セキュリティ・クリアランス制度

民間企業の活躍領域拡大へ

MS&ADインターリスク総研株式会社
基礎研究部 受託調査グループ
マネジャー上席研究員　土居 英一（どい えいいち）

要旨

- 第213回通常国会で審議される予定のセキュリティ・クリアランス制度（以下、「SC制度」）を定めた法案が注目されている。
- 今般のSC制度は、政府の持つ経済安全保障上重要な情報を共有・開示する対象となる人物や施設を特定・管理する制度である。
- 国家安全保障のための制度であるが、企業の事業領域拡大等が期待できる制度でもある。企業は活用可能性を検討すべきである。
- 法案が開示されていない2024年2月中旬の情報に基づき、SC制度の必要性、立法化に向けた検討状況、要配慮課題、企業における活用イメージ等の情報を提供する。

1 経済安全保障強化のため注目されてきたSC制度

2022年末に国家安全保障戦略が閣議決定された。戦後もっとも厳しく複雑な安全保障環境に直面しているとしつつ、「領域をめぐるグレーゾーン事態、民間の重要インフラ等への国境を越えたサイバー攻撃、偽情報の拡散等を通じた情報戦の恒常化」、「国家安全保障の対象が、経済、技術等、これまで非軍事的とされた分野まで拡大」といった背景が指摘され、経済安全保障の強化が明記された。

防衛および経済安全保障に関連する領域の拡大や、対象技術が急速に進展する中、民間企業の役割が拡大している。また、同盟国・同志国との連携がより重要となり、外国政府が保有している情報を民間企業に共有・開示する枠組みの必要性も高まっている。

経済安全保障については2022年5月に経済安全保障推進法が成立し、①重要物資の安定的な供給確保（サプライチェーン強化）、②機関インフラ役務の安定的な提供確保、③先端的な重要技術の開発支援、④特許出願の非公開（秘密特許）といった4点がフォーカスされた。同法は結果的に4点に絞られたものの検討段階からSC制度の重要性は確認されており、また、衆議院・参議院ともにSC制度構築の検討について同法成立時に附帯決議されている。

このような背景・経緯を踏まえ、2024年1月からの第213回通常国会においてSC制度を定める法案（法律名称、「重要経済安保情報の保護および活用に関する法律」）が審議される予定である。なお同法律は、経済安全保障推進法の改正という形で検討されてきたが、上記の通り独立した法律となる予定である。

2 SC（セキュリティ・クリアランス）制度とは

SC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」）にアクセスする必要がある者（政府職員および必要に応じ民間事業者等の

従事者）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。ただし、実際にアクセスするには、当該情報を知る必要性（Need-to-Know）が認められることが前提となる。また、民間事業者等に政府から当該情報が共有される場合には、民間事業者等の保全体制（施設等）の確認である施設クリアランス等も併せて実施される[注1)]（図1）。

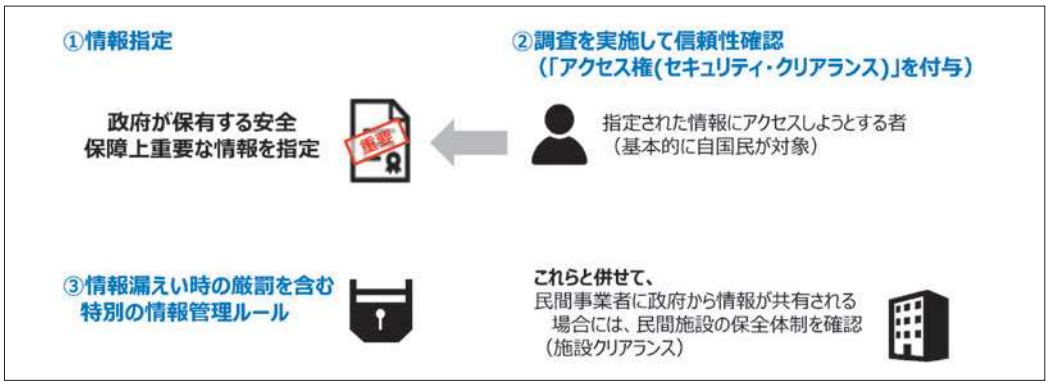
G7諸国で経済安全保障に関連するＳＣ制度が無いのは日本のみとなっている。多くの先進国では既に普及した制度であり、その点では日本は遅れているといえる。米国のクリアランス保有者は民間を含め400万人以上、そのほかの主要国でも数十万人以上いるとされる。官民の割合も米国では官対民がおよそ7対3となっている。

