拡散金融リスク評価に関する調査

調査報告書

令和５年３月

株式会社エヌ・ティ・ティ・データ経営研究所

株式会社ＮＴＴデータ経営研究所

目次

略称について

本書で用いる略称等は、それぞれ次の意味を示すものとします。

全体	FATF	Financial Action Task Force
	DNFBPs	Designated Non-Financial Businesses and Professions（特定非金融業者及び職業専門家）
	FIU	Financial Intelligence Unit（資金情報機関）
	PF	Proliferation Finance（大量破壊兵器拡散金融）
	CPF	Countering Proliferation Financing（拡散金融対策）
	ML	Money Laundering（資金洗浄）
	AML	Anti-Money Laundering（資金洗浄対策）
	FT	Financing of Terrorism（テロ資金供与）
	CFT	Countering Financing of Terrorism（テロ資金供与対策）
	NRA	National Risk Assessment（マネー・ローンダリングやテロ資金供与に関する国によるリスク評価。特に注記がない場合、その結果を踏まえて公表されたリスク評価書を指す）
米国	FinCEN	Financial Crimes Enforcement Network（財務省金融犯罪捜査網）
	OFAC	Office of Foreign Assets Control（財務省外国資産管理室）
	BSA	Bank Secrecy Act（銀行秘密法）
	SWIFT	The Society for Worldwide Interbank Financial Telecommunication（世界銀行間金融通信協会）
英国	NRA-PF	National risk assessment of proliferation financing(拡散金融の国家リスク評価)
	ML/TF NRA	National risk assessment of money laundering and terrorist financing 2020（2020 年　マネー・ローンダリング、テロ資金供与の国家リスク評価）
	SAMLA	Sanctions and Anti-Money Laundering Act（制裁及びアンチ・マネー・ローンダリング法）
	POCA	Proceeds of Crime Act（犯罪収益法）
	CFA	Criminal Finances Act（犯罪財政法）
	TA	Terrorism Act（テロリズム法）
	ATCSA	Anti-Terrorism, Crime and Security Act（反テロリズム、犯罪及び安全保障法）

	TCSP	Trust and Company Service Provider（トラスト又は企業サービスプロバイダー）
	OFSI	Office of Financial Sanctions Implementation（金融機構監督局）
	AMLSF	Anti Money Laundering Supervisors' Forum（AML 監督者フォーラム）
	FCA	Financial Conduct Authority（金融行為規制機構）
	OPBAS	Office for Professional Body Anti-Money Laundering Supervision（専門機関アンチ・マネー・ローンダリング監督局）
	HMRC	Her Majesty's Revenue and Customs（歳入税関庁）
	MOD	Ministry of Defence（国防省）
	CPACC	Counter Proliferation and Arms Control Centre（拡散防止・武器管理センター）
	FCDO	Foreign, Commonwealth & Development Office（外務英連邦開発省）
	DIT	Department for International Trade（国際貿易省）
	BEIS	Department for Business, Energy & Industrial Strategy（ビジネス・エネルギー・産業戦略省）
	CDs	Crown dependencies（王室属領）
	OTs	Overseas Territories（海外領土）
豪州	AUSTRAC	Australian Transaction Reports and Analysi Centre(オーストラリア取引レポート分析センター、疑わしい取引の届出先)
	ABF	The Australian Border Force(豪州国境警備隊)
	AFP	The Australian Federal Police(豪州連邦警察)
	DEC	the Department of Defence(国防省の国防輸出管理局)
	DFAT	The Department of Foreign Affairs and Trade(外務貿易省)
	NIC	The National Intelligence Community(国家情報コミュニティ)
	ABR	the Australian Business Register(豪州事業登録簿)
	ASIC	Australian Securities and Investments Commission(豪州証券投資委員会)

	ABRS	Australian Business Registry Services(豪州事業登録サービス)
	TCSPs	Trust and Company Service Providers(トラスト・アンド・カンパニー・サービスプロバイダー)

