# 日本政府の情報機能（第２回）
## ～その課題と機能強化への処方箋を考える～

市ヶ谷台論壇　会員
斉藤　敏夫

本論考は、日本政府の情報機能の課題と機能強化のための処方箋について論じ考察するものであるが、今回（第２回）及び次回（第３回）では、本論の内容を理解するために必要な情報機能の概要（基礎的知識）につき、述べることとする。今回（第２回）は、①基本用語、②情報機関の任務、③情報サイクル及び④主要情報源について解説し、次回（第３回）は、⑤カウンターインテリジェンス及び⑥政策・運用部門と情報部門との分離と連接について述べる。

## 第１章 情報機能の概要

### 第１節　基本用語

前回（第１回）の序論で指摘したが、日本政府の情報機能を論ずるに当たり必要となる基本的な用語について、日本政府内で共有されている定義が不明である。もちろん、政府内の各情報機関では、日々の情報業務を行うに当たって共通の言語を必要とすることから用語集のようなものは存在するのであろうが、内閣官房が従前から取りまとめている各種公表資料にも、例えば「情報」という言葉の定義が明記されていない。このような事情もあり、本節では、以後、論を進めていくために必要最小限の基本用語について解説する。

#### （１）　インテリジェンス、インフォメーション及びデータ

多くの論者が指摘するように、日本語の「情報」は、「インテリジェンス（Intelligence）」と「インフォメーション（information）」の両方の意味で使われており、まず、これら用語を解説する。また、後述する「処理・解析（processing and exploitation）」という情報サイクルのひとつの段階に当たる言葉を理解するためにも、「（生）データ（(raw) data）」という言葉についても説明する。

本論考では、原則として、米国の情報機関又は国防省（米軍）で使用されている定義をそのまま使用することとしたい。その理由はいくつか挙げられるが、まず、定義が簡潔で理解し易いことが上げられる。また、日本の同盟国であり、平時から重大緊急事態や有事に至るまで共同して対処することを想定する米国（米軍）とは、共通の言葉使いをすることが望ましいこと等からである。

インテリジェンス（intelligence）とは、「外国、（潜在的に）敵対する軍隊若しくは武装集団、又は実際の若しくは潜在的な作戦地域（以下「外国等」という。）に関する有用なインフォメーションを収集、処理、統合、評価、分析及び解釈した結果作成されたもの[1]」を言い、「インテリジェンス・プロダクト（情報成果物）」と呼ぶ場合もある。要するに、インテリジェンスは、情報の提供を受ける者（情報要求者、カスタマー）のニーズを満たすべく作成されるプロダクトであり、その内容には、テーマ・課題、関連する事実関係（経緯、新たな事実等を含む）、

それらに基づく分析、評価、今後の見通し・留意点を含み、かつ、政策判断や意思決定に関する提言を含まないものが一般的である。提言を情報プロダクトに含むべきでないとする理由は、情報部門の任務は、カスタマーへの情報の提供までであって、カスタマー（政策・運用部門）による判断や意思決定に影響を与えるべきではない、との考えからである。なお、インテリジェンスという言葉には、プロダクトを生み出す活動[2]を意味したり、そのような活動を行う機関[3]を意味したりする使い方があるが、それらの意味で使う場合、本論考では、それぞれ情報活動、情報機関と呼ぶこととしたい。

一方、インフォメーション（information）は、後述する生データ（Raw Data[4]）を処理・解析（processing[5]and exploitation[6]）して得られる有用な事実を言い、「素情報又は情報素材」と呼ぶ場合もある。一般的に、収集する生データは膨大なものとなる以上、生データから引き出されるインフォメーションは、インテリジェンス作成のための分析に有用なものでなくてはならない。要するに、情報機能でいうインフォメーションは、分析作業に役立つものであって、無用なもの（ノイズ）まで分析官は必要としない。このように、収集される生データを処理し（processing）、処理して得られるインフォメーションを十分活用して（exploit）有用なインフォメーションに変換する過程が「処理・解析」の段階に当たり、この段階は情報活動の中では目立たないかもしれないが、実は非常に重要な段階である。

例えば、対象国のとある目標に関する信号情報（SIGINT[7] Information）を収集していたとして、日々の収集量は膨大なものとなり得るが、暗号化された信号情報の場合には、それを解読し[8]文字化（処理）して、得られたインフォメーションを活用して有用であると思われるものについては、必要に応じ邦訳及び解説や関連する事項を付して信号情報を作成することとなる。膨大な収集生データの中に、今まで気づかなかった有用なインフォメーションが埋もれているかもしれない。このような場合、処理・解析要員は、自らの判断で又は分析官等からの要求に応えるべく、大量の生データから有用なインフォメーションを引き出す専門性の高い業務を担うこととなる。なお、後述する他のシングルソース・インフォメーション（地理空間情報（ＧＥＯＩＮＴ）、人的情報（ＨＵＭＩＮＴ）など）に係る「処理・解析」作業もそれぞれの特性に応じた専門性の高い作業となるが、ここでの説明は割愛する。

