FATF

FATF報告書

複雑化する拡散金融と制裁回避スキーム

2025年6月

金融活動作業部会（FATF）は、マネロンやテロ資金供与、大量破壊兵器の拡散への資金供与からグローバル金融システムを保護する政策を策定し、推進する独立の政府間組織である。FATFの勧告はマネロン対策（AML）とテロ資金供与対策（CFT）のグローバル基準とみなされる。

FATFについての詳細は、ウェブサイトを参照：**www.fatf-gafi.org**

本書及び/又は本書に含まれる地図は、特定の地域の地位又は主権、国境や境界の画定、並びに地域、都市、領域の名称を害するものではない。

引用：【訳者注：以下のリンクにより、報告書原文（英語）を取得可能】

FATF (2025)、複雑な拡散金融及び制裁回避スキーム、FATF、パリ
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/complex-proliferation-financing-sanctions- evasion-schemes.html

写真提供-表紙：Sergey Nivens/Shutterstock.com

略語・頭字語

AML/CFT Anti-Money Laundering/Countering the Financing of Terrorism（マネー・ローンダリング及びテロ資金供与対策）

AECs Anonymity Enhancing Cryptocurrencies（秘匿性の高い暗号資産）

AIS Automated Identification System（船舶自動識別システム）

APT38 Advanced Persistent Threat 38

UBOI Ultimate Beneficial Ownership Information（実質的支配者情報）

CBDC Central Bank Digital Currency（中央銀行デジタル通貨）

CDD Customer Due Diligence（顧客管理）

CPF Counter Proliferation Financing（拡散金融対策）

CVC Convertible Virtual Currency（兌換性仮想通貨）

DeFi Decentralised Finance（分散型金融）

DNFBP Designated Non-financial Business and Profession（特定非金融業者及び職業専門家）

DPRK Democratic People's Republic of Korea（朝鮮民主主義人民共和国）

EDD Enhanced Due Diligence（厳格な顧客管理）

FIs Financial Institutions（金融機関）

FTB Foreign Trade Bank（フォーリン・トレード・バンク）

FTZs Free Trade Zones（自由貿易地域）

GECC Global Export Control Coalition（グローバル輸出管理連合）

IMO International Maritime Organisation（国際海事機関）

INR Interpretive Note to Recommendation（勧告の解釈ノート）

IRGC Islamic Revolutionary Guard Corps（イスラム革命防衛隊）

ML/TF Money Laundering/Terrorist Financing（マネー・ローンダリング及びテロ資金供与）

MVTS Money or Value Transfer Service（資金移動業者）

NRA National Risk Assessment（国のリスク評価）

OTC Over-the-counter（店頭）

PF Proliferation Financing（拡散金融）

PoE Panel of Experts（専門家パネル）

P2P Peer to Peer（ピアツーピア）

PPPs Public-private partnerships（官民連携）

RGB Reconnaissance General Bureau（朝鮮人民軍総参謀部偵察局）

SARs/STRs Suspicious Activity/Transaction Report（疑わしい取引の報告）

SRB Self-Regulatory Body（自主規制機関）

TCSP Trust and Company Service Provider（トラスト・アンド・カンパニー・サービスプロバイダー）

TFS Targeted Financial Sanctions（標的型金融制裁）

UN United Nations（国際連合）

UNSC United Nations Security Council（国際連合安全保障理事会）

国連安保理決議 United Nations Security Council Resolution（国際連合安全保障理事会決議）

VASP Virtual Asset Service Provider（暗号資産サービスプロバイダー）

WMD Weapons of Mass Destruction（大量破壊兵器）

1. エグゼクティブサマリー

大量破壊兵器（WMD）の拡散とそれに関わる資金供与は世界の安全保障及び国際金融システムの完全性にとって重大な脅威である。テクニカルコンプライアンスと実効性に官民セクターの支えがなければ、高度化した国家・非国家主体が拡散金融対策（CPF）管理の脆弱性に乗じ続けることになる。WMDの壊滅的影響を鑑みると、この不正行為への資金供与を防ぎ、撲滅することは極めて重要である。

複雑な拡散金融（PF）及び制裁回避スキームは国際金融システムにとって大きな脅威である。FATFマンデートに則した本報告書は、これに関わる手法や動向を取り上げ、国、地域、又はグローバルでの脅威・リスク評価を支援する。本調査報告書では、FATF基準が要求する勧告7に詳述された拡散金融に関する特定対象金融制裁（TFS）の回避者が用いる手口のほか、FATF基準の勧告7の対象範囲に含まれないその他の制裁レジーム（国家的又は超国家的制裁など）の回避に用いられる手口を詳しく説明する。

こうした包括的アプローチは、関係する類型同士に共通する課題を含め、脅威と脆弱性に関する最新知識を提供することが狙いである。本書では各国でのPFリスク評価やリスク低減プロセスの参考情報として、注目すべき執行上の課題や模範事例を積極的に取り上げた。制裁回避を幅広い構図で捉えることは、勧告7の要求事項の再定義を意図したものではなく、国家的又は超国家的制裁レジームに対する支持を強いたり、促したりするものでもない[1]。

FATFは、PF及び制裁回避に関連した変化する**脅威や脆弱性**は官民セクターにとって極めて大きな課題であるとみている。現在のリスク環境の特徴として、国家又は非国家主体が調達ネットワークを通じてデュアルユース品（軍民両用品）、技術、知識を入手、調達している実態が挙げられる。現在の世界のPF脅威に基づき、FATFグローバルネットワークは朝鮮民主主義人民共和国（北朝鮮）を最重大主体と認識している。北朝鮮は国連の制裁措置及びFATF基準の対象国である。

PF支援のために獲得された又は移動された資金の推定総額について広く合意された数字はないが、北朝鮮は近年、活動を多様化させながら金融システムにアクセスし、自国のWMD計画のためにより多くの資金を集めている。例えば、北朝鮮は暗号資産関連会社にサイバー攻撃を仕掛け、数十億ドルを得ている。2025年2月にByBitが15億ドル相当の暗号資産を盗難された事件もその一例だ。北朝鮮はこのほか、IT労働者、IT以外の幅広いセクター、及び不正行為によって得た収入をWMD計画に注いでいる。

多くの国々が同様に、イランやロシア連邦が関与する制裁回避スキームの該当事例を指摘するが、両国とも国連の拡散関連制裁の対象でなく、FATFのPFリスクの定義の下でカバーされていない。リスク理解度のばらつきを認識した脅威主体は、国又はセクターレベルの脆弱性を巧妙に突いてPF関連制裁を回避している（セクションI参照）。

不正行為主体は高度なスキームを駆使して制裁を回避し、PFに関する輸出管理の裏をかく。FATFグローバルネットワークから報告された情報に基づき、本報告書では、制裁回避のために仲介者を確保する、実質的支配者情報（BO情報）を隠して金融システムにアクセスする、暗号資産その他の技術を利用する、海事・海運セクターを悪用するという、**4つの主な類型**にスポットライトを当てる（セクションIIを参照）。複雑なPF及び制裁回避スキームに対処するため、本報告書では、PFと制裁回避の検知、捜査・訴追、国内連携・協力、国際協力に関する**課題とグッドプラクティス**を取り上げる（セクションIIIを参照）。

[1] 制裁回避を幅広い構図で捉えることは、FATF基準の勧告1又はそれ以外の部分に関して新たな義務を生じさせるものではない。むしろ、FATF類型報告書は、官民セクターが個々の状況に応じてリスクを評価し、低減措置を講じるための助けになることを意図している。

本調査報告書は、監督官庁又は民間セクター向け**リスク指標**を通じてなど、複雑なPF及び制裁回避スキームに関するFATFグローバルネットワークの知識の強化に貢献すると同時に（別紙A「リスク指標」を参照）、FATFグローバルネットワーク全体としてPF及び制裁回避に関するリスクの理解を前進させる必要性を浮き彫りにする。脅威主体は今後も、PFや制裁回避に対する法域ごとのアプローチの違いを含むCPF管理の弱点をつぶさに調べ上げ、新しい技術や地政学的な勢力図の変化を悪用し続けるに違いない。

複雑なPF及び制裁回避スキームを防ぎ、闘うためには、FATFグローバルネットワークに次の点についての検討が求められる（勧告セクションを参照）。

1) **脅威、脆弱性、類型の知識を定期的に更新する。**現状では、官民セクターの該当リスクに関する知識度が個々に異なっている。
2) **より内容の濃い情報共有を促し、官民セクターにおけるPF・制裁回避の検知能力を高める。**然るべき捜査を開始するには疑わしい取引報告が拠り所となる。
3) 5年以内に、FATF一般用語集に**大量破壊兵器拡散金融（WMD PF）の公式定義を加える。**国際協力をむしばむ法域ごとの違いを克服しなければならない。
4) 3年以内に、**FATFグローバルネットワークのPFリスク評価の水平的レビューを実施する。**各国にPFリスク評価を実施する時間的余裕を設けたうえで模範事例を洗い出す必要がある。

2. 背景

拡散金融に関するFATFの基準及び取り組み

1. 2020年10月、FATFは勧告1及び勧告2（R.1、R.2）とその解釈ノート（INR.1、INR.2）の改訂案を採択し、各国、金融機関、指定非金融業者及び職業専門家（DNFBP）、暗号資産サービスプロバイダー（VASP）に対して各自の拡散金融リスク、すなわちR.7に詳述された特定対象金融制裁（TFS）の潜在的な違反・不履行・潜脱を特定、評価し、理解すること、そして特定したリスクに見合った実効性のある低減措置を講じることを求めた。改訂版勧告は各国にPFリスクに関する国内協力・連携、情報共有の仕組みの強化も義務付けている。

2. FATFは、官民セクターステークホルダーが改訂版勧告に基づく義務を効果的に果たすための支援として、2021年に「拡散金融リスク評価及び低減ガイダンス」[2]を公表し、次の点に関する手引きを示した。

1) PFリスクを特定、評価し、理解するための官民セクターでのリスク評価の実施方法
2) 特定したPFリスクを低減するためのFATF要求事項の実施方法
3) PFリスクの正しい評価及び低減措置を徹底するための監督官庁又は自主規制機関におけるFI、DNFBP、VASPの監督・監視方法

3. 2021年ガイダンスは「2018年拡散金融対策ガイダンス」[3]を補足するものであり、官民セクター双方のステークホルダーに対して国連安保理決議に従ったR.7に基づく義務の理解と実行、制裁回避の抑制を促すことが主な狙いである。これらの前身文書は、2013年に公表された「大量破壊兵器の拡散に対抗するための国連安全保障理事会決議金融条項の実施ガイダンス」である。[4]

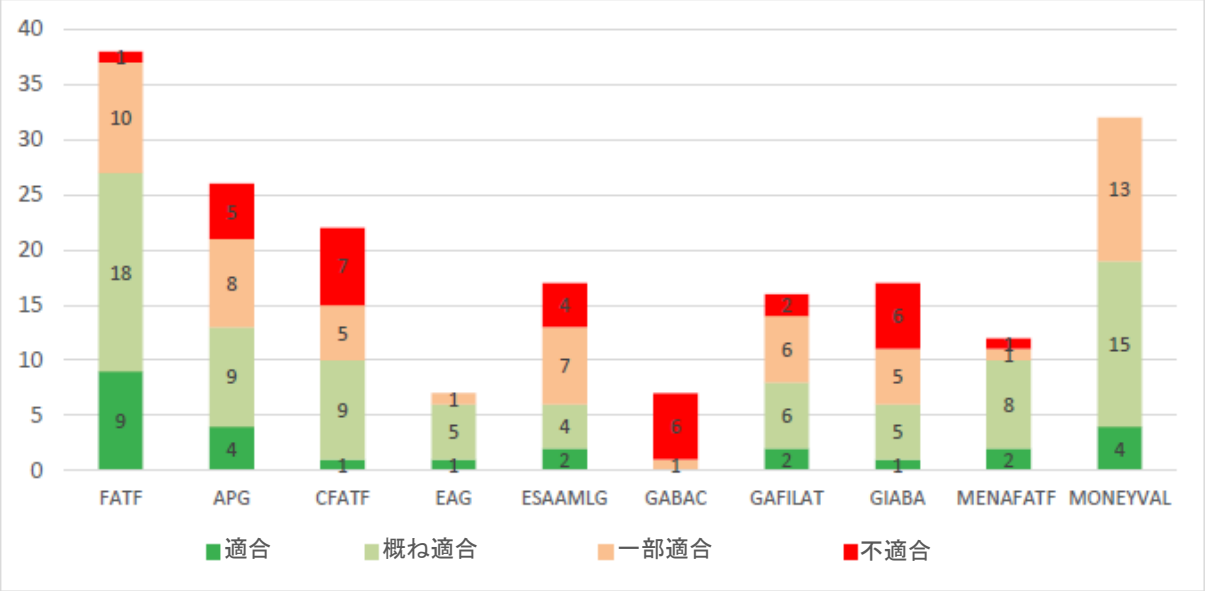
4. これらのガイダンス文書の公表に先立ち、FATFは既存のPFリスクとCPF措置を洗い出し、分析したうえで、手口の進展に関する世界の理解を深めるための「2008年PFタイポロジー（類型）報告書」[5]を公表した。「2010年拡散金融対策：政策策定・協議に関する現状報告書」[6]は2008年報告書を土台とし、国連安保理決議に従ったCPF措置の実施にあたり、特にi) 法制度、ii) 官民セクター間の情報共有と意識向上、iii) 防止措置、iv) 捜査・訴追に関して、検討すべき政策の選択肢を示した。

FATF基準の最新実施状況

5. 第4次相互審査報告書（ME）の評価結果によると、R.7と、拡散に関する国連安保理決議に従ったTFSの施行・執行に、各国が依然として苦戦している。2025年4月時点で[7]、第4次相互審査報告書の対象となった194のFATF・FSRB加盟国のうち、R.7適合国はわずか13%（26カ国）に止まり、およそ半数（46%、89カ国）は一部適合又は不適合であった。

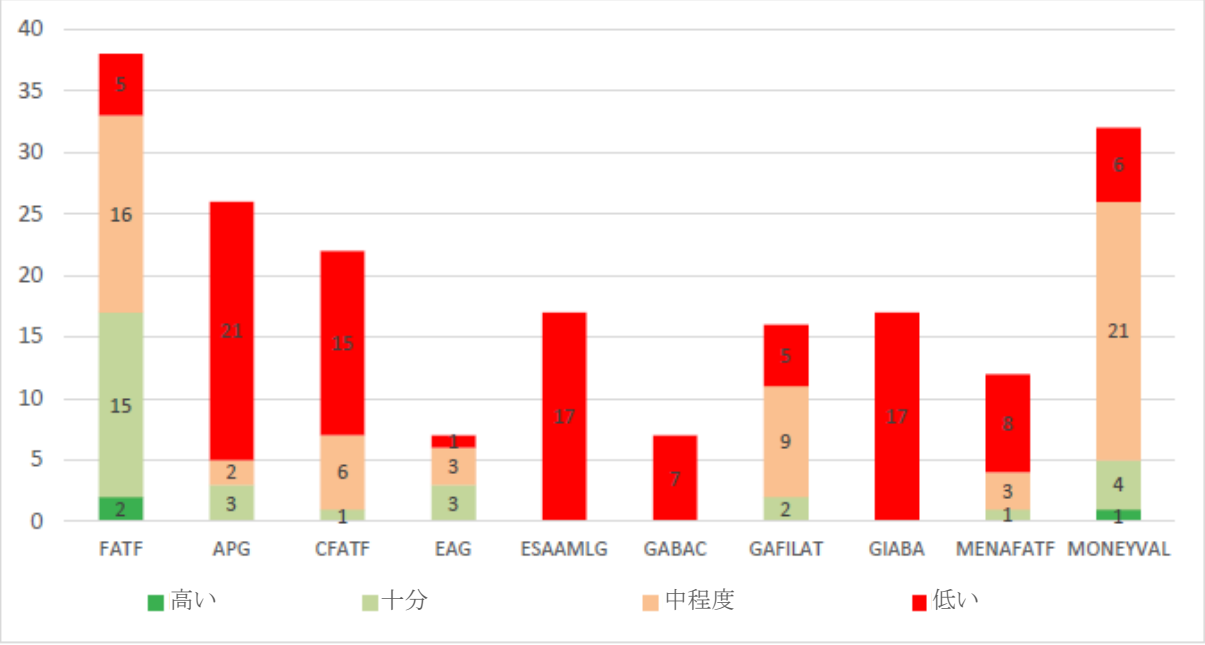
2 FATF (2021) Guidance on Proliferation Financing Risk Assessment and Mitigation.
3 FATF (2018) Guidance on Counter Proliferation Financing
4 FATF (2013) Guidance on the Implementation of Financial Provisions of UNSCRs to Counter Proliferation of Weapons of Mass Destruction
5 FATF (2008) Proliferation Financing Typologies Report
6 FATF (2010) Combatting Proliferation Financing:A Status Report on Policy Development and Consultation
7 FATF (2024) Consolidated Assessment Ratings（FATF（2024年）統合評価結果）

図1.評価結果：R.7に関する法令等の整備状況（Technical Compliance: TC）（2025年4月時点）



6. 同様に、全体的な有効性も依然として低く、審査対象国のうち法制度の有効性11項目（拡散金融に関する国連安保理決議に従ったTFS）が高い又は十分と評価された国は16%に止まった。有効性の評価結果はFATF加盟国・FSRB加盟国間で大きな開きがある（有効性が高い又は十分との評価結果を得た国は、38のFATF加盟国のうち45%、156のFSRB加盟国のうち10%）。

図2.評価結果：有効性（Immediate Outcome: IO）11項目 – 有効性（2025年4月時点）



はじめに

重点事項の概要

7. 本報告書は、これまでに発行された2つのガイダンス報告書、1)「2018 年FATF拡散金融対策ガイダンス – 大量破壊兵器拡散金融に対抗するための国際連合安全保障理事会決議第1718号金融条項の実施」、2)「2021年拡散金融リスク評価及びリスク低減ガイダンス」を土台とし、これらを発展させることが狙いである。本調査報告書は、PFに関わる複雑な制裁回避スキームで現在用いられている手口についての総合知識を読者に提供すると共に、各国でのPFリスク評価とリスク低減に役立つ情報として執行上の課題とベストプラクティスを示す。本報告書では以下の主な用語を使用する。

ボックス1. 主な用語の定義

本報告書では、2010年現状報告書を基に作成された2021年PFガイダンスで使用されている広い現状定義を用いる。

大量破壊兵器(WMD)拡散

核兵器、化学兵器又は生物兵器とその運搬手段及び関連材料(不法な目的に使用されるデュアルユース技術及びデュアルユース品を含む)の製造、取得、所有、開発、輸出、積み替え、仲介、輸送、移転、貯蔵又は使用。

拡散金融(PF)

一部又は全部にかかわらず、大量破壊兵器の拡散を目的に個人又は団体に対して資金、その他の資産又はその他の経済資源を調達、移動、もしくは利用可能にする行為又は資金を供与する行為。大量破壊兵器の運搬手段及び関連物資(不法な目的に使用されるデュアルユース技術及びデュアルユース品を含む)の拡散を含む[8]。

本報告書では、WMD拡散又はPFに関して該当する国際レジームやフォーラムで共有された標準的、普遍的な定義がないことを重ねて強調すると共に、その潜在的影響と該当セクションにおける標準定義の必要性を指摘する。

PFリスク

本報告書において、PFリスクとは、別段の記載がない限り、改訂版勧告1及びその解釈ノート(R.1、INR.1)に従い、厳密かつ限定的に、勧告7に言及されたTFS義務の潜在的な違反・不履行・潜脱を指す。

8. 本報告書は、さまざまな国内・国際機関の幅広い一連の取り組みを土台とし、FATFグローバルネットワークメンバー、監督官庁、FI、DNFBP、VASP、NGO、その他PFに関する制裁回避に取り組む個人もしくは団体の使用を意図して作成されている。

[8] PFに関するこの現状定義は、FATFの2010年現状報告書の定義を基にしている。同報告書は、本報告書はもとより、PF及び制裁回避に関するリスク低減のために幅広い視点から取り組む国にとっては特に、現在でも有意義である。2010年報告書ではPFを、「核兵器、化学兵器及び生物兵器、並びに運搬手段及び関連物資(不法な目的に使用されるデュアルユース技術及びデュアルユース品を含む)を製造、取得、所持、開発、輸出、積替え、仲介、輸送、移転、貯蔵又は使用するために、その全部又は一部について、資金又は金融サービスを提供する行為であり、国内法に違反、又は国際的義務が適用できる部分で違反しているもの」と定義付けている。

目的及び構成

9. 本報告書は、各国でのPFリスク低減活動を支援するため、PFに関する制裁回避の傾向及び手口をグローバルの視点から捉えることを意図している。また、複雑な制裁回避スキーム、脅威、脆弱性の指標を示すと共に、PFに関する制裁回避の検知、捜査、訴追における模範事例と課題を取り上げる。これらの目的を果たすために、本書は4部構成とした。

- **セクション1：**実施計画に従ったプロジェクト範囲の設定。これと併せて、現状を概説し、ケーススタディと文献分析に基づき、制裁回避とPFに関わる脅威と脆弱性を特定する。
- **セクション2：**PFに関する複雑な制裁回避スキームの類型説明。
- **セクション3：**PFの検知、通報、捜査、訴追に関する課題と模範事例の特定。これと併せて、関係するさまざまな国内連携・協力、国際協力の仕組みを概説する。
- **結論・優先領域：**PFと制裁回避に関する全体状況のまとめと、更なる取り組みを必要とする領域の特定。
- **リスク指標：**この別紙は、該当するPF・制裁回避スキームに関わる疑わしい取引や活動を突き止めるにあたり、官民セクター事業体の能力強化のために作成されている。

手法

10. 手法はPF及びPFリスクに関して現在入手できる資料のレビューと精緻化から成り、次の作業を含む。

- PF関連制裁回避の性質と範囲に関する傾向変化を明らかにするための文献レビュー。国連安保理決議第1718号専門家パネル（PoE）報告書を含む。このレビューでは脅威、脆弱性のほか、新たな傾向と手口に注目した。
- FATFグローバルネットワークメンバーへのPF関連制裁回避に関する情報提供の要請。これには、a) PF関連制裁回避の類型や事例の情報源となる戦略的インテリジェンス品又はケーススタディに関する資料、b) リスク評価において特定された脅威及び脆弱性と低減措置、c) 検知、捜査、情報共有の仕組み、d) 模範事例と課題が含まれる。
- FATFグローバルネットワークメンバーから報告されたリスク指標に加え、次の補足報告書も検証した：i) その他の組織及び機関によるPFリスク評価ガイダンス、ii) PF類型研究、iii) 各国が発行したTFSガイダンス。
- 民間セクター、市民社会、学術機関に対しても、パブリックコメントの中で、特に国内連携・協力における課題と模範事例に関して、いくつかの質問に対する回答を呼びかけ、本報告書の材料とした。

3. セクション1.PF関連制裁回避 – 現状、脅威、脆弱性

範囲

本報告書の組み立て

11. リスク評価プロセスの一環として、各国はマネー・ローンダリング（ML）とテロ資金供与（TF）、そして該当の脅威が脆弱性を巧妙に突いて結果を生み出したときに生じるPFリスクを考慮する。[9]FATFグローバルネットワークによると、国際金融システムにとっての最も重大なPF脅威は、国家が資金提供する又はその傘下にある主体がもたらしている。これには、単独の国連制裁対象国である北朝鮮に関わる制裁回避やPF活動に関係する者などが含まれる。

12. 改訂版FATF勧告1の枠組みにおいて、PFリスクとは、厳密かつ限定的に、国連の制裁対象国である北朝鮮のみにフォーカスした勧告7に示されるTFS義務の潜在的な違反・不履行・潜脱を指す。FATF基準で取り上げられたこの狭義のPFリスクに基づき、各法域が特定した主な脅威主体には、北朝鮮と、国連制裁の回避のために北朝鮮を支援する又は北朝鮮に協力する国家主体、個人、団体が含まれる。

13. FATFの2021年PFガイダンスに記されているとおり[10]、WMD拡散とその背後にある資金供与の幅広いリスクの理解は、FATFのPF-TFS義務に関わるリスクの理解に寄与するかもしれない。PFリスクの理解を深めることは、リスクベースの措置やTFSの実行にも有益である。多くのFATF加盟国は、広義のPFに基づき、現在のFATF基準よりも幅広いリスク低減を図る。その結果、各法域から報告された範囲は、北朝鮮（国連制裁及びFATF基準の対象国）とその他の国家主体を含む、現在の世界的PF脅威の理解が反映されている。多くの国は、現在のPF脅威としてイランとロシア連邦を挙げたが、いずれも国連の拡散関連制裁対象国でもFATFが定めたPFリスクの定義に該当する国でもない。

14. 本報告書の範囲は、拡散資金供与者が使う複雑な制裁回避スキームに関する現在の捉え方を示すものであり、結果として導き出される類型の長期的な持続可能性と妥当性を確保し、共通課題に対処するため、該当する場合、制裁レジームにかかわらず、TF及びPFに関する制裁回避スキームをより幅広く検討する。したがって、本報告書ではFATFグローバルネットワークのPFリスクの特定・低減活動を支援する努力の一環として、各法域に最も言及されたすべての主体を取り上げる[11]。

FATFグローバルネットワークのPFリスク評価体験

15. 該当する脆弱性を評価する効果的な手段の一つがPFリスク評価である。FATFグローバルネットワークの多くの国が国内リスク評価の一環としてPFリスク評価を実施済み又は実施中と回答しているが、評価の範囲又はPFに関する脆弱性の理解あるいはその両方がまだ初期段階にあることが伺える。例えば、本報告書のアンケート回答国のうちおよそ半数がPFに関する脆弱性の有無を確認していないと答え、PFに関する脆弱性がないと結論付けた国は6カ国であった。

---

9 FATF (2024) Money Laundering National Risk Assessment Guidance（FATF（2024年）マネー・ローンダリング国のリスク評価ガイダンス）

10 FATF (2021) Guidance on Proliferation Financing Risk Assessment and Mitigation（FATF（2021年）拡散金融リスク評価及び低減ガイダンス）

11 本書のエグゼクティブサマリーその他で述べているとおり、本報告書には、脅威と脆弱性に関する最新知識を提供するため国家的又は超国家的制裁レジームの回避に用いられる手口に関する情報を含み、これにはFATF基準の勧告7でカバーされていない関連類型同士の共通課題も含まれている。制裁回避をより幅広く捉えることは、勧告7の要求事項を再定義することを意図してはいない。

16. 中には、制裁対象国との地理的距離がある、制裁対象国と外交又は通商関係がない、金融セクターが十分発展しておらずグローバル金融市場との一体性が限られている、PFに関するTFSの導入について強固な国の仕組みが整備されている、その法域においてPF事案が特定されていないなどのいくつかの理由によって、PF及び制裁回避に関する脆弱性が低いことが示唆される国もあった。

