

参議院常任委員会調査室・特別調査室

論題	技術流出防止策としてのセキュリティ・クリアランス ～経済安全保障推進法の改正による制度導入に向けて～
著者 / 所属	柿沼 重志 / 内閣委員会調査室
雑誌名 / ISSN	経済のプリズム / 1882-062X
編集・発行	参議院事務局 企画調整室（調査情報担当室）
通号	217号
刊行日	2022-10-6
頁	1-21
URL	https://www.sangiin.go.jp/japanese/annai/chousa/keizai_prism/backnumber/r04pdf/202221701.pdf

※ 本文中の意見にわたる部分は、執筆者個人の見解です。

※ 本稿を転載する場合には、事前に参議院事務局企画調整室までご連絡ください（TEL 03-3581-3111（内線 75044） / 03-5521-7683（直通））。

技術流出防止策としてのセキュリティ・クリアランス

～経済安全保障推進法の改正による制度導入に向けて～

内閣委員会調査室 柿沼 重志

1. はじめに
2. 経済安全保障推進法の法案審議の前に表明された官民の意見や国会論議
3. 経済安全保障推進法制定時の法案審議で行われた国会論議等
4. 特定秘密保護法における適性評価制度
5. 米国のセキュリティ・クリアランス制度
6. おわりに

1. はじめに¹

経済安全保障推進法²は、令和4年5月11日に参議院本会議で法案が可決、成立し、同年5月18日に公布、一部の規定は同年8月1日から施行された。

同法案に関する衆参の内閣委員会や本会議における論議において、繰り返し取り上げられたのが、セキュリティ・クリアランスである。

セキュリティ・クリアランスとは、機密情報へのアクセスを一部の政府職員や民間の研究者・技術者に限定する仕組みであり、AIや量子技術など最先端技術に関する機密情報に触れる関係者に資格を付与して、機密情報にアクセスできる者を明確にし、それらの情報が国外に流出することを防ぐ狙いがあるとされる³。

技術流出防止への対応の巧拙は一国の産業競争力にも影響を与えると考えられ⁴、その意味でも、どのようなセキュリティ・クリアランス制度を我が国として今後導入するかは重要な課題である。なお、機密情報を共有する英語圏の枠

¹ 本稿は、令和4年9月7日の脱稿時点までの情報に基づき執筆している。

² 正式名称は、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律。

³ 『産経新聞』（令4.6.20）

⁴ この点について、世耕経済産業大臣（当時）は、「産業競争力確保の観点からは、技術流出を防止し、我が国企業が開発した技術は我が国企業がしっかりと活用していくといった体制を整えることが非常に重要である。技術流出防止と産業競争力というのは密接に関係していると思っている」旨、答弁している（第196回国会参議院決算委員会会議録第3号14頁（平30.4.23））。

組みである「ファイブ・アイズ」を構成する米国、英国、カナダ、オーストラリア及びニュージーランド、そして韓国等では、民間人に対してもセキュリティ・クリアランスが導入されており、日本も今後、海外との共同の研究開発を進める上で必須の資格となるとされている。

こうした点も踏まえ、衆参の内閣委員会の附帯決議では、「国際共同研究の円滑な推進も念頭に、我が国の技術的優位性を確保、維持するため、情報を取り扱う者の適性について、民間人も含め認証を行う制度の構築を検討した上で、法制上の措置を含めて必要な措置を講ずること」とされている。

経済安全保障推進法の成立後、政府は、セキュリティ・クリアランスの導入に向け、令和5年の通常国会で、経済安全保障推進法の改正案を提出することを検討している旨の報道も出ており⁵、セキュリティ・クリアランスの導入は、まさに経済安全保障における次なる課題として、位置付けられてきた。こうした流れもあり、令和4年8月10日に新たに就任した高市経済安全保障担当大臣も、「セキュリティ・クリアランスは非常に重要だと考えております。これを何としても盛り込みたい。そのような強い思いを持っております。これは国会の附帯決議でもございましたし、既に骨太の方針などにも入っておりますので、しっかりと進めてまいります」と述べている⁶。

本稿では、まず、同年2月に経済安全保障推進法案が国会に提出される以前にセキュリティ・クリアランスについて、官民でどのような意見が出されてきたのか、また、同法案についての法案審議が行われた際の国会議論等についてそれぞれ整理する。

次に、行政機関の職員等（一部、限定的に民間人も含む）を対象とした適性評価制度が盛り込まれている特定秘密の保護に関する法律⁷（以下「特定秘密保護法」という。）における適性評価制度とはどのようなものであり、これまでどのように活用されてきているのかを概観する（なお、同法に基づき秘密指定さ

⁵ 『産経新聞』（令4.6.20）。なお、自由民主党の高市政調会長（当時）は、令和4年7月24日の東京都内の講演で、経済安全保障推進法にセキュリティ・クリアランスが盛り込めなかった点について、「今年はまずは法体系を作ることを優先したので残念なことが残った」と述べた上で、法改正について、「来年を目指して取りかかろうというつもりでいる」との考えを表明したとされている（『読売新聞』（令4.7.26））。

⁶ 高市内閣府特命担当大臣就任記者会見（令4.8.10）（https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20220810kaiken.html）

⁷ 同法は平成25年12月13日公布、平成26年12月10日に施行されている。なお、法律施行日と同日に、衆参両院の情報監視審査会設置を定めた改正国会法も施行されている。情報監視審査会は特定秘密保護制度の運用を常時監視するために設置された常設の機関である。

れるのは安全保障に関わる4分野（防衛、外交、特定有害活動（スパイ行為等）の防止、テロリズムの防止）に限られている⁸。加えて、海外事例の代表例として、米国のセキュリティ・クリアランス制度をそれぞれ概観する。これらを踏まえ、最後に、我が国でセキュリティ・クリアランスを導入する際の主な論点を列挙することとしたい。

2. 経済安全保障推進法の法案審議の前に表明された官民の意見や国会論議

ここでは、経済安全保障推進法の法案審議の前に表明された官（（1）から（3））及び民（（4）から（6））の意見や経済安全保障推進法案の提出前の国会論議（7）について俯瞰する。

