第2章　各国・地域における研究インテグリティに対する取組状況

2.1 米国

トランプ前政権は、政権交代直前の 2021 年 1 月 14 日に「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」（*National Security Presidential Memorandum-33*（NSPM-33））を発出した。同大統領覚書では、「中華人民共和国を含む一部の外国政府は、開かれた科学的交流への相互献身を示しておらず、研究を行うためのコストとリスクを回避するために、米国及び国際的に開かれた研究環境を利用しようとし、それによって、米国、その同盟国、パートナーを犠牲にして、経済及び軍事競争力を向上させようとしている」と説明し、「米国政府が支援する研究開発（R&D）を、外国政府の干渉や搾取から守るための行動を指示する」としている。なお、この文書や、その後の米国における取組においては、「研究セキュリティ（research security）」あるいは「研究セキュリティとインテグリティ（research security and integrity）」という言葉が、「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティ」に相当する意味を有した用語として使用されてきている[15]。

バイデン大統領は、2021 年 1 月の大統領就任後に NSPM-33 を追認する一方で、トランプ政権下の 2018 年に司法省で始まった、大学・研究機関の中国のスパイ研究者の摘発キャンペーンである「China Initiative」は 2022 年 2 月に終了している。

2022 年 1 月 4 日、大統領府 OSTP は、「NSPM-33 実施ガイダンス」（*Guidance for Implementing National Security Presidential Memorandum 33*（NSPM-33））を発表した。同文書の目的は、「連邦省庁に対し、NSPM-33 の実施に関する指針を提供すること」であり、各機関がその実施努力に適用すべき一般的なガイダンス（general guidance）に続き、NSPM-33 で取り上げられた、研究セキュリティの確保に関連する 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の結果、4. 情報の共有、5. 研究セキュリティプログラム）についての詳細なガイダンスを含んでいる。

米国議会の動きとしては、2021 年 1 月に 2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）が制定され、その第 223 条で、すべての連邦政府の

[15] NSPM 33 implementation plan によれば、研究インテグリティは「研究開発活動の提案、実施、評価、報告において、客観性、正直さ、透明性、公平性、説明責任、スチュワードシップなどの専門的な価値観や原則を遵守すること」（Adherence to professional values and principles – including objectivity, honesty, transparency, fairness, accountability, and stewardship – in proposing, performing, evaluating, and reporting research and development activities）と、研究セキュリティ（research security）は「国家や経済の安全保障を損なう研究開発の不正利用を目的とした行為、関連する研究インテグリティの侵害、外国政府の干渉から研究事業を保護すること」（Safeguarding the research enterprise against behaviors aimed at misappropriating research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference）と説明されている。

資金配分機関が研究助成金申請プロセスの一環として現在及び未決の支援についての情報開示を申請する研究者に対して求めることが義務付けられた。また、2022 年 8 月に CHIPS and Science Act が成立した。この法律（2 部構成）は半導体インセンティブに 5 年間で 527 億ドルを計上（appropriation）、そのうち、先端研究開発に 110 億ドル計上すること等とともに、研究セキュリティに関する規定を含んでおり、「外国人人材採用プログラム」（Foreign Talent Recruitment Programs）についてのガイドライン策定、米国科学財団（National Science Foundation: NSF）に Research Security and Policy Office の設置、研究開発助成の申請時にリスク評価を NSF が実施する権限の付与、大学・研究機関や研究者がセキュリティリスクを理解し軽減できるよう、独立したリスク評価センターを設立すること、等の規定を含んでいる。

表 2-1、表 2-2 は、それぞれ研究インテグリティ関連の大統領府等、米国議会における主な動きの年表である。主なものについては以下で、要求と支援（どこからどのどこへ（連邦政府、資金配分機関、大学等研究機関、研究者）、どのような内容）に注目して説明する。

表 2-1：近年の研究インテグリティ関連文書（大統領府等）

発行年	文書名	発行元
2021.1.14	National Security Presidential Memorandum – 33 (NSPM-33)（Presidential Memorandum on United States Government-Supported Research and Development National Security Policy）	ホワイトハウス（トランプ前大統領時）
2021.1.19	Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise <https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf>	Subcommittee on Research Security, Joint Committee on the Research Environment, National Science & Technology Council
2021.8.10	Clear Rules for Research Security and Researcher Responsibility <https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/>	Dr. Eric Lander (President's Science Advisor and Director of the OSTP)
2022.1.4	Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33). <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>	ホワイトハウス
2022.8.31	An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity <https://www.whitehouse.gov/ostp/news-updates/2022/08/31/an-update-on-research-securitystreamlining-disclosure-standards-to-enhance-clarity-transparency-and-equity/>	Morgan Dwyer ら（OSTP）OSTP ブログ

出典：スタンフォード大学ウェブサイト．"Academic Integrity and Undue Foreign Interference" <https://doresearch.stanford.edu/topics/academic-integrity-and-undue-foreign-interference#Policies_&_Resources>などに基づき作成。

表 2-2：近年の研究インテグリティ関連法（米国議会）

発行年	法律名	発行元
2019.12	2020 年度国防権限法（FY 2020 National Defense Authorization Act (NDAA)）※第 1746 条に、大統領府科学技術政策局（OSTP）が主導し、国家科学技術会議（NSTC）に米国科学技術の海外からの干渉等からの保護等を検討するための省庁間ワーキンググループを設置すること、全米アカデミーズに科学技術安全保障円卓会議を設置すること等を規定。	米国議会
2021.1	2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）※第 223 条で研究提案時等の情報開示について規定	米国議会
2022.8	CHIPS and Science Act 2022	米国議会

2.1.1 研究インテグリティの確保に関する要求と支援

本セクションでは、2021 年度[16]までの動きとして、(a) NSPM-33（2021 年 1 月）、(b) Recommended Practices（2021 年 1 月）、(c) 2021 年度国防授権法（2021 年 1 月）の第 223 条、(d) NSPM-33 実施ガイダンス（2022 年 1 月）について説明する。次に、2022 年度の動きとして、(a) CHIPS and Science Act（2022 年 8 月）、(b) OSTP による検討状況公表（2022 年 8 月）、(c) 全米アカデミーズ報告書「米国の技術優位を保護する」(2022 年 9 月)、(d) “Safeguarding Science” Toolkit の発表（2022 年 11 月）、(e) 研究セキュリティプログラムのドラフト公表（2023 年 2 月）について説明する。

(1) 2021 年度までの主な動き

(a) NSPM-33（2021 年 1 月 14 日）

2021 年 1 月 14 日に発出された「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」（*Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*）[17]の宛先は、大統領府レベルの 15 の連邦省庁（財務省、住宅都市開発省を除く）の長官に加え、行政管理予算局（OMB）の長、その他連邦政府独立省庁（環境保護庁、NASA、米国科学財団）の長、研究所等（NIH、スミソニアン協会）の長、さらに、情報機関の長（Director of National Intelligence（国家情報長官（DNI））、Director of CIA（中央情報局）、Director of FBI（連邦捜査局））、The Assistant to the President for National Security Affairs、そして本件取りまとめを担当する Office of Science and Technology Policy（大統領府科学技術政策局）の長が含まれる。研究開発を行う連邦省庁とともに、情報機関に対する指示となっていることが特色と言える。

NSPM-33 の Section 1 ではこの大統領覚書の目的として、「米国政府が支援する研究開発（R&D）を、外国政府の干渉や搾取から守るための行動を指示するものである」とし、「残念ながら、中華人民共和国を含む一部の外国政府は、開かれた科学的交流への相互献身を示しておらず、研究を行うためのコストとリスクを回避するために、米国及び国際的に開かれた研究環境を利用しようとし、それによって、米国、その同盟国、パートナーを犠牲にして、経済及び軍事競争力を向上させようとしている。」と説明する[18]。

---

[16] 本委託調査は 2022 年度以降の動きを中心に調査することとされており、ここでの 2021 年度までと、2022 年度以降の区分は日本の会計年度に基づく。

[17] US Whitehouse. Presidential Memorandum on United States Government-Supported Research and Development National Security Policy. Issued on: January 14, 2021. National Security Presidential Memorandum – 33 <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>

[18] “This memorandum directs action to strengthen protections of United States Government-

Section 2 では、以下の 7 つの用語の定義をしている：「米国研究開発事業への参加者」（“participants in the United States R&D enterprise”）、「米国政府支援研究開発」（“United States Government supported R&D”）、「利益相反」（“conflict of interest(s)”）、「責務相反」（“conflict of commitment(s)”）、「海外政府支援人材採用プログラム」（“foreign government-sponsored talent recruitment program”）、「連邦政府職員」（“Federal personnel”）、「デジタル永続的識別子」（“digital persistent identifier”）。このうち、「米国研究開発事業への参加者」の定義は「研究者（学術研究機関、独立研究機関、医療センター・研究所、民間企業、又は連邦政府センター・研究所）と、連邦研究開発資金の配分及び授与のプロセスに参加する者」[19]である。

Section 3（Roles and Responsibilities）からは大統領覚書の具体的な内容であり、Section 3 では、研究資金を提供する連邦省庁の長等に対する要求事項が列記されている。要求事項は以下のとおりである。

表 2-3：研究セキュリティ・インテグリティ確保のための連邦省庁への要求事項（NSPM-33, セクション 3)

※青は要求事項（連邦省庁に対する要求）、赤は支援事項（連邦資金を受けとる組織への支援）に関連。太字・下線は筆者によるもの。

連邦政府が資金提供する研究の設計・実施・報告・審査、あるいは資金提供に大きな影響を与える、米国研究開発事業の参加者に対して、本大統領覚書の Section 4（b）に沿った適切な**情報の開示を要求**し、適用される連邦法及び規則に基づき、利益相反及び責務相反の有無、どこで起こっているかを確実に判断できるようにする。[20]
連邦資金を受け取る組織が、潜在的な利益相反や責務相反を含む研究セキュリティとインテグリティに対するリスクを特定し管理するための**方針とプロセスを確立し管理**することを確実にするために、その組織に協力する。[21]

supported Research and Development (R&D) against foreign government interference and exploitation.”

“Unfortunately, some foreign governments, including the People’s Republic of China, have not demonstrated a reciprocal dedication to open scientific exchange, and seek to exploit open United States and international research environments to circumvent the costs and risks of conducting research, thereby increasing their economic and military competitiveness at the expense of the United States, its allies, and its partners”

[19] “researchers at academic research institutions, independent research institutes, medical centers and institutes, private companies, and Federal Government research centers and laboratories, as well as those who participate in the process of allocating and awarding Federal R&D funding”

[20] “require that participants in the United States R&D enterprise who significantly influence the design, conduct, reporting, reviewing, or funding of Federally-funded research disclose appropriate information, consistent with Sec. 4(b) of this memorandum, that will enable reliable determinations of whether and where conflicts of interest and commitment exist, consistent with applicable Federal laws and regulations”

[21] “cooperate with organizations receiving Federal funds to ensure that the organizations have established and administer policies and processes to identify and manage risks to research security and integrity, including potential conflicts of interest and commitment”

研究資金、研究セキュリティ、インテグリティに悪影響を及ぼす可能性のある開示を、各機関の監察官（Inspector General）や法執行機関と協力し、適用される法律と整合するように特定する。[22]
開示要求を順守していない疑いのある事例の調査において、必要に応じて各機関の監察官及び法執行機関と協力する。[23]
開示方針への違反や、米国の研究開発事業のセキュリティとインテグリティを脅かすその他の活動への関与に対し、適切かつ効果的な帰結があるようにし、それを適用する。[24]
国土安全保障長官は、国土安全保障省（DHS）が国務省と連携し、米国の研究開発事業に参加・参画しようとする非移民学生及び交換訪問者の外国人個人を国家安全保障上のリスクについて確かに審査する責任がある。国土安全保障長官は、教育及び文化交流プログラムのために米国に来る外国人の合法的な入国と滞在を支援しながら、国家の安全を守るために、留学生及び研究者に関する情報を DHS が保持することを、適用法に沿って確実に行う責任がある。[25]
国家情報長官（DNI）は、米国の研究開発事業の安全保障に関連するような、外国アクターの能力、活動、意図を特定し評価するための情報コミュニティの取組を調整する。[26]
科学技術政策局（OSTP）長官は、米国科学技術会議（National Science and Technology Council: NSTC）を通じて、連邦政府資金による研究開発を外国政府の干渉から守るための活動と、研究セキュリティに対するリスクとこれらのリスクに対応する連邦政府の行動に対する認識を高めるための米国の科学界及び学術界への働きかけを調整する。[27]

[22] “identify, in cooperation with agency Inspectors General and law enforcement agencies as appropriate and as consistent with applicable law, disclosures that have the potential negatively to impact research funding, security, or integrity”
[23] “cooperate with agency Inspectors General and law enforcement, as appropriate, in investigation of suspected instances of failure to comply with disclosure requirements”
[24] “ensure the availability and application of appropriate and effective consequences for violations of disclosure policies and for engagement in other activities that threaten the security and integrity of the United States R&D enterprise.”
[25] “The Secretary of Homeland Security is responsible for ensuring that DHS, in conjunction with the Department of State, screens foreign individuals who are nonimmigrant students and exchange visitors seeking to participate or participating in the United States R&D enterprise for national security risks. The Secretary of Homeland Security is also responsible, consistent with applicable law, for ensuring that DHS maintains information regarding foreign students and researchers to protect national security while supporting lawful entry and stay of foreign individuals coming to the United States for educational and cultural exchange programs.”
[26] “The Director of National Intelligence (DNI) shall coordinate Intelligence Community efforts to identify and assess the capabilities, activities, and intentions of foreign actors as they relate to the security of the United States R&D enterprise.”
[27] “The Director of the Office of Science and Technology Policy (OSTP), through the National Science and Technology Council (NSTC), shall coordinate activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks.”

