資料３

経済安全保障法制に関する有識者会議
第２～４回官民技術協力に関する検討会合
資料

国家間における経済安全保障上の重要技術の共同研究の推進について

２０２４年３月

経済安全保障分野に関する重要技術に係る国際動向等

2023年

5月　G7広島サミット

※　経済的強靭性・経済安全保障に関するG7首脳声明において、最先端の機微な技術が国際の平和と安全に悪影響を及ぼす事態を回避するため、適切に管理することに言及。

※　同月開催の科技大臣共同声明で、G7研究セキュリティ・インテグリティ作業部会の努力に対するコミットメントを確認

5月　豪　「国益にかなう重要技術リスト」更新、「重要技術に関する声明」を公表

※　高度製造・先端材料、AIなどの7分野・37技術を重要技術として特定。

6月　EU　経済安全保障戦略を公表

※　技術セキュリティと技術流出リスクの章にて公開と国際協力がEUの研究、イノベーションの核心であるとした上で、ホライゾン・ヨーロッパ等のEUによる助成がある研究成果の移転について評価する旨を言及。

7月　日EU定期首脳協議

※　経済安全保障のパートにおいて半導体等の研究開発について言及。

8月　日米韓サミット

※　首脳共同宣言で国立研究機関間の協力について言及。

10月　EU　経済安全保障のための重要技術分野に関する勧告

※　技術セキュリティと技術流出に関するリスクを評価する対象となる１０の重要技術のリストを選定。最もセンシティブで差し迫ったリスクをもたらす可能性が高いと考えられる技術分野として①先端半導体、②人工知能技術、③量子技術、④生物工学の4つの分野を特定。

10月　米EU首脳共同声明

※　AIをはじめとする重要新興技術の協力の促進について言及。

2024年

1月　加　「カナダの研究保護のための政府声明」を公表

※　機微技術研究分野のリスト、カナダの国家安全保障に危険を及ぼす可能性のある、軍、国防、国家安全保障機関に関係する指名済み研究機関のリストを公表。

1月　EU 経済安全保障パッケージの公表

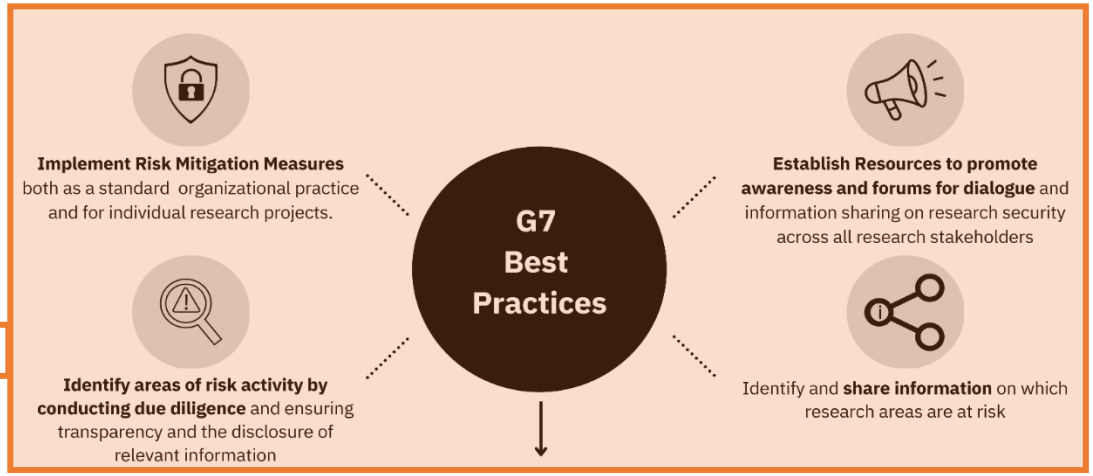
※　デュアルユースの可能性を有する技術の研究開発支援、研究セキュリティの向上などのイニシアティブを発表。

2月　G7研究セキュリティ・インテグリティ作業部会の「ベストプラクティス」文書の完成版を公表

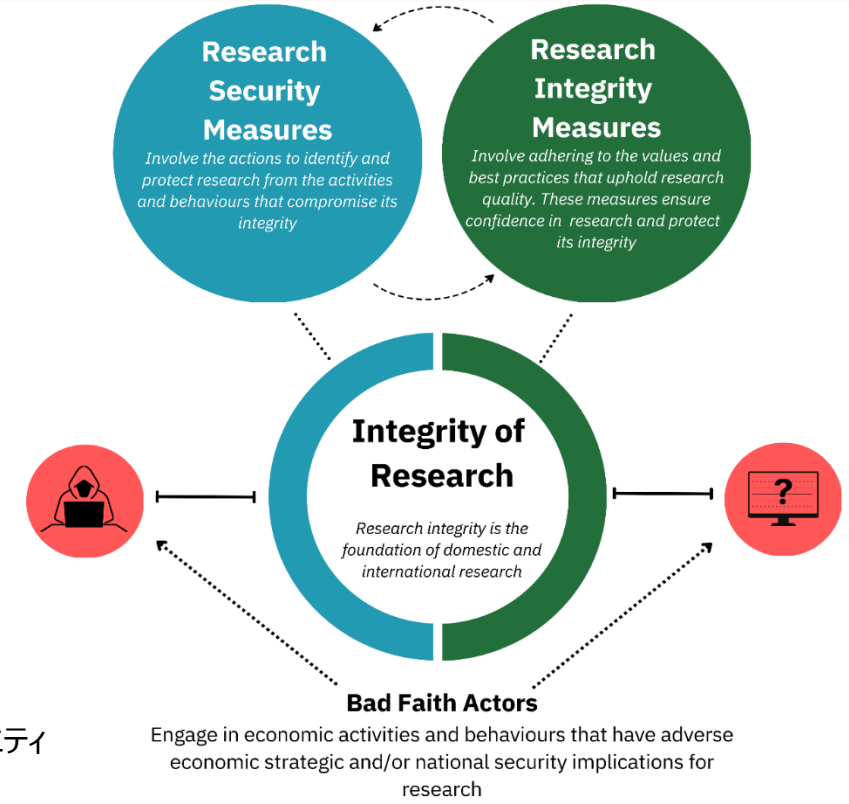
各国が経済安全保障分野に関する重要技術についての政策を公表。
2か国間、複数国間の協議の場においても、経済安全保障分野に関する重要技術について議論されており、国際協力の重要性・必要性が高まっている。

”安全でオープンな研究に向けたG7ベストプラクティス”

◆ 研究の保護に関して個々の利害関係者が全ての責任を負うのではなく、全ての利害関係者間における**共同責任(Shared Responsibility)**の考えの下、４つのベストプラクティスを整理



- 全ての研究関係者間で研究セキュリティとインテグリティに関する**対話・情報共有を行うための場や認識を増進させるリソースを確立**
- リスクにさらされている**研究領域の特定と情報共有**
- **デューデリジェンスを実施**し、透明性と関連情報の開示を確保することにより、**リスク活動の領域を特定**
- 標準的な組織慣行として、個々の研究プロジェクトについて、**リスクの軽減策を実施**



※ G7加盟国により研究エコシステムの状況・構造が異なることから、研究コミュニティのニーズに合わせてベストプラクティスは各国で異なる方法で実装され得る

(出典)”G7 Best Practices for Secure & Open Research”, Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, 2024.

「研究セキュリティ」の定義等（仮訳）

【明確な定義あり】

○ **米 国**

国家安全保障や経済安全保障に損害を与えるような研究開発の不正流用、それに関連する研究インテグリティの侵害、外国政府の干渉から研究事業を保護すること

【参照：Appendix: Definitions, GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT, Subcommittee on Research Security Joint Committee on the Research Environment, Jan 2022】

Research security – Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

【明確な言及あり】

○ **ＥＵ**

関連するリスクを管理すること。関連するリスクとは下記３つ。

①EUやEU加盟国の安全保障に影響を与えるような重要な知識、ノウハウ及び技術の望ましくない移転(例えば、第三国における軍事目的につながるもの)

②EUにおける学問の自由と研究の公正性を侵害する学生や研究者の間で特定の言説を拡散したり、自己検閲を扇動したりするために、第三国によって、または第三国から研究が道具化される可能性がある、研究に対する悪意ある影響

③EUまたはその他の地域を問わず、知識と技術が基本的価値を抑圧または損なうために使用される場合、倫理的または誠実な違反

【参照：Proposal for a COUNCIL RECOMMENDATION on enhancing research security, EUROPEAN COMMISSION, Jan 1st 2024】

SCOPE

1. For the purposes of this recommendation, 'research security' refers to managing risks related to:

(a) the undesirable transfer of critical knowledge, know-how and technology that may affect the security of the EU and its Member States, for instance if channelled to military purposes in third countries;

(b) malign influence on research, where research can be instrumentalised by or from third countries in order to diffuse certain narratives or incite self-censorship among students and researchers infringing academic freedom and research integrity in the EU;

(c) ethical or integrity violations, where knowledge and technologies are used to suppress or undermine fundamental values, whether in the EU or elsewhere.

○ **カナダ**

外国の脅威行為者の地政学的、経済的、安全保障上の利益の増進を助け、カナダに不利益をもたらす可能性のある知識、技術、データを保護する措置

【参照：Research Security Information Update – May 2021】

Broadly speaking, research security refers to the measures that protect knowledge, technologies, and data that could assist in the advancement of a foreign threat actor's geopolitical, economic, and security interests to the detriment of Canada's. The target assets can vary from applications in weapons of mass destruction programs (i.e., chemical, biological, radiological, and nuclear) to dual-use technologies (i.e., technologies with both civilian and military applications), such as artificial intelligence, quantum computing, and bio- and nanotechnology, to intellectual property and confidential information used for research.

○ **OECD**

研究セキュリティの確保とは、国家や非国家による研究への望ましくない干渉を防ぐことを意味し、その主な目的は、研究のエコシステムを保護し、正当な国益と経済的利益を守ること

【参照：Integrity and security in the global research ecosystem】

In a globalised research ecosystem, ensuring research security means preventing undesirable foreign state or non-state interference with research. The main goal of research security is to protect the research ecosystem and thus protect legitimate national and economic interests.

○ **G7**

研究セキュリティは、経済的、戦略的、国家的、国際的な安全保障のリスクをもたらす行為者及び行動から研究コミュニティを保護する活動を含む

【参照：G7 Best Practices for Secure & Open Research】

Research Security: involves the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks.

【その他】

オランダ、英国、豪州は、研究セキュリティに関する取組はあるものの、明確な定義づけや整理はやや異なる模様

※オランダ：「Knowledge Security」、英国：「Trusted Research」「Secure Innovation」のキャンペーン、豪州：「counter foreign interference」のためのガイドラインを大学セクターに発出

【参考】米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書33号（NSPM-33）

◆ 2021年1月、”**米国政府が支援する研究開発を外国政府の干渉や搾取から守るための行動を指示する**”ため、研究開発を行う関係連邦省庁や研究所、情報機関等に対し、国家安全保障大統領覚書（NSPM-33）を発出

◆ 研究セキュリティ・インテグリティの確保に関し、各関係機関に対する主な要求事項は以下のとおり

要請先機関	役割と責務
連邦省庁（研究開発関係）資金配分機関の長	1. 米国の**研究開発事業の参加者へ対する**（利益相反・責務相反の判別に資する）**情報開示の要求** 2. 研究セキュリティ・インテグリティに係るリスクの特定・管理に向けて**研究実施機関に対する協力** 3. （監察官や法執行機関等と協力し）**研究資金や研究セキュリティ・インテグリティに悪影響**を及ぼす可能性のある**情報開示を特定** 4. （監察官や法執行機関等と協力し）情報開示要件の不遵守が疑われる事案の調査 5.情報開示方針の違反や米国の研究セキュリティ・インテグリティを脅かすその他活動への関与に対し、適切かつ効果的な対応（契約打ち切り等）
国土安全保障省（DHS）長官	DHSが国務省と連携し、米国の**研究開発事業に参加している/参加予定の非移民学生及び交換訪問の外国人に係る国家安全保障上のリスクを審査**する責任（DHSが留学生及び外国人研究者に関する情報を適用法に基づき保有することを含む）を有す
国家情報長官（DNI）	米国の研究開発事業における安全保障に関連する**外国関係者の能力・活動・意図を特定・評価**するため、**インテル系コミュニティの取組を調整**
科学技術政策局（OSTP）長官	米国科学技術会議（NSTC）を通じて、連邦政府資金による**研究開発を外国政府からの影響から守るための活動を調整**し、研究セキュリティに係るリスクとそのリスクに対する連邦政府の取組に関する認識を高めるため、**米国のアカデミアへ働きかける**

具体的な取組事項

① 研究セキュリティのリスクと保護に係る認識の向上
② 情報開示の要件とプロセスの強化
③ アクセス及び参加の制限
④ 留学生・外国人研究者の審査
⑤ 情報共有
⑥ 研究セキュリティ教育
⑦ リスクの特定と分析
⑧ 国際研究開発協力の促進と保護

②情報開示の要件とプロセスの強化

（例）連邦省庁は研究開発関係者から下記の情報開示を要求し、資金配分機関はその方針を作成

Tier 1：研究代表者(PI)やその他の主要な研究者/PO/連邦研究所等の内部研究者
Tire 2：プログラム審査者/プログラム諮問委員　※Tier 2には「その他支援状況」の情報開示要求は不要

【開示要求事項】 ※現行及び応募中の情報を含む
- ・所属及び雇用
- ・その他の支援状況（国内外からのその他の資金提供、留学生等のリソース提供を含む）
- ・外国の政府等が主催するプログラムへの参加状況（人材採用プログラムを含む）
- ・国内外のその他の役職及び任命状況（非常勤や名誉職を含む）

③アクセス及び参加の制限

（例）連邦省庁は政府研究施設へのアクセスや利用状況を管理・追跡する方針とプロセスを確立

④留学生・外国人研究者の審査

（例）国務省は、DHSと調整し、留学生や外国人の審査プロセスを強化
⇒ビザ申請の審査で以下情報を収集;雇用・職歴/経済的支援源/教育歴/現在・過去のR&D連携・プロジェクト/現在・申請中の外国政府主催プログラムへの参加状況/学習・研究プログラム/予定している勤務先機関・場所

（例）DHSは国務省からの上記情報を検索可能な中央データベースに含めることの実現可能性と有用性を評価

（参考）研究インテグリティ（Research Integrity）に係る調査・分析報告書, 令和4年度内閣府委託事業, 公益財団法人未来工学研究所

【参考】 米国科学財団（NSF）における研究セキュリティへの対応

◆ 研究セキュリティ政策を統括する組織の設置

CHIPS科学法の要請に基づき、NSF全体の**研究セキュリティ方針に関する調整等を実施**する、**研究セキュリティ戦略・政策室を設置**

◆ 情報共有分析機構の設置

CHIPS科学法の要請に基づき、**外国政府による不当な干渉への対処、研究セキュリティ確保のための意思決定を支援するための客観的根拠を提供**する外部機関、**研究セキュリティ・インテグリティ情報共有分析機関（RSI-ISAO）を設立予定**

