東京海上日動リスクコンサルティング（株）
危機管理グループ
セイフティコンサルタント　山内 利典

リスクマネジメントにおける情報活動

2006 年 7 月 5 日、北朝鮮は日本海に向けてテポドンー2 を含む弾道ミサイル 7 基を発射した。テポドンー2 については 5 月 19 日以降その発射兆候が把握されており、日米は共同で艦艇、航空機を日本海等に展開し発射に際しての情報収集に備えていた。しかし、北朝鮮が 1 日の間に 7 基もの弾道ミサイルを発射したことは、特に日本政府にとってはまさに危機事態であった。政府は、1 基目の発射から 19 分後の 3 時 52 分に緊急警報を発令し、27 分後の 4 時 0 分には首相官邸の危機管理センターに対策室を設置する等の対応をとった。また、2 時間 45 分後の 6 時 18 分には安倍官房長官が緊急記者会見し、北朝鮮に対する厳重な抗議と遺憾の意を表明した。（それぞれの時刻は各種報道による。）

韓国の対応は、これとはやや異なるスタンスのものであった。国防部の合同参謀本部が全軍に態勢の強化を指示したのは 6 時 30 分頃とされており、軍の緊急時の対応の遅れや大統領府の消極的な対応に批判が集中する結果となった。韓国政府は、「日本の対応こそが騒ぎすぎである」と国内メディアの批判に反論したが、こうした日韓の対応の差はどこから来たのであろうか。もちろん大きな問題は南北関係に対する戦略を踏まえてのものであろうし、また、それにかかわる国内政局に配慮してのこともあろう。しかし、北朝鮮による長距離弾道ミサイルの発射が北東アジアの安定に与える影響をどのように捉えるか、言い換えると弾道ミサイル発射という戦略情報をどう分析し、どう活用するか、すなわち戦略情報活動に差があったということができよう。

リスクマネジメントに関して情報が如何に重要であるかは、企業においても同様である。ひとつの情報をどう取り扱うかによってリスクを適切に管理出来ることもあれば、クライシスを乗り切れないこともある。本稿では、軍事分野における情報の取り扱いを参考にしつつ、リスクマネジメントにおける情報活動のあり方を考察する。

1. 情報とは

現在、「情報」という言葉ほどあいまいな言葉は他に例が少ないだろう。今日、この言葉から先ずイメージされるのはコンピュータにかかわる情報であり、演算処理である。かつては「情報」は「諜報」と混同され、スパイの世界のものと思われてきた。そこで先ず、「情報」を定義づけておきたい。軍事分野では次のように定義されることが多い。

1 使命達成のための計画の策定及び実施に必要な知識

2 情報資料を収集し、処理して得た結果

3 広義には、情報を得るための活動及びそのための組織を含む

通信手段や、メディアが極度に発達した今日、情報の洪水、情報の氾濫と言われるようになって久しい。ケーブルテレビでは 100 を越えるチャンネルが放送され、世界中の現地映像がリアルタイムで届けられる。インターネットでは適切な検索無くしては 100 万件に及ぶ項目がリストアップされる例が珍しくない。上の定義からいえば、これらのすべてが「情報」に相当するわけではない。先ず、自分が必要とする知識を「洪水」の中から探し出し、取捨選択することが第一となる。

次に重要なのが、テレビやインターネットから得た知識がそれだけでは必ずしも「情報」たり得ないということである。「情報」とは、「種々のデータや知識からなる『インフォメーション』を、『リクワイアメント』と呼ばれる政策担当者の要求に基づき、収集・評価・分析・統合・解釈というプロセスを通じて精製した結果としてのプロダクト*」である。軍事分野では、精製前の種々のデータや知識を「情報資料(Information)」、精製後のプロダクトを「情報(Intelligence)」と呼んで区別する例が多い。簡単に言えば、我々が指す「情報」とは、リスクマネジメントのために必要な知識であって、諸データを精製した成果物ということになる。以下、本稿では「情報」と「情報資料」を上記の意味で用いる。

注：*「危機管理実務必携」危機管理実務必携編集委員会

なお、上では比喩的に「精製」という言葉を使ったが、軍事分野では通常「処理(Process)」が使われる。これについては後でも述べる。

2. 戦略情報と作戦情報

本稿序文で、北東アジアにかかわる「戦略情報」という言葉を用いた。情報は種々の側面から多種多様に分類されるが、「戦略情報」と「作戦情報」も主要な分類のひとつである。「戦略」という言葉は、軍事分野に限らず企業においても広く用いられており改めて説明の必要はないと考える。あえて言えば、軍事分野においては軍事政策にかかわることやそのための軍事力整備、その運用方針の策定などを指す。同様に企業においても中長期的に経営方針を策定したり、大規模な新規事業展開を計画したりすることを指して頻繁に使われる。こうした「戦略」を策定したり、それを実行したりするために用いられるのが戦略情報である。

