2.4 カナダ

2.4.1 全般的状況

カナダの懸念国、特に中国への警戒感の背景には 2010 年代半ばに発覚した研究機関に対する中国政府が関与したサイバー攻撃事案があるとされる[165]。近年は COVID-19 パンデミックに乗じた研究セキュリティ上のリスクに焦点が当てられている[166]。

カナダの 3 つの主要な連邦研究資金配分機関（FA）は以下のとおり。

- カナダ保健研究機構（Canadian Institutes of Health Research：CIHR）
- カナダ自然科学・工学研究会議（Natural Sciences and Engineering Research Council of Canada：NSERC）
- 社会・人文科学研究会議（Social Sciences and Humanities Research Council of Canada：SSHRC）

上記 3 機関は 2016 年に研究インテグリティに関する共通規範の「Tri-Agency Framework：Responsible Conduct of Research（RCR）」（RCR フレームワーク）を定めている。このフレームワークは FFP（捏造・改ざん・盗用）等の研究不正行為や利益相反行為への注意喚起を行い、発覚時の処理手順及び罰則等を定めている。フレームワークは 2021 年に改定されたが、現状では「研究セキュリティ」や「外国影響」に焦点を当てた規定は盛り込まれていない[167][168]。

カナダ政府の研究セキュリティに関する情報提供サイトに、カナダ公共安全省の「研究セキュリティ情報の更新（Research Security Information Update）[169]」がある。

カナダ政府は研究セキュリティを「外国の脅威者に地政学的、経済的、安全保障上の利益をもたらす一方、カナダに不利益をもたらす可能性のある知識、技術、データを保護するための措置を指す。対象となる資産は、大量破壊兵器計画（化学、生物、放射線、核など）への応用可能な技術から、人工知能、量子コンピュータ、バイオ・ナノテクノロジーなどのデュアルユース技術（民生と軍事の両方に応用できる技術）、研究に用いられる知的財産や機密情報などである（Research security refers to the measures that protect knowledge, technologies, and data that could assist in the advancement of a foreign threat actor's

---

165 CRDS 報告書「オープン化、国際化する研究におけるインテグリティ 2022 ―我が国研究コミュニティにおける取組の充実に向けて―」(2022).p3

166 カナダ政府ウェブサイト" Joint CSE and CSIS Statement – May 14, 2020"<https://www.canada.ca/en/security-intelligence-service/news/2020/05/joint-cse-and-csis-statement.html>

167 カナダ政府ウェブサイト" Tri-Agency Framework: Responsible Conduct of Research (2016)"<https://rcr.ethics.gc.ca/eng/framework-cadre.html>

168 カナダ政府ウェブサイト" Tri-Agency Framework: Responsible Conduct of Research (2021)"https://rcr.ethics.gc.ca/eng/framework-cadre-2021.html

169 カナダ公共安全省ウェブサイト" Research Security Information Update"< https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx >

geopolitical, economic, and security interests to the detriment of Canada's. The target assets can vary from applications in weapons of mass destruction programs (i.e., chemical, biological, radiological, and nuclear) to dual-use technologies (i.e., technologies with both civilian and military applications), such as artificial intelligence, quantum computing, and bio- and nanotechnology, to intellectual property and confidential information used for research)」と定義している。

研究セキュリティの内容を定義し、WMD や量子技術など具体的な分野を挙げる点が特徴的である。

研究セキュリティ上特に考慮が必要な機微分野については、後述のカナダ政府・大学共同ワーキンググループが作成した"National Security Guidelines for Research Partnerships"（国際研究協力に対する国家安全保障ガイドライン）に記述がある[170]。このガイドラインによると外国影響に対し脆弱な研究分野には以下のものが含まれるが、これらに限定されるものではない。

① 航空宇宙
② 人工知能
③ バイオテクノロジー
④ エネルギー生成、貯蔵、送電
⑤ ニューロテクノロジーとヒューマンマシンインテグレーション
⑥ 次世代コンピューティングとデジタルインフラ
⑦ 位置・ナビゲーション・タイミング
⑧ ロボティクスと自律システム
⑨ 重要鉱物及び重要鉱物サプライチェーンに関連する研究（詳しくは、カナダ政府の重要鉱物リストに掲載）
⑩ 重要インフラに焦点を当てた研究パートナーシップ
  - ✓ 重要インフラとは、カナダ人の健康、安全、セキュリティ、又は経済的福利、及び政府の効果的な機能にとって不可欠なプロセス、システム、施設、技術、ネットワーク、資産、サービスを指す。（重要インフラの詳細については、重要インフラに関する国家戦略及び重要インフラに関する行動計画に掲載）。
⑪ 利用することでカナダの国家安全保障に害を及ぼす可能性のある機密個人データへのアクセスの可能性を伴う研究パートナーシップ（以下に限定されない）
  - ✓ 個人を特定できる健康状態又は遺伝子に関するデータ（例：健康状態又は遺伝子検査結果）

[170] カナダ政府ウェブサイト" National Security Guidelines for Research Partnerships"
< https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnership/national-security-guidelines-research-partnerships-risk-assessment-form >

- ✓ バイオメトリクス（例：指紋）
- ✓ 財務（例：支出や負債を含む機密口座情報）
- ✓ 通信（例：私的な通信）
- ✓ ジオロケーション
- ✓ 軍や情報機関のメンバーを含む政府関係者に関する個人データ

