ANDERSON MŌRI & TOMOTSUNE

ECONOMIC SECURITY & INTERNATIONAL TRADE LEGAL UPDATE

2023 年 12 月 22 日

新たなセキュリティ・クリアランス制度の法制化に向けた議論の方向性

弁護士 藤田 将貴 / 弁護士 石川 雅人

Contents

Ⅰ. はじめに

2023 年 2 月に設置された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。）は、同年 6 月に過去 6 回にわたる有識者会議における検討の結果を中間論点整理[1]として公表した。

高市早苗経済安全保障担当大臣はセキュリティ・クリアランス制度の創設を盛り込んだ法案の次期（2024 年）通常国会への提出に向けた準備を進めていると明言しており[2]、有識者会議は中間論点整理を踏まえ、法案化に向けた議論を加速化させている。すなわち、第 7 回有識者会議（2023 年 10 月 11 日）では、今後新たに創設されるセキュリティ・クリアランス制度（以下「新たなセキュリティ・クリアランス制度」という。）の「基本的骨格」が示され、また、第 8 回有識者会議（2023 年 11 月 20 日）では、情報の機微度に応じた信頼性の確認方法や漏えい等に対する罰則のあり方等について議論が行われている。

---

[1] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/chuukan_ronten.pdf

[2] https://www.nikkei.com/article/DGXZQOUA239DT0T20C23A8000000/、https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai7/gijiyousi.pdf、https://www.cao.go.jp/minister/2309_s_takaichi/kaiken/20231010kaiken.html など。有識者会議は 2024 年 1 月にも最終取りまとめを行うとの報道もある（https://www.yomiuri.co.jp/economy/20231217-OYT1T50006/）。

以下では、第 8 回までの有識者会議における議論の状況とそのポイントについて説明する。

II. セキュリティ・クリアランス制度とは

一般に、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（Classified Information、以下「CI」という。）にアクセスする必要がある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を認める制度である。

III. 新たなセキュリティ・クリアランス制度の骨格

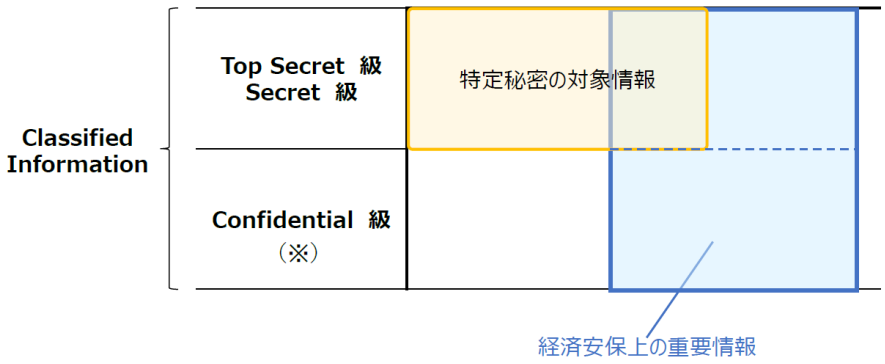
以下では、新たなセキュリティ・クリアランス制度の骨格に関する主な議論の状況とそのポイントについて説明する。

1. 情報の指定

(1) 情報の機微度

米国等では、CI は、漏えいした場合の被害の深刻さ等に応じて、Top Secret、Secret、Confidential 等の複数の階層に分けて管理されているのが一般的である。特定秘密保護法で特定秘密として指定されている情報の機微度は Top Secret および Secret に相当する。

これに対し、経済安全保障上の重要な情報の機微度は、Top Secret および Secret だけではなく、それらの下の階層である Confidential に相当する情報を含む方向で検討がされている（下図参照）。



出典：第 7 回有識者会議「事務局説明資料」[3] 4 頁

新たなセキュリティ・クリアランス制度においては、情報の機微度に応じて制度上の取扱いに差を設けることより、柔軟かつ機動的な運用が図られることが期待される。

なお、有識者会議においては、CI 以外の情報のうち管理の必要性が高いいわゆる CUI（Controlled Unclassified Information）についても守るべき情報として政府がガイドラインを作成すべきではないかといったこ

