Keidanren
Policy & Action

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

－有識者会議最終とりまとめを踏まえて－

2024 年２月 20 日

一般社団法人 日本経済団体連合会

目次

１．背景・経緯

今や国家の安全保障の対象は外交・防衛分野のみならず、経済・技術分野にも広がっている。即ち軍事転用可能な民生技術の獲得競争が激化するとともに、国家を背景としたサイバー攻撃の頻度が増している。

こうした中、わが国として、経済・技術分野においても保全すべき情報を指定し、厳格に管理する必要がある。その際、情報保全・管理に責任を負う政府と、経済・技術分野において主要な役割を担う企業との間の連携、情報共有が不可欠である。

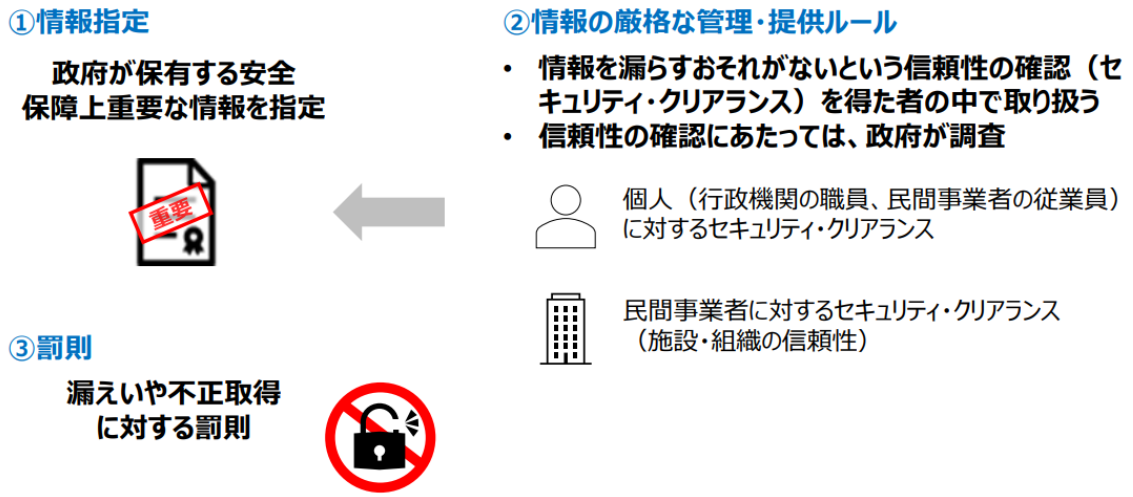
諸外国では、国家による情報保全措置の一環として、安全保障上重要と指定された政府保有情報（以下ＣＩ：Classified Information）にアクセスする必要がある者を、政府が調査して信頼性を確認した上でアクセスを認めるセキュリティ・クリアランス制度が経済・技術分野も含め運用されている。これに対し、わが国においては、特定秘密の保護に関する法律（以下、特定秘密保護法）によって、防衛、外交、特定有害活動防止、テロリズム防止の４分野の情報を対象としたセキュリティ・クリアランス制度として特定秘密制度が規定されており、経済・技術分野の情報は対象となっているとしても、上記４分野に係るものに限られているのが現状である。

また、セキュリティ・クリアランスは、国際共同研究開発や他国の政府調達に参加する際に求められることがあるが、わが国のセキュリティ・クリアランス制度では経済・技術分野の情報は限定的にしか対象とされていないため、わが国企業はそれらへの参加が叶わない、あるいは共有される情報が限定されるなど、結果としてわが国が戦略的優位性・不可欠性を維持・確保する機会を逸しているおそれがある。

以上の現状を踏まえ、経団連は、経済安全保障分野における、相手国から信頼されるに足る、実効性のあるセキュリティ・クリアランス制度の創設を求めてきた[i]。これに対し、政府は、昨年２月に「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）を立ち上げ、今年１月 19 日に「最終とりまとめ」（以下、最終とりまとめ）を公表した。

