研究開発セキュリティ・クリアランス勉強会　報告書

2025 年 3 月 11 日

（目次）

（参考資料）

はじめに

本報告書は、東北大学及び民間企業の有志で構成する勉強会の成果としてまとめたものである。

現在、世界は、大規模な技術開発競争の中に置かれている。先端技術の研究開発を行う、大学を含む各研究機関も、このような動向と無関係であることはできない。

そのような中、日本政府は、2013 年（平成 25 年）以降、特定秘密の保護に関する法律（内閣官房、平成 25 年法律第 108 号）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）（内閣府、令和４年法律第 43 号）、重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）（内閣府、令和６年法律第 27 号）の３本の法律を整備し、情報漏洩防止等のための枠組み作りを進めてきた。

経済安全保障推進法では、特定重要技術として、AI、量子コンピュータ、バイオテクノロジーなどの技術が定められている。他方で、本法律が、米国や欧州といった、先んじて制度作りを行ってきている国々を強く認識していることに鑑みれば、米国の Science and Technology Risk Matrix （S&T リスクマトリックス）がターゲットとしている、量子情報科学（Quantum Information Science & Technology）、高性能計算（High Performance Computing）、人工知能（AI）、バイオテクノロジー（Bioscience & Biotechnology）、バッテリー科学（Battery Science & Technology）、そして、加速器科学（Accelerator Science & Technology）といった分野については、十分な注意が必要であると考えられる。

我が国では、東北大学青葉山新キャンパスにおいて、近年、正に、最新鋭の加速器である「NanoTerasu」を整備し、現在、その利用促進と拡充を進めている。また、東北大学は、2019 年以来、世界の主要 20 放射光施設の Director による国際放射光サミットを主宰し、グローバルな社会課題の解決に向けた提言（AOBA Communique）を行ってきた。NanoTerasu は、最先端の国際的な研究開発の拠点であるとともに、産学が協働で研究を行う、Coalition としての新たなモデルを提示するものであり、2024 年 4 月の運用開始以来、様々な研究者・技術者が同時に参画している。ここでは、情報の厳しい管理が強く求められることに疑問の余地はない。

このような背景の下、本勉強会では、日本、米国を始めとする各国のセキュリティ・クリアランスの状況を把握するとともに、NanoTerasu として、今後直面する可能性がある課題の洗い出しを行った。特に、基礎研究にとって重要なオープンサイエンスとの調和、国際共同研究の推進のための配慮など、大学周辺では十分に議論されてこなかったポイントについても、可能な限り包含した。

ただし、日本の制度は、まだ、議論の緒に就いたばかりである。また、限られた時間の中で、十分な情報を集めることができたかについては、いささか、疑問である。従って、本報告書は、今後の議論の出発点と

してご理解頂ければ幸いである。

今後の先端技術の開発において、日本の研究者・研究機関がリーダーシップを発揮し、国際研究が促進されると同時に、技術の漏洩・不正利用などが生じないことを強く願うばかりである。

研究開発セキュリティ・クリアランス勉強会　座長　　湯上　浩雄

サマリー

科学技術が国際競争力の源泉となる現代社会において、研究開発成果の適切な保護と活用は、将来の国力を左右する重大なテーマである。技術競争が激化する中、単独の国や企業、研究機関での研究開発は限界を迎えつつあり、国際連携や産学連携といった活動は必須になっている。

他方で、研究の大規模化、先端化は急速に進んでおり、共同で利用する大型研究開発インフラが極めて重要な役割を果たしている。例えば、高輝度放射光施設 「NanoTerasu」 は、研究者からのみならず、民間企業からも非常に大きな注目・関心が集まっており、民間主体、あるいは、産学連携の研究開発を通じて、基礎から応用、社会実装に至る様々な重要課題の解決のために利活用が進んできている。

このような状況の中、研究開発の成果としての技術の機密保護、情報漏洩防止の必要性がこれまで以上に増している。それは、１つは、国家の安全保障に係る技術・情報の保護の観点、そして、もう一つは、企業の競争力の源泉となる技術の漏洩防止の観点である。

世界各国は、その重要性を深く理解し、セキュリティ・クリアランス制度を中心とした対応を進めてきた。米国では、伝統的にＴＳ（top secret）及びＳ（secret）に関する厳格な制度を確立していたが、近年、ＣＵＩ（controlled unclassified secret）を含めた、S&T risk matrix の整備が進められている。欧州においても、欧州共通指令の枠組みの下、各国の実情に応じた対応が進んでおり、英国では、欧州のルールに準拠しつつも、独自の枠組みを構築してきている。

我が国においても、2024 年に成立した、「重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）」により、セキュリティ・クリアランスの導入が決定され、今まさに、新たな制度の運用が開始されようとしている。

しかしながら、我が国の経済安全保障分野において、このような制度の導入は初めてのことである。急速に進む研究環境の変化の中で、研究現場での対応は、ある意味、手探りの状態に陥る可能性がある。

そこで、国際卓越研究大学に認定された東北大学では、日本の研究機関のリーダーの一つとして、敷地内にある NanoTerasu の利用環境の促進の観点も含め、研究現場のマニュアルとしての役割も想定しつつ、セキュリティ・クリアランスの関する現状の分析と今後の課題を取りまとめた。

具体的には、まず、日本の制度、欧米の制度を概観する一方で、日本の研究開発機関が直面する課題について整理した。その上で、セキュリティ・クリアランスの必要性の是非を論じ、特に、国際共同研究を推進する上での、制度の国際的整合性の重要性を強調した。最後に、新たな制度を運用するにあたっての、研究現場から見た要望を率直に列記した。

詳しくは、本文に譲るが、本報告書が、研究現場におけるセキュリティ・クリアランスの適切な運用の一助と

なることを切に願う。

第一章 現状認識（各国の動向）

（１） 日本の現状

近年、我が国を取り巻く経済・社会環境は厳しさを増しており、日本においても、経済安全保障の有用性が高まっている。特定秘密の保護に関する法律では、国家機密（機密、極秘）に該当する情報を、「特定秘密」と定義するなど、国際社会と調和のとれた制度構築を進めるため、政府は、以下の法律を制定してきている。

- 特定秘密の保護に関する法律（内閣官房、平成 25 年法律第 108 号）
- 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）（内閣府、令和４年法律第 43 号）
- 重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）（内閣府、令和６年法律第 27 号）

また、関連の法制度として、外国為替及び外国貿易法（外為法、1949 年制定）、DISM（Defense Industry Security Manual）（2023 年 7 月防衛装備庁策定）が存在する。

詳しくは、以下の（表 1-1-1）～（表 1-1-3）に記載する。

（表 1-1-1）

法律名	特定秘密の保護に関する法律	経済安全保障推進法	重要経済安保情報保護活用法
施行年	2014 年	2022 年	2025 年
目的	国家安全保障に関連する情報（「特定秘密」）の保護	経済施策を一体的に講ずることによる安全保障の確保の推進	国家が指定する「重要経済安保情報」の漏洩防止、それによる国民の安全の確保
ポイント	**（法律が指定する「特定機密」の範囲）** **対象分野**：防衛、外交、スパイ活動防止、テロ防止 **指定基準**：情報が漏洩した場合、国家安全保障に著しい影響を与える可能性があるもの **（管理）** 事前に身辺調査を受けた上で認められた者のみアクセス可能、情報漏洩には厳しい罰則（最大 10 年の懲役刑）	サプライチェーン強靭化、基幹インフラの安定的な提供、特定重要技術（AI、量子コンピュータ、バイオテクノロジーなど）の開発支援、特許非公開制度の導入	**（主な狙い）** **国民の安全の確保** **重要経済安保情報の取扱者の制限** **情報漏えいの防止** **（構成）** **①人的クリアランス（PCL: Personal Security Clearance）** 対象としては、国家安全保障上重要な情報を取り扱う個人。基本情報、犯罪歴、財務状況、外国との関係、その他（テロ活動や産業スパイ行為への関与がないこと）についての適性評価を実施 **②施設クリアランス（FCL: Facility Security Clearance）** 対象としては、機密情報を取り扱う企業や研究機関。**人的要件**として、セキュリティ管理者の任命と教育、及び、情報取扱者全員が PCL を取得。今後定めていく**物理的要件**として、侵入感知、機密情報保管エリアの物理的防護措置、**サイバーセキュリティ要件**として、ネットワーク隔離等が挙げられている。

（表 1-1-2）

法律名	外国為替及び外国貿易法（外為法）
制定年	1949 年制定
目的	当初は、我が国の国際収支の均衡を図り、通貨の安定を維持することを目的 現在では、安全保障貿易管理の観点から、大量破壊兵器等の拡散防止、テロリズムの防止等の観点からも重要な役割
規制対象	**支払等**：貿易やサービスの対価の支払い、贈与、寄付など、国際的な資金の移動を伴う取引。海外への送金や海外からの送金なども該当。例えば、共同研究における経費の支払い、海外の研究機関への寄付など **資本取引**：外国企業への投資、外国証券の売買、不動産の取得など、資産の国際的な移動を伴う取引。海外の研究機関への投資や海外の企業との合弁事業などが該当 **役務取引**：特定の技術を外国に向けて提供する取引や、居住者が非居住者に対して提供する取引。ソフトウェアや設計図などの技術情報の提供、技術指導、共同研究などが該当
手続き	**許可**：あらかじめ主務大臣の許可を受ける必要がある取引が対象 **届出**：あらかじめ主務大臣に届け出る必要がある取引が対象 **報告**：事後に主務大臣に報告する必要がある取引が対象
罰則	**懲役**：個人の場合、最大で 10 年の懲役刑 **罰金**：個人の場合、最大で 1,000 万円の罰金。法人の場合、最大で 3 億円の罰金 **行政制裁**：期間を限り輸出又は特定技術の提供等が禁止
技術流失防止	**リスト規制**：大量破壊兵器等に関連する貨物や技術の輸出を規制。経済産業省のリストに掲載されている貨物や技術を輸出する場合には、経済産業大臣の許可が必要 **キャッチオール規制**：大量破壊兵器等に用いられるおそれのある貨物や技術を、たとえリスト規制の対象でなくても、輸出を規制。輸出者が、輸出する貨物や技術が大量破壊兵器等の開発等に用いられるおそれがある場合には、経済産業大臣の許可を取得する必要 **外国ユーザーリスト**：経済産業省の大量破壊兵器等の開発等への関与が懸念される海外の機関に掲載されている企業などに輸出等を行う場合に、必要があれば、経済産業大臣の許可が必要 **役務取引規制**：特定の技術を外国に提供することを規制する制度。技術を提供する相手方の国籍や居住地、技術の内容等に応じて、経済産業大臣の許可が必要

