

米国における大学等の学術研究機関 における研究の規則

機密研究(Classified Research)と
基礎研究(Fundamental Research)

渡部 俊也

東京大学未来ビジョン研究センター 教授

アラ・タマシアン

ハーバード大学 コンプライアンスオフィサー

概要

米国の大学は伝統的に自由でオープンな研究環境を重視してきた。オープンで制限のない研究遂行を可能にすることにより、知識の創造と普及、その迅速な公開が可能となる。そして、このようなオープンな学術研究から得られた結果の公表により、科学者コミュニティはそれらの知見を検証し、科学を進歩させることができる。このためほとんどの大学は、政府によって安全保障関連の研究として分類されているものや、研究成果公開に何等か制限が課された企業からの研究費などの研究プロジェクトは、原則的には受け入れていないとしている。

他方、米国の大学では、特定の情報の開示に制限を加えたプロジェクトであっても、一定の条件下で受け入れている。このような研究については、規制研究：Restricted Research と称し、その中に、秘密情報の守秘義務や、個人情報の保護などを前提とする、企業からの委託研究や、政府による防衛分野の機密研究の委託なども含まれる。米国の各大学はそのような制限の課される研究プロジェクトについて、大学ごとに受け入れ方針を定め対外的に公表している。

本稿では、これらの米国大学における Restricted Research について、成果公開の制約がない Fundamental Research と対比させ、その位置づけや取扱い方針についてまとめる。特に最近日本で制度導入が検討されている所謂 Security Clearance に関係して、Restricted Research の一部をなす機密研究 (Classified Research) において、Security Clearance 制度がどのように運用されているのかについて述べ、我が国の同種の制度設計に関する示唆を得ることを目的とした。

1. 規制研究 (Restricted Research)

米国大学が政府や財団、企業と締結する研究プロジェクトの契約 (グラント契約) に際して、最も重視されるのは、論文公開に対する制限が含まれないことである。企業との連携においては、その成果に関する特許権のとりあつかいについては、所謂 First Refusal Right のようなライセンスの優先交渉権などが設定されるケースなどがあり得るが、論文公開に制限がかかるような条件を認めない大学は多い。これは研究者や機関にとって学術論文の公開が最も重要な原則であり、大学院学生にとっては論文発表が学位の条件であるからである。

その際重要なキーワードが Fundamental Research である。所謂基礎研究であるが、実は米国研究機関にとって、この Fundamental Research とは、日本語でいう基礎研究という意味とはやや異なり、「成果公開可能な研究」ということを指している。それは、日本語の「応用研究ではないという意味での基礎研究」という意味ではなく「科学および工学における基礎および応用研究であって、その結果が通常公表され、科学界で広く共有されるもの」と定義されている(1985年9月21日にレーガン大統領が発行した国家安全保障決定指令-189、NSDD-189はNASの報告書¹)。Fundamental Research がこのように扱われている背景としては、米国の大学が長らく成果の論文公開の自由を含む開放性を重視してきたのに対して、安全保障上の懸念からこれを制約しようとする圧力との相克の結果が、色濃く反映されているといってもよい。実際、米国においては、NSDD-189の発表以降現在に至るまで、科学の開放性と安全保障の両立については常に議論されてきた。

1980年代、連邦政府機関は、米国の大学からソビエトへ軍事技術が流出する可能性について懸念するようになった。そのような懸念がきっかけとなり、AAUと国防総省によって、DoD-University Forumが設立され、共

¹ National Security Decision Directive-189 issued by President Reagan on September 21, 1985; NSDD-189 cites the NAS Report.

有された懸念に対する施策が検討されている²。このような議論の結果として先述した NSDD189 の報告がまとめられることになる。そこには「可能な限り基礎研究は自由であるべきであり、機密の分類指定は、管理が必要であると判断される場合に、連邦政府が資金提供する基礎研究中に生成される情報を管理するためのメカニズムとして使用されるべき³」との表現で、基本的な考え方が示されている。

このような経緯を経て、現在、論文公開可能な Fundamental Research とみなされるか否かをチェックする際に、米国大学が参照する政府の規制としては

- ① 国家によって指定された機密情報に触れるかどうか Classified Information : Executive Order 13526- National security information
- ② 武器国際取引に関する規則および米国輸出管理規則、International Traffic in Arms Regulations (ITAR)、Export Administration Regulations
- ③ 管理された非機密情報 : Controlled Unclassified Information (CUI)
- ④ その他バイオセキュリティに関する規制 : Select Agents Regulations: Department of Health and Human Services & USDA など

の4つの制度があげられる⁴。加えて、企業との契約に基づく研究の場合は、大学は契約内容に論文公開を制限する条項がないかを確認することになる。例えば、企業からの委託条件に知的財産の譲渡を条件とする委託研究などは慎重な検討対象となる。このような研究については、「研究資金提供者が一定期間、研究にかかわる提案や、データ、研究成果の機密保持を要求したり、大学外部の事業者が所有する知的財産をもたらす可能性のある研究」という意味で Proprietary research と称される。その結果、これらの制度や契約に照らして、研究成果の秘匿が義務付けられる機密研究 (Classified Research)、に加えて、研究結果を遅らせる必要がある研究などについては、制限研究 Restricted research と称して、その取扱い方針を大学として定めている大学が多い。米国大学は、制限研究 Restricted research は原則として受け入れていない。

それでは、米国大学がこれらの Restricted Research を一切受け入れないのかというと、この方針にはしばしば例外が示されていて、その許容範囲は大学ごとに異なる。

