連　載
第5回

情報と防災

防衛大学校安全保障・危機管理教育センター長
教　授　太　田　文　雄

カウンター・インテリジェンス

情報を取る機能がインテリジェンスであり、相手が我の情報を取ろうとするのを阻止する機能がカウンター・インテリジェンスです。

一昔前まで、総務省・消防庁にカウンター・インテリジェンスなどは必要有りませんでしたが、今は違います。現在は国際テロ組織といった非国家主体に加え、大量破壊兵器の拡散やサイバー攻撃といった国境を越えた脅威も顕在化してきています。例えば消防庁が採用している化学防護服のメッシュの精度がテロリストに洩れたら、その精度を上回る化学剤をテロの手段として使用されてしまうかもしれません。また旧郵政省も総務省になりましたが、政府が使用するコンピューター・ソフトのはらわたが洩れれば、その弱点を衝くサイバー攻撃がかけられる可能性があります。

さらに厚生労働省の管轄でしょうが、地下鉄構内などで使用される生物・化学剤センサーが、どのようなエイジェントに感知するか、もテロリストに洩れてしまったら、裏をかかれて感知しない生物・化学剤を使用されることになります。国土交通省が管轄している航空機、船舶の構造でも、テロの手段として使用するテロリストに判ったらまずい情報もあるでしょう。

従って、昔は「注意」「秘」「極秘」といった秘密区分を設け、文書管理していたのはせいぜい防衛・外務それに警察くらいだったのでしょうが、これからは全省庁がこうした秘区分スタンダードを採用してカウンター・インテリジェンスに留意しなければならない時代となってきています。

同時に、さきほどの化学防護服などを開発している研究所や、それを製造しているメーカーも適切なカウンター・インテリジェンスを行って貰わなければならない時代となってきています。

2005 年 9 月にクリントン政権時の国防副長官であったジョン・ハムレ氏のオフィスを訪れた時のことです。彼のオフィスには国防総省のカウンター・インテリジェンス組織から彼に送られた楯が飾ってあり、それについて聞いた私に「この組織は私が作った。国防総省のみならず、陸・海・空・海兵隊の各軍内にもカウンター・インテリジェンス組織がある。」と言っていました。カウンター・インテリジェンス組織は国家に一つだけあれば良いというものではなく、それぞれの

組織に必要であるということです。即ちコンピューターを叩く時に電磁波を通じて外部から察知できないように建物のカウンター・インテリジェンスにも意を用いる必要があるでしょうし、採用される人員の身元調査も必要となるでしょう。

私が米国で武官をやっていた1996年9月26日、韓国の海軍武官がペルソナ・ノン・グラータ(好ましくない人物)として米政府から国外退去処分を受けました。彼は米情報組織に勤務する韓国系アメリカ人のコンピューター技術者から秘密情報を盗んでいた、という容疑でしたが、この日の「ワシントン・ポスト」にそのコンピューター技術者と韓国海軍武官との電話交話記録が出ていました。これを見て、米国の同盟国である韓国の武官の電話が盗聴されているということは、当然自分の電話やFAXは、事務所はもちろんのこと自宅までも盗聴されているな、と思ました。これが世界の常識でしょう。

なぜ各国がカウンター・インテリジェンスを重視しているのでしょうか。それはインテリジェンスが即、戦力に繋がり、それを取られることは直接自国の国益を著しく損失することを理解しているからです。

主要国のカウンター・インテリジェンス努力

主要国のインテリジェンスとカイウンター・インテリジェンス組織を整理してみますと下図のようになります。

	米	英	仏	中	イスラエル
インテリジェンス	CIA	SIS (MI6)	DGSE	2局	モサド
カウンター・インテリジェンス	FBI	SS (MI5)	DST	4局	シャバク

CIA(CentrallntelligenceAgency)、中央情報局やFBI(FederalBureauoflnvestigation)、連邦捜査局は有名ですが、英国のSISはSecretlntelligenceService(情報局秘密情報部)SSはSecurityService(情報局保安部)、フランスのDGSEは(DirectionGeneraledelaSecurite

Exterieure)、対外治安総局でDSTは(DirectiondelaSurveillanceduTerritoire)、国土監視局のことです。

ここで米国のカウンター・インテリジェンス組織をFBIとしたことには多少異論が出るかもしれません。9・11テロ事件の後、2002年に議会の委員会で、かつて国家安全保障会議のカウンター・テロリズム長を勤めていたRichardClarke氏は「FBIにインテリジェンス任務は持ち合わせていない」と証言していますし[1]、2004年4月に発表されました9・11以降のインテリジェンス改革に関する議会報告書では、「FBIがカウンター・インテリジェンスの機能を十分に果たしてこなかった」としてイギリスのSS(MI5)のような組織を新設すべきであるとの政策提言を出しています[2]。犯罪取り締まり組織であるFBIでは十分なカウンター・インテリジェンスはできない、との指摘です。

