ビジネスにおけるリスクの早期警戒とインテリジェンスの役割

日本経済大学大学院経営学研究科長　　菅澤　喜男
日本コンペティティブ・インテリジェンス学会長

１．はじめに

インテリジェンスは収集された膨大とも言える情報から生成される優れた意思決定に資する情報と理解すべきものです。顕在化あるいは潜在的な情報を元にリスクが特定化され事前に察知することが可能であるならば、より正確なリスクの具体的な内容について知り得ることが出来ます。しかし、多くのリスクは顕在化せずに潜んでいる場合が多く、我々が普段から接している出来事あるいは現象を見ている限りでは、リスクを特定化することは一般的には難しい場合が多いと思われます。ビジネス環境に応じた情報を収集することで、リスクをより顕在化させるためには、情報収集するだけでは無くインテリジェンスを生成するためのプロセスを理解することでリスクを捉えることが望ましいと考えます。

ここでは、単なる入手された情報を元にリスクを特定化するのではなく、収集された情報から生成されるインテリジェンスをクリエーション（知力・想像力の産物）することでリスクを特定化するために必要な知識と考え方について概説します。図１は、多様な分野にまたがるインテリジェンス領域を区分したものです。インテリジェンスの基本はソーシャル・インテリジェンスと呼ばれる社会全体を対象にしたものです。リスクを特定化し素早く処理するためには、インテリジェンス活動をどのような視点で展開するかが重要です。言い換えれば、インテリジェンス活動は、リスク・マネジメントに含まれるものと考えることができます。図１の図中にあるそれぞれのインテリジェンス領域に関する定義は、3.2節にある表１で示します。図１で示されているイッシュ(Issue)・マネジメントとは、インテリジェンス研究の分野では危機管理として捉えています。

2. リスクの早期発見とインテリジェンス

リスク・マネジメントに関する定義は国際標準化機構（ISO：International Organization for Standardization）あるいは日本工業規格（JIS:Japanese Industrial Standards　Q 0073:2010)によれば、リスク・マネジメントとは「リスクについて、組織を指揮統制するための調整された活動」としています。ここでマネジメントとは「組織を指揮し、管理するための調整された活動」としています。図 1 にあるエンバイロンメンタル・スキャンイングは、組織を取り巻く環境を“精査することで異常な部分を発見（スキャニング)”しようとするものです。そのためには組織を取り巻くビジネス環境について情報収集・分析・評価することが重要です。このようにリスク・マネジメントとインテリジェンスとは、表裏一体の関係があります。さらに、リスクをどのように評価するかと言うリスク・アセスメントとリスク源は、インテリジェンス・クリエーションとして考えるべきです。ビジネ

ス・インテリジェンスは、自身が係るビジネス全体を対象に情報収集・分析・評価を行う活動です。コンペティティブ・インテリジェンスは、競合(ライバル)関係にある組織(企業)に絞り込んで行う活動です。コンペティター・インテリジェンスは、競合組織（企業）を特定な組織（企業）に絞り込んだ活動です。他に、コンシューマー・インテリジェンスは、「データの分析を通じて消費者を総合的に理解する能力」であり、スマートフォンやタブレットと言ったモバイル機器の普及と、膨大なデータを収集し高度に活用するビックデータを利活用する時代において、消費者の行動形態に変化が個人的意思決定のためのデータへの直接アクセスを必要とする新たな機能としての需要を生んでいます。

