安全で開かれた研究のための G7ベストプラクティス

グローバルな研究エコシステムにおけるセキュリティとインテグリティ（*SIGRE*）ワーキンググループ

（日本語仮訳）

2024 年 2 月

目次

ビジョンステートメント

「研究セキュリティと研究インテグリティに関するG7共通の価値観と原則」に以下の記述がある。

> G7各国は、国内外のすべての才能の重要性が認められる共同研究システムの継続を構想する。開放性とセキュリティは、矛盾するものではなく、相補的で、互いに強化し合うものである。

G7各国は、科学研究における自由の尊重が民主主義に欠かせない基盤であり、国際的なパートナーとの間で、信頼に基づき、開かれた研究協力を行うための共通の中心的価値観であることを認識している。G7各国は国際的な研究協力を促進し、その発展の土台となる自由、独立性、開放性、互恵性および透明性という条件を整えることにコミットする。

このビジョンを維持するため、G7各国は、研究セキュリティに関する一連の原則を策定し、承認した。これらの原則は、G7各国と学術界に共通のものであり、研究インテグリティに関して確立された共通の価値観と整合するものである。この研究セキュリティに関する原則および研究インテグリティに関する共通の価値観は、「研究セキュリティと研究インテグリティに関するG7共通の価値観と原則」で打ち出され、文末の附属文書Aおよび附属文書Bに記されている。

上記の研究セキュリティに関する原則および研究インテグリティに関する共通の価値観の実践を支援する目的で、G7各国は、安全で開かれた研究に寄与するプラクティス（慣行）について概略的な情報を提供するためのベストプラクティス（最良の慣行）のリストを策定した。研究のセキュリティとインテグリティを確保する上で、すべてのステークホルダーに果たすべき役割があることを踏まえ、このベストプラクティスは、研究における各々の役割に応じて、政府、研究資金提供者、研究機関、研究者を総体としてまたは個別にその対象とする。G7各国が個別に実施しているベストプラクティスの事例は、附属文書Cで取り上げている。

このベストプラクティス文書を補完するために「バーチャルアカデミー」が開発され、G7の間で、さらにG7の枠組みを越えて、各国のステークホルダーによる研究セキュリティと研究インテグリティに関するプラクティスの実施を支援する予定である。この「バーチャルアカデミー」は、G7各国による研究セキュリティ・研究インテグリティの取組をユーザーが調べるためのリソースであり、参考情報としてベストプラクティスの追加事例やケーススタディも提供していく予定である。

研究インテグリティと研究セキュリティはなぜ重要か

開かれた共同研究は、我々が抱える最も困難で喫緊の課題のいくつかに対して国レベルやグローバルレベルでの対応を下支えするものである。国際的な科学協力の促進は重要である。そのような協力は、発明のペースを速め、我々の研究コミュニティのダイナミズムと開放性を高める。

研究インテグリティ　研究の正当性、社会的関連性、責任および質を守るための職業的価値観、原則およびベストプラクティスの順守を指す。研究者が公正、革新的、オープンで、信頼できる研究環境において協働できる基盤を形成する。研究インテグリティは、個人が自信をもって研究知識を向上させ、研究結果を普及できる状況を確保するものである。

同時に、科学の発展や応用可能性に伴い、知識に不正にアクセスし、移転しようとする者にとって研究が標的になりえる。このような行為者は、自分自身の目的を達成しようとするのであって、研究への資金提供を行った者や研究作業を行った者の功労を認識することはないし、彼らに対して利益をもたらすこともない。こうした行為は、経済的、戦略的、地政学的、またな軍事的目的のために行われ得るが、結果として、研究のセキュリティとインテグリティを含め、国際研究が依拠する基盤を構成する規範と価値観に違反する。

研究セキュリティ　経済的、戦略的なリスクや、あるいは国家的、国際的な安全保障の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行為が含まれている。これは、多くの研究者、研究機関および政府にとって、新たに出現した領域である。G7各国の政府は、我々の研究セキュリティに対する個別的、集団的取り組みが時と共に進化し得るものであり、そのために、何がベストプラクティスであるかについての我々の理解も進化を続けると認識している。研究の質を確保すると同時に、（研究セキュリティの）手法は新たに出現するリスクに合わせて適応させる必要がある可能性があり、さらに、研究機関および研究者による研究活動の自律性を維持し、支援するのに十分な程度に（リスクに対する）釣り合いが取れ、柔軟なものである必要がある可能性もある。この認識を踏まえ、適応性の原則は、あらゆる研究セキュリティに関するベストプラクティスの実施の土台でなければならない。

研究インテグリティと研究セキュリティのリスクの関係については、「研究セキュリティと研究インテグリティに関するG7共通の価値観と原則」の附属文書Bに詳述されている。

研究セキュリティにおける「リスク」とは何か

政府と研究コミュニティの人々は、研究セキュリティについて議論する際、しばしば「リスク」に言及するだろう。本文書で示すベストプラクティスは、研究セキュリティに関係するリスクを特定、理解、軽減する場面におけるものが多いため、リスクの意味を定義することが重要となる。

研究セキュリティにおいて、「リスク」には、次に掲げるような違法または不透明な活動が含まれ得る。

- 研究に対する不当な影響、干渉または悪用。これには、国家、軍隊、それらの代理人、非国家主体、組織犯罪活動によるアイデア、研究成果、知的財産の明白な窃取が含まれる。

- 経済面、戦略面または国家安全保障面で悪影響をもたらす、秘密裡の活動や行為。

研究セキュリティにおけるリスクは、様々な手段を通じて、研究チームまたは研究機関の内部に起因することもあれば、外部に起因することもある。行為者が研究への影響、干渉または悪用のために用いる手段には、インフラ（デジタルインフラおよび物理的インフラの両方）、人および資金提供を通じたものが含まれる。こうした手法は、搾取のきっかけとして不当に使用されることもあるが、正当または適法な手段を通じてアクセスされることもある。その場合は、意図する目的やエンドユーザーにつき透明性のある開示はなされないため、結果として、研究が意図されない形や有害な形で利用される結果になり得る。研究プロジェクトを策定する際には、次に掲げるリスク領域を考慮および評価すべきであり、研究プロジェクトの構成も含めた全体的な計画立案と評価の一環として、研究セキュリティのデューデリジェンスも付加的な側面となる。

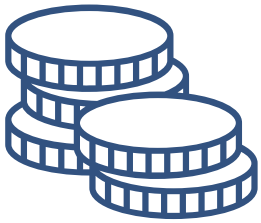
インフラ（デジタルインフラおよび物理的インフラ）

- サイバー関連の脅威は、脆弱性に付けこんだサイバー攻撃（フィッシング、ランサムウェアなど）による研究のデータまたは結果へのアクセスの形式をとることがある。
- 物理的なアクセスは、研究が実施されている施設において研究のデータまたは結果を取得するために利用され得る。

