複雑化する拡散金融と制裁回避スキーム
―FATF（金融活動作業部会）プロジェクトにおけるCo-lead（共同リーダー）の経験を通じて―

国際局調査課 資金移転対策室 総括補佐　**松尾　綱紀**

SPOT

1．プロローグ

2025年7月29日、東京 21時45分（パリ 14時45分、ワシントンDC 8時45分）

*「無事にWebinar[*1]終了。Matthew、Masa、みんなお疲れ様。ライブ配信の視聴者合計は3,012名、FATF（ファトフ）が主催したWebinarで過去最多の参加者ね。」*

1年間に亘ったプロジェクトを他のいくつもの案件と掛け持ちしながら担当し、常に中立的視点から改善策を助言し続けてくれた韓国出身のFATF事務局員が、Webinarの登壇者に告げた。

*「Masa、去年の夏には僕と君以外何もなかったプロジェクトが、今日こんな素晴らしいWebinarに繋がったなんて信じられるかい？」私をプロジェクトのCo-lead（共同リーダー）に誘ってくれた米国人の同僚がつぶやく。NatsとCommanders[*2]をこよなく愛するWashingtonianだが、私と一緒に仕事をするようになってから5年、「カネで選手を集める都会のチームは苦手なんだけど。」と苦笑しつつ、DodgersやCubsのことも気に掛けてWhatsAppにメッセージをくれる心優しい相棒だ。*

「信じられないよ、Matthew。君や、30名のプロジェクトチームメンバーを代表して今日プレゼンをしてくれた4人、みんなと素晴らしい成果が得られて最良の瞬間だよ。」と私。

「ドリームチームね。また一緒に仕事できたことを誇りに思うわ。」3年ぶりに共に仕事をした英国財務省のチームメンバー。各国から提出された数多くのケーススタディから、プロジェクトの目的に沿い読者に有益なものを選りすぐり、報告書をドラフトしてくれた。

間髪を入れず、国連安保理・北朝鮮専門家パネル委員で、我々のプロジェクトを学術的な視点から支えてくれたロンドン大学の教授からメールが届いた。

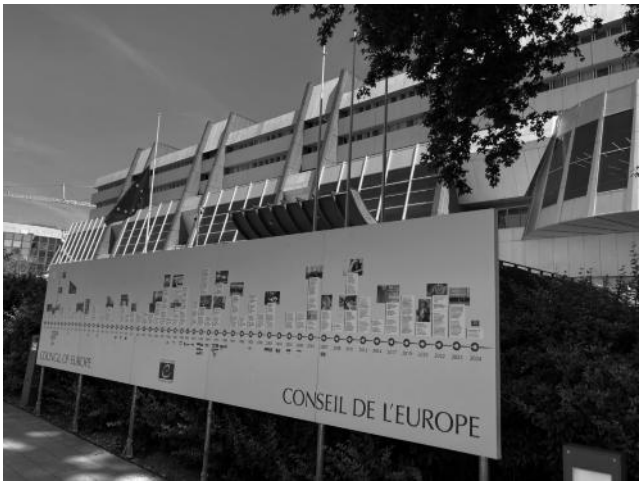
「Masa、Webinarをライブ視聴したよ。成功おめでとう。君も会合中に指摘していたけど、本問題における民間セクターの関与は非常に重要だ。拡散金融への対応は単に国連安保理決議に基づく制裁実施にのみ限定されるのではなく、その周辺事象まで広くとらえるべきだと思うよ。引き続き幸運を祈る。」

本年6月20日（金）パリ時間午前、マネー・ローンダリング（マネロン）・テロ資金供与・拡散金融対策に取り組む多国間の枠組みであるFinancial Action Task Force（FATF：金融活動作業部会）の公式ウェブサイト上に、「Complex Proliferation Financing and Sanctions Evasion Schemes －複雑化する拡散金融と制裁回避スキーム－」と題する報告書（以下「報告書」）が公表された[*3]。その前週、フランス・ストラスブールで開催されたFATF6月全体会合において、下部委員会（RTMG：Risk, Trends and Methods Group）の議論を経て最終採択されたものだ。

拡散金融とは、大量破壊兵器（核・化学・生物兵器）等の開発、保有、輸出等に関与するとして国連安全保障理事会により資産凍結等措置の対象となっている者に、資金又は金融サービスを提供する行為をいう[*4]。

この「報告書」は、拡散金融関連の制裁を回避する

注）本稿の内容は、筆者の所属する組織を代表するものではない。誤りがある場合は全て筆者の責任である。
＊1）本年9月5日現在、FATF YouTube Channelにて視聴可能。FATF's Youtube Channel
＊2）前者は米大リーグのNationals、後者は米フットボールのCommanders。共にWashington DCを本拠地とする。
＊3）https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html
＊4）財務省公式ウェブサイト「知ってる？マネロン等対策」より。本項目に限らず、財務省が取組むマネロン・テロ資金供与・拡散金融対策に関する情報は本ページに詳しいので、是非ご参照いただきたい。
https://www.mof.go.jp/policy/international_policy/amlcftcpf/2.measures.html#sec03