17. こうした理由の多くは、PF脅威主体が国又はセクターの脆弱性を突く可能性を低下させるもっともな要因ではあるが、それでもなお、新しい決済システムを含めた新技術の登場や地政学的緊張関係の高まりなど、近年の世界情勢の大きな変化を検討することが重要である。また、前述の要素は官民セクターが講じるAML/CFT/CPF対策に含まれるより幅広い弱点や、制裁又は輸出管理を迂回するために第三国のさまざまな仲介者を利用するPF・制裁回避脅威主体が蔓延している点を考慮していない（類型1参照）。PF脅威主体は国際金融システムの潜在的盲点を悪用しながら勢力を拡大させていることから、PFに関する脆弱性を見つけ、低減策を講じると共に、こうした脆弱性を防ぐ協調的な努力を強化するためには、更なる支援と活動が必要かもしれない。

現状

18. WMD計画に狙いを定めた国際的、超国家的、国家的な制裁レジームと輸出管理が幅広く実施されているにもかかわらず、国家が資金提供する又はその傘下にある主体は、複雑な調達・資金獲得スキームを巧みに実行し、PF主体やPF活動を支援している。特に、主立った脅威主体は第三国に仲介者を確保し、BO情報を隠し、新しい技術を利用し、海事・海運セクターを悪用することによって、制裁を回避し、資金を集め、デュアルユース品を獲得している（セクション2参照）。

19. FATFは現在の脅威と脆弱性を次のとおり評価している。

現状 – 北朝鮮

20. 北朝鮮は、2006年に同国初の核実験を実施して以降、国際社会から厳しい制裁措置が課されている。2006年に採択された国連安保理決議第1718号では北朝鮮に核実験の中止を要求すると共に、さまざまな対応策の中でもとりわけTFSについては、北朝鮮に対して幅広く、かつ同国のWMD計画に関わる個人及び団体も具体的に対象指定された。

21. およそ20年にも及ぶ国連制裁にもかかわらず、北朝鮮は大陸間弾道ミサイル（ICBM）実験を通じて核爆発装置の開発能力を増強し続けている。北朝鮮は2024年10月31日にもICBMを発射し、「火星19型」と名付けられたこのICBMは、最高高度およそ7,000kmまで上昇し、およそ1,000kmを飛行した。北朝鮮が2021年に新たな5カ年軍事拡大計画を発表して以降、この最新実験でICBMの発射は11回目となる[12]。

22. 北朝鮮がこうした活動を繰り返す一方で、国際社会の活動は、北朝鮮が与える脅威のペースや軌道と一致していない。対北朝鮮国連制裁リストへの追加は、ほぼ10年間行われていない。しかも、国連安保理決議第1718号専門家パネル（PoE）は2024年に解散している。国連安保理決議第1718号専門家パネルの解散は、対北朝鮮制裁違反の監視において大きな課題をもたらしている[13]。多くの国々が、国連安保理決議第1718号専門家パネルが年2回発行する報告書を、国のPFリスク評価の重要な情報源としていた。2024

12 DPRK Korea's latest missile launch a 'grave threat' to regional stability | UN News（北朝鮮が再びミサイル発射、地域の安定性にとって深刻な脅威に | 国連ニュース）

13 Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on Democratic People's Republic of Korea | Meetings Coverage and Press Releases（安保理、対北朝鮮制裁委員会を支える有識者会議のマンデート延長ならず | ミーティング採録・プレスリリース）

年6月のFATF全体会議では、「北朝鮮に関するPFリスク評価を支える信頼できる確かな情報を得る力が第1718号有識者会議のマンデートの打ち切りによって阻まれている」と指摘されている。[14]

23. 本調査を実施するにあたり、FATF代表団は北朝鮮によるWMD計画のための資金獲得を悪化させる要因として、北朝鮮の金融面における連携強化と、北朝鮮の資金獲得手段の多様化という2点を挙げた。

北朝鮮の金融コネクティビティの強まり

24. FATFは2011年以降繰り返し、すべての国が国連安保理決議と一致したTFSを強固に実行し、各国の金融システムを北朝鮮に端を発する不正な資金の流れから守るための対策を導入する必要性を述べてきたが、北朝鮮は近年、国際金融システムとのつながりを強め、FATFが2024年6月に指摘しているとおり、PFリスクが高まっている[15]。

25. 2024年末に発効した露朝包括的戦略的パートナーシップ条約[16]において、両国は税関、金融、銀行業における経済協力に有利な条件を設け、両国の直接的な結び付きを築くために協力し有利な条件を設け、両地域の経済及び投資の可能性について相互理解を深めるなど、協力関係の強化を約束した。複数の北朝鮮系金融機関とその国外代理人が国連安保理決議第1718号の下で対象指定されていることから、経済的結び付きの強化、特にPFと紐付いている北朝鮮系金融機関との銀行取引関係の再構築は、国際金融システムに新たな脆弱性をもたらすおそれがある。[17]

26. 2016年以降、北朝鮮系銀行の受け入れ国は、受け入れ国に対する制裁執行と北朝鮮職員の撤退などを理由に14カ国から4カ国に減り、直近では2023年後半にインドネシアとリビアが手を引いた。しかしながら、2023年から少なくとも2024年半ばまでの間に、隣国とロシアに所在する北朝鮮系銀行が北朝鮮の貿易と資金確保を支える数億ドル相当の取引を手助けした。国連安保理決議第2321号が受け入れ国にその排除を義務付けているにもかかわらず、2024年半ば時点で50人を超える北朝鮮系銀行代理人が国外で活動している[18]。また、国連安保理決議第2270号は受け入れ国に対して既存の代理人事務所の閉鎖を要求し、北朝鮮に国連加盟国領域内での支店、子会社、代理人事務所の新規開設又は営業を禁じている。[19]ある代表団が2024年1月に指摘したところによると、ロ

---

14 High-Risk Countries subject to a Call for Action - June 2024（行動要請対象の高リスク国・地域 – 2024年6月）

15 High-Risk Countries subject to a Call for Action - June 2024（行動要請対象の高リスク国・地域 – 2024年6月）

16 http://en.kremlin.ru/acts/news/75534

17 対北朝鮮制裁に関して国連が指定した金融機関には、タンチョン・コマーシャル・バンク（KPe.003）、バンク・オブ・イースト・ランド（KPe.013）、アムロッガン・デベロップメント・バンキング・コーポレーション（KPe.009）などが含まれる。

18 国連安保理決議第2321号は受け入れ国に対して、北朝鮮系銀行代理人の追放と、北朝鮮との取引に関してその領域内で、もしくはその法域の対象個人又は団体による、官民の金融支援の禁止を求めている。

19 高リスク法域に関するFATFの2024年6月の声明では「FATFは2011年以降、すべての国に対して国連安保理決議に従った特定対象金融制裁の厳格な実行と、北朝鮮に端を発するマネー・ローンダリング、テロ資金供与、拡散金融脅威から金融システムを守るための対策北朝鮮銀行とのコルレス契約の終了、北朝鮮銀行の国内子会社又は支店の閉鎖、；北朝鮮の個人との取引関係及び金融取引の制限）の適用を重ねて強調してきた。こうした呼びかけにもかかわらず、北朝鮮は国際金融システムとのつながりを強め、その結果、2024年2月にFATFが指摘したとおり、拡散金融（PF）リスクが増大している。よって、北朝鮮に対してこれまで以上に警戒を強め、こうした対策を改めて実施、執行する必要がある。国連安保理決議第2270号に示されたとおり、北朝鮮は制裁破りを目的に、フロント企業、シェルカンパニー、合弁会社、複雑で曖昧な所有者構造などを頻繁に使用している。したがってFATFは、加盟国及びすべての国々に、北朝鮮及び北朝鮮に代わって取引を手助けする機能に対して厳格な顧客管理（EDD）を適用することを奨励する。」と述べられている。

シアに拠点を置く銀行が、北朝鮮が外貨を獲得し、国連制裁回避を続けるために、北朝鮮建設労働者をロシアに送る取引を手助けした。

北朝鮮のWMD計画に恩恵をもたらす幅広い資金獲得活動

27. 多くの国が、PF及び制裁回避スキームに最もよく関わる犯罪行為として偽造、不正行為、(サイバー)窃取、武器・麻薬・野生動植物・密輸品その他の品目の闇取引を挙げている。北朝鮮と紐付く個人及び団体がこうした不正行為を実行し、正規取引を悪用してWMD計画の資金を得ているが、特に、新規技術、海事、海運セクターなどのAML/CFT/CPF対策が脆弱又はない国やセクターが狙われる(類型3、4を参照)。近年盛んに行っているIT労働者を使った資金獲得に加え、北朝鮮は次のような幅広いセクター又は不正行為を資金獲得の標的にしていることも知られている。

- **かつら・つけまつげセクター:** 一部の国は、収益性の高いかつら・つけまつげ製品の輸出を利用してより多くの資金を獲得し、自国の戦略的兵器計画を妨げる国際社会からの制裁の影響を抑えようとする北朝鮮の活動を監視している。2024年上期の北朝鮮から隣国への輸出品のうち、かつら・つけまつげ製品はおよそ60%を占める。北朝鮮はこれら製品の原材料を同じ隣国から輸入し、作った半完成品を最終加工と第三国への輸出のために企業へと送り返す。かつらを製造する北朝鮮の貿易会社は国連安保理決議第1718号リスト指定団体の配下にあり、よってかつらの売上が北朝鮮の戦略的兵器計画を支えている可能性が示唆される。国連制裁は企業に対して北朝鮮を原産国とするかつら・つけまつげの購入を禁じてはいないが、最終製品の製品及び購入に関わる企業が国連制裁対象団体とのつながりに気づいていない可能性がある。
- **野生動植物の違法取引:** 北朝鮮による野生動植物の違法取引の大部分は、同国との歴史的なつながりを持つ国が多いサハラ以南のアフリカ諸国で行われている。野生動植物の違法取引は資金を得たい北朝鮮にとってローリスク・ハイリターンな手段である。近年は、サハラ以南のアフリカ諸国が北朝鮮の外交的な存在感を拒んでおり、外交関係者を介したこの経路での利益獲得は徐々に難しくなるかもしれない。また、野生動植物の調達・輸送において第三国国籍者として活動する秘密任務を負った北朝鮮国籍者が今後これまで以上に大きな役割を果たす可能性がある(例えば、野生動植物密売のトランジット国又は仕向国として知られた国の出身者であると装うなど)とRUSIが指摘しており、複数の国がこれに同意している。[20]

現状 – イラン

28. イランに対して最初に発動された国連制裁措置は国連安保理決議第1737号に基づくものであり、それにはウラン濃縮プログラムの中止を求めた国連安保理決議第1696号に同国が従わなかった背景がある。国連安保理決議は核開発計画に関してイランの個人及び団体にTFSが課された事例の第1号である。

29. 国連安保理は国連安保理決議第2231号を通じて「包括的共同作業計画」を承認し、イランは制裁の一部解除及びその他の規定を見返りに核開発計画の制限に同意した。国連安保理決議第2231号に従ってイランの核開発計画に関連する個人及び団体を対象にしたTFS措置が2023年10月に解除され、FATFの勧告7の該当から外れたが、イランと同国に関連する個人及び団体がもたらす脅威を理由に、複数の国が国の制裁制度に基

[20] UN investigating claims of rampant North Korean wildlife trafficking in Africa | NK News(北朝鮮によるアフリカでの野生動植物密売の横行を国連が調査 | NK News)

づき同国にTFSを課している。

30. イランは中東内の軍事化した代理組織と国内外に拠点を置くさまざまな国際犯罪組織（TCO）を頼りに経済制裁の影響を抑えようとしてきた。これまでも広い人脈を持つ海外のビジネスパーソンがイランの石油密売を手助けし、銀行、金取引業者、外貨両替店がマネー・ローンダリングや複雑な制裁回避の重要なパイプ役を務めてきた。さまざまなケーススタディで指摘されているとおり、イランの制裁・輸出管理回避はミサイル、兵器、航空兵器の開発とWMD計画の前進を支えている可能性がある。

31. イランの代理組織、特に外貨両替店は、かつてはISISやアルカイダの資金調達経路であったダークマーケットを利用して利益を得ている。これに関して特に重要な役割を果たしているのがヒズボラであり、ヒズボラは広範囲に密輸活動を展開し、合法・違法取引のグローバルネットワークを持ち、外貨両替店を通じた世界的なマネー・ローンダリングに支配的役割を果たしている。ヒズボラは石油、兵器その他幅広い制裁対象品の密輸にも関与している[21]。

32. ヒズボラはこのほかにも、世界中のあまたの国々の金融機関に侵入し、複数の大陸や商業セクターをまたいだローンダリングスキームを実行している。ヒズボラの工作員は、イランに代わり、制裁措置に反して兵器や機器を入手しようとするなど、ハイリスクな試みにも手を染める。こうした関係性は、イランの海外活動を支える犯罪市場がさまざまな脅威の触媒になっていることを示している。

現状 – ロシア

33. ウクライナへの軍事侵攻を理由にロシア経済に対して国際社会がさまざまな制裁措置を課した結果、ロシア連邦は自国経済と軍事的立場を維持しようと対抗策を講じている。本セクションの前段でも述べたとおり、北朝鮮との包括的戦略的パートナーシップ条約の締結もその一つだ。[22]この条約によって両国の経済的、軍事的結びつきが生まれ、戦略的、戦術的協力関係の強化、軍事支援、防衛力強化を目的とした共同措置などの条項が盛り込まれている（経済連携についてはパラグラフ26を参照）。

34. 2025年4月、北朝鮮は二国間条約に基づくロシア・ウクライナ紛争への派兵を明らかにし、ロシア高官はクルスク州での北朝鮮兵士の活動を明らかにした。[23][24]それ以前、2024年3月の国連第1718号専門家パネル報告書には、国連がウクライナでの北朝鮮製軍需品の存在を調査しているとの言及がある[25]。ロシアと、20年にわたって国連の制裁対象となっている一番のPF脅威主体の北朝鮮との経済的、軍事的なつながりの結果、その延長線で多くの国がロシアをPF脅威とみなしている。

その他の脅威

35. また、多くの国が依然として、テロ組織や犯罪組織などの非国家主体による生物兵器、化学兵器、核兵器を含めたWMDに関わる物資、知識、技術の入手や調達活動を懸念している。国連安保理は2022年11月に、WMD、知識、前駆体物質の非国家主体への拡散防止に重点を置き、国連安保理決議第1540号のマンデートを更新した[26]。FATF

---

21 本書のエグゼクティブサマリーその他で述べているとおり、本報告書には、脅威と脆弱性に関する最新知識を提供するため国家的又は超国家的制裁レジームの回避に用いられる手口に関する情報を含み、これにはFATF基準の勧告7でカバーされていない関連類型同士の共通課題も含まれている。制裁回避をより幅広く捉えることは、勧告7の要求事項を再定義することを意図してはいない。

22 http://kcna.kp/en/article/q/6a4ae9a744af8ecdfa6678c5f1eda29c.kcmsf

23 http://www.rodong.rep.kp/en/index.php?MTJAMjAyNS0wNC0yOS0wMDFAMTVAMUBAMEAxQA==

24 http://en.kremlin.ru/events/president/news/76805

25 https://docs.un.org/en/S/2024/215

26 Security Council Extends Mandate of Committee Monitoring Nuclear, Biological, Chemical Weapons

の2021年PFガイダンスに示すとおり、国連安保理決議第1540号の義務は、勧告7及びその解釈ノートで定めた義務とは別個に存在する。[27]非国家主体がPF主体又はPF活動を支援するために金融システムを悪用した事例はほとんどないが、多くの国はこうした行為の潜在的影響を鑑み、継続的監視が重要であると考えている。また、総合的なPF・制裁回避リスクの理解と低減の意味で、これらの活動の類型も存在するかもしれないため、非国家主体のケーススタディもいくつか本書に掲載している。

脆弱性

36. FATFの2021年PFガイダンスに説明するとおり、脆弱性とは、脅威又は脅威主体によって悪用され得るものや、拡散金融に係る対象を特定した金融制裁の違反、未実施、回避を支援又は促進し得るものを指す。既存のFATF基準に基づき、これは北朝鮮と同国の国連制裁回避を支援する関連主体がもたらす脅威に当てはまる。PFリスクを幅広いレンズから見ている国々にとっては、官民セクターの弱点を突こうと狙っているすべてのPF主体が悪用する脆弱性に当てはまるかもしれない。

37. 各国には国レベル（構造的なものを含む）とセクターレベルで脆弱性を検討することが求められる。国としての、又は構造的な脆弱性には、AML/CFT/CPFに関する法律又は規制枠組みの弱点が含まれることもある。国レベルの脆弱性にはこのほか、経済の規模や複雑さ、非公式/現金経済の程度、法人及び法制度の多様性など、その法域固有の要因も含まれる。[28]特にPFに関わる脆弱性に対する晒されやすさについては、多くの国が地理的位置の重要性を指摘する。この背景要因は、北朝鮮の制裁回避スキームに対する潜在的つながりにおいてとりわけ重要であると考えられる。

38. セクターレベルの脆弱性は、複雑な拡散金融・制裁回避スキームの実行を目的に個人又は団体に悪用され得るそのセクター固有の特性が影響する。例えば、仲介業者や代理店が多く存在する流通チャネルの背景的特徴が、金融の流れ又は資産の移動の追跡を阻害するかもしれない。

PF・制裁回避に関する国レベルの脆弱性

39. FATFグローバルネットワークが特定した、複雑な拡散金融・制裁回避スキームを助長する最も一般的な脆弱性の例を以下に挙げる。

経済・通商要因

40. 国際金融センターとして機能している国は、そのグローバルでの金融の流れと輸送における重要性を踏まえ、PF・制裁回避脅威主体の標的にされていると多くの国が指摘する（類型1参照）。PFの脆弱性は、幅広く多様な顧客層にサービスを提供する国際金融拠点が提供する多種多様な製品及びサービスに起因する。さらにその開放性（経済特区の存在を含む）と越境取引を円滑に行うために確立された金融システムや経済の高度化は、不正拡散ネットワークに特に悪用されやすい。輸送・物流インフラが整備された戦略的港を持つ国々も、デュアルユース品の制裁・輸出管理回避に悪用されやすい。

41. このほか、多くの国がPF・制裁回避スキームにさらされるリスクが高まることを理由

for 10 Years, Unanimously Adopting Resolution 2663 (2022) | Meetings Coverage and Press Releases（安保理、決議第2663号（2022年）を全会一致で採択し、核、生物、化学兵器の監視に関する委員会マンデートを10年延長 | ミーティング採録・プレスリリース）

27 Guidance on Proliferation Financing Risk Assessment and Mitigation（拡散金融リスク評価及び低減ガイダンス）

28 Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf.coredownload.inline.pdf

に、制裁対象国との経済、通商関係の維持に関わる脆弱性に言及している[29]。地政学的な近さ、依存度、歴史的なつながりは、これらの国々が、制裁を回避し、金融システム・資源にアクセスしようとするPF脅威主体にその国のことを知らずに狙われる機会を生み出すかもしれない。

42. 多くの国はPFに関する複雑な制裁回避スキームの防止と検知の意味で、税関の重要性に注目している。税関は国内、地域、国際的な情報収集、情報交換に重要な役割を果たしている（セクション3参照）。

規制上の要因

43. AML/CFTに関する規制整備が各国で前進する一方で、CPFに関する措置のグローバルな実行は今なお後れを取っている（図1、図2参照）。確かな法規制、運用枠組みが整備されていないことによって、一部の国は、拡散ネットワークを阻止し、対抗するために義務付けられた制裁義務や輸出管理を適用できていない。しかも、複雑なPF・制裁回避スキームは取引を不透明化するためのさまざまな手口を駆使しており、それがVASPなど規制されていないセクターや監視が十分でないセクターでの検知をさらに難しくしている。さらに、法人の実質的所有者に関する国内法や透明性が不十分な国では、PFの脆弱性がより深まる。BO情報の入手が難しくなると、一貫した法的枠組みが欠如した国が複数関わっている場合は特に、PF経路を見つけ、辿ろうとする当局の越境捜査が阻害される。

地理的、人口統計的要因

44. 一部の国は、国連、国家的、超国家的制裁レジームの対象国と自国との地理的な近さに関する脆弱性を申告している。地理的な近さは不正ネットワークが資産や資源を国境をまたいで移動させる機会を生み出す原因になり得る。戦略的に重要な位置にある国々は重要な海上交通路や交易路を提供し、そこに隣国関係に必然的に伴う脆弱性が生まれる。例えば、違法物品の密売が関わる貿易ベースの制裁回避スキームは、制裁対象地域に近い国同士で起きやすい（類型4参照）。ケーススタディに示したとおり、東アジアの国々は北朝鮮が手を回した迂回的な金融取引や輸送にさらされるリスクがあり、中東の国々はイランのWMD計画に関わる違法金融経路を作っている可能性がある。このほか、一部の国は、国連制裁対象地域の外交関係者その他関連主体の存在に関わる脆弱性を申告している。

その他の国レベルの要因

45. 上記以外の脆弱性として、グローバル金融システムにおける米ドルに代表される外貨の膨大かつ幅広い使用が挙げられる。各国は、違法な調達又は制裁回避にこれらの通貨又はこれらの通貨建て口座が使用される脆弱性を踏まえ、影響を受ける外貨建て越境取引に注意しなければならない。

46. また、拡散ネットワークは、物品を不正に得るために産業又は技術的要因を悪用しようとする。よって、拡散の影響を受けやすい機微技術又は製品の生産国は、その性質上、PF及びデュアルユース品規制違反にさらされやすい。防衛セクターが大規模な国は、材料、製品、サービスを提供するためにかなりの数の組織を必要とし、結果として、PFネッ

[29] 実際のところ、多くの国が国連、国家的、超国家的制裁レジームの回避に関わる脆弱性の対処に努めているが、FATFの勧告7は、唯一の国連制裁対象国である北朝鮮のみに当てはまる。本書のエグゼクティブサマリーその他で述べているとおり、本報告書には、脅威と脆弱性に関する最新知識を提供するため国家的又は超国家的制裁レジームの回避に用いられる手口に関する情報を含み、これにはFATF基準の勧告7でカバーされていない関連類型同士の共通課題も含まれている。制裁回避をより幅広く捉えることは、勧告7の要求事項を再定義することを意図してはいない。

トワークが複雑なサプライチェーンを悪用する機会が生まれる。

47. 最後に、国連安保理決議第1718号専門家パネル報告書では、北朝鮮が組織的犯罪又は国際犯罪ネットワークを拠り所とし、そうした組織の輸送ルートや仲介者に拡散活動を支援させていると指摘している。

PF・制裁回避に関するセクターレベルの脆弱性

48. FATFグローバルネットワークからの回答とパブリックコメントの結果に基づき、複雑なPF・制裁回避スキームに最もさらされやすいセクターの例を以下に挙げる。

銀行業及びその他金融セクター

49. PF・制裁回避脅威主体に利用されやすいセクターとして、多くの国が銀行業及び保険業を含むその他金融セクターを挙げている。国内又は国際金融取引を実行した結果、PF主体又はPF活動を支える資金が合法・違法行為から生じている又はそこから動かされているかもしれない。こうした取引の性質を曖昧にするためによく用いられる手口に、複数口座の使用や貿易金融関連文書を含めた文書偽造などがある。

50. コルレス銀行は、コルレス先銀行顧客との既存取引関係がないケースが多く、制裁回避に悪用されやすい[30]。複数の民間セクターの事業体が、多様で複雑な口座種別や取引はPF・制裁回避リスクにさらされやすいと指摘し、PFリスクに晒されやすい又はCPF管理の効果が乏しい国との関係が絡むコルレス銀行関係ではなおのことである。例えば、オープン勘定取引を通じた取引は、輸送物品に関する情報が不足し、悪用されやすい。また、電信送金は資金を迅速に移動できる反面、取引目的や裏付け文書が限られるのが通例である。

51. 一部の国は、全国規模の広範なネットワークを有する金融システムや、簡単に手早くアクセスできる銀行サービス、投資資産残高の増加、個人金融資産の潤沢さなどをその他の関連要因に挙げている。

暗号資産及びサービスプロバイダー

52. 多くの国が、越境決済や越境送金に暗号資産が使用される機会が増えている状況を懸念している。PFネットワークは多くの場合、勧告15の実行の遅れを認識し、各国のVASPのAML/CFT/CPF措置の不備を突こうとする（類型3参照）。適用義務に準拠したAML/CFT/CPF要求事項を整備できていない国のVASPが利用される事例もある。各国は、特に偽名で資金が調達又は移動されるPFリスクを懸念する。多くの不正主体は、WMD拡散を支援するための大規模な暗号資産窃取の利益を洗浄するプロセスを含め、サービスと匿名性強化型暗号通貨（AEC）とを組み合わせた暗号資産を使った暗号資産取引において匿名性を強めようとしている。手法を組み合わせたり、他の不透明化手口が使用されると、第三者にとって取引の追跡や出所探しが難しくなる。このほか、北朝鮮による資金獲得活動における暗号資産の役割が各国から指摘されている。

新規及び代替決済インフラ

53. 一部の国家又は非国家主体は、新規決済チャネルやSWIFT決済システムの代替経路を悪用して、国家的、超国家的又は国際的な制裁レジームと紐付く金融接点を避

30 コルレス業務は、既知の迂回国又は経由国やAML/CFT/CPF対策に不備がある国に提供される場合は特にリスクが高い。ただし、コルレス業務のリスクは拡散金融に対しても一様に高いわけではない。コルレス関係のリスク評価をケースバイケースで実施しなければならず、その際常に、コルレス先銀行が導入している内部統制及びリスク低減策を考慮しなければならない。コルレス銀行関係について詳しくは、FATFの*2021年PFガイダンス*を参照。

けようとする。例えば、国家又は非国家主体がP2P決済又はデジタル送金サービスプロバイダーなどの新しいデジタル決済システムを利用するケースもある。[31]

その他のセクターレベルの脆弱性

54. 国連安保理決議第1718号専門家パネル報告書とFATFの2021年拡散金融リスク評価及び低減ガイダンスで指摘されているとおり、各国は、トラスト・アンド・カンパニー・サービスプロバイダー（TCSP）や貴金属・宝石取引業者など、PF・TFSの違反・不履行・潜脱リスクに比較的晒されやすいこれ以外のセクターにも注意を向ける必要がある。[32]

55. このほか各国が挙げたPF・制裁回避主体に悪用されやすいセクターには、航空機、情報テクノロジー（IT）、海事、原子力、造船業などがある。

31 メッセージをやり取りするSWIFT決済システムの代替手段に関してリスク管理に潜在的懸念がある一方で、中央銀行デジタル通貨（CBDC）を使った制裁回避が現時点で理論上存在する。一方で、一部の国は、CBDCを監督官庁が金融取引の流れをより簡単に追跡し、不正金融リスクを低減できる手段と考えている。

32 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

4. セクション2.PF関連制裁回避 – 類型

最新の動向と手口

56. 本報告書では、ケーススタディを次の2つに分けて掲載する。

a. **北朝鮮に関するPF・TFSの回避**、FATF基準の勧告7の対象
b. **その他制裁レジームの回避（国家的及び超国家的制裁措置など）**、FATF基準の勧告7の対象外

57. このセクションでは、FATFグローバルネットワークから寄せられた情報に基づき、複雑な拡散金融・制裁回避スキームに用いられる類型の一部をリストアップして説明する。これらの類型は、PFを示唆する金融取引指標リストとして機能する（別紙A「リスク指標」参照）。

