CRDS-FY2023-RR-08
ISBN 978-4-88890-907-5

調査報告書

# 【概要版】
# 米国における研究セキュリティの取組み
# －研究の開放性と安全の両立に向けて

Efforts of Research Security in the U.S.

- Balancing the Openness and Security in Research Community

報告書の全文(PDF 形式)をご希望の方は、以下までお問い合わせください。
■問合せ先：国立研究開発法人科学技術振興機構 研究開発戦略センター
戦略提案・報告書 担当：crds-report@jst.go.jp

CRDS 研究開発戦略センター
Center for Research and Development Strategy

国立研究開発法人科学技術振興機構

## １．調査の目的と対象

### (1) 調査の目的

- 研究のオープン化、国際化が世界的に進展しており、国内的にも国際的にも開かれていることが、活力ある研究システムのために不可欠であると広く認識されている。一方で、2018 年頃からオープンな研究システムの不当な利用による、研究システムの健全性の毀損と技術流出などを通した国家安全保障への悪影響の認識が共有されはじめてきた。
- このような懸念に対して、我が国を含む多くの国では、責任ある行動による研究、社会に対する説明責任、研究倫理の順守などを行うといった研究インテグリティについて利益相反・責務相反に重点を置いて取組みを強化することで対応が検討され、着手されてきた。近年ではこれらの懸念に対して、どのようなリスクが生じているのか、どのような対応が必要かを検討する研究セキュリティについて、具体的な取組みが進められ始めている。
- 米国においては、「国家安全保障大統領覚書-33 履行のためのガイダンス」（2022 年 1 月）、「半導体・科学法」（2022 年 8 月）が成立し、各種法令によって指針が示され、利益相反・責務相反に関する情報開示のほか、リスク評価、トレーニングプログラムの構築、研究セキュリティプログラムの構築などが実行に移り始めている。これらの取組みは、研究の開放性と研究の安全の両立に向けた取組みであり、研究コミュニティ内における役割分担、合意形成、信頼醸成の観点からも注目に値する。本調査では、米国の政策的動向および大学の動向について、研究セキュリティの観点から進捗（2024 年 2 月まで）について、多角的な観点からまとめることを試みた。

### (2) 調査の範囲

- 米国の研究インテグリティ・研究セキュリティ強化は、「国防権限法」、「NSPM-33」、「NSPM-33 ガイダンス」、「半導体・科学法」によって大きな方向性が示されており、連邦政府（資金配分機関を含む）に対して、研究セキュリティの取組み強化の要請がなされている。本調査では、法律、覚書の要請内容、それを受けた連邦政府機関（資金配分機関を含む）の取組み、研究機関の取組みの順に取り扱う。
- また、先の CRDS 報告書において、研究インテグリティを「研究コミュニティが責任ある行動をとおして研究環境の健全性・公正性を確保することにより、研究の活力を保つとともに社会の信頼を得ることの重要性を示すもの」と定義し、研究インテグリティと研究セキュリティの関係を図のとおり整理してきた。今回の報告書では、研究セキュリティ観点から米国の取組みに着目して直近の動向をまとめた。
- 一方で、米国においては、国家安全保障に悪影響をもたらす懸念がある機密情報（Classified Information: CI）、管理された非機密情報（Controlled Unclassified Information: CUI）の情報保全システムがあり、これが国防分野などの技術情報に適用されてきた歴史もある。今時の研究セキュリティの取組みは、CI、CUI の保護対象を学術研究に拡大するものではなく、リスクベースアプローチによる柔軟な管理措置による強化が求められているものと整理する。CI、CUI と研究開発の関係については参考資料でまとめた。
- 米国の科学技術を取り巻く環境は、政策形成プロセス、科学技術と安全保障に関する歴史的背景、政府負担の研究開発費、研究者数、留学者数など多くの点で我が国の状況と異なっている。本調査は、我が国の研究セキュリティを検討する際の基礎資料の一つとして位置づけられるものである。我が国における研究セキュリティのあり方の検討にあたっては、米国以外の取組みの事例なども参照しつつ、我が国固有の歴史的文化的背景、政策的意思決定の状況、国際戦略などを考慮するべきである。

