資料４

米国におけるセキュリティクリアランス制度の基本情報

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（第３回）
２０２３年3月２７日

法政大学人間環境学部　教授　永野秀雄

概要

- １．機密情報の位置づけ
- ２．なぜセキュリティクリアランスは必要なのか？
- ３．米国のセキュリティクリアランス手続の概要
- ４．米国の民間事業者等に対するセキュリティクリアランス制度の概要
- ５．外国政府等との機密情報の共有
- ６．米国における管理された非格付け情報（CUI）
- ７．米国における科学研究者・研究施設に対するセキュリティクリアランス制度

１．機密情報の位置づけ

- （１）なぜ、国家機密やその指定が必要となるのか？
- 国家は、国益の保護を目的として、国家機密を保全しなければならない。国家機密の保全が十分に機能せず、外部に漏えいすれば、重大な不利益を被ることになる。
- たとえば、外交交渉の前提となる機密情報が、事前に相手国に漏れていれば、その結果は不利なものになる。
- また、防衛に関する機密が他国に漏れれば、対抗措置をとれられてしまうおそれがあるばかりか、同盟国からも信用されなくなる。
- テロ抑止等の治安に関する機密情報が漏洩すれば、多くの国民の生命・財産への侵害を防ぐことが困難になる。
- 保全すべき重要な科学技術が外国に漏洩すれば、防衛力のみならず産業競争力の面でも、不利な地位に陥るおそれがある、など。

１．機密情報の位置づけ

- （２）米国で国家機密指定が可能な情報
- オバマ大統領が2009年に発した大統領令第13526号「機密指定された国家安全保障情報（Classified National Security Information）」第1.4条
- (a) 軍事計画、武器システム、又は作戦、(b)外国政府情報、(c) インテリジェンス活動（秘密活動を含む）、インテリジェンスに関する情報源、方法又は暗号、(d)機密情報源を含む連邦政府の外交関係又は外交活動、(e)国家安全保障に関連する科学的、技術的、経済的事項、(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、(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、又は、(h) 大量破壊兵器の開発、生産、利用に関する情報

１．機密情報の位置づけ

（３）機密情報のレベル

- 基本：大統領令第13526号第1.2条第(a)項において、機密情報のレベルを、当該情報が正当な権限によらずに開示された場合、国の安全保障にもたらされる損害のレベルに応じて、３種類に分類。
- ①「機密（top secret）」：「例外的に重大な損害」が引き起こされる情報
- ②「極秘（secret）」：「重大な損害」が引き起こされる情報
- ③「秘（confidential）」：「損害」が引き起こされる情報

１．機密情報の位置づけ

- （３）機密情報のレベル

- 上位の機密情報ほど、セキュリティクリアランス等の情報保全が厳しくなる。これらのセキュリティクリアランスが認められるのは、米国市民のみ（限定的な例外あり）。なお、機密情報へアクセスするためには、セキュリティクリアランスのほかに、知る必要性（Need-to-Know）の要件を満たす必要がある。

- しかし、日本政府が、①国家安全保障に関連する科学的、技術的、経済的事項や、重要インフラ等に関するセキュリティクリアランス制度を法制化し、②これらの機密情報を日本国と米国をはじめとした外国政府との間における協定で情報共有を承認しあえば、③セキュリティクリアランス要件を満たした日本企業も、これらの機密情報を共有することが期待できる。

1．機密情報の位置づけ

- （3）機密情報のレベル
- 同大統領令第4.3条で規定された例外的に高いレベルの機密保全が必要となる情報：機微区画情報(Sensitive Compartmented Information)
- 機微区画情報とは、国家安全保障上の理由から「機密」、「極秘」、又は「秘」として機密情報とされているのみならず、当該情報が、特に機微な情報源や手段により入手された等の理由により、特別なアクセス制限及び取り扱い要件に服する情報をいう。
- 例：暗号法、衛星等からの偵察調査、通信関連のインテリジェンス情報、核兵器や核攻撃対象に関する情報など。通常、米国は、これらの情報を他国と共有することはないと考えられる。
- 機微区画情報については、高度の情報保全が必要となることから、通常のセキュリティクリアランスよりもさらに厳しい身上調査や要件が課されている。