かつての国家安全保障局(NSA)長官であったオドム元陸軍中将と話した時にも、「FBI のような犯罪取り締まり組織とカウンター・インテリジェンス組織とではメンタリティーが全く違う。FBI はスパイを発見すると、すぐ捕まえて、自分たちの手柄であると公表してしまうが、カウンター・インテリジェンス組織は、スパイを見つけても、すぐには捕まえず、泳がせる。そしてそのスパイが次に誰と接したか、その接した男が次に誰と接するかを追いかけてスパイ網の全貌を明らかにしようとし、場合によっては偽情報を掴ませて、逆に利用しようとする。しかも黒子に徹して決して表面に出ようとしない」と言っていました。

2006 年 8 月に発覚したイギリスの同時航空機爆破未遂事件でも、イギリスの SS(MI5)はパキスタン人の容疑者を 2 ヶ月間も泳がせてテロ組織の全貌を明らかにし、犯行日の直前に逮捕しています。ちなみに英国で最も人気の高い就職先は、2007 年 5 月 1 日付けのフィナンシャル・タイムズによれば、男子では、この MI5 で、女子でも 3 位、男女合計で第 2 位が MI5(第一位は BBC)となっています。私が米国の大学院で学んでいた時も、才色兼備の実にスマートな女性がいましたが、この人は CIA に就職しました。

さて、この時オドム将軍は、冷戦後 15 年以上経った今でも、旧ソ連の KGB(国家保安委員会)の末裔が引き続きロシアのスパイとしてワシントンに暗躍している事実を憂いていました。日本の場合、カウンター・インテリジェンスの機能は警察(あるいは公安調査庁)に委ねられていますが、本来警察は FBI 同様、治安や犯罪の取り締まりを主任務としており、カウンター・インテリジェンスの専門組織ではありません。しかし上記の表からも判りますように、ほとんどの国が「目が見える人と目が見えない人との戦い」にするためにインテリジェンスとカウンター・インテリジェンスという二つの組織を持っていることがわかります。戦術的にも暗視ゴーグルを備えて夜間に昼間と同じ作戦ができる軍隊と、そうでない軍隊とが戦ったら勝敗の帰趨は明らかでしょう。

技術スパイ

米国には防衛保全サービスという組織があって、米国の軍事技術に関して外国がどのようなアクセスを試みているかについて毎年報告書を出しています。最新の報告書は 2006 年 6 月に出されたものですが、その報告書によりますと 2005 会計年度に報告されたスパイ活動の疑いある行為は 971 件と前年よりも 43%増加しており、軍事技術を入手しようと試みた国の数は、1997 年の 37 から毎年約 10 ヶ国のペースで増え、2005 年には 106 ヶ国に増加しています。

報告書は、具体的な国名を挙げず地域としてぼかした形で、そのパーセンテージを示していますが、それによりますと最大の地域は東アジア・太平洋で 31%、次いで中近東で 23%、次にユーラシアで 19%となっています[3]。しかし 2007 年 1 月 3 日付の米紙ワシントン・タイムズによれば米国防当局者の話として、最も積極的な技術スパイ国家は中国、ロシア、イランであるとしており[4]、これが地域名のトップ 3 と符合しています。

軍事技術の内、最も人気のあったのが情報システムに関する技術で約 23%、次いでレーザー・光学が約 11%、航空が約 10%の順になっていますが、2006 年末に発表された中国の国防白書で「情報化戦争に勝利できる情報化軍隊の建設を目標とする」としている記述とも奇妙に符合しています。

技術情報収集の手段としては、女スパイが男性を誘惑してコンピューターのパスワードを聞き出すというケースからコンピューター・ハッキング、盗聴など様々であるとされています[5]。米国では 2006 年末だけとってみても、11 月に「中国が爆撃機の秘密を持っていった」という記事と「中国のインテリジェンス活動を見逃した米国の失敗」を指摘する記事、そして米海軍大学の閉鎖ネットに中国のハッカーが侵入した」とする記事が、また 12 月には米海軍の武器システム技術をロスアンゼルスにある契約会社が中国に流していた」記事を掲載しています[6]。

そして 2008 年 11 月に米議会に提出された『米中の経済と安全保障に関する再検討委員会』の報告書にも「中国の米国に於けるスパイは米技術に対する唯一最大の脅威」と記載されています[7]。

