基礎研レター

日本のセキュリティ・クリアランス
求められる企業の経済安全保障対応

総合政策研究部 准主任研究員　鈴木　智也
(03)3512-1790　tsuzuki@nli-research.co.jp

1――はじめに

来年中の法案成立を目指して、政府は機密扱いとした情報にアクセス可能な人や施設を審査し、認証する「セキュリティ・クリアランス（以下、ＳＣ）制度」の導入に向けた議論を進めている。

今年（2023 年）６月、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は、６回にわたる議論を取りまとめた中間論点整理を公表した。今後、同提言で示された方向性を踏まえて、詳細な制度設計が進められる。

そこで本稿では、すでに導入済である特定秘密保護法と対比したＳＣ制度における特徴を整理し、企業に及ぶメリット・デメリットを踏まえたうえで、企業が取るべき対応について考える。

2――セキュリティ・クリアランス（SC）制度

セキュリティ・クリアランスとは、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を指定することを前提に、当該情報にアクセスする必要がある者（政府職員及び必要に応じ民間の者）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権を付与する制度と説明される[1]。

政府が保有する安保上重要な情報へのアクセスは、基本的には自国民を対象に付与され、特別の情報管理ルールを定めたうえで、当該情報を漏洩した場合には厳罰が科すことが通例である。

日本では、国が機密扱いとした情報を扱う制度として、2014 年から特定秘密保護法が施行されている。今般議論されているＳＣ制度は、これを強化し補完するものとなる。両制度の主な違いは、(1) 機

[1] 内閣官房 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「中間論点整理」（2023 年 6 月 6 日）

Copyright ©2023 NLI Research Institute All rights reserved

密指定される情報の範囲と、⑵ それを扱う適格性評価の２つである［図表１］。

【図表１】セキュリティ・クリアランス制度の特徴

		特定秘密保護法	セキュリティ・クリアランス
法律	成立年	2013年12月6日	未定（2024年頃？）
	施行年	2014年12月10日	（周知・申請・審査に必要な期間を設定？）
機密範囲		狭い	広い
	対象領域	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、の４分野に限定	左記に加えて、経済安保に関する情報、宇宙・サイバー分野の技術情報等に拡大
	秘密区分	単一層（特定秘密）	情報の機微度に応じた階層構造
適格性評価		統一基準のもとで、各行政機関が実施	調査機能の集約等により、効率的に実施
	評価対象	個人：公務員および一部民間企業の職員	個人：公務員及び民間企業の職員 施設：機密情報が共有される民間事業者
	評価基準	〈本人に関するもの〉 ①特定有害活動及びテロリズムとの関係、②犯罪・懲戒の経歴、③情報の取扱いの非違の経歴、④薬物の濫用及び影響、⑤精神疾患、⑥飲酒の節度、⑦信用状態その他の経済的な状況 〈家族・同居人に関するもの〉 氏名・生年月日・国籍・住所	同盟国・同士国（特に米国）との実質的同等性を確保することを重視 ※米国における評価基準 〈本人に関するもの〉 ①暴力的な政府転覆活動・テロ等への関与、②外国との関係、③犯罪歴、④民事訴訟歴、⑤情報通信関係の非違歴、⑥薬物の濫用、⑦精神の健康状態、⑧アルコールの影響、⑨信用状態、⑩知人の連絡先 等 〈家族・同居人に関するもの〉 氏名・生年月日・国籍・住所・社会保障番号 等
	プライバシー	本人の同意が必要	本人の同意が必要
罰則		最高で懲役10年・罰金	（同程度？）

（注）セキュリティ・クリアランス制度は検討中につき、中間的整理等をもとに検討の方向性について記載
日本の「特定秘密」は、諸外国における秘密指定された情報のうち「Top Secret」「Secret」の２階層に該当
（資料）内閣官房「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」資料および「特定秘密保護法と諸外国の秘密保全制度の比較」などをもとに筆者作成

まず、機密指定される情報の範囲については、特定秘密保護法が「防衛」「外交」「特定有害活動（スパイ活動等）の防止」「テロリズムの防止」の４分野に関する一定の要件を満たす事項に限定されるのに対して、ＳＣ制度では、これらに加えて経済安全保障に関する情報（経済制裁に関する分析関連情報や規制制度の審査関連情報など）、宇宙・サイバー分野の技術情報（脅威情報や防御策に係る情報）といった領域まで広がっている。これは、人工知能（ＡＩ）やドローン、ロボットといった民生技術が、軍事転用されるリスクが高まっていることに対応した動きである。安全保障上重要な先端技術が他国に流出することを防ぐ。