わが国でも防衛、外交、特定有害活動防止、テロ防止の4分野に限定された特定秘密保護法に基づくセキュリティ・クリアランス制度により特定秘密を取り扱えるものがいるが、総数は約13万人にとどまり、そのうち民間の割合はわずか3%である。

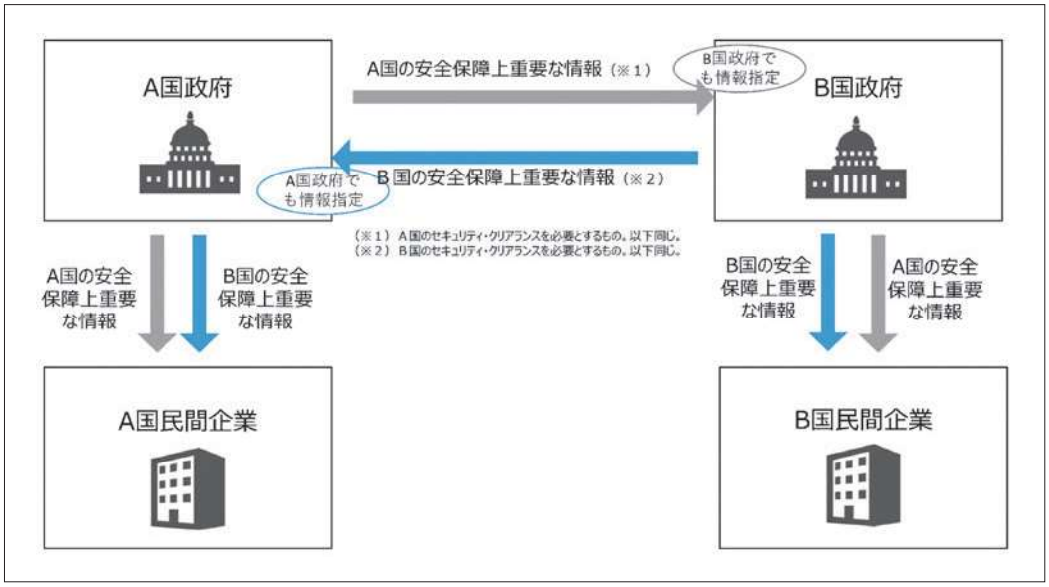
3 主要国との間で通用する実効性のある制度が目指されている

後述するＳＣ制度のニーズの項でも紹介するが、ＳＣ制度を有する他国の民間事業者が扱える同盟国・同志国等のＣＩの入手を日本の民間事業者は認められず、他国との共同開発や最新技術情報交流に参加できない例がある。

そのため、今般のＳＣ制度は、自国で通用するだけでなく、主要国との間で信頼され実効性のある制度となるべきである。なお、国家間の安全保障上重要な情報のやりとりの枠組み構築も必要と考えられており、そのイメージは図２のとおりである。原則、民間企業は政府間のやりとりを通じて情報を自国政府から提供される方向である。



【図1】SC（セキュリティ・クリアランス）制度の概要
（出典: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」）



【図2】安全保障上重要な情報のやりとりのイメージ
（出典: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」）

4 法案のポイント（2024年2月中旬以前の報道等より）

現時点で把握できる法案のポイントは以下の通りである。ただし、これらは国会で変更される可能性がある。

①特定秘密保護法との棲み分け

経済安保の情報に関する適格性評価は、特定秘密保護法と新法の二段構えとなる。機密性が高い「安全保障に著しい支障を与える情報」は特定秘密保護法の制度で対応する。同法は機密漏えいに懲役10年以下の罰則を科す（表1）。

【表1】セキュリティ・クリアランス制度案のイメージ（2024年2月中旬時点）

特筆すべき法体系・対象情報	特定秘密保護法と新法の二段構え 重要経済安保情報の新設
調査主体	首相を機関のトップとする一元的機関
調査項目例	犯罪・懲戒歴、情報の取り扱いの経歴
調査結果・評価・判断	調査結果は10年間有効 機密情報を保有する各省庁が評価・判断実施
罰則	重要経済安保情報を漏えいした場合、5年以下の拘禁刑か500万円以下の罰金、またはその両方