Section 4（Priorities）では、より具体的に、8 項目（「(a) 研究セキュリティリスクと保護への認識向上」、「(b) 情報開示の要件とプロセスの強化」、「(c) アクセス及び参加制限」「(d) 外国人留学生・研究者の審査」、「(e) 情報の共有」、「(f) 研究セキュリティ教育」、「(g) リスクの特定と分析」、「(h) 国際的な研究開発協力の推進と保護」）のそれぞれについて、連邦省庁・資金配分機関に対して求める事項が記載されている。具体的内容は、それぞれ以下のとおりである。

① 研究セキュリティのリスクと保護に関する認識の向上[28]

表 2-4：研究セキュリティのリスクと保護に関する認識の向上に関する事項（NSPM-33，セクション 4 (a)）

※赤は支援事項（連邦研究資金を受けとる組織等への支援）に関連。

要求相手機関	内容
大統領府科学技術政策局の長	DNI 及び必要に応じて他の連邦省庁の長と連携し、米国の研究開発事業に関与して、**研究セキュリティ及び研究インテグリティへのリスク、及びこれらのリスクを軽減するための政策や手段についての認識を高める**。[29]
国家情報長官（DNI）	他の連邦省庁の長と連携し、適用する法に従い、他の省庁、連邦・州・地方政府職員、研究機関、民間セクター、同盟国・パートナーへの普及に適した**研究セキュリティに関する情報・情報成果物を作成**する。[30]

[28] “Enhance Awareness of Research Security Risks and Protections”
[29] “in coordination with the DNI and heads of other agencies as appropriate, shall engage with the United States R&D enterprise to enhance awareness of risks to research security and integrity and policies and measures for mitigating these risks.”
[30] “develop, in coordination with the heads of other agencies, information and intelligence products related to research security that are suitable for dissemination, in accordance with applicable law, to other agencies; to Federal, State, local, and tribal officials; to research institutions; the private sector; and to allies and partners.”

② 情報開示の要件とプロセスの強化[31]

表 2-5：情報開示の要件とプロセスの強化に関する事項（NSPM-33，セクション 4 (b)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（連邦研究資金を受けとる組織等への支援）に関連。

要求相手機関	内容
資金配分機関の長	連邦政府資金による研究開発事業の参加者に対して、潜在的な利益相反・責務相反に関連する**情報の開示を要求**する。[32]
連邦省庁	連邦政府資金による研究開発事業の以下の**関係者**からの情報開示を要求する。 ・連邦政府の研究開発資金を求める、あるいは受け取る主任研究者（PI）及びその他のシニア／キーパーソン。 ・連邦政府研究費の配分プロセスに参加する個人：プログラムオフィサー、査読者、諮問委員会・パネルのメンバー。 ・連邦機関の研究所及び施設の研究者（すなわち、連邦政府に雇用されているか否かを問わず、内部の研究者）（政府所有請負業者運営（GOCO）の研究所・施設を含む）。[33]
連邦省庁	**以下の開示を要求**する。 ・所属及び雇用 ・その他の支援及び資金源 ・海外のプログラム及び契約（「外国政府主催の人材採用プログラム」を含む） ・役職及び任命[34]
資金配分機関の長	【12 か月以内】に下表の情報の開示を求める方針を作成する。[35]（→図 2.1）

[31] “Strengthen Disclosure Requirements and Processes”

[32] “require the disclosure of information related to potential conflicts of interest and commitment from participants in the Federally funded R&D enterprise.”

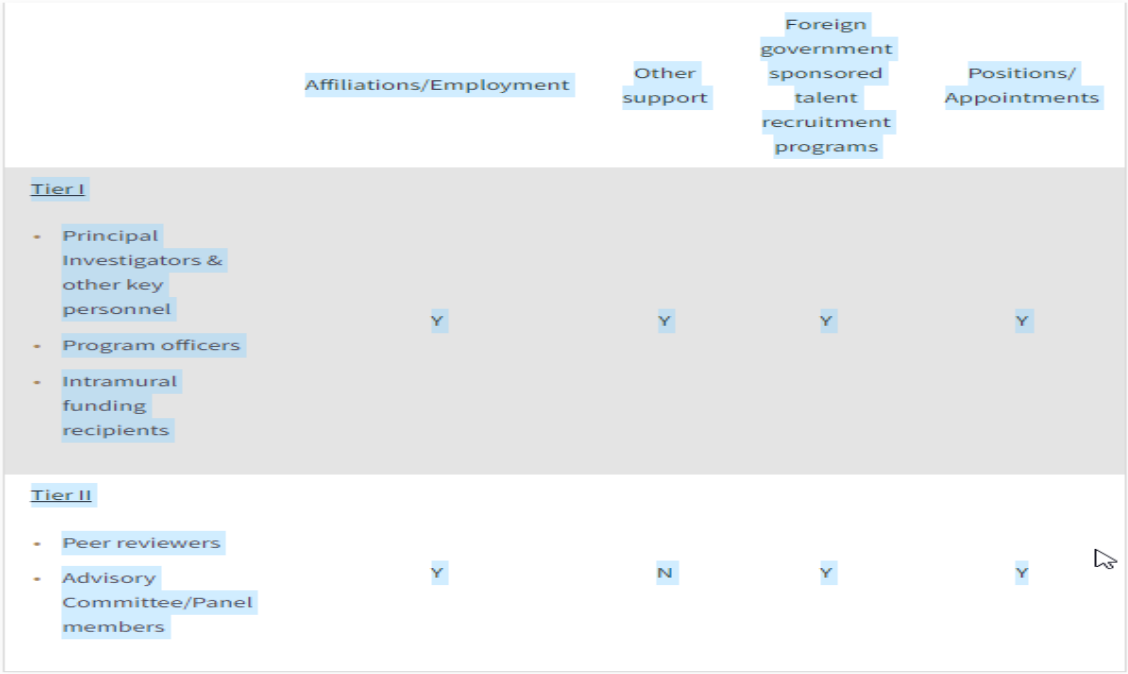
[33] “require disclosure from the following segments of the Federally funded R&D enterprise:
- Principal investigators (PIs) and other senior/key personnel seeking or receiving Federal R&D funding (i.e., extramural funding);
- Individuals participating in the process of allocating Federal funding: program officers, peer/merit reviewers, and members of advisory panels and committees; and
- Researchers at Federal agency laboratories and facilities (i.e., intramural researchers, whether or not Federally employed), including government owned, contractor-operated laboratories and facilities.”

[34] “require the following disclosures, : Affiliations and employment; Other support and funding sources; Foreign programs and contracts（including foreign government-sponsored talent recruitment programs）; and Positions and appointments”

[35] “establish policies requiring disclosure of the information reflected in the table below”

要求相手機関	内容
連邦省庁	初回の情報開示と、開示された**報告の更新**を求める。[36]
資金配分機関	【1 年以内】に連邦研究助成金の支援を受け、あるいはそれに従事する個々の研究者が、その個人の**永続的デジタル識別子**（digital persistent identifier）を提供するサービスに登録する要件に関する方針を作成する[37]。 **[Implementation Guideline (2022/1)で実施細目②を決定（後述）]**
資金配分機関	可能な限り、資金配分機関間で**開示プロセス、定義、書式を標準化**する。[38] **[Implementation Guideline (2022/1)で実施細目①を決定（後述）]**
行政管理予算局の長	OSTP、政府倫理局（Office of Government Ethics）、その他の機関と協力し、利益相反や責務相反の開示に関連する**方針と書式の標準化**を調整する。[39]
教育省長官	高等教育法第 117 条[40]の施行を通じて、**高等教育機関と海外との関係における財政的透明性**を促進することにより、学問の自由と国家安全保障との間のバランスを取ることを引き続き支援する。[41]
連邦省庁	開示要件に対する**潜在的な違反を特定し調査する仕組みと能力を強化**する（そのために、監察官、法律顧問、法執行機関、大学のプログラムオフィスやセキュリティ担当者、民間部門と協力する）。[42]
連邦省庁	**開示要件違反、及び研究セキュリティとインテグリティを脅かすその他活動への関与**に対して、**適切かつ効果的な帰結**を確かなものにする。[43] **[Implementation Guideline (2022/1)で実施細目③を決定（後述）]**

[36] “require initial disclosures and updates to disclosure reporting”
[37] “stablish policies regarding requirements for individual researchers supported by or working on any Federal research grant to be registered with a service that provides a digital persistent identifier for that individual.”
[38] “standardize disclosure processes, definitions, and forms across funding agencies to the extent practicable.”
[39] “work with OSTP, the Office of Government Ethics, and other agencies to coordinate the standardization of policies and forms related to disclosure of conflicts of interest and commitment.”
[40] 総額で 25 万ドル以上の贈与又は契約を海外から受け取っている高等教育機関は教育省に報告する必要がある。
[41] “continue to support the balance between academic freedom and national security by promoting financial transparency in the relationship between institutions of higher education (IHEs) and foreign sources through enforcement of section 117 of the Higher Education Act.”
[42] “strengthen mechanisms and capabilities to identify and investigate potential violations of agency disclosure requirements（そのために work with their Inspector General, General Counsel, law enforcement, university program offices and security officers, and the private sector）.”
[43] “ensure appropriate and effective consequences for violation of disclosure requirements and engagement in other activities that threaten research security and integrity”



	Affiliations/Employment	Other support	Foreign government sponsored talent recruitment programs	Positions/ Appointments
Tier I - Principal Investigators & other key personnel - Program officers - Intramural funding recipients	Y	Y	Y	Y
Tier II - Peer reviewers - Advisory Committee/Panel members	Y	N	Y	Y

図 2-1：資金配分機関の長が開示を求める情報（12 か月以内に方針を作成）

③ アクセス及び参加の制限

表 2-6：アクセス及び参加の制限に関する事項（NSPM-33，セクション 4 (c)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
連邦省庁の長	米国政府の研究施設へのアクセスと利用を管理・追跡する方針とプロセスを各機関が持つようにすること。[44]
連邦省庁の長	【12 か月以内】に、米国研究開発事業の参加者であり、それぞれの機関に現在雇用されている連邦職員が「外国政府主催の人材採用プログラム」に参加することを禁止する方針を定めるか、又は適用可能な既存の方針を明確化すること[45]、など。

[44] “ensure that their respective agencies have policies and processes to control and track access to and utilization of United States Government research facilities”

[45] “establish policies, or clarify existing policies where applicable, that prohibit Federal personnel currently employed by their respective agencies who are also participants in the United States R&D enterprise from participating in foreign government-sponsored talent recruitment programs.”

④ 外国人留学生・研究者の審査

表 2-7：外国人留学生・研究者の審査に関する事項（NSPM-33，セクション 4 (d)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
国務省長官 （国土安全保障省長官と調整）	留学生や研究者の審査プロセスが、米国の研究開発に対するリスクの性質の変化を反映するようにすること。[46]
国務省長官	米国での留学や研究活動を希望するビザ申請者の審査に、ビザ資格に適用されるすべての基準に基づき、リスクに基づくプロセス（risk-based process）を適用する。[47] 米国法に基づく関連基準に基づき、ビザ申請の審査に関連する場合において、領事がビザ申請者に関わる以下の情報を収集し考慮できるよう、必要な措置を講じる。 ・雇用及び職歴 ・経済的支援源 ・教育歴（教育機関、学位、研究指導教官を含む）。 ・現在及び過去の研究開発提携及びプロジェクト。 ・外国政府主催の人材採用プログラムへの現在及び申請中の参加状況。 ・学習・研究のプログラム ・予定されている業務の施設と場所。[48]
国土安全保障省長官	【3 か月以内】に、関連機関に対して以下を実施することを要求するために必要な規制と技術の更新を評価する。 ・留学生・交流訪問者情報システム（SEVIS）において、報告対象となる留学生及び研究者について、Section(d)(i)で規定された情報（※本表上記の情報）を報告すること。 ・SEVIS の更新を毎年、あるいは適切な場合にはより頻繁に行う。[49]

[46] “ensure that vetting processes for foreign students and researchers reflect the changing nature of the risks to United States R&D.”
[47] “apply a risk-based process to vet visa applicants seeking to study or conduct research activities in the United States, based on all applicable standards for visa eligibility.”
[48] “The Secretary shall take such steps as are necessary to ensure consular officers may collect and consider the following information pertaining to visa applicants, wherever relevant to the consular officer’s adjudication of a visa application based on relevant standards under United States law: Employment and employment history; Sources of financial support; Education history, including academic institutes, degree(s), and research advisor(s); Current and prior R&D affiliations and projects; Current and pending participation in foreign government-sponsored talent recruitment programs; Program of study and/or research; and Facility/facilities and location(s) of expected work.”
[49] “assess, within 3 months of the date of this memorandum, any regulatory and technical updates

要求相手機関	内容
	【上記の評価後、3 か月以内】に、国家安全保障担当大統領補佐官（APNSA）に対し、当該要件の実施に関する計画を提供する。[50]
国土安全保障省長官（国務省長官と調整）	【1 年以内】に、検索可能な中央データベースに Section 4 (d)(i)に規定された情報（※本表上記の情報）を含めることの実現可能性と有用性を評価する。[51]

⑤ 情報の共有（Information Sharing）

表 2-8：情報の共有に関する事項（NSPM-33，セクション 4 (e)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
連邦省庁の長	違反者に関する情報を、連邦資金配分機関全体、連邦法執行機関、国土安全保障省、州と共有する。 重大な懸念が生じたが最終決定がなされていない場合においては、他の連邦資金配分機関に通知することを検討する。[52] **[Implementation Guideline (2022/1)で実施細目④を決定（後述）]**

⑥ 研究セキュリティ教育

表 2-9：研究セキュリティ教育に関する事項（NSPM-33，セクション 4 (f)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	要求内容
資金配分機関の長	研究開発活動を行う、又は連邦研究開発資金の配分プロセスに参加する連邦機関の職員が、研究セキュリティのトレーニングを受けることを確実にする。[53]

necessary to require that relevant institutions:

- Report the same information specified above in section 4(d)(i) in the Student and Exchange Visitor Information System (SEVIS), for foreign students and researchers subject to reporting in that system; and,
- Provide updates in SEVIS annually, or more frequently where appropriate."