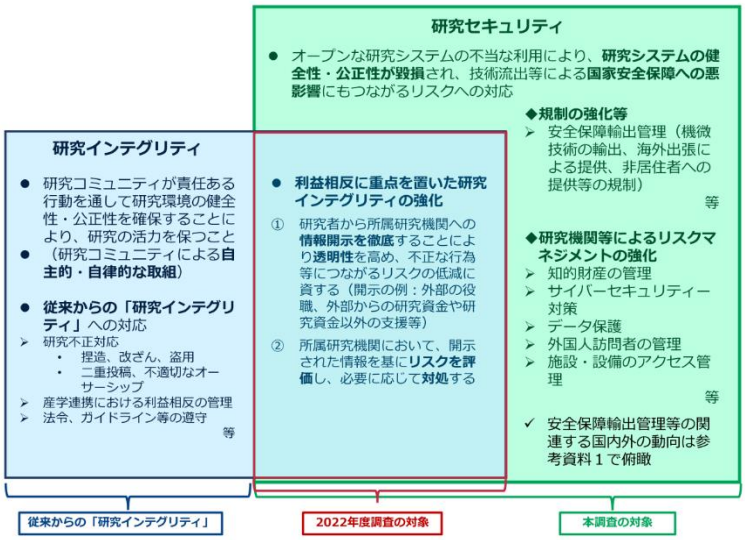


図 1　本調査の範囲（CRDS 作成）

目次

## 2. 米国における研究セキュリティの取組み（概要）

### (1) 米国における研究セキュリティの経緯と根拠法令

- 2018 年ころから米国通商代表部や大統領府の通商製造政策室が相次いで中国の貿易慣行への懸念や技術や知的財産の侵害を懸念する報告書を公表するなど、米国政府においても中国による不正な手段での技術獲得の懸念が高まっていた。
- トランプ政権時に「2019 年度国防権限法（NDAA)」では、軍事研究開発に関する「大学・研究機関などの研究者への不当な影響やそのほかのセキュリティ上の脅威に対する国家安全保障上の保護を支援するイニシアチブ」の策定（同法セクション 1286）が盛り込まれた。また、2021 年 1 月 14 日には、米国政府が支援する研究開発に対する外国政府の不当な干渉や成果の盗取からの保護措置の強化を目的とした、「国家安全保障大統領覚書-33（NSPM-33)」が発表された。
- バイデン政権においても、研究セキュリティに係る多くの政策がトランプ政権から継続されている[1]。「NSPM-33」で規定される研究セキュリティのための措置実施の指針を示している「NSPM-33 履行のためのガイダンス」が発出され、より具体的な対応が進められている。2022 年 8 月に施行された「半導体・科学法（CHIPS and Science Act)」の中でも NSF の対応を中心に研究セキュリティ強化に向けた要求が盛り込まれた。

### (2) 米国における研究セキュリティの取組み

- 米国政府の研究セキュリティ確保に向けた取組みは、「2021 年度国防権限法」、「国家安全保障大統領覚書-33（NSPM-33)」、「半導体・科学法」をとおして連邦政府・資金配分機関に対して、大きく四つの要請（①情報開示、②研究セキュリティプログラムの確立、③リスク評価、④トレーニング）があると整理することができる。
- ①情報開示では、開示要求事項と開示要求フォーマットの標準化が進められており、これらの開示要求事項に併せて大学では情報集約を行う体制を整え始めている。
- ②研究セキュリティプログラムの確立では、プログラムで必要とされる要素が「NSPM-33 ガイダンス」をとおして（a）サイバーセキュリティ、（b）外国渡航のセキュリティ、（c）研究セキュリティトレーニング、（d）輸出管理トレーニングと示されており、それ基づき、大統領府科学技術政策局（OSTP）から「研究セキュリティプログラム」ドラフト、国立標準技術研究所（NIST）から「国際的な科学を守る：研究セキュリティのフレームワーク」が発表されている。外国渡航、研究セキュリティ研修、国際協力、輸出管理研修、サイバーセキュリティ、物理的セキュリティ、内部脅威対策など、個々の大学での対応策の案が示されている。
- ③リスク評価・管理は、資金配分機関を含む連邦政府機関が情報開示要求によって集約した情報に対するリスク評価などへの取組みである。研究セキュリティのリスク評価は、取組みが強化されているところであるが、連邦政府・資金配分機関と研究機関とで役割分担がなされつつあり、いずれの機関においてもリスクの程度に応じた「リスクベースアプローチ[2]」による対応が採用されている。