【写真1】FATF/MONEYVAL合同Plenaryの会場となった欧州評議会（外観）

【写真2】FATF/MONEYVAL合同Plenaryの会場となった欧州評議会（外観）

【写真3】FATF/MONEYVAL合同Plenaryの会場となった欧州評議会（本会議場）

ために用いられる進化する手法と技術の詳細な分析を提供し、制裁を回避しようとする者の手口やその類型（タイポロジー）を整理したものである。

「複雑化する拡散金融とその回避スキーム」プロジェクト（以下「プロジェクト」）は、2024年6月にパリで開催されたFATF全体会合でその立ち上げが承認された。「プロジェクト」は、翌7月から本年6月までの1年間を活動期間とし、2名のCo-lead（共同リーダー）が、プロジェクトメンバーとの議論の上最終報告書を取りまとめ、全体会合に報告することを求めた。私は、米国財務省の同僚とともに、Co-leadとなり、「プロジェクト」実施のためにFATF及びその地域体であるFSRBs（FATF型地域体：FATF-style Regional Bodies）の24か国及び3機関から集った計30人によるプロジェクトチームを組成した。

本稿では、1年間に亘った国際組織のプロジェクトCo-leadの経験を通じて得た、複雑化する拡散金融と制裁回避スキームの現状と問題点、また「報告書」のポイントを概説したい。

2．拡散金融とは何か

（1）FATFと拡散金融

FATFは「Financial Action Task Force」の略で、「金融活動作業部会」と訳され「ファトフ」と発音されることが多い。名称上はあくまでタスクフォースであり「一時的な作業グループ」といった趣だが、1989年の創設後今年で36年目を迎える多国間の枠組みである*5。

FATFは、1989年、G7大蔵大臣・中央銀行総裁会議がフランス議長下で開催された際*6、当時世界的に大きな問題となっていた麻薬取引に端を発するマネロン問題の対応のため、同国を本拠に立ち上げられたものだ。

FATFには38か国・地域及び2つの地域機関が加盟している。それに加え、9つのFSRBsの加盟国と合わせることで世界200カ国以上をカバーし、全ての加盟国

＊5）2024年4月のFATF大臣声明（パラ2）において、FATFがOpen-endedなマンデートを有し活動することが確認されている。https://www.fatf-gafi.org/content/dam/fatf-gafi/FATF/FATF-Ministerial-Declaration-2024.pdf.coredownload.inline.pdf
＊6）フランス革命200周年を機に建設された新凱旋門（La Grande Arche）を会場に開催されたことから一般に「アルシュ・サミット」と呼ばれる。

が同じ基準（FATF40の勧告、解釈ノート等）を適用し、加盟国間の履行状況を相互に審査し合っている*7。

FATFの役割は創設以後順次拡大している。当初は薬物犯罪や重大犯罪に起因するマネロン対策のみを対象としていた。その後、2001年9月に発生した米国同時多発テロ事件を受け、テロ対策のための特別勧告（当初8個、後に9個）が定められた。また、2012年には、イランや北朝鮮の大量破壊兵器の拡散活動の脅威の高まりを受け、拡散金融もその活動対象に含めることとなった。

私は2020年から3年間、財務省国際局からFATF事務局に出向した。創設当時を知るスタッフは少なくなっていたが、「当時はOECD金融企業局の片隅に担当者の机が2つ置かれていただけだったんだ。」といった昔話を聞かせてくれた。日進月歩で進展するマネロン・テロ資金供与・拡散金融のリスクや脅威に対応し、FATF最大の任務である「金融の健全性（financial integrity）」に資するその役割の大きさに比例し、FATF事務局は現在70名以上のスタッフを抱えるまでに成長している。

（2）現状・問題点

そもそも、なぜ「複雑化する拡散金融と制裁回避スキーム」なるプロジェクトが立ち上げられたのだろうか。主な理由として2つ指摘しておきたい。

第一に、拡散金融を巡る問題への対応は緊急性が高いことが挙げられる。前回、FATFが拡散金融に係るタイポロジーの報告書を公表したのは2008年である*8。それ以降約20年が経過し、金融取引の状況は世界全体で劇的に変化している。拡散金融に関しても、国家主体（state actors）のみならずテロ団体などの非国家主体（non-state actors）が、大量破壊兵器（WMD：Weapons of Mass Destruction）プログラムを支援するため、高度な調達ネットワーク、収益獲得スキーム、そして新たな金融技術を用いることで制裁を回避している例が散見される。