一方、戦略情報に対比される情報とは何であろうか。一般によく用いられるのが「戦術情報」である。元々戦略と戦術の区別に関する明確な定義はなく、各国、各時代の軍人、軍事学者が様々な説を述べている*。従って、軍事分野にいる人でさえ「戦術情報」を戦略情報に対比させることが少なくないが、厳密には「戦術」は戦闘局面における「手法」を指している。「術(すべ)」の言葉が指すように戦闘技術に関する事柄を指しており、企業で言えば精密部品の研磨技術や営業活動における話術のようなも

のである。そうした事柄に関する情報が戦術情報であり、戦略情報に対比するには範囲が局限されすぎたものとなる。

注：*一例を示せば、図表１のとおりである。

【図表１：戦略・戦術に関する諸定義】

	戦　略	戦　術
ジョミニ （スイス） 1779-1869	国家の防衛又は敵国侵略・襲撃のために戦地において適切に兵軍を運用する術	兵軍を配列し合戦せしむる術
クラウゼヴィッツ （プロセイン） 1780-1831	戦争目的のためにするいくつかの戦闘使用の学術	一つの戦闘間における戦闘力使用の学術
モルトケ （プロセイン） 1800-1891	戦闘にいたる最良の道程を指示しつつどこで戦うべきかを策する学術	戦闘における諸兵の使用法を教えいかに戦うべきかを指示
カステックス （フランス） 1878-1958	作戦の一般的指導、高級指揮官およびその補助者たるべき幕僚の最高の術であり戦闘の前後におけるもの	兵器による活動を始めてからこれを止めるまでの戦闘中におけるもの
リデルハート （イギリス） 1895-1970	政策の目的遂行のために軍事的手段を配分し使用する術	軍事機材を実際の戦闘で使用するとき、そのような直接の行動のための配備や統制

上表のように戦略と戦術は対比して用いられるが、軍事情報分野で戦略情報に対比されるのは「作戦情報」である。作戦情報は、普通次のように定義されている。

作戦計画の立案及び作戦の実施に必要な情報

ここでいう作戦とは単に軍事作戦に限らず、演習・訓練、種々の課題への対処も含まれる。大規模なイベントなども「作戦」の範疇である。企業においても経営戦略に基づく特定の事業展開など、当面の課題への取り組みがここでいう「作戦」に相当するだろう。そうした「作戦」の立案、実施に必要な情報が作戦情報である。

企業における作戦情報の例

企業における事業展開に例をとって言えば、当該事業の需要の状況、立地の条件、競合他社のシェア、関連法令の細部、その他諸々のリスクなども重要な作戦情報となる。事業展開が実行の過程に至ってからも進捗状況、種々の反応、妨害・障害等に関する現状及びそれらの予測に関する情報は作戦情報である。これらの中には人為的、社会的なもののほかに、当然ながら気象その他の自然現象も含まれる。

ところで、「戦略」と「作戦」を対比したように「戦略情報」と「作戦情報」はまったく別のものであろうか。一般に戦略情報と作戦情報の区分は次のように定義されている。

情報を使用する目的による区分

すなわち、戦略情報と作戦情報の違いは個々の情報の中身にあるのではなく単にそれを使用する目的による区分であり、相互に密接に関連している。例えば、政府レベルの政策決定に資するために作成された多くの戦略情報が、個々の作戦を遂行するための作戦情報としても使用され、逆に、部隊の使命達成のために収集・処理した作戦情報が戦略情報としても有効に使用される。

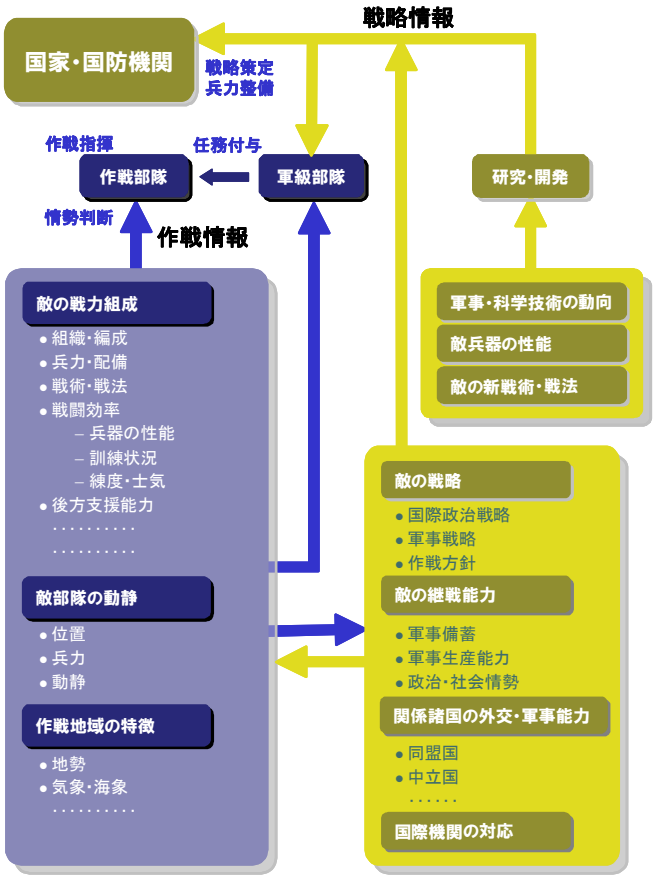
使用目的による戦略情報と作戦情報の例

北朝鮮によるテポドン・ミサイルの発射兆候に関する情報は、種々の外交的・軍事的対応を検討・協議する政府にとっては戦略情報であると同時に、同じ情報が同ミサイルの性能把握や着弾地を観測しようとして配置につくイージス艦や早期警戒機を運用する部隊にとっては作戦情報なのである。

