狙われる日本の技術

流出防止対策の重要性

- 日本の企業、研究機関等が保有する高度な技術情報等は、諸外国の情報収集活動の対象となっています。そのため、機微な技術情報等を保有していれば、組織の規模にかかわらず、合法・非合法を問わず狙われる可能性があります。また、近年のデジタル化の加速を背景に、情報の持出しがかつてよりも容易になっています。
- 技術情報等の流出の影響は、自社の損失だけでなく、取引先をはじめとする関連企業にも及ぶ上、日本の技術的優位性の低下を招くなどして、日本の独立、生存及び繁栄に影響を与えかねません。また、流出した技術情報等が軍事転用され、世界の安全保障環境に懸念を与えるおそれもあります。

技術が流出・狙われた事例

日本の事例

- 外国からの誘引：2020年10月、大阪府警は、大手化学メーカーの元社員が外国企業の社員とSNSを通じて知り合い、営業秘密を漏えいしたとして、不正競争防止法違反(営業秘密侵害)で検挙しました。
- サイバー攻撃：2021年4月、警視庁は、2016年から2017年までの間、日本のレンタルサーバの偽名契約を行ったとして、中国共産党員の男を検挙しました。本件捜査等を通じて、同レンタルサーバ等が JAXAを含む約200の組織に対するサイバー攻撃に悪用され、その攻撃には、中国人民解放軍を背景に持つサイバー攻撃集団が関与した可能性が高いことが判明しました。

海外の事例

- 2020年1月、米司法当局は、ハーバード大学化学研究部門教授を虚偽陳述で逮捕しました。この教授は「千人計画」に参加して中国側から報酬や研究資金を受け取っていたにもかかわらず、当該事実の開示を行わず、不正に米国政府から助成金を受給していました。

外国への流出リスク事例

諜報工作

- 謝礼・脅し・隠蔽：流出事実の発覚を防ぐ極めて巧妙な手法・プロの「スパイ」の心理操作テクニック（一度餌食になると離脱が困難）を使用例）発覚しない持出方法の教示、指示に従うしかないと思わせる状況の創出

幅広い情報活動

- SNSの利用：偽の企業名と女性名で化学メーカーの社員に働き掛け、タッチパネル電子材料に関する技術情報を入手
- 共同研究：米国が制裁対象とする外国ICT企業の日本法人が大学教授に共同研究を提案
- 企業買収：大手企業を主要取引先とする日本の中小企業（半導体関連技術を保有）を買収
- 合弁：有利な条件で日本企業と合弁会社を設立し、軍事転用可能な製品を懸念企業・大学に販売

サイバー攻撃

- 海外拠点を経由：日本の防衛関連企業の海外拠点サーバに侵入した上で日本国内のシステムを攻撃