表1.類型一覧

類型	ケーススタディサブトピック	ページ数
1. 制裁回避のための仲介業者の利用	フロント企業とシェルカンパニー 第三国経由の資金移動 銀行口座と資金供与	21-29
2.BO情報の隠蔽による金融システムへのアクセス	金融アクセスを手助けする第三国のファシリテーター 無許可金融ファシリテーターネットワーク 様々な種別の法人の利用 北朝鮮によるクレジット/デビットカードの悪用	29-37
3. 暗号資産及びその他テクノロジーの利用	規制上の課題 暗号資産を利用した資金移動 暗号資産と資金獲得 北朝鮮のIT労働者を支える海外の団体及び個人	38-46
4. 海事・海運セクターの悪用	船舶IDの改ざん 瀬取り AIS（船舶自動識別装置）送受信の無効化 文書偽造	46-53

類型1：制裁回避のための仲介業者の利用

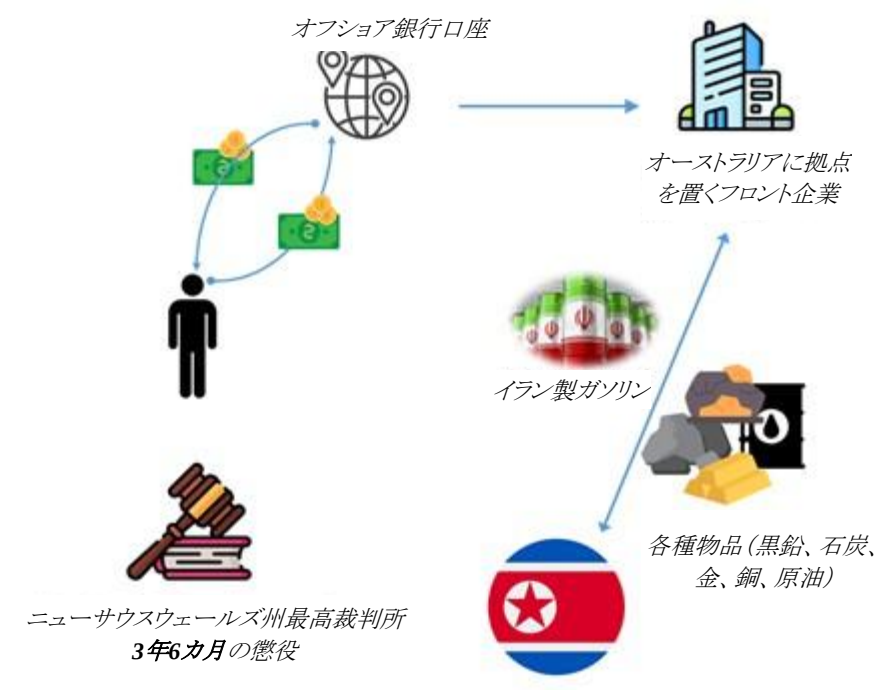
58. 各国からの報告によると、拡散国又は制裁対象国向け物品の調達ネットワークは本当の最終使用者を隠すために複数の仲介者が絡む複雑なスキームを使用している。この手口を使われると、PF・制裁回避事案の検知や捜査が難しくなる。こうした仲介者は、フロント企業、シェルカンパニー、金融ファシリテーター、銀行口座（コルレス銀行関係を含む）、第三国を介した積み替えに関わっていることがあり、こうした仲介者の使用は資金の出所、目的地、目的を隠すうえで重要な役割を果たす。複数の金融システムと規制枠組みの脆弱性を突くことによって、仲介者は拡散ネットワークの検知、制裁回避を助ける（詳しくは「脆弱性」セクションを参照）。

フロント企業、シェルカンパニーの利用

59. 多くの国から、PF・制裁回避ネットワークが第三国に仲介者又はフロント企業として機能する現地法人を立ち上げるか、その目的で現地法人とパートナーを組むことができるとの指摘があった。こうした事業体は、活動実態がないか、または偽の見せかけの下で金融システムにアクセスするための正規に見える取引や決済又は契約の手助け、物品の輸出入を行ったり(デュアルユース品を民間目的のみで申告するなど)、別の名前や所有者構造あるいは国の下で制裁対象団体とのつながりを包み隠すシェルカンパニーであることもある。こうした不正主体が、電子部品、化学薬品、産業機器のほか、制裁・輸出管理規制対象品など、密輸したデュアルユース品が関わるセクターで活動している。

ボックス2. ケーススタディ:オーストラリア拠点の企業構造を利用した制裁回避

2021年7月23日、ニューサウスウェールズ州最高裁判所は、韓国生まれのオーストラリア国籍者に対し、北朝鮮に関するオーストラリア制裁法違反の罪で3年6カ月の懲役刑を下した。被告人はオフショア銀行口座とオーストラリアに拠点を置く一連のフロント企業を使って、北朝鮮との石炭、黒鉛、銅鉱石、金、原油(北朝鮮のためのイラン製ガソリンの代理購入を含む)、ミサイル、ミサイル関連技術を含むさまざまな物品の取引を仲介した。北朝鮮に関する制裁違反では、オーストラリア初の告訴事案となった。



出所:オーストラリア

60. 仲介人は、検知を防ぐ複雑な構造を構築するために弁護士や会計士の支援のほか、複雑なサプライチェーンを作る手助けをし、制裁レジームの抜け穴を突き、禁輸品の虚偽申告や偽の見せかけによる輸送を行うためのアドバイスをする貨物フォワーダーや船舶代理店の支援を得ている場合もある。

61. フロント企業は兵器又は防衛セクター向けデュアルユース品の経路を隠すためによく用いられる手段である。不正主体はこうしたさまざまな複雑な手段を駆使し、要注意品が関わる制裁の回避や輸出管理の迂回の疑いを明らかにしようとする捜査の勢いを弱めさせる。以下の2つのケーススタディでは、そうしたデュアルユース品の最終目的地を隠すための複雑なスキームについて説明する。

ボックス3. ケーススタディ：米国製電子部品をイラン軍事組織に密輸するための制裁回避スキーム

2024年1月、複数年にわたって米国からイランへの米国製電子部品の違法輸出及び密輸を共謀し、これに関して複数の連邦犯罪を犯したとして4人の中国国籍者がコロンビア特別区で起訴された。申し立てによれば、被告はイランによる無人航空機（UAV）に組み込むためのミサイル、兵器、軍用航空機器の開発・製造を指揮するイスラム革命防衛隊（IRGC）とイラン国防軍需省（MODAFL）の関連組織のために米国の輸出管理対象製品を中国と香港経由で違法輸出、密輸した。

2007年5月に始まり、少なくとも2020年7月まで続いた活動において、被告は中国のフロント企業を使って、UAV、弾道ミサイルシステム、その他軍事用途品の製造に使われる可能性のある電子機器、部品を含む米国製デュアルユース品をIRGC及びMODAFLとつながりのある制裁対象企業（Shiraz Electronics Industries (SEI)、Rayan Roshd Afzar及びこれらの関連会社）に輸出した。

被告は、この一連の共謀活動を通じて物品の目的地がイラン及びイラン系企業である事実を隠し、最終目的地と最終使用者に関して米国企業に対し重大な虚偽陳述をした。これらの虚偽行為により、米国企業は当該製品の最終目的地は米国の制裁及び輸出管理法規制に反したイランではなく、中国であるとの偽りの下、偽の見せかけのフロント企業にデュアルユース品を輸出した。米国司法省と商務省が共同で指揮した複数行政機関攻撃部隊による連携がこの複雑な制裁回避スキームに関する起訴に至った。

出所：米国

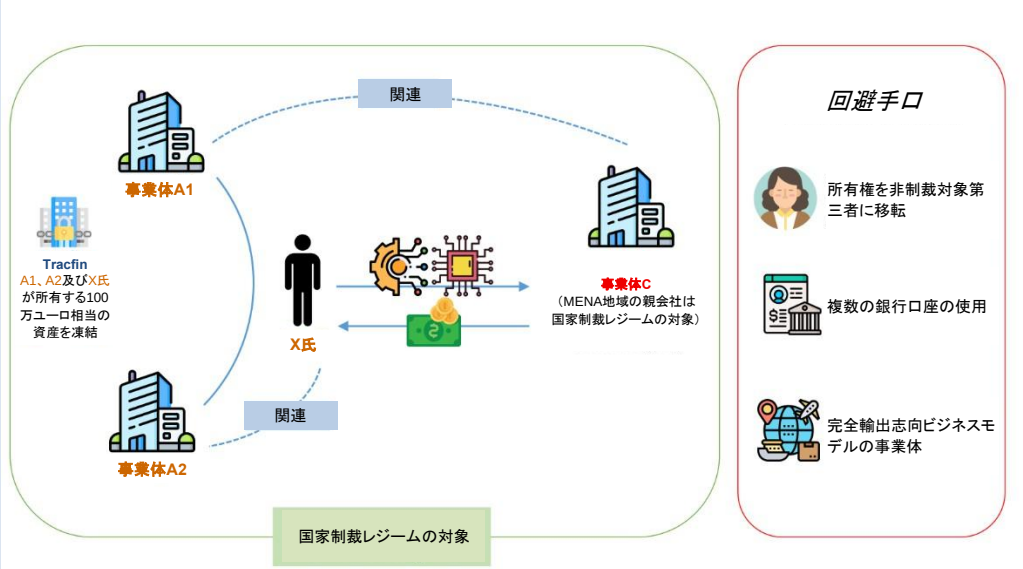
ボックス4. ケーススタディ：仲介者を使ったロシア企業へのデュアルユース品の輸出

フランスに拠点を置く事業体A1と事業体A2は、MENA地域の別の仲介企業（事業体B）に再販される海外製電子部品を購入する仲介者の役割を果たした。仲介役の2社はデュアルユース品を購入した後、その電子部品を米国の制裁対象であるロシアの親会社（事業体C）に供給した。この拡散スキームによって、ロシアの防衛セクターは禁輸品を手に入れ、全体的な能力を高めることができた。

フランスのFIU（資金情報機関）であるTracFinは、このスキームを止めるための各機関の協力を指揮し、A1、A2及びX氏（A1及びA2のUBO）が所有する100万ユーロ相当の資産凍結を行った。米国財務省外国資産管理室（OFAC）はA1、A2及びX氏を制裁対象に指定しているが、現時点で当該個人及び団体はEU又はフランスの規制措置の対象ではない。その後、事業体A1の株式は海外投資家に売却されたものの事業体Cが依然として事業体A1を支配している疑いがあり、TracFinはフランス国内銀行の協力を得て支配力基準に基づき該当者の資金を制限した[33]。事業体A2はX氏が100%所有する。

こうした複雑な制裁回避スキームには数多くのよくある制裁手口が絡み、例えば非制裁対象第三者（個人の妻）への所有権の移転、複数の銀行口座の使用、通過事業体として機能する完全輸出志向ビジネスモデルの企業などが挙げられる。

一番の課題は制裁レジームごとの食い違いであり[34]、結果として資本逃避に至ることがある。制裁を確実、効率的に実施し、各国での資産凍結に法的根拠を持たせるためには、協調的な指定プロセスが有益であろう。



出所：フランス

33 EU法において、支配力基準はその資金又は事業体が制裁対象団体又は個人に支配されているか否かの判断に役立つ。例えば、制裁対象団体又は個人がその資金又は事業体に影響力を持つか、意思決定権がある場合、この点が支配力の有無の判断材料になる。

34 セクション3（パラグラフ105～106参照）及び結論（パラグラフ146、優先領域を参照）で述べるとおり、こうした食い違いはPFに関する制裁回避の検知、捜査、訴追に関する課題の主な要因の一つである。

第三国中継を通じたグローバル化したサプライチェーンと国際貿易の悪用

62. 拡散ネットワークがグローバル化したサプライチェーンと国際貿易を利用し、物品や技術の調達活動を隠していると各国が指摘している。拡散ネットワークは、最終用途の性質を曖昧にするために複数のサプライヤーから構成材を調達し、往々にして監視が厳格でなく、再包装や新しいラベルでの再輸出が可能な自由貿易地域(FTZ)を介して物品を移送している可能性がある。物品は複数の港又は国から送り出すことによって本当の出発地や目的地を隠し、偽の文書や虚偽船積書類、最終使用者証明書、船荷証券を使って積荷又は最終受取人の性質を虚偽表示することがある。例えば、禁止されたミサイル部品の輸送は改ざん書類によって産業機器に偽装されることがある。以下2つのケーススタディでは、輸出管理規制及び制裁回避の検知をより難しくする複雑な中継ルートについて説明する。

ボックス5. ケーススタディ:仲介者を利用した輸出管理規制回避

複数のケースが(同じ類型の繰り返しを示す傾向が見られるが)、第三国企業、場合によってはEU域内の別の法域に拠点を置く企業がイラン人の管理又は支配下にあり、フランスのサプライヤーからデュアルユース品を購入し、イランに再輸出している回避スキームを浮き彫りにしている。

イランの弾道ミサイル計画用物資を供給するあるイラン系企業が、フランスのサプライヤーから複合材料を入手しようとした。当該企業のイラン人責任者は、別のイラン国籍者が経営する第三国の企業を利用し、その第三国企業が複合材料をイランに再輸出した。

2020年、ある工作機械がEU領域を離れる前に欧州のA国、B国、C国に連続して輸出された。この複雑な貿易パターンと書類の変更には、その工作機械が中東のある法域に到着した後、最終目的地のイランへと続くそれ以降の経路をカモフラージュする意図があった。

出所:フランス

ボックス6. ケーススタディ:国際協力を通じた、仲介者を利用したEU制裁回避の検知

2022年、あるポルトガル企業がUAEの仲介者を経由し、申告によれば最終目的地はカザフスタンの企業だとしてUAV用モーターを輸出しようとした。UAV用モーターはEUの対ロシア制限措置第12次パッケージの範囲に該当し、物品の最終目的地がロシア連邦であることを疑わせる強い指標があった。捜査を行ったところ、当該企業は目的地に関する質問を受けた後、物品の輸出を断念した。

当該企業はUAEの貨物転送会社とカザフスタンの小売業者の2つの仲介者を使って制裁回避を試み、最終使用者も隠した。そのカザフスタン企業はロシア企業と強い商業上のつながりがあり、迂回リスクが高い。決済は銀行送金によって行われた。

その後、ポルトガル当局が当該企業を継続監視した結果、2023年に安全・防衛分野の別の物品をセルビアと香港の仲介者を通じておそらくロシアに輸出したことが判明し、どちらの国の仲介者もロシア連邦と強い商業関係のある企業であった。

この事件ではセキュリティインテリジェンスサービスと税関当局が協力し、国際協力と税関調査の助けを借りた情報収集と捜査によって事件が検知された。

この事例は、新しい環境やさまざまな課題に対する調達ネットワークの適応力を物語っている。各国の効果的な協力と円滑なコミュニケーションがあって初めて、この種の脅威を抑制できる。

出所:ポルトガル

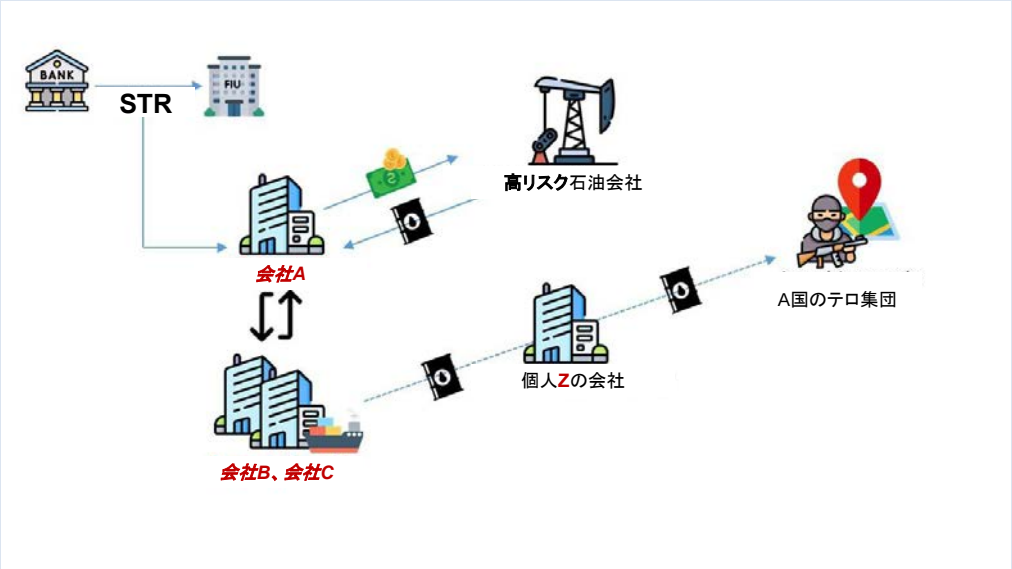
63. このほかにも、制裁対象の国又は団体に近い地域内の中継拠点は、資金や物品を動かそうとする制裁回避者に狙われる。特に、PF・制裁ネットワークは、巨大な規模の商業、金融、貿易活動によって自らの違法行為が隠されることを期待して国際金融センターで自らの行為を隠そうとする。

ボックス7. ケーススタディ:海運会社を使った制裁対象団体への原油の販売

2022年9月、法執行機関(LEA)がアラブ首長国連邦(UAE)FIUから、ある銀行より通報された疑わしい取引報告(SAR/STR)について情報提供を受けた。そのSAR/STRとは、会社Aから高リスク石油会社への電信送金であり、WMD拡散支援に使われることが疑われるという。LEAとUAEFIUは、会社Aとその金融/商業活動について犯罪及び金融捜査を行った。

捜査の結果、会社AはUAEの海運会社2社(会社B、会社C)とつながりのある外国籍の人物が設立したことが判明。また、会社B及び会社CがA国のテロ集団を支援する個人に属することも明らかになった。会社B及び会社Cは、石油を高リスク国から会社B及び会社Cに輸送する際の輸送契約を作成する仲介者として個人Zの会社を使用した。石油はその後、テロ集団に送られていた。

捜査では、会社B及び会社Cが石油の原産地を隠すために書類を偽造し、テロ集団に石油を販売していたことも明らかになった。石油の販売収益は会社Aを一度経由し、そこから高リスク石油会社に送られた。制裁対象団体が拡散を支援するために使用していると疑われるフロント企業である。捜査の結果、送られた資金は総額7,000万USドルに上ることが判明し、LEAは個人Zを含むすべての容疑者を逮捕し、個人ZはイランのPF制裁回避を助ける行為に関与したことを自白、会社は事業活動停止となった。



出所:アラブ首長国連邦

銀行口座の使用と第三国を経由した資金供与

64. PF・制裁回避主体はしばしば、資金の出所、目的地又は目的を隠すために幾層もの金融取引を使用するが、これは昔から使われているマネー・ローンダリングの手口である。多くの場合、複数の国の複数の金融機関を経由して支払いを引き回し、各国で登記されたフロント企業又はシェルカンパニーを使い、規制の抜け穴を突いて追跡活動を妨害する。

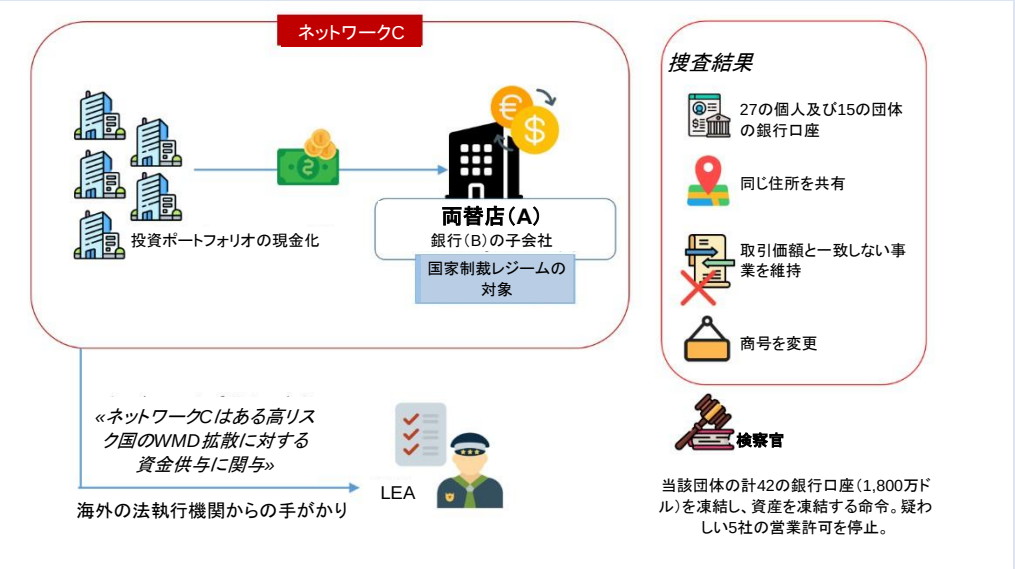
ボックス8. ケーススタディ:PFを支えるための金融システムを悪用した石油輸送

LEAは秘密の情報源から得た情報により、5つのUAE企業と銀行(B)の子会社である高リスク両替店(A)が複数の国内・国外向け高額取引を行ったことを認識した。両替店Aと銀行Bはネットワークの一部であり、米国財務省外国資産管理室(OFAC)の指定団体である。疑いのある5社のうち2社は投資ポートフォリオの現金化と両替店Aへの送金によって資金を得ていた。両替店Aはその資金を銀行Bに送り、制裁対象団体を支援していた。LEAは関係当局(UAEFIU、アラブ首長国連邦中央銀行(CBUAE)、現地登記官、税関)と合同捜査を開始した。

CBUAEは27人の個人と15の団体の銀行口座がネットワークと紐づいていることを突き止めた。現地登記官も、LEAに対して現地視察報告書を提供した。この報告書によって、疑わしい団体が同じ住所を共有し、団体の多くが現地視察前に商号を変更し、取引価額と一致しない事業を行っていたことが判明した。これと並行して、LEAはある海外の法執行機関からネットワークCが高リスク国のWMD拡散に対する資金供与に関与していたことを確認する手がかりを得た。

これらの捜査結果から、UAEFIUとCBUAEの協力の下、検察官が当該団体の資産に対して凍結命令を出し、42の銀行口座、総残高およそ1,800万ドル(6,372万5,065 UAEディルハム)を凍結した。これに加えて、現地登記官が疑わ

しい5社の営業許可を停止処分とした。



出所：アラブ首長国連邦

65. PFネットワークは、法域ごとの国際又は国内制裁レジームの実施状況の違いを利用しようと第三国の金融機関を狙う。不正主体は銀行で口座を開設し、コルレス銀行関係を使って警告信号を出されることなく、国際金融市場に間接的にアクセスできる国際電信送金を行う。不正ネットワークは、疑わしい取引を検知される可能性が低い非公式金融システムや、越境取引に関する報告義務や執行がさほど厳格でない国を使うこともある。

ボックス9. ケーススタディ：IRGCが資金獲得のために使用した、制裁対象団体及び個人で構成された「シャドーバンキング」ネットワーク

2024年6月、OFACはMODAFLやIRGCが利用していた無秩序に広がった「シャドーバンキング」ネットワークの複数の支部を構成するおよそ50の団体及び個人に制裁を課した。このネットワークはさまざまな活動に手を染めていたが、中でもUAVなどの高性能兵器の開発を目的とした米国製電子部品の不正調達や、イエメンのフーシ派やロシアによるウクライナ侵攻を支援するための資金獲得を行っていた。

MODAFLは国際金融システムにアクセスするため、香港、UAE、その他の場所の多数のフロント企業を管理するイランの両替店を使用し、海外での石油販売などの商業活動から得た収益を洗浄し、クリーンな外国通貨に換えている。同じフロント企業は洗浄した外貨を使って国際市場から兵器部品を調達する。

出所：米国

ボックス10. ケーススタディ：仲介者を利用したTFS回避と不動産収益の送金

2015年、北朝鮮のフランス駐在外交官がパリのアパートを購入し、2017年に国連の制裁対象に指定されるまで賃貸していた。制裁対象に指定された後も、継続的にアパートの賃貸収入を得ていた。当該外交官は複数の仲介者と複数の第三国銀行口座が絡むスキームを構築し、最終受益者としての立場を隠した。2019年にある欧州系銀行から警告が発せられた後、収入はエスクロー口座に移された。

出所：フランス

類型2：BO 情報を隠した制裁回避と金融システムへのアクセス

66. 複雑なPF・制裁回避には、多くの場合、虚偽のBO情報が関わっている。最終使用者/最終用途と最終目的地の不透明化によって、官民セクターのどちらにとっても検知が困難になる。また、こうした不透明化の手口の多くがデジタル世界にも持ち込まれ、検知に向けた新たな課題を生み出している。TFSは、指定個人又は団体と、当該制裁対象者が支配又は所有する資金に適用されるため、実質的所有者の特定は制裁回避リスクの低減に役立つ。

第三者ファシリテーターが北朝鮮の金融システムアクセスを支援

67. 北朝鮮は、BO情報の不透明化を含め、国連又は国家制裁レジームを回避し、正式金融システムにアクセスするために、日常的に虚偽行為を働く。北朝鮮は依然として海外のフロント企業やシェルカンパニー、秘密の海外代理人、第三者ファシリテーターを使用しており、本当の原資産所有者、受益者、取引目的を曖昧にすることによって、国際金融システムを通じて、北朝鮮による不正な金融活動から得た数十億ドルを流している。北朝鮮の金融システムにアクセスするための複雑なスキームを支援する国家主体が制裁回避の阻害を難しくしている。

ボックス11. ケーススタディ：北朝鮮とロシアの金融機関が画策した複雑な制裁回避スキーム

2024年9月、米国財務省外国資産管理室（OFAC）は、不正金融スキームを使い、国連安保理決議第1718号で義務付けられたTFSに反して北朝鮮の国際金融システムへのアクセスを可能にしたとして、ロシアとロシアが占領する南オセチアのグルジア地域に拠点を置く5つの団体と1人の個人から成るネットワークを制裁対象に指定した。[35]また、当該団体及び個人は、国連安保理決議第2270号に基づく北朝鮮銀行とのコルレス関係の禁止にも反していた。

この措置は、いずれも国連安保理決議第1718号制裁リストの指定組織である2つの北朝鮮国営組織、フォーリン・トレード・バンク（FTB）とコリア・クワンソン・バンキング・コーポレーション（KKBC）が画策した複雑なスキームをターゲットにしていた。[36]FTBは、北朝鮮の主要外国為替銀行として機能し、北朝鮮がWMD計画や弾道ミサイル計画の資金源確保のために用いる不正金融ネットワークにとって欠かせない存在である。FTBとKKBCはロシア連邦の手を借り、北朝鮮の不正金融ネットワークへのアクセス範囲を広げ続けている。

ロシア中央銀行が画策したスキームでは、ジョージアの南オセチア地域に本部を置くMRB Bank（MRB）がFTBとの秘密の銀行取引関係を築くためにロシア系銀行、TSMR Bank, OOO（TSMR Bank）の隠れ蓑として機能した。TSMR Bankの上級幹部がTSMR Bankを経由したFTBからMRBへの現金預金を手助けした。また、MRBのFTBとKKBC用のコルレス口座開設を取り計らい、北朝鮮代理人と連携して数百万単位のドルとルーブル紙幣をMRBのFTB、KKBC口座に入金した。MRBの少なくともいくつかの北朝鮮口座がロシアから北朝鮮への燃料輸出の支払いに使用されていた。