---

[1] 司法省による米国の研究コミュニティへの中国の脅威について調査を行った「チャイナ・イニシアチブ」はトランプ政権下の2018年に開始されたが、2022年2月に終了したとされている。

[2] 米国の研究セキュリティではリスクベースアプローチについて明確な定義はなされていないが、一般的にリスクベースアプローチとはリスク評価に基づいて意思決定を行うことを指す。費用と便益を比較考慮し社会が受容できるリスク水準を考慮し管理することを指す。環境、医療、原子力の分野における安全確保において採用されており、リスクの定量化された確率に基づく分析がなされるが、研究セキュリティの分野ではリスクの定量化に向けた動きはまだ見られていない。

- ④研究セキュリティのトレーニングでは、NSF が取りまとめ機関となりトレーニングモジュールの構築が進められている。実際にトレーニングを運用する大学がトレーニングモジュール案を作成し、それらを NSF が統合することで、資金的・人的資源が十分ではない大学においても活用できるコンテンツの作成が進められている。
- 重要なことは、連邦政府機関・資金配分機関は、法令、大統領覚書などの方針に基づき研究セキュリティの対応策が講じているが、研究者や研究機関に過度の負担が及ばないよう、大学協会などの研究コミュニティと調整を図っていることである。個々の研究機関・大学が対応策を検討するに至るまでの間には、米国大学協会（AAU）や公立・ランドグラント大学協会（APLU）といった中間的な組織が中心となり、連邦政府・資金配分機関側の対策が研究現場において対応可能なものとなるように、丁寧な議論を重ね合意形成を行っている。