以上、戦略情報と作戦情報について長々と述べたのは企業のリスクマネジメントにおける情報の範囲を理解していただきたいが故である。すなわち、企業経営にかかわる戦略情報と当面の課題への対処に必要な作戦情報の範囲には何ら差があるものではなく、同じ情報が双方に重要な意味を持つことが多いということである。リスクマネジメントにおいても、リスク予防のための情報とクライシス対処のための情報は同じ関係にあり、この観点から企業のリスクマネジメントにおいても常に広い視野で種々の情報資料に注意を払うことが肝要である。

なお、参考までに軍事分野における戦略・作戦それぞれの情報の具体例と両者の関係を模式化して図表 2 に示す。

【図表 2：戦略情報と作戦情報】



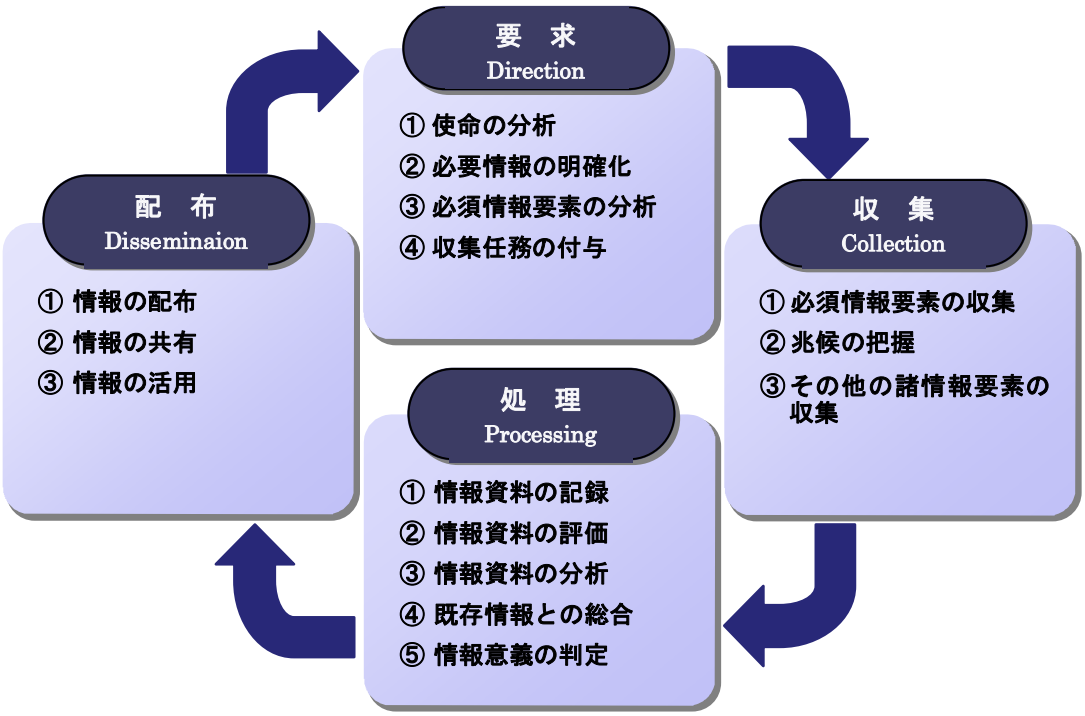
3. 情報活動とは

一般的に危機は突発的に発生するものと思われがちだが、その多くは事前に兆候があり、適切にセンサーを張り巡らして情報資料をうまく処理し、それを有効に活用すれば危機の顕在化を防ぎ、危機が現実のものとなった場合も被害を最小限に抑え得る可能性が高まる。軍事分野においても企業のリスクマネジメントにおいても情報を取り扱う上でのポイントは、次のようなものが挙げられる。

1. 必須の情報は何か
2. 平常時からアンテナを
3. 断片資料から総合情報へ
4. 必要なときに必要な人へ
5. 情報の一元化
6. 情報の適切な活用
7. 不足している情報は何か

こうした観点から情報を取り扱うことを軍事分野では「情報活動(Intelligence Activities)」と呼んでいる。これは、本稿第 1 項の情報の定義で述べた「情報を得るための活動」に相当するものである。一般に情報活動は図表 3 に示す 4 つの情報サイクル(Intelligence Cycle)により構成される。

