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

大学見本市 2024 Innovation Japan
JST研究開発戦略センターセミナー

テクノロジー、サステナビリティ、Well-beingの交差点
～イノベーションの動向を掴む～

「研究開発を守る：各国の研究セキュリティ」

2024年8月23日

JST研究開発戦略センター（CRDS）
安全安心グループ
奥田 将洋

発表内容

１．研究セキュリティとは何か

２．なぜ研究セキュリティが重視されているか

(参考)研究システムの不当な利用

３．諸外国における研究セキュリティ確保の取組み

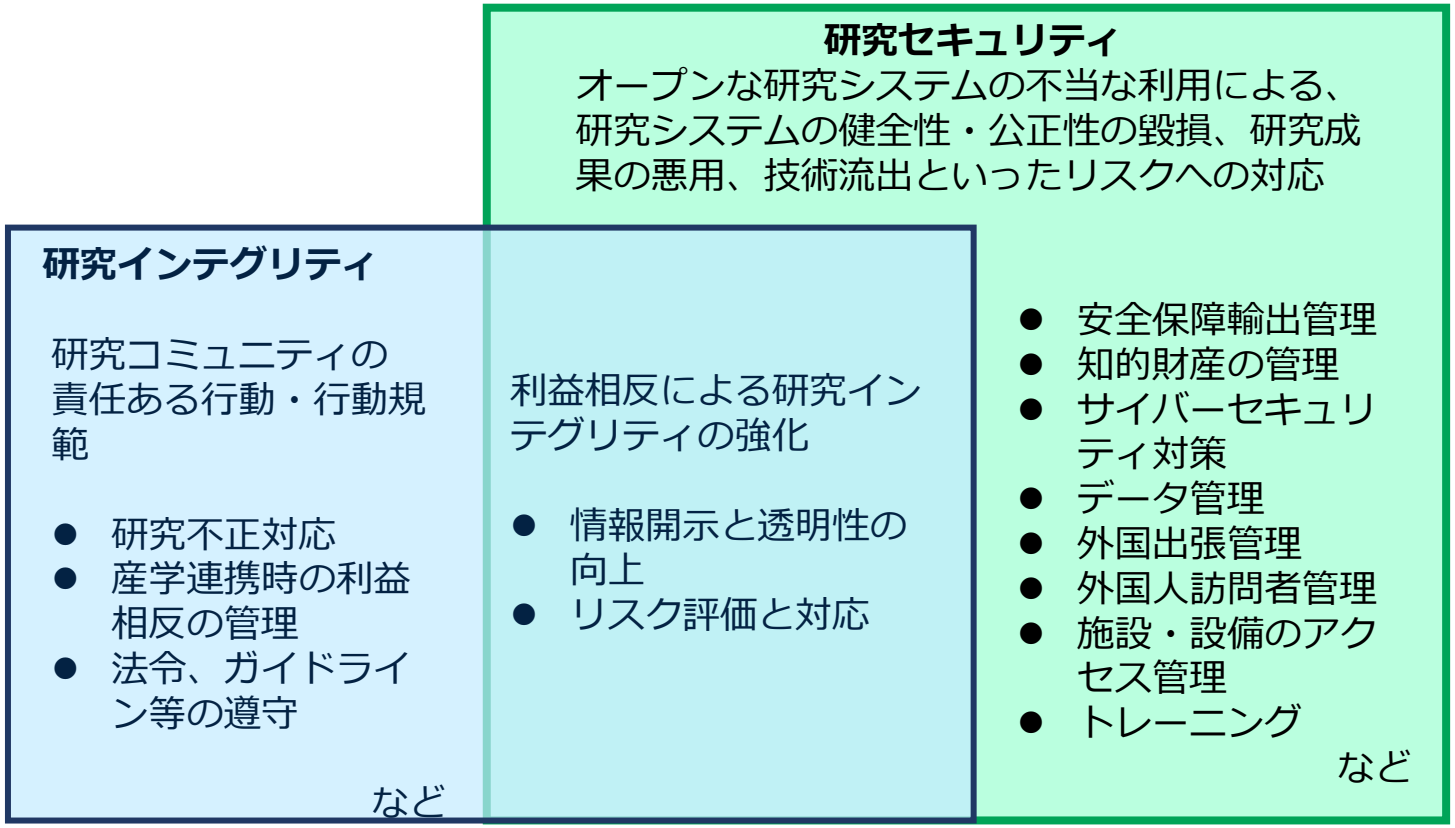
４．日本における研究セキュリティ確保の取組み

５．まとめ　今後の方向性と課題

©2024 CRDS

1．研究セキュリティとは何か

- 研究のオープン化、国際化が進む一方、その不当な利用により研究システムやその成果が毀損されることで、研究成果が不当に悪用されたり、技術流出につながるリスクが増えている。
- このようなリスクへの対応を**「研究セキュリティ」**と呼ぶ。呼び方は各国で様々・・・