（MS&ADインターリスク総研作成）

②新法で新たに定められた機密情報

①よりも機密性の低い「支障を与える情報」を、新法で定める「重要経済安保情報」とする。

③重要経済安保情報の例

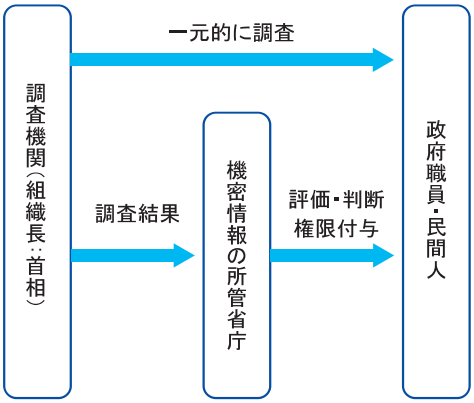
「重要経済安保情報」に指定されるものとして、水道や鉄道などを念頭に「経済活動の基盤」であるインフラに関する情報を挙げている。外国のサイバー攻撃からインフラを守るための計画、研究が念頭にあるとみられる。「革新的な技術」も対象としており、AIなどの情報が該当するとみられる。民間企業にとっては重要経済安保情報の取扱資格を持つことで、これらの分野で国際共同研究に加われるシーンが拡大する利点がある。

④重要経済安保情報指定の有効期間

指定の有効期間は5年間で、更新可能としている。通算の有効期間は30年間で、内閣の承認を得れば、さらなる延長も可能としている。

⑤情報を扱う資格の調査

政府は適格性評価の資格を付与するか審査する際に対象者（政府職員や情報提供を受ける民間企業の従業員）の身辺を、本人の同意を得たうえ調査する。調査は行政機関の長の要請を受けて首相が一元的に実施する仕組みとする。内閣府に専門機関を置く方向である。首相は調査結果を行政機関の長に通知する（図3）。



【図3】適正調査・評価・判断プロセスのイメージ（2024年2月中旬時点）
（MS&ADインターリスク総研作成）

⑥情報を扱う資格の調査結果の評価・判断

機密情報の提供に適した人物かどうかは各省庁が最終的に評価・判断する。調査結果の有効期間は10年以内とする。転職した場合などでも10年以内なら新たに資格を付与する際の再調査を省くことができる。

⑦調査項目例

犯罪・懲戒歴、情報の取り扱いに関する経歴、本人や配偶者の国籍などを含む方向にある。分類すると1.スパイなど特定有害活動やテロとの関係、2.犯罪・懲戒歴、3.情報の取り扱いに関わる非違の経歴、4.薬物の乱用歴、5.精神疾患の有無、6.飲酒の節度、7.借金を含む経済状況などとなる。

⑧情報漏えい時の罰則

重要経済安保情報を漏えいした場合の罰則は、最大で5年以下の拘禁刑か500万円以下の罰金、またはその両方とする。

5 民間事業者等が保有する情報は対象になるか

昨今、デュアルユース（軍民両用）と呼ばれる民生・軍事双方に活用される技術等に注目が集まっている。これは、民間のほうの開発がむしろ進んでいるＡＩ、半導体などの技術、およびＧＰＳのように元来軍事目的であったが民生利用されるようになった技術を指す。

それでは軍事に活用される可能性のある民間の有する技術情報等がすべて重要経済安保情報に指定されるのであろうか。有識者会議[注2)]の最終とりまとめは以下の内容となっている。

「秘密指定の対象となるのは、政府が保有している情報であり、政府が保有するに至っていない情報を政府が一方的に秘密指定することは想定されない」

「政府が民間事業者等から提供を受けて保有するに至った政府保有情報の取り扱いについては、秘密指定すること自体が妨げられるものではないものの、秘密指定の効果は、政府との間で秘密保持契約を締結し、政府が秘密指定している情報と告げられてその提供を受けた者のみおよび、かつ、それは、従前から民間事業者等が保有していた情報と重なる部分がある場合には、当該従前からの保有情報の管理に規制が加わるものではないと整理すべきである」

