注意する ・ 研究のデリケートな内容について話すのは控える ・ 渡航先での人との同伴を控え、性的行為に関連するリスクに注意する　等
3-B. 物理的侵入	・ 滞在するホテルのスタッフが、外国政府のエージェントとして部屋に侵入するなどして、物理・電子的情報の窃取や脅迫を仕掛けてくる ・ 会議スペースに盗聴器や監視が仕掛けられている可能性がある ・ 車に盗聴器や位置情報取得装置が取り付けられている可能性がある ・ 公共の場や公共交通機関での会話が盗聴される可能性がある	・ 出発前に IT 部門に相談し、可能な場合は、使い捨ての携帯電話や旅行に安全なデバイスを使用する ・ 不要な書類・デバイスを携行しない ・ 宿泊先や部屋番号を喧伝しない ・ ホテルや会議室の PC を使用しない　等
3-C. サイバー侵入	・ **通信傍受：**無線通信は監視されている可能性がある ・ **個人情報の詐欺・フィッシング：**攻撃者が自身になりすまし、ランサムウェアなどを含んだ標的型メールを所属組織上の他のユーザーに送信する可能性がある ・ **USB デバイス：**USB ドライブやデバイスは、悪意ある人物がコンピューターにアクセス・侵害するために使用されることがある	・ 渡航前に IT 部門に相談し、すべての電子機器に最新のウイルス対策、暗号化、ファイアウォール、プログラム パッチが適用されていることを確認 ・ 渡航中持ち運ぶデータを最小限にする ・ データを暗号化し、別のストレージデバイスに保管して常に携帯する ・ 外部デバイスを接続しない ・ クラウドストレージにアクセスしない　等

■　人的リスク軽減策

人的リスクの側面では、研究チームのメンバーに関する職歴や潜在的な利益相反・責務相反リスクを評価し、それを軽減する方法について話しあうことを推奨している（表 4.1-70）。

表 4.1-70　人的リスク軽減策の参考情報

実施項目	内容
チームメンバー全員の職歴を確認し、プロジェクトの研究目的との整合性を評価	・　研究チームの全メンバーに対して適切な身元照会と経歴調査を実施する ・　彼らの資格、出版物、所属は、彼らがあなたに伝えた内容と一致しているか。 組織内外で以前にその個人と働いたことのある同僚に、その個人の経歴や研究所属に関する情報を確認するよう依頼することを検討するとよい ・　さらに、SCOPUS または同様のツールを使用して、個人の出版履歴を確認し、検証することもできる
チームメンバーとの共同作業を妨げる可能性のある、既存または潜在的な利益相反や提携関係を評価	・　「チーム メンバーの利益や提携関係が、カナダの国家および経済の安全を危険にさらすような形でチームの研究の完全性を損なう可能性があるか」と自問するとよい
プロジェクトのリスクについて社内で話し合い、必要に応じ外部のチームメンバーを巻き込んでリスクを軽減する計画を立てる	・　チームで潜在的なプロジェクトのセキュリティ リスクについてブレインストーミングを行う ・　オンラインリスク登録テンプレート＊を使用して、共同研究者や共同研究機関の慣行が、組織の倫理および研究活動の基準に準拠しているかどうかを評価できる

■　組織的リスク軽減策

組織的なリスクの面では、パートナーの研究に参加する動機や、研究成果の利用目的が自組織の方針と一致しているか確認することを推奨している（表 4.1-71）。

表 4.1-71　組織的リスク軽減策の参考情報

リスク軽減策の例	内容
パートナーの動機と自分の動機の一致を評価する	
すべてのパートナーの動機が明確であり、知的財産に関する期待を含め、研究チームの目標と一致していることを確認	・プロジェクト期間中、各自の役割、責任、成果物に関して研究チームに何を期待しているか、プロジェクトから何を得たいと考えているか（知財、商業化等）を尋ねる
パートナーのガバナンス構造が透明であるか、プロジェクトにおける協力の最終的な受益者が明確であるかを評価	・パートナーの Web サイトを調べて、組織を率いる人物を特定し、外国の政府、組織、関係者とのつながりがあるかどうかを特定することで、独自のオープンソース デューデリジェンスを実施
他の研究者がこのパートナー組織との連携で良い経験をしたかどうかを調査	・所属機関内外の研究者に連絡を取り、過去の経験や潜在的な懸念に対処するための解決策に関する貴重な情報を収集
パートナーの慣行と貢献が、自機関の倫理と研究活動の基準と一致しているかどうかを評価	・貢献（データ、IP など）が、自機関のポリシーやカナダの法律と一致しているかどうか確認 ・オープンソース・デュー・ディリジェンスの実施を推奨
研究成果の利用目的に関する合意	
出版、会議、教育、マスメディア、ソーシャルメディア、個人的なコミュニケーションなど、プロジェクトの詳細をいつどのように共有するかの計画について合意	・プロジェクトの情報公開について後の意見の相違を最小限に抑えるため、英国の Health Foundation が発行した「医療改善におけるコミュニケーション」ツールキットを参照
プロジェクト関連の IP の潜在的な価値と、それを保護するために何を行う必要があるかを評価	・「この研究プロジェクトを通じてどのような種類の IP が生成される可能性がありますか? この IP の価値を維持するために何をする必要がありますか?」と自問
すべての協力者とパートナーが IP の取り扱い方法について合意していることを確認	・所属機関の適切な担当者に相談して、所属機関の IP に関するポリシー、および関連する機関や管轄区域によって内部ポリシー、法律、施行措置がどのように異なるかをより深く理解

リスク軽減策の例	内容
研究成果の利用目的に関する合意	
学問の自由や商業的利益に対する制限が研究プロジェクトや研究結果の伝達にどのような影響を与えるかについて話し合う	・「結果の伝達に課せられる制限は、研究の完全性や結果を発表する能力に潜在的に有害な影響を及ぼす可能性があるか」と自問
すべての共同作業者とパートナーが、研究結果の想定される用途に納得していることを確認	・プロジェクトの結果の想定される用途についてチームでブレインストーミングを行い、メンバーにプロジェクトを続行することに納得しているかどうかを尋ねる
プロジェクトに関与するすべての研究者が研究を完了するために結果を使用できることを保証するメカニズムが存在することを確認	・所属機関の適切な担当者に、所属機関でどのような対策が講じられているかを確認し、すべてのパートナーおよび協力者にこの要件を認識させる ・NSERC（カナダ自然科学・工学会議）が支援する研究の参加者は、研究者の卒業が知的財産の問題によって妨げられないようにし、公開文献での成果の公開をサポートする必要がある ※研究成果の権利に関する争いによって、成果を論文として公表できない等の問題が生じるリスクを指していると思料される

（3）英国

1）Trusted Research におけるリスク軽減策

■　概要

Trusted Research の学術界向けガイダンスでは、デュー・ディリジェンスの結果に応じたリスク軽減策の段階的な実施は確認できないが、テーマ 2 で報告したデュー・ディリジェンスも含め、人的側面・インフラ的側面・組織的側面のリスク軽減策を紹介している（表 4.1-72）。

表 4.1-72　Trusted Research の概要

項目	概要
リスク軽減策の根拠となる取り組み等	Trusted Research
背景・目的	・Trusted Research は、国際的な研究開発が活発に行われる中で、学術界・産業界の行う研究活動を通じた技術流出により、国家安全保障上のリスクが高まっている背景を踏まえ、NPSA（開始当初は CPNI）、NCSC が主体となって開始されたイニシアティブである ・Trusted Research は、敵対的な行為者による干渉等も含め、英国の研究開発における知的財産、機密研究、人々、インフラを潜在的な盗難、操作、搾取から保護することを目的としてガイダンスやアドバイスの提供を実施するものである ・テーマ 3 では、ガイダンスの中から学術界向けガイダンスを中心にリスク軽減策を調査した [94]
リスク軽減策の指示主体	・政府（規制ではなく、ガイダンスとして実施を推奨するもの）
リスク軽減策の実施主体	・大学の研究者、大学職員
リスク軽減策を実施するタイミング	・指定なし

■　インフラ面のリスク軽減策

インフラ面では、特に研究機関の IT 部門で対策すべき事項として、研究協力におけるリスク対策、及び研究者個人を支援するためのサイバーセキュリティ対策を提供している（表 4.1-73）。

[94] https://www.npsa.gov.uk/trusted-research-academia

表 4.1-73　Trusted Research におけるインフラ面のリスク軽減策

項目		対策
研究協力のためのサイバーセキュリティ	アクセス制御	機密データ、研究、ネットワークのその他の部分へのアクセスは、正当な要件を持つユーザーとパートナーにのみ許可する必要があるとして、NCSC のクラウドセキュリティガイダンスも参照している [95]
	不正アクセスの監視と防止	不正アクセスは、システム ユーザー（内部脅威）からの場合もあれば、パートナーやその他のソース（外部脅威）からの場合もあるとして、NCSC のラテラルムーブメントに対処するためのガイダンスを参照している [96]
	サプライチェーンまたはパートナー組織のセキュリティ	海外のパートナーと連携すると、サプライチェーンリスクがさらに高まる可能性があるとして、パートナー組織、サービスプロバイダー、潜在的に脆弱なコンポーネントに関連するリスクを早い段階で理解しておく必要があるとしている [97]
研究者のセキュリティ確保の支援	個人の従うべきヒント	研究者は所属機関のセキュリティポリシーに沿って状況に応じたサイバーセキュリティ対策が必要としつつも、個人の従うべきヒントとして以下を紹介している（NCSC のガイダンスも参照 [98]） ・ 強力なパスワードを使用してメールを保護する ・ 最新のソフトウェアとアプリのアップデートをインストールする ・ 可能な場合は、メールやコラボレーションプラットフォームで 2 要素認証を有効にする ・ パスワードマネージャーを使用してパスワードを作成し、記憶する ・ 画面ロックでスマートフォンやタブレットを保護する ・ 最も重要なデータを常にバックアップする
	ファイル転送における注意	情報を転送する際に USB ドライブを使用することについて、以下の注意を紹介している ・ USB ドライブのソースがどれだけ信頼できるかを考慮する ・ 設定またはシステム環境設定で、デバイス上で「自動実行」が無効になっていることを確認する（以下、例） ✓ Windows 10: Windows キー + I -> デバイス -> 自動再生 -> メディアとデバイスの自動再生を使用する（オフ） ✓ MacOS は何も実行せず、ファイルをマウントする ・ デバイスが USB ドライブ上のデータにアクセスする前に、ウイルス対策ソフトウェアが自動スキャンを実行するようにする ・ 代替手段（クラウドストレージ、メール、専用のコラボレーションプラットフォーム）の検討

[95] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/lightweight-approach-to-cloud-security

[96] https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

[97] https://www.ncsc.gov.uk/collection/supply-chain-security

[98] https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

■　人的リスク軽減策

人的側面では、海外からの訪問者や研究者を招致する場合や、英国と異なる民主主義的価値観・倫理観を持つ国で勤務するスタッフがいる場合、及び海外の会議などに参加する場合に人的側面から留意すべき事項を提供している（表 4.1-74）。

表 4.1-74　Trusted Research における人的リスク軽減策

観点	対策
海外の研究者と連携する場合	海外からの訪問者や研究者を誘致するにあたって、以下のような対策を行う必要があるとしている ・　利益相反を回避するために訪問スタッフの経歴、過去の仕事、現在の義務をある程度理解する必要があること ・　大学の研究に従事する人（大学の施設や IT ネットワークにアクセスできる人）は、必ず所属機関の人事手順に従って、スタッフまたは学生として記録されるようにすること。短期間の研究派遣であっても、所属機関のポリシーに従う必要があること ・　大学在学中に適切なビザで就労していることを確認すること（英国で特定のコースに応募する海外留学生のビザは、学術技術承認制度(ATAS)[99] の対象となる場合があることに言及）
海外で働くスタッフがいる場合	英国と異なる民主主義的価値観・倫理観を持つ国で勤務するスタッフがいる場合、以下の項目を含めたリスク評価の必要があるとしている ・　海外で働いている同僚に何かあった場合、誰に報告すればよいか? ・　懸念事項や問題がないか、どのくらいの頻度で確認しているか? ・　海外で受け入れる機関とはどのような協定を結んでいるか? ・　その国で遵守する必要がある規則や法律は何か? ・　その機関と締結した契約と矛盾する法律はあるか? ・　彼らが行う業務は英国の輸出規制の対象となるか? ・　あなたの同僚は、勤務先の国の輸出管理法、国家安全保障法、知的財産権に関する取り決めを認識しているか?
海外の会議などに参加する場合	海外の学会参加などで海外渡航する場合、以下の準備を行う必要があるとしている ・　旅行先の国を考慮し、現地の法律や慣習に注意すること ・　共有または提示する情報については慎重に検討すること ・　学問の自由と議論に対するホストの姿勢を理解すること ・　出席料として受け取るいかなる支払いも、利益相反を生じさせたり、契約違反や大学の方針違反に繋がったりしないよう注意すること ・　話せる研究分野と話せない研究分野を明確にすること ・　さらに情報を共有するよう求められた場合は、礼儀正しく、しかし毅然とした態度で臨むこと ・　疑わしい点があれば、上司と大学の関係当局に報告すること

