経済安全保障推進法と民間セキュリティクリアランス制度の導入

大澤　淳

Economic Security Promotion Act and the Introduction of a Security Clearance System in Private Sector

Jun OSAWA

はしがき

近年、日本では「経済安全保障」という言葉が頻繁に用いられるようになった。米中の戦略的競争が激しくなり、経済面でも、経済的な脆弱性の武器化（経済的威圧）や先端技術の囲い込みが起こるようになり、経済安全保障の確保が大きな課題となっている。重要物資・先端技術をめぐる国家間競争の深刻化、そしてサイバー空間での攻防の先鋭化により、国家の安全保障はもはや軍事や外交だけでは語れなくなっている。今や、かつての米ソ冷戦期のようなDIME（外交・情報・軍事・経済）全てを用いた体制間競争の新冷戦の様相[1]が見られるようになってきている。そのような状況では、エネルギーや半導体などのサプライチェーン、通信や重要インフラを支える技術、さらにはそれらに関する機微な情報の保全は、国家の安全保障を左右する重要な要素となっている。

こうした状況のもとで、日本政府が導入を準備している制度の一つが「民間セキュリティ・クリアランス制度」である。これは、政府のみならず民間事業者も含めて、安全保障上重要な情報を取り扱う者について、その適性を政府が事前に評価し、「この人（あるいは組織）には機密性の高い情報を扱わせても大丈夫だ」という認証を与える仕組みである。

本稿では、まず経済安全保障やセキュリティ・クリアランス制度が必要となった国際環境の変化について述べ、次にセキュリティ・クリアランス制度の基本的な考え方を整理した上で、その制度が日本で導入されるに至った背景、既存の特定秘密保護法との関係、新たに制定された「重要経済安保情報の保護及び活用に関する法律」の概要と特徴を確認する。さらに、民間セキュリティ・クリアランス制度の意義と、プライバシーや労働法制への影響など、今後の課題についても検討したい。

第１節　国際環境の変化と経済安全保障、セキュリティ・クリアランスの必要性

１．グローバリゼーションの終焉と新冷戦

経済安全保障を巡る議論が、2019年以降日本国内で急速に進んだ背景には、国際政治上の大きな構造変動がある。第二次大戦後の冷戦期には安全保障が経済より優越する構図であったが、冷戦終結後のグローバル化の進展により、各国はサプライチェーンや投資などを通じて深く相互依存を強め、経済が安全保障よりも優先される時代が続いた。1989年に冷戦が終焉してから2019年頃までの約30年は、ソ連の崩壊による米国一強体制の成立と、2008年のリーマンショックを境目とした多極化の時代に分けることができる。この時代は、国際政治上の大きな緊張が解け、安全保障の論理よりも経済の論理が優先され、ヒト・モノ・カネが活発に国境を越えて自由に移動するグローバリゼーションが特徴であった[2]。

しかし、このグローバリゼーションの時代が、中国の台頭と共に終焉を迎えている。エコノミック・ステイトクラフトや貿易管理の厳格化などのいわゆる「経済安全保障」を巡る議論が諸外国で活発化してきたのも、中国の台頭により、再び国際政治が「体制間競争」に向かうというナラティブが形成されているからである。日本が初めて時代の変化を経験したのは、2010年に中国が対日レアアースの輸出規制を行った事件であった。これを境に、経済的な依存関係それ自体が「武器化」される事

1　Sanger（2024）pp. 436-437.

2　Stiglitz, Joseph E., (2002)

態が顕在化するようになった。

中国を競争相手と位置づけ、冷戦期のような「体制間競争」が再び起こるとの認識の変化の潮目となったのは、米国のペンス副大統領（当時）が2018年10月にハドソン研究所で行った対中戦略演説である[3]。同演説でペンス副大統領は、中国が政治、経済、軍事的手段とプロパガンダを用いて米国に対する影響力と干渉を強め、人権や宗教でも自由を抑圧しているとして、中国との長期戦を覚悟し、経済・戦略的関係をリセットすることを示唆した。

さらに、2021年には、冷戦期のケナンの「長文電報」[4]にあたる論文が、米国のシンクタンク、アトランティック・カウンシルのホームページに掲載された。同論文は、「より長い電報：アメリカの新対中戦略に向けて」[5]と題するもので、ケナンの「長文電報」を意識して米国の元政府関係者が匿名で執筆し、米国を凌駕しようという中国の長期戦略に対抗する米国の新対中戦略を同盟国と共に実施すべき、と訴えている。