例えば、北朝鮮は、2025年2月にドバイを本拠にインターネット上で暗号資産取引を行っているByBitから15億ドルを窃取するなど、暗号資産関連企業へのサイバー攻撃を通じて数十億ドル規模の収益を得ている*9。また、日本、米国、韓国等では、北朝鮮の情報技術（IT）関連の労働者が身元情報を偽装等することで、不正にリモートワークの職を得ている（後述のケーススタディ参照）。このように、北朝鮮はWMD計画のために大規模な不正収入を生み出しているとみられるが、当局によって把握された事案は全体のごく一部に過ぎないと考えられている。

日本は、北朝鮮による暗号資産窃取への対応が喫緊の課題である点を国際場裡で指摘してきた。特に、本年5月に開催されたG7財務大臣・中央銀行総裁会議において採択されたG7「Financial Crime Call to Action」で、「北朝鮮の暗号資産窃取」に係る取組みの重要性が日本の提案に基づき盛り込まれた点は特筆すべきである*10。

このように脅威が増大しているにもかかわらず、FATFが2014年から2024年にかけて行った第4次相互審査の結果を分析すると、法整備状況（TC：Technical Compliance）については、ほぼ半数（46%）の国で拡散金融に対処するための適切な法的枠組みが整備されていない。更に、法令の実効性確保（IO：Immediate Outcome）については、拡散金融に効果的に対処できている割合は16%にとどまっている。

第二に、各国当局や民間セクターの関係者に必要な情報を速やかに提供する必要性も指摘したい。上述のとおり、FATFが自らのマンデートに拡散金融を加えたことを受け、2020年には、従来マネロン・テロ資金供与に係るリスク評価を求めていた勧告1を改訂し、各国は拡散金融のリスクについても特定、評価、理解し、それらのリスクに応じた緩和策を講じることが求められることとなった。そして、本年から始まる第5次相互審査からその実施状況が審査対象となる。これに伴い、FATFは各国が拡散金融リスク評価書を作成

＊7）なお、我が国はFATFの加盟国であると同時に、アジア・太平洋諸国をカバーするAPG（Asia Pacific Group on Money-Laundering）のメンバー国でもある。APGにおいては、2024年9月から約2年間、FATF日本政府首席代表の財務省梶川審議官が共同議長を務めており、本年8月には東京で年次総会を開催した。開催期間中、金融庁が暗号資産とその悪用に関するセミナーを主催し、「プロジェクト」の米・日Co-leadがその概要や意義を説明した。
＊8）https://www.fatf-gafi.org/en/publications/Methodsandtrends/Typologiesreportonproliferationfinancing.html
＊9）https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/
＊10）https://www.mof.go.jp/policy/international_policy/convention/g7/index.htm

するためのガイドラインを2018年及び2021年に公表している*11。

今回公表に至った「報告書」は、拡散金融に関連する制裁回避に対処するために、権限ある当局(competent authorities)、金融機関、特定非金融業者及び職業専門家（DNFBPs)、及び暗号資産サービスプロバイダー（VASPs）が、適切に拡散金融のリスクを評価し、その活動の支援に資することを目的としたものである。

3．「複雑化する拡散金融と制裁回避スキーム」プロジェクト報告書の概要

拡散金融のリスクの特定にあたっても、マネロン・テロ資金に係るリスク評価同様、リスクの「脅威(threats)」、「脆弱性（vulnerabilities)」及び「脅威・脆弱性の影響とその対応（consequences)」の要素に基づき評価することとされている。本稿でもその整理に従って概説する。なお、各項目に「報告書」本体のページ・パラ番号を付すので、更にご関心のある方はご参照いただきたい。

（1）脅威（threats)（「報告書」12頁、パラ18以降）

脅威とは、過去、現在又は将来において、拡散金融に係る対象を特定した金融制裁の履行を回避、違反又は悪用した、あるいはその可能性がある個人又は団体を指す*12。その中には、大量破壊兵器等の開発、保有、輸出等に関与するとして資産凍結等措置の対象となっている者や当該対象者の支援や同調をする個人、団体も含まれる。また、実際に回避、違反又は悪用した、あるいはその可能性があるものだけでなく、間接的に関与したものも含まれる。

上記に基づき、「報告書」においては、現在の状況における脅威を以下のとおり分析している。

ア．北朝鮮

北朝鮮は、拡散金融対策において重要な脅威の主体である。2006年の国連安保理決議第1695号以降20年近くに及ぶ国連制裁*13にもかかわらず、北朝鮮は大量破壊兵器の開発を続けている。例えば、2024年10月、北朝鮮は軍備拡張計画に基づき11発目の大陸間弾道ミサイルを発射し、国際的な制裁への継続的な抵抗を示した。北朝鮮は、違法な資金の流れを隠蔽するための仲介業者（intermediary）や実質的所有者(beneficial ownership）構造の悪用、暗号資産を含む新技術の活用、瀬取り（ship-to-ship transfers）や文書偽造（falsifying documentation）など、様々な制裁回避戦術を用いている。