[99] 英国で特定の機密技術関連分野を勉強または研究したい特定の外国人学生および研究者に適用される、外務・英連邦・開発省（FCDO）に対して申請手続きを行い証明書の発行を受ける制度

■　組織的リスク軽減策

組織的側面においては、パートナー機関と研究協力を推進する際に、テーマ 2 で報告したとおりパートナーとの研究の適合性、法的な枠組み、自身の研究の有するリスク・ターゲットにされる可能性等についてデュー・ディリジェンスを行うことを推奨している（表 4.1-75）。

表 4.1-75　Trusted Research における組織的リスクの確認観点（テーマ 2 より再掲）

確認観点	確認内容
パートナーとの研究の適合性（倫理的または国家安全保障上の懸念）	・組織、機関、団体に関して、懸念の原因となるような公開情報はあるか? ・その情報を考慮すると、あなたが取り組む予定の研究分野で彼らと協力することで、より広範な応用や予期しない結果が生じる可能性があるか? ・研究パートナーが拠点を置く国の自由度と法の状態について、どのような情報が入手可能か? ・以下のようなリソースは、その判断に役立つ ✓　米国輸出管理団体リスト ✓　国連制裁リスト ✓　国の汚職指数 ✓　輸出に対する貿易制限 ✓　人間の自由指数 ✓　世界正義プロジェクト法の支配指数
法的な枠組み	以下のような法的な枠組みについて確認する必要がある ・輸出管理：あなたの研究は輸出管理の対象か ・（外国の）法制：外国のパートナーが運用する可能性のある法的枠組みは何か、影響はあるか ・GDPR：データと情報保護に責任を負うこと ・技術移転オフィス：技術移転を検討する場合、TTO（技術移転オフィス）にアドバイスを求めること ・国家安全保障投資法：2022 年に成立した NSI 法を順守すること
自身の研究の有するリスク・ターゲットにされる可能性	・あなたの研究の応用に関して、倫理的または道徳的な懸念は潜在的にあるか? ・あなたの研究は国内監視や弾圧など、英国と異なる倫理基準を持つ他国の活動を支援するために使用される可能性があるか? ・あなたの研究は敵対的な国家軍に利益をもたらすか、あるいは他の国家主体に提供される可能性があるか? ・あなたの研究には、軍事と非軍事の両方の用途があるか? ・研究のいずれかが英国または他の国の輸出許可規制の対象となる可能性はあるか? ・機密データや個人を特定できる情報を保護する必要があるか? これには、遺伝情報や医療情報、人口データセット、個人の詳細、商用テストデータなどが含まれる場合がある。 ・あなたの研究は、あなたやあなたの組織が利益を得たいと思うような、将来的に商業化または特許取得可能な成果をもたらす可能性があるか?

（4）EU

1）研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書におけるリスク軽減策

■　概要

EU のスタッフ作業文書では、EU 内の大学や研究機関が外国との協力においてリスクを防止するために推奨される行動を提示するものであり、テーマ 2 で報告したデュー・ディリジェンスを含む、価値観、ガバナンス、パートナーシップ、サイバーセキュリティの 4 つのテーマにおいてとることが望ましいリスク軽減策が説明されている[100]（表 4.1-76）。

表 4.1-76　スタッフ作業文書におけるリスク軽減策の概要

項目	概要
リスク軽減策の根拠となる取り組み等	研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書（Tackling R&I foreign interference staff working document）
背景・目的	・　本作業文書は、EU 外の主体との協力において不当な影響から身を守ろうとしている大学や研究機関を支援するためのツールキットとして策定されたものである ・　価値観、ガバナンス、パートナーシップ、サイバーセキュリティの 4 つのテーマを中心に構成されており、各トピック領域ごとに具体的な行動勧告が提示されている。大学や研究機関は、これらを使用して、第三国による望ましくない影響から身を守るための対策を策定することができるが、規制的な拘束力はなく、必ずしも網羅的ではないとしている
リスク軽減策の指示主体	・　欧州委員会（規制ではなく、ガイダンスとして実施を推奨するもの）
リスク軽減策の実施主体	・　EU の大学や学術機関（特に意思決定者）
リスク軽減策を実施するタイミング	・　―（規制ではなく、ガイダンスとして実施を推奨するもの）

■　インフラ面のリスク軽減策

インフラ面では、「サイバーセキュリティ」のテーマにおいて、大学・研究機関の物理的・電子的なインフラのうち脅威にさらされるポイントとその軽減策を解説しており、脅威にさらされやすいポイントとして、ライブラリ、IT インフラ、研究室を挙げている（表 4.1-77）。

表 4.1-77　スタッフ作業文書におけるインフラ面で脅威にさらされるポイント

脅威に晒されるポイント	リスク
ライブラリ	・　高等教育機関や研究機関（RPO）は、科学雑誌や会議録デー

[100] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-publishes-toolkit-help-mitigate-foreign-interference-research-and-innovation-2022-01-18_en

脅威に晒されるポイント	リスク
	タベースのオンラインアクセスに多額の予算を費やしており、この認証情報を取得することで、論文だけでなく 個人情報や機密データ にアクセスされる可能性がある ・ また、予算の限られた機関ではペイウォールを回避する違法サイト を利用する動機付けにもなり、攻撃者が水飲み場攻撃（特定のサイトを感染源とする攻撃）を仕掛ける可能性がある
IT インフラ	・ 高等教育機関（HEI）や研究機関（RPO）の 技術インフラは高度に複雑であり、教育・研究・ビジネス支援のために多様なシステムで構成 されている。 ・ ネットワークへのアクセスは有線・無線の両方で提供され、場合によっては訪問者が認証なしで接続可能なケースもある。一部のサービス（ストレージ、メール、ウェブホスティングなど）は サードパーティのクラウドや外部プロバイダーにアウトソーシング されており、こうした情報はオープンソースインテリジェンス（OSINT）を通じて容易に取得可能である。 ・ そのため、インフラの境界が曖昧になり、セキュリティリスクが増大 している。また、研究機関ではプロトタイプから商用製品まで、成熟度の異なる機器が混在しており、サイバーセキュリティ認証の適用が困難 である。
研究室	・ 多くの研究機器にはセキュリティ・バイ・デザインやデフォルトの安全設計が組み込まれていないため、サイバー攻撃や情報漏洩のリスクが高い。特に、IoT 機器や特殊な計測機器には 脆弱性が多く報告 されており、品質保証が不十分なケースもある。これは特に 低コストの測定機器 に顕著であり ・ コンピュータの専門知識がない操作者が管理者権限を持つと、サイバーセキュリティ上の脆弱性が拡大する。さらに、物理的なセキュリティ対策（キーカードアクセス、USB デバイスの制限など）がない場合、リスクが高まる

そして前述のリスクに対する対策としては、サイバーセキュリティリスクに対する認識向上のための教育・セミナーや、定期的な OSINT 調査による攻撃の検知・防止、インシデント対応計画の策定等による対応及び復旧が挙げられている（表 4.1-78）。

表 4.1-78　スタッフ作業文書におけるインフラ面での対策事項

項目	対策の例
①サイバーセキュリティ	・ 機密コンピューティングを含む、利用可能で実装されてい

項目	対策の例
リスクに対する認識を高める	るすべてのデータ保護技術に関するトレーニングを開発し、セミナーを開催する ・ サイバー衛生に関する研究者、学生、事務・サポートスタッフの教育・訓練そして、リスクを特定し、サイバー攻撃を回避したり対処したりする方法を知る ・ サイバー攻撃が疑われる場合に、わかりやすいエスカレーション・プロセスを開発し、伝達し、報告されたインシデントをトリアージするための単一の窓口を宣伝する ・ サイバーセキュリティリスクのトップ 10 維持し、周知する ・ サイバーセキュリティインシデントに関するベストプラクティスを記載したニュースレターを定期的に発行する
②外国からの妨害行為者によるサイバーセキュリティ攻撃を検知・防止する	・ オープンソースインテリジェンス（OSINT）調査を定期的に設定・実行し、異常値行動にフラグを立てるアラート機能を作成する ・ 研究者、事務・サポート審査手順を作成する。 ・ サイバーセキュリティ認定機器を調達し、機密コンピューティングを含むデータセットの機密保護ソリューションの開発に投資する ・ 必要なレベルに適した物理的アクセス管理を実施する
③外国の干渉によるサイバーセキュリティ攻撃に対応し、そこから回復する	・ 教訓を共有し、共有のブラックリスト、レピュテーションシステム、データベースを更新することにより、状況認識能力を開発する ・ 影響を受ける当事者と対応に必要な当事者の双方が関与する明確なプロセスを含む、インシデント対応計画を策定する。SIM3「セキュリティインシデント管理成熟度モデル」などのインシデント対応モデルから実務や要素を採用する

■　人的リスク軽減策

人的・組織的なリスク軽減策の共通的な認識として、学問の自由が保障されない国家や主体による資金提供、名誉称号、有給ポストなどのインセンティブを利用した試みや、民主主義国においても利益相反による自己利益の優先や、大学が自己検閲を行ってしまうなどの脅威があり、その脅威にさらされる脆弱性は各組織・人によって異なるとして、全てに対応できるワンストップの解決策は存在しないとしている。

人的側面では、前述の脅威と脆弱性に対して、組織レベル・個人レベルで学問の自由と誠実さへのコミットメントを強化するための教育や意思の表明が対策となり得るとしている。

【スタッフ作業文書における人的リスク軽減策】

・　学問の自由と誠実さを、あらゆる学術教育プログラムのコアカリキュラムに組み込むこ

とで、これらの価値観、および関連する権利に関する健全な基礎知識を、学術専門職全体で構築する
- 学問の自由の保護・促進に対応した内部質保証プロセスを検討し、必要に応じて修正する。必要に応じて、学問の基本的価値をカバーするために、各国の外部質保証機関のガイドラインや「欧州高等教育圏における質保証の基準とガイドライン」の更新に協力する
- 学問の国際化の文脈を含め、学問の自由と誠実さの重要性を頻繁に、かつ公に表明する
- 基本的な学問的価値観の重要性と保護について、学生、学務スタッフ、事務スタッフの意識を高める
- 国境を越えた共同活動や交流の文脈において、特に協力協定の書面条項を通じて学問の自由を明示的に盛り込み、関連する行政手続きを通じてこれらの要件を制度化する
- 学問の自由と普遍的価値が危険にさらされている国の機関や個人と交流するすべての人が、そのような環境における人権関連の課題に対処するための十分な訓練を受けていることを確認する

■　組織的リスク軽減策

組織的側面では、「ガバナンス」「パートナーシップ」のテーマにおいて、テーマ 2 で報告したデュー・ディリジェンスも含め、行動規範の公表、外国干渉委員会の設置、リスクマネジメントに係る前提認識の共有やパートナーシップの策定手順の確立といった軽減策が述べられている（表 4.1-79）。