### （２）　カスタマー

情報機能におけるカスタマー（「ユーザー」ともいう。）とは、安全保障に関する政策判断や意思決定に携わる者であって、情報（インテリジェンス及びインフォメーション）[9]を要求し提供を受ける、通常、情報機関の外に所属する者をいう[10]。従前から、日本政府の情報機能の強化に関する提言・報告書は、官邸における情報機能の強化に焦点を当てるものが多く、カスタマーとしては、安全保障に関する政策判断を責務とする者（国家安全保障会議の議長（内閣総理大臣）及び議員（関係国務大臣）並びにその常設事務局である国家安全保障局のスタッフ[11]）が念頭におかれている。しかしながら、カスタマーは、官邸において安全保障に関する政策判断に携わる者だけではない。集合論的には重複する部分もあろうが、外交政策に関する政策判断に関与する者（案件によっては、官邸首脳や国家安全保障会議議員もこの者に含まれる）、防衛政策や部隊運用に関与する者（同上）、領域警備に関与する者（海上保安庁等）、国際テロリズム[12]に対処する者（警察庁、案件によっては自衛隊又は海上保安庁の

特殊任務部隊[13]）も、カスタマーである。例えば、領海警備に携わり相対国への対処の最前線で任務に就く海上保安庁の巡視船の船長及び乗組員も適時なインフォメーションを必要とするカスタマーである。すなわち、情報のカスタマーは、官邸の政策判断者に限らず、適時的確な政策判断や行動の決心を求められる国（行政府）の各部署に所属する政策・運用の意思決定者及びそのスタッフ全てであると言えよう。

### （３）　情報要求

情報のカスタマーは、前項で触れた様に、官邸の政策判断者に限らず、国（行政府）の各部署に所属する政策判断者及び意思決定者並びに彼らのスタッフも対象となる。また、国民の代表者で構成される国会も政府の情報機関が提供する情報のカスタマーとなり得る場合があろう。更に言えば、同盟国及び友好国の情報機関等も、案件によっては、日本政府の情報機関が作成する情報の提供先となり得る。

情報要求の内容は、それぞれのカスタマーの情報関心事項によって異なる。政府の情報コミュニティ（ＩＣ）は、コア・メンバーたる５機関（内閣情報調査室、警察庁、公安調査庁、外務省及び防衛省）に加え、拡大ＩＣとして４機関（金融庁、財務省、経済産業省及び海上保安庁）の合計９機関から構成されている。それぞれの組織に属する政策判断者及び意思決定者並びに彼らのスタッフからなるカスタマーは、基本的には、自分たちが属する組織にある情報機関に対して、自分たちのニーズに応える（任務遂行のための意思決定に資する）情報の提供を要求することとなる。

例えば、外交政策判断に資する情報であれば外務省国際情報統括官組織[14]が、国際テロ対処に必要な情報については警察庁警備局外事情報部[15]が、防衛政策や自衛隊の行動に必要な情報については防衛省情報本部が、それぞれ、情報要求に応じたインテリジェンス・プロダクトを作成・提供する任務を担うこととなる。なお、官邸（国家安全保障会議（局）など）から外交・防衛関連及び国際テロ対処関連の情報要求がある場合には、内閣官房内閣情報調査室の他、必要に応じ、上記外交、国際テロ、防衛各分野の情報機関が対応することとなろう。

情報サイクル活動は、カスタマーによる情報要求からスタートし、それを受けて初めてインフォメーションの収集活動等を開始するとの説明が一般的である。しかしながら、現実の情報活動では、カスタマーが適切な情報要求を出すとは限らない場合がある[16]。また、カスタマーからの情報要求を待っていたのでは、適時な情報提供が出来ないこともあろう。したがって、情報機関は、通例、予め定められている情報関心事項に基づき、又は、政策・運用部門のカスタマーとの日頃の意見交換等を通じて、カスタマーによる具体の情報要求をいわば先取りして、インフォメーションの収集やインテリジェンスの作成を行うように努めているものと思われる。

## 第２節　情報機関の任務

情報機関の任務については、論者によって様々な説明がなされているし、また実際、各情報機関のウエブサイトにはそれぞれ組織の任務を記載している。本論考では次のように記すことが、簡潔で、かつ、ポイントを押さえた情報機関の任務に係る記述だと考える。それは、

