参議院常任委員会調査室・特別調査室

論題	セキュリティ・クリアランス制度導入の方向性と主な論点 ～技術流出の防止等による国力向上を目指した制度構築に向けて～
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	226 号
刊行日	2023-8-25
頁	1-20
URL	https://www.sangiin.go.jp/japanese/annai/chousa/keizai_prism/backnumber/r05pdf/202322601.pdf

セキュリティ・クリアランス制度導入の方向性と主な論点

～技術流出の防止等による国力向上を目指した制度構築に向けて～

内閣委員会調査室　柿沼　重志

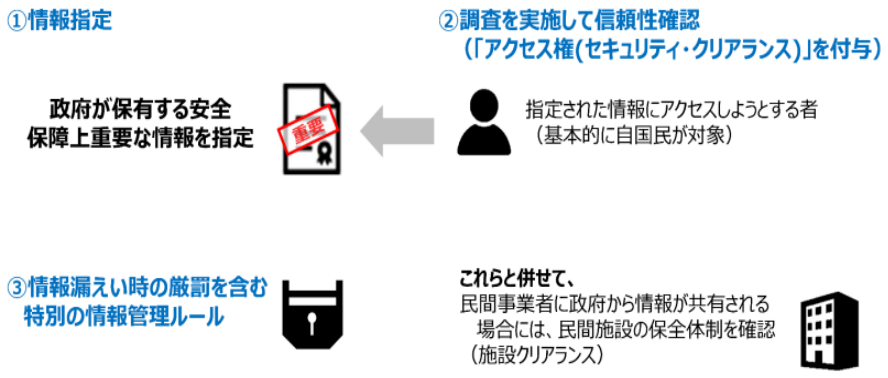
《要旨》

本稿では、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が令和５年６月６日に公表した「中間論点整理」や同有識者会議の議事要旨を基に、セキュリティ・クリアランス制度導入の方向性と主な論点について考察する。

１．はじめに[1]

セキュリティ・クリアランス制度とは、国家における情報保全措置の一環として、①政府が保有する安全保障上重要な情報を指定することを前提に、②当該情報にアクセスする必要がある者（政府職員及び必要に応じ民間の者）に対して政府による調査を実施し、当該者の信頼性を確認した上でアクセス権を付与する制度であり、③特別の情報管理ルールを定め、当該情報を漏洩した場合には罰則を科すことが通例であるとされる（図表１）。

図表１　セキュリティ・クリアランス制度の概要



（出所）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「中間論点整理」（令和５年６月６日）

[1] 本稿は、令和５年８月１日の脱稿時点までの情報に基づき執筆している。

セキュリティ・クリアランス制度は、「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」（令和４年法律第 43 号）（以下「経済安全保障推進法」という。）の法案審議の際に繰り返し取り上げられ、衆参の内閣委員会では、同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旨の附帯決議が付された。なお、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」（平成 25 年法律第 108 号）（以下「特定秘密保護法」という。）は平成 25 年 12 月 11 日に公布、平成 26 年 12 月 10 日に施行されている[2]。

さらに、「国家安全保障戦略」（令和４年 12 月 16 日国家安全保障会議決定、閣議決定）では、「主要国の情報保全の在り方や産業界等のニーズも踏まえ、セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた検討を進める。」とされた。

その後、令和５年２月 14 日に開催された第４回経済安全保障推進会議[3]において、岸田内閣総理大臣から、経済安全保障分野におけるセキュリティ・クリアランス制度の法整備等に向け、制度のニーズや論点等を専門的な見地から検討する有識者会議を立ち上げ、今後１年程度をめどに、可能な限り速やかに検討作業を進めるよう指示があった。これを受け、同年２月 21 日には、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（以下「有識者会議」という。）が設置され、計６回の会議を経て、６月６日に「中間論点整理」を公表している[4]。

本稿では、まず、セキュリティ・クリアランス制度について概観した上で、「中間論点整理」や有識者会議の議事要旨を基に、セキュリティ・クリアランス制度の必要性や同制度の導入の方向性と課題について考察することとしたい。

２．セキュリティ・クリアランス制度の必要性

セキュリティ・クリアランス制度について「中間論点整理」では「国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として

---

[2] 特定秘密保護法における適性評価制度について、拙稿「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～」『経済のプリズム』第 217 号（令和４年 10 月）を参照。

[3] 内閣総理大臣を議長とする会議で、令和３年 11 月 19 日に第１回の会議が開催されている。

[4] その後、６月 16 日に閣議決定された「経済財政運営と改革の基本方針 2023」では、「主要国の情報保全の在り方や産業界等のニーズも踏まえ、セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた法制度等の検討を更に深め、速やかに結論を得る。」とされた。

指定された情報（以下「ＣＩ」(Classified Information）という。）にアクセスする必要がある者（政府職員及び必要に応じ民間事業者等の従業者）に対して政府による調査[5]を実施し、当該者の信頼性を確認した上でアクセスを認める制度である（ただし、実際にアクセスするには、当該情報を知る必要性（いわゆるNeed-to-Know）が認められることが前提となる。また、民間事業者等に政府から当該情報が共有される場合には、民間事業者等の保全体制（施設等）の確認（施設クリアランス）等も併せて実施される。)」と詳細な定義付けがされている。