2.4.2 カナダ政府の取組み

カナダ政府は研究セキュリティの強化に関する取組について下表に見るような時系列で措置を講じてきた。

表 2-40：カナダ政府の研究セキュリティの強化に関する取組

日付	内容
2021 年 7 月 12 日	カナダ連邦政府は、カナダ政府・大学共同ワーキンググループから協力を得た上で、「国際研究協力に対する国家安全保障ガイドライン（National Security Guidelines for Research Partnerships）」を作成・公表した。
2021 年 3 月 24 日	イノベーション・科学・経済開発相、公安相、保健相は、カナダの研究事業のインテグリティ、国家安全保障、長期的な経済競争力と繁栄を守ると同時に、オープンで協力的な研究環境を支援する声明を発表した。
2021 年 2 月 9 日	カナダ安全保障情報局（CSIS）長官が国際ガバナンス・イノベーションセンターで行った講演で、経済のほぼすべての部門において、カナダ企業が敵対的な外国人行為者の標的とされていることを概説した。また、「今日、我々の敵は、国内の小さな新興企業、企業の役員室、あるいは大学の研究室にあるコンピューターシステム上に保有される知的財産や先端研究に、より焦点を当てている」と指摘した。
2021 年 1 月 15 日	カナダ政府は、カナダの研究コミュニティ及びイノベーション・科学・経済開発相と緊密に連携し、世界をリードするカナダの研究を引き続き保護することを公安相に義務づけた。
2020 年 11 月 16 日	カナダ・サイバーセキュリティ・センターは、「2020 年の国家サイバー脅威評価（National Cyber Threat Assessment for 2020）」を発表した。
2020 年 9 月 17 日	カナダ・サイバーセキュリティ・センターは、「研究開発におけるセキュリティの考慮事項（Security Considerations for Research and Development）」に関する出版物を発表した。研究機関は、研究環境とデータを保護する方法、一般的なサイバーセキュリティの脅威を組織

日付	内容
	がどのように理解すべきか、いくつかの基本的なセキュリティ対策を実施する方法に関する情報を得るために、この出版物を確認することが推奨される。
2020 年 9 月 14 日	カナダ政府は、カナダ政府・大学共同ワーキンググループが開発した「Safeguarding Your Research Portal」を開設し、研究コミュニティが研究と知的財産を保護するためのガイダンス、情報、ツールを提供することを開始した。
2020 年 9 月 14 日	イノベーション・科学・経済開発相、公安相、保健相が、カナダの研究コミュニティの全メンバーに対し、COVID-19 ワクチンと治療薬に関連するすべての研究、技術、開発を保護するために特別な予防措置を講じるよう促す声明を発表。
2020 年 5 月 14 日	カナダ通信保安局（CSE）と CSIS は、カナダの研究コミュニティに対し、パンデミック研究に関連するデータと技術が、国家的支援を受けた行為者にとって魅力的な標的になっていることを警告する共同声明を発表。
2020 年 4 月	COVID-19 ワクチン開発に関連して、CSIS がカナダの大学を含むバイオ製薬セクターへの脅威ブリーフィングを開始。
2019 年	公共安全省が「アカデミックなコミュニティにおけるセキュリティ意識の醸成（Building Security Awareness in the Academic Community）」文書を発表。

出典：カナダ公共安全省ウェブサイトから筆者作成

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx>

2.4.3 カナダにおけるアクター

・省庁

カナダにおける研究セキュリティの取組に関する主要なアクターとして以下がある。なお、カナダでは教育は地方分権であり、中央政府は「カナダ政府・大学ワーキンググループ」に協力を要請し、参考となるガイドラインを作成するにとどまる[171]。

[171] カナダの教育は完全な地方自治で中央政府に教育省はなく、高等教育を含め州政府の教育省によって管轄されている。またほとんどの大学は州立である。カナダの 3 つの準州（ユーコン準州、ノースウエスト準州、ヌナブト準州）は、州ほどの憲法上の地位がなく、多くの分野で連邦政府による直接的な統制を受けている。しかし、教育に関しては、連邦政府はその責任を準州政府に委任しており、準州政府は州と協力して中等教育プログラムを提供している。（CICIC ウェブサイト" Ministries/departments responsible for education in Canada"<https://www.cicic.ca/1301/ministries_departments_responsible_for_education_in_canada.canada>）

連邦政府の 3 つの資金配分機関（CIHR、NSERC、SSHRC）に対しては、所管するイノベーション・科学・経済開発省、保健省に加え公共安全省が研究セキュリティの取組を支援する。ただし輸出管理関連法規の「規制品目プログラム（Controlled Goods Program）[172]」や医療倫理規制法令[173]などを除き、研究セキュリティ・研究インテグリティに関する包括的な法規制は存在しない。

外国影響やスパイからの研究コミュニティの保護は、公共安全省の一義的な責務である。サイバーセキュリティ分野では、カナダ安全保障情報局（Canadian Security Intelligence Service（CSIS）：公共安全省傘下）及びカナダ・サイバー・セキュリティ・センター（Canadian Centre for Cyber Security (CCCS)：カナダ通信保安局傘下）が取り締まりを所管する。

【機微な研究分野に関する法規制】

研究分野の中には、軍事力の向上と明らかに関連するものがあり（例えば、核、化学、生物、放射線、宇宙利用など）、カナダでは、これらの分野に関して研究の実施や得られた知識の輸出の際に従わなければならない以下の法令が存在する[174]。

- 通常兵器やデュアルユース品に関連する分野の研究は、輸出入許可法（Export and Import Permits Act：EIPA[175]）の対象となる可能性があり、カナダ国外の研究者への技術移転の前に許可が必要となる場合がある。
- ミサイル・ロケット技術、宇宙技術、化学・生物兵器・薬剤に関する研究も、EIPA の規制対象となる可能性がある。
- 原子力プログラムに関わる、又は原子力プログラムに適用される分野の研究については、EIPA 及び核不拡散輸出入管理規則（Nuclear Non-proliferation Import and Export Control Regulations[176]）の対象となる。
- 防衛生産法（Defence Production Act[177]）の別表（規制品目リスト）に記載されている商品・技術に関連する分野の研究は特に注意が必要であり、上記の規制品目プログラムの対象となる。
- 地域管理リスト（Area Control List[178]）（EIPA に基づく規制）に掲載されている国の研究機関との共同研究は、研究内容にかかわらず、カナダ総務省（GAC）の事前承認

[172] Defence Production Act の既製品目リスト掲載の物品・技術に関する規制
[173] Food and Drug Regulations (FDR) under the Food and Drugs Act (Canada)など
[174] カナダ政府ウェブサイト" Annex A- Sensitive research areas"< https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships >
[175] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/acts/e-19/>
[176] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/regulations/sor-2000-210/index.html>
[177] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/acts/D-1/index.html>
[178] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/Regulations/SOR-81-543/index.html>

が必要となる。

- また、特別経済対策法（Special Economic Measures Act[179]）や国連法（UN Act[180]）に基づく制裁を受けた企業との共同研究についても、GAC の事前承認が必要となる場合がある。