【図表 3：情報活動サイクル】



これらの 4 つの過程は、その重要性に軽重があるわけではない。このサイクルを経ることにより正確な情報が適切に活用できるようになる。上で挙げた 7 つのポイントも同様である。しかし、リスクマネジメントにおいてはこのうち④必要なときに必要な人へ、⑤情報の一元化、が特に重要な意味を持つ。クライシスにおいては情報を緊急対策本部へ集中させて一元化するとともに、社長の的確な意思決定に寄与することが情報活動の使命である。

4. 情報の要求

情報活動のサイクルは情報の要求から始まる。情報の要求には先ず、政策の立案者や決定者、あるいは作戦指揮官が自己に付与された任務を分析し、任務遂行のために必要な情報は何かを明らかにすることが第一である。作戦の目的や目標*を分析し、自分の部隊の能力や敵の戦力などを検討して目的を達成するためのオプションを導き出すのである。このとき必要なのが情報である。情報は当然ながら既存のものも活用するが、上記の分析から不足している情報を明らかにしてそれを要求することになる。

注：*企業においては、「目標」は目的を達成するための個々の実施事項の量（程度）とその期限を言うが、軍事分野においては、上位指揮官の使命を指す。すなわち、上位指揮官はその使命を達成するために部下指揮官に任務を付与し、部下指揮官はその任務（使命）を遂行するために作戦を立案、実施する。このとき自己の使命が作戦「目的」であり、上位指揮官の「目的」は自己の「目標」となる。本稿では、後者の意味で使用している。

企業のリスクマネジメントにおいても、目的や目標を明らかにすることにより収集すべき情報資料がより明確になり、関係者が注意を振り向けるべき対象がより具体的なものとなる。ただ漠然と情報を要求するだけでは、的を射た情報は得られないと認識しなくてはならない。リスクマネジメントにおける目的や目標を明らかにするには、リスクの洗い出しも手法のひとつになるだろう。自社に内在し、あるいは自社を取り巻く種々のリスクを想定してそれらに関連する情報は何かを明確にすることが必要である。

必要な情報が明らかになれば、その情報がどのような要素で構成されるか、あるいは、どんな情報資料から導き出されるかを分析する。これらの情報要素のうち、上で明らかにした必要情報を導くために必要不可欠なものを「必須情報要素(EEI：Essential Element of Information)」という。軍事分野では、こうした要素を情報専門部隊や指揮下の作戦部隊に示し、収集任務を付与するのである。

企業における情報要求の例

一例として、事業継続計画を策定しようとする場合、まず前提となるのが被害想定の設定である。地震災害を前提とした場合どのような規模の地震がどこで起きる可能性が高いのか。発生した場合、社員・家族の死傷はどの程度発生するのか。自社の施設・機材はどの程度の被害を受けるのか。周辺のインフラはどのような状況になるのか。CSR の観点から地域社会からどのような要求が来る可能性があるのか。等々いくつもあげることができる。これらの事項は仮定として設定することもできるが、作戦計画（「事業継続計画」）は仮定が多いほどその計画自体が脆弱なものとなる。そこでより根拠のあるデータ（情報）が必要となるのである。これらが手元になければそれを要求し、後述する「処理」により自社の事業継続に与える影響度等を「判定」することになる。

5. 情報資料の収集

情報資料の収集は、必須情報要素の収集を主眼として行われる。軍事分野では、情報専門部隊や作戦部隊がそれに従事するが、情報資料の収集は戦闘行動の実施と同様に指揮官から出された明確な命令であり、「EEI を無視する罪は、攻撃命令を無視する罪となんら差異はない*1」のである。作戦部隊においては通常の作戦任務の遂行を通じて収集にあたる場合が多いが、割り振られた情報資料の収集も戦闘行動と同じく作戦任務のひとつである。企業においては通常、情報活動任務を専門とする組織はない*2ので、職掌にかかわらず全部門が収集にあたることになる。この場合もそれぞれの所掌業務を通じて必須情報要素の収集にあたるが、この場合上で述べた目的と目標をふまえておくことが重要である。そうすることにより、必須情報要素にかかわる兆候を認識することができ、また、その他の諸情報要素に対しても注意を振り向けることができる。いずれにしても情報資料の収集は経営陣（社長）から命じられた全社員の任務と認識し、常に危機意識をもってアンテナを張り巡らせておくことが肝要である。

注：*1「Intelligence is For Commanders」 Col.Robert R.Glars & Phillip B.Davidson

*2 米国企業では、一般にコミュニケーション部門(Communication Department)が社内外の利害関係者や一般の人々との間で、情報資料の伝達や処理を行う等、情報に関する全ての機能を持っている。また、米国のある多国籍企業は、経営者直轄の情報資料の収集・分析を担当する部署を持っている。その部署は、競合他社の開発動向や開発傾向を経営者に報告するために、専門スタッフが情報資料の収集や他の部署に対する収集の指示及び集められた情報資料の分析にあたっている。（以上「危機と『情報』の取り扱い」東京海上リスクコンサルティング㈱TALISMAN 2001 年 1 月号から）しかし、こうした例は我が国では極めて特殊な例といえ、多くの企業では広報部門の付随的業務として情報を取り扱っているのが実情だろう。