2023年後半には別のスキームの一環として、Russian Financial Corporation Bank JSC（RFC）がFTBと手を組んでモスクワに本社を置くStroytreyd LLC（Stroytreyd）を設立し、消滅したロシア系銀行が保有していた北朝鮮の凍結資金を受け取った。この凍結資産を北朝鮮に送り返す活動の一環として、FRCが所有するTimer Bank, AO（Timer Bank）が数百万ドル相当の資金をFTBの実質的受益者に代わるStroytreydに送金した。北朝鮮の政府高官がRFCと手を組んで北朝鮮・ロシア間のハイレベル経済交流を拡大させ、両国の経済協力を強めさせている。FTBはRFCと連携し、北朝鮮に本部を置くアグリカルチュラル・デベロップメント・バンクを含む、他の北朝鮮系銀行の代わりに口座開設も行っている[37]。

出所：米国

35 https://home.treasury.gov/news/press-releases/jy2590

36 国連安保理決議第1718号制裁リストでは、FTBはKPe.047、KKBCはKPe.025として指定されている。

37 日本政府は、北朝鮮とロシアの協力を手助けしているとして、2025年1月10日付けで4人の個人と5つの団体（MRB Bank、Russian Financial Cooperation、Stroytreyd LLC、TsMRBank、Timer Bank AO）を指定した。

68. 多くの国が指摘するとおり、北朝鮮は外交官を含む国民も当てにしており、金融サービスの提供や大量の現金の輸送を含む資産や資源の輸送を手助けさせている。こうした手口は検知が難しく、外交儀礼上、これらの行為をタイムリーに阻止、妨害することはさらに難しい。

ボックス12. ケーススタディ：北朝鮮外交官の配偶者による保険会社への資金移動

ナイジェリアに本社を置く複数の保険会社に、北朝鮮の国営保険会社、Korea National Insurance Company（KNIC）の債権回収、事業開発、資金回収、資金転送を手助けし、米国の制裁措置を回避するための代理店又は代理人として機能するために、制裁対象である同国外交官の配偶者と手を組んでいる疑いがあった。KNICは、2017年の国連安保理決議第1718号制裁レジームに基づき、対象指定されている（KPe.048）。KNICを介して受け取った資金は最終的に北朝鮮のWMD計画に流用される。

ある金融機関から通報されたSAR/STRによって、ナイジェリア当局は法外な金額の資金が伴う金融活動を検知した。推定取引金額は61万6,000ユーロを超える。疑わしい行為を検知した結果、金融機関は該当口座を凍結し、ナイジェリア当局に改めて報告した。ナイジェリアはこのほかにも追加対策を検討中である。

狙われた保険セクターの脆弱性は、保険会社が国のインフラのためにサードパーティー企業を介して国際保険又は再保険を購入する際の購入経路にあった。また、保険会社の顧客と取引が制裁回避スキームに悪用され、該当事業体のリスク対策を強化する必要性を実証している。

出所：ナイジェリア

69. 北朝鮮が外国籍者やその外国籍者が登記したフロント企業を使ってBO情報を隠し、正規の金融システムにアクセスしたり、それを介して資金を移動させている実態を多くの国が認識している。例えば、FTBとKKBCは、中国系銀行に口座を持つ中国国籍者の名の下でフロント企業ネットワークを構築し、北朝鮮との金融上の結び付きを曖昧にしたうえで国際金融システムを介して資金を移動させている。

ボックス13. ケーススタディ：北朝鮮系銀行・金融サービス – フォーリン・トレード・バンク

2020年5月、米国当局はさまざまな身分で活動していた30人以上の個人に対して、国連の制裁対象であるFTBのためにサービスを提供し、禁止された米ドル建て取引を行った疑いで刑事罰を科したことを明らかにした。起訴内容には、北朝鮮政府の代理人として米国企業が最終的に受け取った金額が記されている。FTBのフロント企業とサードパーティー企業とのそれ以外の支払いも、米国のコルレス銀行を介して決済されていた。

起訴内容に列挙された個人は、この共謀の間、250を超えるフロント企業を介し、米国を中継してコルレス銀行に少なくとも25億ドルの不正決済を処理させていた。これらのフロント企業はオーストリア、中国、クウェート、リビア、マーシャル諸島共和国、ロシア、タイで設立されていた。起訴された個人の多くはこれらの国に活動拠点を置き、FTBの「秘密」支部を運営しながら、中国国内の都市を中心にいくつもの重大な活動を行っていた。

これらの個人はサードパーティーの金融ファシリテーターと手を組み、北朝鮮に代わって汎用品その他の物品購入の決済ができるフロント企業を設立した。精製石油や石炭取引に関する決済も含まれる。このほか、金属、電子機器、電気通信会社への決済も行っていた。被告らは、取引相手が既存会社に疑いと持つと、新しいフロント企業を設立した。FTB代理人同士の意思疎通においては暗号化した支払参照番号が使用されるため、FTB本部は購入を指示し、フロント企業から支払い先への資金の流れを常に正確に見極めることができる。最終的な実際の物品の輸送では、被告らは契約書とインボイスに虚偽の最終目的地と最終使用者を記載していた。

出所：米国

無許可金融ファシリテーターネットワークが制裁回避を支援

70. このほか、イランがBO情報の不透明化を含め、複雑な制裁回避スキームを使用し、自国のWMD計画のためにデュアルユース品を調達していることを多くの国が指摘する。その多くについて、イランが主要金融センターに登記されたフロント企業を使ってイラン政府が支配する両替店から資金を動かしていることが確認されている。

ボックス14. ケーススタディ：違法なTCSPを使ったデュアルユース品取引

オランダでは、イラン国民が複数の法人を設立し、これらの法人はテクノロジーセクターで事業活動を行っていた又は現在も行っている。この中には、高度技能移民にとってオランダの在留許可証を取得しやすいと噂される、認可身元保証会社[38]（RRC）を使用したケースが含まれる。このRRCは、違法なTCSPの一部であるか、直接的な関係性があり、法人登記、銀行口座の開設などのサービスを提供し、（オランダの優遇税制又は租税条約の恩恵を受けるために）少なくとも取締役の半数がオランダ国籍者であることが確認されている。

合法なTCSPはオランダ中央銀行の監督下にあるが、違法なTCSPは提供サービスを複数の法人に分散させている。これによって安価にサービスを提供しているが、こうしたトラストサービスは検知が難しくなる。よって、オランダ中央銀行がこれらの団体を監督することは困難である。この場合、主要な金融センターを介してイランから送られてくるという資金が違法なTCSPが設立したオランダ法人に違法に送られる。その後、資金はこの構造内に送られ、最終的には高度技能移民へと流れる。

この場合の銀行取引明細書には複数の取引が記録され、そこにデュアルユース品がイランに供給されるリスクが生まれる。これらの物品は拡散目的でも使用される。これらの取引はイランの高度技能移民が支配するテクノロジー企業と関係していることもある。したがって、これらの企業がフロント企業として機能していることを結論付けられる。TCSP、特に違法なTCSPが使用され、法人網が構築されることによって、こうした金融取引の検知は極めて難しい。

出所：オランダ

71. 無許可金融サービス業（MSB）は、国家指定又は国連指定テロ集団に代わって活動する個人の資金移動にも利用されることがある。以下は、UAE当局がフロント企業をハワラダー[39]として使用し、数百万ドルを動かしていた複雑なスキームを発見した事例である。これは個人が非国家主体に代わってTF・TFS回避を行った事例であるが、PF関連制裁回避に用いられる複雑なスキームの種別にも関係しているかもしれない。

38 認可身元保証会社とは、外国人の入国支援を行う会社、学校又は団体を指す。
39 ハワラダーとは、ハワラサービスを提供する資金移動仲介者を指す。

ボックス15. ケーススタディ：国連第1267号リスト指定テロ集団のための無許可MSBを使った制裁回避

2022年第1四半期に、UAEの外国人居住者を受取人とする高リスク法域からの電信送金について、地元の両替店からUAEFIUにSAR/STRが通報された。この送金に関わるすべての当事者が、UAEFIUが入手した金融インテリジェンス情報の対象者であった。

UAEFIUの捜査と分析の結果、主たる容疑者は7件の電信送金、計350万USドルを受け取り、ダーイッシュ（ISIL）とジャブハット・アル・ヌスラのメンバーを支援するために高リスク国へ資金を移動させるハラワダーとして機能させるためのフロント企業をUAE内に設立していた。どちらの集団もUAE国家リスト及び国連統合リスト（国連安保理決議 1267/1989）で指定されている。

UAEFIUは国家治安局に容疑者とそのフロント企業の詳細情報を説明し、この事案を共有した。国家治安局はUAEFIU及び中央銀行と協力し、容疑者の金融活動を捜査し、その結果、容疑者の資金とその他資産、総額50万USドルと金4kgの凍結命令を出した。フロント企業の事業活動も差し止めとなった。容疑者は一連の捜査を通じて、ダーイッシュ（ISIL）とジャブハット・アル・ヌスラへの拳銃と弾薬を含む武器購入資金の提供を自白した。

出所：アラブ首長国連邦

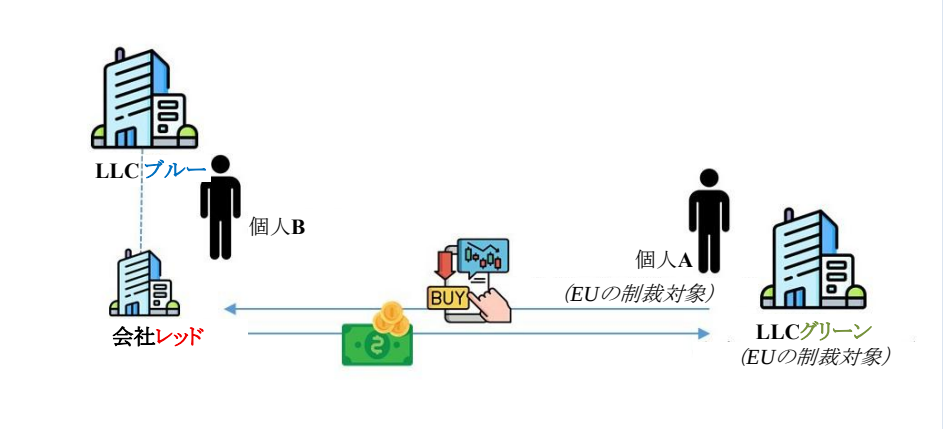
さまざまな種別の法人を使った制裁回避

72. 一部の国は子会社その他の法人を使った実質的所有者情報の隠蔽を指摘している。制裁回避を目的とした複雑なスキームや、AML/CFT/CPF対策に不備のあるセクターを標的にするより単純明快な方法などがよく用いられる手口である。

ボックス16. ケーススタディ:EU制裁回避のための複雑なスキーム

EUの制裁対象である個人Aは、個人Bと共に制裁回避を手助けする複雑なスキームをまとめた。まずは、合同会社(LLC)ブルーの所有者である個人Bが、会社レッドと呼ばれる子会社を設立した。次に、個人Bは会社レッドを使って個人Aが所有するLLCグリーンの株式を取得した。LLCグリーンはある欧州系企業の株式2,850万株を所有していたが、LLCグリーンは個人Aが支配していたため凍結された。よって、会社レッドが個人Aの所有するLLCグリーン株を取得したことによって、その欧州企業の凍結株式を取得することになった。LLCグリーン売却と引き換えに、個人Aは同等の経済的利益を受け取った。

個人Bはロシア拠点企業(LLCブルー、会社レッド、LLCグリーン)と共にこのスキームを使い、リスト対象個人が支配し、EU企業の凍結株式を所有していた非EU会社をEU域内でのこれらの株式の凍結解除のみを目的に売却し、制裁回避を手助けした。



出所:欧州委員会

ボックス17. ケーススタディ：複数の所有者構造を使った真の車両所有者の隠蔽

複数のシェルカンパニーを使った、数十万ユーロに相当する複数台の高級車の真の所有者の隠蔽が行われた。一連のシェルカンパニーの最後の会社であるドイツで登記されたLLCが高級車の所有者であった。当該LLCの公式業務はこれら高級車の管理であったが、制裁執行中央室による広範な捜査によって、当該LLCが真の車両所有者を隠すためだけに機能していたことが判明した。

実際に、当該LLCとその所有車両は、ロシア制裁レジームに基づきEUに指定された個人が支配していた。捜査によって制裁対象個人と当該LLCとのつながりが明らかになった結果、当該車両は凍結された。さらなる捜査によって、これ以外の資産も制裁対象個人に紐付けることができた。

出所：ドイツ

ボックス18. ケーススタディ：子会社を使ったUN指定北朝鮮団体との関係隠し

会社βは建設・公共事業セクターに属し、重機、固定式クレーン、可動式クレーン、掘削機、ローダー、大型トラックなどの他社への供給も行っていた。会社βの主要顧客は会社γと同業のその他中小会社である。会社βの実質的所有者のX氏とマネージャーのY氏は、いずれも国連の制裁対象国である北朝鮮の国籍を持つ。

会社γは農業食品セクターに属し、会社βから農業食品用機械を購入していた。会社βが総額30万ユーロ（2億CFAフラン）を超える異例の数の小切手を現金化した後、セネガルのある金融機関が顧客管理（CDD）を実施したところ、北朝鮮の平壌に本社を置く会社βの親会社が国連第1718号制裁リストに該当していたことが判明した。

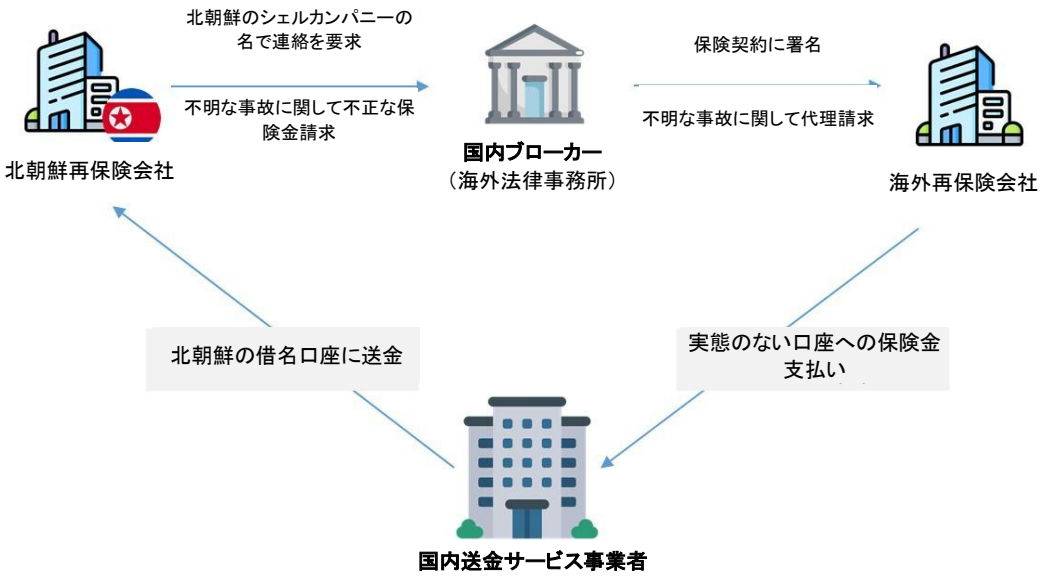
制裁対象団体とのつながりが確認されたため、当該金融機関はSTRをセネガルのFIU（CENTIF）に提出し、会社βの資産は凍結された。STRによってCENTIFは捜査を開始でき、制裁回避スキームにおける会社γの故意の関与は認められなかった。

出所：セネガル

73. 北朝鮮は事故をでっち上げ、国際保険市場から保険金をだまし取ることによって年間数百万ドルを得ている。北朝鮮国内で保険金請求を確認する術がないのをいいことに、北朝鮮の再保険会社は橋や工場などの国のインフラ建設のために国際保険又は再保険を購入し、書類を偽造して保険金を集めている。北朝鮮は、再保険契約を締結し保険金を受け取るために、シェルカンパニー又は借名口座を動員している[40]。

40 北朝鮮に対する保険・再保険は、北朝鮮の核又は弾道ミサイル計画に寄与する可能性のある大量の現金、金、保険サービスの提供を禁じた国連安保理決議第2270号第33項及び36項への違反である。

ボックス19. 事例：北朝鮮による実態がわからない社用車を使った保険詐欺



北朝鮮によるクレジットカード、デビットカードの悪用

74. 複数の国が、北朝鮮関係者が不正に入手した中国国籍者名義の口座を使って自らの金融プロフィールを隠したり、決済や現地通貨の獲得のために暗号資産を悪用し、北朝鮮の継続的な国連制裁回避を手助けするケースが増えていると認識している。

75. 北朝鮮系列銀行が、中国系大手商業銀行が発行した大量のUnionPayデビットカードを不正入手し、何百もの国内口座所有者の名義を使って現地通貨決済を行う目的で不正に管理していることが疑われている。取引や北朝鮮とのつながりを隠すことによって制裁を回避する試みであると同時に、強固な北朝鮮制裁レジームを実施している国を介して利益を得たり、禁輸品を購入しているとの指摘がある。

76. こうした一見分散化した金融ネットワークは、個人の誰かが機能不全に陥った場合の影響を抑える効果があるだけでなく、政府当局によるすべての北朝鮮口座の発見を格段に難しくしている。北朝鮮は不正入手したUnionPayデビットカードを使用して盗んだ暗号通貨から生じた不換通貨を得ているだけでなく、幅広いWMD関連組織のために取引を調整しているとの指摘もある。

類型3：暗号資産及びその他テクノロジーの利用

77. 昨今、制裁対象主体がデジタル経済を悪用する傾向が強まっている。暗号資産その他の新規テクノロジーが、国際的、超国家的、国家的制裁レジームの回避やWMD主体及びWMD活動への資金供与に利用されている[41]。暗号資産は次のような金融の流れを助けるために利用されている。

a) 制裁対象国への直接的な流れ

b) 制裁措置が適用されない仲介する第三国を経由した間接的な流れ。その結果、多くの国が、違法主体による暗号資産その他新規テクノロジーの悪用を主なPF脅威/脆弱性として挙げている。

78. さらに広く見ると、各国は、人工知能など、それ以外の新規テクノロジーから生じる制裁回避課題も指摘している。ただし、この領域でのエビデンスや動向はあまりに初期段階で、結論を導き出すことは難しく、ケーススタディもほとんど存在しない。

規制課題

79. 仮想資産その他のテクノロジーに関連する新しいリスクに対処するための努力が注がれているにもかかわらず、多くの国のVASPはAML/CFT対策に不備がある。2024年4月時点で、FATFグローバルネットワーク加盟国の4分の3が暗号資産及びVASAPに関する国際基準に不適合又は一部適合と評価された[42]。規制や国際的監視の弱点により、このセクターがPFネットワークに悪用されやすい状況がいまだ解消されていない。暗号資産及びVASPに関するFATF基準の実施に法域ごとのばらつきがある限り、枠組みが弱い又は存在せず、検知も阻止も行われない法域でのVASP悪用をPFネットワークに許すことになる。以下のケースが示すとおり、AML/CFT枠組みの対象でありながらも、適用要件の準拠を怠っているVASPの事例もある。

41 2025年3月にインドで開かれた「Private Sector Consultative Forum（民間セクター諮問フォーラム）」では、参加者から新しい金融テクノロジーに伴うリスクが増しているとの声が強くあがり、特にますます複雑で巧妙な手口を使う北朝鮮などの国家主体によるサイバー窃盗での暗号資産の利用が指摘された。

42 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

ボックス20. ケーススタディ：バイナンス執行措置

2023年11月、Binance Holdings Limited（バイナンス）は有罪を認め、送金事業者としての登録を怠ったことを含む複数の制裁プログラムに関わる違反と、国際緊急経済権限法（IEEPA）違反に関する米国司法省の捜査に決着を付けるために40億ドル超の支払いに同意した。バイナンスの創設者兼CEOは、銀行秘密法（BSA）に違反し、有効なAML対策の維持を怠った罪を認めた。

有効なAML対策が行われていなかったことを一つの理由に、違法主体はバイナンスの両替を、暗号資産の出所と所有者を隠した取引の実行、ランサムウェアバリアントから不正に得た収益の移動、ダークネットマーケット取引、交換ハッキング、さまざまなインターネット関連詐欺から得た収益の移動など、さまざまな方法で利用した。

バイナンスユーザーは、SAR/STRの通報なくイランなどの米国の制裁対象国の暗号資産交換業者と取引を行った。バイナンスユーザーウォレットはさまざまなイランの暗号資産交換業者と大量の直接取引を行い、個別には2,000ドル相当以上、総額では5億ドル相当を超える。この総額には制裁対象個人又は団体に関わる暗号資産ウォレットとの複数の取引が含まれる。

出所：米国

暗号資産を使った資金移動

80. 暗号資産は制裁対象国やその関係主体へ流れる資金の動きを隠すために利用されている。暗号資産は特定の手法と組み合わせた場合に、利用者に高いレベルの匿名性を与え、なおかつ資金を瞬時に国境を越えて動かすことができる。また、暗号資産の国際性は、海外VASPがそれぞれに拠点を置く法域の確認、国際協力に必要な時間と資源、規制枠組みの違い、法域ごとに異なる制裁レジームなどの課題を突きつける。特に、各国から寄せられた事例は制裁回避の試みに仮想ウォレットや交換プラットフォームがよく使われていることを実証している。

ボックス21. ケーススタディ:国の制裁対象VASPへの資金移転

ウクライナのFIUは、マネー・ローンダリングや制裁回避に利用される新しいテクノロジーに関する幅広い調査の一環として、国の制裁対象であるVASPを含め、暗号資産交換業者間に疑わしい資金移動があることを発見した。

FIUは、欧州内外の国(英領ヴァージン諸島、香港、英国、エストニアなど)で登記された会社で構成されたある暗号資産交換業者(交換業者A)が別の2つの高リスク暗号資産交換業者(交換業者B及びC)からの暗号資産の受取人であることに気づいた。交換業者Aの所有者はエストニア国籍者として登録されていたが、当該所有者はウクライナのPEP、具体的にはウクライナの政治家の息子と考えられたため、ウクライナFIUの関心を引いた。

交換業者Aは交換業者B及びCから多額の資金を受け取っており、交換業者Bはウクライナ政府が2023年に自国制裁レジームに基づき制裁対象としたロシア人所有VASPと特定された。交換業者Cは、7億USドルの資金洗浄に関与した疑いでその所有者が逮捕された高リスク交換事業者と特定された。ウクライナFIUは、交換業者B及びCは暗号資産トロンのブロックチェーンを使って暗号資産交換業者Aに暗号資産を送り、資金の出所と動きを隠していたと指摘している。

FIUの捜査結果は公判前の捜査の一環として現在検討が進められている。

出所:ウクライナ

ボックス22. ケーススタディ：北朝鮮への資金移動のためのさまざまな手口

2024年12月、韓国政府は北朝鮮のために資金獲得、サイバー攻撃、暗号資産の窃取を行ったとして1つの団体とKim Chol Min、Kim Ryu Songを含む15人の個人を制裁対象に指定した。両名は隣国第313総局の幹部である。[43]北朝鮮は隣国のファシリテーターの協力を得て、暗号資産ウォレット、銀行、電子金融プラットフォーム、その他不換紙幣口座を使って資金を移動させている。北朝鮮は、不正に得た収益を不換紙幣に換えたうえで平壌に多額の資金を送り、暗号資産を換金した不換紙幣収益を使って、制裁対象品の購入や同国のWMD計画への資金源に利用している。

第313総局は北朝鮮の研究開発及び武器その他の分装備品を管理している。このほか、周辺国及び世界各国への自国IT労働者の派遣にも関与している。

出所：韓国

81. PF・制裁回避関連主体は、ますます高度化する手口を使って不正に得た収益を暗号資産を介して洗浄し、資金源を隠している。北朝鮮に代表される国々は、分散型金融（DeFi）の仕組みと言われているミキシングなどの匿名性向上技術、クロスチェーンブリッジ、その他AML/CFT対策を講じていないVASPを使ってこうした活動を続けている。資金洗浄を終えると、制裁回避主体は多くの場合、暗号資産を特定法域に集中して存在するOTC（店頭取引）ブローカーを使って不換紙幣に換える[44]。ケースによっては、北朝鮮がOTCブローカーに、換金した資金を北朝鮮のために物品を購入するフロント企業が保有する銀行口座に送るよう指示することもある。前述のとおり、北朝鮮が不正に入手したUnionPayデビットカードを使って盗んだ暗号資産を換金した不換紙幣預金を受け取ることもある。

ボックス23. ケーススタディ：資金洗浄に使われたミキサーの制裁対象指定

2023年11月、OFACは北朝鮮のための資金洗浄に関与したSinbad.io（シンドバッド）を含む複数のミキサーを制裁対象に指定した。[45]シンドバッドは、北朝鮮が支援するハッカー集団、ラザルスグループの重要なマネー・ローンダリング手段として機能した。シンドバッドは注目を集めたHorizon Bridge、Axie Infinity、Atomic Walletからの窃取を含め、ラザルスグループが盗んだ数百万ドル相当の暗号資産を処理した。シンドバッドはBlender.ioと同様、ビットコインブロックチェーン上で活動し、出所や目的地、取引相手を隠す手段で手当たり次第に不正取引を手助けしている。

出所：米国

43 https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=375771
44 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html
45 XXXXX

ボックス24. ケーススタディ：北朝鮮に関する刑事訴追及び関連執行措置

2023年4月、米国司法省（DOJ）は、暗号資産を使った北朝鮮のための資金獲得を目的に計画されたマネー・ローンダリング共謀における役割を理由にした、北朝鮮のフォーリン・トレード・バンク（FTB）の代理人に対する2件の起訴を明らかにした。被告はOTCトレーダー2人と共謀し、盗んだ暗号資産を洗浄した後、その資金を使って北朝鮮政府に代わり香港に拠点を置くフロント企業を通じて米ドルで物品を購入したという。

このほか、OFACは、この被告が一部は米国企業がIT開発業務のために知らずに採用した北朝鮮労働者に由来する数千万ドル相当の暗号資産を受け取ったとしている。IT労働者は雇用されると暗号資産での支払いを要望し、不正入手した資金を北朝鮮に環流させる複雑なローンダリングの仕組みを介して給与の大半を送ることが知られている。当該FTB代理人は、おそらくIT開発労働者から資金を受け取った後、OTC暗号資産トレーダーにその資金を複数のフロント企業に送るよう指示し、フロント企業はタバコや通信機器などの物品を北朝鮮に代わって購入し、不換紙幣で決済する。こうした活動は、OFACと司法省、連邦捜査局の継続的な連携の証である。この活動では、違法行為を根拠に当該人物を制裁指定している大韓民国とも密接に協力した。

出所：米国

暗号資産と資金獲得

82. 複数の国が、北朝鮮は暗号資産窃取とサイバー攻撃を使って世界中でWMD・弾道ミサイル計画などのための資金を獲得していると指摘している。北朝鮮とその関係主体はこうした活動を実行するにあたり、多くの場合、VASP、DeFiサービス、ブロックチェーンブリッジ開発事業者、暗号資産取引会社、暗号資産に投資するベンチャーキャピタルファンドなど、ブロックチェーン技術・暗号資産業界の組織を標的とする。