（1）技術情報等の適切な管理の在り方に関する研究会報告書

平成20年7月28日に経済産業省の技術情報等の適切な管理の在り方に関する研究会が取りまとめた報告書では、「諸外国においては、特に秘密にすべき情報を扱う組織の職員に対しては、国家安全保障上の観点から、信頼性確認（クリアランス）を行うことが一般的であるところ、我が国においても着実に同制度の導入を図っていく必要がある。この場合において、信頼性確認制度の導入に際し、確認により期待される効果、確認の実施方法、実施上の問題、実効性、基本的人権に係る憲法上の要請との調整、国民的合意形成の必要性等、多くの論点・課題について議論が必要である」とされた。

（2）産業構造審議会通商・貿易分科会安全保障貿易小委員会中間報告

（1）と以下に詳述する（2）の間は10年以上の空白がある。この間も、技術流出防止に関しては、不正競争防止法の改正（平成21年、平成23年、平成27年と相次いで改正）による営業秘密の保護強化⁹を始め、各種の政策対応が行われてきたほか、平成25年には特定秘密保護法を成立させ、行政機関の職員

⁸ セキュリティ・クリアランス制度の創設に当たっては、いわゆる特定秘密の対象分野を広げる手法もあり得たが、政府は同法とは切り離すことを検討している旨の報道も過去に行われていた（『朝日新聞』（令2.8.13））。その後、令和4年5月11日に経済安全保障推進法が成立したことで、現在は同法を改正し、セキュリティ・クリアランス制度を創設することが有力視されている。

⁹ 営業秘密が不正競争防止法の保護を受けるためには、①秘密管理性（秘密として管理されていること）、②有用性（事業活動に有用な技術上又は営業上の情報であること）、③非公知性（公然と知られていないこと）の3つの要件を全て満たす必要がある（同法第2条第6項）。

等については、適性評価の制度が導入されている¹⁰。

令和元年10月8日に経済産業省の産業構造審議会通商・貿易分科会安全保障貿易管理小委員会が取りまとめた中間報告では、「技術力や産業基盤の維持・強化には、国際的な研究開発協力の推進は不可欠であるが、特に、機微技術に関する国際共同研究開発のパートナーとして、諸外国に我が国を受け入れてもらうためには、国際共同研究開発により触れる可能性のある相手国が保有する機微技術に関する情報等に対して、情報保全対策の同等性を担保する必要がある。一方、我が国の情報保全に係る制度としては、特定秘密の保護に関する法律に基づく特定秘密やMDA秘密保護法（日米相互防衛援助協定等に伴う秘密保護法）に基づくMDA秘密に該当する非常に高度な機密情報については、当該情報を受け取ることになる民間人についても処罰対象として情報保全を図る制度が構築されているものの、特定秘密やMDA秘密に該当しない機微技術に係る情報については制度が不十分であるとして、機微技術に関する国際共同研究開発に我が国企業が参加できないという指摘もあり、産業保全に関する今後の対応について検討すべきである」とされた。

（3）統合イノベーション戦略 2020

令和2年7月17日に閣議決定された「統合イノベーション戦略 2020」では、「科学技術・産業競争力を最先端レベルで維持するとともに、国際共同研究を円滑に推進し、我が国の技術的優位性を確保・維持する観点も踏まえ、諸外国との連携が可能な形での重要な技術情報を取り扱う者への資格付与の在り方を検討」とされた。

（4）技術安全保障研究会¹¹による提言

平成30年10月10日に技術安全保障研究会が公表した「諸外国並みの技術安全保障体制の構築を」では、「米国に倣った個人レベルのクリアランス制度を導入し、安全保障上機微に触れる技術の製品の開発にあたっては政府として技術

¹⁰ この点について、日本弁護士連合会は、「取扱者の適性評価制度は、プライバシー侵害性が極めて高いことなどの問題がある」と批判的な意見を表明している（日本弁護士連合会「秘密保護法制定に反対し、情報管理システムの適正化及び更なる情報公開に向けた法改正を求める意見書」（平成25年10月23日））。

¹¹ 技術安全保障研究会は、日本の技術・経済・安全保障に関する学界・官界・経済界の有識者により、平成29年に設立され、内外の情勢分析や提言活動を行っている（座長：玉井克哉東京大学先端科学技術研究センター教授）。

者の適格性保証を行う。特に、非公開特許に指定された技術情報を活用して製品化や研究開発に従事する個人及び組織に対し、セキュリティ・クリアランスの取得を義務付けると共に、防衛省等各府省が実施している現行の秘密取扱者適格性確認制度に組み入れることを検討する」とされた。

次いで、令和2年3月11日に同研究会が公表した「経済安全保障法の制定を」では、「安全保障に係る技術情報、サイバーセキュリティ情報等を扱う企業人、大学研究者等について、一種の資格制度（セキュリティ・クリアランス制度）を導入し、重要情報を扱う権利と責任を付与すべきである（罰則規定を含む）。この資格は、関連組織の求めに応じて、審査を経て対象となる個人に付与されるもので、同盟国・友好国との制度の同等性にも配慮したものとすべきである。また、扱い得る情報の重要度に応じて、いくつかの水準を設ける必要がある」とされた。

（5）経団連による意見¹²

令和4年2月9日に（一社）日本経済団体連合会（経団連）が公表した「経済安全保障法制に関する意見」では、「機微な情報の共有が必要とされる諸外国との共同研究、諸外国政府からの受注などにあたっては、いわゆるセキュリティ・クリアランスと呼ばれる適性評価を受けていることが求められることがある。『統合イノベーション戦略2020』（2020年7月17日閣議決定）においては、『科学技術・産業競争力を最先端レベルで維持するとともに、国際共同研究を円滑に推進し、我が国の技術的優位性を確保・維持する観点も踏まえ、諸外国との連携が可能な形で重要な技術情報を取り扱う者への資格付与の在り方を検討』することが盛り込まれているところ、わが国としても、中長期的課題として、相手国から信頼されるに足る、実効性のある情報保全制度の導入を目指すべきである」とされた。