表 4.1-79　スタッフ作業文書における組織的リスク軽減策

テーマ	大項目	緩和策の例
ガバナンス	①海外からの干渉に対する行動規範を公表する	行動規範には、以下のような保護すべき対象と手順を含める ＜保護すべき対象＞ ・ 学問の自由 ・ データセキュリティと知的財産 ・ 研究、教育、学習支援における卓越性と開放性 ・ 倫理、誠実さ、信頼 ＜含めるべき手順＞ ・ 外国からの干渉（データ侵害や倫理的に不適切な含む）の特定 ・ 内部告発者の保護 ・ 社内の利益相反に対処する
	②外国干渉委員会の設置	既存の組織構造と統合した、教育訓練による意識向上、潜在的リスクのモニタリング、国際協力における研究データや知的資産の管理、関係する研究グループへのアドバイスやサポートに責任を負う委員会を設置する
パートナーシップ	①リスクマネジメントを実施するための一般的な前提条件を策定する	・ パートナーシップに関わる潜在的なリスクと、それを軽減するための機関としての取り組みについて、広く認識させる ・ 輸出管理法および外国直接投資（FDI）の審査に関する意識と知識を高める ・ パートナーシップに関する計画を FI 委員会に報告するための基準を定め、誰が報告のフォローアップに責任を持つかを決める
	②強固なパートナーシップ協定の策定手順を確立する	・ 国際協力のための安全な、あるいはリスクの低い分野を特定する ・ 国際化の一環として、戦略的ビジョンに基づくパートナーシップを確保する ・ セキュリティ、価値観、評判に関する潜在的なリスクをスタッフが評価できるように情報を収集するデュー・ディリジェンスを実施する

（5）豪州

1）UFIT ガイドライン（豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン）におけるリスク軽減策

■　概要

UFIT ガイドラインでは、テーマ 2 で記載したデュー・ディリジェンスの結果に応じた段階的リスク低減策の存在や、ARC 等資金提供機関で大学に要求するリスク軽減策と同一のものかは確認できなかったが、ガイドライン中で大学が認識すべき外国干渉のリスク及びその軽減策を提供している（表 4.1-80）[101]。

表 4.1-80　UFIT ガイドラインの概要

項目	概要
リスク軽減策の根拠となる取り組み等	オーストラリアの大学分野における外国の干渉に対抗するためのガイドライン（Guidelines to counter foreign interference in the Australian university sector）
背景・目的	・ 本ガイドラインは、大学セクターにおける外国の干渉に対するレジリエンスを高めるために、リスクの管理・対処に役立つように開発された ・ ガイドラインは、豪州の大学が既に実施しているリスク管理ポリシーとセキュリティ慣行を基盤として、意思決定者が外国の干渉によるリスクを評価できるように設計された ・ ガイドラインは、大学・研究機関がリスク管理を実施する上で重要なテーマを以下の 4 項目から解説しているほか、ガイドライン（PDF）をサポートするガイダンス資料（Web ページ上で公開）とともに参照される ✓ ガバナンスとリスクのフレームワーク ✓ コミュニケーション、教育及び知識共有 ✓ デューディリジェンスやリスク評価、リスクマネジメント ✓ サイバーセキュリティ ・ テーマ 3 では、テーマ 2 で調査したデュー・ディリジェンスを含む、本ガイドラインが大学や学術機関に実施を推奨するリスク軽減策を調査した
リスク軽減策の指示主体	・ 政府（規制ではなく、ガイドラインとして実施を推奨するもの）
リスク軽減策の実施主体	・ 豪州の大学や学術機関（特に意思決定者）
リスク軽減策を実施するタイミング	・ （本ガイドラインは、既存の大学のポリシーに合わせて参照するように記載されている）

ガイドラインは本文及びそれをサポートするケーススタディやツール等のガイダンス資料から構成される。テーマ 3 では、テーマ 2 で調査したデュー・ディリジェンスも含めリスク軽減策に係る内容を記載した（図 4.1-23）。

[101] https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector

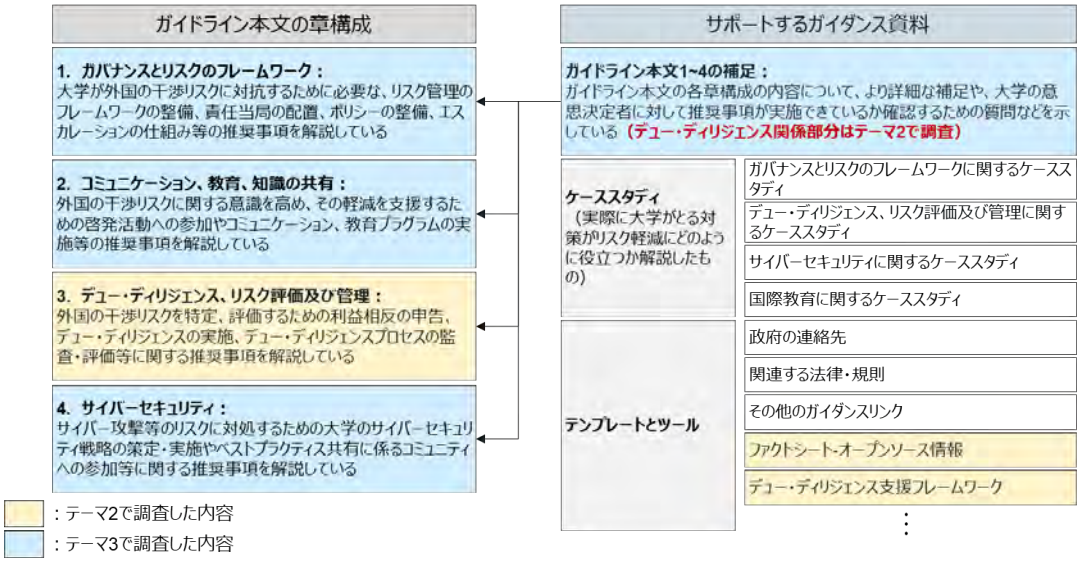


図 4.1-23　UFIT ガイドラインの構成におけるリスク軽減策の位置づけ

■　インフラ面のリスク軽減策

インフラ面では、主にサイバーセキュリティの観点から、脅威モデリングによるサイバー脅威の理解、職員・学生のセキュリティ意識の向上、サイバーセキュリティ戦略の策定、業界・政府との情報交換といった下記のような対策を提供している。

【UFIT ガイドラインにおけるインフラ面のリスク軽減策】

＜脅威モデル技術を利用してビジネスリスクを理解・軽減、サイバーセキュリティ戦略へ反映＞

- サイバー脅威をリスクに結びつける手法として脅威モデリングを紹介しており、大学の守るべき資産や脅威主体（内部者、犯罪者、国家主体等）、潜在的な攻撃方法をマッピングして、サイバーセキュリティ戦略の策定に役立てることを推奨している
- 一般的な脅威モデリングのステップとして、①モデルの範囲定義（組織、アプリ等）、②重要資産の定義（データセット等）、③脅威の定義（不正アクセス、変更、サービス拒否等）、④脆弱性の特定　を紹介している
- また、脅威モデルの例として、以下を参照している
  - ✓ STRIDE (なりすまし、改ざん、否認、情報漏洩、サービス拒否、権限の昇格)
  - ✓ DREAD (被害の可能性、再現性、悪用可能性、影響を受けるユーザー、発見可能性)
  - ✓ PASTA (攻撃シミュレーションと脅威分析のプロセス)
  - ✓ OCTAVE (運用上重要な脅威、資産、脆弱性の評価)
  - ✓ NIST 800-151 - データ中心システムの脅威モデリングガイド

＜サイバーセキュリティを組織全体の人的問題として扱い、適切な管理フレームワークを組み込んだサイバーセキュリティ戦略を実施＞

- 職員や学生のセキュリティ意識を向上させるため、サイバーセーフな行動と意思決定を根付かせる教育プログラム、脅威主体の行動シミュレーション、外部講師による経験やアプローチの共有等を実施することを推奨している
- また、大学がサイバーセキュリティ戦略を策定する際に参考となるフレームワークとして、以下を参照している
  - ✓ 連邦情報セキュリティマニュアル（ISM）
  - ✓ NIST　サイバーセキュリティフレームワーク
  - ✓ ISO 127001

＜セクターや政府とサイバーインテリジェンスと教訓を共有するベストプラクティスのコミュニティに参加＞

サイバーセキュリティに係る最新の情報の収集や、ベストプラクティスの共有等のため、以下のようなコミュニティに参加することを推奨している

- ACSC の脅威インテリジェンス プラットフォームやパートナーシッププログラム
- オーストラレーシア大学情報技術部長協議会（CAUDIT）が主催する取り組み
- 他の大学との共同の事故管理協定を検討

■ 人的リスク軽減策

人的側面では、大学の教職員や学生に対して外国の干渉リスクに対する認識を高めるためのコミュニケーションと教育プログラムを実施することを推奨し、そのためのケーススタディを提供しているほか、テーマ 2 で報告した自組織職員に対する情報開示の義務付けなどが対策として提供されている。

【UFIT ガイドラインにおけるコミュニケーションと教育プログラムの推奨事項】

- 外国干渉リスクに対する意識を高め、その軽減を支援するコミュニケーション計画と教育プログラムの整備
  - ✓ キャンパス内で外国からの干渉がどのように起こる可能性があるか、また大学内または関係当局に懸念を表明する方法に関する情報へのアクセスを提供することで、教職員と学生の意識を高める
  - ✓ 学問の自由や言論の自由に反する自己検閲につながる可能性のある外国からの干渉、脅迫、ハラスメントに関する懸念を大学内で報告する方法を全教職員と学生に奨励する
  - ✓ 学生団体や公開イベントの主催者など、キャンパスを自らの活動に利用する人々に対し、適切な行動に対する期待と、それが満たされなかった場合の結果を伝える
- 外国の干渉リスクがある国際協力やその他のパートナーシップ活動に従事している教職員と学生にトレーニングを提供
  - ✓ トレーニングでは、教職員の経験が貴重なリソースになり得ることを認識し、外国の干渉に対する懸念を認識し、軽減し、対処する方法を取り上げる
- 大学セクター全体の外国干渉対策イベントに参加し、必要に応じて経験と先進的な実践を共有して、レジリエンスを構築
  - ✓ 先進的な実践例を大学の責任当局間で共有
  - ✓ 得られた教訓、先進的な実践、デューデリジェンス情報を機関内で共有
  - ✓ 信頼できる国際パートナーと外国の干渉に対抗するための先進的な実践を共有し、協力と交流の機会に対する信頼を築く
- 政府による大学セクターサポートの活用
  - ✓ 政府機関は、大学が外国の干渉の事例や試みの特定を支援する
  - ✓ 政府機関は the Counter Foreign Interference Coordination Centre などの大学支援機関の連絡先を提供する

■ 組織的リスク軽減策

組織的側面では、大学において外国干渉リスクの管理を行う責任当局の設置、ポリシー及び手順の整備、リスク評価および報告のためのフレームワークの策定、エスカレーションと報告の仕組みが必要であるとしている（表 4.1-81）ほか、テーマ 2 で報告したデュー・ディリジェンスもフレームワークに対策として含まれている。