人

- 研究チームまたは研究機関の外部の者が、セキュリティ上の影響を伴う目的や便益を隠して研究者とパートナー関係になろうとすることがある。
- 研究チームまたは研究機関の内部の者で、知識または財産的価値のある事物に対する直接または間接のアクセスを有するものが、自発的に、または他者からの支援や圧力を受けて、自己または他者の利益のために研究にアクセスしたり、これを窃取したりすることがある。セキュリティに関する予防的プラクティスが弱い場合に、他者によるアクセスが容易になることもある。

資金提供



- 資金提供は、研究のデータ、プロセスおよび成果へのアクセスまたはその移転のためのインセンティブとして利用されることがあり、意図する目的またはエンドユーザーに関する透明性のある開示されない可能性もある。

以降の研究セキュリティ・研究インテグリティに関するベストプラクティスにおいて「リスク」とは、上記のリスクを指している。個別のプラクティスが進化し得るものであるため、上記のリスク分類、およびそれに伴うベストプラクティスは、対処すべきリスクの進化を見越して意図的に幅広く設定してある。

研究セキュリティと研究インテグリティに関するG7ベストプラクティス

研究の保護に関するすべての責任を誰か特定のステークホルダーが負うことはない。それは、すべてのステークホルダーの共同責任である。このことを踏まえて、本文書はベストプラクティスを順に記述し、各プラクティスに関係するステークホルダーそれぞれについて記述する構成としている。リスクに対して釣り合いの取れた、迅速で協調的な対応を確実に取るためには、研究コミュニティのメンバー間の協力が非常に重要である。ステークホルダーらは集団的な取組により、研究セキュリティリスクに対して研究コミュニティ全体を強化することができる。

次のリストに掲げるベストプラクティスは、G7各国が既存のイニシアチブやプログラムの中から特定したものである。

これらのプラクティスの多くは、研究コミュニティ全体、つまり、**政府**、**研究資金提供者**（私的、公的および政府系の資金提供者を含む）、**研究機関**（これらを代表する協会のほか、政府が運営する研究機関を含む）並びに**研究者**に向いたものである。

G7各国の間で研究エコシステムの状況および構造が異なることを踏まえ、各国が自国の研究コミュニティのニーズに合わせ、ベストプラクティスを異なる形で実施することも考えられる。

研究の保護に関する
すべての責任を誰か特定の
ステークホルダーが負うことはない。
それは、すべてのステークホルダーの
共同責任である。

図1：G7ベストプラクティスがどのように研究セキュリティと研究インテグリティを支えているかを表した図

1.すべての研究ステークホルダーの間で、研究セキュリティ・研究インテグリティに対する意識醸成のリソースと、対話と情報共有を促進する場を構築する。

研究セキュリティは、国家安全保障上の懸念として新たに出現した領域であり、多くの個人および機関にとっては新たなリスク項目かもしれない。研究コミュニティ内のステークホルダーの間で二者間および多者間での対話を継続することは、積極的で継続的な情報共有を継続し、意識を高める上で重要である。情報共有は、リソース（すなわち、オンラインのデータベース、研修など）の提供のほか、幅広い研究活動を理解することにより情報を得て、研究コミュニティの現在および将来のニーズについて議論するタスクフォースまたはワーキンググループの設置を通じて達成することができる。

政府、研究資金提供者、研究機関および研究者を含むすべてのステークホルダーは、セキュリティリスクに対する意識を高めたり、セキュリティリスクについて議論したりする際に、特定の個人またはコミュニティをターゲットにすることのないよう注意すべきである。そのような対話の際に使用する語彙や文言は、研究の成功の基盤となる差別、ハラスメント、強制からの自由を確保する上で非常に重要である。

政府： 政府と研究コミュニティ内の多様なステークホルダーとの間における対話および情報共有の場を構築することは、すべてのパートナーが研究環境およびそのセキュリティリスクの理解を深める助けとなりえる。こうした対話は、現在のリスクや出現しつつあるリスクに関する情報の共有、リソースを構築するための研究コミュニティのニーズの特定、研究セキュリティ・研究インテグリティに関する政策の支援など、多くの目的に資する可能性がある。例えば、政府が、研究資金提供者、研究機関および研究者に新しいリスクや慣行について知らせる際に、機密扱いされていない情報を共有しえる。同様に、情報が研究コミュニティから政府に逆流することにより、政府は、研究に適したリスク情報や政策を立案するために十分な研究の文化やプロセスに関する知識を確保できるようになる。

また、政府が研究コミュニティの構成員が情報を取得し、意識を高めるための中核的リソースを創出することを検討しようとするかもしれない。そのような中核的リソースには、現在のリスクおよび出現しつつあるリスクに関する現在の情報を含まれたり、本文書で特定されるベストプラクティスの一部を実施する上で役立つリソースに関する情報源になったりすることも考えられる。

研究資金提供者： 研究資金提供者は、研究資金提供や各種プログラムに関する期待事項を設定する政府機関と定期的に関与の場をもち、研究セキュリティ・研究インテグリティに関係する広範な政策形成を支援することができる。同様に、研究資金提供者が研究機関や研究者と関わりをもつことは、出現しつつある問題や対応されていないニーズを理解する上で非常に重要である。研究資金提供者は、意識を醸成するのに役立つリソースの普及や促進をも支援できる。

研究機関：研究機関は、研究者のニーズを特定する上で非常に重要な役割を担う。自機関の研究者と積極的に対話することにより、リスクの理解におけるギャップを埋め、現在のリスク環境に関する最新の関連情報を提供するためのツールやリソースを、個々の組織における状況やプロセスに合わせて開発することが可能となる。研究機関は、潜在的リスクがある領域やそれを軽減する方法に関してスタッフに定期的に研修を行い、最新の情報を提供することで、スタッフが既存の脅威に対応できるようにすることができる。研究機関は、研究コミュニティ内でリスクに対する意識を醸成する目的で、研究者にリソースを普及することも考えられる。

実施中の政策

2019 年、英国は、英国の学術界内の協力・国外志向の高まりを踏まえ、英国の研究・イノベーション部門における研究セキュリティの理解を深めるというニーズに応えるために、「Trusted Research（信頼される研究）」キャンペーンを開始した。

研究者： 研究者は、有効な意識向上および情報共有に関与することにより、自身の研究を守る力を得ることができ、その中で、国内および国際的な研究エコシステムのインテグリティを守る力を得ることができる。また、研究者は、自身のニーズが十分に明示および理解され、政府、研究資金提供者および研究機関が対処可能となるよう、すべてのレベルにおける対話に貢献するという役割も担っている。

2.リスクにさらされている研究領域を特定し、その情報を共有する。

研究セキュリティ・研究インテグリティに関する情報を幅広く定期的に共有するほかに、リスクを絞った情報を提供すること、つまり、リスクにさらされる可能性が高い研究領域とその手法を特定することが重要である。高リスクの研究領域を特定することは、国際協力およびオープンサイエンスを支持しつつも、一部の研究領域が低リスクの領域よりも高いレベルのセキュリティを必要とすることを認識して、研究セキュリティに対する釣り合いの取れたアプローチを促進することになる。セキュリティおよびインテグリティのリスクにさらされやすい研究領域は、重要な関連性を維持し、科学およびリスク環境における変化に対応するために、常に見直され、更新されるべきである。