「正確で（accurate)、総合的で（comprehensive)、適時な（timely）外国等に関する情報（カウンターインテリジェンスを含む）をカスタマーに提供すること[17]」
である。この記載内容につき、いくつか留意すべき点を記しておきたい。

まず、カスタマーに提供される情報が、正確で、総合的で、かつ、適時なものであることは理想ではあるが、現実にはそのようなことが常にある訳ではない、ということである。換言すれば、accurate, comprehensive, timely は、相互に相反する事態となり得る形容詞であり、三つの要素を満たすことは通常困難を伴う。

例えば、北朝鮮でミサイル発射の兆候（indications）があり、それをカスタマーに提供する必要がある場合には、正確さや総合分析を犠牲にして、適時に（この例では、迅速に）情報（indications and warning[18]）を提供する場合があろう。また、例えば対象国の内政や政治状況等、複数の情報源を使って収集活動をしても、当該国の情報保全の強度が強くて有用なインフォメーションを収集できない場合には、インフォメーション不足により信ぴょう性の低い分析しかできず、正確で総合的なインテリジェンス・プロダクトの提供とはならない場合もあろう。

したがって、正確で総合的な分析を行ったインテリジェンスを作成し情報要求に応えるためには、自前の情報収集能力の向上や同盟国や友好国との情報協力の強化等を通じ、信頼すべき複数の情報源から収集したインフォメーションを活用するとともに、既存のデータベースから関連情報（インフォメーション及びインテリジェンス）を検索した上で、より信ぴょう性の高い事実関係に基づく総合的な分析を行うよう努めることが肝要である。しかしながら、カスタマーの要求に応える質の高いインテリジェンスの作成ができるかは、最終的には、インテリジェンスの作成に携わる分析官らの専門性・多様性、そしてセンス・洞察力に頼ることになる。

また、情報を適時にカスタマーへ提供するためには、予め定められている情報関心事項に基づき、又は、カスタマーからの情報要求を予想して、インフォメーションの収集やインテリジェンスの作成を行うように心がける必要がある。

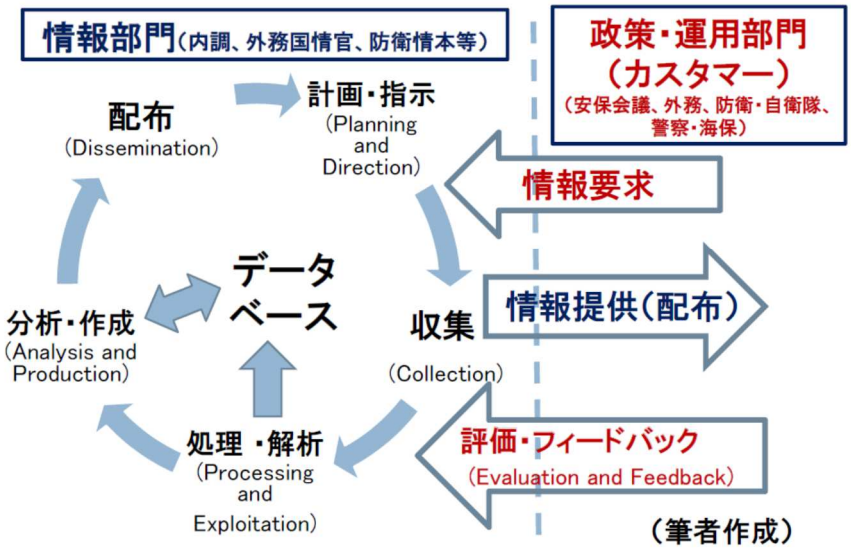
上記情報機関の任務の内容につき、最も留意すべき点を指摘しておきたい。それは、情報は、カスタマーに対して提供されるのであって、カスタマー以外へ提供（漏えい）してはならない、ということである[19]。このためには、次節で述べる情報サイクルにおける活動全般に亘り、保全上の手続きによらない故意又は過失による情報の漏えいや情報の不正取得が発生しないように、人、施設及び情報通信システム上の保全措置を行うことが必要不可欠である。この点については、カウンターインテリジェンスの解説で、改めて言及することとしたい。

## 第３節　情報サイクル

情報（インテリジェンス）サイクルとは、カスタマーからの情報要求に応えるべく、情報機関が行う情報活動を概念的に説明する場合に使用される用語である。「情報プロセス」と呼ぶ場合もある。論者によって、情報サイクルの各段階の区分の仕方が異なる場合があるが、本論考では、計画・指示 (Planning and Direction)、収集 (Collection)、処理・解析（Processing and Exploitation)、分析・作成 (Analysis and Production)、配布 (Dissemination) 、及び評価・フィードバック (Evaluation and Feedback)の６段階で説明を行うこととする。