◆ 情報開示要求

NSPM-33実施ガイダンスの要請に基づき、国家科学技術会議（NSTC）研究セキュリティ小委員会が、**各政府機関用の共通情報開示フォーム**※を作成（NSFのHPで公開）

→NSFでは、研究費申請と授与の方針と手順のガイド（PAPPG）を改訂し、**経歴、現在および申請中の支援、研究協力者やその他の関係者の開示要求を追加**

※研究分野は限定していない。

◆ 研究セキュリティトレーニングモジュールの構築

DoD、DoE、NIH等と連携し、下記の内容の**オンライン研究セキュリティトレーニングモジュールの構築を推進**

NSFのHPで公開されており、無料でダウンロードし活用できる

《トレーニング内容》

- なぜ研究セキュリティが大切か？
- 競争的資金助成とリスク管理・低減（技術盗用リスク）
- 研究活動における国際協力
- 情報開示の重要性

（参考）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, CRDS、2024年

【参考】 米国DoDにおける研究セキュリティへの対応

◆ 2023年6月、DoD/USD(R&E)は国防授権法(NDAA)に基づく外国エンティティ・リストを更新するとともに、NSPM-33を踏まえ、**DoDファンディングを受ける全ての基礎研究プログラムに対し、外国からの影響によって生じる潜在的な利益相反・責務相反の審査を受ける義務を課す**方針を示し、DoDプログラム管理者向けにリスクを適切に軽減するためのガイダンスを提示

Counter Unwanted Foreign Influence on Department-Funded Research at Institutions of Higher Education

	外国人材採用プログラム	資金源	特許	エンティティ・リスト
不可	[2024.8以降] • 2022年CHIPSプラス法10638条(4)(A)(i)-(ix)のいずれかの基準に該当する悪意ある**外国人材採用プログラム(MFTRP)**に参加 • **MFTRPへの参加を禁止する方針がない**機関	—	—	—
リスク緩和措置がない場合不可	[2022.8以降] 2022年CHIPSプラス法10638条(4)(A)(i)-(ix)のいずれかの基準に該当する**外国人材採用プログラム(FTRP)**に参加	**懸念国(FCOC)**または**FCOCとつながりのあるエンティティ**からの資金援助	米国政府が支援する研究から生じた**非公開特許**のうち、米国への提出前に**FCOC**へ提出されたもの、または**FCOCとつながりあるエンティティ**に代わって提出されたもの	[2022.8以降] 下記リスト※のエンティティと**関連**(*association with*) [2019.10以降] 下記リスト※のエンティティと**提携**(*affiliation with*)
リスク緩和措置を推奨	[2019.10から2022.8まで] FTRPに参加 [2022.8以降(2024.8まで)] MFTRPへの参加を禁止する方針がない機関	[2019.10から2022.8まで] FCOCまたはFCOCとつながりのあるエンティティからの資金援助	米国政府が支援する研究から生じた**公開特許**のうち、米国への提出前に**FCOC**へ提出されたもの、または**FCOCとつながりあるエンティティ**に代わって提出されたもの	[2019.10から2022.8まで] 下記リスト※のエンティティと関連 [2019.10まで] 下記リスト※のエンティティと提携
リスク緩和措置を提案	[2019.10まで] FTRPに参加 [2019.10以降] **共同研究者**(論文共著者)がMFTRPまたはFTRPへ参加	[2019.10まで] FCOCまたはFCOCとつながりのあるエンティティからの資金援助	米国政府が支援する研究から生じた**非公開特許**のうち、米国への提出前に**非懸念国**へ提出されたもの、または**非懸念国とつながりあるエンティティ**に代わって提出されたもの	[2019.10まで] 下記リスト※のエンティティと関連 [2019.10以降] **共同研究者**(論文共著者)が下記リスト※のエンティティと提携、または商務省産業安全保障局(BIS)の**拒否人物リスト(Denied Persons List)**に該当
リスク緩和措置は不要	MFTRPやFTRPに不参加	FCOCやFCOCとつながりのあるエンティティから資金援助がない	米国政府が支援する研究から生じた特許について、他国に先行して米国に提出している	• 下記リスト※のエンティティと関連・提携なし • 共同研究者(論文共著者)がBISの拒否人物リストに該当しない

※エンティティ・リスト(各リストの改訂含む)
・BIS Entity List　・Annex of Executive Order (EO) 14032, supersending EOs　・2021年NDAA 1260H / 2019年NDAA 1286

【参考】 米国DoE/NNSAにおける研究セキュリティへの対応

◆ DoE/NNSAにおいては、NSPM-33実施ガイダンスを踏まえ、2022年６月にFinancial Assistance Letter(FAL 2022-04)を発出。**現在・保留中の支援情報についての開示要件として、モデル書式を設定している旨を説明。さらにFY2023に、情報開示要件の更新を予定。**

【FAL 2022-04 の概要】

- DoE/NNSAの大半のプログラムオフィスは、現在・保留中の支援情報の開示を要求しているが、開示に含めるべき情報の種類についてはばらつきがあった。
- NSPM-33実施ガイダンスを踏まえ、すべてのDoE/NNSAプログラムオフィスに、一貫した現在・保留中の支援情報の開示要件を組み込むことを義務付けるとともに、モデル書式を設定。
- 現時点では、グラントオフィサーは、申請者が申請書のどこに現在・保留中の支援情報の開示を含めるべきかなどを判断する裁量を持っているが、DoEはこの方法を再検討する予定で、FY2023に、現在・保留中の支援情報の開示要件の更新を予定。(→第二段階)

【Appendix 1(モデル書式)】

- 「現在・保留中の支援」は、重複、過剰な責務、潜在的な利益・責務相反、及び他のすべての支援源の可能性を特定できるようにすることを目的としている。
- 申請書の一部として、PI、プライム申請者及び提案された補助金レベルの各シニア／キーパーソンは、すべてのスポンサー支援された活動、アワード、アポイントメントのリストを提出しなければならない。
- (以下のいずれも含む：1. 有給か無給か、2. 条件付き贈与か条件なし贈与か、3. 常勤か非常勤か任意か、4. 教員か客員か非常勤か名誉か、5. 現金か現物か、6. 外国か国内か、7. 政府か民間か、8. 個人の研究を直接支援するか、学生・研究スタッフ・スペース・設備・その他の研究費を支援することによって個人を間接的に支援するか)
- 「外国政府主催の人材採用プログラム」への関与はすべて、「現在及び未決の支援」に特定しなければならない。

- 活動ごとに、以下の項目を記載することとする。
  - 活動のスポンサー又は資金の提供者
  - アワードの番号又はその他の識別番号
  - アワードや活動のタイトル。アワードや活動のタイトルが説明的でない場合、提案された研究との重複や相乗効果を明らかにするために、実施されている研究の簡単な説明を追加する。
  - 直接費、間接費、コストシェアを含む、アワード又は活動の総コスト又は価値。応募中の提案については、要求した資金の総額を提示する。
  - アワード期間(開始日～終了日)。
  - そのアワード又は活動に費やされる1年あたりの作業人月。

(参考) FAL 2022-04 Department of Energy Current and Pending Support Disclosure Requirements for Financial Assistance
令和 4年度科学技術基礎調査等委託事業(令和５年３月、(公財)未来工学研究所)pp.66-68

【参考】研究活動の透明性及び説明責任を果たすための研究インテグリティの確保に係る対応について

政府としての対応方針（2021年4月27日統合イノベーション戦略推進会議で決定）

※大学・資金配分機関の専門家等から構成された有識者検討会の提言（2021年3月公表）を踏まえた方針

①研究者自身による適切な情報開示

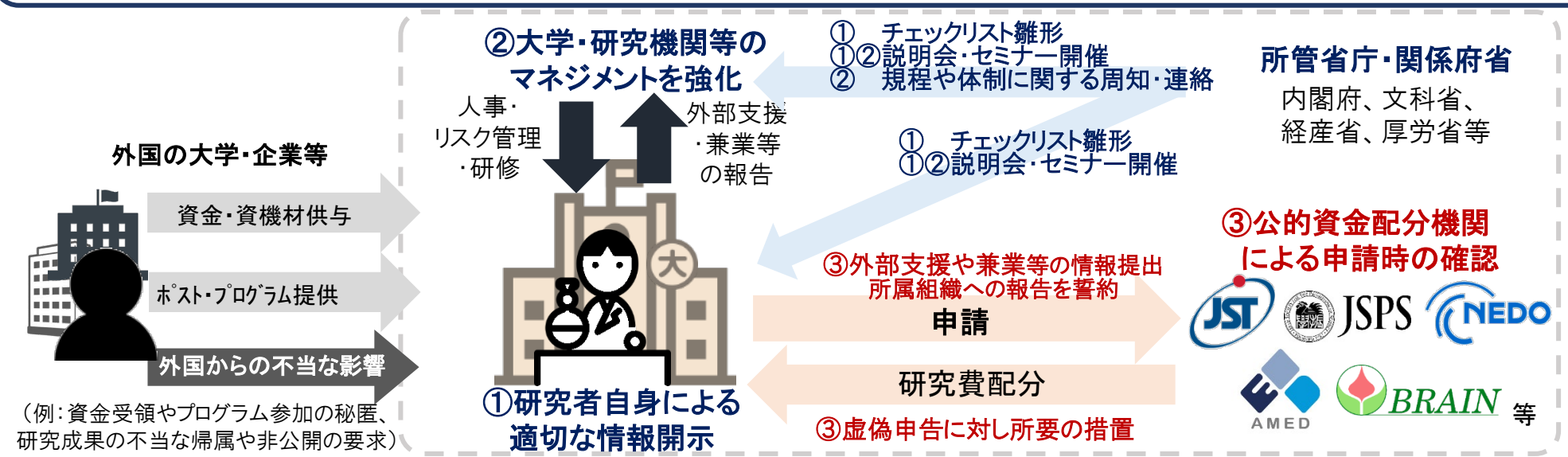
- 研究者、所属機関向けのチェックリスト雛形（機関向けを2023年6月29日改定）を作成、公表・配布【内、文科等】
- 研究者、所属機関等への説明会・セミナーを開催　【内、文科等】

②大学・研究機関等のマネジメントを強化

- 研究者、所属機関等への説明会・セミナーを開催　【内、文科等】
- 関係の規程や体制の整備に関する周知・連絡　【所管省庁】
  （→ 2022年度にﾌｫﾛｰｱｯﾌﾟを実施、2023年度は改定チェックリストも踏まえたﾌｫﾛｰｱｯﾌﾟを継続）

③公的資金配分機関による申請時の確認

- 競争的研究費に関するガイドラインを改定 2021年12月17日　【内、関係省庁】
  - 国外も含む外部からの支援や兼業等の情報の提出、所属機関への適切な報告の誓約を求める
  - 利益相反・責務相反に関する規程の整備の重要性を明示、必要に応じて状況確認
  - 虚偽申告に対し、公表、不採択・採択取消し、研究費返還、最長5年間の応募制限（2022年度の公募から反映）



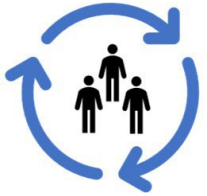
【参考】 国立研究開発法人の機能強化に向けた取組

- 国立研究開発法人（国研）は、我が国の科学技術・イノベーションを支える中核的な機関であり、これまで以上に研究力及びイノベーション創出力を高めていくことが求められている。
- 今後も研究人材や研究マネジメント人材、知財人材などの優秀な人材を国内外から集めるとともに、国際共同研究等のオープンイノベーションを活性化していく必要があるが、人材確保競争の激化や専門人材不足、研究成果の社会実装、**研究セキュリティ・インテグリティ確保に関する問題意識が顕在化**しており、以下の とおり対応の方向性を取りまとめる予定。

【対応の方向性と期待される成果】

対応の方向性（input）

① 柔軟な人事・給与の仕組みによる多様な人材の確保
② 各法人の連携・協力による研究マネジメント人材等の育成
③ 適切な知的財産の管理による研究成果の社会実装の推進
④ **健全な研究推進の前提となる研究セキュリティ・インテグリティの確保**



▼

対応に伴う効果（output）

- 多様で優秀な人材が集まるイノベーティブな環境の醸成
- 法人間連携による、より効率的・効果的な業務実施
- 外国機関との連携や企業等との共同研究の機会拡充
- 国家的課題への機動的な対応、安心して研究に専念できる環境づくり

▼

期待される成果（outcome）

- イノベーション創出につながる多様な人材の確保・育成
- 研究力の向上、研究成果の社会実装
- 組織横断的な業務一体化の推進・産学官連携の活性化・人材の流動性向上

■ 今後のスケジュール（予定）

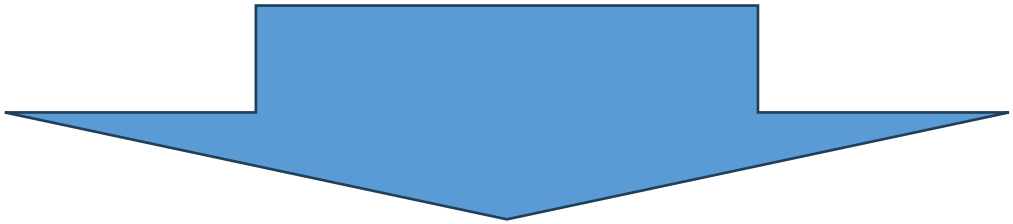
2～3月　関係府省・国研協との調整
3月中　関係府省申し合わせ

今回の対応は、産総研やJAXAの事案等を踏まえて喫緊に対応すべき取組を整理したもの。
引き続き国研協や現場の国研の意見等も踏まえながら、戦略的な国研機能強化に向けて取り組む予定。

※総合科学技術・イノベーション会議（第71回）資料より、検討会合用に事務局で一部を赤字に変更

○国家間における経済安全保障上の重要技術の共同研究の推進について

同盟国・同志国各国が経済安全保障上の重要技術についての政策を公表。
当該政策中、又は2か国間、複数国間の協議でも当該重要技術について同盟国・同志国との連携が議論され、**国際協力の重要性・必要性が高まっている**。
併せて、国家安全保障の確保や、経済安全保障上重要な共同研究を適切に推進する等の観点から、**米国等では研究セキュリティについて議論を深めており、今後、我が国においても同盟国・同志国と同等な取組を検討していく必要がある**。



こうした同盟国・同志国の制度やその実態を踏まえ、我が国が経済安全保障上の重要技術の育成に関して、相手国と対等な立場を維持し、国際協力を深化、拡大させていくためにどのような対策が必要であるか。

本日ご議論いただきたいこと（案）

G7研究セキュリティ・インテグリティ作業部会において、以下の4分野におけるベストプラクティスが整理されているところ、我が国においても必要な対策を検討するべきではないか。

- リスクにさらされている研究領域の特定と情報共有
- デューデリジェンスを実施、透明性と関連情報の開示を確保することにより、リスク活動の領域を特定
- 標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施
- 研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立

➢ リスクにさらされている研究領域の特定と情報共有

米国：NSPM-33により、研究セキュリティとして、米国政府が支援する研究開発を外国政府の干渉や搾取から守るための行動を各政府機関に指示。
　NSFのように、研究コミュニティにNSFから資金提供する際に、研究セキュリティと研究インテグリティとを一体的にとらえて確認を進めていく例や、DoDのように、DoDが支援する基礎研究は、DoDから研究コミュニティに資金提供をする際に、一定のエンティティとの関係性の開示を求める例が存在。