表 4.1-81　UFIT ガイドラインにおける組織的リスク軽減策の推奨事項

項目	推奨事項
責任当局の設置	外国の干渉に対抗するために、人、情報、資産のセキュリティに責任と説明責任を持つ上級行政機関または執行機関として責任当局を設置すべきであるとしており、以下を例として挙げている ・　副学長 ・　最高情報セキュリティ責任者 ・　大学上級職員 ・　適切な上級大学レベルの委員会 その他、外国の干渉を常設議題として追加することや、既存の経営幹部/リーダーシップ/プロジェクト グループの業務委託事項に含めることを検討できるとしている
ポリシー及び手順の整備	大学のコンプライアンスをサポートする既存のポリシーと手順は、外国の干渉リスクの管理の一部として考慮されるとしており、ポリシーと手順の例として以下を挙げている ・　センシティブな研究 ・　贈り物と寄付 ・　インシデント管理 ・　職場における倫理的行動 ・　責任ある研究の実施 ・　学生行動規範 ・　スタッフの行動規範　等
リスク評価および報告のためのフレームワークの策定	全教職員と学生が利用できる明確な外国干渉リスク評価および報告のフレームワークを整備すべきとし、以下を例として挙げている ・　国内外の投資、パートナーシップ、利益相反の開示（外国との提携、関係、財務上のコミットメントなど）の出所を考慮するデュー・ディリジェンスプロセス ・　利害関係の宣言を含むデュー・ディリジェンスチェックの頻度 ・　追加のデュー・ディリジェンスチェックが必要な場合 ・　デュー・ディリジェンスとリスク評価を通じて提起された懸念に対処するプロセス ・　活動が最初に範囲指定されたときと活動の進行中のリスク評価、軽減策、委任レベル、軽減策の承認 ・　プロジェクトのリスクと軽減策の検討と評価を行う方法とその時期 ・　データ、機器、または材料の取り扱いと保管を管理する方法
エスカレーションと報告の仕組み	大学内および政府との間で双方向の情報の流れを促進し、大学のセキュリティ環境に対する理解を深めるメカニズムとして、以下を整備すべきとしている ・　大学内および必要に応じて州または連邦レベルの政府当局に、外国の干渉に関連する可能性のある事件が報告されるタイミング、方法および報告先 ・　教職員と学生が機密性を適切に維持する内部プロセスを通じて外国の干渉に関する懸念をエスカレートする方法 ・　報告された懸念が追跡、解決、記録され、責任当局と共有される方法

（6）韓国

1）国家研究開発革新法におけるリスク軽減策

■　概要

テーマ 2 で調査した国外受益情報報告制度は、韓国政府の研究開発課題（資金提供プログラム）の実施根拠となる国家研究開発革新法において規定されており、同法及び施行令では、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こととなっている（表 4.1-82）。

表 4.1-82　国家研究開発革新法におけるセキュリティ対策の概要

項目	概要
リスク軽減策の根拠となる取り組み等	国家研究開発革新法 国家研究開発革新法施行令
背景・目的	・ 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いる。 ・ セキュリティ課題の分類基準については以下のとおり。 ✓ 「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 ✓ 次の各号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
リスク軽減策の指示主体	・ 政府（資金提供機関）
リスク軽減策の実施主体	・ 研究開発課題に参加する研究開発実施主体
リスク軽減策を実施するタイミング	・ 研究開発課題への申請時及び実施期間中

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[102]ことから、以下にインフラ面、人的側面、組織的側面からセキュリティ対策を整理した。

[102] https://www.law.go.kr/행정규칙/국가연구개발사업보안대책/(2023-39,20231120)

■　インフラ面のリスク軽減策

インフラ面では、研究開発課題を実施する施設・設備に関する入退室管理や規程の整備、電子的なアクセス制限などが求められている（表 4.1-83）。

表 4.1-83　国家研究開発事業セキュリティ対策におけるインフラ面の対策

区分	対策
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
電子的管理策	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 ・　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

■　人的リスク軽減策

人的側面では、研究開発課題従事者の外国人との接触に関する報告を規定しているほか、テーマ 2 で記載した国外受益情報報告制度についても人的側面のリスク軽減策として機能していると思料される。

【国家研究開発事業セキュリティ対策における人的側面の対策】

・　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。

■　組織的リスク軽減策

組織的側面では、外国機関と共同での研究開発を実施する場合の事前の政府承認を規定しているほか、テーマ 2 で記載した国外受益情報報告制度についても組織的側面のリスク軽減策として機能していると思料される。

【国家研究開発事業セキュリティ対策における組織的側面の対策】

- 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
- 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

4.1.4 各国の情報漏洩事案の調査

（1）各国の情報漏洩事案のリストアップ

日本及び調査対象国において、公開情報から 2020 年以降、国立研究機関、大学、民間研究所等において、機関内の人員及びパートナー機関を通じて発生した技術情報等の漏洩事案（未遂及びリスクの発覚含む）をリストアップした。

（2）詳細調査

リストアップした情報漏洩事案のうち、事件に関する詳細情報を得ることのできた事案を中心に、生起した原因を確認したところ、テーマ 2 で調査している各国のデュー・ディリジェンスに関する取り組みが適切に実行されていたならば、未然に防ぐことができた可能性のあることが確認できた（図 4.1-24）。

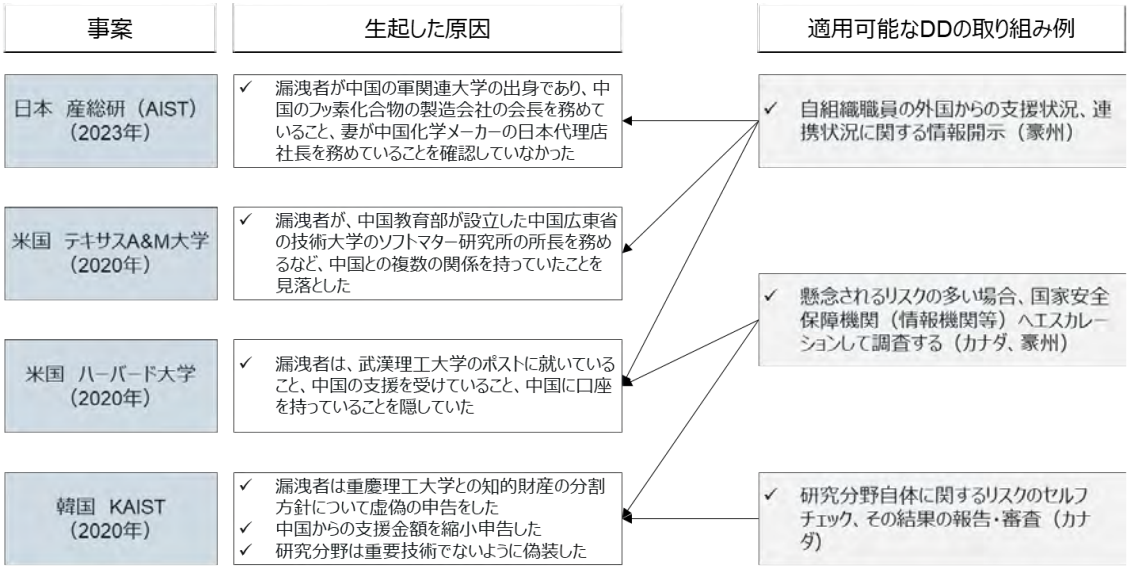


図 4.1-24 過去の情報漏洩事案とそれを防ぎえたデュー・ディリジェンスの取り組み例

4.2 国内外における先端的な重要技術の研究開発動向に関する調査研究

4.2.1 宇宙分野

(1) 技術領域の調査・整理

宇宙分野における技術領域調査・整理のため、国内外の宇宙関連機関等のホームページや学術データベースで、最近対象国等で実施された宇宙分野に関する研究開発プロジェクトや発表された論文等を調査した。(表 4.2-1、表 4.2-2)

表 4.2-1 確認した主な宇宙分野の研究機関等

機関名	国	概要
JAXA (宇宙航空研究開発機構)	日本	日本の宇宙航空研究開発を担う国立の研究開発機関で、人工衛星の打ち上げや小惑星の探査、宇宙天文学等に取り組んでいる。
NASA (米国航空宇宙局)	米国	米国の宇宙・航空研究を担当する主要な政府機関であり、アルテミス計画等の大規模な宇宙探査計画や商業宇宙開発等に取り組んでいる。
DAPRA (国防高等研究計画局)	米国	米国防総省の機関で、米軍が今直面しているニーズではなく、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、実用化の加速をミッションとしている。
UKSA (英国宇宙局)	英国	英国の宇宙研究を担当する主要な政府機関であり、小型衛星技術や宇宙通信等の研究開発等に取り組んでいる。
DASA (防衛セキュリティ促進機構)	英国	英国防衛省の傘下である国防科学技術研究所 (DSTL) の下部組織として設立され、国防・安全保障の効果的なサポートを目的として、国研、大学、民間企業等に対する資金提供、プロジェクト管理を行っている
ESA (欧州宇宙機関)	EU	EU の 22 の加盟国により設立された欧州全体の宇宙開発を推進する機関であり、JAXA や NASA 等とも共同研究を多く実施している。
東京大学	日本	日本における最高学府の 1 つであり、宇宙分野においても小型衛星の編隊飛行技術開発や宇宙観測等の多くの研究開発に取り組んでいる。
大阪大学	日本	日本における最高学府の 1 つであり、宇宙分野においては特にレーザー技術において先進的な研究開発が実施されている。
ジョンスホプキンス大学 応用物理研究所	米国	ジョンスホプキンス大学の研究所で、特に宇宙分野においては NASA と連携し、ニューホライズンズや DART 等の宇宙探査機開発等を多く実施している。

表 4.2-2　確認した主なデータベース

データベース名	概要
Google Scholar	Google Scholar は、Google が提供する無料の学術検索エンジンで学術論文、書籍、特許、学会発表資料、幅広い分野の学術文献が検索可能
ScienceDirect	Elsevier が提供する学術プラットフォームで自然科学、医学、社会科学など幅広い分野を対象として、論文や実験データ等の資料が検索可能
SpringerLink	シュプリンガー・ネイチャー社が運営する電子ジャーナルと書籍のプラットフォームで自然科学、工学、医学分野等の分野における論文等が検索可能

調査の結果、宇宙分野においては、NASA で実施されているアルテミス計画[103]等の月面探査を初めとした宇宙探査プロジェクトや宇宙輸送技術の他、衛星コンステレーション技術、スペースデブリ等の宇宙空間に存在する障害物を除去するための技術(レーザーアブレーション技術)、ロケットエンジンの性能向上等を目的とする技術に関する論文を確認した。(表 4.2-3)

研究開発プロジェクト・論文の詳細については Appendix Ⅱ を参照

表 4.2-3　宇宙分野における研究開発プロジェクト・論文(一部抜粋)

論文・プロジェクト名	時期	国・機関	技術領域
Optimal Satellite Constellation Altitude for Maximal Coverage (最大カバレッジのための最適衛星コンステレーション高度)	2021	豪州 RMIT 大学	効果的な地上カバレッジの確保のための衛星コンステレーション技術
Development and testing of a rotating detonation rocket engine with a racetrack combustor and shear-coaxial injectors (レーストラック燃焼器とシア同軸インジェクタを備えた回転爆轟ロケットエンジンの開発と試験)	2021	米国 アラバマ大学	ロケットエンジンの性能向上のための、回転デトネーション波を利用した燃焼プロセス技術
Space-based laser ablation for space debris removal (スペースデブリ除去のための宇宙レーザーアブレーション)	2021	EU ESA	スペースデブリ除去のためのレーザーアブレーション技術
超高精度フォーメーションフライトと補償光学による合成開口望遠鏡の地上実証	2021 — 2024	日本 東京大学等	静止軌道からの高分解能かつ高頻度の地球観測の実現のための衛星コンステレーション技術
次世代型航空宇宙用推進機の開発研究：MPD スラスタおよび回転デトネーションエンジン	2024	日本 静岡大学等	宇宙空間における活動の自在化のためのロケットエンジン技術

[103] https://www.nasa.gov/humans-in-space/artemis/

調査した論文等の結果を基に、将来の通信インフラの重要な技術となる可能性や、スペースデブリ等の現状のインフラに対する脅威を防止することが可能となる技術等の経済安全保障上の重要性があり、既存の支援対象技術（特定重要技術）に該当しないこと等を考慮し、技術領域を調査・整理した。

4.2.2 サイバー分野

（1）技術領域の調査・整理

サイバー分野における技術領域調査・整理のため、国内外のサイバー関連機関等のホームページや学術データベースで、最近対象国等で実施されたサイバー分野に関する研究開発プロジェクトや発表された論文等を調査した。(表 4.2-5、表 4.2-6)