（6）経済同友会による意見¹³

令和4年2月16日に（公社）経済同友会が公表した「経済安全保障法制に関する意見」では、「法制の実効性を高めるには、経済インテリジェンス機能や情報保全制度などの強化が不可欠である。経済インテリジェンスは、関係する政府機関と民間企業の人材流動性を高めるなど官民連携を強化し、多層的な情報

¹² 経済安全保障推進法案の閣議決定の直前に経済団体から出された意見。

¹³ 同上

把握を行うことが重要である。また、わが国の技術優位性を確保する観点を踏まえ、同盟国・同志国との国際共同研究を推進、強化する必要がある。その際、民間事業者も参加して先端技術共同開発を進めるうえで、機密情報の取り扱い資格者を政府が認定する『セキュリティ・クリアランス』を含む情報保全の仕組みが必要になる。政府は早急に検討を始め、速やかに導入すべきである」とされた。

（7）経済安全保障推進法案の法案審議前に行われた国会論議

まず、令和2年11月27日の衆議院安全保障委員会で、セキュリティ・クリアランスを導入する必要性について問われた政府参考人は、「AI、量子、こういった革新的であり、かつ本質的にデュアルユースな技術の登場等を背景とし、安全保障の裾野が経済、技術分野に急速に拡大をしており、かつ、その領域において新たな課題というものが顕在化している。政府としては、統合イノベーション戦略2020において、国際共同研究を円滑に推進し、我が国の技術的優位性を確保、維持する観点も踏まえ、諸外国との連携が可能な形での重要な技術情報を取り扱う者への資格付与のあり方を検討するという事としており、必要な措置の検討を進めてまいりたいと考えている」旨、答弁している¹⁴。

次いで、令和3年3月11日の参議院予算委員会で、セキュリティ・クリアランス導入の検討状況や導入のスケジュールについて問われた政府参考人は、「統合イノベーション戦略2020においても、科学技術、産業技術力を最先端レベルで維持する、このためにも国際共同研究を円滑に推進し、我が国の技術的優位性を確保、維持する観点が重要とされている。どのような情報保全の在り方が適切か、様々な観点から現在関係省庁が集まり、検討を進めている。論点として決して簡単ではないが、引き続き全力を挙げて関係省庁において必要な措置の検討を進めてまいりたい」旨、答弁しており¹⁵、統合イノベーション戦略2020に沿って前向きな検討を進めるとするものの、導入のスケジュールについては明言を避けている。

さらに、令和4年1月24日の衆議院予算委員会で、セキュリティ・クリアランス導入に対する認識を問われた小林経済安全保障担当大臣(当時)は、「セキュリティ・クリアランスは、主要国を中心に、機微技術に関するものを含めて、主として政府が保有する秘密情報の保全等の観点から導入されているものと承

¹⁴ 第203回国会衆議院安全保障委員会議録第4号2～3頁(令2.11.27)

¹⁵ 第204回国会参議院予算委員会議録第9号7頁(令3.3.11)

知をしている。経済安保に関連して取り組まなければならない課題は多岐にわたっているため、関係省庁と連携をしながら、できることからスピード感を持って対応していきたい」旨、答弁しており¹⁶、政府にとっても優先度が高い課題であると推察される。しかし、プライバシー侵害への懸念等の課題があり、令和4年の通常国会に提出する経済安全保障推進法案にはセキュリティ・クリアランスは盛り込まれていない。

3. 経済安全保障推進法制定時の法案審議で行われた国会論議等

(1) 法案審議の際に行われたセキュリティ・クリアランスに関する議論

セキュリティ・クリアランスとはどういうものかについて、小林経済安全保障担当大臣（当時）は、「セキュリティ・クリアランスについては、主要国を中心に、諸外国では、機微技術に関するものを含め、主として政府が保有する秘密情報の保全の観点から、秘密情報へのアクセス資格を有することを決定する制度として導入されている。また、我が国においては、特定秘密の保護に関する法律に基づいて、政府が保有する特定秘密の取扱いが見込まれる者に対して、第5章に『適性評価』とあるが、適性評価として、その者が特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないことについての評価が実施されている」旨、答弁している¹⁷。

また、セキュリティ・クリアランスを法案に盛り込むことが見送られた理由等について、同大臣は、「セキュリティ・クリアランス制度については、各国との共同研究などを民間部門も含めて進めていく上で、我が国でもクリアランスを取得できないか、そういう声があることは承知をしている。他方、このクリアランス制度というのは、個人の情報に対する調査を含むものであり、こうした制度に対する国民の理解の醸成の度合い、また、海外において実際にクリアランスの取得を要請される具体的事例の検証、こうしたことをまずは踏まえた上で、今後の検討課題の一つになり得ると認識している。いずれにしても、情報流出対策を更に進めていく必要があり、国際共同研究開発を推進することは重要であるので、政府としては、必要な取組の強化に引き続き努めていきたい」旨、答弁している¹⁸。

なお、経済安全保障法制に関する有識者会議において、セキュリティ・クリ

¹⁶ 第208回国会衆議院予算委員会議録第2号7～8頁（令4.1.24）

¹⁷ 第208回国会衆議院内閣委員会議録第13号18頁（令4.3.30）

¹⁸ 第208回国会衆議院内閣委員会議録第11号8頁（令4.3.23）

アランスに関して、どのような議論があったのか等について、同大臣は、「特許非公開に関する分野別の検討会合において、非公開とされた特許出願を取り扱う職員として、クリアランスを受けた者が関与するのが重要ではないかとの意見があったが、その後、この法制にクリアランスを含むべきとの議論にはならず、また、この有識者会議の提言にも含まれなかったことから、今回の法案には反映されていない」旨、答弁している¹⁹。