研究開発関連	**「技術」の定義**：貨物の設計、製造又は使用に必要な特定の情報。技術データ又は技術支援の形態で提供 **技術データ**：技術内容が記載された文書や設計図，仕様書，マニュアル，指示書、プログラム等 技術を外国に向けて提供する取引や、居住者が非居住者に対して提供する取引、又は国外で提供するために持ち出すこと（メール送信等も含む）も対象 外国人研究者が、研究内容に関する情報提供を義務付けられている場合、日本の法律と出身国の法律の両方に抵触しないよう注意する必要 外国人研究者が、研究開発を通じて得た情報を、出身国等に持ち出すおそれがある場合、秘密保持契約の締結やアクセス制限などの措置を講じる必要

（表 1-1-3）

制度名	**防衛産業保全マニュアル（DISM：Defense Industry Security Manual）**
策定年	2023 年 7 月（防衛装備庁）
目的	防衛産業における秘密情報の保護措置に関する包括的なルールを規定した文書。国際水準を踏まえた産業保全の強化を目的 **国際的な防衛装備・技術協力の円滑化**：国際共同研究や海外政府の調達案件に日本企業が参加できるよう、同盟国・パートナー国との間で秘密情報を適切に保護するための「実質的同等」な制度を整備 **防衛産業のセキュリティ強化**：サイバー攻撃を含む諸外国の情報活動などのリスクから、防衛産業における秘密情報を適切に保護 **透明性・信頼性の向上**：防衛装備・技術協力の円滑化を促進 **効率的な制度運用**：「安全性」と「合理性」を両立した効率的な制度運用
構成	「防衛秘密」（防衛秘密の漏えい防止に関する法律で規定されている秘密）、及び、「装備品等秘密」（防衛装備庁の装備品等に係る秘密の保護に関する訓令で規定されている秘密）に分類。「秘密情報」について定義はない **基本原則**：情報の取扱いに関する基本的な原則を定め、漏えい防止、不正アクセス防止、紛失・盗難防止等に必要な措置を規定 **教育・訓練**：従業員に対して適切な教育・訓練を実施 **漏えい防止措置**：リスク管理体制を構築 **情報に関する記録の管理**：作成、受領、保管、廃棄等に関する記録を適切に管理。トレーサビリティを確保 **輸出管理**：防衛装備品等の輸出管理に関するルールを規定 **事故発生時、漏えい等の対応**：procedures を規定。被害の拡大防止と再発を防止 **施設・設備に関する要件**：情報を保管する施設や設備に関するセキュリティ要件（物理的

	なセキュリティ対策）を規定 **サイバーセキュリティ**
セキュリティ・クリアランス	**①人的クリアランス**：秘密情報取扱資格（Personnel Security Clearance） 秘密情報取扱資格として秘密取扱適格性を規定。（ただし、具体的基準に関する詳細は未記載）。「秘密の取扱いに関する適格性の確認等に関する訓令 （平成 21 年防衛省訓令第 25 号）第２条第４号」に規定されている適格性を付与された者が基本 **②施設クリアランス** -**施設要件**：部外者の侵入を防ぐための適切な措置 -**設備要件**：盗難、紛失、破壊、及び漏えいを防ぐための適切な措置 **③サイバーセキュリティ** -**リスク管理**：サイバー攻撃のリスクを評価。適切なセキュリティ対策 -**アクセス制御**：情報へのアクセスは、必要最低限の者に制限 -**ネットワーク・セキュリティ**：外部からの不正アクセスを防ぐための適切な措置 -**マルウェア対策** -**従業員教育** -**インシデント対応**
関連法・ガイドライン	-特定秘密保護法 -防衛秘密の漏えい防止に関する法律 -安全保障貿易管理令 -防衛生産基盤強化法

（２） 世界の動向

①米国の研究開発セキュリティ・クリアランス制度

a. 総論

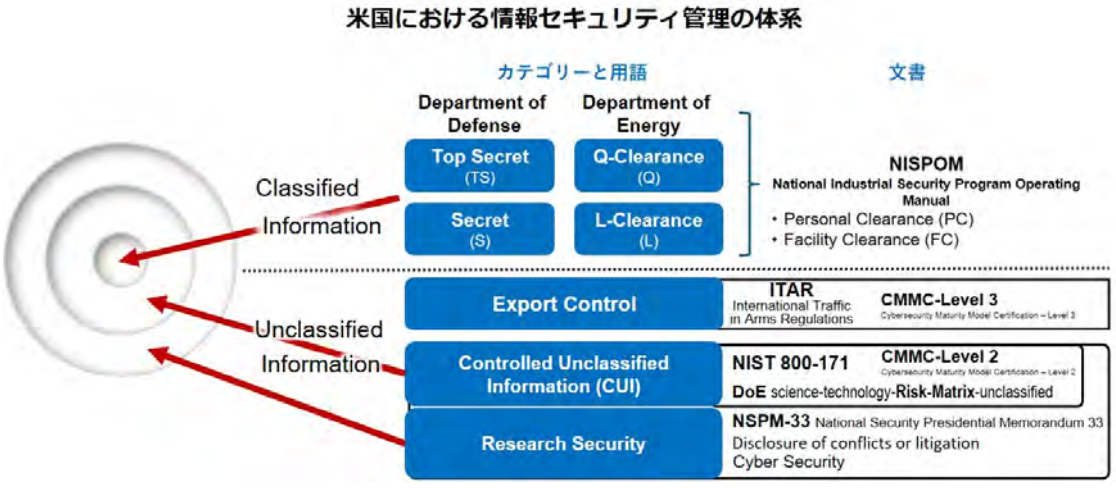
米国では、国家安全保障と経済競争力の維持に係わる研究開発について、高度な情報管理体制を整備している。この制度は、国家機密（Classified Information : top secret & secret）から、戦略的重要性を持つ情報（Controlled Unclassified Information, CUI）までを対象とする。

なお、国家機密は、NISPOM（National Industrial Security Program Operation Manual）を持って管理しており、CUI（管理対象非機密情報）の管理には、NIST SP 800-171 をはじめとするガイドラインを適用している。

（表 1-2-1）

国家機密（Classified Information）	Top Secret（機密）	不正開示が「例外的に重大な損害」をもたらす情報	（例）核関連技術、軍事用途技術、外交情報
	Secret（極秘）	不正開示が「重大な損害」をもたらす情報	
戦略的重要性を持つ情報（Controlled Unclassified Information, CUI）		非機密情報であるが、国家安全保障や経済に重要な影響を与える情報	（例）研究データ、輸出規制対象技術、技術移転関連情報

（図 1-2-2）



これらの制度の中核は、人的クリアランス（Personnel Clearance, PCL）、施設クリアランス（Facility Clearance, FCL）、及び、セキュリティ措置で構成される。PCL は、情報にアクセスする個人の適格性を審査するものであり、FCL は、機密情報を扱う施設の物理的・情報的セキュリティ基準、また、セキュリティ措置は、アクセス制御、データ暗号化、監査ログの保持等を行うためのものである。

CUI の管理では、輸出規制（export control）も重要な柱。関連の規程として、ITAR（International Traffic in Arms Regulations）や EAR（Export Administration Regulations）が存在する。なお、「みなし輸出規制（Deemed Export）」も、この対象となる。

CUI の具体的対象技術については、DOE（エネルギー省）が、「科学技術リスクマトリックス（Science and Technology Risk Matrix, S&T マトリックス）」を作成し、新興分野でのリスク管理を可視化している。これには、量子技術、人工知能（AI）、バイオテクノロジー等が包含される。

b. 各論Ⅰ（国家機密関係）

NISPOM に基づく、人的クリアランス（Personnel Clearance, PCL）、施設クリアランス（Facility Clearance, FCL）、及び、セキュリティ措置の要件等は以下のとおりとなっている。

i. 人的クリアランス（Personnel Clearance, PCL）

（主な要件）

- **市民権**： 原則として米国市民であること
- **身辺調査**：米国政府の「Whole-Person」コンセプトに基づき、13 の国家安全保障裁定ガイドライン（SEAD-4）を総合的に考慮し、過去の経歴、犯罪歴、財務状況、人間関係などを調査
- **背景調査**：バックグラウンドをチェックするために、インタビュー形式の審査や周囲の人物への聞き取り調査
- **適性評価**：対象者の性格や信頼性、誠実さの評価

（手続き）

- 雇用主（通常は、政府機関または政府との契約を持つ企業）がクリアランスを申請。
- 従業員に取得のリクエストを行い、Electronic Questionnaires for Investigations Processing (e-QIP) へのログイン情報を提供。
- 従業員は e-QIP を使用して Standard Form (SF) に記入。過去 10 年間の居住地、雇用履歴、家族に関する情報などを記載する必要。指紋も提供。

- Vetting Risk Operations Center (VROC) が調査を行い、提供された情報を確認。暫定または完全なクリアランスを付与。
- クリアランスが付与された従業員は、最初のセキュリティブリーフィングを受け、担当するプログラムに読み込まれ、SF 312 (機密情報非公開契約) に署名。
- 継続的な評価に登録し、SF 86 記載情報に変更があった場合は 5 年ごとに更新。
- 32 CFR Part 117, NISPOM に定められた報告 (結婚、重大な経済状況の変化、海外渡航など)

ii. 施設クリアランス（Facility Clearance, FCL）

（要件）

- **物理的セキュリティ**：アクセス制御、監視システム、物理的防護、緊急時対応計画（Evacuation Plan）の策定と訓練、保管設備
- **情報管理**：情報分類（Top Secret、Secret、Confidential）に応じたアクセス制御、電子保存や転送の際の暗号化
- **施設セキュリティ担当者**：セキュリティ計画の運用管理、従業員へのセキュリティ教育、定期的な監査対応、情報漏洩時の報告
- **人的クリアランス（PCL）の取得**

（手続き）

- **スポンサーシップ**：連邦政府機関またはその契約者が FCL 取得の必要性を保証
- **セキュリティ計画（Security Plan）**：NISPOM に基づく計画を策定・提出

（審査、発行）

- Defense Counterintelligence and Security Agency (DCSA) が施設の物理的セキュリティ、情報管理体制、従業員のクリアランス資格を評価

iii. セキュリティ措置

2021 年 2 月の連邦規則である「32CFR Part 117, NISPOM」（最新版は 2022 年 12 月 8 日改訂版）として発効された。 機密情報の保護、取り扱い、および保護に関する包括的な基準を規定する。この基準は、請負業者、ライセンシー、グランティー、または証明書保有者によって、開示または開発された機密情報を保護するための要件を確立しており、禁止されている開示を防ぐ。また、「Security Executive Agent Directive (SEAD) 3」によって、クリアランスを取得した人員のセキュリティ報告義務を追加した。主なセキュリティ対策は（表 1-2-2）のとおりとなっている。