国際的な監視の観点から見ると、国連の北朝鮮制裁リストに新たな主体が最後に追加されたのは2017年であり、それ以降新たな指定はない*14。国連安保理決議第1718号に基づき設立され、北朝鮮に関する拡散金融行動を監視するための専門家パネル（POE：Panel of Experts）は、昨年4月、その活動延長決議においてロシアが拒否権を発動（中国は棄権）したことにより活動終了に追い込まれた*15。これにより、北朝鮮の大量破壊兵器に係る活動をグローバルに監視する体制に重大な空白が生じたことで制裁回避活動の追跡と対処が困難になり、FATFの文脈においても、各国による北朝鮮に関連する拡散金融リスクの評価やその低減措置といった対応が阻害されている。

「報告書」は、北朝鮮による大量破壊兵器計画への資金調達に寄与する2つの主要な要因を指摘している。

第一に、北朝鮮の金融面における各種連携強化の動きである。例えば、2024年末、北朝鮮とロシアは包括的戦略的パートナーシップ条約を締結した*16。そこでは、銀行間連携を含む経済協力の強化、両地域の経済・投資可能性に関する相互理解の促進に合意している。2024年時点で、国連安保理制裁により北朝鮮の金融機関関係者は追放対象となっているにもかかわらず、北朝鮮隣国及びロシアに拠点を置く北朝鮮の金融

＊11） https://www.fatf-gafi.org/en/publications/Financingofproliferation/Guidance-counter-proliferation-financing.html
https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html
＊12） FATF "Guidance on Proliferation Financing Risk Assessment and Mitigation" パラ22a。日本語訳は財務省による仮訳。
https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html
＊13） https://www.mofa.go.jp/mofaj/gaiko/unsc/page3_003268.html
＊14） 同上。
＊15） 同上。その後、2024年10月、同年4月に専門家パネルの活動が終了したことを受け、日本を含む同志国は、多国間制裁監視チーム（MSMT: Multilateral Sanctions Monitoring Team）を設立。本年5月、第1回目の報告書を公表した。
＊16） http://en.kremlin.ru/acts/news/75534

関係者らは、北朝鮮の貿易と歳入増加を支援すべく、数億ドル規模の取引を促進していた。こうした金融面での連携の強化は、国際金融システムに脆弱性をもたらしている。

第二に、北朝鮮が歳入を増加させるための手段が多様化しており、これが拡散金融や制裁回避の脅威をさらに深刻化させている。例えば、2024年時点で、北朝鮮の「かつら」と「つけまつげ」の輸出は、北朝鮮隣国に対する北朝鮮の輸出の約60%を占めていた。しかし、これらの取引は制裁対象の北朝鮮貿易会社と関連しており、当該輸出収益が北朝鮮の戦略兵器計画を支えている可能性が示唆されている*17。その他の収入源として、詐欺、サイバー窃盗、武器、麻薬、野生生物の密売などが挙げられる。北朝鮮によるIT労働者による活動については後述する。

イ．イラン

イランも、依然として、複雑化する拡散金融と制裁回避スキームの大きな脅威と認識されている。イランは当初、ウラン濃縮プログラムの停止を義務付けた国連安保理決議第1696号の未遵守により、国連から制裁を受け、新たに決議第2231号が採択された*18。この決議内容のうち、イランに関連する個人及び団体に課された国連の標的型金融制裁は2023年10月に失効したが、多くの国が、イランに対する脅威から、独自に国内制裁プログラムを実施している。

イランは、中東における軍事化された代理組織や、制裁を回避するために外貨両替所や銀行を利用する国際犯罪ネットワークに依存してきた。特に、ヒズボラは、制裁に直接違反してイランの代理として活動し、石油、武器をはじめとする様々な制裁対象物の大規模な密輸活動を行っている。

ウ．ロシア

上述のとおり、ロシアと北朝鮮の経済的・軍事的連携は、ロシアが拡散金融の脅威たりうる懸念を惹起している。 上述の包括的戦略的パートナーシップ条約は、北朝鮮のWMD計画を支える新たな収入源を生み出した。更に、この新たな二国間条約に基づき、北朝鮮兵士がロシア・ウクライナ紛争に派遣されたとの報告もある。こうした経済・軍事関係の拡大は、多くの国でロシアが拡散金融の脅威であるとの懸念を高めるとともに、拡散金融と制裁回避の状況を更に複雑化させている。

エ．その他の脅威

多くの国は、国家主体（state actors）に加え、テロ組織や犯罪組織などの非国家主体（non-state actors）が、生物兵器、化学兵器、核兵器を含む大量破壊兵器に関連する物資、知識、技術を入手・調達しようとする動きを依然として懸念している。この点、2022年11月に更新された国連安保理決議第1540号は、非国家主体への大量破壊兵器の拡散を防止するという世界的なコミットメントを再確認した。これまでのところ、非国家主体が金融システムを悪用して拡散金融を行う主体やその活動を支援していた事例は少ないものの、多くの国は、その潜在的な影響を継続的に監視することが重要と認識している。