83. 2024年、国連有識者会議は北朝鮮に関する報告において、2017～2023年に暗号資産関連会社に対して行われた北朝鮮によるものであることが疑われる計58件、総額およそ30億ドル相当のサイバー攻撃を調査し[46]、北朝鮮政府に代わって世界でサイバー攻撃が実行されていることを指摘した。Chainalysisによると、2023年、北朝鮮と紐付いたハッカーがDeFiのプラットフォームからおよそ4億2,880万ドルを窃取したほか、中央集権型サービス（窃盗額1億5,000万ドル）、取引所（3億3,090万ドル）、ウォレットプロバイダー（1億2,700万ドル）を標的にした。[47]各国は、北朝鮮がITサービス労働者を資金獲得（場合によって賃金を暗号資産で受け取る）と制裁回避のために不正に派遣しているとも指摘している。北朝鮮主体は前述セクションで説明した手口を駆使し、暗号資産で得た収益を洗浄する。

46 S/2024/215

47 Chainalysis 2024 Crypto Crime Report (Page 44-46) Case Study DPRK's Atomic Wallet exploit.（Chainalysis 2024年暗号資産犯罪動向調査レポート（44～46ページ）北朝鮮によるAtomic Walletの悪用）

ボックス25. ケーススタディ：サイバー利用窃盗・不正行為

2021年2月、司法省は、一連の破壊的サイバー攻撃の実行、複数の金融機関と企業から13億ドルを超える資金と暗号通貨の窃取・強要、複数の不正暗号通貨アプリの開発と展開、ブロックチェーンプラットフォームの構築と不正販売など、幅広い共同謀議に関わった疑いで北朝鮮のコンピュータープログラマー3人を起訴した。

起訴内容によると、3人の被告は北朝鮮の軍事諜報機関、総参謀部偵察局（RGB）傘下の組織のメンバーであり、違法ハッキングを行った。[48]こうした北朝鮮の軍事的ハッキングユニットは、サイバーセキュリティコミュニティーでは、ラザルスグループ、Advanced Persistent Threat 38（APT38）など、複数の名前が知られている。

起訴内容によると、共同謀議によって報復又は資金獲得を目的に米国内外で幅広い犯罪的サイバー攻撃が行われたという。このスキームには不正暗号通過アプリの開発と展開、暗号通貨会社を狙った暗号通貨の窃取、スピアフィッシング活動、マリーン・チェーン・トークン、ICO、イニシャル・コイン・オファリングなどが含まれるという。

起訴に含まれる申し立てによると、3人の被告はRGB傘下組織のメンバーであり、北朝鮮政府によって中国やロシアなどの他国に派遣されていたこともある。3人はサイバーセキュリティ研究者らがラザルスグループやAPT 38と呼ぶRGB傘下組織のメンバーであると同時に、起訴内容によれば、これらのグループはデータや金銭への攻撃又は窃取、あるいは北朝鮮の戦略的、金銭的関心に応じた行為を引き起こす単独の共謀罪に関わった。

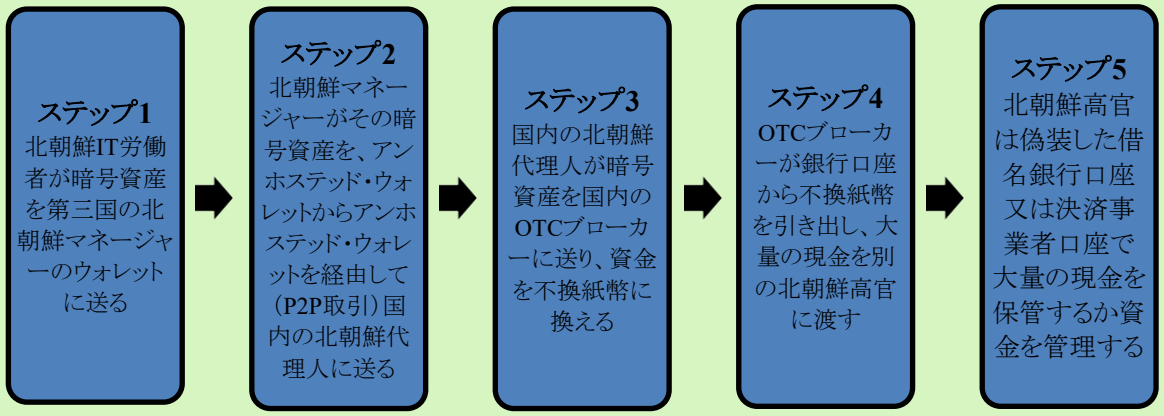
財務省及び司法省は、中国国籍者2人についても、暗号通貨取引所をハッキングして得た1億ドル相当を超える暗号通貨の洗浄の罪で摘発した。訴答書面によると、2018年に北朝鮮の共同共謀者が暗号資産取引所をハッキングし、約2億5,000万ドル相当の仮想通貨を窃取した。盗んだ資金はその後、資金を追跡する法執行を防ぐために数百の自動化暗号通貨取引を経て洗浄された。訴答書面にはこのほか、2017年12月から2019年4月にかけて、2人の被告人が主に暗号通貨交換所へのハッキングから得た1億ドル相当を超える暗号通貨を洗浄したと記されている。OFACは、ラザルスグループに対して重大な支援を行ったとして、2人の被告を制裁対象に指定した。

出所：米国

48 国連安保理決議第1718号リスト上、RGBはKPe.031として指定されている。

84. このほか、北朝鮮は数千人のハイスキルIT労働者を世界各国に派遣し、自国のWMD・弾道ミサイル計画の資金を得ている。こうしたIT労働者は、ソフトウェア・モバイルアプリ開発など、特定のITスキルに対する現在の需要を巧みに利用し、アジア、欧州、北米など世界中のクライアントからフリーランスの委託契約を獲得している。北朝鮮のIT労働者は多くの場合、世界を拠点に働いているとするか、北朝鮮ではないテレワーカーを名乗る。ファシリテーターの身元を使ってプロジェクトを獲得した北朝鮮のIT労働者は、プロジェクトを下請けに出し、自分の身元や居場所をさらにわからなくすることもある。資金は、仲介者の利用やBO情報の曖昧化（類型1及び2を参照）など、さまざまな制裁回避スキームを使って北朝鮮に送られる。暗号資産も北朝鮮への送金に使用される。

ボックス26. 事例：北朝鮮 IT労働者の不正資金本国送金プロセス



収益性の高い事業を隠すための北朝鮮 IT労働者と結託した外国の団体及び個人による不正行為

85. このほか、北朝鮮のIT労働者は外国の個人や企業を引き入れ、資金獲得のための制裁回避スキームにおいて自らの関与を隠そうとする。以下のケーススタディのうち一つは、資金の調達と移動のために日本企業が北朝鮮と関わりのあるIT労働者に狙われた事例、もう一つは、米国籍の者が北朝鮮 IT労働者を手助けするために資金洗浄となりすましを含むスキームに関与した事例である。

ボックス27. ケーススタディ：北朝鮮 IT労働者との実入りの良い取引関係を隠すための不正スキーム

2024年3月、IT関連企業の社長を務めていた韓国籍の者と元従業員が不正行為その他の罪で逮捕された。被疑者らは記録を改ざんし、ある日本企業からオンラインプラットフォームを通じて発注されたアプリを開発するよう中国を拠点にしていると思われる北朝鮮 IT労働者に依頼したことが捜査により判明した。これに関わる資金が北朝鮮のWMD計画に使われる可能性があり、その場合は国連安保理決議第1718号に反するため、この行為は制裁回避スキームを手助けする目的ではないかとの疑いが持たれている。

2024年9月、日本人2名が、北朝鮮 IT労働者であることが疑われる人物と結託して禁止されたFX取引用「自動取引システム」を使用した罪と、違法な顧客データベース登録と口座開設を行った罪で逮捕された。被疑者らには、この不正FX取引から得た資金を北朝鮮に送金した容疑もかけられている。

出所：日本

ボックス28. 米国司法省、ナッシュビルの仲介役を告訴、逮捕し、北朝鮮のリモートIT労働者を使った不正スキームにメスが入る

2024年8月、米国司法省（DOJ）は通貨代替物の洗浄共謀罪及びWMDを含む北朝鮮の不正兵器計画のための資金獲得を目的としたその他複数の罪に問われている米国籍の者1名の起訴状を公開した。法廷文書によると、被告は、米国企業のリモートIT作業要員として海外のIT労働者を斡旋する仕組みに関与した。米国企業は米国を拠点に働く人員を雇い入れたものと思っていた。IT労働者たちは実際には北朝鮮国籍であり、ある米国市民から盗んだ個人情報を使ってこのリモートIT職を得ていた。

法廷文書によると、被告は2022年7月から2023年8月頃にかけて、ナッシュビルの自宅で「ラップトップファーム」を運営していた。被害企業はノートPCを被告の自宅住所の「Andrew M.」宛てに送り、ノートPCを受け取った被告は不正なリモートデスクトップアプリをダウンロード、インストールし、被害企業のネットワークにアクセスしてコンピューターに被害を与えた。このリモートデスクトップアプリによって北朝鮮 IT労働者は中国の拠点から作業でき、被害企業には「Andrew M.」がナッシュビルの被告自宅で作業しているように見えていた。

被告が運営していたラップトップファームとつながりのある海外のIT労働者には、2022年7月から2023年8月頃にかけて25万ドル以上の作業代金が支払われ、その大部分が、米国に実在する個人情報を盗まれた人物の名義で米国内国歳入庁と社会保障局に虚偽申告されていた。

被告及び共謀者らの行為は、被害企業に自社のデバイス、システム、ネットワークの監査、是正費用として50万ドルを超えるコストも発生させた。

被告及び共謀者らは被害企業から支払いを受けるための金融取引を通じて資金洗浄を行い、その資金を被告と海外の口座に送った。いずれも違法行為を遂行し、その結果得た資金の送金を隠すことが目的である。海外の口座には北朝鮮及び中国の主体に関係する口座も含まれる。

出所：米国

類型4：海事・海運セクターの悪用

86. 国際海事機関（IMO）の定義によると、シャドーフリート又はダークフリートとは、「[…]制裁の回避またはその他違法行為を目的に違法活動に従事する船団[…]」を指す[49]。海運セクターは従来から不正主体の一番の標的であり、その複雑さ、国際的活動範囲、匿名性、AML/CFT/CPF措置の不備が利用されている。海事業界には膨大な数の船舶、港、物流、国際規則から成るネットワークが関わり、不正主体による制裁回避又はPFを支える資金獲得に悪用される可能性がある。FATF基準は海事セクターを対象にしていないが、複数の加盟国がこのセクターを、国のPFリスク評価上、重要な脆弱性であると指摘している。その意味で、海事保険の仕組み、海事会社、オープン・レジストリー、商品取引業者、デュアルユース品製造者を含め、海事セクターのさまざまな側面や活動が、制

[49] International Maritime Organisation, “Urging Member States and All Relevant Stakeholders to Promote Actions to Prevent Illegal Operations in the Maritime Sector by the “Dark Fleet” or “Shadow Fleet,” (Dec. 6, 2023).A 1192 33（国際海事機関（IMO）「加盟国及びすべてのステークホルダーに海事セクターでのダークフリート又はシャドーフリートによる違法活動対策を強く呼びかけ」（2023年12月6日）A 1192 33）

裁回避又はPFリスクにさらされる可能性がある[50]。

87. 不正主体はさまざまな虚偽の海上輸送手口を駆使して船舶やその出発港と目的港をごまかし、活動の本当の性質を隠して検知を回避する。一部重複する手口もあるが、手口は主には4つ（船舶識別、瀬取り、AIS（船舶自動識別装置）送受信の無効化・偽装、文書偽造）に大別される。ただし、PFや制裁回避スキームの実行を試みる不正主体は、目的を果たすために複数の手口を使うこともあるため、注意が必要である。

船舶識別情報の改ざん

88. 類型2で説明したとおり、不正主体は実質的支配者情報を隠して制裁スキームを回避し、正規の金融システムにアクセスしようとする。海事セクターにおいては、不正主体が商船を違う船舶として通過させるために船体を物理的に改変したり、真の所有者や活動を隠すために識別情報を不明瞭にする場合がある。例えば、船舶名の上にペンキを塗ったり、偽名の旗を立てたり、一意のIMO船舶識別番号を変えたりして船舶の物理的識別情報を細工することもある。商船を物理的に改変し、識別情報をわからなくすることによって不正主体は匿名性を手に入れ、その船舶を使った違法行為の履歴を隠す。以下のケーススタディでは、対北朝鮮国連安保理決議を逃れるために船舶の識別情報を改変した事例を説明する。

50 APG（アジア・太平洋マネー・ローンダリング対策グループ）事務局は、加盟国の相互審査準備を支援し、地域の新しいリスクに対応するため、国連薬物犯罪事務所の協力を得て、「Shipping Registries and PF Risk Factsheet:Asia / Pacific Group On Money Laundering」（海運レジストリー及びPFリスクファクトシート：アジア・太平洋マネー・ローンダリング対策グループ）を公表した。

ボックス29. ケーススタディ：海事セクターにおける違法石炭による資金獲得

2022年、インドネシア海域を巡視中のインドネシア当局がPetrel 8を拘束した。コモロ船籍のばら積み貨物船、Petrel 8は、違法石炭を北朝鮮に輸送したことを理由に、2017年に国連制裁リストに追加されている。この事案は、インドネシア当局と国連第1718号制裁委員会との連携に基づきインドネシア外務省（MOFA）がインドネシアFIU（PPATK）に情報提供を求めた結果、国際協力を通じて検知されるに至った。

捜査の結果、当該船舶はインドネシアの海運会社PT Lintas Bahari Nusantaraがバンク・セントラル・アジアの融資を受けて日本のUYO Co. Ltdから推定50万円で購入したことが判明。当初の捜査では北朝鮮との直接的な金融的結びつきは見つからなかったが、北朝鮮のための継続的な制裁回避に関与していたことから船舶を拘束した。発見を防ぐために、船舶の識別情報を細工し、偽名の旗を使うなどの手口が使われていた。船舶はおよそ610億ルピア（400万USドル）で購入され、北朝鮮への石炭輸送に使用されていた。Petrel 8の取得には、インドネシア企業から日本企業への資金移動も絡んでいた。

この事例は船舶所有者の変更と密貿易の監視における脆弱性を浮き彫りにし、制裁回避を防ぐために国際協力を強化する必要性を明らかに示している。2023年の国連第1718号制裁委員会との協議を経て、さらなる制裁回避活動を防ぐためにPetrel 8の廃船処分の決定が最も効果的な解決策とみなされた。

出所：インドネシア

瀬取り

89. 瀬取りは洋上において船から船へ船荷を積み替えることを言う。瀬取り自体は合法的な作業であるが、不正主体が積荷の出所又は目的地をごまかす意図でこの方法を悪用することがあり、制裁回避の観点からリスクが高いと指摘されている。瀬取りが行われると、政府当局が制裁品を追跡し、国際制裁違反を見つけることが難しくなる。さらに、透明性が失われることによって、海上保険会社が違法瀬取りに関与する船舶に対してそうとは知らずに外航貨物海上保険を提供する可能性もある。

90. ある法域からの報告によると、北朝鮮は石油精製製品の瀬取りを行うことができる少なくとも28隻のタンカー船団と少なくとも33隻の石炭輸送船団を動かしているという。北朝鮮が関与する瀬取りは、多くの場合、金融機関を介さない現金取引を行い、PF・制裁回避リスクに対する脆弱性がさらに増す。以下のケーススタディでは、不正主体が瀬取りを利用して禁輸品を輸送し、制裁を回避し、検知を逃れるために真の出発地と目的地を隠す事例を詳しく説明する。

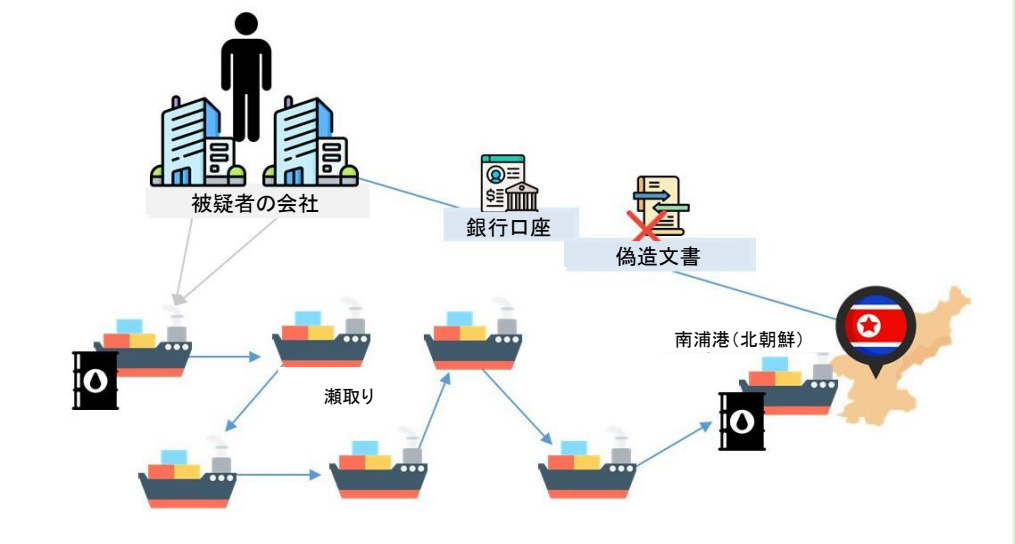
ボックス30. ケーススタディ:海事セクターを利用した北朝鮮への軽油供給

申し立てによれば、2019年後半にある人物が海外の別の5人と共謀し、船舶「MT Courageous」を使った7回にわたる瀬取りを経て、およそ1万2,260メートルトンの軽油を北朝鮮に供給した。最初の6回は洋上で、最後の1回は北朝鮮の南浦港で積み替えを行うことによって供給を成功させていた。同申し立てにより、シンガポールの対北朝鮮国連制裁、及び国連安保理決議第1718号制裁レジームへの違反が疑われる。

被疑者は北朝鮮への軽油の購入・供給代金の支払いを円滑に行うために自らが取締役を務めていた会社の銀行口座を4回にわたって使用したとして告訴されている。また、会社に帰属する書類を2回偽造し、北朝鮮への供給が禁止された軽油の販売代金を受け取るために自らが支配する別の会社の銀行口座を5回にわたって利用したとも言われている。さらに、被疑者は捜査官に嘘の供述をし、証拠を処分し、2019年2月に別の船舶で北朝鮮に軽油を供給したことを警察に言わなかったとされる。

その結果被疑者は、北朝鮮への禁輸品の供給、虚偽口座の使用、犯罪行為からの利益の獲得、司法妨害、禁止取引の非開示など、複数の嫌疑を受けている。また、被疑者が取締役を務めていた最初の会社はシンガポールの対北朝鮮国連規則に反する禁止行為に加担した可能性のある4回の金融資産の移動について、2番目の会社は5回の犯罪収益の獲得について摘発された。

現在も公判手続きが続いている。



出所:シンガポール

ボックス31. ケーススタディ：公海上での北朝鮮船舶への石油積み替え

2017年1月から2022年10月にかけて、台湾の検察官が北朝鮮による制裁違反に関して11件の事案を捜査した。[51]PFに関して最もよく使われる手口は、公海上で台北の石油会社が管理する第三国籍の船から北朝鮮籍の船に石油を積み替えるか、最終的に北朝鮮の船に再販する目的で第三国籍の船に石油を積み替える方法である。

石油製品は今なお台湾の国連制裁違反者が取引によく用いる商品である。台湾法に基づき、公海上での石油取引は違法ではない。外国籍者を含む海運会社の代表者又は実質的所有者、その他仲介業者、複雑な事業構造、ブローカーが関わる表向きには合法の取引が、洋上での瀬取りによって石油の不正な積み替えをわからなくしてしまう。虚偽の輸出情報も使用され、資金の追跡努力を妨げるべくオフショアの会社と口座が使用される[52]。

出所：台湾

AIS送受信の無効化と不正操作

91. AIS（船舶自動識別装置）は船舶の識別情報と位置情報を送受信し、船舶局による動静の追跡を可能にする洋上追跡装置である[53]。不正主体はAISから発信される船舶名、IMO番号、その他一意の識別情報を含むデータを改ざんし、船舶の航行情報を隠すことがある。さらに、シャドーフリートもしばしばAISの送受信を無効化し、まさに「姿を消して」船舶の動静の追跡を止めさせる[54]。

92. 各国から報告され、かつ国連安保理決議第2397号（2017年）に示されるとおり、北朝鮮籍又は北朝鮮が支配、チャーター、操業する船舶は、国連制裁措置を回避し、歴史的に同国のWMD・弾道ミサイル計画に注がれている資金を獲得するために、AIS応答装置を意図的に無効化又は不正操作している[55]。以下のケーススタディでは、対北朝鮮の国連安保理決議違反となる、民間船舶で見つかった北朝鮮で採掘された石炭の発見、拿捕、没収に関して、2件の事例を詳しく説明する。

51 5件は有罪判決、3件は無罪判決が下され、3件は不起訴となった。

52 テロ資金供与対策法第9条1項1号の主観的要素として、相手が制裁対象者であることを「知りながら」取引した被疑者の故意が必要であり、仲介者の介入がこの要素の証明を困難にしている。

53 （国際海事機関（IMO）「船舶自動識別装置の船上利用に関する改定ガイドライン」（2015年12月2日）A 1106 29）

54 IMOは、国際航海に従事する総トン数300を超えるすべての船舶と、大きさを問わずすべての客船に対して、AISの使用を義務付けている。

55 国連安保理決議第2397号

ボックス32. ケーススタディ：北朝鮮で採掘された石炭の船上での発見、拿捕、没収

カンボジアは、2件の事例において北朝鮮が民間船舶を使用して石炭輸出を支援させていたことを明らかにした。これらの行為を禁じた国連安保理決議第2397号及び第2375号の違反に該当する。いずれの事例でも、船舶及びその積み荷は差し押さえられ、被疑者は(1)カンボジアへの不法入国と、(2) カンボジア税関領域への物品密輸を試みたとして、有罪判決を受けた。

カンボジアは国連の義務に従い、対北朝鮮国連制裁措置への違反のおそれがある公海から持ち込まれる物品と入港する船舶を日常的に捜査、調査している。積み荷を隠すためのAISの操作、位置の偽装、瀬取りなど、船舶が積み荷の出所をごまかすために不透明化の手口を用いることもある。直近の2件の船舶拿捕の事例は、違法な積み荷の出所を隠すために北朝鮮籍船舶が使用する手口を示している。

1つめの事例では、2024年2月にカンボジア当局が内燃機船（M/V）「HJL」を拿捕した。当該外国籍船舶は、北朝鮮海域に近づくと、AISの送受信を切った。翌日、当該船舶のAISはHJLが停泊していることを示す位置を示したが、実際には偽の名前で航行を続けていた。HJLがカンボジア領海内に進入した後、カンボジア当局は、疑わしい船舶の情報共有を行っている他の法域の協力を得て、当該船舶を拿捕した。こうした国際協力が北朝鮮で採掘された石炭鉱石1万2,000トンを積んでいたHJLの拿捕につながった。船舶はカンボジア領海に進入したところで停泊し、そこでバイヤーと会っていたとされる。服務規程に従い、積み荷を理由に、検察庁がさらなる捜査と審理のために当該船舶と積み荷を凍結した。

2024年5月の2つめの事例では、4,800トンの石炭鉱石を含む、国連が禁止する積み荷が関わる瀬取りを北朝鮮海域で北朝鮮籍船舶と行ったことを理由に、カンボジア当局が内燃機船「CNI」を拿捕した。その後の捜査の結果、CNIが第三国の物流会社が手配した船舶であること、その会社が北朝鮮で採掘された石炭鉱石を輸入しながらも、書類を偽造して出所を隠していたことが明らかになった。

出所：カンボジア

93. 上記2つの事例が示す脆弱性は、国際水域と地理的に近い場合は特に、各国が監視頻度の増加、巡視隊の配置、領海内の追跡システムの強化を検討する必要があることを浮き彫りにしている。

書類の偽造

94. 積み荷の出所や目的地を隠すための別の手口としては、偽造書類の使用がある。北朝鮮から又は北朝鮮に物品を輸送する際、特にデュアルユース品の輸出時に使用される。この場合、不正主体は出発後に積み荷の輸送書類を改ざんし、実際の最終目的地を隠す。この手口には、拡散団体が多かれ少なかれ直接的に支配する第三国のシェルカンパニーが関わることが多い。税関当局と荷送人から見ると、シェルカンパニーは積み荷の正式な荷受人である。ところが、積み出し後、スポンサーが輸送書類を変え、積み荷の目的地をPFと関係する高リスク法域へと変える。

95. これは、北朝鮮が関わる書類の偽造行為に加え、別の場所で制裁と輸出管理逃れのためによく用いられる手口である。以下のケーススタディでは、不正主体が輸送プロセスの初期段階で輸送書類を改ざんし、デュアルユース品の輸出をごまかす方法を説明する。

ボックス33. ケーススタディ:デュアルユース品の輸送に関する証券及び申告書の偽造

2021年、UAE連邦原子力規制庁(FANR)は、許可申請プロセス中にデュアルユース品を含む疑わしい積み荷を発見した。UAEのフリーゾーンに本社を置く会社Xは、価額がおよそ2万5,000USドル(9万5,040 UAEディルハム)のインバーターの輸出について3件の許可申請を提出していた。インバーターはUAE輸出管理リストの対象品であり、デュアルユース品に分類されている。会社Xの提出書類には船荷証券と売り渡し・購入証(BSP)が含まれていたが、売り主の提供情報に記載された情報と積み荷の原産国との間に矛盾があった。書類によると、これらの品目の目的地は高リスク国であった。

LEAの捜査の結果、会社Xが偽造船荷証券を提出したことが判明し、これには自らが荷送人であると申告されていたが、BSPには売り主としてT国に所在する別会社の名が記載されていた。さらなる捜査の結果、LEAは、売り主とされる会社が主にナッツの取引を行っており、その事業が貿易取引と一致していないと判断した。その後の捜査によって、当該品目は実際にはH国からUAEにその売り主が輸入したものであることがわかった。会社XはU国に複数の支社を有するとの偽造書類を提出して当局に事実誤認させ、イランの核開発計画に対して課された制裁措置を回避しようとした。

LEAはUAEFIU、CBUAE、EOCN、連邦税関当局、FANRと協力して犯罪・金融捜査を行った。会社X敷地内の物的調査の結果、会社Xは高リスク国にあるインバーター売り主のフロント企業として運営されていることが判明した。UAEFIUとCBUAEは会社Xに関わる合計残高3万4,000 UAEディルハム(9,500USドル)に上る3つの銀行口座を特定し、凍結した。さらに、税関からは、BOを隠す目的で作成された輸出入の下請け当事者に関するすべての偽造書類がLEAに提出された。

FANRは積み荷に関する専門報告書を作成してLEAに提出し、当該品目がUAE輸出管理リストに掲載されたデュアルユース品であることを確認した。税関当局は積み荷を押収し、LEAはその凍結命令を出した(9万5,040UAEディルハム(2万6,000USドル)。