ただし、潜在的な軍事、安全保障、諜報の用途が明確でなく周知されていない、あるいは国際的な武器・輸出規制体制がまだ合意に至っていないため、上記の規制が適用されないデュアルユース技術・新興技術についての扱いが問題であり続けている。

・カナダ政府・大学ワーキンググループ

カナダ政府・大学ワーキンググループは、研究を保護し、カナダ国民に最大限の利益をもたらす方法で、オープンで共同研究を推進するために設立された。グループは定期的に会合を開き、Safeguarding Your Research ポータル[181]はこのグループの研究セキュリティの強化に関する取組の結果を広めるための重要なチャネルとなっている。

ワーキンググループには、カナダ政府、資金配分機関・連邦研究機関、大学関係者、大学団体から、次のようなメンバーが参加している。

- カナダ国際関係省（外務省）（Global Affairs Canada）
- カナダイノベーション・科学・経済開発省（Innovation, Science and Economic Development Canada）
- カナダ公共安全省（Public Safety Canada: PS）
- カナダ安全保障情報局（Canadian Security Intelligence Service: CSIS）
- カナダ・サイバーセキュリティ・センター（Canadian Centre for Cyber Security: CCCS）
- カナダ・イノベーション財団（Canada Foundation for Innovation: CFI）
- カナダ国家研究評議会（National Research Council Canada）
- カナダ保健研究機関（Canadian Institutes of Health Research: CIHR）
- 自然科学・工学研究会議（Natural Sciences and Engineering Research Council: NSERC）
- 社会・人文科学研究会議（Social Sciences and Humanities Research Council: SSHRC）
- カナダ研究大学 U15 グループ（U15 Group of Canadian Research Universities）
- カナダ大学連盟（Universities Canada）

179 カナダ政府ウェブサイト“Justice Laws Website” <https://laws-lois.justice.gc.ca/eng/acts/s-14.5/index.html>

180 カナダ政府ウェブサイト“Justice Laws Website” <https://laws-lois.justice.gc.ca/eng/acts/u-2/index.html>

181 カナダ政府ウェブサイト” About the Government of Canada – Universities Working Group” <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/about-government-canada-universities-working-group>

➢ 各大学研究担当副学長

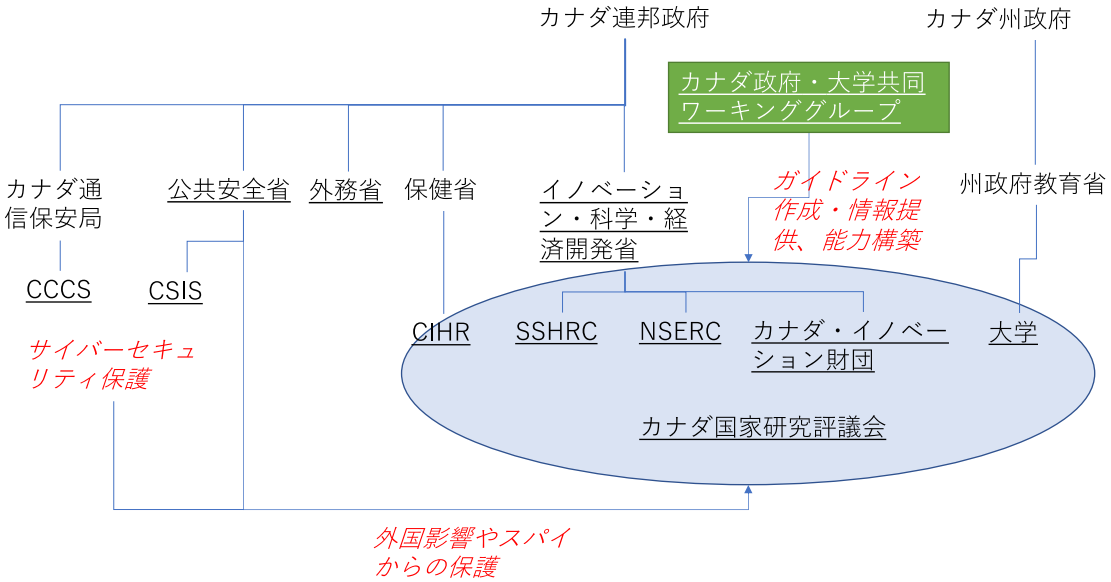

図 2-8：カナダにおける研究セキュリティに関する主要なアクター

2.4.4 規制側・被規制側の主要アクターの研究セキュリティに関する認識

・公共安全省による認識

カナダ公共安全省の年次報告書[182]によれば、同省は外国政府による敵対的な影響力の行使全般を注視している。同省は研究安全保障を脅かす外国による干渉活動を国家主体による敵対的活動（hostile activities by state actors：HASA）として捉え、経済安全保障及び国家安全保障に強く関連するテーマとして研究セキュリティ上の問題を認識し対応しようとしていることがうかがわれる。以下では同報告書中の関連する項目を引用する。

【国家主体による敵対的活動】

国家主体による敵対的活動（HASA）には、外国の国家又はその代理人がカナダの国益と価値を損なおうとするあらゆる行為が含まれる。敵対的活動は、多くの場合、あからさまな直接的軍事攻撃には至らないものの、欺瞞的、脅迫的、腐敗的、隠密的、又は違法な性質を持つ行動を伴う。HASA の脅威は、COVID-19 によって形成されたグローバル環境の結果として悪化し、外国の脅威行為者に彼らの目的を推進する機会を与えている。HASA は冷戦以来見られなかったレベルに達し、現在、カナダの国家安全保障にとって最大の戦略的脅

182 カナダ公共安全省” Departmental Results Report 2021-22”
<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-rslts-rprt-2021-22/index-en.aspx#s311>

威の一つとなっている。それは、カナダの政治システムのインテグリティ、民主的制度、社会的結束、学問の自由、経済、長期的繁栄を標的にしているからである[183]。

【国家安全保障に対する経済ベースの脅威】

カナダ人は、重要な新興技術分野の最先端に身を置き、それが経済成長と発展の重要な原動力となっている。これはカナダに新たな機会をもたらす一方で、国家安全保障上の新たな、そして潜在的に深刻な脆弱性をも生じさせた。特定の敵対勢力は、カナダ経済の重要な分野を利用して、自国の戦略的な軍事、情報、安全保障、経済的利益を高めようとしている。このような活動には、以下がある。