[50] "provide to the APNSA a plan regarding implementation of such requirements."

[51] "assess the feasibility and utility of including the information specified in section 4(d)(i) in a searchable centralized database."

[52] "share information about violators across Federal funding institutions and with Federal law enforcement agencies, the DHS, and State", "consider providing notice to other Federal funding institutions in cases where significant concerns have arisen but a final determination has not yet been made."

[53] "ensure that Federal agency personnel conducting R&D activities or participating in the process of allocating Federal R&D funding receive research security training."

⑦ リスクの同定と分析（Risk identification and analysis）

表 2-10：リスクの同定と分析に関する事項（NSPM-33，セクション 4 (g)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
資金配分機関の長	【12 か月以内】 年間 5,000 万ドルを超える連邦科学技術助成金を受ける研究機関は、「研究セキュリティプログラム」を確立し運営していることを資金配分機関に対して証明することを義務付ける。[54] 「研究セキュリティプログラム」には、サイバーセキュリティ、海外渡航セキュリティ、インサイダー脅威の認識と特定、及び必要に応じて輸出管理トレーニングの要素が含まれるべきである。[55] 米国の国家安全保障や経済安全保障に影響を与える重要な新興技術分野の研究開発で連邦資金を受ける機関には、研究セキュリティプログラムの追加要件が適切かどうか検討する。[56] **[Implementation Guideline (2022/1)で実施細目⑤を決定（後述）]**

⑧ 国際研究開発協力の促進と保護

Promote and Protect International R&D Cooperation

表 2-11：国際研究開発協力の促進と保護に関する事項（NSPM-33，セクション 4 (h)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
国務省長官（OSTP の長と他の連邦省庁の長と調整）	研究セキュリティに対するリスクに対する認識を高め、国際的な保護と対応努力に関する協力を改善する政策と実践を促進する目的で、外国の同盟国やパートナーと協力する。[57]

[54] “require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program.”
[55] “Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training.”
[56] “consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.”
[57] “engage with foreign allies and partners with the goal of promoting policies and practices that increase awareness of risks to research security and improve cooperation on international protection and response efforts.”

Section 5

国家安全保障担当大統領補佐官は、行政管理予算局長、OSTP の長と協力して、この大統領覚書の実施を調整し、毎年、この大統領覚書を実施するために資金配分機関がとった活動の詳細を記した報告書を作成し、大統領に提出しなければならない、としている。

（ただし、年次報告書の公表はこれまでのところ行われていない）

(b) 米国の科学技術研究事業体のセキュリティとインテグリティを強化するための Recommended Practices（2021 年 1 月 19 日）

上記の大統領覚書が出されたのとほぼ同じ時期に、「アメリカの科学技術研究事業のセキュリティとインテグリティを強化するために推奨される実践内容」（Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise）が、米国科学技術会議（NSTC）の「研究環境に関する NSTC 合同委員会」（Joint Committee on the Research Environment）の「研究セキュリティ小委員会」（Subcommittee on Research Security）から公表された。[58]

研究セキュリティ小委員会は、図 2-2 のメンバーであり、上記の大統領覚書の宛先となっていた大統領府レベルの省庁、研究開発に関係する省庁、さらに、情報コミュニティの機関も含む。Subcommittee on Research Security の目的は、「米国の科学技術研究事業のセキュリティとインテグリティを、米国の価値観やイノベーションエコシステムの開放性を損なうことなく強化するために、連邦政府の取組を調整すること」である。特に、「適切かつ効果的なリスク管理の調整、学術研究機関への効果的なコミュニケーションとアウトリーチの提供に関する連邦政府の取組の調整、連邦政府が出資する研究事業のセキュリティとインテグリティに関する研究機関向けのガイダンスの作成、学術研究機関向けの推奨事例の作成に焦点を当てている」と説明している。(p.i)

[58] National Science and Technology Council. Joint Committee on the Research Environment. Subcommittee on Research Security. *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*. January 2021.

SUBCOMMITTEE ON RESEARCH SECURITY

Co-Chairs
Steve Binkley, Department of Energy
Helena Fu, Office of Science and Technology Policy
Rebecca Keiser, National Science Foundation
Mike Lauer, National Institutes of Health
Aaron Miles, Office of Science and Technology Policy

Members

Departments
Department of Agriculture
Department of Defense
Department of Education
Department of Energy
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation

Agencies
Federal Bureau of Investigation
Food and Drug Administration
National Aeronautics and Space Administration
National Institute of Standards and Technology
National Institutes of Health
National Oceanic and Atmospheric Administration
National Science Foundation
National Security Agency
Office of the Director of National Intelligence
United States Geological Survey
United States Patent and Trademark Office

Executive Office of The President
National Security Council
Office of Management and Budget
Office of Science and Technology Policy

出典：National Science and Technology Council. Joint Committee on the Research Environment. Subcommittee on Research Security. *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*. January 2021. p.i.

図 2-2：Subcommittee on Research Security（National Science and Technology Council の Joint Committee on the Research Environment に属する）のメンバー

本文書の目的は、「研究機関（大学、研究機関、民間企業等）が米国の研究事業のセキュリティとインテグリティをより良く保護するために取るべき推奨事項を提示すること」であり、「NSPM-33 を補完するもの」であると説明している(p.1)。

本文書を参考にして、大学・研究機関は研究セキュリティとインテグリティの向上に取り組むことができるものであり、連邦政府から大学・研究機関への一つの支援とみることができる。

本文書では、まず、研究セキュリティとインテグリティを向上させるに当たっての「基本原則と価値」（Foundational principles and values）について説明する。以下がその内容である。これらのうちで、「開放性」、「透明性」、「説明責任」は、研究者個人から研究機関、政府まで、すべてに関係するものであり、「公平性」、「客観性」、「正直さ」、「尊重」は、個人や組織が研究の厳密性と再現性を確保するためにどのように研究を行うべきかの核心となるものであると説明する。「探求の自由」、「互恵主義」、「実力主義的な競争」は、すべての人に関係し、特に政府が保護し育成する責任があるものである、と説明する。

- 開放性（openness）と透明性（transparency）は、生産的な協力を可能にし、潜在的な利益相反・責務相反を適切に開示するのに役立つ。

- 説明責任（accountability）と正直さ（honesty）は、誤りを認め、進歩を妨げかねない行動を正すのに役立つ。
- 公平性（impartiality）と客観性（objectivity）は、不適切な影響や科学的知識の歪曲から守る。
- 尊敬の念（respect）は、全ての人の意見を聞き、貢献できる環境づくりに役立つ。
- 探求の自由（freedom of inquiry）は、個人の好奇心が科学的発見につながるようにする。
- 互恵主義（reciprocity）とは、科学者や研究機関が、全ての協力パートナーに利益をもたらす方法で、材料、知識、データ、施設や自然の場所へのアクセス、及びトレーニングを交換することを確実にするものである。
- 実力主義的な競争（merit-based competition）は、最高のアイデアやイノベーションが前進できるような公平な競争の場を確保するのに役立つ。(p.2)

なお、上の説明で「利益相反」「責務相反」については以下のように定義している（p.2）。

「利益相反」：個人、又は個人の配偶者や扶養家族が、研究の設計、実施、報告、又は資金調達に直接かつ重大な影響を与える可能性のある金銭的利害又は関係を持っている状況[59]。

「責務相反」：複数の雇用主又は他の事業体の間で、個人が矛盾する義務を受け入れたり、負ったりする状況。多くの組織の方針では、組織や資金提供機関の方針や約束を越えて時間を割く義務など、相反する時間の約束を「責務相反」と定義している。雇用主や研究助成機関と不適切に情報を共有したり、情報を隠したりする義務など、その他の種類の矛盾した義務も、研究のセキュリティとインテグリティを脅かす可能性があり、より広い意味での「責務相反」の一要素である。[60]

「これらの基本原則や価値観に反する行動は、研究事業のインテグリティを危うくする。研究事業のインテグリティを脅かす行為は、しばしば研究事業のセキュリティ（研究セキュリティ）に対するリスクももたらす」[61]と説明している。(p.3)

表 2-12 は、研究セキュリティとインテグリティを強化するために推奨される実践内容の 21 項目を示す。文書では各項目について、2～3 段落程度の説明が付されている。

---

[59] “a situation in which an individual, or the individual’s spouse or dependent children, has a financial interest or relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.”

[60] “a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share information improperly with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment.”

[61] “Behaviors that violate these foundational principles and values jeopardize the integrity of the research enterprise. Behaviors that threaten the integrity of the research enterprise often also pose risks to the security of the research enterprise, which we term research security.” (p.3)”

表 2-12：研究セキュリティとインテグリティを強化するために推奨される実践内容

組織的なリーダーシップと監督機能の発揮
1. 研究のセキュリティとインテグリティの重要性を組織の指導層から伝える。
2. 研究セキュリティに対する組織的なアプローチを確保する。
3. 研究セキュリティとインテグリティのワーキンググループやタスクフォースを設置する。
4. 包括的な研究セキュリティプログラムを確立し、運用する。
開放性と透明性への期待を確立する。
5. 利益相反、責務相反、情報開示に関する組織方針を定め、運用する。
6. 潜在的な利益相反や責務相反を特定し、評価するために必要なすべての情報を組織に開示することを義務付ける。
7. 留学生や外国人研究者の情報を報告するための国土安全保障省の要求事項の遵守を徹底する。
8. 永続的デジタル識別子に関する方針を定める。
9. 外国からの贈与や契約を報告するための要件に確実に準拠する。
トレーニング、支援、情報の提供・共有
10. 研究事業の参加者に対して、責任ある研究の実施に関する研修を実施する。
11. 外国政府主催の人材採用プログラムへの参加を検討している者にガイダンスを提供する。
12. 研究セキュリティを強化するために、FBI 地方事務所と協力する。
13. 研究セキュリティとインテグリティに対するリスクを示す可能性のある状況や行動に対する認識を高め、それに対する保護策を講じる。
14. 情報開示に関するポリシーに違反する可能性がある場合、その情報を共有する。
組織の方針を遵守するための効果的なメカニズムを確保する。
15. 研究セキュリティとインテグリティを脅かす情報開示方針違反やその他の行為を発見するための効果的な手段を確立し、行使する。
16. 開示義務違反や研究セキュリティとインテグリティを脅かすその他の行為に対して、適切かつ効果的な帰結があることを保証する。
17. 雇用契約には、研究セキュリティとインテグリティを支援する条項を盛り込む。
共同研究及びデータに関連する潜在的なリスクの管理
18. 正式な研究パートナーシップを評価するための一元的な審査・承認プロセスを確立する。
19. 海外渡航の審査と指導のためのリスクベースのセキュリティプロセスを確立し、運用する。
20. 外国人訪問者及び客員研究者に関連する潜在的なリスクを管理する。
21. 効果的なデータセキュリティ対策を確立し、維持する。

出典：National Science and Technology Council. Joint Committee on the Research Environment. Subcommittee on Research Security. *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*. January 2021. pp.6-15.