例えばイリノイシカゴ大学 (UIC) の方針は「UIC は、機密扱いまたは制限付きの研究を含むいかなる助成金または契約も受け入れず、・・・本ポリシー、他の UIC ポリシー、または一般規則で許可されている場合を除き、大学の名において、または UIC の施設や資源を使用して、機密または制限付き研究を実施することはできません」としている一方で、その例外として、技術試験契約、教員のコンサルティング契約においてスポンサーが特許を申請する時間を確保するために、出版物の提出を最大6ヶ月遅らせることがあげられている。この場合、研究費の申請前に、研究代表者の書面による提案により UIC 研究担当副総長室 (OVCR) により承認される必要がある。さらに Classified Research の禁止に関しても、機密情報への学外からのアクセスを伴うプロジェクトで、国防総省またはその他の該当する連邦政府機関または部署とのイリノイ大学協定によって許可されることで例外的に可能とされている。具体的には「UIC プロボストの承認を得て、政府スポンサーによって文書化された国家安全保障に対する差し迫った脅威に対応する場合、UIC は機密研究に関する本ポリシーのいかなる条項も免

² <http://aueco.org/wp-content/uploads/2016/04/NSDD189.pdf> Report of the DoD-University Forum for Calendar Year 1984.

³ 原文は”To the maximum extent possible fundamental research should remain unrestricted; classification should be used as the mechanism to control information generated during federally-funded fundamental research when it is determined that controls are necessary”.

⁴ Tobin Smith (Vice president, American Association of Universities :AAU) によるプレゼンテーションにおける説明から引用 ; 日米オンラインシンポジウム「国際研究協力における経済安全保障と輸出規制の課題」2022年9月29日、東京大学未来ビジョン研究センター主催 (TMI 総合法律事務所共催)

除または修正することができる。いかなる免除も、可能な限り短い期間で許可され、明確な日没規定を有し、研究責任者が、適切な Security Clearance を含む、機密物質の取り扱いと保護に関するすべての規制要件が満たされていることを証明した場合にのみ、許可される」としている。

同様 MIT に関しては「一般的な方針として、MIT がキャンパス内で機密研究や、例えば政府や産業界の研究スポンサーの許可なしに結果を公表することができないような研究を行わない」としているが、一方「MIT は、国家にとって大きな関心事である科学技術の重要な分野で独自の役割を果たす機関である。知識の追求が、研究結果を直ちに配布することが社会の利益にならないような、極めて重要であるがデリケートな技術分野に関わる場合があることを認識している。このような場合、留学生や学者による出版、分類、アクセスに関するこれらの方針に例外を設けることができるが、それは、その研究分野が MIT の教育的使命にとって極めて重要であり、例外が国益のために明らかに必要である、という非常に稀なケースに限られる、これらの条件が満たされない場合、MIT はその活動を拒否または中止し、学外または他の場所での検討のために提案する。機密扱いやその他の制限のある研究を学内で実施することは、研究所の学術環境を大きく変えることになるため、各プロジェクトは、研究所全体への影響に照らして検討し、対処することが不可欠である。したがって、MIT (リンカーン研究所を除く) の学術組織内で、……制限を課す必要があるすべての研究プロジェクトは、事前にプロボストの承認を受けなければならない、プロボストは教授政策委員会のアドバイスを求め、すべての承認について委員会に通知する」⁵として例外を認めている。

ここで「リンカーン研究所を除く」との表現にあるように、MIT には例外的に **classified Research** を行っている組織が存在する。MIT リンカーンラボは 1951 年にマサチューセッツ工科大学とアメリカ国防総省によって「リンカーン計画」(Project Lincoln) として発足した。最初に取り組んだ米国初の防空システムの研究開発では、デジタルコンピューター、磁気コアメモリー、大規模コンピュータープログラム、モデム、対話型グラフィカルユーザーインターフェースなど、数多くの研究成果を統合したものである⁶。MIT が管理する研究成果の知的財産の技術移転を行うことによって、米軍が革新的な技術進歩を利用できるようにすることを可能にしている。

もっともこのような例外は、大学の研究者が研究を行うことに比べて、大学院教育等に適用する際には、より保守的な方針がとられるようである。MIT の例では「ただし。大学院生、学部生を問わず、学位論文は研究所の研究プログラムの不可欠な一部であり、……学生にクリアランスを要求する論文や、完成時にセキュリティレビューを必要とする論文は、プロボストの事前の承認なしに着手することはできない。卒業論文が関係する場合、プロボストは、既存の方針の変更を伴う場合には、大学院政策委員会の助言をを求めるものとし、すべての承認について同委員会に報告するものとする」⁷としてより慎重な対応を求めている。学位論文が発表できないという事態は、学位取得を目指す学生にとって致命的であることが背景である。

2. 機密研究 (Classified Research) の要件

大学が機密研究 (Classified Research) の実施を、例外的に行うことを決定したとしても、実際に研究グループが Classified Research を実施するためには法令上いくつかの条件が満たされることが必要となる。

⁵ MIT ウェブサイト <https://policies.mit.edu/policies-procedures/140-research-policies-and-public-and-private-support/142-open-research-and-free>

⁶ MIT リンカーンラボウェブページ <https://www.ll.mit.edu/about/history> の記載より

⁷ 5 と同じ <https://policies.mit.edu/policies-procedures/140-research-policies-and-public-and-private-support/142-open-research-and-free>

