ANDERSON MŌRI & TOMOTSUNE

ECONOMIC SECURITY & INTERNATIONAL TRADE LEGAL UPDATE

2024 年 2 月 14 日

セキュリティ・クリアランス制度
―有識者会議による最終とりまとめと今後の方向性―

弁護士 中崎 尚 /弁護士 藤田 将貴 / 弁護士 松本 拓 /弁護士 石川 雅人

Contents

Ⅰ. はじめに

2024 年 1 月 19 日、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、10 回にわたる有識者会議の委員の検討の最終的な結果を「最終とりまとめ」として公表した[1]。

岸田内閣総理大臣は、最終とりまとめが示した方向性を踏まえ、政府が保有する経済安全保障上重要な情報のうち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創設する新法案の 2024 年通常国会への提出に向け、準備を加速化するよう指示した[2]。

以下では、最終とりまとめの内容とそのポイントについて説明する。

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

[2] 第 6 回経済安全保障推進会議における岸田内閣総理大臣発言
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai6/gijiyousi.pdf

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. 新制度の基本的な骨格

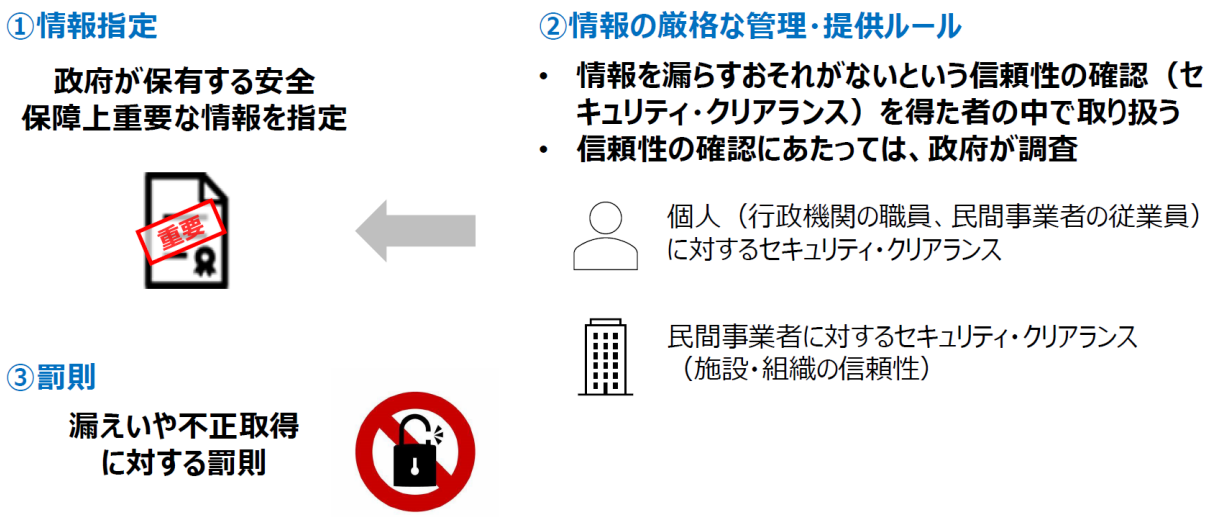
新制度においては、既存の CI 保全制度である特定秘密保護法[3]を踏まえ、

① 政府として秘匿すべき機密情報の指定・解除のルール

② 当該情報に対する厳格な管理・提供のルール（情報へのアクセスの条件としての個人や事業者に対するセキュリティ・クリアランスの仕組みを含む。）

③ 漏えいや不正取得に対する罰則

を定めるべきであるとされた（下図参照）。



出典：第 10 回有識者会議「参考資料」[4] 1 頁

IV. 新制度の具体的な方向性

以下では、新制度の具体的な方向性とそのポイントについて説明する。

1. 情報指定範囲

（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、トップ・シークレット（Top Secret）級、シークレット（Secret）級、コンフィデンシャル（Confidential）級等の複数の階層に分けて管理されているのが一般的で

[3] 特定秘密の保護に関する法律（平成 25 年法律 108 号）

[4] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

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トップ・シークレット級およびシークレット級に相当する。

これに対し、経済安全保障上重要な情報には、トップ・シークレット級およびシークレット級だけではなく、それらの下の階層であるコンフィデンシャル級に相当する情報を含めるべきであるとされた（下図参照）。

出典：第 7 回有識者会議「事務局説明資料」[5] 4 頁

詳細は明らかになっていないが、最終とりまとめ後に示された政府の方針を踏まえると、経済安全保障上重要な情報のうち、トップ・シークレット級およびシークレット級のものは特定秘密保護法によって、コンフィデンシャル級のものは新法によって情報指定・保護され、両制度が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などの必要な措置が講じられるものと考えられる[6]。

なお、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)については、政府がその保全措置について明確な指針等を示していくことの妥当性を含め今後検討を進めていくべきであるとされた。

(2) 対象とすべき情報の分野（経済安全保障上重要な情報）

特定秘密保護法において、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、新制度においては、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、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）といった情報を候補として、政府は指定の対象となる情報の範囲を法令等によりあらかじめ明確にすべきであるとされた。