表 4.2-4　確認した主なサイバー分野の研究機関等

機関名	国	概要
NISC （内閣府サイバーセキュリティセンター）	日本	日本政府のサイバーセキュリティ政策を統括する内閣官房の機関で、主に政府機関や重要インフラ事業者向けのサイバーセキュリティ対策を指導や「サイバーセキュリティ戦略」の策定等を行っている
NICT （情報通信研究機構）	日本	情報通信分野を専門とする公的研究機関であり、量子やAI、サイバーセキュリティ技術の開発、「NICTER」等のシステムの運用等を主に実施している。
NIST （米国国立標準技術研究所）	米国	米国商務省の機関であり、計測科学、標準化等を主に実施している。サイバー分野においてもサイバーセキュリティフレームワークや SP800 シリーズ等、サイバーセキュリティに関するガイドライン等を多く発行している。
DAPRA （国防高等研究計画局）	米国	米国防総省の機関で、米軍が今直面しているニーズではなく、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、実用化の加速をミッションとしている
DASA （防衛セキュリティ促進機構）	英国	英国防衛省の傘下である国防科学技術研究所（DSTL）の下部組織として設立され、国防・安全保障の効果的なサポートを目的として、国研、大学、民間企業等に対する資金提供、プロジェクト管理を行っている
NCSC （英国国家サイバーセキュリティセンター）	英国	英国のサイバーセキュリティ政策を統括する政府機関であり、重要インフラや個人をサイバー脅威から守るためことを目的に、インシデントに対する対応、助言、研究等を実施している
東京大学	日本	日本における最高学府の 1 つで、サイバー分野においては「情報セキュリティ研究教育センター」を設置し、サイバーセキュリティの研究や普及教育等に取り組んでいる。

表 4.2-5　確認した主なデータベース

データベース名	概要
Google Scholar	Google Scholar は、Google が提供する無料の学術検索エンジンで学術論文、書籍、特許、学会発表資料、幅広い分野の学術文献が検索可能
IEEE Xplore	IEEE が提供するプラットフォームで電気工学、電子工学、コンピュータサイエンスなど技術分野に特化した学会論文や技術レポート、規格書等が検索可能
ACM Digital Library	米国に本部を置く国際的な学会である Association for Computing Machinery（ACM）が運営しているプラットフォームであり、コンピュータサイエンスや情報技術に関する論文等が検索可能
SpringerLink	シュプリンガー・ネイチャー社が運営する電子ジャーナルと書籍のプラットフォームで自然科学、工学、医学分野等の分野における論文等が検索可能

調査の結果、サイバー分野においては、DARPA の ANSR プロジェクト [104]のような AI の開発の他、耐量子暗号技術や、ブロックチェーン技術、マルウェア攻撃を検知する技術、ディープフェイクを検出する技術、SMPC（Secure Multi-Party Computation）のような技術まで幅広い研究開発が実施されていることを確認した。（表 4.2-7）

研究開発プロジェクト・論文の詳細については Appendix Ⅱ を参照

表 4.2-6　サイバー分野における研究開発プロジェクト・論文(一部抜粋)

論文・プロジェクト名	時期	国・機関	技術領域
3D 画像識別によるマルウェア検知を目的としたプログラムの挙動の可視化に関する検討	2020	日本 工学院大学 等	マルウェアの検知のための３D画像識別を用いたプログラムの挙動可視化技術
Assured Neuro Symbolic Learning and Reasoning(ANSR) (確実なニューロシンボリック学習と推論)	2022 ～	米国 DARPA	自律システムへの高い信頼性の実現のためのシンボリック推論とデータ駆動型の機械学習を深く統合した新しい AI アルゴリズムとアーキテクチャ
A review of IoT security and privacy using decentralized blockchain techniques (分散型ブロックチェーン技術を使用した IoT のセキュリティとプライバシーの見直し)	2023	米国 カンバーランド大学 等	IoT のセキュリティ問題(プライバシー漏えい等)を解決するための分散型ブロックチェーン技術
計算可能ストレージを用いたログ構造化ファイルシステムへの変換によるランサムウェア対策の提案	2024	日本 三菱電機等	ランサムウェアにより暗号化されたファイル復元のための計算可能ストレージを用いた自動変換技術

[104] https://www.darpa.mil/program/assured-neuro-symbolic-learning-and-reasoning

また、サイバー分野において日本の IPA（Information-technology Promotion Agency：独立行政法人情報処理推進機構）が毎年発行している「情報セキュリティ 10 大脅威[105]」や米国の ONCD（The Office of the National Cyber Director：国家サイバーディレクター室）が発行する「REPORT ON THE CYBERSECURITY POSTURE OF THE UNITED STATES[106]」、英国の NCSC（National Cyber Security Centre：英国国家サイバーセキュリティセンター）が発行する「NCSC Annual Review[107]」、EU の ENISA（The European Union Agency for Cybersecurity：欧州ネットワーク情報セキュリティ機関）が発行する「ENISA Threat Landscape[108]」等によると、世界各国でランサムウェア攻撃、標的型攻撃、DoDS 攻撃、脆弱性を利用した攻撃等の高度な技術を使用したサイバー攻撃が活発に行われていることが判明した。（表 4.2-8）

表 4.2-7　高度なサイバー攻撃の主な種類

種類	概要
ランサムウェア攻撃	パソコンやサーバー等のシステムのロックや、システムに保存されているファイルを暗号化することにより、機器を使用不能にし、その解除に身代金を要求する攻撃
標的型攻撃	特定の企業・組織や業界等を狙って行われるサイバー攻撃の一種で、フィッシングメールやウイルスメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、標的型攻撃は、標的とする特定の企業・組織や業界が持つ機密情報の窃取等明確な目的をもって行われる攻撃
DoDS 攻撃	Web サーバー等の攻撃対象に対して、複数の送信元から同時に大量のパケットや問い合わせを送信することで、攻撃対象のリソースに負荷をかけ、サービス運用を妨害する攻撃である
ソフトウェアの脆弱性を悪用した攻撃	VPN やその他ソフトウェア製品等の脆弱性を狙い、修正が行われる前にそれを標的に攻撃を行い、機密情報の入手やランサムウェアを含むマルウェアの挿入等の攻撃に使用するもの

上記のような各サイバー攻撃に対して、それぞれ対策が採られているものの、現行多く実施されている攻撃検知システム技術では、一度サイバー攻撃として利用されたプログラム等の事例を分析し、分析結果を基に、プログラムに類似したサイバー攻撃等を検知する技術が主となっており、まだ確認されていない未知の手法等によるサイバー攻撃が実施された場合、分析結果等が得られていないため、その攻撃を検知することができず、被害の発生や対応の困難性が生じる等の共通の課題があることが判明した。(表 4.2-9)

[105] https://www.ipa.go.jp/security/10threats/10threats2024.html
[106] https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf
[107] https://www.ncsc.gov.uk/collection/annual-review-2023
[108] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

表 4.2-8　サイバー攻撃への対応及び課題

種類	対応	課題
ランサムウェア攻撃	・ネットワーク侵入への対策 ・侵入範囲拡大防止のための対策 ・暗号化によるシステム停止への対策 ・インシデント対応力の強化	ランサムウェアのセキュリティソフトは基本的に過去にあったランサムウェアの特徴等を学習し、類似したランサムウェア等を検知する仕組みになっているため、新たに登場した未知のランサムウェアに対して無防備となる
標的型攻撃	・役職員の意識向上 ・組織としての対応体制の強化 ・システムによる対策	攻撃手法が多岐にわたり、対象者の組織の状況に合わせて手法を変化させるなど、新たな攻撃手法も次々と現れるため、有効な対策を取ることが困難
DoDS 攻撃	・DoDS 攻撃への平時からの予防対策 ・DoDS 攻撃を受けた場合の対処対策	攻撃手法が多岐にわたり、新たな手法も次々と現れるため、有効な対策を取り続けることが困難
ソフトウェアの脆弱性を悪用した攻撃	・脆弱性に関する情報の収集 ・速やかなアップデートの実施 ・ベンダーから提供された脆弱性の影響を提言する方法の実施 ・日頃のログや通信の監視	ゼロデイ攻撃等、企業が修正プログラムや脆弱性対策情報を公開する前、もしくはそもそもの脆弱性情報を把握する前に攻撃された場合、有効な対策を取ることが困難

調査した論文等の結果を基に、従来のサイバー攻撃対処において共通の課題となっていた事項を解決することが期待され、また近年研究開発も多く実施されており、サイバー空間の活用が今後更に不可欠になると見込まれる状況等から経済安全保障の観点からもより一層重要性が増していくと判断した技術領域を調査・整理した。

4.2.3 海洋分野

（1）技術領域の調査・整理

海洋分野における技術領域調査・整理のため、国内外の海洋研究関連機関等のホームページで、最近対象国等で実施された海洋分野に関する研究開発プロジェクトや発表された論文等を調査した。（表 4.2-12）

表 4.2-9　確認した主な海洋分野の研究機関等

機関名	国	概要
JAMSTEC （海洋研究開発機構）	日本	文部科学省が所管する海洋科学技術に関する研究機関で、海洋の調査・研究を行う独立行政法人。地球環境の把握、海洋資源の利用、地震・火山活動に関する調査研究を実施している
DAPRA （国防高等研究計画局）	米国	米国防総省の機関で、米軍が今直面しているニーズではなく、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、実用化の加速をミッションとしている

NOAA （米国海洋大気庁）	米国	米国商務省の傘下で、海洋と大気に関する研究・監視・予測を行う政府機関。
DASA （防衛セキュリティ促進機構）	英国	国防省所管の機関であり、革新的な技術の発掘と開発支援を通じた、イギリスの防衛・国家安全保障の強化を目的とした活動に取り組む。
NOC （英国国立海洋学センター）	英国	科学技術・イノベーション省所管の機関であり、海洋学の研究と技術開発を行い、英国の海洋政策や環境保護、気候変動対策に取り組む。
東京海洋大学	日本	日本で唯一の海洋分野に特化した国立大学であり、海洋科学や水産学、海洋工学の先進的な研究を行っている。

調査の結果、現在国内外の海洋分野の研究開発機関においては、細かい差異はあるものの、主に海洋状況把握や資源探査に関連した無人機関連技術等の研究開発が多く実施されていることが確認できた。（表 4.2-13）

研究開発プロジェクト・論文の詳細については Appendix Ⅱ を参照

表 4.2-10　海洋分野における研究開発プロジェクト・論文(一部抜粋)

論文・プロジェクト名	時期	国・機関	技術領域
海面から海底に至る空間の常時監視技術と海中音源自動識別技術の開発	2024～	日本 JAMSTEC	海面から海底に至る鉛直断面の常時観測･モニタリングのための海中音源自動識別技術を用いた常時監視システム技術
戦略的イノベーション創造プログラム（SIP） 革新的深海資源調査技術 研究開発計画	2021		レアアース泥等の深海鉱物資源調査の効率化のための深海調査技術･鉱物資源の採取技術
Ocean of Things	2017～	米国 DARPA	広大な海洋エリアにおける持続的な海上状況認識の実現のためのフロートセンサー技術
Manta Ray	2020～		海中での長期間にわたる持続･自律的な活動のための UUV 開発技術
BioLogical Undersea Energy (BLUE)	2024～		センサーシステムの電力の持続的な供給実現のための電力供給技術
無人システム運用プログラム	2020	米国 NOAA	高品質な環境データの収集のための無人航空機･無人海洋システム技術
Look Out! Maritime Early Warning Innovations	2021～	英国 DASA	海上作戦における早期からの状況認識を可能にするための早期警戒技術

現在 K プログラム等では支援対象となっておらず、無人探査やセンシング等にも関連する経済安全保障の観点からも重要となる技術領域を調査・整理した。

4.2.4 バイオ分野

（1）技術領域の調査・整理

バイオ分野における技術領域調査・整理のため、国内外のバイオ研究関連機関等のホームページで、最近対象国等で実施されたバイオ分野に関する研究開発プロジェクトや発表された論文等を調査した（表 4.2-16）。

表 4.2-11　確認した主なバイオ分野の研究機関等

機関名	国	概要
国立がん研究センター	日本	厚生労働省所管。がん治療・予防の研究や診療向上、医薬品開発、患者支援を進める。
NEDO （新エネルギー・産業技術総合開発機構）	日本	経済産業省所管。エネルギー・環境技術や産業技術の研究開発を推進し、実用化支援を行う。
JST （科学技術振興機構）	日本	文部科学省所管。基礎・応用研究の支援、産学連携、社会実装を促進し、科学技術政策を支える。
NARO （農業・食品産業技術総合研究機構）	日本	農林水産省所管。農業・食品に関する技術開発及び資金提供、産学官連携支援を行う。
ARS Agricultural Research Service （農業研究局）	米国	米国農務省所管。農業生産、食品安全、環境保全のための基礎・応用研究を推進する。
ARPA-H Advanced Research Projects Agency for Health （健康高度研究計画局）	米国	米国保健福祉省所管。革新的な医療技術・治療法の開発を促進し、健康・医療課題の解決を図る。