2018年のペンス米副大統領の演説や、2021年の“The Longer Telegram”などは、いわゆる「新冷戦」的な構造の到来を示唆している。20世紀の冷戦は社会主義対自由民主主義の戦いであったが、21世紀の新冷戦では、「デジタル権威主義」と「民主主義＋自由経済」との体制間競争が展開されることとなろう。

米国では安全保障を確保する手段を、DIMEを組み合わせて考えるように教育される。このDIMEは、外交(Diplomacy)のD、情報(Information/Intelligence)のI、軍事(Military)のM、経済(Economy)のEを組み合わせたものである。生存をかけた体制間競争は、このDIMEをすべて動員しての真剣勝負となる。

このDIMEの枠組みの中で、経済力や技術力の確保、サプライチェーンや技術の囲い込み、サイバー空間における先端技術の窃取などが、国家の生存に直結する課題となっている。したがって、経済や技術に関する情報も、もはや単なる「ビジネス情報」ではなく、安全保障上の重要情報として扱う必要が生じているのである。

2. サイバー空間の「安全保障領域化」

2018年のペンス演説では、「中国共産党は「中国製造2025」計画によって、ロボット、バイオテクノロジー、人工知能など最先端産業の90％を支配することを目指しており、（中略）米国の知的財産をあらゆる手段を用いて手に入れるように指示してきた」との警戒感が示されているが、とりわけサイバー空間は、その最前線と言っても良い状況にある。実際にサイバー空間において顕著となっている米中対立の焦点は、米国の技術力・経済力の基盤である知的財産を中国がサイバー攻撃で窃取している点にある。

中国のサイバー攻撃は、知的財産やビジネス秘密の窃取を目的に、先進国の民間企業、研究所、大学などを標的としている[6]。このようなサイバー攻撃は、先進国の保有する先端技術の不公正な強制移転をもたらし、先進国の技術優位を脅かしつつある。このような不公正な手段で入手した技術を用いて、途上国向けの製品を中国企業が製造して輸出している事例も見られるようになっており、自由で公正なルールに基づく自由貿易体制の信頼も揺るがしつつある。

こういったサイバー攻撃で利用されるのが、ネットワーク境界に設置されたITセキュリティ機器の脆弱性である。このようなセキュリティ機器は多くの組織で利用されており、同じIT機器を使用している組織に対しては、同じ手法でサイバー攻撃を行うことができるため、非常に効率的にサイバー攻撃を行うことが可能となる。

さらに、台湾有事を念頭に置いた、中国からの準備行為とみられる偵察・侵入活動もサイバー空間で活発化している。このサイバー攻撃の特徴は、政府機関や基幹インフラ企業等のネットワークに侵入するものの、何も壊さず、ただ潜伏することを目的としている点にある。このようなサイバー攻撃は、有事の際の命令一下、侵入したネットワークを破壊する目的を持って、平時に偵察・侵入行為を行っている、と考えられる。

米国では、2023年春頃から、中国の人民解放軍との関係が疑われる攻撃グループ「Volt Typhoon」が、VPN機器の脆弱性を使って、重要インフラ企業等にサイバー攻撃を行っていることが明らかになっている[7]。また、通信企業、政府、交通機関などのネットワークを標的とした侵害活動も明らかになっている。2025年8月、米、

---

3 “Vice President Mike Pence's Remarks on the Administration's Policy Towards China,” at Hudson Institute, October 4, 2018. https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018

4 Kennan (1947)

5 Anonymous(2018)

6 大澤（2021）

7 Microsoft Threat Intelligence, “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques,” May 24, 2023.

英、豪、加、NZ、独、伊、蘭、チェコ、フィンランド、ポーランド、スペインおよび日本の13カ国は、中国政府が支援するサイバー攻撃グループ「Salt Typhoon」が、こうした侵害活動を行っているとして、国際共同非難を行った[8]。

また、サイバー空間は、情報戦・影響工作の舞台ともなりつつある。影響工作は、社会の分断や不安定化、国家の意思決定への介入を目的として、SNS上の偽情報の流布等を用いて、競争相手国の意思決定に影響を与え、行動の変容を促す。中国やロシアなどの権威主義国が、世界規模で影響工作（FIMI: 外国からの情報操作と干渉）を行っていることが観測されている[9]。