以下では、同制度について、国としての必要性と企業からのニーズについて見ていく。

（１）国としての必要性

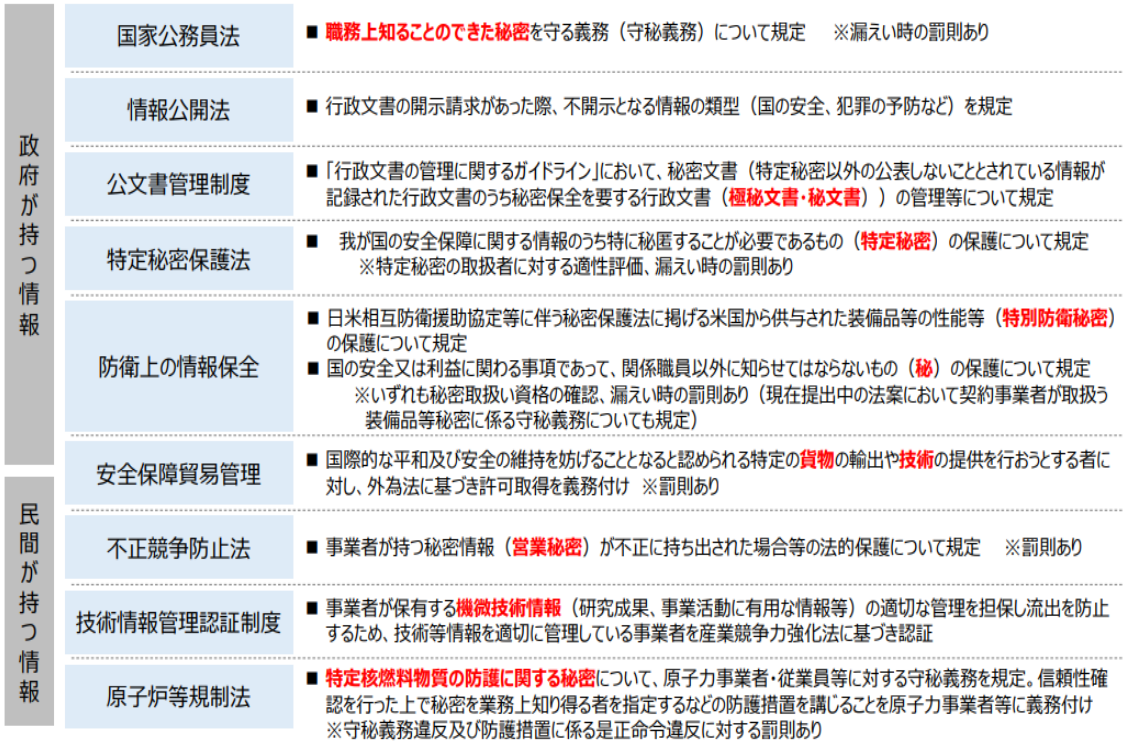
「中間論点整理」では、まず、「安全保障の概念が、防衛や外交という伝統的な領域から経済・技術の分野に大きく拡大し、軍事技術・非軍事技術の境目も曖昧となっている中、国家安全保障のための情報に関する能力の強化は、一層重要になっており、経済安全保障分野においても、厳しい安全保障環境を踏まえた情報漏洩のリスクに万全を期すべく、セキュリティ・クリアランス制度を含む我が国の情報保全の更なる強化を図る必要がある。」と総論的にその必要性が示されている。

次に、「我が国の既存の情報保全制度のうち、例えば、特定秘密保護法の施行により、我が国の情報保全制度の信頼性が高まり、同盟国・同志国との情報共有が一層円滑になった一方、主要国と異なり、同法では政府が特定秘密として指定できる情報の範囲が、防衛、外交、特定有害活動の防止、テロリズムの防止の４分野に関する一定の要件を満たす事項に限られており、経済安全保障に関する情報が必ずしも保全の対象となっていない。こうした特定秘密保護法等に基づく情報保全制度の下で、指定された情報にアクセスできる民間事業者等はいわゆる防衛産業に集中している。このため、経済安全保障上重要な情報に関して、特に、経済関係省庁や防衛産業を超えた民間において、セキュリティ・クリアランス制度を含む情報保全の一層の強化が必要となっている。」旨が記され、特定秘密保護法で指定される４分野に限定せず、その他の経済安全保障に

[5] 令和５年４月７日に開催された有識者会議（第４回）では、企業から「国の政策として行うのであれば、明確な調査基準を設け、国の責任において調査を実施してもらいたい。これを企業にやれといわれても実際にできない。」との意見が出されたとされている（議事要旨８頁)。

関する情報に関しても情報保全強化を図る必要性が示されている[6]。なお、特定秘密保護法を始めとした我が国における情報保全の枠組みは以下のとおりとなっている（図表２、なお同図表中に出てくる法律名のうち正式名称ではないものは注で正式名称を表記、以下、本稿中では略称を使用する）。

図表２　我が国における情報保全の枠組み



（注１）情報公開法の正式名称は「行政機関の保有する情報の公開に関する法律」
（注２）外為法の正式名称は「外国為替及び外国貿易法」
（注３）営業秘密とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報であって、公然と知られていないものを指す。
（注４）原子炉等規制法の正式名称は「核原料物質、核燃料物質及び原子炉の規制に関する法律」
（出所）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１回）（令和５年２月 22 日）資料３

経済安全保障に関する情報で情報保全を図る必要性がある具体的な例につい

[6] 高市経済安全保障担当大臣は、令和５年２月 14 日の記者会見で「特定秘密保護法の場合、国防関係、外交、スパイ活動、テロリズムの４分野に限定されているが、これから作り上げていこうとしているものは、いわゆる『産業版』であり、日本企業が海外の政府調達や、また海外の企業との取引、また共同研究から排除されない環境を作っていくためのものである」旨を述べている（https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230214kaiken.html）。

て、令和５年２月 22 日に開催された有識者会議（第１回）では、有識者会議委員から「経済安全保障の観点からセキュリティ・クリアランス制度をもって保護すべき重要な情報・モノとしては、政府が定める 20 の重要技術分野[7]に関わる情報や技術ということになるかと思う。セキュリティ・クリアランスの基本は戦略的不可欠性[8]を高めるための措置であると同時に、他国に流出することで、我が国の安全保障を脅かすことになる技術が対象となるべきだと考える。」との意見が出されている（議事要旨 11 頁）。

さらに、米国を始めとした海外主要国については、「クリアランス保有者は、米国では民間も含め 400 万人以上、その他の主要国でも数十万人以上いるとされ、官民のクリアランス保有者の比率についても、米国では官対民で７割対３割程度となっているなど、制度として定着している[9]。」とされている[10]。一方、我が国で特定秘密の取扱いの業務を行うことができる者の人数は約 13.2 万人、保有者の比率は、官が約 97％、民が３％となっている[11]。

さらに、「こうした形での情報保全の強化は、安全保障の経済・技術分野への広がりを踏まえれば、同盟国・同志国との間で更に必要となるこれらの分野も含んだ国際的な枠組み[12]を整備していくこととあいまって、既に情報保全制度

---

[7] ①バイオ技術、②医療・公衆衛生技術（ゲノム学含む）、③人工知能・機械学習技術、④先端コンピューティング技術、⑤マイクロプロセッサ・半導体技術、⑥データ科学・分析・蓄積・運用技術、⑦先端エンジニアリング・製造技術、⑧ロボット工学、⑨量子情報科学、⑩先端監視・測位・センサー技術、⑪脳コンピュータ・インターフェース技術、⑫先端エネルギー・蓄エネルギー技術、⑬高度情報通信・ネットワーク技術、⑭サイバーセキュリティ技術、⑮宇宙関連技術、⑯海洋関連技術、⑰輸送技術、⑱極超音速、⑲化学・生物・放射性物質及び核、⑳先端材料科学