国内外のバイオ分野の研究開発機関においては、細かい差異はあるものの、主に個別化医療、食料安全保障、バイオものづくりに関連した技術の研究開発が多く実施されていたことが分かった（表 4.2-17）。

研究開発プロジェクト・論文の詳細については Appendix Ⅱ を参照

表 4.2-12　バイオ分野における研究開発プロジェクト・論文（一部抜粋）

論文・プロジェクト名	時期	国・機関	技術領域
戦略的イノベーション創造プログラム（SIP） スマートバイオ産業・農業基盤技術	2018	日本 NARO	ゲノム編集・オミクス解析を活用した農作物育種技術 持続可能な農業生産のための植物保護技術
戦略的イノベーション創造プログラム（SIP） 次世代農林水産業創造技術	2014-2018		精密ゲノム編集技術と育種技術 バイオマス資源の有効活用と循環型生産技術
SCRUM- Japan	2013-	日本 国立がん研究センター	全ゲノム解析を活用したがんの再発リスク測定
Food Animal Production	2022-	米国 ARS Agricultural Research Service （農業研究局）	食品動物生産の効率向上、産業の持続可能性確保、および製品品質の向上を目的とした研究開発 遺伝学・ゲノミクス研究を通じて、食肉生産の効率化と品質向上に取り組む
Plant Genetic Resources, Genomics and Genetic Improvement	2022-		作物の遺伝資源・ゲノム情報を活用し、農業生産性の向上と食料・繊維・飼料・工業製品の安全な供給を確保するための研究開発
Advanced Analysis for Precision Cancer Therapy	**開始年不明** 現在も進行中	米国 ARPA-H Advanced Research Projects Agency for Health （健康高度研究計画局）	がん治療の個別化と適応性向上のための技術
産業用微生物等の開発・育種及び微生物等改変プラットフォーム技術の高度化	2023-	日本 NEDO	ゲノム編集・遺伝子改変等の技術によって高い物質生産性を有する産業用微生物等の開発
革新的 GX 技術創出事業（GteX）	2023-	日本 JST	DNA 合成・ゲノム編集技術等により CO_2 の固定化能の向上、生産できる化学品の種類の多様化や生産性の向上につながる未知の代謝経路や革新的な微生物を開発

ゲノムに関連する研究開発など、近年、日本の中で注目されているような技術領域を調査・整理した。

5. 調査結果の比較・分析

5.1 国外における経済安全保障の確保に向けた政策動向に関する調査研究

比較・分析では、これまでの調査結果を取り纏めたうえで、調査テーマである①リスクに晒されている研究領域の特定と情報共有、②デュー・ディリジェンスの実施・リスクのある活動の領域の特定、③リスク軽減策　の各施策が実施される全体像を踏まえ、以下の観点から調査結果の比較・分析を行うこととした（図 5.1-1）。

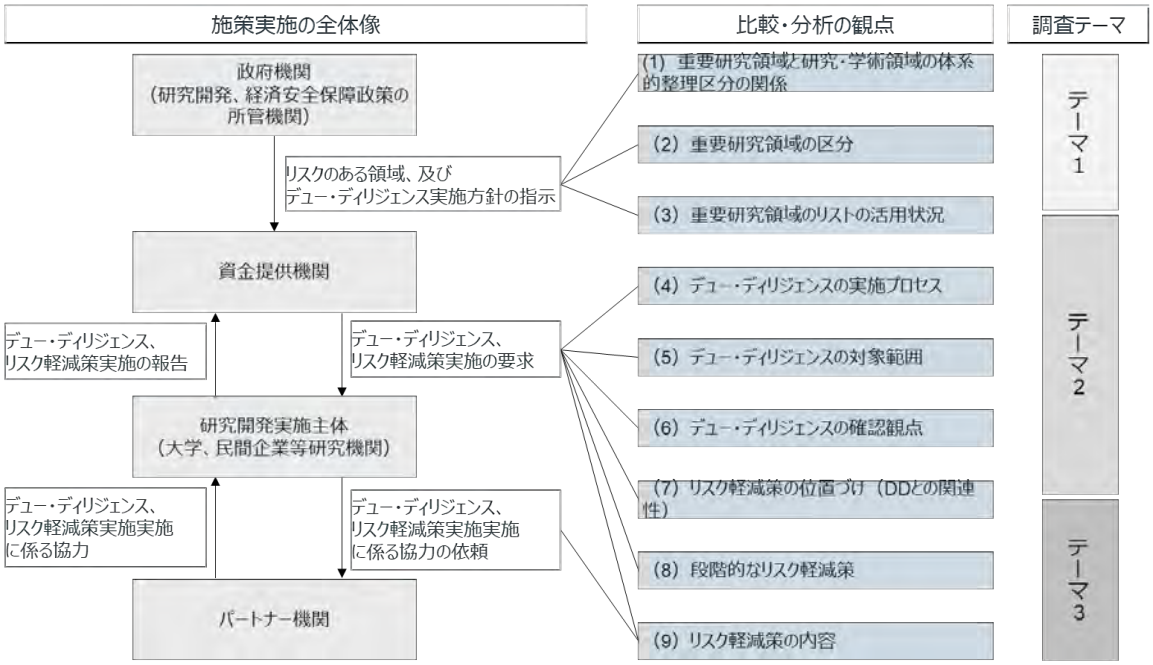


図 5.1-1　施策実施の全体像を踏まえた比較・分析観点

（1）重要研究領域と研究・学術領域の体系的整理区分の関係

各国の研究・学術領域の体系的整理区分と、リスクに晒されている重要研究領域のリストを比較したところ、関連性は見受けられなかった。

研究・学術領域の体系的整理区分は、科学技術政策のための統計収集や予算配分等のための網羅的な分類となっていることに対して、リスクに晒されている研究領域のリストは、国にとってのリスクや経済的利益を念頭においた技術、アプリケーションとして整理されていることが確認できた（図 5.1-2）。

Secsitive Technology Research Area（STRA）	
ハイレベル技術カテゴリ	サブカテゴリ（補足文の例）
1.先端デジタルインフラ技術	• 高度な通信技術 • 高度なコンピューティング技術 • 暗号化手法 • サイバーセキュリティ技術 • データストレージ技術 • 分散型台帳技術 • マイクロ エレクトロニクス • 次世代ネットワーク技術
2. 先端エネルギー技術	• 先進エネルギー貯蔵技術 • 先進的原子力発電技術 • ワイヤレス給電技術
3. 先端材料と製造	• 拡張された従来の材料 • オーキセティック材料 • 高エントロピー材料 • メタマテリアル • 多機能／スマートマテリアル • ナノマテリアル • ・・・
・・・	・・・

カナダ研究開発分類（CRDC）		
区分	グループ	クラス
RDF10：自然科学	RDF101：数学と統計	RDF10101：純粋数学
		RDF10102：応用数学
		RD10103：統計
	RDF102：コンピュータと情報科学	RDF10201：人工知能（AI）
		・・・
	・・・	・・・

図 5.1-2　例：重要研究領域のリスト（STRA）と研究・学術領域の体系的整理区分（CRDC）

（2）重要研究領域の区分

各国で策定されている重要研究領域のリストについて、指定されている領域の区分について整理・比較を行ったところ、分野の数としては各国の指定粒度によって前後するものの、概ね 10 前後の分野数が指定されていることが確認できた。

各国で共通して指定されている分野としては、**人工知能、先端製造、バイオテクノロジー、半導体、宇宙関連技術、先端センシング、ロボティクス**等が確認でき、これらの分野は各国で共通的に経済安全保障上のリスクや重要性が高いと認識されているものと想定される（表 5.1-1）。

表 5.1-1　各国の重要研究領域の比較

国	米国	カナダ	
リスト名	CETs	STRA	Emerging Technology Trend Cards
指定されている分野数	18 分野	11 分野（ハイレベル技術カテゴリー）	10 分野
指定されている分野	① 先端コンピューティング ② 先端工学材料 ③ 先端ガスタービン・エンジン技術 ④ 高度でネットワーク化されたセンシングとシグネチャ管理 ⑤ 先端製造 ⑥ 人工知能 ⑦ バイオテクノロジー ⑧ クリーンエネルギー生成と貯蔵 ⑨ データプライバシー、データセキュリティ、サイバーセキュリティ技術 ⑩ 指向性エネルギー ⑪ 高度自動化・自律化・非クルーイングシステム（UxS）・ロボット工学 ⑫ ヒューマン・マシン・インターフェース ⑬ ハイパーソニックス ⑭ 統合通信・ネットワーク技術 ⑮ 測位・航法・タイミング（PNT）技術 ⑯ 量子情報とそれを可能にする技術 ⑰ 半導体とマイクロエレクトロニクス ⑱ 宇宙技術とシステム	① 先端デジタルインフラ技術 ② 先端エネルギー技術 ③ 先端材料と製造 ④ 高度なセンシングと監視 ⑤ 高度な武器 ⑥ 航空宇宙・宇宙・衛星技術 ⑦ 人工知能とビッグデータ技術 ⑧ ヒューマンマシンインテグレーション ⑨ ライフサイエンステクノロジー ⑩ 量子科学技術 ⑪ ロボティクス・自律システム	・ 見通し外通信とアプリケーション ・ 寒冷気候用衣料の素材と生理学的モニタリング ・ 極超音速兵器への対抗手段 ・ 指向性エネルギー兵器 ・ 寒冷地におけるエネルギー生成と貯蔵 ・ 軍の女性の健康に関する研究 ・ 人員シールド ・ 測位、ナビゲーション、タイミング技術 ・ 宇宙技術 ・ 水中探知

国	英国	EU	豪州	韓国
リスト名	Five Critical Technologies-	Critical Technology Areas	List of Critical Technologies in the National Interest-	国家戦略技術
指定されている分野数	5 分野	10 分野（うち最も差し迫ったリスクのあるものは 4 まで）	7 分野	12 分野
指定されている分野	① 人工知能（AI） ② エンジニアリング生物学 ③ 未来の通信 ④ 半導体 ⑤ 量子技術	① 先端半導体技術 ② 人工知能（AI）技術 ③ 量子技術 ④ バイオ技術 ⑤ 先端接続性、ナビゲーション、デジタル技術 ⑥ 先端センサー技術 ⑦ 宇宙、推進技術 ⑧ エネルギー技術 ⑨ ロボット工学、自律システム ⑩ 先端材料、製造、リサイクル技術	① 高度な製造および材料技術 ② AI テクノロジー ③ 高度な情報通信技術 ④ 量子技術 ⑤ 自律システム、ロボット工学、ポジショニング、タイミング、センシング ⑥ バイオテクノロジー ⑦ クリーンエネルギー生成および貯蔵技術	① 半導体・ディスプレイ ② 二次電池 ③ 先端モビリティ ④ 次世代原子力 ⑤ 先端バイオテクノロジー ⑥ 航空宇宙・海洋技術 ⑦ 水素 ⑧ サイバーセキュリティ ⑨ AI

また、各国に共通して見られた人工知能、先端製造、バイオテクノロジー、半導体、宇宙関連技術について、他国に比してその細目を記載している米国、カナダ、豪州で比較したところ、粒度には各国の差異があるものの、以下のような共通的なキーワードが確認できた（表 5.1-2）。

人工知能：機械学習、自然言語処理 先端製造：3D プリント、ナノマテリアル バイオテクノロジー：バイオ製造、ゲノム解析 半導体：製造プロセス全般 宇宙関連技術：推進技術