特定秘密保護法では、機密情報の秘密区分は「特定秘密」の単一層で管理し、比較的機密度の高い情報のみを対象としてきたが、ＳＣ制度では、諸外国のように情報が漏洩した場合の被害の深刻さ等に応じて、「Top Secret」「Secret」「Confidential」など複数階層で管理される見込みだ。

 | Copyright ©2023 NLI Research Institute All rights reserved

適格性評価では、対象となる人の範囲も拡大する。特定秘密保護法は、主に行政機関の職員を対象[2]としてきたが、ＳＣ制度では、機密となる情報の範囲が経済や技術等にも広がるため、民間企業の職員も広く対象となる。また、施設における情報管理も厳しく求められる。情報漏えいを防止するため、機密情報を扱う施設には、専用の区画を設けるなど適切な対応が求められる見込みだ。

加えて、評価基準が厳格化することも予想される。今般の中間論点整理では、ＳＣ制度について「相手国から信頼されるに足る実効性のある制度」とすることが強調されている。とりわけ、米国との実質的同等性を確保する重要性が指摘されており、評価基準も米国に近いものとなる可能性は高い。すでに各国のＳＣ制度は、相違点を踏まえつつ相互承認されている。例えば、米国のＢレベルは英国のＡレベルに相当するといった具合だ[3]。日本も機微情報をしっかり扱っていると諸外国から確信が持たれる仕組みとするため、同程度に厳格な基準が求められる。

ただ、日本では適格性評価において、犯罪歴、違法薬物の使用歴、飲酒の節度、交友関係、精神疾患、財務情報など、多様な身辺調査が行われることに対して懸念の声も上がっている。実際の運用では、プライバシーに深く立ち入る適格性評価は、本人同意が大前提となり、対象者の同意がなければ、適格性評価は実施されない仕組みとなる。

なお、資格保有者が機微情報を漏洩した場合には罰則もある。特定秘密保護法には、10 年以下の懲役および 1,000 万円以下の罰金に処するとの規定があり、ＳＣ制度においても、同程度の罰則が設けられる見込みである[4]。

3――企業から見たSC制度

ＳＣ制度は、米国や英国のほか、ドイツやフランスなどの欧州諸国、豪州や韓国などのアジア諸国でも導入されている。民間人を対象としたＳＣ制度を導入していないのは、実のところ主要国の中で日本だけである。そのようなＳＣ制度が日本で導入された場合、企業が得られる主なメリット・デメリットは、以下のように整理される。

1｜制度導入のメリット（ ビジネス機会の拡大 ／ 産業競争力の向上 ／ セキュリティの強化 ）

１つ目は、ビジネス機会の拡大である。例えば、地経学研究所のアンケート調査[5]によると、「日本に現状セキュリティ・クリアランス制度がないことにより、参画することのできなかった案件や会議などはありますか」との質問に対し、回答した 73 社のうち 40 社（54.8%）が「これまでなかったが、将来的に参画できないことが予想される」と回答している。

海外の政府や企業との取引においてＳＣを保有していることが、入札参加や会議出席の前提条件となっているものもあり、ＳＣが無いと声すら掛からない案件も存在する。日本でＳＣ制度が導入され

---

2 2021 年末時点の資格保有者は、公務員 130,853 人（全体の 97.4%）および一部民間企業の職員 3,444 人
3 國分俊史「エコノミック・ステイトクラフト 経済安全保障の戦い」日本経済新聞社 2020 年 5 月 8 日
4 日経新聞「経済安保の機密漏洩に罰則　高市氏、改正法案提出を明言」（2023 年 8 月 24 日）
5 地経学研究所「経済安全保障 100 社アンケート結果」（2022 年度調査）

Copyright ©2023 NLI Research Institute All rights reserved

れば、日本企業がこのような案件に参入することも容易になる。

２つ目は、産業競争力の向上である。日本にＳＣ制度が導入されれば、企業は機微に触れるという理由で、これまで拒まれて来た機微情報にアクセスすることが可能となる。共同開発に臨む他国研究機関と、より踏み込んだ協力ができるようになる。とりわけ、軍事転用可能な人工知能やドローン、量子コンピュータといったデュアルユース技術は、民生分野でも重要かつ有望な技術となっており、そのような分野で機微情報の共有が進むことは、今後の成長機会を広げるうえで意義は大きい。