[8] 戦略的不可欠性とは、もともとはＰＨＰ Geo-Technology 戦略研究会が令和２年４月に公表した報告書（「ハイテク覇権競争時代の日本の針路」）で提言された考え方であり、他国が決定的に重要と考える領域において代替が難しい地位を獲得することを指す（村山裕三「日本の経済安全保障政策への展望」村山裕三編著『米中の経済安全保障戦略』（芙蓉書房出版、令和３年））。

[9] 各国政府資料を基に有識者会議事務局にて調べた情報（令和５年５月時点で判明しているもの）。

[10] 令和５年３月 27 日に開催された有識者会議（第３回）では、企業から「Need to know の原則の下で、プロジェクトに必要な単位の人間で情報共有できるような仕組みとしてほしい。」との意見のほか、「海外と比べると、日本の方が、事業規模に比して、特定秘密保護法等のセキュリティ・クリアランス保有者が少ない印象があり、お互いの技術を交流させて様々な提案をするということになると、日本のセキュリティ・クリアランス保有者を増やしていく方向になると考える。」との見通しが示されたとされる（議事要旨４頁）。

[11] 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（令和５年６月版）。

[12] 既存の国際的な枠組みとしては、我が国は、米、仏、豪、英、印、伊、韓、独、NATO の９か国・機関との間でそれぞれ情報保護協定（協定に従って相互に提供される情報を受領する締約国の国内法令の範囲内で適切に保護するための手続等について定めるもの）を締結済み（米、印、韓との協定は、軍事情報のみが対象）。

が経済・技術の分野においても定着し活用されている国々との間での協力を一層進めることを可能とし、ひいては、国家安全保障戦略が示す我が国の安全保障に関わる総合的な国力[13]の向上にも資するものである[14]。」とされている。

（２）企業からのニーズ

経済界からは、既に経済安全保障推進法案の審議前から、セキュリティ・クリアランス制度の導入に向けて前向きな意見が表明されていた。一例として、令和４年２月 16 日、経済同友会からは、「我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。」旨の意見が示されている[15]。

こうした点も踏まえつつ、企業からのニーズについて、「中間論点整理」では、「スタートアップも含めた様々な企業から、同盟国等の政府調達等において、国際的に通用するセキュリティ・クリアランスの制度や国際的な枠組みがあれば変わったのではないかという観点から、主に以下のような声が聞かれた。」として、セキュリティ・クリアランス制度が整備されていないことによるビジネスチャンスの逸失等のデメリットのほか、衛星・ＡＩ・量子、Beyond５Ｇといった次世代技術の国際共同開発に関する機会を我が国企業が獲得するといった意味で、将来を見据えた同制度のニーズが示されている（図表３）[16]。

---

[13] なお、「国家安全保障戦略」（令和４年 12 月 16 日国家安全保障会議決定、閣議決定）では、総合的な国力の主な要素として、①外交力、②防衛力、③経済力、④技術力、⑤情報力の５つを挙げている。

[14] 令和５年６月 11 日に一般財団法人交詢社が主催したフォーラムにおいて、高市経済安全保障担当大臣は、「経済安全保障推進法を見直し、セキュリティ・クリアランス制度を創設することで、日本のビジネスチャンスを逃さず、経済のパイを大きくすることが全世代の安心感につながる。国力をしっかりと強くする。そして、持続的な成長への道を開く」旨を述べたとされる（『産経新聞』（令 5.7.24））。

[15] 「経済安全保障法制に関する意見」（令和４年２月 16 日、経済同友会）

[16] 高市経済安全保障担当大臣は、令和５年６月６日の記者会見で「海外政府の調達に入ろうと思ったときに、日本の民間のビジネスマンが、デュアル・ユース技術の分野において、なかなか入札の説明会にも呼んでもらえないことや、民間企業同士の研究開発でも、機微な情報が得られずに契約に至らなかったこと、研究者の方が学会やカンファレンスに出る時に、クリアランス・ホルダー・オンリーということで重要な先端技術に触れる機会がないことも伺い、このまま放置しておくと、日本企業がみすみす海外においてビジネスチャンスを失ってしまうとの危機感が非常に強くあり、できるだけ速やかに法制度として整備をしたい。」旨を述べている（https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230606kaiken.html）。

図表３　セキュリティ・クリアランス等に対する企業からの主な声

○ある海外企業から協力依頼があったが、機微に触れるということで相手から十分な情報が得られなかった。政府間の枠組みの下で、お互いにセキュリティ・クリアランスを保有している者同士で共同開発などができれば、もう少し踏み込んだものになったのではないか。
○自衛隊の装備品とは関係ない国際共同開発において、セキュリティ・クリアランス保有者がいなかったために、秘密指定されていないが管理が必要な情報（以下「ＣＵＩ」（Controlled Unclassified Information）という。）の開示を受けるまでに長い時間を要したにもかかわらず契約に至らなかったことや、最終的に開示を受けることができたが周辺情報だけに留まったこともあった。
○防衛と民生が一緒になったデュアル・ユース技術に関する会議に参加する際、クリアランス・ホルダー・オンリーであるセミナー・コミュニティがあり、これらに参加できず最新のデュアル・ユース技術に触れることができない。
○宇宙分野の海外政府からの入札に際し、セキュリティ・クリアランスを保有していることが説明会の参加要件になっていたり、商業利用分野であってもＣＩが含まれているので詳細が分からない等の不利な状況が生じている。
○様々なサイバーセキュリティ・インシデントが起きている中で、政府側や諸外国が保有している様々な情報が共有されれば、個々の企業のセキュリティ・レベルの向上、ひいては我が国全体のセキュリティ・レベルの向上にもつながる。
○セキュリティ・クリアランス制度の導入によって、将来的に、例えば衛星・ＡＩ・量子、Beyond５Ｇといった次世代技術の国際共同開発に関する機会が拡充してくるのではないか。

（出所）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「中間論点整理」（令和５年６月６日）より筆者作成

こうした企業からの声に関して、「中間論点整理」では「経済・技術の分野にも対応した制度の下でセキュリティ・クリアランスを保有していれば、その結果として、その他の場面でも、いわば『信頼できる証』として対外的に通用することになるのではないかということを示唆している」とされている。