- カナダの国家安全保障にとって重要な部門や産業への外国投資
- カナダの国家安全保障にとって重要な商品、技術、ノウハウの輸出
- 機密性の高い技術や知的財産（IP）の開発のために、学術研究機関と、敵対的な外国人によって支配された、あるいはそれに関係する団体との間で結ばれるパートナーシップ

【研究セキュリティ】

カナダの国家安全保障コミュニティは、国家安全保障や経済的意義を持つ最先端の研究、企業秘密、知的財産のスパイ行為や盗難がもたらす脅威に取り組み続けている。公共安全省は、カナダの研究機関のセキュリティ態勢を強化するための多くのイニシアティブに関与した。2016 年以降、公共安全省はワークショップ、ツール、リソースを提供する Safeguarding Science イニシアティブを通じて、第一線の研究者や学術コミュニティと直接関わることで、研究セキュリティ上の脅威に対する意識を高めてきた。2021-22 年、Safeguarding Science チームは、関係者向けのオンラインワークショップの数を 33%増やし、カナダ全土で合計 1487 人が参加した。

・資金配分機関の認識

理工系の公的研究・資金配分機関であり、研究セキュリティ上のリスクにさらされやすい NSERC の研究セキュリティに関する現状認識は以下のとおりである（戦略文書"NSER 2030"[184]より）。

- 科学と工学のスピードと複雑さが増すにつれ、カナダの世界レベルの研究は、盗難、スパイ行為、知的財産の不正移転の標的になっている。NSERC は政策立案者や研究者とともに、世界の力学が変化する中で研究セキュリティを実践し、研究の中核

[183] Public Safety Canada. Public Safety Canada 2021 Transition Book - Issues Book: National Security.
<https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20220223-2/006/index-en.aspx>
[184] NSERC ウェブサイト "NSERC 2030: Discovery. Innovation. Inclusion."
< https://www.nserc-crsng.gc.ca/NSERC-CRSNG/NSERC2030-CRSNG2030/report-rapport/index_eng.asp >

的価値であるインテグリティ、公平さ、信頼、説明責任、学問の自由を堅持しながら、研究のエコシステムを可能な限りオープンで必要な限り安全なものにするよう努めている。
- NSERC は、私たちの価値観に合致し、カナダの研究エコシステムに大きな付加価値をもたらす世界中の研究助成機関とパートナーシップを構築する。
- NSERC は、カナダの最も有望な研究者や研究機関が、国際的な同業者との強力なパートナーシップを構築することを支援する。
- NSERC は、カナダ研究調整委員会（Canada Research Coordinating Committee：CRCC）のリーダーシップのもと、他の機関や組織とともに、国際協力への「チーム・カナダ（３機関・CFI・連邦科学機関）」アプローチにおける熱意あるパートナーとなる。
- NSERC は、連邦政府のパートナー、学術機関、研究組織、個々の研究者とともに、カナダの知識、データ、知的財産を外国の脅威から守り、カナダの経済的繁栄、国家安全保障、研究事業の健全性を確保する。

NSERC が 2015 年に発表した前回の戦略プランの”NSERC 2020”では、グローバル化の方向性が強調されており(Go Global)、研究セキュリティに関する記述は見られず、むしろ国際共同研究の推進や留学生の受け入れ拡大が研究活動に関する国際社会でのカナダのプレゼンスを高めるために必須との認識が示されていた[185]。研究セキュリティや国家安全保障を強調する現在の戦略はこうした立場からの方向転換であると評価できる。

・カナダ政府・大学ワーキンググループの認識

同ワーキンググループのウェブサイト[186]によると、以下のように研究の国際化・オープン化のもたらす恩恵を強調しつつも、研究セキュリティ上のリスクの高まりを懸念している様子がうかがえる。
- 強い経済を築き、すべてのカナダ人の生活を向上させるためには、オープンで協力的な研究環境が必要である。カナダはオープンで協力的な研究と科学に取り組んでいる。教員、学生、知識の交流は、カナダが革新的な知識集約型社会・経済となるために必要な連携と能力の構築に寄与する。
- ただし、カナダ政府と大学は、カナダ国民が研究への多大な投資から引き続き利益を得られるようにすることは、共通の責任であると認識している。このため、大学、政府省庁、連邦助成審議会、国家安全保障機関は、継続的な関与活動の一環として定期的に連絡を取り合い、研究の安全性を確保するために協力している。

185 NSERC ウェブサイト “NSERC 2020”< https://www.nserc-crsng.gc.ca/nserc-crsng/nserc2020-crsng2020/index_eng.asp>
186 同上

2.4.5 リスクアセスメント

「国際研究協力に対する国家安全保障ガイドライン」で説明されているように、研究パートナーシップがカナダの国家安全保障にもたらす可能性のあるリスクを評価するために、連邦研究補助金申請に際しリスクアセスメント調査票を使用する義務がある[187]。以下ではNSERC におけるリスクアセスメントの流れを参考に具体的な運用を見ていきたい。

【基本的な判断枠組み】

研究者は、研究パートナーシップの申請書を NSERC のアライアンス助成金プログラムに提出する際に、リスクアセスメントを完了しなければならない。

NSERC が高リスクと判断したパートナーシップ助成金申請については、必要に応じて国家安全保障関連省庁・機関や研究者コミュニティのメンバーが関与し、国家安全保障審査を受けることになる。

国家安全保障上のリスクが高いと評価されたプロポーザルには、資金が提供されない。

【プロセスの概要】

1.研究者

- 研究者は、リスク質問票を記入し、特定されたリスクの根拠を説明する。研究者は、機関とともにリスク軽減計画の作成に貢献する。

2.研究機関

- 機関は、リスク質問票のレビューと検証を行う。
- 研究機関は、特定されたリスクに効果的に対処するために、研究者がリスク軽減計画を策定することを支援する。
- リスク調査票とリスク軽減計画（該当する場合）は、該当する助成金申請書に添付して提出する。

3.助成機関[188]

