「経済安全保障推進法」企業に求められる対応

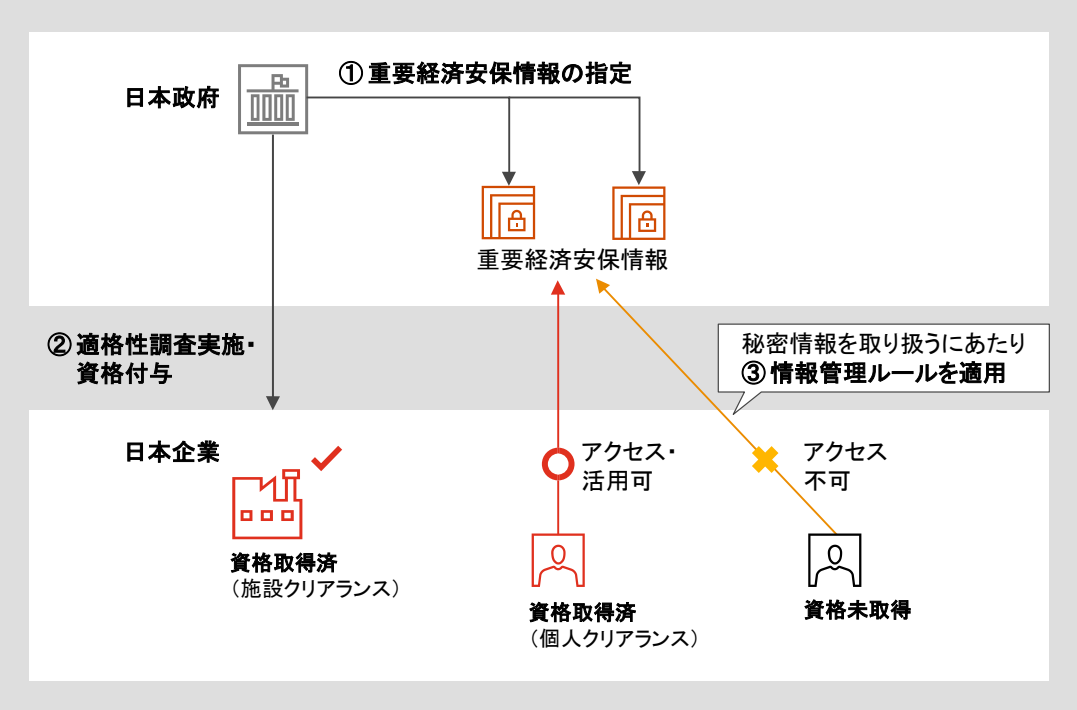
経済安全保障分野におけるセキュリティ・クリアランス（適格性評価）制度の企業影響について

連載コラム「『経済安全保障推進法』企業に求められる対応」では、2022年に成立した経済安全保障推進法の主要施策について、これまで5回に分けて解説してきました。第6回となる今回は、2024年の通常国会での法制化が見込まれている経済安全保障分野におけるセキュリティ・クリアランス（適格性評価）制度について、その施策内容と企業に及ぼす影響を解説します。

セキュリティ・クリアランス（適格性評価）制度とは

セキュリティ・クリアランス（適格性評価）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であるとして指定された情報にアクセスする必要がある政府職員や民間事業者などに対して、政府が調査を実施し、信頼性を確認した上でアクセスを認める制度です（図表1）。

図表1：経済安全保障分野におけるセキュリティ・クリアランス（適格性評価）制度の仕組み



出典：内閣官房資料をもとにPwC作成

セキュリティ・クリアランスとは

国家の情報保全措置の一環として、

1. 政府が保有する安全保障上重要な重要経済安保情情報を指定し、
2. 当該情報にアクセスが必要な者の調査を行った上で資格を付与し、
3. 情報管理規則を定め、当該情報の漏洩者に罰則などを課す制度

