

[論文]

金融インテリジェンスの誕生と発展： 9-11テロとグローバルな金融危機を触媒に

Birth and Development of Financial Intelligence: Catalyzed by the 9-11 Terror and Global Financial Crisis

保井 俊之

Abstract

Financial Intelligence is defined as the intelligence for national security required, collected and analyzed by financial-oriented institutions using financial methods to provide in financial format to policy-makers. It started in 1990's mainly from law enforcement activities to combat with anti-money laundering. 9-11 terror in 2001 made it prepared to outreach toward new battle-field in financially fighting asymmetrical warfare with unconventional threat. With emerging perception of North Korea and Iran as vital national security threats against her, the United States started to vigorously apply financial intelligence to those countries from 2005. The US intelligence community currently puts primary priority to financial markets and services as its activities domains for intelligence since outbreak of global financial crisis in fall 2007.

要 旨

金融インテリジェンスは国家安全保障のために、金融に特化した組織により、金融の手法により要求・収集・分析され、金融のフォーマットで政策決定者に提供されるインテリジェンスと定義される。金融インテリジェンスは主として1990年代、マネーロンダリング対策のための法執行活動として出現した。そして2001年9月11日の米国における同時多発テロは金融インテリジェンスの活動分野を、非伝統的な脅威と戦う非対称な戦争の分野へと拡大した。さらに2005年から米国は北朝鮮及びイランを重大な安全保障上の脅威とみなすようになり、これらの国に金融インテリジェンスを活発に適用するようになった。2007年秋に発生したグローバルな金融危機により、米国のインテリジェンスコミュニティは金融サービス及び金融市場をインテリジェンス活動の主要な領域とみなすようになっている。



Toshiyuki YASUI

- 慶應義塾大学院システムデザイン・マネジメント研究科教授
- 東京大学教養学部教養学科国際関係論分科卒業
- 教養学士
- 〒223-8526 横浜市港北区日吉4-1-1 慶應義塾日吉キャンパス 協生館
- 045-564-2461
- t.yasui@z2.keio.jp
- Professor, Graduate School of System Design and Management, Keio University
- Graduated from Faculty of International Relations, the School of Arts and Sciences, the University of Tokyo
- Bachelor of Liberal Arts
- Collaboration Complex, Keio Hiyoshi Campus, 4-1-1 Hiyoshi, Kohoku-ku, Yokohama

1 問題の所在と分析の視角

1.1 問題の所在と論述の方向

金融インテリジェンスについて、これまで通説となる定義は存在してこなかった。金融インテリジェンスの題を持つ近年出版された代表的書籍には、Berman et al. [1] 及びHansen [2] があるが、いずれも消費者や企業経営者に財務諸表の読み方や投資の尺度となる経営指標を教えることを目的としており、国家安全保障に不可欠な情報活動としての金融インテリジェンスに関する定義及び説明は行っていない。

そこで本稿では、まず国家活動としての金融インテリジェンスについて定義し、その特徴を明らかにする。さらに金融インテリジェンスがどのような経緯から生まれ、どのような事件を契機に重層的に発展してきたかについて俯瞰する。その上で、金融インテリジェンスの発達がもっとも著しい米国インテリジェンスコミュニティを主要な分析対象としつつ、日本の状況との対比も意識した上で、2001年の米国同時多発テロの発生と2007年秋のグローバルな金融危機の発生が金融インテリジェンスの発展に決定的な触媒となったことを述べる。

1.2 先行論文と金融インテリジェンスの定義

インテリジェンスに関する総括的かつ代表的な文献のひとつであるLowenthal [3] (8頁) は、インテリジェンスの作業概念を「国家安全保障に重要な特定のパターンの情報が要求され、分析され、政策決定者に供給されるプロセス」としている。その上で同書はインテリジェンスの成立要件として、①組織としてのインテリジェンス、②過程としてのインテリジェンス、③製品のインテリジェンスの3つが具備されることを求めている。

このようなインテリジェンスの定義と要件は金融分野におけるインテリジェンス活動とまったく無縁ではない。むしろインテリジェンスの制度的な認知の場となった冷戦初期の米国インテリジェンスコミュニティにおいて、金融は経済に包含される形で、インテリジェンス活動の主要な領域と認識されていた。例えば、CIAの誕生及び初期の発展に学術的かつ実践的な寄与をした学識者の代表的存在であるシャーマン・ケントはインテリジェンスの主要カテゴリーとして経済インテリジェンスを挙げている。ケントは代表的著作であるKent [4] の第1部「インテリジェンスは知識である」の中で、第二次世界大戦は国家がその軍事、経済、政治、文化及び経済活動のすべてを動員した総力戦であったこと、さらに冷戦は米ソの経済力の持久戦であるとの認識を背景に、経済戦(economic warfare)こそ非伝統的な戦争の主要部分であるとした上で、「(インテリジェンス)の報告要素とし

て、(インテリジェンスを行う者は) 現下の経済情勢を追い続ける責務がある」(同書34頁)と指摘している。

以上のインテリジェンスの定義を踏まえれば、金融インテリジェンスは、①組織：金融に特化した組織により、②過程：金融の手法により要求、収集及び分析され、③製品：金融のフォーマットで政策決定者に提供されるインテリジェンスと定義されることになる。例えば、米国財務省の反マネー・ローンダリング及びテロ資金対抗部局がテロ資金の送金手口に関する情報を収集及び分析し、国家安全保障会議(NSC)に提供することは、典型的な金融インテリジェンス活動である。

1.3 金融インテリジェンスの特徴

金融インテリジェンスの特徴としては、次の3つが挙げられる。

1つ目の特徴としては、前述のKent [4] も指摘しているように、非伝統戦である経済戦の一つである金融戦(financial war)を戦う際に金融インテリジェンスが多く用いられることである。例えば、2001年以降のグローバルなテロとの戦いにおいて、イスラム過激派グループなど非国家主体との戦い及びインテリジェンスの領域はテロ資金の調達及び送金の摘発等を巡るものであった。

2つ目の特徴としては、金融インテリジェンスが、麻薬取締り、脱税の摘発及び反マネー・ローンダリング措置など国境を越える犯罪捜査に代表される国際的な法執行(international law enforcement)活動として用いられることが多いことにある。その理由について、これもインテリジェンス活動の代表的文献のひとつであるShulsky and Schmitt [5] は、金融インテリジェンスと国際法執行の活動の性質が類似していることから、インテリジェンスのアプローチが国際組織犯罪捜査の手法として活用されるのだとしている(同書4-5頁)。

さらに3つ目の特徴として、むしろ現代のインテリジェンス活動の主要な対象領域が金融サービス及び金融市場に向けられることになったことが近年とみに認識されるようになったことが挙げられる。地政学的リスクとインテリジェンス活動の関係を国家が行うインテリジェンスに限定することなく説明したBremmer and Kent [6] は、通常の発生確率である正規分布では稀にしか起こらないような確率帯での事件事故の発生が頻発する傾向をファット・テイルと呼んだ上で、ファット・テイルのリスクが現れる現代の国際政治においては、いかなる政治的リスクにも増して地政学的リスクが国家や市場、そして個人々の安全保障にとって実存的な脅威となり得ること、そして地政学的イベント、特に国際的戦争が金融市場を創出したり破壊したりする可能性を指摘している