いまやインターネット空間だけでなく、重要インフラに接続された制御システムや、個人の認知空間、民主主義プロセスに関わる情報環境まで含めて、広い意味での「サイバー空間」が安全保障の対象となりつつある。

攻撃主体は国家だけでなく、国家と関係を持つハッカー集団、犯罪組織、さらには個人にまで多様化し、攻撃手法も高度化している。最近では、一度ネットワークに侵入すれば、多数のシステムを「一網打尽」にできるような攻撃も存在し、脆弱性情報の管理と共有が極めて重要になっている。この脆弱性情報の共有との関係で、民間セキュリティ・クリアランス制度は重要な役割を持っている。

日本では、独立行政法人情報処理推進機構（IPA）などが中心となって脆弱性情報の公表・対策を進めているが、脆弱性の公表から攻撃者による悪用までの時間が、最短で24時間程度にまで短縮されているとの指摘もあり、公表前の段階での関係者間の安全な情報共有が急務となっている。こうしたサイバー安全保障上のニーズが、民間も巻き込んだセキュリティ・クリアランス制度の導入を後押ししている。

第２節　セキュリティ・クリアランス制度の基本概念

1. セキュリティ・クリアランスとは何か

セキュリティ・クリアランスとは、国家安全保障上重要な情報を保全するために、重要な情報を扱える「人」および「施設」を指定し、情報の漏洩を管理する制度である。具体的には、次の要素から構成される。

① **情報の区分指定**
まず、政府が保有する情報のうち、安全保障上特に重要であって、漏洩すると国の安全に重大な影響を及ぼしうるものを「機密情報」として指定する。例えば、防衛計画、サイバー防御の詳細、重要インフラの脆弱性情報などが典型である。

② **人のクリアランス**
次に、そうした機密情報にアクセスする必要のある者（公務員だけでなく、必要に応じて民間企業の従業者も含む）について、政府が事前に調査・適性評価を行い、「この人物は機密情報を漏らすおそれが低い」と信頼性を判断した上で、当該者に情報へのアクセス権を付与する。

③ **施設のクリアランス**
情報を扱うのは人だけではない。機密情報を保管・処理する施設や情報システム、組織体制についても、適切なセキュリティ水準を満たしているかどうかを政府が確認し、要件を満たす事業者の施設のみが機密情報を扱えるようにする。

④ **厳格なルールと罰則**
さらに、機密情報の管理ルールを明確に定め、それに違反して情報を漏えいした場合には、刑事罰を含む厳しい制裁を科すことで、情報漏洩への抑止力を確保する。

このように、セキュリティ・クリアランスは単なる「秘密指定制度」ではなく、「誰が」「どのような環境で」「どのような情報に」アクセスできるかを総合的に管理する枠組みである。

2. 保全の対象となる機密情報とは

機密情報とは、外部に知られると組織や個人に不利益・危険が生じる恐れがあるため、情報へのアクセスや利用が厳しく制限されている情報のことを指す。機密情報は、国家安全保障上との関わりで定義されるが、例えば米国では、「漏洩した場合、国家の安全保障や国際関係に甚大な被害を与えるような情報」とされており[10]、現在は、オバマ政権時代の大統領令13526で定義されており、機密保持レベルの必要に応じて、機密（Confidential）、秘密（Secret）、最高機密（Top Secret）の３段階が設定

8　国家サイバー統括室、警察庁「「ソルトタイフーン（Salt Typhoon）」に関する国際アドバイザリーへの共同署名について」（2025年8月27日）。https://www.npa.go.jp/bureau/cyber/pdf/20250827.pdf

9　EEAS] (2025)

10　小谷（2012）162ページ

されている[11]。

英国の場合「英国、または友好国の安全保障や治安に損害を与えるような情報、人命に関わる情報、国際関係に影響を与えるような情報、英国に長期的な経済上の損害を与える情報」と定義されている[12]。英国政府の最新の情報保全規則では、米国と同様に機密保持レベルの必要に応じて、取扱注意（Official）、秘密（Secret）、最高機密（Top Secret）の３段階が設定されている[13]。