まず誰でも Classified Research に参加できるわけではなく、Classified Research の実施に当たって必要となる機密情報 (Classified Information) へアクセスするため、Security Clearance と称する資格が不可欠となる。

Security Clearance は、米国等の「国家による安全保障関連の情報保全制度で設けられた人的および施設面でのアクセス制限の制度」である。米国では大統領令第 13526 号等によって定められる Top Secret, Secret, Confidential の 3 階層の機密情報 (Classified Information) に関するもので、①軍事計画・兵器システム又は軍の運用 ②外国政府情報、③インテリジェンス活動・情報源・方法又は暗号 ④機密情報源を含む連邦政府の外交関係又は対外活動 ⑤国家安全保障に関連する科学的・技術的・経済的事項 ⑥核物質又は核施設の防護策のための政府プログラム ⑦国家安全保障に関連するシステム・設備・インフラ・プロジェクト・計画・防護サービスの脆弱性又は能力 ⑧大量破壊兵器の開発等 等が定められている。イギリス、フランス、ドイツ、カナダ、オーストラリアに関しても同様の 3 階層または 2 階層の対象情報に対するアクセス制限制度が設けられている⁸。

大学等の研究機関がこのような機密情報を用いた機密研究に従事する場合は、その研究が行われる施設のクリアランス (Facility Clearance) が同時に必要となる。この審査では、施設の情報管理体制、組織の管理体制 (誰がどのような役割を果たしているか)、各組織の Key Management Personnel を特定して、機密情報の共有範囲を判断していくというような審査プロセスを経る。同時にその組織の外国機関による支配や影響 (Foreign Ownership, Control, or Influence : FOCI) についても審査がなされる。ここで、外国の利害関係者が、直接的または間接的に、機密情報への不正アクセスにつながりかねない、または機密契約の履行に悪影響を与えかねない方法で、その会社の経営または業務に影響を与える事項を指示または決定する力を持っていると判断される場合、その会社は FOCI の下で運営されているとみなされ Facility Clearance の対象としては不適格とされる。その組織が FOCI 下にあるかどうかを判断するにあたっては、会社の所有権と支配力、外国の利害関係者、外国の利害関係者の政府に関する要因を総合的に検討するとしている。具体的には、米国のターゲットに対する経済および政府スパイ活動の記録、無許可の技術移転の実施および/または関与の記録、アクセスされる情報の種類と機密性、関連する米国の法律、規制、契約の遵守の記録などが審査の対象となる⁹。これら一連のプロセスについては DCSA から詳しいガイドラインが示されている¹⁰。

もっとも大学関係者がクリアランスを取得することは、必ずしもその大学において Classified Research を行うことのみが目的ではなく、その研究者が参加しているプロジェクトを実施するうえで、政府機関が有している機密情報が必要な場合なども含まれる。この場合は施設のクリアランスは必要ない。

いずれにしても大学に所属する個人が、Security Clearance を必要とするのは、何等か政府が関係するプロジェクトに参加することに伴うものである。その契約が成立するためには、国防総省、国務省、エネルギー省などの機関が、「その研究者が契約を遂行するためには、機密情報へのアクセスを必要とする」との判断がなされることが前提となる。そして、雇用主である大学が契約に署名することでその必要性を承認し、その個人が機関の審査のためにクリアランス申請資料を提出して、審査を行い機関の承認を受けるといったようなプロセスとなる。要

⁸ 審査に際しては、国家安全保障上の適格性の有無が判断され、それは、安定性、信頼性、裁量、キャラクター、誠実さ、米国に対する疑いのない忠誠心などが含まれる。他方適格性を判断する際、以下の要因で差別することはないとしている：人種、カラー、宗教、セックス、国籍、障がいについて、性的指向、メンタルヘルスのカウンセリングだけで否定的な結論を出すことはできない。

⁹ DCSA のウェブサイト <https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/> に記載がある。原典は 32CFR Part 117(NISPOM), § 117.11(FOCI),(6)Factors

¹⁰ <https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Facility-Clearances/>

画すると、大学に所属する個人が Security Clearance を取得するケースは、あくまで大学が組織としてその必要性を認めて契約主体となるのであり、「機密情報に触れる個人が、個人的に資格を取得する」というスキームとは全く異なる。その際、しばしば研究を行う本人だけでなく、大学の学長やプロボストなどの組織の管理者も Security Clearance の取得が求められることがある。

例えばカリフォルニア大学は、約 70 年にわたり、米国エネルギー省 (DOE) の 3 つの国立研究所 (ローレンス・バークレー国立研究所、ロスアラモス国立研究所、ローレンス・リバモア国立研究所) の運営を管理してきたが、特にロスアラモスとリバモアは、高度な機密研究業務に従事してきた。大学がこれらの研究所を効果的に管理するためには、あるグループ (Key Management Personnel) が機密情報にアクセスする必要がある、そのため学長を含む大学幹部も Security Clearance を持つことが要求される¹¹。ただし Classified Research すべての大学がそうであるわけではなく、Classified Research を行っている大学 (MIT など 20 程度) の学長などの KMP であっても、ガバナンス上機密情報を知る必要がない場合は Security Clearance を免責される可能性がある。

