CRDS 研究開発戦略センター
Center for Research and Development Strategy

国立研究開発法人科学技術振興機構

大学等の研究セキュリティ確保に向けた文部科学省関係施策に係る検討会
（2024年10月17日開催）

諸外国における研究セキュリティの取組み

– 政府・資金配分機関によるリスク評価と大学への支援を中心に

2024年10月17日

JST研究開発戦略センター

諸外国における研究セキュリティの取組み（概要）

【米】各省庁・資金配分機関の目的に合わせたリスク評価

- 大統領覚書、半導体・科学法等の大方針に基づき、**省庁・資金配分機関ごとに安全保障上のリスクを評価**。NSFでは2025年度から試行として量子分野に対象にリスク評価を予定。基盤的研究を対象にしたDOE、DODプログラムでも**①申請者、②所属機関、②技術**の観点からリスク評価を実施。
- NSFの公募で大学で実施するSECUREセンターの設置で、①大学・研究機関のための**ワンストップ情報共有コンソーシアム**、②**潜在的なセキュリティリスク分析**を前進。

【英】政府、資金配分機関、大学がｶﾞｲﾄﾞﾗｲﾝ作成し導入

- 2019年から国家保護安全保障局（NPSA）が**「Trusted Research ガイダンス」**を発表し研究セキュリティを推進。
- 資金配分機関（UKRI）は、研究機関の関連法・規則の遵守、違反時の資金提供停止・返還要求などガイドラインを発行。EPSRC、UKRIでは、国際協力時に**公募審査プロセスの中でのデューデリジエンス**を実施。
- **研究協力アドバイスチーム（RCAT）**など大学支援も進む。

【豪】政府の外国干渉対策の一環として研究ｾｷｭﾘﾃｨ推進

- 政府全体で取り組む「外国干渉対策」の取組みが学術界に対しても展開。
- 資金配分機関（ARC）は、2023年に**公募から審査段階におけるリスク評価として「外国干渉枠組み」**を公表2。審査の各段階で特定されたリスクに対して緩和策を実施。
- ARCは、リスク評価の段階で**ASIO等安全保障関連の機関の助言**を求める。

【加】政府が機微技術分野と懸念機関をリスト化・公表

- 「Shared responsibility」をコンセプトに掲げ、**政府-アカデミアWG**を中心に2018年から議論開始。
- **①「機微な研究分野」**と**②「指定研究機関」リストを公開**し、資金配分機関、大学ともにリスク評価を実施。
- 資金配分機関では、研究申請内容とリストを照合し、リスク緩和策を実施。**安全保障上の懸念は公安省等の助言**を求める。
- **相談窓口、体制強化のための基金**など大学への支援が豊富。

【蘭】政府がガイドラインを示し、大学による自律的管理

- 教育文化科学省が中心的な役割を果たし**「Knowledge Security」**をコンセプトに掲げ研究セキュリティを推進。
- 政府によるガイドラインと相談窓口によって、**大学・研究機関による自律的管理**が進む。資金配分機関(NWO) は、大学がガイドラインの要件に従い管理していることを確認する。
- EU以外からの研究者の入国についてスクリーニングを行う「Knowledge Security Screening Act」が検討されている。

【仏】政府による技術保護制度で研究セキュリティを実施

- 2012年から安全保障、経済的な観点から技術保護をする制度**「科学技術潜在力の保護制度（PPST）」**を運用。一部の大学では国防安全保障管理官（FSD）によるアクセス管理実施。

【独】大学での輸出管理の徹底と対中対応の転換の兆し

- 中国への技術流出懸念への対応は、**輸出管理の徹底**から開始。
- アカデミアの対中認識の転換、連邦教育研究省によるガイドラインの策定、相談窓口の設置などが検討される予定。

NSF: 国立科学財団
UKRI: 英国研究・イノベーション機構

EPSRC: 工学・物理科学研究会議
NPSA: 国家保護セキュリティ局 (旧CPNI)

ARC: オーストラリア研究会議
NOW: オランダ科学研究機構

略称

国	略称	正式名称	日本語訳
米	CFR	Code of Federal Regulation	連邦規則集
	DARPA	Defense Advanced Research Projects Agency	国防高等研究計画局
	DOD	Department of Defense	国防総省
	DOE	Department of Energy	エネルギー省
	FBI	Federal Bureau of Investigation	連邦捜査局
	NAS	National Academy of Sciences	全米アカデミーズ
	NIH	National Institutes of Health	国立衛生研究所
	NIST	National Institute of Standards and Technology	米国国立標準技術研究所
	NSF	National Science Foundation	米国立科学財団
	NSPM	National Security Presidential Memorandum	国家安全保障大統領覚書
	ODNI	Office of the Director of National Intelligence	国家情報長官室
	OSTP	Office of Science and Technology Policy	米国科学技術政策局
	USC	United States Code	合衆国法律集
英	BBSRC	Biotechnology and Biological Sciences Research Council	英国バイオテクノロジー・生物科学研究会議
	BEIS	Department for Business, Energy & Industrial Strategy	ビジネス・エネルギー・産業戦略省
	CPNI	Centre for the Protection of National Infrastructure	国家インフラ保護センター
	DSIT	Department for Science, Innovation and Technology	科学・イノベーション・技術省
	EPSRC	Engineering and Physical Sciences Research Council	英国工学・物理科学研究会議
	NPSA	National Protective Security Authority	国家保護安全保障局（旧CNPI）
	RCAT	Research Collaboration Advice Team	研究協力アドバイスチーム
	UKRI	UK Research and Innovation	英国研究・イノベーション機構
	UUK	Universities UK	英国大学協会
豪	AISO	Australian Security Intelligence Organisation	豪州保安情報機構
	ARC	Australian Research Council	豪州研究会議
	CFI	Countering Foreign Interference	外国干渉対策
	UFIT	University Foreign Interference Taskforce	大学外国干渉タスクフォース
加	ISED	Innovation, Science and Economic Development Canada	イノベーション・科学・経済開発省
	NSGRP	National Security Guidelines for Research Partnerships	研究協力に関する国家安全保障ガイドライン
	STRAC	Sensitive Technology Research and Affiliations of Concern	機微技術研究と懸念される提携関係
蘭	NOW	Dutch Research Council	オランダ研究会議
	UNL	Universities of the Netherlands	オランダ大学連盟
仏	FSD	Security and Defense Officer	国防安全保障管理官
	PPST	Protection of the Scientific and Technical Potential	科学技術潜在力の保護制度
	ZRR	Restrictive Regime Zones	制限領域
独	BND	Bundesnachrichtendienst	連邦情報局
	DAAD	German Academic Exchange Service	ドイツ学術交流会

アウトライン

諸外国における研究セキュリティの取組み
– 政府・資金配分機関によるリスク評価と大学への支援を中心に

1. **諸外国における研究セキュリティの取組み**
2. **リスク提示**
3. **リスク評価、リスク管理・緩和策**
4. **意識啓発**
5. **政府等による大学・研究機関への支援**
   - 相談窓口
   - 一元的な情報共有の仕組み（ポータルサイト等）
   - アカデミアと政府とのコミュニケーション
   - アカデミアと法執行機関・情報機関とのコミュニケーション

参考資料

アウトライン

諸外国における研究セキュリティの取組み
– 政府・資金配分機関によるリスク評価と大学への支援を中心に

1. 諸外国における研究セキュリティの取組み
2. リスク提示
3. リスク評価、リスク管理・緩和策
4. 意識啓発
5. 政府等による大学・研究機関への支援
- 相談窓口
- 一元的な情報共有の仕組み（ポータルサイト等）
- アカデミアと政府とのコミュニケーション
- アカデミアと法執行機関・情報機関とのコミュニケーション

参考資料

1．諸外国における研究セキュリティの取組み（全体像）

- 諸外国（米、英、加、豪、蘭）の取組みを比較*。

※本資料は赤枠を中心に紹介

ガイドライン	■ 大学・研究機関が実施する研究セキュリティの手順書 • 研究活動の原則（学問の自由・開放性・公平性）、研究セキュリティの目的、具体的な対策等から成る	
リスクの提示	■ 何がリスクかを明示 ① 懸念される主体 ② 潜在的リスクがあるとされる技術分野	
情報開示	■ 情報開示の場面・方法（いつ、どのように） • 国際連携が発生する場面（外国の研究者・客員の受入、外国出張、共同研究、役務調達等）で情報開示を求める。 ■ 開示内容（何を） • 経歴、支援（金銭、現物寄付）、契約内容等	
リスク評価	■ **政府・資金配分機関が実施する場合** →本資料はこちらを中心に紹介 • 研究費の申請時に申請者が必要情報（経歴、現在・申請中の研究費等支援、連携先等）を情報開示 • 申請書の審査時に①懸念される主体と②技術内容からリスク評価 • 加、豪、蘭は、安全保障関係部局が審査に関与・助言	■ **大学・研究機関が実施する場合** • 国際連携が発生する場面（外国の研究者・客員の受入、外国出張、共同研究、役務調達等）でのリスク評価 • オープンソースによるデューデリジェンス。判断に迷う場合は、政府の窓口に相談（英、加、蘭）
リスク管理・緩和	■ **政府・資金配分機関が実施する場合** →本資料はこちらを中心に紹介 • 申請者や大学と協議の上、リスク緩和策実施（以下例示） - 大学による「リスク緩和計画」の策定 - トレーニング頻度、進捗報告頻度を増やす - アクセス管理、サイバーセキュリティ、データ管理 - 研究プロジェクトの参画者の交代 - 不採択（できるだけ不採択の件数は出したくない）	■ **大学・研究機関が実施する場合** • 指針やガイドライン等に基づき体制整備（以下例示）： - 体制整備（意思決定権限、部署間連携、専門部署） - 施設アクセス管理 - サイバーセキュリティ、データ管理 - 安全保障輸出管理等法令遵守 - トレーニングの実施 - 記録・報告プロセス
意識啓発	■ トレーニングの実施 ■ ケーススタディ	
大学への支援	■ 相談窓口 ■ 情報共有の仕組み（ポータルサイト、説明会の実施等） ■ 政府とアカデミアのコミュニケーション ■ 法執行機関、諜報機関、安全保障部局とアカデミア	

*デスクトップ調査の際に研究セキュリティの取組みが積極的に行われている国を対象としている点に留意。

1．諸外国における研究セキュリティの取組み（全体像）

- リスクの提示では、研究セキュリティのために新たにリストを作成する国と既存の制度を活用する国がある。
- リスク評価、緩和では、資金配分機関が研究費採択時に評価する国と、大学の自律的な管理に委ねる国がある。
- 資金配分機関でリスク評価を行う際は、国家安全保障の観点から技術評価する仕組みを導入している国もある。

	米 	英 	豪 	加 	蘭 
ガイドライン	あり • 政府：OSTP、NIST	あり • 政府：NPSA • FA：UKRI • 大学：UUK	あり • 大学外国干渉タスクフォース	あり • 政府-大学WG • 大学：U15	あり • 政府：ｲﾉﾍﾞｰｼｮﾝ・科学経済開発省と大学協会等で共同作成
リスクの提示	• 主体：「懸念国」「懸念事業体」、1286 List • 技術：　-	• 主体：制裁リスト等 • 技術：国家安全保障・投資法の17分野を参照	• 主体：制裁リスト等 • 技術：「国益のための国家重要技術」を参照	• 主体：指定研究機関ﾘｽﾄ • 技術：機微技術研究分野リスト	• 主体：制裁リスト等 • 技術：EUのデュアルユース規制
リスク評価	**省庁、FAごとに対応** • NSF：TRUST（2025予定） • DOE：RTES評価 • NIH, DOD*：意思決定マトリックス	**EPSRCで実施** • 公募審査時に連携先、客員研究員等と各種制裁リストとの関係を確認	**ARCで実施** • 重要技術分野への申請者の利益相反を確認 • 安保部局のレビュー有り	**3つのFAで実施** • NSGRPガイドライン • STRAC方針 • 安保部局の助言あり	**大学の自律的管理** • 資金配分機関は、大学がガイドラインを導入、遵守しているか確認
リスク管理・緩和	• 「リスク緩和計画」策定 • DOD：参画者交代、トレーニング・報告頻度増、不採択	• 追加情報の提供依頼 • リスク緩和策の策定 • 資金提供条件の追加	• 追加情報の提供依頼 • リスク緩和策の策定	• 「リスク緩和計画」策定 • 不採択	• 資金配分機関は、大学がガイドラインを導入、遵守しているか確認
意識啓発	• NSF：トレーニング構築 • FBI：ケース紹介等アウトリーチ	• NPSA：自己評価モニタリング	• UFIT：ケーススタディの作成	• 政府：トレーニング • 政府：ケース紹介、WS等アウトリーチ	• 大学協会：自己評価モニタリング
大学への支援	• NSF主導・大学運営：相談窓口、分析センター • ODNI: 専用ｳｪﾌﾞｻｲﾄ • NAS: 円卓会議 • FBI/DHS: アウトリーチ	• DSIT: 相談窓口 • NAPSA: アウトリーチ	• 政府-大学のTF • ASIO: アウトリーチ	• 公安省：相談窓口、大学へのアウトリーチ • 政府：専用ウェブサイト • 政府-大学WG	• 政府：相談窓口 • 政府：専用ウェブサイト

NSF: 国立科学財団
ODNI: 国家情報長官室
NAS: 米国科学アカデミー
UKRI: 英国研究・イノベーション機構
NPSA: 国家保護セキュリティ局 (旧CPNI)
UUK: 英国大学協会
EPSRC: 工学・物理科学研究会議
BBSRC: ﾊﾞｲｵﾃｸﾉﾛｼﾞｰ・生物科学研究会議
DSIT: 科学技術イノベーション省
ARC: オーストラリア研究会議
UFIT: 大学外国干渉タスクフォース
*米国防総省は、基礎研究局の対応を取り上げている

（参考）その他の国の取組み

- ドイツ、フランスでは、調査時点（2024年10月）では、前頁5か国のようなガイドライン策定、リスク評価、リスク緩和等の対策は見られない。
- 一方で、ドイツでは連邦教育研究省によるガイドラインの策定、相談窓口の設置などが検討されている。
- フランスでは、輸出管理の1つであるPPSTによる技術情報管理の枠組みの適用の拡大が議論されるなど、各国の事情を踏まえた取組みが進みつつある。

■ **情報機関、輸出管理担当行政からの注意喚起**

- 2020年、連邦情報局（BND）が孔子学院等中国の科学技術研究・教育の脅威について報告。
- 連邦経済・輸出管理庁が輸出管理マニュアルで、中国との学術交流に関する留意点を記載。

■ **輸出管理の徹底**

- マックス・プランク協会等の研究機関で、輸出管理の徹底や国際協力のためのガイドライン策定。

■ **大学・アカデミアの対中対応の転換の兆し**

- ドイツ学術交流会(DAAD)が「中国のアカデミアとの交流に向けた指針」(2024)を発表。リスクを最小限に抑え、透明性を確保するなど大学の行動指針を示す。
- 連邦教育研究省「ポジションペーパー：研究セキュリティ」(2024)を発表。以下の検討が始まる。
  - 大学向けの**ガイドライン策定**
  - ステークホルダーを巻き込む**意見調整の場**
  - **相談窓口**（オランダを参考）

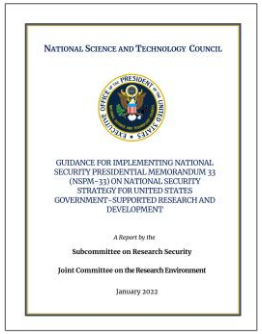
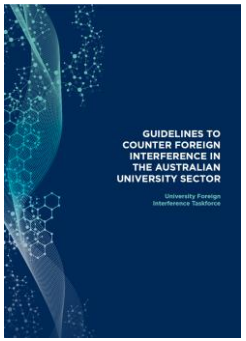
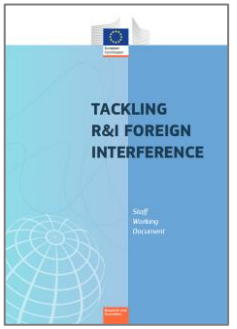
■ **「科学技術潜在力の保護制度（PPST）」**

- 2012年成立。公的・私的機関の戦略的知識、専門知識、機密技術へのアクセスと情報を保護する制度。
- 国家の経済的利益を損なう、国家の防衛力を損なうリスクがある場合の経済情報保護政策の一つ。
- 管理が必要とされる情報は、「制限領域（ZRR）」で物理的・非物理的アクセスを許可。
- 違反時は刑法による罰則が適用。輸出管理、外国投資管理制度を補完する位置づけ。

■ **PPSTの適用拡大の検討**

- 同制度を新興技術の管理に適用する議論が出ているが、軍事利益、テロなどを想定した高い水準の規制であることから、用途が定まらない新興技術への適用には課題があると指摘。
- フランス国立研究機構（ANR）では、2024年の行動計画で「科学技術潜在力の保護制度」（PPST）が入る。申請者に対して、PPSTに従った施策を講じることを推進するとされている。

（参考）各国の研究セキュリティのガイドライン

米	英	豪	加	EU	蘭
「NSPM-33履行のためのガイダンス」(2022)	「アカデミア向けTrusted Researchガイダンス」(2019)	「大学外国干渉タスクフォース（UFIT）ガイドライン」(2019,2021更新)	「国際研究協力に対する国家安全保障ガイドライン」(2021)	「研究イノベーションでの海外からの干渉に対処するためのスタッフ作業文書」	「国家知識セキュリティガイドライン」(2022)
					