カナダ：研究セキュリティについて、加政府として11の機微技術分野のリストを公表。加政府の研究開発支援を受ける場合に、当該11分野に該当すれば、一定のエンティティとの関係性について開示を求めている。

英国・豪州・オランダ：研究インテグリティと一体的にすすめており、リスクにさらされている研究領域としての特定はない。
　なお、各国の関係省庁が国家安全保障の観点から重要な技術の選定等を行っている。

日本：研究インテグリティとしては、諸外国と同様、対象となる研究領域についての区別は存在しない。
　なお、経産省の有識者会議において、経済安全保障上重要な物資・技術の特定と政策アプローチについて検討例あり。

- ✓ **各国では、研究コミュニティを対象として研究セキュリティ・インテグリティの取組を実施している。その中で、研究インテグリティの取組みを基礎としつつも、更にリスクの高い研究領域を特定し、リスクマネジメントの観点から必要とする場合に、より一層の対策を求めている。**
- ✓ **我が国においても、海外の同志国と同様、研究インテグリティの取組を基礎としつつ、更に、まずは国際的な共同研究の取組みを視野に入れ、政府の資金支援を行う際の特定の分野※における更なる対策について、資金支援を行う各省庁において、検討を行うことが必要ではないか。**

※例えば、経済産業省の有識者会議の資料のように、研究セキュリティを更なる取り組みを要する経済安全保障上の重要技術として、経済安全保障の観点から技術優位性のある分野（これから技術優位性を確保しようとする戦略分野も含むもの）とすることが一案。

【参考】経済安全保障上重要な物資・技術の特定と政策アプローチ

※経済産業省：経済安全保障に関する産業・技術基盤強化のための有識者会議（２月2日）資料３より

- コンピューティング、クリーンテック、バイオテック、防衛等の分野は、将来にわたる我が国の経済安全保障上の産業・技術基盤として不可欠。それぞれの分野で特に**重要なサプライチェーンに注目し、その維持・発展に政策資源を集中的に投入**する。
- 経済安全保障上重要なサプライチェーンにおいて鍵を握る**物資・技術を特定したうえで**、技術革新の動向、**我が国における相対的な優位性、対外依存度を分析・把握**し、強靱化に向けた**適切な政策手段を当てはめていく**。
- また、**経済安全保障上重要な物資を改めて洗い出した上で、リスク・脅威に対応した適切な政策手段を整理し、経済安保法の「取組方針」に反映させる。**

＜経済安全保障の観点から重視すべき物資・技術の整理＞

	将来の不可欠性・自律性の獲得 ① 破壊的技術革新が進む領域	不可欠性の維持 ② 我が国が技術優位性を持つ領域	自律性の回復 ③ 技術のコモディティ化・対外依存の領域
コンピューティング	次世代コンピューティング （例：量子コンピュータ・先端半導体）	製造装置・部素材・機器 等 （例：MLCC・光ファイバー・複合機）	レガシー半導体 等
クリーンテック	次世代クリーンテック （例：ペロブスカイト・全固体電池）	製造装置・部素材 等	重要鉱物 等
バイオテック	バイオものづくり （例：合成生物学・バイオファウンドリ）	検査・分析装置 等	抗菌性物質製剤 等
防衛・宇宙関連分野	防衛・宇宙分野の先進技術	航空機部素材 等 （炭素繊維・エンジン用素材）	航空機部素材 等 （大型鍛造・鋳造）
各領域に対する取組の方向性	技術優位性の創出	機微技術の流出・拡散防止	過剰依存構造の防止・是正

※ 点線枠内の物資・技術は例示

- デューデリジェンスを実施、透明性と関連情報の開示を確保することにより、リスク活動の領域を特定
- 標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施

米国：NSPM-33実施ガイダンスに基づき、各政府機関共通の情報開示フォームを作成。
各政府機関は、資金支援をする際、申請者による各項目の情報の開示を求める。

カナダ：**機微技術研究分野リスト、指定研究機関リスト**を公表。リスク軽減のための大学・研究機関等によるデューデリジェンス（DD）を推奨。また、今春より、**政府から資金支援を受ける場合は、申請者に対して両リストにもとづく所要の確認を求める予定**。

英国：英国の大学・研究機関等がリスク情報を活用した意思決定ができるように、政府が一般的な**共同研究等についてのチェックリストを作成するとともに、**問い合わせに対して助言と緩和策を提供する体制を整備。更に、英国政府のFAである**UKRIは、資金支援をする際、大学・研究機関等に対して、当該チェックリストに基づく所要の行動を求めている**。

日本：研究インテグリティの確保に係る対応について、政府としての方針に基づき、関係部局において研究者、所属機関向けのチェックリスト雛形を作成、公表・配布

→各国政府は、**研究セキュリティ・インテグリティに関して、特に政府からの資金支援の決定時における情報開示に関するガイドラインや具体的な開示項目の作成。**

- ✓ **我が国においても、政府の資金支援を行うに際して、デューデリジェンスの実施方法、デューデリジェンス実施に資するようなチェックリスト等の検討が必要ではないか。**
- ✓ **その際、公開可能な研究全般については、研究セキュリティ・インテグリティの取組が実効性を持った実施に繋がるよう、ガイドライン・チェックリスト等を作成し、関連機関において所要の確認をするといった実態的に有効な手法についての検討が必要ではないか。**

本日ご議論いただきたいこと（案）

➢ 研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立

→米国では、NSPM-33において研究セキュリティ・インテグリティの確保に関し、連邦省庁（研究開発関係）資金配分機関の長、国土安全保障省（DHS）長官、国家情報長官（DNI）、科学技術政策局（OSTP）長官に対して対策を要求。

→各国では、水際対策や研究コミュニティ等からの相談・助言やアウトリーチ活動等において、**研究関係機関以外も参加して政府関係機関間の連携促進に関する取組**を実施。

✓ **我が国においても、研究資金を提供する省庁・機関のみの活動だけでなく、水際対策なども含め、捜査・公安当局、法執行機関等も含めた政府内の関係機関の連携を促進していくべきではないか。**

✓ **研究資金を提供する省庁・機関等を中心に、研究機関等からの相談等の窓口設置や政府と研究コミュニティとの双方向の情報交換の場の創設やその機能の強化について検討が必要ではないか。**

経済安全保障上の重要技術に係る研究開発成果の社会実装と技術流出対策の検討

２０２４年４月

これまでの技術流出に関する主要な報道等

【主要な報道】

2018年　高周波フィルタ世界シェア６割のBroadcom(元米国企業をシンガポール企業が買収)がQualcommの買収を計画

※　対米外国投資委員会(CFIUS)は中国への技術流出を懸念し「国家安全保障に対する脅威」を理由に買収停止を命令。Broadcomはその後本社を米国に移転。

2020年　日本電波工業はSAWフィルタを手掛ける子会社の株式を中国企業に譲渡

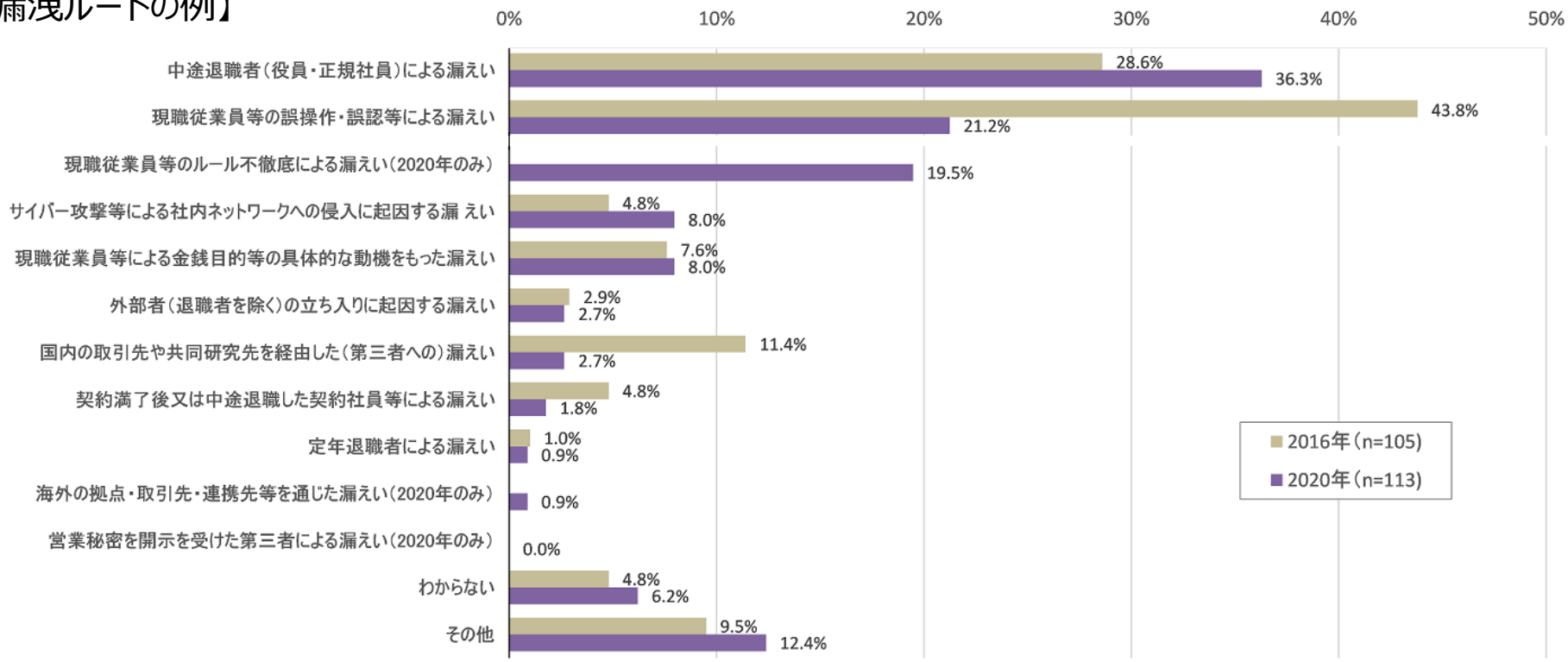
米司法省は天津大学教授をBAWフィルタ技術の産業スパイで有罪判決

2021年11月　パナソニックは、保有するフィルムコンデンサーの特許が侵害されているとして、中国電子部品メーカーのアモイ・ファラトロニックを提訴

2023年6月　産総研職員が不正競争防止法の容疑で逮捕

※　産総研で行った研究の成果を中国企業に漏えいしたとして、警視庁公安部は産総研の主任研究員(中国籍)を不正競争防止法違反(営業秘密の開示)容疑で逮捕

【情報漏洩ルートの例】



【出典】 情報処理推進機構HP：https://www.ipa.go.jp/archive/security/reports/2020/ts-kanri.html （3月29日確認、赤枠削除）

米国「CHIPS法」（2022年8月成立）

- **半導体関連の設備投資等の支援が可能な基金**を含め、**５年間で計527億ドル（約7.6兆円）**の**資金提供**。また、半導体製造・装置の**投資課税**についても、**4年間の25%の税額控除が可能に**。
- 助成対象者から安全保障上の懸念国への投資等を禁じるガードレール条項も含まれている。

		支援策	担当機関	金額（5年間）	支援内容
半導体	予算（全527億＄）	①半導体関連投資等補助基金	商務省	390億＄	✓ **半導体及び関連材料・装置**の製造・組立・検査・先端パッケージ・R＆Dに関して、米国内の施設及び設備の**新増設・刷新を財政的に支援**（融資・債務保証含む）
		②R＆D基金	商務省	110億＄	✓ NSTC、国家先端パッケージ製造プログラム、その他の研究開発、人材開発プログラム
		③防衛基金	国防省	20億＄	✓ マイクロエレクトロニクス・コモンズ（大学発のプロトタイプ作成、技術の「研究室から工場へ」、人材育成）
		④国際技術保障とイノベーション基金	国務省 DFC等	5億＄	✓ 情報通信技術セキュリティや半導体サプライチェーンに関する有志国政府との協力を支援
		⑤人材育成基金	NSF	2億＄	✓ 近い将来不足する国内の半導体人材育成の開始
	税制	⑥投資減税	財務省	-	✓ **半導体製造施設の建設・製造装置、半導体製造装置製造**に対する投資について、**25%の税額控除**
ORAN（予算）		公共ワイヤレス通信サプライチェーン基金	商務省	15億＄	✓ OpenRANやソフトウェアベースのワイヤレス通信技術促進のための革新的技術へ支援(※)④基金でも通信分野へ支援

ガードレール条項

１）【助成】助成期間中における助成対象者による**懸念企業（中露等国営企業等，米国制裁指定企業等）**への安全保障上脅威となる**共同研究・技術ライセンスの禁止**。
２）【助成及び税額控除】助成・税額控除適用対象者に対し、**中国**等の**国家安全保障上懸念を有する特定国**における28nm未満の**先端半導体（レガシー半導体は除く）製造施設**の**新規建設及び製造能力の拡大**を**禁止**。(財政支援開始後10年間適用)

（注）$1=145円で計算。（出所）米国上院HP

【出典】 第９回 産業構造審議会 経済産業政策新機軸部会（2022年11月２日） 資料３

技術流出経路に応じた現状・課題

技術流出の経路は様々であり、「モノ」「カネ」「ヒト」といったそれぞれの**技術流出経路**が存在している中、**特に政府からの資金支援を行う研究開発プロジェクトに関して、入口から出口までの段階に応じた「ヒト」による技術流出等への対策が課題**

流出経路	現状	課題例
「モノ」による技術流出等（輸出管理等）	◆ 海外進出、共同研究、ライセンス供与など、日本企業が意思をもって行う技術移転 ◆ 軍事転用可能な技術は、**外為法（輸出管理）**の対象	◆ これまで原則として国際レジームに基づき、管理対象を**兵器不拡散・過剰蓄積防止の考え方に限定**。 ◆ また、国際レジームではコンセンサス形式を前提とするため、我が国として管理すべきと考える技術を特定しても、**コンセンサス形成に時間がかかる**。
「カネ」による技術流出等（投資管理等）	◆ 対内直接投資に基づく企業買収 ◆ 対象業種については、**外為法（投資管理）**の対象	◆ 機微技術獲得を目的とした懸念ある投資の増加、**内外の経済安保を巡る状況変化に即して投資管理の在り方を適宜、見直すことが必要**。 ◆ 外国投資家や市場の動きにも配慮しつつ、**必要な経済安全保障の維持・強化と投資促進のバランス**の実現を図ることが必要。
「ヒト」による技術流出等	◆ 引き抜きなどによる技術者の転職 ◆ 転職に伴い営業秘密を漏洩した場合は不競法の対象となるが、転職そのものを制限する法令はない ◆ 営業秘密を不正な方法により取得、開示等する行為 ◆ 適切な営業秘密管理を行っている前提で、**不競法**の対象	◆ 転職時に秘密管理や競業避止などの**誓約書**を求めるケースもあるが、**拒否されることもあるなど、実効性が不明であり、そのことを前提とした営業秘密管理が必要。** ◆ 何を営業秘密として扱うかは**企業自身の判断に委ねられる**ため、必ずしも国として重要な技術が適切に管理されているとは限らない。

