国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau
National Diet Library

論題 Title	米国のセキュリティ・クリアランス制度と日本における議論―研究者への適用をめぐって―
他言語論題 Title in other language	U.S. Security Clearances and the Debate in Japan: How Should They Apply to Researchers?
著者 / 所属 Author(s)	福田　健志（FUKUDA Takeshi）／行政法務課
書名 Title of Book	変化する国際環境と総合安全保障　総合調査報告書（Comprehensive Security in a Changing International Environment）
シリーズ Series	調査資料 2021-3（Research Materials 2021-3）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
刊行日 Issue Date	2022-03-25
ページ Pages	109-127
ISBN	978-4-87582-889-1
本文の言語 Language	日本語（Japanese）
キーワード keywords	セキュリティ・クリアランス、適性評価、秘密保護法、新興技術、安全保障
摘要 Abstract	現在日本では、研究者を対象とするセキュリティ・クリアランス制度の必要性が議論されている。米国の制度の概要とその研究者への適用について紹介し、日本における議論の論点をまとめる。

米国のセキュリティ・クリアランス制度と日本における議論
―研究者への適用をめぐって―

国立国会図書館　調査及び立法考査局
行政法務課　福田　健志

目　　次

キーワード：セキュリティ・クリアランス、適性評価、秘密保護法、新興技術、安全保障

はじめに

セキュリティ・クリアランスとは、政府が、ある個人について、秘密情報を取り扱う適性を有すると認定すること(1)、又はそうした個人に付与される資格である(2)。米国では、政府が機密指定した情報を取り扱う個人の適性を認定する制度がある。日本では、「特定秘密の保護に関する法律」（平成 25 年法律第 108 号。以下「特定秘密保護法」）に基づく特定秘密を取り扱う行政機関の職員等の適性評価制度がある。政策決定には、その判断を支援するための情報が不可欠であり、セキュリティ・クリアランス制度は、特に国家安全保障に係る政策決定に必要な秘密情報が外部に漏えいすることを防ぐための制度である(3)。

近年、技術覇権をめぐる米国と中国の対立の中で、国家安全保障上重要な技術の流出防止が課題となっている。これを背景に、日本では、研究者を対象とするセキュリティ・クリアランス制度の必要性が議論されている。米国では、連邦政府から資金の提供を受け、機密指定された研究を実施する研究者に対して、セキュリティ・クリアランスが実施されている。本稿では、米国のセキュリティ・クリアランス制度の概要とその研究者への適用について紹介し、日本における議論の論点を整理する。

Ⅰ　米国のセキュリティ・クリアランス制度

1　機密指定制度

米国の連邦政府が保有・作成・管理している情報の機密指定制度は、現在、オバマ（Barack H. Obama）大統領が 2009 年 12 月に発した大統領令第 13526 号を中心に運用されている(4)。同大統領令に基づき、大統領や大統領が指定した行政機関の長等は、連邦政府が保有・作成・管理している情報について、同大統領令が規定する事項(5)に関するものであり、正当な権限によらずに開示された場合に国家安全保障上の損害が生じることを合理的に予想することができ、かつ、その損害を特定又は説明することができる場合に、機密指定することができる（大統領令第 13526 号第 1.1 条）。機密情報のレベルは、重要度が高い順に「Top Secret」、「Secret」、「Confidential」のいずれかが設定される（大統領令第 13526 号第 1.2 条）。

大統領令第 13526 号のほか、「原子力エネルギー法」（Atomic Energy Act of 1954）は、原子力関連技術に関する機密情報として、「開示制限データ（Restricted Data）」(6)等を規定している。

＊　本稿におけるインターネット情報の最終アクセス日は、令和 3（2021）年 12 月 28 日である。

(1)　Michelle D. Christensen, “Security Clearance Process: Answers to Frequently Asked Question,” *CRS Report*, R43216, 2016.10.7, p.1. <https://crsreports.congress.gov/product/pdf/R/R43216/7>

(2)　小林良樹『なぜ、インテリジェンスは必要なのか』慶應義塾大学出版会, 2021, p.234.

(3)　同上, pp.228, 234-236; 永野秀雄「米国の連邦行政機関における適性評価制度の概要」大沢秀介監修 , 山本龍彦ほか編『入門・安全と情報』成文堂, 2015, pp.60-61.

(4)　Executive Order 13526 of December 29, 2009, *Federal Register*, vol.75 no.2, January 5, 2010, pp.707-731.（以下「大統領令第 13526 号」）本大統領令の内容については、以下の文献を参照した。永野秀雄「米国における国家機密の指定と解除―わが国における秘密保全法制の検討材料として―」『人間環境論集』12 巻 2 号, 2012.3, pp.1-102.

(5)　該当事項は以下のとおり。(a) 軍事計画、武器システム又は作戦に関する情報、(b) 外国政府情報、(c) インテリジェンス活動（秘密活動を含む）、インテリジェンスに関する情報源若しくは手法又は暗号に関する情報、(d) 機密情報源を含む連邦政府の外交関係又は外交活動に関する情報、(e) 国家安全保障に関連する科学的、技術的又は経済的事項に関する情報、(f) 核物質又は核施設に対する安全防護策に関する連邦政府プログラムに関する情報、(g) 国家安全保障に関連するシステム、施設、社会基盤、プロジェクト、計画又は防護サービスの脆弱性又は能力に関する情報、(h) 大量破壊兵器の開発、生産又は利用に関する情報（大統領令第 13526 号第 1.4 条）。

同法に基づく機密情報には、政府の情報に限らず、例えば民間事業者が民間資金で実施した研究に係る情報も含まれる(7)。

大統領令第13526号は、機密情報を正当な権限を有しない者に開示した者に対して、戒告や休職処分、セキュリティ・クリアランスの失効等の制裁を規定している（第5.5条）。また、機密情報を含む重要な情報の漏えいについては、様々な法律に罰則が規定されている。例えば、大統領令第13526号に基づく機密情報を含む国防秘密について、これを合法的に取り扱っていた者が、悪意で権限のない者に送信した場合等に、罰金又は10年以下の拘禁刑を科すこととされている(8)。

2　セキュリティ・クリアランス制度の概要

機密情報を取り扱うことができるのは、身上調査を経て行政機関の長から適性を認定された者、すなわちセキュリティ・クリアランスを保有する者に限定される(9)。大統領は、機密情報へのアクセスに関する大統領令及び規則を定める権限を有する(10)。現在、セキュリティ・クリアランス制度の原則を規定しているのは、クリントン（Bill Clinton）大統領が1995年8月に発した大統領令第12968号である(11)。また、政府から業務を請け負う契約事業者等や、重要インフラを運営する民間事業者等における機密情報の保全について、それぞれ大統領令が発出されている。

(1) 大統領令第12968号に基づく制度

(i) 原則

セキュリティ・クリアランスを付与されるのは、原則的に米国市民に限られる（大統領令第12968号第3.1条(b)）(12)。また、セキュリティ・クリアランスを有する個人は、業務上必要がある（need-to-know）機密情報に限ってアクセスが認められ、あらゆる機密情報にアクセスで

---

(6)　開示制限データとは、①核兵器のデザイン、製造、使用、②特別な核物質の生産、③エネルギー生産における特別な核物質の利用に関するあらゆるデータのうち、機密が解除されたものを除くものである（42 U.S.C. § 2014(y); 岡本篤尚『国家秘密と情報公開―アメリカ情報自由法と国家秘密特権の法理―』法律文化社, 1998, p.207.）。

(7)　Arvin S. Quist, “Security Classification of Information: Volume 1. Introduction, History, and Adverse Impacts,” 2002.9.20, p.89. Federation of American Scientists website <https://sgp.fas.org/library/quist/index.html>

(8)　18 U.S.C. §§ 793(d), 793(f); 松井茂記「諸外国は国家の秘密と市民の自由にどう向き合っているか　アメリカ」田島泰彦・清水勉編『秘密保全法批判―脅かされる知る権利―』日本評論社, 2013, pp.182-185.

(9)　大統領や副大統領、連邦議会議員、最高裁判事等には、セキュリティ・クリアランスの保有は求められていない。ただし、例えば連邦議会議員の場合、取り扱うことができる機密情報は、職務上必要があるものに限られる（Christensen, *op.cit.*(1), p.4.）。なお、各省長官を含む、上院の承認に基づいて大統領が任命する政治任用職が機密情報を取り扱うためには、セキュリティ・クリアランスが必要とされる。この場合、主に連邦捜査局（FBI）が身上調査を担当する（Office of Personnel Management, “Presidential Transition Guide to Federal Human Resources Management Matters: Election Year 2020,” 2020.12, p.57. <https://www.opm.gov/about-us/our-people-organization/office-of-the-director/executive-secretariat/presidential-transition-guide-2020.pdf>）。

(10)　50 U.S.C. § 3161.「国家安全保障法」（National Security Act of 1947）の1994年改正（Intelligence Authorization Act for Fiscal Year 1995, Pub.L. No.103-359, 108 Stat. 3423(1994).）による。ただし、それ以前から、セキュリティ・クリアランス制度は大統領令に基づいて実施されてきた。これらの大統領令は、連邦憲法の外交と軍事活動に関する大統領権限に基づいて定められてきたとされる（永野　前掲注(3), p.63.）。