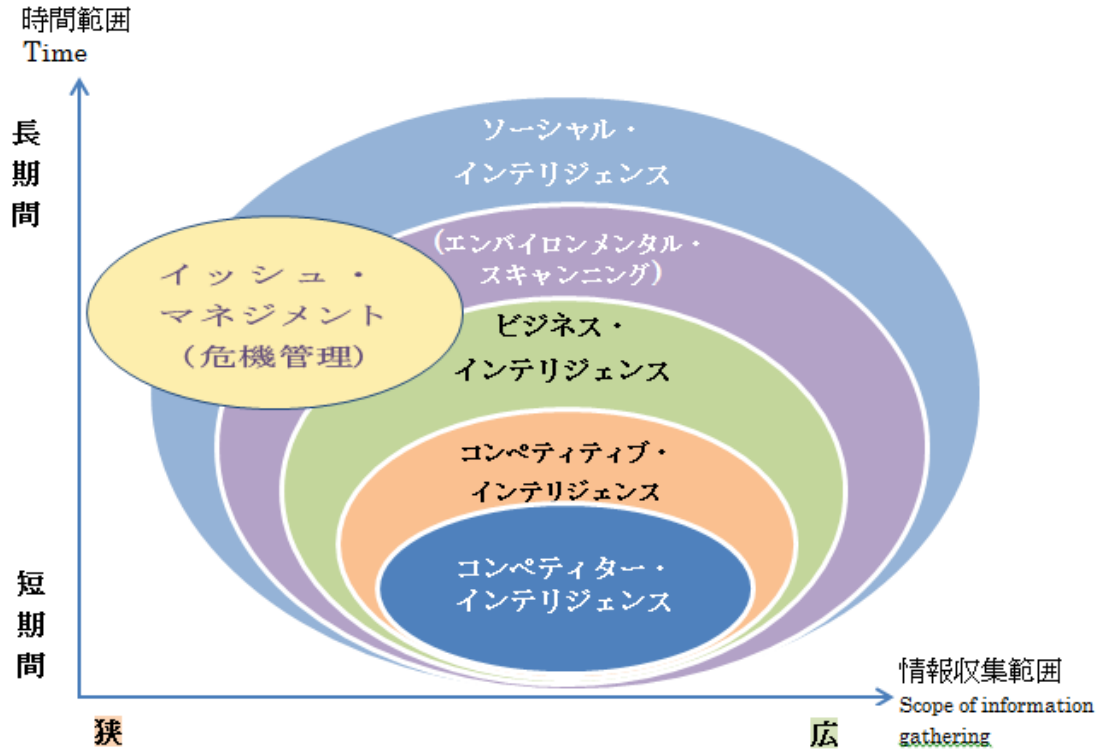


Figure2.1 外部情報の収集範囲とインテリジェンス領域

図 1. インテリジェンス領域の区分

3. 知識、情報、データの違いと相互作用

インテリジェンスという用語は、“知識”という用語と密接に関連しています。しかし、知識という用語について、独自の定義はあいまいな感じがします。その内容や背景、あるいは専門家達によりそれぞれ異なる考え方があるために、それぞれの立場で定義をしているようです。ここでは、リスク・マネジメントの中で知識、情報、データの違いを認識した上で情報、知識、データの違いとその概念を理解することは、リスクを特定化し分析・評価するアセスメントと密接な関係があります。つまり、潜んでいるリスクを早期に特定化しその内容を知るためには情報収集・分析・評価をするためにはインテリジェンス活動

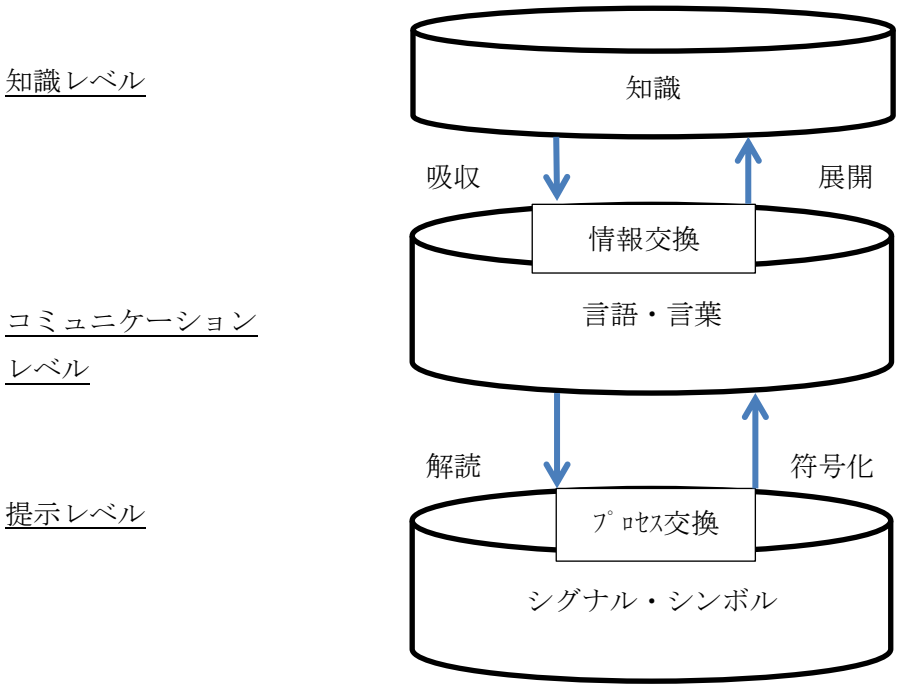
が必要不可欠です。

デービスとボトキン（Davis, Botkin 1994）によると、データは４つの違った形態でもたらされるとの指摘があります。つまり、①数値、②言葉、③音、④イメージであり、これらは特定の状況に関連していない限り意味を形成しないが、この４つの違ったデータあるいは全てリスクに成り得る前兆を認識する信号として捉えることができます。情報については、意味のあるオブジェクト指向パターンにアレンジされた分析済みデータであると指摘しています。さらに、情報の有用性や価値については、受け手の吸収能力（外部の知識を検証し活用する能力）（Cohen, Levinthal 1990）によるところが大きいものと思われます。一度受け手が情報を取り入れ翻訳し評価することで、その情報を利用あるいは使用することで知識(Koruna 2001)としての議論が可能となると考えられます。ここでは、知識は経験、認識および個々の問題解決能力（Probst et al. 1999）の統合として理解することにします。したがって、知識は常に行動指向的であり個人的なものです。組織としての知識に関しては、プロボスト（Probst et al. 1999)の定義によれば、「個々の経験と集約された経験であり、全ての基礎となる情報を保有する組織が問題解決のためにアクセスが可能な認識やスキルの統合として組織が有する知識基盤」としています。

図 2 にデータ、情報そして知識の受け渡しや相互作用についてその概念を示しておきます。図 2 に示した概念が受け入れられるとすると、個人から別の個人へ、さらには組織へと直接的かつ正式な知識として受け渡しすることは可能では無いことになります。事実、知識の一部は、低いレベルへの受け渡しを行うためには、知識を要約することで理解できることもあります。その結果、相互作用としてのメカニズムは、別のレベル間で継続的に理解されるべきものです（Probst et al. 1999)。さらに、受け手が順々に情報を再翻訳しなければならないため、元の特徴が失われることもあり得ます（Boisot 1983, 1998)。さらに、ポランニ（Polanyi 1966)は、一部の知識は、明確な知識に結び付けることが可能であり、図 2 で示されるような方法で受け渡しができると指摘しています。明確な知識は、他方では、情報やデータを介して簡単に結び付けることで受け渡しが出来るものではなく、比喩や類推により個人間で直接に行う相互作用でのみ受け渡しが可能であると捉えられています。このように知識と知識創造の進化は、組織の知識基盤の質・量ともに豊かにするものです。したがって、組織学習（Probst et al. 1999）として解釈することも可能です。組織学習の有効性と効率は、企業の吸収能力（Cohne & Levinthal 1990)、企業文化（Cook & Yanow 19968)、そして洞察から成長へと新しいコンセプトに適用する企業の能力（Senge 1990）によるものであるとされています。ジュナカー（Junnarkar 1997）は、企業の挑戦は、成功や優れたコンセプトから学習することが出来るので、他の優れたコンセプトにも適用することが出来るとしています。更に、このような考え方を適用学習、あるいはシングルループ学習（既に備えている考え方や行動の枠組みにしたがって問題解決を図る）と呼ばれています。また、同時に、組織は否定的な学習やダブルループ学習（既存の枠組みを捨てて新しい考え方や行動の枠組みを取り込むことです）も受け入れる必要があり、こ