※ 第３回経済安全保障に関する産業・技術基盤強化のための有識者会議（2月2日）
資料３「経済安全保障に関する産業・技術基盤強化アクションプラン（策定後の進捗と今後の方向性）」を参考に、事務局にて作成

【参考】 検討中の技術流出対策例

● 技術流出対策は喫緊の課題。時間軸を考慮し、できることから早急に取り組む必要。

技術移転（輸出管理）

- ◆ 現在、産業構造審議会・安全保障貿易管理小委員会では、**輸出管理制度の見直しに向けた議論をしている。**
- ◆ 特に、貨物と異なり、技術は一度流出すれば管理が難しいため、**技術に注目した新たな管理の在り方**が、重要な論点。
- ◆ **今春を目途に中間報告を取りまとめる予定**であり、これを踏まえて、具体的な制度改正や体制整備を進めていく。

買収（投資管理）

- ◆ 関係省庁、地方支分部局との連携も通じて、国内産業界や投資家も含めた**対話や情報提供・収集を強化**する。また、**審査・モニタリング体制の更なる強化**を図る。
- ◆ 審査対象業種につき、**軍事転用防止、重要サプライチェーンの途絶防止等の観点で、業種の加除につき不断の見直しを行う。**
- ◆ 制度面について、2019年外為法改正時に「施行5年後の状況」の検討が求められていることも勘案した上で、**投資管理制度の在り方について検討する。**

人材流出

- ◆ 人を通じた技術流出を防止するためには、**就職時や転職時などにおける営業秘密管理を徹底**することが必要だが、就職機会の公平性や転職の自由の観点から、**対応に躊躇する企業の声**も多く聞かれる。
- ◆ 就職時から退職後まで、企業がどのように人材管理を行うべきかといったガイドライン整備を含め、他国の例も参考に対応を検討。

関連

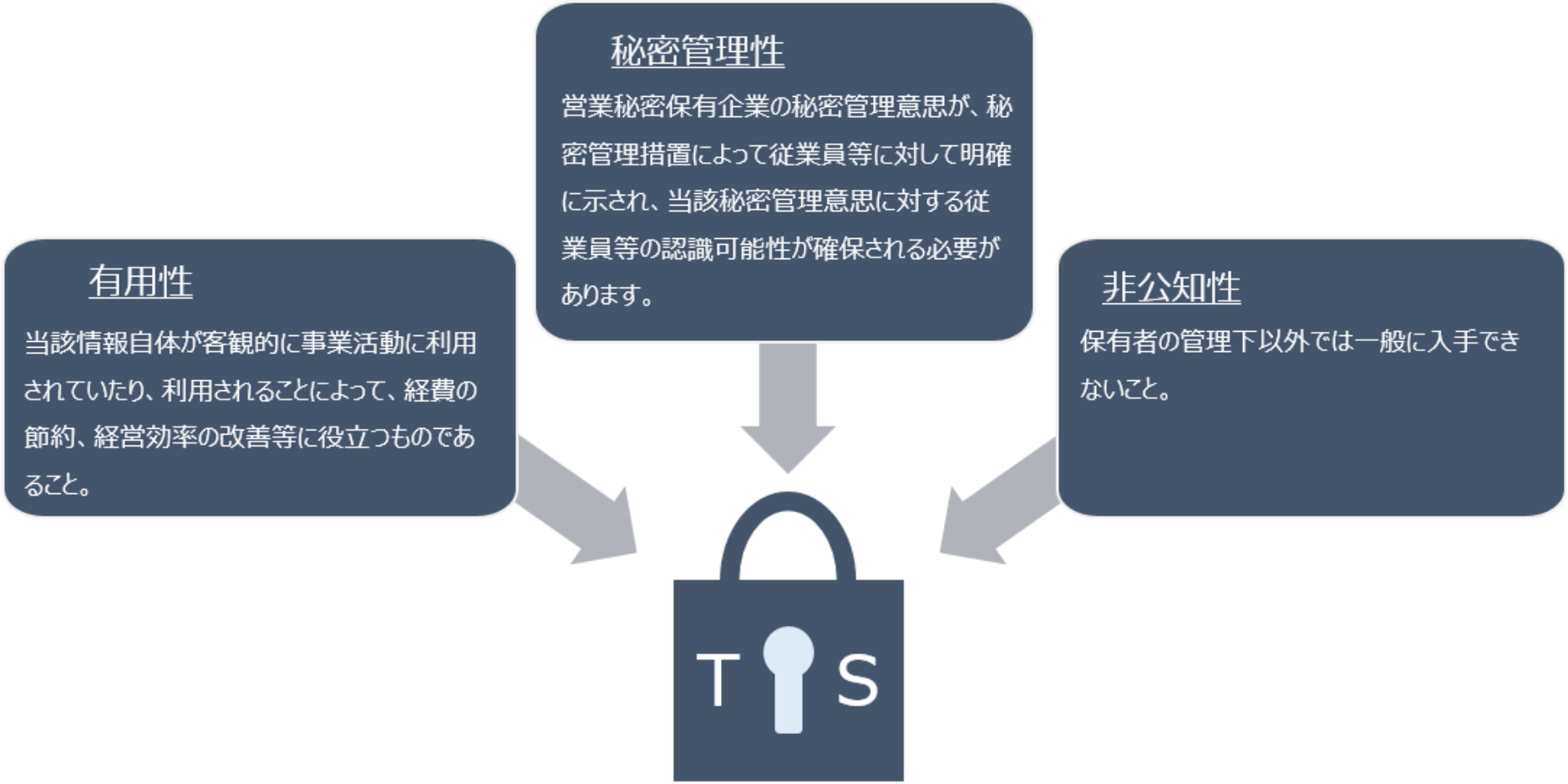
不正取得・開示（営業秘密管理）

- ◆ 経済安保推進法に基づくサプライチェーン支援（半導体等）では、技術管理の徹底を**採択要件として設定。**今後、**国費で行う重要技術開発プロジェクト**に関し、**同様の措置を拡大**していく。
- ◆ 他方、一律の要件化は、特に中小・ベンチャーの参入障壁となり、イノベーションの阻害要因に。このため、事業の性質に応じ、適切な技術管理を行っている場合に**優遇すること**や、管理経費を**支援対象**とすることも検討。

※ 第３回経済安全保障に関する産業・技術基盤強化のための有識者会議（2月2日）
資料３「経済安全保障に関する産業・技術基盤強化アクションプラン（策定後の進捗と今後の方向性）」を参考に、事務局にて作成

【参考】 不正競争防止法と営業秘密

不正競争防止法では、企業が持つ秘密情報が不正に持ち出されるなどの被害にあった場合に、民事上・刑事上の措置をとることができる。そのためには、その秘密情報が、不正競争防止法上の「営業秘密」として管理されていることが必要



【出典】 経産省HP： https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html （3月29日確認）

【参考】 技術流出防止と不正競争防止法（１／２）

1.営業秘密侵害罪

■ **概要**

不正競争防止法では、「営業秘密」に対する様々な不正行為を不正競争と定めて、違反・侵害に対し、違反者への罰則（刑事措置）を規定している。

■ **主な対象行為**

- **図利加害目的**で、詐欺等行為又は管理侵害行為によって、営業秘密を不正に取得・使用・開示する行為（例：産業スパイによる営業秘密の不正窃取）
- 営業秘密を保有者から示された者が、**図利加害目的**で、その営業秘密の管理に係る任務に背き、（イ）媒体等の横領、（ロ）複製の作成、（ハ）消去義務違反＋仮装、のいずれかの方法により営業秘密を領得・使用・開示する行為（例：従業員による営業秘密の持ち出し）
  - 「**不正の利益を得る目的**」とは、公序良俗又は信義則に反する形で不当な利益を図る目的のことをいい、自ら不正の利益を得る目的（自己図利目的）のみならず、第三者※に不正の利益を得させる目的（第三者図利目的）も含まれる。
    ※ 「第三者」には、ライバル関係にある企業・研究機関などだけでなく、**外国政府機関・関係者なども含まれ、これらの相手への開示なども処罰の対象となる**。

■ **国外犯処罰**

日本国内において事業を行う営業秘密保有者の営業秘密については、日本国外での不正取得・不正使用・不正開示行為も処罰対象。

■ **法定刑**

自然人：**10年以下の懲役若しくは2,000万円**（**海外使用等は3,000万円**）**以下の罰金**又はその併科

2.技術流出に対する不正競争防止法による対処

海外への技術流出に対して、不正競争防止法によって適切に対処できるよう、累次法改正を行い、**①目的規定の改正**や**②国外犯処罰規定の創設・拡大**等を行ってきた。

① 目的規定の改正について

- **平成21年改正により**、**外国政府を利する目的等による営業秘密の 不正な使用・開示等がその対象となるよう**、営業秘密秘密侵害罪の目的要件を「不正の競争の目的」から**「不正の利益を得る目的で、又はその保有者に損害を加える目的」（図利加害目的）**に改めた。

② 国外犯処罰規定の創設・拡大について

- **平成17年改正により**、営業秘密の**日本国外での不正使用・開示行為のみを処罰対象**とした。
- **それに加えて、平成27年改正により**、海外からの侵害（特に海外からの営業秘密不正取得行為）に対して広く刑事罰の抑止力をもって保護する必要から、**不正取得・領得行為にまで拡大**した。また、日本国外での侵害行為（不正開示・不正使用等）に対して、通常よりも重く処罰が可能とする規定**（海外重罰規定）を導入**した。

【出典】 第２回知的財産戦略本部構想委員会（2024年2月14日）
資料３「技術流出と不正競争防止法」

【参考】 技術流出防止と不正競争防止法（２／２）

3.逐条解説による解釈の明確化

■ 問題意識

- 我が国企業・研究機関から海外への技術流出が、依然として続いている。
- こうした中、外国の法令遵守のために、日本の不正競争防止法に違反する行為がなされる可能性が懸念される。
- 技術流出事案に適切に対応するため、以下の点を明確にする必要がある。
  - ① **外国政府を利する目的は「図利」目的（主観的構成要件）に該当する。**
  - ② **外国法令に基づく行為であること自体は違法性阻却事由に該当しない。**

■ 逐条解説における対応

① 平成21年改正により目的要件を**「不正の利益を得る目的で、又はその保有者に損害を加える目的」（図利加害目的）**に改めた際に、逐条解説において、以下の点を明記した。

- 「**不正の利益を得る目的**」とは、自ら不正の利益を得る目的のみならず、**外国政府・関係者を含む第三者に不正の利益を得させる目的も含まれる**。

② 逐条解説中の海外重罰の対象となる「開示」に関して、以下のような文言を追記し、解釈の明確化を図る。（2024年3月末公表）

- 営業秘密侵害罪について、**当該行為が、政府に対して情報提供を義務付けることを内容とする外国の法令に基づく行為であることの一事をもって、違法性が阻却されるものではない**。

【出典】 第２回知的財産戦略本部構想委員会（2024年2月14日）
資料３「技術流出と不正競争防止法」

【参考】 経済安保推進法に基づくサプライチェーン強靱化における対応（技術流出防止措置要件の追加）

我が国が**優位性を有する特定重要物資やその部素材**について、その**中核的な技術がひとたび流出すれば、将来における当該物資の外部依存につながり得る**ことに鑑み、以下の**技術流出防止措置を実施することを計画の認定要件として追加**。（2024年３月）

※ 対象物資は、**工作機械・産業用ロボット**、**航空機の部品**、**半導体**、**蓄電池**、**先端電子部品**
（いずれも認定に係る特定重要物資・その原材料等に関するもの。）

＜安定供給確保取組方針＞（抜粋）

（ア） **コア技術**（生産に有用かつ中核的な技術及び当該取組の成果である技術）及び**コア技術の実現に直接寄与する技術**（以下「**コア技術等**」という。非公知のものに限る。）へのアクセス管理
・コア技術等に**アクセス可能な従業員を必要最小限の範囲に制限し**、併せて**適切な管理を行うために必要な体制や規程を整備**する

（イ） コア技術等にアクセス可能な従業員の管理
・上記従業員の**相応な待遇（賃金、役職等の向上）**を確保するなど、**退職等を通じたコア技術等の流出を防止**する措置を講じる
・上記従業員が**退職する際にはコア技術等の守秘義務の誓約**を得る
・関係法令に十分配慮しつつ、**退職後の競業避止義務の誓約**についても上記従業員に同意を得るための取組を行う

（ウ） 取引先における管理
・取引先がコア技術等の全部又は一部を有する場合、保有の事実及びその詳細について、当該取引先と**秘密保持契約を締結**する
・（ア）、（イ）に相当する内容の措置を講じることを求め、関係法令に十分配慮しつつ、その**履行状況を定期的にレビューするなど取引先からのコア技術等の流出を防止するために必要な措置**を講じる

（エ） 技術移転等
・コア技術等の技術移転により、**取組対象物資の外部依存・供給途絶に陥る蓋然性が高まることのないようにすること**
・申請者又はそのグループ会社が**次に掲げる＜他者又は他国に対する行為＞**のいずれか**を行おうとする場合**であって、
①又は②に該当するときは、当該行為を実施する前に十分な時間的余裕をもって**物資所管省庁（経産省）に相談**を行うこと

＜他者又は他国に対する行為＞
- 他者**（申請者の子会社を含む）**に対し、**コア技術等に係る知的財産権を移転**する、供給確保計画の認定の対象とする取組に係る**事業を譲渡する**等、**コア技術等そのものを移転**する場合
- 他者に対し、**コア技術等を提供**する場合
- 他者と**コア技術等に関する共同研究開発**を行う場合
- 他国において**コア技術等に係る研究開発**を行う場合
- 他国において供給確保計画の認定の対象とする品目のうち**コア技術等を用いたものを生産する拠点を建設**し、又は**既存の生産拠点における設備投資**を行い、結果として**当該生産拠点における当該品目の製造能力が10%を超える割合で増強**する場合
（ただし、当該生産拠点で生産する当該品目の85%以上が当該他国で消費される場合を除く。）

① コア技術等の**強制的な技術移転のおそれ**があること、又は**他者の属性**※**によりコア技術等の流出のおそれ**があることを**申請者が知った場合**
※「過去５年間において、国際連合の決議その他国際的な基準に違反した実績がある者」又は「外国政府等による影響を受けて事業を行う者」
② ①のおそれがあるとして物資所管省庁（経産省）から**事前相談をすべき旨の連絡を受けた場合**

【参考】 経済安全保障上重要な物資・技術の特定と政策アプローチ

- コンピューティング、クリーンテック、バイオテック、防衛等の分野は、将来にわたる我が国の経済安全保障上の産業・技術基盤として不可欠。それぞれの分野で特に**重要なサプライチェーンに注目し、その維持・発展に政策資源を集中的に投入**する。
- 経済安全保障上重要なサプライチェーンにおいて鍵を握る**物資・技術を特定したうえで**、技術革新の動向、**我が国における相対的な優位性、対外依存度を分析・把握**し、強靱化に向けた**適切な政策手段を当てはめていく**。
- また、**経済安全保障上重要な物資を改めて洗い出した上で、リスク・脅威に対応した適切な政策手段を整理し、経済安保法の「取組方針」に反映させる。**