(11)　Executive Order 12968 of August 2, 1995, *Federal Register*, vol.60 no.151, August 7, 1995, pp.40245-40254.（以下「大統領令第12968号」）大統領令第12968号は、その後数回の改正を経ている。このうち、ジョージ・W・ブッシュ（George W. Bush）大統領が2008年6月に発した大統領令第13467号（Executive Order 13467 of June 30, 2008, *Federal Register*, vol.73 no.128, July 2, 2008, pp.38103-38108.）により、現在は国家情報長官が制度を監督する中心的な機関とされている（“Security Executive Agent.” Office of the Director of National Intelligence website <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent>）。

(12)　例外として、特別な専門知識を持つ外国人には、特定のプログラムやプロジェクト等に関する機密に対するアクセスが認められる場合がある（大統領令第12968号第2.6条）。

きるわけではない（大統領令第 12968 号第 2.5 条(a)）。

（ii）実施手順

以下、連邦政府職員がセキュリティ・クリアランスを取得する場合を念頭に、セキュリティ・クリアランスの実施手順を述べる。

(a) 申請

各行政機関は、職員や求職者が、業務上、機密情報にアクセスする必要があると判断した場合、Top Secret、Secret、Confidential のどのレベルの機密情報にアクセスする必要があるかに応じて当該職員等のアクセスレベルを決定する[13]。当該職員等は、申請書類を提出するとともに、身上調査を実施する行政機関が、各種個人情報を参照することに同意する必要がある（大統領令第 12968 号第 1.2 条(e)）。

(b) 身上調査

申請を受けて、身上調査が実施される。身上調査は、原則として国防総省の国防カウンターインテリジェンス・保全庁が一元的に実施している[14]。調査では、申請者本人との面談や、友人や同僚、家主、隣人等への照会等が実施される[15]。行政機関によっては、ポリグラフ検査（いわゆる「嘘発見機」を用いた検査）を実施している[16]ほか、最近では公開されているソーシャルメディアの情報も活用している[17]。

(c) 認定

身上調査の結果を受けて、各行政機関の長が、当該職員等のセキュリティ・クリアランスを認定する[18]。

(d) 定期的な再調査と資格の失効

セキュリティ・クリアランスの保有者は、定期的に再調査を受けてその資格を更新する必要がある。定期的な再調査は、少なくとも Top Secret の場合は 5 年、Secret の場合は 10 年、Confidential の場合は 15 年に 1 回実施することとされてきた[19]が、近年はこれをアクセスレベ

---

⑬　これら 3 つのレベルのほかに、「機微隔離情報」（Sensitive Compartmented Information）や「特別アクセスプログラム」（Special Access Programs）と呼ばれる機密区分が存在する。前者はインテリジェンスの情報源や手法が含まれる情報であり、後者は高度に機微な政策、プロジェクト、プログラムに関する情報である。これらの区分は特に慎重な取り扱いが必要とされる機密情報を対象としており、これを取り扱う職員等には、Top Secret よりも厳しい身上調査が実施され、その人数は限定される（Christensen, *op.cit.*(1), p.2.）。

⑭　“Background Investigations.” Defense Counterintelligence and Security Agency website <https://www.dcsa.mil/mc/pv/investigations/> なお、CIA や FBI など、身上調査を自ら実施している機関もあるとされる（“Before You Apply: Understanding Government Background Checks.” Yale Law School website <https://law.yale.edu/student-life/career-development/students/career-pathways/public-interest/you-apply-understanding-government-background-checks>）。

⑮　“Investigations, Adjudications and Clearance Processes at a Glance: Investigations Process Details.” Defense Counterintelligence and Security Agency website <https://www.dcsa.mil/mc/pv/mbi/gicp/>

⑯　“Security Executive Agent Directive 2 (Revised): Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position,” 2020.9.1, p.2. Office of the Director of National Intelligence website <https://www.dni.gov/files/NCSC/documents/Regulations/Security-Executive-Agent-Directive-2-20201005.pdf>

⑰　“Security Executive Agent Directive 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications,” 2016.5.12, p.3. *ibid.* <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf>

⑱　認定は、申請者の人格や、他国との利益相反や強迫を受ける可能性の有無、規則を遵守する意思と能力の有無を基準として行われる（大統領令第 12968 号第 3.1 条 (b); 永野　前掲注(3), p.65.）。その際、申請者の米国への忠誠、外国の影響、外国の利益を優先する傾向、性行動、私行、経済的な状況、アルコール消費、薬物の使用、精神状態、犯罪行為、機密情報を含む保護された情報の取扱い、業務外活動、情報技術の使用状況を総合的に勘案することとされている（“Security Executive Agent Directive 4: National Security Adjudicative Guidelines,” 2017.6.8, p.6. *ibid.* <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>）。

ルに関わらず5年に1回実施する傾向にある[20]。また、後述するように、今後は定期的な再調査に代わって「継続審査」が導入されることが予定されている。

セキュリティ・クリアランスの資格は、個人が機密情報へアクセスする必要が生じなくなった場合に失効する（大統領令第12968号第2.1条(b)(4)）。ただし、例えばセキュリティ・クリアランスの保有者が、行政機関を退職し、再就職先で再び機密情報へアクセスする必要が生じた場合、新たに身上調査を受けることなくセキュリティ・クリアランスが再び有効となる場合がある[21]。

（ⅲ）不服申立て・再審査

新規の申請や定期的な再調査の結果、セキュリティ・クリアランスが認定されなかった場合[22]、申請者等は、機密情報を取り扱う必要のない職種への配置転換や、場合によっては免職となるなど、不利益を受ける可能性がある[23]。そのため、不認定となった申請者には、その理由や決定の根拠に関する告知を受ける権利、不服申立てや当該行政機関の長によって設置される再審査委員会による再審査を請求する権利が認められている（大統領令第12968号第5.2条）。ただし、セキュリティ・クリアランスの認定は行政機関による裁量行為とされ（大統領令第12968号第3.1条(b)、第5.1条）、過去の連邦最高裁判決でも、セキュリティ・クリアランスの不認定を裁判で争うことはできないとされている[24]。

(2) 契約事業者等における機密情報の保全制度

連邦政府から業務を請け負う民間事業者や、連邦政府から資金の提供を受けて研究を行う研究機関（以下「契約事業者等」）における機密情報の保全は、ジョージ・H・W・ブッシュ（George H. W. Bush）大統領が1993年1月に発した大統領令第12829号（国家産業保全プログラム）に基づいて実施されている[25]。

国防長官等は、業務上、機密情報へアクセスする必要がある契約事業者等の従業員や研究者に対して、身上調査の上、セキュリティ・クリアランスを認定する[26]。その実施手順は、連邦政府職員の場合とほぼ同じである[27]。セキュリティ・クリアランスに係る費用は、連邦政府が負担している[28]。また、契約事業者等は、機密情報を取り扱う適性を有することについて、

---

⑲ 32 C.F.R. Attachment A to Subpart B of Part147(b), Attachment C to Subpart B of Part147(b).

⑳ Christensen, *op.cit.*(1), pp.6-7.

㉑ *ibid*, p.7.

㉒ 申請に対してセキュリティ・クリアランスが認定されなかった件数について、連邦政府は統計を公表していない（永野秀雄「米国における科学者・技術者に対するセキュリティクリアランス―量子情報科学を中心に―（上）」『CISTEC journal』192号, 2021.3, p.162.）。ただし、2020年の国防総省への不服申立て件数は、529件とされ（Marko Hakamaa, “Top Reasons for Security Clearance Denial in 2020,” 2021.1.6. Clearancejob.com website <https://news.clearancejobs.com/2021/01/06/top-reasons-for-security-clearance-denial-in-2020/>）、認定されないケースが一定数あることが分かる。

㉓ 永野　前掲注(3), pp.73-76.

㉔ Dep’t of the navy v. Egan, 484 U.S. 518 (1988). 本判決は連邦政府職員に係るものだが、その法理は、契約事業者等に係る裁判にも適用されている（同上, pp.73-74, 76-77.）。

㉕ Executive Order 12829 of January 6, 1993, *Federal Register*, vol.58 no.5, January 8, 1993, pp.3479-3483.

㉖ 国防長官は、契約事業者等の従業員のセキュリティ・クリアランスの認定等の業務について、連邦政府の中心的な執行機関とされており（大統領令第12829号第202条(a)）、情報機関等を除く行政機関の契約事業者等については、身上調査だけでなく、セキュリティ・クリアランスの認定も国防長官が実施している（“National Industrial Security Program (NISP).” Defense Counterintelligence and Security Agency website <https://www.dcsa.mil/mc/ctp/nisp/>; 32 C.F.R. §§ 117.3(b), 117.10(a)(1).）。

㉗ 32 C.F.R. § 117.10.