[3] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai7/siryou.pdf

とや CUI を扱う者についても犯罪情報や財務情報を確認する人的スクリーニングを行うことが必要ではないかといったことが議論されている。

(2) 情報の範囲(経済安全保障上の重要な情報)

特定秘密保護法では、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(スパイ活動)の防止、テロリズムの防止の 4 分野に関する情報に限られている。

これに対し、新たなセキュリティ・クリアランス制度においては、秘密指定の対象となる経済安全保障上の重要な情報を、「国家およ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」とする方向で検討が進められている。

具体的には、①サイバー関連情報(サイバー脅威・対策等に関する情報)、②規制制度関連情報(審査等にかかる検討・分析に関する情報)、③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)、④国際協力関連情報(国際的な共同研究開発に関する情報)という類型のうち機密性が高い情報がこれに当たるのではないかという方向で議論がされている。なお、これらの情報の中には特定秘密として指定できる情報の範囲(上記 4 分野)に該当し得る情報が含まれており、特定秘密保護法との関係の整理も必要となっている。

経済安全保障上の重要な情報の範囲については議論が続いており今後の議論の行方を注視する必要があるが、少なくとも現時点においては、経済安全保障上の重要な情報の範囲は経済安全保障推進法に基づく特許の非公開化に関する特定技術分野のようにあらかじめ一定の範囲に限定されているわけではないため、非常に広範な民間事業者に影響が及ぶ可能性がある。

(3) 秘密指定する情報の保有者等

政府が秘密指定する情報は政府が保有している情報であり、政府が外部から受領した情報を秘密指定した場合、その効果は原保有者には及ばないという方向で検討がされている。

この考え方を採った場合、原則として、民間事業者が保有している情報は、政府に共有されない限り秘密指定されることはなく、また、政府の秘密指定によって当該情報の原保有者である民間企業にセキュリティ・クリアランスが要求されることも、当該民間事業者が第三者に当該情報を提供する場合に当該第三者にセキュリティ・クリアランスが要求されることもないという帰結となる。

なお、特定秘密保護法では政府と民間事業者が秘密保持契約を締結した上で政府から民間事業者に特定秘密が提供されており、新たなセキュリティ・クリアランス制度においても、秘密指定された情報は、政府と民間事業者が秘密保持契約を締結した上で民間事業者に提供されることが想定される。

2. セキュリティ・クリアランスの対象範囲等

(1) 対象となる民間事業者

クリアランスの対象者は、基本的に政府から CI の共有を受ける意思を示した民間事業者となる方向で検討が進められている。ただし、有識者会議においては、サイバー関連情報を利用する基幹インフラ事業者に対しては、米国等から秘密指定されたサイバーセキュリティに関する防御策等を共有するため、当該事業者の意思表示によるのではなく、セキュリティ・クリアランスの対象となるよう義務として規制すべきではないかとの意見も出ている。

また、CI に触れることになる民間事業者の会計監査を行う監査法人や、サイバーセキュリティ監査を行う法人、法律事務所、特許事務所、環境監査を行う法人も、必要に応じ、クリアランスの対象になり得るのではな