＜経済安全保障の観点から重視すべき物資・技術の整理＞

	将来の不可欠性・自律性の獲得 ① 破壊的技術革新が進む領域	不可欠性の維持 ② 我が国が技術優位性を持つ領域	自律性の回復 ③ 技術のコモディティ化・対外依存の領域
コンピューティング	次世代コンピューティング （例：量子コンピュータ・先端半導体）	製造装置・部素材・機器 等 （例：MLCC・光ファイバー・複合機）	レガシー半導体 等
クリーンテック	次世代クリーンテック （例：ペロブスカイト・全固体電池）	製造装置・部素材 等	重要鉱物 等
バイオテック	バイオものづくり （例：合成生物学・バイオファウンドリ）	検査・分析装置 等	抗菌性物質製剤 等
防衛・宇宙関連分野	防衛・宇宙分野の先進技術	航空機部素材 等 （炭素繊維・エンジン用素材）	航空機部素材 等 （大型鍛造・鋳造）
各領域に対する取組の方向性	技術優位性の創出	機微技術の流出・拡散防止	過剰依存構造の防止・是正

※ 点線枠内の物資・技術は例示

当該領域のうち、「技術流出による経済安全保障上の不利益が見込まれるもの」（P14）が本議論の射程

サプライチェーン強靱化における技術流出防止措置（P８）の主な対象

※第３回経済安全保障に関する産業・技術基盤強化のための有識者会議（2月2日）
資料３「経済安全保障に関する産業・技術基盤強化アクションプラン（策定後の進捗と今後の方向性）」を元に事務局作成

日本版バイ・ドール制度の概要

- 国が企業、大学、研究機関等に委託した研究開発において得られた特許権等の知的財産権は、産業技術力強化法第１７条により、研究開発を受託した者に帰属させることが可能とされている（いわゆる「日本版バイ・ドール制度」）　。
- このため、国が実施するほぼ全ての委託研究開発プロジェクトで、研究開発の受託者に知的財産権を帰属させることも可能となるような委託契約がなされている。
  （なお、一部の委託研究開発については、成果の保全等が必要なことから、本制度を適用せずに、当該成果に係る知財を国の所有とする場合がある。）
- ただし、**当該知的財産権の移転等にあたっては、**子会社又は親会社への移転等を除き、**あらかじめ国の承諾を受けることを条件**としている。

・ 産業技術力強化法（平成十二年法律第四十四号）（抄）

（国が委託した研究及び開発の成果等に係る特許権等の取扱い）

第十七条　国は、技術に関する研究開発活動を活性化し、及びその成果を事業活動において効率的に活用することを促進するため、国が委託した技術に関する研究及び開発又は国が請け負わせたソフトウェアの開発の成果（以下この条において「特定研究開発等成果」という。）に係る特許権その他の政令で定める権利（以下この条において「特許権等」という。）について、次の各号のいずれにも該当する場合には、その特許権等を受託者又は請負者（以下この条において「受託者等」という。）から譲り受けないことができる。

一　特定研究開発等成果が得られた場合には、遅滞なく、国にその旨を報告することを受託者等が約すること。

二　国が公共の利益のために特に必要があるとしてその理由を明らかにして求める場合には、無償で当該特許権等を利用する権利を国に許諾することを受託者等が約すること。

三　当該特許権等を相当期間活用していないと認められ、かつ、当該特許権等を相当期間活用していないことについて正当な理由が認められない場合において、国が当該特許権等の活用を促進するために特に必要があるとしてその理由を明らかにして求めるときは、当該特許権等を利用する権利を第三者に許諾することを受託者等が約すること。

四　**当該特許権等の移転又は当該特許権等を利用する権利**であって政令で定めるもの**の設定若しくは移転**の承諾をしようとするときは、**合併又は分割により移転する場合及び当該特許権等の活用に支障を及ぼすおそれがない場合として政令で定める場合を除き**、**あらかじめ国の承認を受けること**を受託者等が約すること。

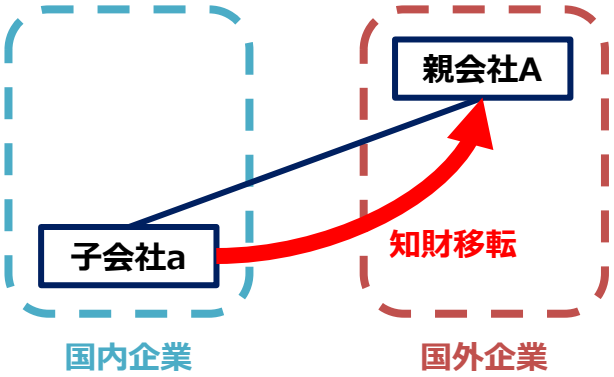
２・３　（略）

日本版バイ・ドール制度の運用について（１／２）

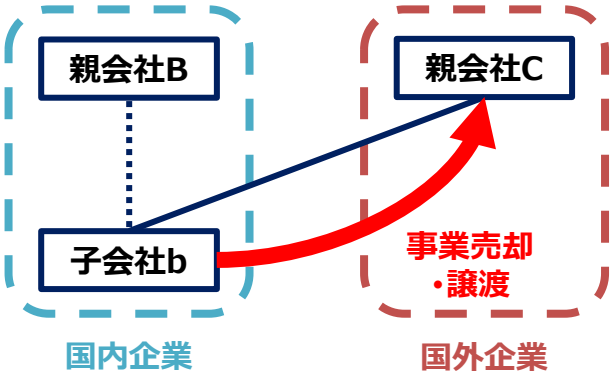
- 日本版バイ・ドール制度では、国の委託研究開発から生じた知的財産権を受託者（民間企業等）に帰属することを可能としているが、受託者の**子会社又は親会社が国外企業**である場合等、**国による委託研究の成果が国外流出することを防止できない**可能性がある。
- 想定されうるケースとしては例えば以下のケースが考えられる。
  - ① 国外企業の日本法人が親会社に知財を移転する場合
  - ② 国内企業の子会社がＭ＆Ａ等により新たに国外企業の子会社となり、当該国外企業に事業売却・譲渡を行う場合
  - ③ 国内企業の本社が国外に移転し、国外企業となる場合

【想定されるケース】

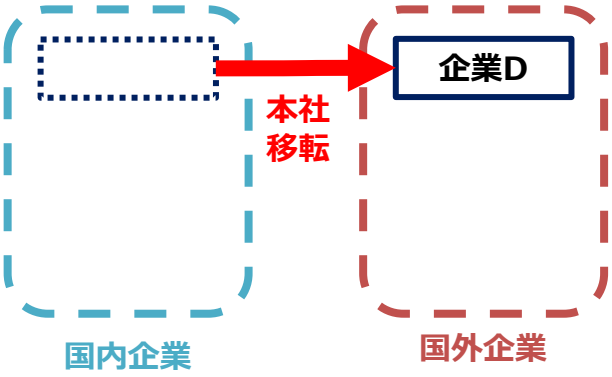
①国外企業の日本法人が親会社に知財を移転する場合



②国内企業の子会社が新たに国外企業の子会社となる場合



③国内企業の本社が国外に移転する場合



日本版バイ・ドール制度の運用について（２／２）

- 一方、経済産業省は「委託研究開発における知的財産マネジメントに関する運用ガイドライン」を作成し、**国外企業たる親会社又は子会社への知財の移転**に当たっては、「**研究開発の委託者に事前連絡**の上、**必要に応じて契約者間の調整を行う**ことについて、委託契約書において定めておくことが重要」としている。
- しかし、**ガイドラインの適用対象は経済産業省又は経済産業省所管の独立行政法人が委託する技術**に関する研究開発にとどまっている。
- そこで、国による経済安全保障上重要な技術の委託研究開発の成果のうち、我が国が技術優位性を有するもの（例えば、**国の委託による特定重要技術の研究開発成果**のうち、**社会実装段階にあるもの**、**特定重要物資に係る安定供給確保取組方針において技術流出防止措置が求められているコア技術**）について国外企業等に知財を移転する場合は、**受託者に事前連絡を求める**とともに、**委託者は当該事前連絡を確認の上、契約者間の調整を行う**よう徹底することが必要ではないか。

• 委託研究開発における知的財産マネジメントに関する運用ガイドライン（抄）

はじめに

○ 本ガイドラインの位置付け

本ガイドラインは、上記閣議決定等を受け、経済産業省が日本版バイ・ドール規定を含む産業技術力強化法を所管する立場から、国の委託による研究開発プロジェクトにおいて、国の担当者が知的財産マネジメントを実施するに当たり考慮すべきと考えられる事項を取りまとめたものである。

○ 本ガイドラインの適用対象

本ガイドラインは、経済産業省の予算により、経済産業省又は経済産業省所管の独立行政法人が委託する技術に関する研究開発を適用対象とし、平成２７年７月１日以降に公募を開始するものから実際に適用するものとする。

２－２－２ 委託研究開発の成果の取扱い

（７）フォアグラウンドＩＰの移転の事前承認

③親会社又は子会社への移転等について

国費を投じて実施した研究開発の成果について、日本版バイ・ドール制度の適用状況を把握する観点から、**親会社又は子会社（これらの会社が国外企業等である場合に限る。）への移転等の場合**には、**プロジェクト参加者は、研究開発の委託者に事前連絡**の上、必要に応じて**契約者間の調整を行う**ことについて、委託契約書において定めておくことが重要である。

本日ご議論いただきたいこと（案）

○経済安全保障上の重要技術の研究開発成果の社会実装と技術流出防止について

今後、経済安全保障上の技術流出した際の影響が大きい重要技術に関して、特に**国の資金による委託等により行われる社会実装を見据えた研究開発の成果を念頭**に、主要同盟国・同志国の対応（米：CHIPS・科学法など）やサプライチェーン強靱化における技術流出対策も参考にしつつ、**その社会実装**と**技術流出防止**に必要な対応を検討。

破壊的技術革新が進む技術（破壊的革新技術）をはじめ、将来の技術優位性の創出を目指す技術であって、かつ技術流出による経済安全保障上の不利益が見込まれるものを対象に国の資金による委託等により行われる社会実装を見据えた研究開発プロジェクトに関しても、入口から出口までの段階に応じた技術流出対策について検討が必要ではないか。

- 経済安全保障上重要な技術の流出対策（サプライチェーン強靱化における技術流出防止策の準用等）

（例）

- ✓ 技術へのアクセス管理
- ✓ 技術にアクセス可能な従業員の管理
- ✓ 取引先における管理
- ✓ 技術移転等の際の所管省庁等への相談
- ✓ リスクに応じたデューデリジェンス、モニタリング（オープンソース情報や開示情報に基づくもの等）の仕組みその他について

- 日本版バイ・ドール制度に基づき、取得した知財を国外企業に移転する場合の事前連絡、確認の徹底について

経済安全保障法制に関する有識者会議
分野別検討会合（官民技術協力）での議論の報告（案）

2024 年５月 20 日

１．国家間における経済安全保障上の重要技術の共同研究の推進について

（１）背景・現状

- 技術は我が国の自律性・不可欠性の重要な一部を構成するものであり、我が国の科学技術力を向上のためにも、オープンで自由な研究環境を確保し、国際協力をよりいっそう推進する必要がある。
- 一方で、研究活動の国際化、オープン化に伴う研究の不正流用や技術流出のリスクも指摘されており、こういったリスクへの対処は経済安全保障上の喫緊の課題となっている。
- 国際社会では、近年、各国が経済安全保障上の重要技術についての政策を公表し、2 か国間、複数国間の協議の場においても、経済安全保障上の重要技術についての議論が盛んに行われており、同盟国・同志国等の間で協力の重要性、必要性が高まっている。
- こうした中、Ｇ７では「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[1]」において、研究インテグリティを「研究の正当性、社会的関連性、責任及び質を確保して守るための職業的価値観、原則及びベストプラクティスの順守」と定義し、「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」し、「公正で革新的、オープンで、信頼性のある研究環境の中で協力するための基盤を形成するもの」とされている。また、研究セキュリティを「経済的、戦略的なリスクや国家的、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活動」とし、「リスクにターゲットを絞った研究セキュリティの施策は、学問の自由、研究インテグリティ、オープンサイエンス、透明性、相互利益のための信頼性のある協力体制の基盤を強化できる」としており、研究セキュリティと研究インテグリティの双方に取り組むことを推奨している。
- 特に、国家間における経済安全保障上の重要技術の共同研究の推進にあたっては、海外の国家や非国家による研究への不当な干渉を防止する研究セキュリティの観点からの取組が重要であり、責任ある国際協力（responsible international cooperation）を推進していく必要がある。
- 主要国も、研究セキュリティの取組を推進しており、2024 年に入り 1 月には EU、カナダが研究セキュリティに関連する政策を発表している。また、2024 年 4 月の日米首脳会談における日米首脳共同声明「未来のためのグローバル・パートナー」においても、

[1] https://ised-isde.canada.ca/site/science/sites/default/files/attachments/2023/1135-g7-common-values-and-principles-on-research-security-and-research-integrity_.pdf

重要・新興技術の振興及び保護等によって、日米の技術的な優位性を高めるとともに、我々の経済安全保障を強化するとの文言[2]が盛り込まれている。

- 日本ではこれまで内閣府（科学技術・イノベーション推進事務局）を中心に「研究活動の国際化、オープン化に伴う新たなリスクに対応する研究インテグリティの確保に係る対応方針[3]」に基づいて取組が行われてきたが、産業技術総合研究所の外国籍研究者による機密情報漏洩事案の発生（2023 年 6 月）、宇宙航空研究開発機構に対するサイバー攻撃（2023 年 11 月）もあり、研究セキュリティの観点からも取組の強化・徹底が求められている。

（２）研究セキュリティに係る各国の動向

- 外国からの不当な影響への対応の必要性については各国とも認識している一方、研究セキュリティといった言葉の捉え方は各国で異なっており、米国のように政府文書で明確に定義を定めている国、カナダや EU のように政府文書で言及している国、英国や豪州のように類似の概念に基づいて取組を進めている国など様々である。また、各国の政策文書には科学的発見とイノベーション促進の基盤として、学問の自由や研究活動の開放性が不可欠である旨、記載されており、各国とも国際協力を適切に進めるために研究セキュリティが必要であると位置づけている。
- 米国では、2021 年「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」（NSPM-33）や 2022 年「NSPM-33 実施ガイダンス」において、研究セキュリティが明確に定義されるとともに、情報開示の要件とプロセスの強化、リスクの特定と分析等、自国政府が支援する研究開発を外国政府の干渉や搾取から守るための行動についての指示がなされた。また、2022 年「CHIPS・科学法」も併せ、国防省やエネルギー省等の関係連邦省庁や、米国科学財団（NSF）等の資金配分機関において、研究セキュリティを確保するための各種取組が進められている。
- カナダでは、2021 年、政府より「研究パートナーシップに関する国家セキュリティ指針」を発表し、この方針を実施するための予算措置が 2022 年度からなされるなど、研究セキュリティ関連の取組を進めているところ。2024 年には、政府より 11 の「機微技術研究分野リスト（Sensitive Technology Research Areas）」と「指定研究機関リスト（Named Research Organizations）」を公表。また、同年初頭より、主要研究助成機関

---

[2] Leading on Innovation, Economic Security, and Climate Action
The United States and Japan aim to maximally align our economic, technology, and related strategies to advance innovation, strengthen our industrial bases, promote resilient and reliable supply chains, and build the strategic emerging industries of the future while pursuing deep emissions reductions this decade. Building on our efforts in the U.S.-Japan Competitiveness and Resilience (CoRe) Partnership, including through the U.S.-Japan Economic Policy Consultative Committee (our economic "2+2"), **we intend to sharpen our innovative edge and strengthen our economic security, including by promoting and protecting critical and emerging technologies**.