表 5.1-2　重要研究領域の細目の比較

国	米国	カナダ	豪州
リスト名	CETs	STRA	List of Critical Technologies in the National Interest-
人工知能	・機械学習 ・ディープラーニング ・強化学習 ・知覚と認識 ・AI の保証と評価技術 ・基礎モデル ・生成 AI システム、マルチモーダルモデル、大規模言語モデル ・トレーニング、チューニング、テストのための合成データアプローチ ・計画、推論、意思決定 ・AI の安全性、信頼性、セキュリティ、責任ある利用を向上させる技術	・AI チップセット ・コンピュータービジョン ・データサイエンスとビッグデータ技術 ・デジタルツイン技術 ・機械学習 ・自然言語処理	・ニューラルネットワークやディープラーニングを含む機械学習 ・AI アルゴリズムとハードウェアアクセラレータ ・音声とテキストの認識、分析、生成を含む自然言語処理
先端製造	・先進アディティブ・マニュファクチャリング（積層造形） ・クリーンで持続可能なスマート・マニュファクチャリング ・ナノマニュファクチャリング ・軽量金属製造 ・製品・材料回収を支援するものを含む先進的製造技術および技法	・従来の材料の拡張 ・オーセティック材料 ・高エントロピー材料 ・メタマテリアル ・多機能／スマート材料 ・ナノマテリアル ・積層造形用粉末材料 ・2 次元（2D）材料　等	・3D プリントを含む付加製造 ・重要な鉱物の抽出と処理 ・先進複合材料 ・高仕様の加工プロセス ・半導体および高度な集積回路の設計と製造

国	米国	カナダ	豪州
バイオテクノロジー	・核酸、ゲノム、エピゲノム、タンパク質の合成と設計ツールを含むエンジニアリングを含む新しい合成生物学 ・機能的表現型のためのマルチオミクスとその他のバイオメトロジー、バイオインフォマティクス、計算生物学、予測モデリング、分析ツール ・亜細胞、多細胞、マルチスケールシステムのエンジニアリング ・無細胞システムと技術 ・ウイルスおよびウイルス送達システムの工学 ・生物／生体インターフェース ・バイオマニュファクチャリングとバイオプロセス技術	・バイオ製造 ・ゲノム配列解析と遺伝子工学 ・プロテオミクス ・合成生物学	・合成生物学（生物学的製造を含む） ・神経工学と脳コンピューターインターフェース ・ゲノムと遺伝子の配列解析と分析 ・ワクチンと医療対策 ・核、抗ウイルス、抗生物質を含む新薬
半導体	・設計および電子設計自動化ツール ・製造プロセス技術と製造装置 ・CMOS（相補型金属酸化膜半導体）技術を超えるもの	・先進的な半導体製造（堆積、コーティング、リソグラフィー、イオン化/ドーピング、および熱管理技術などのその他のコアプロセスとサポートプロセスなど）	—
宇宙関連技術	・宇宙空間でのサービス、組立、製造、およびそれを可能にする技術 ・費用対効果の高いオンデマンド、再利用可能な宇宙打上げシステムを実現する技術 ・二重星雲空間および／または新規軌道へのアクセスと利用を可能にする技術 ・宇宙観測用のセンサーとデータ解析ツール ・宇宙推進 ・先進的な宇宙船発電 ・新しい宇宙船の熱管理 ・有人宇宙飛行の実現 ・耐障害性と経路多様性に優れた宇宙通信システム、ネットワーク、および地上局 ・宇宙打ち上げ、航続距離、安全技術	・先進的な風洞 ・軌道上整備、組立、製造システム ・ペイロード ・推進技術 ・衛星 ・宇宙ベースの測位、ナビゲーション、タイミング技術 ・宇宙ステーション ・ゼロエミッション/燃料航空機	—

（3）重要研究領域のリストの活用状況

各国の重要研究領域のリストの活用状況を比較したところ、リストの傾向としては、国の科学技術政策上の重点分野の形成や、関係する省庁間の取り組みの調整、政府支援施策等の根拠とするために、政府機関や研究コミュニティに対して情報を提供しているものが多く見られた（米国、英国、EU、豪州、韓国）。

また、各領域の内包する経済・安全保障上のリスクへの対処については、関係機関への情報提供や参考程度に留まるものもある一方、具体的に研究セキュリティ・インテグリティに係るデュー・ディリジェンスやスクリーニング基準等に用いられるリストも見られた（カナダ、豪州）（表 5.1-3）。

表 5.1-3　重要研究領域のリストの目的・活用状況の比較

国	米国	カナダ	
リスト名称	Critical and emerging Technologies（CETs）	Sensitive Technology Research Areas（STRA）	Emerging Technology Trend Cards
リストの目的	政府機関や研究コミュニティに対する情報提供（一部技術情報保護のための参考）	連邦助成評議会および CFI（カナダイノベーション財団）に提出されるすべての助成金申請に対するスクリーニング基準	研究コミュニティに対する情報提供
活用方法の詳細	・CETs は、政府機関や研究コミュニティ等にとって技術競争・国家安全保障上の重要技術に関する情報リソースとして活用されることが前提となっている ・しかし一部で機密情報の不正流用や悪用から研究を保護するための参考とできる旨も記載されている	・STRA は連邦助成評議会および CFI（カナダイノベーション財団）に提出されるすべての助成金申請に適用される ・STRA のサブカテゴリに該当する研究プロジェクトは、従事する研究者が指定研究機関(NRO)に所属する、もしくは NRO からの支援を受けている場合申請対象外となる	・トレンドカードは「研究セキュリティのデュー・ディリジェンスの目的で、政府の機密研究分野のリストに追加または置き換えるものではない」とされるため STRA のような活用方法は想定されていないと思われる ・しかし「デュアルユースの新興テクノロジーに関して、セキュリティに対するリスクを最小限に抑える」ことに役立てるという記載もあるため、研究コミュニティに対して当該技術がデュアルユースである（リスクがある）ことを周知する意図もあるものと想定される

国	英国	EU	豪州	韓国
リスト名称	The UK Science and Technology Framework-five critical technologies	Critical Technology Areas	List of Critical Technologies in the National Interest	国家戦略技術
リストの目的	科学技術政策上の重点分野の形成、政府支援施策の根拠	加盟国と共に集団的リスク評価を行い、リスク低減策を講じる	科学技術政策上の重点分野の形成、政府支援施策の根拠 デュー・ディリジェンスの対象となる研究分野のリストとしての活用	科学技術政策上の重点分野の形成、政府支援施策の根拠 政府の支援する研究開発事業における、セキュリティの強化や情報提供を求める分野の特定
活用方法の詳細	5 大重要技術（five critical technologies）は The UK Science and Technology Framework において科学技術政策上の重点分野を形成しており、今後の政府施策の根拠となっているが、内在するリスクの特定や研究セキュリティに活用するような記載は現状確認できない	リスク低減策については、現時点では具体的には決定しておらず、リスク評価後に加盟国と協議すると述べている。（2024 年春にリスク評価の結果新たな低減策を講じる可能性があるとしていたが、現状確認できない）	・リスト及び併せて公表された「重要な技術に関する声明」では、「重要技術セキュリティ対策を提供する」旨が記載されているのみであり、具体的な活用方法は確認できていない ・しかし、政府の主要な資金提供機関である豪州研究会議（ARC）は、「重要技術に該当する研究の助成申請にはリスク要因の検討を行う」旨述べており、デュー・ディリジェンスの対象となる研究分野のリストとしても活用されていると想定される	国家戦略技術は、「国家戦略技術育成に関する特別法」に定められている国による研究開発事業（国家戦略技術研究開発事業）の実施や、その保護・育成に係る諸施策の対象となる 国家戦略技術研究開発事業ではセキュリティの強化や情報提供を研究開発実施主体等に求められることとなる

（4）デュー・ディリジェンスの実施プロセス

各国のデュー・ディリジェンスの全体的な実施プロセスについて比較したところ、英国、豪州、カナダでは資金提供機関が研究開発実施主体（申請者）に対してデュー・ディリジェンスの実施を指示してその結果を受け取り、資金提供機関が最終的なリスク評価・資金提供可否の判断を行っているのに対して、米国、韓国では資金提供機関が必要な情報の開示を研究開発実施主体に対して指示し、開示された情報に基づきリスク評価を行う点で差異が見られた（表 5.1-4）。

EU（ドイツ）では、現状は大学や研究機関にリスク低減策の一つとしてデュー・ディリジェンスの実施を推奨しているものの、詳細なツールやリソースは今後策定予定となっていた。

また、研究開発実施主体にデュー・ディリジェンスを実施させる米国以外の国の取り組みを比較したところ、**①目的や対象、確認観点のみを示しているもの、②大まかなプロセスを示しているもの、③具体的な作業手順まで示しているもの** に大別でき、現状の調査結果では、カナダの NSGRP におけるデュー・ディリジェンスのガイダンスが最も詳細に作業手順を示していることが確認できた（図 5.1-3）。

表 5.1-4　各国のデュー・ディリジェンスの全体的なプロセスの比較

国	米国	韓国	カナダ	英国	豪州
デュー・ディリジェンスの根拠となる取り組み・ガイドライン（所管）	・NSPM-33 実施ガイダンス（NSTC） ・CFIP（DARPA） ・NIH Dicision Matrix ・TRUST	・国外受益情報報告制度	・NSGRP（ISED）	・Trusted Research ガイダンス群（NPSA、NCSC） ・Due diligence guidance and supporting documents（UKRI）	・豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン（UFIT）
デュー・ディリジェンスの実施者	・　資金提供機関		・　資金提供機関 研究開発実施主体（申請者）		
デュー・ディリジェンスのプロセス	①　資金提供機関が申請者に対して情報開示を求める ②　申請者から情報を開示 ③　資金提供機関は開示された情報から、機関内の一定の基準に基づきリスクを評価		①　資金提供機関が申請者に対してデュー・ディリジェンスの実施を求める ②　申請者からデュー・ディリジェンスの実施結果を報告・申請 ③　資金提供機関は申請者のデュー・ディリジェンスの結果を基に最終的なリスクを評価		

※EU（ドイツ）では、現状は大学や研究機関にリスク低減策の一つとしてデュー・ディリジェンスの実施を推奨しているものの、詳細なツールやリソースは今後策定予定となっている

図 5.1-3　各国のデュー・ディリジェンス実施者に示しているプロセスの比較

（5）デュー・ディリジェンスの対象範囲

各国のデュー・ディリジェンスの対象範囲としては、EU、カナダ、豪州、英国はパートナー機関を対象としているが、研究活動自体を対象としたもの、自組織の職員を対象とした情報開示要求も含め「デュー・ディリジェンス」と呼称している場合があるなど、取り組みやガイドラインによって差異が見られた（表 5.1-5）。

表 5.1-5　各国のデュー・ディリジェンスの対象範囲の比較

国	ガイドライン・取り組み	実施者	対象範囲		
			研究活動	パートナー機関	自組織（職員）
米国	・ NSPM-33 実施ガイダンス ・ CFIP ・ NIH Dicision Matrix ・ TRUST	・ 資金提供機関	―	●	●
カナダ	・ National Security Guidelines for Research Partnerships（NSGRP）におけるデュー・ディリジェンス	・ あらゆる研究者 ・ 特定の資金提供プログラム申請者	●	●	―
	・ NESRC、CIHR、SSHRC における取組	・ あらゆる研究者 ・ 特定の資金提供プログラム申請者	● （政府に準じる）	● （政府に準じる）	―
EU	・ 研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書	・ EU の大学・研究機関	●	●	―
	・ DFG 勧告	・ DFG への助成金を申請する研究者	●	●	―
英国	・ Trusted Research ガイダンス群	・ 大学の研究者 ・ 大学職員	●	●	―
	・ Due diligence guidance and supporting documents	・ UKRI の助成金申請者	―	●	―
豪州	・ 豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン（UFIT）	・ 豪州の学術機関(特に意思決定者)	●	●	●
	・ 豪州研究会議（ARC）の取り組み	・ 特定の資金提供プログラム申請者	● （政府に準じる）	● （政府に準じる）	● （政府に準じる）
韓国	・ 国外受益情報報告制度	・ 研究開発課題の主任研究者	―	―	●

（6）デュー・ディリジェンスの確認観点

各国のデュー・ディリジェンスの確認観点を比較したところ、研究活動・パートナー・自組織といった対象ごとにある程度共通的であることが確認できた（表 5.1-6）。

パートナー組織や自組織職員に係る利益相反、責務相反のリスクについては共通的に米国、カナダ、英国、豪州、韓国で確認されているが、申請者の研究活動自体の持つリスクについても分析を推奨している点で、EU、カナダ、豪州、英国は米国、韓国と差異が見られる。