(同書38-40頁)。このようにインテリジェンスの伝統的かつ主要な対象のひとつである地政学的リスクと金融サービス及び金融市場が不可分かつ深く結びついていることが、2007年秋からのグローバルな金融危機の中で深く認識されるに至っている。

2 4つの発展段階

金融インテリジェンスは以下の4つの段階を経て生成及び発展してきたと考えられる。

第1期は1988年から2001年の9-11テロまでの時期であり、いわゆる国際マフィア等による国境を越えた麻薬取引やマネー・ロンダリングの摘発のため、金融情報を使った法執行活動の国際的協調として金融インテリジェンスが活用された時期である。この時期は「国際的法執行活動との未分化期」と名づけられよう。

第2期は9-11テロから2005年頃までの時期で、9-11テロにより始まった米国を中心とするテロとの戦いのための戦線を、金融サービスにも拡張といった時期である。この時期の特徴としては、対テロ戦線に金融領域の作戦が組み込まれていったために、インテリジェンスの活動としても金融面での手法がクローズ・アップされた時期である。この時期は「対テロ戦期」と名づけられよう。

第3期は北朝鮮及びイランが米国の主要な脅威として認識され始めた2005年頃から2007年秋までである。米国のブッシュ政権は9-11テロ後、北朝鮮やイラン等をテロ国家として制裁対象にするとともに、非伝統的戦争及び圧迫の手段として金融制裁など金融インテリジェンスを駆使した制裁手段を活用した。この時期は「金融インテリジェンスと金融制裁の活用期」と名づけられよう。

第4期は2007年秋のグローバルな金融危機発生以降の時期である。この時期はグローバルな地政学的リスクとして金融危機そのものが意識された時期であり、インテリジェンスの主要な対象領域が金融情勢になった。この時期は「金融インテリジェンスのコア対象期」と名づけられよう。

これら4つの発展段階における金融インテリジェンスの特徴とその含意を以下、実例をもとに分析する。

2.1 国際的法執行活動との未分化期(1988-2001)

国連麻薬新条約が1988年に採択され翌89年のアルシユ・サミットでマネー・ロンダリングの犯罪化義務付けと金融活動作業部会(FATF)が設置されると、

FATFが国際的な反マネー・ロンダリング 協調とそれに随伴する金融インテリジェンスの結節点となった。FATFは反マネー・ロンダリング 措置に関する国際取極めである「FATF・40の勧告」(FATF The Forty Recommendation)を90年に採択した。そして主要先進8か国を中心に、金融インテリジェンス・ユニット(FIU)が設置¹⁾され、95年には各国FIUの国際的なネットワークであるエグモント・グループが発足している。この時期FATFは、各国FIUの協調と情報交換の促進を第一義にしつつ、加盟国・地域同士の相互審査を使い、いわゆるピア・プレッシャーのアプローチにより国際的な反マネー・ロンダリング態勢の構築を目指した。また、より強力な措置として、2000年にはFATFが反マネー・ロンダリングに関する非協力国・地域の公表を始めている。しかし、この時期には金融インテリジェンスとFTAFを中心とする国際的法執行活動は分化していない状態にあったと言えよう。

2.2 対テロ戦期(2001-2005)

2001年9月11日の米国同時多発テロはFATFの活動の内容をも大きく変えることとなった。テロとの戦いを重視する米国はFATF加盟国・地域に働きかけ、FATFは「テロ資金対策に関する特別勧告」(FATF Special Recommendations on Terrorist Financing)を採択した。

この特別勧告では、テロ資金供与行為を犯罪とすること、テロに関する「疑わしい取引」の届出の義務化、電信送金に関する正確かつ有用な送金人情報の付記を、1,000米ドル相当価額を閾値として実施すること等が規定されている。

また2003年にFATFは「40の勧告」を改訂し、マネー・ロンダリングを犯罪として処罰する範囲の拡大・明確化、金融機関の預送金受入時の顧客の本人確認徹底、法人形態を悪用したマネー・ロンダリングへの対応、及びこれまでは金融機関だけであった「疑わしい取引」の届出義務適用先をいわゆるゲート・キーパーと呼ばれる非金融業者及び職業専門家にも拡大すること、等が勧告に新たに盛り込まれた。

なお、FATFが加盟国・地域を対象に実施する加盟国・地域同士のピア・プレッシャーによる相互審査では、銀行監督に関する国際的枠組みであるバーゼル銀行監督委員会が2006年10月に「実効的な銀行監督のための中核となる諸原則」(いわゆるバーゼル・コア・プリン

1) 金融インテリジェンスユニットの設置が先進主要国首脳会議で正式に合意されるには、1998年のバーミンガム・サミットまで待たねばならなかった。

シブル)及び同方法書(いわゆるコア・プリンシプル・メソドロジー)²⁾を改訂し、マネー・ローンダリング防止や反テロ資金対策にかかる金融機関の本人確認義務を強化したことを受け、加盟国・地域で対策強化が図られているものの、審査の結果が近年とみに厳しいものとなる傾向がある³⁾。

さらに、9-11テロの発生を受け、直後の2001年10月に制定された米愛国者法(US Patriot Act)は米国のインテリジェンス関係者にとって、金融インテリジェンスを対テロ戦争の重要な手段として用いる大きな枠組みを提供することになった。

すなわち米愛国者法第311条は、国務長官及び司法長官等との協議の上、米国の金融機関と取引のある外国金融機関がマネー・ローンダリングの主要懸念先(primary money laundering concern)に特定された場合、5つの特別措置⁴⁾を発動する権能を財務長官に与えている。

この5つの特別措置のうち、金融インテリジェンス及びエンフォースメント活動に大きな意義を付与したのが、米国の金融機関に対して主要懸念先に特定された外国金融機関の決済・コルレス口座の開設・維持を制限・禁止できるとした条項である。基軸通貨ドルの決済の場合、世界各国の金融機関がいわゆるカバー・ペイメントという手法を用い、大量かつ短時間に金融機関相互の決済を、ニューヨークに所在するマネーセンターバンクを結節点にして決済を行っている。米愛国者法はあくまで米国の国内法であり、外国政府が監督権限を有する外国金融機関を拘束するものではないが、主要懸念先に指定されればニューヨークのマネーセンターバンクをはじめとする米国の金融機関はコンプライアンスリスクから当該懸念先との決済・コルレス取引を拒絶するようになる。した