• 資金配分機関に対して、①情報開示、②リスク評価・管理、③トレーニングモジュールの構築、④研究セキュリティプログラム（国際協力、サイバーセキュリティ、輸出管理等）確立を要請。 • その他、NIST「国際的な科学を守る」等	• リスク評価、利益相反の可能性、国際協力におけるサイバーセキュリティ、外国人研究員受入時、海外出張時の情報開示などチェック項目を示す。 • その他、UKRI「Trusted Researchとイノベーション原則」等	• 大学における外国干渉経対応するためのガイドライン。 • ガバナンスの構築、教育や知見共有の機会の確保、金銭的利害関係等の開示やデューデリジエンス、サイバーセキュリティ対策等を要請	• 外国の干渉、スパイ活動、望ましくない知識移転によってもたらされる国家安全保障上のリスクを特定し、リスク軽減を実施するためのガイドライン。 • その他、「機微技術の研究と懸念される提携に関する方針」等	• 大学、研究機関が外国からの干渉対応を行うための包括的な戦略を策定する際のベストプラクティスを示す。	• 研究活動における国際協力時に大学が実施するリスク評価、リスク管理に関するガイドライン。 • 大学・研究機関等よる自律的な規制を前提

NIST：米国国立標準技術研究所
UKRI：英国研究・イノベーション機構

アウトライン

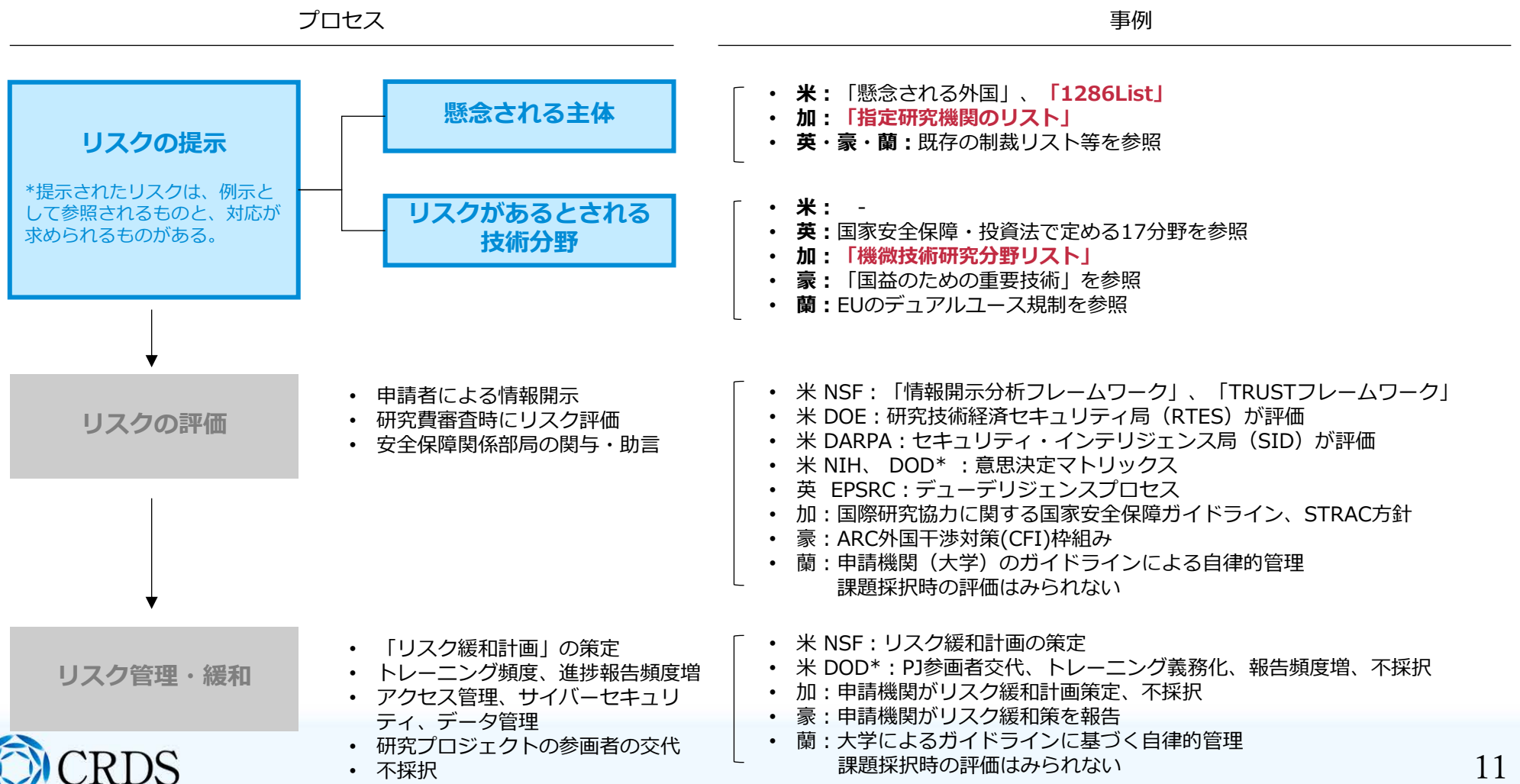
諸外国における研究セキュリティの取組み
– 政府・資金配分機関によるリスク評価と大学への支援を中心に

1. 諸外国における研究セキュリティの取組み（全体像）
2. **リスク提示**
3. リスク評価、リスク管理・緩和策
4. 意識啓発
5. 政府等による大学・研究機関への支援
   - 相談窓口
   - 一元的な情報共有の仕組み（ポータルサイト等）
   - アカデミアと政府とのコミュニケーション
   - アカデミアと法執行機関・情報機関とのコミュニケーション

参考資料

2．リスクの提示

- 研究セキュリティ上の①懸念される主体、②潜在的リスクがある技術分野については、既存の制裁リストや安全保障貿易管理の技術リストの参照が推奨されることがある。
- 既存のリストの他、研究セキュリティのための新たなリスト作成の動きがあり、リスクに応じた対策が行われる。
- リストを作成している米国やカナダでは、リストの目的を示しており、リストの適用範囲、意義の検討が重要。



*米DODは基礎研究局のプログラムが対象

米国 懸念される学術機関・人材採用プログラム

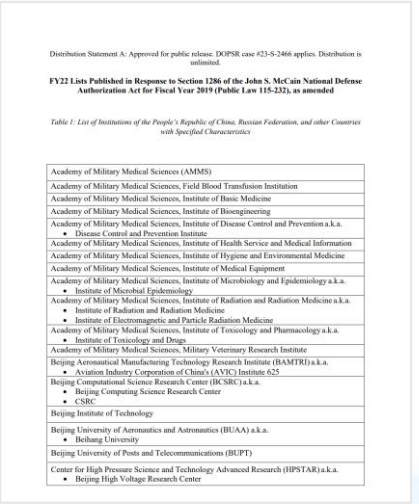
■ 研究セキュリティに対応した懸念される学術機関・人材採用プログラムのリスト

- 全省庁、資金配分機関共通で、**悪質な外国の人材採用プログラムへ研究参加制限**が課されている（OSTP Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs）。

外国の人材採用プログラム	• 対象となる団体（外国が直接支援しているかどうかは問わない） 外国またはその指定機関、外国に拠点を置く団体、外国が資金提供している団体、 外国と提携している団体 • 内容（※外国の人材採用プログラムに該当しないプログラムも規定 現金、研究費を含む現物支給、将来の報酬の約束、無料の外国出張、少額でない物品、高い敬称・キャリアアップの機会、その他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
悪質な外国の人材採用プログラム	以下のうち1つでも該当するもの ① 国務長官が定義する「懸念される外国」（現在（2024年1月1日現在）**中国、北朝鮮、ロシア、イラン**を含む ）がスポンサー ② 2019年度国防権限法第第**1286条**(c)(8)の学術機関 →→（**通称：1286 List**） ③ 2019年度国防権限法第第**1286条**(c)(9)の人材採用プログラム →→（**通称：1286 List**）

■ 1286 List

- 「特殊な特徴を持つ機関のリスト」と「外国の人材採用プログラム」から成る。2019年国防権限法§1286により作成されたことから通称「1286 List」と呼ばれる。
  - **「特殊な特徴を持つ機関のリスト」**：中華人民共和国、ロシア連邦等の機関で約50機関掲載。
  - **「外国の人材採用プログラム」**：米国の国家安全保障上の利益を脅かす外国の人材プログラムが挙げられており、長江学者奨励計画、広州市海外高度人材プログラム等６プログラムの他、半導体・科学法セクション10638 (4)(B)(i)または(ii)の基準を満たすプログラム



Distribution Statement A: Approved for public release. DOPSR case #23-S-2466 applies. Distribution is unlimited.

FY22 Lists Published in Response to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended

Table 1: List of Institutions of the People's Republic of China, Russian Federation, and other Countries with Specified Characteristics

Academy of Military Medical Sciences (AMMS)
Academy of Military Medical Sciences, Field Blood Transfusion Institution
Academy of Military Medical Sciences, Institute of Basic Medicine
Academy of Military Medical Sciences, Institute of Bioengineering
Academy of Military Medical Sciences, Institute of Disease Control and Prevention a.k.a. • Disease Control and Prevention Institute
Academy of Military Medical Sciences, Institute of Health Service and Medical Information
Academy of Military Medical Sciences, Institute of Hygiene and Environmental Medicine
Academy of Military Medical Sciences, Institute of Medical Equipment
Academy of Military Medical Sciences, Institute of Microbiology and Epidemiology a.k.a. • Institute of Microbial Epidemiology
Academy of Military Medical Sciences, Institute of Radiation and Radiation Medicine a.k.a. • Institute of Radiation and Radiation Medicine • Institute of Electromagnetic and Particle Radiation Medicine
Academy of Military Medical Sciences, Institute of Toxicology and Pharmacology a.k.a. • Institute of Toxicology and Drugs
Academy of Military Medical Sciences, Military Veterinary Research Institute
Beijing Aeronautical Manufacturing Technology Research Institute (BAMTRI) a.k.a. • Aviation Industry Corporation of China's (AVIC) Institute 625
Beijing Computational Science Research Center (BCSRC) a.k.a. • Beijing Computing Science Research Center • CSRC
Beijing Institute of Technology
Beijing University of Aeronautics and Astronautics (BUAA) a.k.a. • Beihang University
Beijing University of Posts and Telecommunications (BUPT)
Center for High Pressure Science and Technology Advanced Research (HPSTAR) a.k.a. • Beijing High Voltage Research Center

出典：国防総省「高等教育機関におけるDOD資金による研究における好ましくない影響への対抗」（2023.6）

（参考）米国 「懸念される外国」「懸念される事業体」

- 「懸念される外国」、「懸念される事業体」は、連邦行政命令集（CFR）の定めに準じる。商務省のプログラムでは、 「懸念される外国」、「懸念される事業体」からの参加者について、以下の取扱いとしている。
- **「懸念される外国」からの参加**：合法的に米国に滞在している個人がR&Dプログラムへ参加できなくなることはない。ただし、研究セキュリティの評価対象となる。審査で承認されれば、研究所のチーム、プロジェクトチーム、または研究所のメンバーとして参加する資格がある。
- **「懸念される事業体」からの参加**：「懸念される事業体」 がR&Dプログラムへの参加することはできない。

懸念される外国 （Foreign Country of Concern）	「半導体・科学法」における「懸念される外国」は、15CFR Part 231に準ずる（Sec. 10638）。 • 10 U.S.C. § 4872(d)に定められる国 - 北朝鮮／中国／ロシア／イラン • 国務長官が国防長官、国務長官、国家情報長官と協議の上、米国の国家安全保障または外交政策に有害な行為を行っていると判断した国
懸念される事業体 （Foreign Entities of Concern）	「半導体・科学法」における「懸念される事業体」は、15 CFR Part 231に準ずる（Sec. 10638）。 a. 国務長官によって外国テロ組織に指定されている事業体（8 USC 1189） b. 財務省外国資産管理局（OFAC）のSpecial Designated Nationals and Blocked Persons List （SDN List）に含まれている事業体 c. 10 USC § 4872(d) に記載されている外国政府によって所有、管理、または管轄もしくは指示を受けている事業体 d. 司法省により有罪判決を受けた活動に関与したとされる外国事業体 - 合衆国法典18編37章、951条、（スパイ活動法） - 合衆国法典18編951条または1030条 - 武器輸出管理法（AECA） - 原子力法1954 - 輸出管理改革法2018 - 国際緊急経済権限法 d. 商務長官が国防長官および国家情報長官と協議の上、米国の国家安全保障または外交政策に有害な無許可の行為に関与していると判断した外国事業体

CFR: Code of Federal Regulations (連邦行政命令集)
USC: United States Code (合衆国法律集)

カナダ 指定研究機関のリスト

- カナダ政府は、「機微技術の研究と懸念される提携に関する方針」を発表（2024年1月）。
- カナダの資金配分機関から研究費を受け、**機微な研究分野を推進する全ての研究者に対して、指定研究機関のリスト（Named Research Organizations）との繋がりを確認する必要**があるとした。
- リストは、**軍、国防、および国家安全保障機関と直接的または間接的な繋がりにより、カナダの国家安全保障に最も高いリスクをもたらし得る研究組織および研究機関**がして選定されている。
- 2024年9月時点で103機関が指定されており、内訳は以下のとおり。
  - **中国: 85機関**
  - **イラン: 12機関**
  - **ロシア: 6機関**
- 記載は正式名称と通称の両方が併記されている。
- 本リストは更新される。

A B C D E H I J K L M N O P R S T U X #

正式名称

A

A.A. Kharkevich Institute for Information Transmission Problems, IITP, Russian Academy of Sciences (Russia)

Academy of Military Medical Sciences (People's Republic of China)
Known alias(es): AMMS

通称

Academy of Military Science (People's Republic of China)
Known alias(es): AMS

Aerospace Research Institute (Iran)
Known alias(es): ARI

Air Force Medical University (People's Republic of China)
Known alias(es): Air Force Medical University; Air Force Military Medical University; Fourth Military Medical University; Fourth Medical University

Air Force Research Institute (People's Republic of China)
Known alias(es): Air Force Equipment Academy; Key Laboratory of Complex Aviation System Simulation

Air Force Xi'an Flight Academy (People's Republic of China)
Known alias(es): PLA Air Force Xi'an Flight Academy; Air Force Xi'an Flight Academy; Xi'an Flying College of PLA Air Force

Airforce Command College (People's Republic of China)
Known alias(es): PLA Air Force Command College; Air Force Command College; AFCC; PLA Air Force Command Academy

Airforce Communication NCO Academy (People's Republic of China)
Known alias(es): Dalian Communications NCO Academy

Airforce Early Warning Academy (People's Republic of China)
Known alias(es): Wuhan Radar Institute

Airforce Engineering University (People's Republic of China)
Known alias(es): AFEU

Airforce Flight Academy Shijiazhuang (People's Republic of China)
Known alias(es): PLA Air Force Shijiazhuang Flight Academy; Shijiazhuang Flying College of the PLA Airforce; Shijiazhuang Flight College of Air Force

Airforce Harbin Flight Academy (People's Republic of China)
Known alias(es): Harbin Flight College of Air Force

Airforce Logistics University (People's Republic of China)

Army Academy of Armored Forces (People's Republic of China)
Known alias(es): Army Armored Forces Academy; Armored Forces Engineering Academy

Named Research Organizations 4

January 2024

出典：ISED「Named Research Organizations」

カナダ 機微技術研究分野のリスト

- カナダ政府は、「機微技術の研究と懸念される提携に関する方針」を発表（2024年1月）。
- **カナダの研究開発にとって重要**であると同時に、技術的優位性を不正に流用することで**カナダに損害を与えようとする外国政府、非政府団体の関心がありうる新興技術**について「機微技術研究分野」としてリストを公開。
- リストの発行は、カナダ政府（イノベーション・科学経済開発省）とされている。
- 本リストは更新される。

1 先進的な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
- 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 先進エネルギー技術

- 高度なエネルギー貯蔵技術
- 先進的な原子力発電技術
- ワイヤレス電力伝送技術

3 先端材料と製造

(先端材料)
- 従来の材料の拡張
- オーセチック材料
- 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
- 超伝導材料
- 2次元（2D）材料

（先進製造業）
- 付加製造（3Dプリント）
- 先進的な半導体製造
- 重要材料製造
- 4次元（4D）印刷
- ナノ製造
- 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
- クロスキューセンサ
- 電界センサー
- ｲﾒｰｼﾞﾝｸﾞ、光学デバイス、センサ
- 磁場センサー（または磁力計）
- マイクロ（ナノ）電気機械システム（M/NEMS）
- 測位、ナビゲーション、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) センサネットワーク

5 高度な武器　*具体例なし

6 航空宇宙・宇宙・衛星技術

- 風洞インフラ
- 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
- データ科学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 人間と機械の統合

- 脳コンピュータインターフェース
- エクソスケルトン
- 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
- ウェアラブル脳科学