出所:アラブ首長国連邦

ボックス34. ケーススタディ：輸出国が定める輸出法に基づくデュアルユース品の申告漏れ

2020年、インド税関当局はパキスタンに向かうアジア籍船舶を拿捕した。インド当局は捜査の過程で積み荷がデュアルユース品であることが書類上申告されていなかったことを確認した。インド当局の捜査員は、積み荷が高感度高エネルギー材料のほか、ミサイル用モーターの断熱、化学コーティングに用いられるオートクレーブであると認定した。センシティブ品目はインドを含む複数の法域が参加するミサイル技術管理レジームのデュアルユース輸出管理リストに含まれる[56]。

押収した積み荷の船荷証券は、輸入者と長距離弾道ミサイル開発に関与する国家開発コンプレックスとのつながりの証拠である。

出所：インド

56 複数の当局から正式な許可を得ずにこれらの装置を輸出した場合、現行法及び協定への違反となる。

5. セクション3.PFリスク低減における課題と模範事例

SAR/STRと制裁スクリーニングによる検知

96. PF・制裁回避手口を検知するにあたり、各国はSAR/STR義務と堅牢な制裁スクリーニングの突合に大きく頼っている。こうした手法を補い、グローバル規模で不正行為を効果的に見つけて対処するには、これ以外にも、国境を越えた情報の共有、各機関の連携、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などの手段がある。

97. 多くの国が、PF・制裁回避スキームを検知し、複雑かつ変化する手口を見つけて対処するには、確実なSAR/STR義務の履行が頼りだと報告している。さまざまな国内の法的枠組みや通報義務が報告事業体にSAR/STRの申告を義務付けていることがあるが、それはより幅広くPF・制裁回避に関係しているためである。複数の国が、報告事業体の義務の範囲には徹底した顧客管理の実施、法規制の遵守、高リスク国が関わる取引の監視、疑わしい取引が見つかった場合のSAR/STR義務の履行などが含まれていると述べている。

SAR/STR及び制裁スクリーニングによるPF・制裁回避の検知に関する模範事例

98. このほか、複数の国がSAR/STRの有効性を高めるために報告事業体の義務として内部ポリシー及び手順を含む自動化制裁スクリーニングシステムを組み込むことを求めている。制裁スクリーニングシステムに国際、国内の制裁リストを組み込むことによって、報告事業体は個人や団体に合致していることを確認でき、高リスク取引、制裁対象個人、団体、活動に関わるキーワードを使用できる。国によっては、スクリーニング中に見つかった明らかな検出が、SAR/STRを提出し、制裁に基づく凍結資産や制裁対象団体に紐付く取引について当局に情報提供を行うなど、報告事業体によるその後の義務の履行のきっかけになることもある。以下の2つのケーススタディでは、SAR/STRを発端にした捜査について説明する。

ボックス35. ケーススタディ：ネガティブニュースクリーニングとSAR/STRによってデュアルユース品の違法購入を発見

2つのフランス系企業が米国製デュアルユース電子部品購入の仲介者として機能した。当該部品は、一連の団体を通じて米国の制裁対象に指定されるロシア企業に再販された。

この事案は、民間セクターと協力していたフランス当局によって検知された。TracFinが該当個人と団体（当該団体のUBO）を狙いにした「警戒の呼びかけ」を発行した後、ロシアに関するネガティブニュースと銀行から寄せられたSAR/STRのモニタリングを行っていた。TracFinの呼びかけには、夫がOFAC SDNに指定された後1カ月もしない間に当該団体のうち一社のマネージャーに指名された当該個人の妻も警戒対象に含まれていた。

捜査は各機関の強い協力のみならず、資本逃避を防ぎ、捜査を終えるまで今ある資金を事実上使用できなくするための関係銀行との定期的なフォローアップなど、金融機関との円滑な連携を必要とした。

出所：フランス

99. 複数の国が、法令遵守を支え、検知能力を高めるために、官民連携を通じた教育研修、アウトリーチ、専門ガイダンス、仕組みのモニタリングにリソースを投じている。その意味で、助言書、ガイダンス、国又は国際的に特定された指標の公表が、報告事業体が制裁回避やPF活動の疑いを検知し、義務を果たすために具体的なSAR/STRを提出する手助けになる。一部の国は、規制対象事業体にこれらの助言書や注意喚起に基づくSAR/STRの届出を義務付ける形で国内の法的枠組みを定め、検知能力のさらなる強化を図っている。

ボックス36. ケーススタディ：FIのSAR/STRの届出を円滑化する詳細な注意喚起の発行

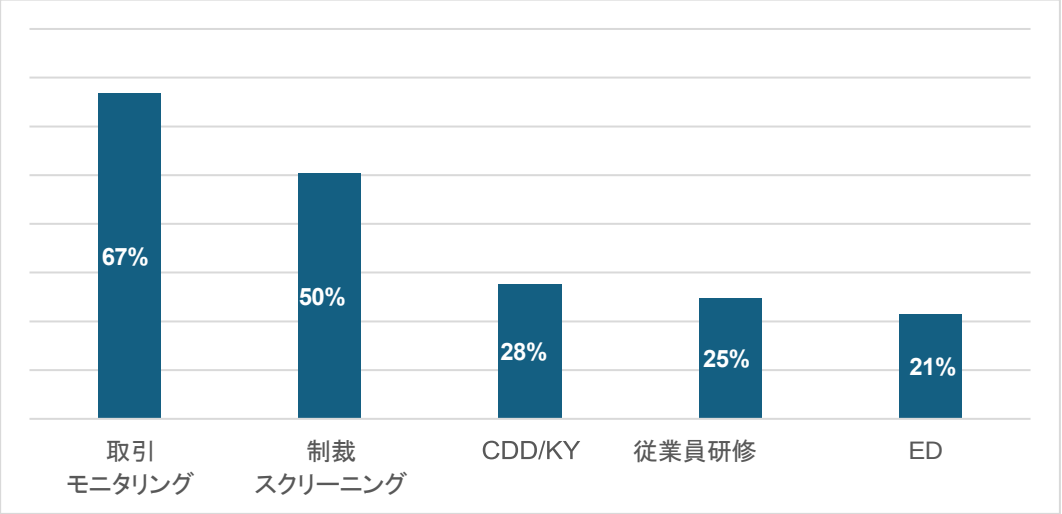
BISとFinCENは、ロシア及びベラルーシに関する米国輸出管理回避に関わる金融機関からのSAR/STRの届出を円滑化するため、2022年共同注意喚起を発行した。その内容は、BISの現在の輸出規制の概要、輸出管理回避が懸念される商品リスト、輸出管理回避が疑われる取引の金融機関による特定を助ける取引又は行動に関する警戒信号例など、金融機関に対する情報提供である。また、FIがSAR/STRを届け出る際にキーワードとして「FIN-2022-RUSSIABIS」を使用するよう求めた。

2023年11月には、この注意喚起を拡大し、世界の輸出管理回避に関する警告信号を説明したBIS・FinCEN共同注意喚起が改めて発せられた。この注意喚起では、SAR/STRを届け出る際にキーワードとして「FIN-2023-GLOBALEXPORT」を使用するよう求められた。FIから届出のあったSAR/STRは、グローバル輸出に関するキーワードを使ったものより、ロシアに関するキーワードを使ったものの方が多く、その主な理由としては、ロシア及びベラルーシに課された輸出規制の方が幅広いことや、情報を受け取るFIにとって関連する可能性のある金融取引の方が見つけやすいことが考えられる。

出所：米国

100. FATFのパブリックコメントに回答した民間セクター事業体の多くが、制裁回避・PFに関するリスクを低減する最善策は、顧客管理、包括的リスク評価、制裁スクリーニングツール、SAR/STRの届出に至る可能性がある継続的なモニタリング、従業員研修、ポリシー・手順、ネガティブニューススクリーニング、厳格な顧客管理（EDD）などの主なAML/CFT予防策に紐付けられると答えている（民間セクターが挙げた模範事例については図3を参照）。また、貿易に関わるマネー・ローンダリング対策、リアルタイムのアラート、先進テクノロジーソリューションも重要性が高い手段として挙がった。その一方で、堅牢な情報共有の仕組みがなければ、民間セクターが標準的なリスク管理プロセスで複雑なPF・制裁回避スキームを検知するのは難しいかもしれない。

図3.制裁回避検知の模範事例



SAR/STR、制裁スクリーニングによるPF・制裁回避の検知における課題

101. およそ3分の1の国がPF検知の手法にSAR/STRを使用しているとは答えなかった。相当な数の国がPFを犯罪としていないため、この点が一部の国がSAR/STRをある程度しか利用していない理由かもしれない。PFを犯罪行為としていない国がSAR/STRの中でPFを見つけるよう報告事業体に求める可能性は低い。それでも報告事業体がPF主体に関するSAR/STRを届け出る可能性はあるが、こうした不正行為の検知の複雑性に関する詳しいガイダンスがなければ、SAR/STRとPF活動を紐付ける重要情報が抜け落ちてしまうかもしれない。

102. また、制裁リストを国のSAR/STR枠組みに組み込み、スクリーニングツールを活用することは、PF・制裁回避の疑いの検知において重要な役割を果たすことができる。一部の国は、制裁スクリーニングの照合に課題があると指摘する。個人又は団体を誤検出したり、一般キーワード検索に基づく無関係な情報を抽出した経験があるからだ。また、合致させるには生年月日、氏名、別名、複数のバリエーションの名前、名前の読み方又は綴りの違い、パスポート番号など、複数の識別子を必要とするため、照合アルゴリズムは誤検出が起きやすい。ただし、EDDや、会社登記やBO情報などのオープンソースインテリジェンスの使用、他のデータベースを使った情報の裏付けなど、緩和策もある。

103. 各国からは、指定非金融業者及び職業専門家（DNFBP）の間でPF義務の理解や法令遵守が広がっていないことについて別の課題が指摘された。DNFBP団体の多くはPF関連活動の監視や報告における自らの責務を認識していない。[57]一部の国では、これが、当局が金融機関以外のセクターでPF活動を検知するのが難しい原因になっていることもある。一方で、民間セクターの事業体は、セクターを問わず、該当のSAR/STRに関して公的セクターからのフィードバックがなく、この課題に対処することが難しいと回答している。

その他の検知手法

104. SAR/STRや制裁のスクリーニング照合を補うこれら以外の検知方法として、クロスボーダーインテリジェンス、各機関の連携、国際協力、モニタリングツールを通じた情報共有などが挙げられる。各国が複数の検知情報源を使って不正金融・回避スキームを包括

57 FI、DNFBP、VASPによるリスク低減策について詳しくは、2021年FATF PFガイダンス、セクション2「PFリスクの低減」を参照。

的に捉えることが多い点に注意が必要である。

105. 多くの国が、PF関連活動、特に高リスク国や高リスク交易路との結び付きの発見と捜査に税関当局と越境インテリジェンスが重要な役割を果たすと回答している。税関当局は地域又は国際機関と協力して、捜査、税関申告、輸出入データ、許認可申請に関する情報交換を行い、拡散資金供与者の制裁回避に関わる疑わしい違反行為の検知、捜査の改善を図ることができる。こうした情報交換は検知能力の向上につながり、違反疑いの捜査を助けることができる。特に、この領域の主な活動は、高リスク国への資産の流れ、防衛材料、戦略的物品、デュアルユース品を含む物品の動きと外国貿易活動の分析と監視である。インテリジェンスの共有と法令遵守を徹底するための法域ごとの規制枠組みは、PF・制裁回避に関する違反行為の疑いの検知において税関当局が果たす重要な役割を強調するものである。

上記以外の検知策を使ったDF・制裁回避検知の模範事例

各機関の連携

106. 多くの国がPF・制裁回避の検知における各機関の連携の重要性を指摘している。特に、LEAによる捜査と他の管轄当局との情報交換は、国内の機関、共同捜査、啓発活動からの事案照会に至ることもあり、指定個人及び団体の資金・資産の金融の流れを明らかにする手助けになり得る。インテリジェンスの収集と、これを補う捜査活動は、PF・制裁回避が疑われる事案の特定、検知に必要な部門横断的アプローチである。

ボックス37. ケーススタディ:規制されたデュアルユース品の輸出に関する各機関の連携

2017年、FINTRACはカナダの法執行機関から自主的な情報提供を受けた。カナダの電子機器会社が規制対象のデュアルユース品を組み込んだ回路の出荷に関与した疑いがあるという。

SAR/STRによると、当該企業の取引活動がロシア・東欧の資金洗浄スキームを示唆するいくつかの主要な属性と一致した。あるSAR/STRに含まれていた情報は次のとおりである。

- 資金の出所は複数の地位の高い人物
- 人物の所在地はロシア、アゼルバイジャン、その他東欧諸国
- 複数の地位の高い人物が資金洗浄を目的にシェルカンパニーを設立
- シェルカンパニーはタックスヘイブンの国で登記
- 資金はタックスヘイブンの国のシェルカンパニーを通じて送金
- デュアルユース品の積み替え又はその他違法金融活動におそらく仲介国が関わり(複数の欧州諸国を含む)、当該企業はそこから資金の電子送金を受けた。原産国が電子資金送金を依頼した事業体の記載住所と合致しないケースもあった。また、当該企業はロシアの住所の個人及び団体が依頼した電子資金送金の受取人であった。

SAR/STRには、当該企業の資金は株主への複数の支払い小切手と、オンライン決済処理会社への電子資金送金を介して使い尽くされていることが示されていた。

当該企業に関するFINTRACの情報開示の影響を尋ねたところ、カナダの法執行機関は、情報開示をきっかけに新たな捜査を開始し、これまで知られていなかった新たな対象者が明らかになったと回答し、FINTRACの情報開示と協力が、関与するネットワークを把握し、事案の法執行全般を成功させる重要要因になったと語った。FINTRACから提供された情報がパートナー国における正式起訴につながったとも述べている。

出所:カナダ

107. このほか、一部の国は、動向、類型、指標を含むガイダンス文書の公表が疑わしい活動の検知に欠かせないと指摘している(国内連携・協力のセクションを参照)。

国際協力

108. PF・制裁回避のグローバル性を考えると、インテリジェンス又は情報共有を通じた国際協力は検知と防止の重要手段である。効果的な検知策には、国内当局と海外のパートナーとの協調的アプローチが必要である。例えば、FIUはエグモント・グループ(Egmont Group)を通じて情報共有を行うことができる。Egmont GroupはFIU間の情報共有を円滑化し、PF又は制裁に関わる疑わしい金融活動の検知を強化する重要な役割を果たしている。また、国際協力によって国際貿易の動きに伴うリスクを各国が体系的に分析でき、国のリスクプロファイルの強化に役立つ。

監視ツール

109. 監視ツールもPF・制裁回避の検知に重要な役割を果たす。こうした監視ツールで

はオープンソースインテリジェンスなどさまざまなデータソースと、高度なブロックチェーン手法を活用する。管轄当局はオープンソースインテリジェンスを使って、例えば会社登記、実質的所有者情報、衛星画像、地理空間データなど、幅広い情報にアクセスでき、不正主体ネットワークの発見に役立てられる。

110. 複数の国が、ブロックチェーン解析ツールも制裁回避やPF活動の検知に有用であると指摘している。暗号資産の使用は検知の複雑さを高めるが、パブリックブロックチェーン上で運営される暗号資産取引は追跡が可能である。ブロックチェーン解析によって監督当局は資金の流れを監視、追跡し、疑わしい活動を見つけ出し、暗号資産における一部の不透明化を抑えることができる。詳しくは、類型3（暗号資産及びその他テクノロジーの利用）を参照。

その他の検知手法を通じたPF・制裁回避の検知における課題

111. 回答国からは、制裁プログラム、これに関わる多岐にわたる制裁対象団体リスト、国の法的要件、さまざまな執行規則の法域ごとの違いなど、検知における複数の課題が指摘された。もう一つの大きな課題として、北朝鮮が金融サービスの提供や大量の現金輸送を含む制裁対象の資産や資源の輸送を外交官に手助けさせている点がある。北朝鮮は規制や捜査手段を逃れるために外交特権を悪用する。多くの国が、実質的所有者情報の収集や入手可否にばらつきがあることを懸念する。その結果、PF・制裁回避の検知が複雑化する（詳しくは、類型2及び「脆弱性」のセクションを参照）。

捜査・訴追

112. FATFの報告書「Combating PF: A Status Report on Policy Development and Consultation in 2010」（2010年[58]拡散金融対策：政策策定・協議に関する現状報告書）の公表以降、PF・制裁回避の防止及び撲滅のための法的枠組みは大幅に強化された可能性があるが、2025年時点で効果的な捜査・訴追事例はいまだ乏しい。2010年FATF報告書で説明されているとおり、PF事案の訴追の難しさはいくつかの課題に起因し、例えば、PFが犯罪とされていないこと、PF事件の証拠収集、PF活動の国際性、不正行為を隠すための金融仲介者の使用、実効性に欠けた輸出管理枠組み、広く受け入れられたWMD PFの定義の欠如、及び、国際協力を含め、このトピックに対する法域ごとのアプローチの違いなどが挙げられる。FATFグローバルネットワークからの回答を踏まえると、共通する主な課題の多くが、複雑なPF（と制裁回避）事案の円滑な捜査、訴追を阻害しているようである。

捜査の手法と仕組み

PF捜査の模範事例

113. 多くの国が、効果的なPF・制裁回避捜査は金融犯罪事案に標準的に用いる手続きと、協力先機関との協力にかかっていると回答している。SAR/STRは金融活動における異常なパターンを見つけ、把握するうえで重要な情報である。SAR/STRの活用は、制裁回避や不正行為に関わる企業と個人とのつながりを明らかにする助けにもなる。

114. 一部の国は、これ以外の重要な捜査手段として、検知の回避に悪用されることもある暗号資産の追跡を挙げている。捜査官はブロックチェーン解析を通じて、たとえ少額であっても資金を辿ることができ、金融パターンや関係団体・個人とのつながりを明らかにできる。

58 拡散金融対策

115. 金融データ上のパターンや異常な活動を見つけ、PFを抑制するうえで高度な解析が重要な役割を果たす。これらのツールは捜査官が団体同士のつながりを明らかにし、制裁回避に関与する人又は組織のネットワークを見つける助けになる。例えば、高度な解析は口座、取引、当事者を結び付けるリンク解析を助け、違法ネットワークの運営実態が明らかになる。リアルタイムの監視ツールは、疑わしい活動が検知された際に当局のいち早い行動を可能にする。金融機関や税関記録、インテリジェンスレポートなど複数の情報源から得たデータを組み合わせることも捜査の有効性と完全性を高める。これらのツールは資金源を隠すために匿名性を高める技術が使用された場合の異常な取引パターンの発見や検知にも有効である。この情報を当局間で共有することによって、PFとの闘いにおいてツールがより大きな効果を発揮する。

116. いくつかの国が、秘密捜査官や秘密の情報源を活用するなど国際犯罪組織（TCO）や薬物密売人の捜査と同じ手法を検討する重要性を指摘している。

ボックス38. ケーススタディ：核物質密売人に対抗するための秘密捜査官と秘密の情報源

2024年2月21日、米国司法省（DOJ）と米国麻薬取締局（DEA）は、ミャンマーから他国への核物質密売人ネットワークと共謀した罪で被告に優先起訴状を発行したと発表した。この共謀において、被告と共謀者らはタイで麻薬・兵器密売人を装っていたDEAの秘密捜査官（「UC-1」）に核物質サンプルを見せた。タイ当局の協力により核原料サンプルは押収され、その後、米国の法執行機関の監視下に移管された。後日、米国の核犯罪科学研究所がサンプルを分析した結果、当該サンプルにウランと兵器級プルトニウムが含まれていることが確認された。

被告と共謀者は2022年4月にも国際的な麻薬密売罪、銃器犯罪で起訴されており、いずれも留置命令が下されていた。

優先起訴状に含まれる申し立てによると、被告は2020年の初めからUC-1とDEAの秘密の情報源（「CS-1」）に対し、自分は大量の核物質を入手でき、売りたいと伝えていた。同年後半、被告はUC-1に岩のような物質と放射線量を測定するガイガーカウンターが写った一連の写真のほか、写った物質にトリウムとウランが含まれることを示すラボ解析のページを送った。被告からの繰り返しの問い合わせに応え、UC-1はDEAの捜査の一環として、核物質を核兵器計画に使う目的のイラン人将官（以下、「将官」）を装ったUC-1の仲間に売るために被告側のブローカーを助けることに同意した。被告はその後、将官にその目的ならウランよりもさらに「良い」、より「強力な」「プルトニウム」を提供すると申し出た。

核物質の入手に関する話し合いの最中、被告はさらにミリタリーグレードの兵器を購入したいとUC-1に持ちかけた。そこで2021年5月、被告はUC-1に地対空ミサイルを含む兵器リストを渡し、ミャンマーのある反政府民族グループ（「CC-1」）のリーダーに代わりUC-1から購入したいと伝えた。被告は別の共謀者2人（「CC-2」「CC-3」）とともに、UC-1に対し、CC-1の兵器購入資金としてCC-1が被告を介し将官にウランを売るよう持ちかけた。

2025年1月8日、被告は、ウランと兵器級プルトニウムを含む核物質のミャンマーから他国への密売を共謀した罪と、国際的な麻薬密売と銃器に関する容疑を認めた。

出所：米国

117. 最後に、多くの国が、専門タスクフォースや専門家作業部会を立ち上げるなど、定期会合を通じた各機関の連携の重要性を指摘している。金融機関、税関当局、LEAが協力することによって、捜査を強化し、先回り的に資産を凍結し、PF・制裁回避に関わる輸送を差し止めることができる。

ボックス39. 法域での事例：PF・制裁回避を撲滅するための専門タスクフォースと作業部会

- **フランス：**TracFin（金融情報機関）が率いる専門タスクフォースが制裁対象のロシアの団体に電子部品を供給していた2つの会社（事業体A1、事業体A2）の捜査を行った。この2社は仲介者として機能し、購入した部品を第三国の別会社を経由して制裁対象グループに移送していた。タスクフォースにはTracFin、金融機関、法執行機関が参加した。銀行から届出のあったSAR/STRを分析し、両社の金融の流れを監視し、実質的所有者の関与を追跡した。こうした協調的努力の結果、両社の資産を凍結し、事業を差し止めとした。
- **インドネシア：**作業部会が国連制裁措置に反して北朝鮮への石炭輸送に関与していたばら積み貨物船、Petrel 8の捜査を行った。タスクフォースには外務省、税関当局、FIU（PPATK）が参加した。金融インテリジェンスと輸送記録を組み合わせることによって、インドネシアの会社が所有し、過去にも同様の活動で制裁が課されていた船舶を突き止めた。タスクフォースは米国制裁委員会とも連携し、船舶は拿捕し、最終的には解体された。

出所：フランス、インドネシア

PF捜査の遂行における課題

118. PF捜査は通常、マネー・ローンダリング（ML）やテロ資金供与（TF）の捜査とはさまざまな意味で異なっている。PFではWMD計画を支援する資金活動に注目する。多くは制裁回避のためにフロント企業、貿易、複雑な所有構造を利用する強力な国家主体又はグループが関与する。違法資金の出所を隠すMLやテロに資金を提供するTFと違い、PFの捜査は輸出管理や制裁措置の潜在的違反行為に関するインテリジェンスに頼るところが大きい。PFの方が、捜査が困難な場合もある。他の2つと比べてリスク意識が低く、多くの場合、違法目的で使用される合法の物品（規制対象品を含む）が関わるからである。捜査官にはより強力な国内・国際協力とPF事案を解明するための高度な解析ツールが必要であり、これらはML又はTF事案で通常必要とするものよりも複雑であることもある。

119. 多くの国が、フロント企業や多層化された所有構造、小規模で頻繁な取引を使ったPFスキームなど、同じような課題に直面していると申告する。こうした手口によって、正確なデータと強力な連携が頼りのLEA、規制当局、金融機関、FIU、検察官などのステークホルダーにとって、実質的所有者や複雑なスキームに関わる組織の追跡が非常に難しくなる（類型2参照）。

120. もう一つの課題が金融機関や規制された事業体でのPFリスク、動向、手口に関する認識が不足している点だ。SAR/STRの質を高めるためのPFリスク研修も不十分である。本報告書の前段で述べたとおり、多くの国がPFを犯罪としていない。PFに関するSAR/STRの件数と質が不足している理由の一つはこの点にあるかもしれない。

121. さらに広く見ると、政府機関や民間セクター事業体でのリソース不足も多くの国にとって課題である。特に、小規模国は複雑な事案を取り扱う資金もノウハウも十分でないことがある。優先順位の問題かもしれず、それが官民セクターでのリソース配分に影響している。国によっては、PF行為を訴追するためにPFを含む主たる罪を立証する場合や、付随的な罪を使う場合もあるかもしれないが、一貫した犯罪化アプローチを備えた国の不足がPF関連事案の捜査と訴追における国際協力の阻害要因になっている可能性がある。

122. 最後に、越境事案には他国との協力が欠かせないが、認められる証拠を検討する際のルールの違い、金融犯罪の定義の違い、双罰主義がないことなどの法制度の違いが、越境捜査の遂行に難題を突きつけている。国同士に情報共有の協定がなければ、捜査のための情報提供依頼が大きく遅れたり、拒まれたりする可能性がある（国際協力セクションを参照）。

訴追その他の手法

PF事案の訴追に関する模範事例

123. 多くの国が、複雑なPF・制裁回避事案の訴追は捜査よりもさらに複雑であると申告している。PF・制裁回避事案を首尾良く訴追に持ち込むには強力な法的枠組みが必要であり、これにはPF及びその関連行為を定義付けた明確な法と、証拠の収集能力、法廷での提示能力も含まれる。

124. 捜査機関と検察官との協調的な努力も揺るぎない立件には欠かせない。前例からの学びと、PF・制裁回避の犯人が使用する類型や新しい手口についての知識が、捜査の成功確度を高め、ひいては訴追の成功にもつながる。さらに、グローバルでのパートナーシップもPF事案の訴追に重要な役割を果たし、こうした複雑な犯罪に対処するうえでの国際協力の価値を明確に示している。最後に、国から流出する資金については特に、没収と財産回復に関する本格的な規則を整備することで訴追につながりやすくなるかもしれない。

PF事案の訴追における課題

125. 多くの国が複雑なPF・制裁回避事案の訴追が難しいと申告している。一部の国は、規制品又は禁輸品が制裁対象法域に送られたことを証明する証拠集めの難しさを指摘する。証拠に関わる課題を克服できない場合、検察官は司法妨害罪や偽造罪などPF犯罪を隠すための余罪で犯罪者を追及することがある。外交特権が特定のPF又は制裁回避事案の追及の制約になるとの指摘もある。

126. 各国が直面するもう一つの課題として、金融活動がPF又は制裁回避と直接関係していることの証明が挙げられる。特に証拠が複数の国に広がっている場合に難易度が増す。証明には詳細な文書と強力な国際協力が必要であり、こうした複雑な事案では必ずしも容易ではない。

127. 国同士の情報やインテリジェンスの共有は、法執行上の相違をやわらげる手助けになり、各国は越境事案により効果的に対処し、PFネットワークによるグローバル金融システムの脆弱性の悪用を防ぐことができる。しかしながら、多くの国にこうした仕組みが欠けている。