１．機密情報の位置づけ

- （３）機密情報のレベル
- 「管理された非格付け情報（Controlled Unclassified Information: CUI）」
- オバマ大統領が2010年11月４日に発した大統領令第13556号「管理された非格付け情報」に基づき、機密情報には該当しないものの、一般市民への情報公開が原則的に制限される情報。
- このCUIの取扱いについては、機密情報の取扱いで必要となる厳格なセキュリティクリアランスは求められておらず（米国では、セキュリティクリアランスと呼ばれていない簡易な身上調査のみ）、かつ、条件を満たせば米国市民でなくてもアクセスできる。
- CUIは、機密情報ではないものの、サイバー攻撃により大量のデータが盗まれると、防衛装備や構造物等の設計や仕様などが、かなりのレベルで推測されてしまう恐れがある。

２．なぜセキュリティクリアランスは必要なのか？

- なぜセキュリティクリアランスは必要なのか？ 特に、米国において個人についてのセキュリティクリアランスが設けられている５つの理由（米国法を研究した上での永野説）

- （１）　現実に外国政府等の工作員等が存在し、機密情報にアクセス可能な個人への接触を試みて不正に機密情報を取得しようと活動していることから、これによる機密情報の漏えいリスクをできるだけ低減させるため、当該リスクのある個人を機密情報を取り扱う職務に就けないようにするためである。

- （２）　一度、機密情報が外国等に漏えいしてしまうと、これにより国家安全保障上の損害を十分に回復できない事態が生じることから、予防的な側面が強く不確実性は残るものの、人的側面からの機密保全制度として、セキュリティクリアランス制度を設けている。

２．なぜセキュリティクリアランスは必要なのか？

- （３） セキュリティクリアランスは、個人の履歴や経済状況等の個人情報をもとにして適性を判断するので、憲法で保障されたプライバシー権等に対する人権侵害を引き起こす可能性を内包しているからこそ、これらの問題を回避するために、本人の同意を得て実施することや、当該情報の目的外使用の制限をはじめとして、その基本的な制度枠組みを法令によって定めている。

- （４） セキュリティクリアランス制度を法令に基づく制度とすることで、機密情報にアクセスする職に就く被用者等について、人事上の公平性を担保することができる。これは、法令により具体的な身上調査の範囲や判断基準を定め、さらには一定の苦情申立て等に関する制度を設けることで、行政機関の長による裁量に一定の制約を課している。

２．なぜセキュリティクリアランスは必要なのか？

- （５）　セキュリティクリアランスとその運用に関して、行政機関等は、一定程度、国民に対する説明責任果たす必要があり、また、議会は、セキュリティクリアランス制度の運用に対して民主的統制を行うべきであることから、同制度の法令による規制が存在している。

- その他のセキュリティクリアランス制度の必要性

  - 施設クリアランス：①機密情報が盗まれないようにするため、②危険な施設へのアクセスを制限するため（軍事施設の破壊等の防止など）。※民間企業（法人）に対するセキュリティクリアランスを含む。

  - サイバーセキュリティに関するセキュリティクリアランス：①ハッキングや破壊等の防止、②防御策の秘密保全等のため。人に対するセキュリティクリアランス及びセキュリティ基準の設定。

３．米国のセキュリティクリアランス手続の概要

（１）セキュリティクリアランス制度を構成する６段階の手続

第１段階は、個々の行政機関により、ある職が機密情報に日常的にアクセスする国家安全保障職等に該当すると判断される場合には、どのレベルの機密情報にアクセスするセキュリティクリアランスが必要となるかを決定する手続である。このような職に就く個人に対して、セキュリティクリアランスが求められることになる。このレベル決定は、システム化されている。