研究インテグリティと研究セキュリティ

米国 — **Research Security**

英国 — **Trusted Research**

豪州 — **Countering Foreign Interference**

カナダ — **Research Security**

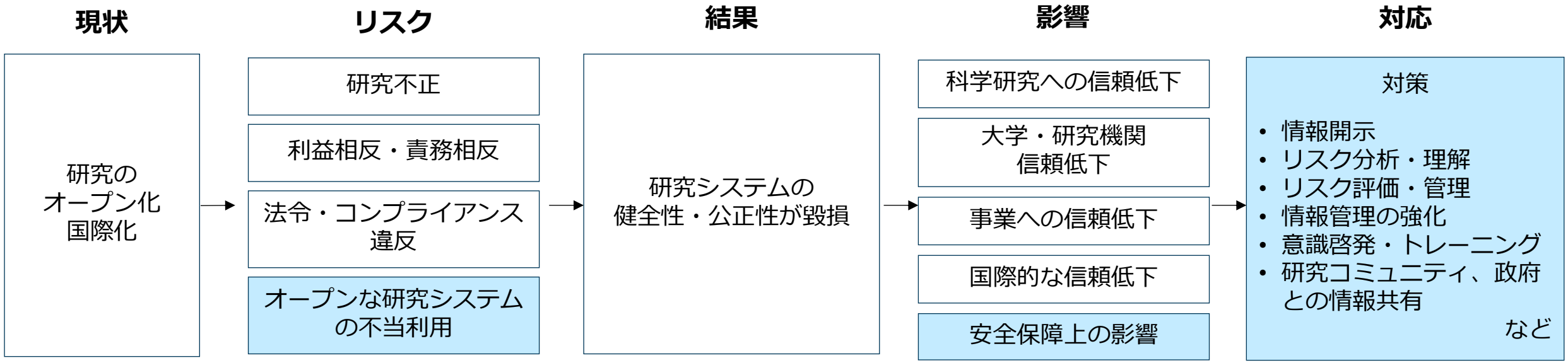
日本 — **研究インテグリティ**

「研究セキュリティ」を示す言葉は様々

©2024 CRDS

2．なぜ研究セキュリティが重視されているか？

- 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ともに**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**。
- 不当利用によって、研究の健全性・公正性が毀損される。その影響として、研究や事業の信頼低下を招く。安全保障上の影響が生じることもある。
- **活力ある研究システムを維持するため**にも研究セキュリティが重要。対策として**情報開示、リスクマネジメント、意識啓発やトレーニング**などがある。