なお、軍事分野における収集の手段には①視認（敵部隊の発見、兵器・装備品の状況等）、②測定、測量、観測（レーダー観測、敵が発射する電波の測定、戦場の測量等）、③閲読（公刊文書、関係文献・文書の参照等）、④聴取（一般放送・敵の通信の傍受、捕虜・住民・戦場から帰ってきた味方部隊からの聴き取り等）、⑤写真、録音、録画（衛星写真、潜水艦が発する音響の分析等）、⑥物件の取得（鹵獲（ろかく）品の分析等）、⑦統計調査（敵の通信頻度の統計分析等）、⑧情報交換等がある。これらの多くは専門の機材や特殊な手法による活動であるが、実際には情報の元となる資料の 80～90%以上は一般公開されている資料によっているといわれる。企業における収集活動は、当然ながらほとんど全てが公然かつ合法手段によるが、上の例のようにほとんどの情報が一般公開されている資料によって作成されることに留意すべきである。

企業における収集活動の例

例えば企業経営においてどのようなリスクを抱えているかを調査する（リスクの洗い出しという）場合、諸文献や報道資料、報告書により事例を研究したり（閲読）、種々の数値実績を分析（統計調査）したりする。また、施設の立地や老朽度を計測（測定、測量）したり現場の勤務・安全環境を実地検分（視認）したりするだろう。製造業であれば当然ながら製品の抜き取り検査も行うし他社製品の研究（物件の取得）も行うであろう。さらには従業員、顧客、労働組合等からもアンケートや面談により何かのヒントを得ようと情報収集（聴取）する。このように企業においても情報資料の収集の手法は基本的には軍事情報の分野となんら変わることはない。

6. 情報資料の処理

前述のとおり、情報資料は処理することによりはじめて情報となる。処理は、①記録(Filing)、②評価(Evaluation)、③分析(Analysis)、④総合(Integration)、⑤判定(Interpretation)の手順を経るのが一般的であるが、情報資料の内容の緊急度によってはこれらの手順を並行して実施する。いかに正確な情報であっても、時機を失すればその価値のほとんどが失われるからである。従って、情報資料のうち緊急に配布する必要があるものについては、直ちに配布される場合もある。ただし、この場合には未処理の情報資料であることを明示することが重要である。また、情報資料の処理においては、情報要求との関連性、当該情報資料の利用範囲、現在及び将来における情報としての利用価値を検討するとともに、先入観にとらわれて安易な推測に基づく根拠薄弱な情報を作成しないように留意することが肝要である。

① 記録

記録とは、当該情報資料の処理作業を容易にするとともに、後日も利用できるように入手期日、入手先（通常「情報源」又は「資料源」という）等を分類整理し、記入又は編集することである。今日では多くの場合データ処理システムに入力することがこれに該当する。情報資料の種類によっては、資料源や収集機材からデータリンク等により直接自動入力される。文書情報資料についてもフォーマット化されたものについては同様である。企業においても各種のデータが社内 LAN や各地の事業所を結ぶネットワークシステムにより自動入力されるのが一般化している。要は、自社の業務に必要な「必須情報資料」が適切にデータベース化されていることが肝要である。

② 評価

評価とは、当該情報資料が以後の処理作業にとってどの程度有用なものであるかを検討することを指す。具体的には、その資料源の「信頼性」と当該情報資料の「正確性」を評価する。このとき「信頼性」と「正確性」は別の観点であることに留意が必要である。すなわち、その資料源の信頼性が高いからといって当該情報資料が常に正確とはいえないことに注意しなければならない。大手新聞社と責任者不明のインターネットサイトには信頼性に格段の差があるのは明白である。信頼性はその収集、処理能力や過去の実績を勘案して評価する必要がある。信頼性の観点からは、自らが直接一次資料を収集したものが一番高いといえる。しかし、自ら収集したものでも常に100%正確とは限らない。見まちがいもあれば先入観に基づく思い違いもあるからである。

このように正確性の評価は信頼性の評価よりさらに難しい。大手新聞社の記事だからといって、内容が常に正確とは限らない。事件報道に出ている関係者の年齢すら各紙を比べてみれば異なっていることは珍しくない。特に取材源が匿名のときはもちろんのこと、「○○筋」、「××関係者」あるいは「△△省高官」といった場合でも注意が必要である。その人物が本当に当該事項を知る立場にあったのか、一部の事実に憶測を交えて述べたのではないか、極端な場合には、記者が誘導し記者自身の思い込みで書いたのではないのか等を想定してみる必要がある。また、統計資料の場合には、データの範囲、条件などに注意する必要がある。

「信頼性」と「正確性」

筆者の経験でも、最も信頼性の高い情報源のひとつである米軍から得た情報ですら、内容について相手とディスカッションした結果、その情報の正確性に疑念を抱いた例は皆無ではなかった。また、偵察活動から帰投した偵察機搭乗員から聞き取り調査を実施したところ、すでに提出されていた報告書の内容が微妙に変化したり、記載されていなかった重要な事実が判明したこともある。このように犯罪捜査で「ウラをとる」ように、情報資料の正確性を高めるためには複数の資料源からの資料を照合することが重要となる。