第２段階は、セキュリティクリアランス制度における申請手続である。まず、この制度の対象となる国家安全保障職等につき、現職の連邦公務員又は求職者が、その職の継続や応募のために、該当する標準書式に個人情報等を記入又は入力し、当該行政機関の保全担当官に提出する。この標準書式においては、身上調査を行う連邦政府機関が、自らの個人情報にアクセスすることに同意することが求められる。

３．米国のセキュリティクリアランス手続の概要

第３段階では、身上調査機関による調査が行われる。身上調査機関では、提出された標準書式に記載された情報に基づき、調査担当者が、具体的な身上調査を行う。そして、調査に基づいた報告書が作成され、身上調査を依頼した行政機関に送付される。

第４段階では、調査依頼を行った行政機関の保全決定担当官（Security Adjudication Officer）が、当該個人にセキュリティクリアランスを認定すべきか否かを決定する。

３．米国のセキュリティクリアランス手続の概要

第５段階は、不服申立て段階である。セキュリティクリアランスが認められなかった個人は、当該決定に対して不服申立てを行うことができる。

第６段階は、一定期間の経過に伴い、セキュリティクリアランスの再調査とこれに基づく認定を行う手続である。一度、セキュリティクリアランスが認められた個人についても、一定の期間が経過すると、再調査等によりその更新が求められる。

以下、上記のうち、基本的な理解に必要な箇所のみ説明する。

３．米国のセキュリティクリアランス手続の概要

- （２）身上調査を行う機関
- 2019年10月から、国防総省に新設された国防カウンターインテリジェンス・保全庁（Defense Counterintelligence and Security Agency: DCSA）」が、身上調査等を担当。
- DCSAは、105の連邦行政機関の被用者等に対して身上調査を行っている。これは、インテリジェンス機関等で独自にセキュリティクリアランスを実施する機関等を除き、DCSAが全連邦行政機関の約95％の身上調査を実施していることを意味している。
- DCSAは、これらの身上調査に関する業務以外にも、かつて国防保全局（DSS）が行っていた内部脅威対策プログラム、施設関連の保全及びカウンターインテリジェンスに関する業務を遂行している。

３．米国のセキュリティクリアランス手続の概要

（２）身上調査を行う機関

- DCSA は、国防総省及び他の35の連邦行政機関の委任を受けて、当該行政機関の民間の請負人等に対して国家産業保全プログラム運用マニュアル（National Industrial Security Program Operating Manual: NISPOM）（2020年12月21日から行政規則化された。また、その下部規範として国防総省マニュアル（全２巻）が存在）を運営する機能も担っている。つまり、民間の請負人等の人及び施設（法人含む）に対するセキュリティクリアランスを行っている。

- 大学や民間の研究機関にも適用される。

３．米国のセキュリティクリアランス手続の概要

（３）連邦行政機関による判断基準

- セキュリティクリアランス制度においては、行政機関の長等による恣意的な判断を防ぐため、法令による統一的な判断基準と手続を採用している。
- 現在用いられているものは、クリントン大統領が1995年に発した大統領令第12968号「機密情報へのアクセス」をブッシュ大統領が2008年７月に大統領令第13467号で改訂したものである。
- これらの大統領令を具体的な判断基準に落とし込んだものが、保全行政責任者指令第４号「国家安全保障判断指針」（Security Executive Agent Directive No.4, National Security Adjudicative Guidelines)である。

３．米国のセキュリティクリアランス手続の概要

（３）連邦行政機関による判断基準

- この判断指針では、セキュリティクリアランスの審査にあたり、「指針A. 米国への国家忠誠」、「指針B. 外国の影響」、「指針C. 外国の利益を優先する傾向」、「指針D. 性行動」、「指針E. 個人的行為」、「指針F. 財産に関する配慮」、「指針G. アルコール消費」、「指針H. 薬物への関与又は誤使用」、「指針I. 精神状態」、「指針J. 犯罪行為」、「指針K. 保護された情報の取扱い」、「指針L. 業務外活動」、「指針M. ITシステムの使用」という指針を用いて総合的な判断が行われている。

