連　載
第１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

## 情報の重要性とインテリジェンス

卑近な例として、皆さんが、買い物に出かけたとしましょう。目的の店に行ったところが、そのお店が休みということがよくあります。事前に電話をして、閉店日の情報を入手しておけば、時間と足代を無駄にすることもなかったのに、と思うでしょう。

日本語の情報を英語に訳すと、データ、インフォメーション、インテリジェンスの三通りの訳語がでてきます。例えば、本日の湿度は20%、風速20rn/secというのは単なるデータに過ぎません。これを例年の同じ頃や前後の日々の状況と比較して「本日は湿度が低く、風が強い」とすれば、それはインフォメーションになるでしょう。さらに一般的な国民のニーズに合致するような形として「乾燥注意報」や「火災予防警報」としますと「それでは、今日は焚き火を止めよう」といった「判断・行動するために必要な知識[1]」であるインテリジェンスとなります。

しかし、風速20m/secという数値を聞いただけで「今日は火災の発生率が高い」と判断し、個人的な遠出の行動を控える消防士さんもいるでしょうし、「本日は湿度が低く、風が強い」ということを聞いただけで待機すべき消防員を増やそうと判断・行動する消防署長さんもいるでしょう。要するにカスタマー(顧客)のニーズによって、それが単なるデータなのかインフォメーションなのかインテリジェンスなのかが変わってきます。

日本語の「情報」がインフォーマーションを指しているのかインテリジェンスなのかが不明な場合が多いので、インフォメーションを「情報」と訳し、インテリジェンスを「諜報」としている場合や、逆にインテリジェンスを「情報」とし、インフォメーションを「情報素材」と区別している向きもあります。そこで誤解を避けるため、私は敢えて日本語を使用せず、インテリジェンスという原語のまま使っていきたいと思います。

アメリカで『インテリジェンス』という本を書いたマーク・ロウエンサル氏は、「インテリジェンスとは政策決定者のニーズに合致するように収集、精査されたインフォメーション」であるとし、「全てのインテリジェンスはインフォメーションであるが、インフォメーションは必ずしも全てインテリジェンスとは限らない」と書いています2。しかしながら、この前半の定義について、私に異論があります。その理由はインテリジェンスのカスタマー(顧客)は単に政策決定者だ

けでなく、第一線で任務に従事している消防士も、また将来の装備開発に携わっている人達も立派なカスタマーだからであって、政策決定者のニーズだけに限らないからです。ロウエンサルはCIA の出身者ですから、CIA にとってのインテリジェンス・カスタマーは確かに政策決定者なのですが、普遍的な定義としては「政策決定者のニーズ」は「カスタマー(顧客)のニーズ」とすべきでしょう。特に今後、消防士が化学・生物兵器によるテロに対処する事態が考えられますので、第一線の消防士に対しても大量破壊兵器についてのインテリジェンスが必要となってくるでしょうし、将来の装備服を開発する部署にいる人達にも、大量破壊兵器から身を防護するためにはどのような防護衣を考案しなければならかいか、といったインテリジェンスも大切になってくるでしょう。

そしてインテリジェンスの内容はカスタマーによって異なってきます。例えば、消防庁本庁の上層部に報告する内容と、現場で作業に従事する消防士に対するインテリジェンスと、将来の装備開発をする部署に提供するインテリジェンスとは自ずと異なってきます。

## インテリジェンスは必ずしも秘密とは限らない

既に述べましたようにインテリジェンスとは「判断・行動するために必要な知識」ですので、それが秘密であるとは限りません。最近、テレビで「日本の情報戦略」といった番組が組まれるようになりましたが、その中でインテリジェンスの専門家と称する人が、インフォーマーションを入手可能な情報、インテリジェンスを入手できない情報、と区別して定義していました。また同じく日本でよくインテリジェンスについての本を出している人が「敵対勢力あるいはライバルについての秘密情報をインテリジェンスといって、単なるインフォメーションとは区別する」とか「対象側が隠している本音や実態すなわち機密を当方のニーズに合わせて探り出す合目的的な活動がインテリジェンスである」と定義していましたが、私はこの定義に関して疑問があります。