（2）脆弱性（vulnerabilities）（報告書16頁、パラ36以降）

脆弱性とは、拡散金融に係る金融制裁の違反、未実施、又は回避を支援・促進する可能性のある脅威や脅威主体によって悪用される可能性のある要因を指す*19。FATF勧告7が対象とする国連安保理に基づく制裁は、現在北朝鮮のみを対象としているが、拡散金融リスクをより広い視点で捉えている国にとっては、北朝鮮に限らず全ての拡散金融主体によって悪用される脆弱性に適用されることになる。

脆弱性の分析は国家レベルとセクターレベルで行われるため、本稿もその分類に従う。

ア．国家レベルの脆弱性分析

経済及び貿易要因：拡散金融及び制裁回避を目論

＊17）例えば、米外国資産管理局（OFAC）は、米のe.l.f Cosmetics社が中国の2業者から輸入したつけまつげの原材料が北朝鮮産であり、OFACの規制違反を問われた事例を公表している。本件では、e.l.f Cosmetics社がOFACに996,080ドルを支払うことで和解した。https://ofac.treasury.gov/recent-actions/20190131
＊18）https://www.mofa.go.jp/mofaj/press/release/press3_000185.html
＊19）FATF "Guidance on Proliferation Financing Risk Assessment and Mitigation" パラ22b。日本語訳は財務省による仮訳。https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

む主体は、国際的な金融ハブである国や、主要な港湾や物流インフラを有する国を標的とすることが多い。こうした国は、提供するサービスの幅広さ、世界的資金フローの規模の大きさ、開放経済における輸送活動といった点で、金融や軍民両用品（民生用と軍事用の両方の用途を持つ物品）輸送に利用されやすく、脆弱性が高いといえる。

規制要因：各国がマネロン・テロ資金対策の強化で大きな進歩を遂げている一方、拡散金融に特化した措置の実施はなお改善の余地が大きい。このギャップは、国際金融システムの健全性と国連制裁義務の遵守にとって深刻な課題となっている。拡散金融や制裁回避スキームが益々複雑化する中、たとえ法律が存在していても、その検知と執行に必要な人的・資金的リソースや専門知識は不足しがちである。また、法人の実質的支配者の透明性に係る国内法制が脆弱な国では、当局が資金の流れを追跡したり、資産の最終的な所有者を特定したりすることが困難となりうることから、規制要因に起因する拡散金融の脆弱性が更に深刻化するといえる。

地理的及び人口統計学的要因：国連安保理決議に基づく制裁や、各国による独自制裁の対象となる国に地理的に近いことも重大な脆弱性を生み出しうる。日本をはじめとして東アジアに位置し北朝鮮に近い国々は、拡散金融に関連する迂回的な取引や違法な輸送に係る脆弱性が高いと認識している。また、戦略的に重要な位置にある国は、しばしば重要な航路、自由貿易地域、あるいは交通量の多い国境検問所を支配しており、これが近隣諸国の脆弱性を高める例もある。また、よく見落とされる脆弱性として、国連制裁対象地域の外交官やその他の代表者の存在がある。これらの人物は、資産の移動、機密情報の収集、あるいは制限措置の回避に関与する可能性がある。

イ．セクターレベルでの脆弱性分析

銀行及びその他の金融セクター：拡散金融に対して最も脆弱なセクターとして、まず、国境を越えた取引に従事する銀行及びその他の金融セクターが挙げられよう。脅威の主体は、複数の口座、貿易文書の偽造、取引の階層化など、解明を困難にする様々な手法を用いて、資金の流れの本質と目的を隠蔽する。特に貿易金融は、軍民両用品や制裁対象品目の移動を隠蔽するために頻繁に悪用されている。また、電信送金は効率的ではあるものの、取引の目的や裏付けとなる書類に係る情報が限られているため、制裁回避の主要な手段となる傾向がある。

暗号資産（virtual assets：VA）及び暗号資産サービスプロバイダー（virtual assets service providers：VASPs）：多くの国において、伝統的な金融監督を回避する目的も含め、国境を越えた資金移動に暗号資産が利用されている事例が増加している。拡散金融を目論む主体は、特にVA/VASPs対策のためのFATF勧告15の履行状況が各国において均一でないことを積極的に悪用していると考えられている。規制が整備されている国でさえ、VASPsのコンプライアンス遵守のレベル次第でリスクが高まる。例えば、ミキシングサービスは、北朝鮮のWMDに関連するものも含め、大規模な暗号資産窃取による収益の洗浄に頻繁に悪用されているとされる。こうした新しく複雑な暗号資産の手段は、取引の追跡や資金の真の出所・送金先を特定することを極めて困難にしている。

新たな代替決済インフラ：一部の国家主体及び非国家主体が、制裁執行に関連する従来の金融チャネルを回避するために、現地通貨決済の利用促進や、SWIFTの代替手段やP2P取引など、新たな代替決済インフラを利用していることにも留意すべきである。