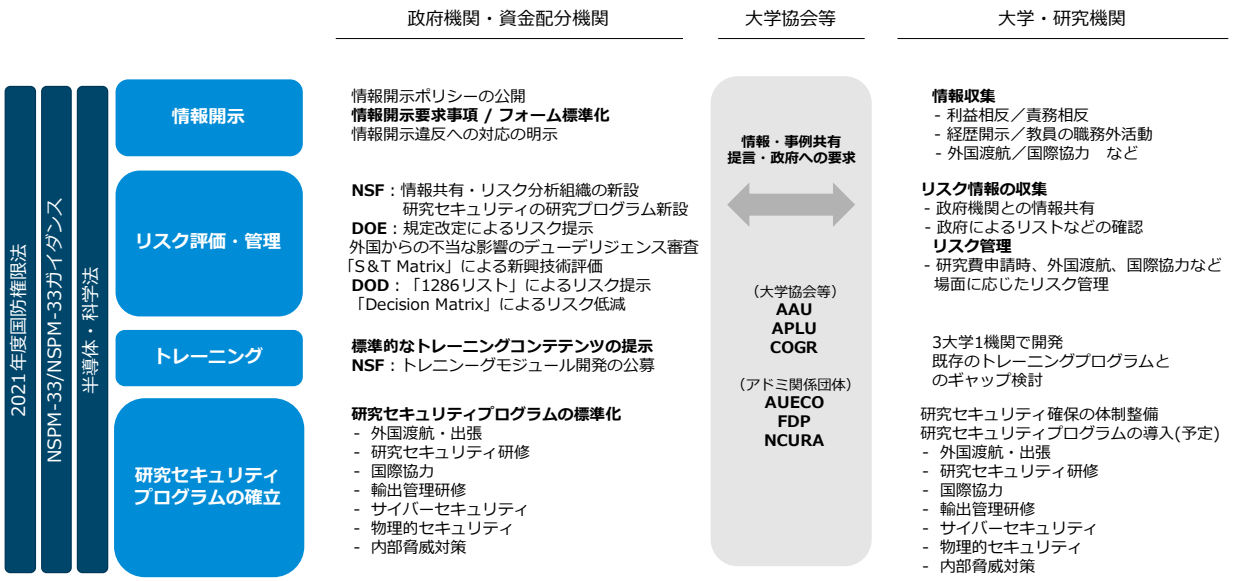


図 2　米国における研究セキュリティ確保に向けた取組みの俯瞰（CRDS 作成）

(3) 米国における研究セキュリティの取組みのまとめ

米国の研究セキュリティの取組みは、研究の開放性への制限をできるだけ最小限にしつつ、国家安全保障および経済競争力を確保するという、両者のバランスを保つための取組みである。これらの取組みから得られる示唆として 4 点を挙げた。

（研究セキュリティの目的共有と研究セキュリティ強化のもたらす影響の検討）

- 研究インテグリティや研究セキュリティは類似する概念であると同時に、研究者、政策担当者かなど置かれている立場や国によって解釈が異なる。解釈が多様であるからこそ行政文書で明確にすることは、目的共有と言う観点でも重要な役割を果たしていると考えられる。
- なぜ研究セキュリティが問題なのかについて、コミュニティ間で共有することの重要性が確認されていた。例えば、「セキュリティ」というワードから、研究の開放性と対峙する概念と受け取られうることから、各種法令、ガイダンスの策定過程においても研究の開放性が確認されている。また、連邦政府機関（資金配分機関を含む）の個別の研究セキュリティ施策にあたっても、基盤的研究の開放性や開かれた科学が前提にあることが確認されている。

- 研究セキュリティの取組みが特定の国の出身の研究者に対して、差別的な取扱いとならないこと、また外国人差別の助長につながることがないように、資金配分機関および大学双方で丁寧なコミュニケーションが図られている。

（リスクベースによる研究セキュリティリスク管理）

- 米国の研究セキュリティでは、リスク評価に基づいて意思決定を行うリスクベースアプローチを採用し、リスクの程度に合わせてリスク管理を試みている。リスクがあることによって機械的に一律の対応（たとえば、リスクの有無によって研究申請を不採択にするなど）を行うのではなく、リスクの程度に応じたリスク低減策が検討されている。
- 大学では、連邦政府機関（資金配分機関を含む）の示す方針を参照しながら、リスク評価が必要とされる国際協力の場面を整理し、既存のコンプライアンスや輸出管理などの取組みを活用しながら、個々の機関に合う研究セキュリティ体制の構築を試みている。また、現在の研究環境における最新のリスク動向を把握するために、法執行機関等からの情報提供を受けている事例もある。
- また、NSF を中心に新興技術が持ちうる両義性が米国の安全保障や経済的競争力へ与えうる潜在的リスクについても検討を始めている。また全米アカデミーズからもこれまでの技術流出対策の限界と、協調的なリスク管理（開放性を確保しながら安全保障上の課題にも対処する）の必要性が示されるなど検討が始まっている。ただし、新興技術の持ちうる両義性のリスクについての線引きはケースバイケースでなされており一律な基準は示されていない。

（多層的な人材育成）

- 研究者のみならず行政機関、資金配分機関職員、大学・研究機関のアドミニストレーター含む研究コミュニティ全体での意識向上に向けた取組みが行われている。
- 国家情報長官室（ODNI）、FBI、商務省など情報・防諜機関や法執行機関を中心にして収集されている外国の懸念団体や事例について、連邦政府機関間および大学・研究機関の間でも共有を行っている。NSF においては、法執行機関、情報・防諜機関との情報共有にあたって、限られた少数の職員であるがセキュリティクリアランスを取得している人材が確保されている。
- NSF では、研究事業に対する研究セキュリティ上の脅威の潜在的な影響を評価する方法論など、研究セキュリティを分析対象とした研究セキュリティのための研究プログラム（Research on Research Security Program）を立ち上げており、研究セキュリティに携わる人材の裾野を広げる取組みが行われている。