がって、主要懸念先への指定は、その金融機関が米国の金融ネットワーク、ひいてはグローバルなドル決済のネットワークから締め出されることを意味するのである。

このことは、後述する2005年のバンコ・デルタ・アジア事件をきっかけに米インテリジェンスコミュニティに強く意識されるようになる。

さらに、事件発覚の時期はやや後ろにずれるものの、米インテリジェンス関係者が金融インテリジェンスを積極的に対テロ戦に活用していることを米国の一般国民にも強く印象付けたのは、2006年6月に発覚したブッシュ政権によるSWIFTデータの秘密閲覧事件である。

この事件は、ベルギーに本部があり、送金・決済メッセージに関する共通プラットフォームをグローバルに提供しているSWIFT⁵⁾の取引データベースを米財務省、CIA及びFBIが9-11テロ後、アルカイダのテロ活動監視等のために、組織的かつ密やかにアクセスし続けたことが2006年6月23日付のニューヨーク・タイムズ紙他の報道⁶⁾で暴露されたものである。そしてこの記事が掲載されることを察知した米財務省は同日、テロリストファイナンス追跡プログラム(Terrorist Finance Tracking Program: TFTP)の存在を自ら公表し、①TFTPが1977年国際緊急事態経済権限法(IEEPA)や大統領行政命令第13224号に法的根拠を持つ合法的な活動であること、②アクセス対象もSWIFTに召喚状を出した上でアルカイダ、ハマス、ヒズボラ等の国際テロリストの捜査目的に極めて限定したものであること、③SWIFTの監督に当たっている主要先進国の中央銀行はTFTPの活動について告知されていたこと、等を併せて説明している。

TFTPの最も強力な推進者の一人と目されているスチュワート・リービー財務次官(テロ及び金融インテリジェンス担当)は、同年7月11日に米下院金融サービス委

2) バーゼル・コア・プリンシプル及び同メソドロジーは、1990年代後半に発生したアジア通貨危機の教訓として、G7財務相・中央銀行総裁会議が加盟各国の金融セクターの評価実施をIMFに要請。IMFが評価するためには統一的な基準及び方法の指定が必要であったことから、その作成をバーゼル銀行監督委員会へ要請し、前者は1997年、後者は1999年に完成したもの。IMFはこれらに基づき加盟国に対して「金融セクター評価プログラム」(FSAP)を130国超に実施してきた。

3) 例えば、2007年6月に公表された対中国の相互審査では、40の勧告のうち、遵守=8、ほぼ遵守=12、部分的遵守=13、非遵守=7、及び9のテロ特別勧告のうち、遵守=0、ほぼ遵守=4、部分的遵守=3、非遵守=2となった。また、2008年10月に公表された対日審査では、40の勧告のうち、遵守=4、ほぼ遵守=17、部分的遵守=9、非遵守=9、適用なし=1、及び9のテロ特別勧告のうち、遵守=0、ほぼ遵守=2、部分的遵守=6、非遵守=1となった。

4) 5つの特別措置とは、①特定の金融取引の記録保持・報告、②米国金融機関の特定の口座の外国人受益者の特定、③外国金融機関が米国金融機関に開設した決済口座を利用する外国金融機関顧客の特定、④外国金融機関が米国金融機関に開設したコルレス口座を利用する外国金融機関顧客の特定、⑤特定の銀行の決済・コルレス口座の開設・維持の制限・禁止、である。当該特別措置の発動に当たり、①から④については国務長官及び司法長官との協議、また⑤については国務長官、司法長官及び連邦準備制度(FRB)議長との協議、がそれぞれ財務長官に法律上求められている。

5) Society for Worldwide Interbank Financial Telecommunicationの略。本部はベルギーにあり、209か国の8,908金融機関等が加盟する協同組織。1973年に発足し、77年にメッセージの送付業務を開始した。現在、1日平均1,450万件のメッセージを送付している。

6) 例えば、Eric Lichtblau and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror", New York Times, June 23, 2006を見よ。

員会監視捜査小委員会で開催された公聴会において、「カネの行き先を追跡すること (following money) はテロリストとその支援者を特定し探知するために、最も有益な情報源のひとつ」(U.S. Department of Treasury [7] (1頁))とした上で、「TFTPはこれらすべての努力の鍵となる部分」(同2頁)と評価し、国民のプライバシーが国家によって侵される危険があるとの批判に対しても、むしろニューヨーク・タイムズ紙他の暴露記事の掲載のほうがテロに対する戦いにおけるTFTPの有効性を減じているとし、「新聞が本件の報道を決定したことを大変残念に思う」(同3頁)とまで証言している。

このように、米インテリジェンス関係者は、この時期に対テロ戦の一翼を担う重要な手段として、金融インテリジェンス及びそれに随伴するエンフォースメントに覚醒していったと見ることができよう。

2.3 金融インテリジェンスと金融制裁の活用期 (2005-2007)

この時期の金融インテリジェンスの特徴は、米愛国者法第311条に代表される金融取引に着目したインテリジェンス及びエンフォースメントの手法が、北朝鮮やイランなどによる核兵器及び弾道ミサイル開発の脅威が顕在化したことを受け、これらの国家への対応策として積極的に用いられるようになったことである。

代表的な活用事例としては、2005年9月のバンコ・デルタ・アジア事件が挙げられる。

これはマカオに所在する地場銀行バンコ・デルタ・アジアにある口座が同行の上級行員と共謀の上北朝鮮政府関係者により偽造ドル札のマネー・ローンダリングに使用されていたことが米財務省の金融インテリジェンス活

動により突き止められ、同行が米愛国者法第311条の適用を受け、マネー・ローンダリングの主要懸念先に指定された事件である⁷⁾。当該口座に預金されていた金額は2,500万ドルと近年のグローバルな金融取引の規模と比べてはさほど大きな額ではなかった。しかし前節で述べたように米国の金融ネットワークからこの銀行が締め出される結果となり、後に標的となった北朝鮮当局の預金は米愛国者法の適用外であるニューヨーク米連邦準備銀行からロシアの金融機関を経由して北朝鮮に送金が認められたものの、北朝鮮の核を巡る6者協議のプロセスに北朝鮮が一時一切応じなくなるなど、同制裁の威力を北朝鮮に見せつけたと米国の政府及び議会関係者に改めて認識させることとなった。

例えば、U.S. Congressional Research Service [8] は同事件で活用された金融インテリジェンス及びエンフォースメントの手法について、「バンコ・デルタ・アジア事件の金融的効果は期待されたよりも大きかった」と評価し、その理由として、「(米国がとった金融インテリジェンスの手法が、) 主要な北朝鮮法人の国際金融の活動拠点を奪い、平壤政権要人の秘密個人口座を閉鎖に追い込んだだけでなく、北朝鮮の正当な貿易にも支障を生じさせた模様であること」、さらに「米国以外の銀行も米国の法的制裁が課されるのではないかと懸念し、北朝鮮との取引を切断するに至ったこと」(同8頁)を挙げている⁸⁾。