そして、「このような制度においては、機微な情報を扱う者について信頼性の確認を行う必要があることはもちろんのこと、信頼性の確認を含む情報保全全般が米国を始めとする主要国との間でも認められるものでなくてはならないと考えられる[17]。」とされている。

[17] この点について、衆議院内閣委員会に参考人として出席した佐橋亮東京大学東洋文化研究所准教授は、「セキュリティ・クリアランスを導入するのであれば、簡易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る」旨の意見を述べている（第 208 回国会衆議院内閣委員会議録第 14 号９頁（令 4.3.31））。

３．新たな制度の方向性

「中間論点整理」では、新たな制度の方向性として、①ＣＩを念頭に置いた制度、②主要国との間で通用する実効性のある制度、必要となる国際的な枠組み、③政府横断的・分野横断的な制度の検討の３点を挙げている（図表４）。

図表４　新たな制度の方向性

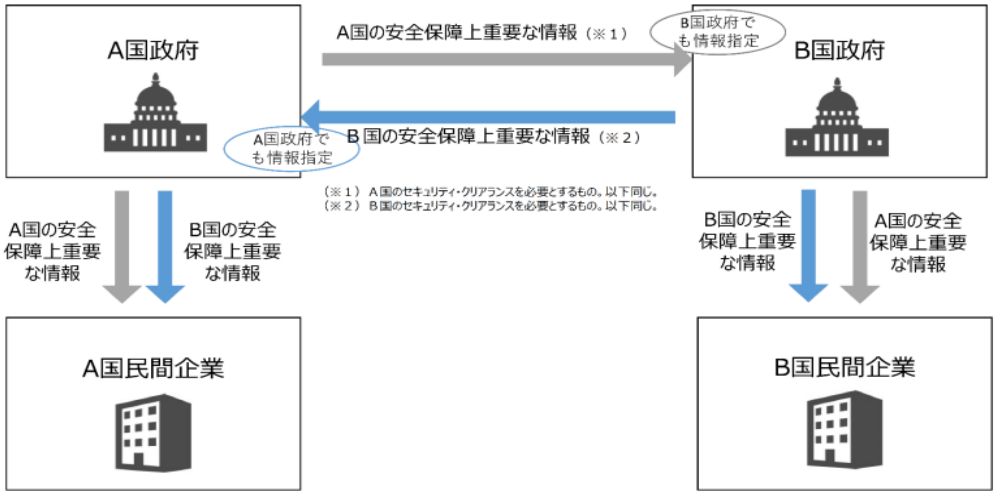
①ＣＩを念頭に置いた制度 ・セキュリティ・クリアランス制度とは、あくまで国として守らなければならないＣＩにアクセスする必要がある者（政府職員及び必要に応じ民間事業者等の従業者）に対して政府が調査を行い、当該者の信頼性を確認した上で、アクセスを認めるというものであることから、経済安全保障分野を中心にセキュリティ・クリアランス制度の在り方を検討していく上でも、あくまで、情報保全の主たる対象はＣＩであることを前提に検討していくことが必要である。 ・政府から民間事業者等にＣＩが共有される場合には、当該民間事業者等の従業者及び民間事業者等の保全体制（施設等）について、ＣＩを取り扱うに足る旨の信頼性の確認がなされる必要がある。
②主要国との間で通用する実効性のある制度、必要となる国際的な枠組み ・今回の検討に当たっては、新たに設けられる制度が「相手国から信頼されるに足る実効性のある制度」とならなければ意味がなく、そこを目指すということが重要である。 ・ここでいう相手国とは、特に米国や英国を始めとする欧州等の主要な同志国を指すが、これらの国の情報保全制度は米国と比較的整合性のある実効的な制度となっており、こうした同盟国・同志国の制度も踏まえ、検討を進めていくことが必要である。 ・制度整備を踏まえ、同盟国・同志国との間で新たに必要となる国際的な枠組みについても検討を進めていくべきである。
③政府横断的・分野横断的な制度の検討 ・我が国では既に、特定秘密保護法等を始めとした情報保全制度があり、防衛分野を中心に、政府及び民間事業者等の間では情報保全体制が構築されている実態があることから、今回の検討が既存の諸制度と切り離されたものとなると、政府内だけではなく、民間事業者等にとっての運用コストや管理コストが増すことにもつながる。このため、経済等の新たな分野を含めた政府横断的・分野横断的な視点を持ち、従来の防衛分野における情報保全制度を始め既存の諸制度等との整合性にも配慮しつつ、あるべき制度を検討することが必要である。 ・また、情報保全制度だけではなく、情報公開法や公文書管理法といった他法令とも関係することが想定されるため、これらとの整合性についても今後検討が必要である。

（出所）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「中間論点整理」（令和５年６月６日）より筆者作成

ＣＩを念頭に置いた制度、主要国との間で通用する実効性のある制度という

のは、図表４の説明のとおりである。次に、必要となる国際的な枠組みが意味するところであるが、これを理解するためには、国家間の安全保障上重要な情報のやり取りのイメージ（図表５）を想起する必要がある。

図表５　国家間の安全保障上重要な情報のやり取りのイメージ



（出所）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「中間論点整理」（令和５年６月６日）

より具体的には、第１に政府が保有する安全保障上重要な情報へのアクセス権であるセキュリティ・クリアランスは、基本的には自国民を対象に付与されるという点、第２に外国政府の安全保障上重要な情報にアクセスするためには、自国政府を通じて行う必要があるという点を踏まえれば、同盟国・同志国との間で新たに必要となる国際的な枠組みについても検討を進めていくべきとの方向性が導出されるということである[18]。これに関連し、令和５年３月 27 日に開催された有識者会議（第３回）では、委員と企業との意見交換の場で、「ファイブ・アイズ[19]に属する国家間において、どのような情報が共有されているかは

[18] 令和５年３月 27 日に開催された有識者会議（第３回）では、企業からは「同盟国・同志国との連携がより重要となってくる中で、各国政府間での取組も進んできている。そうした中で、企業の立場からも、外国政府が保有している情報を共有・開示してもらうことで、様々な役割を果たしていけるのではないかと考えている」旨の意見のほか、「期待として、外国の政府との間での合意の下ではあるが、企業間での相互の情報共有が円滑になることがある。実際、外国政府が保有する機微な情報についてのアクセスが得られず、日本から効果的な提案ができなかったことや、外国の企業が保有している機微な技術が得られないために、日本側で効果的な活用ができない等の課題があった」旨の意見が出されたとされている（議事要旨２～３頁）。