- これらの詳細については、長すぎるので省略。

３．米国のセキュリティクリアランス手続の概要

（４）定期的再調査手続

- 機密、極秘、秘に対応するセキュリティクリアランスの定期的再調査が必要となる期間は、①機密の場合は６年（2017年に５年から６年に延長された）、②極秘の場合は10年、③秘の場合は15年である。
- この定期的再調査手続は、商用データベース、連邦政府のデーターベース及びその他の合法的に利用可能な情報を用いて常に自動チェックを行う継続的身元審査手続（continuous vetting process）に移行中ではあるものの、現時点では、定期的再調査を補うものであって、これに代わるものではないとされている。

米国におけるセキュリティクリアランス保持者の報酬

TOTAL COMPENSATION BY CLEARANCE

	Avg. Total Compensation	% of Respondents
Confidential	$83,041	0.7%
Secret	$86,671	35.6%
Top Secret	$107,148	12.8%
Top Secret/SCI	$110,796	33.9%
DoE (Q or L)	$107,754	1.9%
Intel	$130,432	5.9%
DHS	$103,483	2.3%
Public Trust	$86,416	2.6%
Other Gov't Agency	$99,965	4.3%

Jillian Hamilton, Survey Results Show a Top Secret Clearance Can Earn Higher Compensation, ClearanceJobs (Aug. 18, 2022), *available at* https://news.clearancejobs.com/2022/08/18/survey-results-show-a-top-secret-clearance-can-earn-higher-compensation/.

４．米国の民間事業者等に対するセキュリティクリアランス制度の概要

- 米国で民間企業のセキュリティクリアランス制度が、行政機関のものとは別制度である理由

- 国家の防衛、重要インフラの防護及びその他の国家安全保障に関する事業の実施には、民間企業の協力が欠かせない。
- 今日の先進国では、防衛装備にしろ、サイバー関連設備にしろ、これらの全てを国営企業が製造・運営することはできない。このため、これらの装備等の製造等などあたっては、国の機密情報を民間企業と共有して業務を遂行してもらう必要がある。
- しかし、民間企業は、国とは別個の法人であり、また、通常は株式会社制度等により運営されており、国が支配しているわけではない。
- このため、政府とは別のセキュリティクリアランス制度が設けられている。

４．米国の民間事業者等に対するセキュリティクリアランス制度の概要

- 具体的には、
  ①機密情報を扱う民間企業等の取締役・被用者等からの機密漏えいを防ぐための個人に対するセキュリティクリアランス（本人同意が必要）、

- ②当該民間企業の施設からの機密漏えいを防ぐための施設クリアランス、及び、

- ③当該民間企業等が外国関係の株主等に支配されて機密情報が不正にアクセスされたり、外国等に流出することを防ぐ制度などが必要となる→「外国による所有権、管理又は影響（Foreign Ownership, Control, or Influence: FOCI）」に関する規制が設けられている。

４．米国の民間事業者等に対するセキュリティクリアランス制度の概要

- FOCIの概要
- ①民間の法人が、法人としてのセキュリティクリアランスを取得するために、「外国関係者に関する申請書」を主務保全官庁（Cognizant Security Agency: CSA；多くの場合、国防総省）に提出。
- ②審査により、FOCIの下にあると決定された民間の法人は、その問題を無効化するか軽減するための保全措置が認められるまで、その施設クリアランスは認められない。
- ③民間の法人は、この問題を解決するために、「FOCI行動計画（FOCI action plans）」により対応することになる。