- 助成機関は、助成の評価基準に記載され、確立されたピアレビュープロセスに従って、受領したすべての研究パートナーシップ提案の科学的メリットの評価を実施する。
- 助成機関は、助成金申請書に添付されたリスク質問表とリスク軽減計画（該当する場合）を検討し、国家安全保障を考慮した評価が必要な申請については、関連する

187 カナダ政府ウェブサイト” The National Security Guidelines for Research Partnerships’ Risk Assessment Form” <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnership/national-security-guidelines-research-partnerships-risk-assessment-form>

188 Science.gc.ca website. “Risk Assessment Review Process” <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process >

申請書類はカナダ公共安全省に照会される。この照会は、通常、科学的メリット評価が成功したと判断された後、助成機関によって資金調達の決定が下される前に行われる。

- 助成機関から照会された申請書を受け取ると、カナダ公共安全省は最初の審査を行い、提案された研究プロジェクトの国家安全保障評価をどの安全保障機関が主導するのかを決定する（カナダ公共安全省、カナダ安全保障情報局、又はカナダ通信保安局）。主導する機関は、それぞれの権限と任務の下、評価を実施し、カナダ公共安全省に結果を知らせる。カナダ公共安全省は、評価結果及びアドバイスを助成機関に返却する。
- 助成機関は、科学的メリット評価の結果とともに、国家安全保障評価とカナダ公共安全省から受けた助言を考慮し、各申請に対する資金提供を最終決定する。

2.4.6 地域ごとの懸念への対処

カナダは広大な国土を有し、産業構造や天然資源の分布にも地域ごとに特徴がある。このような特性に鑑み、カナダで科学研究を行う際に直面する可能性のある外国干渉を含む特定のリスクについて詳しく知りたい場合、以下のように、カナダ安全保障情報局（CSIS）が作成した「Protect Your Research（研究を保護する）」から地域別（ブリティッシュコロンビア、アルバータ、サスカチュワン、マニトバ、オンタリオ、ケベック、ニューファンドランド・ラブラドール、プリンスエドワード島、ニューブランズウィック、ノバスコシア、ユーコン、ノースウェストテリトリーズ、ヌナブトの各州・準州）ファクトシートの概要を参照することができる[189]。

例えばブリティッシュコロンビア州では以下のような外国脅威（狙われやすい分野、具体的な標的、想定される手法）が挙げられている。

表 2-41：ブリティッシュコロンビア州における外国脅威の例

分野	• テクノロジー • バイオ医薬品 • 健康 • 輸送（航空宇宙、鉄道、環境対応車、海事機器、サプライチェーン） • アカデミア • エネルギー • マニュファクチャリング

[189] カナダ政府ウェブサイト”Protect your research”<https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/who-are-you-risk/protect-your-research-regional-factsheets >

標的	• STEM 分野の先端研究・機器 • 知的財産権 • 重要インフラ資産 • 個人を特定できる情報（例：財務情報、健康情報など） • 政府情報 • 通信機能 より具体的な例としては、設計図、試験結果、製造又はマーケティング計画、独自の規格方式又はプロセス、従業員情報、ベンダー及び供給者情報、ソフトウェア、投資データ、企業戦略、アクセスプロトコル、及び特許などが挙げられる。
手法	• サイバー・エスピオネージ（スパイ） • ヒューマン・エスピオネージ • 技術・ノウハウの盗用と不正移転 • カナダの機密データの取得と活用 • 重要インフラへの外国からのアクセスとコントロール • インサイダー脅威 • 敵対的な海外投資 • リバースエンジニアリング • 破壊工作 • 搾取的ライセンス契約 • エリシテーション[190]

2.4.7 大学での取組み

(1) マギル大学[191]

マギル大学（McGill University）では、学術研究及び国際協力において、長年にわたりオープンな姿勢を貫いてきた。しかし、現在は研究セキュリティを確保し、外国からの干渉に対する保護を実施することは同様に重要な大学の責任であると認識されている[192]。留学生や客員教員、民間企業の協力者、外国政府の代表者、非営利団体、活動家、営利目的の競争相手など、自分たちの目的や利益のためにマギル大学の研究や研究者にアクセスしよう

190 お世辞を言ったり、関心を示したり、誘導尋問をしたり、相互の利害を主張したり、無知を装ったりして、情報を引き出そうとすること。これらのテクニックは、業務とプライベートの両方の場面で使われることがある。

191 マギル大学ウェブサイト”Foreign Interference” <https://www.mcgill.ca/research/about/foreign-interference >

192 マギル大学では「外国からの干渉（Foreign Interference）」について「外国政府やその他の団体による、不当な影響力を行使しようとする、あるいは学術の中核的価値を侵害するような行為や活動を指す。このような干渉には、サイバーセキュリティ攻撃や、知的財産やアイデア財産に関連する情報収集活動が含まれる場合がある」と定義している。

とする人々が現れる可能性があり、コントラクター、職員、学生も含め、研究チームや研究機関の内部にいる人々は、研究やイノベーションに不適切にアクセスしたり、盗んだりするように、他者から支援や圧力を受ける可能性がある。

こうした問題意識から、マギル大学では 2020 年に外国干渉ワーキンググループ（McGill Foreign Interference Working Group）を設立し、同グループが大学全体の取組を指導している。同グループは研究イノベーション担当の副学長クラスなど 12 名のメンバーで構成されている。同グループの目的は、マギル大学の研究者が自らの研究、知的財産、知識開発を保護するために必要な教育・支援と、外国からの干渉に対する保護を実践することである。外国からの干渉を監視するため同グループは定期的に開催され、国家安全保障局との活発な連携が行われている。マギル大学は、さらなる調査が必要と思われる研究セキュリティ上の懸案事項が生じた場合、同グループに意見を求める。

マギル大学が整備する具体的な規定類としては、

- MOU の提案、キャンパス訪問、国際交流事業に関するガイドライン
- サイバーセキュリティに関するガイドライン
- 利益相反報告に関する規制
- 研究データ管理規定
- 研究提携、データ保護、海外からの訪問者に関するガイドライン（現在作成中）