(c) 2021 年度国防権限法（National Defense Authorization Act: NDAA）（2021 年 1 月）

2021 年 1 月 1 日に 2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）が制定され、その第 223 条（42 U.S.C. § 6605（Disclosure of funding sources in applications for Federal research and development awards）として法編纂）で、すべての連邦研究機関（資金配分機関）が申請プロセスの一環として現在及び未決（pending）の支援についての情報開示を申請する研究者から求めること等が義務付けられた。

申請者は、過去 3 年間に受けた、又は現在受けている、又は申請中（未決）の外国政府や外国組織からの資金提供や支援をすべて開示しなければならない。申請者は、自分自身や共同研究者が外国政府や外国組織から受けた、又は現在受けている、任命や称号、職位や役職をすべて開示しなければならない。開示された情報は、連邦政府のデータベースに保存される。開示義務違反が発覚した場合には、連邦政府は助成金の支払いを停止したり、返還を求めたりすることができる。

表 2-13：2021 年度国防権限法第 223 条「連邦研究開発アワード（awards）への申請書における資金源の開示」

※青は要求事項（連邦省庁・資金配分機関等に対する要求）。

(a)　開示要求（Disclosure requirement）

要求相手	要求内容
連邦研究機関	各連邦研究機関は、当該機関からの研究開発アワードの申請書の一部として、以下を要求するものとする。
研究者（提案者）	(1)申請書に記載された、研究に参加する個人が (A)開示時点において、個人が受けている、又は受けると予想される、現在及び未決のすべての研究支援の金額、種類、及び提供元を開示すること。 (B)開示が現在、正確かつ完全であることを証明すること。 (C)支援の授与前に機関の要請があった場合、及び授与期間中に機関が適切と判断した場合に、当該開示を更新することに同意すること。
研究者を雇用するエンティティ	(2)当該アワードを申請するエンティティは、当該エンティティに雇用され、申請書に記載された各対象者が、第(1)項に基づく要件を知らされていることを証明すること。

注）「連邦研究機関」（federal research agency）とは、年間の外部研究費が 1 億ドルを超える連邦機関（研究資金配分機関）をいう。アワードは助成金（grant）、契約（contracts）、研究協力（cooperative agreement）を含む。エンティティは大学や研究機関を通常は意味する。

(b) 一貫性（Consistency）

要求相手	要求内容
科学技術政策局長	科学技術政策局長（Director of the Office of Science and Technology Policy）は、国家科学技術会議（National Science and Technology Council）を通じて行動し、2020 会計年度国防権限法（公法 116-92；42 U.S.C. 6601）1746 条(a)に基づく権限[62]に従い、(a)項に基づき連邦研究機関が発する要件に一貫性があることを確保する。

(c) 強制執行（Enforcement）

要求相手	要求内容
連邦研究機関	(1) 連邦研究機関は、第(a)項に基づき個人が開示した現在及び未決の研究支援が、連邦法又は機関の条件に違反する場合、研究開発アワードの申請を却下することができる。 (2) 研究開発賞に対する事業体の申請書に記載された対象個人が、(a)項に基づく情報の開示を故意に怠った場合、連邦研究機関は、以下の措置の 1 つ以上を講じることができる。 (A) 申請を却下する。 (B) 当該機関が当該個人又はエンティティに授与した研究開発アワードを一時停止又は終了させる。 (C) 当該個人又は団体に対する当該機関からの一切の資金提供を一時的又は永久的に中止する。 (D) 連邦規則集第 2 編第 180 部（part 180 of title 2, Code of Federal Regulations）、後継規則、又は他の適切な法律や規則に従って、個人又は団体を政府資金の受領から一時的又は永久に停止又は免除する。 (E) 第(a)項に基づく開示の不履行について、さらなる調査のために関係省庁の監察官に、又は刑事法もしくは民事法に違反したかどうかを調べるために連邦法執行当局に照会する。 (F) 他の機関に警告するために、個人又はエンティティをコンプライアンス違反として「連邦アワード受領者パフォーマンス・インテグリティ情報システム」（Federal Awardee Performance and Integrity Information System）に登録する。 (G) 個人又はエンティティに対して、適用される法律又は規則の下で許可されるその他の措置をとる。

[62] 2020 年度国防権限法（FY 2020 National Defense Authorization Act (NDAA)）第 1746 条で OSTP が主導し、NSTC に米国科学技術への海外からの干渉等からの保護等を検討するための省庁間ワーキンググループの設置すること、OSTP は検討の調整をすること等とされている。

	(3) 第(2)項に記載された強制措置は、以下の場合にのみ、エンティティに対して講じることができる。 (A) エンティティが第(a)項(2)の要件を満たしていない。 (B) エンティティは、対象個人が第(a)(1)項に基づく情報の開示を怠ったことを知りながら、申請書が提出される前に当該非開示を是正するための措置を講じなかった。 (C) 当該連邦研究機関の長が以下のように決定する。 (i) そのエンティティは、対象となる個人によって所有、支配、又は実質的に影響を受けている、及び (ii) 当該個人が、故意に第(a)(1)項に基づく情報の開示を怠った。 (4) 通知 (1)又は(2)に基づく措置を講じようとする連邦研究機関は、可能な限り、連邦規則集 2 巻 180 部、後継規則、又はその他の適切な法律もしくは規則に従って、当該措置の対象となる各個人又はエンティティに、当該措置の具体的な理由を通知し、当該個人及び団体に、提案された措置に異議を申し立てる機会及び手続きを提供しなければならない。 (5) 証拠となる基準 第(2)項(D)に基づき資格停止又は剥奪を求める連邦研究機関は、連邦規則集第 2 編第 180 部、後継規則、又はその他の適切な法律又は規則に定められた手続き及び証拠基準に従うものとする。

注)「連邦規則集第 2 編第 180 部（part 180 of title 2, Code of Federal Regulations）」は、OMB Guidelines to Agencies on Governmentwide Debarment and Suspension (Nonprocurement)である。
出典）Cornell Law School. Legal Information Institute. 42 U.S. Code § 66–5 - Disclosure of funding sources in applications for Federal research and development awards <https://www.law.cornell.edu/uscode/text/42/6605>に基づき作成。

(d) NSPM-33 実施ガイダンス（2022 年 1 月 4 日）

2022 年 1 月 4 日、NSPM-33 を実施するためのガイダンスを発表した（*Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*）。公表したのは、前術の文書と同じく、米国科学技術会議（NSTC）の「研究環境に関する NSTC 合同委員会」（Joint Committee on the Research Environment）の研究セキュリティ小委員会（Subcommittee on Research Security）である。[63]

[63] National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States*

本文書の目的は、「連邦省庁に対し、NSPM-33 の実施に関する指針を提供すること」であり(p.i)、各機関がその実施努力に適用すべき一般的なガイダンス（general guidance）に続き、NSPM-33 で取り上げられた 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の帰結、4. 情報の共有、5. 研究セキュリティプログラム）におけるより詳細なガイダンスを含む（p.ix)。

NSTC の議長であり、科学技術に関する大統領補佐官、かつ OSTP の長である Dr. Eric Lander は、前文で以下のように本文書の位置づけ、今後の課題について説明している（p.x～xi)。

- 我々が直面している研究セキュリティ上の課題は現実的かつ深刻であり、中国政府を含む一部の外国政府は、我々の最先端技術を不正に取得しようと懸命に努力している。これは容認できない。
- この実施指針は、私が 2021 年 8 月に打ち出した原則、すなわち、米国のセキュリティと開放性を守ること、善意の研究者が容易かつ適切に遵守できるよう明確にすること、政策が外国人嫌悪や偏見を助長しないようにすることを反映したものである。しかし、これらの重要な目標を達成するためには、まだまだやるべきことがある。
- 次の段階として、私は現在、連邦研究機関に対し、今後 120 日以内に、あらゆる連邦研究助成機関が使用できる（必要に応じて修正する）モデル助成金申請書と説明書（model grant application forms and instructions）を共同で開発するよう指示している。その目的は、政府が知るべきことを明確に記述し、研究者がどの資金配分機関に申請するかにかかわらず、可能な限り同じ情報を同じ方法で報告できるようにすることである。
- NSPM-33 に関する現在の取組は、研究者が連邦政府に情報を開示する方法を明確にし、簡素化しようとするものであるが、NSPM-33 の実施に関する他の重要な課題、すなわち、政府が研究資金や支援に関する決定を下す際にこの情報をどう利用するのかについては対処されていない。そのような課題も同様に重要であり、OSTP は将来的にそれらに対応するつもりである。

なお、このガイダンスでは、”research organization（研究組織）”、”federal research agency（あるいは research agency）（連邦研究省庁又は研究省庁）”について以下のように定義している。

”research organization”：「連邦研究機関に研究開発助成を申請した、又は助成を受けた事業体。この用語は、2021 年 NDAA（国防受権法）第 223 条に定義される「事業体」と同じ意味である。」[64]

Government-Supported Research and Development. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>

[64] “An entity that has applied for or received an R&D award from a Federal research agency. This term has the same meaning as “entity” as defined in Section 223 of the NDAA for 2021.”

”federal research agency（research agency）”:「年間 1 億ドル以上の外部研究費を有する連邦省庁。この用語は、NSPM-33 の「資金配分機関」と同じ意味を持つ。」[65]

①情報開示の要件と標準化（Disclosure requirements and standardization）

・NSPM-33 の関連箇所は、Section 4(b)である。
・ガイダンスの目的は、「開示要件（誰が何を開示するか、関連する制限と除外など）、開示プロセス（更新、訂正、認証、裏付け文書の提供など）、及び省庁横断的な統一性の期待度について明確にする」ことである。
・以下の 15 項目の実施ガイダンスについて説明している[66]。なお、1.と 2.については標準化により、申請者の負担を軽減するという意味で「支援」とここでは分類している。

表 2-14：「情報開示の要件と標準化」についての実施ガイダンス項目

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

項目内容	要求元	要求先
1. 開示要求事項の標準化	―	連邦省庁
2. 開示様式・書式の標準化	―	連邦省庁
3. 査読者・諮問委員会委員の所属・役職の開示要件	連邦省庁	査読者等
4. 学生を含める開示要件の拡大の可能性	―	連邦省庁
5. 研究開発助成の申請プロセス（助成及び助成後の要素を含む）において要求される Tier I 開示要件に関連する情報収集	―	連邦省庁

[65] Any Federal department or agency with an annual extramural research expenditure of over $100,000,000. This term has the same meaning as “funding agency” in NSPM-33.

[66] 1. Standardization of disclosure requirements
2. Standardization of disclosure forms and formats
3. Requirements for peer reviewer and advisory committee member disclosure of affiliations and positions
4. Potential broadening of disclosure requirement to include students
5. Collection of information associated with the required Tier I disclosure requirements within R&D award application processes (including pre-award and post-award elements)
6. Collection of information related to financial conflicts of interest within R&D award application processes
7. Exclusions from disclosure requirements within R&D award application processes
8. Clarification regarding exclusion of gifts from disclosure requirements
9. Requirements for disclosing core facilities and shared equipment
10. Requirements for disclosing participation in foreign programs
11. Requirements for disclosure of foreign contracts to research agencies
12. Just-in-time submission of application information
13. Requirements for updating disclosures after an award has been made
14. Process(es) for individuals to correct inaccurate or incomplete submissions
15. Requirements and processes for research organizations applying for R&D awards to provide certification related to disclosure requirements

項目内容	要求元	要求先
6. 研究開発助成の申請手続きにおける利益相反に関連する情報収集	連邦省庁	研究組織
7. 研究開発助成申請プロセスにおける開示要求事項の適用除外	―	連邦省庁
8. 贈答（gifts）を開示対象外とすることについての明確化	―	連邦省庁
9. 中核施設及び共用設備の開示要件	連邦省庁	研究者
10. 海外プログラムへの参加に関する開示要件	連邦省庁	研究者
11. 資金配分機関に対する外国契約の開示要件	連邦省庁	研究者
12. 申請情報のジャストインタイム提出	―	連邦省庁
13. 助成後の開示内容の更新の必要性	連邦省庁	研究者
14. 不正確又は不完全な提出を個人が訂正するための手続き	―	連邦省庁
15. 研究開発助成を申請する研究機関が、開示要件に関連する証明書を提出するための要件と手続き	連邦省庁	研究組織

表 2-15：Tier I と Tier II の参加者の情報開示要件

Table 1. General NSPM-33 disclosure requirements for Tier I and Tier II participants.

Disclosures Required From:	Organizational Affiliations/ Employment	Positions/ Appointments	Foreign gov.-sponsored talent recruitment programs[3]	Current and pending support/ Other Support
Tier I • Principal investigators (PIs) and other senior/key personnel • Program officers • Intramural researchers[4]	Y	Y	Y	Y
Tier II • Peer reviewers • Advisory committee/Panel members	Y	Y	Y	N

出典：National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022. p.2.

表 2-16：研究開発助成プロセスにおける個人情報・専門家情報の開示のガイダンス

Table 2a. Guidance for disclosure of personal and professional information within R&D award application processes.

Type of Activity to be Disclosed	Biographical Sketch	Current & Pending/ Other Support	Annual Project Reports	Post-Award Information Terms & Conditions
PERSONAL INFORMATION				
Professional preparation (e.g., educational degrees)	✓			
Organizational Affiliations[#]	✓			
Academic, professional or institutional appointments, whether or not remuneration is received, and whether full-time, part-time, or voluntary	✓			
Paid consulting that falls outside of an individual's appointment; separate from institution's agreement		✓	✓	✓
RESEARCH FUNDING INFORMATION				
Current and pending support: All R&D projects currently under consideration from whatever source, and all ongoing projects, irrespective of whether support is provided through the proposing organization, another organization, or *directly* to the individual, and regardless of whether the support is direct monetary contribution or in-kind contribution (e.g., office/laboratory space, equipment, supplies, or employees)		✓	✓	✓
Current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs[6]	✓ (Appropriate placement may be contract-dependent)			
In-kind contributions not intended for use on the project/proposal being proposed		✓	✓	✓
Visiting scholars funded by an entity other than own institution		✓	✓	✓
Students and postdoctoral researchers funded by an entity other than own institution		✓	✓	✓
Travel supported/paid by an entity other than own institution to perform research activities with an associated time commitment		✓	✓	✓
Certification by the individual that the information disclosed is accurate, current, and complete		✓	✓	✓

[#]Some agencies may collect this information in Collaborators and Other Affiliations.

出典：National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022. p.4.

表 2-17：プロジェクト情報の開示のガイダンス

Table 2b. Guidance for disclosure of project information.

Type of Activity to be Disclosed	Facilities and Other Resources	Other
PROJECT INFORMATION		
In-kind contributions that support the research activity for use on the project/proposal being proposed	✓	
Private equity, Venture, or other capital financing*		✓
Supporting Documentation (e.g., contracts, grants, other agreements)^		✓

*See implementation guidance point 6 below.
^See implementation guidance point 11 below.

注：金銭的な利益相反がある場合には、株式等の情報開示が必要になる（第 2 項目）。また、海外政府との契約（外国人人材採用プログラムを含む）等がある場合にはその契約等の情報開示が必要になる（第 3 項目）。

出典：National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022. p.5.

