参議院常任委員会調査室・特別調査室

論題	経済安全保障分野の情報保全強化に関する検討状況と論点 ～セキュリティ・クリアランス制度の創設に向けて～
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	235 号
刊行日	2024-3-14
頁	1-24
URL	https://www.sangiin.go.jp/japanese/annai/chousa/keizai_prism/backnumber/r06pdf/202423501.pdf

経済安全保障分野の情報保全強化に関する検討状況と論点

～セキュリティ・クリアランス制度の創設に向けて～

内閣委員会調査室　柿沼　重志

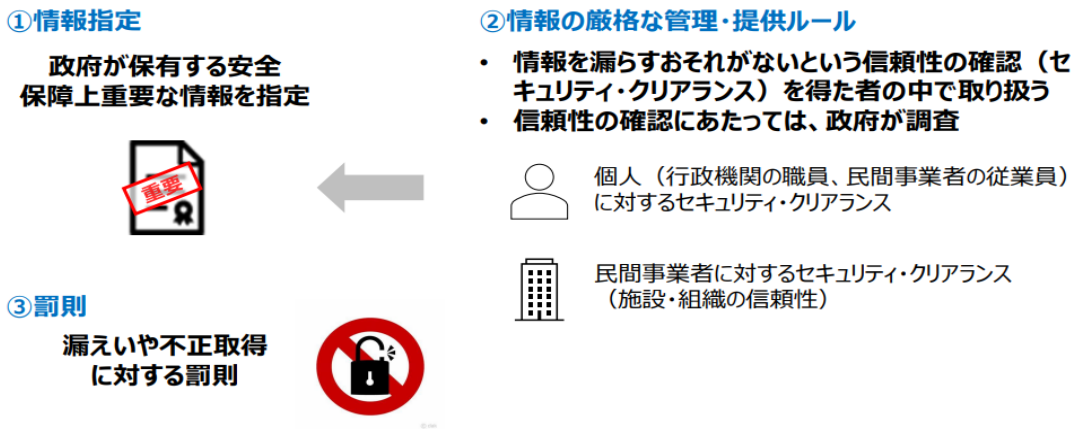
《要旨》

本稿では、経済安全保障分野の情報保全強化に関する検討状況と論点について、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。）の「最終とりまとめ」を題材の中心として整理を行う。

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、政府が保有する安全保障上重要な情報として指定された情報（ＣＩ[2]）に対して、アクセスする必要がある者のうち、情報を漏らすおそれがないという信頼性を確認した者の中で取り扱うとする制度である。なお、漏えいや不正取得に対する罰則を定めるの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）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）

[1] 本稿は、令和６年３月１日の脱稿時点までの情報に基づき執筆している。
[2] Classified Information の略。

「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」（以下「経済安全保障推進法」という。）（令和４年法律第 43 号）の法案審査において、衆参内閣委員会では、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[3]。

その後、「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。

次いで、令和５年２月 14 日に開催された経済安全保障推進会議[4]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た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、高市経済安全保障担当大臣に対して指示があった。これを受け、同 21 日に、有識者会議が設置された。

有識者会議は、同年６月６日に「中間論点整理[5]」を公表した後、同論点整理をベースに更なる検討を進め、令和６年１月 19 日に「最終とりまとめ」を公表した[6]。なお、有識者会議は「最終とりまとめ」について、委員間における検討の最終的なとりまとめの結果であり、政府に対し、本とりまとめが示した方向性を踏まえ、法整備を含めた対応を促すものであるとした。

次いで、令和６年１月 30 日に開催された経済安全保障推進会議において、岸田総理は、「政府保有の経済安全保障上の重要情報を保護・活用していくべく、コンフィデンシャル[7]級の情報を保護の対象とする制度を新法により創設するとともに、既存の情報保全制度である特定秘密保護法とシームレスに運用していく必要があります[8]」と発言している。その後、令和６年２月 27 日にセキュリティ・クリアランス制度を創設するための新法である「重要経済安保情報の保護及び活用に関する法律案」が閣議決定され、同日国会に提出された。

---

[3] 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（以下「特定秘密保護法」という。）」（平成 25 年法律第 108 号）は平成 25 年 12 月 13 日に公布、平成 26 年 12 月 10 日に施行されている。

[4] 議長は内閣総理大臣であり、令和３年 11 月 19 日に創設された。

[5] 中間論点整理までの議論については、拙稿「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～」『経済のプリズム』第 226 号（令和５年８月）を参照。

[6] それに先立ち、令和６年１月 17 日の有識者会議で最終とりまとめ案が示されている。

[7] 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を指す。

[8] <https://www.kantei.go.jp/jp/101_kishida/actions/202401/30keizaianpo.html>

以下では、「最終とりまとめ」を題材の中心として、経済安全保障分野の情報保全の強化に向けた検討状況と論点について、整理を行うこととしたい。

２．セキュリティ・クリアランス制度の必要性

（１）国としての必要性

「最終とりまとめ」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えい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」旨が示されている。

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明示的に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」とされている。

なお、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（令和４年末時点で、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数は約 13 万人、保有者の比率は、官が 97％、民が３％）[9]」とされている。

（２）企業からのニーズ

[9] 各国政府資料を基に内閣官房にて調べた情報（令和５年５月時点で判明しているもの）。日本については、「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報告」（令和５年６月版）。

「最終とりまとめ」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」とされている（図表２）。

図表２　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（いわゆるＣＵＩ（Controlled Unclassified Information））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、Beyond ５Ｇ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）有識者会議「最終とりまとめ」（令和６年１月 19 日）

こうした企業からの声に関して、「最終とりまとめ」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」とされている[10]。

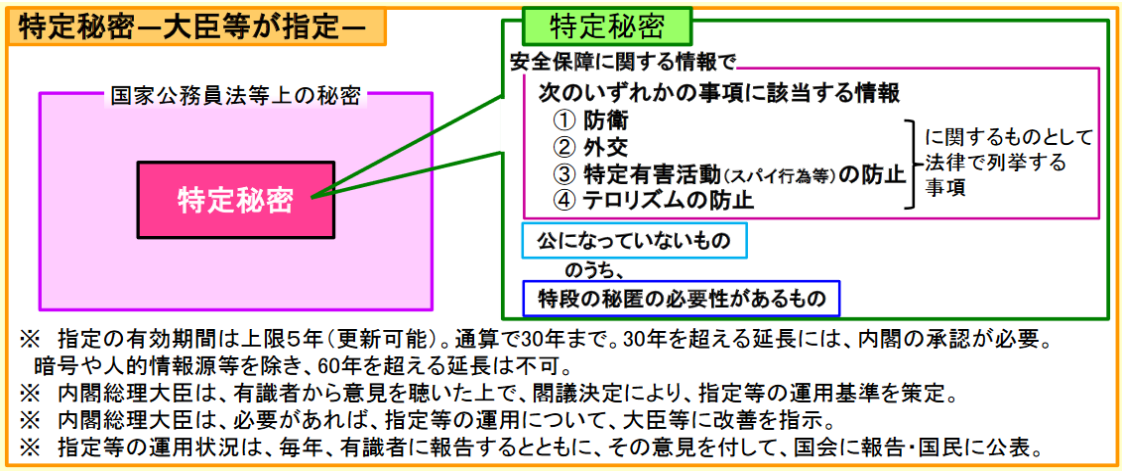
[10] セキュリティ・クリアランス制度の導入について、経済安全保障推進法案の審査において衆