次に、セキュリティ・クリアランスを検討していく際に、個人情報についての懸念の声が国民にあることに対する認識について、同大臣は、「諸外国の例を見ると、セキュリティ・クリアランス制度には個人の情報に対する詳細な調査が含まれており、こうした制度に対する国民の理解の醸成の度合いを十分に検証する必要があると考えている。諸外国の例や特定秘密保護法の適性評価の調査項目を例とすれば、機微な情報にアクセスするポストへの異動や国際共同研究などを行うに先立ち、通常は上司などに報告義務のない犯歴、薬物やアルコールの依存症歴、また精神疾患、信用状態その他の経済的状況などのセンシティブな個人情報を報告させて調査することとなっていて、本人の同意を得るとはいえ、そうした調査に応じることとなることへの理解や、その評価対象者のみならず、関わりが深い家族や同居人についても、特定有害活動やテロリズムとの関係について調査することへの理解、調査の結果、クリアランスが得られなかった者が企業や研究機関内に生まれることへの理解などが社会一般に醸成される度合いというものを検証していく必要がある」旨、答弁している²⁰。

また、本人が不同意の場合やクリアランスが否定や撤回された場合の不利益取扱いの問題について、同大臣は、「特定秘密の指定及びその解除並びに適性評価の実施に関する統一的な運用を図るための基準において、適性評価は、特定秘密の取扱いの業務を行った際に特定秘密を漏らすおそれがないことについての評価であり、人事評価又はその他の能力の実証を行うものではなく、人事評価のために適性評価の結果を利用等してはならないとされている。なお、適性評価の実施に同意しなかった者や、適性評価の結果、特定秘密を漏らすおそれがないと認められなかった者は、特定秘密を取り扱わない部署に配置換えされたり、特定秘密を取り扱う部署には配置されなかったりすることにはなるが、これは特定秘密の保護のための措置であって、不利益な取扱いには当たらない

¹⁹ 第 208 回国会衆議院内閣委員会議録第 13 号 19 頁（令 4. 3. 30）

²⁰ 第 208 回国会衆議院内閣委員会議録第 13 号 20 頁（令 4. 3. 30）

と認識している」旨、答弁している²¹。

次に、セキュリティ・クリアランスへの評価や課題について、衆議院内閣委員会に参考人として出席した東京大学東洋文化研究所の佐橋亮准教授は、「セキュリティ・クリアランスは、今後、国際競争や、機微技術の取扱いに関して国際的な共同開発などに入るときに、民間でも非常に有用になってくると思う。ただ、このときに考えなくてはいけないのは、国際的に通用する枠組みにするということであり、そのためには、背景調査も含めた綿密な制度設計というのが必要になってくる。私は、導入するのであれば、簡易的な形で導入するのではなく、本格的な導入、国際的に通用するものが必要であって、そういったしっかりとした制度設計にしていきたい」旨の意見を述べている²²。一方で、衆議院内閣委員会に参考人として出席した東北大学の井原聰名誉教授は、「私は原則反対である。人権に関わるわけだが、当人だけではなく、その背後につながる関係者たちにも大きな影響を与える」旨の意見を述べている²³。

なお、セキュリティ・クリアランスの導入は行われなかったが、法案の中でも、いわゆる特定重要技術（図表1）に関して、一定の技術流出防止策は講じられている。

図表1 特定重要技術の定義

「**先端的技術**」：「将来の」国民生活及び経済活動の維持にとって重要となり得る先端的な技術
「**特定重要技術**」：「先端的技術」のうち①～③のいずれかに該当するもの（複数該当もあり得る）

①【 当該技術を外部に不当に利用された場合 】において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの ⇒ 当該技術の適切な管理が必要
②【 当該技術の研究開発に用いられる情報が外部に不当に利用された場合 】において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの ⇒ 研究開発に関する情報の適正な管理や、守秘義務の求めが必要
③【 当該技術を用いた物資又は役務を外部に依存することで外部から行われる行為によってこれらを安定的に利用できなくなった場合 】において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの ⇒ 我が国が国際社会における自律性、優位性、ひいては不可欠性を確保・維持する必要

（出所）「第2回経済安全保障重要技術育成プログラムに係るプログラム会議資料」（令4.8.8）より作成

²¹ 第208回国会衆議院内閣委員会議録第13号20頁（令4.3.30）

²² 第208回国会衆議院内閣委員会議録第14号9頁（令4.3.31）

²³ 第208回国会衆議院内閣委員会議録第14号10頁（令4.3.31）

この点について、小林経済安全保障担当大臣は、「この法案の中で措置する協議会²⁴においては、機微な情報を含む有用な情報の共有や協議が安心して円滑に行われるように、構成員に罰則付きの守秘義務を新たに課すこととした。それに加えて、構成員に必要な保全措置を講じることを法律上求めることとしており、まずはこの法律の下で必要な技術流出対策を講じつつ、官民技術協力というものを推進していく」旨、答弁している²⁵。

（２）「経済財政運営と改革の基本方針 2022」

令和４年６月７日に閣議決定された「経済財政運営と改革の基本方針 2022」では、「国際共同研究等における具体的事例の検証等を踏まえつつ、重要情報を取り扱う者への資格付与について制度整備を含めた所要の措置を講ずるべく検討を進める」とされている²⁶。

４．特定秘密保護法における適性評価制度²⁷

以下では、（１）から（３）で特定秘密保護法における適性評価制度に関する主な規定を整理するとともに、（４）から（６）では特定秘密保護法による適性評価制度の運用状況について、データを整理した上で概観する。

（１）特定秘密の取扱者の制限

ア 取扱者の制限

特定秘密の取扱いの業務は、特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないことについての評価（以下「適性評価」という。）により、特定秘密を漏らすおそれがないと認められた者でなければ、行ってはならないこととしている。ただし、行政機関の長、国务大臣、内閣官房副長官、

²⁴ 経済安全保障推進法第 62 条第 1 項では、国の資金により行われる特定重要技術の研究開発等について、研究開発大臣（文部科学大臣、経済産業大臣等）が、特定重要技術研究開発基本指針（同法第 60 条で規定）に基づき、個別プロジェクトごとに、研究代表者の同意を得て協議会を設置することが規定されている。詳細については、拙稿「4つの柱で構成される経済安全保障推進法案－経済活動への過度な介入回避と規制の実効性確保は両立可能か－」『立法と調査』No. 444（令 4. 4）9～11 頁を参照。

