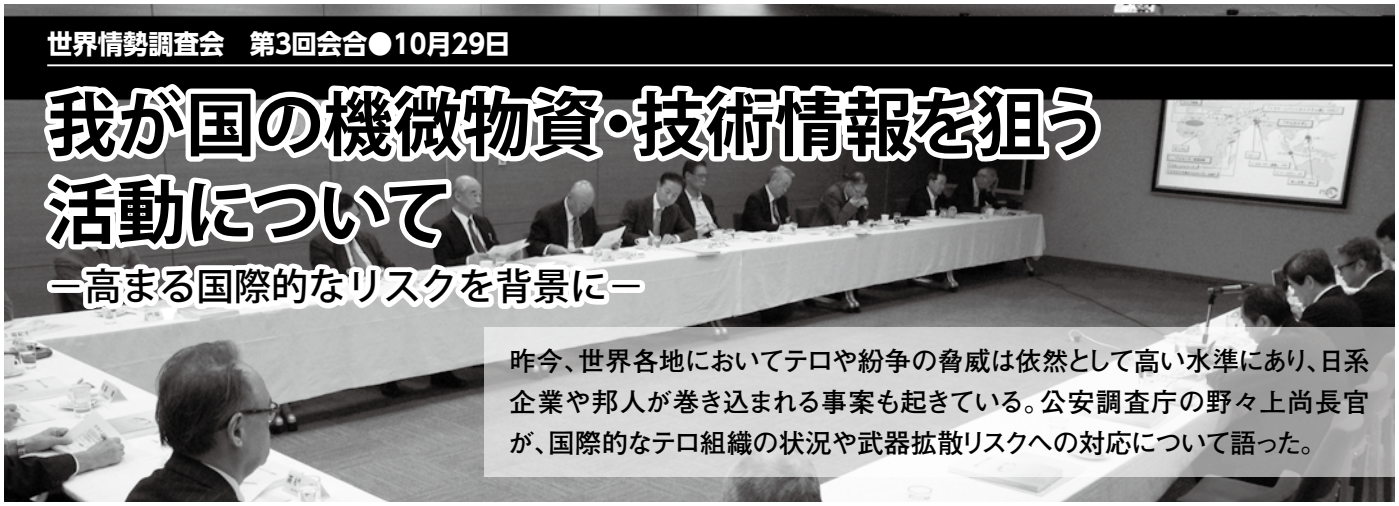
世界情勢調査会　第3回会合●10月29日

我が国の機微物資・技術情報を狙う活動について

―高まる国際的なリスクを背景に―



昨今、世界各地においてテロや紛争の脅威は依然として高い水準にあり、日系企業や邦人が巻き込まれる事案も起きている。公安調査庁の野々上尚長官が、国際的なテロ組織の状況や武器拡散リスクへの対応について語った。

講演

野々上 尚 氏

公安調査庁 長官

大量破壊兵器等の拡散防止には民間も対策が必要

現在、欧米諸国などで、アルカイダ関連組織やISIL（イラク・レバントのイスラム国）などによるテロの脅威が広がっている。これは日本にとっても無縁ではない。テロ組織によって邦人が死傷する事件が発生しており、海外在留邦人や日本の海外権益は現実的な脅威にさらされている。

中でも顕在化しているのが、大量破壊兵器等拡散の脅威だ。テロリストはもとより、北朝鮮などの懸念国による諜報活動が活発化しており、そのターゲットはかつては政治家、外交官、軍・政府職員だったが、現在は民間企業、学術機関を狙った活動が盛んになっている。従って、国家機関による対策だけでなく、民間における対策が必要な状況である。懸念国はさまざまな手法で兵器の製造・開発に使用できる機微物資の調達を謀っており、民間企業でも調達動向や手法に関する最新情報の把握が不可欠だ。

標的となる技術分野としては、情報通信、軍事、環境、先端素材、医療・製薬、農業分野などの広範な分野が考えられる。それらについては直接発注だけでなく、フロント（ダミー）企業経由、仲介企業経由などのパターンで、商取引を装った窃取が行われる危険性がある。例えば、「顧客またはその所在地が規制対象リストに掲載されたものに似ている」「商品のスペックが顧客の業務と合致しない」「配送日が曖昧だったり配送先が不適当」など、物資や運送に関して少しでも不審な発注があれば、十分な警戒が必要である。

また、共同開発を通じた技術窃取の危険性もある。懸念国の企業・研究機関と共同開発を行う際には、軍部との関係性や開発技術の用途、軍事転用の可能性などについて、疑念の有無を調べることが求められる。さらに、展示会を契機とした情報窃取の危険性もある。懸念国の関係者が1対1の面談を求めてきた場合には、慎重に臨むべきだ。企業における対外的な窓口は営業部門が担うことが多いが、研究開発部門が扱う仕様書を持ち出すよう要求されることもあり、管理を適切に行うなどの万全な体制を取っておく必要がある。

営業秘密の漏えいに関して官民が連携して情報交換を

最近、特に増えているのがサイバー攻撃による情報窃取だ。研究開発データはもとより、個人情報までもが標的にされている。それをきっかけに重要なデータが盗まれる可能性があるので、すべての企業は注意が必要である。大企業では比較的対策が進んでいるようだが、中小企業では十分な対策が講じられていないところも多いだけに、下請事業者やその先にまで目を配らなければならない。

特定の企業・組織の機密情報を狙った標的型メールについては、「外部に公開していない担当者の氏名、メールアドレスが使用されていないか」「重要な会議や出張等の直前に送信されていないか」「部外者が知り得ない内容が使用されていないか」などの判断基準があるので、それを参考にして社内情報の流出を阻止していただきたい。

日本政府は、『官邸における情報機能の強化の方針』（2008年2月）、『「世界一安全な日本」創造戦略』（2013年12月）などを通して、公安調査庁等の情報収集関係機関の業務強化を打ち出している。これを受けて、公安調査庁では、大量破壊兵器等の拡散防止に向けた水際での未然阻止に資する情報、監視すべき懸念調達に関する情報など、さまざまな情報を関係機関等に提供している。

また、拡散防止に向けた産学官連携にも取り組んでおり、各種産業分野と学術・研究機関、行政との連携を図っている。その一環として、経済産業省が開催する「営業秘密官民フォーラム」への協力も行っている。これは、官民の実務者間で営業秘密の漏えいに関する最新手口やその対応策について情報交換する場で、年1～2回開催する。こうした取り組みを通じて、企業の皆さまに、情報流出のリスクに対する意識を高め効果的な対策を講じていただきたいと考えている。欧米に比べて危機管理が甘いといわれる日本だが、もはや認識不足は許されない時代なのである。