2005年のバンコ・デルタ・アジア事件での金融インテリジェンスに関する米国の成功体験は、金融インテリジェンスの位置づけを安全保障上の重要戦略の一つとしてブッシュ政権に直ちに認識されることになった。特に北朝鮮関連では、リービー米財務次官が2008年4月1日に

7) 北朝鮮の通貨偽造、麻薬取引及び大量破壊兵器関連輸出等の活動について、米務省で本件の調査及び政策立案を担当したDavid A. Asherはthe Nautilus Institute発行の論文“*The North Korean Criminal State : its Ties to Organized Crimes, and the Possibility of WMD Proliferation*”, November 15 2005において、①通貨偽造などの活動は北朝鮮の年間輸出総額の35~40%に上っていること、②偽造米ドル「スーパー・ノート」100ドル札がアジア金融機関へ流入していること、③これらの事実は2005年夏までにFBI及びU.S.シークレット・サービスが実施した「王の魔力と煙を吐く龍捜査作戦」(the Royal Charm and Smoking Dragon Investigations)で判明したことを指摘している。同論文の出所は、<http://www.nautilus.org/fora/security/0592Asher.html>

8) 米財務省金融犯罪法執行ネットワーク (FinCEN) は、2009年6月18日に全ての米金融機関向けに“*North Korea Government Agencies' and Front Companies Involvement in Illicit Financial Activities*”と題する勧告 (advisory) を発出し、累次の国連安保理決議や北朝鮮の不正な金融活動を踏まえ、米金融機関は北朝鮮関連と目される金融取引について相応のリスク軽減措置をとるべきこと、北朝鮮のドル口座への監視を強めていること、国連決議上禁輸となっている北朝鮮の奢侈品調達のための金融サービスを提供すべきではないこと、北朝鮮の顧客による多額の現金預金及びそれに伴う偽造通貨受渡リスクに引き続き警戒すべきこと、を求め、併せて監視強化のために北朝鮮の17行の金融機関の個別名を明らかにしている。

米上院銀行委員会の公聴会で証言し、偽造通貨に捜査権能を持つ米シークレットサービス⁹⁾が北朝鮮のドル偽造活動を捜査し続けており、「スーパーノート」として知られる高品質の偽造ドル札¹⁰⁾が表に表れ続けている旨の証言をわざわざ行っている¹¹⁾ことが、米国の金融インテリジェンスの具体的成果を顕示することによる北朝鮮に対する牽制効果という点で注目される。

ブッシュ政権が2006年3月に改訂した「米国の国家安全保障戦略 (National Security Strategy of the United States)」は、「米国は公私のパートナーとともに、国際金融システムを犯罪者、テロリスト、マネー・ロンダリングの実行犯、腐敗した政治指導者の悪用から守ってきた。我々はFATF等の国際枠組を使い、このグローバルシステムを透明かつ汚れた資本による悪用から守っていく。我々はならず者の金融機関及び非金融業者 (rogue financial players and gatekeepers) を摘発、遮断、孤立させる新たなツールを開発しなければならない」¹²⁾と記述している。

2006年版米国国家安全保障戦略におけるこの記述は、ブッシュ政権が2006年の段階で金融インテリジェンスを安全保障戦略の主要な柱と認識していたことを示している。

このような流れを受け、ブッシュ政権は金融インテリジェンスの枠組を安全保障上の大きな脅威とみなしてい

たイランに対応する施策に余すところなく活用することとなった。

また、イランの核開発・核拡散関与を巡り2006年12月、2007年3月及び2008年3月の3次にわたり出された国連安保理決議を背景に、FATFは2007年10月及び2008年10月の2度にわたり、イランの反マネー・ロンダリング・反テロ資金対策の不備を厳しく非難し、各国の金融機関にイランとの金融取引を行うことへのコンプライアンス・リスクの高まりを指摘する勧告を出している。FATFの2度にわたる特定同一国を対象とする勧告は異例であり、上述の米国の安全保障戦略におけるFATFを政策的な梃子の役割として重視する見解と軌を一にするものと判断される。

米財務省は金融インテリジェンスの活用が定着したこと¹³⁾を背景に、米国独自の対イラン金融制裁にも踏み込んでいく。これまで1979年国際緊急事態経済権限法及び2000年イラン不拡散法並びに関連の大統領命令で禁止されてきた米国金融機関のイラン向け金融取引の例外として認められてきた、いわゆるUターン取引¹⁴⁾についても、2006年9月のサデラット銀行への禁止措置の適用から始め、2007年1月にはゼバ銀行、同10月にはメリ銀行及びメラット銀行、とイランの大手銀行の禁止対象指定を順次拡大してきた。そして2008年11月には対イランUターン取引を全面的に禁止するに至った。この米国のイラン

9) U.S. Secret Serviceは元来、南北戦争期に米国で出回った偽造通貨の取締りのために設立された機関であり、大統領など要人警護を米議会から正式に授けられたのは1913年になってからである。1984年には、米議会から新たにクレジットカード犯罪取締りの権能を授けられ、さらに1994年にはThe 1994 Crime Bill Public Law (103-322)の成立により、米国の国外で偽造米通貨を製造、売買、所持する者を米国国内の取扱いと同様に起訴できることになった。そして2001年の米愛国者法の成立により、コンピュータ犯罪や通貨偽造罪に関する取締り権能が強化された。U.S. Secret Serviceは2002年の本土安全保障省の設置により、これまで属していた財務省から同省へ移管された。以上の出所はU.S. Secret Serviceウェブサイト (<http://www.secretservice.gov>) による。同機関は本土安全保障省への移管後も、長年財務省の管轄下にあったことから、財務省との関係が深いと見られている。

10) 米国における北朝鮮経済の研究者として定評のあるピーターソン国際経済研究所の主任研究員であるMarcus Nolandは、2006年4月25日、米上院本土防衛政府問題委員会の連邦金融運営・政府情報・国際安全保障小委員会の公聴会で“*How North Korea Funds its Regime*”と題する証言を行ない、北朝鮮の作成する米ドル偽札「スーパーノート」は控えめに見積もっても1989年までには出現していたと述べている。同証言の出所は、<http://www.iie.com/publications/paper>。

また米議会調査局の報告書のひとつ (Raphael F. Pearl and Dick Nanto, “North Korean Counterfeiting of U.S. Currency”, March 22, 2006) は、他の民間推計を引用しつつ、北朝鮮の通貨偽造額は1989年以来総額4,500万ドルに達し、その収益は年間1,500~2,500万ドルに上ると見積もっている。

11) U.S. Department of Treasury, Under Secretary of Terrorism and Financial Intelligence Stuart Levey Testimony Before the Senate Committee on Finance, April 1 2008, HP-898のうち、3. Combating the Illicit Financial Conduct of Rogue Regimesの章のNorth Koreaの項を参照。出所は<http://www.treas.gov/press/releases/hp898.htm>