²⁵ 第 208 回国会参議院内閣委員会会議録第 13 号 18 頁（令 4. 4. 26）

²⁶ 同日閣議決定された「新しい資本主義のグランドデザイン及び実行計画」でも、「重要情報を取り扱う者への資格付与のための所要の措置について、国際共同研究等における具体的事例の検証を踏まえ、検討を進める」とされている。

²⁷ （１）から（３）までの記述については、柳瀬翔央「我が国の情報機能・秘密保全－特定秘密の保護に関する法律案をめぐって－」『立法と調査』No. 347（平 25. 12）及び内閣官房「特定秘密の保護に関する法律【逐条解説】」（平 26. 12. 9）を参考にしている。

内閣総理大臣補佐官、副大臣、大臣政務官等は適性評価を要せず特定秘密の取扱いの業務を行うことができる。

イ 適性評価の実施

a 適性評価の実施者及び評価対象者

適性評価は、行政機関の長又は警察本部長（以下「評価実施者」という。）が実施する。行政機関の長による、適性評価の対象となる者（以下「評価対象者」という。）は、行政機関の職員又は適合事業者²⁸の従業者であり、警察本部長による評価対象者は、都道府県警察の職員である²⁹。

b 適性評価の調査事項

適性評価は、評価対象者について、次に掲げる事項についての調査を行い、その結果に基づき実施するものとしている。

- ①特定有害活動及びテロリズムとの関係に関する事項（評価対象者の家族及び同居人の氏名、生年月日、国籍及び住所を含む。）
- ②犯罪及び懲戒の経歴に関する事項
- ③情報の取扱いに係る非違の経歴に関する事項
- ④薬物の濫用及び影響に関する事項
- ⑤精神疾患に関する事項
- ⑥飲酒についての節度に関する事項
- ⑦信用状態その他の経済的な状況に関する事項

なお、平成 25 年 3 月の衆議院内閣委員会で、調査事項について、より具体的に示すべきではないかと問われた菅内閣官房長官（当時）は、「現行の秘密取扱者適格性確認制度における調査は、職員の任用に関して、任命権者の権限の範囲内で実施しているものであり、調査事項を明らかにした場合、対抗措置を講じられるなど、政府の情報保全に支障を及ぼすおそれがあることから、これを明らかにすることは適当ではないと思う。また、法の下での平等、思想、信条の自由の精神に基づいて、適正に運用をしている

²⁸ 物件の製造若しくは役務の提供を業とする者で、特定秘密の保護のために必要な施設設備を設置していること等の基準に適合するものと定義されている。

²⁹ 日本弁護士連合会は、同会のホームページで、「秘密保護法には、『特定秘密』を取り扱う人を調査し、管理する『適性評価制度』というものが規定されています。調査項目は、ローンなどの返済状況、精神疾患などでの通院歴…等々、プライバシーに関する事項を含め、多岐にわたります。秘密を取り扱う人というのは、国家公務員だけではなく、一部の地方公務員、政府と契約関係にある民間事業者で働く人も含まれます」としており、適合事業者を対象に含めることに批判的な立場を取っている（https://www.nichibenren.or.jp/activity/human/complcity_secret/secret/problem.html）（令和 4 年 9 月 7 日最終アクセス）。

と思う」旨、答弁している³⁰。

c 適性評価の手續

適性評価は、あらかじめ、評価対象者に対し、調査を行う旨等を告知した上で、その同意を得て実施される。

評価実施者は、前掲の7事項について調査を行うため必要な範囲内において、①評価対象者やその関係者に質問、②評価対象者に資料の提出を要求、③公務所³¹又は公私の団体³²に照会ができる。

適性評価を実施したときは、その結果を評価対象者に対し通知するものとし、特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないと認められなかった旨を通知するときは、適性評価の円滑な実施の確保を妨げない範囲内において、その理由を通知するものとしている。

また、評価対象者は、実施された適性評価について評価実施者に対し苦情の申出をすることができ、評価実施者は、評価対象者から苦情の申出を受けたときはこれを誠実に処理し、処理の結果を苦情の申出をした者に通知するものとしている。

d 個人情報等の目的外利用及び提供の禁止

行政機関の長及び警察本部長は、特定秘密の保護以外の目的のために、①適性評価の実施について同意しなかったこと、②適性評価の結果、③適性評価の実施に当たって取得する個人情報を、国家公務員法上の懲戒の事由等に該当する疑いがある場合を除き、自ら利用し、又は提供してはならないものとしている。

(2) 運用基準の策定及び本法律の解釈適用

ア 統一的な運用を図るための基準

政府は、特定秘密の指定、解除及び適性評価の実施に関し、統一的な運用を図るための基準を定めるものとし、基準の策定又は変更時には、我が国の安全保障に関する情報の保護、行政機関等の保有する情報の公開、公文書等の管理等に関し優れた識見を有する者の意見を聴かなければならないこととしている。

³⁰ 第183回国会衆議院内閣委員会議録第3号34頁(平25.3.15)

³¹ 「公務所」とは、国家機関のほか地方公共団体の機関を指す。

³² 「公私の団体」とは、学校、病院、医院・診療所、商工会議所、会社、組合、信用情報機関等社会機能を営む団体が広く含まれる。

なお、平成 26 年 10 月 14 日に、「特定秘密の指定及びその解除並びに適性評価の実施に関し統一的な運用を図るための基準」が閣議決定された³³。

イ 本法律の解釈適用

本法律の適用に当たっては、これを拡張して解釈して、国民の基本的人権を不当に侵害するようなことがあってはならず、国民の知る権利の保障に資する報道又は取材の自由に十分配慮しなければならないこととし、また、出版又は報道の業務に従事する者の取材行為については、専ら公益を図る目的を有し、かつ、法令違反又は著しく不当な方法によるものと認められない限りは、これを正当な業務による行為とするものとする。