128. 訴追の成功には教育研修や意識向上の活動も欠かせないが、多くの金融機関、企業、あるいは検察官でさえも、PFのリスクや複雑さの理解が不足している。適切な教育研修は、疑わしい活動に気づき、PFスキームの機能を理解するうえで有用であり、PF事案の取り扱いに関してリソースやノウハウが限られた国においては特にこれが重要である。

制裁違反を阻止するためのその他の手段

129. このセクションですでに概説したとおり、政府機関がTFS違反の刑事訴追を検討する場合がある。このほか、PFに関するものを含め、TFS違反行為の救済として別の執行の選択肢を検討する国もある。多くの国が複雑な拡散金融・制裁回避事案の訴追に著しい課題を抱えているようであり、その他の手段の追求は然るべき状況において検討の価値があるかもしれない。

ボックス40. 法域での事例：刑事訴追の補完又は代替としての民事・刑事執行措置

- **欧州委員会：**2024年4月24日付けEU指令2024/1226では、すべての加盟国の自然人に対する刑事罰及び法人に対する刑事又は非刑事罰の共通基本基準を定める新しいルールが導入され、これまでの法的な抜け穴を解消するとともに、何よりもEU制裁措置違反の抑止効果が高まった。[59]
- **英国：**金融制裁違反は犯罪行為とみなされる場合があり、有罪の場合は最長7年の懲役刑が下される。金融制裁違反の救済措置には民事と刑事両方の執行選択肢がある。法執行機関は金融制裁違反に対して訴追を検討する場合もある。2017年法に基づき構築された罰金制度が、金融制裁法違反に対して刑事訴追に代わる手段を提供し、財務省が管轄する金融制裁執行局（OFSI）が罰金を科す[60]。
- **米国：**OFACの捜査・執行機関は民事のみに対応し、DOJ、DHS、商務省がこの領域で行使する刑事制裁執行権限とはまったくの別物である。必要に応じた執行措置では、堅牢かつ有効な制裁遵守プログラムの重要性を強調し、特に複雑な国際取引に関わる企業に対して制裁回避スキームへの関与を防ぐための対策の徹底を呼びかける。
- 2023年4月、タバコ・シガレットメーカーのブリティッシュ・アメリカン・タバコ（BAT）は、OFACの対北朝鮮及びWMD拡散国制裁措置違反の疑いについて民事責任の解決金として5億861万2,492ドルの支払いに同意した。タバコ及び関連製品の輸出とその輸出代金の受領において、BATは米国の金融機関に、制裁対象北朝鮮銀行の封鎖された財産利益を含む電信送金の処理と金融サービスの輸出、北朝鮮へのタバコ輸出の手助けをさせた[61]。

---

59 新しいルールには、すべての加盟国において制裁措置違反の刑事捜査と刑事訴追を可能にする狙いがある。これにはEU制裁措置の違反及び回避に関する犯罪行為の一覧が含まれ、例えば、資産凍結の不履行、渡航禁止・武器禁輸の違反、禁止又は制限された経済・金融サービスの提供、凍結すべき資産の第三国への移転、凍結すべき資産を隠すための虚偽情報の提供などが挙げられる。EU制裁措置の対象となる収益、手段、資産の凍結及び没収に関する強化されたルールも含まれる。さらに、加盟国内又は加盟国間の管轄当局やその他関係EU機関、団体、事務所、当局との協力とコミュニケーションの強化も新しいルールの狙いである。

60 Financial sanctions enforcement and monetary penalties guidance - GOV.UK（金融制裁の執行及び罰金に関するガイダンス - GOV.UK）

61 法廷文書によると、BAT Marketing Singapore（BATMS）は、コロンビア特別区で申告された犯罪情報について、BATとBATMSが共謀して銀行不正を働き、IEEPAに違反した罪を認めた。BATは同じ罪に関して訴追猶予の合意を締結した。

- 2022年4月、OFACは、オーストラリアに本社を置く国際貨物フォワーダー・物流会社のToll Holdings Limited（Toll）と、北朝鮮、イラン、シリアが関与する取引の処理を含む複数の制裁制度違反の疑いについて和解合意を結んだ。Toll社の法令遵守機能に十分なリスク管理とデュー・ディリジェンスがなかったことが大きな弱みとなった[62]。

出所：欧州委員会、英国、米国

国内連携・協力

各機関の協力の仕組み

130. 実効性のある各機関の協力の枠組みは複雑な拡散金融・制裁回避スキームに関するリスク低減に有用である。実効性のある各機関の協力の枠組みを構築するには、関係政府機関同士の継続的な協力と連携が必要であると各国が指摘している。多くの国にとって、関係主体にはAML/CFT/CPF当局者、LEA、監察官、裁判官、輸出入管理・許認可当局、税関、国境管理、インテリジェンス機関などが含まれる。各国はこれら管轄当局の密接な協力と連携が該当情報の遅滞のないやり取りを円滑化すると述べている。こうした各機関の協力プロセスを通じて、政府機関はTFSレジーム違反その他該当のPF活動の疑いに対して捜査を開始し、遂行するための最善の態勢を整えることができる。

各機関の協力の模範事例

131. FATFグローバルネットワークからの回答によると、各国は3つの重複カテゴリーのいずれかに該当する各機関の協力の仕組みを活用してPF・制裁回避に対処している。1) PF-TFSを含むTFSに関する一般的連携、2) PF-TFSと輸出管理規則に特化した連携、3) PF-TFSと輸出管理規則に特化した連携と、複雑な拡散金融・制裁回避事案の捜査、訴追、その他手段を開始するためのより幅広い連携）。

132. FATF勧告7に基づき、FATFグローバルネットワークには、PFに関するすべての国連安保理決議に従うため遅滞のないTFSの実行が義務付けられている[63]。多くの国はPF-TFSを実行するための法的枠組みを整備していると答えており、それには多くの場合、TFSに関する既存の各機関の協力の仕組みを活用することが含まれる。この種の各機関の協力の仕組みがあることによって、各国は勧告7に示されたTFSの潜在的な違反・不履行・潜脱に対処するための最低限のルールベースの要求事項を満たすことができる。

---

62 同社は海上、航空、鉄道輸送に関して同社のグローバルユニットが受け渡すか受領するおよそ3,000件の支払いを米国の金融機関を通じて行い、米国の制裁対象であるか、国連もしく米国の制裁国に居住する個人又は団体に利益を与えた。同社の法令遵守機能は、該当期間の半分以上、さまざまな事業部門に広がるおよそ600件の代金請求、データ、決済、その他のシステムアプリケーションを含め、自らの事業の複雑さに見合ったポリシー及び管理策の検討を怠った。執行措置の結果、Toll社の米国制裁措置の遵守に関してある銀行が懸念を示し、その後同社は2016年6月に米国制裁対象国とのすべての取引を中止し、リスクへの晒されやすさの低減を図った。ところが、同社は制裁対象の個人又は団体が関わる決済を防ぐための法令遵守ポリシー又は手順を導入せず、国連又は米国の制裁対象法域に居住する人物が関わる輸送であるかどうかの検査もしなかった。

63 各国は、国連憲章第7章に基づき国連安全保障理事会が指定するか又はその権限下にある個人又は団体もしくは自らの裁量で当該個人又は団体の代わりに活動する個人又は団体、ないしは当該個人又は団体が所有するか支配する個人又は団体の資金又はその他資産を遅滞なく凍結し、当該個人又は団体に対して直接的又は間接的にもしくは当該個人又は団体の利益のために供される資金及びその他資産がないようにしなければならない。ただし、指定された個人又は団体の代わりに活動するか、その管理下にある者、もしくは当該個人又は団体に所有又は支配された者は国家的・超国家的制裁レジームに基づき指定されることはない。

ボックス41. FSRB事務局の例：GAFILATによる加盟国を対象にしたTFS凍結の模擬演習

GAFILAT（ラテンアメリカ金融活動作業部会）は加盟国を対象に、FATF基準に従ったTFSの実行に関して各機関の協力プロセスをテストする模擬演習を実施している。GAFILATが構築した手法とマニュアルに従い、加盟国はTFS能力と管理の仕組み（官民セクターに整備された仕組みを含む）をテストするためのシナリオに対処する。

この模擬演習は、加盟国に自国のTFSシステムの弱みと強みを見つけるための実用的な手段を提供することが目的である。演習後、GAFILATは参加加盟国にフィートバックと助言を伝える非公開報告書を提供する。2024年以降、GAFILATは3つの加盟国に対してTF-TFSプロセスが関わる3回の模擬演習を実施した。今後は、残りの加盟国に対してPF-TFSプロセスにフォーカスしたセッションを含め、さらに模擬演習を続ける予定である。

出所：GAFILAT

133. デュアルユース品に関しては、輸出管理当局が多くの市販品の輸出管理を担っている。これらは商用と軍事又は拡散用途の両方で用いることができる「デュアルユース品」と呼ばれることも多い。[64]多くの国は国連安保理決議第1718号に従ったTFS義務以上の対策を講じ、PF・制裁回避に対する幅広いリスク管理手段として輸出管理規則を優先的に実行している。

ボックス42. 法域での事例：輸出管理規則を取り入れた各機関の協力の仕組み

- **インド：**PFに関して運営とポリシー上の連携を目的とした複数の仕組みが構築され、例えばSCOMET（特殊化学品、有機体、素材、設備、技術）の許認可についての省庁間作業グループ（IMWG）などがあり、デュアルユース品及びその関連事項の輸出許認可申請を検討している。このほか、2005年インドWMD法に基づいて構築された複数機関の連携メカニズムは、IFU-Indiaが議長を務め、規制当局、法執行機関、その他関係組織が参加する[65]。

64 国家安全保障、外交政策、供給不足、核不拡散、ミサイル技術、化学・生物兵器、地域の安定、犯罪防止、テロの懸念などの特定の状況においては、デュアルユース品の輸出には許可が必要である。許可の必要有無は、その品目の技術特性、目的地、最終用途、最終使用者、その他最終使用者の行為による。許可を必要としない場合でも、これ以外に輸出前に満たすべき要求事項が定められていることがある。以下2つの事例では、PF・制裁回避に関する輸出管理規則に特化した事例を説明する。

65 WMD法の該当規定に従い、WMD及びその輸送システム、核及び核関連品目、化学兵器及び関連品目、生物兵器及び関連品目、デュアルユース品の輸出管理に関する国内の各種諮問員会が定期的に会議を招集する。この会議には、WMD法その他WMD、その輸送システム又は関連するデュアルユース品及び技術に関する該当のインド政府法の関連規定に関わる政策及び関連事項を検討するため、インド政府の関係組織が参加する。

- **シンガポール**：省庁間輸出管理委員会（IMC-EC）がシンガポールの輸出管理枠組みを監督する。これにはWMDの拡散とPFに関する政策及び運用上の問題も含まれる。IMC-ECの議長は外務省が務め、関係する政策・法施行機関が参加する。IMC-ECはこのほか、該当の国連安保理決議に関するシンガポール国内での実施状況を監視し、WMDの拡散又はPFに関する情報又はインテリジェンスを受け取った場合は省庁間フォローアップの調整役を担う。

出所：インド、シンガポール

134. 本報告書の前段で述べたとおり、こうした幅広いWMD拡散リスクとそれを支える資金供与の理解は、PF-TFSの潜在的な違反・不履行・潜脱リスク（すなわちFATF基準で取り上げられている狭義のPFリスク）の理解を助け、リスクベースの対策とTFSの実行に役立つ可能性がある。このような観点から、以下の事例では複雑なPF・制裁回避の捜査、訴追、その他手段を開始するにあたっての幅広い連携を取り上げている。

ボックス43. 法域での事例：幅広いPFリスクに対処するための各機関の協力の仕組み

- **日本**：警察庁と財務省が共同議長を務めるマネロン・テロ資金供与・拡散金融対策政策会議の下、財務省と金融庁が「共同検査」を実施する。この共同検査では、それぞれの監督官庁の検査官の知識と検査情報の共有、さらには金融機関による該当法規制の効果的かつ効率的遵守徹底の観点から、財務省の外国為替検査と金融庁のAML検査を共同で実施する。さらに、海上自衛隊（JMSDF）の船舶又はその他資産が国連安保理決議で禁止されている瀬取りなどの不正海事活動が疑われる行為を検知した場合、防衛省は関係省庁に情報を提供する。
- **マレーシア**：マレーシアのCPFレジームの複数機関による協力・連携を補うものとして、主に2つの関係機関間グループがある。一つは投資貿易産業省の戦略的貿易管理官（STC）が議長を務める戦略的貿易活動委員会（STAC）で、もう一つはマレーシア国立銀行が議長を務める国家マネー・ローンダリング対策連携委員会（NCC）である。STACの主な任務は、戦略的品目及び技術の輸出、通過、積み替え、仲介を規制する2010年戦略的貿易法（STA 2010）の執行である。多くの場合、PF事項に関する執行機関及び専門機関が参加する。AML/CFT/CPFに関する省庁が参加するNCCは、ML/TF/PF対策に関わる国の戦略の策定、実行、監視に責任を負う。
- **米国**：輸出管理法法令執行課（商務省産業安全保障局（BIS）に設置）はFinCENの銀行秘密法（BSA）データにアクセスでき、輸出コミュニティと協力して刑事罰、行政罰を裏付けるための捜査を行っている。一方で、BISは2018年輸出管理改革法（ECRA）の権限の下、輸出規制（EAR）を通じてデュアルユース品、特定軍需品、市販品に関する輸出管理を運営し、執行する。BISは違反行為を防ぎ、捜査を実施するにあたって輸出コミュニティと協力し、犯罪罰、行政罰を裏付ける証拠集めを行う。このほか、FinCEN、OFAC、米国の法執行機関とも密接に協力し、PF、制裁回避、輸出管理制度の回避を通じた違法な調達を監視している。

出所：日本、マレーシア、米国

各機関の連携における課題

135. 各国からは円滑な国内連携に対するさまざまな阻害要因が指摘されたが、多くの課題は、PFリスクに対処するにあたっての全般的な理解や賛同がML、TFリスクと比べて不足している現状に紐付けられている。PF・制裁回避ネットワークは多くの場合、その裏に国家主体の存在があることから、インテリジェンスコミュニティとの定期的コミュニケーションが必要であり、巧妙な会社構造を解明して制裁回避スキームに対処するには実用的な情報を入手できることが重要である。

136. 一方で、一部の国は、情報アクセスを制限する海外相手国が関わる場合など、インテリジェンス共有の阻害要因を指摘している。こうした課題は、PF主体又はPF活動に対して速やかな措置を講じるための情報と選択肢をタイムリーに共有するにあたって、事態を複雑にする。ある法域では理解不足がPFの優先順位付けに影響しており、関係当局がそのトピックに注目し、関係情報を共有し、政府間照会にタイムリーに応じるプロセスを困難にしている[66]。

137. 一部の国は、PF・制裁回避スキームに伴うリスクに適切に対処するにあたって関係するリソース、知識、経験、技術が足りていないと申告している。FATFグローバルネットワーク加盟国の多くがこの10年、FATF基準に則したPF対応のために専任リソースを設けて法的枠組みを更新してきたが、PF関連対策の効果的な実行が大きく改善されるには至っていない。2025年4月時点で、第4次相互審査報告書の対象となった194カ国のうち半数以上（54%、105カ国）がR.7適合（13%（26カ国）又は概ね適合（41%、79カ国）である一方で、この105カ国中、IO.11の有効性が高い又は十分と評価された国はわずか24%（25カ国）に止まる。全体では、評価対象国のうちIO.11の有効性が高い又は十分と評価された国は17%（194カ国中32カ国）である（図1、図2参照）。

138. 一方、勧告1の文脈で見た場合、勧告7に示されたPF-TFSリスクを特定し、評価し、理解する義務は、PFのリスク評価を実施する世界的努力を底上げしており、これが今後の有効性の改善につながるかもしれない。半数以上の国が過去5年内にPRリスク評価又はNRAのPFの章を実行したと報告している一方で、およそ4分の1の国が初回PFリスク評価を実施中であり、2025年までにプロセスが完了する見通しだと答えている。

官民セクター間の情報共有

139. 官民連携（PPP）は、ステークホルダー間の連携強化において価値あるプラットフォームになり得る。こうした連携には、政府が民間セクターの窓口と有益な情報（類型、回避指標、模範事例、課題など）を共有する狙いがある。公的セクターから実用的な情報が共有されれば、民間セクターは自社の顧客記録や取引記録を分析し、制裁回避の疑いを含めて現在又は過去の不正行為の可能性を洗い出すための態勢を整えられる。結果として、この種の情報交換によって、公的セクターは顧客のプライバシーを維持する責任を果たしながら、リスクを特定して低減する能力と、民間セクター事業体に対して狙いを絞ったガイダンスを提供する能力を高められる。

140. 多くの国は、情報共有の支えとして、取引や貿易パターンに着目した、PF・制裁回避スキームに関するリスク指標や警告信号を構築し、監視していると回答している（別紙「拡散金融関連」を参照）。また、多くの国は定期的なアウトリーチ活動や啓発活動を通

66 このプロジェクトに関して、一部の国は、関係する情報やケーススタディの共有を制限する当局間の壁に遭遇したと申告している。また、複雑な拡散金融・制裁回避スキームの性質に鑑み、FATFグローバルネットワークの他国に対してインテリジェンスその他の機密情報の機密解除ができないと申告する国もある。

じて官民セクターとリスク指標リストを共有している。しかしながら、半数近くの国は指標や警告信号の構築、管理を行ったとは回答していない。そうした国ではPFリスク指標とその他金融犯罪との区別がされていないか、複雑なPF・制裁回避が優先されていないことを示唆しているかもしれない。多くの国はPF・制裁回避活動の検知をSAR/STRに頼っていることから、官民セクターの情報の隔たりが防止策の効果的な実行を妨げている可能性がある。

公的セクターでの模範事例

141. およそ3分の1の国がTFSの法的枠組みの実行を通じた民間セクターへのアウトリーチ活動に専念していると回答した。SAR/STRの受領や、遅滞なきTFSの実行などが含まれる。一方で、同じ数の国がさまざまなPPPを通じて必ずしもPFに特化することなく官民セクターの連携強化を図っていると回答している。ただし、その場合はPF及び制裁回避に関する問題を話し合える作業部会その他の仕組みが設けられている。一部の国は、財務省、FIU、規制当局が参加するだけでなく、法執行機関とインテリジェンス機関が主導する民間セクターへのアウトリーチ活動も行っていると回答した。

ボックス44. 法域での事例：PF・制裁回避に関する公的セクターから民間セクターへのアウトリーチ活動

- **フランス：**中央銀行が管轄する銀行業及び保険監察官と財務省を通じて、民間セクターに情報提供し、情報交換する「啓発」の仕組みが設けられている。官民セクターの情報交換の主な対象者は、金融機関のほか、DNFBPや人道支援活動を行う非営利団体（NPO）を含む、リスクに最もさらされやすいと考えられるセクターの実務担当者である。FIUがフランス国内の金融機関（銀行、クレジットカード会社）と適宜会議を開き、その中で拡散金融のテーマを取り上げることもある。これらの報告事業体は、2023年に届出のあったSAR/STRの52.6%を占め、当局にとって最も重要な存在である。この会議には2つの目的がある。1つは認識の向上、もう1つはPF対策枠組みにおいて銀行が直面する可能性のある弱点と課題の対処である。TRACFINが国内大手銀行との一連の会議を主催してPFに関する理解を深めてもらうと同時に、PF事案の検知とCPFメカニズムの実行において直面している課題についてフィードバックを収集する。
- **米国：**輸出規制（EAR）を運営し、執行する商務省のBISが、FinCENやその他米国政府機関と協力し、金融機関向けにガイダンスやアドバイザリーを定期的に発行している。こうした公表物では、金融機関が米国の輸出管理の回避に紐付けられる可能性のある取引を見つける際の助けとなる警告信号やリスク指標などが説明されている。最近の公表物では、世界の制裁・輸出管理回避、イランのUAV関連活動、ウクライナ・ロシア紛争がもたらすPF脅威をテーマに取り上げた[676869]。

出所：フランス、米国

67 FinCEN & BIS Joint Notice, FIN-2023-NTC2, November 6, 2023（FinCEN・BIS共同通達、FIN-2023-NTC2、2023年11月6日）

68 Microsoft Word - Iran UAV Industry Advisory - Final For Posting June 9 10AM (003)（Microsoft Word – イランUAV業界アドバイザリー – 最終版、6月9日午前10時投稿（003））

69 FinCEN and Bis Joint Alert for OCC-OGC-FO（OCC-OGC-FOに関するFinCEN・BIS共同通達）

公的セクターにおける課題

142. PF・制裁回避の性質、国家主体が関与する頻度、インテリジェンスの収集を考えると、その多くに公での共有が難しい機密情報が関係することになる。多くの国がPPPの仕組みを整備しているが、その主な目的は一般にSAR/STRの有効活用の改善であり、PF又は制裁回避の問題に特化した連携事例はほとんどない。およそ4分の1の国が民間セクターへのアウトリーチ活動の範囲としてPF・制裁回避関連の問題に関するSAR/STRを受け取っていると回答している。一方で、シンガポールと英国はPF・制裁回避に関する官・民又は民・民間の情報共有の課題を克服するためにPPPを利用している。

ボックス45. 法域での事例：PF・制裁回避に関する情報共有の壁の克服

- **シンガポール：**2024年4月1日、シンガポール金融管理局（MAS）はデジタルプラットフォーム「COSMIC」（Collaborative Sharing of Money Laundering/Terrorist Financing Information and Cases：マネロン/テロ資金供与情報・事案の協調的共有）を立ち上げ、シンガポール国内の大手商業銀行6行との運用を開始した。COSMICによってFIは複数の「警告信号」が表示された顧客情報を互いに安全に共有できる。所定の基準値に達すと警告信号が表示され、金融犯罪の可能性を示すことができる。これによってFIでの犯罪行為の検知が容易になり、その阻止も容易になる。COSMICは現時点で商業銀行業務における3つの主な金融犯罪リスク（法人の悪用、違法目的での貿易金融の悪用、拡散金融）にフォーカスしている。COSMICの目的はFIにおける不正主体の特定と、不正行為又はネットワークを阻止するための速やかなアクションの支援であり、金融システムの法執行と監視を支えることにもなる。
- **英国：**法執行機関（LEA）が民間セクターとのインテリジェンスの共有のために定期的に活用しているのが共同マネー・ローンダリング・インテリジェンス・タスクフォース（JMLIT）である。民間セクターは反対にLEAに情報提供を行う。これにより民間セクターは戦略的類型や手口の脅威を理解することができる。先日は、金融制裁執行局（OFSI）がJMLIT内に制裁回避室を設け、英国系FIが共同議長を務める。

出所：シンガポール、英国

民間セクターにおける模範事例

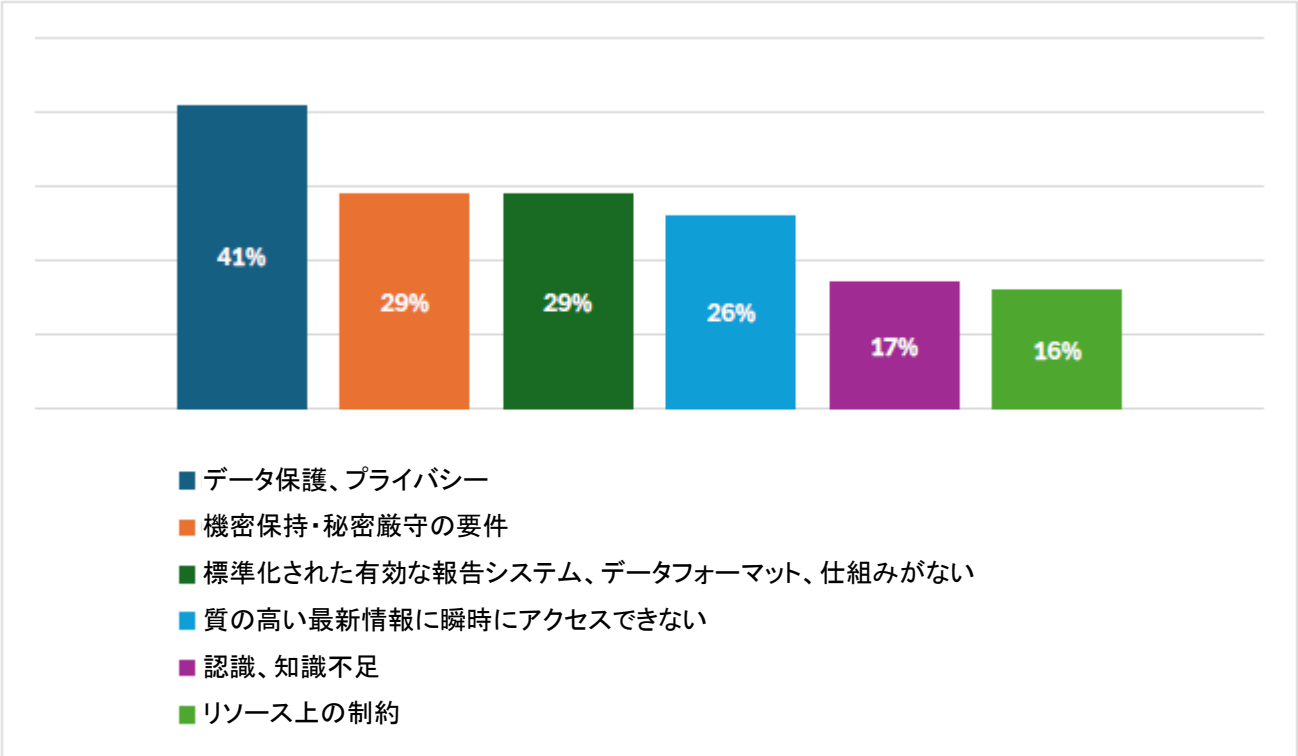
143. 多くの民間セクター事業体が、PPPは官・民又は民・民間のPF・制裁回避問題に関する情報共有の促進に有益な手段であると回答している。一方で、民間セクターが情報共有に関して模範事例よりもはるかに多くの課題を報告したことは注目に値する（以下、「民間セクターにおける課題」を参照）。また、公的セクターが現在のPPPの取り組みを改善し、拡大させるためのいくつかの提案もあった。例えば、民間セクター事業体は、FIU及び法執行機関との情報共有プロセスの合理化、公的セクターからインテリジェンスがタイムリーに共有されるための一貫した方法、他国での官民情報共有を推進するためのより明確な法的枠組み・ガイダンスの整備を求めている。さらに、一部の民間セクター事業体は、セクター間の共有が欠けていることによって情報共有の効果が弱められているとも指摘する。その場合でも、複数の民間セクター事業体がセクター間のPF・制裁回避リスクの話し合いと分析の前進にFATFが有益な役割を果たせると考えている。

民間セクターにおける課題

144. 金融機関、DNFBP、VASPは複雑な拡散金融・制裁回避スキームを防ぎ、抑制するうえで重要な主体である。しかしながら、概して民間セクター事業体はMLやTFに比べてPFの理解が不足している。そのため、現在のPPP事例のほとんどはPF-TFSリスクに関する公的セクターの意識向上、SAR/STRの届出に関する情報提供が主なテーマであり、民間セクターが複雑な拡散金融・制裁回避スキームを見つけて検知するための具体的なステップを学ぶ機会にはなっていないようである。こうした複雑なスキームを見つけ、報告するには、貿易取引や複数の当事者間でやり取りされる大量の情報など、該当行為を評価するためのガイダンスがより多く提供されることが民間セクターにとって有益だと考えられる。関連文書もさまざまな形式や媒体で保管されていることがあり、それらのデータと国際又は国内制裁リストとの照らし合わせが難しい。