12) National Security Council of the United States, National Security Strategy of the United States, June 2006 revised, のうち、IV. Ignite a new era of global economic growth through free markets and free tradeの最終段落による。出所は<http://georgebush-whitehouse.archives.gov/nsc/nss/2006>

13) Robert Wright, “Stuart Levey’s War” November 2, 2008, New York Timesは、リービー財務次官が2006年1月にバーレーンを訪問した際、金融セクターという政府が直接関与する以外の経済活動を通じて安全保障上の目的を達する施策が中国から中東まで昔のシルクロードのようにつながる現代の金融とエネルギーの流れの中で、有効な政策手段になることに覚醒したと記している。

14) 非米国金融機関同士が米国以外のある国への送金または決済を行う過程で米国内の金融機関のコルレス口座を資金が通過する金融取引。米国金融機関をU字の底に見立て、上方の非米国金融機関から送金が入り、U字の底の米国金融機関の口座に資金が滞留せず、そのまま別の非米国金融機関の口座へ資金が抜けることから、Uターン取引の通称がある。

向け独自金融制裁の影響から、2007年夏以降主要国の金融機関は対イラン金融機関向け金融取引を順次縮小または廃止する動きを見せている。

イランへの圧力として金融インテリジェンス及びエンフォースメントを活用する動きはオバマ新政権になっても継続している。例えば、オバマ大統領は大統領選挙中の2008年6月4日に、米国の有力なロビー団体であるアメリカ・イスラエル公共問題委員会（AIPAC）の政策会議で演説し、イランへの対応について、「（イランがこのままの姿勢でいれば、）我々はロシア・中国とともに国連安保理でより強い制裁を主張するのを強化することになり、イランの現体制を孤立させるすべての手段、すなわち融資保証の停止及び金融制裁の拡大から、イランへの石油精製製品の禁輸、傘下にあるコブズ・フォースがまさにテロ組織と認定されているイラン革命防衛隊と連携する（イラン）企業のボイコットまでの手段、を見つけ出すために、欧州、日本、湾岸諸国とともに作業していくだろう」¹⁵⁾と演説している。オバマ政権はイランへのエンゲージメントを優先課題に挙げ、軍事手段の性急な行使を適用可能な政策オプションから退けているが、それだけに北朝鮮への対応で効果を挙げたと自認する金融インテリジェンス及びエンフォースメント、そしてこの国際連携に重点を一層置く可能性がある。

さらに直近では、米財務省の金融インテリジェンスの活動の成果として、イランと北朝鮮の大量破壊兵器開発技術関連の資金決済の関係を明るみに出す事例も公表されている。

米財務省は2009年6月30日、U.S. Department of Treasury [9]において、北朝鮮のミサイル技術拡散計画に関与したとして、ホンコン・エレクトロニクス、タンチョン商業銀行（Tanchon）及び朝鮮鉱業開発貿易公社（KOMID）の3法人を資産凍結の対象として指定したと発表した。同発表によれば、ホンコン・エレクトロニクスはイランのキシユ島（The Kish Island）に所在する法人で、北朝鮮有数の武器取扱い業者で弾道ミサイ

ル及び通常兵器の主要な輸出者であるKOMIDと平壤所在の金融機関であるTanchonとの間で数百万ドルにも及ぶ核拡散関連の資金移転を行っていたとされる。またTanchonは、先に米財務省が独自の金融制裁の対象にいち早くしたゼバ銀行との間でイランのミサイル開発計画関連の金融取引を行ったとされている¹⁶⁾。

このホンコン・エレクトロニクスの事例は、米財務省が金融インテリジェンスの手法を北朝鮮及びイランという米国にとっての二つの大きな安全保障上の脅威に対して、有機的かつ重層的に適用していることを示す好例と言えよう¹⁷⁾。

2.4 金融インテリジェンスのコア対象期（2007ー）

2007年秋以降のサブプライムローン問題、さらに2008年9月に米証券大手リーマンブラザーズが破綻して以来全世界へ波及した金融危機は、金融インテリジェンスにインテリジェンス政策上の新たな位置づけを与えた。

デニス・ブレア米国家情報長官は2009年2月12日、オバマ政権となって初めての「インテリジェンスコミュニティ年次脅威評価」（Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence）を米上院情報委員会に提出した。

この報告書はグローバルな金融危機の遠大な影響を米国にとっての脅威の筆頭に挙げている。その上で、同報告書は具体的に「米国の主要な短期的安全保障上の懸念は、グローバルな経済危機及びその地政学的含意である」（Dennis C. Blair [10] 2頁）と脅威の中身について述べ、さらに経済の回復が遅れば遅れるほど米国の戦略上の利益が大きく損なわれかねないこと、そして経済危機が1～2年間続けば各国の国家体制を揺るがす不安定性が増幅されるリスクを指摘している。それを米国が懸念しなければならないのは、「経済ナショナリズムの盛り上がりに加え、経済危機により米国の同盟国・友好国が防衛・人道上の義務を完全に履行できなくなり、その

15) オバマ選対が2008年大統領選挙のために立ち上げたウェブサイトであるOrganizing for America / BarakObama.comの中で、Remarks of Senator Barack Obama : AIPAC Policy Conference, Washington, DC June 04, 2008を参照。出所はhttp://www.barakobama.com/2008/06/04/remarks_of_senator_barack_obama

16) 米財務省は2009年7月30日及び8月11日、北朝鮮に対する追加の金融制裁措置を発表。特に8月11日公表の制裁措置では、Korea Kwangson Banking Corp. (KKBC) を先に制裁対象とされたTanchon等の国際金融取引に深い関与があったと認定している。これらの制裁は米当局が北朝鮮に対する金融制裁について、イランとのWMD関連取引とのつながりも念頭において一層の推進を行っている状況証拠のひとつと理解できよう。

17) 米財務省のみならず国務省も、2009年6月12日にフィリップ・ゴールドバーグ元ボリビア大使を大使級の国連安保理決議第1874号履行調整官に任命し、同調整官を7月初めにマレーシアと中国、さらに8月後半にはシンガポール、タイ、韓国及び日本に、財務省、国防総省及び国家安全保障会議の担当者とともに派遣し、北朝鮮に対する金融制裁等について意見交換を行うこととするなど、金融制裁を北朝鮮に対する圧力とレバレッジに活用しようとする積極的姿勢を示している。

ことが米国の国益に反する政治的副作用をもたらす可能性が大きい」(同2頁末尾)からである。

金融危機をもたらした原因とその地政学的リスクにもたらす影響は、CIA創設の思索上の父であるシャーマン・ケントが冷戦初期に経済インテリジェンスとしてその重要性を見通していたように、グローバリズムの転換点と評される2007年秋以降、インテリジェンスの対象の中心課題に戻ってきたのである。

この流れは金融に関するエンフォースメントの領域でも同様であり、2009年4月にロンドンで開催されたG20首脳会合の終結時に発表された首脳宣言付属文書では、「すべての国・地域に対して、金融健全性規制、租税及び反マネー・ローンダリング・反テロ資金に関する国際基準の遵守を求める」¹⁸⁾との文言が盛り込まれた。