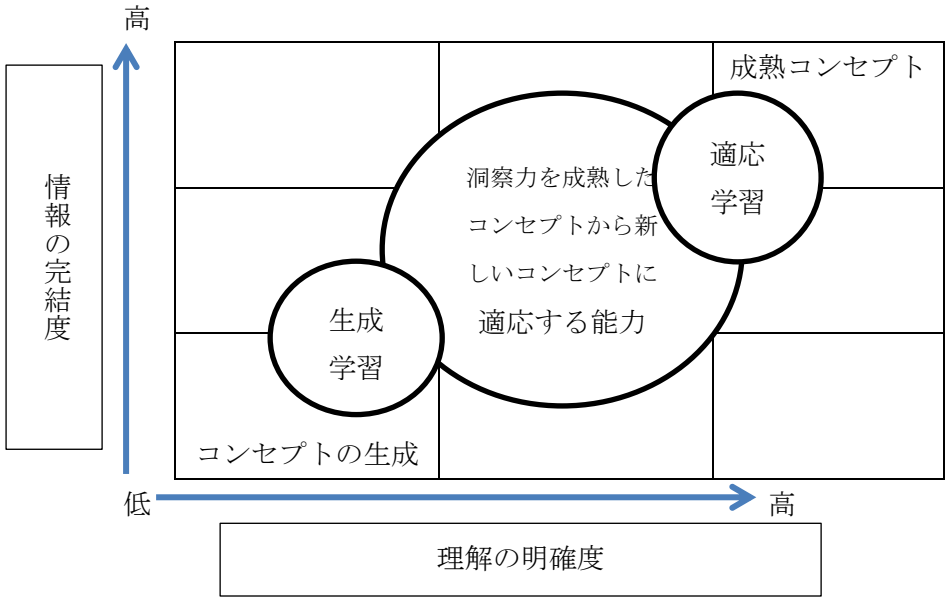
れは組織内で誕生し成長した新しいコンセプトの数を把握することで明らかにされるものです。さらに、これらの異なるタイプの学習は、組織内の別のスキルを必要とします。

組織学習の結果は、図 3 に. 示すように、新たに誕生したコンセプトから、成熟したコンセプトまでのパスそして両方のパスに共通するのは、より完成した情報とより高い理解度の両方が必要です。ここでの知識とは、企業の最も重要な資源として受け入れ、組織学習は、潜在的な競争上の優位性を得るための前提となります。



出所：Pascal Savioz.(2004). Technology Intelligence, Concept Design and Implementation in technology-based SMEs,Palgrave macmilan. pp.9 を加工

図 2.　データ、情報、知識の譲渡と相互作用



出所：Pascal Savioz.(2004). *Technology Intelligence,* Concept Design and Implementation in Technology-Based SMEs, Palgrave Macmilan. pp.10 を加工

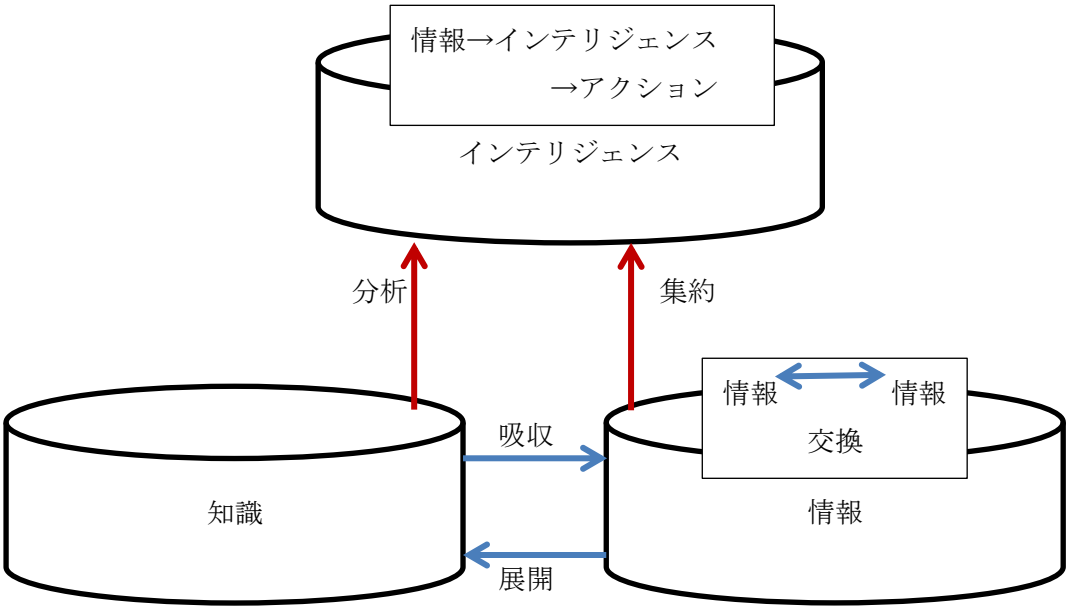
図 3.　適応学習対生成学習

3.1.　早期警戒のためのインテリジェンス

知識をどのように理解するかの概念については、既に前章で概説した知識とインテリジェンスの間には非常にあいまいな違いのみが存在していると思います。ある者はインテリジェンスを知識の同義語として理解しており、他の者はインテリジェンスを情報と知識の間にある、「何か」であるとして理解している研究者もいます。

フルド（Fuld 1995)は、「分析された情報」として議論し、プレスコットやスミスは、（Prescott、Smith 1989)は、「インテリジェンスは、信頼性と意味が確定された情報である」と言明しています。ベヤント（Bryant et al. 1997）は、行動関係を強調し、「インテリジェンスは、意思決定が可能な限界まで分析された情報」であるとしています。