②デジタル永続的識別子（Digital Persistent Identifiers）

・NSPM-33 の関連部分は、Section 4(b)(v)である。

・本項目のガイダンスの目的は、「研究機関が、管理負担を軽減しながら研究セキュリティとインテグリティを強化するために、デジタル永続的識別子（DPI）（あるいは永続的識別子（Persistent Identifiers: PID））を開示プロセスにどのように組み込むかを説明する」ことである。

・以下の 7 項目について説明している。[67] なお、申請者・申請機関の負担を軽減するという意味で「支援」とここでは分類している。

[67] "1. Incorporation of DPIs into grant and cooperative agreement application and disclosure processes
2. Requiring DPIs versus providing as an option for disclosures
3. Categories of individuals provided a DPI option for disclosures
4. Use of available DPI services
5. Common/core standards that a DPI service should meet to be included as an option for disclosure in Federal grant and cooperative agreement application processes
6. Ensuring interoperability across multiple options for DPI service
7. Potential for public disclosure of information provided to research agencies via a DPI service"

表 2-18：「デジタル永続的識別子」についての実施ガイダンス項目

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

項目内容	要求元	要求先
1. 助成金及び協力協定の申請及び開示手続きへの DPI の組み入れ	―	連邦省庁
2. DPI を要求するか、あるいは情報開示のオプションとして提供するか。	―	連邦省庁
3. DPI を情報開示の選択肢として提供する個人のカテゴリー	―	連邦省庁
4. 利用可能な DPI サービスを利用する	―	連邦省庁
5. 連邦補助金及び協力協定の申請手続きにおいて、DPI サービスが開示の選択肢として含まれるために満たすべき共通/中核的な基準	―	連邦省庁
6. DPI サービスの複数のオプションにまたがる相互運用性の確保	―	連邦省庁
7. DPI サービスを通じて連邦政府省庁に提供された情報の一般公開の可能性	―	連邦省庁

③情報開示要件違反への対応（Consequences for Violation of Disclosure Requirements）

・関連する NSPM-33 の項目は Section 4(b)(ix) である。
・本項目の目的は、「連邦政府省庁及び研究機関のための適切なレベルの柔軟性を維持しながら、適用される法律及び規制と一致する、情報開示要件の違反に対する適切な対応を決定するためのガイドラインを提供する」ことである。
・実施ガイダンスは以下の 8 項目についてそれぞれ記述されている。[68]

[68] "1. Consequences for violation of disclosure requirements
2. Other potential administrative actions available to research agencies to address noncompliance with disclosure requirements
3. Factors for consideration in determining appropriate administrative actions and other consequences
4. Provision of more detailed information regarding administrative remedy and enforcement processes
5. Encouraging individuals to come forward and correct past omissions
6. Notice and due process in agency consideration and application of regulatory administrative action
7. Circumstances for potential imposition of consequences on research organizations
8. Circumstances for potential suspension or denial of Higher Education Act (HEA) Title IV funds"

表 2-19：「情報開示要件違反への対応」についての実施ガイダンス項目

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

項目内容	要求元	要求先
1. 開示要件違反への対応	―	連邦省庁
2. 開示要求の不遵守に対処するために連邦政府省庁が利用可能なその他の潜在的行政措置	―	連邦省庁
3. 適切な行政措置及びその他の対応を決定する際に考慮すべき要素	―	連邦省庁
4. 行政上の救済措置及び執行プロセスに関するより詳細な情報の提供	―	連邦省庁・NSTC 研究セキュリティ小委員会
5. 個人が名乗り出て過去の不作為を訂正することを奨励する。	―	連邦省庁
6. 規制当局の行政措置の検討・適用における通知と適正手続き	―	連邦省庁
7. 研究組織に対して対応する可能性のある状況	―	連邦省庁
8. 高等教育法（HEA）第 IV 章の資金が停止又は拒否される可能性がある状況	―	連邦省庁

注）高等教育法（HEA）第 IV 章は、連邦政府による学生への奨学金プログラム（federal student financial aid）についての規定である。

表 2-20：開示要件不順守の研究機関に適用可能な、非強制的な行政措置・救済措置の例

Table 3. Examples of non-enforcement administrative actions and remedies that may apply to research organizations for noncompliance with disclosure requirements.

Category	Examples	Citation
Monitoring/ administrative actions	• Financial and performance reports • Site visits • Video conferences, telephone calls, e-mails	2 CFR §200.329, Monitoring and reporting program performance
Remedies for noncompliance	• Specific award conditions • Require payments as reimbursements rather than in advance • Withhold authority to proceed to next phase pending evidence of acceptable performance within a given performance period • Require additional, more detailed financial reports • Require additional project monitoring • Require the organization to obtain technical or management assistance • Establish additional prior approvals	2 CFR §200.208, Specific conditions.
	• Withhold cash payments pending correction of the deficiency • Disallow all or part of the cost of the activity/action not in compliance • Wholly or partly suspend or terminate the Federal award • Withhold further Federal awards for the project or program	2 CFR §200.339, Remedies for noncompliance

出典：National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022. p.13.

④情報共有（Information Sharing）

・関連する NSPM-33 の項目は、Section(e)である。

・本ガイダンス項目の目的は、「違反及び違反の可能性に関する情報を連邦省庁が共有できる状況を明確にするとともに、そのような共有が、プライバシーやその他の法的・合理的な保護を尊重するためにどのように制限されるかについての保証を提供すること」[69]である。

・ガイダンス項目は、以下の 5 項目である。[70]

[69] "Provide clarity regarding circumstances when agencies may share information regarding violations and potential violations, and provide assurance regarding how such sharing will be limited to respect privacy and other legal and reasonable protections"

[70] "1. Circumstances for research agency sharing with other agencies information about violations of disclosure requirements
2. Circumstances for appropriate research agency sharing of information prior to final determination of a violation
3. Mechanisms for research agency sharing of information regarding violations with each other and with the public
4. Mechanisms for research agency sharing of information regarding potential violations
5. Proper sharing of information about violations and potential violations"

表 2-21：「情報共有」についての実施ガイダンス項目

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

項目内容	要求元	要求先
1. 連邦政府省庁が開示義務違反に関する情報を他連邦機関と共有する状況	―	連邦省庁
2. 違反の最終決定前に連邦政府省庁が情報を適切に共有する状況	―	連邦省庁
3. 連邦政府省庁が違反行為に関する情報を、連邦政府省庁相互及び一般市民と共有するための仕組み	―	連邦省庁
4. 連邦政府省庁が違反の可能性に関する情報を共有するための仕組み	―	監察官・連邦省庁
5. 違反行為及び違反の可能性に関する情報の適切な共有の仕組み	―	連邦省庁

⑤研究セキュリティプログラム（Research Security Programs）

・関連する NSPM-33 の項目は、Section 4(g) である。

・本ガイダンスの目的は、「研究セキュリティプログラムの要件、研究組織がどのように要件を満たすことが期待されるか、また、連邦政府省庁がどのようにプログラムの内容開発に貢献するかについて、明確にする」ことである。

・ガイダンスは以下の 9 項目について説明されている。[71]

[71] “1. Requirements for research security programs
2. Determination of which research organizations are subject to the requirement
3. Standardization of program requirements across organizations
4. Process for finalizing and implementing the requirement
5. Development of research security program content
6. Ensuring that cybersecurity elements of research security programs meet the objectives of the requirement
7. Certification of compliance with the requirement
8. Discretion of research organizations in structuring research security programs
9. Timeline for research organizations to establish compliance”

表 2-22：「研究セキュリティプログラム」についての実施ガイダンス項目

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

項目内容	要求元	要求先
1. 研究用セキュリティプログラムへの要求事項	連邦省庁	研究組織
2. どの研究組織が要求事項の対象となるかの決定	連邦省庁	研究組織
3. 組織横断的なプログラム要求事項の標準化	連邦省庁	研究組織
4. 要求事項の最終決定と実施のプロセス	―	OSTP（NSTC 研究セキュリティ小委員会、OMB 等と調整）
5. 研究セキュリティプログラム内容の開発のための指導的な技術的支援の提供	―	連邦省庁（特に、National Counterintelligence Task Force 、National Counterintelligence and Security Center）
6. 研究セキュリティプログラムのサイバーセキュリティ要素が、要求事項の目的に合致していることを確認する。	連邦省庁	研究組織
7. 要求事項への適合の証明	連邦省庁	研究組織
8. 研究セキュリティプログラムの構築における研究組織の裁量	連邦省庁	研究組織
9. 研究組織がコンプライアンスを確立するためのタイムライン	連邦省庁	研究組織

(2) 2022 年度の動き

(a) The CHIPS and Science Act of 2022 (H.R. 4346)（2022 年 8 月 9 日）

The CHIPS and Science Act of 2022 は 2022 年 8 月 9 日にバイデン大統領が署名し、成立した。米国で半導体を生産するインセンティブの創出に関する活動を行うため、CHIPS 基金（Creating Helpful Incentives to Produce Semiconductors for America Fund）を設立し、その資金を提供する等の内容を含む。

法律は、Division A（CHIPS Act of 2022）と、Division B（Research and Innovation）の 2 部構成である。Division A では、半導体インセンティブに 5 年間で 527 億ドルを計上（appropriation）、そのうち、先端研究開発に 110 億ドル計上すること、米国内の半導体製造施設に対する新たな投資税額控除などが含まれる。また、中国での半導体製造能力拡大が制限され、CHIPS 資金と投資税額控除の受給者は、レガシーチップの製造を除き、10 年間中国での半導体製造の拡大を禁止することが規定されている。Division B では、研究開発プログラムに対する 1700 億ドルの支出権限（authorization）がなされ、NSF（810 億ドル）、DOE（170 億ドル）、NIST、その他の DOC を含む複数の連邦機関の研究開発イニシアティブに対する 5 年間の資金の支出権限が認可された。[72]

また、この法律は、Division B に研究セキュリティに関する規定を含む（Division B : Title III−National Science Foundation for the Future, Subtitle D−NSF Research Security と、Title VI−Miscellaneous Science and Technology Provisions, Subtitle D−Research Security など）。具体的には、表 2-23 に示すように、以下のような NSF に対する要求規定を含んでいる。[73]

- Research Security and Policy Office を設置し、研究開発助成の申請及び NSF への情報開示に関するリスク評価を実施する権限を付与すること。
- 研究機関や研究者がセキュリティリスクを理解し軽減できるよう、独立したリスク評価センターを設立すること。
- 研究セキュリティの責任者を設置し、研究者にガイダンスとリソースを提供する。

[72] Julia Jester, Toby Smith. Chips and Science Act. Association of American Universities. ARIS Office Hours, October 28, 2022; About the "CHIPS and Science Act" <https://beta.nsf.gov/chips>
[73] NSF. “About the "CHIPS and Science Act"” https://beta.nsf.gov/chips
https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/
https://www.aau.edu/key-issues/chips-and-science-act-summary-research-security-provisions

表 2-23：The CHIPS and Science Act of 2022 の研究セキュリティ関連の規定の概要

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

要求・支援の対象	内容
大統領府科学技術政策局（OSTP）	外国人人材採用プログラム（Foreign Talent Recruitment Programs）のガイドライン作成（Sec.10631） ・（FY2020 国防授権法 1746 条に基づき設立された）省庁間ワーキンググループと連携し、連邦研究機関に対し、外国人人材採用プログラムに関する統一したガイドラインを配布することを OSTP に要求。ガイドラインは、各連邦研究機関のすべての職員が外国人人材採用プログラムに参加することを禁止し、外国人人材採用プログラムの特徴を定義して説明する。2021 年度国防授権法 223 条に従い、研究助成申請書の主要研究者は、外国人人材採用プログラムの契約・協定・取決めの当事者である場合に情報開示しなければならず、また、悪意のある外国人人材採用プログラムに参加することはできない。
資金配分機関（一部は、資金配分機関→研究者・研究機関）	悪質な外国人人材採用プログラム（Malign Foreign Talent Recruitment Program）への参加の禁止（Sec.10632） ・各連邦機関に対し、研究助成金提案プロセスの一環として、提案書提出時又はその後毎年、助成期間中、対象個人が悪質な外国人人材採用プログラムに参加していないことを証明するよう求める方針を確立することを要求する。
	契約等をレビューするための資料を研究機関に要求する権限付与（Sec.10633） ・各連邦機関は、要請に応じて、研究開発助成の申請書に記載された全ての対象者について、外国人人材採用プログラムへの参加に特有の契約書、補助金、又は外国人任命、外国機関への雇用、その他の合意書の写しを含む、補足書類を提出するよう機関に求める権限を有している。研究機関と協議の上、契約、助成金、協定が、機関が支援する活動の能力を阻害する、又は機関が支援する活動との重複を生じさせると判断された場合、連邦研究機関と受領機関は、対象者の代替又は助成からの除外、助成額の削減、助成の停止/終了を開始することができる。各連邦機関は、最終的な行政措置が取られる前に、全ての対象者のプライバシーを保護し、措置の正当な理由を提供し、対象者にコメントや反論を提供し上訴する機会を与えるために必要な措置を講じるべきである。
	連邦政府研究資金を使う研究者：研究セキュリティ研修要件（Sec.10634） ・資金配分機関は、研究資金の公募申請の一部として、申請書に記載された各対象者は研究セキュリティ訓練の修了（過去 1 年以内）を認証するという要件を設ける。 ・大学・研究機関は、雇用されている各対象者がそのような訓練を修了していることを証明する。 ・研究セキュリティ研修の内容は、サイバーセキュリティ、国際共同研究、海外渡航、海外からの介入、資金の適切な使用に関する規則、情報開示、責務相反、利益相反に焦点を当てる。
Comptroller General（GAO 長官）	研究資金の会計（Sec.10635） ・Comptroller General（※GAO の長官）に対し、研究のために懸念される外国組織が利用できる連邦資金に関する調査を実施することを要求する。この調査は、研究のために懸念される外国組織が利用できる連邦資金の量、種類、要件に関する評価を含むものとする。
NSF（一部は、NSF→研究者・研究機関）	Office of Research Security and Policy と Chief of Research Security の維持（Sec.10331-10332） ・NSF に、NSF 長官室内に少なくとも 4 名のフルタイムスタッフを擁する Research Security and Policy オフィスを維持することを要求。
	Office of Research Security and Policy にリスクアセスメントの実施権限を付与（Sec.10336） ・NSF の監察官室（OIG）と連携して、NSF Office of Research Security and Policy が、研究開発助成の申請と NSF への情報開示について、オープンソースの分析・解析ツールの利用を含むリスク評価を実施する権限を付与する。

