経済安保分野におけるセキュリティ・クリアランス制度の法制化に向けた最終とりまとめが公表（2024.1.19）

２０２４年２月１６日

弁護士　小坂光矢

＜目次＞
1. セキュリティ・クリアランス制度について
(1) 特定秘密保護法
(2) 諸外国における制度
2. 最終とりまとめで示された方向性
(1) 情報の範囲・分野、区分
(2) 保護措置
(3) プライバシーや労働法制等との関係
(4) 漏えい等に対する罰則

2024 年 1 月 19 日、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による最終とりまとめが公表されました。経済安保分野のセキュリティ・クリアランス制度（以下「SC 制度」といいます。）のあるべき方向性をとりまとめたものであり、SC 制度の拡充によって、日本の安全保障の総合的な国力の向上に資するのみならず、民間事業者の観点からは、クリアランスの取得によってこれまで参加できなかった諸外国の政府調達や、衛星・AI・量子、Beyond 5G といった次世代技術の国際共同開発に参加できる機会を獲得することなどが期待されています。
最終とりまとめを踏まえた具体的な法案（仮称：重要経済安保情報の保護及び活用に関する法律案。以下「新法案」といいます。）は、2024 年 1 月 26 日に召集された通常国会において提出・審議される予定です。本ニューズレターでは、現在の日本における SC 制度と諸外国の状況、最終とりまとめの概要について解説することとし、新法案については、新法案の具体的な内容が分かり次第、随時解説いたします。

1. セキュリティ・クリアランス制度について

(1) 特定秘密保護法

SC 制度は、政府職員や民間事業者等の従業者が、政府が安全保障上重要な情報として指定した情報（Classified Information。原則として政府が保有するものに限られます。以下「CI」といいます。）にアクセスする必要がある場合に、政府がそれらの者を調査してその信頼性を確認する制度です。
現在の日本における SC 制度に関する法律には、特定秘密の保護に関する法律（以下「特定秘密保護法」又は「法」といいます。）があり、①防衛、②外交、③特定有害活動の防止、及び④テロリズムの防止という 4 分野について特定秘密の指定等の対象とされています。特定秘密を取扱うには、特定秘密保護法が求める保護措置を講じる必要があり、（A）行政機関の場合は、(a)秘密保護規程の策定及び規程に基づく適切な情報管理の実施、並びに(b)特定秘密を取扱う業務者に対する調査及び調査結果に基づく信頼性の確認（評価）（Personnel Security Clearance：PCL。以下では「信頼性確認」といいます。）の 2 つが、（B）民間事業者等の場合は、(c)特定秘密の保護のために必要な施設設備を設置していること等の基準に適合していること（Facility Security Clearance：

FCL)、及び(b)信頼性確認（PCL）の２つが、講ずべき保護措置とされています。信頼性確認（PCL）は行政機関の長が実施することとされています。

【特定秘密に対して求められる保護措置】

主体	保護措置	該当条文等
（A）行政機関	(a) 秘密保護規程の策定及び規程に基づく適切な情報管理の実施	法５条１項、施行令 11 条
	(b) 取扱者の信頼性確認（PCL）（※）	法 12 条
（B）民間事業者等	(c) 特定秘密の保護のために必要な施設設備を設置していること等の基準に適合していること（FCL）	法５条４項、施行令 13 条

（※）調査事項は、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の７点（法 12 条２項各号）。

(2) 諸外国における制度

アメリカやイギリスをはじめとする欧州等の主要な同盟国・同志国が運用する SC 制度では、現在の日本の特定秘密保護法の下で特定秘密に指定され得るものよりも広い範囲・分野の情報が対象となっており、また秘密の区分も日本より細かく設定されています。

参考として、アメリカの SC 制度では、以下のような情報が SC 制度の対象とされています。

【アメリカの SC 制度の対象となる情報の区分、及び範囲・分野】

情報区分		概要	クリアランス対象情報の範囲・分野
クリアランス対象情報（CI）	Top Secret 級	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	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
	Secret 級	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	
	Confidential 級	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	
その他取扱注意情報	Controlled Unclassified Information（CUI）	機密情報には該当しないが、一般市民への情報公開が原則的に制限される情報	―

特定秘密保護法は、諸外国との情報保護協定において、Top Secret 級や Secret 級に相当する CI の保全枠組みと位置づけられているため、日本には Confidential 級や CUI に該当する情報についての情報保全制度が存在していないことになります。