6 SC制度のニーズ

⑴国家のニーズ

- 安全保障環境が厳しさを増すにつれ、国家安全保障における情報能力の強化も重要さを増しており、経済安全保障分野においてもＳＣ制度を含むわが国の情報保全の強化のニーズが高まっている。
- 民生・軍事の技術の境は曖昧となっており、もはや防衛・外交等の情報だけでなく、経済・技術の情報も安全保障上の重要さを増している。

⑵民間企業のニーズ

経済界からは以前よりＳＣ制度導入について前向きな意見が表明されていた。たとえば経済同友会は2022年2月に、わが国の技術優位性確保のため同盟国・同志国との共同研究を推進・強化すべきで、そのためにもＳＣ制度の導入を政府は検討すべきといった意見を示している。

そのほか、企業からのＳＣ制度を希望する声を以下に例示する[注3)]。

- 海外企業から協力依頼があったものの機微に触れる情報を十分に得られなかった。ＳＣ制度があれば踏み込めた取り組みになったと考える。
- 自衛隊装備品と関係ない国際共同開発で、SC保有者がいなかったため、秘密指定されていないが管理の必要な情報「ＣＵＩ」（Controlled Unclassified Information）の開示に時間を要することや、周辺情報の開示に留まったことがあった。
- デュアルユース技術の会議における情報交流の場への参加資格がSC保有者のみであったため、参加できず最新の技術に触れることができなかった。
- 宇宙分野の海外政府の入札に際し、説明会の参加要件がＳＣ保有であった。商業利用分野でもＣＩが含まれているため詳細がわからない等の不利な状況が生じている。
- サイバーセキュリティインシデントの多様化にあたり、政府や諸外国の保有情報が共有されれば、企業単位、ひいてはわが国全体のセキュリティレベルの向上につながる。
- ＳＣ制度の導入により、将来的に、たとえば衛星・ＡＩ・量子・Beyond5G等の次世代技術の国際共同開発の可能性が拡充すると思う。

これらから、国との事業等に際する場合以外のシーンでも、SCが信頼性の証明となることを企業は期待していると窺える。同時に、新しい制度が米国をはじめとする主要国にも認められ信頼されるものでなくてはならないと考えていることも窺える。

7 日本企業が諸外国の機密情報を共有できるための基礎条件

それでは、日本企業が諸外国の機密情報を共有できるようにするにはどうしたらよいのであろうか。日本企業が諸外国の機密情報を共有できるための基礎条件は、永野（2023）によると、次のように述べられている。

「日本政府が、①国家安全保障に関連する科学的、技術的、経済的事項や、重要インフラ等に関するセキュリティ・クリアランス制度を法制化し、②これらの機密情報を日本国と米国をはじめとした外国政府との間における協定で情報共有を承認しあえば、③セキュリティ・クリアランス要件を満たした日本企業も、これらの機密情報を共有することができる」

さらには、有資格者・施設が相手国から信頼されるに足る実効性のある制度であるため、調査・評価の内容やレベル、その後の管理状況、漏えい時の罰則が想定する諸外国の納得のいく実質的同等性を確保することも肝要となろう。

8 海外民間事業の制度活用

米国等においては、特に機密情報を扱う事業や国家安全保障に重要な事業においては、ＳＣの取得は一般的なようである。具体的には、防衛関連事業以外にも、サイバーセキュリティ事業、情報・通信事業、航空宇宙事業、核関連事業、コンサルティング事業（政府機関や国家安全保障問題に関連する契約を扱う企業等）、金融事業（政府契約に関連する金融サービス等）、法律事務所（国家機密に関連するケース等）、研究開発（国家安全保障に影響を与えうる技術やデータを扱うプロジェクト関連等、大学も含まれる）にて活用されているようである。また、金融業、ＩＴ関連業、電気機械製造業、製薬業、エネルギー関連業等の政府取引を含まない領域で、いくつかの企業はＳＣ制度のような内部プロセスを設けているようである。