ここでは、ビジネス活動におけるリスクの早期警戒(Gilad, 2004)として利活用するためのインテリジェンスとして捉えるためには、リスク・アススメント（評価）の最初のプロセスとなるリスクを早期に特定化し警戒に資するために「分析された情報でリスクを特定化し最良のリスク対応を行うための意思決定に資するために分析された優れた情報」と理解することにします。したがって、インテリジェンスそのものは、知識とは対照的ですが行動指向ではないために、リスク対応の行動を起こす基本（たとえば決定を促す）を確固たるものにする役割があると考えます。また、理解の明確度の深さと情報の完結度は、状況に左右されることになります。さらに、知識とは違い、インテリジェンスは個人的なものではないと言うことが大きな違いです。図 4 に情報、知識とインテリジェンスの相互作用を概念的に示しておきます。



出所：Pascal Savioz.(2004). Technology Intelligence, Concept Design and Implementation in Technology-Based SMEs,Palgrave macmilan. pp.12 を参考

図 4.　情報、知識とインテリジェンスの相互作用

3.2.　情報とインテリジェンスは違う

リスクを早期に特定化するために情報を収集・分析・加工をすることで優れたリスク対応とその処理をするための意思決定を行うためには、収集した情報からインテリジェンスをクリエーションしなければならなりません。つまり収集した情報から知力・想像力の産物として生成するためには、組織（企業）としてインテリジェンス活動を行うことが必要不可欠である。しかし、インテリジェンスの定義とその活動に関する概念あるいは定義は、情報を扱う軍事・政治・ビジネスなどの分野により異なります。

ヨーロッパ諸国、特にドイツには大量の難民が押し寄せており、受け入れには多くの問題・課題がありますが、特に各国を悩ましているのは難民と称してテロリストも受け入れているのではないかが危惧されています。難民とテロリストを選別することは極めて難しい様であるが、「言葉」で見分けるしか方法が無いとも言われています。例えば、出身地の言葉の「なまり」を持っているかなどです。このように分析・評価された正しい情報を選別することは、リスク対応には欠かせないことは言うまでもありません。

グローバル化の進展は情報伝達が切れ目なく、かつ驚異的な速度で伝播することで「情報が普遍化」します。つまり、情報収集と言う意味では、どこの面あるいは場所を切り取っても良く似ている情報が手に入ることになります。同じような情報が大量に出回り入手できる環境の中では、物事がますます普遍化することで誰でもが類似した情報を手に入れ

ることが可能となります。つまり氾濫した情報の中から正しい情報を得るためには、当然時間とコストがかかります。

本来、情報の価値は、収集された情報を分析し評価した上でクリエーションされるものであり、単に情報と言う文言だけであれば、何か特段の意味を持っている訳ではありません。情報の価値は収集された情報を分析・評価することからクリエーションされるので、分析の信頼性を確保するためには、時として膨大な情報を収集する必要があります。分析・評価された情報は、組織（企業）では意思決定を左右するような極めて優れた情報、つまりインテリジェンスとして最高経営責任者や意思決定者により利用されることになります。ここで言う意思決定者とは、リスクを特定化し対応策をマネジメントする責任者を指します。

ここで、表 1 は世界の研究者が定義している代表的な「インテリジェンスの定義」を整理したものです。

表 1. インテリジェンスの定義

国語辞典 Google 辞書	1. 知性，知能，理解力　2. 情報，諜報
Sherman Kent	インテリジェンスとは知識である，そして組織であり活動である。
北岡　元	「インフォメーション」を収集し，それを分析して生産されるもので，「判断・行動のために必要な知識」。
手嶋　龍一	「収集した情報を精査し，裏を取り，周到な分析を加えたインフォメーション，それが「インテリジェンス」」。
小谷　賢	「インフォメーションはただ集めてきただけの生情報やデータ，インテリジェンスは分析・加工された情報」。
中西　輝政	まず，第一に，国策，政策に役立てるために国家ないし国家機関に準ずる組織が集めた情報の内容を指す。二つ目に，「インテリジェンス」という語には，そういうものを入手するための活動自体を指すという場合がある。それから，三つ目に，そのような活動をする機関あるいは組織つまり「情報機関」そのものを指す場合がある。
菅澤　喜男	インテリジェンスとは，「分析された優れた情報」であり，「信頼性と意味が確定された情報」。
2006 年 3 月 28 日 小泉政権下での政府答弁	一般に，知能，理由，英知，理解力，情報，知的に加工・集約された情報等を意味するもの。
日本コンペティティブ・インテリジェンス学会 Intelligence	目的に応じて必要な情報を収集し調査・分析。評価することで，意思決定に資する価値ある情報として新たに生成されたものである。

Management, Vol.5, No.1/2014)	

出展：菅澤 喜男(2014): インテリジェンス・マネジメントが目指すもの、日本コンペティティブ・インテリジェンス学会、Intelligence Management、Vol.5, No.1（2014）

インテリジュエンスに関する各種の考え方を概観して見ると、それぞれの専門領域でのインテリジェンスの重要性が叫ばれています。例えば、ビジネスにおけるリスクを早期警戒するために必要なインテリジェンスは、リスクとインテリジェンスの関係から捉えるとするならば、デロイトが提唱するリスク・マネジメントの進化形とされ、「守りに入るのではなく、賢くリスクを取りながら事業価値の向上に貢献する」が上手くあてはまるように思います。

日本型の組織の一つの特徴として、縦割的な組織で意思決定が行われると言われますが、インテリジェンスの世界では意思決定者とインテリジェンス・コミュニティ（ここでコミュニティとは企業内組織であれば数人、外部の組織との連携であっても決して大人数では無いのが一般的です）と呼ばれるグループが情報収集・分析・評価を行い、その結果を報告する相手（つまり顧客としての意思決定者）とが直結した組織がインテリジェンスを利活用するためには相応しいと考えられています。日本コンペティティブ・インテリジェンス学会の定義は、日本型の意思決定プロセスの中で如何にインテリジェンスが利活用されるかに重点を置いた定義であると言えます。