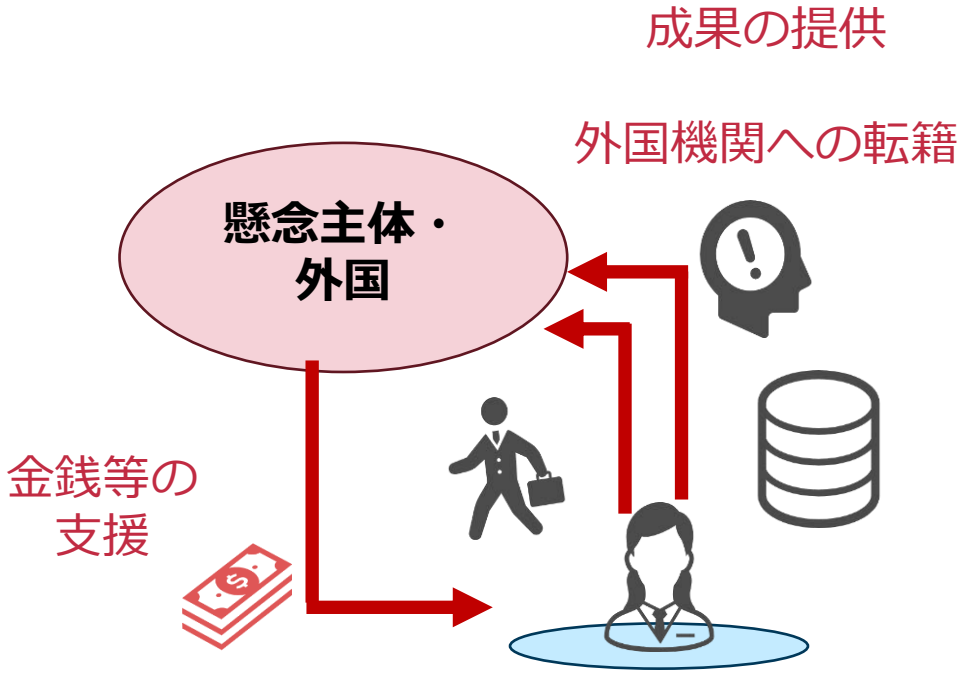
©2024 CRDS

（参考）研究システムの不当な利用

- 2010年代以降、外国等懸念主体による知財、人材、技術獲得などの行為、活動が活発になっている。以下のような行為、活動が各国の調査で明らかになっている。

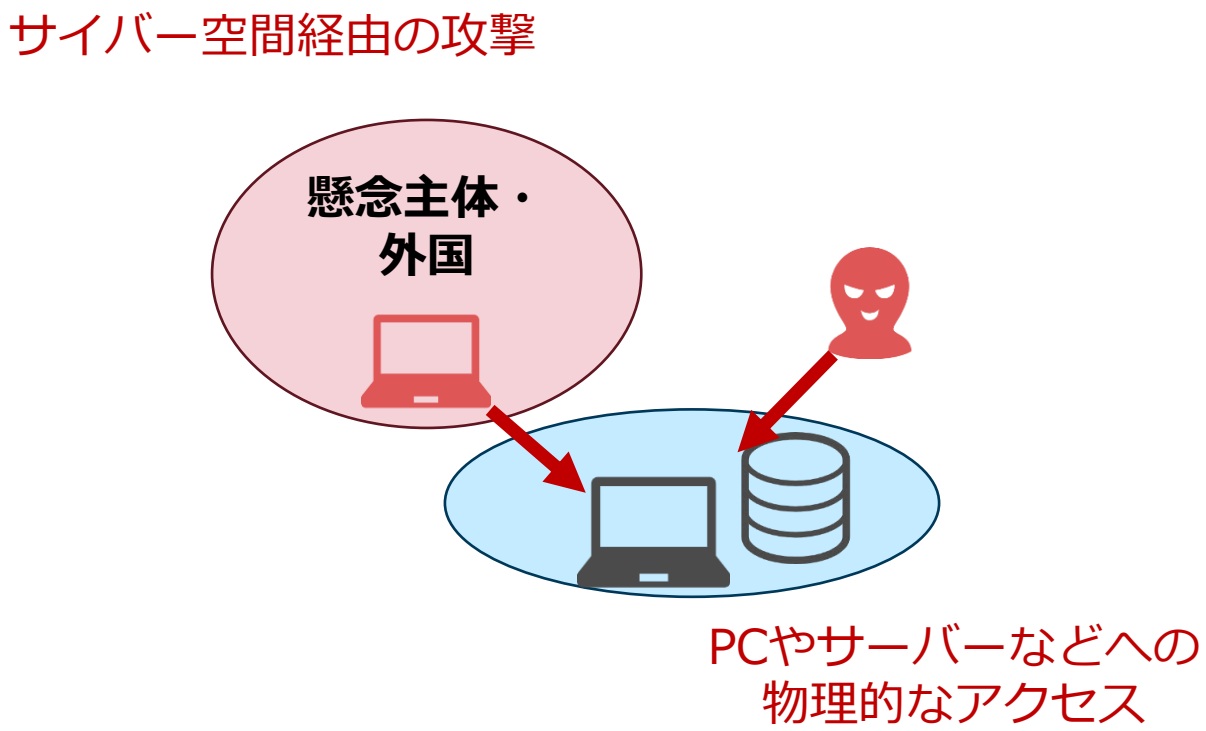