Security Clearance 制度については、日本においても整備が必要なのではないかという議論がある。その点、2013年に成立し翌年施行された特定秘密の保護に関する法律(平成 25 年第 108 号(Specially Designated Secrets Act on the protection of Specially Designated Secrets:略称 SDS Act) は、日本の安全保障に関する情報のうち特に秘匿することが必要であるものを「特定秘密」として指定し、取扱者の適性評価の実施や漏えいした場合の罰則などを定めており、これが Security Clearance と類似あるいは相当の制度といえる。ただこの制度の対象情報としては、公になっていない情報であって、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特段の秘匿の必要性があるものとされ、① 防衛、② 外交、③ 特定有害活動 (スパイ行為等) の防止、④ テロリズムの防止の 4 項目について別表において詳細が定められている。この制度においては Security Clearance の対象となるものについては行政機関の者のみではなく、民間事業者が対象となる場合がある。具体的には、行政機関が特段の必要があると認めた場合は、適合事業者との契約に基づき、適合事業者に特定秘密を提供等することができるとしている。適合事業者は、契約に従い、特定秘密の適切な保護のために必要な措置を講じ、行政機関 が従業者には適性評価においてを実施し、特定秘密を漏らすおそれがないことと認められた従業者に者として、特定秘密の取扱いの業務を行わせると規定されている。

しかしその場合でも米国等の Classified Information の対象と比較すると、保全対象が極めて限定されている点や、日本の特定秘密は Top Secret, Secret の 2 段階に対応するものと情報保護協定上整理されており米国の CI の分類での Confidential に相当する分類が欠けている点でも相違があるなどから、米国で行われている Classified Research に相当する研究が、日本では十分行えないという指摘がある。またさらに類似の制度を持つ国同士で機微技術に関する共同研究開発を行う際、または同種技術を用いた製品の受注に際して、同様の制度がないことが支障になるというような指摘がある。

例えば日本の民間事業者が米国現地法人を設立して、その現地法人の現地国籍の従業員と法人施設が、一定の要件を満たせば米国の Security Clearance を受けることはできる。しかしその場合現地で得られた情報は、日本本社には開示することができないため、例えば米国における技術的要請に対して、日本本社の技術によって課題を解決できるかどうかなどの検討が十分行うことができないということになる。これは相当する制度を有する他

¹¹ 大学側の Policy: Regents Policy 1600: Policy on Security Clearance for Access to Federal Classified Information から、このような方針としていることが分かる。
<https://regents.universityofcalifornia.edu/governance/policies/1600.html>

国では情報共有が可能となる場合が想定されるため、他国との競争条件として不利であるということになる¹²。

3. 米国大学における研究の分類と機密研究（Classified Research）の実態

3.1 米国大学における研究の分類

ここでは、2で述べてきた公開制限や秘密保持といった観点での米国の大学が行う研究の分類を検討する。この図ではカテゴリとして基本 Fundamental に分類される Non Restricted Research と Restricted Research に大別し、さらにそれぞれを2つずつの分類に分けている。このうち Fundamental としているのは、冒頭に述べた、「科学および工学における基礎および応用研究であって、その結果が通常公表され、科学界で広く共有されるもの」であって輸出管理上の例外扱いされているものを指している。この中でも利用する情報がすべてまさに Fundamental の研究活動によって創出された共有情報のみである場合と、所謂 CUI（Controlled Unclassified Information）と言われる管理すべき情報を用いる場合がある。この CUI は「管理された非機密情報」などと訳される。例としては、米国政府が定めた情報区分で政府機関が取り扱う安全保障および原子力に係る情報のうち、機密情報（Classified）ではないが適切に保護すべき情報を指す。この情報区分には安全保障関係だけではなく様々な管理すべき情報が含まれている。CUI を規定している根拠としては大統領令 13556 号(CUI)、連邦行政規則 32 編 2002 条（32 CFR Part2002）や NIST SP 800-171 がある。連邦政府外のシステムと組織に存在する管理された非格付け情報（CUI）の保護は、連邦政府機関にとって最も重要なものであり、連邦政府の指定されたミッションとビジネス運用を行うための能力に直接影響を及ぼす可能性があるものと認識されている。

したがってこのような情報を用いた研究であれば、その情報自身を公開することはできない。そのため、研究論文等に、CUI に指定されている管理すべき情報が紛れ込んでないかどうかについて Review process が設けられている。そして、成果公開を制限する特別な条項がない前提であれば、そのような CUI 情報を用いた研究成果であっても、CUI が含まれていない限り成果公開は自由である。この点、研究成果の公開自身を制限する Classified Research とは異なる。このような、Review と 成果公開の可否を審査するということは全く異なることは重要である。この際、発表される技術情報は、輸出管理上のみならず輸出の管理の基礎研究例外として扱われる。ただしこれらの Fundamental の研究によって得られた試作品などの製品については、輸出管理の例外には当たらず、輸出管理対象となるため、必要な許可申請を得ることなく、不用意に国外に持ち出すことはできない。

一方、成果公開に制限を加える Restricted Research についても、大きく 2つのカテゴリに分けられる。ひとつは政府の指定する Classified Information を利用した Classified Research である。その他にも企業から委託を受ける研究プロジェクトでは、研究成果の公開を制約する可能性がある。企業が研究成果を営業秘密として秘匿したい場合、企業による審査を経ない限りは、研究成果を論文発表することができないが、加えて、企業にとって不都合な研究結果、例えばその会社の医薬品の効果が乏しい、または副作用が発見された場合などを秘匿したいというような場合は、利益相反および研究倫理の問題が生じる。このような条件が付された契約では、大学は受け入れには相当慎重にならざるを得ない。他方、特許出願の目的で 6 か月程度の公開制限を課したり、一定