いかという方向で検討が進められている。

(2) クリアランスの種類

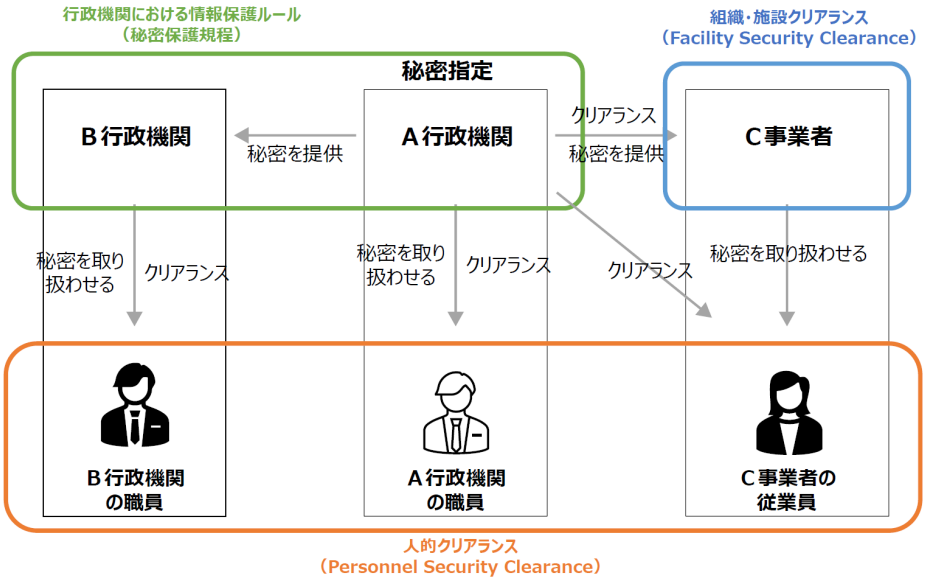
以下の種類のクリアランスを実施する方向で検討が進められている(下図参照)。

① 個人に対するクリアランス(「人的クリアランス」):
CI を扱う民間事業者の取締役、被用者等からの CI の漏えい可能性を確認・評価するためのもの

② 事業者に対するクリアランス(「ファシリティ・セキュリティ・クリアランス」):

a 「法人(組織)クリアランス」:
外国の所有、管理または影響(FOCI:Foreign Ownership, Control, or Influence)による当該民間事業者からの CI の漏えい可能性を確認・評価するためのもの

b 「施設クリアランス」:
当該民間事業者の施設の保全体制を確認・評価するためのもの



出典:第 8 回有識者会議「事務局説明資料」[4] 7 頁

(3) 人的クリアランス

上記(2)①の人的クリアランスの対象は、CI を取り扱う可能性がある個人であると考えられる。米国等において、人的クリアランスは、原則として、自国の国籍を有する者に付与することとされており、新たなセキュリティ・クリアランス制度においても、人的クリアランスは、原則として、日本国籍を有する者に付与されることが想定される。

また、人的クリアランスは、本人の同意を前提としたものであるが、プライバシー等の懸念があるため、プライバシーや労働法令との関係を踏まえる必要があるという方向で検討が進められている。

特定秘密保護法における適性評価においては、①特定有害活動およびテロリズムとの関係に関する事項

[4] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai8/siryou.pdf

（家族および同居人の氏名、生年月日、国籍、住所を含む。）、②犯罪および懲戒の経歴に関する事項、③情報の取扱いにかかる非違の経歴に関する事項、④薬物の濫用およ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することとされているところ、新たなセキュリティ・クリアランス制度においても、同様の事項について調査を行うことが想定される。

(4) ファシリティ・セキュリティ・クリアランス

ア 法人（組織）クリアランス

上記(2)②-aの法人（組織）クリアランスの対象は、基本的には、政府からCIの共有を受けようとする事業者であると考えられる。法人（組織）クリアランスの対象がCIの共有を受けようとする事業者だけなのか、それとも、例えば、親会社や子会社、関連会社といった関係にある事業者も対象になるのかについては、今後の議論を注視する必要がある。なお、日本企業であっても米国の現地法人が米国のクリアランスを取得できるのと同様、外国企業の日本法人については、日本の法人として登記されている場合には法人（組織）クリアランスの対象となり得る方向で検討が進められている。

また、上記のとおり、自らCIを取り扱う者は人的クリアランスの取得を求められることになるが、それとは別に取締役会議長やCEOに相当する者を始めとする役員については、CIを自ら取り扱わない場合であっても、FOCI(Foreign Ownership, Control, or Influence)の観点から、ファシリティ・セキュリティ・クリアランスを取得するための要件として、人的クリアランスを取得させるべきではないかといったことが議論されている。これはある企業において人的クリアランスの取得が求められる役員が外国人である場合、当該企業はファシリティ・セキュリティ・クリアランスを取得できない可能性があるため問題となる。すなわち、人的クリアランスは原則として日本国籍を有する者に付与されることになるため、外国人の役員は原則として人的クリアランスを取得できないことが想定される。また、役員自身は日本国籍を有していても、役員の配偶者等が外国人であるといった家族の事情で人的クリアランスを取得できない場合も想定される。

このようにファシリティ・セキュリティ・クリアランスを取得するための要件としてどのような範囲の役員について人的クリアランスの取得が求められるかは外国人の役員がいる企業を中心に影響が大きいと考えられるため、今後の議論を注視する必要がある。