政府：政府は、研究資金提供者、研究機関および研究者と協力して、リスクにさらされている領域の特定が正確であり、研究部門のニーズに適っていることを確保すべきである。政府は、自国の研究コミュニティが特定の領域におけるリスクの理解を支援する役割を担っており、その役割には、次に掲げるようなリスク領域に関する情報を提供することが含まれる。

- 軍事力または諜報能力を高めることと明確に結び付く領域

- 軍事／諜報および民生の両方で利用できるデュアルユース領域
- 顕著な経済的利益をもたらす可能性がある領域
- 機微な個人データまたは全体として機微になり得る大規模データセットにアクセスする可能性がある領域
- ある国の市民の健康、安心、安全または経済的福祉および政府の効果的な機能にとって必要不可欠であるプロセス、システム、施設、技術、ネットワーク、資産、サービスを含む、重要インフラの領域
- 国家において優先される経済的または戦略的な利益に関わる領域

研究資金提供者：研究資金提供者は、最も高リスクの研究領域にフォーカスする、対象を絞った方法で研究セキュリティ・研究インテグリティに関する要求事項を実施すべきである。また、研究資金提供者は研究者に関与し、プロジェクトおよび潜在的リスクを完全に理解できるようにするべきである。

研究機関：研究機関は、政府が機微であるとみなす研究領域において自機関がいかなる研究活動を実施しているかを把握しているべきである。そうすれば、研究機関は、研究者が自身の研究が高リスクであると判断するのを助け、かつ、情報共有を通じて研究者を支援することができる。

研究者： 研究者は、自身の研究およびその研究が発展している環境を最もよく理解している。研究者は、自身の研究が流用され悪用され得る方法を検討し、自身の研究が機微とみなされるかを判断するために既存の政府指針に従い、かつ、自身の研究に対してデューデリジェンス活動を実施するために政府、資金提供者または研究機関から提供されるツールを使用すべきである。

実施中の政策

2023 年 6 月、米国防総省（Department of Defense、DoD）は、外国からの影響に起因する利益相反に関して基礎研究プロジェクトを精査するための同省全体を対象とした方針を導入した。DoD は、この方針に従い、潜在的な研究セキュリティリスクを低減させるために、基礎研究プロジェクト提案をリスクベースでセキュリティ審査することになる。

3.デューデリジェンスを実施し、透明性および関連情報の開示を確保することにより、リスクのある活動の領域を特定する。

リスクの原因となるものは多様であり、リスク軽減措置を策定するためには、脅威が出現する可能性がもっとも高い領域を確定することが非常に重要である。 リスクの主要な発生手段を確定することにより、リスク軽減措置の実施などのベストプラクティスをより効果的に実施することができる。

政府： 自国の研究コミュニティと共に、政府は、研究資金提供者、研究機関および研究者を対象としてデューデリジェンスおよび透明性に関する要求事項を定める政策枠組みを策定する責任を負うべきである。このような枠組みは、特定されたリスクから研究を守るための保護手段を設けた上で、研究、科学およびイノベーションを促進しつつ、国益とグローバルな利益の均衡を図るべきである。

また、政府および国家安全保障機関は、研究コミュニティにリスクを特定するための態勢を整備させ、政策枠組みが研究を保護する上で整合性を保つために、脅威をもたらす環境を定期的に評価しつつ、研究コミュニティにとって最も喫緊のリスクに関して研究機関および研究者に指針を提供すべきである。政策枠組みは定期的な評価を通じて見直され、研究コミュニティのニーズおよび研究セキュリティ・研究インテグリティの目的に引き続き合致しているかが検討される。政府には、リスクの傾向に関するより深い洞察があり、可能な場合には、リスクの特定を支援するために、情報を共有することもありえる。さらに、政府は、学問の自由の維持、差別やハラスメントの回避という原則を確保するために策定した政策枠組みに対して、意図しない悪影響が生じていないことを監視すべきである。

研究資金提供者： 研究資金提供者は、研究プロジェクトにおけるリスク領域を特定、評価および軽減するという目的を果たすために政府が策定した政策枠組みの実施に責任を負う。資金提供の申請では、リスクを特定するためのデューデリジェンスの実施と、関連する潜在的リスクの開示が透明性のある形で明示されるべきである。こうしたリスクの特定を支援するために、資金提供者は、申請者によるリスクの開示や特定に関して政府または自身が策定した指針およびアプローチを利用すべきである。そのようなアプローチは、研究者が自身の行ったリスクの開示と評価を容易に、透明性のある形で示せるようなものとすべきである。申請を審査する際、資金提供者は、その研究提案のリスクと科学的なメリットや利益を比較検討することに責任を負う。

これには、例えば、プロジェクトパートナーの評価や利益相反または所属先の開示が含まれる。外国の政府、軍隊、それらの代理人等の組織は、研究情報（データなど）、研究知見、研究成果としての知的財産および技術にアクセスするために、パートナーシップの利用または研究者や研究コミュニティのメンバーを通じて不正な知識の移転を進めようとすることがある。こうしたリスクを減らすために、資金提供者は、誰が研究プロジェクトに関与しており、どのような関係性であるかを理解すべきである。個人が、そうであると知りながら、またはそうとは

知らずに、国家安全保障を害するおそれのある方法で、望ましくない知識の移転を手助けするように手引きされたり、強要されたりすることがある。

資金提供者は、潜在的な利益相反に関する情報の透明性および開示を要求し、資金提供申請書にそうした要求事項を含めることで当該要求事項を標準化することを検討してもよい。これには、プロジェクトに関与する個人に関する情報（所属組織、職務、有料コンサルティング活動）や、外国政府を含め、対象の研究に対する他の資金源（現物、人員または現金の拠出）の開示が含まれ得る。

研究の自由を守り、差別やハラスメントを回避するという原則を維持するために、研究資金提供者は、研究セキュリティ・研究インテグリティに関するプログラムの実施において意図しない悪影響を監視し、さらに、研究資金提供プログラムにおいて差別およびハラスメントが許容されないような措置を講じるべきである。

研究機関：研究機関は、自機関の研究者がリスクを特定、評価を行い、情報開示の透明性を確保するのを支える能力を構築することができる。研究機関は、執行部レベルが主導権を担い、研究セキュリティ・研究インテグリティに関する事項に責任を負って、統一的なアプローチの確保を支援することを検討することも考えられる。研究セキュリティリスクは、例えば、組織のリスクフレームワークやリスクレジストリ、または研究インテグリティのための組織的枠組に統合することもできる。研究プロジェクトに関係するレピュテーション、倫理および国家安全保障上のリスクについては、新たに出現する懸念事項に研究機関が迅速に対応し、適応できるようにするために、執行部レベルで定期的に議論すべきである。研究機関は、リスクマネジメントに関する意思決定の責任を負う者が、自身の責任範囲を明確に理解し、どのような場面でさらに上位のレベルに上申すべきかを判断するための適切な支援を受けられるようにすべきである。