企業のリスクマネジメントにおいて、上述のような情報資料の「評価」を行う事例は少ないかもしれない。しかし、近年多く見られるような内部告発やセクハラ等の訴えに対応する場合、上記手順の考え方は参考になるだろう。

③ 分析

分析とは、その情報資料がもつ要素を各種の側面から明らかにすることである。軍事情報で敵の位置を得た場合を例にとれば、それを地図上にプロットすることが分析の第一歩となる。これにより、自分や友軍部隊、さらには敵の基地などとの位置関係が明らかになり、以後の処理作業に結びつく。この作業もほとんどの場合自動化されている。例えば、米海軍が使用しているOED(OSIS Baseline Upgrade (OBU) Evolutionary Development)という目標情報処理システムは、「全ての資料源(All-source)による目標データを自動プロットし、他の位置データと自動照合して同一目標と判定されるものを関連づけ、航跡データとして管理*」することができる。

注：*Federation of American Scientists
http://www.fas.org/irp/program/process/obu.htm

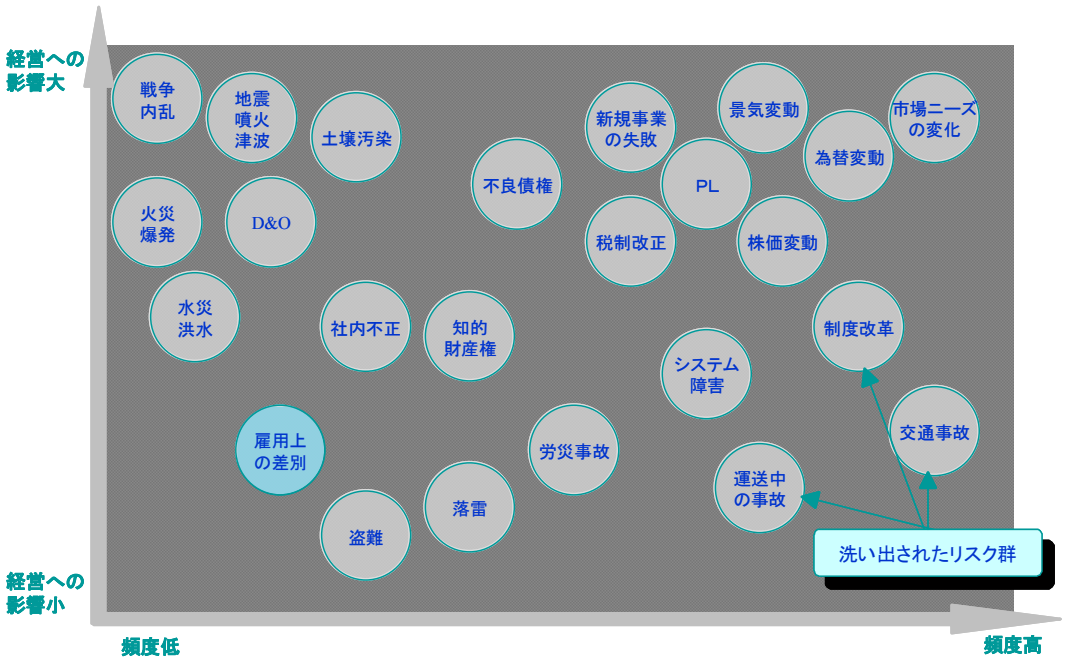
テポドン・ミサイルの例

2006 年 7 月 5 日、北朝鮮のテポドン・ミサイルが発射された際、当初想定された飛翔距離よりはるかに短い北海道西方海域に落下し、発射は失敗したのではないかといわれた。この情報資料は、①当初から短距離での発射を企図した、②燃料の注入量が適正でなかった、③飛翔中にロケットエンジンが故障した、④2 段目のロケットが分離しなかった、⑤ロケットの本体又は構成部位の強度が弱かった、等いくつかの分析ができる。これらはいずれも仮定であるが、合理的な仮定を設定しそれぞれを各種の側面から検証することにより次の処理過程に進むことができる。

企業においても各種の資料が様々な手法で分析されている。統計的分析は最も一般的なものであろうが、先入観や希望的観測にとらわれて統計手法を誤らないことが重要である。リスクマネジメントの観点からは、数値データに限らず各種の情報資料が分析対象になるだろうが、その資料が持つ要素を細分化すること、合理的な仮定を設定することがポイントとなる。図表 4 は、洗い出した種々のリスクを発生頻度、発生した場合の影響度の 2 つの側面から分析するリ

スク分析の手法（リスクマップ）の一例である。

【図表４：リスクマップによる分析の例】



④ 総合

総合とは、分析した情報資料の諸要素を既存の情報、他の情報資料と照合、一体化して断片資料から意味を持つ情報へと組み立てていくことである。一見無関係な情報資料でも、各種の側面から他の資料と組み合わせてみると思わぬ実態が浮かび上がってくることがある。よく例えられるのがジグソーパズルであるが、それとの違いは処理作業の総合では全く無関係なチップが多く混ざっていることである。また、既存のチップの中から関係のあるものを探し出すことである。それだけに柔軟な発想と深い知見が重要となる。先のテポドン・ミサイルの例でいえば、北朝鮮の国内情勢、技術動向、転用可能資材の輸入状況、各国の対応、さらには気象条件等とも組み合わせてみることが必要であろう。総合にあたって重要なのは、あらゆる可能性を排除せず、できる限り多くの組み合わせを試してみることである。