---

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

[6] 第 6 回経済安全保障推進会議における岸田内閣総理大臣発言 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai6/gijiyousi.pdf、高市内閣府特命担当大臣記者会見 令和 6 年 1 月 30 日 https://www.cao.go.jp/minister/2309_s_takaichi/kaiken/20240130kaiken.html 参照。漏えいした場合、安全保障に著しい支障を生じさせる情報は特定秘密保護法で特定秘密に指定し、安全保障に支障を生じさせる情報は新法で経済安全保障上重要な情報として指定する方向であるとの報道もある（『経済安保、情報漏洩に懲役 5 年以下の罰則 新資格で新法』日本経済新聞 2024 年 2 月 2 日 https://www.nikkei.com/article/DGXZQOUA01BT30R00C24A2000000/

(3) 民間事業者が保有する情報

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、秘密指定の効果は原保有者には及ばないと整理すべきであるとされた。

この考え方を採った場合、原則として、民間事業者等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事業者等にセキュリティ・クリアランスが要求されることも、当該民間事業者等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。

2. 情報の管理・提供ルール

(1) 対象となる民間事業者等

セキュリティ・クリアランスを受けることとなる者は、政府職員のほか、政府から CI を受ける意思を示し、政府と秘密保持契約を結んで政府が保有する CI の内容に触れることを要する業務を行おうとする事業者およびその従業者とすべきであるとされた。この点、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たが、このような一定の事業者に対するセキュリティ・クリアランスの取得の義務付けについては最終とりまとめには盛り込まれなかった。

なお、公認会計士、弁護士等については、職務上 CI にアクセスする必要があったとしてもセキュリティ・クリアランスの対象から例外的に除外すべきであるといった議論はされていないことに留意する必要がある。

(2) クリアランスの種類

行政機関内における適切な情報管理のほか、以下の種類のクリアランスを実施すべきであるとされた(下図参照)。

① 個人に対するクリアランス(PCL:Personnel Security Clearance)
CI を扱う民間事業者等の取締役、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(FCL:Facility Security Clearance)
以下の要件が満たされているかどうかを確認・評価するためのもの

a. 物理的管理要件
情報の物理的な保全という観点から、民間事業者等が保有する施設の適格性を確認・評価する。

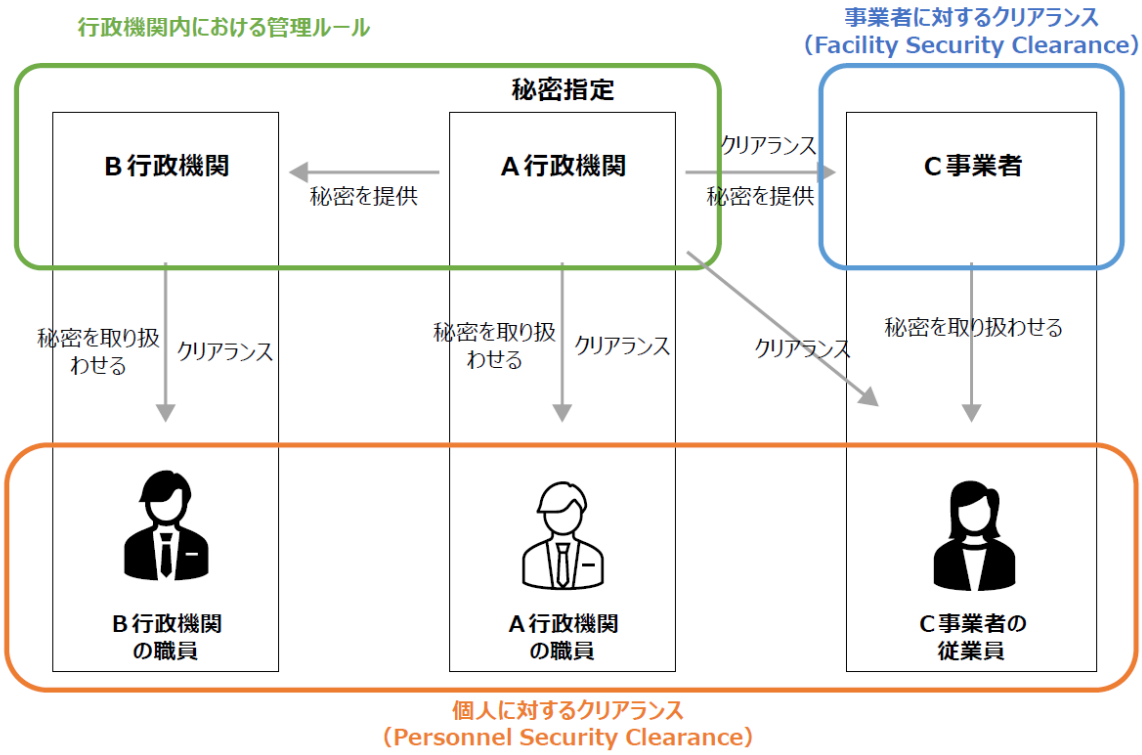
b. 組織的要件
外国の所有、管理または影響(FOCI:Foreign Ownership, Control, or Influence)の観点から、当該民間事業者等の株主構成や役員構成といった事業者そのものの属性や組織の適格性を確認・評価する。