要求・支援の対象	内容
NSF（一部は、NSF→研究者・研究機関）	オンラインリソースの開発（Sec.10334） ・NSF に対し、研究組織及び個人の研究者向けに、最新情報を含むオンラインリソースを開発するよう要請。
	研究不正等についての研究の公募継続（Sec.10335） ・NSF に対し、研究不正や研究インテグリティの侵害、有害な研究行為に関する研究を含む、研究行為や研究環境に関する研究を支援するための研究助成を継続することを要求。
	責任ある研究実践についての研修（Sec.10337） ・責任ある研究実践についての研修に関する 2007 年 America COMPETES Act の Sec.7009 を修正。ポスドク研究者、教員、上級職員を含めるよう要件を拡大。 ・プログラムは、メンター（研究指導者）の訓練、メンターシップ、潜在的な研究セキュリティの脅威に対する認識を高めるための訓練、連邦輸出管理・情報開示・報告要件に関する訓練を含むことを明記。
	研究セキュリティ・インテグリティ情報共有分析センター（Research Security and Integrity Information Sharing Analysis Organization）の外注（Sec.10338）
	Controlled information へのアクセスを持つ研究分野を同定する計画作成（Sec.10339） ・NSF に対して、国家情報長官室（ODNI）及び他の連邦機関と協議の上、主要技術重点分野を含む NSF が支援する研究分野で、controlled unclassified 情報（CUI）又は controlled classified 情報へのアクセスを伴う可能性のあるものを特定する計画を策定するとともに、研究助成に関して働く NSF 職員又は NSF 研究開発助成の対象者に CUI 又は controlled classified information へのアクセスを適宜付与するにあたりデューディリジェンスを行うことを要求。
	孔子学院を設置する研究機関への資金提供の原則禁止（Sec.10339A）
	研究倫理・社会的影響について公募提案書への記載を求める（Sec.10343） ・NSF に対し、利害関係者からの意見を踏まえ、助成金提案の指示書（instruction）を改訂し、研究開発費の支給に先立ち、倫理的・社会的配慮を提案の一部として含めることを義務付けることを要求する。利害関係者の意見を考慮し、NSF は何をもって「容易に予見可能又は定量化可能なリスク（readily foreseeable or quantifiable risk）」とするかについて明確なガイダンスを作成する。
エネルギー省長官	研究セキュリティに対処するツールの開発（Sec.10114） ・DOE 長官に対し、国家情報長官室（ODNI）が特定した脅威を反映した科学技術リスクマトリックスなど、研究セキュリティリスクを管理・軽減するためのツールやプロセスを開発・維持し、対象となる支援の下で実施される活動がもたらす米国の知的財産喪失のリスクや米国の国家安全保障への脅威を判断しやすくするよう要請。
GAO	GAO に対して NIST の研究セキュリティポリシー、プロトコル等についての調査研究を行うよう要求（Sec. 10247）
大学等研究機関	NSF に海外からの資金支援の有無を毎年報告（Sec.10339B） ・研究機関は、毎年 NSF に対し、贈与や契約を含め、当該機関が懸念される外国（foreign country of concern）に関連する外国資金源から直接又は間接的に受ける 5 万ドル以上の現在の資金援助について、要約文書の形で報告しなければならない。
研究者等	懸念される個人又は団体の禁止。（Sec.10636） ・新設の NSF Directorate for Technology, Innovation and Partnerships を含む、特定のプログラムに対する助成、アワード、プログラム、支援、その他の活動を受けること又は参加することを、懸念事項とされた人物又は団体（persons or entities identified as a concern）に禁止する。

出典：AAU. The CHIPS and Science Act of 2022 (H.R. 4346): Research Security Provisions. Last updated August 8, 2022. <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf> 等に基づき作成。

(b) OSTP アップデート情報の発表（2022 年 8 月 31 日）

2022 年 8 月 31 日に、大統領府科学技術政策局（OSTP）は研究セキュリティに関する検討の最新情報を発表した。米国科学技術会議（NSTC）の研究セキュリティ小委員会（SRS）は、連邦政府の研究省庁、研究セキュリティ活動を主導する省庁、研究コミュニティと数ヶ月にわたって討議し、連邦科学資金配分機関に助成金や共同研究契約を申請する研究者の潜在的な利益相反や責務違反を評価するための標準的なデータフィールドと情報開示の指示書の作成に成功した。全ての連邦科学資金配分機関は、標準化されたフォーマットの採用に向けて動き出すことに同意している。パブリックコメントとレビューのプロセスは 2022 年 8 月 31 日に Federal Register に掲示され、開始され、10 月 31 日まで意見が求められた。[74,75]

米国研究コミュニティとの関与

SRS は、2022 年春に「エンゲージメント・アワー」を訪れた約 40 の組織から意見を聞いた。これらの組織は、全米の公立・私立大学、様々な科学分野を代表する専門組織、研究セキュリティとインテグリティの強化に取り組む非営利組織、特にアジア系アメリカ人、太平洋諸島民、ハワイ先住民のコミュニティを代表する学術・擁護組織など、米国の研究エコシステムに貢献する多様な組織を代表するとのことである。これらの組織から提起されたアイデア、懸念や疑問点は、NSPM-33 方針の継続的な策定と実施に反映されるものであり、OSTP と SRS のメンバーが米国の研究コミュニティと協力することにコミットしていることを表す、としている。

SRS は 2022 年秋に、勧告と我々の学んだ教訓をまとめた公的な報告書を発表する予定である（※2023 年 2 月時点で公表は確認できない）。また、将来的にはエンゲージメント・アワーを追加する予定で、特に、地方の大学、歴史的に黒人の多い大学、ヒスパニック系の大学、トライバルカレッジ、その他の少数民族を支援する大学、地域の大学、コミュニティカレッジからの意見を聞くことに関心が高いとのことである。

---

[74] An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity (Morgan Dwyer, Principal Assistant Director for National Security, Office of Science and Technology Policy; Christina Ciocca Eller, Assistant Director of Evidence and Policy and Co-Chair of the National Science and Technology Council Subcommittee on Research Security, Office of Science and Technology Policy; and Ryan Donohue, AAAS Science and Technology Policy Fellow and Senior Policy Advisor, and Member of the National Science and Technology Council Subcommittee on Research Security, Office of Science and Technology Policy)
https://www.whitehouse.gov/ostp/news-updates/2022/08/31/an-update-on-research-securitystreamlining-disclosure-standards-to-enhance-clarity-transparency-and-equity/

[75] Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support. A Notice by the National Science Foundation on 08/31/2022
https://www.federalregister.gov/documents/2022/08/31/2022-18746/agency-information-collection-activities-request-for-comment-regarding-common-disclosure-forms-for

デジタル永続的識別子（Digital Persistent Identifiers）

研究者が効果的な PID ポリシーを策定するために必要な法的、政策的、技術的、実施上の考慮事項に対処するため、SRS は OSTP とエネルギー省が主導する省庁間討議を招集した。2022 年 3～5 月に、ほぼ全ての科学研究費助成機関からなるこの PID サブグループは、7 回の会合を開催した。研究者 PID ポリシーの策定と実施に関する情報、ベストプラクティス、教訓が共有された。同サブグループは、各機関が政策立案と実施にどのようにアプローチするかについて、より良い情報を提供するための内部ツールキットを開発している。

NSPM-33 の PID に関する規定を実施するための長期的なビジョンは、研究者が自分の PID を、履歴書と同じように、資金源、研究成果、所属などの重要情報を常に最新の状態に保つことができるようにすることである。研究者は自分の PID をあらゆる連邦助成申請システムに同期させることができ、負担低減と潜在的な善意のミスを減らすことができる。実装の鍵となるのか、情報開示データフィールドの標準化であり、統合を容易にするために何が必要かを省庁と PID 開発者の双方に明確にするとのことである。

研究セキュリティプログラム

研究セキュリティプログラムを強化するために、SRS は NSPM-33 実施ガイダンスに詳述されている要件と、2022 年の「CHIPS and Science Act」の規定を検討して、さらに明確にするように努めた。NSPM-33 では、2 年連続で 5000 万ドル以上の連邦科学技術助成金を受ける研究機関に対し、NSPM-33 と関連する実施ガイダンスが定めた基準を満たす「研究セキュリティプログラム」を備えていることを証明するよう、連邦科学資金配分機関が要求することを指示している。これらの基準には、研究セキュリティプログラムの 4 つの特定分野、すなわち一般的な研究セキュリティ研修、海外渡航セキュリティ、サイバーセキュリティ、輸出セキュリティ（必要に応じて）が含まれる。CHIPS and Science Act は、研究セキュリティ研修に関する要件を、高等教育機関又はその他の研究機関の職員として連邦科学技術資金の受給を申請するすべての者に拡大した。

研究セキュリティプログラムの要件が、研究機関のコスト及び管理負担への影響を最小限に抑えて満たされるようにするため、連邦政府は、実施ガイダンスよりもさらに詳細に要件を規定する予定である。研究セキュリティプログラム基準の草案は、2022 年の秋に正式なパブリックコメント期間として利用できるようになると予定されていた、その後、やや遅れて、2023 年 2 月後半に草案が公表されている（→49 頁を参照）。

(c) 米国アカデミー報告書「米国の技術優位を保護する」（2022 年 9 月 29 日）

米国の全米アカデミーズ（全米科学・工学・医学アカデミー）は、報告書「米国の技術優位を保護する」（*Protecting U.S. Technological Advantage*）を作成し、オープンネスと競

争の時代において、国家安全保障にとって戦略的に重要な技術をいかに保護するかについて、大統領府や連邦政府機関への政策提言をするとともに、「科学技術安全保障円卓会議」が設置される等、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場となっている。

まず、2022 年 9 月 29 日に公表された報告書「米国の技術優位を保護する」は、国防省の国防高等研究計画局（DARPA）と米国科学財団（NSF）の依頼を受け、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術の保護についてレビューするため、国家安全保障にとって重要な領域の研究の実施と商業化に関する政策と実践を検討する特別委員会を開催し、検討した結果に基づいている。[76]

全米アカデミーズが DARPA と NSF に検討を依頼されたのは以下の 3 つの質問である。[77]

1. 今日の競争的環境において、政府資金配分機関は、特定の技術を保護することと商業化のオプションの利点と欠点を考慮して、科学の開放性をどのように評価又は制限し、アイデアから商業化への移行を奨励すべきか。
2. 研究で発見された進歩、特に米国の国家安全保障に重大な影響を与える可能性のある進歩の生産と商業化に関する市場や制度の課題があるとすれば、どのような解決策が必要であろうか。
3. 研究、生産、商業化、技術保護に関連する適切な政策変更で、米国が資金提供する研究から生まれた進歩の米国内及び米国に利益をもたらすためのマーケティング/実用化を加速するのに役立つものは何か（特に国家安全保障上のリーダーシップにとって重要な技術について）

報告書の第 6 章は、開放と競争の時代に米国が技術を保護する方法について、委員会の結論と提言を書いている。(表 2-24)

[76] National Academies of Sciences, Engineering, and Medicine 2022. *Protecting U.S. Technological Advantage*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26647.
[77] 同上. p.11.