(3) 罰則

特定秘密を取り扱うことを業務とする者が特定秘密を漏らしたときは「10 年以下の懲役」とし、公益上の必要により行政機関から特定秘密の提供を受け、これを知得した者が漏らしたときは「5 年以下の懲役」としている。

また、特定秘密を保有する者の管理を害する行為により、特定秘密を取得した者は、「10 年以下の懲役」とし、これら漏えい又は取得行為の未遂の罰則規定に加え、共謀³⁴、独立教唆³⁵、煽動³⁶に対する罰則規定等も設けている。

なお、特定秘密保護法と国家公務員法の罰則を比較したのが下表である（図表 2）。

図表 2 特定秘密保護法と国家公務員法の罰則の比較

	特定秘密保護法	国家公務員法
取扱業務者による漏えい（故意）	10 年以下の懲役（又は情状により 10 年以下の懲役及び 1 千万円以下の罰金）	1 年以下の懲役又は 50 万円以下の罰金 ※「職員」による「職務上知り得た秘密」の漏えいを処罰。「職務上知り得た秘密」は、職員が職務の執行に関連して知り得た秘密のすべてをいい、職員が担当して
業務知得者による漏えい（故意）	5 年以下の懲役（又は情状により 5 年以下の懲役及び 500 万円以下の罰金）	

³³ その後、同基準は、令和元年 12 月 10 日、令和 2 年 6 月 16 日及び令和 3 年 6 月 11 日に一部変更が行われている。

³⁴ 2 人以上の者が漏えい行為等の実行を具体的に計画して合意すること。

³⁵ 漏えい行為等を実行させる目的をもって、人に対して、当該行為を実行する決意を新たに生じさせるに足る懲慥行為をすること。

³⁶ 人に対して、当該行為を実行する決意を生ぜしめ又は既に生じている決意を助長させるような勢のある刺激を与えること。

		いる職務に直接関係する秘密、すなわち「職務上の秘密」のほか、担当職務外の秘密であっても職務の遂行に関連して知り得たものが含まれる。
未遂処罰の有無	有	無
取扱業務者による漏えい（過失）	2年以下の禁錮又は50万円以下の罰金	無
業務知得者による漏えい（過失）	1年以下の禁錮又は30万円以下の罰金	無
取得行為	10年以下の懲役（又は情状により10年以下の懲役及び1千万円以下の罰金） ※外国の利益若しくは自己の不正の利益を図り、又は我が国の安全若しくは国民の生命若しくは身体を害すべき用途に供する目的に限る。	無
未遂処罰の有無	有	無
共謀 独立教唆 煽動	5年以下の懲役 ※取扱業務者による漏えい及び取得行為の共謀、独立教唆、煽動。 3年以下の懲役 ※業務知得者による漏えいの共謀、独立教唆、煽動。	1年以下の懲役又は50万円以下の罰金 ※秘密の漏えいを企て、命じ、故意にこれを容認し、そのおかし又はそのほう助をした者を処罰。

（出所）内閣官房「特定秘密の保護に関する法律【逐条解説】」（平26.12.9）より作成

これによれば、適性評価を行わないと原則扱えない特定秘密に関する罰則は通常の状態公務員の守秘義務よりもかなり重いことが分かる。

なお、特定秘密保護法と同様に民間人についても処罰対象として情報保全を図る制度であるMDA秘密保護法（日米相互防衛援助等に伴う秘密保護法）についても特定秘密保護法とほぼ同様の罰則が設けられている³⁷。

³⁷ 詳しくは、内閣官房「特定秘密の保護に関する法律【逐条解説】」（平26.12）の別添3の資料を参照。

(4) 指定件数

令和3年末時点で指定されている特定秘密の件数は659件（令和2年末時点における件数613件に、対象期間中に指定された49件が加わった一方、対象期間中に指定の有効期間が満了した1件、対象期間中に指定が解除された2件が除かれたことによる）であった。

なお、各行政機関別の指定件数は下表のとおりである（図表3）。

図表3 各行政機関において指定されている特定秘密の件数

	(年末、件)							
	平成 26	平成 27	平成 28	平成 29	平成 30	令和 元	令和 2	令和 3
国家安全保障会議	1	2	3	4	5	6	7	8
内閣官房	49	57	66	73	81	87	94	102
内閣府	0	0	0	0	0	0	0	0
国家公安委員会	0	0	0	0	0	0	0	0
警察庁	18	24	29	34	38	43	41	45
金融庁	0	0	0	0	0	0	0	0
総務省	2	3	5	6	7	9	11	11
消防庁	0	0	0	0	0	0	0	0
法務省	1	1	1	1	1	1	1	1
出入国在留管理庁						1	1	1
公安調査庁	10	12	16	20	22	24	26	30
外務省	35	38	39	37	38	39	40	41
財務省	0	0	0	0	0	0	0	0
厚生労働省	0	0	0	0	0	0	0	0
経済産業省	4	4	4	4	4	4	4	4
資源エネルギー庁	0	0	0	0	0	0	0	0
海上保安庁	15	16	17	18	19	20	21	22
原子力規制委員会	0	0	0	0	0	0	0	0
防衛省	247	270	289	302	319	318	349	375
防衛装備庁		16	18	18	17	17	18	19
合計	382	443	487	517	551	569	613	659

(注1) 出入国在留管理庁は、平成31年4月に発足。

(注2) 防衛装備庁は、平成27年10月に発足。

(出所) 内閣官房「特定秘密の指定及びその解除並びに適性評価の実施の状況に関する報告（各年版）」より作成

(5) 適性評価の実施件数

令和3年中に適性評価を実施した機関(24機関)が同期間中に適性評価を実施した件数は、全体で27,602件³⁸(行政機関の職員等への実施件数が26,485件、適合事業者の従業者への実施件数が1,117件)であった(図表4)。