秘密取扱施設許可（施設クリアランス）を受ける必要がある[29]。この際、当該事業者等が外国からの出資を受けている場合は、これにより機密情報の漏えいや業務への支障が生じるおそれがないこと等を確認することとされている[30]。

(3) 重要インフラを運営する民間事業者等における機密情報の保全制度

契約事業者等以外の重要インフラを運営する民間事業者における機密情報の保全は、州政府や地方自治体における機密情報の保全とともに、オバマ大統領が2010年8月に発した大統領令第13549号に基づいて実施されている[31]。

機密情報へアクセスする必要がある従業員に対するセキュリティ・クリアランスの実施手順は、連邦政府職員の場合とほぼ同じである[32]。セキュリティ・クリアランスの認定は、当該事業者等に機密情報を提供する行政機関が行うのが原則だが、各行政機関は、この権限を国土安全保障省に移譲することが認められている[33]。近年は、重要インフラをサイバー攻撃から守るため、政府と民間事業者の間でサイバー攻撃に係る機密情報を共有する取組が進められている[34]。

3　制度の運用と近年の見直し

(1) 制度の運用状況

2019会計年度（2018年10月～2019年9月）中にセキュリティ・クリアランスが新たに認定された者及び定期的な再調査によって更新した者は、合計約96万人である。2019年10月1日時点で、セキュリティ・クリアランスの保有者は約424万人である。このうち、実際に機密情報にアクセスしている者は、約295万人である[35]（次頁表参照）。

(2) 近年の制度の見直し

近年のセキュリティ・クリアランス制度の大きな課題は、認定までにかかる期間の短縮と、制度に対する信頼性の確保である。

米国の機密指定制度については、本来は機密に該当しない情報を機密指定する「過剰な機密指定」によって、本当の機密は何かが不明確になり、政府の政策判断を誤らせること、政府の説明責任が損なわれ国民からの信頼の低下を招くこと、機密の管理に必要なコストの増大を招

---

(28) Christensen, *op.cit.*(1), p.8.
(29) 32 C.F.R. § 117.9(a)(4).
(30) 32 C.F.R. §§ 117.9(c)(6), 117.11(a)(1).
(31) Executive Order 13549 of August 18, 2010, *Federal Register*, vol.75 no.162, August 23, 2010, pp.51609-51614. 本大統領令が主に対象とする民間事業者は、重要インフラ及び主要リソースに関連する事業者である（第5条(g)）。関連する産業として、食料、エネルギー、金融、水、情報通信、運送等が挙げられる（Department of Homeland Security, "A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level," 2008.9, p.9. <https://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf>）。
(32) Department of Homeland Security, "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive," 2012.2, p.11. <https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/implementing-directive.pdf>
(33) *ibid.*, p.14.
(34) Robert K. Knake, "Sharing Classified Cyber Threat Information with the Private Sector," 2018.5.15. Council on Foreign Relations website <https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector>
(35) National Counter Intelligence and Security Center, "Fiscal Year 2019 Annual Report on Security Clearance Determinations," 2020.4, pp.6-8. Federation of American Scientists website <https://sgp.fas.org/othergov/intel/clear-2019.pdf>

表　セキュリティ・クリアランスの年間認定者数及び保有者数

	2019 会計年度中の資格認定者数 (注 1)		資格保有者数（2019 年 10 月 1 日時点）			
			総保有者数		（うち in access） (注 2)	
区分 (注 3)	Conf/Secret	Top Secret	Conf/Secret	Top Secret	Conf/Secret	Top Secret
連邦政府職員	470,461	182,062	2,185,768	711,404	（1,090,170）	（605,579）
契約事業者等	121,941	157,964	533,009	497,271	（472,398）	（472,576）
不明 (注 4)	23,890	7,820	141,100	175,385	（135,230）	（173,803）
小計	616,292	347,846	2,859,877	1,384,060	（1,697,798）	（1,251,958）
合計	964,138		4,243,937		（2,949,756）	

（注 1）セキュリティ･クリアランスを新たに取得した者と定期的な再調査によって更新した者の総数である。
（注 2）資格保有者のうち、実際に機密情報にアクセスしている者の数。この区分から除かれるのは、例えば将来の必要性を見越して前もって資格を申請・取得した者である。
（注 3）「Conf/Secret」は、Confidential の資格を持つ者と Secret の資格を持つ者の総数である。
（注 4）「不明」は、集計に用いたシステム上の制約により、連邦政府職員と契約事業者等のいずれの区分に該当するかが不明な者等の数である。
（出典）National Counter Intelligence and Security Center, “Fiscal Year 2019 Annual Report on Security Clearance Determinations,” 2020.4, pp.6-8. Federation of American Scientists website <https://sgp.fas.org/othergov/intel/clear-2019.pdf> を基に筆者作成。

くこと等の弊害が見られることが指摘されてきた(36)。また、過剰な機密指定は、2001 年 9 月の同時多発テロ事件後に安全保障に関連する役職が増加したこと(37)とも相まって、セキュリティ・クリアランスを必要とする者の増加を招いたとされる(38)。これにより、セキュリティ・クリアランスの申請から認定までに 1 年以上も要するなど手続が長期化し、人材確保への支障や手続に係るコストの増大等の弊害が指摘された(39)。

一方、2000 年代後半以降、セキュリティ・クリアランスを保有する軍人や契約事業者の従業員による情報漏えい事件や銃撃事件が相次いで発生した(40)。また、2019 年まで身上調査を

(36)　三木由希子「アメリカの秘密保護法制の実態　多すぎる機密は政策判断を誤らせる 米国での聞き取りでわかったこと」『Journalism』290 号, 2014.7, p.128; James B. Bruce et al., “Secrecy in U.S. National Security: Why a Paradigm Shift is Needed,” 2018.11, pp.13-14. Rand Corporation website <https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE305/RAND_PE305.pdf>

(37)　Silvestre Reyes, “Security Clearance Reform: Upgrading the Gateway to the National Security Community,” Report110-916, House of Representatives, 2008.11.20, p.5. <https://www.congress.gov/110/crpt/hrpt916/CRPT-110hrpt916.pdf>

(38)　ローレンス・レペタ（渡辺武達訳）「140 万人が最高機密に接近可能な米国　秘密保全制度が国家を脆弱化する」『Journalism』283 号, 2013.12, pp.90-91.

(39)　Reyes, *op.cit.*(37), p.8.

(40)　①2010 年 5 月、陸軍軍人のブラッドリー（現在はチェルシー）・マニング（Chelsea Manning）が、機密軍事情報等を内部告発サイト「ウィキリークス」に提供したとして逮捕され、その後有罪判決を受けた（「ウィキリークス　米公電暴露　情報提供、マニング上等兵に有罪　米軍法会議」『毎日新聞』2013.7.31, 夕刊 .）。②2013 年 6 月、国家安全保障局から業務委託を受けていた民間事業者の従業員だったエドワード・スノーデン（Edward Snowden）は、同局の機密情報を大量に暴露した（土屋大洋「インターネットとインテリジェンス第 7 回　壊れたセキュリティ・クリアランスと秘密保護」『治安フォーラム』230 号, 2014.2, pp.64-65.）。③2013 年 9 月、元海軍軍人で、海軍省から業務委託を受けていた民間事業者の下請業者の従業員だったアーロン・アレクシス（Aaron Alexis）が、ワシントン D.C. の海軍工廠内で銃撃事件を起こし、12 名を殺害した（Department of Defense, “Internal Review of the Washington Navy Yard Shooting,” 2013.11.20, pp.1-2. Center for Homeland Defense and Security website <https://www.hsdl.org/?view&did=750745>）。①では、当時 22 歳で下位の階級にある者が Top Secret の資格を保有していることが疑問視された（レペタ　前掲注(38), pp.90-91.）。②③では、両者が資格を取得してから数年が経過していたこと、両者が転職を経ているにもかかわらず、前職時に取得した資格が、再就職後も追加の身上調査なしで有効とされていたことが疑問視された（土屋　同, p.65; Department of Defense, *idem*, p.43.）。

担当していた人事管理局から多くの調査業務を受託していた民間事業者による不適切な調査が疑われたこと[41]や、サイバー攻撃によって人事管理局から身上調査に関するものを含む大量の個人情報が流出する事案が発生したこと[42]により、制度に対する信頼が大きく損なわれた。オバマ政権は、機密情報の漏えい防止策として、職員等の「インサイダー」が絡む内部的脅威を発見・防止するための取組[43]やセキュリティ・クリアランスの対象者の見直し[44]等を実施した。

その後、トランプ（Donald J. Trump）政権において、身上調査業務は人事管理局から国防総省の国防カウンターインテリジェンス・保全庁に移管された[45]。身上調査業務に従事する職員の増加や照会にテレビ会議システムを用いること等により[46]、最近のセキュリティ・クリアランス取得にかかる日数は短縮され、Top Secret で平均 158 日、Secret で平均 81 日、定期的な再調査で平均 176 日となっている[47]。

(3) 現在の取組

セキュリティ・クリアランスの認定までにかかる期間の更なる短縮と、制度に対する信頼性の確保という観点から、現在、主に以下の 2 つの取組が推進されている。

(ⅰ) 相互認定（Reciprocity）

現在、セキュリティ・クリアランスの認定は、原則的に各行政機関の長が実施している。しかし、所属先や契約先の行政機関が代わるたびに新たに身上調査を受けセキュリティ・クリアランスを取得し直す必要が生じれば、多くの手間とコストがかかる。これに対して「相互認定（Reciprocity）」とは、ある行政機関の長による認定を、全ての行政機関の長が受け入れることである[48]。これまでも相互認定は推進されてきたが、組織間の情報共有や信頼感の不足によ

⑷1　人事管理局から身上調査業務を受託していた USIS 社の元従業員からの告発により、同社が、2008 年から 2012 年にかけて、契約内容に沿った調査を実施していなかったことが疑われた。2015 年 8 月、司法省は、同社が、業務の見返りとして主張していた受託金を放棄することに合意したと発表した（“U.S. Investigations Services Agrees to Forego at Least $30 Million to Settle False Claims Act Allegations,” 2015.8.19. Department of Justice website <https://www.justice.gov/opa/pr/us-investigations-services-agrees-forego-least-30-million-settle-false-claims-act-allegations>）。

⑷2　2015 年 6 月、人事管理局から、連邦政府職員や契約事業者の従業員等の身上調査に関する情報が流出したことが発覚した。流出した情報には、約 2,150 万人分の個人情報が含まれるとされた（“Cybersecurity Incidents: What Happened.” Office of Personnel Management website <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>）。