それは次回で述べるインテリジェンス源の種類の中に OSINT(OpenSourceIntelligence - 公開情報―)という用語があるからです。インテリジェンスが必ず秘密であるとするならば、公開情報から得られる OSINT という言葉をどのように理解したらよいのでしょうか。米国のインテリジェンス・コミュニティーは、2001 年の 9・11 やイラクにおける大量破壊兵器の存在を誤判断して戦争に踏み切ってしまった教訓から、2005 年に『米インテリジェンスの変革(TransformingU.S.Intelligence)』という本を纏めました。その中には、今後国境を越えた脅威評価に、公開情報源を統合していくことが如何に大切かを強調した論文が出ています[3]。

また、かつて米国防情報庁長官であったウィルソン退役陸軍中将が「インテリジェンスの 90%は公開情報から得られる。残りの 10%の秘密活動の方がより劇的ではあるが、本物のインテリジェンスの英雄はシャーロック・ホームズであって、ジェームス・ボンドではない[4]」と言っています。ジェームス・ボンドは英国のインテリジェンス組織である情報局秘密情報部

(SecretIntelligenceService-SIS-)の一員ですが、インテリジェンスが必ず秘密であるならば、何もインテリジェンスの前にシークレット(秘密)という言葉を付けなくても良いはずです。さらには知能指数を 1(z(インテリジェンス・クォーシェント)のように「インテリジェンス」という言葉を使用していることをどう考えたら良いのでしょうか。

私がかつて、米海軍兵学校の交換教官をしていた 1980 年代、当時の校長であったローレンス海軍少将が「インテリジェンスという言葉ほど誤って解釈されている言葉はない」と言っていたことを今でも鮮明に思い出します。インテリジェンスは必ずしも秘密とは限らないのです。

## 危機管理の第一歩はインテリジェンスを生かすこと

次にインテリジェンスと危機管理の関連について考察してみたいと思います。危機管理は、まず「察知」、次に「回避」そして「対応」という時系列で整理されます。この三段階全てにインテリジェンスは不可欠ですが、特に初動の「察知」は将にインテリジェンスそのものと言えるでしょう。従って、色々な兆候を示す情報を生かすことが危機管理の第一歩と言えます。

次に「回避」の段階ですが、得られた情報を分析・評価することにより危機の方向性と速さを予測し、さまざまな施策によって我が身(国)に危険が及ばないようにすることです。

最後に「対応」は整理したインテリジェンスから予測できる被害を最小限に抑えるように対策を講じることになるでしょう。このように、インテリジェンスは危機管理の全てに必要となりますが、とりわけ初動の「察知」には死活的重要性を持つことになります。

スイス政府編の『民間防衛』には「昼間、人口 13 万人の都市の上空 600 メートルにおいて、20 キロトンの原爆が爆発したとして、それが急襲されたときには 35%しか助からないけれども、警報があった場合には 60%が助かり、全員が避難所にいる場合には 90%が助かる」というデータがでています 5。事前にインテリジェンスを持っているかいないかによって被害者の数が大きく異なってくることを示している好例でしょう。

## これからの安全保障環境と省庁間協力

これまでの安全保障環境は主として国家対国家の抗争でしたが、これからは国家ではないテロ組織や大量破壊兵器の拡散が問題となってきます。

日本では非国家主体といっても余り馴染みがありませんが、ここ約 15 年位を振り返ってもほぼ毎年のように被害を受けていることが判ります。1990 年 4 月にオウム真理教団が東京都内でボッリヌス菌大量散布未遂事件を引き起こしています 6。1993 年にはやはりオウム真理教が東京の亀戸や横浜方面で炭疽菌を空中に散布しました。幸いにして毒性のないワクチン用の菌だった