[19] 米国、英国、カナダ、オーストラリア、ニュージーランドの５か国による機密情報共有の枠

明らかではないが、サイバーセキュリティに関する情報は広く共有されていると思われる。ＩＳＡ（Industrial Security Agreement：産業保全協定）が、二国間で相互にセキュリティ・クリアランスを認め、機密指定された情報を共有するための協定となる」旨の見解が示されている（議事要旨３頁）。

さらに、政府横断的・分野横断的な制度の検討とは、「今回の検討が既存の諸制度と切り離されたものとなると、政府内だけではなく、民間事業者等にとっての運用コストや管理コストが増すことにもつながる。このため、経済等の新たな分野を含めた政府横断的・分野横断的な視点を持ち、従来の防衛分野における情報保全制度を始め既存の諸制度[20]等との整合性[21]にも配慮しつつ、あるべき制度を検討することが必要である。」ということである。

４．具体的な方向性

（１）情報指定の範囲

「中間論点整理」では、まず、「経済安全保障上重要な情報を指定していくに当たっては、我が国として真に守るべき政府が保有する情報に限定し、そこに厳重な鍵をかけるというのが基本的な考え方である。同時に、アクセスを認められている者の間では、Need-to-Know の原則の下でスムーズな情報交換ができるようにするべきである。」とされている。

その上で、「特定秘密保護法においては、政府が特定秘密として指定できる情報の範囲は、防衛、外交、特定有害活動の防止、テロリズムの防止の４分野に関する一定の要件を満たす事項に限られているが、例えば、経済制裁に関する分析関連情報や経済安全保障上の規制制度における審査関連の情報、サイバー分野における脅威情報や防衛策に係る情報、宇宙・サイバー分野等での政府レベルの国際共同開発にもつながり得る重要技術情報といった情報などの中には、政府として、上記４分野と同様又はそれに準ずるものとして厳格に管理すべき情報もあると考えられるところ、経済関係省庁等も含めて政府内で議論を深め、上記４分野との整理も含め情報指定の範囲についての検討を深めるべきである」とされている。ここでは、政府が保有する安全保障上重要な情報として指定さ

組みのこと。

[20] 前掲の図表２を参照。

[21] 令和５年２月 22 日に開催された有識者会議（第１回）では、自由討議の中で「今後の検討に当たっては、今我が国にある制度との連続性も問題になってくるわけで、特定秘密保護法や不正競争防止法との関係をどう整理するのかも大きな論点だと考える。」との意見が出されたとされている（議事要旨５頁）。

れた情報であるＣＩに該当する情報が含まれる例として、経済制裁に関する分析関連情報や経済安全保障上の規制制度における審査関連の情報、サイバー分野における脅威情報や防衛策に係る情報、宇宙・サイバー分野等での政府レベルの国際共同開発にもつながり得る重要技術情報が挙げられている。なお、米国におけるクリアランス対象情報の範囲･分野は以下のとおりである(図表６)。

図表６　クリアランス対象情報の範囲・分野（米国）

①軍事計画・兵器システム又は軍の運用
②外国政府情報
③インテリジェンス活動・情報源・方法又は暗号
④機密情報源を含む連邦政府の外交関係又は対外活動
⑤国家安全保障に関連する科学的・技術的・経済的事項
⑥核物質又は核施設の防護策のための政府プログラム
⑦国家安全保障に関連するシステム・設備・インフラ・プロジェクト・計画・防護サービスの脆弱性又は能力
⑧大量破壊兵器の開発等

（出所）経済安全保障分野におけるセキュリティ･クリアランス制度等に関する有識者会議「中間論点整理」（令和５年６月６日）より筆者作成

そして、「このように厳格に管理すべき情報については、米国等では、ＣＩを漏えいした場合の被害の深刻さ等に応じて、トップ･シークレット(Top Secret)、シークレット（Secret)、コンフィデンシャル（Confidential）等の複数の階層に分けて、機微度に応じた複層的な管理をするのが一般的である点にも留意が必要である。」とされている。なお、米国やドイツ、カナダでは３つの階層、英国やフランスは２つの階層に区分して管理されているとされている（米国の区分は図表７)。

図表７　クリアランス対象情報の区分（米国）

トップ・シークレット（Top Secret） 不当な開示が国家安全保障に著しく深刻な損害を与えると合理的に予想し得るもの
シークレット（Secret） 不当な開示が国家安全保障に重大な損害を与えると合理的に予想し得るもの
コンフィデンシャル（Confidential） 不当な開示が国家安全保障に損害を与えると合理的に予想し得るもの

（出所）経済安全保障分野におけるセキュリティ･クリアランス制度等に関する有識者会議「中間論点整理」（令和５年６月６日）より筆者作成

また、「我が国の特定秘密保護法では、特定秘密という単一の層しか規定されていないが、諸外国にも通用する制度を目指していく観点からは、情報指定の範囲を経済分野等も対象としていくとともに、単層構造から複層構造になるようにしていくことも検討すべきである。その際、特定秘密は、我が国が諸外国と締結している情報保護協定上では、トップ・シークレットとシークレットの２階層に対応すると整理されており、それらの下の階層であるコンフィデンシャルに相当する情報の取扱いについても検討する必要がある[22]。」とされ、機微度に応じた複層的な管理を行う必要性が示された。

さらに、「上記の検討に当たっては、新たな技術開発の進展など経済安全保障分野における変化の速さ等も踏まえて必要な情報を柔軟に指定できるような制度設計が望ましいほか、政府以外の様々な関係者の意見も踏まえつつ、情報の指定・解除に当たっては機動的に対応できるようにしていくことの検討も必要である[23]。」とされ、新たな技術開発の進展などを踏まえて必要な情報を柔軟に指定できるような制度設計及び機動的な情報の指定・解除の必要性が示された。

（２）信頼性の確認（評価）とそのための調査

「中間論点整理」では、まず、「政府による調査とその調査結果に基づく信頼性の確認（評価）については、政府の重要な情報にアクセスし得る限られた者を特定する重要なプロセスである」とされている。