加えて、研究機関は、複数のプロジェクトや研究分野を対象とし得る、研究機関全体のリスクの特定および評価に責任を負うべきである。例えば、インフラに関するリスク（物理的インフラおよびデジタルインフラの両方）を特定することは、物理的なアクセス制御およびサイバーセキュリティ制御が、特定のプロジェクトのために個人の研究者によって設定されるのではなく、研究機関レベルで設定されることが多いことを踏まえれば、通常、研究機関レベルの責任となるであろう。加えて、研究機関は、研究成果が透明性のある形で文書化され、すべての当事者に賛同できるものとなるよう、研究協定の文言を精査すべきである。

研究の自由を守り、差別およびハラスメントを回避するという原則を維持するために、研究機関は、研究セキュリティ・研究インテグリティに関するイニシアチブの実施における悪影響を監視し、関連する研究資金提供者または政府にその結果を報告することにより、悪影響が直ちに対処されるようにすべきである。

実施中の政策

2021 年 7 月、カナダ政府は、国家安全保障上の考慮事項を研究パートナーシップの構築、評価および資金調達に組み込むために、「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）」（「本ガイドライン」）を導入した。本ガイドラインが適用される研究資金提供プログラムの申請者は、リスクアセスメントフォームにリスク軽減計画を含めて提出しなければならない。

研究者： 上記のとおり、研究者は、自身の研究分野および自身が実施している研究を最もよく知っており、また、その結果として、政府その他の信頼できる情報源から提供されたリスク情報に支えられた上で、潜在的なリスク活動の領域（特に、パートナーシップおよび人員に関するものを含む）を最もよく特定できる立場にあることが多い。リスクの特定を支えるために、研究者も、自身の研究のインテグリティおよびセキュリティに対する潜在的リスクを特定、評価および軽減することにコミットすべきである。これには、自身の研究機関および研究資金提供者に適切な情報を開示することが含まれる。研究機関および研究資金提供者は、研究者にとっては直ちに明らかではないが、出現しつつあるリスクの傾向について、より幅広い知識を有していることがあるからだ。これにより、研究者は、より幅広いリスク状況やリスクにおける変化を把握することができる。

パートナーおよびチームメンバーの動機および利害関係を理解することは、潜在的リスク領域を特定するのに役立ち得る。デューデリジェンスによる精査を完了することにより、個人の自律が害されている可能性があること、機微な研究領域において外国政府、軍事若しくは保安部門と関連を示す兆候、研究者の知的財産へのアクセスや窃取を行っていると知られている国において自身のパートナーが活動していることを示す情報、または透明性が不十分であることを示唆する情報が示されるなど、リスク指標が観察されることがある。プロジェクトに関与する者についてよく知り、これらの者の動機や目的を理解することは、潜在的リスクを特定し、軽減するのに役立つ。パートナーシップがどの程度、正式なものであるかにかかわらず、プロジェクトに関与する者について知ること、また、協力の指針となる明確で、共有され、文書化されたプロセスを有することは、研究のインテグリティにとって有益であり、これを支えるものでもある。これにより、研究者は、潜在的リスクが特定され、透明性をもって対処されていることを理解し、自信をもって研究を進めることができる。

研究者は、研究セキュリティ・研究インテグリティの施策が特定の個人またはコミュニティを対象にすべきではないことを理解する必要があり、また、自身の研究機関、研究資金提供者または政府に対し、差別またはハラスメントの発生を明らかにし、それらが直ちに対処されるようにすべきである。

4.標準的な組織内の慣行として、また個別の研究プロジェクトに対して、リスク軽減措置を実施する。

リスクが存在する場面やリスクの程度を確定すれば、研究コミュニティの構成員は、概して、リスクに対処し、軽減しやすくなる。 リスク軽減は、リスクの発生可能性と影響を研究者、その研究機関、研究資金提供者および政府にとって許容可能な水準にまで減少させることを目的とする。リスク軽減措置は、従うべき基準を策定するという方法により組織レベルで実施することができ、リスクの程度を高める特徴があるプロジェクトに対して、状況に応じたリスク軽減のアプローチを取る方が適切な場合には、プロジェクトレベルで実施することもできる。軽減措置は、安全で開かれた研究を確保するために、リスクの程度に相応的なものとすべきである。軽減措置は、時と共にリスクの変化に適合させる必要が出てくることがあり、軽減措置が現在のリスクに適切に対処できているか、または新しい懸念事項に対応するための変更が必要であるかを判断するために、定期的に見直しをすると効果的である。

また、研究資金提供者や研究機関などのステークホルダーは、組織レベルとプロジェクトレベルの両方でリスクガバナンスを実施することを検討するのも良い。組織的リスクおよび個別の研究プロジェクトに伴うリスクを評価および軽減するための組織的な方針とプロセスを整備することは、意思決定プロセスの整合性を確保する上で非常に重要である。

政府： 政府は、リスク軽減に関する指針を提供するという有益な役割を担っている。政府は、リソースおよび情報共有の仕組みを策定することにより、ベストプラクティスによって研究コミュニティの他の構成員を支援することができる。

研究資金提供者： 研究資金提供者は、研究セキュリティ・研究インテグリティに関して自身が定める申請プロセスにおいて特定の要求事項を求めることを検討するか、または一定のリスク軽減措置が資金提供のための標準的な期待事項であるとする方針や条件を設定することが考えられる。また、資金提供者は、特定のプログラムの参加者が、研究コミュニティの既存のベストプラクティスや進化中のベストプラクティスに従い、自身の研究の保護に関して一定の研修を受けるという要求事項を満たし、サイバーセキュリティ計画を整備し、データ管理の手段を規制するように申請者に奨励または要求することを検討こと も考えられる。さらに、研究資金提供者は、申請者が提出する研究提案を受け取るという立場にあるため、リスク軽減の幅広いベストプラクティスを特定し、策定できる可能性が高い。そして、（政府と共に）研究コミュニティ全体にリスク軽減措置に関する指針を広く行き渡らせることができる。

研究機関： 研究機関は、自機関およびその研究者を保護するために多様な措置を実施することを検討することができる。例えば、研究機関は、適切なサイバーセキュリティのプラクティスや物理的アクセス制御の採用、自国の関連する法的義務の遵守の徹底、知的財産の保護手段の策定を検討することが考えられる。