4. インテリジェンスとして取り扱う情報の種類

インテリジェンスとして取り扱う情報の種類は多種あるが、ここでは比較的良く知られている８種類を紹介しておきます。

①公開情報：オシント(Osint(Open Source Intelligence)
②信号情報：シギント(Sigint: Signal Intelligence)
③人的情報：ヒューミント（Humint: Human Intelligence)
④視覚情報：イミント(Imint: Imagery Intelligence)：視覚情報を収集する。
⑤測定値・記号情報：マシント（Masint:Measurement & Signatures Intelligence)
⑥電子的情報：エリント（Elint: Eletronic Intelligence)
⑦地理空間情報：ゲオント（Geoint：Geospatial Intelligence)
⑧電子計算機・通信ベースの情報：コミント(Comint: Computer/Communication Intelligence)

情報化時代にいて提供される情報は実に膨大かつ多種多様であり、その流通経路も多岐に渡り、情報発信者からは利用者の姿は見えない存在であり、情報は正と負のリスクとなり得ます。特にインテリジェンスの利活用において最も重要視されているのは、シギントとヒューミントです。さらに、極めて重要な意思決定を行う際に求められる優れた情報は、

アナログ的な情報です。つまり人間が持っている情報と言うことになります。

ここで、シギントの種類については、次のような種類がある。

- 通信情報（COMINT、Communication intelligence）
  - ・傍受、盗聴、暗号解読
  - ・無線通信の類は、暗号の解読だけでなく量や頻度といった解析（通信解析）も大きな手がかりになるが、そういったものはOSINTの手法となる。
- 電子情報（ELINT、Electronic intelligence）
  - ・非通信用（レーダー等）の電磁放射からの情報収集。
- 外国信号計測情報（FISINT、Foreign instrumentation signals intelligence）
  - ・テレメトリー、ビーコン信号等からの情報収集。
- 音響情報（ACINT、Acoustic intelligence）
  - ・SOSUSなどからの水中音響情報などによる潜水艦、艦船および水中武器の音響情報収集。

表2.　知られているシギントの収集を行っている各国の情報機関

機関	英文	国
国家安全保障局	National Security Agency（NSA）	アメリカ合衆国
政府通信本部	Government Communications Headquarters(GCHQ)	イギリス
政府通信保安局	Government Communications Security Bureau(GCSB)	ニュージーランド
警察庁警備局、防衛省情報本部、陸上自衛隊通信団、外務省大臣官房情報通信課	警察庁 National Police Agency(NPA) 防衛省 Ministry of Defense(MOD) 情報本部 Defense Intelligence Headquarters(DIH)	日本
軍事偵察局	La Direction du Renseignement Militaire;(DRM)	フランス
連邦保安庁、連邦軍参謀本部情報総局	連邦保安庁：Federal Security Service of the Russian Federation(FSB) 連邦軍参謀本部情報総局：Glavnoye Razvedyvatelnoye Upravleniye、（GRU）　英：Main Intelligence Directorate of the General Staff	ロシア
国防電波局	Försvarets radioanstalt（FRA）	スウェーデン
中国人民解放軍総参謀部第三部（技術偵察部）	China PLA General Political Department	中国

連邦情報局第二課	Bundesnachrichtendienst;（BND） 英：Federal Intelligence Service	ドイツ

※Wikipedia より　2015/12/05 まで

次に、ヒューミントを収集している各国の情報機関は、次のような機関があります。

表 3.　知られているヒューミントの収集を行っている各国の情報機関

機関	英文	国
中央情報局	Central Intelligence Agency（CIA）	アメリカ
ロシア連邦対外情報庁	Federal Security Service of the Russian Federation（FSB）	ロシア
イギリス情報局秘密情報部	Secret Intelligence Service（SIS）	イギリス
フランス陸軍情報旅団情報編集グループ	Brigade de renseignement：BR）	フランス
イスラエル諜報特務庁（モサッド）	HaMossad leModiʿin uleTafkidim Meyuḥadim　（スウェーデン語？）	イスラム
公安警察（警視庁公安部、各県警察本部警備部等の俗称）、法務省公安調査庁、陸上自衛隊中央情報隊	英: National Police Agency, NPA 英：Public Security Intelligence Agency, PSIA 英：Military Intelligence Command：MIC	日本
朝鮮人民軍偵察総局	正確な英文名は不明	北朝鮮
中国人民解放軍総参謀部第二部（総参謀部情報部	正確な英文名は不明	中国
連邦情報局 第一課	Bundes Nachrichten Dienst; BND、 英：Federal Intelligence Service	ドイツ

※Wikipedia より　2016/1/20 調べ

5.　的確な情報収集と利活用

インイェリジェンスを如何に上手く利活用するかは、日本型の組織としては難しい面があります。つまり、縦割り組織とミドルアップ的な意思決定プロセスの中で正確な情報をどのように収集し、その結果を意思決定者に伝えるかが問題となります。解決策の一つとして考えられるのは、少人数構成でインテリジェンス担当部署を設け、意思決定者との連携が出来るような仕組みを構築することが良いと考えます。欧米企業では、インテリジェンスの利活用は極めて盛んであり、その利活用の多くはリスクを事前に回避するための早期警戒、つまりアーリーワーニング(Gilad, 2004)としての活動です。

インテリジェンスを組織として利活用するための一連のプロセスとしては、米国の中央インテリジェンス局（CIA：Central Intelligence Agency）が提唱したインテリジェンス・