表 5.1-6　各国に共通したデュー・ディリジェンスの確認観点

対象	確認観点	確認事項の細目例
研究活動	研究内容自体のリスク	・研究分野のデュアルユース性、応用先の倫理的・道徳的懸念 ・多くの個人情報や機密情報を扱うか ・輸出規制に抵触するか ・外国投資規制に抵触するか ・自国の保護すべき重要技術分野や重要物資に該当するか
	研究内容のポテンシャル（外国からの魅力）	・　技術成熟度 ・　商業化または特許取得可能な成果をもたらす可能性はあるか ・　自国の国益を著しく向上させる可能性はあるか ・　パートナーの国の国益を著しく向上させる可能性はあるか
	サイバーセキュリティ	・　アクセス制御や不正アクセスの監視・防護は十分か ・　共同研究の中で、自身の施設・ネットワーク・資産にパートナーはアクセスできるか
パートナー	自律性・透明性の欠如、非倫理的行為の有無	・　パートナー所在国の民主主義、自由、政治腐敗等のスコアは ・　軍・治安機関との関係など、外国政府の影響や干渉を受けているか ・　輸出規制のエンドユーザーに該当しているか ・　国連や自国の制裁リストに該当しているか ・　テロ組織、マネーロンダリングとの関係はないか ・　詐欺、賄賂、スパイ活動、汚職、知的財産の侵害を行っているか
	パートナーの持つ意思・能力	・　パートナーやその上位機関・政府は、当該研究分野で知的財産を蓄積しているか ・　当該研究分野におけるパートナーの能力（自身の方が著しく高くはないか）
自組織（職員）	外国との提携・関係性	・　外国の支援を受けているか ・　外国の機関で職位を有しているか ・　外国の大学や政府、軍・警察等治安機関と連携しているか

（7）リスク軽減策の位置づけ

テーマ 3 において、テーマ 2 のデュー・ディリジェンスに係る取り組み・ガイドラインと関連したリスク軽減策や、その周辺規則・機関のリスク軽減策を調査した。

その位置づけとしては、カナダは NSGRP の適用される研究開発プログラムにおいてデュー・ディリジェンスを実施し、その結果に基づきリスク軽減計画を実施することを求めており、デュー・ディリジェンスの結果とリスク軽減策に明確な連動が確認できる点で各国との差異が確認できた。

その他、米国の NSF 研究セキュリティトレーニングや、英国、EU、豪州については、デュー・ディリジェンス結果との明示的な関連性は確認できないものの、研究セキュリティ・インテグリティ上の脅威やリスクを示したうえで、ガイドラインとして大学や研究機関に実施を推奨するものとなっている（表 5.1-7）。

表 5.1-7　各国のリスク軽減策の位置づけ

国	米国		カナダ	英国	EU	豪州	韓国
リスク軽減策が確認できた取り組み・ガイドライン	NSF 研究セキュリティトレーニング	NIH GPS におけるリスク軽減策	NSGRP におけるリスク軽減策	Trusted Research におけるリスク軽減策	研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書におけるリスク軽減策	UFIT ガイダンスにおけるリスク軽減策	国家研究開発革新法におけるリスク軽減策
リスク軽減策の指示主体	NSF（規制ではなく、ガイダンスとして実施を推奨するもの）	NIH（助成金申請時に要求するもの）	NSERC、CIHR、SSHRC 等の資金提供機関 カナダ公安省、カナダ安全保障情報局、または通信安全保障局（追加のリスク軽減措置の要求）	政府（規制ではなく、ガイダンスとして実施を推奨するもの）	欧州委員会（規制ではなく、ガイダンスとして実施を推奨するもの）	政府（規制ではなく、ガイダンスとして実施を推奨するもの）	政府（資金提供機関）
リスク軽減策の実施主体	研究機関の研究者や管理者	NIH の支援する研究開発プログラムへの申請者	NSGRP が適用される資金提供プログラムへの申請者	大学の研究者、大学職員	EU の大学や学術機関（特に意思決定者）	豪州の大学や学術機関（特に意思決定者）	研究開発課題に参加する研究開発実施主体
リスク軽減策を実施するタイミング	—（規制ではなく、ガイダンスとして実施を推奨するもの）	研究開発プログラムへの申請時、及び実施中	NSGRP が適用される資金提供プログラムへの申請が受理され、資金提供が決定されたのち、プロジェクト期間中に実施することとなっている	—（規制ではなく、ガイダンスとして実施を推奨するもの）	—（規制ではなく、ガイダンスとして実施を推奨するもの）	—（本ガイドラインは、既存の大学のポリシーに合わせて参照するように記載されている）	研究開発課題への申請時及び実施期間中
リスク軽減策とテーマ 2 のデュー・ディリジェンス結果との関連性	—	—	デュー・ディリジェンス結果に基づき、リスク軽減計画を提出、実行することとなっている	—	—	—	—

（8）段階的なリスク軽減策

デュー・ディリジェンス結果に応じた段階的なリスク軽減策については、例えば米国CFIP、NIH Dicision Matrixなどのリスク要因ごとにリスクレベルを設定している場合については、主任研究者の交代や助成金授与の可否判断も含めて段階的なリスク軽減策を講じている可能性があるものと見ることができる。

（9）リスク軽減策の内容

リスク軽減策の内容については、まず、テーマ2にて記載したデュー・ディリジェンスについては、自組織職員や研究者の利益相反・責務相反リスクや、パートナー機関を通じた外国の不当な干渉や情報漏洩のリスクを検知する取り組みであることから、人的・組織的なリスク軽減策の一部と見ることができる。

その他、インフラ面のリスク軽減策ではサイバーセキュリティに係るものが主であり、組織としてのサイバーセキュリティ対策の整備を促す趣旨のものから、個人が実施すべきパスワード管理やファイル転送時の留意事項等の対策が確認できた。

人的側面のリスク軽減策は、自組織及び組織外の人員に対する利益相反・責務相反のチェックや、海外勤務時の人的な留意事項（人との接触等）、意識啓発・トレーニングの提供等が確認できた。

組織的側面のリスク軽減策は、テーマ 2 で報告したパートナー組織に対するデュー・ディリジェンスの実施や、そのための自組織内のガバナンス体制の整備が確認できた（表5.1-8）。

表 5.1-8　各国のリスク軽減策の内容

項目	米国		カナダ	英国
リスク軽減策が確認できた取り組み・ガイドライン	NSF 研究セキュリティトレーニング	NSF GPS におけるリスク軽減策	NSGRP におけるリスク軽減策	Trusted Research におけるリスク軽減策
インフラ面のリスク軽減策	・渡航先やデータの種類に適したセキュリティ対策 ・出荷に関する安全規制や記録要件の確認 ・輸出管理規制を確認し、電子的な共有にも留意 ・制限された技術設備や情報の保護	・個人情報をポータブルデバイスに保存しない、保存する場合は暗号化する ・パスワード保護等の手段により個人情報へのアクセスを制限 ・送信前に受信側のセキュリティレベルを確認	・自組織及びパートナー組織におけるサイバー安全教育の実施、サイバーセキュリティ対策の慣行 ・国内外への移動におけるデバイスの管理	・研究協力におけるアクセス制御、不正アクセスの監視と防止、サプライチェーンまたはパートナー組織のセキュリティ対策の実施 ・研究者個人への認証情報管理やファイル転送時の留意事項の提供
人的リスク軽減策	・共同研究者のスクリーニング ・契約条件や要求事項の確認により、悪意のある外国人人材採用プログラムでないか確認 ・自己の関与する事項や外国との関係については、早期に開示し、適切な管理を行う	・FCOI の確認に関する情報開示等（テーマ 2 にて記載） ・FCOI が確認された場合、FCOI レポートの提出を求める	・チームメンバー全員の職歴を確認し、プロジェクトの研究目的との整合性を評価 ・チームメンバーとの共同作業を妨げる可能性のある、既存または潜在的な利益相反や提携関係を評価 ・プロジェクトのリスクについて社内で話し合い、必要に応じ外部のチームメンバーを巻き込んでリスクを軽減する計画を立てる	・海外からの訪問者や研究者を誘致するにあたっての経歴、過去の仕事、現在の義務の理解 ・英国と異なる民主主義的価値観・倫理観を持つ国で勤務するスタッフがいる場合のリスク評価 ・海外の学会参加などで海外渡航する場合の留意事項の提供
組織的リスク軽減策	―	同上	・パートナー機関へのデュー・ディリジェンス（テーマ 2 にて記載） ・パートナーの動機と自分の動機の一致を評価 ・パートナーとの研究成果の利用目的に関する合意	・パートナー機関へのデュー・ディリジェンス（テーマ 2 にて記載）

項目	豪州	EU	韓国
リスク軽減策が確認できた取り組み・ガイドライン	UFIT ガイダンスにおけるリスク軽減策	研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書におけるリスク軽減策	国家研究開発革新法におけるリスク軽減策
インフラ面のリスク軽減策	・脅威モデル技術を利用してビジネスリスクを理解・軽減、サイバーセキュリティ戦略へ反映 ・サイバーセキュリティを組織全体の人的問題として扱い、適切な管理フレームワークを組み込んだサイバーセキュリティ戦略を実施　等	・トレーニングやセミナー、ベストプラクティスの共有等によりサイバーセキュリティリスクに対する認識を高める ・外国からの妨害行為者によるサイバーセキュリティ攻撃を検知・防止するための OSINT 調査や認定機器の調達、物理的なアクセス管理	・研究開発課題を実施する施設・設備に関する入退室管理や規程の整備 ・電子的なアクセス制限 ・情報システムの使用記録の保管
人的リスク軽減策	・自組織職員への情報開示の義務付け（テーマ 2 にて記載） ・外国干渉リスクに対する意識を高め、その軽減を支援するコミュニケーション計画と教育プログラムの整備、トレーニングの提供　等	・組織レベル・個人レベルで学問の自由と誠実さへのコミットメントを強化するための教育の実施や意思の表明	・研究開発課題従事者の外国人との接触に関する報告を規定 ・国外受益情報報告制度への対応（テーマ 2 にて記載）
組織的リスク軽減策	・パートナー機関へのデュー・ディリジェンス（テーマ 2 にて記載） ・責任当局の設置 ・ポリシー及び手順の整備 ・リスク評価および報告のためのフレームワークの策定 ・エスカレーションと報告の仕組み	・パートナー機関へのデュー・ディリジェンス（テーマ 2 にて記載） ・行動規範の公表 ・外国干渉委員会の設置 ・リスクマネジメントに係る前提認識の共有 ・パートナーシップの策定手順の確立	・外国機関と共同での研究開発を実施する場合の事前の政府承認を規定 ・国外受益情報報告制度への対応（テーマ 2 にて記載）

5.2　国内外における先端的な重要技術の研究開発動向に関する調査研究

（1）宇宙分野

将来の通信インフラの重要な技術となる可能性や、スペースデブリ等の現状のインフラに対する脅威を防止することが可能となる技術等の経済安全保障上の重要性があり、既存の支援対象技術（特定重要技術）に該当しないこと等を考慮し、技術領域を調査・整理した。

（2）サイバー分野

従来のサイバー攻撃対処において共通の課題となっていた事項を解決することが期待され、また近年研究開発も多く実施されており、サイバー空間の活用が今後更に不可欠になると見込まれる状況等から経済安全保障の観点からもより一層重要性が増していくと判断した技術領域を調査・整理した。

（3）海洋分野

現在 K プログラム等では支援対象となっておらず、無人探査やセンシング等にも関連する経済安全保障の観点からも重要となる技術領域を調査・整理した。

（4）バイオ分野

主に個別化医療、食料安全保障、バイオものづくりに関連した技術の研究開発が多く、ゲノムに関連する研究開発など、近年、日本の中で注目されているような技術領域を調査・整理した。

6. Appendix

6.1 AppendixⅠ：政策動向調査_調査先機関リスト

6.2 AppendixⅡ：技術動向調査_各分野の論文・研究開発プロジェクトリスト