３．新たな制度の基本的な骨格

「最終とりまとめ」では、「今回の制度の検討に当たっては、特定秘密制度の中で整備するにせよ、経済安全保障に特化した別の制度として整備するにせよ、既存の特定秘密制度との整合性や連続性に配慮することが、諸外国との関係でも、ＣＩを管理する政府及びＣＩへのアクセスを要する民間事業者にとっても重要である。このため、仮に別の制度として整備するのであれば、基本的には、特定秘密保護法の構造を参照しつつ、新たな制度を検討することが適当である」とされている。なお、特定秘密保護法の構造は以下のとおりである（図表３）。

図表３　特定秘密保護法の構造

①特定秘密として指定できる情報の範囲、指定、有効期間等（第３条、第４条、別表）

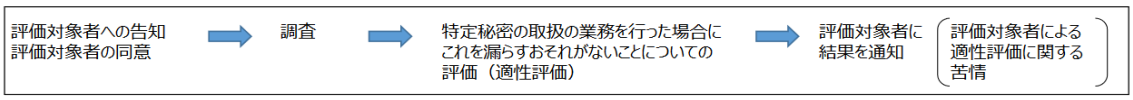


②適合事業者への特定秘密の提供（第８条）

○　行政機関の長は、特段の必要があると認めたときは、適合事業者との契約に基づき、適合事業者に特定秘密の提供等することができる。

○　適合事業者は、契約に従い、特定秘密の適切な保護のために必要な措置を講じ、従業者（適性評価を実施し、特定秘密を漏らすおそれがないと認められた者）に特定秘密の取扱いの業務を行わせる。

③適性評価の手続（第 12 条、第 13 条及び第 14 条）



（出所）有識者会議における内閣官房資料（「特定秘密保護法概要」）（令和５年４月 25 日）等により作成

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、「導入するのであれば、本格的な導入、国際的に通用するものが必要であって、簡易な形で導入するのではなく、そういったしっかりとした制度設計にしていただきたい」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））。

また、「最終とりまとめ」では、新たな制度の基本的な骨格について、「①政府として秘匿すべき機密情報の指定・解除のルールを定めた上、②当該情報に対する厳格な管理や提供のルールを定め、併せて、③漏えいや不正取得に対する罰則も定めるのがＣＩ保全制度の基本的な骨格であり、②の管理・提供ルールの中で、情報へのアクセスの条件として個人や事業者のセキュリティ・クリアランスの仕組みを設ける必要がある」旨の新たな制度の基本的な骨格が示されている。

４．新たな制度の具体的な方向性

（１）情報指定の範囲

まず、制度の対象とすべき情報の分野として、「最終とりまとめ」では、「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[11]。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[12]」とされている。

その上で、経済安全保障上重要な情報、すなわち国家及び国民の安全を支える我が国の経済的な基盤の保護に関する情報の候補は以下のとおりとされている（図表４）[13]。

図表４　経済安全保障上重要な情報の候補

サイバー関連情報
■ サイバー脅威・対策等に関する情報
規制制度関連情報
■ 審査等に係る検討・分析に関する情報

[11] この点について、日本経済団体連合会は「制度の対象となる情報は、政府が保有する経済・技術分野の情報の中でも特に国家として厳格に保全すべき情報に限定すべきである。経済・技術分野において、民間の企業・個人等が保有している情報や必ずしも重要でない情報までをも対象とすれば、民間の自由な活動を阻害し、かえって国力の重要な要素である経済力・技術力を毀損しかねない」旨の意見を表明している（日本経済団体連合会、『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提言』３頁（令 6.2.20））。

[12] 特定秘密保護法では第３章（第６条～第 10 条）で、特定秘密の提供について規定されているが、経済安全保障上の重要情報に関しても同様の規定が整備されるものと考えられる。

[13] この４類型について、令和５年 10 月 11 日に開催された有識者会議（第７回）では、事務局（内閣官房）から、「有識者会議の事務局が各省庁に対し、幅広く、何らかの経済性を帯びるような情報であって、保全が必要と考えられるような情報について提出の依頼をし、集まってきたものを事務局が類型化したものである」旨の説明がなされている（議事要旨９頁）。

調査・分析・研究開発関連情報
■ 産業・技術戦略、サプライチェーン上の脆弱性等に関する情報
国際協力関連情報
■ 国際的な共同研究開発に関する情報
（注）上記には、特定秘密保護法上の別表に該当し得ると思われる情報も含まれている。

（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）

そして、「最終とりまとめ」では、「そうした情報について、特定秘密制度によるにせよ、別の制度になるにせよ、シームレスに、取扱者のセキュリティ・クリアランスを含む厳格な管理が行われるようにすべきである。また、指定の対象となる情報の範囲については、法令等によりあらかじめ明確にしておくべきである」とされている。

また、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）[14]、シークレット（Secret）[15]、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。すなわち、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いるが、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政府保有情報も、同様に法律に基づく情報指定の対象となるようにすべきである」とされている。

「最終とりまとめ」におけるこれらの指摘を踏まえ、令和６年１月 30 日に開催された経済安全保障推進会議において、岸田総理は、「政府保有の経済安全保障上の重要情報を保護・活用していくべく、コンフィデンシャル級の情報を保護の対象とする制度を新法により創設するとともに、既存の情報保全制度である特定秘密保護法とシームレスに運用していく必要があります」とした上で、高市経済安全保障担当大臣に対し、「クリアランスの新制度が我が国の既存の情報保全制度とシームレスに運用されるよう、特定秘密保護法の運用基準[16]の見

[14] 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を指す。
[15] 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を指す。
[16] 「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」

直しの検討を含め、必要な措置を講じてください」との指示を出したとされる[17]。

岸田総理の指示によれば、情報を機密の度合いで２段階に分ける情報保全の枠組みを検討していると考えられ、それを踏まえた日米の情報保全の枠組みを図示すると、下図のようになる（図表５）。

図表５　日米の情報保全の枠組みの比較

<table>
<tr><th>日本</th><th>米国</th></tr>
<tr><td rowspan="2">特定秘密</td><td>トップ・シークレット</td></tr>
<tr><td rowspan="3">漏えいした場合、安全保障に「著しい支障」
→現行の特定秘密保護法で対応
加えて、特定秘密保護法の運用基準を見直し</td><td>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</td></tr>
<tr><td>シークレット</td></tr>
<tr><td>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</td></tr>
<tr><td>経済安全保障上の重要な情報</td><td>コンフィデンシャル</td></tr>
<tr><td>漏えいした場合、安全保障に「支障」
→新法で制度を創設
（※Ｇ７で日本が唯一制度未整備）</td><td>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</td></tr>
</table>