情報機関における情報サイクル活動とカスタマーとの関係を概念図（一例）として表すと、＜図１＞のようになる。

＜図1＞情報サイクルの概念図




（１）　計画・指示(Planning and Direction)及び評価・フィードバック(Evaluation and Feedback)

「計画・指示」とは、カスタマーからの情報要求を受け又は予想し、インテリジェンス作成に関する計画を立案し、関係機関（部署）に対してインフォメーションの収集等の指示を行い、インテリジェンス・プロダクトのタイムリーな提供を管理することをいう[20]。また、情報サイクルの第６段階目に当たる「評価・フィードバック[21]」は、カスタマーからの情報要求を満たしているか等を確認し、以後のプロダクト作成への反映やその他情報サイクル全般業務を評価・改善することであるが、この業務も「計画・指示」担当部署が関わる仕事である[22]。

「計画・指示」を担当する部署は、それぞれの情報機関に置かれている。現行の組織を前提に述べると、官邸（内閣官房）のカスタマー（官房長官、官房副長官及び彼らのスタッフ）からの情報要求については、原則として、内閣情報調査室の「計画・指示」担当部署[23]が、情報要求の内容に応じ、収集等の計画・指示を行うこととなる。また、各情報機関により構成される合同情報会議において、情報評価書作成計画を作成する場合もあろう。外務省や防衛省等のカスタマーからの情報要求を受ける情報機関は、一義的にはそれぞれの組織にある情報機関である。各情報機関（部署）には「計画・指示」担当部署又は担当官が置かれており[24]、プロダクト作成のためのインフォメーション収集を含む諸活動を管理する任を負っている。

（２）　分析・作成 (Analysis and Production)

通例、情報サイクルの解説では、「計画・指示」の次に「収集」を説明するが、本論考では先に「分析・作成」を説明する。「分析・作成」とは、「処理・解析」されたインフォメーション、又は、既存のデータベースを活用して、それらを分析等した上で、インテリジェンスを作成することである[25]。カスタマーからの情報要求に情報機関が十分応えているか否かは、ひとえにインテリジェンス・プロダクトの出来栄えにかかっており、その主役は「分析・作成」

担当部署の分析官ら及びそのチームリーダーである。プロダクト作成に当たり、具体的にどのようなインフォメーションを求め、又は、何に着目してデータベースを検索して事実関係を整理の上、分析等してプロダクトを作成するかは、基本的には彼らの技量にかかっている。したがって、インフォメーションの「収集」要求は、「計画・指示」担当部署から概要の要求は行うのであろうが、細部に亙る具体的なインフォメーションの要求は、「分析・作成」担当の部署からのものとなる。

後述する信号情報（ＳＩＧＩＮＴ）や地理空間情報（ＧＥＯＩＮＴ）などのシングルソース情報収集機関（部署）は、予め定められた情報関心事項に基づき日夜データ収集を行い、それらを「処理・解析」して有用なシングルソース・インフォメーションを作成・配布及びデータベース化し、オール・ソース・プロダクト作成担当の分析官は、収集されたシングルソースのインフォメーションやデータベースに蓄積されている情報（インフォメーション及びインテリジェンス）にアクセスしてプロダクトを作成する。もし、プロダクト作成のために必要とするインフォメーションがない又は不足する場合には、適切なシングルソースの情報収集機関（部署）へ内部手続きを経て要求し、当該収集機関は、既存の収集データの中から、又は、新規に収集するデータの中から、上記分析官が必要とするインフォメーションを生成するよう努めることとなる。

### （３）　収集 (Collection)及び処理 ・解析(Processing and Exploitation)

「収集」とは、データを取得し処理担当へ提供することである[26]。情報源毎のシングルソース・インフォメーションについては、後述する。

「処理・解析」とは、収集される生データを十分活用し有用なインフォメーションに変換することを言い、このことについては、本章第１節で、信号情報の例を使って「処理・解析」の内容を説明した。しかしながら、情報源毎に「処理・解析」する要領は異なっており、それぞれの作業には、それぞれの専門性や技術・ノウハウが求められる。

### （４）　配布 (Dissemination)

配布とは、カスタマーへの情報提供、又は、分析官等による情報（インテリジェンス）プロダクトに係るカスタマーへのブリーフィングをいう。配布の要領としては、紙による配布・供覧もあれば、カスタマーの執務室に情報プロダクトを共有するための専用イントラネットシステム[27]の端末がある場合には、当該端末を使用して情報プロダクトへアクセスして受領することもあろう。また、定期・不定期を問わず、ブリーフィングルームに複数のカスタマーに集まってもらい、担当分析官等が自らブリーフィングすることにより、情報プロダクトを提供し、かつ、カスタマーからの「評価・フィードバック」を情報部門が貰う場合もある。