その他のセクターレベルの脆弱性：伝統的な金融セクターに加え、複雑な法的構造の形成に関与する企業サービスプロバイダーや、宝石・貴金属業者などのセクターは、高価値で輸送が容易な手段を提供しているため制裁対象者が国境を越えて資金を移動するための代替となりやすく、拡散金融

及び制裁回避のリスクに特に晒されやすいと分析している。また、航空、海事、原子力、造船業も、軍民両用品や技術との関連性から、悪用されやすいと分析している。

（3）ケーススタディによる手口分析（報告書21頁、パラ56以降）

「報告書」では、4つの主要な類型として、ア．制裁回避のための仲介業者（intermediary）の利用、イ．金融システムへのアクセスのための実質的支配者情報（beneficial ownership Information）の隠蔽、ウ．暗号資産（virtual assets）等の新技術の利用、エ．海運セクター（maritime sector）の悪用に分類し、それぞれの類型における様々な拡散金融と制裁回避スキームにおける手法を分析している。

「報告書」の一つの特徴として、本プロジェクトの射程（scope）に従い、FATF勧告7でその実施が求められている特に北朝鮮に対する拡散関連の標的型金融制裁（Targeted Financial Sanctions）の回避事例と、FATF基準では義務付けられていない各国独自の制裁制度の回避事例の両者を包含しつつ、前者を緑・後者を青に明確に色分けの上記載している点が挙げられる。幅広いケーススタディを検討することで、異なる類型における脅威、脆弱性、共通の課題について、より包括的かつ最新の理解を深めるための工夫である。以下、代表的な事例を抜粋する。

ア．類型1：制裁回避のための仲介業者の利用

第一の類型は、制裁を回避し軍民両用品の輸送を容易にすべく、仲介業者を利用することである。

【オーストラリアの事例（「報告書」22頁、Box 2)】

2021年、豪・ニューサウスウェールズ州最高裁判所は、豪国民を北朝鮮関連制裁法違反で起訴した。この事件では、当該人物はオフショア銀行口座と豪に拠点を置くフロント企業を利用して、北朝鮮に代わって購入したイラン産ガソリン、ミサイル、ミサイル関連技術など、様々な物品について北朝鮮との貿易を仲介していた。

イ．類型2：実質的支配者情報の隠蔽による制裁回避と金融システムへのアクセス

制裁回避スキームが、外国に拠点を置くフロント企業や外国人、無認可の金融仲介業者、マネロン・テロ資金対策規制が緩い地域にある子会社、偽名で不正に取得したデビットカードやクレジットカードなどの第三者仲介業者を利用して、実質的支配者情報（beneficial ownership information）を隠蔽している事例を紹介している。

【オランダの事例（「報告書」33頁、Box 14)】

認知度の高い有名企業と違法なトラスト・アンド・カンパニー・サービスプロバイダーを巧みに利用することで、イランからとされる資金が、主要な金融センターを経由してオランダの法人に違法に送金された。資金が最終目的地に到達するまでに、実質的支配者と取引目的を不明瞭にしたため、金融機関がスキームの全体像を把握できなかったものである。

ウ．類型3：暗号資産及びその他のテクノロジーの利用

暗号資産（virtual assets）は、制裁対象国への直接的な資金移動や、異なる制裁体制を有する第三国を経由した間接的な資金移動を促進するために利用されている。ミキシング、DeFi（分散型金融）契約、クロスチェーンブリッジなどの匿名性向上技術を用いて、資金の出所と送金先を隠蔽している。また、制裁対象者が暗号資産サービスプロバイダー（VASPs）等を標的としてサイバー攻撃などを行い、資金を調達していることも確認されている。

この点、2025年3月にインドで開催されたPrivate Sector Collaborative Forumで設けられた拡散金融に係るパネルセッションにおいて（日本から財務省梶川審議官が登壇)、民間セクターからの参加者の多くが、新興金融技術、特に複雑かつ最新の手法を用いる北朝鮮を含む国家主体による暗号資産の窃取に関連するリスクの高まりを強調していた点も特記しておきたい。

【韓国の事例（「報告書」41頁、Box 22)】

2024年、韓国は北朝鮮に代わって資金を調達し、サイバー攻撃を仕掛け、暗号資産を窃取したとして、1つの団体と15人の個人を制裁対象とした。これら

の個人には、北朝鮮の兵器やその他の軍事装備の研究開発を管理する組織である「313総局」の幹部が含まれていた。北朝鮮は海外の仲介者の支援を受け、仮想ウォレット、銀行、電子金融プラットフォームなどを利用して資金を換金・移動し、制裁対象の物資の購入や北朝鮮のWMD計画への資金提供に使用していた。

より広い視点で見ると、デジタル経済と新興技術は制裁分野に新たな課題をもたらしている。例えば、日・米・韓は、北朝鮮がITセクターを悪用し、IT労働者が偽の身元を使って検知を免れ資金を調達していることを報告している*20。