また、民間事業者等における FCL との関係でも、諸外国においては、（A）物理的管理要件（外壁、扉、窓、警報装置等の建物構造の保存措置や不正アクセス防止措置等の情報管理上の措置）だけではなく、（B）組織的要件（CEO や取締役会議長が PCL を取得していることや外国人の株式保有割合、役員の国籍等）も求められることが一般的ですが、日本の特定秘密保護法では（B）組織的要件は求められていません。

2. 最終とりまとめで示された方向性

(1) 情報の範囲・分野、区分

最終とりまとめでは、SC 制度の対象となる情報の範囲・分野として、以下の 4 分野が例示されました。

- 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（審査等にかかる検討・分析に関する情報）
- 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）

新法案における指定対象となる情報の範囲・分野が上記 4 分野に限られるかは現時点では不明ですが、最終とりまとめでは、指定の対象となる情報の範囲は法令等によりあらかじめ明確にされるべきとされています。
また、最終とりまとめでは、現行の特定秘密保護法がカバーしていない Confidential 級の情報についても情報指定の対象とすべきであるとされています。これに対して、諸外国の SC 制度における CUI に相当する情報の取扱いについては、今後の検討によることとされています。

以上をまとめると、新法案では、以下のオレンジ色文字下線部分に変更がなされると考えられます。

【新法案における変更点】

情報区分		情報の範囲・分野
クリアランス対象情報（CI）	Top Secret 級及び Secret 級（漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるもの。特定秘密保護法 3 条 1 項）	① 防衛 ② 外交 ③ 特定有害活動の防止 ④ テロリズムの防止 ⑤ サイバー関連情報（追加） ⑥ 規制制度関連情報（追加） ⑦ 調査・分析・研究開発関連情報（追加） ⑧ 国際協力関連情報（追加）
	Confidential 級（SC 制度の対象に追加）	
その他取扱注意情報	Controlled Unclassified Information（CUI）	今後検討を進める。

(2) 保護措置

PCL の調査項目や評価における着眼点については、基本的に特定秘密制度と差を設ける理由はないとされているため、現在と同様の内容になることが見込まれます。なお、特定秘密保護法の下では各行政機関がそれぞれ実施している調査機能を 1 つの機関に一元化することにより、調査結果の「ポータビリティ」（既に調査を受けた対象者が異動・退職するなどした場合にも、一度得られた調査結果を組織や部署を超えて有効とすること）等を確保することが重要であるとされています。
また、FCL についても、特定秘密保護法と同様の厳格な対応を適用していく必要があるとされているため、基本的には現在と同様の内容とすることが想定されているようです。もっとも、上述のアメリカ等の諸外国における組織的要件（CEO・取締役会議長による PCL の取得、外国人の株式保有割合、又は役員の国籍等）を要求するか否かは明言されておらず、主要国の例も参照しつつ実効的かつ現実的な制度を整備していくべきとされているため、今後の注視が必要と考えられます。

(3) プライバシーや労働法制等との関係

特定秘密保護法の下では、信頼性確認は対象者の同意の下に行われることが前提であり（法 12 条 3 項）、行政機関・民間事業者等が、評価対象者が信頼性確認の実施に同意しなかった事実や評価結果等の個人情報を、特定秘密の保護以外で利用・提供すること（例えば、不合理な配置転換などの不利益取扱いを行うこと等）は禁止されています（法 16 条）。これらの点については、新法案においても同様とされる見込みです。なお、最終とりまとめでは、不利益取扱いの予防措置として、CI を取り扱う業務に就くことが予定される求職者については、セキュリティ・クリアランスが必要となることを採用前に告知した上で、信頼性確認を受ける機会を設けること等により、採用内定後の内定取消しや採用後の解雇等の不利益取扱いに至ることを予防するという運用の在り方も検討

されるべきであるとされています。

(4) 漏えい等に対する罰則

特定秘密保護法では、特定秘密を漏えいした場合、10 年以下の懲役、又は情状により 10 年以下の懲役及び 1000 万円以下の罰金の対象となるとされています。最終とりまとめでは、Top Secret 級や Secret 級の情報の漏えいに関する罰則は、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とされていますが、Confidential 級の情報の漏えいに関する罰則の水準については、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検討することとされています。なお、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の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ています。

以 上