（研究セキュリティにおける関係機関間ネットワーク）

- 連邦政府機関（資金配分機関を含む）は、個々の機関での研究セキュリティの対応の違いが研究現場の負担とならないよう、政府機関間で個別の政策について情報共有を行っている。
- 大学やアドミニストレーターによる中間団体（AAU、COGR、AUECO など）が、連邦政府機関（資金配分機関を含む）から個別に行政文書や指針を集約し、更新情報をウェブサイト等に掲載するなど発信を行っている。また、研究セキュリティに取り組む大学間における良好事例共有の機能も果たしている。その他、連邦政府機関等から示された方針に対して、現場で受け入れられない事項について意見を集約

し、連邦政府機関等に意見を示す活動も行っている。

- NSF を中心に、政府機関、関係団体、研究機関間で情報共有・調整を行い、新たな施策に対して研究コミュニティ内で丁寧な合意形成を行うことが重要視されている。担当者がバイネームで繋がり、公式・非公式のチャネルを使って、継続した議論が実施されている。

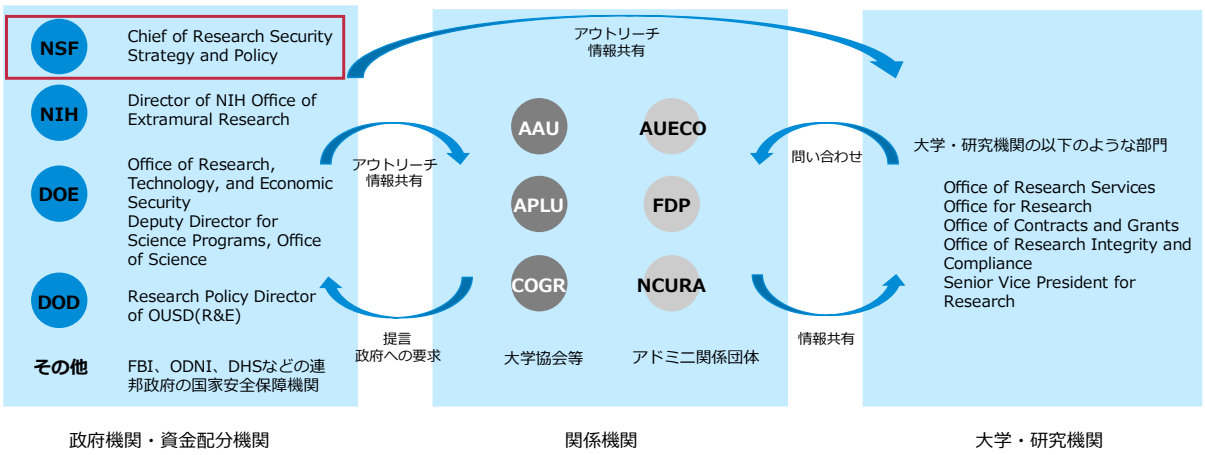


図 3 米国の研究セキュリティにおける関係機関間ネットワーク（CRDS 作成）

3. 参考：米国の機密情報・管理された非機密情報（CUI）と研究開発（概要）

（1）米国の機密情報・管理された非機密情報（CUI）

- 米国では政府の保有する国家安全保障に関わる情報について特定・分類、保護する制度やプログラムを保有している。その主たる制度として、国家安全保障情報（NSI: National Security Information）制度と、管理された非機密情報（CUI：Controlled Unclassified Information）に関する制度がある。
- 一般的に大学・研究機関で実施されている基盤的研究（fundamental research）は、国家安全保障情報と CUI の枠組みの外に位置づけられている。科学技術情報おいて、その成果が不正に用いられることで国家安全保障に悪影響をもたらす懸念があるものについては、機密情報保護や輸出管理制度などをとおして極めて限定的な範囲で保護されてきた。
- 国家安全保障情報制度および CUI の制度は、①情報の特定（identification）・分類（classification）と②保護（protection）の過程に分けて整理することができる。①、②に係る方針や運用手順が大統領令、連邦政府規則集、運用時のガイドラインとして示されている。