今後は、最終とりまとめを踏まえ、政府において、法案を策定することが想定されるが、法制化にあたっては、以下の諸点を十分考慮されたい（以下、「 」内は最終とりまとめからの抜粋）。加えて、最終とりまとめ公表後に新制度が特定秘密制度とは異なる制度として整備される方針が示されたことを踏まえ、両制度のシームレスな運用について併せて提言する[ii]。なお、法案成立の暁には、政省令等において詳細が規定されることになろうが、その際には、必要に応じて改めて意見を申し述べる。

【図１：いわゆる「セキュリティ・クリアランス」制度の概要】



出典：有識者会議（第 10 回）参考資料

２．基本的な考え方

制度設計にあたっては、以下を踏まえ、経済安全保障分野の情報保全に国家として万全を期す一方、情報にアクセスする企業・個人から見た予見可能性を確保することによって、わが国の戦略的優位性・不可欠性の維持・確保に資する必要がある。

第一に、外交、防衛等の分野のセキュリティ・クリアランス制度を規定している特定秘密保護法に基づく特定秘密制度等の既存の仕組みとの整合性を確保する必要がある。この点、最終とりまとめが、新たな制度の検討にあたっては、「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」としていることは重要である。

第二に、相手国から信頼されるに足る、実効性のある制度を目指す必要がある[iii]。わが国の情報力の強化にあたっては、わが国政府自身の情報収集・分析能力を高めることと並行して、諸外国から安全保障上重要な情報の共有を受けることが不可欠であり、その基盤となるのが、相手国から信頼されるセキュリティ・クリアランス制度である。なお、このことは諸外国の制度と全く同じ内容の法制化を求めることを意味しない。上述のとおり、特定秘密制度等の国内既存制度との整合性を確保することが先決であり、その範囲内で諸外国の制度との機能的同等性を出来る限り確保することが重要である。

第三に、経済・技術分野における情報漏えいの防止および情報力の強化という国としての必要性に加え、企業側のニーズをも踏まえる必要がある。上述のとおり、企業からは、国際共同研究開発や諸外国の政府調達への参加にあたって、セキュリティ・クリアランスの必要性が指摘されているところである。ただし、クリアランスを付与するにあたって、企業に過度な要件を課すことになれば、企業は制度の活用を忌避し、わが国の戦略的優位性・不可欠性の維持・確保につながらないばかりか、経済安全保障の確保に必要な官民の情報共有が進まない結果となりかねないことから、この点、十分な配慮が必要である。

第四に、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（以下、重要情報）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。

第五に、制度の対象となる民間事業者は、上記第四の考え方に基づき政府が指定した重要情報の共有を受ける意思を示した者に限定すべきである。当該情報の共有を受ける意思のない者まで対象とすることは、経済・技術分野における民間の自由な活動を明らかに阻害するものである。

第六に、上記第五にあるように、重要情報の共有を受ける意思を示した民間事業者において重要情報を取り扱う業務に従事する個人のクリアランス（信頼性の調査・評価）にあたっては、当該個人のプライバシーに十分な配慮が求められるとともに、信頼性の調査・評価の結果の目的外利用は厳に避けなければならない。当該民間事業者と従業者との間において十分なコミュニケーションが確保される必要がある。

３．新たな制度の具体的な方向性

（１）情報指定の範囲

上記基本的な考え方の第四で述べたとおり、制度の対象とすべき情報は、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重要情報に限定すべきである。この点、最終とりまとめが「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」としている点は適切である。加えて、「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。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、（中略）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」と記述していることも妥当である。

【図２：情報区分のイメージ】

	政府由来情報 （政府保有・民間へ共有）	民間由来情報 （民間保有）
CI（Classified Information）レベル	A	D
CIレベル未満の要保護情報	B	E
その他の情報	C	F

＊有識者会議　「中間論点整理」を経団連事務局が一部加工

その上で、最終とりまとめにおいて、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として、サイバー、規制制度、調査・分析・研究開発、国際協力に関連する情報が経済安全保障上重要な情報の候補として挙げられているが、これらのうち、一定の要件を満たす、真に守るべき情報の範囲を「法令等によりあらかじめ明確にしておくべきである」。