（出所）『日本経済新聞』（令 6.2.3）及び『読売新聞』（令 6.2.16）等を参考に作成

また、「最終とりまとめ」では、制度の対象とすべき情報の分野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にも鑑み、情報の指定・解除[18]に当たっては柔軟かつ機動的に対応できるように、政府以外の様々な関係者の意見も踏まえつつ、制度設計すべきである」とされている。なお、「これらの重要な情報のうち、要件を充足するものについては、各省庁において適切に情報指定されていくことが望ましく、各行政機関のリテラシーを高めるとともに、国家安全保障局等が中心となって、政府全体の総合調整を適切に実施していくべきである」とされている[19]。

（平成 26 年 10 月 14 日閣議決定、令和３年６月 11 日最終変更）

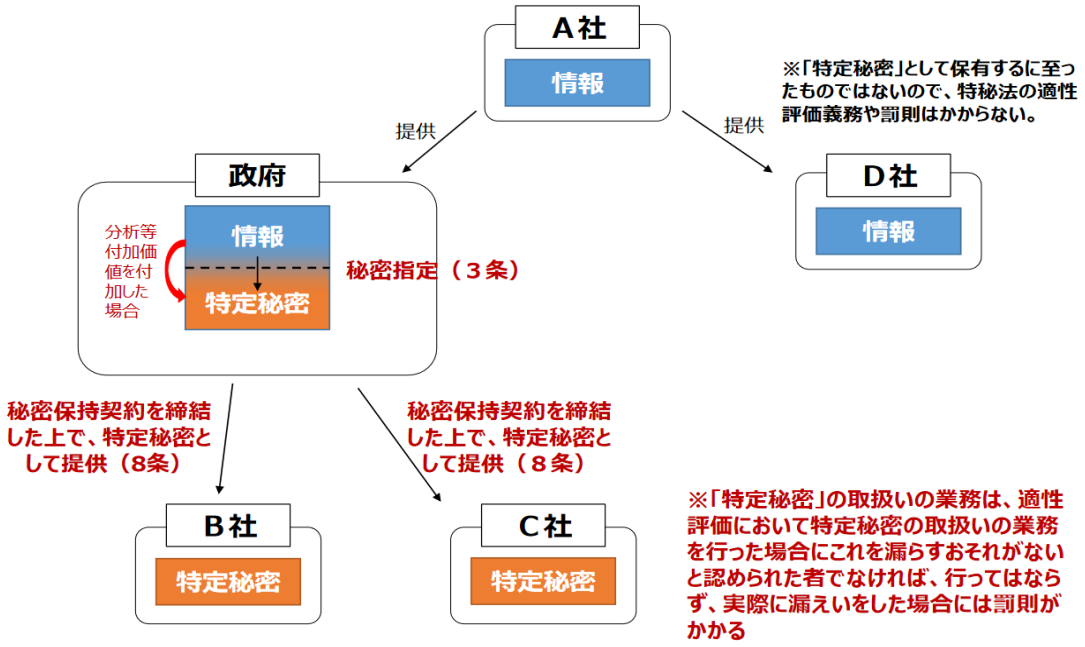
[17] 〈https://www.kantei.go.jp/jp/101_kishida/actions/202401/30keizaianpo.html〉

[18] 特定秘密保護法第４条第７項では、「行政機関の長は、指定をした情報が前条第１項に規定する要件を欠くに至ったときは、有効期間内であっても、政令で定めるところにより、速やかにその指定を解除するものとする」と規定されており、経済安全保障上の重要情報に関しても同様の仕組みが整備されるものと考えられる。

[19] この点に関連して、令和５年 10 月 11 日に開催された有識者会議（第７回）では、委員から

民間事業者等が保有する情報に関しては、「秘密指定の対象となるのは、政府が保有している情報であり、政府が保有するに至っていない情報を政府が一方的に秘密指定することは想定されない」とされている。また、「政府が民間事業者等から提供を受けて保有するに至った政府保有情報の取扱いについては、秘密指定すること自体が妨げられるものではないものの、秘密指定の効果は、政府との間で秘密保持契約を締結し、政府が秘密指定している情報と告げられてその提供を受けた者にのみ及び、かつ、それは、従前から民間事業者等が保有していた情報と重なる部分がある場合には、当該従前からの保有情報の管理に規制が加わるものではないと整理すべきである」とされている。この点は特定秘密保護法上で、民間提供情報を特定秘密に指定した場合にその効果が及ぶ範囲（図表６）を参考に制度設計が行われるものと考えられる。

図表６　民間提供情報を特定秘密に指定した場合にその効果が及ぶ範囲



（出所）有識者会議「事務局説明資料」（令和５年 11 月 20 日　内閣官房）

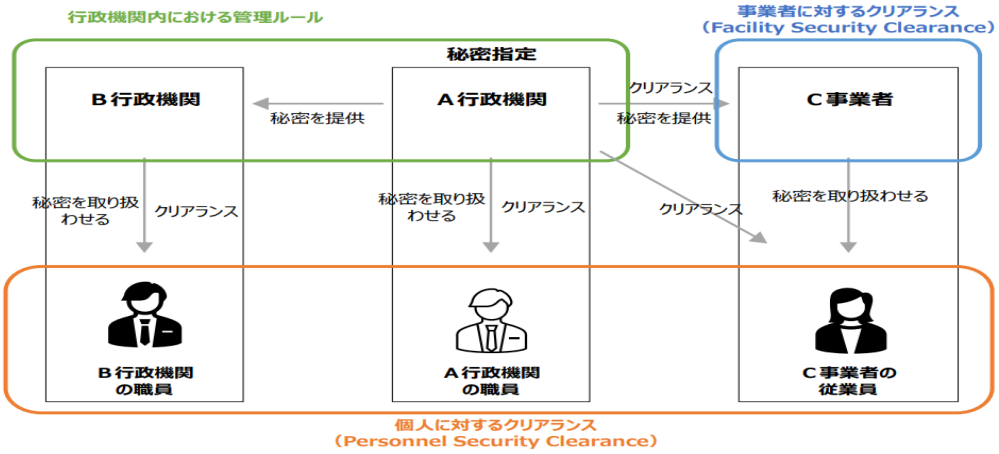
「今後、セキュリティ・クリアランス制度を経済安全保障分野にまで広げるという際には、10年前の特定秘密保護法制定当時と比べて、技術革新が激しく、地政学的リスクも日々変化し、生成技術やデジタル技術といった様々な技術が日々革新されていることを踏まえると、これらの情報が重要情報か否かを審査する者が専門家でなければ困るだろう。専門家を名乗る各省の担当官が、これらの情報を重要情報ではないと判断してそのまま指定されないのは非常に困るため、技術に関するリテラシーが必要である。これらの情報がどれだけ経済的な影響力があるかということを、審査担当官がきちんと審査できるということを担保する必要がある」との指摘がなされている（議事要旨 12 頁）。

図表６のＡ社やＤ社には特定秘密保護法の適性評価義務や罰則はかからない一方で、Ｂ社やＣ社には特定秘密を漏えいした場合には罰則がかかる。

（２）情報の管理・提供ルール

セキュリティ・クリアランス制度に関わる情報の管理や提供のルールについて、「最終とりまとめ」では、①行政機関内における管理ルール、②行政機関・民間事業者の別を問わず情報に接する必要性のある個人に対するクリアランス（Personnel Security Clearance：ＰＣＬ）、③事業者に対するクリアランス（Facility Security Clearance：ＦＣＬ）、の３つがあるとされている（図表７）。