ので、死傷者は出ませんでしたが、毒性があったら大惨事になるところでした。

1994 年 6 月には松本市の住宅街でサリンにより死者 7 名を出しています。1995 年 3 月には地下鉄サリン事件で約 4,000 人の人達が死傷しました。こうしてみますと我が国は始めて生物・化学兵器を使用したテロが発生していたことがわかります。1996 年 12 月にはペルーの日本大使公邸がトゥパク・アマルというテロリスト・グループによって約四カ月間占拠されるという事件が発生しました。1997 年 11 月には、エジプトのルクソールにおいて日本人観光客がテロリストによる銃の乱射を受けました。1999 年 10 月にはアランドラ・レインボー号が海賊によって乗っ取られました。2000 年 1 月には政府各省庁のウェッブ・サイトがサイバー攻撃を受けました。2001 年のいわゆる 9・11 テロと翌年のバリ島のテロにおいても日本人は巻き添えを食いました。2003 年 11 月にアルカイダが東京を攻撃する旨の警告を出し、それ以降 2004 年末までに日本をターゲットとするテロ予告が合計 6 回出されています[7]。2005 年の 3 月にはマラッカ海峡において「章駄天」の乗組員が海賊によって拉致され、10 月には第二のバリ島テロも起こりました。

伝統的な国家間の危機で主たるプレーヤーは軍でありましたが、テロや大量破壊兵器の拡散との戦いにおいて、軍の果たす役割は一部に過ぎません。むしろ犯罪取り締まりと治安の維持を任務としている警察が最前線であることは、2005 年のロンドン同時多発テロでも明らかです。フランスやイタリアのように軍警察を保有している国は、対テロ戦において、その有効性が立証されています。9・11 で真っ先に出動し、最も犠牲者が多かったのは消防でした。国境を越えた脅威が引き起こす危機に対処するためには、警察(海上にあっては海上保安庁)のみならず出入国管理を始めとする法執行機関との緊密な連携が欠かせません。さらには、国際テロ組織の資金源を絶つためにも経済関係省庁の協力も必要となって来るでしょう。日本の場合、国内に過激なイスラム教徒が多数いる訳ではないので多くの場合、実行犯も資金を始めとするロジ物資も海外から進入してくることになります。それを水際で食い止めるのが税関であり、出入国管理でしょう。9・11 でもマドリードやロンドンでも航空機や列車といった交通機関が武器として使われましたが、これらの厳格なチェックは国土交通省の任務となります。また日本の場合厳格な火薬類取締法がありますが、この厳格な制定・適用は法執行機関が行うことになるでしょう。さらに 9・11 後 6 週間で制定された、FBI 等の法執行機関に大幅な捜査権限の拡大を認めるパトリオット法のような法律 8 も、将来日本でも検討することになると、その場合には法律の制定機関もからんできます。最後に国際テロの動向を把握するためにはインテリジェンス機能は絶対欠かせません。

このように国境を越えた脅威に対応するためには、省庁間協力が欠かせないことが将来の方向性となってきます。

## 参考文献

1 北岡元、『インテリジェンスの歴史』(慶應義塾大学出版会、2006 年)16 頁。

2 Mark M.Lowenthal,Intelligence,CQPress,2003,p.2.

3AmySands,"lntegratingOpenSourcesintoTransnationalThreatAssessments",TransformingU.S.Inte!ligenc e(GeorgetownUniversityPress,2005),pp.63-78.

4 RichardS.Friedman,"OpenSourceIntelligence:AReviewEssay,"Parameters28,no.2(Summer1998),pp. 159-165.

5 スイス政府編、『民間防衛』、原書房、昭和 53 年 8 月 25 日第 4 刷、74-75 頁。

6 NBCR 防護・危機管理専門家共著『NBCR テロと市民の安全について』(NBCR 対策推進機構、平成 18 年 8 月)25 頁。

7 2003.10.18(オサマ・ビン・ラディン)、2003,11.16(アブ・ムハンマド・アブラジ)、2004.3,11(アブ・ハフス・アル・マスリ旅団)、2004.3.18(アブ・ハフス・アル・マスリ旅団)、2004.5.7(オサマ・ビン・ラディン)、2004.10.1(アイマン・ザワヒリ)。

8

国際社会経済研究所監修、『ネット社会の自由と安全保障』(NTT 出版、2005 年 3 月)147 頁。