なお、各情報機関で作成される情報は、もちろん、情報コミュニティ内でも内部ルールに従い共有される必要がある。特に、オールソースのインテリジェンス・プロダクトを作成する各機関の分析官にとっては、自分が作成するプロダクトのために有用なシングルソース・インフォメーションやインテリジェンスに情報機関の垣根を超えてアクセスすることが必要である。また、そのためには、情報コミュニティ内で情報を共有するための保全強度の高い

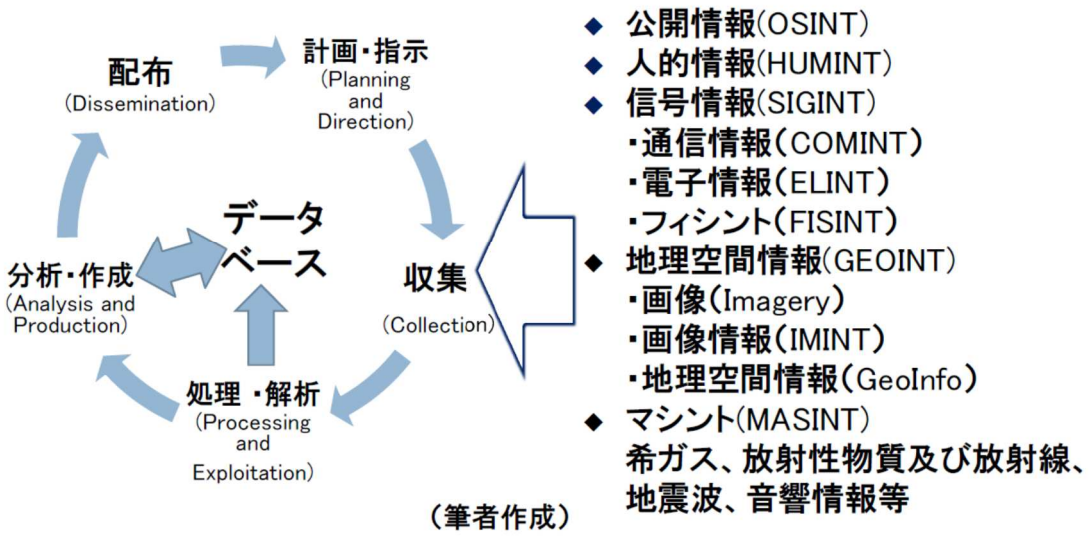
閉じたシングルソース情報毎のイントラネットシステムが構築されている必要があろう。

## 第４節　主要情報源（Basic Intelligence Sources）

主要な情報源について説明する。第２節で情報機関の任務は、「正確で、総合的で、適時な外国等に関する情報をカスタマーに提供すること」である旨述べたが、正確で総合的な分析・評価を行い情報（インテリジェンス）を作成するためには、複数の情報源から入手したデータを活用しそれらをチェックの上、より信ぴょう性の高い事実（インフォメーション）に基づき、分析・評価を行うことが必要である。

ここで、情報源を切り口に整理したインフォメーション（及びそのインフォメーションを分析・評価して作成されるインテリジェンス）の区分を示すこととする。本論考では、５つに分類して説明する。すなわち、公開情報 Open-Source Intelligence (OSINT)、人的情報 Human-Source Intelligence (HUMINT)、信号情報 Signals Intelligence (SIGINT)、地理空間情報 Geospatial Intelligence (GEOINT)（画像情報 Imagery Intelligence (IMINT)は GEOINT に含めて取り扱う。）及びマシント Measurement and Signature Intelligence (MASINT)である。

<図2>主要情報源（Basic Intelligence Sources）




（筆者作成）

### （１）　公開情報 Open-Source Intelligence (OSINT)[28]

公開情報（ＯＳＩＮＴ）は、文字通り、公に活用可能なインフォメーションであり、新聞・雑誌等の記事に限らず、テレビ、ラジオ、インターネットで開示されている情報も含まれる。膨大なデータやインフォメーションから、有用なインフォメーションを引き出すには、類別され時間軸で整理されたデータベースの構築が必要である。公開されているインフォメーションが事実である保証はなく誤りである場合が多々あり、また、当局が意図した偽情報（disinformation）を流すこともあり得るし、記者のバイアスが掛かる場合もあり得る。外国語の情報については、必要に応じ、邦訳と解説を付すとともに、分析・評価を加えて、公開情報を作成することとなる。