また、社会全体がデジタル化・情報化する中で、サイバー・セキュリティに対する重要性も増している。デジタルのシステムや製品に関して、市場投入後に発見される脆弱性のうち、修正プログラムが開発されて、一般開示される前のものは「ゼロディ情報」と呼ばれる。このゼロディ情報は、サイバー攻撃の強力な手段にもなる。ＳＣ制度がなければ、この機微情報へのアクセスが制限されることになり、リスク管理面で他国研究機関や企業に劣後することにもなりかねない。実際、米国では「自動運転に対するサイバー攻撃防御（AI、地図情報、画像解析技術 など）」に関するゼロディ情報は、「テスラやGMには開示されるがシリコンバレーに出入りしていても日本企業には開示されない可能性」が大きいといった指摘もある[6]。ＳＣ制度の導入は、経済安保面で基幹インフラの安全性・信頼性確保が重要になる中で、製品の信頼性を高め、企業のブランド価値を向上させるものとなる。

さらに、海外のＳＣ資格保有者を持続的な人材として、企業内部で資源化できる意義も大きい。例えば、米国では日本企業に転職した場合、ＳＣの更新を認めていないため、資格保有者が更新のタイミングで転職している事態があるとされる[7]。ＳＣ制度の相互承認が図られるようになれば、日本企業に在籍しながら海外のＳＣ資格を継続できる可能性も高まる。企業はＳＣ資格保有者を通じて、海外の機密情報にアクセスし、その知識を企業の研究開発に活かすことが可能となる。

３つ目は、セキュリティの強化である。上述のゼロディ情報を用いたサイバー・セキュリティ面の強化に加えて、自社で機微情報を扱う人や施設の適格性が事前に分かるため、重要な情報が漏洩するリスクを低減することができる。例えば、直近の 2023 年６月には、産業技術総合研究所の上級主任研究員が、フッ素化合物に関する技術を中国企業に漏洩させる事案が発覚した。この事件で漏出した情報は、安全保障上の機微情報ではなかったとされるが、情報管理の重要性が広く理解された。これまでにも、技術者が退職後に機密情報を持って他国企業に転職し、最先端技術を流出するといった事件が起きて来た。ＳＣ制度では、情報漏洩に対する罰則も強化されることから、抑止力として機能することにもなる。

2｜制度導入のデメリット（ コストの増加 ／ 制約要因の追加 ）

１つ目は、コストの増加である。従業員がＳＣ資格を取得する場合、通常であれば企業が審査費用を負担することが想定される。米国では、政府がＳＣ制度の運用に必要な資金を拠出するため、個人や企業にコストが掛からない仕組みとなっている。一方、豪州では、運用コストを削減するため、企業が審査コストの一部を負担する仕組みとなっている。審査費用は、機密情報へのアクセス・レベル

[6] 杉田定大「米中新冷戦の中での日本企業の生き残り戦略（2020 年 10 月 6 日）
[7] 國分俊史（同 2020）

 Copyright ©2023 NLI Research Institute All rights reserved

に応じて変わり、毎年見直される。2023年時点における初期審査費用は、保護された機密情報へのアクセスが許可される「Baseline」では884豪ドル(約８万円)、特定の状況下で一時的に“TOP SECRET”へのアクセスが許可される「Negative Vetting Level １」では1,355豪ドル（約13万円)、断続的な“TOP SECRET”へのアクセスが許可される「Negative Vetting Level ２」では2,486豪ドル（約24万円)、非常に機密性の高い情報にアクセスすることも許可される「Positive Vetting」では15,280豪ドル（約145万円）である。資格には有効期限があり、７年から15年で更新する必要がある。日本でのコスト分担がどうなるかは、今後の設計次第となるが、国の財政事情を考えると、企業に追加的なコスト負担が生じる可能性は相応に高いと思われる。

加えて、従業員がＳＣ資格を取得するためには、企業の情報管理体制も厳しく問われるようになる。機密情報の生成・受信・保存などを行う場合には、機密情報を扱う専用の区画の設置や入退室管理システムを導入するなどして、物理的なセキュリティを高めることが必要であり、基本的なネットワーク・セキュリティ（サイバー・セキュリティ）を強化することも求められる。また、機密情報を扱うには、機密情報を保護・破棄・配布する管理プロセスが必要であり、その手順を順守する体制も構築しなければならない。このような体制作りには、コストが掛かることが予想される。