日本の場合、米国や英国のような政府統一基準ではなく、後述する特定機密保護法（特定秘密を規定）に加えて、日米相互防衛援助協定等に伴う秘密保護法（特別防衛秘密を規定）、国家公務員法（政府情報の守秘義務を規定）、自衛隊法（防衛秘密を規定）、秘密情報を取り扱う省庁（外務省、防衛省、警察庁）の訓令（それぞれ省庁毎に極秘、秘などを規定）、政府機関の情報セキュリティ対策のための統一基準（機密性情報１～３を規定）で別々に区分が定められており、秘密を漏らしたときの罰則も、それぞれの法令によっている。

日本で民間をカバーする情報保全制度も多岐にわたっており、最も厳しいのは防衛装備品等の秘密を規定した「防衛生産基盤強化法」だが、これ以外に民間企業の従業員による情報漏洩を規定する「不正競争防止法（営業秘密を規定）」、「マイナンバー法（個人情報を規定）」、「貸金業法・割賦販売法（信用情報を規定）」、「原子炉等規制法（特定核燃料物質の防護に関する秘密を規定）」など複数の法律が存在する。

第３節　既存のセキュリティ・クリアランス制度――特定秘密保護法

１．特定秘密保護法の概要

日本にはすでに、セキュリティ・クリアランス制度を定めた法律として、2013 年に成立し、2014 年に施行された「特定秘密保護法」[14]が存在する。同法は、防衛、外交、特定有害活動の防止、テロリズム防止の４分野において、特に秘匿する必要がある情報を「特定秘密」として指定し、その漏えいを防ぐことを目的とした法律である。特定秘密の取扱者に対しては、故意に漏らした場合に最大10年の懲役といった重い刑事罰が定められている。また、それまで政府内で統一的に存在していなかった公務員におけるセキュリティ・クリアランス制度を初めて定めた。同法では、機密情報の取扱者の適性評価の仕組みも制定された。

具体的には、特定秘密の取扱者を「適性評価により特定秘密の取り扱いの業務を行った場合にこれを漏らすおそれがないと認められた行政機関の職員若しくは事業者の従業員又は都道府県警察の職員に限る」と限定した上で、取扱者に対する適性評価手順を定めている。特定秘密の取り扱いが見込まれる者は、あらかじめ７項目（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）について調査を受けることとされ、対象者の同意を得た上で、これらの項目について行政機関の長が評価を実施する[15]。

しかし、この制度は主として防衛・外交など「伝統的」な安全保障分野に限られており、経済安全保障、とりわけサイバーやサプライチェーン、先端技術などに関する情報を包括的にカバーするものではなかった。また、取扱者のほとんどは官側であり、民間事業者の関与は限定的であった点も特徴である。

２．特定秘密保護法と官民情報共有の限界

特定秘密保護法の下でも、安全保障上の特段の必要による事業者への特定秘密の提供の場面で、民間の事業者が一定の形で秘密の取り扱いに関わる場面は想定されていたものの、制度上あくまでも安全保障に限定された状況下でのみ民間への情報共有が可能であり、官民情報共有に用いるには適当な枠組みではなかった。また、罰則の重さや情報の秘匿性ばかりが社会的に注目され、情報保全と民主主義・表現の自由とのバランスをめぐる議論が激しくなったことも、制度の積極的な活用を難しくした側面がある。

こうしたなかで、経済安全保障の観点やサイバー防護の観点で、政府が保有する機密情報や、外国から提供さ

11　Executive Order 13526-Claffidied National Security Information, December 29, 2009. https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information

12　小谷（2012）162 ページ

13　Government Security Classifications Policy, August 5, 2024. https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html

14　特定秘密保護法については、内閣官房の特定秘密保護法関連ホームページ参照。https://www.cas.go.jp/jp/tokuteihimitsu/index.html

15　内閣官房「特定秘密の保護に関する法律の概要」https://www.cas.go.jp/jp/tokuteihimitsu/gaiyou.pdf

れた機密情報についても、官から民へ共有する必要が生じてきた。さらに、国際的な技術協力や共同研究を円滑に進めるためにも、民間側から米国が求めるセキュリティ・クリアランスの制度導入が求められるようになり、民間を含むセキュリティ・クリアランス制度への議論が高まっていった。

