



令和6年
2月15日
第42号

発行
内外政治
研究G
代表 宮田修一

国益を守る経済安全保障整備

「セキュリティ・クリアランス制度」法案提出へ

政府は開会中の通常国会に経済安全保障上の国益を守るための「セキュリティ・クリアランス（適性評価）制度」に関する法律案を提出します。

この制度は、政府が保有する安全保障上の「重要経済安保情報（Critical Information）」にアクセスする必要がある政府

民間の研究・技術者も対象に

法整備については、令和4年12月に閣議決定した「国家安全保障戦略」で政府としての検討を進める方針が示された経緯があります。昨年2月から議論を重ねてきた有識者会議が1月下旬に「最終とりまとめ」を提出してしました。

現在の「特定秘密保護法」が、外交や防衛、スパ

職員や民間の研究・技術者に対し、政府が事前調査で当該者の信頼性を確認してアクセスの権限を与えるものです。高市早苗・経済安全保障担当大臣が先頭に立ち、準備を進めてきました。法案の名称は「重要経済安保情報の保護及び活用に関する法律」となる見込みです。

イ、テロの4分野を対象とし、そのほとんどは国家公務員が対象であるのに対し、今回の法整備は民間技術者も含めたセキュリティ・クリアランス制度の経済技術版とも言えるものです。

軍事技術と経済技術の境界薄れ

安全保障の概念は伝統的な防衛・外交の領域から「経済・技術の分野」に大きく拡大。軍事技術と

非軍事技術の境目が曖昧となつて来ており、経済安全保障分野においても情報漏洩のリスクに備える必要が強まっています。日本はG7のなかで唯一法整備がされていないため、諸外国との共同研究や外国政府の入札に参加できないなどの弊害も指摘されています。

技術漏洩には企業・法人にも罰則

法案でとりわけ大切なのは法律の実効性を担保する「漏洩等に対する罰則」です。

法案の罰則には、経済安全保障上のシークレッツ情報については、報道によると、5年以下の拘禁刑か500万円以下の罰金を課し、法人（民間企業等）の事業活動の一環として漏洩があった場合は法人を処罰する点などが規定される見込みです。また、対象者が退職したあとも罰則を適用することも検討されています。

セキュリティ・クリアランス制度等に関する有識者会議の「最終とりまとめ」



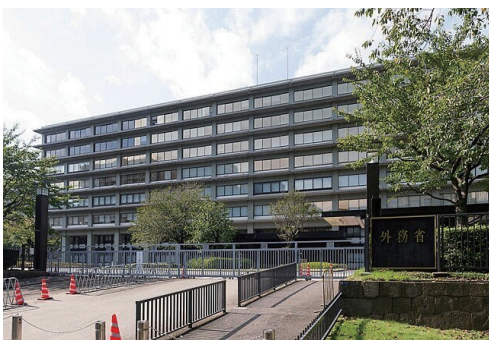
中国のサイバー攻撃で外務省公電が漏洩

「能動的防衛」の法整備を

外務省と在外公館とで機密情報を含む公電を送受信するシステムが令和2年（2000）に中国からサイバー攻撃を受け、情報が外部に漏洩していたことが明らかになりました。

漏洩の具体的な内容やどのようにサイバー攻撃がなされたのかは不明ですが、これを把握した米政府の国家安全保障局が日本側に伝えて対応を求めたと言われます。

公電は相手国の極秘情報が含まれているため秘匿が前提となっていますが、中国当局が、中国大使館から外務省に送られた情報を入手していた可



中国からサイバー攻撃を受けていた外務省

能性が高いと見られ、我が国の情報セキュリティの脆弱性が浮き彫りになりました。

公電は外部からの傍受を防ぐため、不特定多数が利用する通常のインターネット（公衆回線）とは別に、特殊な暗号を使って独立した専用回線のように使える「IPV6 PN」という通信システムで送受信されていますが、これが破られたことになりす。

日本政府や外務省は、マスコミの取材に対して「情報セキュリティ上の性質上、回答を差控える」としており、どのような対策が行われたのかなどは不明です。一方の中国側は報道官が「知らな

い」としか答えていません。日本は令和6年度に「内閣サイバーセキュリティセンター」の要員を増やす予定ですが、与党自民党内では、攻撃を受ける前に先手を打って防衛する「能動的サイバー防衛」のための法整備を求める声が強まっています。