サイクル([菅澤, 2015)呼ばれるサイクルで行うことが良いとした方法があります。ここではリスク対応と早期警戒を中心としたプロセス例を図.5 に示します。

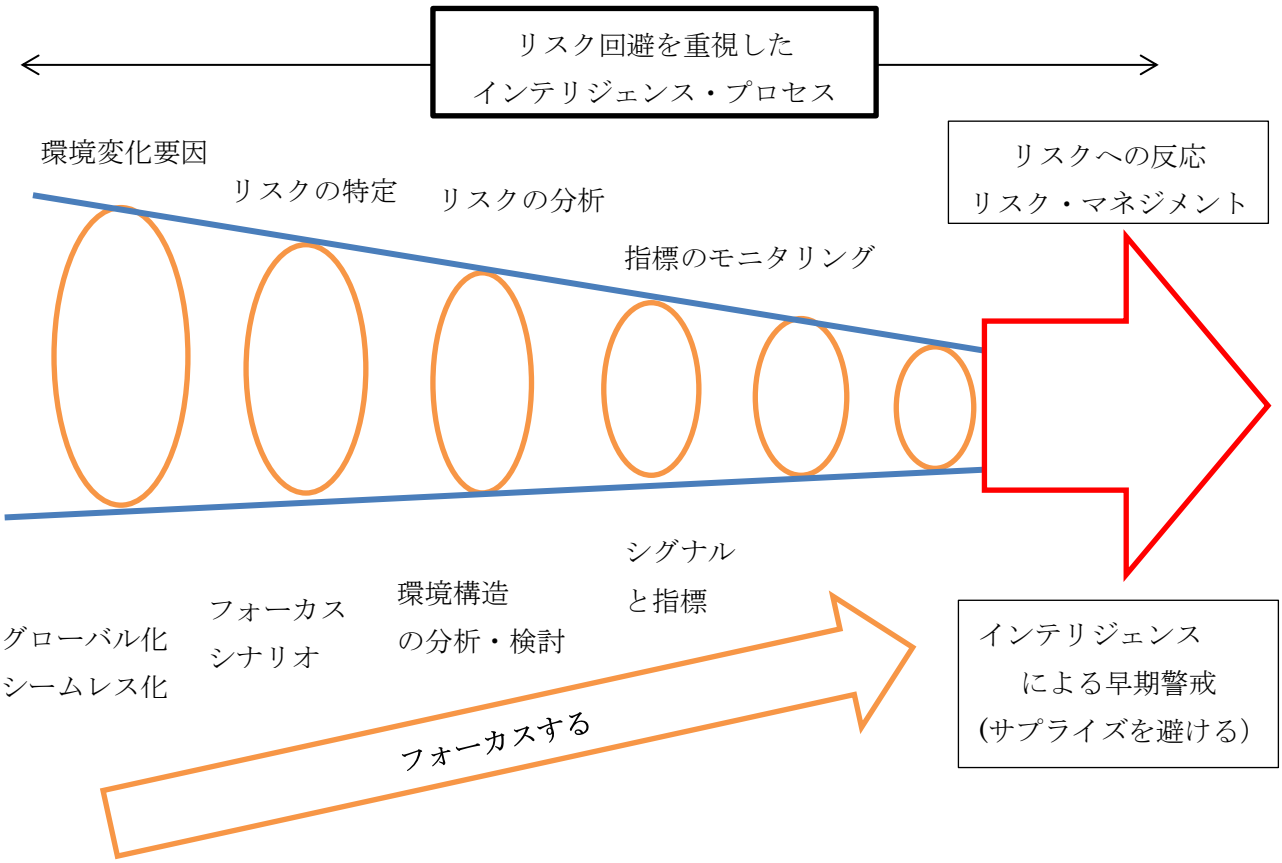


図 5. リスク対応としての早期警戒を中心としたインテリジェンス・プロセス

6. リスクが発生する可能性のあるところからシグナル（信号）を捉える

リスクの発生について国際標準化機構（ISO）のガイドライン「リスク・マネジメントの用語、規格における使用するための指針（ISO/IEC GUIDE 73:2002)」によれば、事象の発生確率と事象の結果と定義しています。また、リスク・マネジメントでは、損失だけを負のリスクとするのではなく、プラス要因としての利益を得るリスクを正のリスクも考慮されるべきです。その後に改訂された Guide73:2009 では、「目的に対する不確かさの影響」としています。この不確かさとは、確率を意味しており「不測の事態」をどのように捉えるかを問題としています。

リスクはどのような形で目に見えて来るかは予測がし難いために、リスクが発生するであろう環境に焦点を当て、その意図・動機・目標などについて組織の状況を直接的あるいは間接的に示す必要があります。インテリジェンスを利活用する基本は情報収集にありま

すが、求める必要な情報がどこにあるのかは、あるいは何処に潜んでいるかは、リスク分析者としてある程度の経験と知識が求められます。多種多様かつ複雑に絡み合った情報は、リスクが潜んでいると思える環境、場所などで発生しシグナル（信号）として発信されています。リスクとなり得る兆候はシグナルとして認知できる場合がありますが、リスクに関するシグナルの中には、脅しもあれば警告を与えることもあり、ある種の特別な行動(あるいは現象など)の兆候として捉えることができます。

ここで組織（企業）が取る行動がリスクとなる場合を例として、リスクがシグナルとして現れる幾つかのパターンを捉えてみます。リスクをシグナルとして捉える目的と必要性は、次に示す４項目に集約されることが知られています。

① リスクとなる相手（あるいは対象）は、その行動を通じて、さまざまな方法でシグナルを出している。シグナルの中には、脅しもあれば警告を与えることもあり、ある種の行動の兆候として捉えることができるものがある。

② リスクとなる相手が取る行動の全てでは無いが、その大部分がリスクとなる相手の動向を知ることで自らがリスクを避けるための戦略策定にとって有用な情報をもたらす。

③ リスクとなる相手のシグナルを正確に読み取れば、リスク回避のために必要な戦略策定上、極めて役に立つ。

④ 優れたシグナルを捉えることができるならば、リスクとなる相手の脅威とその戦略および能力を把握するためには有効である。

6.1. リスクがシグナルとして認知される９つのリスクタイプ

リスクとなり得るシグナルは、次に示す２つの相反する役割を持っています。

① リスクとなり得る相手の動機、意図、目標を示す手がかりとなるシグナル

② 真実を隠す見せ掛けのシグナル

次に、良く知られているシグナルとしては９つのタイプがあります。

（タイプ１）事後の発表

・事後の発表は、発表した組織（企業）自身がその公開した情報に注目されたことで、「競争相手などの行動に変化が生じるかもしれない」ということを発表した組織（企業）が確認するためになされる。