第４節　経済安全保障推進法と民間セキュリティ・クリアランス議論の高まり

1．経済安全保障推進法と附帯決議

2022 年（令和 4 年）、日本では「経済安全保障推進法」が制定された[16]。この法律は、戦略物資の確保や重要技術の獲得を通じて、「戦略的自律性」と「戦略的不可欠性」を確保し、我が国の独立・生存・繁栄を経済面から支えることを目的とするものである。具体的には、(1) 重要物資の安定的な供給の確保、(2) 基幹インフラ役務の安定的な提供の確保、(3) 先端的な重要技術の開発支援、(4) 特許出願の非公開に関する 4 つの制度がこの法律によって創設された。

同法の審議過程では、国際共同研究の円滑な推進や日本の技術的優位性の確保・維持のために、「情報を取り扱う者の適性について、民間人も含め認証を行う制度の構築を検討し、法制上の措置も含め必要な措置を講ずるべき」との附帯決議が行われた[17]。これは、民間セキュリティ・クリアランス制度を本格的に検討するよう、国会から政府に求めたものと位置づけられる。

2．経済団体からの間セキュリティ・クリアランス制度導入要請

また、経済界からも、民間セキュリティ・クリアランス制度の必要性を指摘する声が上がった。日本経済団体連合会や経済同友会は、経済安全保障法制に関する意見書の中で、機微な情報を取り扱う国際共同研究や外国政府との契約を行う際に、セキュリティ・クリアランスを受けていることが求められるケースがあることを指摘し、日本も「相手国から信頼されるに足る、実効性のある情報保全制度」を導入すべきだと主張した[18]。

たとえば、先端半導体、量子技術、宇宙・防衛関連技術などの分野では、同盟国・同志国との共同研究開発において、機密情報を相互にやり取りする必要がある。この際、相手国側から見ると、「日本の企業や研究者が、どの程度の水準で情報を守れるのか」という点が重要な判断材料となる。その意味で、セキュリティ・クリアランス制度は、単に「守る」ためだけでなく、「国際協力」「国際共同開発」を行う上で不可欠の要件であるとも言えよう。

第５節　「重要経済安保情報の保護及び活用に関する法律」

1．法律制定への道筋

こうした議論を踏まえ、当時の岸田総理は、2023 年 2 月の経済安全保障推進会議において、「経済安全保障分野におけるセキュリティ・クリアランス制度のニーズや論点等を専門的な見地から検討する有識者会議を立ち上げ、今後 1 年程度をめどに、可能な限り速やかに検討作業」を進めるように指示を出した。この指示を受けて、「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」が 2023 年 2 月から 2024 年 1 月にかけて 11 回開催され[19]、2024 年 1 月 19 日に「有識者会議の最終とりまとめ」[20]を公表した。

2024 年 1 月 30 日、当時の岸田総理は、経済安全保障推進会議で、有識者会議の最終とりまとめを踏まえ、セキュリティ・クリアランス制度に関する新法案を早急にとりまとめ、令和 6 年通常国家に提出する方針を示した。これを受けて、2024 年 2 月 27 日には、「重要経済安保情報の保護及び活用に関する法律案」他の閣議決定が行われ、法律案が国会に上程された。

2.「重要経済安保情報の保護及び活用に関する法律」概要

16　経済安全保障推進法については、内閣府ホームページ参照。https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html

17　令和 4 年 4 月 6 日衆議院内閣委員会。https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000220820220406016.htm

18　日本経済団体連合会「経済安全保障法制に関する意見」（令和 4 年 2 月 9 日）https://www.keidanren.or.jp/policy/2022/015_honbun.pdf
経済同友会「経済安全保障推進法の成立について」（令和 4 年 5 月 11 日）https://www.doyukai.or.jp/chairmansmsg/comment/2022/220511_1641.html

19　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　ホームページ。https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html

20　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」令和 6 年 1 月 19 日。https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf

2024年5月10日「重要経済安保情報の保護及び活用に関する法律」が国会で成立し2025年5月16日から施行されている。同法は、経済安全保障上重要な情報を「重要経済安保情報」として指定し、その保護と、必要に応じた活用を図ることを目的としている。

行政機関の長は、自らの所掌事務に関する情報のうち、公になっておらず、その漏洩が我が国の安全保障に支障を与えるおそれがあるため、特に秘匿することが必要なものを「重要経済安保情報」として指定する。「重要経済安保情報」には、サイバー脅威や対策に関する情報、サプライチェーン上の脆弱性情報、産業・技術戦略に関する分析、国際共同研究開発に関する情報などが含まれると整理されている。特別防衛秘密や特定秘密に該当する情報は除外されており、従来の特定秘密保護法と重複しないよう配慮されている点も特徴である[21]。