9 人間と機械の統合

（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 ロボット工学と自律システム

- 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

CRDS

出典：ISED「Sensitive Technology Research Areas」を元にCRDSで作成

オランダ 「国家知識セキュリティガイドライン」

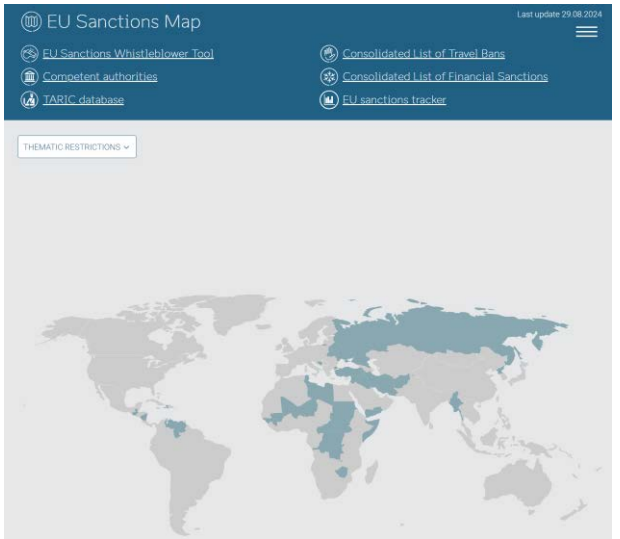
■ リスクの対象となる知識領域

- EUの**デュアルユース規制（「二重用途物品に関する規制」）**に基づくデュアルユース製品、技術。オランダではEUの同規則に準じる。
- 同規則は、基礎研究を対象外としているが、基礎研究と応用研究の線引きは明確ではない。基礎研究と応用研究を区別するために、同ガイドラインでは、**① TRL**（TRL1、2 は基礎研究）と**② 資金源**から判断をすることを推奨。TRLの評価にあたっては、**カナダ政府の「TRL評価ツール」**を推奨。
- 国家安全保障上の懸念がある研究領域かどうかについては、国家情報安全保障局（AIVD）に相談できるとされている。

■ リスクの対象となる主体

- リスクの高い国：
  - 国際的な**制裁リスト**に掲載されている国（EU Sanction Map）。
  - **国家情報安全保障局（AIVD)、軍事情報安全保障局（MIVD）**が発表している「国家主体の脅威評価」や「年次報告書」を参照することを推奨。
  - その他の国際ランキングと指標：
    - Academic Freedom Index
    - Freedom in the World Report published by Freedom House
    - Democracy Index published by The Economist Intelligence Unit
    - World Justice Project Rule of Law Index published by the World Justice Project

EU Sanction Map



出典：オランダ政府「国家知識セキュリティガイドライン」(2022)

アウトライン

諸外国における研究セキュリティの取組み
– 政府・資金配分機関によるリスク評価と大学への支援を中心に

1. 諸外国における研究セキュリティの取組み
2. リスク提示
3. **リスク評価、リスク管理・緩和策**
4. 意識啓発
5. 政府等による大学・研究機関への支援
   - 相談窓口
   - 一元的な情報共有の仕組み（ポータルサイト等）
   - アカデミアと政府とのコミュニケーション
   - アカデミアと法執行機関・情報機関とのコミュニケーション

参考資料

3．リスク評価、リスク管理・緩和策

- リスク評価プロセスでは、**自動的に不採択にするのではなく、リスクベース評価を行い緩和策**が検討される。
- 安全保障観点からのリスク評価は、**安全保障の専門家（安全保障部局）**による関与。申請書の**テクニカルメリットと安全保障リスクの判断はガバナンスを分ける**。
- 審査プロセスや基準の透明性の確保によって、大学・研究機関の対策において予見可能性が高まる。

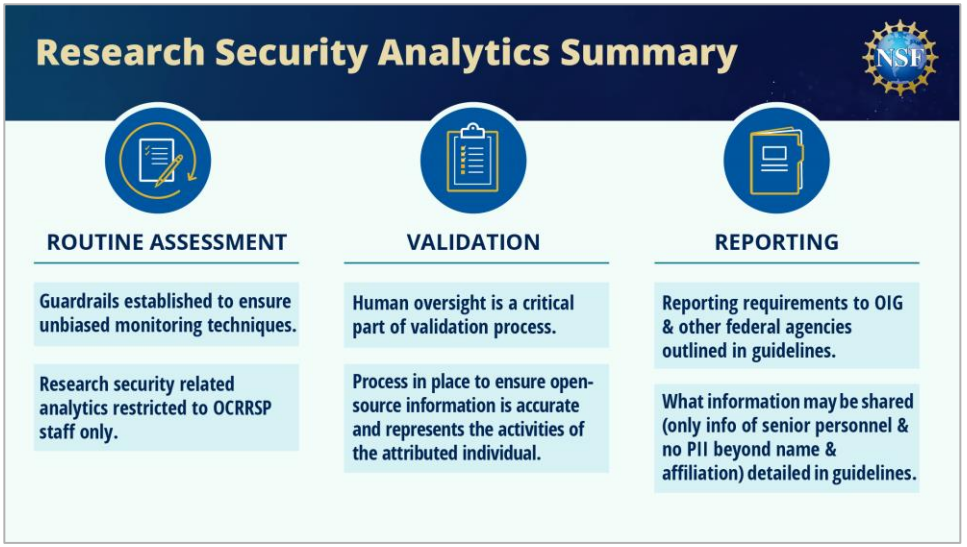
プロセス		事例
リスクの提示 *提示されたリスクは、例示として参照されるものと、対応が求められるものがある。	**懸念される主体**	• 米：「懸念される外国」、「1286List」 • 加：「指定研究機関のリスト」 • 英・豪・蘭：既存の制裁リスト等
	リスクがあるとされる技術分野	• 米：　- • 英：国家安全保障・投資法で定める17分野を参照 • 加：「機微技術研究分野リスト」 • 豪：「国益のための重要技術」を参照 • 蘭：EUのデュアルユース規制を参照
リスクの評価	• 申請者による情報開示 • 研究費審査時にリスク評価 • **安全保障関係部局の関与・助言**	• **米 NSF：「情報開示分析フレームワーク」、「TRUSTフレームワーク」** • **米 DOE：研究技術経済セキュリティ局（RTES）**が評価 • **米 DARPA：セキュリティ・インテリジェンス局（SID）**が評価 • **米 NIH、 DOD*　：意思決定マトリックス** • **英　EPSRC：デューデリジェンスプロセス** • **カナダ：国際研究協力に関する国家安全保障ガイドライン、STRAC方針** • **豪：ARC外国干渉対策(CFI)枠組み** • **蘭：**申請機関（大学）のガイドラインによる自律的管理 課題採択時の評価はみられない
リスク管理・緩和策	• 「リスク緩和計画」の策定 • トレーニング頻度、進捗報告頻度増 • アクセス管理、サイバーセキュリティ、データ管理 • 研究プロジェクトの参画者の交代 • 不採択	• **米 NSF：リスク緩和計画**の策定 • **米 DOD*：**PJ参画者交代、トレーニング義務化、報告頻度増、不採択 • **加：**申請機関が**リスク緩和計画策定、不採択** • **豪：**申請機関が**リスク緩和策**を報告 • **蘭：**大学によるガイドラインに基づく自律的管理 課題採択時の評価はみられない

*米DODは基礎研究局のプログラムが対象

NSFにおける研究費申請書のリスク評価、管理・緩和

- NSFでは現状、申請時に開示させた情報を直接採択には活用しないとしている。
- 2025年1月より量子分野から、研究費申請時のリスク評価・緩和を開始予定。

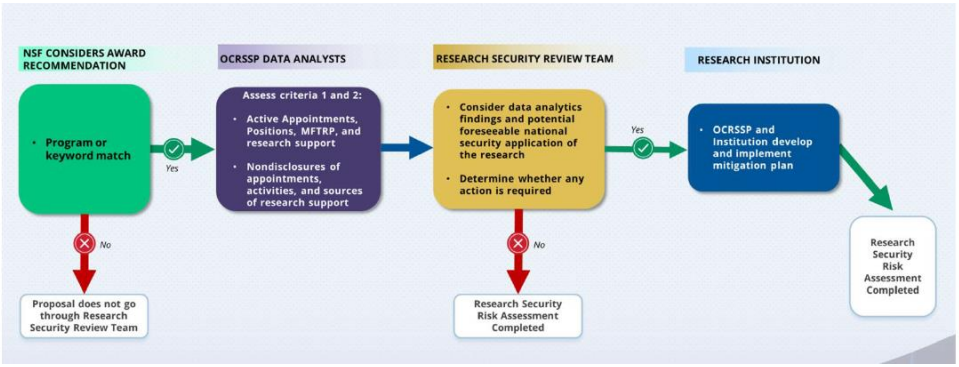
開示情報分析



- 開示された情報の評価・開示情報の検証・報告は、**研究セキュリティー戦略・政策統括室（OCRSSP）** のみ実施。他部署は行えない**（ガバナンス）**。
- 公開情報（論文・特許データ）に基づき、開示情報を分析・検証*
- 虚偽等が合った場合、監察総監室（OIG）、法執行機関、情報機関等への報告　⇒ **採択には使用しない**
- 分析結果は、**研究セキュリティ理解促進活動のために活用**

*特定の国籍、人種によって明示的、暗黙的に設計されたデータクエリによる分析は禁止

TRUST フレームワーク



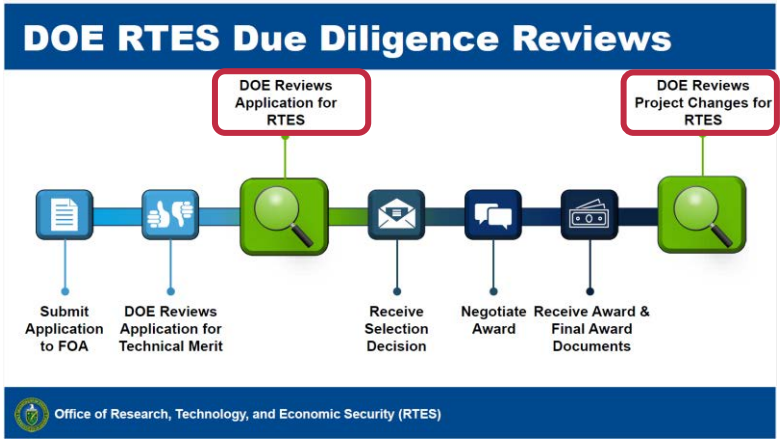
- NSFが資金提供する研究に対して、外国からの影響の可能性（potential）を特定するためのフレーム
- 量子分野からパイロット事業として実施予定（2025年度）
- **データ分析**：OCRSSPによる公開情報（論文・特許）に基づくデータ分析
- **専門家レビュー**：レビューチーム（5-6人）を編成。**NSF以外に連邦政府の国家安全保障専門家**を含める。
- **リスク緩和策**：研究機関から追加情報の収集、リスクの緩和と技術管理の検討

出典：NSF Guidelines for Research Security Analytics
NSF Policy Memo, Trusted Research Using Safeguards and Transparency (TRUST)

その他の資金配分機関におけるリスク評価、管理・緩和

- DOEでは、安全保障に関するリスク評価は、**技術評価とは別に研究技術経済セキュリティ局(RTES)**が実施。
- NIHでは、外国からの干渉への**対応方針と手続きについて透明性を確保**するため意思決定マトリックスを提示。

エネルギー省



*赤枠はCRDSで追記

- **国際部に研究技術経済セキュリティ局(RTES)**設置：技術メリット審査と調整してデューデリジェンスを実施（上赤枠）
- **開示情報：**
  個人：経歴、申請中の支援等
  組織（大学・研究機関）：外国の所有/支配の割合、全取締役のリスト等
- **リスク評価プロセス：**
  申請書提出 → 技術メリット評価 → RTESが評価→採択→受託→プロジェクトの変更時にRTESが評価
- **リスク評価の観点：**
  - **技術：**機微性、インフラ、知財等
  - **個人：**外国の人材採用プログラム、利益相反、責務相反等
  - **機関：**外国による所有権、管理、影響等

NIH(国立衛生研究所)

緩和策 **必要**

緩和策 **推奨**

緩和策 **提案**

Rating	Factor 1: Foreign Talent Recruitment Program[4,5]	Factor 2: Foreign Funding[4,5]	Factor 3: Affiliation with Foreign Institutions or Entities[4,5]
Mitigation measures required. **Contact recipient institution for more information.**	Indicators of active (ongoing) participation in a malign foreign talent recruitment program (MFTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022. [Note: this factor/rating is automatically disqualifying]	Indicators of undisclosed or incompletely disclosed active (ongoing) funding from a Foreign Country of Concern (FCOC) or an FCOC-connected entity	Indicators of an undisclosed or incompletely disclosed active (ongoing) affiliation with an institution or entity located in or connected to a Foreign Country of Concern (FCOC).
Mitigation measures recommended. **Contact recipient institution for more information.**	Within the past 5 years: Indicators of past participation in a malign foreign talent recruitment program (MFTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022. Or Indicators of undisclosed or incompletely disclosed active (ongoing) participation in a foreign talent recruitment program (FTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022	Within the past 5 years: Indicators of undisclosed or incompletely disclosed past funding from a Foreign Country of Concern (FCOC) or an FCOC-connected entity. Or Indicators of undisclosed or incompletely disclosed active (ongoing) funding from a foreign country or foreign entity that is not a Foreign Country of Concern (FCOC) or an FCOC-connected entity.	Within the past 5 years: Indicators of undisclosed or incompletely disclosed past affiliation with an institution or entity located in or connected to a Foreign Country of Concern (FCOC). Or Indicators of an undisclosed or incompletely disclosed active (ongoing) affiliation with an institution or entity located in or connected to a foreign country that is not a Foreign Country of Concern (FCOC).
Mitigation measures suggested. **Consider contacting recipient institution.**	Within the past 5 years: Indicators of undisclosed or incompletely disclosed past participation in a foreign talent recruitment program (FTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of	Within the past 5 years: Indicators of undisclosed or incompletely disclosed past funding from a foreign country or foreign entity that is not a Foreign Country of Concern (FCOC) or an FCOC-connected entity.	Within the past 5 years: Indicators of an undisclosed or incompletely disclosed past affiliation with an institution or entity located in or connected to a foreign country that is not a Foreign Country of Concern (FCOC).

←**リスク評価観点**
- 外国の人材採用プログラム
- 外国からの資金
- 所属先／外国の機関・団体

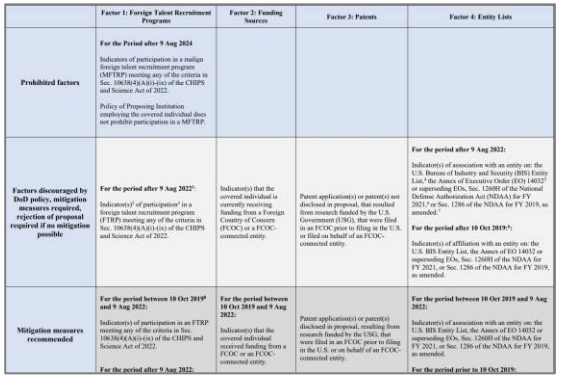
- 外国からの干渉の可能性を検討するための方針として**「NIH Decision Matrix」**を公開（2024.8）**外部研究オフィス（OER）**が開示情報評価。
- **リスク評価の観点：**
  - 外国の人材採用プログラム
  - 外国からの資金
  - 所属先・外国の機関団体
- **意思決定オプション：**
  - **緩和策 必要**：現在「悪質な外国の人材採用プログラム」等関与
  - **緩和策 推奨**：過去5年以内「悪質な外国の人材採用プログラム」等関与
  - **緩和策 提案**：過去5年以内「外国の人材採用プログラム」等関与
  - **緩和策 不要**：過去5年以内「外国の人材採用プログラム」等関与なし
- **緩和策**：申請者・機関への問い合わせ内容を確認、緩和策が検討、監察総監室（OIG）への報告

出典：
NIH Decision Matrix for Assessing Potential Foreign Interference for Covered Individuals or Senior/Key Personnel

その他の資金配分機関におけるリスク評価、管理・緩和

- DOD、DARPAではリスク評価プロセスや観点を示している。評価プロセスや観点の透明性の確保によって、申請者や大学・研究機関による対策が行いやすくなる。

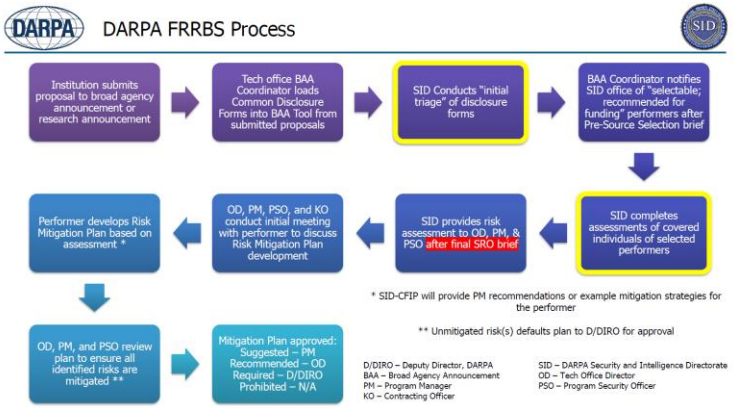
国防総省（基礎研究局）



	Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
Prohibited factors	For the Period after 9 Aug 2024 Indicators of participation in a malign foreign talent recruitment program (MFTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022. Policy of Proposing Institution employing the covered individual does not prohibit participation in a MFTRP.			
Factors discouraged by DoD policy, mitigation measures required, rejection of proposal required if no mitigation possible	For the period after 9 Aug 2022[2]: Indicator(s)[3] of participation[4] in a foreign talent recruitment program (FTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.	Indicator(s) that the covered individual is currently receiving funding from a Foreign Country of Concern (FCOC) or a FCOC-connected entity.	Patent application(s) or patent(s) not disclosed in proposal, that resulted from research funded by the U.S. Government (USG), that were filed in an FCOC prior to filing in the U.S. or filed on behalf of an FCOC-connected entity.	For the period after 9 Aug 2022: Indicator(s) of association with an entity on: the U.S. Bureau of Industry and Security (BIS) Entity List,[6] the Annex of Executive Order (EO) 14032 or superseding EOs, Sec. 1260H of the National Defense Authorization Act (NDAA) for FY 2021,[7] or Sec. 1286 of the NDAA for FY 2019, as amended.[8] For the period after 10 Oct 2019[9]: Indicator(s) of affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.
Mitigation measures recommended	For the period between 10 Oct 2019[9] and 9 Aug 2022: Indicator(s) of participation in an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022. For the period after 9 Aug 2022:	For the period between 10 Oct 2019 and 9 Aug 2022: Indicator(s) that the covered individual received funding from a FCOC or an FCOC-connected entity.	Patent application(s) or patent(s) disclosed in proposal, resulting from research funded by the USG, that were filed in an FCOC prior to filing in the U.S. or on behalf of an FCOC-connected entity.	For the period between 10 Oct 2019 and 9 Aug 2022: Indicator(s) of association with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended. For the period prior to 10 Oct 2019:

- DOD基礎研究局では、**高等教育機関における外国からの影響への対応**として、**「Decision Matrix」**を公開（2023.6）
- **リスク評価の観点**：
  - 外国の人材採用プログラム／資金元／特許／エンティティリスト
  - 参照リストとして「1286 List」公開
- **意思決定オプション：**
  - 不採択
  - リスク緩和 推奨
  - リスク緩和 提案
  - リスク緩和 不要
- **リスク緩和策**：
  - **意識向上トレーニングの受講を義務**
  - **報告頻度の増加を義務付**
  - **リスクがあると判断された個人を交代**
  - **対象者の契約書を国防総省に提出　等**

DARPA



- DARPAでは、**セキュリティ・インテリジェンス局（SID）**が、開示情報の確認、リスクの提示実施
- **基盤的研究リスクベースセキュリティレビュー方針**：
  - SIDが開示情報をトリーアージ、採択可能性のある実施者のリスク評価を実施
  - 受託予定者と技術オフィスディレクター（OD）、PM、プログラムセキュリティオフィサー（PSO）、契約オフィサー（CO）が共同で**「リスク緩和計画」**の検討
  - 受託予定者が「リスク軽減計画」を策定
  - OD、PM、PSOが「リスク緩和計画」をレビュー
- 意思決定オプション、リスク緩和策は左のDOD基礎研究局と同じ方針。

出典： DOD Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education
DARPA Fundamental Research Risk-Based Security Reviews Policy and Process

（参考）研究セキュリティ・プログラムのガイドライン

- OSTPでは「対象機関における研究セキュリティ・プログラムのガイドライン」を発表（2024.7.9）。
- 2021年1月に発表された国家安全保障大統領覚書-33 （NSPM-33）で、資金配分機関に対して、連邦政府の研究費を受ける研究機関向けに「研究セキュリティ・プログラム」確立することを要求。
- 約3年半かかり「研究セキュリティ・プログラムのガイドライン」が発表された。

■ **タイトル**：**「対象機関における研究セキュリティ・プログラムのガイドライン」**
（Guidelines for Research Security Programs at Covered Institutions）
■ **発行年月日**：2024年7月9日
■ **発行元**：大統領府科学技術政策局（OSTP）

■ **ポイント**：

- 2021年1月のNSPM-33の要請に基づき、**研究機関において組織横断的かつ統一的に、研究セキュリティ・プログラム**を実施するため、標準化された要求事項を明らかにしたもの。
- 対象は「年間5000万ドルを超える額」を受領している研究機関。ドラフトと異なり、5000万ドルを判断するための参照資料を提供。
- 研究機関は、機関で実施する研究セキュリティ・プログラムが同ガイドラインの要件を満たしていることの証明が必要となる。
- 研究セキュリティ・プログラムの構成要素として以下の4項目が提示（ドラフト時と同じ内容）。研究機関ですでに実施している内容（NSFのトレーニングモジュール、商務省産業安全保障局、国務省国防防衛機管理総局のコンプラプログラム等）に沿った内容として再提示。

①サイバーセキュリティ　②海外渡航のセキュリティ
③研究セキュリティのトレーニング　④輸出管理のトレーニング


JULY 09, 2024

White House Office of Science and Technology Policy Releases Guidelines for Research Security Programs at Covered Institutions

OSTP › NEWS & UPDATES › REPORTS AND DOCUMENTS

Today, the White House Office of Science and Technology Policy issued guidelines to federal research agencies on research security programs at certain universities and federally-funded research institutions.

To address risks posed by strategic competitors to the U.S. research and development (R&D) enterprise, the Biden-Harris Administration is implementing several measures to improve research security while preserving the openness that has long enabled U.S. R&D leadership and without exacerbating xenophobia, prejudice, or discrimination.

大統領府HP、研究セキュリティプログラムに関するガイドラインを発表（20240709）

（参考）研究セキュリティ・プログラムの要件

- 「対象機関における研究セキュリティ・プログラムのガイドライン」の(II)では、研究セキュリティ・プログラムの要件を示してる。
- 対象機関の定義、研究セキュリティ・プログラムに含める内容（①サイバーセキュリティ、②海外渡航のセキュリティ、③研究セキュリティのトレーニング、④輸出管理のトレーニング）の要件を定めている。
- 研究機関は、機関で実施する研究セキュリティ・プログラムが上記要件を満たしていることの証明が求められる。

対象機関の定義 Definition of Covered Institution		• NSPM-33で定める「年間5,000万ドル以上、連邦政府から科学技術支援を受けている研究機関」。 • NSPM-33で定める対象研究機関 A) 高等教育機関、連邦政府出資研究開発センター（FFRDC）又は非営利研究機関 B) 年間5,000万ドル以上とは、 ① 最新版の the Survey of Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutionsに報告されている連邦政府の研究開発事業に参加し、提供されたされた研究開発費の3年間の平均金額 ② 最新版のthe Survey of Federal Funds for Research and Developmentに報告されているFFRDCに対する連邦政府の研究開発費の3年間の平均金額
プログラム必須内容	(1) サイバーセキュリティ	高等研究機関に対して、半導体・科学法で記載されているサイバーセキュリティ・リソース（NISTが公開しているもの）と一致する内容のプログラムを実施することの証明を求める。
	(2) 海外渡航時のセキュリティ	A) 海外渡航の安全に関する研修を定期的に実施し、証明 B) 安全保障上のリスクに関する研究開発費の条件に従い、組織的記録を含む出張報告プログラムの実施
	(3) 研究セキュリティのトレーニング	A) NSFの提供するトレーニングモジュールの修了の義務づけと証明
	(4) 輸出管理のトレーニング	A) 商務省産業安全保障局が実施する関連研修の受講を義務付と証明 B) ① 米国の輸出管理およびコンプライアンス要件の遵守と研修の証明 ② 外国のスポンサー、共同研究者、パートナーシップの審査要件の遵守と研修の証明

※「対象研究機関における研究セキュリティ・プログラムのガイドライン」より該当箇所を抜粋し、CRDSで一部編集。

英国 EPSRCのデューデリジェンスアプローチ

- 工学・物理化学研究会議（EPSRC）では公募審査プロセスの中でデューデリジェンスを実施。
- 応募者に対して、必要に応じた追加情報の提供やリスク緩和策の提示を求める。

■ **工学・物理科学研究会議（EPSRC）のデューデリジェンス**

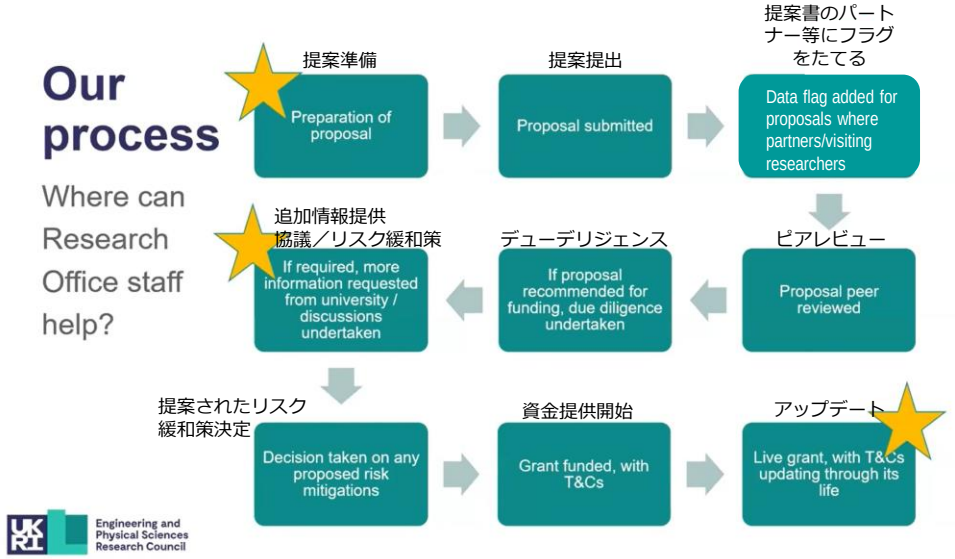
- プロジェクトの連携先や客員研究者に焦点を当てたアプローチを導入
- 応募者や大学には以下の確認を期待：
  - 申請書内の連携先や客員研究者が、**英国の武器禁輸や貿易制裁等と関与しているか**
  - 連携先の**研究機関が制裁対象国等の支配下**にないか

■ **高リスクとみなされる要素**

- **技術的観点：**輸出管理対象、国家安全保障・投資法の対象17分野、デュアルユース技術
- **申請時の以下の情報が欠如している場合：**
  - 協力環境やパートナーの影響、IP保護
  - 連携先や客員研究者の個人情報や機微情報へのアクセス
  - プロジェクトの参加人員の国外の大学等での活動
  - リスク緩和策

■ **デューデリジェンスに基づく対応**

- 潜在的な懸念や情報の欠如があった際に、**追加の協議、追加の情報提供、追加のリスク緩和措置、資金提供条件の追加**等を行う。



出典：Youtube「EPSRC Research Office Webinar 2023」を元にCRDSで和訳を追加

① **課題提案受付後：**審査開始前に、全ての申請書に対して「1．国際共同研究であるか？」、「2．”サンクションリスト”で指定のパートナーや訪問研究者が参加しているか？」を確認する簡単なアンケートを行い、参加有りの場合はマークする。

② **審査後：**採択候補課題で①でマークした提案には、原則「適性評価」を実施し、必要に応じて追加情報の提供を依頼し、リスクの低減策を策定する。

③ **採択決定：**リスクの低減策を評価し、付帯条件付採択とする。その付帯条件への対応状況により、付帯条件を調整する。

④ **研究開始後：**研究セキュリティの変化についてモニターを行う。

（参考）英国 国家安全保障・投資法

■ **国家安全保障・投資法（National Security and Investment Act）**

- ビジネス・エネルギー・産業戦略省(BEIS)は、2022年1月に外国からの投資・買収に関する通知を義務化する「国家安全保障・投資法」を施行。
- 英国の国家安全保障に影響を及ぼす可能性のある**外国企業や投資家による企業の合併や買収について、政府の審査・介入を強化**。
- 大学・研究機関を含む英国内の法人を対象とし、届け出を義務化する**17の機微な技術分野**を指定。

■ **大学・研究機関への影響**

- 委託研究、受託研究、研究職のスポンサー、研究テーマのスポンサー、知財のライセンス供与等の契約を通じて、大学・研究機関の支配権を得る場合、NSI法に基づく「取得」となる。
- 政府が合理的に安全保障上のリスクがあると判断する場合は「調査」の対象となる。
- 政府は大学・研究機関向けの**「ガイダンス」の提供**し、専門チームによる相談窓口である**研究協力アドバイスチーム (RCAT)** を設置し、理解促進を行っている。

届け出が必要な17技術分野

先端材料	国防
先端ロボティクス	エネルギー
AI	軍事・汎用品
原子力	量子技術
通信	衛星・宇宙技術
コンピュータハード	緊急サービスの供給
政府の主要な供給	合成生物学
暗号認証	輸送
データインフラ	

大学・研究機関の対応

大学・研究機関への外国の関与
- 委託研究・受託研究
- 研究者・講座の後援
- 研究テーマのスポンサー

契約を通じた**大学・研究機関の資産の支配権を取得**

↓

大学・研究機関が行うべき判断・対応
- 各事業の届出の要否
- 政府からの調査（Call on）への対応

←
- 「ガイダンス」
- 研究協力アドバイスチーム (RCAT)

豪州　研究費申請書のリスク評価・管理・緩和

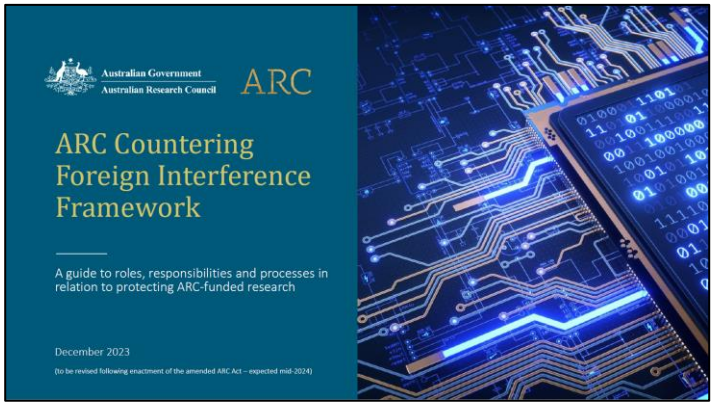
■ **タイトル：外国干渉対策(CFI)枠組み**
ARC Countering Foreign Interference Framework

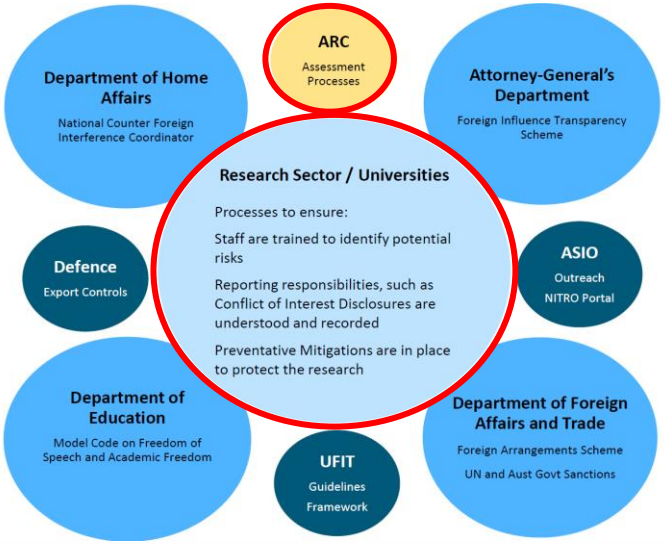
■ **発行年月：**2023年12月
■ **発行元：**オーストラリア研究会議（ARC）
■ **概要：**

- 豪州の資金配分機関であるオーストラリア研究会議（ARC）は、研究開発費(競争的資金等)の申請段階、申請時の内容変更、審査の段階において、**情報開示やデューデリジエンス、必要に応じたリスク緩和を行うための枠組み**を公開。
- ARC、大学、研究者、他の政府機関の役割と責任を含むプロセスを明確化。
- 本枠組みは、「大学や政府機関における潜在的な外国からの干渉リスクの特定・管理を支援する他のフレームワーク、ガイドライン、ツール、慣行を補完し、連携するもの」（右下図）

■ **助成ライフサイクルの各段階における評価**

- ARCは助成のライフサイクルの**あらゆる段階でリスク評価**
- 研究を守るための適切なリスク緩和を確保するよう、各段階で**リスクベース・アプローチ**がとられる。





出典：ARC「ARC Countering Foreign Interference Framework」
赤枠はCRDS出追記

豪州　ARC 外国干渉対策(CFI)枠組み

大学
申請書のレビュー

- 職員が全ての開示要件を認識し、潜在的なリスクを特定し報告するための訓練を受けるようにする
- 申請書に記載された参加者全員のCFIチェックを実施
- UFITガイドライン等で説明されたデューデリジエンスの実施
- 潜在的なリスクの特定、適切なリスク緩和策を講じていることの確認

→ARCへの申請書の提出

ARC
申請書の審査

- 申請書の情報と公開情報から潜在的なリスクを特定
- 申請が「重要技術*」にあたる場合、以下のリスクも検討

1. 現在または最近の海外からの財政支援
2. 外国人材プログラムへの現在または最近の関与、海外の大学との義務関係
3. 現在または最近の外国政府等との関係
4. 現在または最近の制裁対象との関係

- 必要に応じて**安全保障関連機関**に助言を求める
- 必要に応じ大学に追加の保証を要求

問題あり

安全保障関連機関
によるリスクレビュー

- 追加の情報を用いレビューを実施
- リスクが高ければARCに通知

追加の保証の要求

- 特定されたリスクに対して適切な緩和策が施されていることを大学がARCに保証

ARCによる追加情報の審査

- 追加情報によるレビュー
- 高リスクの場合、ARCに通知

問題なし

最終決定

- 潜在的なリスクが特定され、適切な緩和策が講じられているかを報告
- 資金提供の最終決定

*「重要技術」とは、豪州政府による「List of Critical Technologies in the National Interest」。2021年に首相内閣省(重要技術政策調整室)で作成され、2023年に産業・科学・資源省で更新。7分野として、先端製造・材料技術／AI技術／高度な情報通信技術／量子技術／自律システム／ロボット工学／測位、測時、センシング／バイオテクノロジー／クリーンエネルギーの生成と貯蔵技術が公表。