図表７　情報の主な流れと管理・提供ルールのイメージ



（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）

「最終とりまとめ」では、まず、行政機関内における管理ルールについては、「特定秘密保護法では、各行政機関が秘密保護規程を設けて適切な情報管理を実施している」とした上で、「新たな制度においても、情報公開法や公文書管理法といった他法令との関係も踏まえながら、必要な規程を整備すること等によって、適切な情報管理に努めるようにすべきである」とされている。

次に、個人に対するクリアランスについては、「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）は、政府が保有する経済安全保障上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ころ、調査すべき項目や評価における着眼点といった点については、基本的に、特定秘密制度と差異を設ける理由はないと考えられる」とされている。なお、特定秘密保護法で定められる調査項目及び評価における着眼点は以下のとおりである（図表８及び図表９）。

図表８　特定秘密保護法で定められる調査項目

①　特定有害活動及びテロリズムとの関係に関する事項 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 ※①には、家族（配偶者・父母・子・兄弟姉妹、配偶者の父母及び子）及び同居人の氏名・生年月日・国籍・住所を含む

（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）

図表９　特定秘密保護法に基づく評価における着眼点

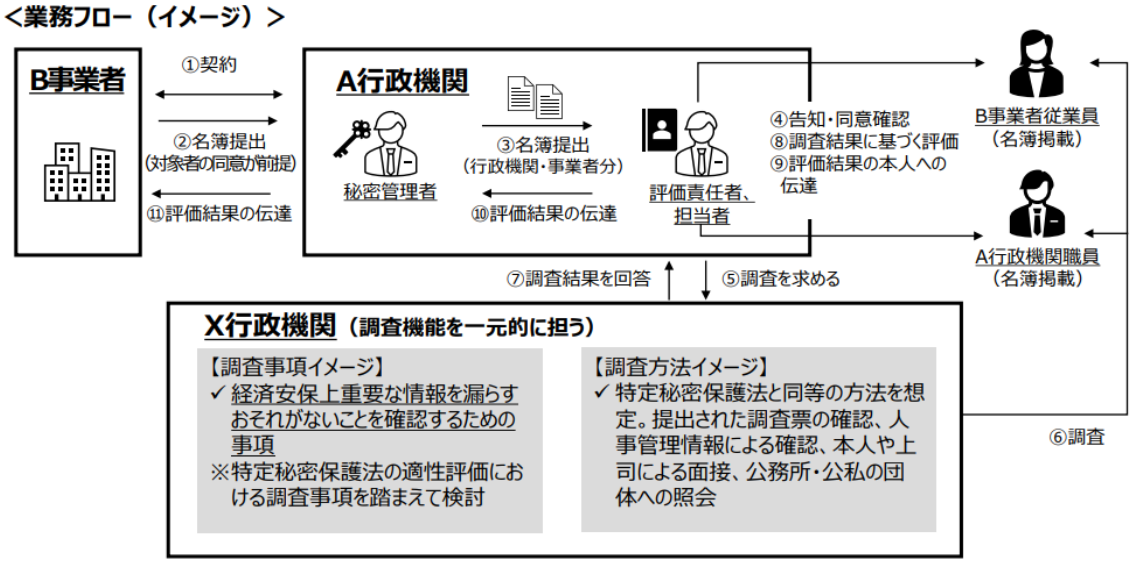
①評価の基本的な考え方
行政機関の長は、調査の結果を基に、評価対象者が特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないかどうか、以下の視点から、評価対象者の個別具体的な事情を十分に考慮して、総合的に判断するものとする。この場合において、調査を尽くしてもなお、評価対象者が特定秘密を漏らすおそれがないと認めることについて疑念が残る場合には、特定秘密の漏えいを防止し、もって我が国及び国民の安全を確保する特定秘密保護法の目的に鑑み、特定秘密を漏らすおそれがないと認められないと判断するものとする。 ア　情報を自ら漏らすような活動に関わることがないか イ　情報を漏らすよう働き掛けを受けた場合に、これに応じるおそれが高い状態にないか ウ　情報を適正に管理することができるか エ　規範を遵守して行動することができるか オ　自己を律して行動することができるか カ　職務の遂行に必要な注意力を有しているか キ　職務に対し、誠実に取り組むことができるか
②評価の際に考慮する要素
行政機関の長は、評価を実施するに当たり、調査により判明した事実について、以下の要素を考慮するものとする。 ア　特定秘密保護法第 12 条第２項各号に掲げる事項についての評価対象者の行動又は状態（以下「対象行動等」という。）の性質、程度及び重大性 イ　対象行動等の背景及び理由 ウ　対象行動等の頻度及び時期 エ　対象行動等があったときの評価対象者の年齢 オ　対象行動等に対する自発的な関与の程度 カ　対象行動等がなくなり、又は再び生ずる可能性

（出所）「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」（平成 26 年 10 月 14 日閣議決定、令和３年６月 11 日最終変更）

他方で、「新たな制度においては、情報保全の効果を棄損しない範囲で適切に効率化の検討をすべきである」とされた。具体的には、「調査と信頼性の確認（評価）は別のプロセスであり、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を前提に、調査機能を一元化することにより、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となるような一定の『ポータビリティ』を持たせることが重要である」とされた。調査機能の一元化について、高市経済安全保障担当大臣は、「一つの部署を政府内に設けて、そこが責任を持つ[20]。また、大事な個人情報であるので、これをしっかりとセキュリティを固めて守るということも大事だと考えている」旨の答弁を行っている[21]。

なお、調査機能の一元化の基本的な考え方と効果・業務フローのイメージは下図のとおりであり、同図中のＸ行政機関が調査機能を一元的に担う機関である。Ｘ行政機関の調査事項イメージは、経済安全保障上重要な情報を漏らすおそれがないことを確認するための事項とされている。また、Ｘ行政機関の調査方法イメージは特定秘密保護法と同等の方法を想定しており、Ａ行政機関職員やＢ事業者従業員から提出された調査票の確認、人事管理情報による確認、本人や上司による面接、公務所・公私の団体への紹介とされている（図表 10）。

図表 10　調査機能の一元化の基本的な考え方と効果・業務フローのイメージ



（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）

[20] 内閣府に専門機関を置く方向である旨が報じられている（『日本経済新聞』（令 6.2.2））。
[21] 第 212 回国会衆議院内閣委員会議録第２号 31 頁（令 5.11.8）

また、「最終とりまとめ」では、「信頼性が確認された後又は信頼性の確認手続中に本人側の事情変更があった場合に、信頼性の確認（評価）を行う各行政機関や調査機関がこれをタイムリーに把握できるよう、本人からの自己申告等の仕組みを確保するとともに、信頼性が確認された後に各行政機関と本人とのコミュニケーション等により継続的に状況を把握する仕組みについても検討していくべきである」とされている。

なお、事業者に対するクリアランスについて、「諸外国においても、民間事業者等が保有する施設などの物理的管理要件だけではなく、当該民間事業者等の株主構成や役員構成といった組織的要件を確認することとしている」とされている（図表 11）。特に、「外国による所有、管理又は影響（ＦＯＣＩ:Foreign Ownership,Control or Influence）[22]』を管理する規定を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。