¹² ただし日本で諸外国と同等の Security Clearance 制度が整備されたとしても、民間事業者に対して直ちに外国政府が機微情報の共有を認めるわけではもちろんなく、政府が保有する安全保障上重要な情報へのアクセス権（Security Clearance）は、基本的には自国民を対象に付与されるため、何らかの協定に基づき、外国政府の安全保障上重要な情報にアクセスするためには、自国政府を通じて行うことになる。

の製品開発期間の発表を制約するなどの条件を企業が希望することもあるが、このようなケースではプロボストオフィスが、その受け入れ可否を判断することになる。

カーネギーメロン大学では「企業等が所有する知的財産をもたらす研究。企業は、大学で開発された発明やアイデアに由来する製品を販売したいと考えるかもしれません。そのため、データへのアクセスや進行中の研究についての議論を「知る必要がある」個人に制限し、研究結果や結果を検証するために必要なデータの公表を一定期間遅らせることを求めるプロジェクトに資金を提供することを希望する場合があります」としたうえで、これらのプロジェクトを受け入れようとする場合は、大学の審査を受けることとしている。カーネギーメロン大学のケースでは、「スポンサー・リサーチ部門は、承認前に、すべての提案書と契約書が本ガイドラインに適合しているかどうかを審査するものとする。これらのガイドラインに適合しないものは、大学研究評議会（URC）に付託され、審査と学長への適切な措置の勧告が行われます」としており、受け入れ決定後も「研究責任者は、プロジェクトに参加するすべてのメンバー（教員、職員、学生）に対し、研究に関連する情報の発信に課される制限を通知する責任を負う。これは、プロジェクトの開始前、または個人が既存のプロジェクトに参加する前に行われなければならない」としている¹³。また「プロボストオフィスは、制限付き研究プロジェクトの研究責任者から、研究に課されたすべての制限を認識していること、およびすべての参加者にこれらの制限を通知したことを証明する署名入り文書入手する責任を負う」としており、事前の審査とともに、そのような条件での研究を受け入れた研究責任者には、プロジェクトメンバーに対する契約内容の説明を義務付けている。

最後のカラムが機密研究の領域を示している。通常このような **Classified Research** では成果の論文公開も制約される。基本このカラムの研究を受け入れた場合、研究に従事するものは **Security Clearance** の対象となるし施設もクリアランスの対象となる。

一方、この表の青い領域で基礎研究に従事している場合は、以上述べてきた様々な制限を受けることはないが、プロセス管理やリスク管理に関してはむしろ厳しく求められており、また研究を行う上で影響を受ける可能性のある関係性の申告が義務つけられている。これらは **Integrity and Security** の管理と称されており、最近米国大学において発覚している、外国機関による研究への介入や研究情報の不当な窃盗などの事件¹⁴を背景としたものである。そしてこのような問題を防止するため、大学はリスク評価と管理計画を策定するようになった。同時に政府やファンディング機関は大学に、そのような管理を強く求めるようになってきている。具体的には、大学に開示することなく個人的な利益を受ける見返りに、研究成果を特定の海外の団体に提供するなどが禁じられている。米国における **Integrity and Security** の管理は、政府の指示によって始まったということではなく、外国機関の研究に対する望ましくないリスクを認識した米国大学が、自ら始めたハイリスクパートナーリングマネジメント¹⁵の実践が発端となっている。一方、研究セキュリティに関する最近の懸念に対応するため、米国政府は、2021年1月14日付の国家安全保障大統領覚書第33号（NSPM-33）において、政府の方針として特定の要件を定めている。この内容としては、①外国政府の干渉・搾取からの米国の研究開発体制の保護：NSPM-33は、米国のR&D体制に大きな影響を与える個人の、潜在的な利益相反および責務相反に関連する情報の開示要件を強化・標準化すること。②研究開発体制のインテグリティの保護：知的資本を保護し、研究の不正流用を防

¹³ カーネギーメロン大学ウェブページ <https://www.cmu.edu/policies/research/restricted-research.html#:~:text=Restricted%20research%3A%20includes%20all%20classified,publication%20of%20the%20research%20results.>

¹⁴ 最近の事例としてはハーバード大学の Charles Lieber 博士が雇用契約を大学に申告せずに中国の大学における研究業務に従事していたことが発覚して逮捕され、その後有罪が確定した事件などが伝えられている。

¹⁵ 渡部俊也、東京大学未来ビジョン研究センター政策提言：米国大学が行うハイリスクパートナーリング管理の実態と日本の大学への示唆（暫定版）2019年2月

ぎ、米国の納税者の資金の責任ある管理を確保し、同時に米国と世界に利益をもたらす研究とイノベーションを育むオープンな環境を維持するための、措置を講じる。具体的には連邦政府職員に対して、外国政府が支援する人材採用プログラムへの参加を禁止し、省庁に対して、連邦政府の研究施設へのアクセスと利用の管理を指示し、研究開発資金の配分を担当する連邦政府機関職員に対して、研究セキュリティに関するトレーニングを受けることを要求するという項目などからなる。

冒頭述べたように、米国大学が行う研究の大半は **Fundamental Research** であり、その点日本と米国のアカデミアの連携などを考えるうえで、この **Integrity and Security** の管理が十分行われているかどうかという点が重要となる。逆に **Fundamental Research** では、そこで利用する情報も公開情報であり、研究成果も公開するのだとしても、その研究過程は一切管理する必要がないということではない。その研究をどのような連携関係で行うのか、またその過程の情報管理や知財として確保するなどには十分管理を行う必要がある。特に最近はこのような管理について強化される傾向があり、例えば NSF の資金提供を受ける大学では、教員の教育プログラムが義務付けられたり、その大学のビジターに関しても一定のバックグラウンドチェックが求められるなどの制度の検討がなされている¹⁶。