（２）　人的情報 Human-Source Intelligence (HUMINT)[29]

人的情報（ＨＵＭＩＮＴ）は、人を介して入手する情報である。論者によっては、人的情報の収集活動をスパイ活動（espionage）や秘密活動（clandestine activities）と同義だとして又は関連付けて扱う者もいるかもしれないが、人的情報の収集活動の大部分は、一般の外交官や駐在武官等の公の大使館員により行われる。更に言えば、研究機関や大学の研究者同士の意見交換や、通常の外交交渉における政府首脳同士又は事務方同士の意見交換等により得られるインフォメーションも人的情報に分類される。情報機関に属する者以外の例えば政策部門の者が聞いた相手国カウンターパートからのインフォメーションも人的情報として、自らの情報機関へ提供・共有されることが必要である。また、同盟国や友好国の情報機関との意見交換から得られる情報も受け手側（我が方の情報機関）から見ると人的情報として整理すべきものもあろう。

人的情報には、後述する信号情報（ＳＩＧＩＮＴ）や地理空間情報（ＧＥＯＩＮＴ）などでは代替できない有用なインフォメーションが含まれている場合がある。例えば、国際テロリズムに関する情報や、外国等の政策判断・意思決定に関わる者又はそのスタッフの意向などについては、人的情報が決め手になる場合があろう。その一方で、人的情報は、人を介するが故の誤認・誤解やバイアス又は偽情報の恐れがあり、他のインフォメーションによる検証が必要不可欠であることは言うまでもない。

（３）　信号情報 Signals Intelligence (SIGINT)

電波情報と呼ぶ場合もあるが、収集対象は電波（３００万メガヘルツ以下の周波数の電磁波[30]）に限らないので、本論考では、信号情報（ＳＩＧＩＮＴ）と呼ぶこととする。信号情報は、通信情報（COMINT: Communications Intelligence[31]）、電子情報（ELINT: Electronic Intelligence[32]）及びフィシント（FISINT: Foreign Instrumentation Signals Intelligence[33]）から成る。通信情報は対象国等の通信傍受により収集するデータ（インフォメーション）から作成されるインテリジェンスをいう。サイバースペース（Cyberspace）における対象国等の情報通信システムから得られるデータ（インフォメーション）もこの概念に含まれる。電子情報は対象国等の武器やレーダ等（核爆発や放射線源を除く）から発信される非通信の放射線（電磁波や粒子線）が収集対象で、それらから生成される技術的情報及び位置を割り出す情報である。また、フィシントは、対象国等の航空宇宙機材や地上（水上）又は地中（水中）機材が試験又は実運用に伴い放出する電磁波等を捕捉することにより得られるインフォメーション及びインテリジェンスをいう。例えば、試験中のミサイルから送信されるテレメトリー信号とか、軍用機の敵味方識別信号などが収集対象となる。

（４）　地理空間情報 Geospatial Intelligence (GEOINT)[34]

地理空間情報（ＧＥＯＩＮＴ）は、画像（Imagery[35]）や地理空間情報（Geospatial Information[36]）を解析・分析して、地形（海底地形を含む）の特色や地球上における諸活動を記述し評価しそして視覚的に描いたもので作成されるインテリジェンス・プロダクトを言い、画像

（Imagery）、画像情報（IMINT: Imagery Intelligence[37]）及び地理空間情報（Geo Info）から構成される。

画像とは、対象を視覚化したものに撮像の時刻と位置データなど（メタデータ）を付記したものである。撮像の手段は、軍事衛星や汎用（商用）衛星に限らない。有人や無人の偵察航空機も撮像手段である。また、撮像手段に搭載されるセンサーは可視光領域や赤外線領域のものだけでなく、曇天や雨天でも撮像可能な合成開口レーダ（ＳＡＲ[38]）もある。これら各種手段により得られる対象（目標）を捉えた３次元画像データ（時系列で整理されたデータを含む）と地理空間に関するインフォメーション（山や川などの自然の地形や標高など、鉄道、道路、発電所などのインフラ施設、工場、研究所、軍事施設などの各種主要施設等）を材料に、情報要求を満たすよう作成されるプロダクトが、地理空間情報（ＧＥＯＩＮＴ）である。通常、プロダクトは３次元（時間軸も入れると４次元）で表示可能なものである。