加えて、米国等における法人（組織）クリアランスでは、FOCI(Foreign Ownership, Control, or Influence)の観点から、クリアランスの付与に当たり、経営陣や出資元の外国資本等の保全上の影響を考慮することとされており[5]、新たなセキュリティ・クリアランス制度においても同様に外国による影響等を審査することが想定されるところ、外為法に基づく対内直接投資審査制度との整合性を含め、どのような要件が設けられるかが注目される。

イ 施設クリアランス

上記(2)②-bの施設クリアランスについて、米国等における施設クリアランスにおいては、建物構造上の保全措置や情報管理上の措置といった措置を講ずることが求められている[6]。また、特定秘密保護法においては、特定秘密を保有し、その取扱いを行うことができる適合事業者は、特定秘密の保護のために必要な施設設備の設置や特定秘密を取り扱う場所への立入りおよび機器の持込みの制限のほか、業務管理者の指名、使用する電子計算機の制限、従事者に対する教育といった措置を講ずることなどが求められている。新たなセキュ

---

[5] 第8回有識者会議 2023年11月20日内閣官房『事務局説明資料』12頁

[6] 第8回有識者会議 2023年11月20日内閣官房『事務局説明資料』12頁

リティ・クリアランス制度においても、これらと同様の措置を講ずることを求められることが想定される。

(5) クリアランスの実施方法等

調査は少なくとも本人の同意を得て行われることを前提とする方向で検討が進められているが、法制化の段階で調査事項等の詳細が明らかになるのか、情報の機微度に応じて調査の深度が異なるのかといった点が注目される。

他方で、調査結果については一定のポータビリティ(調査結果が一定期間、組織や部署を超えて有効であること)が確保され、所管行政機関や契約ごとにセキュリティ・クリアランスが必要となる制度としない方向で検討が進められている。

3. 罰則

漏えいに対する罰則としては、特定秘密保護法の罰則(10 年以下の懲役または 1,000 万円以下の罰金)と同程度の罰則とする方向で検討が進められているが、有識者会議においては、これでは罰金額の上限が低いとの意見も出ているほか、新たなセキュリティ・クリアランス制度では特定秘密保護法では保護の対象となっていない Confidential に相当する情報を秘密指定することが想定されているため、情報の機微度に応じた罰則とすることも検討されている。

また、クリアランスへの同意拒否や調査結果を理由とする不合理な配置転換等の不利益取扱いに対する罰則を設ける方向で検討が進められている。

Ⅳ. おわりに

企業のニーズは、セキュリティ・クリアランスを保有することにより、国際共同開発や同盟国・同志国の政府調達等において企業が CI の共有を受けることができるようにするところにあり、これを実現するためには、米国や英国を始めとする相手国から信頼されるに足る制度、すなわち相手国のセキュリティ・クリアランス制度と実質的に同等といえる制度が求められる。加えて、次期通常国会への法案提出に向けて時間的制約がある中ではあるが、政府には、プライバシーへの配慮や適切な情報管理、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等を踏まえた上で、秘密指定する情報の範囲やセキュリティ・クリアランスの対象範囲について明確な考え方を示すことが期待されている。

企業としては、新たなセキュリティ・クリアランス制度が運用面も含めて同盟国等の制度と同等のものとなるか否か、ファシリティ・セキュリティ・クリアランスを取得するための要件として人的クリアランスの取得が求められる役員の範囲、セキュリティ・クリアランスの取得・管理および情報保全のための体制整備に伴う負担の程度、CUI(Controlled Unclassified Information)の取扱いといった点を中心に、今後も議論を注視していく必要がある。

以上

■ 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

■ 本ニュースレターの執筆者は、以下のとおりです。
弁護士　藤田　将貴（masaki.fujita@amt-law.com）
弁護士　石川　雅人（masato.ishikawa@amt-law.com）

■ ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

■ ニュースレターのバックナンバーは、こちらにてご覧いただけます。

「アンダーソン・毛利・友常法律事務所」は、アンダーソン・毛利・友常法律事務所外国法共同事業および弁護士法人アンダーソン・毛利・友常法律事務所を含むグループの総称として使用しております。