１．本調査の目的と概要

（1）背景と目的

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資金凍結等措置の対象となっている者に、資金または金融サービスの提供をする行為を指す。

拡散金融対策にかかる国際基準は、FATF（Financial Action Task Force、金融活動作業部会）において、2012 年以降決定・公表されており（勧告 7[1]等）、大量破壊兵器の拡散及びこれに対する資金供与の防止等に関する国連安保理決議を遵守するため、対象を特定した経済制裁（金融制裁措置等）を実施することを各国に求めている。しかし、こうした枠組みに基づき、我が国を含む国際社会が協調して北朝鮮やイランに対して経済制裁を実施している状況下でも、こうした国や地域へ、大量破壊兵器等及び関連物資・技術などの移転が行われているとみられる。このため、2020 年 10 月、FATF は勧告 1（Assessing risks and applying a risk-based approach）を改訂し、2025 年以降順次実施される第 5 次相互審査以降適用されることとなった。具体的には、FATF 加盟国は、同勧告 1 に基づいて、「勧告 7 で言及されている国連制裁決議に基づく金融制裁義務（資産凍結措置）の潜在的な違反・不履行・潜脱」と定義されている拡散金融リスクについて各国が評価することが求められることになった。

日本においても、第 4 次相互審査報告書の公表を契機として、政府一体となって強力に対策を進めるため、日本政府として「行動計画」[2]を公表。この中では、「1（1）リスクの評価の刷新」として、「マネロン、テロ資金供与及び拡散金融に対する理解を向上させるため、リスク評価手法の改善等によって、国のリスク評価書である犯罪収益移転危険度調査書を刷新する」とされるとともに、資産凍結措置の実効性向上に向け、制度整備や執行強化を行うことが明記されており、政府において順次取組みを進めているところ。

また、マネロン・テロ資金供与・拡散金融対策政策会議が決定・公表した「マネロン・テロ資金供与・拡散金融対策の推進に関する基本方針（2022 年 5 月 18 日）」においては、拡散金融を通じた大量破壊兵器の拡散活動の助長が、我が国や国際社会にとっての大きな脅威であり、拡散金融対策の強化が不可欠であるとされた。そして、対策強化の一環として、「国連安保理決議等に基づく制裁措置の違反、不履行、潜脱のリスクを分析・把握し、そのリスク低減のための措置を講じるプロセスを確立し、実効性を高めていく」ことが明記されており、政府として着実に取り組む必要がある。

一方、国際的にみると、国連制裁委員会の下部組織として、制裁措置の履行に関する情報

---

[1] 勧告 7「大量破壊兵器の拡散金融」において、各国は、大量破壊兵器の拡散及びこれに対する資金供与の防止・抑止・撲滅に関する国連安保理決議を遵守するため、対象を特定した金融制裁措置を実施しなければならないとしている。

[2] 「マネロン・テロ資金供与・拡散金融対策に関する行動計画」（2021.8）

の収集，審査及び分析等を行う制裁委員会専門家パネルが制裁措置の実施を改善するための行動について勧告を行っているところ、各国においても、これまで、米国・英国・豪州・ポルトガル・ラトビア等の国々で拡散金融に関するリスク評価書が策定・公表されている。

こうした他国の拡散金融リスク評価書や国連安保理制裁報告書等、その他国内関係機関が有する情報等を踏まえつつ、国連制裁決議に基づく金融制裁義務に加え、独自制裁義務（北朝鮮）を実施してきた日本に相応しい拡散金融リスク評価を行うがある。さらに、当該リスク評価を踏まえ、金融機関等によるリスクベースでの資産凍結措置の実施を進めていくことが求められる。

以上を踏まえ、拡散金融対策の更なる対策の高度化に向け、国連制裁決議に基づく金融制裁義務に加え、独自制裁義務（北朝鮮）を実施してきた日本に相応しい拡散金融リスク評価を行うため、他国の拡散金融リスク評価書や国内関係機関が有する情報等を調査・分析した。