大学研究者のリクルート活動

ポジション、高報酬、研究環境の提供による研究者や成果の獲得



サイバー攻撃

サイバー・物理的手段によるデータ盗取



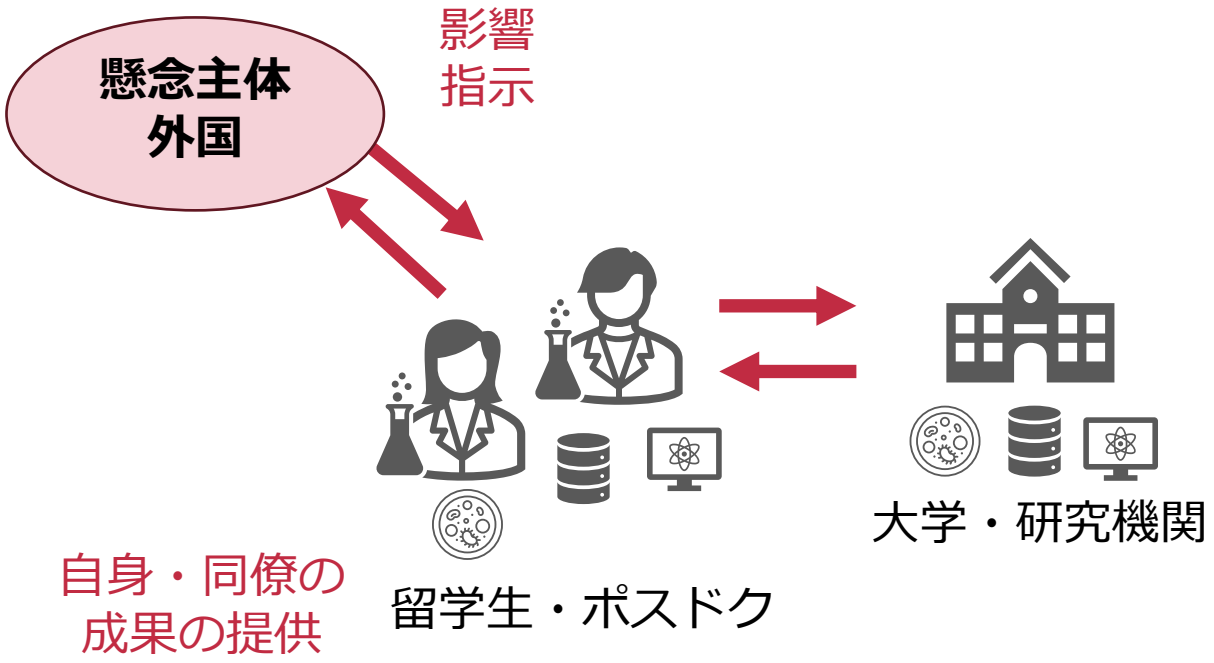
©2024 CRDS

（参考）研究システムの不当な利用(続き)