また、「特定秘密保護法の下での個人の適性評価とそのための調査については、関係行政機関がそれぞれ実施することになっており、政府統一基準の下で運用されているところ、政府内の人事異動によって、改めて適性評価とそれに伴う調査を実施することとしている点等につき、更に運用の実態を踏まえつつ、情報保全の効果を棄損しない範囲で効率性を追求するべく検討を深める必要がある。」とされているほか、「企業からは、現行の枠組みの中で、政府と複数の契

---

[22] 令和５年２月 22 日に開催された有識者会議（第１回）では、自由討議の際に「情報指定の範囲を特定秘密保護法の４分野に加えて経済安全保障という部分にどう広げていくかというのは最大の課題、焦点である。特定秘密保護法の罰則は最大 10 年と重い罰則であることから情報指定が抑制的になっているが、経済安全保障の世界になった場合に、機密性の程度に応じた区分を考えるべきである。」旨の意見が表明されている（議事要旨９頁）。

[23] 令和５年３月 14 日に開催された有識者会議（第２回）では、委員と企業との意見交換の際に、「ある機関が情報をＣＩに指定したり、もしくはＵＩ（Unclassified Information）に指定すれば、以降は一切変更しないというのではなく、民間の意見や学術的な判断を経た上で、状況に応じ、機動的にＵＩからＣＩに変更したり、反対にＣＩからＵＩに変えるのがよいということか」との委員からの質問に対して、企業からは「そのとおり」との回答がされている（議事要旨 11 頁）。

約をしている場合に、それぞれを所管する行政機関等から調査を別々に受けなければならないといった声が聞かれている点にも留意が必要である。」とされている。

そして、「米国等主要国の例も参考に、最終的な信頼性の確認は、その情報保全に責任を持つ行政機関が行うことが想定されるが、例えば、調査については、既存の諸制度との整合性や防衛省・防衛産業等の運用実態に留意しつつ、その機能を一元的に集約する可能性も含め、調査結果につき一定のポータビリティ性（調査結果が一度得られれば、一定の有効期間の間、当該調査結果が組織や部署を超えて有効であること。例えば、政府職員が政府内の異動や政府から民間事業者等への異動を経ても結果が有効、あるいは、民間事業者等において、他の所管行政機関や契約にも当該調査結果が有効であること等が含まれ得る。）が確保されるよう、また、その適正な水準が維持されるよう、政府全体で統一的な対応を行っていくことが望ましい。また、こうした検討に当たっては、政府における限られた資源を効率的・効果的に活用する観点も踏まえることが必要である」とされている。

（３）産業保全（民間事業者等に対する情報保全）

「中間論点整理」では、まず「経済安全保障施策を進める中で、政府が保有する経済安全保障上の重要な情報を民間事業者等に共有していく場合も多くなると考えられる」とされた上で、「特定秘密保護法等を始めとした情報保全制度の下では、民間事業者等の従業者に対する調査や民間事業者等の保全体制（施設等）の確認が規定されているが、防衛産業にとどまらず、政府からＣＩの共有を受ける意思を示した民間事業者等及びその従業者であって、ＣＩへのアクセスを真に必要とするものについて、同様の厳格な対応を適用していくことが必要になると考えられる。」とされている。

民間事業者等に対する情報保全について、「例えば、米国においては、国家産業保全計画（NISP：National Industrial Security Program[24]）及びその運用マニュアル(NISPOM:National Industrial Security Program Operating Manual[25])において、民間企業等の非政府組織が遵守すべき事項が包括的に規定されてお

[24] 大統領令により設立された、米国政府の契約相手方に対して秘密情報の保護を義務付ける制度。
[25] 大統領令に基づき、米国政府の契約相手方に対して秘密情報の保護を義務付けるための細部事項を定めた文書。

り、その中には物的保全に関する規定や、民間企業等の非政府組織のガバナンスにおける『外国による所有、管理又は影響（FOCI：Foreign Ownership, Control or Influence[26]）』を管理する規定のほか、サイバーセキュリティに関する規定等もあることから、こうした制度も参考にしながら検討を深めることが必要である。」とされている。

（４）プライバシー等との関係

「中間論点整理」では、まず「重要情報を取り扱う業務に従事する従業者については、信頼性の確認とそのための調査が必要となる。」とされている。そして、「当該調査は、本人の意思に反して行われるものではなく、ＣＩへのアクセスを必要とするためセキュリティ・クリアランスを真に必要とする者の任意の了解の下で行われるものである」との基本的な考えが明示されている。

こうした基本的な考えを踏まえつつ、「現行の制度においても、特定秘密等に関わる政府職員や民間事業者等の従業者については、本人の同意を得るに当たって丁寧な手順[27]を踏んだ上で、一定の調査が実施されているが、経済安全保障上の重要な情報等に係るセキュリティ・クリアランス制度の検討に当たっても、同様に丁寧な手順を踏んだ上で本人の同意を得て調査を行うことが大前提である。その際、信頼性の確認のために収集された情報の管理が適切になされることは必須である。」とされている。

また、制度の検討に当たっての留意点としては、「信頼性の確認を受ける対象者が広がり得ることや、企業においては一般に雇用主からの求めによって信頼

---

[26] 令和５年４月７日に開催された有識者会議（第４回）では、委員から「FOCI については、まだ我が国で十分な理解がされていないと思われる。米国における同制度は、機密指定された情報を政府と共有している企業等が、外国関係者（foreign interests）による株式の保有などにより支配されていないかどうかを事前に審査するものである。これをチェックしないと、外国関係者による機密情報へのアクセスを排除することができない恐れが生じる。」との発言があったとされる（議事要旨 13 頁）。

[27] 令和５年４月７日に開催された有識者会議（第４回）では、政府側の説明として、「特定秘密保護法においては、評価対象者となった方からの同意を得て、運用基準に定められている質問票に記入していただくという手続が必要になる。この質問票には、ご本人のみならず家族や同居人の方に国籍や、帰化歴があるかといった詳細な情報を記入して頂く必要があるが、非常に時間と手間を要するものである。」とされている（議事要旨 12～13 頁）。なお、特定秘密保護法第 12 条第３項は、適性評価の実施に当たり、あらかじめ評価対象者に対し、前項各号に掲げる事項（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）について調査を行う旨等を告知した上でその同意を得ることを規定している。

性の確認を受けることを念頭に置きつつ、信頼性の確認のための調査とプライバシーの関係[28]や従業者の処遇への影響の考慮を含めた労働法令との関係[29]を十分踏まえ、適切な形で整理を行うことが必要である。」とされている。