（表 1-2-2）

セキュリティ措置	説明
情報システム セキュリティ	アクセス制御、認証メカニズム、暗号化、ファイアウォール、侵入検知システムなどのセキュリティ技術を実装。情報システムをサイバー脅威から保護。
初期セキュリティ ブリーフィング	請負業者、従業員に初期セキュリティブリーフィングを提供。ブリーフィング内容は、脅威認識、防諜認識、情報セキュリティ分類の概要、報告義務と要件、トレーニング、セキュリティ手順と義務など。
リスク管理 フレームワーク	リスクを管理するために使用される 7 段階のプロセス。継続的なリスク軽減戦略に対応。準備、分類、選択、実装、評価、承認、監視など。
ログの監視 セキュリティ監視	ユーザーアクティビティの監視、ログのリアルタイム分析、または、定期的なレビュー。セキュリティイベントの迅速検出。これには、疑わしいアクティビティの特定、潜在的な脅威または脆弱性の検出、および適切な対策の開始が含まれる。
物理的セキュリティ	不正アクセスまたは破壊から保護。
トレーニングと 意識向上	従業員にセキュリティプロトコルと機密情報の保護の重要性について定期的なトレーニングセッションを提供。

c. 各論Ⅱ（CUI 関係）

CUI については、NIST SP 800-171（CUI 管理ガイドライン）、輸出規制等に基づき、管理されている。また、DOE が策定した「リスクマトリックス（Science and Technology Risk Matrix）」がリスク管理を可視化している。

i. NIST SP 800-171

（主な要件）

- **アクセス制御**： 必要最小限のアクセス権付与、ユーザー認証の徹底
- **メディア保護**：暗号化など
- **監査と説明責任**：監査ログの保持ほか
- **人的セキュリティ**
- **物理的保護**：サーバーや端末が置かれる施設へのアクセス制限
- **セキュリティ評価**
- **その他（全 14 項目）**

ii. 輸出規制（Export Control）1 ： International Traffic in Arms Regulations（ITAR）

（対象及び特徴）

- 防衛物資リスト（United States Munitions List: USML）に掲載された物品や技術（例：武器システム、軍用航空機、軍事用ソフトウェア、暗号化技術）
- 米国以外への技術移転を厳しく制限
- 技術やデータが電子的に共有された場合も規制の対象（例：デジタルファイル共有、電子メール）

iii. 輸出規制（Export Control）２ ： Export Administration Regulations（EAR）

（対象及び特徴）

- 米国商務省が運用しており、軍事・民生両用技術（デュアルユース技術）や特定の商業技術を管理
- **商業用途および軍事用途の技術・製品**：EAR 規制対象リスト（Commerce Control List: CCL）に記載された項目（例：半導体技術、人工知能（AI）、量子技術、高性能コンピュータ）
- 輸出に許可が必要な「エンドユーザー」や「エンドユース」を指定
- 輸出先国（特に、中国、ロシア、イランなど）や利用目的に応じて、制限を厳格化

iv. 輸出規制（Export Control）３ ： Office of Foreign Assets Control（OFAC）

（対象及び特徴）

- 米国財務省が運用
- **特定の国や団体に対する経済制裁プログラムを管理**：経済制裁対象国（例：北朝鮮、イラン、ロシア、中国の一部組織）、テロ組織や武器拡散に関与する団体
- 場合によっては、取引や技術移転を全面禁止
- 特定の国との共同研究や技術移転には、厳しい制限

v. 輸出規制（Export Control）４ ： Deemed Export（みなし輸出）

（対象及び特徴）

- 米国国内で外国人が技術やデータにアクセスする場合も輸出と見なす規制
- **対象**：EAR または ITAR に準拠する技術、米国内の研究施設や企業で働く外国人研究者や留学生
- 技術や情報を国外に移転しなくても、規制の対象
- 特定の国籍（例: 中国、ロシア、北朝鮮、イラン）の研究者が対象の場合、事前に許可が必要

d. 各論Ⅲ（Critical & Emerging Technology 関係）

Critical & Emerging Technology については、外国政府による研究の影響力の排除の徹底と、基礎研究と国家安全保障のバランスの維持を図るため、NSPM-33（国家安全保障大統領覚書第 33 号）に基づき、連邦資金を受ける研究機関に、セキュリティと透明性の向上を義務付けている。

i. NSPM-33（国家安全保障大統領覚書第 33 号）

（主な要件）

- **利益相反の開示** ： 外国政府や機関からの財政支援や契約の報告
- **セキュリティトレーニング**
- **サイバーセキュリティ対策**

e. Science and Technology Risk Matrix （S&T リスクマトリックス）

S&T リスクマトリックスは、米国エネルギー省（DOE）が策定したツールで、国家安全保障や経済競争力に影響を及ぼす可能性のある新興技術分野を評価・管理する目的で使用される。このマトリックスは、特定の技術や研究分野が国家にとってどれだけのリスクを持つかを可視化し、リスク管理と意思決定の指針として機能している。上記の全ての規制は、リスクマトリックスによる評価と連動し、特に対象技術が重要分野に該当する場合、輸出や情報共有を制限する可能性がある。

（目的）

- **リスク評価と管理**：国家安全保障に及ぼすリスクを定量的・定性的に評価、リスクに応じた制限措置や管理方針
- **基礎研究と機密研究のバランス**
- **懸念国との共同研究の管理**：中国、ロシア、北朝鮮、イランなどの懸念国に関連するプロジェクトを監視、不適切な技術移転を防止

（マトリックスの構造）

3 つのカテゴリー、すなわち、**グリーン（Green）**（リスクが低く、国際的な共有や基礎研究が自由に行える分野）、**イエロー（Yellow）**（中程度のリスクがあり、追加の管理措置が必要な分野）、**レッド（Red）**（高リスク分野であり、厳格な制限と管理が必要）からなる。

（対象）

- **量子情報科学（Quantum Information Science & Technology）**：量子コンピューティング、量子通信、量子センシング、高度な暗号技術
- **高性能計算（High Performance Computing）**：スーパーコンピュータ、計算シミュレーション、防衛や気候予測、医薬品開発
- **人工知能（AI）**：機械学習、自然言語処理、画像認識技術、データ解析や軍事用途、監視システム
- **バイオテクノロジー（Bioscience & Biotechnology）**：遺伝子工学、合成生物学、バイオ医薬品、疫病対策やバイオマテリアルの開発
- **バッテリー科学（Battery Science & Technology）**：次世代エネルギー貯蔵技術（リチウムイオン電池、全固体電池）、再生可能エネルギーや電動車両
- **加速器科学（Accelerator Science & Technology）**：粒子加速器、次世代放射光技術、医療、材料科学、防衛技術

f. その他の関連規制

i. Economic Espionage Act（EEA）

1996 年に制定され、特に、国家支援による経済スパイ行為に焦点を当て、企業秘密を盗む行為を連邦犯罪として扱い、厳しい刑罰を規定アクセス制御を行う。

ii. Defend Trade Secrets Act （DTSA）

2016 年制定であり、企業秘密を保護し、不正な持ち出しや使用に対して民事訴訟を可能にするものである。国内外の企業や個人による不正使用に対して、米国内での救済を提供する。

iii. Cybersecurity Maturity Model Certification（CMMC）

防衛産業を中心に、サイバーセキュリティの基準の義務付けを行う。連邦政府との契約に基づく情報管理の強化を目的としている。

iv. Committee on Foreign Investment in the United States （CFIUS）

米国企業への外国投資を審査するものであり、国家安全保障にリスクをもたらす場合は取引をブロックすることができる。米国企業の重要技術が外国に渡るリスクを事前に審査することとなる。

②欧州の研究開発セキュリティ・クリアランス制度

A) 総論

欧州の研究開発セキュリティ・クリアランス制度は、国家および地域の安全保障を確保しつつ、国際的な科学技術連携と経済成長を支える枠組みである。2013 年の欧州理事会決定（Decision 2013/488/EU）をもとに、EU Classified Information（EUCI）の統一的管理基準を制定した。これにより、加盟国間での機密情報共有が可能となるとともに、各国の独自基準を尊重する柔軟性も許容している。

同制度は、情報漏洩や技術流出を防ぐだけでなく、研究機関と企業が国際的な競争力を維持し、信頼性を高めるための基盤を提供する。国際共同研究の推進においては、日本を含むパートナー国との協調を可能にするものでもある。

EU は、セキュリティ・クリアランスの中核として、以下を運用している。

①人的クリアランス（Personnel Clearance, PCL）：

機密情報にアクセスする個人の信頼性を評価する制度。特に Top Secret や Secret レベルの情報には厳格な審査基準を適用。個人データ保護についての規定も存在。

②施設クリアランス（Facility Clearance, FCL）

機密情報を取り扱う施設の適格性を認証する制度。また、セキュリティ措置/上記の分類とクリアランスを支える措置として、セキュリティ措置を含む。

なお、欧州の輸出規制は、特にデュアルユース技術に重点を置いており、「Regulation (EU) 2021/821」に基づいて運用される。

（表 1-2-3）

国家機密（Classified Information）	Top Secret（機密）	不正開示された場合、EU または加盟国の利益に例外的かつ深刻な損害を与える情報	（例）核関連技術、軍事用途技術、外交情報
	Secret（極秘）	不正開示された場合、深刻な損害を与える情報	
	Confidential	不正開示された場合、損害を与える情報	
戦略的重要性を持つ情報（Restricted）		不正開示された場合、不利益をもたらす可能性がある情報【1】。研究データや技術移転関連情報などが含まれる。これらは NIST SP 800-171 に基づく米国の管理基準と類	（例）研究データ、輸出規制対象技術、技術移転関連情報

	似した厳格なセキュリティ措置が求められる【4, 9】。	

B) 各論Ⅰ（国家機密関係）

欧州における国家機密の管理は、厳格な情報分類とセキュリティ・クリアランス制度を基盤とし、人的クリアランス（Personnel Clearance, PCL）と施設クリアランス（Facility Clearance, FCL）がその中核を成す。また、これらを支える多層的なセキュリティ措置を実施している。

i) 人的クリアランス（Personnel Clearance, PCL）

PCL は、EU Classified Information（EUCI）へのアクセスを許可する個人の適格性を評価する制度である。

（主な要件）

- **忠誠心**： EU または加盟国に対する忠誠心がある
- **犯罪歴**：過去の犯罪行為や懲戒処分の履歴がない
- **財務状況**：借金や破産歴がなく、経済的な脆弱性がない
- **外国との関係**：外国籍の配偶者や外国団体との接触が安全保障上のリスクとならない
- **その他**：テロ活動やスパイ行為への関与がないこと。