- 2010年代以降、外国等懸念主体による知財、人材、技術獲得などの行為、活動が活発になっている。以下のような行為、活動が各国の調査で明らかになっている。

留学生による技術情報の収集

許可された/許可されないアクセスによる情報流出



大学の意思決定への影響

寄付等の金銭的支援、人的支援によって
大学の意思決定に影響

©2024 CRDS

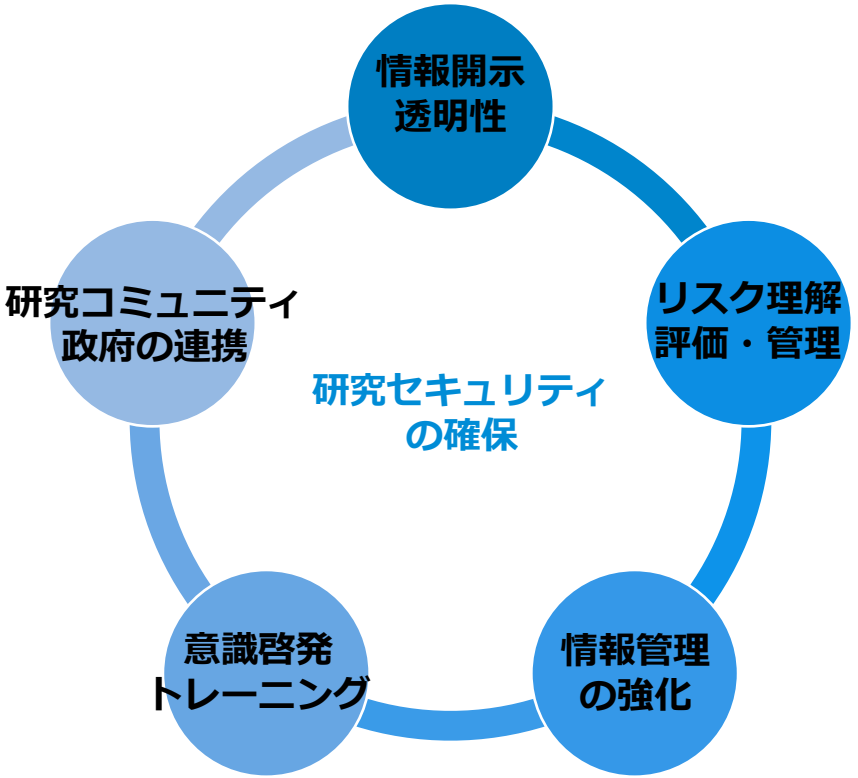
諸外国における研究セキュリティ確保の取組み

- **情報開示**による透明性確保、**トレーニングや意識啓発**、**情報管理**、**リスク管理・評価**がある。
- 取り組みの実施に向けた**政府からのガイドライン提示**や大学・研究機関間での**情報共有**など、**関係者間の連携も重要**。

研究セキュリティに関する各国の取組み例

米国	• 政府機関出資の研究開発での情報開示と情報開示フォーム統一 • リスクベースでのセキュリティ：必要な部分に追加的な保護 • 国の資金配分機関によるトレーニングモジュール開発
英国	• 国際研究協力上の研究セキュリティリスク対策の助言機関を政府内に設置
カナダ	• 研究セキュリティリスク特定のためのトレーニングやチェックリスト等をまとめて提供
豪州	• 研究セキュリティ関連のガイドラインの中で大学の体制整備やサイバーセキュリティ対策を推奨

研究セキュリティの一般的な取組み (現在の調査から)



©2024 CRDS

日本における研究セキュリティ確保の取組み

- 日本は研究セキュリティに関する取組を、研究不正や利益相反・責務相反対策である**研究インテグリティの新たな領域として位置付け**。
- この中で、情報開示などを強化。その他、輸出管理など、従来からの取組みの強化も行われている。