これは、金融インテリジェンスの特徴であるインテリジェンスとエンフォースメントの密接な連関という文脈においても、金融インテリジェンスがコアの情報収集及び活動対象であることがG20諸国の首脳レベルでも認知されることになったと考えることができよう。

2.5 金融インテリジェンスのコア対象期の特長

2007年以降、インテリジェンスの対象の中核にグローバルな金融危機とその波及による地政学的影響が据えられるようになり、金融インテリジェンス先進国の米国ではとりわけ、インテリジェンス活動の力点及び体制に変化の兆しが見られる。

その変化のひとつは、OSINTの一層の重視である。

国家情報長官室は2009年6月、「2009年国家インテリジェンス 消費者ガイド」(2009 National Intelligence a consumer's guide)と題する報告書を公表した。このガイドはインテリジェンスの消費者であるホワイトハウスや米連邦議会のみならず、一般向けにも米国のインテリジェンスの力点や態勢がどのようなものであるかについ

てインテリジェンス部局自らが平易に解説した、類例のない解説書となっている。

この解説書では、インテリジェンスのソースとして、まず公開情報から得られるインテリジェンスであるOSINTを挙げ、次いで人的情報収集であるHUMINT、信号情報等を活用するSIGINT、地理等の画像情報が中心となるGEOINT、機械・物理情報を総合するMASINTの順に論じていく(Office of the Director of National Intelligence [12] 12頁)。このようにOSINTをインテリジェンスの手法の筆頭に置く考え方は、HUMINT、SIGINT、GEOINT、及びMASINTの4つのソースを代表的なインテリジェンス手法と考えるインテリジェンス理論の通説¹⁹⁾の理解とは一線を画すものと考えられる。

このようなOSINT重視は、国家情報長官が2008年7月に公表した「ビジョン2015: グローバルにネットワーク化し統合されたインテリジェンス事業体」(Vision 2015: A Globally Networked and Integrated Intelligence Enterprise)の考え方を踏襲するものであった。

この「ビジョン2015」報告書はグローバルな金融システムの危機や地球規模での大規模気候変動などの事態は米国のインテリジェンスコミュニティにどのような課題を提示しているか、そしてその処方箋は何かについて長期的視野に立ち分析を試みたものである。同報告書は「シフトする戦略的風景」と題する第1章において、専門の異なるインテリジェンス関係者が協力と連携を深め、オープン・ソース情報に広範なアクセスを図ること、そして深い専門性に基づく統合されたインテリジェンスの報告を政策当局者に行うことの重要性を強調している(Director of National Intelligence [13] 5頁)。

以上のようなオープン・ソース分析及び金融等に特化した専門性の高い分析の重視は、2009年1月にオバマ政権が誕生した後は、インテリジェンスの要求・消費側の

18) ロンドンサミット首脳宣言の金融システム強化に関する付属文書であるAnnex: Declaration on Strengthening the Financial System: London Summit, 2 April 2009の4頁参照。出所は<http://www.londonsummit.gov.uk/resources/en/PDF/Annex-strengthening-fin-sysm>

19) 例えばLowenthal [3]は、インテリジェンスのソースとして、GEOINT、SIGINT、MASINT、及びHUMINTの4つを挙げ、OSINTについては前述の4つのソースとは異なり、インテリジェンスの対象と得られた情報が1対1対応のプロセス(end-to-end processes)とならないことから、OSINTをインテリジェンス・ソースとしては一段低く取り扱う見方を示している(Lowenthal [3] 77頁)。

20) ギブス大統領報道官はサマーズNEC議長がEDBを毎朝オバマ大統領に行うことについて冒頭、記者からの質問を待つことなく自ら発表しており、オバマ政権の経済金融情報分析に対する積極性を表すものと考えられる。会見の具体的なやりとりについては、ホワイトハウスウェブサイト(http://www.whitehouse.gov/the_press_office/Press_Briefing_1-22-09)を参照のこと。

21) パネックCIA長官はEIBの目的について、「米国の政策当局者が銀行破綻や失業の増加の後遺症に驚かぬようにするため」と説明している(出所は例えば、ワシントンポスト2009年2月26日付紙 Joby Warrick記者執筆記事 "CIA Adds Economy To Threat Updates: White House Given First Daily Briefing")。

22) 例えば、米国の公共放送であるNational Public Radiotは2009年7月6日付のTom Gjelten記者執筆のニュース記事"World Economy Becomes Focus For CIA Recruiting"で、CIAが分析の中核にグローバルな金融危機を据えたことから、採用活動の焦点を金融専門家にシフトし、ブルンバーク・ラジオに広告を流し始めたことを報道している(出所は、<http://www.npr.org/templates/story/story.php?storyId=106290889>)。

選好としても顕著になっている。

例えば、ギブス大統領報道官は2009年1月のオバマ大統領就任後初の記者会見において、これまで歴代の大統領がインテリジェンスコミュニティから毎朝受けてきた大統領向けブリーフィング（Presidential Daily Briefing : PDB）に加え、ラリー・サマーズ国家経済安全保障会議（NEC）議長が説明役となり経済関係のブリーフィング（Economic Daily Briefing : EDB）を毎朝行うことを発表している²⁰⁾。そして翌2月にはレオン・パネッタ中央情報局（CIA）長官が記者会見において、上記のEDBに加え、グローバルな金融危機の国際的な影響に力点を置いたCIA独自の経済インテリジェンスブリーフィング（Economic Intelligence Briefing : EIB）を2月25日から毎朝大統領向けに開始したことを明らかにした²¹⁾。

そしてグローバルな金融危機とその含意をインテリジェンスの主要な分析課題に掲げる問題意識は政策当局者のみならず、米国インテリジェンスコミュニティにも共有されている。

例えば、国家情報評議会（National Intelligence Council）が2008年11月に公表した長期展望「グローバルトレンド2025：変容した世界」（Global Trends 2025 : A Transformed World）では、グローバル化した経済が直面する大きな課題について、金融の多極化、国家資本主義、グローバルな経済不均衡等のキーワードを使いながら巻頭で深く論述され、経済の不安定性が地政学的な主要リスクになる可能性が指摘されている（National Intelligence Council [14] 1 - 17頁）。

さらにグローバルな金融危機がインテリジェンスのコアの対象になった現実を反映し、CIAは世界的な金融の中心であるニューヨークのウォール街等から金融専門家を分析官として採用する人員強化にも乗り出している。具体的には、CIAが金融専門家に対する分析官募集のラジオ広告を開始したことが2009年7月に在米各紙等により報道²²⁾されており、米国インテリジェンスコミュニティがリソースの面でも金融インテリジェンスの分析に本腰を入れ始めたことが観察できる。