なおこれらのすべてのカテゴリで、論文公開ではなく、研究成果に基づいた試作品などに関しては、輸出管理の対象となることは留意する必要がある。

また一方これらの研究プロジェクトの制度とは別に、安全保障上の機微技術であり公開するべきでないと考えられた特許出願について公開を延期し、秘密とする秘密特許制度が存在し、企業の発明などでは適用されることがある。原理的に大学の発明でもこれが適用される可能性があるが、実態上大学の研究成果に対しては、ほとんど秘密特許制度による公開制限は行われていないと考えてよい。

表 1 米国大学における研究プロジェクトの分類

Categories		Information used for research		Research results	Products based on research result
Non Restricted Reserach	Fundamental	Public Information	Open to the public	Open to the public by publishing	Under export control
		CUI	Public disclosure restrictions	Open to the public by publishing	Under export control
Restricted Research	Proprietary Research	May Include Confidential Information	Public disclosure restrictions	Public disclosure restrictions	Restricted by contract and/or under export contro
	Classified Research	CI	Confidential	Confidential	Confidential

(注) ここで **Confidential** としているのは CI の 3 階層の一つという意味ではなく、機密であるとする意味で使っている

¹⁶ 米国関係機関、大学等へのヒアリングによる

3.2 米国大学における機微度が異なるカテゴリ間の研究の関係

以上述べてきたように、米国大学においては、おおむね **Fundamental Research** に従事しているものの、例外的とはいえ、成果公開制限に関して、異なるカテゴリの研究を同一組織内で行っているケースが存在する。このような異なるルールの研究を同一組織において実施するうえでは、マネジメント上の留意点があるものと思慮される。具体的には、①**Fundamental Research** から **Classified Research** への移行、あるいは、②その逆のケース、さらに、③同一の研究者が双方にかかわるケース、などに対応する管理方法が重要になるものと考えられる。

最初に、**Fundamental Research** から **Classified Research** への移行に際して生じ得る問題について述べる。年限が確定した **Fundamental** の要件を満たすプロジェクトであれば、その期間の研究の成果については論文公開が保証されており、成果が機微であるという理由で公開制限がかけられるということはない。米国大学では **DARPA** をはじめ米軍関係のスポンサーによる研究プロジェクトが行われている例は少なくないが、多くは **Fundamental Research** の要件を満たした形で行われている。このようなケースでは、仮に米軍関係のスポンサーのプロジェクトであっても、成果が出たのちに公開制限が強制的に行われることはない。他方そのプロジェクトの成果が、防衛技術用途などに利用できると判断され、後継プロジェクトが **Classified Research** となる場合はありえる。その場合、それまで研究してきたメンバー研究者が、**Classified Research** に参加する場合は **Security Clearance** を取得する必要があるし、通常の大学のキャンパスの研究室で継続することはできないため、継続して研究者が参加する場合は **Security Clearance** を取得し、専用の施設等に移って研究に参加することになる。

もっとも大学等の研究者にとっては以降の論文発表ができなくなるため、**Classified Research** に参加する動機は乏しい（その結果、研究者が新たなメンバーに入れ替わることもある）。その場合でも過去に遡及するかたちで、それ以前のプロジェクトの成果に関して公開制限がかけられることはない。

ただしこのような研究を行っている機関等にヒアリングした結果からは、プロジェクトの管理者が、論文公開の方法などにアドバイスを与えることは、しばしばあるようである。基礎研究の成果であってもことさらに応用面を強調すると、機微な要素が含まれる懸念があることから、自然な形でプロジェクトの管理者と研究者のあいだでのコミュニケーションの中で、そのような工夫が行われることがあるというのが実態であろう。

もっとも、一般的には論文発表を専ら業績とする研究者にとっては **Classified Research** への参加の動機が乏しいものの、防衛関係の深い技術開発に一定期間従事することが、研究者にとって魅力があるケースは一定程度ある。**Classified Research** のプロジェクト管理者にとっても、それまで研究プロジェクトを担ってきた主要な研究者に参加を期待するケースもある。その場合自らの研究者としてのキャリアにプラスになると考え、またクリアランスの取得が可能な場合は、そのようなオファーに応じるケースもある。この場合一定期間のプロジェクトが終了すれば、再び **Fundamental Research** のプロジェクトに戻ることも可能である。その場合 **Classified Research** に従事した経験が基礎研究でも役立つと考えられていることは重要である。学生や大学院生に関しても、論文発表が卒業や修了要件である場合は **Classified Research** への参加は困難である一方、論文発表のウエイトが低い学部学生などでは、希望する就職先との関係などから、**Security Clearance** を取得して **Classified Research** に参加するケースもあるようである。学生が就職する際に **Security Clearance** が必要な職場もあるため、そのような就職先を希望する学生にとっては、予め **Security Clearance** を取得しておくことはメリットがある。さらに **Security Clearance** は、学生が政府機関によってはインターンでも求められることがある。ハーバード大学ロースクールでは、大学ではそのようなケースに関して情報提供を行っている¹⁷。

¹⁷ハーバード大学ロースクールの就職情報掲載サイト <https://hls.harvard.edu/bernard-koteen-office-of-public>

