



技術情報流出防止ネットワーク・山梨
山梨情報保全通信

山梨県警察本部警備第一課
第2号

諸外国による巧妙な技術情報の獲得手法

諸外国からの不法行為などによる技術情報の流出はさまざまな手口を使って行われます。今回はそのうち2例を紹介します。

機密情報を狙うサイバー攻撃！

近年、機密情報の窃取を目的としたサイバー攻撃が世界各国で問題となっており、日本も例外ではありません。

過去には、国内企業など約200社に対し、**日本製ソフトウェアの脆弱性を悪用した大規模なサイバー攻撃**が発生しておりますが、警察による捜査の結果、「T i c k」というサイバー攻撃集団によって実行されたものであり、**某国の組織が関与している可能性が高いと判断**されています。

サイバー攻撃を防ぐためには、情報セキュリティの向上が重要です。

「独立行政法人 情報処理推進機構（I P A）」が、情報セキュリティ対策についてわかりやすく解説していますので、是非ホームページをご覧ください。



直接、従業員に接触する手口もあります！

令和2年1月、大手通信関連会社の元従業員の男が、同社に在職中の平成31年2月及び3月、**某国の政府職員から唆され、同社の営業秘密を不正に取得**した不正競争防止法違反の罪で検挙されました。

某国の政府職員は、元従業員の男を飲食店で接待し、繰り返し情報を入手していたとみられています。

このように、諸外国による技術情報の獲得手法については、サイバー攻撃だけでなく、直接、従業員と接触する手口もあるのです。

特に、**営業秘密にアクセス可能な立場（役職）の従業員については、狙われるリスクが高い**ことから注意が必要です。



このような事例は氷山の一角です。少しでも不安・不審に感じることがあれば「技術情報流出防止ネットワーク・山梨」事務局にご相談ください。



【事務局】 山梨県警察本部警備第一課
電話 055-221-0110
内線 5872・5873