⑷3　廣瀬淳子「【アメリカ】機密情報保護に関する大統領令」『外国の立法』No.250-1, 2012.1, pp.2-3. <https://dl.ndl.go.jp/view/download/digidepo_3382150_po_02500101.pdf?contentNo=1>

⑷4　各機関の取組により、2014 会計年度の間に、セキュリティ・クリアランスの保有者は全体で約 12% 減少した。減少分の多くは、各機関が将来の必要性を見越して前もってセキュリティ・クリアランスを申請・取得させていた者等、実際には業務において機密情報へのアクセスを必要としていなかった者であるとされる（Emily Kopp, “Government Cuts Security Clearances by 12 Percent,” *Federal News Network*, 2015.4.23. <https://federalnewsnetwork.com/management/2015/04/government-cuts-security-clearances-by-12-percent/>）。

⑷5　“Background Investigation Mission Moving to DoD,” 2019.7.29. Defense Counterintelligence and Security Agency website <https://www.dcsa.mil/Portals/69/documents/news/DCSA_Press_Release_TOF.pdf>

⑷6　Nicole Ogrysko, “How NBIB Slashed the Security Clearance Backlog by 300,000 in Nearly a Year,” *Federal News Network*, 2019.6.17. <https://federalnewsnetwork.com/nbib-transfer-to-dod/ 2019 / 06 /how-nbib-slashed-the-security-clearance-backlog-by-300000-in-nearly-a-year/>

⑷7　2020 会計年度第 4 四半期時点における、申請のうち手続が早く完了した上位 90% の平均値。このうち、身上調査にかかった日数は、Top Secret で平均 118 日、Secret で平均 58 日、定期的な再調査で平均 110 日となっている（John Ratcliffe et al., “Security Clearance, Suitability / Fitness, and Credentialing Reform,” 2021.1, pp.16-17. Federation of American Scientists website <https://sgp.fas.org/othergov/omb/clearance-2021-01.pdf>）。

⑷8　“Security Executive Agent Directive 7: Reciprocity of Background Investigations and National Security Adjudications,” 2018.11.9, p.2. Office of Director of National Intelligence website <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf>

り十分浸透していないとされ[49]、産業界からは、一層の徹底を求める声が挙がっている[50]。

（ii）継続評価（Continuous Evaluation）及び継続審査（Continuous Vetting）

前述した情報漏えい事案等を受けて、連邦政府内では、定期的な再調査の周期が長く、セキュリティ・クリアランス保有者の状況の変化に対応することができないことが課題として指摘された[51]。これに対して、「継続評価（Continuous Evaluation）」とは、商用データベースや連邦政府のデータベースを自動的に随時チェックするシステム等を用いて、資格保有者の適性を継続的に確認することである[52]。現在実施されている継続評価は、定期的な再評価に代わるものではなく、これを補完するものと位置付けられている[53]。今後、新たなシステムの開発等により、継続評価の手法を用いた「継続審査（Continuous Vetting）」[54]に移行することが予定されており、これは定期的な再調査に代わるものになるとされている[55]。

Ⅱ　米国におけるセキュリティ・クリアランス制度の研究者への適用

前述した大統領令第 13526 号は、機密指定の対象となる事項の 1 つに「国家安全保障に関連する科学的、技術的又は経済的事項に関する情報」（第 1.4 条(e)）を挙げている。連邦政府は、様々な研究機関に対して資金を提供しているが、研究内容が上記大統領令に該当する場合、当該研究は機密指定を受け、これに従事する研究者にはセキュリティ・クリアランスの取得が必要とされる[56]。連邦政府が運営する研究機関の研究者には連邦政府職員と同様の制度が、それ以外の大学や民間事業者、政府所有・請負人運営研究機関（Government-Owned, Contractor-Operated Laboratories. GOCO 機関）[57]の研究者には、契約事業者等と同様の制度が適用される[58]。

研究の機密指定は、国家安全保障の観点からその必要性が指摘される一方で、科学技術の発展に不可欠とされる、研究成果の自由な公開やオープンな研究環境を制限するものでもある。また研究者にとっては、研究成果の公開が制限されることにより、研究が評価される機会が失

⑷⑼　Government Accountability Office, “Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight is Needed to Sustain Momentum,” GAO-11-65, 2010.11, pp.26-31. <https://www.gao.gov/assets/gao-11-65.pdf>

⑸⑽　Nicole Ogrysko, “Industry Urges DCSA to Accelerate Security Clearance Transformation Efforts,” *Federal News Network*, 2021.5.27. <https://federalnewsnetwork.com/defense-main/2021/05/industry-urges-dcsa-to-accelerate-security-clearance-transformation-efforts/>

⑸⑴　“Suitability and Security Processes Review: Report to the President,” 2014.2, p.8. Obama Whitehouse website <https://obamawhitehouse.archives.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf>

⑸⑵　例えば、国防総省では、商用データベースや連邦政府のデータベースから、クリアランス保有者の犯罪行為や疑わしい資金の移動を自動的に検出するシステムを運用している。同システムがこれらの情報を検出した場合、担当職員が当該クリアランス保有者について分析を開始することとされている（Government Accountability Office, “Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders,” GAO-18-117, 2017.11, pp.25-27. <https://www.gao.gov/assets/gao-18-117.pdf>）。

⑸⑶　“Security Executive Agent Directive 6: Continuous Evaluation,” 2018.1.12, p.2. Office of Director of National Intelligence website <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf>

⑸⑷　大統領令第 13764 号（Executive Order 13764 of January 17, 2017, *Federal Register*, vol.82 no.13, January 23, 2017, pp.8115-8129.）第 3 条 (e)、第 3 条 (h)

⑸⑸　“Trusted Workforce 2.0 and Continuous Vetting.” Defense Counterintelligence and Security Agency website <https://www.dcsa.mil/mc/pv/cv/>

⑸⑹　永野　前掲注⑵⑵, pp.154-155.

⑸⑺　連邦政府が所有しているが、大学、民間事業者等の請負人が運営する研究機関。これに対して、連邦政府が所有し運営する研究機関を政府所有・運営研究機関（Government-Owned, Government-Operated Laboratories. GOGO 機関）という（同上, pp.154-155.）。

⑸⑻　同上, pp.154-156.

われることなどの不利益が生じる[59]。そのため、米国における研究の機密指定とセキュリティ・クリアランス制度の研究者への適用については、国家安全保障と科学技術の発展のバランスをいかにとるかが課題とされてきた。

1　研究の機密指定

(1) 連邦政府資金の配分状況

連邦政府は、連邦政府が提供する研究開発費の対象を、その研究段階に応じて、「基礎研究（Basic Research）」、「応用研究（Applied Research）」、「開発（Experimental Development）」に分類している[60]。研究開発費は、連邦政府内の機関や大学、民間事業者、GOCO 機関等に配分される。このうち、基礎研究と応用研究に係る研究開発費が最も多く配分されるのは、大学である。一方、開発に係る研究開発費が最も多く配分されるのは、民間事業者である[61]。

(2) 機密指定されない研究

前述した大統領令第 13526 号は、明らかに国家安全保障と関係のない基礎的な研究の機密指定を禁じている（第 1.7 条(b)）。機密指定される研究（以下「機密研究」）の範囲に関する重要な文書が、1985 年にレーガン（Ronald Reagan）大統領が発した国家安全保障決定指令第 189 号（以下「NSDD-189」）である[62]。同指令は、連邦政府から資金の提供を受ける基礎研究及び応用研究のうち、通常その成果が研究コミュニティ内で広く公表・共有されるものを「基礎的研究（Fundamental Research）」と定義し、その成果は原則として政府による公開制限を受けないとした。一方、基礎的研究のうち、国家安全保障の観点から公開制限が必要なものは機密指定するとした。本規定は、機密指定以外の行政の裁量による公開制限を認めない趣旨でもある[63]。

前述のとおり、大学は、連邦政府から基礎研究と応用研究に係る研究開発費を最も多く配分されているが、その約 8 割は国立衛生研究所と国立科学財団からのものである[64]。両者は、研究開発費の対象となる研究について、原則としてその成果の公開は制限しないとしている[65]。また、大学は国防総省からも資金提供を受けているが、そのほとんどは基礎研究か応

59　Tricia Bishop, “Universities Balance Secrecy and Academic Freedom in Classified Work,” *Baltimore Sun*, 2013.9.13. <https://www.baltimoresun.com/education/bs-md-higher-ed-intelligence-20130911-story.html>

60　「基礎研究」とは、特定の応用や利用を考慮することなく、主に現象や観察可能な事実に潜む新たな知識の獲得を目的として実施されるものである。「応用研究」とは、基礎研究と同様に新たな知識の獲得を目的として実施されるが、主に特定の実用的な目的や目標のために行われるものである。「開発」とは、研究等から得られた知識を利用して、新たな製品・製法の生産や既存製品・製法の改良を目指すものである（Executive Office of the President Office of Management and Budget, “Preparation, Submission, and Execution of the Budget,” Circular No.A–11, 2021.8, p.3 of Section 84. <https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf>; 池上敦士「安全保障貿易管理シリーズ（第 3 回）米国における基礎研究と情報公開」『防衛技術ジャーナル』461 号, 2019.8, pp.18-24.）。

61　2019 会計年度の研究開発費においては、基礎研究に係るものの 5 割以上、応用研究に係るものの約 3 割が大学に配分された。一方、開発に係るものの 5 割以上は民間事業者に、3 割以上は連邦政府内部に配分された（“Federal Funds for Research and Development: Fiscal Years 2019–20,” Table 27, 39, 51. National Science Foundation website <https://ncses.nsf.gov/pubs/nsf21329>）。

62　“National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical and Engineering Information,” 1985.9.21. National Archives website <https://catalog.archives.gov/id/6879779>

63　*ibid.*

64　“Federal Funds for Research and Development: Fiscal Years 2019–20,” *op.cit.*(61), Table 27, 39.