【日本の事例（「報告書」45頁、Box 27）】

2024年3月、韓国籍のIT 関連会社社長と元従業員を詐欺罪等で通常逮捕した。同事件の被疑者らは、捜査の中でオンラインプラットフォームを通じて、日本企業から受注したアプリ開発等を中国に所在するとみられる北朝鮮IT 労働者に依頼していたことが判明した。当該行為は、北朝鮮のWMD計画に資金が流用される可能性があり、また国連安保理決議1718号に違反する制裁回避策に関与した疑いがある。

【米国の事例（「報告書」46頁、Box 28）】

2024年8月、米国司法省は、北朝鮮のWMDを含む違法兵器計画のためのマネロン共謀及びその他の複数の犯罪で米国人を起訴した。被告人は、海外のIT労働者が米国企業でリモートIT業務獲得を支援する計画に関与した。北朝鮮籍のIT労働者は盗取した米国人の個人情報を使用しリモートIT業務を獲得した。北朝鮮のIT労働者は中国国内の拠点から業務を行い、25万ドル以上の報酬を受け取ったが、米国外の口座には北朝鮮及び中国の関係者に関連する口座が含まれていた。

エ．類型4：海運セクターの悪用

FATF基準は海運セクターを明示的に対象としていないが、多くの国が当該分野を主要な脆弱性及び制裁回避のカテゴリーと認識している。これは、海運業界が船舶、港湾、物流などからなる幅広いネットワークを構築しているところ、拡散金融を通じ収益を得るためにこれらが悪用されているためである。その手法には、船舶の身元の隠蔽、船舶自動識別システム（AIS：Automatic Identification System）の操作、税関当局が審査する文書の偽造、そして船舶間の積み替え（STS：Ship-to-ship transfers）による貨物の出所や目的地の偽装などが含まれる。

【シンガポールの事例（「報告書」49頁、Box 30）】

被疑者が国外の5名と共謀し、取引書類を偽造の上、北朝鮮を最終港とする瀬取りによる貨物輸送を通じて、北朝鮮に1万2,000トン以上の軽油を供給した。

（4）グッドプラクティスと課題（「報告書」54頁、パラ96以降）

ア．民間セクターのグッドプラクティスと課題

拡散金融及び制裁回避スキームを検知するため、各国は「疑わしい取引の報告（SAR/STR：Suspicious Activity/Transaction Report）」と制裁スクリーニングとの突合に大きく依存している。国境を越えた情報の共有、機関間の連携、国際協力、オープンソース情報やブロックチェーン分析を含む監視ツールといった他の検知方法と合わせて活用する場合が多い。

他方で、約3分の1の国が、拡散金融事例の検出方法として「疑わしい取引の報告」を利用していないとした点にも留意が必要である。これは、それらの国において拡散金融自体が犯罪化されていないため、報告対象主体に対し「疑わしい取引の報告」で拡散金融事例の特定を義務付ける可能性が低いためと考えられる。この点、当局が「疑わしい取引の報告」の適用対象事例が拡散金融に関する違法行為にも繋がりうることにつき、更なる指針を提供する余地があることを示唆している。

また、「報告書」は、特定非金融業者及び職業専門家（DNFBPs）の拡散金融に関する理解と関連義務の遵守率の低さという問題点も指摘している。多くのDNFBPsは、拡散金融関連活動の監視と報告に係る自らの責任を認識しておらず、これにより当局は金融機関以外のセクターにおける拡散金融を検知することが

*20）2024年3月26日、財務省、外務省、警察庁、経済産業省は、「北朝鮮IT労働者に関する企業等に対する注意喚起」を公表した。https://www.mof.go.jp/policy/international_policy/gaitame_kawase/press_release/20240326.html

困難となりうる。

イ．公的セクターのグッドプラクティスと課題

「報告書」では、多くの国が拡散金融及び制裁回避スキームの特定における当局間連携の重要性を強調している。具体的には、法執行機関による捜査及び他の権限ある当局との情報交換は、事案紹介、共同捜査、意識向上に繋がり、制裁指定された個人・団体の資金や資産の流れの解明に資すると指摘している*21。そして、拡散金融及び制裁回避スキームに係る傾向、類型、指標を含むガイダンス資料の公表が、疑わしい取引の検知に不可欠であるとも指摘している。また、拡散金融と制裁回避スキームがクロスボーダーで行われる性質を踏まえ、情報収集と情報共有を通じた国際協力も検知と防止における重要な手段である。

当時に、各国は、制裁プログラムの管轄権や関連する制裁対象団体リストの相違、各国の法的要件、様々な執行規則など、事案の把握・解明における課題も認識している。また、前述のとおり、北朝鮮が外交官を利用して、金融サービスの提供や制裁対象資産の移転（現金の大量輸送を含む）を容易にしていることも課題としている。多くの国は、実質的支配者情報の収集や入手可能性の一貫性の欠如を懸念しており、これが拡散金融及び制裁回避スキームの実態把握を更に複雑なものとしていると認識している。