1. 重要経済安保情報の指定

重要経済基盤に関する情報で、公になっていないもののうち、漏えいした場合に安全保障に支障を与える恐れがある情報

指定の有効期限は5年以内。最長で30年まで延長可

2. 適格性調査実施・適正資格付与

民間事業者に対して調査実施・資格付与

民間事業者に情報共有する場合、民間施設の保全体制も確認（施設クリアランス）

3. 情報管理ルール適用

政府は罰則を含む情報管理ルールを制定

情報漏洩時の罰則は5年以下の拘禁刑もしくは500万円以下の罰金またはその両方

これまで日本では、2014年施行の特定秘密保護法において防衛、外交、特定有害活動の防止、テロリズムの防止の4分野の情報に関するセキュリティ・クリアランス制度が規定されていましたが、経済安全保障に関する情報は必ずしも保全対象となっていませんでした。

しかし、世界情勢の不安定化や地政学的な緊張の高まりを背景に、安全保障の概念が経済や技術の分野に拡大しています。また、軍事技術と非軍事技術の境目も曖昧となり、経済安全保障分野における情報漏洩リスクを低減する情報保全の重要性が世界的に高まっています。2023年5月のG7広島サミットでは、最先端の機微技術が国際平和と安全を脅かす軍事力の増強のために利用されることを防止するために、経済安全保障分野における機微情報を適切に管理する必要があるとの趣旨が首脳宣言に盛り込まれました。

日本政府は2023年2月に立ち上げた「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」において法制化に向けた検討を進め、2024年の通常国会にて法案を提出しました。

「重要経済安保情報の保護及び活用に関する法律案」の概要について

2024年の通常国会に提出された「重要経済安保情報の保護及び活用に関する法律案」（以下、法律案）は、重要なインフラや物資のサプライチェーンなど「重要経済基盤」に関する情報であって、公になっていないもののうち、その漏えいが日本の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるものを「重要経済安保情報」と定義し、保護対象とすると規定しています。具体例として、サイバー脅威・対策などに関する情報や、サプライチェーン上の脆弱性に関連する情報などが示されています。原則として政府が保有する情報を対象とし、民間事業者が独自で保有する営業秘密や企業秘密が勝手に法律の保護対象にならないとされています。

重要経済安保情報の指定の有効期限は5年以内とし、最長で30年まで延長可能とされています。重要経済安保情報の保護に必要な設備の設置などの基準は政令で定められ、政府が実施する適性評価において漏洩のおそれがないと認められた者にのみ、重要経済安保情報が提供されます。

適格性評価は本人の同意を得た上で実施され、有効期間は10年とされました。調査は「重要経済基盤毀損活動との関係（評価対象者の家族および同居人の氏名、生年月日、国籍、住所を含む）」「犯罪および懲戒の経歴」「情報の取り扱いに係る非違の経歴」「薬物の濫用および影響」「精神疾患」「飲酒についての節度」「信用状態その他の経済的な状況」などを対象に行われます。情報漏洩時の罰則は5年以下の拘禁刑もしくは500万円以下の罰金、またはその両方とされました。適格性評価には、個人の適正を評価する「個人クリアランス」だけでなく、重要経済安保情報の保護のために必要な施設設備の設置などを定める政令の基準に適合している事業者かどうかを評価する「施設クリアランス」の仕組みがあります。施設クリアランスを取得した事業者は、行政機関と契約を締結したうえで重要経済安保情報を受け取ることになります。

一方で、法律案では詳細が規定されず、法案成立後の政省令や細則、ガイドラインの内容を確認する必要がある内容として、適格性評価の対象となる企業の役員の範囲、施設クリアランスへの対応のための企業負担に対する政府からの支援内容（補助金などの有無）、企業の株主構成や役員構成といった組織的要件の評価有無、従業員への適格性評価に関する労使協定締結の義務化の要否、調査を拒否または資格を得られなかった従業員に対する不利益措置を禁止するための運用基準、機密指定や適性評価の状況を独立して検証する仕組みなどが挙げられます。企業においては、法制後に発表される政省令や細則、ガイドラインの内容を確認するとともに、所管省庁による説明会などで詳細を確認する必要があります。