出典： ARC 「ARC Countering Foreign Interference Framework」（CRDSで和訳）

カナダ 研究費申請書のリスク評価、管理・緩和

- カナダの資金配分機関（3機関：Tri-agency）では、２つの政府方針に則ってリスク評価、管理・緩和を実施。

	「研究協力に関する国家安全保障ガイドライン」 (National Security Guidelines for Research Partnerships: NSGRP)	**「機微技術の研究と懸念される提携関係に関する方針」** (Policy on Sensitive Technology Research and Affiliations of Concern: STRAC policy)
リスク	• 研究プロジェクトの**連携先組織**のリスク	• **機微技術研究**における**指定研究機関**リストに掲載されいてる機関との関係
適用範囲	• 連邦政府の助成に基づく研究プログラムの**一部** • 民間部門との研究協力のある資金提供プログラムに適用	• 大学を対象とした連邦政府による研究費配分の**全部**
申請段階の要件	• 民間部門との連携がある場合 • 資金配分機関の研究費に申請する研究者 • 「リスク評価フォーム（Risk Assessment Form）」を記入・提出	• 申請書で役割を持つ研究者 • 「宣誓供述書（Attestation Form）」を記入・提出
助成期間中の要件	• 助成金受領者は、リスク評価フォームおよび決定通知書で特定されたリスクに対して緩和措置を実施。	• 助成金で支援されるプロジェクトに参画する研究者は、指定研究機関から資金または現物支援を受けることはできない。

出典：Implementation of the Policy on Sensitive Technology Research & Affiliations of Concern (STRAC)よりCRDSで作成

カナダ 研究費申請時のリスク評価、管理・緩和

- 「研究協力に関する国家安全保障ガイドライン」（NSGRP）に基づきリスクアセスメントレビューを実施。
- 資金配分機関が持つリスク評価委員会で、国家安全保障部門の評価の必要性が判断された場合、カナダ**公安省等の安全保障関連機関によってリスク評価が**なされる。

情報開示

研究費申請書
「リスク評価フォーム」
提出

- 申請者は**「リスク評価フォーム」**（右図）作成
- 「リスク評価フォーム」では、**①研究内容**（6問）、**②連携先**（4問）について質問

リスク評価

資金配分機関
審査

- リスク評価委員会
- 国家安全保障部門の評価の必要性の有無を判断し、安全保障部門に送付

リスク評価
不要

リスク評価 要

国家安全保障部門
審査

- **公安省、安全保障情報局、通信安全保障局**のいずれかによる審査
- 場合によってグローバル連携省等関係機関とも検討
- 審査結果を資金配分機関に戻す

ピアレビュー

- 技術メリットの審査
- リスク評価フォームはピアレビュー担当に共有されない

リスク管理

採択

- 技術メリット評価と安全保障評価の結果を通知
- 不採択申請者に対して、安全保障評価の結果について面談機会あり

研究開始

- **「リスク緩和計画」**（次頁）に基づいて研究実施

「リスク評価フォーム」


Innovation, Science and Economic Development Canada / Innovation, Sciences et Développement économique Canada

Protected When Completed

National Security Guidelines for Research Partnerships
Risk Assessment Form

Save As | Print | Reset

Family name of applicant: | Initial(s) of all given names of applicant: | Grant administering institution:

Introduction

The Risk Assessment Form is a tool to identify and assess potential risks that research partnerships may pose to Canada's national security as outlined in the National Security Guidelines for Research Partnerships and to develop effective mitigation measures.

In answering the Risk Assessment Form questions, you will provide information – to the best of your ability – that is specific to your proposed area of research and prospective research partner organizations. This information will be used to assess national security risks where the proposed research partnership could expose the research project to foreign interference, espionage or theft from foreign governments, militaries and other organizations, and also pose potential risks to the wider Canadian research enterprise.

For the purpose of the National Security Guidelines for Research Partnerships, a partner organization is any organization that plays an active role in the project and/or supports a research partnership through cash and/or in-kind contributions. Examples of a partner organization's role may include:

- Sharing in intellectual leadership or providing expertise;
- Active participation in research activities, and/or
- Application of research results and/or active participation in translating or mobilizing the knowledge produced to help achieve the desired outcomes of the project.

National security risks may be described as, but not limited to circumstances where there are potential instances of foreign interference, espionage, intellectual property theft or unauthorized knowledge transfer that:

- contribute to the advancement of military, security, and intelligence capabilities of states or groups that pose a threat to Canada; and/or
- disrupt the development of Canadian research and innovation, weaken the resiliency of critical infrastructure, or jeopardize the protection of sensitive data of Canadians.

The information collected will not be used to substantiate if you are compliant with any legislative or regulatory requirements that may apply to your proposed research project. The collection of this information will be used to assess the overall risk profile of your research project.

Who needs to complete the Risk Assessment Form?

Anyone can use the Risk Assessment Form to conduct due diligence when establishing and/or continuing partnerships with national, international and multinational partners.

This form may be required for specified federal research funding opportunities. You should consult the appropriate program literature associated with the funding opportunity to which you are applying to determine if you are required to submit a Risk Assessment Form with your grant application.

Depending on the specific funding opportunity, the "applicant" may be an individual, on behalf of any co-applicants, or may be a post-secondary or research institution.

What resources and tools may assist you?

You are encouraged to conduct open-source research to complete the Risk Assessment Form and to consult with your partner organization(s), where appropriate, to validate the information. For more information, consult the comprehensive guide Conducting Open Source Due Diligence for Safeguarding Research Partnerships.

Additional guidance and resources, including Public Safety Canada's Safeguarding Science Workshop and the Canadian Security Intelligence Service's threat briefing and checklist, that may assist in the completion of this form can be located on the Safeguarding Your Research portal.

ISED-ODEB3026 (2023/03), Page 1 of 8

Save As | Print | Reset

Canada

出典：Tri-agency guidance on the National Security Guidelines for Research Partnerships (NSGRP)、Safeguarding Your Research「Risk Assessment Review Process」を元にCRDSで作成

（参考）研究機関におけるリスク緩和策

- 特定されたリスクが現実化した場合の影響を軽減するために、適切な**リスク緩和計画**を作成する必要がある。
- リスク緩和策の実施にあたっては、**Risk-targetedな緩和策**を実施することで、オープンで協力的な研究パートナーシップを追求しながら、研究セキュリティを実現するものとする。

■ リスク緩和の方法

- トレーニングの実施
- カナダ政府、関係機関発行のガイダンスの採用
- データ管理計画
- サイバーセキュリティ計画
- 「必要に応じた」アクセス制限と内部プロトコル
- 機関内部での定期的な報告メカニズム

■ リスク緩和計画の内容

強力なチームの構築（体制構築）	• 研究プロジェクトの全参加者の経歴を確認。当該プロジェクトの研究目的との整合性を評価 • 潜在的な利益相反や提携関係を評価 • 機関内でリスクを議論。必要に応じて外部の専門家を招聘
連携先機関の研究目的（動機）の確認	• 連携先の研究目的（動機）が、自機関のものと合致するか • 連携先のガバナンス構造が透明であり、最終的な受益者が明確か • 他の研究者が当該連携先組織と良い関係を持った経験があるか • 連携先の活動、慣行が自機関の倫理と研究活動方針と合致するか
サイバーセキュリティとデータ管理	• サイバーセキュリティ、データ管理のトレーニングの受講 • サイバーセキュリティ、データ管理を連携先との間でも実施 • 海外渡航時のデバイス管理のプロトコルへの同意
研究成果の利用目的の合意	• 成果の発信の仕方（論文、学会、メディア、SNS等）の合意 • IPの潜在的価値の評価と保護 • 研究への協力者、連携先とが IP の取り扱い方法について合意 • 研究者および連携先の双方で研究結果の想定される用途を理解

カナダ 研究費申請時のリスク評価、管理・緩和

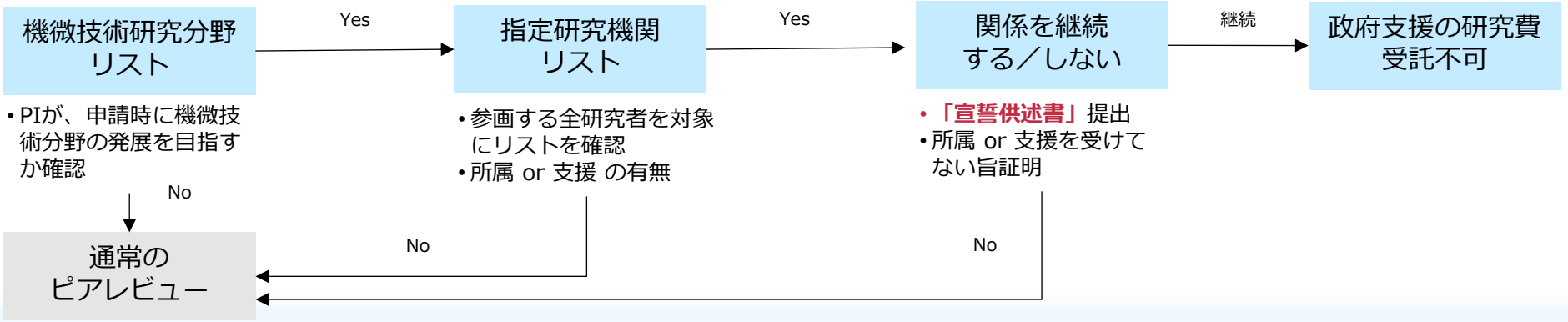
■ **タイトル：「機微技術の研究と懸念される提携に関する方針」**
（Policy on Sensitive Technology Research and Affiliations of Concern：STRAC）

■ **発行年月：**2024年1月

■ **概　要：**

- 2024年1月より、機微性の高い技術研究分野に携わる研究者は、カナダの**国家安全保障にリスクをもたらす可能性のある機関に所属または資金提供または現物による支援を受けている場合、研究助成を受けることができなくなった**。
- 機微性の高い技術分野として**「機微技術研究分野のリスト」**(15頁)、国家安全保障のリスクをもたらす可能性のある機関として**「指定研究機関のリスト」**(14頁)を公表。
- 大学を対象とした連邦政府による研究費配分に参画する研究チームのメンバーは、指定研究機関の所属および支援がない旨、「宣誓供述書（Attestation Form）」に記入し提出する。

■ **研究者の助成金申請時の新たな手順**：



出典： ISED 「Policy on Sensitive Technology Research and Affiliations of Concern」を元にCRDSで作成

アウトライン

諸外国における研究セキュリティの取組み
– 政府・資金配分機関によるリスク評価と大学への支援を中心に

1. 諸外国における研究セキュリティの取組み
2. リスク提示
3. リスク評価・リスク管理・緩和策
4. **意識啓発**
5. 政府等による大学・研究機関への支援
   - 相談窓口
   - 一元的な情報共有の仕組み（ポータルサイト等）
   - アカデミアと政府とのコミュニケーション
   - アカデミアと法執行機関・情報機関とのコミュニケーション

参考資料

4．意識啓発

- 研究コミュニティにおけるセキュリティ文化の意識醸成のため、**トレーニングプログラムの構築、モニタリングのモデル、ケーススタディの公開**などが行われている。
- 研究コミュニティにとって、なぜ研究セキュリティが重要か、なにが問題なのか、といった**目的意識の共有が強く意識**されている。
- 意識啓発は、研究者、研究管理者など研究コミュニティだけでなく、行政・資金配分機関職員も含め、研究開発に携わる全ての人を対象にし、**継続的な取組み**が重要。

トレーニング・プログラム

- 政府・資金配分機関が主導し、研究セキュリティ・トレーニングプログラム構築
- オンラインで公開し、誰もが受講可能

[事例]
- 米：NSFの研究セキュリティトレーニング
- 加：研究セキュリティトレーニング

モニタリング

- 大学・研究機関の研究セキュリティの取組みの成熟度(maturity)を自己評価するためのツール

[事例]
- 英：Trusted Research「評価フレームワークとユーザーガイド」
- 蘭：知識セキュリティの能力成熟度モデル

ケース・スタディ

- 研究者・研究機関が遭遇する具体的なシナリオ作成
- 研究セキュリティ侵害が、研究者、研究コミュニティに与える影響を紹介

[事例]
- 米：FBIが訴追事例をプレスリリースで公開
- 加：政府がオンラインで5つのシナリオ公開
- 豪：外国干渉の対策TF(UFIT)がオンラインで公開

その他（説明会・イベント）

- 法執行機関等による大学・研究機関への説明会

[事例]
- 米：FBI、DHSは大学でシンポジウムや説明会を開催し、アウトリーチ。

米国の研究セキュリティトレーニング

■ NSF職員向けトレーニング

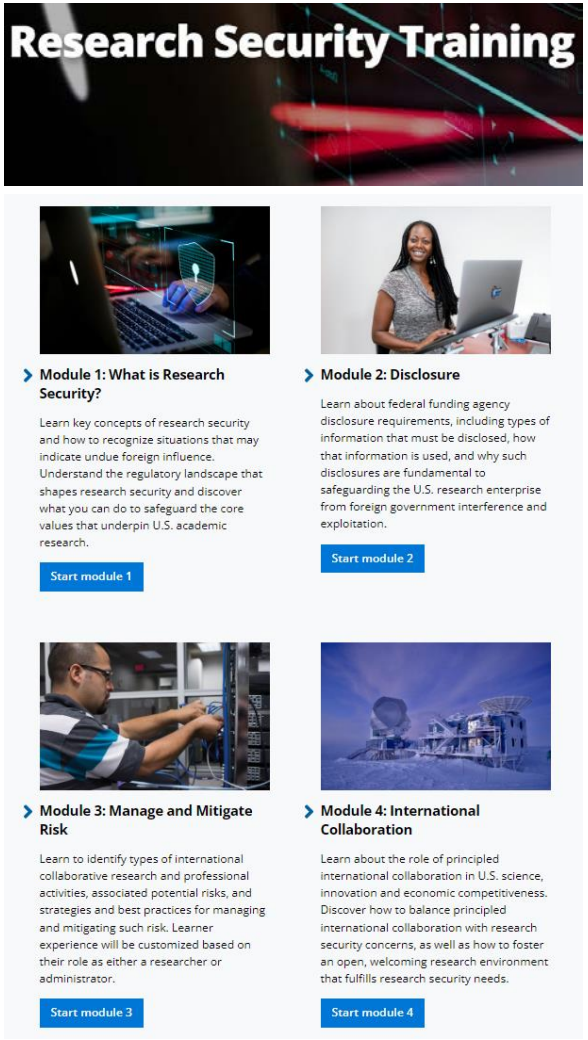
- NSF スタッフ向けに2 つのトレーニングコースが開発されている。

科学とセキュリティのトレーニング Part１	• NSFの開示ポリシーと外国政府人材募集プログラムに関する新しいポリシー • 受講義務：**全NSF職員と請負業者**、年1回
科学とセキュリティのトレーニング Part2	• POが助成前の情報のリスク評価をどのように処理すべきか • 助成後の情報を取り扱うための内部プロセスの実装について概説 • 受講義務：**NSFの全POと助成金管理者**

■ 研究コミュニティ向けトレーニング

- NSF、NIH、DOE、DODと連携し、トレーニングモジュールを開発。開発は公募で行い大学等にコンテンツの検討を行わせた（総額150万ドル、1件あたり50万ドル）。2024年1月に以下4つのコンテンツを**オンラインで公開**。
- 対象：**連邦政府の研究費の申請書に名前が記載される者**
- OSTP「研究セキュリティ・プログラムガイドライン」においてトレーニング受講と証明が必須。

モジュール 1	**研究セキュリティとは何か？** • 研究セキュリティの主要概念と不当な外国からの影響を示す可能性
モジュール 2	**情報開示の重要性** • 情報開示の項目、開示された情報の使用方法、外国政府干渉と情報開示の必要性
モジュール 3	**リスクの管理と緩和** • 国際共同研究及び海外での専門家活動の種類と潜在的なリスク
モジュール4	**国際協力の重要性** • 国際協力と研究セキュリティの懸念とのバランスをとる方法や戦略



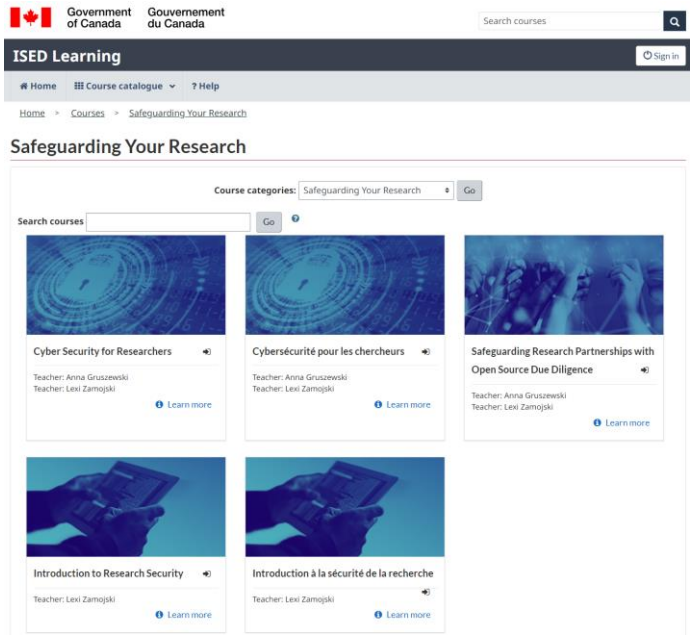
出典：NSF公開「研究セキュリティトレーニング」
https://new.nsf.gov/research-security/training

４．意識啓発

カナダの研究セキュリティトレーニング

- カナダ政府は、研究者に研究を保護するための知識とリソースを提供するため、3つのコースを開発。
- オンラインで公開し誰でも受講可能。各コースの所要時間は約 30 – 40 分