表 2-24：米国アカデミーズ報告書「米国の技術優位を保護する」の提言

提言 1 ・大統領は、大統領令（executive order）を通じて、基礎研究は可能な限り無制限のままであることが米国の方針であることを明確に再確認すべきである。さらに、大統領令は、連邦政府機関と連携して、科学技術政策局（Office of Science and Technology Policy）に、大統領令の発行から 120 日以内に、開かれた研究環境と制限された研究環境の基準を定めるように指示すべきである。 ・さらに、大統領令は、連邦政府機関に対し、助成金や契約の下での業務について、授与前に適切な環境を指定し、オープンな研究環境で実行できる支援業務の量を最大化するよう指示すべきである。この指定を行う際、いかなる制限や推奨される制限も、資金提供を受ける特定の研究助成金や契約にのみ適用され、資金提供を受ける機関全体に普遍的でないことを明確に表明すべきである。（p.79）
提言 2 ・米国科学財団（NSF）は、技術革新における米国のリーダーシップに必要な優秀な科学、研究、工学、革新的人材の開発、誘致、保持に不可欠な米国のイノベーションシステムの要素を定義する取組に出資し、調整する必要がある。NSF は、この取組に他の連邦科学機関、大学、研究機関、教育者、研究集約型企業を巻き込むべきである。NSF は、この取組開始から 180 日以内に、調査結果の詳細を記した報告書を作成する必要がある。 ・これらの調査結果に基づき、科学技術政策局は、連邦研究機関、国土安全保障省、国務省と連携し、国内の研究人材の育成、国際研究協力の機会の拡大、訓練や雇用のために優秀な人材を米国に引き付け維持することを目的とした政策やプログラムを通じて、科学技術におけるリーダーシップを促進する国家戦略を策定するべきである。（p.81）
提言 3 ・国家安全保障会議（National Security Council）、国家科学技術会議（National Science and Technology Council）、国家経済会議（National Economic Council）は、米国の技術リーダーシップやその他の国益にとって戦略的に重要な脅威や脆弱性を特定し評価するための省庁間プロセスを開発し主導するべきである。このプロセスには、各脅威について、連邦機関がリスクに対処する際に使用する関連リスク管理戦略及び評価基準の策定が含まれるべきである。これらのリスク管理戦略の実行は、「政府全体」のアプローチを確保するために、上記の省庁間プロセスによって調整され、監督される必要がある。 ・この省庁間リスク管理プロセスから得られる戦略は、以下のとおりとする。 ➢ 国家や経済の安全保障に影響を与える技術関連の脅威を、研究開発プロセスのできるだけ早い段階で定義するという意味で、プロアクティブなものである。 ➢ 敵対者の計画、行動、意図、能力を含むグローバルな現実と、保護すべき技術、保護できない技術に関する合理的なリスク受容の判断に基づく戦略的なものである。 ➢ 関連する脅威と脆弱性についての最新の理解に基づいており、必要に応じて調整され

るという点で、タイムリーである。 ➢ 輸出管理、情報分類、対米外国投資委員会（Committee on Foreign Investment in the United States）の決定など、技術保護のためのさまざまなメカニズムが、リスクを効果的に低減又は軽減するような方法で指示・調整される統合的なものである。 ➢ 適応性があり、特定された技術分野を科学、技術、国家安全保障の総合的な専門家による定期的なレビューの対象とするメカニズムがある。 ➢ 動的／反復的であり、脅威の状態の変更を正当化するような技術、環境、行為者に変化がないことを確認するための定期的な見直しがある。 ➢ 米国のイノベーション・リーダーシップに不必要かつ意図しない障壁をもたらすことがないよう、悪影響がないかどうかを評価する。（p.83）
提言 4 ・国家科学技術会議、国家安全保障会議、国家経済会議は、戦略的に重要なプラットフォームを特定し、その開発、管理、使用を対象とする協調的なリスク管理戦略を開発するための新しい政策枠組みを共同で開発すべきである。この新しい枠組みの要素は以下を含むべきである。 ➢ 米国の利益にとって不可欠な特定の技術プラットフォームを定義し、指定すること。 ➢ セキュリティ、インテグリティ、相互運用性、制御機能、ユーザー制御の性能基準など、プラットフォーム開発に含まれるべき技術的特徴や要件の特定に民間部門を関与させること。 ➢ 国際的なガバナンス機構、利用協定、規制アプローチ、貿易協定、コンテンツ要件、法執行協力協定など、プラットフォーム開発者又は利用者間の信頼関係を確立し管理するための首尾一貫した政府全体の戦略を開発すること ➢ 共有プラットフォームの使用に関連するセキュリティ又は信頼の問題に対するさまざまな対応を確立し、参加機関が適切な「インシデント対応」能力を計画・準備すること。

以下は同報告書の中で、本調査に関連を持つ部分の抜粋である。

<u>提言１と２について</u>

・ 現在のアプローチは、技術が開発され使用される状況について、時代遅れの仮定に基づいている。その第 1 の前提は、米国は新技術の開発において圧倒的な優位性を享受しており、この優位性は敵や競合相手を「アウトイノベート」（”outinnovating”）することによって守ることができる、というものである。第 2 の前提は、戦略的に重要な技術は、明確な目的を持った個別的なもの（discrete, with well-defined purposes）であるということである。第 3 の前提は、これらの技術は連邦政府の研究所や政府支援の学術研究から生まれ続け、その後、より広い用途のために商業化されるということである。第 4 の

前提は、技術関連のリスク管理は、主に特定の「重要技術」を不正な使用、所有、生産から保護することによって達成できるというものである。

- 今日の非常に競争の激しいグローバルな技術環境では、これらの仮定はもはや有効ではない。委員会の見解では、米国の技術的優位性を守るためには、「技術管理」（technology controls）を超えた根本的な発想の転換が必要であり、新しいアプローチの基礎を築くことが必要である。
- 競合国に対する米国の最大の優位性は、技術へのアクセスを制限する能力ではなく、同盟国と協力して新技術をいち早く開発し展開する能力に根ざしている。この優位性を最大化するために不可欠な戦略には、国内の研究・技術革新エコシステムの規模とスピードを促進すること、研究者やイノベーターを支援するためにリスクを取る環境を育成すること、世界で最も優秀な科学・工学・イノベーション人材を引き付け、維持し、支援することが含まれる。提言 1 及び 2 は、これらの戦略を支援するものである。

提言 3 について

- 技術に関連するリスクを管理するための現在の米国のアプローチは、これらの技術の所有、使用、製造に対する制限、又はそれらの開発に必要な知識や材料に対する制限に基づいている。技術革新のスピードと規模、民間発の技術の増加傾向を考えると、現在のリスク管理アプローチ（risk management approach）は有効性に限界があり、場合によっては逆効果になる可能性がある。その代わりに、米国政府は、米国が直面する技術関連の脅威と脆弱性を定義し、米国の技術リーダーシップに生じるリスクに対応するための効果的な戦略の実施を調整することに焦点を当てるべきである。これらの戦略を支える行動は、公共部門と民間部門、複数の連邦政府機関、そして必要であれば国際的なパートナーとの間で行われるかもしれない。提言 3 はこの問題に対処するものである。

提言 4 について

- 今日の技術システムは、その機能性、生産性、使用において、プラットフォームに依存し、多くの場合、プラットフォームの必要な構成要素となっている。プラットフォームは、プラットフォーム上のあらゆる技術を悪用することができる新しい共有の脆弱性をもたらしている。共有プラットフォームに固有の共依存性は、プラットフォームに対する制限や制御が、米国の国家安全保障や競争力を強化する有益な利用を含む、プラットフォームを利用するすべてのものを混乱させ、非常に大規模な意図しない結果を引き起こす可能性があることを意味する。プラットフォームを管理又は制御する分散化された、そしてしばしば国際的なガバナンスシステムは、基準、貿易、国際協定、規制、法執行を担当する複数の機関の間で、又は民間団体や国際パートナーとの間で、連邦政府の協調行動を必要とするかもしれない。提言 4 はこの問題に対処するものである。[78]

[78] 同上. pp.77-78.

全体的な結論としては、以下のように、同報告書は、①イノベーションと技術における戦略的優位性を高めるためには、開かれた研究環境と適切に制限された環境のバランスが重要である、②米国の政策は、リスクと創造性のバランスを適切に取りながら、研究活動に最適な環境を提供することを目指すべきである、③米国のイノベーションエコシステムを弱めず、新技術の開発と適用能力を保護・強化することが、特定の技術を保護することよりも重要である、としている。

- 米国の全体的な目標は、イノベーションと技術における戦略的優位性を最大限に高めることであるべきである。科学的発見とイノベーションは、広く開かれた参加が望ましいので、この目的を達成するための重要な要素は、開かれた研究環境で適切に実行できる仕事の量を最大化することであり、それによって科学と工学における米国のリーダーシップを促進し、優れた人材を引き付け、新技術につながる発見を強化することである。米国の利益を守るためにオープンな環境が適切でない特定のケースについては、連邦研究開発（R&D）資金提供者は、適切に制限された環境を必要とする特定のケースを明確に指定するリスク情報に基づく決定を行うべきである。
- 技術革新を行う上で、米国はオープンな研究開発環境と制限された研究開発環境の両方を持つことで利益を得ることができる。オープンな研究環境とは、参加、情報共有、出版に関する制限が比較的少ない環境であるが、研究プロセスのインテグリティを確保するための基本的な要件が含まれている。オープンな環境で行われる研究、トレーニング、教育は、研究者の才能を惹きつけ、発見のための創造的で革新的な条件を育成し、新しいアイデアや技術の開発を加速させるため、米国に利益をもたらす。オープンな環境でこの仕事を行うことは、情報や人の移動によって、知識やノウハウ、成果が敵に流れてしまうというリスクをもたらす。しかし、イノベーションリーダーにとっては、情報流出のリスクを軽減し、さらに新しい技術を革新することができるため、ほとんどの研究開発活動において、オープン化のメリットはリスクを上回る。イノベーションリーダー国よりも「速く走る」ことができる。
- すべての研究関連業務がオープン環境に適しているわけではないが、ほとんどの研究関連業務がオープン環境に適している。しかし、特定の用途においては、研究、開発、生産、及び関連する活動を、参加、協力、情報の共有、及び結果の普及を制限する制限付き環境に閉じ込める必要がある。これは、知識、ノウハウ、生産、及び技術の利用が、知識や情報を適切に使用するよう委託された人々に限定されることを確実にするためである。このような場合、敵対者に機密技術を広めるリスクを下げることは、そのような環境で行われる仕事の創造性と生産性に対する制限の悪影響を上回る。米国の政策は、ある研究活動に最も適したタイプの研究環境を指定することによって、これらのリスクの適切

なバランスを取るという目的を持つべきである。[79]

- 今日、米国は他国との人材獲得競争の激化に直面しており、これには外国人又は外国籍の科学者や技術者を米国から引き留めたり、引き離したりすることを目的とした特定のプログラムも含まれている。この競争に対する現在の米国の対応は、断片的で防衛的であり、外国人人材の採用を促進する代わりに、米国市民や機関による外国人人材プログラムへの参加を制限することに主眼を置いている。一貫した連邦政策は、米国市民のための国内 STEM 教育・訓練機会を強化する取組と、学生や労働者として海外の優秀な人材を惹きつける取組とを結びつけていない。現在の政策アプローチでは、人材誘致において長年の優位性を与えてきた米国のイノベーションシステムの特徴を強化・防衛する必要性を十分に考慮していない。[80]
- 今日の相互依存的でグローバルなイノベーションシステムにおいて、最大の脅威は、米国がそのイノベーションエコシステムを不注意に弱める一方で、他国が技術開発と商業化において米国が歴史的に優位に立ってきた行動を模倣し続けることである。この脅威に対抗するため、米国は新技術を開発し、その技術を軍事・商業の両分野の問題に適用する能力を保護し、拡大する必要がある。この能力を保護し強化することは、特定の技術を保護することよりも極めて重要である。[81]

「科学技術安全保障円卓会議」の設置とワークショップの開催

2019 年 12 月に成立した 2020 年度国防権限法（FY 2020 National Defense Authorization Act（NDAA））第 1746 条に、大統領府科学技術政策局（OSTP）が主導し、国家科学技術会議（NSTC）に米国科学技術の海外からの干渉等からの保護等を検討するための省庁間ワーキンググループを設置することとともに、全米アカデミーズに「科学技術安全保障円卓会議」（National Science, Technology, and Security Roundtable）を設置することが規定された。円卓会議は、米国科学財団、エネルギー省、国防省等の連邦省庁が全米アカデミーズと合意し設置することとされている。

円卓会議の概要は、表 2-25 のとおりである。第 1 回円卓会議は 2020 年 11 月に開催され、2022 年 12 月の第 8 回円卓会議までこれまでに計 8 回の会議が開催されてきている。[82]

[79] 同上．p.79.
[80] 同上．p.81.
[81] 同上．p.85.
[82] National Academies website. “National Science, Technology, and Security Roundtable” <https://www.nationalacademies.org/our-work/national-science-technology-and-security-roundtable>

表 2-25：全米アカデミーズ「科学技術安全保障円卓会議」の概要

参加者	以下の機関等の代表者及び実務者を含める。 ・連邦科学省庁、情報機関、国家安全保障機関、法執行機関 ・高等教育機関、連邦政府研究所、産業界、非営利研究機関を含む米国科学事業の主要関係者
設置目的	A) 科学の進歩及び科学技術における米国のリーダーシップに必要な開かれた意見交換、及び国際的な才能を確保しつつ、米国の国家及び経済の安全を守ることに関連する重要な問題の探求。 B) 外国の干渉、サイバー攻撃、盗難又はスパイ行為を含む連邦政府が資金配分する研究開発におけるセキュリティ上の脅威及びリスクの特定及び考察を促進すること。 C) B)で特定された脅威及びリスクを、非機密データ及び関連事例の共有を含め、学術及び科学コミュニティに伝えるための効果的なアプローチの特定。 D) B)で特定された脅威及びリスクへの対処及び軽減するためのベストプラクティスの共有。 E) 外国の脅威に伴うリスクを軽減及び対処すべく政府及び学術・科学コミュニティによる短期及び長期にわたる潜在的対応についての検討。

出典：2020 年度国防権限法（FY 2020 National Defense Authorization Act (NDAA)）第 1746 条の規定に基づき作成。

さらに、同円卓会議の関連活動として、全米アカデミーズは、科学界と国家安全保障界の代表者、その他の連邦関連機関及び民間部門を集め、連邦政府が資金提供するオープンな科学研究システムを安全なものとし、強化するためのアプローチを検討するために 2022 年にワークショップを 4 回開催している（2022 年には 7 月 7 日・18 日・22 日、11 月 14~15 日）。