⑤ 判定

判定とは、分析、総合により明らかになった実態を情報要求及び作戦目的（企業においては当面の課題への対処）の観点から解釈(Interpretation)することである。その事実が当面の軍事環境の中でどのような意味を持ち、作戦にどのような影響を与える要素をもっているかを判断する。従って、当然ながら今後の動向に関する見積りも含まれなければならない。見積りは、処理の過程で得られた十分な根拠、その他既存の情報を踏まえていることが必要である。リスクマネジメントの基盤となる情報は、以上の処理手順により作成されたものであることが重要である。

なお、危機発生時(Crisis)には、上記手順は並行して実施されるほか、情報担当者の頭の中で瞬時に行わなければならない場合もある。それゆえ情報担当者には広い知見が要求されるほか、常に作戦の目的と目標を理解していることが重要となる。「事態収拾の目標が予め提示されてい

れば社員や役員は躊躇なく行動し、情報を正確に伝えることができる（「危機発生時の広報」前掲 TALISMAN 2000 年 12 月号）」のである。

7. 情報の配布

処理により作成された情報は、要求元に報告される。報告の手段は、口頭、報告書、図表、プレゼンテーション等種々あるが、それ自体は問題ではない。要は、適時、適切に報告されることが重要である。処理を十分に行うあまり、報告のタイミングを失してはその価値は半減するにとどまらないだろう。後でも触れるが、処理の最終責任は当該情報の使用者にある。当該情報の使用のタイミングを決定するのも情報の使用者である。「リスクマネジメント体制を構築する際に重要なことは、社長にいかに早く正確な情報を伝え、意思決定をサポートするか（前掲「危機発生時の広報」）」ということにある。

さて、特に戦略情報の場合、同じ情報要求が複数の機関に出される場合が多い。米国を例にとれば、CIA(Central Intelligence Agency)や DIA(Defense Intelligence Agency)その他の情報機関が同一の情報要求に応える場合も多々ある。このとき報告する情報の結果が異なる場合どうなるのであろうか。情報に関しては素人である政策担当者にとってはどの情報を採用してよいのか判断に迷い、極端な場合結局なんら情報がなかったのと同じ結果となってしまう恐れがある。そこで特に国家政策にかかわる戦略情報の場合、情報関連組織（Intelligence Community）の間で情報を付き合わせ、結論（判定）の調整が行われることが少なくない。（このことは、「3. 情報活動とは」の項で述べた「情報の一元化」とは別の問題である。）これは情報を総合するという意味では価値あることではあるが、種々の政治的思惑から結論がゆがめられる恐れは否めない。しかも、こうした傾向が行き過ぎると「最終的には情報の中身が薄まって、玉虫色の、政策の立案・執行に役立たないものが出来上がってしまう。つまり、情報(Intelligence)そのものの『知的レベル』が低下してしまう（前掲「危機管理実務必携」）」ことになる。

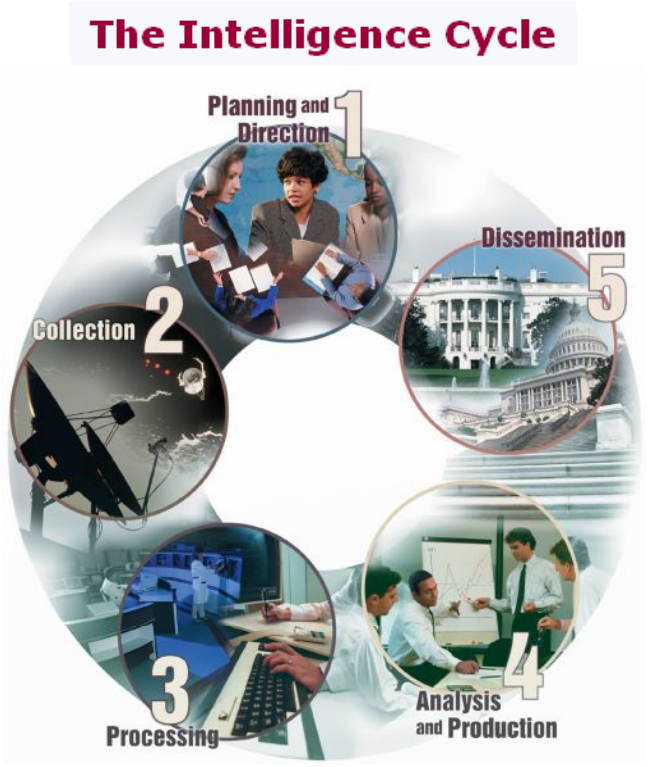
こうした傾向は企業のリスクマネジメントにおいてもまま見られることではないだろうか。各部門の利害が対立し、経営層に上げるべき情報が疎外されたり、内容が恣意的に取捨選択されたりすれば、経営層の健全な意思決定に支障を及ぼすことは明らかである。特に、ワンマン体制にある経営組織においてはこうした傾向に陥りやすいので留意すべきである。なお、米国においては、結論の調整が困難な場合、統合できなかった情報についても少数意見として付記されるのが普通である。それぞれの資料源の特質が異なる場合、このことは情報配布において重要である。