研究セキュリティ入門 	研究セキュリティがなぜ重要なのか、そして研究者とその仕事が研究セキュリティの理解を深める（言語：英仏） **[内容]** • 研究セキュリティがなぜ重要なのか • 研究者と研究活動において研究セキュリティの理解を深めることでなぜ利益を得るのか
サイバーセキュリティ 	第一線の研究者や学術管理者がどのようなサイバー セキュリティ対策を実施し、従うべきかを解説（言語：英仏） **[内容]** • サイバー脅威環境の概要 • 適切なサイバーセキュリティ慣行に関するアドバイス **[ゴール]** • 潜在的なサイバーセキュリティの課題に対して、十分な知識を下に意思決定できるようにするう
オープンソース・デューデリジェンス 	オープンで協力的な研究環境の重要性とオープンソースによるデューデリジェンス手法（言語：英語） **[内容]** • オープンソースのデューデリジェンス手法 • 研究協力先が実在するかを確認する方法 • 研究協力先の動機が明確であることを確認する方法 • 不当な干渉や影響の明白な潜在性がないことを確認する方法

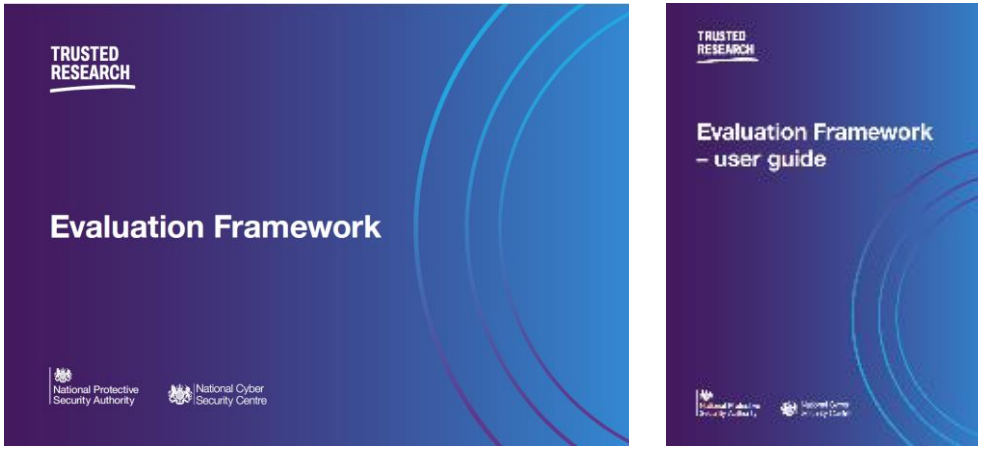


出典：カナダ政府「研究セキュリティトレーニングコース」
https://learning-apprentissage.ised-isde.canada.ca/course/index.php?categoryid=49&lang=en

英国 Trusted Research「評価フレームワークとユーザーガイド」

■ **タイトル：Trusted Research「評価フレームワークとユーザーガイド」**
■ **発行元：** NPSA／NCSC
■ **発行年：**2024年4月

■ **目的：**
- 大学・研究機関が、研究セキュリティの成熟度を自己評価するためのツール。NPSAのガイダンスを補完するために開発される。
- 研究セキュリティの成熟したアプローチの形成支援をすることを目的とする。



出典：Trusted Research「評価フレームワークとユーザーガイド」

- **フレームワークを採用することで、大学・研究機関が研究セキュリティに真摯に取り組んでいることを証明することに繋がる方法である。**
- **第三者機関による評価(監査や検査)に用いるものではない。**
- あらゆる研究分野、学術機関に適用できるが、特に研究集約型の機関や国家安全保障投資法の17分野のような機微な分野を扱う機関にとって重要となる。

■ **使い方**
- 自己評価開始の時点で、組織がフレームワークを採用したと見なすことができる。自組織の研究セキュリティの成熟度を測定し、モニタリングすることを約束したことを意味する。
- 研究セキュリティの実施に責任を持つ部門が使用(組織により異なる)
- 成熟度を正直に評価するための基礎、十分に安心できる部分と、より取り組む部分を強調する。
- 政府関係者(RCAT)とのやり取りの中でも用いることができる。

NPSA：国家保護安全保障局
NCSC：国家サイバーセキュリティセンター

英国 評価フレームワーク: カテゴリと評価レベル

- 7つのカテゴリを**3レベル（基礎（Foundation)、中程度(Intermediate)、成熟(Developed)）**で評価する。
- 現時点では英国のほとんどの機関が基礎レベル以下とみられるとされる。時間の経過とともに成熟度レベルが向上するよう、このフレームワークが役立つことを期待する、と記載される。

評価のカテゴリと検討事項

カテゴリ	検討事項
役員の承認とガバナンス	• 誰がリスク管理・対応の責任者か • どのように、どのような範囲のリスクを評価しているか • コンプライアンスの責任者や関連機関との窓口は誰か
コミュニケーション	• セキュリティ文化を根付かせるためのプログラムの実施 • 職員とのコミュニケーションとその到達度は
トレーニング	• トレーニングプログラムの運営、新規プログラムの要否は • 希望者への外部学習を支援しているか • 規制への理解を要する職員が必要な知識にアクセスできるか
組織のリスクと協力	• リスク管理のための適切な方針と手順があるか • 方針や手順は適用対象の人々に広く理解されているか • リスクの記録、リスクの調査能力を有するか
人材・プロセス・ガイダンス	• 外国渡航の支援を行っているか • コンプライアンス違反にどのように対処しているか • デューデリジエンスの責任者がおり十分訓練されているか
データと機器	• 研究インフラに十分なサイバーセキュリティ手順の有無 • 機密性の高い研究に組織のネットワークが利用されているか
インパクト測定	• 従業員を対象とした定期的なセキュリティ調査の実施と調査遂行能力の有無 • トレーニングの実施能力、高リスクの共同研究の記録、輸出管理記録等、職員の研究セキュリティへの関与の証明

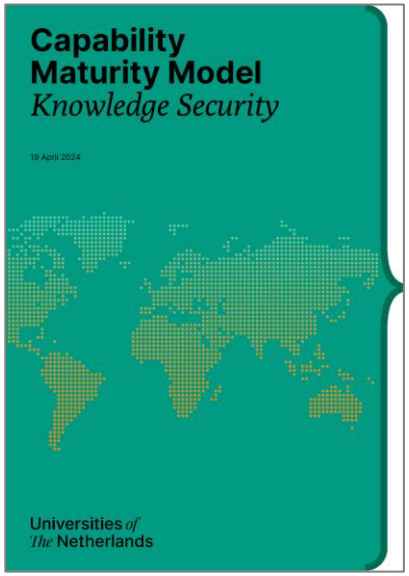
評価レベルと検討事項

レベル	検討事項
基礎 Foundation	• 基本的な研究セキュリティを確立するための最低限の基準 • 研究セキュリティの問題をカバーする既存の方針やプロセスがあることに重点
中程度 Inter-mediate	• 組織で懸念される特定の分野に関する対策。 • 独自の研究リスクマネジメントフレームワークの作成など
成熟 Developed	• 広範なセクターに対して優れたセキュリティ慣行のロールモデルを示す。他機関の検討の際のベンチ-マークとして機能。 • 職員アンケート等の結果、NPSAやNCSNとの関わりを通じて研究セキュリティに対する積極的な関与やセキュリティ文化を証明できる。

知識セキュリティの能力成熟度モデル（１）

- **タイトル：能力成熟度モデル（Capability Maturity Model）**
- **発行年月：**2024年4月
- **発行元：**オランダ大学協会（UNL）
- **対　象：**大学・研究機関
- **概　要：**

• オランダ政府が公表した「知識セキュリティガイドライン」に対して、**大学・研究機関が自機関の対応策の進捗（成熟度）を自己評価するためのモデル**。
• 外部機関による評価ではなく、自大学にとってどのレベルが望ましいかを分野ごとに評価することが重要である。
• 成熟度を測る項目は、ガバナンス、リスク評価、意識向上などの大項目で9つ（20小項目）、成熟度を測るレベルは**「初期（initial）」から「継続的な改善（Continuous improvement）」までで5段階**（詳細次頁）。



項目
概要
目的
レベル１
～
レベル５
情報源
参考資料

Risk assessment framework

Area	Risk assessment
Description	Risk assessment framework
Ambition	Knowledge security risks are identified for internal purposes to determine actual risk profiles, and relevant researchers and management are offered support and advice on knowledge security measures.
Level 1: initial	• There is no formal risk assessment that prescribes in which cases support and advice on knowledge security is needed. • Relevant staff members identify knowledge security risks on an ad-hoc basis.
Level 2: repeatable	• Relevant risks for knowledge security and corresponding advices are communicated to relevant staff. The communication includes an argumentation to clarify which elements have been relevant in drafting the advice.
Level 3: defined	• A risk assessment procedure and framework is defined. Due diligence is part of this risk assessment methodology. • Periodic reporting to higher management includes a description how the risk assessment methodology provides the information required to draft the advice.
Level 4: managed and measurable	• The university periodically evaluates the risk assessment methodology, and improves this if and when necessary. • Periodic reporting to higher management includes an evaluation of experiences with the risk assessment methodology.
Level 5: continuous improvement	• Support and advice to researchers, support staff and managers is in place and continuously evaluated and improved (if needed) in a cyclical process. • The risk assessment methodology is explained in training and awareness-raising activities.
Source / reference	VSNU Kader Kennisveiligheid, chapter 4; National Knowledge Security Guidelines (2022), chapter 5.

Vulnerability of research facilities

Area	Risk assessment
Description	Vulnerability of research facilities
Ambition	A vulnerability assessment of the most valuable research facilities is performed for internal purposes. Risk mitigating measures are taken to address these vulnerabilities when and where possible. Reporting of the vulnerabilities and measures is treated with confidentiality.
Level 1: initial	• Some faculties, institutes or service departments are aware of knowledge security risks in relation to their research facilities. • Mitigating measures are only proposed when the faculty is confronted with an (urgent) incident.
Level 2: repeatable	• Some knowledge security risks have been identified and described for some of the most valuable research facilities. • Risk mitigating measures are informally described.
Level 3: defined	• Roles and responsibilities are described and communicated. • An internal vulnerability assessment is conducted periodically in terms of knowledge security. These assessments are treated with confidentiality. • Periodic reporting informs higher management of the measures taken. These reports are treated with confidentiality.
Level 4: managed and measurable	• Knowledge security staff periodically discuss the vulnerabilities with managers of the research facilities and jointly propose adjustments if and when necessary. These discussions are treated with confidentiality. • The effects of these measures are periodically reported to higher management. These reports are treated with confidentiality.
Level 5: continuous improvement	• The overviews and the methods of the internal vulnerability assessments are evaluated and improved (if needed) in a cyclical process.
Source / reference	VSNU Kader Kennisveiligheid, chapter 4; National Knowledge Security Guidelines (2022), chapter 6.

出典：オランダ大学協会「能力成熟度モデル（Capability Maturity Model）」

4．意識啓発 – モニタリング

知識セキュリティの能力成熟度モデル（２）

- 20のサブカテゴリ（左表）を5段階（「初期（initial）」から「継続的な改善（Continuous improvement）」）のレベル（右表）で評価する。

評価のカテゴリと検討事項

カテゴリ	検討事項
学術の価値	• 学術の価値
	• オープン・サイエンス
	• 倫理
	• 包摂性と差別
ガバナンスとフレーム	• ガバナンス・責任・プロセス
	• 知識セキュリティ方針
	• 導入プログラム
法制度（制裁、輸出管理）	• 法制度と監督
リスク評価	• リスク評価フレームワーク
	• 研究施設の脆弱性
リスク管理	• 安全保障に配慮したパートナーシップ、資金、博士課程学生、客員研究員の受入れ
	• 関連する安全、セキュリティリスクの管理
トレーニング、意識向上	• スタッフと管理職のトレーニング
	• コミュニケーション計画
	• 出張に関するリスク認識と対策
国際的連携、調達、契約	• 国際化
	• 研究協力
	• 教育協力
人事	• 採用
サイバーセキュリティ	• サイバーセキュリティ

評価レベルと検討事項

レベル		検討事項
1	初期 Initial	• 対策が規定されていない、部分的にしか規定されていない、一貫性のない方法で実施 • 個人への依存度が高い
2	繰り返し Repeatable	• 体系的かつ一貫した方法対策が実行 • ただし正式な方法が確立していない
3	定義（規定される） Defined	• 対策が文書化され、構造化された正式な方法で実行 • 対策の実行が証明され、試験され効果が検証されている • 定期的報告（年次報告書や会議等）を行い、知識セキュリティに関連する戦略的意思決定に繋がる
4	管理され評価が可能 Managed and measurable	• 対策の有効性が定期的に評価（機関ごと）され改善され、文書化 • 定期的報告（年次報告書や会議等）で知識セキュリティ方針の実施の有効性を報告
5	継続的な改善 Continuous improvement	• 学内統一の知識セキュリティプログラムによって、継続的かつ効果的な戦略的管理、リスクによる問題が解決される。 • PDCAサイクルの実施

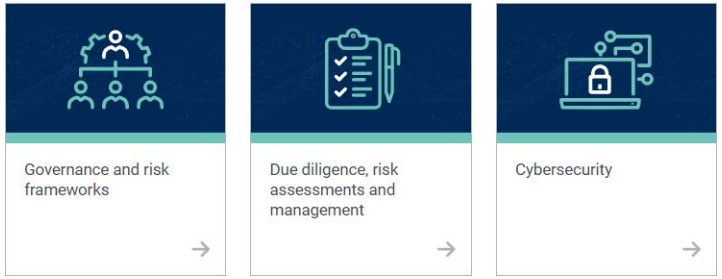
出典：オランダ大学協会「能力成熟度モデル（Capability Maturity Model）」

4．意識啓発 – ケーススタディ

- 大学・研究機関の具体的なシナリオに沿った事例（ケーススタディ）を例示。
- ポータルサイトなどのオンラインで公開し、研究コミュニティが閲覧可能。

Case studies

The following illustrative case studies demonstrate how actions taken by universities can help to mitigate foreign interference risks. These examples are intended to demonstrate the nature of potential risks and to guide universities in their response. The approaches taken by universities in these examples may not be applicable in their entirety to all situations and circumstances.



出典：豪教育省「Guidelines to counter foreign interference in the Australian university sector」

- ガバナンスとリスクフレームワーク：5ケーススタディ
- デューデリジェンス、リスク管理：3ケーススタディ
- サイバーセキュリティ：1ケーススタディ
- 国際的教育活動：3ケーススタディ

Scenario 1 - Cyber Security and Good Hygiene/Safe Practices

Kate is a professor and researcher who is preparing to take a three-week vacation to visit her family in another country. A long-time university colleague, who is now the vice-dean of a university in that country, has invited Kate to give a lecture on her work to a group of postgraduates at the university during her visit. Prior to departure, Kate downloaded remote access software onto her computer to access files stored on her home university's network while abroad, including a research project that has not yet been published. Once on site, she remotely accessed her account from a state-sponsored university computer, where she downloaded information to prepare for her speaking engagement, and then delivered the lecture.

出典：カナダ政府「Safeguarding Your Research」ウェブサイト

- シナリオ1 - サイバー セキュリティ
- シナリオ2 - 外国の人材採用プログラムへの参加
- シナリオ3 - 内部脅威と研究情報の盗取
- シナリオ4 - 定められた手順に従わない
- シナリオ5 - セキュリティと旅行

アウトライン

諸外国における研究セキュリティの取組み
– 政府・資金配分機関によるリスク評価と大学への支援を中心に

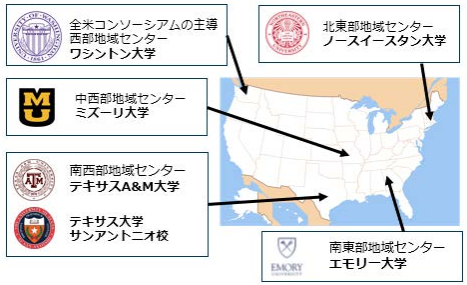
1. 諸外国における研究セキュリティの取組み
2. リスク提示
3. リスク評価・リスク管理・緩和策
4. 意識啓発
5. **政府等による大学・研究機関への支援**
   - 相談窓口
   - 一元的な情報共有の仕組み（ポータルサイト等）
   - アカデミアと政府とのコミュニケーション
   - アカデミアと法執行機関・情報機関とのコミュニケーション

参考資料

5．大学への支援 - 相談窓口

- 大学・研究機関に対する専門的知識の提供、助言、情報共有のための相談窓口を設置（詳細は参考資料）。

SECUREセンター



出典：公開情報元にCRDS 作成

- 運営：**大学（資金NSF）**
- 場所：全国6大学
- 人員：－
- 規模：6,700万ドル（5年）
- 機能：
  - **情報共有**：共有ツール、ベストプラクティス、トレーニング提供
  - **分析**：情報収集、データ編集、保存、分析ツール・技術開発

研究協力アドバイスチーム(RCAT)

Research Collaboration Advice Team

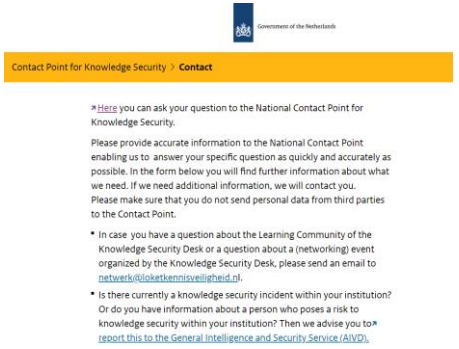
- 運営：**DSIT**
- 場所：全国5カ所
- 人員： 15名スタッフ、12名アドバイザー
- 国際共同研究における安全保障上のリスク関する公的助言窓口
- 国際研究活動における規制、リスク管理、政府との協力等助言

研究セキュリティセンター

出典：公開情報元にCRDS 作成

- 運営：**公安省**
- 場所：全国5カ所
- 人員：6名（各都市）
- 政府方針の情報提供
- 地域のアドバイザーネットワーク
- 政府へのアクセス支援

政府連絡窓口


Government of the Netherlands

Contact Point for Knowledge Security > **Contact**

*Here you can ask your question to the National Contact Point for Knowledge Security.