（手続き）

申請者は国家安全保障機関に詳細な質問票を提出

（審査）

- 犯罪歴、財務状況、外国との接触状況を含む包括的な調査の実施
- 必要に応じて面談
- 調査プロセスは「Whole Person」コンセプトに基づき、個人の全体的な信頼性を評価

（発行）

- 国家安全保障機関が適格性を認定。認定は通常 5～10 年間有効
- 更新時には再審査が必要
- 背景調査は繰り返し実施

ii) 施設クリアランス（Facility Clearance, FCL）

FCL は、施設が EUCI を適切に保護する能力を有していることを認証する制度である。物理的、人的、サイバーセキュリティの側面で高い基準を満たすことが求められる。

（要件）

- **物理的セキュリティ**：監視カメラ、入退室管理システム、防弾ガラス、セキュアエリアの設定
- **情報管理**：機密情報の暗号化、アクセス制御、保管方法の適正化
- **人的セキュリティ**：人的クリアランス（PCL）の取得

（手続き）

対象施設が FCL 取得の必要性を証明し、申請者は国家安全保障機関に申請書を提出

（審査）

施設の物理的構造、情報管理体制、従業員の適格性に基づく評価

（発行）

基準を満たすと判断されれば FCL を付与。認定後も定期的な監査と再評価が必要

iii) セキュリティ措置

PCL および FCL を支える多層的なセキュリティ措置がある。アクセス制御（必要最小限のアクセス権限付与と認証プロセスの徹底）、監視システム（24 時間稼働の監視カメラ、侵入防止センサーの設置）、サイバーセキュリティ（ネットワーク隔離、暗号化通信、監査ログの保持）が柱となっている。

C) 各論Ⅱ（Restricted、輸出規制関係）

欧州においては、Restricted 情報や輸出規制が、特に軍事転用可能なデュアルユース技術の管理の中心的役割を担い、国家安全保障および国際的な経済安定性を維持するための基盤を提供する。

i) Restricted 情報の管理

Restricted 情報は、保護が必要とされる情報の中で、最も低い機密レベルに該当するが、EU または加盟国の利益に不利益をもたらす可能性がある情報が含まれる。Restricted 情報の管理は、欧州理事会決定 2013/488/EU（Council Decision 2013/488/EU）に基づく。

（Restricted 情報保護のプロトコル）

- 必要最小限のアクセス制限を設け、関係者のみが情報にアクセス可能
- 情報の適切な取り扱いについて従業員に教育を実施
- サイバーセキュリティ対策として、暗号化やアクセスログの監視を適用
- 施設クリアランス（FCL）が求められない場合が多いが、アクセス制御や情報廃棄に関する標準的なセキュリティ手続きが適用
- 加盟国内での取り扱い基準は国家ごとに若干異なる場合があるが、統一的な EUCI 保護基準を適用

ii) 輸出規制

「Regulation (EU) 2021/821」が基本となる。国際的な平和と安全を維持し、技術や製品の不正利用を防ぐことを目的とする。

（主な要件）

- 「デュアルユース品目リスト（Annex I）」に、規制対象となるユース品目を詳細に記載。AI 技術、量子通信、先端材料科学などが含まれる
- リストに記載されていない品目でも、不正使用のリスクがある場合には許可が必要（キャッチオール規制）
- 輸出者は、エンドユーザーおよびエンドユースの適格性を評価し、リスクを管理するためのプログラムを実施（内部コンプライアンスプログラム（ICP））

（手続き）

- **自己評価**：輸出対象がデュアルユースリストに該当するかを確認。
- **許可申請**：特定の国やエンドユーザーへの輸出には、許可を取得する必要。
- **監査と報告**：輸出取引の記録を保持し、監査に応じる義務。

（デュアルユース技術の具体例）

- **AI 技術**：監視システムや自律型兵器への転用可能性
- **量子通信技術**：暗号通信の軍事用途
- **先端材料科学**：軽量防弾素材や耐熱性材料な。

D) 各論Ⅲ（Critical & Emerging Technology 関係）

欧州における重要かつ新興技術（Critical & Emerging Technologies: CET）の管理は、「Regulation (EU) 2021/821」、および、「欧州理事会決定 2013/488/EU（Council Decision 2013/488/EU）」を基礎に運用されている。

これらの規制は、輸出管理、技術共有、研究開発におけるセキュリティ措置を包括的に規定する。リスク評価と保護措置を実施する枠組みを提供している。また、管理は、EU Classified Information（EUCI: European Union Classified Information）に基づく。

i) 対象技術分野

- **量子情報科学（Quantum Information Science）**
  量子通信、量子暗号技術、量子コンピューティング（情報セキュリティと国家安全保障に直結）
- **人工知能（Artificial Intelligence）**
  機械学習、自然言語処理、画像認識（軍事監視システムや自律型兵器への転用可能性）
- **バイオテクノロジー（Biotechnology）**
  遺伝子工学、合成生物学、バイオ医薬品（疫病対策やバイオマテリアルの開発に応用。）
- **先端材料科学（Advanced Material Science）**
  軽量防弾素材、高温耐性材料、エネルギー貯蔵材料（航空宇宙やエネルギー分野での応用）

ii) 規制の枠組み

（主な要件）

- デュアルユース技術として、「Regulation (EU) 2021/821」の附属書 I にリストアップされている場合、輸出許可が必要
- サイバーセキュリティ基準に基づく厳密な情報管理が必須

E) EEAS （European External Action Service）

欧州には、米国の「科学技術リスクマトリックス」のような具体的なマトリックス構造は存在しないが、2023 年 6 月に発表した「欧州経済安全保障戦略」に基づき、以下の４つのカテゴリーを特定している。これに基づき、それぞれに対する評価と対応を強化することを目指す。

- サプライチェーンの強靭性（エネルギー安全保障を含む）
- 重要インフラストラクチャの物理的およびサイバーセキュリティ
- 技術のセキュリティと技術流出
- 経済的依存関係の兵器化と経済的強制

この戦略に基づき策定された勧告である、EEAS （European External Action Service）では、上記の 4 つのリスクのうち、「技術リスクと技術流出」に焦点を当てており、また、「重要エンティティ回復力指令（CER）」では、重要インフラストラクチャの強靭性確保を

目指す。CER 指令が定める 10 の重要技術分野は、先端半導体、人工知能（AI）、量子技術、バイオテクノロジー、高度な接続性・ナビゲーション・デジタル技術、高度なセンシング技術、宇宙および推進技術、エネルギー技術、ロボット工学および自律システム、先端材料製造・リサイクル技術となっている。

また、2023 年 10 月 3 日、欧州委員会は、特に機密性が高く、差し迫ったリスクをもたらす可能性が高い 4 つの技術分野（先端半導体、人工知能（AI）、量子技術、バイオテクノロジー）を特定した。

F) その他の関連規制

EU Cyber Security Act (Regulation (EU) 2019/881)：

EU Cyber Security Act は、加盟国間でのサイバーセキュリティ協力やサイバー製品の認証枠組みの整備や EU サイバーセキュリティ機関（ENISA）の強化などを目的としており、EU 内での情報共有と統一的なサイバーセキュリティ対策を推進するものである。主に以下について言及されている。

- サイバーセキュリティ認証スキーム: さまざまな製品、サービス、プロセスに対して、異なるレベルのサイバーセキュリティ認証スキーム。
- 自己適合宣言と第三者認証: 製品やサービスの製造者は、自己適合宣言を行うか、第三者機関による認証を受けることができる仕組み。
- ENISA の役割:サイバーセキュリティ認証スキームの開発や維持、加盟国へのアドバイス、情報共有など。
- 市場監視:、サイバーセキュリティ認証を受けた製品やサービスが市場に出回る際に、加盟国は適切な市場監視を行うことについて。

European Cybersecurity Strategy：

欧州委員会が策定した戦略であり、サイバー脅威に対する共同対応の枠組みを整備するための指針となるものである。EU 加盟国間の情報共有、連携強化、共同防衛体制の構築に向けた包括的な方針を示している。具体的には以下について言及されている。

- サイバーレジリエンスの強化: EU の重要インフラ、公共機関、企業、そして市民のサイバーレジリエンスを強化し、サイバー攻撃に対する防御力と回復力を高めることについて。
- サイバー脅威の抑制: サイバー犯罪の取り締まり、国際協力の強化、サイバーセキュリティ能力の向上を通じて、サイバー脅威を抑制することについて。
- EU のサイバーセキュリティ産業の育成: 革新的なサイバーセキュリティソリューションの開発と展開を促進し、EU のサイバーセキュリティ産業を育成することについて。

- グローバルなサイバー空間における EU の役割強化: 国際的なサイバーセキュリティ規範の策定と、パートナーシップの構築、能力開発支援を通じて、グローバルなサイバー空間における EU の役割を強化することについて。

④ 英国の研究開発セキュリティ・クリアランス制度

A) 総論

英国のセキュリティ・クリアランスは、政府による機密情報や資産へのアクセス管理、および、国家安全保障上のリスク軽減のための制度であり、EU とは独自の制度となっている。

従来、英国政府は、情報および ICT システムを評価するために、2014 年 4 月に、政府セキュリティ分類ポリシーに基づき、3 つのセキュリティ分類レベル（OFFICIAL、SECRET、および TOP SECRET）を設定していたが、2018 年、これら 3 つのレベルに加え、政府セキュリティ分類（GSC）に、「Official-Sensitive」の概念を導入した（（表 1-2-4）参照）。これは、より機密性の高い情報に適用されるものとなっている。

また、機密性の高い情報については、以下の詳細分類も併用している。

- **PERSONAL**：不適切なアクセスにより、損害が生じる可能性のある、個人またはグループに関する機密性の高い情報。
- **COMMERCIAL**：不適切なアクセスにより、BIS または商業パートナーに損害を与える可能性のある、商業的または市場で機密性の高いデータ。
- **LOCALLY SENSITIVE**（or LOCSEN）：海外で現地採用された職員がアクセスできない機密性の高い情報の流通の制限。

さらに、情報へのアクセス権を付与するセキュリティ・クリアランスは、（表 1-2-5）のカテゴリーに分類されている。セキュリティ・クリアランスのレベルと情報レベルには対応関係ある。

なお、セキュリティ・クリアランスは、雇用期間や特定のプロジェクトに応じて一定期間有効となっている。

（表 1-2-4）

情報レベル	**定義**	**不適切なアクセスによる影響例**
TOP SECRET	最も機密性の高い情報。不適切なアクセスは、国家安全保障に壊滅的な損害を与える可能性。	国家機密の漏洩、諜報活動の妨害、軍事作戦の失敗
SECRET	非常に機密性の高い情報。高度な脅威に対する防御のために、強化された保護対策が必要。	国家安全保障の脅威、外交関係の悪化、経済的損失
OFFICIAL	公共部門で作成または処理される情報のうち、機密性が低いもの。特に、OFFICIAL-Sensitive は OFFICIAL の中でも比較的機密性の高い。	業務の混乱、評判の失墜、金銭的損失 個人情報漏洩、プライバシー侵害、差別