[3] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/integrity_housin.pdf

に申請のあった機微技術分野の研究に関連する助成金申請について、「当該資金で支援される活動に関与する研究者が指定研究機関リストにある機関に所属する、またはそこから資金等の支援を受けている場合は資金が提供されなくなる」と発表した。この他、オープンソースデューデリジェンスのガイダンスを公表する等、研究セキュリティを確保するための各種取組が進められている。

- EU では、「欧州経済安全保障戦略」の実施の一環として、2024 年に研究セキュリティに関する理事会勧告を提案。当該勧告案では、研究セキュリティの政策的枠組みの確立、支援体制の構築、資金提供機関を通じたセーフガードの導入、大学等の研究機関における研究セキュリティアドバイザーの任命を奨励、デューデリジェンスとリスク管理プロセスの導入等を推奨しており、研究セキュリティを確保するための各種取組が今後具体化されていくとみられる。

  また、EU 加盟国でも関連の取組が進められており、例えばオランダでは、研究セキュリティと類似の概念として「知識の安全保障（knowledge security)」を掲げている。2022 年、国際共同研究において機会と安全上のリスクを検討することが求められる、大学・研究機関の管理者に向けて「知識の安全保障に関する国家ガイドライン」を公表し、オランダ研究科学機構（NWO）に資金支援の申請書を提出する際は、同ガイドラインを遵守することが要件とされる等、研究セキュリティを確保するための各種取組が確認できる。
- 英国では、政府が自国の研究・イノベーション部門の継続的な成功に不可欠な国際研究協力の完全性を確保することを目的に、2019 年より「Trusted Research」キャンペーンを開始した。同キャンペーンは、英国の研究者、大学、産業界が国際協力に自信を持ち、潜在的なリスクに関して十分な情報に基づいた意思決定を行えるよう支援し、研究者や職員を潜在的な盗用、悪用、窃取から保護するための取組であり、アカデミアや産業界に対してそれぞれガイダンスを発出している。また、大学向けの公的な相談窓口である「研究協力アドバイスチーム（Research Collaboration Advice Team)」を設置し、国際共同研究における国家安全保障上のリスクについての相談や質問への個別対応も行っている。さらに政府は、開放性と独立性を維持しつつ、大学内の研究セキュリティ能力を開発するための資金オプションも含め、英国の大学を外国による国家安全保障上の脅威から守るための方策に関する協議を今夏から開始する意向を表明している。
- 豪州では、政府と大学や資金配分機関が共同で設置したタスクフォースが、「大学セクターに対する外国干渉に対抗するためのガイドライン」を発出し、外国干渉を受けるおそれのある職員に対し、外国の所属等の情報開示の要求や意思決定者に外国干渉リスクを知らせるためのデューデリジェンスの実施を推奨している。また、同ガイドラインに基づいて、各大学で自主的な取組が進められるとともに、資金配分機関である豪州研究評議会（ARC）において、競争的資金の申請が重要技術に該当する場合はそのリスクを検討する等、研究セキュリティを確保するための取組が確認できる。

- 日本では、2021 年 4 月、統合イノベーション戦略推進会議において「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[4]」を決定し、この政府方針に基づいて競争的研究費に関するガイドラインの改定[5]、研究者、所属機関向けのチェックリスト雛型を作成[6]するなどし、これらの研究インテグリティの取組のフォローアップ調査、大学等関係機関へのアウトリーチを実施してきた。2024 年 3 月には、国立研究開発法人改革の中で研究セキュリティ・インテグリティの確保・徹底について関係省庁申し合わせを公表[7]した。これにより G7 の取組を紹介する形以外で、初めて研究セキュリティについて政府文書の中に記載された。

（３）オープンで自由な研究環境を確保し、同盟国・同志国と対等な立場で国際共同研究を実施するために必要な研究セキュリティ対策（相手国から求められ得る研究セキュリティの対策）について

- 米国をはじめとした各国の政策文書でも、研究におけるオープン性や協力の重要性が謳われている一方、米国 NSPM-33 に記載されているように、一部の国は、このオープンな研究環境を利用して、研究実施のコストとリスクを回避しつつ、不当に自国の競争力を増大させようとしている。これらを踏まえて、研究成果の公開の原則等を維持し、オープンで自由な研究環境を確保したうえで国際協力を推進していくために、研究セキュリティについての施策を検討すべきである。
- 同盟国・同志国の制度やその実態を踏まえ、我が国が経済安全保障上の重要技術の育成に関して、相手国と対等な立場を維持し、国際協力を深化、拡大させていくためにどのような対策が必要であるか。以下、G7 での整理[8]に沿って①リスクにさらされている研究領域の特定と情報共有、②デューデリジェンスを実施し、透明性及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。標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施、③研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立、の３つの柱に沿って記載する。

①　リスクにさらされている研究領域の特定と情報共有

- 各国では、研究インテグリティの取組を基礎としつつも、リスクの高い研究領域を特定

---

[4] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/integrity_housin.pdf

[5] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/shishin.pdf

[6] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/checklist1.pdf（研究者向け）
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/checklist2r.pdf（大学・研究機関向け）

[7] https://www8.cao.go.jp/cstp/stsonota/kinoukyouka/kinoukyouka.html

[8] “G7 Best Practices for Secure & Open Research”, Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, 2024.

し、研究コミュニティを対象として研究セキュリティ・インテグリティの取組を実施している。我が国においても、これまで実施してきた研究インテグリティの取組を基礎として、その取組を徹底し、これを実効性のある実施に繋げることが研究セキュリティの取組として重要である。その上で、リスクの高い研究領域を含む特定の領域の国際共同研究を推進していく上で、相手国から求められる場合や、同志国等と対等な立場で実施することを念頭に、競争的研究費を投入する研究プログラムの性質に応じ、特定の研究領域[9]における諸外国の先進的な取組と同等の研究セキュリティの取組を行っていくことが必要であり、当該研究プログラムの資金支援を行う各府省において当該研究セキュリティの取組の検討を行うことが必要ではないか。

- なお、リスクの高い研究領域の特定にあたっては研究者・研究機関、資源配分機関、関係省庁等が十分に検討・議論することが重要である。

② デューデリジェンスを実施し、透明性及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。標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施

- 諸外国では、デューデリジェンスの実施にあたり、研究者や研究機関が参照するチェックリストやガイドラインを公表している。我が国においても、政府の資金支援を行う研究開発プロジェクトに関して、実効的なデューデリジェンスの実施に資するようなガイドライン、チェックリストの手順書等の検討が必要ではないか。
- その際、リスクマネジメントの観点からリスクに応じた段階的な対応が可能となるよう検討を行うことが必要と考えられる。
- 具体的には、競争的研究費による研究については、研究成果の公開が可能な研究であることが想定されるが、政府方針に基づく研究インテグリティの取組が実効性を持った実施に繋がるよう、ガイドライン、チェックリスト等を作成・周知し、資金配分機関や研究機関等において所要の確認を徹底するといった実態的に有効な手法についての検討が必要ではないか。
- また、諸外国の先進的な取組と同等の研究セキュリティの取組が、リスクの高い研究領域を含む特定の領域の国際共同研究の実施において、相手国から求められる場合や、特定の研究領域において同志国等と対等な立場で実施するために必要な場合もあると考

[9] 例えば、2024 年 4 月の日米首脳会談における日米首脳共同声明「未来のためのグローバル・パートナー」において例示された分野（We are committed to strengthening our shared role as global leaders in the development and protection of next-generation critical and emerging technologies such as AI, quantum technology, semiconductors, and biotechnology through research exchange and private investment and capital finance, including with other like-minded partners.）の他、経済産業省の有識者会議の資料（経済安全保障に関する産業・技術基盤強化アクションプラン改訂版 令和 6 年 5 月）のように、研究セキュリティを更なる取組を要する経済安全保障上の重要技術として、経済安全保障の観点から技術優位性のある分野（これから技術優位性を確保しようとする戦略分野も含むもの）とすることが一案。

えられる。また、上記に加えて、パイロット、トップランナーとして、諸外国の先進的な取組と同等の取組が必要な場合は、先行的に研究セキュリティの取組を実施することも想定される。こうした諸外国の先進的な取組の一例として、例えば、外部の公開情報に基づいたデータリソースの利用や、複数の研究機関でコンソーシアムを形成してデューデリジェンスを行う仕組みを創設するなどして、様々な形で公開情報に基づいたデューデリジェンス（以下「オープンソースデューデリジェンス」という。）等の充実によるリスクマネジメントを実施していくことも考えられるのではないか。

- 実際にこのような取組を行っていくにあたり、まずは、オープンソースデューデリジェンスの具体的な事例を蓄積し、研究現場の規模や実情に応じたより効果的な実施方法を検証し、蓄積した好事例を横展開していくことが一つのやり方ではないか。

③ 研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立

- 我が国においても、研究資金を提供する省庁・機関のみの活動だけでなく、水際対策なども含め、捜査・公安当局、法執行機関等も含めた政府内の関係機関の連携を促進していくべきではないか。
- 研究資金を提供する省庁・機関等を中心に、研究機関等からの相談等の窓口設置や政府と研究コミュニティとの双方向の情報交換の場の創設やその機能の強化について検討が必要ではないか。

（４）今後の課題・留意点等

- 米国では、NSPM-33 において、研究セキュリティ・インテグリティ確保のための連邦省庁、特に国土安全保障省（DHS）に対し、国務省（DOS）と連携して留学生・外国人研究者の審査することを要求[10]。我が国においても、入国時における審査を徹底するなど、関係省庁が緊密に連携して水際対策を更に強化するべきではないか。
- 経済安全保障をめぐる国際的な動きに応じた対応をするため、研究セキュリティ・インテグリティに関するリスクの特定等に関する調査分析機能を強化する必要があるのではないか。
- 各関係機関の現場において、規模や実情に応じた研究セキュリティ・インテグリティの取組を徹底するために必要な体制や、先行的な取組の実施等についても検討していく必要があるのではないか。

---

[10] 未来工学研究所「研究インテグリティ（Research Integrity）に係る調査・分析」（令和 5 年 3 月）
国土安全保障長官は、国土安全保障省（DHS）が国務省と連携し、米国の研究開発事業に 参加・参画しようとする非移民学生及び交換訪問者の外国人個人を国家安全保障上のリスクについて確かに審査する責任がある。国土安全保障長官は、教育及び文化交流プログラムのために米国に来る外国人の合法的な入国と滞在を支援しながら、国家の安全を守るために、留学生及び研究者に関する情報を DHS が保持することを、適用法に沿って確実に行う責任がある。

- 研究セキュリティ・インテグリティの取組はオープンな環境を確保し、国際協力をよりいっそう推進するためのものであり、取組の推進により特定国や特定の研究者の差別助長につながらないよう十分な配慮が必要。

２．経済安全保障上の重要技術の研究開発成果の社会実装と技術流出防止について

（１） 背景・現状

- 2023 年６月、産業技術総合研究所の職員が不正競争防止法違反の容疑で逮捕される事案が発生するなど、企業等が持つ「営業秘密」の漏洩を巡る摘発が後を絶たない状況である。
- そのような中、米国では 2022 年８月、「CHIPS・科学法」を制定し、半導体関連の設備投資等の支援が可能な基金を含め、５年間で計 527 億ドル（約 7.6 兆円）の支援提供を決定した。加えて、助成対象者から安全保障上の懸念国への投資等を禁じるガードレール条項を公表した。
- 技術流出の経路は様々であるが、大きく「モノ」による技術流出、「カネ」による技術流出、「ヒト」による技術流出の３つに分類できる。このうち、「モノ」及び「カネ」による技術流出については外為法における輸出管理及び投資管理の対象であり、現在、別途、技術流出対策のための検討が進められているところである。
- 「ヒト」による技術流出については、営業秘密を不正な方法により取得、開示する行為について、適切な営業秘密管理を行っている前提で不正競争防止法の対象となる。営業秘密管理の一環として、転職時に秘密管理や競業避止などの誓約書を求めるケースもあるが、実効性が不明という課題も指摘されているところである。また、安全保障の裾野が経済分野に急速に拡大する中、国として重要な技術を適切に管理することが喫緊の課題である。
- そこで、経済安全保障推進法に基づくサプライチェーン支援においては、2024 年３月、我が国が優位性を有する特定重要物資やその部素材について、その中核的な技術がひとたび流出すれば、将来における当該物資の外部依存につながり得ることに鑑み、以下の技術流出防止措置を実施することを計画の認定要件として追加したところである（詳細は参考参照）。
  （ア） コア技術等へのアクセス管理
  （イ） コア技術等にアクセス可能な従業員の管理
  （ウ） 取引先における管理
  （エ） 技術移転等
- また、日本企業 770 社が回答した質問調査によって、営業秘密の漏洩を検知する活動を行っていない企業は、自社では営業秘密漏洩が起きていないと回答しているのに対して、検知活動を行っている企業は営業秘密漏洩を経験したとする回答が有意に増加することが示されている。実際に多くの営業秘密漏洩が起きているにもかかわらず、自

社の営業秘密の漏洩に気づいていない企業が多く、実際の漏洩は公表されている数値よりはるかに多いことが示唆されている[11]との情報がある。

（２） 国からの資金支援を行う研究開発プロジェクトに関する入口から出口までの段階に応じた技術流出対策の検討

- 経済安全保障推進法に基づくサプライチェーン支援においても、我が国が優位性を有する特定重要物資やその部素材について、国から資金支援を行う場合、一定の技術流出防止措置を求めているところである。そこで、国からの資金支援を行う研究開発プロジェクトに関しても、我が国の技術優位性の強化を目指す技術領域及び将来の我が国の技術優位性の創出を目指す技術領域における社会実装を見据えた研究開発成果の技術流出防止のため、入口から出口までの段階に応じた対策が必要である。
- 具体的には、主に、
  ・破壊的技術革新が進む技術をはじめ、将来の技術優位性の創出を目指す技術領域
  ・我が国が技術優位性を持つ技術領域のうち、既に一定の技術流出防止措置を求めている特定重要物資を除く領域
  として各府省が支援し、決定する社会実装を見据えた研究開発プログラム（特に、国際共同研究にあたり相手国から求められる場合や、同志国等と対等な立場で実施するために必要な場合に、各府省が決定する研究開発プログラムも含む。）を対象領域とするべきではないか。