・リスクとなり得る競争相手などが新たな設備拡充、販売実績など、既に完了した事柄を発表する場合が大半である。

（タイプ２）業界事情についての競争相手からのコメント

・リスクとなり得る競争相手などが、その業界の状況についてのコメントを発表することは珍しくない。

・リスクとなり得る競争相手などが業界の需要動向や価格の予測、将来の生産能力の推定、原材料の高騰など、外部要因の重要性に関するコメントである。

・このようなコメントが、業界についてリスクとなり得る相手であるが、例えばライ

バル企業などが抱いている仮説を明らかにし、恐らくその仮説に基づいて策定されるであろう戦略を知る手がかりが得られるからである。

・例えば、業界に関するコメントなどは、自らの組織以外の組織にも同じような仮説を抱かせ、誤解や争いが起こることを最小限に抑えようとする意識的あるいは無意識的な試みと言える。

（タイプ３）自らの行動についてのコメントと説明

・　自らの行動に関する説明は、意識的か無意識的かは別として、少なくとも次の３つの役割がある。

① その動きの必然性を他社に納得させ、その動きに追従されるか、あるいは、その動きを挑発と受け取らないようにさせる役割がある。

② 顧客の囲い込みなどを目的とした意志表示としての役割がある。新たな事実の発表や計画など、膨大な資金と困難が伴うことを過大に発表することである。その背景には、リスクとなり得る競争相手などに同様な分野への野望出を思いとどませるとの狙いがある。

③ 自らが資源を大量に投入し、長期に渡り、その新しい目的向って注力することを約束することで、リスクとなり得る競争相手などの意欲を封じ込むためである。

（タイプ４）リスクとなり得る競争相手などの現在の戦略と実行可能ではあったが実行しなかった戦略との比較

・実際には選択できたのに、選択せずに別の弱気な戦略をとったということは、自らの組織以外の組織を懐柔する意図を示すシグナルである。

・例えば、シグナルとして通常は出さない、価格、広告費、設備拡充、改良点など、リスクとなり得る相手に関するある種の動機について重要なシグナルを提供してくれる。

（タイプ５）新しい戦略の導入方法

・狭い地域での活動に向けた発表なのか、あるいは当初より主要な地域に向けて強引に発売されたのかと言った、新しい戦略の導入のされかたもリスクとしてのシグナルとなる。

（タイプ６）過去の目標とのズレ

・どのような戦略要素においても、これまでの目標との間にズレが生じた場合は、そのズレに注目しシグナルの意味を探り、リスクとなり得る競争相手などの分析を行なわなければならない。

・例えば、高級品だけを生産していた企業が、普及品の生産に踏み切った場合などは、その企業の目標あるいは仮説に大幅な変更があったことを示すリスクとなり得るシグナルとなる。

（タイプ７）業界で前例のない行動

・業界の規範からずれた行動は、普通は攻撃的なシグナルとみるべきである。

・例えば、過去に一度もディスカウントしたことが無い企業がディスカウントをしたなどがある。
・予想をしていなかった国あるいは地域に、新規工場を建設するなどが危険なシグナルとなる。

（タイプ８）間接的な反撃

・間接的な攻撃とは、ライバル関係にあるリスクとなり得る競争相手などの動きに直接対抗するのではなく、間接的に対抗する手を打つことである。
・例えば、ライバル関係にあるリスクとなり得る競争相手などに対して不快なシグナルを表明し、進出してきた相手に近い将来重大な反撃を加えるという意思表示となる。
・もし、間接的な反撃が、ライバル関係にある競争相手などの「飯の種」になっているような場合であれば、重大な警告シグナルと見るべきである。

（タイプ９）攻撃用のブランド

・間接的な反撃と関連のあるシグナルである。リスクに成り得る競争相手などの脅威にさらされているか、あるいはさらされる恐れがある組織は、その脅威の元になっている組織を「コラシメル」だけの効果をもつ攻撃的な方策を講じることがある。
・この目的以外に攻撃用の方策は、リスクとなり得る競争相手などに対する警告、抑止、もしくはその攻撃の「ほこさき」を吸収するための「攻撃専用部隊」のようなものである。
・攻撃専用部隊は、リスクとなり得る競争相手などからの重大な攻撃の開始に先立ち、ひっそりと情報を公開することなく行動することに注意すべきである。これが、リスクとなり得る競争相手などへの警告となる。このようなリスクに関するシグナルは、大規模なプロパガンダの中で攻撃手段として用いられる場合に多く見受けられる。

他にも間接的な反撃として、リスクとなり得る競争相手などの動きに直接抵抗するのではなく、間接的に対抗するような手段を講じる場合がある。あるいは攻撃用の方策を用意することで、リスクとなり得る相手からの脅威に対して、戒めのための目的だけの攻撃手段を試す場合がある。

7.　微弱なシグナルはリスクとして早期警戒が必要

素早い変化に基づくリスク対応の中で営まれるマネジメントでは、組織（企業）が有するあらゆる資源を賢明に管理・運営することが重要かつ必要不可欠です。そのためには様々な環境に対して正確かつタイムリーな情報が必要です。さらに、全体的におとなしい環境で変化が少ない社会ほど、人間の主張が過激さを見つける情報に偏ることで、意外性を見出すリスクとチャンスの両方が増大するとも言えます。また、収集した情報が正確であればあるほど、過激な情報になることがあるので、意思決定者あるいはリスク管理者は敬遠