日本企業へのメリットと懸念事項について

日本企業の視点で見たときのセキュリティ・クリアランス制度のメリットと懸念事項について解説します（図表2）。

図表2：セキュリティ・クリアランス（適格性評価）制度導入の企業のメリットと懸念事項

出典：内閣官房資料をもとにPwC作成

まず、メリットとしては、機微情報へアクセスできるようになることで機微情報を含む政府案件の受注可能性や、外国政府・企業との協業可能性が広がる点が挙げられます。これまでセキュリティ・クリアランス制度が日本に存在しないことで、日本企業が外国政府の保有する機微な情報についてアクセスできないために政府の調達・委託案件などに効果的な提案ができないという課題や、外国企業が保有している機微な技術が得られないために日本側で効果的な活用ができないといった課題が指摘されていました。セキュリティ・クリアランス制度の導入によって、日本企業による機微情報へのアクセスが実現することで、経済安全保障分野における国際的なビジネス機会の拡大や、競争力の向上に繋がると考えられます。

また昨今、さまざまなサイバーセキュリティ関連のインシデントが起きる中で、日本政府が保有している、または海外政府から日本政府が提供を受けるサイバーセキュリティ関連の機微情報を日本企業に開示してもらうことで、日本企業や政府のセキュリティレベルの向上につながることも期待されます。さらには、新たなセキュリティ・テクノロジーのイノベーション創出やサービス提供を日本企業が行うといったことも考えられます。

一方で懸念事項は大きく3点が挙げられます。1点目として、社内外協業や政府調達の前提要件となった場合の対応コストが増加したり、非対応時の相対的競争力が劣後したりするといった、競争力上のリスクが挙げられます。2点目として、メディアや市民から国による私権制限（守秘義務）やプライバシーの侵害に加担しているとの批判を受けるといった社会的リスク、そして3点目として、思想信条や労働法規性上の平等保障の観点から、現行の労働法制が変更され、それに基づく企業の人事管理・労務管理のオペレーション変更が必要となる法的リスクが挙げられます。

日本企業がとるべき対応について

日本企業においては法制後の制度運用開始を見据えて、セキュリティ・クリアランス取得にあたって自社にどのような影響が及ぶかを事前に検討し、対応を進めることで、競合他社への優位性確保や国際プロジェクトへの速やかな参画が実現することが考えられます。

具体的には、自社への影響の事前検討として、①影響を受ける部署・役員・事業ポートフォリオの特定、②必要となる予算・体制・施設などの確認および整理、③影響を踏まえた対応方針の作成（社内体制、社内システム、人材雇用・研修、ガバナンス制度、社内規則の刷新など）が挙げられます。加えて、制度導入後の事業機会獲得に向けた準備として、④国内外セキュリティ・クリアランス人材の獲得または育成に向けたプランニング、⑤国内外政府案件参画に向けた準備、⑥海外政府・企業との共同研究に向けた調整、⑦国内競合他社の動きの確認などが挙げられます。

PwC Japanグループが2023年8月に実施した「PwC Japan企業の地政学リスク対応実態調査2023」において、「セキュリティ・クリアランスの運用開始に向けてどのような対応を行っているか」という質問に対して「制度の内容理解」「事業影響の事前検討」「社外専門家への相談」といった回答が上位となったことからも、既に日本企業が対応を始めていることが分かります。

なお、経済安全保障推進法の主要施策の1つである「基幹インフラの安全性・信頼性確保」において「特定社会基盤事業者」に指定された民間事業者に対しては、米国などの同盟国や同志国から日本政府に対して共有されるサイバーセキュリティに関する防御策などの機微情報が日本政府から共有されることも想定されます。その際には、特定社会基盤事業者におけるセキュリティ・クリアランスの取得が前提となると考えられるため、本制度についても対応の事前検討が推奨されます。

執筆者

坂田 和仁
PwC Japan合同会社
地政学リスクアドバイザリー マネージャー

連載コラム「『経済安全保障推進法』企業に求められる対応」

地政学的な緊張が高まるなか、自国の脆弱性や潜在的なリスクを低減させる「経済安全保障」の取り組みが各国で進んでおり、日本企業のビジネスへの影響も拡大することが予想されます。2022年に成立した経済安全保障推進法が企業活動に及ぼす影響や、日本企業が安定したビジネス環境を維持し、国際競争力を向上させるために求められる対応について解説します。

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/economic-security.html