強力な研究セキュリティ・研究インテグリティのプラクティスを奨励するために、研究機関は、自機関の研究者を対象として研究セキュリティ・研究インテグリティに関する行動規範を策定することもできる。行動規範では、当該機関内の研究者を対象とする幅広い基準を定めることができる。また、研究者が不正アクセス、悪意ある干渉または強制の場面に直面した場合にどのように対応すべきかに関する期待事項を定めることもできる。スタッフが問題または懸念事項を報告する際の適切な方針およびプロセスを整備することは、リスクに関する情報共有や、リスクの特定および軽減に役立つ。

実施中の政策

ドイツ国内の 120 を超える研究機関、組織および楽興会は、各地域で「セキュリティに関する研究における倫理委員会（Committee for Ethics in Security-Relevant Research）」を設置し、研究者や研究機関が自身の研究のセキュリティ関連の側面に関する疑念に対して助言を与えている。この委員会は、ドイツ国立科学アカデミー・レオポルディーナとドイツ研究振興協会が 2014 年に導入し、2022 年に改訂版を発表した「セキュリティに関する研究の取り扱いに関する勧告（Recommendations for Handling of Security-Relevant Research）」に従い設置された。

また、研究機関は、サイバーセキュリティや物理的セキュリティについてのグッドプラクティスに関する基準について、研修の実施を検討することもできる。スタッフが海外出張や国際的な情報の送受信・共有をしている場合、自身と自らが取り扱う機微な情報の安全性をどのように保つかに関して十分な知識を得られるように説明や研修を受け、準備を整えておくべきである。

研究者：リスク軽減措置を実施するために、研究者は、明確なリスク削減の段階を設けたリスク軽減計画を策定することができる。理想的には、リスク軽減計画は、懸念事項が存在する可能性のある領域に関して早期の精査を通じて特定されたリスクに対処するために、研究者の研究機関や研究資金提供者の支援を受けて策定されることが望ましい。研究者が選択するリスク軽減戦略は、利益とリスクとの均衡を図るべきであって、協力、国際的な人材の誘致または持続可能な資金調達を行う研究者の能力を抑制すべきではない。リスク軽減計画は可能な限り具体的であることを目指すべきで、特定されたリスクの種類によって内容が異なり得る。

こうしたリスク軽減措置は、研究プロジェクトのすべてのメンバーで共有される文書化された措置や手順とともに、研究の健全性を確保する既存のプラクティスに組み込み、実施するとともに確実に順守されるよう追跡することがあり得る。メンバーは、どのような管理が実施されているかを知っておくべきである。研修や新たにプロジェクトに加わるメンバーへの説明の手順を策定して、プロジェクト開始時点およびプロジェクト実施期間全体を通して、リスクが適切に管理されるようにすべきである。そのような研究セキュリティ・研究インテグリティのプラクティスは、一般的な研究プラクティスに一体として組み込まれた場合に最も効果を発揮できる。

おわりに

開かれた共同研究は、我々が世界の最も困難な問題のいくつかに対応することを可能にする。研究インテグリティは、研究者がグローバルな研究環境で活躍する際の基盤として機能するものである。上記のベストプラクティスは、研究インテグリティを支えるために、研究コミュニティが各々の研究を保護するためのプロセスや取組を構築し、改善するのを助け、相互の信頼に基づいた共同研究システムの運用と継続を可能にすることを目的としている。こうしたベストプラクティスは、学問の自由、オープンサイエンス、透明性・情報開示・誠実性、差別・ハラスメント・強制からの自由、社会的信頼の醸成、機関の自律など、多くの重要な研究インテグリティの原則に従って研究を支えるために策定されたものである。

研究セキュリティは、世界中の研究コミュニティにとって新たに出現した領域であり、だからこそ、今後進化していく概念である。上記のプラクティスは、対応策の相応性および適切性を確保するために、新たに出現するリスクに合わせて適応させ続けるべきである。

附属文書A－研究インテグリティに関する共通の価値観

学問の自由：人の参加を可能にすることに重きを置き、学術環境において研究を指導し、実施し、発表する自由が、研究の基本思想である。真実を追究し、学生を教育し、知識と理解を普及させることが研究機関の基本的な使命である。学問の自由には、研究者が学術的探究に対して外部からの不当な影響や制限を受けることなく、自律と雇用の保障のある環境が必要である。

差別、ハラスメント、強制からの自由：差別、ハラスメント、強制が存在しないことは、研究成功の基礎となる価値である。研究コミュニティのすべての構成員は、差別、ハラスメント、いじめ、強制、本人や家族の安全への脅威のない状態に置かれるべきである。差別　、ハラスメント、強制は、個人、グループ、機関、または政府により行われうる。これには、主体自身の目的、利益、方向性に基づいて、組織が個人に対し、本人の意思や利益に反する非倫理的または不正な行為を強制するケースや、嫌がらせを行うケースが含まれる。

公平性、多様性、包摂性：公平性・多様性・包摂性（EDI）とは、すべての研究活動（採用手続き、キャリア展望を含む）におけるアクセス、多様性、非差別の原則の積極的な推進である。これらは研究のあらゆる側面で必要とされる。EDIは、多様なアイデア、文化、見解の余地を与え、アイデンティティや思考の多様性に貢献するものである。研究コミュニティ、エコシステム、事業に誰もが自由に参加できるよう確保することは、革新的で繁栄する包摂的な世界の構築の助けとなる。

機関の自律：　研究機関は、エビデンス、データ、ピアレビューに基づいて知識を自由に追求し、普及させることができる場合にのみ、学生、教職員、社会に対する使命を果たすことができる。機関は、自らの使命を自由に追求することが可能であるべきである。こうした使命は、ガバナンスの監視と指示に基づいている場合もあれば、コミュニティや現地のニーズを満たすものである場合もある。いずれにせよ、機関の自律には、すべての個人と機関が自由であり、外部からの望まれない影響から保護された、安全で安心できる環境が必要とされる。

オープンサイエンスおよび研究へのアクセス：研究コミュニティのすべての構成員は、イノベーションのインセンティブを維持しつつ、研究結果、データ、方法、インプットのオープンな共有と交換を積極的に支持するべきである。オープンサイエンスとは、科学と研究のインプット、アウトプット、プロセスを最小限の制約ですべての人が利用できるようにすることであり、プライバシー、セキュリティ、倫理的配慮に対する完全な尊重、ならびにアイデア、研究成果、知的財産の適切な保護の下で実践されるべきである。社会のすべての構成員が過去に実証済みの研究に立脚していくことを可能にすることで、オープンサイエンスは新たな発見のペースを速め、他の人々の生活やわれわれの社会を向上させ、研究の質の向上に寄与する。

社会的信頼の醸成：一般市民や研究に携わるすべての人々の信認を維持するように研究を実施し、追求することは、科学や研究への取り組みの継続的な成功のために不可欠である。インテグリティに貢献する者として、科学研究活動に従事するすべての主体は、機微なデータや研究にアクセスする際に信頼の期待に応えられることを実証するよう務めるべきである。そのためには、研究結果の目的、用途、所有権に関して、すべてのパートナーの間での熟慮に基づき、明確かつ共有された理解が必要である。こうした理解が研究のすべての段階、すべての所管領域で支持され、尊重されるべきである。社会的信頼の維持には受託責任も必要であり、それには適切な監督と管理をすべてのレベルで反映させる必要がある。政府や資金提供機関には、その意思決定、ならびに高等教育機関や研究機関との関係についての受託責任がある。高等教育機関と研究機関には、自機関の従業員や学生との関係、ならびにスポンサーとのコミュニケーションにおける受託責任がある。