この法律の特徴は、「保護」と同時に「活用」を掲げている点にある。行政機関は、我が国の安全保障確保に資する活動を促進するために必要があると認める場合には、一定の基準に適合する事業者（適合事業者）に対して、契約に基づき重要経済安保情報を提供することができる、と規定している。この仕組みにより、例えばサイバー脅威情報やサプライチェーンの脆弱性情報を民間事業者と共有し、防御能力の向上やリスク管理の高度化につなげることが想定されている。

特定秘密保護法と同様、重要経済安保情報の取扱者の制限が規定されており、重要経済安保情報の取り扱いの業務は、原則として、適性評価において重要経済安保情報の取り扱いの業務を行った場合にこれを漏らすおそれが無いと認められた者でなければ行ってはならない、と規定されている。

3. 民間セキュリティ・クリアランスにおける人的クリアランスの仕組み

「重要経済安保情報の保護及び活用に関する法律」では、重要経済安保情報を扱う業務は、原則として、適性評価において「情報を漏らすおそれがない」と認められた者にしか行わせてはならないとされる。この適性評価は、行政機関の長が対象者の同意を得たうえで行い、実際の調査は内閣総理大臣が一元的に実施する形が想定されている。適性評価の有効期間は10年とされ、一定期間ごとに見直しが行われる。

調査内容には、特定秘密と同様の項目が含まれ、犯罪・懲戒歴、情報取扱いに関する非違の経歴、薬物の乱用・影響、精神疾患、飲酒の節度、信用状態などの調査項目が規定されている。また、重要経済基盤毀損活動との関係として、家族や同居人の氏名・国籍・住所といった情報も調査対象となる。この点は、プライバシー保護や差別防止との関係で、今後も議論が予想される部分である。

さらに、同法では個人のクリアランス資格の「ポータビリティ」（持ち運び）制度が導入される。これにより、一度ある行政機関で適性評価を受けて資格を取得した者は、一定期間（10年以内）であれば、別の行政機関の業務に就く際にも、再度ゼロから調査を行うことなく、既存の評価結果を活用できる仕組みとなっている。特定秘密保護法における適性評価との連続性も意識されており、特定秘密の取扱い経験者については、一定期間に限り新法上の適性評価を省略できるとされている。

4. 民間セキュリティ・クリアランスにおける施設クリアランスと適合事業者

もう一つの柱が「施設クリアランス」である。重要経済安保情報を扱う事業者については、「適合事業者」として政府から認定を受ける必要がある。政令で定める基準に従い、情報保護のために必要な施設・設備を備えているか、情報管理体制が適切か、従業者教育が十分かといった点が審査される。

行政機関と適合事業者との契約には、取り扱い従業者の範囲、情報保護を管理する責任者の指定、必要な施設・設備、従業者教育の実施、必要に応じた情報の返還義務などが盛り込まれる。これにより、情報のライフサイクル全体を通じて、漏洩リスクを最小化することが狙いである。

5. 罰則と実効性の確保

重要経済安保情報の保護を実効あるものとするために、同法は詳細かつ重い罰則規定を設けている。例えば、重要経済安保情報の取扱業務に従事する者が、その業務によって知り得た情報を漏らした場合には、5年以下の拘禁刑または500万円以下の罰金、あるいはその併科が科される。業務に従事しなくなった後も同様であり、未遂も処罰対象とされる。

さらに、外国の利益や自己の不正な利益を図る目的で、欺まんや脅迫、不正アクセスなどの手段で重要経済安保情報を取得した場合にも、5年以下の拘禁刑または500

---

21 重要経済安保情報の保護及び活用に関する法律については、内閣府　重要経済安保情報保護活用法ホームページ参照。https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html

万円以下の罰金などが規定されている。共謀・教唆・煽動も処罰対象であり、国外犯にも適用される。また、企業の代表者や従業者が法人の業務に関連して違反行為を行った場合には、行為者個人のみならず法人にも罰金刑が科される。

このように、罰則はかなり重く設定されており、抑止力の観点からは一定の効果が期待される一方で、内部告発や公益通報など正当な行為まで萎縮させないよう、法運用におけるバランスが重要な課題となる。