ワークショップでは、世界的に優秀な STEM 人材の獲得と維持、国際的な科学研究協力の促進、不正な海外からの干渉への対策などもテーマとして取り上げている。また、ワークショップでは、米国政府が支援する基礎研究の中で最も大きな割合を占め、多くの先端アプリケーション、新興技術、イノベーションを生み出している大学と連邦政府出資の研究開発センター（FFRDC）にも焦点を当てている。このワークショップでは、以下のようなトピックを取り上げた。(1) 重要な価値と資産としてのオープンサイエンスとテクノロジー研究、(2) グローバルな科学的関与と外国人人材の獲得、(3) 国際研究協力の利益とリスク評価、(4) オープンサイエンスの文脈における研究セキュリティ、(5) 科学研究コミュニティとセキュリティコミュニティの協力促進。

例えば、2022 年 11 月 14～15 日のワークショップでは、大学（インディアナ大学、カーネギーメロン大学、スタンフォード大学等）、連邦研究開発センター（ローレンスリバモア

国立研究所）、非営利機関、連邦政府機関（CIA）からの参加者の間で、以下のテーマについて、それぞれ約 1 時間ずつ討論した[83]。

- 国際的な STEM 人材と米国の研究競争力
- 国際共同研究：メリットと課題
- 代替アプローチの実用的な考察とリスク・ベネフィット
- コミュニティの自発的積極的関与（buy-in）とサイバーリスクの管理
- 科学研究、国家安全保障、法執行のコミュニティ間の協力関係の促進

(d) “Safeguarding Science” Toolkit の発表（2022 年 11 月 15 日）

2022 年 11 月 15 日に国家情報長官室（Office of the Director of National Intelligence）の米国防諜・セキュリティセンター（National Counterintelligence and Security Center: NCSC）が研究セキュリティ・インテグリティに対する広範なリスクに直面する研究者を支援するために、連邦政府機関、大学関係者と協力し、「Safeguarding Science ツールキット」（Safeguarding Science toolkit）を作成して公表した。このツールキットは、研究関係者が政府及び学術界のセキュリティのベストプラクティスにアクセスし、個々のニーズに合わせてツールを選択することを助けることが意図されている。[84]

このツールキットは、NSF、米国国立標準技術研究所（National Institute of Standards and Technology (NIST)）、運輸省及び連邦航空局（Federal Aviation Administration (FAA)）、保健福祉省、ホワイトハウス科学技術政策局、米国大学協会（American Association of Universities）と共同で NCSC によって開発され、インテグリティ、コラボレーション、開放性、セキュリティを重視する堅牢で弾力性のある米国の研究エコシステムを促進し、そのすべてがイノベーションを促進することを意図している。

NSPM-33 実施ガイダンスの「研究セキュリティプログラム」の第 5 項目（Development of research security content）では以下のように説明されていた。

> 連邦政府は、研究機関の裁量で研究セキュリティプログラムに組み込むことができるよう、研修内容やプログラム上のガイドライン、ツール、ベストプラクティスの開発を支援するための標準的な技術支援を提供する予定である。特に、国家防諜タスクフォース（National Counterintelligence Task Force）の代表機関が、米国防諜・セキュリティセンターと連携して、研究機関が研究セキュリティプログラム及びトレーニングの要件を満た

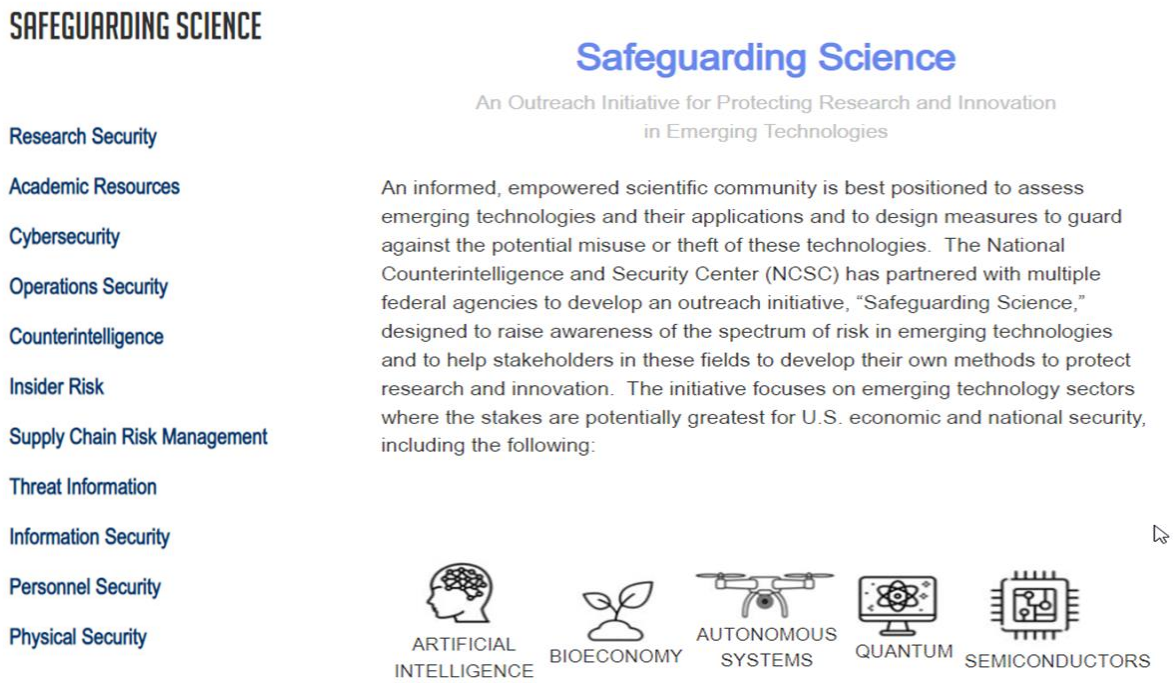
[83] Openness, International Engagement, and the Federally Funded Science and Technology Research Enterprise - A Workshop
<https://www.nationalacademies.org/event/08-29-2022/openness-international-engagement-and-the-federally-funded-science-and-technology-research-enterprise-a-workshop>

[84] “Safeguarding Science toolkit launched to help researchers defend scientific integrity.” NSF News. November 16, 2022
https://beta.nsf.gov/news/safeguarding-science-toolkit-launched-help

すために活用できるコンテンツを共同開発する。連邦政府は、研究機関向けの研究セキュリティプログラム情報及び実施リソースを開発・維持し、研究セキュリティプログラム内で使用するのに適したリソースを含むコミュニティコンソーシアムの形成を支援することを検討する必要がある。実務上可能な限り、プログラム内容の開発は、政府と組織との共同作業とすべきである。

このポータルサイトの作成について、NSF の研究セキュリティ戦略政策課長の Keiser 氏は「NSF は、連邦機関のパートナーと協力して、新しいオンラインの Safeguarding Science ツールキットの研究セキュリティセクションを提供できることを嬉しく思う」「このコンテンツを NSPM-33 実施ガイダンスの主要分野と合わせることで、現在進行中の研究セキュリティイニシアティブとそのガイダンスの意味を学界がより理解できるようにする。私たちは、研究コミュニティに役立つ情報とツールを提供し続けることを楽しみにしている」と述べている。

また、NSF 長官の Sethuraman Panchanathan 氏は「このツールキットは、研究者がオープンな共同研究を行うための枠組みを提供すると同時に、盗難や悪用などの脅威を寄せ付けないための保護を確立するもの」「このツールキットは、研究コミュニティや米国政府の科学・情報機関と連携し、リスクに対処するための情報、ベストプラクティス、ツールを共有し、研究エコシステムの繁栄を確保するために国際協力を推進する NSF の取組を示すものである」と述べている。



出典：Safeguarding Science: An Outreach Initiative for Protecting Research and Innovation in Emerging Technologies
<https://www.dni.gov/index.php/safeguarding-science>

図 2-3：「Safeguarding Science」ポータルサイト

(e) 「研究セキュリティプログラム」のドラフト公表（2023 年 2 月 28 日）

2023 年 2 月 28 日に大統領府科学技術政策局（OSTP）の研究セキュリティ小委員会が公表した「研究セキュリティプログラム標準要件案（DRAFT Research Security Programs Standard Requirement）」は、NSPM-33 実施ガイダンスの最後の条項である「研究セキュリティプログラム」に関するものである[85]。具体的には、NSPM-33 のセクション 4(g)は以下のとおりである。

> リスクの特定と分析：資金提供機関の長は、年間 5,000 万ドルを超える連邦科学技術支援を受ける研究機関に対し、その機関が「研究セキュリティプログラム」を確立し運営していることを資金提供機関に証明するよう求めるものとする。機関の「研究セキュリティプログラム」には、サイバーセキュリティ、海外渡航セキュリティ、内部脅威の認識と特定、及び必要に応じて輸出管理トレーニングの要素が含まれるべきである。資金提供機関の長は、米国の国家及び経済の安全保障に影響を与える重要かつ新興の技術分野における研究開発のために連邦政府の資金提供を受けている機関に対し、「研究セキュリティプログラム」の追加要件が適切であるかどうかを検討しなければならない。

対象研究機関は過去 2 年間の連続する各会計年度において、年間 5,000 万ドル以上の連邦科学技術支援を受けた研究組織である。連邦科学技術支援を受け、維持するための条件として、対象研究機関は、条件を満たす研究セキュリティプログラムを維持していることを証明しなければならない。自己認証は、対象となる研究機関に対し、年 1 回、SAM.gov（System for Award Management : U.S. General Services Administration が運営するウェブサイト）で集中的に行われる。

海外渡航のセキュリティ、研究セキュリティのトレーニング、サイバーセキュリティについてそれぞれ説明されている。このうち研究セキュリティのトレーニングについての説明は以下のとおり。

> 研究セキュリティのトレーニングは定期的に更新されなければならず、研究セキュリティの脅威の認識、識別、内部脅威などの構成要素を含む。研修は、教員、職員、学生など、適切な人員に合わせたものとする必要がある。対象となる研究機関は、毎年、そのトレーニングが要件を満たしていることを証明しなければならない。研修プログラムには、以下の分野での指導が含まれていなければならない。
>
> 1. 研究セキュリティが米国の研究開発にとって重要である理由と、何が海外からの干

[85] Subcommittee on Research Security. National Science and Technology Council. Office of Science and Technology Policy. DRAFT for Public Comment. DRAFT Research Security Programs Standard Requirement. Prepared by the Interagency Working Group on Research Security Programs, Subcommittee on Research Security, National Science and Technology Council. <https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf>

渉に当たるかを理解すること。
2. 米国の研究セキュリティの指針としての非差別の重要性。
3. 情報開示方針とそれがどのように使われるか。特に利益相反や責務相反について。
4. リスクの特定、管理、軽減（特に外国人人材採用プログラム、インサイダー脅威など）。
5. 資金の適切な使用。
6. 国際協力の価値と課題。
7. 責任ある海外渡航の実践。
8. サイバーセキュリティの基本的な衛生管理及びデータ保護の実践。ソーシャルエンジニアリングの脅威やサイバー侵害の認識と対応を含む。
9. 知的財産及びデータ保護の要件とベストプラクティス。

この「研究セキュリティプログラム標準要件」に対してのパブリックコメントの募集が 2023 年 3 月 2 日に開始された。2023 年 6 月 5 日を期限として意見が求められている。[86]

OSTP は、関心のあるあらゆる利害関係者からのコメントを募集している。特に、OSTP は、研究セキュリティプログラムの要件の対象となる研究機関、研究者、研究機関を代表する専門組織、米国の研究エコシステム全体の多様な利益を代表する組織からの意見に関心をもっている。

特に以下の点についてのコメントが求められている。

1. 公平性（equity）：NSPM-33 の実施ガイダンスでは、研究セキュリティの方針と実践が公平かつ非差別的に実施されることを求めている。標準要件において、衡平性と非差別の基本的な約束が守られていないと思われる部分があるかどうか。
2. 明確性（clarity）：研究セキュリティプログラムの標準要件が明確であることが不可欠である。明確であることで、公平性、透明性、及びコンプライアンスが可能になる。特に、組織が標準要件の規定を理解し、遵守する能力に関連する、標準要件全体の明確さに関するコメントを求める。本基準の要求事項がどの程度明確であり、素直に採用できるのかどうか。
3. 実現可能性（feasibility）：研究セキュリティプログラム標準要件は、対象組織が採用を実現可能であると考える場合に、最も成功する。このことを念頭に置いて、標準要件には、実装の点で懸念される側面があるか。ある場合、その方法と理由は何か。
4. 負担（burden）：実現可能性と密接に関連するのは、負担である。研究コミュニティとの関わりから、金銭的な負担であれ、事務的な負担であれ、負担に対する懸念が高いことを理解することができた。標準要件の条項は、SAM.gov での認証の一元化や、

[86] Office of Science and Technology Policy. Request for Information; NSPM 33 Research Security Programs Standard Requirement. Federal Register / Vol. 88, No. 44 / Tuesday, March 7, 2023 / Notices <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement>

研究セキュリティトレーニングの開発に対する技術支援など、負担を軽減することを目的に設定されている。標準要件を実施する上で、研究コミュニティの負担を軽減するための他の方策はあるかどうか。

5. コンプライアンス：標準要求事項の草案では、要求事項への準拠の主要なモデルとして「自己認証」を提案しており、標準要求事項の発行から 1 年後に最初の認証が必要であるとしている。これらのアプローチについて、どのように考えるか。他に考慮すべき点はあるか。