65　US Department of Health and Human Services National Institutes of Health, “NIH Grants Policy Statement,” 2021.4, p. IIA-118. <https://grants.nih.gov/grants/policy/nihgps/nihgps.pdf>; National Science Foundation, “Grant General Conditions,” 2021.10.4, p.32. <https://www.nsf.gov/bfa/dias/policy/gc1/oct21.pdf>

用研究に係るものであり、例外を除き、機密指定されて公開を制限されることはないとされる(66)。

(3) 機密指定される研究

連邦政府だけでなく大学や民間事業者の研究者も参加し、初めて大がかりに実施された機密研究は、第二次世界大戦時の原子爆弾の開発計画、通称マンハッタン計画であるとされる(67)。今日、核兵器の備蓄等に関する機密研究は、ローレンス・リバモア国立研究所やロス・アラモス国立研究所等、エネルギー省が所管し民間事業者が運営するGOCO機関で実施されている(68)。

また、国防総省は、資金提供した研究開発プロジェクト等に係る機密指定マニュアルの中で、当該プロジェクトが国家的優位性（National Advantage）をもたらす場合、機密指定の対象になり得るとしている。そして、その際の判断基準として、当該プロジェクトの内容やその一部を構成する特定の技術情報等が漏えいした場合に、米国の外交や経済、軍事活動に悪影響を及ぼすか否か、また当該プロジェクトや技術情報等の存在や成果が、外国政府による対抗策の開発等を惹起するか否か等を挙げている(69)。

2　大学の対応

研究機関のうち、教育機関でもあり、研究成果の自由な公開とともに、研究者間の活発な交流や国籍にとらわれない研究者の登用等、オープンな研究環境を重視する大学については、これに相反する機密研究への関わり方が問題とされてきた。各大学は、機密研究に対するガイドライン等を定めているが、多くの有力大学は、キャンパス内での機密研究の実施を許可していないとされる(70)。一方で、大学が運営するGOCO機関等、一般のキャンパスから物理的に離れた施設等では機密研究が実施されている場合がある(71)。こうした場合、大学は、行政機関から秘密取扱施設許可を受けるほか、これに従事する研究者及び学長等の幹部職員にセキュリティ・クリアランスの取得を求めている(72)。

---

(66) 岡村浩一郎「米国の大学における国防研究―国防研究費による大学研究支援の枠組み―」国立国会図書館調査及び立法考査局編『冷戦後の科学技術政策の変容―科学技術に関する調査プロジェクト2016報告書―』（調査資料2016-4）国立国会図書館, 2017, pp.109-111, 118. <https://dl.ndl.go.jp/view/download/digidepo_ 10314918 _po_ 20170309.pdf?contentNo=1>

(67) Quist, *op.cit.*(7), pp.78-79.

(68) James L. Schoff et.al., “A High-Tech Alliance: Challenges and Opportunities for U.S.-Japan Science and Technology Collaboration,” 2021.7, pp.11-12. Carnegie Endowment for International Peace website <https://carnegieendowment.org/files/Schoff_etall%20U.S.-Japan_final.pdf>

(69) Department of Defense, “Subject: Instructions for Developing Security Classification Guides,” *Manual*, no. 5200.45, 2020.9.15, pp.13-14, 20-22. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520045 m.pdf?ver=2018-04-06-075606-737> 具体的に国防総省が進めている機密研究の事例として、最近では、敵国による核兵器搭載可能なミサイルの発射をAIを用いて予測するシステムの開発研究が報じられた（Phil Stewart, “Deep in the Pentagon, a Secret AI Program to Find Hidden Nuclear Missiles,” *Reuters*, 2018.6.5. <https://jp.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J>）。

(70) Rory Truex, “Addressing the China Challenge for American Universities,” 2020, pp.1-3. Johns Hopkins Applied Physics Laboratory website <https://www.jhuapl.edu/Content/documents/Truex-STEM.pdf>

(71) 下田隆二「米国主要大学の研究公開ポリシーについて」（日本学術会議　第7回安全保障と学術に関する検討委員会　参考資料2）2016.12.16. 日本学術会議ウェブサイト <http://www.scj.go.jp/ja/member/iinkai/anzenhosyo/pdf23/anzenhosyo-siryo7-sanko2.pdf> 例えば、マサチューセッツ工科大学は、キャンパス内では機密研究をしないことを一般的なポリシーとする一方（同, p.3）、GOCO機関であるリンカーン研究所では機密研究を実施している（“Working with Lincoln Laboratory.” Massachusetts Institute of Technology Office of the Vice President for Research website <https://research.mit.edu/integrity-and-compliance/export-control/working-lincoln-laboratory>）。

3　1980年代以降の機密研究の経緯

(1) NSDD-189の背景

冷戦下の1980年代初頭、軍事関連を含む様々な分野において米国とソ連の技術力の差が急速に縮まっていること、それらが、非合法な手段によるものも含む米国からの技術流出によって起きていることが指摘され、大学等の研究機関における対策を強化する必要があるとする意見が挙がった(73)。これに対して、1982年、全米科学アカデミー等が設置した研究者委員会は、大学や研究者の交流を通じた技術流出は非常に限定的であり、大学で実施される基礎研究及び応用研究は、原則的に機密研究とするべきではないとした。一方、同委員会は、明らかに短期間で装備品に転用され得る等の諸要件を満たす研究は機密指定するべきであるが、これらを大学が実施する場合は一般のキャンパス外の施設で実施するべきであると提言した(74)。前述のNSDD-189は、この報告を受けて発出されたものである(75)。

(2) 対テロ対策と機密研究等の拡大

2001年9月の同時多発テロ以降、新たなテロの発生を防ぐ観点から、連邦政府による機密指定権限が強化された(76)。また、機密指定されない研究についても、連邦政府が、研究成果の公開や外国人研究者の参加に制約を課すことが増えたとされる(77)。

特に、2001年秋に米国で発生した炭疽菌事件(78)を契機として、病原性微生物等の生物剤や毒素を用いたバイオテロ対策の観点から、生命科学分野における機密研究の在り方が問題となった。従来、生命科学は機密研究の主要な対象とはされてこなかった(79)が、遺伝子操作技

---

(72) 例えば、カリフォルニア大学は、総長室が定める機密研究の実施に関する規則において、機密指定された業務を遂行する者や学長等の幹部職員に対して、セキュリティ・クリアランスの取得を求めている（永野　前掲注(22), pp.152-153.）。

(73) Jason E. Thomas et al., "Recommendations to Address Government Concerns Regarding Intellectual Property Theft from American Research Universities by China and Other Foreign Entities while Preserving the Process of Fundamental Research," 2019.4.21, pp.63-69. Texas A&M University website <https://oaktrust.library.tamu.edu/bitstream/handle/1969.1/187023/PSAA%20676%20Cap%202%20-%20AAU%20Report%20Final%20Draft%20Spring%202019%20Gamache.pdf?sequence=1&isAllowed=y>

(74) Panel on Scientific Communication and National Security et al., "Scientific Communication and National Security," Washington, D.C.: National Academy Press, 1982, pp.1-2, 5. <https://www.nap.edu/read/253/chapter/2>; 岡村　前掲注(66), p.117.

(75) "National Security Decision Directive No. 189 : National Policy on the Transfer of Scientific, Technical and Engineering Information," *op.cit.*(62)

(76) 2003年3月、ブッシュ大統領は、当時機密指定制度を規定していた大統領令を改正した。それまで、機密指定の対象となる事項の一つとして「国家安全保障に関連する科学的、技術的又は経済的事項に関する情報」が挙げられていたが、同改正により、「国境を超えるテロリズムからの防衛に関するものを含む」とする文言が追加された。なお、現在機密指定制度を規定している、2009年12月に発出された大統領令第13526号では、テロリズムに関する文言はなく、同改正以前と同様の文言となっている（前掲注(5)参照。）。また、ブッシュ大統領は、2001～2002年に、それまで機密指定権限がなかった行政機関の長に対して、相次いで同権限を与えた。その中には、多くの研究開発費を大学等に提供する国立衛生研究所を所管する保健福祉長官も含まれた（Genevieve J. Knezo, ""Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information," *CRS Report for Congress*, RL33303, 2006.12.29, p.3. Federation of American Scientists website <https://sgp.fas.org/crs/secrecy/RL33303.pdf>）。

(77) Council on Governmental Relations and Association of American Universities, "Restrictions on Research Awards: Troublesome Clauses 2007/2008," 2008.7, p.21. Columbia University website <https://research.columbia.edu/sites/default/files/content/RCT%20content/Export%20Controls/COGR_AAU_TroublingClauses_2007_2008.pdf>

(78) 2001年9～11月、致死性の高い炭疽菌の乾燥胞子が入った手紙がテレビ局や新聞社、上院議員事務所に送られ、郵便局員や病院職員ら5人が死亡し、17人に呼吸困難などの感染症状が出た事件（「炭疽菌　謎残る幕引き　自殺した米研究者の単独犯と断定　物証・動機、決め手なし」『朝日新聞』2008.8.21.）。

(79) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism*, Washington, D.C.: National Academies Press, 2004, p.100. <https://www.nap.edu/read/10827/chapter/1>