その際、最終とりまとめにもあるとおり、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、機微度に応じて複層的に管理している諸外国と同様に、新たな制度においては、「現行の特定秘密制度が対応していない諸外国のコンフィデンシャル（Confidential）級のＣＩにも対応する形」とし、「同様に法律に基づく情報指定の対象」とすべきである[iv]。

【図３：ＣＩの機微度の区分】

米国の区分	特定秘密制度等	有識者会議
Top Secret（機密）	● 特定秘密としてクリアランスを実施	経済安全保障上重要な情報を新たに指定しクリアランスを実施すべき
Secret（極秘）		
Confidential（秘）	● 防衛省のみクリアランスを実施 ● 他省庁は国家公務員法に基づく罰則のみ	

（経団連事務局作成）

また、各省庁において適切に情報指定がなされるよう、「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」ことが重要である。

（２）情報の管理・提供ルール

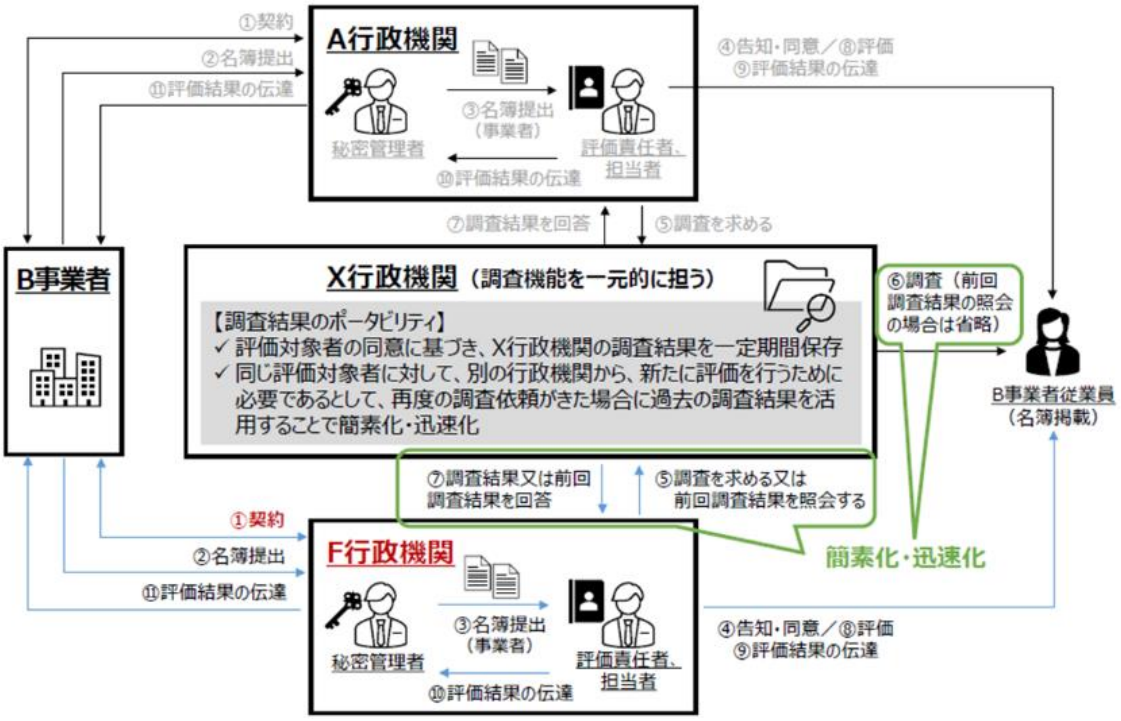
①個人に対するクリアランス（個人の信頼性に関する調査と評価）

最終とりまとめが指摘するとおり、特定秘密保護法の下では、「政府と複数の契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」のが現状である。この点、新たな制度の設計にあたって、企業からは、クリアランスのポータビリティを確保してほしいとの要望がある。即ち、信頼性の調査・評価の結果、クリアランスを一度得られた者については、一定の有効期間の間、当該クリアランスが他省庁においても有効とされれば効率的である。