上記①の個人に対するクリアランスについては、調査と信頼性の確認(評価)は別のプロセスであるとした上で、政府における調査機能を一つの機関に集約し[7]、調査結果に一定のポータビリティ(調査結果が一定期間、

[7] 調査は内閣総理大臣が一元的に実施する仕組みで、内閣府に専門機関を設置する方向であるとの報道もある(『経済安保、情報漏洩に懲役 5 年以下の罰則　新資格で新法』日本経済新聞 2024 年 2 月 2 日

組織や部署を超えて有効であること)を持たせることによって[8]、手続の効率化や民間事業者等の負担の経験を図るべきであるとされた。

有識者会議においては、上記②-bの組織的要件の1つとして、CEOや取締役会議長に相当する者のPCL取得を要求すべきではないかといった議論がされていた。最終とりまとめにおいても組織的要件としてPCL取得が求められる者の範囲について結論は出ていないが、米国においてはPCL取得が原則として自国の国籍を有する者に限られていることとの関係上、PCL取得が求められる者の範囲は実務的には重要である。



出典:第10回有識者会議「参考資料」[9] 4頁

3. プライバシーや労働法制等との関係

(1) 評価対象者への丁寧なプロセス

個人に対するクリアランスは、丁寧な手順を踏んで調査対象者本人の同意を得て行うことを前提とすべきであるとされた。

(2) プライバシーとの関係

行政機関においては、調査の実施に当たり取得する個人情報の目的外での利用や提供を禁じるべきであるとされたほか、無用に長期にわたって個人情報が保管され続けないような配慮や調査対象者本人から所属する民間事業者等を介在せずに情報を提供させるなどの工夫をすべきであるとされた。

---

https://www.nikkei.com/article/DGXZQOUA01BT30R00C24A2000000/)

[8] 調査結果の有効期間は10年以内とする方向であるとの報道もある(『経済安保、情報漏洩に懲役5年以下の罰則 新資格で新法』日本経済新聞2024年2月2日 https://www.nikkei.com/article/DGXZQOUA01BT30R00C24A2000000/)

[9] 前掲注4と同じ

(3) 不利益取扱いの防止等

調査に対する本人の同意の拒否・取下げや調査結果を理由とする不合理な配置転換などの不利益取扱いなどを禁止すべきであるとされた。

また、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通知されることおよび異を唱える機会を確保すべきであるとされた。

4. 罰則

漏えいした情報の機微度がトップ・シークレット級およびシークレット級の場合の罰則は特定秘密保護法の罰則と同様の水準にすべきであるとされた。また、コンフィデンシャル級の情報を漏えいした場合の罰則については、国内法とのバランスを踏まえて政府において検討すべきであるとされた[10]。さらに、両罰規定を置くことについても検討すべきであるとされた。

5. 情報保全を適切に実施していくための取組

政府においては、新制度について分かりやすい説明を尽くすとともに、民間事業者等から見て分かりやすい基準等を作成・公表すべきであるとされた。また、民間事業者等においては、政府から提供された情報を取り扱う専用の区画や施設を設ける必要があることから、それに伴う負担に対する支援の在り方についても合理的な範囲で検討すべきであるとされた。

Ⅴ. おわりに

企業にとっては、新制度により、国際共同開発や同盟国・同志国の政府調達等において CI の共有を受けることが期待できる一方で、調査への対応や秘密指定された情報を取り扱う区画や施設の整備といった負担を抱えることになるほか、調査対象者本人からの同意の取得やプライバシーとの関係、不利益取扱いの防止等にも配慮しなければならないこととなる。今後、政府には、法律案の国会審議等を通じて企業がこれらのメリット・デメリットを踏まえてセキュリティ・クリアランス取得の要否等を判断できるよう、新制度について分かりやすい説明を尽くすことが求められる。

また、新制度の下で従業員等にセキュリティ・クリアランスを取得させようとする企業においては、セキュリティ・クリアランスの取得を踏まえた採用・配置方針の立案や従業員等に対する情報保全措置に関する教育・研修の実施などを通じて、新制度の下で要求される情報保全措置を適切に講ずるための環境を徐々に整えていく必要がある。

以上

[10] 新法案によって創設される制度が保護の対象とする政府が保有する経済安全保障上重要な情報のうちコンフィデンシャル級の情報を漏えいした罰則は 5 年以下の懲役とする方向であるとの報道もある(『経済安保情報、新法で保全に網　民間の商機を確保』日本経済新聞 2024 年 2 月 2 日 https://www.nikkei.com/article/DGXZQOUA021VN0S4A200C2000000/)

■ 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　中崎　尚（takashi.nakazaki@amt-law.com）
弁護士　藤田　将貴（masaki.fujita@amt-law.com）
弁護士　松本　拓（taku.matsumoto@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。