過熱するサイバースパイ活動

論　風

日本危機管理学会理事長
国際社会経済研究所主幹研究員
原田　泉

国民利益保護へ対応急げ

はらだ・いずみ　慶大大学院修士修了。日本国際貿易促進協会などを経てＮＥＣ総研から国際社会経済研究所へ。現在同主幹研究員。早稲田大学非常勤講師なども務める。60歳。東京都出身。

最近、国家としてのサイバースパイ活動が顕在化している。

国家のスパイ活動をつかさどる情報機関（インテリジェンス機関）は、国家の安全保障の観点から情報を収集・分析し、政府首脳に報告することを主な任務とする。一般にその機能は４つに分けられる。合法非合法を問わずひそかに情報を収集する「諜報」、外国のスパイの摘発などの情報防衛を行う「防諜」、自らが有利になるような情報を流す「宣伝（プロパガンダ）」、そして相手につかませた情報により自らに有利な状態をつくる「謀略」であり、「謀略」には暗殺、破壊活動などの非合法工作活動を含む場合もある。

現在、諜報では、一般公開情報から収集する「オシント」や人を介した情報収集の「ヒューミント」もさることながら、サイバー空間が拡大するにつれ通信や電子信号を傍受して情報を得る「シギント」が中心的存在になってきている。そしてこのシギントでは、いかに巨大な量のデータを収集し、貯蔵、保存、管理、分析する能力、いわゆるビッグデータの技術と予算の力がサイバー諜報能力の差となり、外交や安全保障を支えている。

米国支配からの脱却

インターネットはもともと米国の対ソ軍事戦略で開発され、冷戦構造崩壊後急速に世界へ普及した。それが2013年のスノーデン事件で、米国の世界監視システムであり情報収集ツールであることが明らかにされ、米国はいみじくもサイバー諜報での圧倒的な力を他国に見せつける形となった。これに対し各国とも監視が嫌でもネットやスマホを使わぬわけにはいかず、テロ対策では英米の情報機関に頼らざるを得ない現実から、専ら自らのサイバー防衛力強化に努めているのである。

また、欧州連合（EU）は米国の監視から加盟国の国益を守るため、域内の個人情報保護を強化し、中国も習近平国家主席とオバマ前米大統領との首脳会談以降、サイバー空間での米中協調共存を主張する展開となっている。

一方、ネットは、米国、中国、ロシア、北朝鮮、イスラエルなどのサイバー戦争の場となり、サイバースパイが暗躍する場にもなっている。10年にはイスラエルと米軍が開発したといわれるマルウエア「スタクスネット」のサイバー攻撃でイランの核施設の機器が破壊されている。また、既に世界60カ国以上がインフラ破壊や諜報といったサイバー攻撃力を開発し整備しているという。先のロシアによる米大統領選挙へのサイバー攻撃は、偽ニュースや暴露による世論誘導と社会混乱であり、宣伝戦であり謀略戦でもある。

求められる国際規制

このようにサイバースパイは諜報、防諜から宣伝、謀略へと拡大し、国際関係に多大な影響を及ぼすまでに至っている。にもかかわらず、従来通りスパイ活動が国際法の埒外で良いのだろうか。サイバー犯罪条約の普及と、北大西洋条約機構（NATO）がサイバー活動のガイドラインとしてまとめた文書「タリン・マニュアル」の尊重はもちろんであるが、わが国が率先してサイバースパイに対する規制の国際的合意作りを進めるべきだと思われる。

他方、それが実現するか否かにかかわらず、国民の利益と権利を守るため、現状を直視してサイバー攻撃への対抗措置を含むサイバー防衛力の強化を図るほか、非合法工作活動を除外した対外情報機関を設立してサイバー諜報活動を強化することが喫緊の課題となろう。加えて、暗号、人工知能（AI）の独自開発、また、重要インフラなどの従業員の適格性を審査する信頼確認制度や通信傍受などに関する法整備、機微なデータセンターの国内設置などの施策も進めなければならない。

当然これらを実施するに当たっては専守防衛の原則の下、権力の暴走をチェックする第三者機関の設立が必要不可避となろう。民主主義のチェックアンドバランスを機能させることこそ成熟した民主主義国の証しである。