とりわけプライバシーの問題については、経済安全保障推進法の法案審議の際にも議論が行われ、小林経済安全保障担当大臣（当時）からは、「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、クリアランスが与え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。」旨の答弁があった[30]。

（５）情報保全を適切に実施するための官民の体制整備

「中間論点整理」では、まず「新たな制度を実効的なものとするためには、官民双方において、主要国の実態や動向も踏まえながら、適切な体制や設備を整備する必要がある」とされている。

そして、政府においては、「情報保全を適切に実施するための必要な体制整備の在り方を検討する必要がある。また、実際の保全措置を講ずるに当たっては、適切な情報保全の観点から専用の区画や施設を設ける必要がある。」とされている。その一方で、民間事業者等においても、「同様の区画や施設を設ける必要が

---

[28] この点について、令和５年４月７日に開催された有識者会議（第４回）では、企業から「セキュリティ・クリアランスは背景調査を伴うものなので、人権問題と常に裏腹である。背景調査を求める場合には、これを民間の裁量に任せるのではなく、政府の責任において、明確な制度を法制度上担保してほしい」旨の意見が出されたとされる（議事要旨７頁）。

[29] 例えば、労働基準法第３条では、「使用者は、労働者の国籍、信条又は社会的身分を理由として、賃金、労働時間その他の労働条件について、差別的取扱をしてはならない。」と規定されており、こうした労働法制上の要請との整合性を図りながら、情報保全のルールを構築していくことが求められる。

[30] 第 208 回国会衆議院内閣委員会議録第 13 号 20 頁（令 4.3.30）

あり、民間事業者等にとっては少なからぬ負担となる。こうした民間事業者等における保全の取組に対する支援の在り方について、合理的な範囲内で検討していく必要がある[31]。」とされている。

５．その他

（１）ＣＩ以外の重要な情報の取扱い

「中間論点整理」では、セキュリティ・クリアランス制度の在り方を検討していく上では、主たる対象はＣＩであることが前提であるとしつつも、「ＣＩ以外の重要な情報にも何らかの形で情報保全措置を講ずることが必要ではないかと考えられる。例えば、情報の機微度はＣＩに指定するほどではないものの厳格に管理した方がよいと考えられる政府保有情報や、民間事業者等が保有している情報であって国として保全が必要と考えられる情報などが挙げられる。」とされている。これは、①政府が保有するＣＩレベル未満の要保護情報及び②民間事業者等が保有している情報であって国として保全が必要と考えられる情報の双方の取扱いについての問題提起であると思われる。

これらの情報の取扱いについては、「米国等の主要国においても取組に差があるが、情報の重要性等を考慮すれば、必要に応じ、信頼性の確認のための調査も含め、ＣＩに対するものほど厳格ではないが、一定の保全措置を講ずる必要性についても検討を進める必要があると考えられる。」とされている。また、「特に、民間事業者等が保有している情報については、国が一方的に規制を課すことは、民間活力を阻害する懸念もあることに留意が必要。」とされている。その上で、「民間事業者等として必要性がある場合に、民間事業者等自身が必要に応じ自主的な調査を含む情報保全措置を講ずる必要性も指摘されている。検討の結果、環境整備を行う場合には、特にプライバシーや労働法令との関係も十分踏まえ、民間事業者等任せにせず、政府が明確な指針等を示していくことの妥当性を含め検討を進める必要がある[32]。」とされている。

さらに、「上記の取組を進める上で、公文書管理に関する諸制度のみならず、

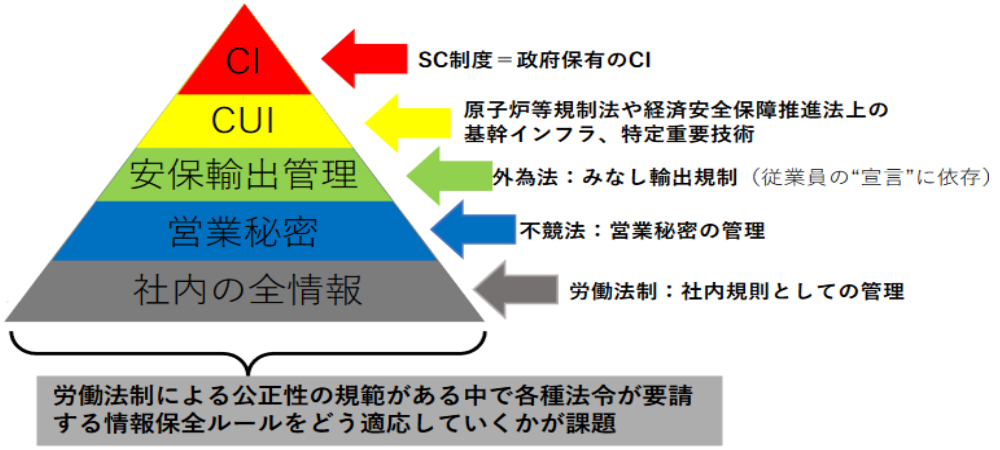
---

[31] この点について、令和５年３月 14 日に開催された有識者会議（第２回）では、委員から「追加的なコストに関して、財政的支援も含め、何らかの形でディスインセンティブとならないような配慮・対応が必要。」との意見があったとされる（議事要旨 15 頁）。

[32] この点について、令和５年３月 14 日に開催された有識者会議（第２回）では、企業から「セキュリティ・クリアランスをＣＵＩまで含めていくと、従業員をどういった形で管理するかは難しい課題である。労働法制と情報保全の整合性を図って、考え方を示してほしい。」旨の意見があったとされる（議事要旨８頁）。

原子炉等規制法、営業秘密制度（不正競争防止法）、特許出願非公開制度や輸出管理制度等の既存の関連制度との関係も踏まえつつ、望ましい情報保全の在り方を検討していくことが必要である。」とされている。この点については、令和５年３月 14 日に開催された有識者会議（第２回）で企業から提出された情報保全関連制度の鳥瞰的な整理に関する資料が参考になる（図表８）。

図表８　情報保全関連制度の鳥瞰的な整理



（注）ＳＣ制度＝セキュリティ・クリアランス制度（現行制度を前提としたもの）
（出所）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２回）（令和５年３月 14 日）資料４

