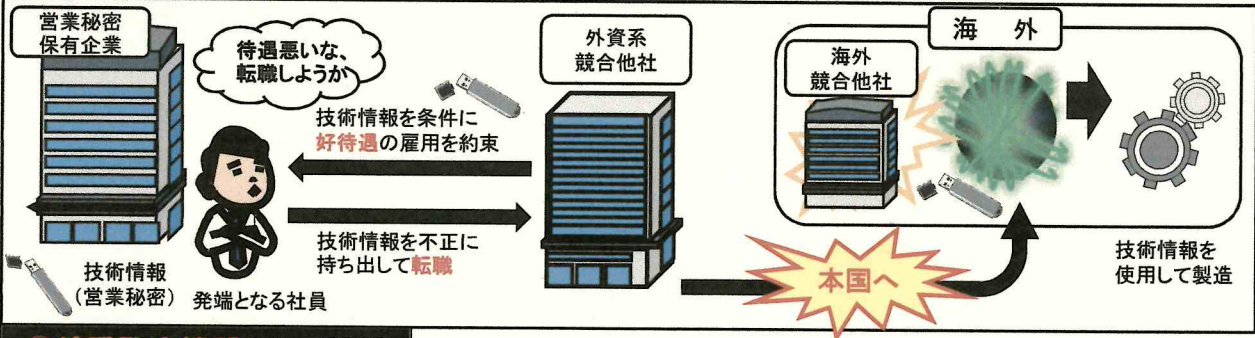


産業スパイの「魔の手」はすぐそこに！

自分の会社は大丈夫だと思った人は **要注意**

神奈川県内には、優れた技術やノウハウを保有する事業者が多く存在します。
今回は、会社の**機密情報が狙われて海外へ流出するケース**について紹介します。

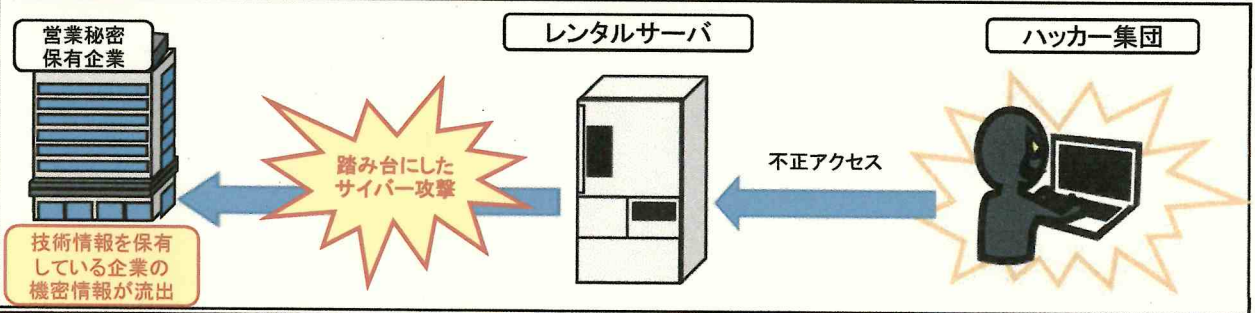
①外資系企業による接触



②外国政府機関による接触



③ハッカー集団が関与していると疑われるサイバー攻撃による方法



ポイント

上記①と②のケースのような不正行為におよぶ社員には「借金により生活が困窮」、「会社の待遇等に不満」等の**動機**があり、自分の行為を**正当化**して営業秘密を持ち出したりするのです。営業秘密文書保管場所の施錠状況を組織的に確認したり、採用・退職時に秘密保持契約書を徴収するほか、**社内相談窓口**を設けるなど、不正行為が行われる**機会**をつくらせない対策をすることが重要です。

また、上記③のケースは、ハッカー集団がセキュリティシステムの弱点を狙ったサイバー攻撃により、企業等の機密情報が流出したものです。社員や研究員の危機管理意識を高めるとともに、**アクセス権限付与を最小限とする**などの情報管理の強化やサイバー攻撃への対処法を**点検**することが大切です。

▼ SEAGULL事務局(外事第一課内) ▼

〒231-8403 横浜市中区海岸通2丁目4番 神奈川県警察本部

相談窓口 Email : seagull@police.pref.kanagawa.jp