術の進歩等により、これらの技術がテロリストに悪用される危険性が指摘されるようになった[80]。これに対して、全米研究評議会に設置された研究者委員会は、これまで公開の原則の下に研究が進められてきた生命科学分野において研究の機密化を進めることは、若手研究者の他分野や他国への流出を招き、バイオテロ対策に限らず感染症対策等に係る研究開発にも悪影響が出ると指摘した[81]。

その後、2008年8月に司法省が前述の炭疽菌事件は陸軍の研究所に所属する研究者によるものだったと断定した[82]ことを受けて、指定生物剤・毒素を取り扱う研究者の身上調査[83]の強化が課題となった。その際、前述の研究者委員会の提言に応じて連邦政府に設置された、研究者による諮問機関「国家バイオセキュリティ科学諮問委員会」は、指定生物剤・毒素を取り扱う研究者に対して、例えばセキュリティ・クリアランスで実施されているような身上調査を実施することとした場合、他分野への研究者の流出を招くおそれがあると指摘した[84]。その後、身上調査の強化は、指定生物剤・毒素のうち、悪用された場合に特に大きな被害をもたらすおそれがあるものを取り扱う研究者のみを対象として実施することとされた[85]。これは、バイオテロ対策と研究開発の推進とのバランスをとったものと評されている[86]。

(3) 近年の新興技術等を巡る議論

近年、米国は、技術覇権をめぐる中国との対立の中で、国家安全保障上重要な技術の流出防止策を強化しており、例えば輸出管理[87]においては、「新興技術（Emerging Technologies）」[88]や「基盤的技術（Foundational Technologies）」を新たな管理の対象とすることとした。前者にはAIや量子科学技術等が、後者には半導体製造装置等が対象になり得るとされ[89]、これらに係る研究については今後、機密指定も進むとする指摘がある[90]。一方で、特に新興技術につ

---

80 小林靖「バイオセーフティ、バイオセキュリティとデュアルユース」四ノ宮成祥・河原直人編著『生命科学とバイオセキュリティ―デュアルユース・ジレンマとその対応―』東信堂, 2013, p.51.

81 Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *op.cit.*79, pp.99-101.

82 『朝日新聞』前掲注78

83 2001年の炭疽菌事件以降、公衆衛生と安全に深刻な脅威を与え得る指定生物剤・毒素を取り扱う研究者の欠格要件（1年を超える拘禁刑の犯罪歴、違法薬物の使用、不法滞在、精神障害等）が定められ、指定生物剤・毒素を取り扱う研究者は、FBIが電子記録のチェック等によって実施する「セキュリティ・リスク評価」を受けることとされていた（Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *op.cit.*79, pp.53, 58; "FSAP Security Risk Assessments FAQs." Department of Health and Human Services website <https://www.hhs.gov/guidance/document/fsap-security-risk-assessments-faqs>）。

84 National Science Advisory Board for Biosecurity, "Enhancing Personnel Reliability among Individuals with Access to Select Agents," 2009.5, pp.6, 10. <https://osp.od.nih.gov/wp-content/uploads/NSABB_Final_Report_-on_-PR-5-29-09.pdf>

85 指定生物剤・毒素のうち、悪用された場合に特に大きな被害をもたらすおそれがある「Tier 1」に指定されたものを取り扱う研究者は、前掲注83の「セキュリティ・リスク評価」に加え、各研究機関が実施する「適性評価」を受けることとされた。同評価では、住所歴や犯罪歴、同僚等へのインタビューに基づく情報のほか、必要に応じて信用調査情報や薬物検査を活用することも認められている（Center for Disease Control and Prevention, Animal and Plant Health Inspection Service, "Suitability Assessment Program Guidance," 2017.3, pp.4-7. <https://www.selectagents.gov/compliance/guidance/suitability/docs/Suitability_Guidance.pdf>）。

86 Gregory D. Koblentz, "From Biodefense to Biosecurity: the Obama Administration's Strategy for Countering Biological Threats," *International Affairs*, vol.88 no.1, 2012.1, p.143.

87 輸出管理とは、武器や軍事転用可能な貨物・技術が、自国及び国際社会の安全性を脅かす国家やテロリスト等、懸念活動を行うおそれのある者に渡ることを防ぐため、貨物の輸出、技術の提供を管理する制度を指す（森本正崇「輸出管理の概要（1）輸出管理とは・国際輸出管理レジーム」『貿易と関税』757号, 2016.4, pp.75-79.）。

88 一般に、新興技術とは、新規であるとともに、その成長スピードが速く、社会経済に対して潜在的に大きな影響を有する技術を指す（岸本充生「新興技術を社会実装するということ」国立国会図書館調査及び立法考査局編『ゲノム編集の技術と影響―科学技術に関する調査プロジェクト2020報告書―』（調査資料2020-5）国立国会図書館, 2021, pp.102-103. <https://dl.ndl.go.jp/view/download/digidepo_11656216_po_20200508.pdf?contentNo=1>）。

いては、もともと民間で汎用性のある技術として開発されたものであり、国家が開発を主導しこれを管理していくことは困難な面があるとされる(91)。また、新興技術は、既に様々な研究分野においてNSDD-189が規定する基礎的研究の中に浸透しており、この中から管理を強化すべき分野を切り分けて特定することは困難とする指摘もある(92)。

トランプ大統領は、2021年1月の大統領覚書の中で、行政機関や研究機関に対して、研究の機密化を含む現行の技術の流出防止策に対して改めて認識を深めるよう求めた。その一方で、連邦政府が資金を提供する研究開発の多くは、NSDD-189が規定する基礎的研究のように広く共有されるものであり、こうした研究開発の公開性と共同性は、米国におけるイノベーションの推進や国家安全保障に寄与するものであるとした(93)。同覚書は、バイデン（Joe Biden）政権も引き継いでいる(94)。

Ⅲ　日本の適性評価制度と研究者を対象とする新たな制度に関する議論

日本では、特定秘密保護法に基づき、特定秘密を取り扱う行政機関の職員等を対象に、セキュリティ・クリアランスに相当する(95)適性評価が実施されている。Ⅲでは、本制度の概要を紹介した上で、現在政府が検討を進めているとされる、研究者を対象とするセキュリティ・クリアランス制度の必要性に関する議論について整理する。

1　特定秘密保護法に基づく適性評価制度

(1) 特定秘密の指定

特定秘密保護法に基づき、行政機関の長(96)は、同法が規定する事項（防衛・外交・特定有

---

(89) 2018年8月、「2019会計年度国防授権法」（John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub.L. No.115-232, 132 Stat. 1636(2018).）の一部として、「輸出管理改革法」（Export Control Reform Act of 2018: ECRA）が成立した（50 U.S.C. §§ 4801 et seq.）。商務省は、同法に基づき新たに輸出管理の対象となり得る新興技術の代表的な分野として、①バイオテクノロジー、② AI・機械学習技術、③測位技術、④マイクロプロセッサー技術、⑤先進コンピューティング技術、⑥データ分析技術、⑦量子情報・量子センシング技術、⑧物流関連技術、⑨付加製造技術（3Dプリンティング等）、⑩ロボット工学、⑪ブレインコンピュータインターフェース、⑫極超音速技術、⑬先端材料、⑭先進監視技術を挙げた（"Review of Controls for Certain Emerging Technologies," *Federal Register*, vol.83 no.223, 2018.11.19, pp.58201-58202. <https://www.govinfo.gov/content/pkg/FR-2018-11-19/pdf/2018-25221.pdf>）。また同省は、基盤的技術については、半導体製造装置等が対象となり得るとした（"Identification and Review of Controls for Certain Foundational Technologies," *Federal Register*, vol.85 no.167, 2020.8.27, pp.52934-52935. <https://www.govinfo.gov/content/pkg/FR-2020-08-27/pdf/2020-18910.pdf>; 角田昌太郎「各国の輸出管理と対内直接投資管理をめぐる動向」『レファレンス』845号, 2021.5, pp.35-36. <https://dl.ndl.go.jp/view/download/digidepo_11673568_po_084502.pdf?contentNo=1>）。

(90) Schoff et.al., *op.cit.*(68), p.6. 例えば、量子科学技術に係る研究の機密化が進む可能性が指摘されている（永野秀雄「米国における科学者・技術者に対するセキュリティクリアランス―量子情報科学を中心に―（下）」『CISTEC journal』193号, 2021.5, pp.255-258.）。

(91) 鈴木一人「研究レポート　米中の技術覇権争いと安全保障」2021.1.8. 日本国際問題研究所ウェブサイト <https://www.jiia.or.jp/column/post-30.html>

(92) JASON and The MITRE Corporation, "Fundamental Research Security," 2019.12, p.32. National Science Foundation website <https://www.nsf.gov/news/special_reports/jasonsecurity/JSR- 19 - 2 IFundamentalResearchSecurity_ 12062019 FINAL.pdf>

(93) "National Security Presidential Memorundum-33 : Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," 2021.1.14. Trump Whitehouse website <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>

(94) Eric Lander, "Clear Rules for Research Security and Researcher Responsibility," 2021.8.10. Whitehouse website <https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/>

(95) 小林　前掲注(2), p.235.