（表 1-2-5）

カテゴリ	情報レベル	説明
Baseline Personnel Security Standard（BPSS）	**OFFICIAL (一部)**	厳密にはセキュリティ・クリアランスではない。すべてのクリアランスレベルの基礎となる雇用前のスクリーニング。身元確認、英国での就労資格、雇用履歴、犯罪歴などの確認。
Accreditation Check（AC）	**OFFICIAL (一部)**	空港のセキュリティ制限区域への立ち入りを必要とする空港職員や航空会社の乗務員への適用。身元、雇用・教育履歴、犯罪歴などの確認。通常は、最長 5 年間、または、12 か月間有効。
Counter Terrorist Check （CTC）	**OFFICIAL-Sensitive (一部)**	テロの脅威にさらされる可能性のある情報や場所にアクセスする必要がある場合に必要。警察官や関連職員、政府機関職員、民間請負業者などが対象。基本は、10 年毎見直し。
Security Check（SC）	**SECRET (一部)**	機密情報へのアクセス、および監督下での極秘情報へのアクセスを必要とする場合に必要。3 年間の居住と Baseline Personnel Security Standard の取得の 2 段階。
Developed Vetting（DV）	**TOP SECRET (一部)**	極秘情報へのアクセス、およびより機密性の高い役割を担う場合に必要。政府機関や諜報機関、軍関係者などが対象。
その他		より強いレベルの、Enhanced Security Check（eSC）、Enhanced Developed Vetting （eDV）も存在。

（表 1-2-6）現行の OFFICIAL カテゴリーの旧カテゴリーとの対応

旧カテゴリ	現行カテゴリ	説明
CONFIDENTIAL	**OFFICIAL-Sensitive** もしくは **Secret**	明確な国家安全保障の側面がある場合、または保護された証人に関連する場合。
RESTRICTED	**OFFICIAL**	政策文書、商業文書、または事件記録など
PROTECT	**OFFICIAL**	事記録、市民または犯罪者事件記録、および一般行政などの個人データなど

UNCLASSIFIED	**OFFICIAL**	公開された情報・個人データ・その他の機密を含まない情報、トレーニング資料など

B) 各論Ⅰ（人的クリアランスと施設クリアランス）

英国では、個人の信頼性を評価する「人的クリアランス」と、施設のセキュリティレベルを評価する「施設クリアランス」の 2 つが存在する。

① 人的クリアランス（Personnel Security Clearance, PSC）

個人が機密情報や資産にアクセスするのに適格であるかどうかの判断プロセスであり、レベルが高くなるほど、調査はより詳細かつ広範囲に及ぶ。例えば、DV クリアランスでは、申請者の家族や友人への面接、財務状況の精査などを実施する。なお、5 年間の居住が前提となる。

（手続き）

- **スポンサーによる申請**：雇用主や請負業者など、スポンサーによる申請が必要
- **質問票の提出**：経歴や状況に関する詳細な情報を質問票に記入
- **身元調査**：身元、国籍、移民ステータス、雇用履歴、犯罪歴などの調査
- **信用調査**：信用情報の調査（より高いレベルのクリアランスで必要）
- **セキュリティサービスによる調査**：セキュリティサービスによる調査を受診（より高いレベルのクリアランスで必要）
- **面接**：調査官による面接

② 施設クリアランス（Facility Security Clearance, FSC）

- 施設が機密情報や資産を保護するための適切なセキュリティ対策を講じているかどうかの評価プロセス
- 機密情報や資産を扱う企業や組織に必要。国防省や主要な請負業者など、契約当局のスポンサーが必要
- 取得には、物理的セキュリティ、人的セキュリティ、サイバーセキュリティなど、さまざまなセキュリティ対策を講じる必要

③ 人的クリアランスと施設クリアランスの関係

人的クリアランスと施設クリアランスは相互依存関係となっている。例えば、施設が FSC を取得していても、そこで働く個人が適切なレベルの人的クリアランスを取得していなければ、機密情報や資産へのアクセスは不可能である。

C) 各論Ⅱ（輸出規制関係）

武器や軍事技術、デュアルユース品などの輸出、仲介、技術支援、通過、移転を制限する規制である。輸出管理法 2002、輸出管理令 2008、EU 理事会規則（EC）第 428/2009 号（北アイルランドでは、Brexit 後も特例的に、2021 年 5 月 20 日の欧州議会および理事会の規則（EU）2021/821）に基づいている。

輸出規制の対象となる物品や技術を輸出または移転する場合、輸出管理共同ユニット（ECJU）から輸出許可を取得する必要がある。また、外国との機密文書のやり取りについては、分類レベルと関連する条約を含む、特定のマーク要件（例えば、米国製の機密文書の場合、「CONFIDENTIAL USML/REL USA and GBR Treaty Community」のようにマーク）が必要となる。

さらに、軍事転用可能な技術や情報を含む研究開発プロジェクトでは、輸出規制の遵守が不可欠となっている。

（対象）

- 軍事用途に特化して設計または改造された軍需品、ソフトウェア、技術、および民生用と軍事用の両方に使用できるデュアルユース品。（具体的な規制内容は、戦略的輸出管理リスト）。
- 具体的には、核物質、特殊材料、材料加工、電子機器、コンピュータ、通信・情報セキュリティ、センサー・レーザー、航法・航空電子工学、海洋、航空宇宙・推進力などの物品や技術など。

（手続き）

- **輸出許可の申請**：ECJU に輸出許可を申請。申請には、輸出者、輸入者、最終需要者、輸出または移転の目的、物品や技術の詳細などの情報が必要。
- **審査**：ECJU の審査では、輸出規制の目的、国際的な義務、英国の安全保障などの要素を考慮。
- **輸出許可の取得**：輸出許可には、有効期限、輸出または移転できる数量、条件などが記載。

D) 各論Ⅲ（Critical & Emerging Technology 関係）

政府は、2023 年 2 月、科学技術イノベーション省（DSIT）を新設し、技術革新による機会と課題への対応を強化した。この際、以下の 5 つの技術分野を重点分野として特定した。また、サイバーセキュリティに関する包括的なガイドラインや文書も公開している。

技術分野	説明	主な取り組み
人工知能 (AI)	人間のように思考・学習するコンピュータシステムの開発	国家 AI 戦略、英国防衛 AI 戦略

技術分野	説明	主な取り組み
量子技術	量子力学の原理を利用した、従来の技術では不可能な処理能力を持つ技術	国家量子戦略、量子技術研究開発への投資
半導体	電子機器の基幹部品	国家半導体戦略、半導体産業への投資
通信	情報伝達技術	ワイヤレスインフラストラクチャ戦略、6G 研究開発
エンジニアリングバイオロジー	生物学的なシステムやプロセスを工学的に応用する技術	エンジニアリングバイオロジー戦略、バイオテクノロジー産業への投資

第二章　日本の研究開発機関が直面する課題

本章では、世界での研究開発セキュリティの動向と研究開発現場における現状を踏まえ、潜在的なリスクと、それに対する対応の必要性を列挙する。

NanoTerasu を念頭に置いていることから、本施設の目指す、「最先端研究」、「研究力強化」、「産学共創」という３つの課題領域に分けて検討する。さらに、「産学共創」の領域では、知的財産の保護、秘密特許の活用、そして、スタートアップ企業との連携におけるセキュリティに関する留意点など、特有の課題を列挙した。

本章で提示する課題は、現状の制度や取り組みにおける改善の余地を示すものであり、過度に悲観的な状況を強調するものではない。しかしながら、これらの課題を放置すれば、日本の研究開発活動が本来持つ潜在能力を十分に発揮できず、国際的な競争力を損なう可能性が高まる。

従って、ここに挙げられた課題に対して、具体的な対策を講じることの重要性を改めて確認したい。

（１）最先端施設における課題

放射光のような大型研究施設は、日本の最先端の研究を牽引している。当該施設では、成果公開とその成果のデータベース化（例：タンパク質構造解析データベース）といったオープンサイエンスを前提してきた。たとえ企業が競争力維持のために秘匿性を求めるような研究データであっても、従来の共用制度では公開が前提となっていた。

このような中、産学がコアな課題に取り組む際に、オープンサイエンスの原則がブレーキとなる事例が生じてきている。協調領域と競争領域の切り分け、両領域の健全な関係性の構築に向け、NanoTerasu では、ニーズ起点で課題解決を行うスキーム、コアリション制度を導入することとした。これは、共用利用とは別に、産学が共同で研究を行うための成果専有と非公開のデータ利用を可能にする枠組みである。

今後、NanoTerasu では、国家安全保障に関わる研究や、特に機密性の高い技術開発などへの対応のために、「ディープテック・コアリション」のような考え方も不可欠となると考えられる。その際、以下のような点について、検討が避けられない。

- 世界のニーズ課題に対応できるセキュリティ・クリアランスの基準
- 情報管理体制
- セキュリティに関する教育や研修

（２） 研究力強化における課題

国際共同研究の推進や研究インフラの共用化を推進するためには、「ファシリティの先端性維持」と「コアな課題にチャレンジできる産学共創スキーム」の２つの課題の克服が必要となる。

他方で、研究施設の維持・発展には、多大な費用が必要となる。従来の共用利用の方式である、

運営費回収のための料金設定では、最先端の施設・設備の維持や高度な人材の確保が困難である。ファシリティの先端性を維持するためには、減価償却費や人件費などを考慮した、民間的な経営センスに基づいた料金設定が必要となる（NanoTerasu では、Coalition スキームは、償却費や人件費などを考慮した民間的な料金設定を採用している）。

研究力強化には、産学が連携してコアな課題にチャレンジできる仕組みが必要である。これまでも、大野英男氏（h-index = 100, Scopus 調べ）、細野秀雄氏（h-index = 135, Scopus 調べ）、橋本和仁氏（h-index = 132, Scopus 調べ）らは、スピントロニクス、デバイス、触媒などの企業の抱えるコアな課題に取り組むことで、高い成果創出と学術的評価を獲得してきた。

これらにより、次世代の研究者の育成と、産学共創エコシステムが進化したのも事実であり、今後は、さらに、日本の研究力の大幅な向上が期待されている。

（３） 産学共創における課題

① 知的財産の保護

産学共同研究の成果については、迅速かつ的確な知的財産の出願と保護が不可欠である。他方で、国際競争の激化や技術の高度化に伴い、企業秘密を含むコアな課題に産学が連携して取り組む必要性が急速に向上している。