① 「ヒト」による技術流出等への対策

- 経済安全保障推進法に基づくサプライチェーン支援において、先行して技術流出防止措置要件を定めていることから、上述の研究開発プログラムに関しても、当該技術流出防止措置要件を踏まえつつ、対策を講じることが有効といえる。
- 対象技術は、社会実装を見据えた研究開発を行うものであることを鑑み、国の支援を受けて行う研究開発の成果及びその活用の際に必要となる技術の設計・生産・利用の各段階において有用かつ中核的な技術（ソフトウェアを含む）（以下「コア重要技術」という。）及びコア重要技術の実現に直接寄与する技術（以下「コア重要技術等」という。）のうち非公知のものとすることが考えられる。
- 技術流出防止策としては、コア重要技術等に関して、経済安全保障推進法に基づくサプライチェーン支援における対策を踏まえ、当該対策における（ア）から（ウ）までにあたる事項に相当する事項を充足するにあたり、リスクに応じ、オープンソースデューデ

[11] https://www.semanticscholar.org/paper/Empirical-study-regarding-the-leakage-of-know-how-Hirai-Watanabe/525532821be1b0af5baa574f3f00455f430eaa9c

リジェンス等の技術流出防止の取組を行うことが有効といえる。その際、企業ヒアリングの結果から得られた以下に挙げるような、事業や研究開発の国際化を前提にした上での企業等での独自の取組による営業秘密管理強化の好事例も参考にすることも考えられるのではないか。

（ア）技術へのアクセス管理

・物理環境のセキュリティ整備として、社内のワーキングエリアにおける段階的なセキュリティゾーンを区分けし、それぞれのゾーン内で取扱可能な文書等の情報区分を規定する。

・研究開発段階のもの、実際に生産・製造を視野に入れた開発段階のもの等、それぞれの研究内容に合わせて、技術へアクセス可能な従業員の範囲を適切に設計する。特に、例えば生産・製造技術の場合、生産・製造を視野に入れた開発段階においては、生産・製造プロセスの全工程にまたがって技術の全体像を知る従業員をできる限り限定するとともに、当該従業員に対しては所要の処遇を行う。

（イ）技術にアクセス可能な従業員の管理

・重要な技術をもつ従業員を把握し、当該従業員への外部からの接触の有無を確認するなど、リスクの管理を行う。

・退職後の競業避止義務の誓約について、重要な技術をもつ従業員に同意を得、一定期間有効なものとするための取組として、ストックオプションの行使や割増退職金支給の条件として、競合他社に転職しないことを定める。

（ウ）取引先（共同研究パートナー等のサードパーティを含む）における管理

・取引先を経由した技術流出防止のため、取引先のリスクを評価するチェックリストを作成するとともに、取引先から提出された情報を元にリスク評価を行い、公開・非公開部分の適切な線引きを行った上で戦略的に連携を行う。

（ア）から（ウ）まで共通　リスクマネジメントの観点からのデューデリジェンス、モニタリング等の仕組み

・リスクに応じ、デューデリジェンスを実施する。例えば、Need to know の原則に基づき、特定のプロジェクトに関してはプロジェクト毎に本人の同意を得たうえで、個別に、秘密保持契約の締結、本人からの情報提供、本人による情報管理等に関する誓約の取得、オープンソースデューデリジェンスなど、アクセス可能な従業員の選定にあたり、そのプロジェクトの参加の段階から、プロジェクト毎の性質に応じた段階的なリスク管理として所要のデューデリジェンスを実施する。

・リスクマネジメントの観点から、重要な情報が適切に管理されているか、情報を大量に持ち出す等不自然な動きが無いか等について業務の IT 化とあわせてモニタリングを実施する。さらに、怪しい挙動が確認された際、メールを含む電子コミュニケーションやデータストレージについて監査できる体制を構築する。

・全社員が遵守すべき情報管理規律を整備するとともに、当該規律遵守の署名やフォ

ローアップを実施する。

・内閣府（科学技術・イノベーション推進事務局）が公表している研究インテグリティのチェックリスト等を参照し、社内やサードパーティのリスク等に関する取組について、社内での啓発活動等を行う。

・経済安全保障担当の部署横断的な組織を設置し、関係部局からの情報を集約し、総合的な相談窓口業務や組織横断的なリスクマネジメントを実施する。

- なお、技術流出防止対策を講じるにあたっては、プロジェクトに参画する研究者からの過度な敬遠を防ぐため、それぞれの研究の特性やリスクにあわせたメリハリのある必要十分な対策を講じるべきである。例えば、研究者の記憶にとどまる残留情報の管理などは、研究者からの過度な敬遠につながる場合があるため、研究者の記憶にとどまる残留情報は開示や使用の制限の対象外とするなど留意が必要である。

②日本版バイ・ドール制度の特定条項の論点（特に経済安全保障上の重要技術に係る社会実装を目的とする政府等からの研究開発委託の際における特許権等の海外移転の整理）

- 国が企業、大学、研究機関等に委託した研究開発において得られた特許権等の知的財産権は、産業技術力強化法第１７条により、研究開発を受託した者に帰属させることが可能とされている（いわゆる「日本版バイ・ドール制度」）。
- このため、国が実施するほぼ全ての委託研究開発プロジェクトで、研究開発の受託者に知的財産権を帰属させることも可能となるような委託契約がなされている。
  （なお、一部の委託研究開発については、成果の保全等が必要なことから、本制度を適用せずに、当該成果に係る知的財産権を国の所有とする場合がある。）
- ただし、当該知的財産権の移転等にあたっては、子会社又は親会社への移転等を除き、あらかじめ国の承諾を受けることを条件としている。
- 日本版バイ・ドール制度では、国の委託研究開発から生じた知的財産権を受託者（民間企業等）に帰属することを可能としているが、受託者の子会社又は親会社が国外企業である場合等、国による委託研究の成果が国外流出することを防止できない可能性がある。
- 想定され得るケースとしては例えば、①国外企業の日本法人が親会社に知財を移転する場合②国内企業の子会社がM&A等により新たに国外企業の子会社となり、当該国外企業に事業売却・譲渡を行う場合③国内企業の本社が国外に移転し、国外企業となる場合が考えられる。
- 一方、経済産業省は「委託研究開発における知的財産マネジメントに関する運用ガイドライン」を作成し、国外企業たる親会社又は子会社への知財の移転にあたっては、「研究開発の委託者に事前連絡の上、必要に応じて契約者間の調整を行うことについて、委託契約書において定めておくことが重要」としている。

- しかし、ガイドラインの適用対象は経済産業省又は経済産業省所管の独立行政法人[12]が委託する技術に関する研究開発にとどまっている。
- そこで、少なくとも、国による経済安全保障上重要な技術の委託研究開発の成果について国外企業等に知財を移転する場合は、受託者に事前連絡を求めるとともに、委託者は当該事前連絡を確認の上、契約者間の調整を行うよう徹底することが必要ではないか。

（３） 今後の検討課題・留意点等

- 経済安全保障上の重要技術の研究開発成果の社会実装を見据え、今後の研究開発プログラムの検討、実施にあたり、各府省において、技術流出防止策をとるべき研究開発プログラムを特定し、当該プログラムにおける技術流出防止策を新たに徹底する必要があるのではないか。
- 事業や研究開発の国際化を前提にした上での企業等での独自の取組による営業秘密管理強化の好事例も参考にして、必要な技術流出防止策対策を円滑に実施するための施策について検討する必要があるのではないか。

---

[12] 経済産業省所管の独立行政法人・研究開発法人である NEDO の業務委託契約標準契約書においては、ガイドラインの適用にあたり、以下のような条項を設け、子会社・親会社への知的財産権の移転等における国の承諾を不要とする規定を、国外企業への移転に限り適用除外している。

（知的財産権の所属）
第 31 条
3　乙は、次の各号に掲げる事項を遵守しなければならない。
一～三　（略）
四　当該知的財産権の移転（第３１条の６第１項に規定する持分の放棄を除く。以下この号において同じ。）、又は特許権、実用新案権若しくは意匠権についての専用実施権（仮専用実施権を含む。）又は回路配置利用権若しくは育成者権についての専用利用権（以下「専用実施権等」という。）の設定若しくは移転の承諾をしようとするときは、あらかじめ甲の承認を受けるものとすること。ただし、合併又は分割により移転する場合、及び次のいずれかに該当する場合は、この限りではない。
イ　乙が株式会社であって、その子会社（会社法第２条第三号に規定する子会社をいう。）又は親会社（会社法第２条第四号に規定する親会社をいう。）に当該知的財産権の移転又は専用実施権等を設定若しくは移転の承諾をする場合（ただし、その子会社又は親会社が日本国外に存する場合を除く。）

【参考】 経済安保推進法に基づくサプライチェーン強靱化における対応（技術流出防止措置要件の追加）

我が国が**優位性を有する特定重要物資やその部素材**について、その**中核的な技術がひとたび流出すれば、将来における当該物資の外部依存につながり得る**ことに鑑み、以下の**技術流出防止措置を実施することを計画の認定要件として追加**（2024年３月）

※　対象物資は、**工作機械・産業用ロボット**、**航空機の部品**、**半導体**、**蓄電池**、**先端電子部品**
（いずれも認定に係る特定重要物資・その原材料等に関するもの。）

＜安定供給確保取組方針＞（抜粋）

（ア）**コア技術**（生産に有用かつ中核的な技術及び当該取組の成果である技術）及び**コア技術の実現に直接寄与する技術**
（以下「**コア技術等**」という。非公知のものに限る。）へのアクセス管理
・コア技術等に**アクセス可能な従業員を必要最小限の範囲に制限し**、併せて**適切な管理を行うために必要な体制や規程を整備**する

（イ）コア技術等にアクセス可能な従業員の管理
・上記従業員の**相応な待遇（賃金、役職等の向上）**を確保するなど、**退職等を通じたコア技術等の流出を防止**する措置を講じる
・上記従業員が**退職する際にはコア技術等の守秘義務の誓約**を得る
・関係法令に十分配慮しつつ、**退職後の競業避止義務の誓約**についても上記従業員に同意を得るための取組を行う

（ウ）取引先における管理
・取引先がコア技術等の全部又は一部を有する場合、保有の事実及びその詳細について、当該取引先と**秘密保持契約を締結**する
・（ア）、（イ）に相当する内容の措置を講じることを求め、関係法令に十分配慮しつつ、その**履行状況を定期的にレビューするなど取引先からのコア技術等の流出を防止するために必要な措置**を講じる

（エ）技術移転等
・コア技術等の技術移転により、**取組対象物資の外部依存・供給途絶に陥る蓋然性が高まることのないようにすること**
・申請者又はそのグループ会社が**次に掲げる＜他者又は他国に対する行為＞**のいずれか**を行おうとする場合**であって、
①又は②に該当するときは、当該行為を実施する前に十分な時間的余裕をもって**物資所管省庁（経産省）に相談**を行うこと

＜他者又は他国に対する行為＞
- 他者**（申請者の子会社を含む）**に対し、**コア技術等に係る知的財産権を移転**する、供給確保計画の認定の対象とする取組に係る**事業を譲渡する**等、**コア技術等そのものを移転**する場合
- 他者に対し、**コア技術等を提供**する場合
- 他者と**コア技術等に関する共同研究開発**を行う場合
- 他国において**コア技術等に係る研究開発**を行う場合
- 他国において供給確保計画の認定の対象とする品目のうち**コア技術等を用いたものを生産する拠点を建設**し、又は**既存の生産拠点における設備投資**を行い、結果として**当該生産拠点における当該品目の製造能力が10%を超える割合で増強**する場合
（ただし、当該生産拠点で生産する当該品目の85%以上が当該他国で消費される場合を除く。）

① コア技術等の**強制的な技術移転のおそれ**があること、又は**他者の属性**※**によりコア技術等の流出のおそれ**があることを**申請者が知った場合**
※「過去５年間において、国際連合の決議その他国際的な基準に違反した実績がある者」又は「外国政府等による影響を受けて事業を行う者」

② ①のおそれがあるとして物資所管省庁（経産省）から**事前相談をすべき旨の連絡を受けた場合**

引用：経済安全保障法制に関する有識者会議 官民技術協力に関する検討会合（第３回）資料１

経済安全保障法制に関する有識者会議　分野別検討会合（官民技術協力）での議論の報告（案）概要

１．国家間における経済安全保障上の重要技術の共同研究の推進について

（１）背景・現状

●経済安全保障上の重要技術に関して、国際協力の推進（プロモーション）と不正流用や技術流出のリスク管理（プロテクション）の両面からの検討が必要となっており、国際社会では、近年、各国が関連の政策を公表。同盟国・同志国等の間で協力の重要性、必要性が高まっている。

●G7では研究セキュリティと研究インテグリティの双方に取り組むことを推奨。
経済安全保障上重要な技術の国際共同研究を推進するにあっては研究セキュリティの観点が重要であり、
責任ある国際協力（responsible international cooperation）を推進していく必要。

●主要国で研究セキュリティの取組が推進されており、今年4月の日米首脳共同声明でも重要・新興技術の振興及び保護等によって、日米の技術的な優位性を高めるとともに、我々の経済安全保障を強化するとされており、日本でも取組の強化・徹底が求められている。

（２）研究セキュリティに係る各国の動向

●外国からの不当な影響への対応の必要性については各国とも認識している一方、研究セキュリティといった言葉の捉え方は各国で異なっているが、各国の政策文書には科学的発見とイノベーション促進の基盤として、学問の自由や研究活動の開放性が不可欠である旨、記載されており、各国とも国際協力を適切に進めるために研究セキュリティが必要であると位置づけている。

（３）オープンで自由な研究環境を確保し、同盟国・同志国と対等な立場で国際共同研究を実施するために必要な研究セキュリティ対策（相手国から求められ得る研究セキュリティの対策）について

●研究成果の公開の原則等を維持し、オープンで自由な研究環境を確保したうえで国際協力を推進していくために、
研究セキュリティについての施策を検討。

●同盟国・同志国の制度やその実態を踏まえ、相手国と対等な立場を維持し、国際協力を深化、拡大させていくための方策についてG7で取りまとめられているベストプラクティスの柱に沿って整理。

①リスクにさらされている研究領域の特定と情報共有

●これまで実施してきた研究インテグリティの取組を基礎として、
- その取組を徹底することによる研究セキュリティの取組。
- その上で、リスクの高い研究領域を含む特定の領域の国際共同研究を推進していく上で、相手国から求められ場合や、同志国等と対等な立場で実施することを念頭に、競争的研究費を投入する研究プログラムの性質に応じ、特定の研究領域における諸外国の先進的な取組と同等の研究セキュリティの取組の実施が必要。

●検討にあたっては十分に研究現場の関係者とのコミュニケーションをとることが重要。

②デューデリジェンスを実施し、透明性及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。
　標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施

●実効的なデューデリジェンスの実施に資するように、研究者や研究機関が参照するチェックリスト、ガイドライン、手順書等の作成を検討
●リスクマネジメントの観点からリスクに応じた段階的な対応が可能となるよう検討を行う必要。

➢競争的研究費による研究については、研究成果の公開が可能な研究であることが想定されるが、政府方針に基づく研究インテグリティの取組が実効性を持った実施に繋がるよう、ガイドライン、チェックリスト等を作成・周知し、資金配分機関や研究機関等において所要の確認を徹底するといった実態的に有効な手法について検討。