がある。

カナダ公共安全省は、2021 年 5 月にマギル大学の科学者・学術者向けに開催される「Safeguarding Science Against Foreign Interference Workshop」を開催し外国干渉ワーキンググループもこれに協力した。ワークショップでは、円卓会議方式の質疑応答が行われ、兵器拡散リスク（化学、生物、放射線、核拡散、デュアルユース技術拡散のリスク）、サイバーセキュリティ、知的財産の盗難、その他のセキュリティに配慮した研究組織を維持するためのベストプラクティスに関する情報が提供された。また、カナダの機関、研究者、学術関係者が直面している特定のリスクを認識し緩和するのに役立つツールも提供された。

外国干渉ワーキンググループが推奨する、マギル大学関係者が参照すべき政府等のガイドラインや資料として以下が挙げられている。

- The Research Security Information Update (en anglais) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx>
- Le point sur la sécurité de la recherche (en français) <https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-fr.aspx>
- Mitigating economic and/or geopolitical risks in sensitive research projects (U15/Universities Canada) <https://science.gc.ca/site/science/en>

- Travel security guide for university researchers and staff (U15/Universities Canada) <https://science.gc.ca/site/science/en>
- Safeguarding Your Research, Government of Canada Portal <https://science.gc.ca/site/science/en/safeguarding-your-research>
- Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus (Association of American Universities/Association of Public and Land-grant Universities) <https://www.aau.edu/sites/default/files/Blind-Links/Effective-Science-Security-Practices.pdf>
- Guidelines to counter foreign interference in the Australian university sector released (Australian Government) <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector>
- Canadian Security Intelligence Service (CSIS) Public Report 2020 <https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report.html>
- Foreign Interference and You (CSIS) <https://www.mcgill.ca/research/files/research/aose_foreigninterferencehandout_-_digital.pdf>
- L'ingérence étrangère et vous (SCRS) <https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210722/015/index-fr.aspx
- Guidelines on the National Security Review of Investments <https://ised-isde.canada.ca/site/investment-canada-act/en/guidelines/guidelines-national-security-review-investments>

(2) トロント大学[193]

トロント大学（University of Toronto）では 2021 年 8 月 30 日より、国際的なパートナーシップに携わる教員は、「研究パートナーシップ・セキュリティ情報文書（Research Partnership Security Information Document）」に必要事項を記入するよう求められている。これは、カナダ政府による研究セキュリティの重視政策に沿ったもので、カナダ政府・大学ワーキンググループによる提言に対応したものある。

トロント大学が外国干渉に関連して特に整備したガイドラインや規定としては以下がある。

193 トロント大学ウェブサイト"Safeguarding Your Research"< https://global.utoronto.ca/safeguarding-your-research/>

① 「国際的な研究パートナーシップの構築：原則とアプローチ（Engaging in International Research Partnerships: Principles and Approaches）[194]」：トロント大学では、教員や部局が国際的なパートナーシップを締結する際に考慮すべき一連の原則を策定した。教員が国際的なパートナーシップに関与する前にこれらを確認し、生産的で安全なパートナーシップを締結することが期待される、としている。

② 「国際的パートナーシップのための研究パートナーシップ・セキュリティ情報文書（Research Partnership Security Information Document for International Partnerships）[195]」：特定のプロジェクトを進める前に、PI（研究責任者）が「国際パートナー」と関わることの適切性と潜在的リスクを評価するためのツールである。国際パートナーとは、トロント大学と研究協力（大学院での研修や起業の機会も含む）を行っている、カナダ国外にある団体（学術団体、企業、政府、非営利団体など）と定義されている。法人の場合、カナダ国内に子会社やオフィスがあっても、本社がカナダ国外にある場合は、この書類に記入する必要がある。PI は大学の承認を得るために研究計画書・契約書を提出した後 2 週間以内に、本書類を提出する必要があり、提供された情報は一元的に審査され、2 週間以内に審査完了となる。必要に応じて、副学長室（国際担当）、副学長室（研究・イノベーション担当）、又は所属部門の担当者が、提案されたパートナーシップについて申請者と協議を行う。

194 トロント大学ウェブサイト” ENGAGING IN INTERNATIONAL RESEARCH PARTNERSHIPS: PRINCIPLES AND APPROACHES”<https://global.utoronto.ca/wp-content/uploads/2015/08/Engaging-in-International-Partnerships.pdf>

195 トロント大学ウェブサイト“Research Partnership Security Information Document for International Partnerships”<https://redcap.utoronto.ca/surveys/?s=PMF483RY8NMNNDJL >

2.5 欧州連合（EU）

2.5.1 研究インテグリティの確保に関する要求と支援

(1) 「研究・イノベーションにおける外国からの干渉に対応するためのスタッフ作業文書」（2022 年 1 月）

2022 年 1 月に、欧州委員会は「研究・イノベーションにおける外国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) を発表した[196]。本文書は、「スタッフ作業文書」というタイトルであることからも分かるように、欧州連合加盟国や、大学・研究機関に対して法的拘束力を持つものではないが、海外からの干渉を防止し、対処するために、大学・研究機関がどのような行動を取ることができるかを具体的に記述しており、チェックリストとして利用することも可能である。

前文では、文書の目的等について以下のように説明している。

- 「本書は可能な限り具体的であることを目指すが、(海外からの干渉に対処するための) 万能のアプローチは存在せず、各組織が独自の対策を講じる必要がある。この文書は、包括的な戦略を策定するためのツールキットとして作成されたもので、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 つのカテゴリーに分類された主要な注目分野をカバーする。」
- 「本スタッフ用作業文書は、HEI（高等教育機関）及び RPO（研究実施機関）が、学問の自由、インテグリティ、機関の自治（academic freedom, integrity and institutional autonomy）などの基本的価値を守り、職員、学生、研究成果・資産を保護する努力を支援するために、海外からの干渉（foreign interference）を軽減するための実務に関する情報を提供することを目的として作成された。したがって、本規定は国際的な共同研究を制限するものではなく、むしろ可能な限り開放的で、必要な限り閉鎖的な国際的共同研究を促進することを意図している（promote international collaboration that is as open as possible and as closed as necessary）。さらに、HEI や RPO に新たな事務処理の負担を強いるものではなく、可能な限り既存の仕組みの中に可能な措置を組み込むことを推奨する。」
- 「このスタッフ作業文書は、加盟国及び利害関係者と共同で作成され、ベストプラクティスの目録及び証拠の収集として意図されており、網羅的でも拘束力があるわけでもない。つまり、多くの問題について詳細な情報を提供しているが、この文書に含まれていない要素もあるかもしれない。さらに、インスピレーションの源として利用されるべきものである。加盟国や組織は、同じテーマについて他の手段を採用することを検討してもよい。抵抗