同資料に基づき、企業からは、①政府保有のＣＩのみならず企業が保有する情報の中には、外為法（みなし技術輸出規制[33]などが典型例）や原子炉等規制

[33] みなし技術輸出規制とは、日本国内において「非居住者」に対して特定の機微情報を提供することを目的とする取引を管理する制度であり、外為法第 25 条第１項に基づき事前に経済産業省の許可が必要になる。従来は、本邦人が原則「居住者」として扱われることはもとより、本邦内の事務所に勤務する外国人も「居住者」とされ、これら「居住者」間の技術提供はみなし技術輸出規制の対象外であった。従って、企業内における技術提供は原則対象外とされていた。また研究者、留学生等の本邦に入国後６か月以上経過した外国人も「居住者」とされていたため、大学等によるこれらの人への技術提供が、みなし技術輸出規制の対象外となる場合があった。令和３年 11 月 18 日に公表された経済産業省令・通達（同省令・通達は令和４年５月１日に施行）によって、「居住者」への技術提供であっても、「非居住者」に技術提供を行うのと事実上同一と考えられる場合、換言すれば、「居住者」が「非居住者」の強い影響下にある場合には、みなし技術輸出管理の対象であることが明確にされた（大川信太郎「経済安全保障と外為法に基づくみなし輸出管理の明確化について」『経団連タイムス』No. 3524（令和３年 12 月２日）等を参照）。なお、図表８の中で、従業員の“宣言”に依存とあるのは、従業員の自己申告に依拠した制度運用であることを指していると考えられる。この点について、令和５年３月 14 日に開催された有識者会議（第２回）では、企業から「昨年５月に運用が始まった外為法のみなし輸出制度、これも結局従業員の善意に依拠する制度運用になっている。実際、そ

法に基づき従業員の情報へのアクセスを規制する法令がある、②また、企業が不正競争防止法に基づき保有する営業秘密の保護を図るためには、一定の情報管理が必要となる、③セキュリティ・クリアランス制度、個別規制法、不正競争防止法などで要請される情報保全の方策に関して、関連する政府担当部署は複数あるが、企業の視点から見れば、特定情報に関する従業員のアクセス権の制限を労働法制上の要請との整合性を図りながら導入し、全情報の管理体系を確立する必要がある、④政府サイドの情報保全に関する考え方を明確に提示してもらいたい、との見解や要望が示されており、前述の「中間論点整理」の記述はこれらを受けた政府の姿勢を示したものと考えられる。

（２）信頼性の確認に係る理解の促進

「中間論点整理」では、信頼性の確認に係る理解の促進について、「諸外国では、信頼性の確認を受けることで社会での活躍の幅が広がるものと認識されているとの声も聞こえている。こうした認識に鑑み、処遇面[34]も含め、このような信頼性の確認に係る理解の醸成に努めることが重要である。」とされている。

６．おわりに

政府は、「中間論点整理」で示された方向性を踏まえ、今後は詳細な制度設計を含めた更なる検討を進めるものと思われる。なお、「中間論点整理」では、身辺調査の詳細や、秘密を漏えいしてしまった場合の罰則に関してはあまり言及されていない点について、高市経済安全保障担当大臣は、令和５年６月６日の記者会見の場で「これから法整備に向けて詳細な議論を詰めていく段階である。罰則については、特別の情報管理ルールを定めて、情報漏えいした場合には厳罰を科すことが通例であり、国際社会の中で通用する制度にしなければならない。その他の詳細はこれからであり、内閣法制局との相談もしなければならない。」旨を述べている[35]。

情報指定の範囲をどうするのかについては、機微な技術の流出防止との観点

の従業員がどういった人物であるかについて国籍も含め差別的に扱うことができない。」旨の意見があったとされる（議事要旨８頁）。

[34] この点について、令和５年２月 22 日に開催された有識者会議（第１回）では、企業から「セキュリティ・クリアランス等を受ける労働者に特別手当を支払うことを検討すべきと考える。米国で機密（Top Secret）レベルのセキュリティ・クリアランスを持つ労働者の平均賃金は、日本円換算で 1,300 万円を超えている。負担ばかりを労働者に課すのは不適切であり、これに報いる在り方というものも考えるべきである。」旨の意見があったとされる（議事要旨 13 頁）。

[35] https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230606kaiken.html

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をどう図るのかが重要である。こうした「中間論点整理」で示された論点のほか、身辺調査の詳細、例えば、適性評価事項の項目をどう設定するか、また、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[36]等、更には、秘密を漏えいしてしまった場合の罰則等が制度設計に向けた主な論点となると思われ、法案提出までにこうした点を中心に議論を深める必要があろう。

なお、セキュリティ・クリアランス制度に関する政府内での検討が本格的に行われたのは、経済産業省が平成 20 年当時に設置した「技術情報等の適切な管理の在り方に関する研究会[37]」であると思われ、同研究会が同年 7 月 28 日に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、現在と同じような問題意識が既にこの当時にも持たれていたことが分かる。その後、15 年が経過しているが[38]、いまだに我が国はセキュリティ・クリアランス制度が未整備であり、そして、この間、我が国の国際競争力は低下傾向を続けている[39]。この点については、セキュリティ・クリアランス制度の未整備が長年続き、技術流出[40]や国際共同研究の機会の逸失等が生じたことが、国際競争力の維持・強化にマイナスに影響した

---

[36] 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））。

[37] 委員15名から構成される研究会で、報告書の公表に至るまで９回の研究会が行われている。なお、当時の委員名簿を見ると、今般の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の座長である渡部俊也東京未来ビジョン研究センター教授も委員として名を連ねている（平成 20 年当時の肩書は東京大学先端技術研究センター教授）。

[38] この間、特定秘密保護法は平成 25 年 12 月 13 日公布、平成 26 年 12 月 10 日に施行されている。

[39] ＩＭＤ（スイスのビジネススクールである国際経営開発研究所）の国際競争力ランキングを時系列的に見ると、平成 20（2008）年当時の日本は 22 位となっており、その後、下落傾向が続き、直近の令和５（2023）年は 35 位となっている。なお、同ランキングにおいて、平成元（1989）年から平成４（1992）年まで４年連続で日本は１位であった。

[40] 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））。

可能性があると考えられる。

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・クリアランス制度は我が国にとって必須になると考えられる。その一方で、セキュリティ・クリアランス制度については、プライバシーの侵害への懸念を背景とした否定的な意見も依然として存在する[41]。政府においては、こうした意見にも十分に配意し、丁寧で慎重な制度設計を行うことが求められる。

（内線 75103）

[41] セキュリティ・クリアランス制度の創設について、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（第 208 回国会衆議院内閣委員会議録第 14 号 10 頁（令 4.3.31））。