9 SC制度によるリスクはないのか

ＳＣ制度にもリスクは存在する。以下の通り制度に関連するリスク例を挙げる。制度設計や運用にて配慮すべきリスクと考える。

制度設計上、最も注目されるリスクのひとつは、身辺調査で集める個人情報の管理やプライバシー侵害への対応である。

制度化により機密情報を保有できる民間人の人数は圧倒的に増加する可能性があるものの、調査・評価はプライバシーの問題に大いに踏み込むため、個人がオプトアウトできる権利対応や調査情報の管理等は厳格に運用されるべきである。

日本で国籍などを問うて選別することもリスクとして懸念する。日本では国籍・民族等に関連した人権問題は極めてデリケートに配慮すべき事柄である。国籍の多様化を企業が進めるなかで運用時にも企業は当事者として丁寧な配慮が必要であろう。

米国のＳＣ制度の調査・評価では、外国の影響、外国の利益を優先する傾向、外国政府や外国法人との接触といった項目が重視されているとみられる。同盟国・同志国以外との関係を考えるうえで、米国等から実質的同等性を認めてもらえるかどうかもリスクと考える。

他国の諜報機関所属者が紛れて制度認証を得て、国家の安全保障関連の機密を他国へ漏らすリスクも考えられる。国だけでなく企業でも注意する必要が生じうる。

調査された個人の機微な情報を所属企業が知るべきでないため、国だけでなく企業側も企業内で調査事項を聞き出すことの無いよう内部統制すべきであろう。

ＳＣを得られなかった際、ＣＩを取り扱う業務に就けないことはやむをえないものの、同意拒否や評価結果等を理由に不合理な配置転換などの不利益な扱いをすべきでない。企業による調査結果（ＳＣ適用・非適用）等の目的外利用のリスクにも、法に記載されるかどうかによらず道義的に厳格に対応すべきである。

国の機密情報の秘匿性が高まることで生じかねない汚職等のリスクも考えられる。

10 SC制度導入に向けて

経済・技術の情報が組織や国同士の安全保障や各種競争に重要であることは周知の事実である。ただ、その重要な情報の種類が広がっていることが今回のＳＣ制度導入の肝である。

第四次産業革命の時代と呼ばれ始めて久しい。コンピューターの情報処理能力の格段の進化等をベースに、多様な技術が同時多発的に急速な進化を遂げている。そしてついにはそれらの技術の社会実装が進む段階に入っている。ＲＮＡワクチン等の遺伝子工学、生成ＡＩ、宇宙ビジネス、ドローン等である。中長期的には、次世代のＡＲ/ＶＲ、自動運転、量子コンピューター等の本格的な実装も待ち構えている。このような技術革新等を踏まえれば、社会のリスク、たとえば、今般フォーカスした経済安全保障に関するリスクも多様化するのは当然であろう。また、その多様化に民間企業も積極的に対処できるかどうかは、各企業の問題にとどまらず、国家レベルで重要である。ひいては、ＳＣ制度はわが国と同盟国・同志国を含めた陣営の強化に必要である。今回のＳＣ制度導入は、わが国においてこれ以上制度化が遅れてはならないという背景があったと考える。

ＳＣの取得は日本や諸外国の国家機密レベルの情報を活用するビジネスチャンス拡大につながりうる。さらには、無論、違法な活用はできないものの、なんらかの形で新しい自社の価値創造の糧ともなりうる。したがって、民間の企業におかれては、自社での制度の直接・間接[注4)]の利用可能性を検討されるべき

と考える。ただし、有識者会議により「必要があれば専用の区画や施設も設けていくべきである」と述べられている等、CIの管理コストなどの丁寧な検討は必要となろう。

安全保障関連の機密情報の適切な管理運用は、SC制度ができれば万事うまくいく問題ではない。同時に、制度が軽薄化し適切に運用されない、形骸化し本質を欠いた運用となる事態も避けられるべきである。

以上

参考文献・資料等

- 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「議事録」、「中間論点整理」、「最終とりまとめ」2023-2024年<https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html>（最終アクセス2024年2月14日）
- 永野秀雄「米国におけるセキュリティクリアランス制度の基本情報」2023年7月

注）

1）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「最終とりまとめ」

2）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

3）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」の情報をMS&ADインターリスク総研が要約

4）間接というのは、CUIを含めた管理への拡張や、政府取引を含まない領域の重要情報に対するSC制度のような内部プロセスの導入を指している