情報配布でもうひとつ重要な問題は、配布先が必ずしも要求元に限らないということである。情報は、それを必要とする関係先すべてに配布されるべきであり、これは一般に「情報の共有」という言葉で表現される。言い換えると「必要なときに必要な人へ」ということである。このとき基準となるのが、先に述べた目的と目標である。それぞれが目的と目標をしっかり捕らえていれば、自分以外の誰と誰がこの情報を必要とするかはおのずと明らかになるはずである。情報の共有とは、無制限、無秩序に情報を垂れ流すのではなく、当該情報を必要とするのは誰かを踏まえておけば、配布のタイミングを失することもなくなる。

ところで、軍事分野、特に秘匿情報についてはその取り扱いが厳しく制限される。一般に秘匿情報の配布には、「Need to Know」の原則が重視される。これはその任務達成に必要かどうかということであり、その人の職位や階級には関係ない。したがって、その情報を配布しなかったために相手部隊に何らかの危険、損害が予想されるとしても、逆に配布した結果全体の目的、目標の達成により大きな支障をきたす場合には配布されないことになる。企業においてこうした事例は想定されないだろうが、企業においても種々の企業秘密を有している。その取り扱いは、単に「社外秘」等の区分を付与するだけでなく、真に必要な配布先は誰かを踏まえておく必要があるだろう。

以上、情報活動のサイクルを述べたが、処理の手順のうち総合と判定が極めて重要な意味を持つ。それゆえ 4 つのサイクルのうち処理の手順のうちの総合と判定を独立した位置づけとして、5 つの過程からなるサイクルとする考え方もある。図表 5 は、その一例である。

【図表 5：CIA の情報活動サイクル】



【出典：米国 CIA ホームページ】

8. 情報の使用

前項までで情報とは何か、情報はどのように作られるか、そして情報はどのように配布されるかについて述べてきた。では、配布された情報はどうなるのであろうか。

情報とは「使命達成のための計画の策定及び実施に必要な知識」であることは本稿の最初に確認した。従って、情報は使命達成を指揮する指揮官（実際にはこれを補佐する組織、危機発生時には「対策本部」を含む）に集中されなければならない。言い換えれば「情報の一元化」である。一元化された情報は指揮官の意思決定のために使用され、作戦（事態への対処）が遂行される。指揮官には事態の推

移に伴い新たな意思決定が要求される。そのとき再び不足している情報は何かが検討され、新たな情報要求が示される。このように、情報は指揮官の意思決定のために使用され、そしてまた新たな要求が生まれるという循環を繰り返す。

ところで、これまでに情報とは情報資料を処理した結果であることを見てきた。そして情報は指揮官（経営陣）の下に一元化されることを述べた。これらの情報内容のすべての責任は情報作成者にあるのであろうか。ここで作戦指揮（会社経営）に関する最高の知見と最大の情報量を有しているのは指揮官であることに注目しなければならない。この観点からは、一元化された情報は指揮官にとっては「情報資料」なのである。指揮官は、その情報を使用するに当たって自らの知見に基づき、自ら「判定」しなければならないのである。その判定に基づき自らその情報の使用（又は不使用）とそのタイミングを決定しなければならない。従って、指揮官は情報の出来具合を批評はしても批判してはならない。ましてや、自分の意に沿わない情報に怒ったり、悪い情報に報告者をしかったりすれば、適時、適切な情報は二度とこないと考えなくてはならない。

情報の使用については、情報の配布に関しても言える。情報作成者は、要求元へはもちろん、それ以外への関係先へも情報を配布する。しかし、指揮官が自らの判断で配布先を指示する場合がある。このとき、配布は単に情報の伝達にとどまらず、情報の「使用」ということができる。なぜなら部下指揮官は当該情報を「判定」して、現在の目的・目標の範囲内で自らが対処すべき事項の有無を再検討・実施するからである。現在の任務に直接かかわらなくても、今後の任務を想定して必要な準備を行うであろう。情報とはそういうものであり、また、そうでなければならない。情報を与える側も、受ける側も目的・目標とともにこのことを常に踏まえておく必要がある。

一般企業のリスクマネジメントにおける情報とは、単に事実（かどうかはわからない）の伝達のみに注意が向けられがちだが、特に危機発生時には一層冷静に状況を判断しなければならず、情報の取り扱いに十分な配慮が必要である。本稿は、主として企業の中堅層を念頭において書いたが、リスクマネジメント面で何らかの参考になれば幸甚である。

以　上

（第　　号　2006 年 8 月発行）