3 金融インテリジェンス態勢：日米比較

この節では、金融インテリジェンスの実施体制について、金融インテリジェンスの体制整備が最も進んでいる

と考えられている米国の事例を日本の事例と比較する観点から分析する。

3.1 米国の態勢

米国政府内では、インテリジェンスに関する全体政策の大枠を決定するのは大統領を中心とするホワイトハウスの政策決定部門であり、国家安全保障会議（NSC）が大きな役割を果たしている。その下に個別の政策実施機関として、国家情報長官（DNI）がとりまとめるCIAや陸海空海兵沿岸警備隊の5軍の情報部などの各インテリジェンス機関がある²³⁾。

金融インテリジェンス及び反マネー・ローンダリング・反テロ資金のエンフォースメントの実施に傾斜した組織としては、米財務省のテロ・金融インテリジェンス担当財務次官以下の部門が特に注目される²⁴⁾（**機構図は図1**）。

同財務次官は金融インテリジェンス及び反マネー・ローンダリング・反テロ資金対策の政策立案及び執行指揮を行う。そしてその傘下にあるインテリジェンス及び分析室（OIA）、外国資産管理室（OFAC）及び金融犯罪執行ネットワーク（FinCEN）が執行に当たる。

FinCENは米国の金融インテリジェンスユニットになっており、米愛国者法、銀行秘密法（Bank Secrecy Act）及び関連の大統領令等に基づき、米国の金融機関から顧客に関する疑わしい取引の届出（Suspicious Activity Report : SAR）を受理する。受理されたSARは連邦司法捜査当局、税関、国境警備隊、インテリジェンス機関等との情報交換や捜査連携に活用される。

またOFACは資産凍結などの制裁措置の執行に当たる機関である。

このように米国の金融インテリジェンス及びエンフォースメントの組織と機能は、米財務省のテロ・金融インテリジェンス担当次官を結節点にし、政策及び執行が上部に当たるNSCと下部に当たるOIA、FinCEN及びOFACと切れ目なくつながる体制となっているところに特徴がある。

また米国のマネー・ローンダリング対策の法的根拠面での特色として本庄資 [11] は、1986年マネー・ローンダリング規制法により脱税がマネー・ローンダリング摘発の対象前提犯罪となっており（同書33, 63, 及び148

23) 米国のインテリジェンスコミュニティの概要については、Office of the Director of National Intelligence, "2009 National Intelligence : a consumer's guide" (http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf), 及びCody M. Brown, "The National Security Council : A Legal History of the President's Most Powerful Advisers", Project on National Security Reform, 2008による。

24) 本節の分析は、主として米財務省ウェブサイト (<http://www.treas.gov>)、FinCENウェブサイト (<http://www.fincen.gov>)、及びOFACウェブサイト (<http://www.treas.gov/ofac>) による。

頁), 米国の連邦租税当局である財務省傘下の内国歳入庁 (IRS) が金融インテリジェンスの枠組に参加して、租税関係情報から金融インテリジェンスのくみ上げが行われていることを明らかにしている。

3.2 日本の態勢

米国の金融インテリジェンスの態勢が政策と執行を継ぎ目なく実施する機能一元集中型とすれば、日本の態勢は、政策と執行が分離するツイン・ピークス型に²⁵⁾喩えられる。

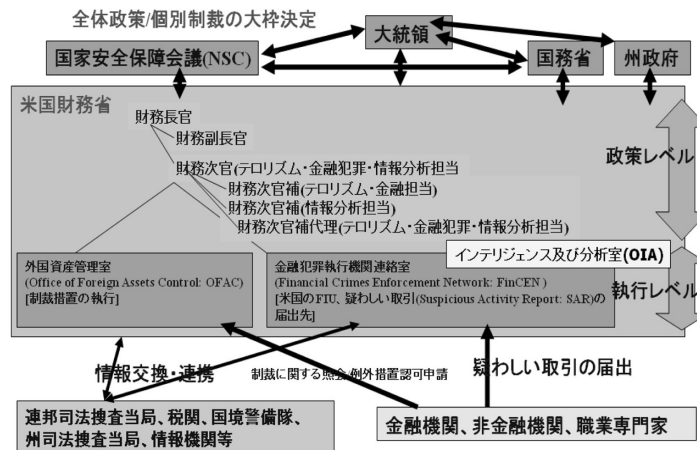


図1：米国の金融インテリジェンスの態勢

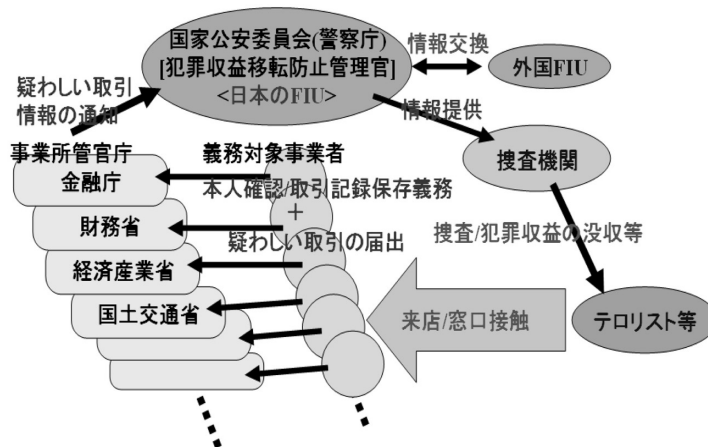


図2：日本の金融インテリジェンスの態勢（執行）

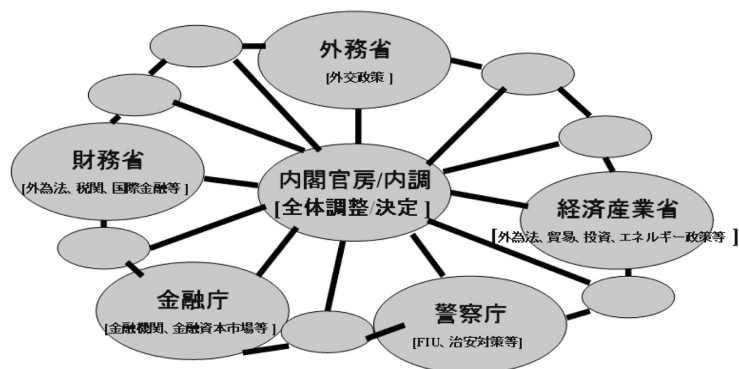


図3：日本の金融インテリジェンスの態勢（政策）

すなわちエンフォースメントについては、これまでの本人確認法及び組織的犯罪処罰法を統合・拡充する形で2007年に施行された犯罪収益流通防止法に基づき、金融機関や専門職等の義務対象事業者が本人確認と取引の記録保存を行ない、その中から抽出された疑わしい取引を、金融庁をはじめとする各事業所管官庁が日本の金融インテリジェンスユニットである国家公安委員会（警察庁刑事局犯罪収益移転防止管理官）²⁶⁾に通知し、さらに各捜査機関や外国FIUとの情報交換及び連携に生かされるというサイクルになっている（組織図は図2）。