透明性、情報開示、誠実性：機密扱いでない研究の方法、データ、成果を、必要な場合に機密性を維持しつつ、完全に透明性のある形で相互共有することは、共同研究、インテグリティ、アイデアと情報の自由な流れのためにきわめて重要である。研究者の所属、利益の競合または相反、資金源の開示における透明性も、実施される研究のインテグリティを確保する上で重要である。透明性には誠実性が必要である。補完的な価値として、誠実性には、研究の提案、開発、実施、レビュー、報告、伝達の際に率直で虚偽やごまかしのないことを必然的に伴う。これは研究のすべての側面に適用され、他者の研究を認め、研究結果に基づいた正当な主張や賢明な解釈を行うことが含まれる。

附属文書B－研究セキュリティに関するG7原則

国家の利益と世界的な利益のバランス：科学・研究パートナーシップのための資金提供は引き続き、主として科学的メリットの評価と卓越性に基づいたものとし、必要な場合には国家や経済の安全保障へのリスクに対する適切かつ釣り合いのとれた考慮や軽減を図るべきである。

開放性の維持と研究セキュリティ：政府はオープンサイエンスを後から取って付けるのではなく、研究を非公開のままにしておく正当性が認められない場合はアクセス可能にすることを約束するべきである。オープンサイエンスにも制限はあるべきで、もし普及した場合に倫理的、地政学的または国家安全保障上の悪影響を及ぼし得る研究に安全措置を講じる義務にオープンサイエンスが優先することはないと認識されている。

共同研究と対話：開放性と同時にセキュリティを維持するコミュニティを追求するためには、研究に携わるすべての主体が互いに支援し、関わり合う努力をするべきである。政府は、研究者と共に共通のリスクに取り組み、アプローチの共有から利益を得ることを目標として、リスクの性質に関する有意義な情報共有に取り組むことを約束するべきである。。

積極的な取り組み：政府は、教訓やベストプラクティスに基づいて研究セキュリティと研究インテグリティのリスクを管理し軽減させるための積極的かつ予防的な施策を講じるよう、尽力するべきである。。

リスクとの釣り合い：リスクに対する対応は釣り合いのとれた、適切な規模にするべきである。研究セキュリティに対するリスクに適切な対応をするためには、特に、研究悪用の潜在性やリスクの総体的な水準といった要因を考慮するべきである。

責任の共有：動的で絶えず変化する研究リスクに対処するためには、研究セキュリティと研究インテグリティに対するリスクへの対処や管理に関して研究コミュニティのすべての構成員が各自の明確な役割と責任を認識し、理解するべきである。

説明責任（Accountability）と責任（Responsibility）：個人や組織は、自己の行動が許容されている基準から逸脱している場合などには、自己のすべての行為について説明責任を負うべきである。

適応性：過度に厳密なアプローチは有益な研究を遅延させるリスクを伴うことを認識しつつ、研究セキュリティの施策は動的であるべきである。変化のない固定的なアプローチは、重大な阻害要因につながり、新たなリスクや新興のリスクに対する説明責任を負うものとは言えない。

附属文書C－ベストプラクティスの例

欧州委員会－研究インテグリティの標準運用手順

EU の「研究インテグリティの標準運用手順（Standard Operating Procedures for Research Integrity、SOPs4RI）」の各事例は、上記のベストプラクティスのうちの一つを反映している。

1.SOPs4RI（研究インテグリティの標準運用手順）は、欧州委員会が資金を提供する、4 カ年（2019 年～2022 年）のマルチパートナープロジェクトである。SOPs4RI は、欧州の研究実施機関（Research Performing Organisation、RPO）および研究助成機関（Research Funding Organisation、RFO）全体でプロセスの変革を促すことを目的としている。

2.SOPs4RIは、RPOおよびRFOが研究インテグリティを醸成し、有害なプラクティスを減少させるのを助ける、オンラインで自由に、簡単にアクセスできるできる「ツールボックス」を提供する。SOPs4RI は、RPO および RFO が強力な研究インテグリティ文化を促進するガバナンス関連の取り決めを行う際に依拠できる「標準運用手順（SOP）」とガイドラインのインベントリを設ける。

3.欧州委員会が把握したところによれば、「捏造、改ざんおよび盗用（Falsification, Fabrication and Plagiarism、FFP）」といった研究に関するグッドプラクティスに対する深刻な違反が生じることは比較的まれであり、そのような行為には科学者のうちの 1%から 2%しか関与していないと推定される。しかし、「疑わしい研究行為（Questionable Research Practices、QRP）」として知られる、深刻度が低い問題（不良な研究設計、方法および分析など）は、さらに頻繁に発生している。そのため、研究者が準拠し、自身の研究をより良く構築することができるようにするための直感的に理解できる指針を提供することは、健全な研究環境を確保するための欧州委員会のアプローチにおいて不可欠である。

4.異なる学問分野における研究により、従前の研究結果を再現するのは難しいことが多いということが示されている。選択的な報告、手法の不十分な説明等の QRP が再現性問題の原因であるとしばしば考えられている。再現性問題および非効率的な研究環境は、研究を遅らせるだけではなく、プロセスを不明瞭にして、リソースを停滞させたり、研究ネットワークの他の領域から関与する者（監督機関など）を妨害したりすることがある。これにより、利用されれば研究セキュリティが害されるような機会や盲点が生まれる。

英国－Trusted Research ポータル

(1) すべての研究ステークホルダーの間で、研究セキュリティ・研究インテグリティに対する意識醸成のリソースと、対話と情報共有を促進する場を構築する

英国には、世界中からの投資を惹きつける、活気ある研究・イノベーションセクターがある。英国の研究の半数以上が国際的パートナーシップの恩恵を受けている。 国家保護安全保障局（National Protective Security Authority、NPSA）および国家サイバーセキュリティセンター（National Cyber Security Centre、NCSC）による「Trusted Research（信頼される研究）」キャンペーンは、英国の学術界のコラボレーション・国外志向の高まりを踏まえ、英国の研究・イノベーションセクターにおける研究セキュリティの理解を深めるというニーズに応えるために 2019 年に開始された。

Trusted Research は、英国の研究・イノベーションセクターが成功し続ける上で必須である、国際共同研究システムのインテグリティを支えることを目的としている。これは、特に、科学・技術・工学・数学（STEM）の分野、デュアルユース技術、新興技術や商業的に機微な研究領域の研究者に関係する。ここで提供される助言は、研究・大学コミュニティとの協議の上で作成されており、英国の世界トップレベルの研究・イノベーションセクターが、知的財産や機微な研究および個人情報を保護しつつ、国際的な科学協力を最大限に利用することを支援するよう設計されている。