害活動[97]の防止・テロリズムの防止）[98]に関する情報であって、公になっていないもののうち、その漏えいが安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるものを「特定秘密」として指定する（第3条第1項）。また同法は、特定秘密を取り扱う者が業務により知得した特定秘密を漏らした場合、10年以下の懲役等に処する（第23条第1項）等の罰則を規定している。

(2) 適性評価制度

特定秘密保護法は、特定秘密を取り扱う業務に従事する者を、適性評価[99]によって特定秘密を漏らすおそれがないと認められた者に限定している（第11条）[100]。行政機関の長は、当該行政機関の職員及び当該行政機関から業務を請け負う「適合事業者」[101]の従業員が、新たに特定秘密を取り扱う業務に従事することが見込まれる場合、適性評価を実施する（第12条第1項第1号）。適性評価は、本人の同意を得て実施することとされ（第12条第3項）、評価対象者及び知人その他の関係者への質問や公私の団体への照会（第12条第4項）等によって実施される[102]。適性評価から5年を経過し、当該職員等が引き続き特定秘密を取り扱うことが見込まれる場合、当該職員等に対して再び適性評価が実施される（第12条第1項第2号）。評価対象者は、適性評価の結果等について、行政機関の長に対して書面で苦情を申し出ることができる。苦情の申出を受けた行政機関の長は、これを誠実に処理し、評価対象者に処理の結果を通知しなければならない（第14条）。

特定秘密保護法の制定に際して、適性評価制度については、プライバシーに関わる情報が評価されることにより評価対象者が過度に萎縮することや、適性評価を受けることに同意しなかった者が人事上不利益を受ける可能性があること、調査事項とされた精神疾患に対する偏見を生むおそれがあること等が指摘された[103]。一方、制度の開始後には、適性評価の結果、適

---

(96) 内閣法制局、消費者庁、文部科学省、農林水産省、水産庁、国土交通省、気象庁及び環境省の長はこの対象とはなっていない（「特定秘密の保護に関する法律施行令」（平成26年政令第336号）第2条）。

(97) 特定有害活動とは、いわゆるスパイ活動や、大量破壊兵器関連物資の拡散を助ける活動など、外国の利益を図る目的で行われ、かつ、我が国及び国民の安全を著しく害し、又は害するおそれのある活動をいう（内閣官房特定秘密保護法施行準備室「特定秘密の保護に関する法律【逐条解説】」2014.12.9, pp.92-93. <https://www.cas.go.jp/jp/tokuteihimitsu/pdf/bessi_kaisetsu.pdf>）。

(98) 特定秘密保護法別表は、4事項のうち特定秘密となり得る情報について、さらに細目を規定している。

(99) 2009年4月、「カウンターインテリジェンス機能の強化に関する基本方針」（平成19年8月9日カウンターインテリジェンス推進会議決定）に基づき、行政機関の職員を対象に、「特別管理秘密」の取扱いに係る適性を評価する制度が導入された。特定秘密保護法の制定に至る検討に際しては、同制度の課題として、法令上の位置付けが必ずしも明確でないこと、行政機関から業務を請け負う民間事業者等の職員が対象となっていないこと等が挙げられ、適性評価制度を秘密保全のための法制の中で明確に位置付け、必要な規定を設けることの重要性が指摘された（秘密保全のための法制の在り方に関する有識者会議「秘密保全のための法制の在り方について（報告書）」2011.8.8, pp.8-9. 首相官邸ウェブサイト <https://www.kantei.go.jp/jp/singi/jouhouhozen/dai3/siryou4.pdf>）。

(100) 行政機関の長や副大臣、大臣政務官等は、適性評価を受けることなく、特定秘密を取り扱うことができる（同条）。また、制度の運用を常時監視するために両院に設置された情報監視審査会に所属する国会議員（各8名）に対しては、適性評価を行わない代わりとして、審査会に提出された特定秘密を他に漏らさない旨宣誓することが義務付けられている（「衆議院情報監視審査会規程」（平成26年6月13日議決）第4条第1項；「参議院情報監視審査会規程」（平成26年6月20日議決）第4条第1項；青井未帆ほか『逐条解説特定秘密保護法』日本評論社, 2015, p.289.）。

(101) 物件の製造又は役務の提供を業とする者で、特定秘密の保護のために必要な施設設備を設置していることその他政令で定める基準に適合する事業者。行政機関の長は、特段の必要があると認めたときは、適合事業者と契約を締結し、特定秘密を提供したり保有させたりすることができる（第5条第4項、第8条第1項）。

(102) 適性評価において調査事項となるのは、特定有害活動及びテロリズムとの関係に関する事項（評価対象者の家族及び同居人の氏名、生年月日、国籍及び住所を含む。）、犯罪及び懲戒の経歴に関する事項、情報の取扱いに係る非違の経歴に関する事項、薬物の濫用及び影響に関する事項、精神疾患に関する事項、飲酒についての節度に関する事項、信用状態その他の経済的な状況に関する事項である（第12条第2項）。

性が認められなかった事例は僅かであったことから、実効性に対して疑問の声が挙がっている[104]。

2020年中の適性評価の実施件数は、約6万件である。2020年末時点で、特定秘密を取り扱う業務を実施することができる者の数は約13万人であるが、このうち、適合事業者の従業員は約3千人である[105]。

2　研究者を対象とする新たな制度に関する議論

(1) 政府による検討

2019年10月、経済産業省に設置された産業構造審議会通商・貿易分科会安全保障貿易管理小委員会（以下「経産省小委員会」）は、国家安全保障上重要な機微技術[106]の管理の在り方について、中間報告をまとめた。同委員会は、その中で、国内の機微技術を「育てる」ための施策の一つとして国際共同研究の推進を挙げた。一方で、日本では特定秘密に該当しない機微技術に係る情報の保全制度が不十分であり、相手国が保有する機微技術に係る情報の保全が担保できず、機微技術に関する国際共同研究に参加できないおそれがあるとして、セキュリティ・クリアランス制度を含む産業保全策の強化を検討するべきであるとした。また、機微技術を「守る」ために、政府から資金の提供を受けた研究に関して、機微技術に係る研究成果の公開の在り方について、公開の制限を含めて検討する必要があるとした[107]。

その後、2020年8月、政府が、国際共同研究の推進を目的として、AI等の新興技術を扱う研究者の信用度を保証する資格制度の新設について検討していることが報じられた。報道によれば、政府は、研究者本人の申請に応じて、政府が身上調査を実施し研究者に資格を付与する仕組みを検討しているとされた。また、新制度は特定秘密保護法の適性評価制度とは切り離し、「民間人への信用保証の提供に徹した仕組み」を目指すとされており、「科学技術・イノベーション創出の活性化に関する法律」（平成20年法律第63号）を改正する案が有力と報じられた[108]。

---

(103)「官民の数万人対象　「適性評価」に批判　精神疾患の治療歴など調査」『朝日新聞』2014.8.25.

(104)「特定秘密取り扱い　資格者急増12万人　漏えいリスク懸念」『毎日新聞』2018.5.24. 2020年中に実施された適性評価のうち、特定秘密を漏らすおそれがないと認められなかったのは1件だった（「特定秘密の指定及びその解除並びに適性評価の実施の状況に関する報告」2021.6, p.10. 内閣官房ウェブサイト <https://www.cas.go.jp/jp/tokuteihimitsu/pdf/r03_0611_houkoku.pdf>）。

(105)「特定秘密の指定及びその解除並びに適性評価の実施の状況に関する報告」同上, pp.10-11, 23-24. 適正評価を受けた適合事業者の従業員のうち大部分は、内閣官房、防衛省、防衛装備庁のいずれかの長による適正評価を受けた（同, p.24.）。2020年の適性評価の実施件数は、前年（約2万件）と比べて大幅に増加したが、これは前回の適性評価から5年を経過する者に対して、再度適性評価を実施したことによるものとされる（同, p.11.）。

(106)　同委員会は、「機微技術」を、「我が国の安全保障を確保し、もって経済の健全な発展を実現する上で、その優位性を保ち、脆弱性を解消すべき重要な技術」と定義している（「産業構造審議会通商・貿易分科会安全保障貿易管理小委員会中間報告」2019.10.8, p.4. 経済産業省ウェブサイト <https://www.meti.go.jp/shingikai/sankoshin/tsusho_boeki/anzen_hosho/pdf/20191008001_01.pdf>）。

(107)　同上, pp.18-20. 自由民主党政務調査会新国際秩序創造戦略本部は、国家安全保障の観点から保全と育成をすべき分野を速やかに指定し、技術優越の確保・維持を図るべき具体的な重要技術を特定する必要性を指摘した。そして、これらの技術のうち機微な技術に関しては、「政府資金が投入された研究開発成果の公開のあり方」や「機微情報の取扱いに係る資格のあり方（セキュリティ・クリアランス）」に関する検討を進めるべきであると指摘した（自由民主党政務調査会新国際秩序創造戦略本部「提言「経済安全保障戦略」の策定に向けて」2020.12.16, pp.15-16. <https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/201021_1.pdf>）また、有識者からは、サイバーセキュリティの観点から、日本の民間事業者が外国政府等の保有する機微な脆弱性情報にアクセスすることができるよう、民間事業者を対象とするセキュリティ・クリアランス制度が必要であるとする指摘がある（國分俊史「主要国で日本にだけ存在しないセキュリティクリアランス制度　米国が日本のIoT製品に押す「脆弱」の烙印」『Wedge』352号, 2018.8, pp.54-56.）。

(108)「「技術漏らさぬ人材」国が保証　欧米並みの資格　創設方針」『朝日新聞』2020.8.13;「先端情報共有に「資格」研究者ら　秘密保持保証」『日本経済新聞』2020.8.28.