（2）調査概要

FATF の拡散金融に関するガイダンス[3]を参考に、他国の拡散リスク評価書、国連の拡散金融リスクに関する専門家パネルレポート、国内外における拡散金融や北朝鮮・イランへの資金移転に関する個別事案（日本による北朝鮮との間の輸出入禁止措置違反事案や瀬取り等に関する国内外の事案を含む）等の文献調査を行った。

なお、FATF で要求される拡散金融リスク評価のスコープが「国連制裁決議に基づく金融制裁義務（資産凍結措置）の潜在的な違反・不履行・潜脱」であることから、国連安保理決議の対象である北朝鮮及びイランを中心とした金融制裁義務の潜在的な違反・不履行・潜脱に係る主体や手段、手法（フロント企業、暗号資産、瀬取り等）等に焦点をあてた。

（3）実施スケジュール

本調査は、2023 年 1 月に開始し、文献調査を進めるとともに、得られた結果に基づいて総合的な分析を実施した。この調査結果を 2023 年 3 月末に報告書としてとりまとめた。

[3] FATF “Guidance on Proliferation Financing Risk Assessment and Mitigation”（2021.7）

２．本調査の実施方法

（１）調査対象文献

本調査では、先述の背景・目的を踏まえ、以下の図表 1 に示す文献を対象に調査を実施した。

図表 1：調査対象文献

国・地域	文献名称	発行機関
日本	Anti-money laundering and counter-terrorist financing measures JAPAN Mutual Evaluation Report（2021）	FATF
	外為法違反事例	一般社団法人 安全保障貿易 情報センター
米国	National Proliferation Financing Risk Assessment（2022/2018）	US Treasury
英国	National risk assessment of proliferation financing-September（2021）	HM Treasury
豪州	Proliferation Financing in Australia（2022）	AUSTRAC
（国連）	Report of the expert panel assisting the committee overseeing its sanctions against the Democratic People's Republic of Korea（2020～2022）	UN Security Council
（FATF）	Guidance on Proliferation Financing Risk Assessment and Mitigation（2021）	FATF

（２）調査手法

各文献より国内外の拡散金融における「脅威」を特定し、国内外の「取組」を精査した上で、国内の「脆弱性」を中心にとりまとめを行った。

１．調査項目

まず、FATF“Guidance on Proliferation Financing Risk Assessment and Mitigation（2021）”（以下、「FATF ガイダンス」）を参考に、拡散金融のリスクや、国・金融機関等に求められる対応等の観点から調査項目を以下のとおり整理した（図表 2)。

図表 2：調査項目

分類			調査項目	FATF ガイダンス規定箇所
脅威	取組み	脆弱性		
○			①拡散金融の主体、協力者	4b,52,80,81
	○	○	②国のリスクアセスメント（リスクの特定・評価）	15～49,56,57
	○	○	③金融機関等のリスクアセスメント（リスクの特定・評価）	15～49,56,57
	○	○	④国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）	4a,56,57
	○	○	⑤金融機関等による標的型金融制裁への対応	4a,56,57,64～66,68～78,82
	○	○	⑥その他企業（貿易会社等）による標的型金融制裁への対応	57,68,82
	○	○	⑦国の金融機関等に対する拡散金融対策の監督・アウトリーチ	57,60～63,67,83～85
	○	○	⑧国のその他企業（貿易会社等）に対する拡散金融対策の監督・アウトリーチ	57,60～63,67,83～85
	○	○	⑨国の拡散金融機関対策に係る組織・体制（組織間の連携、調整等の観点を含む）	57～61
		○	⑩国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）	21
		○	⑪拡散金融に利用される金融機関等と金融サービス	31,37,39,52,
		○	⑫拡散金融に利用されるその他の産業と貿易等の形態や品目等	39,37,52
		○	⑬拡散金融に利用されるその他の手段（サイバー攻撃等）	29,39