Trusted Research：

- 英国の研究およびイノベーションに対する潜在的リスクを概略する。
- 研究者、英国の大学および産業パートナーが国際共同研究に信頼を置き、潜在的リスクに関する情報を得た上で意思決定を行うことを支援する。
- 研究およびスタッフを盗用、悪用または搾取の可能性からどのように守るのかを説明する。

「Trusted Research for Academia（信頼される研究、アカデミア向け）」指針に加え、英国は、学術界のリーダーを対象として一部の重要な考慮事項を概略する「 Trusted Research for Senior Leaders（信頼される研究、シニアリーダー層向け）」と、海外に滞在する間の脅威情報および実施すべき実践的なリスク軽減措置を提供する「Trusted Research Countries & Conferences（信頼される研究、国と会議）」を策定した。さらに、国際共同研究の開始時点で研究者が使用するための Trusted Research チェックリストを提供している。

米国－国防総省からの資金提供による高等教育機関の研究に対する外国からの望まない影響への対抗

(2)　リスクにさらされている研究領域を特定し、その情報を共有する

2023 年 6 月、米国防総省（Department of Defense、DoD）は、外国からの影響に起因する利益相反に関して基礎研究プロジェクトを精査するための同省全体を対象とした方針を導入した。この方針には、2 通の文書が添付されている。

- 「基礎研究提案におけるリスク軽減策決定のための意思決定マトリクス（Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions）」
- 「2019 会計年度国防授権法（修正を含む）第 1286 条への対応として公表する 2022 会計年度リスト（Fiscal Year 2022 Lists Published in Response to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 as amended）」
    - 問題のある活動に関与していると確認されている外国機関および米国の国家安全保障上の利益に脅威をもたらすと確認されている外国人材プログラムを特定したリストを含む。

DoD は、この方針に従い、潜在的な研究セキュリティリスクを軽減するために、基礎研究プロジェクト提案をリスクベースでセキュリティ審査する。基礎研究プロジェクト提案をリスクベースでセキュリティ審査する際の DoD の目標は、次の通りである。

- DoD が資金提供する基礎研究のセキュリティを確保すること。
- 対象となる個人に対して、潜在的な利益相反・責務相反を明らかにする情報を完全に開示させること。
- 基礎研究を行う者に対し、許容される行為および奨励される行為のほか、DoD から研究資金提供を受ける上で困難をもたらし得る活動に関する明確なメッセージを提供すること。

リスクベースのセキュリティ審査は、少なくとも、技術的なメリットに基づき資金提供対象として選定された基礎研究プロジェクト提案のすべてに対して行われる。

フランス－国内の科学技術の可能性の保護

(2)　リスクにさらされている研究領域を特定し、その情報を共有する

フランスの科学技術リソースは、科学的活動（基礎または応用）および技術的発展に必要なすべての有形・無形の資産により構成される。そのようなリソースの重要な要素は、フランス刑法典（French Criminal Code）第 410-1 条において定義される国家の基本的な利益にとって不可欠なものとなっている。

「国家の科学技術の可能性の保護（Protection of the Scientific and Technical Potential of the Nation、PPST）」のためのシステムは、フランスの領域内に所在する公的機関および私的機関（研究所、企業など）が持つ、流用または不正取得されると次のような脅威が発生し得る最も「機微な」知識、専門知識および技術を保護することを目的としている。

- フランスの経済的利益が害される。
- 外国の軍備が強化されるか、フランスの国防力が低下する。
- 大量破壊兵器およびその運搬手段が拡散する一因となる。
- フランスまたは外国においてテロ目的で利用される。

このシステムは、フランス刑法典第 413-7 条に基づくもので、次の 3 通の施行文書を中心に整備されている。

- 2011 年 11 月 2 日デクレ（法令）第 2011-1425 号
- 2012 年 7 月 3 日首相命令
- 2012 年 11 月 7 日付省庁間通達

具体的には、PPST は、対象の研究主体に法律上および行政上の保護を与え、当該研究主体が次に掲げる行為を行えるようにする。

- 関係省庁の意見を求めることにより、「制限区域（restricted zone、ZRR）」という一定の区域への物理的アクセスおよび論理的アクセスを制御すること。
- 研究主体の評判および競争力に影響を及ぼす悪意ある行為（情報の不正使用、機微なデータの窃取または不正取得、反競争的行為、情報システムへの侵入など）につき、法的保護手段を設けること。
- 研究主体のセキュリティ水準を引き上げる上で政府の支援を受けること。
- 保護の問題を意識した、責任ある作業チームを構築すること。
- 研究・産業パートナーシップを奨励する、信頼されるコミュニティの一員となること。

PPST は、随時出現する懸念事項に適応していく、生きたシステムである。2022 年 3 月に 2 通のデクレ（法令）が発布され、必要な警戒レベルを下げることなくアクセス申請に関係する通知の処理に要する時間を削減するために、ZRR へのアクセス申請処理の最適化を進める。

このようにして、PPST は、フランスの基本的な利益の保護に寄与するものであり、また、関係する研究主体が自身の機微な知識およびノウハウを保護する上で利用できるツールにもなっている。

カナダ－国際研究協力に対する国家安全保障ガイドライン

(3) デューデリジェンスを実施し、透明性および関連情報の開示を確保することにより、リスクのある活動の領域を特定する

2021 年 7 月、カナダ政府は、研究パートナーシップの策定、評価および資金調達に国家安全保障上の考慮事項を組み込むために、「国際共同研究に対する国家安全保障ガイドライン（National Security Guidelines for Research Partnerships）」（「本ガイドライン」）を導入した。本ガイドラインは、大学の代表者らと協議の上策定されたものであり、研究コミュニティが研究セキュリティに対するリスクについて一貫し、リスクを対象としたデューデリジェンスを実施しやすくするものである。

本ガイドラインが適用される研究資金提供プログラムの申請者は、リスク軽減計画を含めてリスクアセスメントフォームを提出しなければならない。申請者は、次に掲げる事項の評価の際に透明性を確保していることが要求される。

- 自身の研究領域が軍民両用（デュアルユース）となる可能性があるか、または自国の安全保障上の能力や利益を高めようとする外国の政府、軍隊、それらの代理人等の行為者のターゲットとなる可能性があるか
- 提案されている研究パートナーが国家安全保障上のリスクをもたらすか

国家安全保障上のリスクとは、次のいずれかの効果を有する外国からの干渉、諜報、知的財産の窃取または知識の不正移転として説明し得るが、これらに限定されない。

- カナダに対して脅威をもたらす国家または集団の軍事、安全保障、諜報の能力を引き上げる一因となる。
- カナダの研究の発展を妨害するか、重要インフラのレジリエンスを弱めるか、カナダ国民の機微データの保護を脅かす。