図表4 令和3年中の各行政機関の適性評価の実施件数

行政機関名	行政機関の職員等	適合事業者の従業者	計
内閣官房	370	252	622
内閣府	48	0	48
警察庁	975	0	975
(警察庁)	(217)	0	(217)
(都道府県警察)	(758)	0	(758)
金融庁	3	0	3
消費者庁	7	0	7
総務省	18	0	18
消防庁	11	0	11
法務省	7	0	7
出入国在留管理庁	15	0	15
公安調査庁	69	0	69
外務省	269	21	290
財務省	74	0	74
文部科学省	46	4	50
厚生労働省	1	0	1
農林水産省	5	0	5
水産庁	15	0	15
経済産業省	53	0	53
資源エネルギー庁	6	0	6
国土交通省	36	0	36
気象庁	8	0	8
海上保安庁	186	0	186
環境省	10	0	10
防衛省	23,987	389	24,376
防衛装備庁	266	451	717
合計	26,485	1,117	27,602

(出所) 内閣官房「特定秘密の指定及びその解除並びに適性評価の実施の状況に関する報告」(令4.6)より作成

³⁸ 令和元年中は22,987件、令和2年中は59,958件となっている。なお、令和2年中の実施件数が前年に比して大きく増加しているのは、主に行政機関の長が直近に実施した適性評価から5年を経過することにより、再度適性評価を実施したことによるものとされている。

適性評価を実施した 24 の行政機関のうち、対象期間中の実施件数が最も多かったのは、防衛省（24,376 件、全体の 83.3%）であった。そして、警察庁（975 件、全体の 3.5%）、防衛装備庁（717 件、全体の 2.6%）、内閣官房（622 件、全体の 2.3%）がそれに続く形となっている。なお、適合事業者への実施件数 1,117 件のうち、防衛装備庁、防衛省、内閣官房の 3 機関が占める割合は 97.8% となっており、同 3 機関に集中していることが分かる。

また、評価対象者の同意がない限り、行政機関は適性評価を実施することはできないとされているが、令和 3 年中に、適性評価の対象者が同意をしなかった件数は、全体で 3 件であり、その全てが防衛省であった。なお、適性評価の対象者が同意をしなかった件数とその内訳について、平成 27 年中以降の状況を取りまとめたものが下表になる（図表 5）³⁹。それによれば、平成 27 年中及び平成 30 年中には、適合事業者で適性評価に同意をしなかった件があった。

図表 5 適性評価の対象者が同意をしなかった件数とその内訳

年中	件数	内訳
平成 27	36 件	防衛省 28 件（職員 20 件、従業者 8 件）、内閣官房 7 件（職員 1 件、従業者 6 件）、外務省 1 件（職員）
平成 28	10 件	防衛省 7 件（職員）、外務省 2 件（職員）、防衛装備庁 1 件（職員）
平成 29	3 件	防衛省 1 件（職員）、外務省 1 件（職員）、資源エネルギー庁 1 件（職員）
平成 30	5 件	防衛省 2 件（職員）、内閣官房 2 件（従業者）、海上保安庁 1 件（職員）
令元	3 件	防衛省 2 件（職員）、内閣府 1 件（職員）
令 2	5 件	防衛省 4 件（職員）、国土交通省 1 件（職員）
令 3	3 件	防衛省 3 件（職員）

（注）括弧の中の職員は、行政機関の職員、従業者は適合事業者を指す。

（出所）内閣官房「特定秘密の指定及びその解除並びに適性評価の実施の状況に関する報告（各年版）」より作成

³⁹ 特定秘密保護法の施行は平成 26 年 12 月 10 日であり、平成 26 年中は適性評価を実施した件数自体が 0 件であり、従って、適性評価の実施に同意をしなかった件数も 0 件である。

さらに、特定秘密保護法では、評価対象者は、適性評価の結果その他当該対象者について実施された適性評価について、書面で、行政機関の長に対し、苦情の申出をすることができるものとされているが、令和3年中に申出があった苦情の件数は0件であった⁴⁰。

5. 米国のセキュリティ・クリアランス制度⁴¹

(1) 制度の概要

米国では、機密情報を取り扱うことができるのは、身上調査を経て行政機関の長から適性を認定された者、すなわちセキュリティ・クリアランスを保有する者に限定される。セキュリティ・クリアランスを付与されるのは、原則的に米国市民に限られる。また、セキュリティ・クリアランスを有する個人は、業務上、知る必要がある (need-to-know) 機密情報に限ってアクセスが認められ、あらゆる機密情報にアクセスできるわけではない。

大統領は、機密情報へのアクセスに関する大統領令及び規則を定める権限を有する。また、機密情報のレベルは、重要度が高い順に「Top Secret」、「Secret」、「Confidential」のいずれかが設定される⁴²。

また、機密情報を正当な権限を有しない者に開示した者に対して、戒告や休職処分、セキュリティ・クリアランスの失効等の制裁が規定されている。

さらに、機密情報を含む重要な情報の漏えいについては、様々な法律に罰則が規定されている。例えば、大統領令第13526号に基づく機密情報を含む国防秘密について、これを合法的に取り扱っていた者が、悪意で権限のない者に送信した場合等に、罰金又は10年以下の拘禁刑を科すこととされている⁴³。

なお、2019年10月1日時点で、セキュリティ・クリアランスの保有者は約

⁴⁰ 適性評価制度の創設以来、毎年0件が続いている。

⁴¹ 福田健志『米国のセキュリティ・クリアランス制度と日本における議論—研究者への適用をめぐって—』(国立国会図書館 調査及び立法考査局、令4.3)を参考にしている。

⁴² 米連邦捜査局(FBI)は令和4年8月8日、トランプ前大統領の邸宅を家宅捜索し、多数の機密文書を押収(「Top Secret」に指定される文書を含む)したとされる。なお、裁判所が公開した資料から、FBIが①スパイ活動法違反、②捜査妨害を目的とした文書の処分や隠蔽、③政府文書の違法な取扱い等の疑いでトランプ前大統領を捜査していることが分かったとされる(『日経新聞』(令4.8.14))。その後、米司法省は、同年8月26日、前述のFBIの捜索の根拠を説明した「宣誓供述書」を開示したとされる。なお、トランプ前大統領は、「宣誓供述書はひどく編集されている」「魔女狩りだ」などとSNSに相次いで投稿し、捜査を批判したとされる(『読売新聞』(令4.8.28))。