| | 情報の分類・識別 | | 保護 | |
|---|---|---|---|---|
| | 根拠 | ガイドライン<br>運用マニュアル | 根拠 | ガイドライン<br>運用マニュアル |
| **国家機密情報**<br>National Security Information System | • 大統領令13526号 | • 32 CFR*1 2001<br>• 関係省庁・機関は運用マニュアル・命令を作成<br>- DOD M 5200.01*2<br>- DOE O 475.2B*3 | • 大統領令12968号（連邦政府機関向け）<br>• 大統領令12829号（連邦政府と契約する機関向け） | • NIST SP 800-53*4<br>• 32 CFR 117 (NISPOM*5) |
| **管理された非機密情報**<br>Controlled Unclassified Information System | • 大統領令13556号 | • 32 CFR 2002<br>• 関係省庁・機関は運用マニュアル・命令を作成<br>- DOD I 5200.48<br>- DOE O 471.7 | • 32 CFR 2002 | • NIST SP 800-171*6<br>• FIPS PUB 199*7 |

*1 CFR = 連邦規則集
*2 DOD M = 国防総省マニュアル
*3 DOE O = エネルギー省命令
*4 NIST SP 800-53 = 連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策
*5 NISPOM = 国家産業保全プログラム運用マニュアル
*6 NIST SP 800-171 = 連邦政府外のシステムと組織における管理された非格付け情報の保護
*7 FIPS PUB = 連邦情報処理規格

図 4 米国の国家機密情報・CUI の根拠規定（CRDS 作成）

(2) 国家機密情報保護制度

- 現在の米国における国家機密情報の識別・分類は、「大統領令 13526 号」（Classified National Security Information）を根拠とし[3]、連邦規則「32CFR2001」（Classified National Security Information）が導入のための規則として設けられている。
- 機密情報を指定できる権限は、大統領、副大統領から各省庁の長と上級幹部職員、さらに連邦政府職員へと権限を委譲している（1.3 条）。大統領府から、大統領首席補佐官、国家安全保障担当大統領補佐官、国土安全保障・テロ対策担当大統領補佐官、国家麻薬管理政策局長、大統領府科学技術政策室などが指定されており、行政機関からは、国務長官、財務長官、国防長官、司法長官、エネルギー長官、国土安全保障長官、国家情報長官、航空宇宙局長などが指定されている。NSF は機密指定権限を保有しない。
- 機密対象は 8 項目設けられており、科学技術に関するものはその中の一つである 1.4 条（e）国家安全保障に関連する科学的、技術的、経済的事項が定められている。この項目には研究開発に係る情報が含まれ得ることが推察できるが、具体的にどのような基準でどのような内容が「科学的、技術的、経済的事項」となり得るかは示されていない。
- 国家安全保障に明らかに関連しない基礎科学研究情報（basic scientific research information）については、機密指定を禁止または制限する対象と定められている（1.7 条）。

| | |
|---|---|
| 機密指定権<br>（1.3 条） | • 大統領、副大統領<br>• 大統領が指定した行政機関の長と上級幹部職員<br>• 権限を委任された連邦政府職員<br>- 機密指定権限を持つ機関の長は職員に権限の委任を行う事ができる<br>- 権限を委任された職員は適切な分類、機密解除に関する研修を受ける |
| 機密対象 | (a)　軍事計画、武器システム、又は作戦 |

[3] 歴史的に軍部の情報を秘密指定情報としたのが、1912年の将軍命令（General Order）第3号まで遡る。現在の大統領が国家機密指定権限を持つようになったのが、1940年ルーズベルト大統領時の「大統領令8381号」である。そして機密指定の対象を国家防衛（National Defense）から「国家安全保障（National Security）」へと拡大したのが、トルーマン大統領時の「大統領令10290号」である。

| | |
|---|---|
| （1.4 条） | (b)　外国政府情報、<br>(c)　インテリジェンス活動（秘密活動を含む）、インテリジェンスに関する情報源、方法、又は暗号<br>(d)　機密情報源を含む連邦政府の外交関係、又は外交活動<br>(e)　国家安全保障に関連する科学的、技術的、経済的事項<br>(f)　核物質、又は核施設に対する安全防護策に関する連邦政府プログラム<br>(g)　国家安全保障に関連するシステム、施設、社会基盤、プロジェクト、計画、防護サービスの脆弱性又は能力<br>(h)　大量破壊兵器の開発、生産、利用に関する情報 |
| 機密分類の禁止・制限<br>（1.7 条） | (a)　以下の目的で情報を機密指定、機密維持、機密解除を行ってはならない<br>（1）　法令違反、非効率、行政上の過誤の隠匿<br>（2）　個人、組織、又は省庁の窮迫を防ぐこと<br>（3）　競争の抑止<br>（4）　国家安全保障の保護を必要としない情報の公開の防止・遅延<br>(b)　国家安全保障に明確に関連しない基礎科学研究情報は機密指定してはならない<br>(c)　機密指定解除された後、特定の場合を除き再度機密指定を行ってはならない |