最終とりまとめでは、信頼性の調査と評価は別のプロセスであるとし、「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」とする一方、評価は、当該情報の保全に責任を持つ行政機関が行うことを前提としている。以上のような対応は、企業の当初の要望からすれば、十分とは言えない一方、重要情報の指定が各行政機関において行われることに鑑みれば、一定の合理性が認められる。したがって、最終とりまとめにあるとおり、「調査機能の一元化を通じて、調査結果を一つの機関に集約し、当該機関が調査実務を担うことで、（中略）信頼性の確認を受ける者の重複調査の負担を減らし」ていくことが重要である。

また、個人に対する調査にあたり、当該個人に本人確認の書類等の提出を求める場合は「ワンスオンリー」の考え方に基づき負担の軽減に努めるべきである[v]。加えて、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る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」としているが、被評価者に過度の負担を課すことのないように留意すべきである。

【図４：調査機能の一元化とポータビリティのイメージ】



出典：有識者会議（第９回）資料

②事業者に対するクリアランス（民間事業者等に対する情報保全）

「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」。また、「諸外国においても、こうした事業者に対するクリアランス制度は整備されており、民間事業者が保有する施設などの物理的管理要件だけではなく、当該民間事業者の株主構成や役員構成といった組織的要件も確認することとしている」。したがって、最終とりまとめにおいて、「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」とされていることは適切である。政府においては、今後、国内既存制度との整合性を踏まえて現実的な制度とするとともに、国際的にも通用する実効的な制度となるよう諸外国の理解を得ていくべきである。

（３）プライバシーや労働法制等との関係

特定秘密制度と同様、新たな制度における個人の信頼性確認にあたっては、幅広い項目にわたり個人情報等を調査することが想定される。したがって、特定秘密制度と「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」ことは当然である。

また、調査にあたり収集された個人情報等は厳格に管理される必要がある。

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」としていることは適切である。

加えて、「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、（中略）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れるべきである」とされていることは妥当である。そうした事態が起きないよう、労使間の緊密なコミュニケーションを行うことが何より重要であり、それを超えて「同意プロセスの瑕疵や不当な取扱いを実効性をもって防ぐための方策」について検討するのであれば、特定秘密制度との整合性、当該方策が民間事業者に与える影響等に十分配慮すべきである。

（４）漏えい等の罰則

漏えいに対する罰則については、最終とりまとめが指摘するとおり、諸外国にも通用する実効的な水準であることを前提に、保全対象となる情報の重要度に応じて、トップ・シークレット級、シークレット級の情報については、特定秘密保護法と同水準とすること、コンフィデンシャル級の情報については、不正競争防止法や国家公務員法等との整合性を踏まえて定めることが適当と考えられる。

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」とされているところ、仮にそのような規定を設ける場合であっても上記のケースに限定すべきである。

（５）情報保全を適切に実施していくための取組み

最終とりまとめが指摘するように、「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」であり、そのため、政府は「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」と考える。とりわけ、民間事業者との関係では、①制度の対象となる情報は、わが国として真に守るべき政府が保有する情報に限定されること、②制度の対象となる事業者は、政府からＣＩの共有を受ける意思を示した事業者に限定されること、を周知することが無用な誤解を防ぐ上で重要

である。また、対象となる民間事業者がＣＩを適切に保全できるよう、「事業者から見て分かりやすい基準等の文書を作成、公表していく」必要がある。

なお、諸外国との重要情報の共有を促進するとともに、民間事業者の国際共同研究開発や諸外国の政府調達への参加につなげていくためには、セキュリティ・クリアランス制度そのものに加え、政府間の協定締結等も必要であると考えられる[vi]。この点、「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」との最終とりまとめを踏まえた政府の取組みが期待される。