他方、政策については、金融インテリジェンスはインテリジェンス全体の政策決定の中で内閣官房情報調査室がとりまとめるの中心となり、各政策所管官庁がハブ・アンド・スポーク型に連携をとる形になっている（組織図は図3）。

前節で見た米国の金融インテリジェンスの態勢に比べ、日本型の態勢は執行と政策決定が別のインテリジェンスサイクルにより追及されるところにある。さらに、政策面で金融インテリジェンスに特に傾斜した組織または機能の萌芽は今のところ見られていない。

また、米国の法執行態勢に比べて、日本は脱税がマネー・ローンダリングの対象前提犯罪になっておらず、租税情報から金融インテリジェンスを抽出する態勢にはなっていないものと推定される。

4 まとめ

以上を総括すれば、金融インテリジェンスは元来経済インテリジェンスの一分枝として冷戦初期から注目されていたにもかかわらず、やがて半ば忘れられていたものの、90年代に至りマネー・ローンダリング対策のエンフォースメントの手法として復活したものである。そして金融インテリジェンスは9-11テロの発生を触媒にしてテロとの戦いの外延で意義あるものと意識されるようになった。

金融インテリジェンスをインテリジェンスの中心として活用することに目覚めたのが、米財務省テロ・金融イ

ンテリジェンス担当部局をはじめとする米国の金融に特化したインテリジェンス組織である。これらの組織は2005年のバンコ・デルタ・アジア事件及び2006年に発覚したTFTPでの成功体験を通じて金融インテリジェンスの有用性に確信を深めていったのである。

そしてブッシュ政権のその確信は、北朝鮮やイラン等米国が安全保障上の脅威と感じている諸国への対応に当たり、非軍事的オプションの主要対応策として金融インテリジェンスを意識するという手法の確立につながることになる。

そして2007年秋以降のグローバルな金融危機は米インテリジェンスコミュニティの感じる脅威の巻頭に金融危機及びその地政学的含意を置くこととなり、金融インテリジェンスの優先度をさらに高めることになったと言える。

他方で、金融インテリジェンスの実施態勢について日米を比較すれば、政策決定と執行が継ぎ目なくつながる米国の態勢に比べ、日本では金融インテリジェンスに特化した政策決定の機能が見当たらず、さらに政策と執行を接続する機能も必ずしも確立していないと考えられる。

また、今後の研究課題としては、インテリジェンスの手法として金融インテリジェンスと他のインテリジェンスとでは特に異なるところはないと考えられている²⁷⁾ものの、金融インテリジェンスが特に効果を発揮し得る情報収集の局面や分析手法の開発に関する方法論の開拓が望まれる。

謝辞

本論文の作成に当たっては、匿名の2名の査読者から大変有益なご意見を頂いた。記して謝意を表したい。本論文の作成はすべて公表資料に基づいており、本論文の意見にわたる部分は、執筆者がかつて属した、または現在属する組織の見解を表すものではない。本論文に誤りが残っているとすれば、それはすべて執筆者の責任である。

25) 本節の記述は、内閣官房情報調査室「内閣官房情報調査室2009」(<http://www.cas.go.jp/saiyou/panfbasui2009.pdf>)、金融庁「金融庁の1年：平成18事務年度」第17章(<http://www.fsa.go.jp/common/paper/18/honpen/17.pdf>) 168～170頁、及び警察庁刑事局組織犯罪対策部犯罪収益移転防止管理官ウェブサイト(<http://www.npa.go.jp/sosikihanzai/jafic/index.htm>)による。

26) 日本の金融インテリジェンスユニット(FIU)は、発足以来金融監督庁、及びその後身の金融庁が担ってきたが、FATF勧告等により本人確認義務等が金融庁の所管する金融機関以外にも広がったことを受け、2007年4月以降、国家公安委員会に移管された。

27) 企業の財務最高責任者(CFO)向けの記事を掲載するウェブサイトであるCFO.comは、2009年2月13日付でDavid M. Katzによる”SEC Should Adopt CIA Methods, Lawyers Say”と題する記事を掲載し、このところ証券不正事件の摘発に遅れをとることの多い米証券取引委員会(SEC)はむしろCIAのインテリジェンス手法を捜査に取り入れるべきと論じている。この記事は、金融インテリジェンスと他のインテリジェンスの手法にほぼ異なることがないとの前提に立って思考する考え方を紹介するひとつの例となっている。出所は<http://www.cfo.com/printable/article.cfm/13131360>

参考文献

- [1] Karen Berman and Joe Knight with John Case, Financial Intelligence, Harvard Business School Press, Boston, Massachusetts (2006)
- [2] R. Brook Hansen, Developing Financial Intelligence, Author House, Bloomington, IN (2006)
- [3] Mark M. Lowenthal, Intelligence : From Secret to Policy, Fourth Edition, CQ Press, Washington, DC (2009)
- [4] Sherman Kent, Strategic Intelligence for American World Policy, Princeton University Press, Princeton, New Jersey (1951)
- [5] Abram N. Shulsky and Gary J. Schmitt, Silent Warfare : Understanding the World of Intelligence, Mana Publications, New Delhi, India (2006)
- [6] Ian Bremmer and Preston Keat, The Fat Tail : The Power of Political Knowledge for Strategic Investing, Oxford University Press (2009)
- [7] U.S. Department of Treasury, Testimony of Stuart Levey, Under Secretary Terrorism and Financial Intelligence U.S. Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations, July 11, 2006 HP-05, 米財務省ウェブサイト
(<http://www.treas.gov/press/releases/hp05.htm>) (2006)
- [8] U.S. Congressional Research Service, Mary Beth Nikitin et al., North Korea's Second Nuclear Test : Implications of U.N. Security Council Resolution 1874, July 1, 2009 (2009)
- [9] U.S. Department of Treasury, Treasury Targets North Korea's Missile Proliferation Network, June 30, 20069 TG-191, 米財務省ウェブサイト
(<http://www.treas.gov/press/releases/tg191.htm>) (2009)
- [10] Dennis C. Blair, Director of National Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, 12 February 2009, The Office of the Director of National Intelligence, DNIウェブサイト
(<http://www.dni.gov/testimonies.htm>) (2009)
- [11] 本庄資, 米国マネー・ロンダリング : 米国財務省・IRS-CI捜査, 税務経理協会, 2006
- [12] Office of the Director of National Intelligence, 2009 National Intelligence a consumer's guide, 米情報長官室ウェブサイト
(http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf) (2009)
- [13] Director of National Intelligence, Vision 2015 : A Globally Networked and Integrated Intelligence Enterprise 米情報長官室ウェブサイト
(http://www.dni.gov/Vision_2015.pdf) (2008)
- [14] National Intelligence Council, Global Trends 2025 : A Transformed World 米情報長官室ウェブサイト
(http://www.dni.gov/nic/NIC_2025_project.html) (2008)