➢リスクの高い研究領域を含む特定の領域の国際共同研究の実施において、相手国から求められる場合や、同志国等と対等な立場で実施するために必要な場合、諸外国の先進的な取組と同等の研究セキュリティの取組が必要。
（パイロット、トップランナーとして先行的に研究セキュリティの取組を実施する場合も含む）
一例として、外部のデータリソースの利用や、複数の研究機関でコンソーシアムを形成してデューデリジェンスを行う仕組みを創設するなどして、様々な形で公開情報に基づいたデューデリジェンス（オープンソースデューデリジェンス）等の充実によるリスクマネジメントを実施していくことも検討。得られた好事例を横展開。

③研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立
●研究資金を提供する省庁・機関のみの活動だけでなく、捜査・公安当局、法執行機関等も含めた政府内の関係機関の連携を促進。
●研究資金を提供する省庁・機関等を中心に、研究機関等からの相談等の窓口設置や政府と研究コミュニティとの双方向の情報交換の場の創設やその機能の強化について検討。

（４）今後の課題・留意点等
●関係省庁が緊密に連携して水際対策を更に強化することを検討。
●経済安全保障をめぐる国際的な動きに対応するため、研究セキュリティ・インテグリティに関するリスクの特定、分析能力の強化を検討。
●各関係機関の現場において、規模や実情に応じた研究セキュリティ・インテグリティの取組推進のための体制整備、先行的な取組の実施を検討。
●研究セキュリティ・インテグリティの取組推進にあたり、特定国、特定の研究者の差別の助長につながらないように十分な配慮が必要。

２．経済安全保障上の重要技術の研究開発成果の社会実装に向けた技術流出防止について

（１）背景・現状

●2023年６月、産業技術総合研究所の職員が不正競争防止法違反の容疑で逮捕される事案が発生するなど、企業等が持つ「営業秘密」の漏洩を巡る摘発が後を絶たない状況。

●技術流出の経路は様々であるが、「モノ」及び「カネ」による技術流出については外為法の対象であり、現在、別途、技術流出対策のための検討が進められているところ、「ヒト」による技術流出については、適切な営業秘密管理を行っている前提で不正競争防止法の対象となるものの、実効性が不明という課題も指摘。

●安全保障の裾野が経済分野に急速に拡大する中、国として重要な技術を適切に管理することが喫緊の課題。

（２）政府からの資金支援を行う研究開発プロジェクトに関する入口から出口までの段階に応じた技術流出対策の検討

●経済安全保障推進法に基づくサプライチェーン支援においても、我が国が優位性を有する特定重要物資やその部素材について、国から資金支援を行う場合、一定の技術流出防止措置を求めているところ。

●国からの資金支援を行う研究開発プロジェクトに関しても、入口から出口までの段階に応じた対策が必要。

●具体的には、主に、
A)破壊的技術革新が進む技術をはじめ、将来の技術優位性の創出を目指す技術領域
B)我が国が技術優位性を持つ技術領域のうち、既に一定の技術流出防止措置を求めている特定重要物資を除く領域
として各府省が支援し、決定する社会実装を見据えた研究開発のプログラムを対象領域とすべき。

①ヒトによる技術流出等への対策

●対象技術は、社会実装を見据えた研究開発を行うものであることを鑑み、国の支援を受けて行う研究開発の成果及びその活用の際に必要となる技術の設計・生産・利用の各段階において有用かつ中核的な技術（ソフトウェアを含む）（「コア重要技術」）及びコア重要技術の実現に直接寄与する技術（「コア重要技術等」）のうち非公知のものとすることが考えられる。

●技術流出防止策としては、経済安全保障推進法に基づくサプライチェーン支援における対策を踏まえ、リスクに応じ、デューデリジェンス及びモニタリング・監査等の技術流出防止の取組を行うことが有効。その際、（ア）から（ウ）までに挙げるような、事業や研究開発の国際化を前提にした上での企業等での独自の取組による営業秘密管理強化の好事例を参考にすることも考えられる。
（ア）技術へのアクセス管理
（イ）技術にアクセス可能な従業員の管理
（ウ）取引先（共同研究パートナー等のサードパーティを含む）における管理
（ア）から（ウ）まで共通　リスクマネジメントの観点からのデューデリジェンス※、モニタリング等の仕組み
（※一例として、秘密保持契約の締結、本人からの情報開示、本人による情報管理等に関する誓約の取得、オープンソースデューデリジェンス）

②日本版バイ・ドール制度の特定条項の論点
（特に経済安全保障上の重要技術に係る社会実装を目的とする政府等からの研究開発委託の際における特許権等の海外移転の整理）

●日本版バイ・ドール制度の運用においては、受託者の子会社又は親会社には国の承諾なしに知財を移転することが可能であり、受託者の子会社又は親会社が国外企業である場合等、国による委託研究の成果が国外流出することを防止できない可能性がある。
●経済産業省はガイドラインにおいて、国外企業への知財の移転に当たっては、委託者への事前連絡と契約者間の調整を求めており、少なくとも、国による経済安全保障上重要な技術の委託研究開発においては、これを徹底する必要。

（３）今後の課題・留意点等

●経済安全保障上の重要技術の研究開発成果の社会実装を見据え、今後の研究開発プログラムの検討、実施にあたり、各府省において、技術流出防止策をとるべき研究開発プログラムを特定し、当該プログラムにおける技術流出防止策を新たに徹底
●必要な技術流出防止対策を円滑に実施するための施策について検討

1．国家間に係る経済安全保障上の重要技術の共同研究の推進について

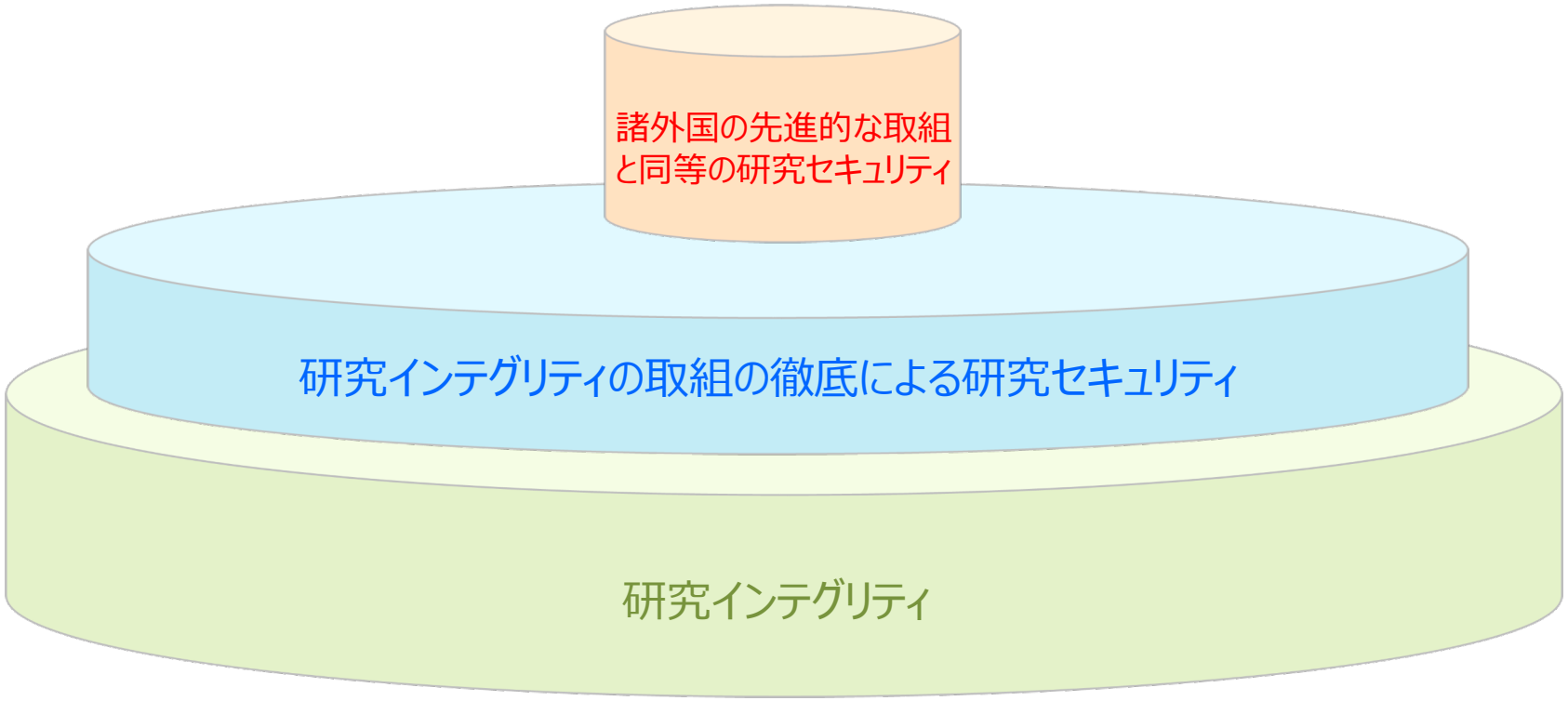
日本では、2021年4月に統合イノベーション戦略推進会議で決定した政府としての対応に基づき、以下を実施。

- 競争的研究費の適正な執行に関する指針の改定（2021年12月関係府省連絡会申し合わせ）
- 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（雛型）（2021年12月研究者向け、大学・研究機関向け作成、2023年6月大学・研究機関等向け改定）

→ 研究者自身による適切な情報開示、研究機関等による開示された情報の確認、公的資金配分機関による競争的研究費の申請時の確認
外国の機関等との連携の際にその組織や相手方の参加メンバーの情報、連携・契約の目的を確認

<table>
<tr><th colspan="2">趣旨</th><td>研究インテグリティの取組の徹底による研究セキュリティの取組
（エフォート管理を主体としたリスク管理）</td><td>諸外国の先進的な取組と同等の研究セキュリティの取組
（リスク管理の観点から追加的に実施）</td></tr>
<tr><th colspan="2">対象</th><td>競争的研究費を投入する全ての研究プログラム（国の資金により委託等により行われる研究プログラムをいう。以下同じ）</td><td>競争的研究費を投入する研究プログラムのうち、リスクの高い研究領域を含む特定の領域の国際共同研究にあたり、相手国から求められる場合や、特定の研究領域において同志国等と対等な立場で実施するためなどに必要な場合に、各府省が決定するもの※
上記プログラムのほか、
「パイロット、トップランナーとして先行的に実施する場合」も含む</td></tr>
<tr><th rowspan="4">取組の主体</th><th>政府</th><td colspan="2">● 外国パートナー等について開示情報・チェックリストにより得られる情報の確認に係る手順書（デューデリジェンス（DD）の手順書）の作成・周知
※オープンソースDDの対象となる研究プログラム、リスク管理の手法等を各府省が決定
（決定にあたっての基準は何らかの形で提示）</td></tr>
<tr><th>資金配分機関（FA等）</th><td>● 政府方針に基づき、共有システムにおける開示情報の確認を徹底</td><td>● 左記に加え、オープンソースDD等の充実によるリスク管理</td></tr>
<tr><th>研究機関等</th><td>● 政府方針に基づき、所属研究者に係る開示情報の確認を徹底</td><td>● 左記に加え、オープンソースDD等の充実によるリスク管理</td></tr>
<tr><th>研究者</th><td colspan="2">● 政府方針に基づき、共有システム等によるFA、所属研究機関等への情報開示の徹底
● チェックリスト・手順書の活用</td></tr>
</table>

【参考】イメージ


諸外国の先進的な取組
と同等の研究セキュリティ
研究インテグリティの取組の徹底による研究セキュリティ
研究インテグリティ

2．経済安全保障上の重要技術の研究開発成果の社会実装に向けた技術流出防止について

技術領域		我が国が技術優位性を持つ技術領域		将来の我が国の技術優位性の創出を目指す技術領域
趣旨		特定重要物資のサプライチェーン強靱化における技術流出防止 （技術流出防止措置の先行事例）	我が国の技術優位性の強化を目指す技術領域における社会実装を見据えた研究開発成果の技術流出防止	将来の我が国の技術優位性の創出を目指す技術領域における社会実装を見据えた研究開発成果の技術流出防止
①主な対象領域		・特定重要物資のうち、安定供給確保取組方針において技術流出防止措置を実施することとされている物資※1 （工作機械・産業用ロボット、航空機の部品、半導体、蓄電池、先端電子部品）	・我が国が技術優位性を持つ技術領域（左記を除く）として各府省が支援し、決定する研究開発プログラム※1 ※特に、国際共同研究にあたり相手国から求められる場合や、同志国等と対等な立場で実施するために必要な場合に、各府省が支援し、決定する研究開発プログラムも含む。	・破壊的技術革新が進む技術（破壊的革新技術）をはじめ、将来の技術優位性の創出を目指す技術領域として各府省が支援し、決定する研究開発プログラム
②対象技術		・支援を受けて行う生産に有用かつ中核的な技術 ・支援を受けて行う研究開発の成果である技術 「コア技術」 ・コア技術の実現に直接寄与する技術 （いずれも非公知のものに限る）	・支援を受けて行う研究開発の成果及びその活用の際に必要となる技術の設計・生産・利用の各段階において有用かつ中核的な技術（ソフトウェアを含む） （コア重要技術） ・コア重要技術の実現に直接寄与する技術 （コア重要技術等） （いずれも非公知のものに限る）	
具体的な技術流出防止策	**③社内・従業員における管理**	・対象技術を特定し、これにアクセス可能な従業員を必要最小限の範囲に制限 ・管理のための体制／規程等の整備 ・退職等を通じた技術流出の防止の取組 （従業員の相応な待遇確保等） ・競業避止義務の同意を得るための取組	・左記を踏まえつつ、企業の技術管理対策も参考にした上で、リスクに応じ、 ✓ 秘密保持契約の締結 ✓ 本人からの情報提供 ✓ 本人による情報管理等に関する誓約の取得 （デューデリジェンスの一例） ✓ オープンソースDD ✓ モニタリング・監査 等 の技術流出の防止の取組	
	④取引先における管理	・対象技術を保有する取引先と秘密保持契約を締結し管理を実施（取引先においても③に相当する措置を求め、履行状況の定期レビューを行うなど）		
	⑤技術移転等の管理	・他者又は他国に対する対象技術の移転等※2は事前に所管省庁等への相談 （※2　移転、ライセンシング、共同研究開発、他国での研究開発／生産拠点設置・増強）	左記に同じ	

※1 我が国が技術優位性を持つ技術領域のうち、主な対象領域を記載。

【参考】イメージ

経済安全保障上重要な技術として国からの資金支援※を行う技術（☆）

※社会実装を見据えた研究開発等の資金支援

☆のうち、技術流出防止措置を検討すべき領域

将来の不可欠性・自律性の獲得

① 将来の我が国の技術優位性の創出を目指す技術領域

不可欠性の維持

② 我が国が技術優位性を持つ技術領域

②のうち、サプライチェーン強靱化における技術流出防止措置の対象技術領域※

（※技術流出防止措置要件を追加し対応）

自律性の獲得・過剰依存の低減

③　①②以外の国からの資金支援を行う経済安全保障上の重要技術