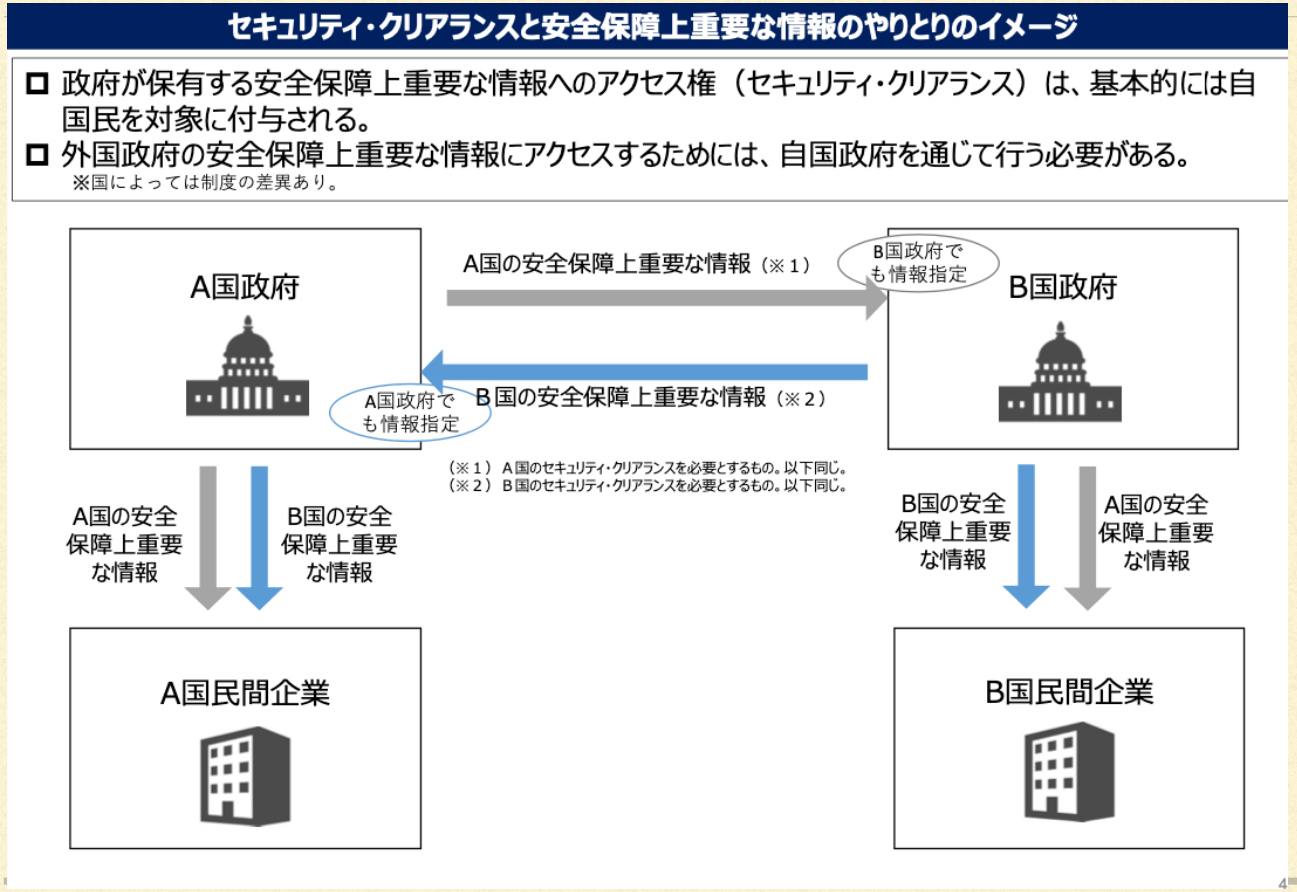
４．米国の民間事業者等に対するセキュリティクリアランス制度の概要

- FOCI関連の判断要素（総合的に判断される）
- (1) 米国をターゲットとした経済に関する又は外国政府によるスパイ事案に関する過去の履歴。
- (2) 正式に認可されないまま実施された技術移転に関する過去の履歴。
- (3) 関連する米国法令及び契約の遵守に関する過去の履歴。
- (4) 当該法人がアクセスすることになる情報の類型及び機微性。