図表 11　事業者に対するクリアランスの諸外国の例

	物理的管理要件	組織的要件の例 （外国による影響等（ＦＯＣＩ））
米国	○　建物構造の保全措置（例：外壁、扉、窓、警報措置　等） ○　情報管理上の措置（例：不正アクセス防止措置　等） ○　その他	○　クリアランス(注2)付与にあたり、対象事業者の経営陣（例：国籍等の人定事項）、出資元の外国資本等の保全上の影響を考慮(注3) ○　その上で、ＦＯＣＩの影響がある場合でも、一定の緩和措置を講じた上でクリアランスを付与する場合あり
イギリス(注1)		○　クリアランス(注2)付与にあたり、対象事業者の経営陣（例：国籍等の人定事項）、出資元の外国資本等の保全上の影響を考慮 ○　取締役の少なくとも 50%がイギリスに居住し、かつ、イギリス国籍であること
ドイツ		○　クリアランス(注2)付与にあたり、対象事業者の経営陣（例：国籍等の人定事項）、出資元の外国資本等の

[22] 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。」旨の発言が行われている（議事要旨 13 頁）。

		保全上の影響を考慮
フランス		○　クリアランス(注２)付与にあたり、対象事業者の経営陣（例：国籍等の人定事項）、出資元の外国資本等の保全上の影響を考慮

（注１）特に国防省との契約時の規定を掲載。
（注２）内閣官房の資料では「施設クリアランス」と表記されていたが、事業者に対するクリアランスという意味で使われていると解し、本稿では単に「クリアランス」と表記。
（注３）公開されている申告フォーム（ＳＦ（Standard Form）328）に、発行済み株式の５％以上を外国人が保有しているか、外国企業の 10%以上の持ち分を保有しているか、取締役会メンバー等に外国人がいるか等の質問項目があり、申告フォームに該当項目がある場合には、ＦＯＣＩ下にあるといえるか、ＦＯＣＩのリスクが許容範囲内か、リスク低減措置が取られるか、という観点からリスク評価を実施。
（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）を一部加工

また、「最終とりまとめ」では、「国内においても、現行制度の運用や主要国の例も参照しつつ、我が国の企業等の実情や特定秘密保護法、外国為替及び外国貿易法、会社法等との整合性も踏まえながら、実効的かつ現実的な制度を整備していくべきである」とされている[23]。

（３）プライバシーや労働法制等との関係

「最終とりまとめ」では、プライバシーや労働法制等との関係について、①評価対象者への丁寧なプロセス、②プライバシーとの関係及び③不利益取扱いの防止等の３点を挙げている。

まず、評価対象者への丁寧なプロセスについては、「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」とした上で、「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」とされている。

そして、「本人の同意は、言うまでもなく、任意かつ真摯なものでなければならず、そのような真の同意を得るには、あらかじめ本人に対して、どのような調査が行われるのかを含め、同意の判断に必要な事項が知らされること、及び

[23] 令和５年 12 月 20 日に開催された有識者会議（第９回）では、事務局（内閣官房）から「私どもとしては、施設クリアランスを米国あるいはその他の同志国との関係において信頼される制度を作るということの中で考えていく。制度は各国それぞれであり、ＦＣＬにしても、米国は安全保障の仕組みが社会経済全体に行き渡っているが、徐々に安全保障の考え方を経済システムの中に取り入れ、経済安全保障として変化しつつある日本で、どこまでできるのかという現実論も考える必要がある」旨の発言が行われている（議事要旨 17 頁）。

同意を拒否し又は取り下げても不当な取扱いが行われないことが担保されることが重要である」とされている。また、「経済安全保障に関するセキュリティ・クリアランスは民間に広がっていくことが想定されるところ、民間事業者等の従業者にあっては、行政機関から同意確認を受けるより前に、まず所属事業者等により、行政機関に提出する名簿に掲載するための同意確認が行われることとなるため、この場面における同意についても、同様に同意の判断に必要な事項が知らされるとともに、同意の拒否や取下げを理由とする不当な取扱いが行われないことが確保されるべきである」とされている[24]。

次に、プライバシーとの関係については、「信頼性の確認に当たって収集される情報は、対象者の個人情報であり、行政機関において厳重に管理されることが必須である」とした上で、「この点、特定秘密制度では、評価対象者が適性評価の実施に同意せず又は同意を取り下げたこと及び評価対象者についての適性評価の結果その他適性評価の実施に当たって取得する個人情報について、特定秘密保護の目的以外での利用や提供が禁じられているところ、新たな制度においても、同様の措置を講じることが必要である」とされている。加えて、「民間事業者等の従業者にあっては、調査において行政機関が収集した個人情報が所属事業者等に共有されるべきではなく、本人から行政機関への回答に所属事業者を介在させないなど、ここで収集される個人情報が所属事業者等の目に触れないような運用上の工夫もなされるべきである」とされている。

そして、不利益取扱いの防止等については、「信頼性確認を受けることへの同意を拒否し若しくは取り下げ、又は評価の結果セキュリティ・クリアランスを得られなかった場合に、ＣＩを取り扱う業務に就けないのは制度上やむを得ないが、それを超えて、かかる同意拒否・取下げや評価結果を理由に不合理な配置転換などの不利益取扱いを受けることは許容されるべきでなく、そうした不利益取扱いを含む調査結果等の目的外利用は、特定秘密保護法と同様に禁止さ

[24] この点について、朝日新聞の社説は、「有識者会議は、適性評価は『任意かつ真摯な』本人同意が前提とし、同意を拒否したり、『適性』が認められなかったりした場合でも、配置転換など不利な取り扱いを禁じるよう求めた。だが、従業員が会社からの求めを自らの意思通り断れるのか、疑問が残る。対象者を守る視点を徹底しなければならない」と指摘している（『朝日新聞』（令 6.1.19））。同様に、日本弁護士連合会は、「適性評価を受けるか否かは『任意』とされるが、これを拒めば、企業等が取り組む研究開発や情報保全の部署から外されたり、企業等の方針に反するものとして人事考課・給与査定等で不利益を受けたりする可能性も否定できない」と指摘している（日本弁護士連合会、『経済安全保障分野にセキュリティ・クリアランス制度を導入し、厳罰を伴う秘密保護法制を拡大することに反対する意見書』７～８頁（令 6.1.18））。

れるべきである」とされている。

さらに、「評価の結果セキュリティ・クリアランスを得られなかった場合には、その結果と理由が本人に速やかに通知されること及び異を唱える機会が確保されることも重要である」とされている[25]。

（４）漏えい等の罰則

ＣＩ保全制度においては、「情報保全の実効性を担保する観点からも、主要国に通用するという観点からも、漏えい等に対する罰則を定めることは重要である」とされた[26]。なお、諸外国における情報漏えい等に対する罰則は以下のとおりである（図表 12）。