NanoTerasu でも、コアリション制度の下での産学共創の機微な研究開発への希望が寄せられているが、迅速な意思決定を如何に実現するか、長期的な連携が維持可能か、秘密保持は大丈夫か、オープンサイエンスとの両立は可能なのか、といった点に関する懸念も顕在化してきている。

日本では、経済安全保障推進法に基づく「特許出願非公開制度」が導入されたところであり、国家安全保障に関わる技術の漏洩を防ぐ手段として期待も高まっている。

② スタートアップ企業との連携、M&A への留意

イノベーションの重要なプレイヤーとして、スタートアップ企業が期待されており、先端研究施設においても積極的に共同研究を進めることが必要となってきた。他方で、スタートアップの出口として、IPO や M&A が想定されている場合、**技術流出リスク**（海外ファンドによる M&A に伴い、スタートアップ企業が保有する技術や人材が海外に流出するリスク）、**成長阻害リスク**（M&A 後、スタートアップ企業の autonomy や agility が失われ、成長が阻害されるリスク）といったリスクにも予め留意しておくことが不可欠になっている。

リスク軽減には、秘密保持契約の締結、知的財産権の明確化、デューデリジェンスの徹底など、適切な対策を講じる必要がある。

第三章 産学共創におけるセキュリティ・クリアランスの必要性

（１） 大型研究施設と研究開発セキュリティ・クリアランス

NanoTerasu のような、世界的に注目されている大型研究施設は、先端技術の研究開発や国際的な学術交流の核となる存在とならなければならない。そこで、NanoTerasu では、世界に稀に見る独自の制度（コアリション制度）の下、100 を超える企業・大学・研究機関が参画し、世界的に見ても前例のない規模で、産学官連携による研究開発を行っている。そのコアリション制度の下では、全ての利用が、成果専有を前提としており、事前審査や事後の成果公開を求められることがない。また、コアリションメンバー企業は、解決したい課題に応じて適切な学術研究者の紹介を依頼することができる。依頼を受けた一般財団法人 光科学イノベーションセンター（以下、「財団法人」）は、メンバー学術機関の提出した人財リストの中から候補者を選び、秘密保持契約の下で企業と学術研究者のマッチングを行うことになっている（コアリション・マッチング）。

特に産業界の参画メンバーは、企業秘密や知的財産の保護のため、データの非公開を希望する場合がある一方で、国際的な研究拠点においては、海外からのアクセスも多く、技術流出やサイバー攻撃などのリスクへの対策は必須の課題となっている。

国際連携に対応しつつ機密レベルに該当する経済安全保障に関連する可能性がある情報を守るための解決方法が、国内外から信頼される、研究開発セキュリティ・クリアランスのレベル確保であると考えられる。

（２） プラットフォームとしての NanoTerasu の新たな挑戦

NanoTerasu は、産官学が出資した財団法人が、その建屋を所有し、自ら専用のビームラインを整備・保有している。従って、施設やオペレーションについて、自ら所有する部分については、財団法人自身のマネージメントが可能である。

我が国の大学における産学連携研究開発の歴史やその環境の特異性を踏まえれば、大型実験施設として関係機関が共存し、コストの適正な分担を行いつつも、専有部分についてはマネージメント可能であるという、NanoTerasu のコアリション制度のメリットを最大限に活用すべきである。

NanoTerasu としては、まずは米国の基準を満たすことを念頭に、政府を含めたステイクホルダーの英知を結集し、NISPOM、NIST SP 800-171、DISM などを参考にしつつ、（３）の条件を満たすような、新たなマネージメント・オペレーションの仕組みと、それを支えるハード・ソフトをできるだけ迅速に構築する必要がある。なお、財団法人の構成員が、セキュリティ・クリアランスが必要となる研究開発を行う場合には、財団法人との契約の中で、クリアランスに係る各種手続きの必要性について、明確に決めておく必要がある。

さらに、NanoTerasu からのデータの有効活用と、企業が自ら保有するデータやノウハウを組み合わせたデータ解析を安全・確実に行うためには、特に、情報の収集、移送、蓄積、処理について、最高水準の安全性を確保することが求められる。データの移送を極力無くし、仮に、移送する場合

には量子暗号を用いるといった最も安全な手段を選択し、そして、できるだけ高度なデータ処理を現場にて行うことが求められる。NenoTerasu では、こういった活動ができ、セキュリティ・クリアランスにも対応したデータセンターを一刻も早く整備しなければならない。

知的財産の保護についても、国際特許を取得せず、国内特許のみで、第 3 国へ知的財産が流出することのないような仕組みも必要である。TS にあたる最高機密の知的財産については、昨今、特許申請をしないでカプセル化することにより知的財産を保護する方法もとられている。NanoTerasu を活用した場合、その知的財産をカプセル化した事実を記録し、企業・学術がカプセル化した知的財産の保有権利を強化する新しい仕組みの検討も急がなければならない。

（３） 産学共創の場における、セキュリティ・クリアランスの 4 つの柱

国のセキュリティ・クリアランス制度は施設及び人的クリアランスが二つの柱となっているが、産学共創の場であるナノテラスにおいては、これらに加え情報セキュリティと、マネージメントが重要であると考えられる。

① 施設クリアランス（FCL）

施設全体として機密情報を適切に管理する能力を認証するためのものであり、該当区域を他の区域から完全に独立させ、

- 物理的セキュリティ（施設への侵入防止、設備の保護、盗難・紛失・破壊・漏えい防止などの適切な措置）
- アクセス管理（入退室管理、情報アクセス制限などの適切な措置）
- 物理的な情報盗難の防止（無窓、無線通信の防止など）

を徹底することが求められる。このため、クリアランスが必要となる区域を共同利用スペース・設備から完全に分離し、管理することが求められる。

② 人的クリアランス（PCL）

人的クリアランスの付与にあたっては、政府が機密情報等にアクセスする個人の信頼性を評価することから、研究機関等としては、所属する研究者等が日頃から情報を適切に管理し、研究インテグリティ・セキュリティの確保に取り組めるよう、適切な環境を整備する必要がある。

③ 情報セキュリティ（サイバーセキュリティ）

実験・計測現場、および、データが存在する区域については、米国 NIST や国防総省のガイドラインも参考に、物理的攻撃、サイバー攻撃等のリスクを適正に評価し、リスク管理を徹底することにより、適切なセキュリティ対策を行うことが求められる。特に、アクセス制御（情報へのアクセスを必要最低限の者に制限）、ネットワーク・セキュリティ（外部からの不正アクセスを防ぐための適切な措置）、マルウェア対策などについては、最大限の注意が必要であり、システムログの収集・分

析や異常検知を行うとともに、頑強な建屋・施設、厳重な侵入管理と合わせて進めることが求められる。

また、ネットワークについては、インターロック／安全停止信号等のやむを得ない例外を除き、一般のネットワークとの完全な分離を行う必要がある。仮に、異なる地点に関係する機材が存在する場合には、それらを結ぶネットワークは専用線とし、さらに、その間の通信は FIPS 140-2 認証等を受けた暗号化アルゴリズムを導入しなければならない。

加えて、インシデントや災害に対する準備も周到に行う必要もあり、脆弱性評価、侵入テストといったシステム面から、定期的な訓練といった実践面での対応も必要である。さらに、関連施設に勤務する職員の人的セキュリティ・クリアランスと職員教育も忘れてはならない。

④ マネージメント・オペレーション

施設管理、人材マネージメント、情報システムのオペレーション等の全てを一体的に管理・運営する、マネージメント・オペレーション組織の確立・構築は急務である。加えて、監査体制の構築と定期的な監査の実施、総合的な訓練の実施、常時／移籍時の教育は必須である。

また、通常の運用時だけではなく、建設段階やメンテナンス時などについても、外部の作業員等が危険の原因となることのないよう、人的セキュリティ・クリアランスや厳重なアクセス管理を行う必要がある。さらに、仮に、システムの運用中に何らかの作業を行う場合には、そのシステムから完全に隔離された作業環境、システム環境で行い、導入や接続時には、十分なテスト及びセキュリティ検証を行う必要がある。

加えて、リスク低減と異常発見時の早急な対応を可能とするため、全工程のリアルタイム記録を収集・保存し、監査・分析を行うとともに、システム停止前のソフトやデータのフル・コピーを実施・保存し、速やかな構成復元が確実に実施できる環境を整えなければならない。

第四章　国際連携に向けた欧米との相互性・互換性の確保

国際的な産学連携や国際共同研究を安心して進めるためには、研究者が不用意に制度的制約に陥ることのないようにすることが最低限の条件となる。その基本となるのは、日本と欧米の関連する制度のコンパチビリティ（相互性・互換性）を確保することである。

（１） 直面する課題

国際的プロジェクトを実施する場合、異なる地域の規制やセキュリティ基準（米国の NIST SP 800-171 や欧州の GDPR など）に対応しなければならない局面が多数存在する。特に、様々な情報や技術が、機密情報に該当するのかを地域毎に正確に認識し、適切な管理を行うことが必要となる。

しかしながら、個々の地域でそれぞれ対応することは極めて煩雑であることも事実である。例えば、海外の研究機関を相互に訪問した場合、入構基準に相違があると問題が発生することなどが想定される。

一方で、日本のセキュリティ・クリアランス制度については、制度が導入されたばかりであり、細部の基準の設定は今後の作業となっており、現在、運用を行っている各国の機関との連携も重要と考えられる。

（２） 対応の方向性

研究機関の立場から見れば、セキュリティ・クリアランス制度の運用ルールや評価基準が公開されることは、制度の理解を促進する。特に、データの機密性に応じた分類基準が明確化・透明化されれば、容易に国際比較が可能となるものと考えられる。

他方で、米国と欧州では、Top Secret、Secret、Classified/Confidential/Official-sensitive、CUI/ Official/Restricted などの体系としては類似の部分も多いが、細部になると、リスクマトリックスなど、異なる部分も生じている。

我が国としては、最も連携関係の強い米国を参照して対応の方向性を検討することが求められる。まずは、各国の制度を尊重しつつ、機能的同等性を確保することが望ましい。

（３） 放射光施設等の先端研究開発インフラにおける国際連携に向けた欧米との相互性・互換性の確保

現在のところ、日本も含めた各国の放射光施設は主に公的機関の配下にあり、個々の国や地域に閉じた存在となっている。国際的な拠点としての機能を十分に発揮する、真の国際研究拠点になるためには、世界中の研究者や企業が連携できるプラットフォームへの進化が期待される。

一方、NanoTerasu は、その計画段階から、国際放射光サミットなどを通じて、世界中の放射光施設とのネットワークを構築してきており、世界ニーズ・課題を日本が主体的発掘する視点・発

