モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース／第89号

⚠技術情報や研究データは適正に管理されていますか？

日本には、先端技術を保有する企業やアカデミアが多数存在しています。これらの技術や研究成果の中には、軍事転用が可能なものもあり、その情報が国外に流出した場合、日本の安全保障上、重大な影響が生じかねません。

そこで今回は、実際にあった技術流出の検挙事例と対策方法についてご紹介します。

スパイ工作による技術流出

○ 国立研究開発法人の外国人研究者が、平成30年４月に、中国に所在する企業が使用するメールアドレスに対して、同研究所の営業秘密であるフッ素化合物の合成技術情報の研究データを送信したとして、令和5年6月に警視庁が外国人研究者を不正競争防止法違反の罪で逮捕しました。

○ こうしたパターンでは、外国が企業などの情報にアクセスしやすくなるよう、**スパイとなる者を仕立てて情報を盗ませる**といったケースもあるので、注意が必要です。

技術流出を防ぐためには～対策方法～

重要 POLICE

① 秘密情報に「近寄りにくくする」ための対策
例：アクセス権の限定／秘密情報を保存したPCはインターネットにつながない

② 秘密情報の「持出しを困難にする」ための対策
例：私物USBメモリ等の利用・持込み禁止

③ 漏えいが「見つかりやすい」環境づくりのための対策
例：レイアウトの工夫／防犯カメラの設置

④ 「秘密情報と思わなかった」という事態を招かないための対策
例：マル秘表示／ルールの策定・周知

⑤ 社員のやる気を高めるための対策
例：ワークライフバランス／社内コミュニケーション

出典：経済産業省「秘密情報の保護ハンドブック」

ご相談頂ければ、技術流出の手口などを個別に紹介させていただきます。
まずは、最寄りの警察署または、事務局までご相談ください。

京都府警察本部モノづくりプリザーブ事務局
075-451-9111

府警ＨＰリンク