(2) 主な論点

研究者を対象とする新たな制度については、身上調査を実施する予算や人員の確保といった実施に際しての課題[109]のほか、以下のような論点がある。

(ⅰ) 国際共同研究の推進

Ⅱ-3(3)で前述したように、近年、米国は、技術覇権をめぐる中国との対立の中で、国家安全保障上重要な技術の流出防止策を強化している。一方で日米両国は、国際共同研究の推進によって、これらの技術を育成することを目指している。例えば、両国は、2021年4月の首脳会談において「日米競争力・強靱性（コア）パートナーシップ」に合意し、この中でAIや量子科学技術等の研究開発で協力していくことを確認した[110]。また、日本政府は、「第6期科学技術・イノベーション基本計画」（令和3年3月26日閣議決定）の実行計画として位置付けられる「総合イノベーション戦略2021」（令和3年6月18日閣議決定）において、総合的な安全保障や科学技術外交の推進の観点から、国際共同研究を戦略的に推進するとしている[111]。

これに関し、日本が国際共同研究を推進するに当たって、米国等の国際共同研究の相手国から、研究者を対象とするセキュリティ・クリアランス制度の新設を含む、技術の流出防止策の強化が求められる可能性があるとする指摘がある[112]。

政府が関わる国際共同研究における機密情報の共有手続として、例えば米国防総省は、同省が作成・保持する機密情報を開示する手続を定めている。同手続では、開示を検討する際に、セキュリティ・クリアランス制度を含む相手国の法制度等を検証することにより、当該国の機密保全能力を審査することとしている。また、同手続では、当該機密情報にアクセスする相手国の個人に対して、当該国の政府によって認められたセキュリティ・クリアランスの保有を求めている[113]。このように、政府が関わる国際共同研究においては、研究者を対象とするセキュリティ・クリアランス制度の存在が、機密情報の円滑な共有に寄与するとする指摘がある[114]。

また、例えば民間事業者が民間資金によって共同研究を実施するケースなど大統領令第13526号に基づく機密研究とはならない場合においても、米国の大学や民間事業者は、自主的な経営判断として機微技術の管理強化に動いているとされ、日本の大学や民間事業者が国際共同研究のパートナーから排除されないようにするためには、機微技術を取り扱う研究者に対するセキュリティ・クリアランス制度が必要であるとする指摘がある[115]。

---

(109) 『日本経済新聞』同上

(110) 「日米競争力・強靱性（コア）パートナーシップ」p.1. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/files/100194418.pdf>

(111) 「統合イノベーション戦略2021」（令和3年6月18日閣議決定）pp.9, 12-13. 内閣府ウェブサイト <https://www8.cao.go.jp/cstp/tougosenryaku/togo2021_honbun.pdf> 政府が関わる国際共同研究の仕組みの一例として、「戦略的国際共同研究プログラム」（SICORP）がある。同プログラムは、文部科学省及び科学技術振興機構が、相手国の政府機関等と合意・協力の上、それぞれの国で研究者からの提案申請を募り、共同研究を支援するものである（「国際共同研究って何しているの？」科学技術振興機構ウェブサイト <https://www.jst.go.jp/inter/aboutsicorp.html>）。

(112) 例えば、量子科学技術分野では、2019年12月に日本と米国が署名した「量子協力に関する東京声明」において、同分野における協力を進めるための方策の一つとして、研究セキュリティを推進する誠実な協力に着手することが盛り込まれている。この「研究セキュリティ」には、セキュリティ・クリアランス制度を適用することが含まれるとする指摘がある（永野　前掲注(22), p.150.）。

(113) "Chapter 3: National Disclosure Policy," *International Programs Security Handbook*, 2010.4, pp.3-2, 3-7-3-10. Defense Security Cooperation University website <https://www.dscu.mil/documents/publications/international_programs_security_handbook/Chapter3_04052010.pdf>

(114) Schoff et.al., *op.cit.*(68), pp.9-10, 40.

(115) 細川昌彦「企業も大学も「機微技術」の管理を急げ　米中技術覇権で問われる「アクセス天国・日本」の対応」『中央公論』1636号, 2020.3, pp.123-124.

（ⅱ）特定秘密保護法との関係

Ⅱの冒頭で前述したように、米国においてセキュリティ・クリアランスは、研究者が、連邦政府から資金の提供を受けて、政府が機密指定した研究を実施する場合に必要とされるものである。日本でもこれと同様の制度とする場合、特定秘密保護法の適性評価制度を研究者に適用することも考えられる。現在の特定秘密保護法は、特定秘密の対象となり得る研究開発を防衛・外交・特定有害活動の防止・テロリズムの防止に係るものとしているが、例えば、これを米国の大統領令第 13526 号のように、より包括的に国家安全保障に関連する科学技術を対象とすることも提案されている(116)。また、現行制度においても独立行政法人等（国立研究開発法人、国立大学法人等）は適合事業者になり得るとされる(117)。一方、Ⅱ-3(3)で前述したように新興技術はもともと民間で開発されたものであるが、現行の特定秘密保護法が対象とするのは基本的に行政機関が保有する情報であるとされる(118)。

政府は新たな資格制度を特定秘密保護法の適正評価制度とは切り離したものとすることを検討しているとされるが、その理由として、特定秘密の対象範囲が広がる場合や、大学等が適合事業者となり、研究者のみならず学長等に対して適性評価を実施する必要が生じる場合に(119)、世論や大学等の反対が予想されることが指摘されている(120)。

（ⅲ）罰則規定や民間人のプライバシーに関わる情報を国が収集することの是非

政府が検討していると報じられた新たな資格制度については、情報を漏えいした者に対する罰則の導入が検討されているとされる(121)。米国等では民間人にも罰則が適用されており、「国際的な潮流からいえば、罰則適用は致し方ない」とする指摘がある(122)一方、「共同研究を促進する法律に罰則はそぐわない」とする指摘もある(123)。また、研究者本人の申請を前提とするとされているものの、身上調査において民間事業者の従業員も含む研究者のプライバシーに関わる情報を国の機関が収集するべきなのか、検討が必要とする指摘がある(124)。

（ⅳ）研究成果の公開の在り方

2019 年 10 月の経産省小委員会の中間報告は、政府から資金の提供を受けた研究等に関して、機微技術に関する研究成果の公開の在り方について検討する必要があるとした。米国の機密研究をめぐる議論にも見られたように、研究成果の公開は、研究開発の進展に資するものであり、研究機関が公開の制限という判断をすることは難しいとする指摘がある(125)。

---

(116)　Schoff et.al., *op.cit.*(68), p.39. なお、現在の特定秘密保護法においても、特定秘密に指定され得る情報の事項を示した同法別表には、防衛・外交・特定有害活動の防止・テロリズムの防止の各事項に関係する研究開発が規定されている。例えば、量子科学技術を用いてこれらの事項に関係する暗号技術を開発した場合、当該暗号技術は特定秘密の対象となり得るとする指摘がある（永野　前掲注(22), p.152.）。

(117)　内閣官房特定秘密保護法施行準備室　前掲注(97), pp.69-70.

(118)　第 204 回国会衆議院経済産業委員会議録第 13 号　令和 3 年 5 月 14 日　p.5.

(119)　適合事業者の要件の一つとして、特定秘密の保護のために必要な施設設備を設置していることがある。そのため、大学が適合事業者となる場合、施設設備について管理権を有する学長や総長、施設担当理事等にも適性評価を実施する必要が生じるとする指摘がある（永野　前掲注(22), p.152.）。

(120)　同上, p.152;『朝日新聞』前掲注(108)

(121)　『日本経済新聞』前掲注(108)

(122)　小谷賢「対中防諜と秘密保全体制の強化を」『Voice』518 号, 2021.2, p.58.

(123)　『日本経済新聞』前掲注(108)

(124)　小谷　前掲注(122), p.58.

(125)　「G7、研究データ流出防止　中国念頭 指針策定で合意へ　軍事転用を警戒」『日本経済新聞』2021.6.9.

（v）対象となる技術

2019年10月の経産省小委員会の中間報告は、保全制度が不十分である情報として、特定秘密に該当しない機微技術に係る情報を挙げている(126)。また、政府が検討していると報じられた新たな資格制度については、その対象となり得る技術の例として、AIや量子科学技術が挙げられている(127)。今後、制度の対象となる技術の範囲をどのように設定するのかが課題となる。

おわりに

これまで見てきたように、米国では、連邦政府から資金の提供を受け、機密研究を実施する研究者に対して、セキュリティ・クリアランスを実施してきた。研究の機密指定とセキュリティ・クリアランスの実施は、国家安全保障上重要な技術の流出防止策としてその必要性が指摘されている。一方で、研究コミュニティを中心に、科学技術の発展の観点から、研究成果の公開やオープンな研究環境の重要性を指摘する声もある。そのため、これまでの冷戦や同時多発テロを契機とした機密研究やセキュリティ・クリアランスの在り方に関する議論においては、国家安全保障と科学技術の発展のバランスをいかにとるかが課題とされてきた。

近年の技術覇権をめぐる米中対立を背景に、国家安全保障上重要な技術の流出防止策の強化が課題となる中、日本では、研究者を対象とするセキュリティ・クリアランス制度の新設が議論されている。同制度により、国際共同研究の推進や技術の流出防止が期待される一方で、罰則規定等、同制度には慎重な検討を要する事項も含まれる。また、制度設計の仕方によっては、研究成果の公開やオープンな研究環境を制限する可能性もあり、その対象となる技術の範囲をどのように設定するのかも課題となろう。研究者を対象とするセキュリティ・クリアランス制度については、米国における議論も踏まえ、国家安全保障と科学技術の発展の双方の観点からの検討が必要とされる。

（ふくだ　たけし）

(126)　産業構造審議会通商・貿易分科会安全保障貿易管理小委員会　前掲注(106), p.19.
(127)　『日本経済新聞』前掲注(108)