図表 12　諸外国における情報漏えい等に対する罰則

	スパイ行為等	その他の情報漏えい等
米国	根拠：合衆国法典第 18 編 （刑法及び刑事訴訟法）	
	外国政府を援助する目的での国防に関する情報の外国政府関係者への漏えい（§794） →死刑、終身刑、有期刑	国防に関する情報の合法/非合法所持者による他者への伝達（§793） →10 年以下の拘禁刑、罰金刑 暗号及び通信諜報に関する機密情報の漏えい（§798） →10 年以下の拘禁刑、罰金刑 政府職員・政府との契約者等による職務上保有する機密文書の権限なき持ち去り（§1924） →５年以下の拘禁刑、罰金刑
イギリス	根拠：公務秘密法	
	国の安全又は利益を損なう目的での敵を利する情報の収集、伝達（1911　§１） →３年以上 14 年以下の拘禁刑、罰金刑	保安又は諜報の活動に従事する者によるその地位によって得た保安又は諜報に関する情報の漏えい（1989　§１） →２年以下の拘禁刑、罰金刑 政府職員又は政府との契約者によるその地位によって得た防衛に関する情報

[25] この点について、毎日新聞の社説は、「適格性の評価に不服がある場合に説明を求めることができる手続きは必要だ。政府が恣意的に判断することのないよう、第三者による検証など透明性を高める手立てを議論すべきだ」と指摘している（『毎日新聞』（令 6.2.8））。

[26] 令和５年 11 月 20 日に開催された有識者会議（第８回）では、委員から「実質的同等性の確保という観点から海外との比較が大事だと考えており、その一つの重要な要素が罰則の程度だと思う。その意味で、罰則の諸外国との比較は、必要条件だと思う。ただし、国によって法体系が異なり、軽重の付け方はそれぞれの国の思想に拠るところもあるので、単純に同じ年数でなければならないと言うつもりはない」旨の意見が表明されている（議事要旨 20 頁）。

		の有害な漏えい（1989 §２） →２年以下の拘禁刑、罰金刑 政府職員又は政府との契約者によるその地位によって得た国際関係に関する情報又は他国から入手した秘密情報の有害な漏えい（1989 §３） →２年以下の拘禁刑、罰金刑
ドイツ	根拠：刑法	
	国家秘密の外国勢力への漏えい（§94） →１年以上の拘禁刑 上記のうち、特別な地位を濫用した場合 →終身刑、５年以上の拘禁刑 上記のうち、対外的安全に特に重大な損害を与えるおそれを生じさせた場合 →終身刑、５年以上の拘禁刑	国家機密を権限のない者に触れさせ、又は公衆に知らせ、国の対外的安全に重大な損害を与えるおそれを生じさせる行為（§95） →６月以上５年以下の拘禁刑（特に重大な事案にあっては１年以上 10 年以下） （おそれの発生が過失による場合は、５年以下の拘禁刑、罰金刑（§97(1)）） 公務員、公共サービス委託先業者等が、その地位により得た情報を漏えいし、重要な公共の利益を危険にさらす行為（§353b） →５年以下の拘禁刑（危険の発生が過失による場合は、１年以下の拘禁刑）
フランス	根拠：刑法	
	国民の基本的利益を損なうおそれがある情報の外国政府や外国企業への漏えい（§411-6） →15 年以下の拘禁刑、22 万５千ユーロ（約 3,645 万円(注)）の罰金刑	国防上の秘密情報を職務上保有する者による漏えい（§413-10） →７年以下の拘禁刑、10 万ユーロ（約 1,620 万円(注)）の罰金刑 上記以外の者による国防上の秘密情報の窃取等（§413-11） →５年以下の拘禁刑、７万５千ユーロ（約 1,215 万円(注)）の罰金刑

（注）令和６年２月 19 日時点の為替レートである１ユーロ＝約 162 円で換算。
（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）を一部加工

また、「最終とりまとめ」では、経済安全保障上重要な情報のうち、トップ・シークレット級及びシークレット級の情報については、「特定秘密保護法の法定刑と同様の水準とすることが適当であることは言うまでもないが、コンフィデンシャル級の情報に対してどのような水準としていくかは、不正競争防止法や国家公務員法など漏えい行為を処罰する国内法とのバランスも踏まえながら、政府において具体的に検討していくべきである」とされている（図表 13）[27]。

[27] この点について、政府による経済安全保障上重要な情報に関する適格性評価は、特定秘密保護法と新法の二段構えとなる。機密性が高い「安全保障に著しい支障を与える情報」は特定秘

図表 13　情報の漏えい等に対する罰則を定めている主な法律

	行為	取扱にかかる法律でのPCL/FCL規定の有無	罰則（カッコ内は法人に科される罰金額※）
不正競争防止法	現職の役員又は従業者が、図利加害目的で、営業秘密の管理に係る任務に背き、営業秘密を使用又は開示	×	10年以下／2,000万円以下（なし）
特定秘密保護法	特定秘密の取扱いの業務に従事する者が、その業務により知得した特定秘密を漏洩	○	10年以下／1,000万円以下（なし）
マイナンバー法	個人番号利用事務等に従事する者又は従事していた者が、正当な理由なく、特定個人情報ファイルを提供	×	４年以下／200万円以下（１億円以下）
	個人番号利用事務等に従事する者又は従事していた者が、その業務に関して知り得た個人番号を自己若しくは第三者の不正な利益を図る目的で提供	×	３年以下／150万円以下（１億円以下）
衛星リモセン法	衛星リモートセンシング記録保有者が、公益上の必要や非常事態への対応等により行う場合以外で、衛星リモートセンシング記録を提供	×	３年以下／100万円以下（同左）
貸金業法割賦販売法	指定信用情報機関の役員若しくは職員又はこれらの職にあった者が、信用情報提供等業務に関して知り得た秘密を漏洩	×	２年以下／300万円以下（同左）
原子炉等規制法	原子力事業者等及びその従業者並びにこれらの者であった者が、正当な理由がなく、業務上知ることのできた特定核燃料物質の防護に関する秘密を漏洩	△	１年以下／100万円以下（同左）
国家公務員法自衛隊法	職員／隊員が、職務上知ることのできた秘密を漏洩	×	１年以下／50万円以下（なし）
防衛生産基盤強化法	装備品等秘密の取扱いの業務に従事する従業者が、その業務に関して知り得た装備品等秘密を漏洩	×	１年以下／50万円以下（なし）

（注１）※法人の代表者や従業者が、その法人の業務に関して違反行為をしたときは、行為者を罰するほか、その法人に対しても罰金刑を課すもの。
（注２）法律名は一部略称。
（注３）原子炉等規制法は、特定核燃料物質の防護に関する秘密について、原子力事業者・従業者等に対する秘密保持義務を規定。信頼性確認を行った上で秘密を業務上知り得る者を指定するなどの防護措置を講じることを原子力事業者等に義務付けている。
（出所）有識者会議「参考資料」（令和６年１月 17 日　内閣官房）を一部加工

また、「漏えい等が法人の事業活動の一環として行われた場合に法人を処罰する規定を置くことについても検討すべきである」とされている。なお、特定秘密保護法にはこうした「両罰規定」は規定されていない。

（５）情報保全を適切に実施していくための取組

「最終とりまとめ」では、「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、情報保全の重要性を理解した上で、適切に対応していくことが重要である」とした上で、「まずは、政府において、こうした理解が国民に広く醸成されるよう、新たな制度の具体的な中身やその必要性、どのような事業者に影響が及ぶのか等について、分かりやすい説明を尽くしていくべきである。