Please provide accurate information to the National Contact Point enabling us to answer your specific question as quickly and accurately as possible. In the form below you will find further information about what we need. If we need additional information, we will contact you. Please make sure that you do not send personal data from third parties to the Contact Point.

* In case you have a question about the Learning Community of the Knowledge Security Desk or a question about a (networking) event organized by the Knowledge Security Desk, please send an email to netwerk@loketkennisveiligheid.nl.
* Is there currently a knowledge security incident within your institution? Or do you have information about a person who poses a risk to knowledge security within your institution? Then we advise you to* report this to the General Intelligence and Security Service (AIVD).

出典：オランダ政府「Knowledge Security」ウェブサイト

- 運営：**オランダ政府**
- 場所：オンライン窓口
- 人員：－
- 機能：専門知識と助言を提供。関係省庁（内務省、外務省、防衛省、法務省、教育文化科学省、経済省等）と繋がり、ワンストップ窓口
- 過去の問合せ380件以上（中国、イラン、ロシア、中東との国際協力関係）

NSF: 国立科学財団
DSIT: 科学技術イノベーション省

5．大学への支援 – 一元的な情報共有の仕組み

- 研究セキュリティの関連情報は、省庁をまたぐ情報を扱うことから、情報を一元的にまとめているポータルサイトを開設し情報共有している。
- ユーザーインターフェイスに配慮したデザイン。

Safeguarding Science

出典：ODNI「Safeguarding Science」ウェブサイト

- 運営：国家情報長官室（ODNI）
- 大統領府、関係省庁の政策文書
- ガイドライン
- リスク評価・軽減
- 諸外国の動向
- 関係機関のガイダンス　　等

Safeguarding Your Research

出典：カナダ政府「Safeguarding Your Research」ウェブサイト

- 運営：カナダ政府が運営
- 背景やリスクの提示
- ガイドライン
- 各種ツール
  - デューデリジェンス・ガイダンス
  - ケーススタディ
  - 輸出管理関連法令
  - サイバーセキュリティ
  - 国防省、カナダ軍からの情報
  - トレーニングコース
  - 諸外国の動向

Knowledge Security

出典：オランダ政府「Knowledge Security」ウェブサイト

- 運営：オランダ政府
- 知識セキュリティとは
- リスク分析
- ツールとフレームワーク
- アカデミック・コア・バリュー
- 法的枠組み
- サイバーセキュリティ
- 国際連携
- 人事政策
- Q&A

5．大学への支援 – アカデミアと政府とのコミュニケーション

- 政府、資金配分機関、大学・研究機関で情報共有、意見交換できる枠組みが設置。ガイドライン策定等で機能。
- 大学協会、科学アカデミー、研究マネジメント人材の団体などが、政府の取組みに意見・提言を発表。

政府機関・資金配分機関、大学協会等の中間団体、大学の研究管理部門によるネットワーク（公式／非公式）（詳細 参考資料）

科学技術安全保障円卓会議（National Science, Technology, and Security Roundtable）（詳細 参考資料）

- 設立： 2020年
- 目的・機能：
  - 「2020年度国防権限法」（§6484）に基づき全米アカデミーズ（NAS）に設置。
  - 法執行機関・情報機関のコミュニティと産業界および学術研究コミュニティの代表者の意見交換の場
  - これまでに13回開催（2024.3時点）

- 大学協会が研究セキュリティに関する政策提言を発表。最近では、研究セキュリティ人材やリソースについて提言。
- **Russell Group**, “Research Security: A Shared Responsibility”（2024.9.10）
- **英国大学協会（UUK）**, “Opportunity, growth and partnership: A blueprint for change from the UK's universities”（2024.9.30）

大学外国干渉タスクフォース(UFIT)

- 設立：2019年
- 目的・機能：
  - 政府と大学協会（Group of 8, Universities Australia）が共同で設置
  - 外国の干渉リスクに対する防衛を強化が目的
  - UFITガイドライン作成主導

大学協会（Group of 8）：

- ガイドライン作成でも大学協会が共同議長
- 政府の外国干渉対策や輸出管理に関する政策に対してコメントを公表。

カナダ政府 – 大学ワーキンググループ（詳細 参考資料）

- 設立: 2018年
- 目的・機能：
  - セキュリティリスクを緩和が目的
  - カナダの研究データと知財を保護するベストプラクティスを共有
  - リスク緩和ツールやガイドライン作成・開発の作業
  - 政府と大学との間で情報共有、意見交換の場として機能
- 構成員：カナダ政府、資金配分機関、大学コミュニティ

5．大学への支援 – アカデミアと法執行機関・情報機関とのコミュニケーション

- 政府-資金配分機関-大学・研究機関によるコミュニケーションの枠組みが設置。
- 大学協会、科学アカデミー、研究マネジメント人材の団体などが、政府の取組に意見・提言を発表。

連邦捜査局（FBI）

- 高等教育機関を対象にしたアカデミック・サミットや地域の向けの会議・イベントを開催し意識啓発（2018-2019）
- **アカデミック・リエゾン・プログラム**：FBIと大学の窓口。研究環境に関する研修を提供。

国土安全保障省（DHS）

- **国土安全保障捜査局（HSI）：**高等教育を情報収集の場として利用する外国組織の米国における事例を調査
- **DHS Project Shield America、Project Campus Sentinel**：高等教育機関へのブリーフィング実施

- 英国保安局（MI5）にある**国家保護セキュリティ局（NPSA, 旧CPNI）**が研究セキュリティの取組を主導。重要インフラ保護の一環としてTrusted Researchのキャンペーンを展開（2019）
- オリバー・ダウデン副首相（当時）は、英国24大学の副学長を招き、MI5長官と国家サイバーセキュリティセンター（NCSC）最高責任者によるセキュリティブリーフィングを実施（2024.4）

- **オーストラリア保安情報機構（ASIO）**が国全体の外国干渉対策の一環として教育・研究分野の対策にも協力
- 議会の情報・安全保障委員会による調査に対して大学等が協力し外国干渉に関する事例を提出

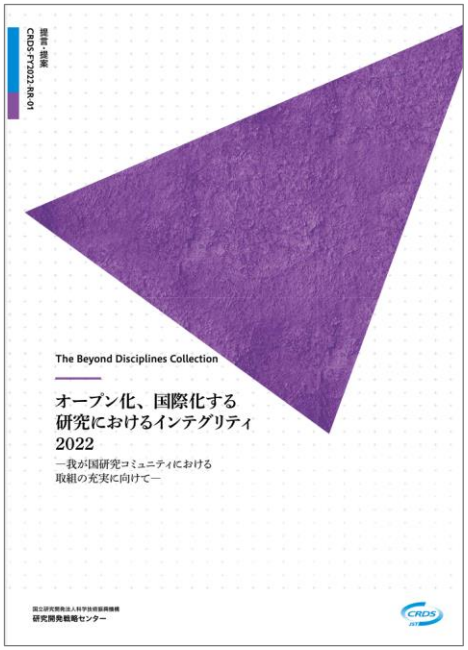
カナダ公安省

- **「科学を守るイニシアティブ（Safeguarding Science Initiative）」**：オープンサイエンスと国際協力とセキュリティの確保にむけた公安省のイニシアチブ。
  - ワークショップ開催による意識啓発
  - 研究セキュリティーセンターの所管
  - トレーニングモジュールの開発
- 「カナダ政府 – 大学ワーキンググループ」にも構成員として参加

参考資料

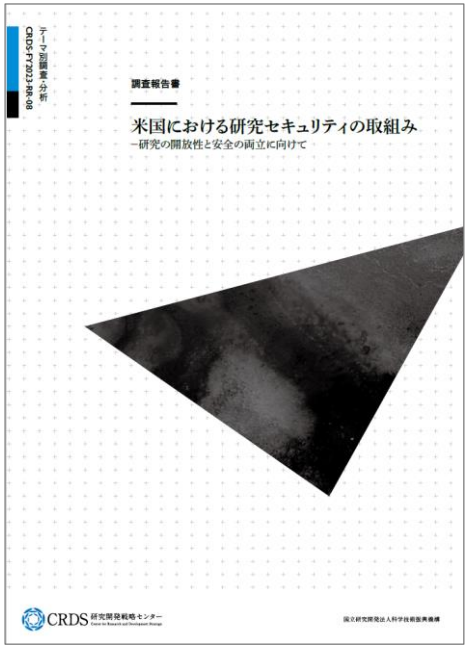
研究インテグリティ・研究セキュリティに関するCRDS報告書

「オープン化、国際化する研究におけるインテグリティ」（2020年10月）



「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年5月）

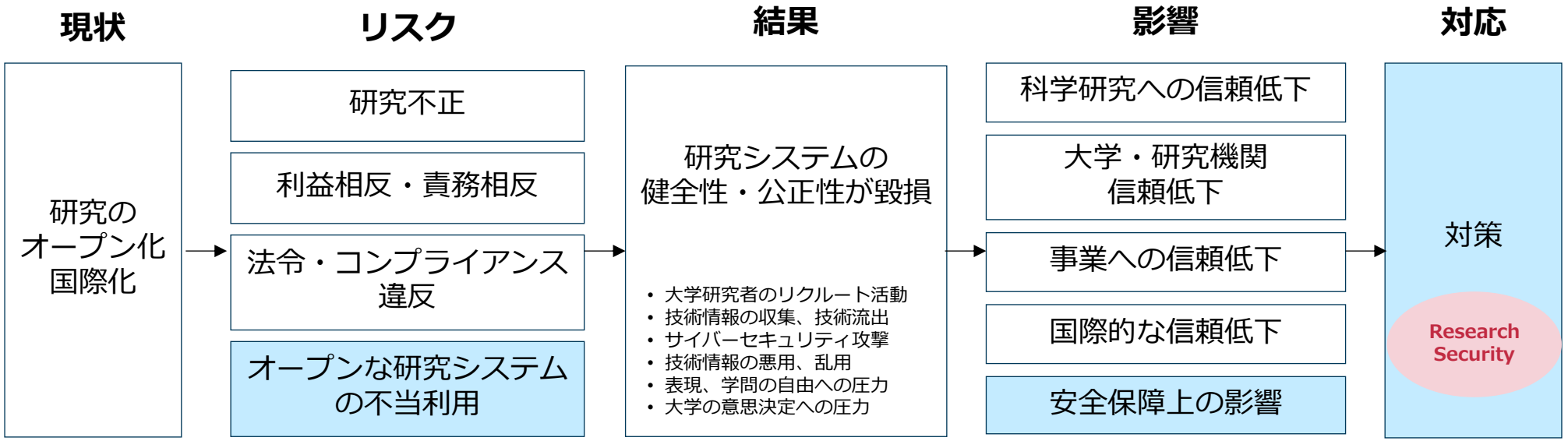
「日本語仮訳：グローバルな研究エコシステムにおけるインテグリティとセキュリティ OECD 科学技術産業ポリシーペーパー（130号）」（2022年11月）



「米国における研究セキュリティの取組み－研究の開放性と安全の両立に向けて」（2024年3月）

オープンな研究システムの不当利用への対応

- 研究のオープン化、国際化の進展に伴い、研究不正や利益相反と併せてオープンな研究システムの不当利用によるリスクが顕在化。
- 研究システムの不当利用によって、研究の健全性・公正性が毀損される。大学・研究機関、研究者、研究事業の信頼低下を招くと同時に**安全保障上の影響**が生じることがある。
- **「研究セキュリティ」は、オープンな研究システムの不当利用への対応**として位置づけられる。
- 活力ある大学・研究機関の研究システムを維持するために「研究セキュリティ」が重要とされる。



研究活動における原則

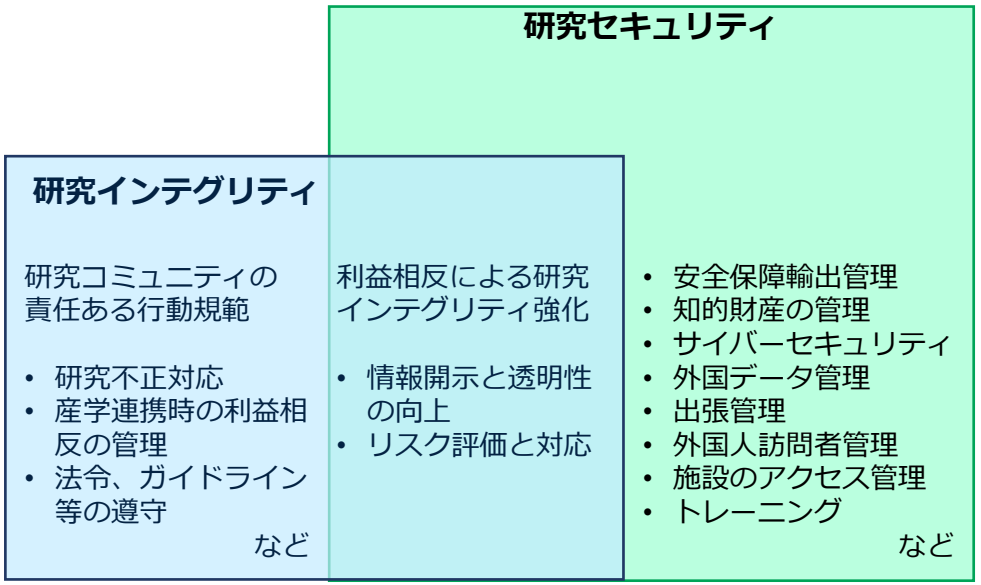
- 研究セキュリティの議論にあたっては、研究の開放性の他、**研究活動における一般的な原則（学問の自由、研究の公正、表現の自由、客観性、公正性、透明性、公平性、説明責任）が前提**に有ることが確認されている。
- 加えて、研究セキュリティの取組によって、**差別的取扱が行われない**こと、研究活動、研究者、研究機関に対して**過度の負担や不必要な損害を与えないこと**が確認されている。

米	英	豪	カナダ	EU	オランダ
					
•基盤的研究の開放性：基盤的研究の成果には可能な限り最大限に制限をかけない（NSDD-189） •「科学力の強さのためには、創造性を確保できる研究環境が必要。自由にアイディアを交換できる環境の確保」(JASON「基盤的研究の安全保障」(2019)) •少数民族や人種的マイノリティへの差別的な扱いを行わない(NSPM-33ガイダンス)	研究における潜在的リスクを説明しつつ、研究の国際関係の発展・維持が英国の研究とイノベーション成功の鍵である、と説明 （「Trusted Research Guidance for Academia」（2019））	豪州の大学の世界的な研究業績は国際化と開放性に基づく。大学の自治、学問の自由を基盤とする国際的連携は世界中の優秀な頭脳との知識の共有と発展を促進すると言及。 （UFIT「豪大学部門に対する外国の干渉に対抗するためのガイドライン」(2019)」	カナダの研究エコシステムの根底にある基本原則 •学問の自由 •機関の自治 •表現の自由 •公平性、多様性、包摂性 •研究の公共性 •透明性 •インテグリティ（誠実性） •連携 （カナダ政府「国際研究協力に対する国家安全保障ガイドライン」）	普遍的的権利、公共財である学問の自由 •高等教育機関自治 •学問の自由とインテグリティ •学生および教職員の参加 •高等教育に対する公的責任および高等教育に対する公的責任 （欧州委「Tackling R&I foreign interference」）	学術の中核的価値(Academic Core Value) •学問の自由 •研究の公正性 •オープンサイエンス •科学における倫理 •包摂性と無差別 （オランダ政府「National knowledge security guidelines」）

研究インテグリティと研究セキュリティ

- 研究インテグリティは、一般的に研究活動における研究コミュニティの責任ある行動を通して研究環境の健全性・公正性を確保する行動規範を表す。
- 研究システムの健全性・公正性が毀損されうるリスクから研究および研究コミュニティを保護する手段・対策として、**「研究セキュリティ」「Trusted Research」「Knowledge Security」**などが使われる。

研究インテグリティと研究セキュリティ



研究システムの不当利用への対応を表す言葉

	Research Security
	Trusted Research
	Countering Foreign Interference
	Research Security
	Knowledge Security
	研究インテグリティ*