想を持つ場としての位置づけを確立しつつある。

このような中、NanoTerasu における先進的な研究開発の実施の要望が関係各方面から急速に高まっている。今後、国家の安全保障にも係る TOP シークレットレベルの技術に関与する可能性も十分にあり、機密情報を取り扱う能力が、かつてないほど重要となっている。

NanoTerasu から見れば、各国のセキュリティ・クリアランス制度の相互性・互換性が確保できれば、さらに円滑な国際連携と研究開発を促進することが可能と考えられ、真の国際連携プラットフォームの形成に向けて、以下の 3 つの課題について政府等の関係機関が対応していくべきである（詳細は第五章）。

- セキュリティ基準の相違の除去
- 機密情報の定義の統一化
- アクセス基準の共通化（施設への物理的アクセス、データや知的財産へのアクセスなど）

（4） NanoTerasu の現在および今後の取り組み

政府等の関係機関の対応をただ待つのではなく、NanoTerasu では、まずは、国内の基準及び米国の各種基準に準拠すべく、以下の対応を早急に進めなければならない。その上で、必要に応じて、欧州の基準への対応を図る。

- **関係国の基準への準拠** ： セキュリティ基準やデータ管理に関する基準に準拠
- **情報交換** ： セキュリティ・クリアランス制度の運用ルールや評価基準に関する、関係国（同志国）との情報交換。
- **PCL への対応** ： TOP シークレット、CUI も念頭におきつつ、研究者、施設職員、そしてユーザーの PCL 取得に向けた体制作りと教育
- **国際放射光サミットの活用** ： サミットの場を通じた、日本のセキュリティ・クリアランス体制の有効性と国際的なコンパチビリティの確認

第五章　行政への要望

現行の制度下においても、NanoTerasu としては、国際共同研究、産学連携研究の新たなプラットフォームの先行事例となるために、自らできる限りの制度的対応を行っていくことが必要である。しかしながら、このような動きを後押しし、国内外で定着させ、加速させるために、本報告書では、敢えて、行政に対する要望を列記する。

（１）　国際的に協調できるコンパチビリティの確保、わかりやすい申請マニュアル等の作成

研究機関にとって最も必要であるのは、制度・ルールの明確化である。まずは、以下の点にも配慮しながら、分かりやすい申請マニュアルの作成を要望する。

- 専門用語を避けた、平易な言葉での記述。
- 図表や事例を効果的に活用した、視覚的な理解しやすさ。
- 手続きの流れの明確化。
- 申請手続きの簡素化。

また、申請や運用における評価基準の明確化も重要であり、特に、以下の情報が可能な範囲で公開されれば、研究機関としても対応がより容易になる。

- 情報セキュリティに関する基準
- 申請から承認までの処理期間

いずれにしても、行政と研究機関との間での継続的なコミュニケーションも必要であり、特に、設備クリアランスや情報セキュリティについては、技術の急速な進歩に応じた基準や対応方法のあり方に関する緊密な議論が不可欠であり、必要に応じて、制度や運用の見直しが求められる。

そして、関連する制度のコンパチビリティ（相互性・互換性）の確保に向けた同志国の政府間での話し合いを期待する。

（２）　研究開発に係るパーソナル・クリアランスの基準の明確化と欧米との互換性・相互性の確保

パーソナル・クリアランスについては、最終的には、欧米との互換性・相互性が確保されることが望ましい。また、身元調査や経歴審査の範囲、クリアランスのレベル設定、クリアランスの有効期間、相互認証の枠組みなどに配慮した制度設計を期待する。

（３）　大型研究開発設備のファシリティ・クリアランスの基準の明確化と欧米との互換性・相互性の確保

ファシリティ・クリアランスについては、国際的な互換性の担保を念頭に、物理的セキュリティ対策（施設への侵入防止、設備の保護など）、アクセス管理（入退室管理、情報アクセス制限など）、情報セキュリティ対策（ネットワーク・セキュリティ、データ暗号化など）などの基準の明確化が必要である。

（４） 情報セキュリティに係る基準の明確化と欧米との互換性・相互性の確保

政府には、データの機密性に応じた分類基準、データの取り扱いに関するルール、サイバーセキュリティ対策、情報漏洩発生時の対応 procedures などについて、まずは米国との互換性・相互性を確保し、続いて、欧州との整合、そして、最終的には同志国間での統一的なルール作りを期待する。

（５） 初期の事例に対する、指導・助言の充実

制度の円滑な導入を促進するためには、申請を行う者に対して、申請手続きに関する個別相談、セキュリティ対策に関する技術的な助言、クリアランスを取得した施設を他の事業者が視察する際の助言などを行うとともに、関連情報の提供を充実させていく必要がある。

（６） パーソナル・クリアランスとファシリティ・クリアランスの両方を必要とする産学共創基盤における研究開発を行う場合の支援

最先端技術の研究開発では、個者の努力のみでは解決が困難な課題も多く、そこでは大型研究開発インフラの利用や産学共創が突破口となり得る。開発対象がセキュリティ・クリアランス確保を要する課題の場合には、それら産学共創の基盤となる研究開発インフラもまたセキュリティ・クリアランスに対応していることが必須となる。

セキュリティ・クリアランス制度は新たな制度であるため、まずは、プラットフォームとしての整備が不可欠と考えられる。

このためには、産学共創基盤の整備への補助金、他の事業者による施設の視察等に係る助言が重要となる。

その際、プラットフォームでのテーマとしては、欧米の制度運用も参考にしながら、経済安全保障に関連するものである必要がある。これまでの例としては、エアロスペース分野用途の先端炭素繊維強化プラスチック技術（高温耐性 CFRP、熱可塑性 CFRP、超音波溶着技術、リサイクル CFRP 等）、半導体材料・半導体製造装置技術の開発、カーボンニュートラル・サーキュラーエコノミーに関する研究開発、量子技術・AI 技術などの高度データ処理技術などの中の、経済安全保障に関連する分野がある。

さらに、日本には、最先端の重要技術を有する中小企業も多く見られるため、関係する中小企業との連携を進めるとともに、地域住民との情報共有なども図っていくべきである。

また、NanoTerasu のような、多くの企業・学術機関が、組織として、戦略的に、エコシステムに参画し、先進的な産学共創研究、国のプロジェクト、国際共同研究が行われている施設をモデルケースの実証の場とすることで、参画する全国の企業・大学にモデルケースの成果を容易に発信することが可能になる。

（７） 人材育成への支援

セキュリティ・クリアランス制度の運用、セキュリティ対策に精通した人材育成を進めるために、大学や研究機関におけるセキュリティ教育プログラムの開発、セキュリティ専門人材の育成のための研修プログラムの提供を政府が支援するとともに、セキュリティ専門人材の育成そのものについても、支援制度の創設する必要がある。

（８） 先行事例の共有

先行事例を収集し、分析した上で、事例集の作成、セミナーやワークショップの開催、オンラインデータベースの構築などの活動を通じ、成功事例や失敗事例を広く共有することが重要である。

（９） 申請者との継続的な対話の実施と、課題を踏まえた運用等の見直し

定期的な意見交換会の開催やオンライン・フォーラムの開設などにより、産学官での対話を継続し、アンケート調査なども踏まえて、制度の運用状況や課題を把握し、必要に応じ、運用等の見直しを行うことが求められる。

（１０） 当局間での継続的な国際的情報交換と相互認証の促進

政府は、関係する国際会議や二国間・多国間協議に積極的に参加し、国際的なセキュリティ・クリアランス制度に関する情報共有を図るとともに、諸外国との間での相互認証の推進などによる、国際的な連携強化を進めるべきである。また、多国間での情報共有のためのプラットフォーム構築についてリーダーシップを取ることが望ましい。

（１１） 国際共同研究に関する共同ガイドラインの策定

各国との連携を行う中で、国際共同研究に関連して、特に、情報セキュリティに関する基準、知的財産権の取り扱い、紛争解決 procedures 等に係る共同ガイドラインを作成することが求められる。

【本勉強会の構成員】

＜委員＞

旭化成株式会社	専務執行役員	山岸　秀之
株式会社東芝	上席常務執行役員	佐田　豊
三菱重工業株式会社	常務執行役員 CTO	伊藤　栄作
株式会社 IHI	常務執行役員	久保田 伸彦
株式会社日立製作所	研究開発グループ シニアチーフエキスパート	山田　真治
一般社団法人 日本経済団体連合会	常務理事	岩村　有広

＜東北大学＞

東北大学	副学長・教授	湯上　浩雄
東北大学	総長特別補佐・教授	高田　昌樹（(一財)光科学イノベーションセンター　理事長)
東北大学	参与・特任教授	佐藤　文一
東北大学（事務局代表）	特任教授	渡邉　真史

【検討経緯】

第 1 回勉強会

日時：令和 6 年 12 月 10 日（火）11:00～12:00

開催方法： オンライン会議（Zoom）

議題：

1. 本勉強会の趣旨と運営規程
2. 米国視察の報告
3. 研究開発セキュリティクリアランスに関する検討事項
4. その他

第 2 回勉強会

日時：令和 7 年 2 月 4 日（火）16:00～17:00

開催方法： オンライン会議（Zoom）

議題：

1. 前回議事録の確認(資料 1)
2. 研究開発セキュリティ・クリアランス勉強会(スケルトン案)の報告と検討(資料 2)
3. その他

第 3 回勉強会

日時：令和 7 年 3 月 11 日（火）11:00～12:00

開催方法： オンライン会議（Zoom）

議題：

１．前回議事録の確認（資料 1）

２．研究開発セキュリティ・クリアランス勉強会（報告書案）について（資料２）

３．その他

（次ページ以降は、参考資料）

【参考１】

--（日本関係）----------

資料 1-1 特定秘密の保護に関する法律
https://laws.e-gov.go.jp/law/425AC0000000108

資料 1-2 経済安全保障推進法
https://laws.e-gov.go.jp/law/504AC0000000043

資料 1-3 重要経済安保情報保護活用法
https://laws.e-gov.go.jp/law/506AC0000000027/20250516_000000000000000

資料 1-4 「経済安全保障上の重要技術に関する技術流出防止策についての提言～国が支援を行う研究開発プログラムにおける対応～」（経済安全保障法制に関する有識者会議、2024 年 6 月 4 日）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r6_dai10/siryou4.pdf

資料 1-5 DISM（Defense Industry Security Manual）（防衛装備庁）
https://www.mod.go.jp/atla/img/en/dism/dism2023_en.pdf

（参考 HP）

- ✓ https://www.cas.go.jp/jp/tokuteihimitsu/
- ✓ https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html
- ✓ https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html
- ✓ https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai4/teigen.pdf
- ✓ https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf
- ✓ https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai9/siryou10.pdf
- ✓ https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai7/gijiyousi.pdf