さらに MIT など Classified Research を大学の一部で実施している大学の研究者では、一方のプロジェクトで CI を扱う Classified Research を実施していて、同時に Fundamental Research に従事している例もある。この場合 Classified Research に従事するため Security Clearance を取得しており、かつその研究は専用の施設（リンカーンラボ）で実施する一方、通常のキャンパスで Fundamental Research にも従事しているケースがある。もちろん Classified Information については一般の研究には用いることはできず、両者は情報管理や成果のとりあつかいルールなどが厳然と区別されている一方、双方にまたがって研究を行うことのメリットもあるのではないかと推察される。

4. 米国研究制度の特徴と日米研究連携の課題

ここまで見てきたように、米国における大学等の研究機関が実施している研究開発の制度の特徴としては、下記のような特徴をあげることができる

- ① 自由でオープンな研究環境が重要であり科学的成果は公表されることでテストされるべきという考え方に基つき、米国輸出管理 (EAR) における Fundamental Research Exemption の対象となる範囲の Fundamental Research を重視して、この条件を満たさない研究は、基本受け入れないとする方針を掲げている大学が多いこと。その場合研究に利用する情報として管理すべき CUI が含まれている場合は、研究発表の際にそれらの CUI が紛れ込んでないかどうかを Review することがあっても、研究成果そのものの発表を制限することはないこと。
- ② 最近では特定国によって、Fundamental Research の公開性を悪用し、軍事技術に利用するため、研究プロセスに関する情報やノウハウを窃盗する事例が生じたことを背景に、外国機関との共同研究などの影響を把握し、その望ましくない影響を防止、減少させるための Integrity & Security の管理が義務付けられている。
- ③ 他方、例外的に、Classified Information を用いて行う Classified Research を、意義や条件等を審議して受け入れる場合があり、その場合は、参加する研究者は Security Clearance を取得する必要がある。その場合、Security Clearance の対象でない同僚との交流や情報共有に追加の制約を受ける可能性があるため、研究を行う施設と組織については Facility Clearance を得なくてはならないのと同時に、研究成果の研究発表や論文公開は制限される。
- ④ また企業等からの委託研究について公開制限が課せられる場合も、Classified Research と同様に例外的に受け入れについて審議して受け入れを行うことがある (Proprietary Research)
- ⑤ これらの異なる研究カテゴリ間では、研究者が一方から一方へ移動したり、兼任したりすることがあるが、両者のルールは厳然として区分されている。

これらの特徴は、大学等の学術研究の役割として、成果公開によって評価される知識の創出に重点をおいていることから、そのような価値を損なう制約を政府の防衛機密に関係するものであれ、企業の要請であれ、例外と

[interest-advising/opia-job-search-toolkit/security-clearances/](#) では「ほとんどの連邦政府機関は、夏期、学期、および大学院の志願者に対し、採用前にある程度のセキュリティ・チェックを受けるよう求めています。・・・正規雇用の場合は、推薦者、元雇用者、同僚、友人、隣人、家主、高等教育機関、クレジット／軍事／税務／警察記録など、より広範なチェックが必要になる場合があります。機密情報にアクセスしたり、国家安全保障に携わったりする場合は、「Security Clearance」が必要になる場合があります、さらに高度な審査が必要になります。歴史的に Security Clearance を必要とする機関には、司法省、CIA、国防総省の一部が含まれます。しかし、DOJ やその他の連邦政府機関では、適性検査や Security Clearance の取得に長期間を要し、一部の申請者にとって大きな障害となることがあります」との説明がある。

位置づけ、受け入れに際しては慎重な経営判断を行っているという構図が明らかである。その結果、双方の人の移動はあるものの、両者は明確に切り分けられており、そのコントラストは明瞭である。

一方成果公開を許す **Fundamental Research** については、ルールとしての透明性や公開性を損ねる試みを排除する仕組みとして **Integrity & Security** 管理が導入されている。この考え方は 2023 年時点で G7 各国の合意事項となっている¹⁸。

以下、このような制度で運用されている米国大学と研究協力を行う際に、日本の研究制度に求められることを検討する。第一に日本では **Classified Research** を行う制度として **Classified Information** を用いた **Security Clearance** や **Facility Clearance** 等の制度を有しないことから、仮にこれらの分野での連携が行われる場合は、致命的な問題となる。文字通りの防衛研究に関して日米の大学等の研究機関が参加することは考えにくいだが、サイバーセキュリティや高度防護技術などのデュアルユース領域で日米または同様の制度を有する関係国の研究協力を行う場合は、当然ながら厳密な秘密管理が必要であり、大学等の学術研究機関が貢献できる可能性はあるだろう。その点これらの制度整備は不可避免的に必要であると考えられる¹⁹。その点はむしろ大学より民間企業においてはより重要な障害になりえる。**Security Clearance** 等の制度は主要国では整備されており、これらの各国間では民間企業等の協力も行われている一方、日本に相当する制度がないことは、これらの国々との民間企業間での協力体制が取りにくいとする指摘がある。

また CI と同じく CUI についても日本では相当する制度はないことも課題である。実際には米国の民間の研究開発において利用される情報は CI よりも CUI がより重要であるとする意見もある²⁰。

これらの課題はあるものの、本稿で示しているように米国大学における研究の太宗は **Fundamental Research** であり **Classified Research** はごく例外的であることは重要である。**Fundamental Research** の領域については、日本の大学等の研究機関には、米国と同等また G7 の合意事項でもある **Integrity & Security** 管理を十分に行うことが求められる。一方それ以外の制約は極力課さないことが、円滑な研究交流において重要であると考えられる。その点米国の輸出管理で認められている、幅広い **Fundamental Research Exemption** が、日本の輸出管理では認められていないことについては検討を要する。例えば、日米共同研究で、日本のリスト規制技術分野を扱う場合でも、成果を公開することを企図する研究であれば、米国側では **Fundamental Research** と認められれば、外国籍研究者の参加や公開前の途中段階での技術の提供に制限はないが、日本側は外国籍研究者の参加や公開前の米国への技術提供にあたり、経済産業省からの許可が必要であるため、米国側で最悪 **Fundamental Research** として認められず、米国大学が参加できないおそれも生じ得る²¹。これまでこのような事例があったわ