４．米国の民間事業者等に対するセキュリティクリアランス制度の概要

- FOCI関連の判断要素（総合的に判断される）
- (5) 当該法人の直接的、中間的及び最終親会社の存在を考慮した上で、外国関係者が当該法人の過半数又は少数者（minority）の地位を占めているか否かを含めたFOCIの提供元、性質及び程度。
- (6) 関係する二国間及び多国間の情報保全及び情報交換合意の性質。
- (7) 外国政府による全部若しくは一部の直接的・間接的な所有又は支配。
- (8) 当該法人の運営若しくは経営を管理し又はこれらに影響を及ぼす外国権益（foreign interests）の能力を示唆する又は明示するその他の要素。

５．外国政府等との機密情報の共有



第１回資料３　（4p）

６．米国における管理された非格付け情報（CUI）

- CUI（８ｐ参照）については、外国人によるアクセスも可能であり、機密情報にアクセスするための厳格なセキュリティクリアランスは不要である。しかしながら、米国の民間企業が採用試験のときに一般的に用いているものに類する人的スクリーニング（バックグラウンドチェック）が行われている。

- 代表的な民間企業による人的スクリーニング：①標準的な犯罪歴調査（standard criminal background check）、②信用調査（credit check）、③国籍、④その他（薬物検査等）。

- 理由：米国では、日本の民法第715条とは異なり、使用者責任を、問題を起こした被用者に対する採用段階における調査義務の懈怠ととらえる「過失雇用責任（negligent hiring liability）」法理が（州の）コモンロー上確立している。このため、使用者が、その抗弁として採用前に合法な人的スクリーニングを行うことが認められているため、そのサービスを提供する身上調査会社が発展して利用されている。

７．米国における科学研究者・研究施設に対するセキュリティクリアランス制度

- 国家安全保障決定指令第189号「科学的、技術的及び工学情報の移転に関する国家政策」

- 米国では、レーガン大統領が1985年に発した国家安全保障決定指令第189号「科学的、技術的及び工学情報の移転に関する国家政策」では、連邦政府資金を受給する大学や研究機関における基礎研究における成果は、最大限可能な限りにおいて制限しないものの、国家安全保障の観点から、これらの研究により生み出された情報を管理する必要が生じる場合があるとして、その場合には、各行政機関が、事前に秘密指定制度を適用するか否かを決定することとしている。

- 連邦政府が研究資金を供与した研究で、秘密指定がなされたものについては、①大学・研究機関・民間企業で秘密を扱う研究施設に施設クリアランスが行われ、②関係者に対して人的セキュリティクリアランスが行われる。

７．米国における科学研究者・研究施設に対するセキュリティクリアランス制度

- トランプ大統領は、退任直前の2021年１月14日に、国家安全保障大統領覚書第33号「連邦政府により支援された研究開発に関する国家安全保障政策についての大統領覚書」を発出した。
- 本覚書の目的は、連邦政府が資金供与を行う研究開発について、外国からの干渉や搾取を防ぎ、保護を強化するための制度構築を行うこと。
- 本覚書には直接のセキュリティクリアランスに関する規定はないが、利益相反（conflict of interest）と責務相反（conflict of commitment）が起きないように、研究者等に対する従来よりも厳しい情報開示を求めること、内部脅威対策、外国旅行に関する保全策、サイバーセキュリティ、輸出入管理等を規定。

参考

- 「米国における科学者・技術者に対するセキュリティクリアランス ー量子情報科学を中心に(上)」CISTEC journal 192号148頁以下（2021年3月）。
- 「米国における科学者・技術者に対するセキュリティクリアランス ー量子情報科学を中心に(下)」CISTEC journal 193号242頁以下（2021年5月）。