密保護法の制度で対応する。同法は機密漏えいに 10 年以下の懲役刑等の罰則を科す。それよりも機密性の低い「支障を与える情報」を新法で定める「重要経済安保情報」と位置付け、同情報を漏えいした場合は５年以下の拘禁刑等の罰則を科す旨が報じられている（『日本経済新聞』（令 6.2.2）、『読売新聞』（令 6.2.16））。なお、令和４年６月に改正刑法が成立し、令和６年６月からは懲役及び禁錮が廃止され、これらに代わるものとして、拘禁刑が創設される。

その際、特に、諸外国では、このような信頼性の確認を受けることで処遇面も含めて社会での活躍の幅が広がるものと認識されているということを踏まえることも重要である」とされている。

また、「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。この点について、政府においては、「経済安全保障上の重要情報を管理するための保護規程を整備するとともに、調査に関して取得・作成した文書等について公文書管理法や個人情報保護法に基づき厳重に管理していくべきであるほか、実際の保全措置を講ずるに当たり、必要があれば、専用の区画や施設も設けていくべきである」とされている。

さらに、「セキュリティ・クリアランス制度を日本の民間事業者等の海外ビジネス展開につなげていくためには、それを後押しするような同盟国・同志国との連携も重要であり、政府においては、今回の制度整備を踏まえ、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取組を進めていくべきである」とされている[28]。

このほか、「民間事業者等においても、実際に政府から経済安全保障上の重要情報が提供された際には、専用の区画や施設を設ける必要があるが、こうした施設等の整備は、民間事業者等にとっては少なからぬ負担となるとも考えられる。かかる負担については、民間事業者等が政府からの協力要請に応じてＣＩに触れることとなる場合など、経緯や実態も踏まえて、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[29]」とされている。

５．ＣＩ以外の重要な情報の取扱い

「最終とりまとめ」では、ＣＩ以外の情報について、「諸外国でもセキュリ

---

[28] セキュリティ・クリアランスの制度化について、鈴木一人東京大学公共政策大学院教授兼国際文化会館地経学研究所長は「重要なのは米英など英語圏５か国の枠組み『ファイブアイズ』と同等の基準を備えることだ。加盟国との共同研究に日本の技術者が参加できる環境の整備が急務だ。日本が同盟国・同志国との連携を強化して先端技術分野で国際競争力を高め、経済的威圧に負けない体制構築を図ることが求められている」旨を指摘している（『産経新聞』（令5.9.16））。

[29] 日本経済団体連合会は、「検討にあたっては、追加的に必要な施設や人員等も『保全の取組』として考慮することが求められる」としている。また、同連合会は、「能動的サイバー防御を実施するためには、政府から業務に携わる民間事業者等に対し、サイバー攻撃等に関するＣＩを含む重要情報を提供する必要が出てくると想定されるところ、当該民間事業者および従業者については、政府の要請に応じて信頼性確認を行ったうえで、セキュリティ・クリアランスを付与することが想定される」といった将来的な課題についても指摘している（日本経済団体連合会、前掲注 11、８～９頁）。

ティ・クリアランスの対象ではないため、今回のセキュリティ・クリアランス制度の検討の射程からは外れるが、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の取扱いについては、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、今後検討を進めていくべきである」とされている。また、「このうち、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であり、民間事業者等が営業秘密として自主的に管理していくことが基本であると考えられるが、他方で、民間事業者等が自らのために営業秘密をしっかりと管理していくことは、我が国の経済安全保障にも資する面がある」とされている。そこで、「政府として、民間事業者等が真に必要な情報保全措置を講じられる環境を整えていけるよう、民間事業者等任せにせず、明確な指針等を示していくことの妥当性も含め検討を進める必要がある」とされている。

６．主な論点

セキュリティ・クリアランス制度創設に向けては、以下のような論点が挙げられる。

①主要な同盟国や同志国に通用する制度となるための要件

「最終とりまとめ」では、セキュリティ・クリアランス制度の整備を検討するに当たっては、「主要な同盟国や同志国に通用するものとしなければならない」とされているが、そのための要件は具体的にどういうものなのか（秘密指定する情報の範囲や罰則による抑止力などか）。また、主要な同盟国や同志国に通用するセキュリティ・クリアランス制度を我が国が整備することにより、どのような効果が期待されるのか。

②民間人のクリアランス保有者が拡大する見通しとそれによる懸念点

「最終とりまとめ」で示されているとおり、米国ではセキュリティ・クリアランスの保有者が民間も含め 400 万人以上いるとされ、官民のクリアランス保有者の比率も７：３程度になっているとされる。一方、我が国では、特定秘密の取扱いの業務を行うことができる者は約 13 万人で、官民の保有者の比率は、官が約 97%、民が３％とされる。

今般、経済安全保障関連の情報保全制度が新たに創設されることで、我が国のクリアランス保有者の数もかなり増えることが見込まれるが、どのぐらいの

規模になると見込んでいるのか。また、民間人の保有者の比率はどの程度まで高まると考えているのか。また、それによる懸念点として、どのようなことが考えられるのか。

③情報指定の範囲

どのような情報が経済安全保障上重要な情報として指定されるのか曖昧であるとの批判があるが、どのように明確化していくのか。曖昧であることによって懸念される点はないのか[30]。

④中小企業・小規模事業者がセキュリティ・クリアランス制度の対象となる可能性等

どの程度の数の中小企業・小規模事業者がセキュリティ・クリアランス制度の対象となる見通しであるのか。特に、中小企業・小規模事業者に対しては、どのような情報が経済安全保障上の重要な情報として秘密指定される対象になるのか、また、信頼性確認のための調査についてはどのような調査が行われるのか、政府が分かりやすく丁寧に説明する必要があるのではないか。

⑤一元的調査機関の規模感等

一元的な調査機関について、高市経済安全保障担当大臣は、令和５年７月 21 日の記者会見で、「それなりの人員と規模感を持った組織が必要だ[31]」と述べている。一元的調査機関については、どのような組織を創設することを考えているのか（組織の規模感等）[32]。また、一元的調査機関はどのように個人情報の管理を行っていくのか。

⑥クリアランスの取得が事実上の強制になってしまうことへの懸念

民間事業者等の従業者が組織からセキュリティ・クリアランスの取得を求められた場合、その求めを断ることは容易ではなく、事実上の強制になってしまうのではないか。

⑦不利益取扱いの防止

「最終とりまとめ」では、「信頼性確認を受けることへの同意を拒否し若しくは取り下げ、又は評価の結果セキュリティ・クリアランスを得られなかった場合に、ＣＩを取り扱う業務に就けないのは制度上やむを得ないが、それを超え

---

[30] この点について、日本弁護士連合会は「適正な秘密指定がなされているかどうかをチェックするための政府から真に独立した機構を作ること」を提案している（日本弁護士連合会、前掲注 24、１頁（令 6.1.18））。

[31] <https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230721kaiken.html>

[32] 調査は行政機関の長の要請を受けて首相が一元的に実施する仕組みとし、内閣府に専門機関を置く方向である旨の報道もある（『日本経済新聞』（令 6.2.2））。