資金提供者は、申請の正確性を確保するために、オープンソース情報を使用して行政上のリスク検証を行い、必要な場合は、国家安全保障関連機関に申請書を付託して、リスクに関する評価および助言を受ける。セキュリティリスクというのは進化するものであり、世界のどこからでもやって来るという認識の上で、本ガイドラインはケースバイケースでリスク評価を実施することとしており、特定の国や企業を指定していない。

本ガイドラインは、カナダの研究が可能な限りオープンで、必要な限り安全であるようにするためのものであり、研究者、研究機関、資金提供者および政府の間にデューデリジェンスに関する共同責任があることを認識している。国家安全保障上許容できないリスクをもたらすと評価されるか、またはリスクを適切に軽減することができない研究パートナーシップの申請に対しては、資金は提供されない。

日本 – 研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト

(3) デューデリジェンスを実施し、透明性および関連情報の開示を確保することにより、リスクのある活動の領域を特定する

近年、研究活動の国際化・オープン化に伴う新たなリスクにより、開放性、透明性といった研究環境の基盤となる価値観が損なわれる懸念や、研究者が意図せず利益相反・責務相反に陥る危険性が指摘されている。このような状況の下、2021 年 4 月 27 日、統合イノベーション戦略推進会議において、研究インテグリティの確保に係る政府の対応方針として、「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティの確保に係る対応方針について」が決定された。

この政府の対応方針に基づき、内閣府は、2021 年 12 月、大学・研究機関等における研修等での利用により研究者や大学・研究機関等の理解醸成を促す目的で、研究者向けのチェックリスト雛形および大学・研究機関等向けのチェックリスト雛形を作成した。

チェックリスト雛形は、研究者や大学・研究機関等の立場から、次の事項の管理を徹底するための質問で構成されている。

- 利益相反・責務相反が適切に管理されないリスク、技術流出・情報流出につながるリスク、信頼の低下リスク等のリスク
- 外国の機関・大学等との連携・契約や、外国からの報酬・物品の提供に係る手続き
- 外国の機関・大学等との連携・契約の相手方に関するリスク

その後、大学・研究機関等向けのチェックリスト雛形は、不正競争防止法違反事案を受け、2023 年 6 月に改定された。

大学・研究機関等が上記の雛形を利用し、自機関特有の要求事項や状況を加味した独自のチェックリストを作成することが望ましい。

イタリア – 国家研究プログラム：オープンサイエンスに関する国家計画

(4) 標準的な組織内の慣行として、また個別の研究プロジェクトに対して、リスク軽減措置を実施する

2022 年 6 月、イタリア政府は、「オープンサイエンスに関する国家計画（National Plan on Open Science、*Piano Nazionale Scienza Aperta*）」を発表した。この国家計画は、イタリアの科学コミュニティが過去数年にわたりオープンサイエンスの領域で行ってきた次のような取り組みを支援する参考文書である。

- 複数のイタリアの大学による、EU の「研究評価改革の推進のための有志連合（Coalition on Advancing Research Assessment、CoARA）」への参加。「研究評価の改革に関する合意（Agreement on Reforming Research Assessment）」は、研究の質と影響力を最大化するという包括的目標の下、研究、研究者および研究実施機関を対象として、研究評価プラクティスの変更に関して共有される方向性を定めるものである。
- CoARA。イタリアの大学の学長らによる常設会議により開始されたフォーカスグループ。
- 「イタリア再現性ネットワーク（Italian Reproducibility Network）」が 2023 年初めに始動した。この非営利組織は、多数のアウトリーチ活動および教育活動を通じ、オープンサイエンス慣行を促進、支援および保護することを目的としている。

「オープンサイエンスに関する国家計画」は、次のようなオープンサイエンスに関するアプローチの要素で構成されている。

- 学術論文へのアクセスのための有料の壁の撤廃
- アクセス可能なデータおよびコード
- イタリアの大学の評価制度
- 研究エコシステムのセキュリティとインテグリティの確保

この国家計画は、科学コミュニティが上記のアプローチに合致するルールやインセンティブに関する様々な仕組みを構築する余地を残しつつ、明確な方向性を示すものである。そういった意味で、この国家計画は最初の一歩に過ぎず、透明で、信頼され、公正な研究環境に向けて必要な変化を促進し、採用するためには、まだ多くの労力が必要である。

ドイツ

(4)　標準的な組織内の慣行として、また個別の研究プロジェクトに対して、リスク軽減措置を実施する

ドイツ国内の 120 を超える研究機関、組織および学協会は、各地域で「セキュリティ関連の研究における倫理委員会（Committee for Ethics in Security-Relevant Research）」（ドイツ語で KEF）を設置し、研究者や研究機関が自身の研究のセキュリティ関連の側面について抱える疑念に助言を与えている。この委員会は、ドイツ国立科学アカデミー・レオポルディーナ（German National Academy of Science Leopoldina）とドイツ研究振興協会（German Research Foundation、DFG）が 2014 年に導入し、2022 年に改訂版を発表した「セキュリティ関連の研究の取り扱いに関する勧告（Recommendations for Handling of Security-Relevant Research）」に従い設置された。この勧告は、セキュリティ関連の研究の問題に係る学術セクターの意識や科学の自己統治を強化することを目的としている。勧告によれば、セキュリティ関連の研究には、第三者が人間の尊厳、生命、健康、自由、財産、環境または平和共存を害する形で悪用し得る知識、製品または技術を生み出す可能性がある科学研究が含まれる。この種の研究は即座に悪用することが可能で、潜在的損害が著しい場合、「懸念あり（of concern）」として指定される。

KEF は、通常、分野横断的であるため、セキュリティ関連の研究の疑念に存するリスクや利益に重みづけをする際、倫理、法律、人文科学などの関連する分野の専門家と共に役割を果たす。 KEF は、悪用リスクにさらされている研究領域に関して助言を与え、定期的にイベントを開催することなどにより、自らの研究のセキュリティ関連の側面に対して研究者の意識を高める。また、カウンセリングや能力開発などを通じ、研究者が自身の研究が悪用されるリスクに対処し、これを軽減する上での責任を強化する重要な役割も果たしている。さらに、研究プロジェクトを倫理的に説明することを支援し、それにより、特に悪用のリスクが高い研究領域における資金提供申請の審査の精度を上げることに寄与している。さらに、KEF は相談業務の一環として倫理的評価を行うことにより、セキュリティ関連の研究を正当化することもできる。透明性を与え、倫理的考察を推進することにより、研究に対する社会の信頼を強化することにも役立っている。

KEF の設置および業務は、2015 年に DFG とレオポルディーナが設置した諮問機関である「セキュリティ関連研究の取り扱いに関する共同委員会（Joint Committee on the Handling of Security-Relevant Research）」の支援を受けている。この共同委員会は定期的にイベントを開催して、KEF 間の情報交換を促進し、KEF の能力を構築し、現時点で高リスクの研究領域に対する意識を高めている。