地理空間情報（ＧＥＯＩＮＴ）は、１９９０年代半ば以降、急速に進化してきた情報分野である。特に、米ソ冷戦が終わり、米国の軍事衛星技術の一部が民需に解放され[39]、例えば、可視光領域で分解能１ｍ[40]の撮像が可能な汎用（商業）衛星が利用可能となったこと、デジタル技術と解析のためのソフトウエアの発達により、画像データから位置データを含む地理空間情報（Geo Info）を生成することが比較的に容易になったこと等により、画像情報を主体とした総合分析（オールソース・アナリシス）情報（インテリジェンス）が作成されるようになったと言われている。しかしながら、画像データ（時系列の画像データを含む）から有用なインフォメーションを引き出す解析及び分析に関する作業は、画像情報に関与する分析官らの技量・能力に頼るところが大である。例えば、未経験者にとっては、画像から有用なインフォメーションを引き出すということそれ自体、簡単なことではない。対象（目標物）に関する広範囲な知識と洞察力、関連するインフォメーションとの比較・照合などがあって初めて画像から有用なインフォメーションを引き出すことができる。

### （５）　マシント　Measurement and Signature Intelligence (MASINT)[41]

最後に、マシント（ＭＡＳＩＮＴ）について説明する。これは、技術的手段で収集して得られるインフォメーション及びインテリジェンスで画像や信号情報以外のものをいい、固定又は移動目標の位置、航跡、識別や特徴を記したものである。希ガス、放射性物質及び放射線、地震波、音響情報等がマシントに含まれる。

例えば、対象国が地下核実験をした場合、地震観測所で地震波を観測する、航空機を飛行させ放射性物質の収集や核爆発に伴い発生する（キセノン、クリプトン等の）希ガス元素の検知が出来ないか観測することがあるが、そのような活動で収集するデータ、インフォメーションに基づき作成されるインテリジェンスがマシントに相当する。また、水上艦艇や潜水艦等の水上・水中システムから発せられる音響情報（位置データや個艦を特定し得る音紋等のインフォメーション）や海洋に関する潮流、海水温分布、塩分濃度分布等の各種ビックデータもマシントに分類される。

次回（第３回）に続く

[1] Intelligence: The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. JCS/DOD,“DOD Dictionary of Military and Associated Terms (As of September 2018)," (以下「DOD Dictionary」という。) (http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-09-28-100314-687)（２０１８年 10 月 10 日）

[2] The activities that result in the product. (DOD Dictionary)

[3] The organizations engaged in such activities. (DOD Dictionary)

[4] Raw data/ Data element: A basic unit of information built on standard structures having a unique meaning and distinct units or values. (DOD Dictionary)

[5] Processing: A system of operations designed to convert raw data into useful information. (DOD Dictionary)

[6] Exploitation: Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. (DOD Dictionary)

[7] SIGINT (Signals Intelligence): Intelligence derived from communications, electronic, and foreign instrumentation signals. (DOD Dictionary)

[8] 解読できない収集データは、そこからインフォメーションを引き出すことは出来ないので、暗号解読作業を試みることとなる。

[9] 本論考では、爾後単に「情報」という場合には、インテリジェンスとインフォメーションの両方の意味とし、個別の意味に特定する場合には、情報（インテリジェンス）若しくはインテリジェンス又は情報（インフォメーション）若しくはインフォメーションと明記する。

[10] インテリジェンスを作成するに当たって、各情報機関に属する分析官等は、インフォメーションや関連するインテリジェンスにアクセスする必要があるが、当該分析官等は、カスタマーとして情報の提供を受けるのではなく、正確で総合的なプロダクトを作成するために必要な情報にアクセスする立場である。

[11] 国家安全保障会議設置法（昭和 61 年法律第 71 号）第３条から第５条まで及び内閣法（昭和 22 年法律第５号）第 17 条。

[12] 特定秘密保護法ではテロリズムを「政治上その他の主義主張に基づき、国家若しくは他人にこれを強要し、又は社会に不安若しくは恐怖を与える目的で人を殺傷し、又は重要な施設その他の物を破壊するための活動をいう」と定義している。（同法第１２条第２項第１号）

[13] 都道府県警察の特殊部隊（SAT：Special Assault Team）、海上保安庁の特殊警備隊（SST: Special Security Team）、陸上自衛隊の特殊作戦群（SFG: Special Forces Group）及び海上自衛隊の特別警備隊（SBU: Special Boarding Unit）がテロ対処部隊として知られている。

[14] 外務省本省の場合、政策局・地域局も情報機能を有しており、そのことが同省がインテリジェンス面で抱える最大の問題であるとの指摘がある。（ＰＨＰ「日本のインテリジェンス体制の変革」研究会『日本のインテリジェンス体制 変革へのロードマップ』株式会社ＰＨＰ総合研究所、平成 18 年６月（以下「２００６年ＰＨＰ報告書」という。）33 ページ等）