て、かかる同意拒否・取下げや評価結果を理由に不合理な配置転換などの不利益取扱いを受けることは許容されるべきでない」との旨が明記されているが、こうした点をどのように担保し、実効性のある制度とするのか。

⑧施設クリアランスを確保する民間事業者向けの支援

民間事業者等が機密情報の生成・受信・保存等を行う場合には、機密情報を扱う区画の設置や入退室管理システムを導入する必要があり、民間事業者等にとっては少なからぬ負担となることが予想される。こうした点について、政府はどのような民間事業者等を対象に支援を行っていくのか。例えば、中小企業・小規模事業者のみ対象とするなど、企業規模で対象を決めるのか。もしくは、政府からの協力要請に応じてＣＩに触れるような場合には、企業規模にかかわらず対象とするのか。

⑨両罰規定の狙いと期待される効果

「最終とりまとめ」では、「漏えい等が法人の事業活動の一環として行われた場合に法人を処罰する規定を置くことについても検討すべきである」とされているが、具体的にどのような制度設計を考えていて、どのような抑止効果を期待しているのか[33]。

⑩クリアランスを取得するインセンティブ

民間事業者等には、従業者がセキュリティ・クリアランスを取得することで、国際共同研究に参加できるようになる等のメリットがあるが、従業者側にとっては調査を受ける負担が大きいだけでは、クリアランスを取得するインセンティブが弱いのではないか。こうした点を解消するため、政府として何らかの支援策を考えているのか。「最終とりまとめ」では、「諸外国では、このような信頼性の確認を受けることで処遇面も含めて社会での活躍の幅が広がるものと認識されている」ことが指摘されているが、こうした認識を社会で醸成していくために、政府としてどのような取組をしていくのか。

⑪ＣＩ以外の重要な情報の取扱い（特に民間事業者等が保有している情報）

「最終とりまとめ」では、ＣＩ以外の重要な情報の取扱い、特に民間事業者等が保有している情報の取扱いについて、「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であり、民間事業者等が営業秘密として自主的に管理していくことが基本であると考えられるが、他方で、民間事業者等が自らのために営業秘密をしっかりと管理していくことは、我が国の

[33] この点について、産経新聞の社説は、「個人だけではなく組織に対する処罰規定も含めて漏えいには厳正に対処すべきである」旨を指摘している（『産経新聞』（令 6.1.24））。

経済安全保障にも資する面がある」とした上で、「政府として、民間事業者等が真に必要な情報保全措置を講じられる環境を整えていけるよう、民間事業者等任せにせず、明確な指針等を示していくことの妥当性も含め検討を進める必要がある」とされている。

どのような指針をいつ頃までに策定していくことを考えているのか。また、営業秘密の保護を強化するためには不正競争防止法の見直しも視野に入れる必要があるのではないか[34]。

⑫新法を制定する理由（特定秘密保護法との関係）

経済安全保障上の重要な情報を保全するための新法と特定秘密保護法とのシームレスな運用とは具体的にどのような意味なのか。また、令和５年８月１日の記者会見で、高市経済安全保障担当大臣は、経済安全保障上のセキュリティ・クリアランス制度の構築については、経済安全保障推進法に新たな章立てを行う旨の考えを表明していた[35]が、結論的には、新法制定による対応及び特定秘密保護法の運用基準の見直しによる対応となり、特定秘密保護法の改正や経済安全保障推進法の改正にしなかったのはなぜか[36]。

⑬新法制定による経済安全保障に関するコンフィデンシャル級の情報とその他の分野のコンフィデンシャル級の情報への対応に生じる不均衡への懸念

新法制定によって、経済安全保障に関するコンフィデンシャル級の情報がセキュリティ・クリアランス制度による対象となり、それなりに重い罰則がある情報保全制度となる一方で、その他の分野のコンフィデンシャル級の情報については、機密漏えいに対する処罰も国家公務員法上の比較的軽い罰則でしか対応できないとすれば、不均衡が生じ、適当ではないのではないか[37]。

⑭特定秘密保護法と同様の国会等による秘密指定・解除等に係る監視の必要性

---

[34] この点について、「営業秘密の保護が弱いと、日本企業の不利益となるだけでなく、半導体や蓄電池など戦略的な分野での最先端技術を日本に移転することを躊躇させる要因にもなる」との指摘がある（玉井克哉、兼原信克編著『経済安全保障の深層』（日本経済新聞出版、令和５年 12 月）、283 頁）。

[35] <https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230801kaiken.html>。

[36] この点について、小谷賢日本大学教授は「特定秘密保護法は本来、運用基準の見直しでなく、経済安保を４分野に追加するなど、法改正した方が分かりやすい」旨を指摘している（『読売新聞』（令 6.2.16））。

[37] この点について、令和６年１月 17 日に開催された有識者会議（第 10 回）では、委員からは「今回の法律で経済安全保障に関わる Confidential について規定すると仮定すると、それ以外の各行政機関が管理している Confidential 相当の情報も含めて対応する必要がある。そうしないと、機密漏えいに対する処罰が国家公務員法上の軽い罰則でしか対応できないなど、様々な不均衡が生じるおそれがあると思う」との懸念が示されている（議事要旨４頁）。

特定秘密保護法と同様に、コンフィデンシャル級の経済安全保障に関する情報の指定についても国会の情報監視審査会等による秘密指定・解除等の監視は必要ではないのか[38]。

今後を展望すると、半導体やＡＩを始めとして、同盟国・同志国との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、同制度に対しては、国民の知る権利及びプライバシー権の侵害や個人情報保護の問題等を懸念する否定的な意見も依然として存在する[39]。

国会においては、上記の論点を始めとして、法案提出後に、セキュリティ・クリアランス制度に係る論議が深化することが期待される。そして、政府においては、国会における論議や産業界や法曹界やマスコミ等を含む多方面からの意見にも十分に配意した丁寧で慎重な制度設計を行うことが求められる。

（内線 75103）

---

[38] この点について、朝日新聞の社説は、「特定秘密保護法では、国会の情報監視審査会が監視する仕組みがある。同様の体制整備はもちろん、更なる強化も検討すべき」旨を指摘している（『朝日新聞』（令 6.1.29））。また、日本弁護士連合会は「経済安全保障分野の情報保全制度を秘密保護法に取り込まないとすれば、秘密保護法の制定時に野党や市民の批判に応え、秘密保護法制が恣意的なものとならないように用意した、秘密の指定制度、違法秘密の指定禁止（ただし、法令ではなく運用基準による。）、衆参両議院の情報監視審査会や独立公文書管理監による秘密指定の監督など秘密保護法による規制さえ受けないこととなる可能性がある。秘密保護法制において情報監視審査会や独立公文書管理監などが果たしている役割を考慮しても、弊害はより大きなものとなると言わなければならない」と警鐘を鳴らしている（日本弁護士連合会、前掲注 24、４頁）。さらに、小谷賢日本大学教授も「国会が新法案の運用状況を積極的に審査すれば、制度の信頼性・透明性が高まる」としている（『読売新聞』（令 6.2.16））。

[39] セキュリティ・クリアランス制度の創設について、経済安全保障推進法案の審査において衆議院内閣委員会に参考人として出席した井原聰東北大学名誉教授は「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））。