また、民間事業者は、セキュリティ・クリアランスの取得に伴い生じる施設の整備費用等の負担も勘案した上でＣＩの共有を受ける意思を示すこととなろうが、「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」場合は、「経緯や実態を踏まえて、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」ことが妥当である[vii]。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。

４．ＣＩ以外の重要な情報の取扱い

ＣＩ以外の重要な情報について、最終とりまとめでは、「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。基本的な考え方で示したとおり、ＣＩ以外の重要な情報についても、民間事業者等が保有している情報までをも対象とすれば、民間の自由な活動を阻害し、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ため、「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」である。最終とりまとめは、さらに「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」としているが、今後、ＣＩ以外の重要な情報の取扱いに関して、政府として検討していく場合は、経団連として改めて意見を申し述べたい。

５．特定秘密制度等とのシームレスな運用

新たな制度を「仮に、特定秘密制度とは別の制度として整備することになるのであれば、諸外国ではＣＩは一つの制度で管理されているということとの関係にも十分に留意し、シームレスな運用を目指していくべきである」との最終

とりまとめの指摘は重要である。

その後、新たな制度については、トップ・シークレット／シークレット級を対象とする特定秘密制度とは別の制度として整備されることとなり、コンフィデンシャル級の情報のみが対象となる方向である[viii]。その結果、企業が国際共同研究開発や他国の政府調達に参加する際にトップ・シークレット／シークレット級のセキュリティ・クリアランスが求められた場合、新たな制度では対応できないことになる。一方、現行の特定秘密制度の下では、対象となっている経済・技術分野の情報は限定的であり、必ずしも上記のような企業のニーズに応えることができないと考えられる。この点、岸田総理から、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（特定秘密保護法の運用基準）の見直しの検討を含め必要な措置を講じるよう指示が出されたところ[ix]、特定秘密として指定される経済・技術分野の情報を拡充することなどを通じて、企業のニーズに対応すべきである。

以　上

---

[i] 経団連「経済安全保障法制に関する意見」（2022 年２月９日）
https://www.keidanren.or.jp/policy/2022/015_honbun.html

[ii] 経済安全保障推進会議（2024 年１月 30 日）において、高市早苗経済安全保障担当大臣は、既存の情報保全制度である特定秘密保護法がトップ・シークレット／シークレット級のものを保護する制度であることを踏まえ、コンフィデンシャル級のものを保全するための新たな制度を創設する方針を示した。これを踏まえ岸田文雄総理大臣は、セキュリティ・クリアランス制度に関する新法案の今通常国会への提出に向けて準備を加速するとともに、新制度がわ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の見直しの検討を含め必要な措置を講じるよう指示した。

[iii] 脚注ｉを参照。

[iv] 脚注ⅱのとおり、新制度はコンフィデンシャル級の情報を対象とする見込みである。

[v] 「デジタル社会の実現に向けた重点計画」（2023 年６月９日閣議決定）
情報通信技術を活用した行政の推進等に関する法律（以下「デジタル手続法」という。）では、デジタル３原則（①個々の手続・サービスが一貫してデジタルで完結する（デジタルファースト）、②一度提出した情報は、二度提出することを不要とする（ワンスオンリー）および③民間サービスを含め、複数の手続・サービスをワンストップで実現する（コネクテッド・ワンストップ）。）を基本原則として明確化するとともに、国の行政手続のオンライン化を原則としている。

[vi] 有識者会議（第２回）では企業から「諸外国ではＩＳＡ（Industrial Security Agreement）という仕組みがあり、２国間でＣＩ（Classified Information）を共有できるようにしている。アメリカとイギリスでは 2000 年にＩＳＡが締結され、セキュリティ・クリアランスの相互適用によって、研究開発、技術情報の共有、防衛装備品の連携促進等を含む包括的な連携が行われている」といった発言があった。

[vii] 例えば、2022 年 12 月に改定された国家安全保障戦略では能動的サイバー防御を導入する旨が明記された。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。

[viii] 脚注ⅱを参照。

[ix] 脚注ⅱを参照。