２つ目は、制約要因の追加である。例えば、適切な情報管理の徹底には、機密情報を扱う従業員はＳＣ資格を保有している必要があるが、それは企業における人員配置の柔軟性が、一部で影響を受けることを意味する。米国の場合、セキュリティ許可を受け取るまでには、すべてが順調に行った場合でも半年から１年ほど掛かる。企業はその間、人材をフル活用できない状態に置かれる。

また、他国からの影響が懸念される場合、取引関係やガバナンス構造の見直しを迫られる可能性もある。それらは企業の自由な経済活動を阻害し、政府の民間への関与を強めるものとなる。

4――企業における取組み

日本全体で見れば、ＳＣ制度は諸外国との競争条件を揃える制度として、メリットが大きな制度となる可能性は高い。ただ、コスト面を考えると、負担に見合ったメリットを得られるのは、大企業を中心とした基幹インフラ事業者や、公官庁との取引関係を持つ一部企業に限られる可能性はある。

企業としては、自社における影響を見極めることが、ＳＣ制度導入を見据えた対応の第一歩となる。企業内に海外のＳＣ資格保有者がいるか否かを確認し、その価値について再考する。ＳＣ制度と自社ビジネスとの関係を整理し、企業に及び得る影響を整理しておくことが必要である。ＳＣ制度から恩恵を受けられると考えられるのであれば、法施行後の資格申請に向けて準備する。ＳＣ制度の対象となる人や施設を把握し、事前に個社独自の適格性審査をしておくことは、迅速な資格取得に向けて有効だろう。その際、情報漏洩に関して対策に不備[8]があれば、対策を講じておくこともできる。米国のＳＣ制度では、施設クリアランスにおいて「機微情報を扱う従業員に加え、取締役会会長、ＣＥＯま

[8] 経済安全保障推進法では、基幹インフラ事業者として、電気、ガス、石油、水道、鉄道、貨物自動車輸送、外航海運、航空、空港、電気通信、放送、郵便、金融、クレジットカードの14業種を指定している。

 | Copyright ©2023 NLI Research Institute All rights reserved

たは社長、および担当役員もセキュリティ・クリアランスを保有すること」も要件の１つとなっている[9]。制度詳細が明らかになった際には、人材配置の観点から対象者を確認することが肝要である。

5――おわりに

地政学的な緊張は、グローバルな経済環境を激変させた。多極化に向かう世界の潮流を踏まえれば、これまでの制約のない形でのグローバル化や自由貿易は、もはや難しくなったと考えざるを得ない。少なくとも、経済効率性だけが重視された在り方は変わり、企業は自らのリスクを管理するために、経済安全保障が経済を規定していく在り方を受入れ、対応を進めて行かなければならない。ＳＣ制度の導入は、まさにその一例だと言える。

企業にとってＳＣ制度は、コストを増し制約を課すという意味ではデメリットであるが、不確実性が高まる時代に、国家のインテリジェンス情報を活用し、産業競争力を高め、セキュリティの強化などを図れるという意味ではメリットである。企業は信用や信頼という価値観の比重が高まる世界で、この制度をうまく活用していくことが求められる。

今年６月に閣議決定された「経済財政運営と改革の基本方針 2023」（骨太の方針）には、ＳＣ制度について「主要国の情報保全の在り方や産業界等のニーズも踏まえ、セキュリティ・クリアランス を含む我が国の情報保全の強化に向けた法制度等の検討を更に深め、速やかに結論を得る」と記載された。有識者による論点整理が終わり、これから制度の詳細な設計が始まることになる。法案成立・施行には、まだ少し猶予があることから、今のうちに対応を検討しておくことが肝要である。

【参考文献】

・國分俊史「エコノミック・ステイトクラフト 経済安全保障の戦い」日本経済新聞社 2020 年 5 月 8 日
・杉田定大「米中新冷戦の中での日本企業の生き残り戦略（2020 年 10 月 6 日）
・一般社団法人日本経済団体連合会「Action(活動) 週刊 経団連タイムス No.3591」（2023 年 5 月 25 日）
・内閣官房 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「中間論点整理」（2023 年 6 月 6 日）

9 一般社団法人日本経済団体連合会「Action(活動) 週刊 経団連タイムス No.3591」（2023 年 5 月 25 日）

（お願い）本誌記載のデータは各種の情報源から入手・加工したものであり、その正確性と安全性を保証するものではありません。また、本誌は情報提供が目的であり、記載の意見や予測は、いかなる契約の締結や解約を勧誘するものではありません。