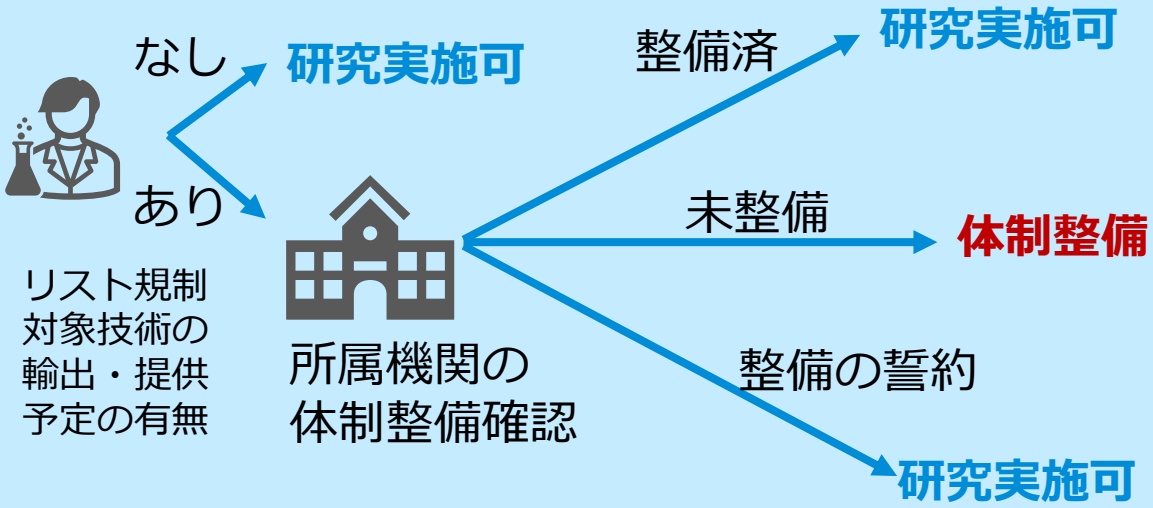
日本の研究セキュリティの取組み

情報開示
- 国際研究連携の透明性確保
- 所属機関や資金提供元への必要な情報の申告
- 政府：チェックリスト(ひな形)の提供、アウトリーチ

マネジメント体制強化
- 情報開示の体制(変更・更新を含む)
- リスクマネジメント体制
  - ✓ 研究者からの相談の窓口
  - ✓ 契約や研究資金等の提供の管理部門
  - ✓ 意思決定のための体制
- 政府：新たなリスク事例の共有

出所：内閣府科学技術・イノベーション推進事務局
「研究インテグリティの確保に係る対応方針（概要）」

輸出管理の強化
- みなし輸出管理明確化(2022年5月～)
- 資金提供の際の輸出管理の要件化

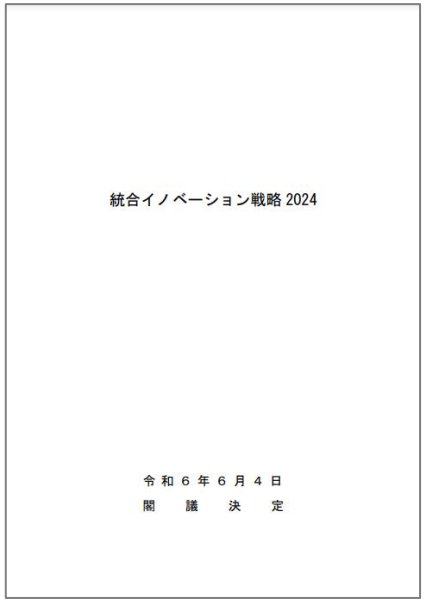


参考：日本学術振興会「安全保障貿易管理の要件化について」
<https://www.jsps.go.jp/file/storage/kaken_g_1629/r6jimurenbessi2.pdf>