196 European Commission. Directorate-General for Research and Innovation. *Tackling R&I Foreign Interference. Staff Working Document* (2022/1)

力の構築と海外からの干渉の事案への対応は、適切な場合には、地域及び国の当局と協議し、その支援を受けて行われるべきものである。」

ここで「海外からの干渉（foreign interference）」については、「外国の国家レベルの行為者によって、あるいは外国の国家レベルの行為者のために行われる活動で、強制的、隠密的、欺瞞的、又は腐敗させるものであり、欧州連合（EU）の主権、価値、利益に反するものである」[197]と冒頭の用語説明で定義している。

このような海外からの干渉の目的は、「海外の行為者の政治的、社会的、文化的、経済的、技術的利益を促進すること」であり、以下を含む。

- 海外の行為者の利益となる情報を不法に取得すること。
- 海外の行為者に有利となるように意思決定に影響を与えること
- 海外の行為者に反すると認識される価値観を弱体化する。」

また、海外の行為者は、目的を実現するために、以下のような海外からの干渉の戦術を展開可能であると説明している。

- 戦略的意思決定者に対する影響力のある代表者による政治的圧力
- 投資、寄付、資金提供、融資といった形での財政支援
- 戦略的地位にある人物を脅し、勧誘し、又は配置する
- 遠隔地又は現地でサイバーセキュリティを侵害するデジタル侵入
- 現地の利益に反する、又は海外の利益を促進する偽情報の流布

また、上述のように、海外からの干渉に対処すべきであるが、そのような対応は「国際的な共同研究を制限するものではなく、むしろ可能な限り開放的で、必要な限り閉鎖的な国際的共同研究を促進することを意図」していることが強調されている（”*as open as possible and as closed as necessary*”）。「オープンサイエンス」（Open Science）が欧州では推進されており、それと「海外からの干渉」の防止とを、バランスを取って達成することが意図されているとみられる。第 1 章では、以下のように説明している。

- オープンサイエンスの実現は欧州委員会の政策的優先事項である。オープンサイエンスは、必ずしもオープンかクローズかという二項対立的なものではなく、むしろ研究の性質に応じて研究成果のさまざまな種類や側面をオープンにしたりしなかったりする、オープンさのスペクトラム（spectrum of openness）であることに注意することが重要である。このことは、「可能な限りオープンに、必要な限りクローズに」（as open as possible and closed as necessary）というモットーに反映されている。研究成果は、プライバシー、安全保障、政治、軍事、商業上の理由から、正当な理由によって公開されないことがある。

197 “activities that are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU).”

また、海外からの干渉に対応するためには、「多次元的なアプローチ」を取るべきであると説明している。

- 高等教育機関と研究機関は、外国の研究者や組織との共同研究に対して恐怖心を抱くような文化ではなく、海外からの干渉に対抗するための自覚と連帯責任を持つ文化を醸成することが重要である。対応は共同研究のリスク、範囲、性格に比例させ、デューディリジェンスや複数の情報源から情報を得るべきである。本スタッフ作業文書に示された対策は、高等教育機関と研究機関における海外からの干渉に対する戦略的方針を策定するための初期導入として役立つものである。高等教育機関と研究機関は、これらの可能な対策を基に、それぞれのニーズや環境に応じて独自の内部対策を講じることが期待される。

既に述べたように、「海外からの干渉」（foreign interference）への対応策について、本報告書では、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 つの類型に分けて、リストアップし、説明している。以下の表はこれらをまとめたものである。

表 2-42：「海外からの干渉」への対応策

価値観

1. 学問の自由が危険にさらされている国やパートナー機関を特定する。
・ 最初の方向付けとして、「世界の学問の自由度指数」（AFi）を参考にする。
・ 次に、その国や特定のパートナー機関の研究・教育・制度環境について、より詳細に評価する。
・ その後、学問の自由を損なう外部要因の動機を分析し、欧州の研究者や機関を制限したり道具化したりする外部要因の能力を監視する。
2. あなたの教育機関における学問の自由とインテグリティに対する外部からの圧力を理解するために、脆弱性評価（vulnerability assessment）を実施する。
・ 機関及び/又はプロジェクト固有の脆弱性評価を実施する。
・ 外部のアクターとの既存の協力関係によって、何らかの依存関係が生じていないかどうかを確認する。
・ すべてのパートナーシップ協定が学問の自由を適切に保護していることを確認する。
・ 研究者に授与される名誉学位だけでなく、外部からの任命を監視する。
・ 学問の自由や普遍的な価値が危険にさらされている機関と交流するすべての人にトレーニングを提供する。
・ 学問の自由に対する脅威を機関内でマッピングするための報告メカニズムを構築する。
3. 機関及び個人レベルで学問の自由とインテグリティへのコミットメントを強化する。
・ 特定の脆弱性が特定されたら、それに対処する。
・ 学問の自由と普遍的価値が危険にさらされている機関と関わるすべての人にトレーニングを提供する。
・ 学問の自由とインテグリティを、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。

・　学問の自由とインテグリティの重要性を、頻繁に、そして公に表明する。
・　学問の基本的価値の重要性と保護について、学生、教員、事務職員の意識を向上させる。
・　外部のアクターが抑圧しようとする研究テーマに取り組む学者を支援する。
・　学問の自由が脅かされている国からの客員学者や新入生に対する専用の支援プログラムを立ち上げる。
・　迫害されている学者や学生を保護するために、（一時的な）聖域を提供することを支援する。
・　民主主義の誓約書への署名を検討する。
4. 抑圧的な環境下にあるパートナーとの協力を継続する。
・　非自由主義的な制度環境にいる学生、学友、機関に汚名を着せたり、疎外したりしないようにする。
・　抑圧的な環境が学問の自由にどのような影響を与えうるかについて、認識と理解を深める。
・　抑圧的な環境での危険な研究が、関連する委員会によって自動的に拒否される（それによって抑圧される）ことがないように、標準的な倫理手順を見直す。
・　抑圧的な環境における監視リスクの管理を支援するため、データとデジタルセキュリティに関するガイダンスと個別の技術支援を提供する。
・　ハラスメント、拘留、失踪のケースに対処するための緊急手順を設定する。
・　抑圧的な環境との協力に対処するために調整された、透明性と審査メカニズムにコミットする。