*日本では研究システムの不当利用への対応を表す言葉として「研究インテグリティ」の解釈を拡大し運用している。

研究インテグリティと研究セキュリティ

	米	英	豪	カナダ	G7	オランダ
オープンな研究システムの不当な利用への対応	**Research Security** 研究セキュリティとは、国家又は経済の安全保障を損なう研究開発の不正利用を目的とした行為、研究インテグリティの侵害に類する行為、そして外国政府からの不当な干渉から研究機関を保護することである。 （NSPM-33）	**Trusted Research** 英国の知的財産、機密性の高い研究・人材・インフラを、敵対的なアクターによる干渉の結果として発生する潜在的な盗取、操作、搾取から保護することを意味する研究・イノベーション分野の用語」 (UKRI)	**Countering Foreign Interference** 外国からの干渉に対する意識を高めるためにリスクに晒されているセクターに関与する。リスク軽減戦略を通じて豪州社会の回復力を構築する、外国の干渉活動から直接防御するために政府機関を調整する、違法行為の取り締まり (ASIO)	**Research Security** 研究セキュリティとは、不要なアクセス、妨害、窃盗によって研究に起こりうるリスクを特定する能力及びこれらを最小限に抑え、科学的研究や発見の一部であるインプット、プロセス、および製品を保護する対策を指す。 （Safeguarding Your Research）	**Research Security** 研究セキュリティとは、経済的、戦略的、および/もしくは、国家および国際的な安全保障リスクをもたらす行為者や行動から研究コミュニティを保護するための行動が含まれる。特に研究に対する不当な影響、干渉、不正流用、国家・軍・非国家主体・犯罪組織によるアイディア・研究成果・知財の盗取などのリスクが関連する。	**Knowledge security** 機密情報や技術の望ましくない移転を防ぐこと。移転がオランダの国家安全保障に影響を与えることを防ぐこと。加えて知識の安全保障とは、国家や国が教育や研究に及ぼす秘密裏に実施される行為の影響に対抗すること。 （「National knowledge security guidelines」）
研究インテグリティ	研究活動の提案、実施、評価、報告において、客観性、公正性、透明性、公平性、説明責任、スチュワードシップなどの専門的な価値観や原則を遵守すること (NSPM-33ガイダンス)	研究プロセスのあらゆる側面で信頼を促進する方法で研究を実施すること：研究成果公表・研究の手順、データ収集・成果利用の公正な実施、研究規範や手順の遵守など (UKRI)	豪州の研究コミュニティが研究に対して責任を持って倫理的に誠実に実施されることを期待 （ARC）	研究者は知識の探求と普及において、誠実、説明責任、オープン、公正に最善の研究慣行に従うよう努めなければならない、という行動指針 （Model Policy on Scientific Integrity）	研究インテグリティとは、研究ミュニティを支える専門的な価値、原則、好事例を遵守することである。これらは公平でイノベーティブで開放的で信頼できる研究環境の基盤を形成する。（研究セキュリティとインテグリティにおけるG7共通の価値観と原則）	研究活動における誠実性、慎重性、透明性、独立性、責任などの5つの原則 (Netherlands Code of Conduct for Research Integrity)

米国 NSF支援によるSECUREセンター

- 米国では、大学・研究機関の研究セキュリティを支援するための新たな情報共有組織として、**SECUREセンター**を設置（2024年7月）。

■ **背景と目的**
- 「半導体・科学法」に基づき、国立科学財団（NSF）において、研究コミュニティが研究セキュリティ上のリスクを特定・緩和するための情報共有機関を設置する。
- 研究セキュリティリスクに関する情報共有、コミュニティへの研究セキュリティトレーニングの提供、研究コミュニティと政府の資金提供機関との協力を強化する。

■ **SECUREセンター**
- ワシントン大学が主導し、全米各地の6大学が地域センターとして機能。

■ **SECURE Analytics**
- SECUREセンターで利用される専門知識を提供する
- テキサスA&M大学が主導し、フーバー研究所、Parallaxが協力。

■ **予算規模：**5年間で6,700万ドル（うち5,000万ドルをワシントン大学に、1,700万ドルをテキサスA&M大学）

図 SECURE Centerの場所

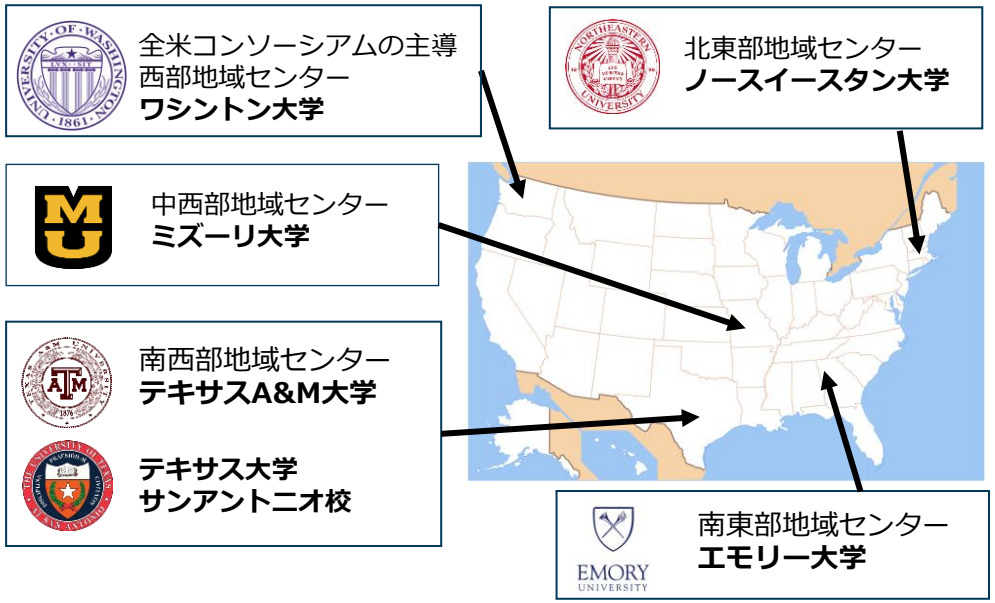
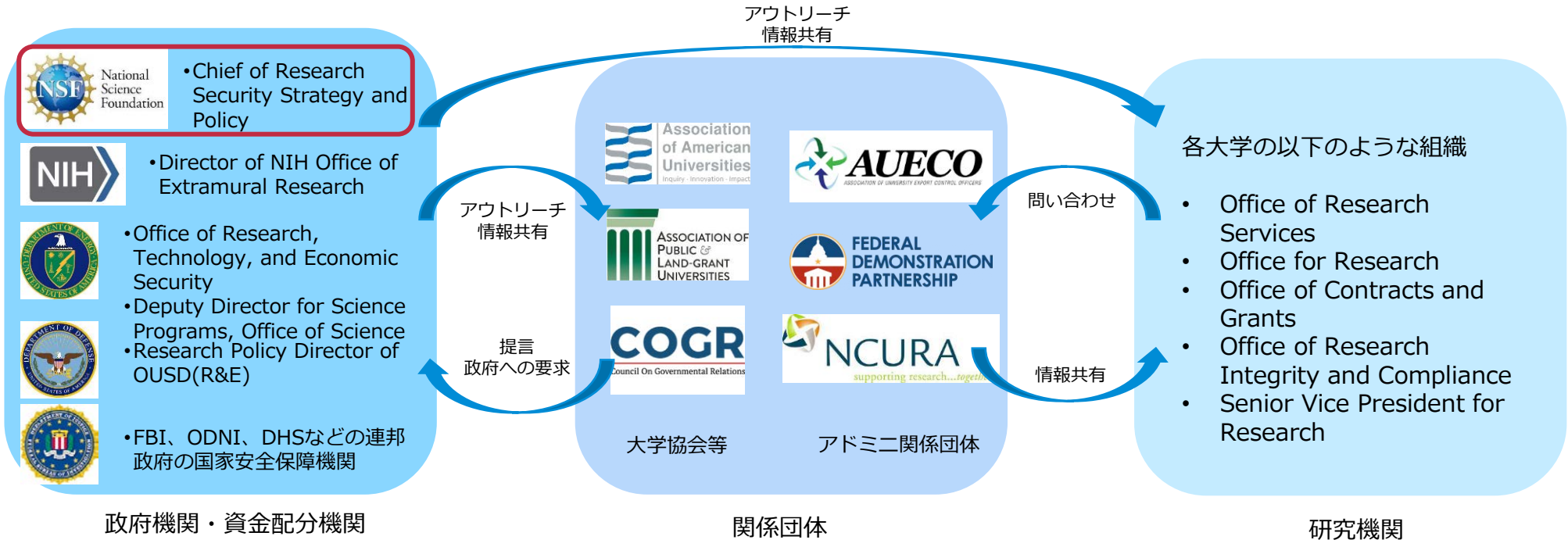


表 SECURE Analyticsの主な活動や機能

• 研究コミュニティが、研究成果や知財に関する外国組織の不適切な行動を特定できるようにするための情報センター	• 脅威の情報と保護・対応の取組みの教訓を研究コミュニティと共有
• 研究セキュリティインシデントの情報収集、データ編集、保存、分析ツール・技術開発	• 研究者やスタッフにセキュリティリスクと対応に関するトレーニングと支援の提供

米国の関係者によるネットワーク構築と情報共有の仕組み

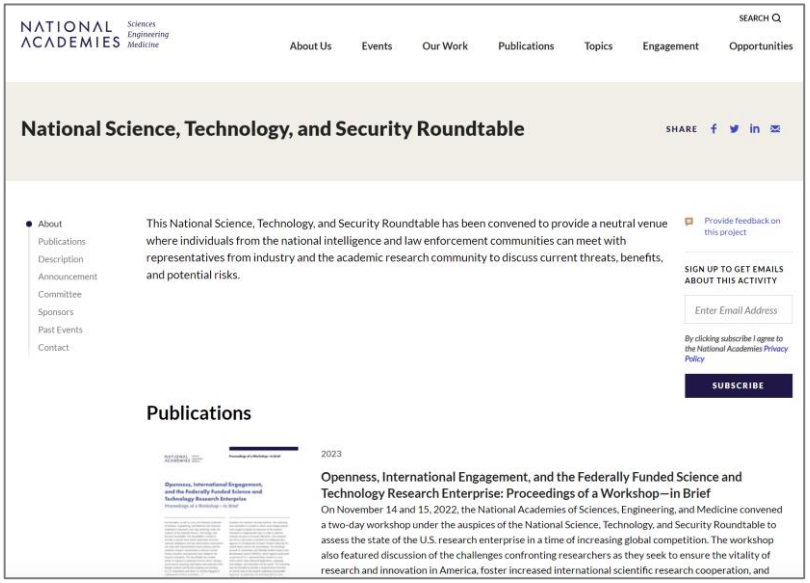
- NSFを中心に、政府機関、関係団体、研究機関間で情報共有・調整が行われている。
- 政府機関間、政府機関と関係機関は月に1-2回程度の公式・非公式の会合を実施し、透明性高く議論を継続。
- 政策文書において不明確な点がある場合は、中間にある関係団体からコメントが提示される。
- 大学・研究機関が実務的判断に迷う際には、関係団体機関へ問い合わせ、類似事例に基づく対応を実施している。
- 研究セキュリティという新たな課題に対して情報共有を行うエコシステムが形成されつつある。



米国の関係者によるネットワーク構築と情報共有の仕組み

■ **科学技術安全保障円卓会議（National Science, Technology, and Security Roundtable）**

- **「2020年度国防権限法」（§6484）**に基づき設置。
- 研究コミュニティとそのほかのセクターの間での情報共有や意見交換を公式に行える場の一つとして、**全米アカデミーズに設置**されている。
- 国家情報機関および法執行機関のコミュニティの個人と産業界および学術研究コミュニティの代表者が会し、オープンな研究と国際協力に対する現在の脅威、利益、および潜在的なリスクについて話し合うことができる中立的な場として機能。
- 代表的な支援機関には国防総省、国立衛生研究所が参画。
- これまでに13回開催されている（2024年3月時点）。



出典：National Science, Technology, and Security Roundtableウェブサイト

英国 DSITの研究協力アドバイスチーム(RCAT)

■ **名　称：**研究協力アドバイスチーム
（Research Collaboration Advice Team：RCAT）

Research Collaboration Advice Team

■ **設　立：**2022年3月

■ **目的・機能：**
- DSITに国際共同研究における安全保障上のリスクについて公的な助言(official advice)を行う窓口として設置
- 国際研究協力における国家安全保障上の懸念に対応するため、研究機関に信頼できる助言を提供する
- 研究文化の段階的な変化を支援、Trusted Researchに対する理解と応用を深める研究機関と協力
- 研究機関の抱える問題について情報を収集・共有し、業界と政府の理解を助ける
- 研究者が①国際的な活動の際適用される規制、②敵対者の戦術、これが研究者や研究に及ぼす危険性、そのリスクの管理、③リスクへの対処、政府との協力への理解の深化
- 学術機関による、国家安全保障にとっての研究基盤の重要性を反映したポリシーの設計と実施の支援

■ **RCATの国内拠点：**
バーミンガム、カーディフ、エディンバラ、ロンドン、サルフォード(15名のスタッフと12名のアドバイザー)

■ **協力相手：**
- (政府関連)　NPSA, NCSC, UKRI等
- (学術コミュニティ)　UUK等

■ **成果と評価：**
- 研究機関や研究室が直面する問題について350件超の助言を実施（右表）。
- RCATが実施する業界調査に対して90件の回答が集まる。
- Russell Groupでは、ポリシーブリーフ”Research Security”の中で、RCATを「迅速な情報共有による既存の法律でカバーされない新興の脅威に対応」する注目すべき取組みとして評価。

RCATの相談対応実績（2022-2023進捗報告書より）

輸出管理	32%
個別の問題	23%
国家安全保障投資法	18%
組織のガバナンスと研究セキュリティポリシー	15%
アカデミックテクノロジー承認スキーム	9%

カナダ政府 – 大学ワーキンググループ

■ **名　称：**カナダ政府 – 大学ワーキンググループ
（the Government of Canada – Universities Working Group）

■ **設立年：**2018年

■ **目的・機能：**

- 研究を保護し、カナダ国民の利益を最大化する方法でオープンで協力的な研究を推進するために設立
- 行政組織と研究コミュニティが継続的な関与していくために、定期的に連絡を取り合う場として機能
- カナダ政府、大学コミュニティ、およびそれらを代表する協会のメンバーが参画
- 研究セキュリティ上のリスクを特定、リスク緩和ツールやガイドライン作成・開発の作業にも取り組んでいる

カナダ政府 – 大学ワーキンググループ メンバー

（行政機関）

- グローバル連携省（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）
- 公安省（Public Safety Canada ）
- サイバーセキュリティセンター（Canadian Centre for Cyber Security）
- 安全保障情報局（Canadian Security Intelligence Service ）

（資金配分機関等）

- 保健研究機構（Canadian Institutes of Health Research）
- カナダ・イノベーション財団（ Canada Foundation for Innovation ）
- 自然科学・工学研究会議（Natural Sciences and Engineering Research Council ）
- 社会科学・人文科学研究会議（Social Sciences and Humanities Research Council ）
- 国立研究会議（National Research Council Canada ）

（大学コミュニティ）

- U15カナダ（U15 Group of Canadian Research Universities ）
- カナダ大学協会（Universities Canada ）
- 研究担当副学長

出典：カナダ政府ウェブサイト「Safeguarding Your Research」

カナダ 研究セキュリティセンター

■ **名称　：**研究セキュリティセンター
（Research Security Centre）

■ **設立年：**2022年

■ **概　要：**

- 研究コミュニティ、大学への指導と助言を行い研究セキュリティの能力強化するため「研究セキュリティセンター」が設置。
- 2022年度予算で5年間で1,260万ドル、継続的に290万ドル。
- 所管：カナダ公安省

■ **場　所：**各都市に6名のアドバイザーが常駐

- 地方にある研究セキュリティアドバイザーネットワークと、首都圏にある中央ハブから構成される。
- 各都市に6名のアドバイザーが常駐

  - ビクトリア市 ：British Columbia、Yukon、Northwest Territories含む
  - エドモントン市：Alberta 、Saskatchewan、Manitoba含む
  - グレータートロントエリア：Ontario、Nunavutも管轄
  - ケベック市：Quebec州全域
  - ハリファックス市：New Brunswick、Nova Scotia、 Prince Edward Island、Newfoundland、Labrador含む

図：カナダの研究セキュリティセンター（CRDS作成）

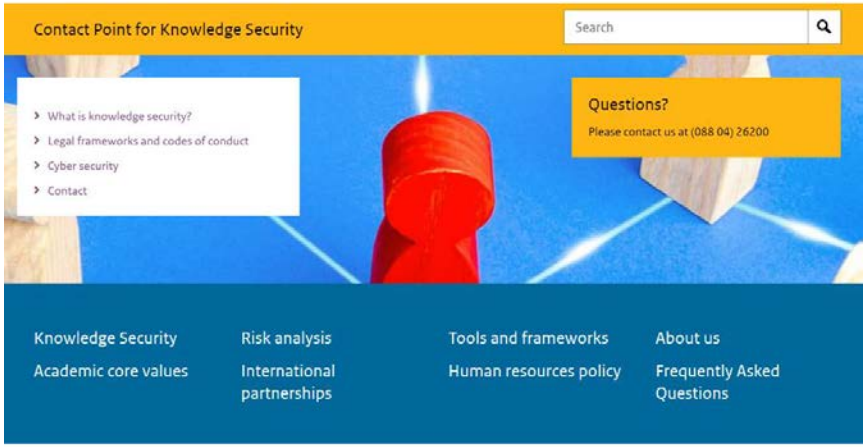
■ **機　能：**

1. 政府方針の実施と情報提供：「国際研究協力に対する国家安全保障ガイドライン」、「機微技術の研究と懸念される提携に関する方針」等の実施するため情報提供を行う
2. 地域のアドバイザーネットワーク：学術機関や研究者に、科学の保護に関するワークショップ、関与、情報ツールを提供する
3. カナダ政府の支援へのアクセス：政府支援へのつなぎ

オランダ 知識セキュリティに関する窓口

- **名　称：**知識セキュリティに関する政府連絡窓口（National Contact Point for Knowledge Security）
- **設　立：**2021年12月
- **概　要：**

- 知識セキュリティに対応する大学・研究機関を対象に、専門知識とアドバイスを提供する連絡窓口として設置。
- 窓口は、関係省庁（内務省・国王関係省、外務省、防衛省、法務省、農業・漁業・食料安全保障・自然省、教育文化科学省、経済省）と繋がっており、ワンストップサービスを提供。
- 設立後、これまでに380件以上の問合せに対応。問合せの多くが中国、イラン、ロシア、中東諸国との国際協力に関するもの。
- 最近は、ベストプラクティスの共有ができるネットワーキング・イベントも開催している。
- 窓口が提供するアドバイスには法的拘束力はなく、大学・研究機関が自ら自律的に対策を講じることが奨励されている。



出典：オランダ政府「Knowledge Security」ウェブサイト