[15] 日本政府は、平成 27 年（２０１５年）12 月８日、邦人関連事案に関する国際テロ情報の収集等を抜本的に強化するため，①国際組織犯罪等・国際テロ対策推進本部（本部長 内閣官房長官、副本部長 国家公安委員会委員長）に「国際テロ情報収集・集約幹事会」、②内閣官房に「国際テロ情報集約室」、③外務省（総合外交政策局）に「国際テロ情報収集ユニット」を置くこととした。（第 23 回 犯罪対策閣僚会議（平成 27 年 12 月８日）資料２）

[16] ２０１４年１月、国家安全保障会議の事務局である国家安全保障局が約 70 人体制で発足して以降、同局からの情報要求が随時行われるようになった、とされている。（ＰＨＰ「国家安全保障会議検証」プロジェクト『国家安全保障会議―評価と提言―』株式会社 ＰＨＰ研究所、２０１５年（以下「２０１５年ＰＨＰ報告書」という。）、40～42 ページ等）

[17] 米国大統領令（行政命令） Executive Order 12333 - United States Intelligence Activities（以下「大統領令 EO12333」という。）(Part1, 1.1(e))によれば、comprehensive の代わりに insightful（洞察力ある）という形容詞が使用されている。なお、米国ＣＩＡの任務には、例えば、２０１１年５月に実施されたウサマ・ビン・ラーディン殺害作戦のように、大統領の承認を得て行う秘密工作活動（covert action activities）があるが、日本の情報機関にはそのような任務

はない。
[18] Indication: information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. Warning intelligence: (Those intelligence activities intended to detect and report) time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests.（DOD Dictionary）
[19] 情報機関の外にいるカスタマーも、自分たちが受領したインテリジェンスを、保全手続きによらずにカスタマー以外の者へ提供してはいけないことは言うまでもない。
[20] Planning and Direction: the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (DOD Dictionary)
[21] Evaluation and Feedback: Continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (DOD Dictionary)
[22] 情報組織に対する監察部門があれば、評価・フィードバックについて、監察部門が業務監察する場合もあろう。
[23] 内閣情報調査室の場合は、総務部門が担当部署になると考えられる。
[24] 外務省国際情報統括官組織においては、外務省組織規則（平成 13 年外務省令第 1 号）には記載されていないが、筆頭室である「第一国際情報官室」ではないかと推察する。防衛省情報本部については、情報本部組織規則（平成 9 年総理府令第 1 号）によれば、担当情報官又は情報の収集整理に関する総合調整・計画を所掌する計画部であると推察できる。
[25] Analysis and Production: the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (DOD Dictionary)
[26] Collection: the acquisition of information and the provision of this information to processing elements. (DOD Dictionary)　なお、本文では、この information をデータと意訳した。
[27] カスタマーや情報職員は在外公館にも所在することから、情報部門で管理するイントラネットシステムは在外公館にも配置されていることを想定する必要がある。
[28] OSINT: Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. (DOD Dictionary)
[29] HUMINT: A category of intelligence derived from information collected and provided by human sources. (DOD Dictionary)
[30] 電波法（昭和 25 年法律第１３１号）第２条第１号。
[31] COMINT: Technical information and intelligence derived from foreign communications by other than the intended recipients. (DOD Dictionary)
[32] ELINT: Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources (DOD Dictionary)
[33] FISINT: A subcategory of signals intelligence, consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. (DOD Dictionary)
[34] GEOINT: The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (DOD Dictionary)
[35] Imagery: A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (DOD Dictionary)
[36] Geospatial Information: Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (DOD Dictionary)

[37] IMINT: The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (DOD Dictionary)
[38] SAR（synthetic aperture radar）とは、レーダの一種で、航空機や人工衛星に搭載し、移動させることによって仮想的に大きな開口面（レーダの直径）として働くレーダをいう。
[39] １９９４年３月、米国ホワイトハウスは、「リモートセンシング宇宙能力への外国のアクセスに係る米国政策(US Policy on Foreign Access to Remote Sensing Space Capabilities) 」という主題の大統領令（Presidential Decision Directive/NSC-23 (March 9, 1994) ）を決定した。この政策の基本的な目標は、上記分野における米国産業競争力の維持・強化にあった。
[40] 分解能が１ｍであるという意味は、１ｍ離れていれば二つの画素（ピクセル）として撮影されるということである。したがって、例えば、分解能が１ｍだと、５ｍ位の乗用車なのか10ｍ位のバス・トラックなのか識別可能となり、有用なインフォメーションとなり得る。
[41] MASINT: Measurement and Signature Intelligence is technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. (https://www.dni.gov/index.php/what-we-do/what-is-intelligence)（２０１８年 10 月 10 日）