4．官民連携の重要性

マネロン・テロ資金対策同様、拡散金融対策においても、当局が自国のリスクを適切に把握し、その情報を適時に民間セクターに提供し、それぞれの事業者が自己の取引に鑑み改めてそのリスクを認識し必要に応じて低減策を講じていく必要がある。大量破壊兵器の拡散に繋がりうる取引の最前線に位置する民間セクターの事業者とは引き続き緊密な連携が必要である。この観点から、「報告書」では、官民両セクターの関係者が、拡散金融及び制裁回避スキームに関連する疑わしい取引を少しでも検知できるよう、巻末にAnnexとして疑わしい取引の端緒をリスト化し「Risk Indicators」として掲載している。

日本においても、関係者の理解の一助とすべく、現在最終報告書の日本語への翻訳作業を行っている。完成次第、その翻訳版を元に積極的にアウトリーチを行っていく予定である。第5次対日相互審査の本番といえるオンサイト審査は2028年7月頃。実際に残されている時間は想像以上に短いが、辿るべき道のりは未だ長い。

5．エピローグ

2025年4月8日、東京 8時15分（パリ 1時15分、ワシントンDC 4月7日19時15分）

「2月のFATF全体会合で、X国の首席代表が『FATFのマンデートである、勧告7が対象としている国連安保理決議に基づく制裁及びその回避行為と、そのマンデート外である、各国による独自制裁とその回避行為を、明示的に書き分けるべきだ。』と指摘したよね。いずれのカテゴリーも、このプロジェクトの射程に含めて良いと明確に承認されている。とはいえ、X国の提案のように明示的に書き分ける方法については、我々の間でも2月の全体会合前に既に議論していたし、各国から最終報告書への合意を取り付けるためには、その提案に沿って修正した方がいいかもしれないね。」と私。

「そうだね。X国の首席代表は、報告書の冒頭に置くExecutive Summaryからその点を明記すべき旨要請していたから、早速修正案を作ってみたよ。また、ケーススタディもcolour coding（色分け）してみた。この後すぐにMasaに送るから、東京の業務時間中に目を通しコメントを付して、（ワシントンDCの）明朝までに僕に返送してくれるかな。そうすれば、パリ時間の夕方までに、僕が事務局と一当たりしておくよ。それを基に、明日事務局も交えた3者でビデオチャットして方向性を最終確認し、チームメンバーに修正ドラフトを送付しよう。」と相棒。

米国のCo-leadは、2020年から3年間、私がFATF事務局で中東・アフリカ諸国のマネロン・テロ資金・拡散金融対策の改善を支援する会合の責任者であった際、米国代表メンバーとして共に活動していた。私が

*21）「報告書」69頁。日本も財務省・金融庁による合同金融・外為検査や、防衛省による各省間との即時情報共有等をグッドプラクティスとして提供している。

審査対象国と質疑応答中でメモを取れないときには、「MasaとXXのやり取りをご参考まで。」と、そっとサポートしてくれた。

昨年7月、その年の春に日本が初めて公表した「拡散金融リスク評価書[22]*」の知見を「プロジェクト」に活かすべきと考え、私はメンバーに応募した。既にCo-leadの一翼に名乗りを上げていた彼が候補者リストに私を見つけ、共に旧知のFATF事務局員を通じて声を掛けた。「日本にとって、拡散金融は地政学的観点から戦略的に重要な問題であるはず。Matthewと一緒にCo-leadをやらないか。」と。*

プロジェクト期間中、我々はお互い、日本時間の朝、米国時間の夜にコミュニケーションを取ることが多かった。彼は、職場から自宅に戻り、かわいい盛りのお嬢さんを横目に少しリラックスした雰囲気で。私は、まだ人影まばらな朝の静かなオフィスで。1年間で、プロジェクトチーム会合や事務局との打ち合わせなど、公式・非公式を含めたビデオ会合は40回以上、Co-lead間のメールのやり取りは500通以上に及んだ。

この場を借りて改めて、本プロジェクトのCo-leadを担うことに寛大なご理解と後押しをいただいた財務省国際局関係者の皆様、常に建設的議論に貢献してくれた24か国・3機関から集った30人のプロジェクトチームメンバー、そして卓越したリーダーシップでプロジェクトを主導してくれたCo-leadであるMatthew Spivack氏（米財務省Senior Policy Advisor）に心から敬意を表すとともに、謝意を伝えたい。

【写真4】左からRTMG印共同議長、筆者、米Co-lead（Matthew Spivack氏）、蘭共同議長

松尾　綱紀　国際局 資金移転対策室 総括補佐

2010年以降、通算7年以上に亘りFATF関連業務を担当。その間、2011-2015年にOECD金融企業局、2020-2023年にFATF事務局へ出向。本年7月より現職。Queen Mary, University of London 法学修士（国際金融・銀行法）

＊22） https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20241219114338.html