第６節　民間セキュリティ・クリアランス制度の意義と課題

1. 意義：国際協力の基盤としての情報保全

民間セキュリティ・クリアランス制度の意義は、日本の企業・研究機関が国際的な経済・技術協力の「信頼できるパートナー」として認知されるための基盤を提供する点にある。同盟国や同志国は、自国の安全保障にかかわる機微な情報を共有する相手に対して、「どのような制度で情報を守っているか」を重視する。その意味で、国際的に通用する水準の情報保全制度を国内に整備することは、日本の技術力や産業競争力を国際的な枠組みの中で活かしていくうえで不可欠である。

また、サイバー脅威やサプライチェーンリスクは、政府だけでは対応できない問題であり、重要インフラを運営し、技術開発を担うのは多くの場合民間事業者である。民間セキュリティ・クリアランス制度は、こうした民間の主体を国家安全保障の枠組みに組み込み、情報の双方向的な共有を可能にするという点で、大きな転換だと評価できる。

2. 課題

一方で、制度には多くの課題も存在する。第一に、適性評価で調査される情報の範囲が広く、本人だけでなく家族や同居人の氏名・国籍・住所まで含まれることから、プライバシー保護や差別のリスクが懸念される。精神疾患の有無や飲酒習慣、信用状態なども調査対象となるため、健康情報や経済状態といったセンシティブな個人情報が行政によって収集・管理されることになる。

このような調査が、本人の同意に基づくものであるとしても、実際には「適性評価を受けなければ仕事に就けない」という事実上の強制力が働きうる。また、特定の国籍や出自を持つ者が不利な扱いを受けるリスク、精神疾患を経験した者が不当に排除されるリスクなども想定される。したがって、プライバシー保護や労働法制と整合的な運用を確保するための、企業内のガバナンスや救済手段の整備が不可欠である。

第二に、民間企業にとっては、施設クリアランスを取得するためのコストや、内部統制の強化による企業文化への影響も重要な論点である。厳格なアクセス制御や監視体制を導入することは、情報漏えいリスクの低減につながる一方で、従業員間の信頼関係や柔軟な働き方に影響を及ぼす可能性がある。

また、適合事業者となるために必要なセキュリティ設備や人材の確保は、中小企業にとって大きな負担となりうる。その結果、特定の大企業のみが機密情報にアクセスでき、国際共同研究や政府調達の機会を独占するような構造が生まれる可能性もある。制度設計にあたっては、こうした格差の拡大を防ぎつつ、必要なセキュリティ水準を確保するバランスが求められる。

第三に、重い罰則が設けられていることから、「安全保障」を理由に不都合な情報が過度に秘匿される事態が生じる、との懸念も指摘されている。

これまで見てきたように、経済安全保障の重要性が高まるなかで、日本が国際的な技術協力やサプライチェーンの中で信頼されるパートナーであり続けるためには、国際水準に合致した情報保全制度を整備することが不可欠である。その意味で、民間を巻き込んだセキュリティ・クリアランス制度の導入は、避けて通れない選択肢となっている。

（参考文献）

Anonymous (2018), “Longer Telegram: Toward a new American China strategy,” Atlantic Council Strategy Paper, January 27, 2018. https://www.atlanticcouncil.org/wp-content/uploads/2021/01/The-Longer-Telegram-Toward-A-New-American-China-Strategy.pdf

EEAS（European Union External Actions）, “3rd EEAS Report on Foreign Information Manipulation and Interference Threats”, March 2025.

Kennan, George F. (1947), “The Sources of Soviet Conduct,” Foreign Affairs, Vol. 25, No. 7, pp. 566-582.

Sanger, David E. (2024), New Cold War, Crown Publishing, New York.

Stiglitz, Joseph E., (2002), Globalization and Its Discontents, WW Norton & Co Inc.

Mulder, Nicholas (2022), The Economic Weapon, Yale University Press.〔三浦元博訳，(2023)『経済兵器』日経 BP。〕
Lowenthal, Mark M.（2009）, Intelligence: From Secrets to Policy, CQ Press.〔前田宏訳，(2011)『インテリジェンス』慶應義塾大学出版会。〕
小谷賢（2012）『インテリジェンス』ちくま学芸文庫。
大澤淳（2021）,「産業競争力を奪うサイバー攻撃の脅威」産経新聞社『正論』2021 年 7 月号。