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。
・　以下の保護を確保する。 ➢　学問の自由 ➢　データの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、インテグリティ、信頼。
・　以下の手順を含む。 ➢　海外からの干渉の特定（データ漏洩や倫理的に問題のある研究を含む）。 ➢　内部告発者の保護。 ➢　内部利益相反への対処。
2. 海外からの干渉委員会（Foreign Interference Committee）を設置する。
・　委員会は既存の組織構造と統合され、以下を担当する。 ➢　教育・訓練による意識改革 ➢　潜在的なリスクの監視 ➢　国際協力における研究データ及び知的資産の管理。関係する研究グループへのアドバイスや支援の提供。 ➢　リスク管理及びリスク軽減 ➢　海外からの干渉の調査

パートナーシップ

1. リスクマネジメントシステムを導入するための一般的な前提条件を整備する。
・ 海外からの干渉調査委員会（Foreign Interference Investigative Committee）は、手順を見直し、必要な場合はそれを拡大・強化することで、すべてのパートナーシップにおいて知識のセキュリティと学問のインテグリティが保護されるようにすべきである。
・ 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の方法について、幅広い認識を高める。
・ リスク管理戦略への支持を高める。
・ 輸出管理法及び外国直接投資（FDI）審査に関する認識と知識を高める。
・ 機関の「クラウンジュエル」（※王冠を飾る宝石のような価値あるもの）を特定し保護し、第三国からの潜在的な技術的、安全保障的、経済的利益を理解する。
・ パートナーシップに関する計画を「海外からの干渉委員会」に報告するための基準を定め、報告のフォローアップに責任を持つ者を決定する。
・ 様々なタイプのパートナーシップに対するデューディリジェンスの最低レベルを定義する。
・ 海外からの干渉委員会は、リスク管理小委員会又は作業部会を設置することができる。
2. 強固なパートナーシップ合意を策定するための健全な手順を確立する。
・ ポジティブなアジェンダの開発：国際協力のための安全又は低リスクの領域を特定する。
・ パートナーシップの準備：国際化の一環として、戦略的なビジョンに基づくことを確認する。
・ パートナー組織について、またその国の研究システムにおける位置づけについて、正しい知識を身につける。
・ デューディリジェンスの実施：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。
・ パートナーシップ協定を慎重に交渉する：金銭的な約束、知的財産権、データ管理、オープンサイエンスなど、責任の透明性を確保する。
・ 合意の履行の監視：海外からの干渉の可能性に関する問題に焦点を当てる。
・ 協力の成果を評価し、将来の関与のための教訓を得る。

サイバーセキュリティ

1. サイバーセキュリティリスクの認知度向上
・ 機密コンピューティング（confidential computing）を含む、利用可能で実装されてい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。
・ 研究者、学生、事務・支援スタッフに対し、サイバー衛生（cyber hygiene）に関する教育・訓練を行い、リスクを特定し、サイバー攻撃を回避・対処する方法を知ってもらう。
・ 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・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連絡窓口を周知する。
・ サイバーセキュリティリスクのトップ 10 リストの維持と伝達を行う。
・ サイバーセキュリティインシデントを説明するベストプラクティスを掲載したニュースレターを定期的に発行する。

2. 海外からの干渉行為者によるサイバーセキュリティ攻撃を検知し、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、異常な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・支援スタッフの審査手順を策定する。
・ サイバーセキュリティ認証を受けた機器を調達し、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（confidentiality protection solutions）の開発に投資する。
・ 必要なレベルに応じた物理的なアクセス制御を実施する。
・ オフィス/企業活動クラスターにおいて、オペレーティングシステムとインストールされたアプリケーションの集中管理アプローチを開発し、ローカル管理権（LAR）を無効化及び削除する。
・ 重要なサービスやリポジトリにアクセスするための二要素認証（2FA）を有効にし、既知の悪意あるウェブサイトや侵害するウェブサイトへのアクセスを禁止するブロックリストを維持・実施する。
3. 海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う。
・ 教訓を共有し、共有ブラックリスト、評価システム、データベースを更新することにより、状況認識能力を向上させる。
・ 影響を受ける当事者と対応に必要な人物の双方が参加する明確なプロセスを含む、インシデント処理のための計画を策定する。SIM3 セキュリティインシデント管理成熟度モデル（SIM3 Security Incident Management Maturity Model）などのインシデント処理モデルから慣行や要素を採用する。
・ フォレンジック準備機能を導入し、対応にかかる時間を短縮する。
・ 違反したスタッフの懲戒処分を行い、その際、デジタル調査の証拠も含める。
・ インシデントに対して、関連する法執行機関、国家情報・セキュリティ機関、知的財産局、データ保護当局を関与させる。

出典：European Commission. Directorate-General for Research and Innovation. *Tackling R&I Foreign Interference*. Staff Working Document (2022/1).

(2) Horizon Europe Program Guide Version 2（2022 年 4 月 11 日）

欧州連合の研究資金プログラム（2021～2027 年）である Horizon Europe のプログラムガイドは 2021 年 6 月 17 日に初版 Version 1.0 が公表され、その後、Version 1 は Version 1.1、1.2、1.3、1.4、1.5 とマイナー修正が加えられた。2022 年 4 月 11 日に公表された Version 2 では、上述の「研究・イノベーションにおける海外からの干渉（R&I Foreign Interference）」に関する段落が、文書の第 8 章「8. International cooperation and association」に追加される等の修正がされている[198]。追加されたのは以下の文章である。

・ 「欧州委員会は、『研究・イノベーション（R&I）の海外からの干渉』に取り組むためのツールキットを発表した。この文書は、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に関する多くの勧告を提供しており、高等教育機関や研究実施機関

[198] European Commission. *Horizon Europe Program Guide*. Version 2. 11 April 2022. <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf

が国際的な R&I に取り組む際の支援を提供することを目的としている。Horizon Europe に参加するすべての人は、この文書及び国レベルで存在する同等のアドバイスをよく理解し、提出予定のプロポーザルとの関連性を検討することが推奨される。」