（時として逆鱗に触れることもあります）したいとの意識が強くなることにも注意を払うべきです。

シグナルとは、組織（企業）の意図、動機、目標、もしくは自らの組織内の状況を直接あるいは間接的に示す行動でもあります。特に微弱なシグナルからもたらせるリスクは、変化の兆候であり早期警戒として細心の注意が必要です。いかなる組織（企業）も情報あるいはシグナルを出すことなく、社会で活動することは困難です。

8. インテリジェンスの政治化を避ける

インテリジェンスは、当然正しく利活用されるべきです。しかし、意思決定者にとり都合の良い情報だけをインテリジェンスとして報告することにより、リスクの取り違いや意思決定を誤ることが起こり得ます。これはインテリジェンスの政治化と呼ばれ、いわゆる情報操作ともいえる歪曲された情報を提供することで、自分に有利な条件あるいは意思決定を促すものです。リスクを特定化することで自身が危害を被る場合等は、様々なインテリジェンスの政治化が横行することになります。つまりインテリジェンスの政治化とは、意思決定者あるいはインテリジェンス結果の報告者のどちら側にとって都合の良い情報だけを信じることです。例えば、儲からないギャンブルと知りながらも止められない理由として、トーナス・ギロビッチ著、人間この信じやすきもの]新曜社刊　意思決定のためのリスクマネジメント　ページ 161 によれば、「人は勝った時と負けた時の記憶を極めて巧妙に改変するために、懲りもせずに過ちを繰り返す。自分の信念に都合の悪い情報を都合良く解釈しようとしているのである」と指摘していることからもうかがい知ることができます。

最近ではイラク戦争開戦に関する、アメリカの CIA がブッシュ大統領に提出した報告書が典型的な「インテリジェンスの政治化」と呼ばれています。周囲にある問題として、どのような状況であれ重要な決定を行う意思決定者に対して、正しいインテリジェンスを提供できる組織（企業）風土を醸成しておくことが重要です。

9. インテリジェンス調査の実際

インテリジェンス調査に関する報告書は、調査依頼者側以外の者が目にすることはありません。組織（企業）の最高意思決定に資する内容が含まれているためです。もし、インテリジェンス調査報告書を調査依頼者以外で見たと言うことであれば、それはインテリジェンス調査ではありません。欧米では、インテリジェンス調査は、多くの場合はインテリジェンス調査を専門にしているエージェントが行います。当然ですが、調査を行う前には調査依頼者側と調査を実施する双方とが機密保持契約(NDA)を締結します。さらに、インテリジェンス調査は、情報収集の対象が極めて具体的であり、一般的には KITs(Key Intelligence Topics)と呼ばれる箇条書になっている対象となる収集すべき情報内容が調査依頼者側から調査開始前に示されます。

私自身が過去 10 年余りで行ったインテリジェンス調査を実施した例としては、次のよう

な内容です。

① ヨーロッパ市場における認証制度を運用している実力者名と所属機関名

② 社会インフラとしての交通網整備を検討している国から見た輸出国側の政策と様々なメディアから発信されたシグナルを期間を限定した上で収集する

③ 日本企業の海外工場の従業員のモラルと生産能力

などがあります。

エージェントからのインテリジェンス調査報告は、調査依頼者側の意思決定あるいはリスクの早期警戒に資する内容です。しかし、インテリジェンス調査を実施すれば、KIT's に従って収集される全ての情報が集まることはありません。一般的には、90%程度の情報が経験的に見て集まります。未収集の 10%程度の情報については、概ね推測が出来るようになります。

文献

Boisot, M.H. (1983). Convergence Revisited: The Codification and Diffusion of Knowledge in a British and A Japanese Firm: Journal of Management Studies, Vol. 20(1), pp.159-190.

Boisot, M.H. (1998). Knowledge Assets: Securing Competitive Advantage in the Information Economy. Oxford, Oxford University Press.

Bryant, pp.J. Coleman, J.C. & Krol, T.F. (1997). Organizing a Competitive Technical Intelligence Group: Ashton, W.B. & Klavans, R.A. (eds.), Keeping Abstract of Science and Technology: Technical Intelligence in Business. Columbus, Ohio, Batelle Press.

Cohen W.M. & Levinthal, D. A.(1990). Absorptive capacity: A New Perspective on Learning and Innovation, in: Administrative Science Quarterly, Vol. 35(1), pp. 128-52.

Cook, S.P.N. & Yanow, D.(1996) Culture and Organizational Learning, in Cohen, M.D. & Sproull, L.S. (eds), Organizational Learning. Thousand Oaks, Sage Publishings.

Davis, S.& Botkin, J.(1994). The Coming of Knowledge-based Business, in：Harvard Business review, Vol.71(5), pp.165-170.

Fuld, L.M.(1995). The New Comtitor Intelligence: The Complete Resorce for Finding, Analyzing and Ushing Information About Your Competitors, New York, John Wiley & Sons.

Gilad Benjamin.(2004). Early Warning, American Management Association.

Junnakar, B.(1997). Leveraging Callective Intellect by Building Organizational capabilities, in：Expert Systems with Applications, Vol.1381), pp.29-40.

Senge, PP.(1990). The Fifth Discipline. The Art and Practice of the Learning Organization. New York, Currency / Doubleday.

菅澤喜男(2015). 諜報機関から学ぶ競争競合相手分析と戦略シナリオ～公開情報は宝の山～、監修：日本コンペティティブ・インテリジェンス学会、ヴィジ・インテリジェンス出版、電子出版・コンテン堂（http://contendo.jp/）

Prescott, J.E. 6 Smith, D.C. (1989). A Framework for the Design and Implementation of Competitive Intelligence Systems, in:Snow, C.C. (ed), Strategy, Organization design, and Human Resource management. Greenwich, C.T, Jai Press.

Probst, G.J.B., Raub, S. & Romhard,(1999), Wissen managen. Frankfurt/Wiesdaden, Frankfurter Allgemeine, Gaber.