145. 多くの民間セクター事業体は、これ以外にも情報提供に関して複数の課題を指摘しており、例えば、データプライバシー規定の実施のばらつき、その他規制当局の制限事項や法域ごとの違い、機密保持又は信用上の懸念、インテリジェンス発信の遅れ、データフォーマットのばらつき、リソース上の制約などを挙げている（図4参照）。特に、民間セクターはデータプライバシーと防止対策の義務とのバランスを取るのが難しいと強調する。また、一部のノンバンク金融機関とDNFBPは、現在のアウトリーチ活動はどちらかと言えば大手銀行業務にフォーカスしており、セクター別ガイダンスの必要性を指摘している。

図4.情報共有における主な課題



国際協力

146. 一貫した執行を促し、不正主体が防止対策の脆弱な国や事業体を標的にする機会を抑えるには、官民セクターはPF・制裁回避に関する法的枠組みに足並みの揃ったアプローチで取り組むことが有益である。TFSの実行など、FATFが定めた基準と、PFの犯罪

化や特定事例における輸出管理の強化なども含まれ得る、各国が採用した基準によって、PF防止に向けた共通の枠組みが作られる。例えば、金融機関の悪用に対して類似した対策を執行している国は、国際金融システムに潜在する脆弱なつながりを抑えることができる。輸出管理と最終使用者確認の標準化を推し進めることによって、機微技術が禁止された用途に転用されるのを防ぎ、それを支える拡散金融を阻止することができる。

147. 国際協力は、暗号資産などの新しい金融テクノロジーに伴う新しい脅威に対処するうえでも極めて重要である。このような状況から、前述のとおり、FATF暗号資産コンタクト・グループはこれまで、暗号資産に関する効果的なAML/CFT/CPF対策の実施について課題や模範事例を集中的に話し合い、特にDNFBPによる暗号資産の窃盗や悪用リスクの高まりを取り上げている。

国際協力に関する模範事例

148. 一部の国は、効果的な国際協力は政府、金融機関、民間セクター主体間のインテリジェンスのやり取りが頼りであると述べている。疑わしい取引、制裁対象団体、高リスク活動に関する情報共有は、PFネットワークや制裁回避者の特定と阻止に有効である。例えば、国境をまたいだSAR/STRの共有は、拡散に紐付いた複雑な取引チェーンの解明に役立つ。多くの国のFIUは、他のFIUとの協定や覚書（MOU）の締結によって、PF活動に関するインテリジェンスを含め、インテリジェンスの交換が可能になると述べている。例えば、FIUの活動を促進するエグモント・グループは160カ国以上の安全なコミュニケーションと連携を支援し、実用的な情報のリアルタイムの共有を可能にしている。

ボックス46. ケーススタディ：規制対象デュアルユース品の輸出に関する国際協力

FINTRACはあるFIUから、その国の金融機関から届出のあったSAR/STRを詳しく説明した自発的情報提供を受けた。90件、総額およそ250万USドルの疑わしい電信送金が報告されていた。自発的情報提供には、別の法域の国家制裁レジーム対象団体が関与するロシア防衛セクター向けデュアルユース品の不正調達を目的とした電信送金が含まれていた。SAR/STRはいくつかの潜在的マネー・ローンダリング指標のほか、そのFIUの法域の指定団体からカナダの事業体と高リスク国の事業体への不正調達活動を目的とした複数の電信送金を特定していた。

FINTRACはその自発的情報提供の評価を行ったうえで、SAR/STRと電子資金送金レポートによってFINTRACに報告された金融活動を詳しく説明した情報開示文書を作成した。情報開示文書には、カナダの団体と、ロシアの最終使用者へのデュアルユース/軍事品の違法輸出が疑われたことからかつて捜査対象になったことがある、関連個人/企業との金融取引などが記載されている。また、SAR/STRには「ロシア・東欧の資金洗浄スキーム」に関する既知のマネー・ローンダリング類型と一致する取引も記載され、カナダの制裁解除後、ロシア事業体との取引が続いていた。

情報開示パッケージには、疑わしい違法調達ネットワークの概要が説明されている。情報開示文書は複数の連邦情報開示受領者とその他のFIUに送られた。

出所：カナダ

149. 法執行における越境協力によって、各国はPF・制裁回避の複雑性と越境性に対処できる。多国間タスクフォースは、ネットワークの捜査と解体において政府機関のリソースと知識の底上げに役立つ。例えば、協調的活動は、WMD計画のための調達と資金供与に従事する拡散ネットワークが使用するフロント企業、仲介者、複数カ国が関わる複雑なルートの解明に効果を発揮する。

ボックス47. ケーススタディ：スペイン国家警察、EUのカウンターパートの協力を得てPFに対抗

スペインは先頃、他のEU加盟国の国際協力を必要とする複数の事案に遭遇した。いずれの事案でも、仲介企業が材料の目的地を隠していた。関与団体は企業ネットワークであり、子会社の一部とマネージャーが他国に所在していた。これ以外にも、活動を助ける「ファシリテーター」、すなわち仲介者が存在した。金融分析の結果、それぞれの事案で検知された主なリスク指標として、異常な販売数量、移転の出所、量の違いが検知された。

一つの事案では、国家警察が、フロント企業と仲介者を介した推定500万ユーロ相当の防衛材料、具体的には軍用機部品のロシアへの転売を捜査した。捜査の結果、関連する支払いと、フロント企業の販売活動による支払いの洗浄が明らかになった。EU加盟国の枠組み内の国際協力によって、陸路と空路を使い、いくつもの国を通過した複雑なルートを経由した積み荷の捜査が可能になった。

別の事案では、国家警察がEU制裁措置に基づき禁止されている80万ユーロ相当を超える化学物質のロシアへの転売を捜査した。これらの物質の一部は爆薬の前駆物質又は化学兵器の前駆物質である。当該化学物質は、輸出に先立ち、スペイン国内の港にあるフリーゾーンに保管されていた。国内では国家警察と税関が共同捜査を実施したが、陸路で輸送が行われたことから、欧州域内の国境をまたぐ材料のルートを捜査するために他国の関係機関の協力を要した。

出所：スペイン

ボックス48. ケーススタディ：米国と北朝鮮のWMD計画に資金供与していたROK制裁主体[70]

2024年3月、OFACは大韓民国（ROK）の協力を得て、ロシア、中国、アラブ首長国連邦に拠点を置き、北朝鮮のために資金を獲得し、金融取引を手助けしていた6名の個人と2つの団体を制裁対象に指定した。これらの主体を通じて獲得された資金は、国連安保理決議第1718号に基づき義務付けられたTFSに反し、最終的に北朝鮮のWMD計画の支援に注がれていた。ROKも、海外の北朝鮮IT労働者を通じて不正資金供与と資金獲得に関与したとして同じ6名の個人と団体を共同で指定した。

70 Department of the Treasury, “Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program,” (March 27, 2024), Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program | U.S. Department of the Treasury（財務省「北朝鮮の大量破壊兵器計画への資金供与主体に対する財務省の制裁措置」（2024年3月27日、）北朝鮮の大量破壊兵器計画への資金供与主体に対する財務省の制裁措置 | 米国財務省）

この措置は指定北朝鮮系銀行の代理人と海外で北朝鮮 IT労働者を雇い入れている企業を狙ったものである。北朝鮮系銀行の代理人とIT労働者、それを雇い入れていた会社は資金を獲得し、北朝鮮政府にとって重要な外貨を獲得していた。これらの主体は主にはロシアと中国に所在するネットワークを通じて活動し、スキームを取りまとめ、フロント企業又はシェルカンパニーを設立し、不正資金を動かし隠すための秘密銀行口座を管理し、北朝鮮の違法WMD・弾道ミサイル計画に資金供与していた。

出所：米国

150. 一部の国と、国連薬物・犯罪事務所（UNODC）、世界銀行などの国際機関は、リソースが限られた国の制度・執行能力を強化するために教育研修、技術支援、資金を提供している。プログラムでは規制枠組みの改善、監視システムの強化、官民セクターでのPFリスクに関する意識向上を重点にしている。効果的な輸出管理と最終使用者確認を実施するためのノウハウを提供するとともに、拡散に関わる金融活動を検知、報告するための高度な監視システムを各国が導入するのを支援することは、拡散金融に効果的に対抗するうえで極めて重要である。

ボックス49. 法域での事例：欧州プログラム「EU P2P」

「EU P2P（Partner to Partner）」輸出管理プログラムには、世界で取引されるデュアルユース品・武器の輸出管理を強化する狙いがある。欧州委員会と欧州対外行動庁が管理し、Expertise Franceが調整役を務めるプログラムは、デュアルユース品輸出管理における国際協力、武器貿易条約の実施、武器輸出管理の推進、強化を目的とし、そのために安全保障と経済的検討事項のバランスを考慮しながら国内又は地域内の能力を強化する。プログラムにはPFリスクに関する啓発活動や国の金融拡散リスク評価を策定するための技術支援などが含まれる。

出所：フランス

国際協力における課題

151. 本報告書の別段で述べたとおり、法的枠組みや制裁プログラムの法域ごとの違い（「検知、捜査、訴追」セクションで述べたPFの犯罪化の考え方の違いを含む）が、複雑な拡散金融・制裁回避スキームに対する効果的な国際協力における一番の課題になっている。PFネットワークと制裁回避の仲介者たちは、国境を越えて活動し、規制の格差を悪用し、複数の金融システムや国際貿易を駆使して、世界の安全保障に脅威をもたらしている。したがって、こうしたリスクに対処するには、不正行為の防止、検知、阻止に向けた政府機関の能力を高めるための強固な国際協力が欠かせない。また、多くの国はPF・制裁回避を効果的に監視し、対抗するインフラやノウハウが不足していることから、国や国際機関同士の協力も必要不可欠である。

6. 結論・優先領域

152. 多くの国がこの数年の間にPFリスク評価すでに完了しているか、2025年末までに第1回が完了予定である一方で、FATFグローバルネットワークは複雑な拡散金融・制裁回避スキームに関わる脅威と脆弱性の特定と軽減において個々の国がそれぞれ違う段階にある。残念ながら、PF・制裁回避に対抗し、これを阻止する共同の努力は、この先ますます難しくなるかもしれない。十分なリソースを持つ国家、非国家主体は、今後も執行、防止対策、法的枠組みの脆弱性をつぶさに調べ、新しいテクノロジーや変わり続ける地政学的情勢を利用し続けるはずだ。

153. こうした変化するPFリスクに対して国際金融システムを守る最善の策は、世界のCPF対策を構成する既存又は萌芽期のつながりを強化することである。この10年、各国は自国のCPFの法的枠組みの更新とPF-TFSの実施において目覚ましい前進を果たしたが、CPFレジームの効果的な実行においては力を合わせた躍進が必要かもしれない。改訂版FATF勧告1の文脈において、FATFグローバルネットワークはすでにこの目標に向けて前進するための青写真を備えている。2021年PFガイダンスで示したとおり、各国には自国のPFリスクの特定、評価、理解、低減が求められる。また、民間セクター事業体には、PFリスクを特定、評価、監視、管理、低減するプロセスの導入が求められるが、既存のTFSや法令遵守プログラムの枠組みの中でこれを行っている可能性がある。[71][72]各国にはこのほか、PFリスクに対処するために、例えば検知・報告ツール、国内連携・協力、捜査・訴追、国際協力などによる追加努力が必要かどうかの検討も求められる。[73]

154. 本調査報告書では、PF・制裁回避主体が不正行為を隠し、拡散国又は制裁対象国に送られるデュアルユース品その他品目の本当の最終使用者を隠すために、頻繁に仲介者を使用する実態を明らかにした。巧妙なスキームを駆使して制裁回避に関与する個人、会社、国の身元を不透明にし、その結果、不正行為の検知が難しくなる。複雑な拡散金融・制裁回避スキームの防止、抑制に向けたFATFグローバルネットワークの共同の前進を後押しするために、いくつか検討すべき優先重点領域がある。

---

71 Guidance on Proliferation Financing Risk Assessment and Mitigation（拡散金融リスク評価及び低減ガイダンス）

72 PFリスクの観点から、金融機関又はDNFBPが取り入れるリスクベースの対策は、特定対象金融制裁の潜在的な違反・不履行・潜脱を検知し、防ぐことによって、勧告7の厳格な要求事項の完全実行を強化し、補うことが目的である。セクター内でのPFリスク低減策を判断するにあたって、各国はそのセクターに関連するPFリスクを検討しなければならない。リスクベースの対策を取り入れることによって、管轄官庁、金融機関、DNFBPはその対策が特定したリスクに見合うことを確認でき、リソースの最も有効な配分方法を判断できるはずだ。

73 勧告2及びその解釈ノートに従い、各国は拡散金融リスクをより効果的に低減するための各機関の協力枠組みを整備する必要がある。

CPFに関するFATFのさらなる活動に対する勧告

a) **PFの定期的更新:**本書の現在の状況、動向、手口のセクションの定期的な更新を検討する。PF・制裁回避リスクは、今後しばらくの間、FATFグローバルネットワークが対処すべき重要課題であり続けることが予想される。一方で、この問題の集団的理解の助けになる脅威、脆弱性、類型は、間違いなく変化し続け、形を変え続ける。PFリスク評価の性質を踏まえ、最新情勢の理解を維持することが各国と民間セクターにとって重要である。国連安保理決議第1718号専門家パネル報告書がなくても、FATFは主要ステークホルダーのリスク環境監視を支援しなければならない。

b) **官民セクター連携の推進:**FATFイベントの一環として民間セクターへのアウトリーチ活動の組み立てに本報告書とパブリックコメントからのインサイトを使用することを検討する。また、そのフィードバックにより、CPF対策を強化するためにFI、DNFBP、VASPと協力して講じることができるアクションにより狙いを絞ったフォローアップガイダンス報告書に役立てる。例えば、2026年にPrivate Sector Consultative Forumで関連セッション又はセッションシリーズを開催するなどが考えられる。PF・制裁捜査を開始するにあたってSAR/STRに大きく頼っていることがFATFグローバルネットワークから報告されていることから、該当セクターで官民の情報共有を強化するために協調的アウトリーチ活動とガイダンスをさらに活用できる。

c) **WMD PFの定義:**5年以内にWMD PFの正式な定義をFATF一般用語集に加えることを検討する。その際、FATFグローバルネットワークのPFリスク評価の水平レビュー結果を考慮する。本報告書で概説したとおり、PF・制裁回避アプローチの法域ごとの違いがこのトピックに関する発見、捜査、国際協力を阻害し、複雑にしている可能性がある。広く認められた統一的な定義は、PF・制裁回避の防止、抑止におけるフラストレーションを軽減できるかもしれない。

d) **PF NRAの水平レビュー:**3年以内に、FATFグローバルネットワークのPFリスク評価の水平レビューを実施することを検討する。本報告書で説明したとおり、PFリスクの特定、評価、理解、低減とそのための新しい手法の活用は、各国でそれぞれに段階が違う。また、PF・制裁回避に関する脆弱性の理解にもばらつきがあるようである。FATF基準に従ってPFリスクをさらに深く理解する官民両方のセクターに課せられたこの先の重要タスクを踏まえると、FATFグローバルネットワークにPFリスク評価のための時間的猶予を与えたうえでの水平レビューは、模範事例の洗い出しに役立つかもしれない。

出所:インド、シンガポール

別紙A:リスク指標

1. 以下に示す指標は、このプロジェクトの過程でFATFが受け取った情報から導き出した一例である。これらの指標は、該当するPF・制裁回避スキームに関わる疑わしい取引や活動を突き止めるにあたり、官民セクター事業体の能力強化のためにまとめたものである。特定したいくつかの指標はPF・制裁回避に直接又はそれに特化したつながりがないように見えたり、別の形態の不正行為を示唆しているかもしれないが、それでもPF・制裁回避スキームを特定するにあたって関連性がある場合もある。

指標の使い方

2. 指標は異常又は疑わしい行為の発生確率が高いことを示す場合がある。ある顧客又は取引に関して一つの指標が存在する場合、それだけでPF又は制裁回避取引の疑いを保証するものではなく、その指標が必ずしもそうした行為を明確に指し示すものでもないが、必要に応じてさらなる監視、検証を開始すべきことを示唆している可能性がある。同様に、複数の指標の存在もより入念な検証を必要とする根拠になることがある。1つ以上の指標が疑わしい取引又は活動を示唆するかどうかも、その機関又は市場参加者が提供する事業、製品、サービスと、顧客との関係性によって変わる。

3. 以下に列挙する指標は官民セクターのどちらにも当てはまる。後者については、指標はデュアルユース品その他関連セクターで活動するかそれらと接点のある銀行、資金移動業者、指定非金融業者及び職業専門家、暗号資産サービスプロバイダー、中小企業、大規模コングロマリットに当てはまる。民間セクターにおいて、これらの指標は法令遵守、取引監視、調査分析、顧客オンボーディング・関係管理、その他PF、制裁回避、前提犯罪の防止活動を行う領域の担当者による使用を意図している。

4. リスク指標の一部は、多くの場合、外部ソースが有する各種データエレメント(金融取引、税関データなど)との相互比較が必要である。外部データを拠り所にすることから、民間セクターは以下に列挙した指標のすべてを監視することはないかもしれない。一部のリスク指標については、民間セクターは法執行機関又はFIUとの関わりを通じてなど、管轄官庁から追加の背景情報が必要になる。これらの指標を使用するにあたり、民間セクター事業体は、顧客管理プロセス中に顧客から得た情報、該当する場合は取引に関わる貿易金融手法、その他該当する背景的リスク要因など、顧客プロフィールの完全性も考慮しなければならない。

5. 下表に3つに大別したリスク指標をまとめている(1) 顧客情報/行動、2) 取引、3) 貿易活動)。顧客情報/行動指標はCDDを実施する際に活用できる。取引指標は輸出取引を含む取引を監視する際に活用できる。貿易活動指標は幅広いリスク管理プロセスで考慮すべきさらなる文脈を示す場合がある。各カテゴリーの一部リスク指標は重複しているが、FATFグローバルネットワークは官民セクターを支援するためできる限り多くの情報提供を優先することを求めた。

1. 顧客情報/行動

1. 所有者、資金源、関与する国/事業体（特に制裁対象国）を隠すために企業事業体（シェルカンパニーなど）を使用する。
2. 取引の多層化によって最終使用者を隠す。調達エージェントを使って会社、ブローカー、仲介者を何層にも重ね、積み荷、意思疎通、金融を経由させる。
3. 顧客が輸入品/輸出品とのつながりを隠すために複雑な構造を使用する。例えば、多層化した信用状、フロント企業、仲介者、ブローカーを使用するなど。
4. 最終顧客を隠すために標準的ビジネス文書を変える。
5. 当事者の詳細情報がWMD制裁又は貿易管理に基づく指定当事者と類似している（氏名、住所、電話番号など）。
6. 所有構造が不明瞭な会社、シェルカンパニー又はフロント企業が所有する銀行口座、又はそれらが実行する取引である。
7. 顧客が規制された又は高リスクの物品や技術の供給、販売、輸送に関与している。
8. 現在制裁対象の個人又は団体と顧客が過去に取引を行っていた、又は関係を維持している。
9. 当事者が不正転売の懸念がある国に物理的に所在している（領域を経由して拡散されやすい物品の提供、又はその資金供与が可能な国）。
10. 顧客又は顧客の相手方が国の制裁レジームで指定された団体又は個人と取引を行っている、又は国の制裁レジームで指定された団体又は個人に関してリストアップされた識別子とのつながりを含む取引を行っている（eメールアドレス、物理的住所、電話番号、パスポート番号、兌換性仮想通貨（CVC）アドレスなど）。
11. 顧客がデュアルユース品又は輸出管理対象品を取り扱う大学又は研究機関と関係がある。
12. 取引に民間の最終使用者を自称する者が関わっており、基本調査の結果、その住所が軍用施設又は懸念される国の軍用施設と同一の場所であることが示唆される。
13. 顧客が明らかな経済的又はビジネス上の目的がなく、新しい船舶を取得する。
14. ビジネスモデルが完全輸出志向であり、通過事業体として機能している。
15. 会社が海上輸送、輸出入、繊維、衣料品、漁業、海産物の業界で活動している。
16. 顧客が取引に関して機密保持を主張する。又は制裁、PFに関する規制遵守について不適当な懸念を示す。
17. 取引に、商業登記上、「特殊目的」のプロジェクトに従事しているとされる事業体が関わっている。
18. 顧客が契約を獲得するために同僚の個人情報を借りるよう要求する。
19. 顧客が通常の事業と無関係な物品を取引し、デュアルユース機器又は技術が関わっている可能性がある（例：反応器、工作機械、ミサイルシステム部品など）。
20. 顧客の連絡先情報（電話番号など）が仕向国と合致しない。
21. 顧客が銀行、荷送人、第三者の詳細情報（最終使用者、用途、会社所有者

など）の提供を拒む。
22. 不正行為のフロント企業として機能する会社が相当量の取引を取り扱っているにもかかわらず、オンライン上に存在しない。
23. 合法企業から届いたように見える違法な問い合わせをするためのeメール又はウェブアドレスのサイバー上のなりすまし。多くの場合、既知の取引関係が利用される。
24. IPアドレスが、顧客が申告した場所と一致しない。
25. 過度に一般的、非記述的、もしくは別のよく知られた企業と簡単に間違えられるような企業名である。また、企業名のつづりを違う書き方でよく間違えている。

2. 取引

1. 取引に同じ最終使用者の海外銀行口座から複数の類似サプライヤーへの少額支払いが関わっている。
2. 取引に関して、懸念される国から予定されていた決済ルートが、別の国又は別の会社を通じたルートへと直前に変更される。
3. 金融システムを通じて禁止された取引を経由した結果、金融機関が国の制裁レジームに反する決済を処理することになった。
4. 資金が会社間を周期的に流れている可能性がある。一方が支払いを止め、他方が同じ受益者に対して支払いを開始した。
5. 顧客が実際の物品取引から物理的に距離のある金融サービスを使っているか、そのような取引を行っている（又はその両方）。
6. 金融取引書類から制裁対象当事者又は国の言及が省かれている。
7. 取引が、制裁執行が弱いことで知られる又は不正取引スキームに従事していることで知られる国又は金融センターを通過している。
8. 複数の金融機関チェーンを含む、複雑又は異例の決済ルートが使われる。特にPF対策又は制裁が不十分な国を通過している。
9. 取引に、よく知られた積み替え国と併せて、決済のためにオープン勘定/オープンクレジットラインが使用される。
10. 実際の最終使用者ではなく発行銀行宛ての信用状に基づく購入が行われる。
11. 顧客が、口座開設が認められる前に、デュアルユース品又は輸出管理対象品に関して信用状の発行を要求する。
12. 預金口座の預金残高が急増した後、現金が引き出される。そうした取引が行われた可能性を示す。
13. 顧客が直近の現金預金と同等の金額を海外に送金する。
14. 顧客が製品の支払いのために個人の口座を使用する。
15. 複数の銀行口座が使用される。
16. 貿易取引に明確な根拠がない。又は多額の支払いの理由がない。特に顧客

の通常の事業活動と一致しない場合。

17. 物品の数量と金額が決済量と一致しない。
18. 顧客がKYC/AML対策を回避するために暗号資産での決済を要求する。
19. 暗号資産サービスプロバイダーを通じた送金を行う。特に規制が厳格でない国が関わる場合や、適切なデュー・ディリジェンスのない分散型取引が使用される場合。
20. 制裁規制回避のために使用されることがある資金送金システム（ハワラ）など、非公式又は代替チャネルが使用される。
21. 制裁対象の暗号通貨取引所が関わっていないことを装うために、暗号資産の新しいアドレスを作る。
22. 取引に、グローバル輸出管理連合（GECC）加盟国以外に拠点を置く、2022年2月24日以降に法人化された企業からの防衛又はデュアルユース品の支払いが関わっている。

3. 貿易活動

1. 品目が貨物フォワーダーの手元に到着した後、輸出者の知るところなくその品目の輸送指示を変える。
2. 顧客履歴や商慣行と矛盾する輸送指示に直前に変更される。
3. 最終荷受人又は最終目的地の輸送書類が輸送前又は輸送中に変更される。
4. 顧客が本人確認書類に記載されたものとは違う住所への輸送を要求する。
5. 品質が輸出先の国の技術水準と一致しない製品が輸出されようとしている。
6. 取引に通常の地理的貿易パターンと一致しない物品の輸送が関わっている。関与国が通常その種の物品を輸出又は輸入しない、通常は消費しないなど。
7. 貿易取引に軍事又は核プログラムで使用可能な機械類又は材料が関与している（例：高張力鋼、遠心分離機など）。
8. 貨物フォワーダー又は航空チャーター便の運航者が最終使用者として記載されている。
9. 製品が遠回りな手段で輸送される。小型船又は旧式船舶が使用されるなど。
10. 品目が小さな荷物で頻繁に中心地点に届き、そこで組み合わされる。
11. 取引に高リスク積み替え地域で活動する貨物フォワーダーが関わっている。
12. 規制対象品の目的地を禁止された目的地に変えるためによく使用される積み替えポイントを経由する形で購入の経路が設定されている。
13. 取引にその製品に対して異例の輸送経路や目的地が関わっている。
14. 貿易書類において、貨物フォワーダー/通関業者がその製品の最終目的地として記載されている。

15. 物品の目的地/輸送先の国がその国ではない。もっともらしい理由が特になく収益が受け渡しされる。
16. 輸送ルートや積み出し港、荷受人、船舶代理店を隠すために船荷証券や送り状などの船積書類が偽造される。
17. 制裁品又は輸出管理対象品の名前を変える。最終使用者を隠すために虚偽の契約書を使う。
18. 商業送り状などの裏付け書類に実際の最終使用者が記載されていない。
19. 検知を回避するために、書類上、誤った物品分類をする。規制対象品に対してそうではない説明を用いるなど。
20. 商業、輸送、金融書類の記載情報に矛盾がある。例えば、送り状と船荷情報に矛盾があるなど（物品の種別、重量、価額、目的地）。
21. DNFBPの輸出者が第三国を示す原産国ラベルを貼付するなどして北朝鮮で製造された物品の出所を偽装する。
22. 第三国のサプライヤーが顧客又はその他関係当事者に知らせずに、製造を北朝鮮の工場で行う又は下請けに出すように変える。
23. 北朝鮮籍商船が識別情報を物理的に改変し、別の船舶として通過する。
24. 高級品を第三国の中央倉庫に頻繁に送る。
25. 規制対象の高級品に関わる取引で新しい購入者に急に変える。
26. 建築材の購入、輸送。
27. 記載されたビジネス目的と無関係な金融活動が相当量行われる。繊維、漁業、石炭輸出と無関係な支払いなど。
28. 製造業又は貿易業の顧客が工業製品に関する取引又はその他の貿易取引に現金を使用する。
29. 貨物の申告価格が輸送コストに対して少ない。
30. 船舶の船籍が頻繁に変更される。
31. FTZ（自由貿易地域）が関わっている。FTZはセンシティブ品目の出所や動きを不透明化する際に利用されることがある。