--（米国関係）----------

資料 2-1 NISPOM（National Industrial Program Operation Manual）
https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom

資料 2-2 国家安全保障裁定ガイドライン（SEAD-4）
https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf

資料 2-3 NIST SP 800-171（CUI 管理ガイドライン）
https://csrc.nist.gov/pubs/sp/800/171/r3/final

資料 2-4 リスクマトリックス（Science and Technology Risk Matrix）(DOE)
https://www.energy.gov/science/articles/science-technology-risk-matrix

資料 2-5 International Traffic in Arms Regulations （ITAR）
https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

資料 2-6 Export Administration Regulations （EAR）
https://www.trade.gov/buyusa-japan-export-administration-regulations
https://www.bis.gov/regulations

資料 2-7 Office of Foreign Assets Control（OFAC）
https://ofac.treasury.gov

資料 2-8 Deemed Export（みなし輸出）
https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports

資料 2-9 NSPM-33（国家安全保障大統領覚書第 33 号）
https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

資料 2-10 Economic Espionage Act（EEA）
https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf

資料 2-11 Defend Trade Secrets Act （DTSA）
https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf

資料 2-12 Cybersecurity Maturity Model Certification（CMMC）
https://www.cybersecuredashboard.com/wp-content/uploads/2020/08/CMMC_ModelMain_V1.02_20200318.pdf

資料 2-13 Committee on Foreign Investment in the United States （CFIUS）
https://crsreports.congress.gov/product/pdf/RL/RL33388
https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables

--（欧州関係）----------

資料 2-14 Council of the European Union. Council Decision 2013/488/EU on the security rules for protecting EU classified information. Official Journal of the European Union, 2013
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013D0488

資料 2-15 European Commission. Regulation (EU) 2021/821 on the Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items. Official Journal of the European Union, 2021
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0821

資料 2-16 European Commission. Horizon Europe Programme Guide: Legal and Financial Rules. European Commission, 2021
https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf

資料 2-17 European Defence Agency. Cyber Defence Programme. EDA Document, 2021
https://eda.europa.eu/docs/default-source/brochures/2021-eda-cyber-defence.pdf

資料 2-18 European Commission. EU Cybersecurity Strategy for the Digital Decade. European Commission, 2023

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

資料 2-19 European Parliament. Artificial Intelligence Act: Establishing a European Legal Framework. European Parliament Report, 2023 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

資料 2-20 European Commission. How to Handle Security-Sensitive Projects. European Commission, 2021 https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects_en.pdf

資料 2-21 European External Action Service (EEAS). https://www.eeas.europa.eu/_en

資料 2-22 European Commission. Commission Publishes New Guidelines for Annual Report on Dual-Use Export Controls. European Commission, 2024 https://policy.trade.ec.europa.eu/news/commission-publishes-new-guidelines-annual-report-dual-use-export-controls-2024-01-25_en

資料 2-23 European Data Protection Supervisor (EDPS). Security Measures for Personal Data Processing. EDPS Document, 2016 https://www.edps.europa.eu/sites/default/files/publication/16-03-21_guidance_isrm_en.pdf

資料 2-24 European External Action Service (EEAS). Commission recommends carrying out risk assessments on four critical technology areas. European Union, 2023 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735

資料 2-25 REGULATION (EU) 2021/821 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0821

資料 2-26 COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488

資料 2-27 European Union. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). Official Journal of the European Union, 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202500038

--（英国関係）----------

資料 2-28 Government Security Classifications Policy (HTML) - GOV.UK, 21 Jan, 2025

https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html

資料 2-29 National security vetting: clearance levels - GOV.UK, 21 Jan, 2025
https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels

資料 2-30 Security Clearances - What do the changes mean for you? - SDSC-UK, 21 Jan, 2025
https://www.sdsc-uk.co.uk/exhibitor-news-articles/security-clearances-what-do-the-changes-mean-for-you

資料 2-31 Guide to UK Government Security Classification Levels | Kahootz, 21 Jan, 2025
https://www.kahootz.com/guide-uk-information-security-classification-system/

資料 2-32 Government Security Classifications HANDLING INSTRUCTIONS and GUIDANCE for BIS staff - GOV.UK, 21 Jan, 2025
https://assets.publishing.service.gov.uk/media/5a7f054340f0b62305b84a02/Government_Security_Classification_guidance.doc

資料 2-33 United Kingdom Security Vetting: Applicant - GOV.UK, 21 Jan, 2025
https://www.gov.uk/guidance/united-kingdom-security-vetting-applicant

資料 2-34 Facility Security Clearance (FSC) Policy and Guidance for UK Defence Suppliers and MOD Contracting Authorities, 21 Jan, 2025
https://assets.publishing.service.gov.uk/media/65f1c6789812278a47f613a6/20240313-MOD_Facility_Security_Clearance_Policy_and_Guidance_v1.4.pdf

資料 2-35 UK strategic export controls - GOV.UK, 21 Jan, 2025
https://www.gov.uk/guidance/uk-strategic-export-controls

資料 2-36 The UK Science and Technology Framework - GOV.UK, 21 Jan, 2025
https://www.gov.uk/government/publications/uk-science-and-technology-framework/the-uk-science-and-technology-framework

資料 2-37 The UK Science and Technology Framework: one year on - techUK, 21 Jan, 2025
https://www.techuk.org/resource/the-uk-science-and-technology-framework-one-year-on.html

資料 2-38 Government technology standards and guidance - GOV.UK, 21 Jan, 2025
https://www.gov.uk/guidance/government-technology-standards-and-guidance

【参考２】 NanoTerasu の動向

１．施設の概要

- 2024 年 4 月に運用を開始した 3GeV 高輝度放射光施設。我が国初の、低エミッタンス電子ビーム蓄積リングを有する最新鋭の放射光施設である。既存の放射光施設は“第三世代”放射光源とよばれ、それらと区別するため“第四世代”と呼ばれている。MAX-IV（スウェーデン）、ESRF-EBS（EU：ESRF のアップグレード）、SIRIUS（ブラジル）に続き、NanoTerasu は世界で 4 番目の第四世代施設となった。 2024 年 7 月には、ALS-U（米国アルゴンヌ国立研究所）が第四世代に加わった。
- 総建設費は、380 億円。官民地域パートナーシップという、新しいスキームで、国側（主体：QST）が 200 億円を、地域パートナー側（代表：一般財団法人光科学イノベーションセンター、宮城県、仙台市、東北大学、東経連）と利用を予定する 100 社を超える民間企業、研究機関が 180 億円を拠出し建設した。国は枢要部である加速器を建設。地域パートナーは、土地造成と、基本建屋の建設を行った。
- また、放射光を利用するビームライン（総数 28 本が建設可能）のうち、QST が共用ビームライン 3 本を整備し運営、地域パートナーが 7 本を整備し運営している。
- 2023 年仙台地区で開催された G7 科学技術大臣サミットのサイド・イベントとして、NanoTerasu 視察（5 月 14 日）、及び、「量子技術が切り拓く未来」（主催：東北大学，（一社）量子技術による新産業創出協議会（Q-STAR）、共催： 内閣府，文部科学省，経済産業省）が、NanoTerasu 実験ホールで開催された。

２．設置・運用形態

- 世界で初めて「コアリション利用」を導入した。すなわち、建設資金を拠出し地域パートナーに加わった利用者（コアリションメンバー）が 7 本の独自のビームライン（コアリションビームライン）を専有利用することが可能。

３．コアリッションのメリット、課題

（メリット）

- ✓ 過去の国主体の利用モデルから脱却した柔軟な利用形態（課題申請の免除等）により、迅速な研究開発が可能。
- ✓ 企業や大学が独自に計測データを管理でき、機密性の高い研究開発が可能となっている。

（課題）

- ✓ 共用エリアとコアリションエリアを明確に分け、専有利用の際の機密性の次元を高める必要がある。
- ✓ コアリション利用においては、各機関や企業から参加する研究者、NanoTerasu 職員、いずれについても、アクセス権の制限が不可避である。

✓ 多様な利用者間でのデータ共有において、暗号化通信やアクセス制御の強化が不可欠。定期的なセキュリティ監査も必要。

４．人のアクセス制限の評価ポイント

✓ 研究者の信頼性評価　：　各利用者の経歴や所属機関を評価

✓ 職員の適格性認証

５．海外の動向

✓ 同様の最新鋭施設が、次々と建設・計画中

✓ 建設中：

SLS2.0（スイス、2025 年完成予定）、韓国、

中華人民共和国（上海、北京）、ロシア、

✓ 計画中： SOLEIL-II（フランス）、ALS-U（米国ローレンスバークレー国立研究所）、

Elettra（イタリア）、ALBA（スペイン）、SPring-8-II（日本）

【参考３】 研究開発関連デジタルデータ保護に関する欧米の比較

米国・統合型デジタルシステム

米国では、研究開発や防衛関連プロジェクトで取り扱う電子データやデジタル資産の管理を効率化するため、申請から審査、モニタリングまでをデジタル化したシステムを広く導入。例えば、連邦職員の審査に用いられる eApp（Electronic Application）や、連邦政府全体の調査プロセスを管理する NBIS（National Background Investigations System）など

これらのシステムにより、申請者のデジタル情報（アクセスログ、行動履歴など）を自動的に分析し、リスク評価をリアルタイムで行う仕組みが確立

デジタル情報の暗号化、二要素認証、アクセスログの記録といった技術的対策が徹底。また、連邦機関間で統一されたルールのもと、クリアランス保持者の状態は定期的に再評価され、継続的なモニタリングが実施

欧州・分散型・国別対応

欧州では、連邦的なデジタル情報クリアランス制度は存在せず、各国ごとに異なる管理基準や手続きを採用。各国は、国家安全保障に係る情報保護と同時に、GDPR など個人情報保護の厳格な規制の枠組みを踏まえながら、デジタル資産を管理

欧州におけるデジタル情報管理は、デジタル情報クリアランスの対象となる情報の取り扱いにあたり、プライバシー保護とのバランスが強く求められる。具体的には、個人データの保護に関する厳格な規制の下で、アクセス権の付与や監視の方法が設定され、透明性と個人権の尊重を前提とした管理・運用を実施

技術的対策は存在するものの、米国ほど中央集権的・自動化されたシステムは未整備

（注）

eApp ： 以前は e-QIP と呼ばれていた、連邦職員の審査に用いられる電子申請システム

NBIS ： 連邦政府全体の調査プロセスを管理するシステムで、セキュリティクリアランスの申請、審査、更新などが行われる。

GDPR ： EU における個人データ保護に関する規則であり、EU 域内で事業を行う企業は GDPR を遵守する必要がある。