¹⁸ G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group の成果資料が下記に示されている

https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/annex2_sigre.pdf

¹⁹ ただし現状の特定秘密保護法との関係をどのように整理するかは課題である。特定秘密保護法については本稿では詳細は述べないが、防衛分野を中心に、政府及び民間事業者等の間では情報保全体制が構築されて運用されている実態があることから、政府のセキュリティクリアランス制度に関する有識者会議の中間論点整理

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/chuukan_ronten.pdf においては、「経済等の新たな分野を含めた政府横断的・分野横断的な視点を持ち、従来の防衛分野における情報保全制度を始め既存の諸制度等との整合性にも留意しつつ、あるべき制度を検討することが必要である」としている

²⁰ 経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議：中間論点整理（2023年5月6月） https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/chuukan_ronten.pdf

²¹ **Fundamental Research** の定義として、EAR では、「科学、工学または数学の研究であって、その成果は通常公開され、研究コミュニティ内で広く共有されるものであり、研究者が所有権または国家安全保障上の理由から制限を受け入れていないものをいう。」と定義されている (§ 734.8 (c))。外為法の規制を受ける研究は、**Fundamental Research** と見なされないおそれがある。

けではないものの、近年日本の輸出管理は厳格化しており、米国の輸出管理の運用とは大きく異なる点は、今後改善すべきであると考えられる²²。

この点、例えば日本の政府プロジェクトで米国等との連携を想定している場合、中途半端に論文公開の制限があるような規定があると、**Fundamental** としての連携の支障となる可能性がある。もとより米国においても、制度的には秘密特許制度があり、日本のように対象技術分野の指定もないことから、あらゆる大学の特許出願で指定される可能性は否定できず、指定されれば論文公開も制限されることになるが、従来の運用から事実上この可能性は考慮されていない。日本の制度も例外的な可能性について、あくまで例外でありその主旨などをしっかり説明することで懸念を生じさせないことが大切である。

要約すれば、米国の研究制度は、**Fundamental** の領域を含む **Non Restricted** と **Classified** を含む **Restricted** のコントラストは明瞭であり、日本の制度においてもあいまいな線引きではなく、制度には明瞭な区分と運用を取り入れ、それぞれを明確に説明できるようにすることが重要であると考えられる。

5. まとめ

本稿では米国大学における **Restricted Research** について、成果公開の制約がない **Fundamental Research** と対比させ、その位置づけや取扱い方針についてまとめた。特に **Classified Research** を実施するために必要な **Security Clearance** や **Facility Clearance** などの制度は、日本でも必要であると述べた。

他方、国際研究交流において体操を占める **Fundamental Research** において必要な **Integrity & Security** 管理は重要であることに加え、輸出管理においてはむしろ規制緩和が必要であることを示した。要は米国のようなコントラストの利いた制度設計が必要なのであり、そのような2つの領域を最大限効果的に組み合わせることで、国際的なオープンな環境での知の集積を促進するとともに、目的が明確で厳密に情報管理すべき **restricted research** から成果を得る新たなナショナルイノベーションシステムの構築を試みることにつながる。

文献

1. 渡部俊也、吉岡(小林)徹「安全保障の観点における特許登録延期制度および補償金に関して — 所謂「秘密特許制度」に関する論点 — 」未来ビジョン研究センター安全保障研究ユニット：2021年度ワーキング・ペーパー・シリーズ No.5 2021年7月14日
2. 渡部俊也「米国 NDAA2019 の **Emerging Technology** とは何か— 輸出管理業務の拡大と技術政策への影響—」*Cistec Journal* 183 115-124 2019年9月
3. 開催報告書「日米研究協力における日本の輸出管理運用の課題[日米オンラインシンポジウム:国際研究協力における経済安全保障と輸出規制の課題] 2022年09月29日 <https://ifi.u-tokyo.ac.jp/event/13682/>

²²米国では、研究成果を公開前に **Fundamental Research** を行っている研究者に提供することは公表済み資料の提供と同じ扱いとなる。米国の大学の研究の太宗が **Fundamental Research** であることと併せ、大学内の輸出管理に要する手続きも相当程度削減されていることが考えられる。

4. 渡部俊也「米国大学が行うハイリスクパートナーリング管理の実態と日本の大学への示唆（暫定版）」東京大学政策ビジョン研究センター「産学および社会連携システム研究ユニット」政策提言 http://pari.ifi.u-tokyo.ac.jp/publications/policy190227_uiusp.html 2019年2月
5. 渡部俊也「米大学で浸透する自主管理「外国の影響」にどう向き合うか」東洋経済新報社、東洋経済 2021年6/26号掲載箇所68-69、2021年6月

謝辞

本稿作成に当たっては、米国および日本の政府機関、大学及び企業のインタビューなどを参考にさせていただきました。関係各位に心から感謝申し上げます。また輸出管理との関係の記載については、東京大学産学協創推進本部の副本部長である中尾圭介氏に記載を願いました。ご貢献に厚く感謝申し上げます