2007 年 4 月にイージス艦の秘密が揺曳したことで日本では大きなニュースとなりましたが、イージス艦の戦闘管理に関する技術情報を中国が米国から盗み出していたことは上記「中国のインテリジェンス活動を見逃した米国の失敗」(2006 年 11 月 24 日付)と「スパイ調査」(2006 年 12 月 15 日付)というワシントン・タイムズの記事に既に掲載されています。また海上自衛隊のイージス艦の秘密を持ち出した 2 等海曹の配偶者が中国からの不法滞在者であったことが明るみに出ましたが、中国人民解放軍の総政治部の規則によれば軍人の配偶者は同じ中国国籍でも香港やマカオの市民であってはならず、また少数民族出身者であれば結婚を諦めるよう説得されている 8 ほどカウンター・インテリジェンスが徹底しています。

米海軍兵学校で「インテリジェンスと国家安全保障政策」の教務を実施しているカックラン教授と 2006 年 9 月に面談した際、教授は CIA から貰ったという MICE(ねずみの複数形)の字が書かれたコーヒー・カップを手にしながら、敵に情報を与えてしまう動機は、この 4 文字に表されている、と語ってくれました。「M は Money(金)、1 は Ideology(思想)、C は Compromise(妥協)、E は Ego(利己)です」と。私が「Sex の S がないですね」と問うと、彼は「それは Compromise(妥協)に含まれる」と回答してくれました。Ideology(思想)については今日、マルクシズムや北朝鮮の主体思想に信奉して情報を与える人は少ないでしょうが、過激なイスラム教を信奉して国際テロ組織に情報を売り渡す人は出てくるかも知れません。

我が国でも、潜水艦技術が中国側へ漏洩した記事[9]や、潜水艦などに転用可能な技術をロシアに漏らしたとする記事[10]が出たり、また 2007 年年頭には無人航空機(UAV)を中国に輸出して「外国為替及び外国貿易法」違反容疑が明るみに出た事案、3 月にはトヨタグループの自動車部品会社デンソーで 1980 年代後半に中国の軍事関連企業に勤務していた中国人技術者(技術部係長)が産業用ロボットのデータを大量にコピーして社外に持ち出している疑いがあることが県警の捜査で判明した事案が続出しており、他人事とは言えなくなっています。我が国では普通の国と違

って秘密保護法のような法律がありませんので、検挙された場合の罰則が軽かったり執行猶予となったりして、外国のスパイは容易に我が国の軍事技術にアクセスできるようです。

こうした状況から経済産業省では 2007 年 9 月に「技術情報等の適正な管理の在り方に関する研究会」を 15 名の専門家の元に発足させましたが、私もカウンター・インテリジェンスの観点から委員に指定されて毎月 1 回の会合に出席しています。2008 年 1 月 15 日の読売新聞は一面トップで「産業スパイ防止へ新法一来年法案提出「情報窃盗」摘発一」という記事を掲載しましたが[11]、これには以上のような背景があるのです。

1 DavidFrumandRichardPerle,flnEndtoEvi/,BallantineBooks,2004,p.169.

2 CongressionalResearchService,CRSReportforCongress,FBIInte!!igenceReformSinceSeptember11,2001: IssuesandOptionsforCongress,TheLibraryofCongress,Apri16,2004,p.CRS-40.

3 U.S.DefenseSecurityService,Techno!ogyCo/lectionTrendsintheU.S.Defense.lndustry,June2006,p.4.

4 BillGertz,ForeignSpyActivitySurgesToFi/lTechnologGap,WashingtonTimes,January3,2007,p.3.

5 Techno/ogyCo/lectionTrendsintheU.S.Defenselndustry,p.28.

6 BillGertz,Chinaboughtbombersecrets,November23,2006,FacultyChinalnte/,November24,2006,Chinese hackerspromptNavyco/legesiteclosure,November30,2006,Spyprobe,December15,2006,`WashingtonTimes

7 U.S.-ChinaEconomicandSecurityReviewCommission,2007ReporttoCongress,Nov2007,p.7.

8 OfficeofNavallntelligence,China'sNavy2007,104.

9「潜水艦資料持ち出し中国軍関係者入国図る元貿易業者、大使館出入り」、平成 19 年 2 月 7 日、産経新聞

10「ロシアに機密漏らす一潜水艦など転用可一」、平成 17 年 10 月 20 日、読売新聞

11「産業スパイ防止へ新法一来年法案提出「情報窃盗」摘発一」平成 20 年 1 月 15 日、読売新聞