©2024 CRDS

まとめ 今後の方向性と課題

- 研究セキュリティの重要性は一層高まる：国際化・オープン化に伴うリスクから研究者や研究機関を守る



「統合イノベーション戦略2024」(2024年6月4日)

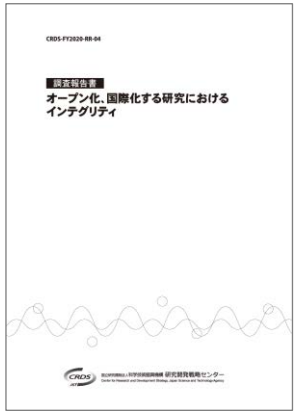
「研究活動の国際化・オープン化に伴うリスクに対し、**大学や研究機関における研究セキュリティ・研究インテグリティの確保**に取組むとともに、技術流出防止の観点から投資審査等の体制強化、留学生・外国人研究者等の受入れ審査強化、大学・研究機関・企業等における機微な技術情報の管理強化、政府研究開発事業における安全保障貿易管理の要件化に**引き続き取り組んでいく**」

「統合イノベーション戦略2024 」P.16より

- 当面の重要事項：情報開示とリスク管理、法令遵守、セキュリティ文化の醸成
- 諸外国も研究セキュリティ確保に向けた取組みを継続
- 科学研究の開放性と研究セキュリティのバランスが重要

©2024 CRDS

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

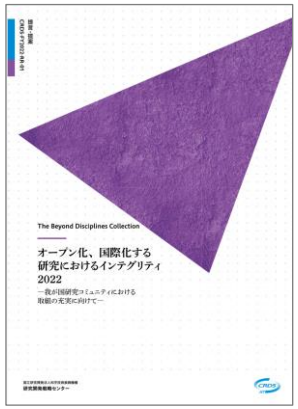


**「オープン化、国際化する研究における
インテグリティ」
（2020年10月）**

https://www.jst.go.jp/crds/report/CRDS-FY2020-RR-04.html

**「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）**

https://www.jst.go.jp/crds/report/CRDS-FY2022-XR-01.html



**「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）**

https://www.jst.go.jp/crds/report/CRDS-FY2022-RR-01.html

**「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）**

https://www.jst.go.jp/crds/report/CRDS-FY2023-RR-08.html

©2024 CRDS

■作成担当■
奥田 将洋 フェロー （安全安心グループ）

CRDS-FY2024-XR-04
その他報告書

テクノロジー、サステナビリティ、Well-beingの交差点 ～イノベーションの動向を掴む～
「研究開発を守る：各国の研究セキュリティ」

令和6年8月 August 2024
ISBN 978-4-88890-940-2

国立研究開発法人科学技術振興機構　研究開発戦略センター
Center for Research and Development Strategy, Japan Science and Technology Agency

〒102-0076 東京都千代田区五番町7 K’s五番町
電 話　 03-5214-7481
E-mail crds@jst.go.jp
https://www.jst.go.jp/crds/

本資料は著作権法等によって著作権が保護された著作物です。
著作権法で認められた場合を除き、本資料の全部又は一部を許可無く複写・複製することを禁じます。
引用を行う際は、必ず出典を記述願います。
なお、本報告書の参考文献としてインターネット上の情報が掲載されている場合には、本報告書の発行日の1ヶ月前の日付で入手しているものです。
上記日付以降後の情報の更新は行わないものとします。

This publication is protected by copyright law and international treaties.
No part of this publication may be copied or reproduced in any form or by any means without permission of JST,
except to the extent permitted by applicable law.
Any quotations must be appropriately acknowledged.
If you wish to copy, reproduce, display or otherwise use this publication, please contact crds@jst.go.jp.
Please note that all web references in this report were last checked one month prior to publication.
CRDS is not responsible for any changes in content after this date.

Copyright © 2024 CRDS All Rights Reserved.