(3) 管理された非機密情報：CUI

- 機密情報として扱われるもの以外の情報（非機密情報）の中でも、一定の保護や配布（アクセス）の管理を必要とするものがある。これらは「管理された非機密情報（Control Unclassified Information: CUI）」とされるオバマ政権の「大統領令 13556 号」発出以降の取組みである。
- 今日の CUI に含まれる情報は、各連邦政府機関固有の方針や手順によって管理・保護されていたが、こうした形での情報管理は不明確な情報公開制限や組織間での情報共有の障壁の一因とされた。そのため、現在連邦政府内での統一的な管理に向けた体制整備が進められている。
- CUI は政府が作成、所有する情報または政府のために、政府に代わってある機関が作成した情報のうち、法律などで管理が求められるものである。
- CUI となる情報の種類は、法律や規制などに基づいて各省庁にて特定された後、ISOO の承認を受けて CUI カテゴリに登録される。カテゴリの中にはプライバシーや税、法執行、調達など 20 のカテゴリが登録されている。安全保障はこの中の一つであり、CUI のすべてが国家安全保障に係る情報保護制度である CI を補完するものではない。

| | | | |
|---|---|---|---|
| 1.重要インフラ | 6.インテリジェンス | 11.NATO | 16.独自の事業情報 |
| 2.防衛 | 7.国際協定 | 12.核（原子力） | 17.Provisional |
| 3.輸出管理 | 8.法執行 | 13.特許 | 18.統計 |
| 4.金融 | 9.法律 | 14.プライバシー | 19.税 |
| 5.移民 | 10.自然および文化財 | 15.調達および取得 | 20.輸送 |

- 連邦政府機関の委託を受ける事業者などが CUI を扱う場合、「NIST SP800-171」のような指針に基づく情報管理が求められる。大学・研究機関も同様である。ただし、現在のカテゴリに基盤的研究に係るものは含まれていない。
- 今後基盤的研究に関連するような情報が CUI のカテゴリに加えられることへの懸念がある。この点について科学助言グループである JASON は NSF の委託を受けて作成した基盤的研究の研究セキュリティの報告書の中で、大学で生成される情報を CUI として保護することは推奨しない立場を示している。

(4) 基盤的研究と成果の公開の原則

- 機密情報、CUI と基盤的研究（fundamental research）との関係については、基盤的研究が機密情報および CUI の外に置かれているとされている。その根拠として、「国家安全保障決定指令 189 号（NSDD-189)」が位置づけられており、基盤的研究の成果には可能な限り最大限に制限をかけない方針を掲げている。
- NSDD-189 では、「科学技術における米国の主導的地位を確保することは、米国の経済的・物理的な安全保障にとって不可欠な要素」であるとしながら、「科学力の強さのためには、創造性を確保できる研究環境が必要で、それは自由にアイディアを交換できる環境の確保」が必要として、研究の開放性（オープンサイエンス）の重要性を確認している。
- 基盤的研究について、「科学と工学の基礎研究および応用研究を意味し、その成果は通常公開され科学界で広く共有されるもの」と位置づけられ、同指令の目的は、「機密分類を受けていない連邦政府出資の基盤的研究の実施、または報告については、可能な限りその成果に制限をかけない（無制限)」ことにあるとしている。
- 研究セキュリティの強化に向けた取組みが実施されているが、そこにおいても NSDD-189 が定める研究開放性の原則を遵守することが確認されており、同指令は現在も基礎科学研究の開放性原則として連邦政府の政策の基盤となっている。