⁴³ 手塚悟慶慶應義塾大学教授によると米国では情報漏えいが発覚した者は「二度と政府の関わる仕事に就けない」というとされている(『日経新聞』(令2.8.28))。

424 万人であり、このうち、実際に機密情報にアクセスしている者は約 295 万人である。

(2) クリアランス（信頼性確認）の実施手順

連邦政府職員がクリアランスを取得する場合の実施手順は以下のとおりになる（図表 6）。

図表 6 クリアランスの実施手順

① 申請	<ul style="list-style-type: none"> 各行政機関は、職員や求職者が、業務上、機密情報にアクセスする必要があると判断した場合、Top Secret、Secret、Confidential のどのレベルの機密情報にアクセスする必要があるかに応じて当該職員等のアクセスレベルを決定する。 当該職員等は、申請書類を提出するとともに、身上調査を実施する行政機関が、各種個人情報を参照することに同意する必要がある。
② 身上調査	<ul style="list-style-type: none"> 申請を受けて、身上調査が実施される。 身上調査は、原則として国防総省の国防カウンターインテリジェンス・保全庁が一元的に実施している。 調査では、申請者本人との面談や、友人や同僚、家主、隣人等への照会等が実施される。
③ 認定	<ul style="list-style-type: none"> 身上調査の結果を受けて、各行政機関の長が、当該職員等のクリアランスを認定する。
④ 定期的な再調査と資格の失効	<ul style="list-style-type: none"> クリアランスの保有者は、定期的な再調査を受けてその資格を更新する必要がある。 定期的な再調査は、少なくとも Top Secret の場合は 5 年、Secret の場合は 10 年、Confidential の場合は 15 年に 1 回実施することとされてきたが、近年はこれをアクセスレベルに関わらず 5 年に 1 回実施する傾向にある。 また、今後は定期的な再調査に代わって「継続審査^(注)」が導入されることが予定されている。 クリアランスの資格は、個人が機密情報へアクセスする必要がなくなった場合に失効する。
⑤ 不服申立て	<ul style="list-style-type: none"> 不認定となった申請者には、その理由や決定の根拠に関する告知を受ける権利、不服申立てや当該行政機関の長によって設置される再審査委員会による再審査を請求する権利が認められている。

(注) 商用データベースや連邦政府のデータベースを自動的に随時チェックするシステム等を用いて、資格保有者の適性を継続的に確認することを「継続評価」といい、定期的な再評価を補完するものと位置付けられている。今後、新たなシステムの開発等により、継続評価の手法を用いた「継続審査」に移行することが予定されており、これは定期的な再調査に代わるものになるとされている。

(出所) 福田健志「米国のセキュリティ・クリアランス制度と日本における議論－研究者への適用をめぐって－」112～113 頁及び 117 頁

一方、連邦政府から業務を請け負う民間事業者や、連邦政府から資金の提供を受けて研究を行う研究者に対する機密情報の保全についても、身上調査の上、クリアランスを認定することとなっており、その実施手順は、連邦政府職員の場合とほぼ同じである。なお、クリアランスに係る費用は、連邦政府が負担している。

6. おわりに

セキュリティ・クリアランスを導入するに際しては、①審査主体をどうするのか（米国では政府（国防総省）が主体となっているが、オーストラリアでは政府機関が数十社の民間調査会社に委託しているとされる⁴⁴）、②機密情報の対象範囲をどうするのか（機微な技術の流出防止との観点が重要である一方で、研究成果の公開や自由な研究環境を制限する可能性もあり、両者の適度なバランスが求められる）、③適性審査の対象とする研究者や技術者の対象範囲をどうするのか⁴⁵、④情報を漏えいした場合の罰則をどうするのか、⑤適性評価事項の項目をどう設定するか、⑥適性評価の審査に要する期間はどの程度とするか、⑦資格が認められなかった場合に不服を申し立てる仕組みをどのように構築するか等が主な論点となろう。

特定秘密保護法における適性評価制度のこれまでの運用状況や海外先進諸国の制度の運用状況等を踏まえ、政府においては、セキュリティ・クリアランスの制度設計に関する作業を今後本格化していくものと思われるが、その際には、プライバシーの侵害への懸念を背景とした意見も依然として存在する⁴⁶点にも十分に配慮し、慎重な制度設計が求められる。その意味でも、セキュリティ・クリアランス制度の導入に向けた経済安全保障推進法の改正法案が提出され、同法案の国会審議が行われる際には、政府側からの丁寧で分かりやすい答弁によって、国民の理解が醸成されることが必要である。

今後を展望すると、半導体やAIを始めとして、国際的な共同研究の必要性はますます高まり、技術流出防止策としてのセキュリティ・クリアランスは必

⁴⁴ 『日本経済新聞』（令 2. 8. 28）

⁴⁵ 政府は、特定重要技術に関する官民協議会の参加者を対象に適性評価を行い、順次、適用を拡大していきたい考えである旨の報道もある（『産経新聞』（令 4. 6. 20））。

⁴⁶ 例えば、日本弁護士連合会は、「次の法制化では民間の研究者にセキュリティ・クリアランス制度（秘密取扱者適格性確認制度）を導入することが検討されており、特定秘密の保護に関する法律における適合事業者の適性評価制度を批判する立場からは、更に研究者の活動への制約が危惧される」旨の意見を示している（日本弁護士連合会「経済安全保障法について政府に対して、法の実施過程において説明を尽くし慎重な運用を求める会長談話」（令 4. 7. 25））。

須となる。このほか、セキュリティ・クリアランスの効果的かつ精緻な制度設計は、米国等が機密情報を共有する「ファイブ・アイズ」の枠組みに我が国が参画していくためにも欠かせないとも指摘され⁴⁷、もはや先送りは許されない。

(内線 75103)

⁴⁷ 例えば、経済安全保障法制に関する有識者会議委員でもある角南篤公益財団法人笹川平和財団理事長がそのような指摘を行っている（『読売新聞オンライン』（令 4. 3. 18））。