なお、分類に利用した「脅威」「取組」「脆弱性」の概念は、FATF ガイダンスの規定を踏まえた以下の定義に基づいている（図表 3)。

図表 3：本調査における「脅威」「取組」「脆弱性」の定義

項目	定義
脅威	● 過去、現在、将来において、拡散金融に係る標的型金融制裁の不履行を回避、違反または悪用した、またはその可能性がある指定された個人または団体 ✓ 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 ✓ 上記の支援者やそれらの者に同調する個人、集団　等
取組み	● 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に、直接的または間接的に資金や金融サービスの提供をする行為を抑止するための取組 ✓ 国や金融機関等によるリスクアセスメント ✓ 金融機関等による標的型金融制裁への対応 ✓ 国による金融機関等に対する監督・アウトリーチ　等
脆弱性	● 脅威によって悪用されうる、もしくは拡散金融に係る標的型金融制裁の違反、不実施、回避を支援または促進しうるもの ✓ 上記の「取組み」における弱点 ✓ 拡散金融に利用されやすい金融サービス、貿易取引　等

また、「取組み」に関連する②～⑨の調査項目については、FATF ガイダンスより国や金融機関等に求められる取組みを抽出のうえ類型化し、「取組みのポイント」として整理した。この結果を以下の図表 4 に掲載する。

図表 4：FATF ガイダンスを踏まえた取組みのポイント

② 国のリスクアセスメント（リスクの特定・評価）
● 定期的なリスク評価の実施と公表 ✓ 拡散金融のリスクを定期的に特定、評価、低減する（最新の評価を維持する） ✓ リスク評価の結果は所管省庁、特定の民間部門に加え、一般に公表する ● 体制・手順の整備（関係省庁、民間部門、他国との情報共有・連携を含む） ✓ リスク評価のための調整や執行の権限、リソースを有する機関を任命する ✓ リスク評価の計画を立案し、関係機関や利害関係者を特定する ✓ 利用可能な情報を徹底的にレビューし、リスクベースの戦略立案に活用できるよう包括的な分析を行う ✓ 民間部門から必要な情報を収集する ✓ 自国が決定した手法を用いて標的型金融制裁の違反、未実施、回避のリスクを評価する（FATF は一律的な評価手法を規定していない） ✓ データの収集と分析、調査結果の文書化、関係機関等での共有、一般公表のための

手順を規定する
- ✓ リスク評価の手法や分析、結果について、金融機関、DNFBPs、VASPs と協議、情報共有を実施する
- ✓ リスク評価の経験を有する国や直面するリスクの性質が類似する国と連携する

● 包括的かつ具体的な検証
- ✓ 利用可能な情報を徹底的にレビューし、リスクベースの戦略立案に活用できるよう包括的な分析を行う
- ✓ 経済・社会・産業構造等、標的型金融制裁の違反、未実施、回避に影響する国の特徴を考慮する
- ✓ リスク低減に必要なリソース配分の優先順位付けに有用な情報を提供する
- ✓ 国連安保理専門家パネルの報告書で確認された違反、非実施、回避の方法、傾向、類型、他国のリスク評価、その他事例等をリスク評価の目的や範囲を定めるための予備的な分析に活用する
- ✓ 経済・産業の特徴、コンプライアンス意識、資金移動の複雑さ等を踏まえ、リスクの高い業態を特定する
- ✓ マネロン・テロ資金供与リスクとの相違を認識する（必ずしも資金洗浄を伴わない、合法/非合法両方の活動から資金調達される、制裁対象の活動を偽装するために構築された国際ネットワークが存在する、複数の法域を跨って敢行される、フロント企業やシェル企業が利用される 等）

③ 金融機関等のリスクアセスメント（リスクの特定・評価）

● 定期的なリスク評価の実施・見直しと公表
- ✓ 拡散金融のリスクを定期的に特定、評価、低減する（最新の評価を維持する）
- ✓ データの収集と分析、評価結果の文書化とその維持管理、当局報告等の手順を規定する

● 体制・手順の整備
- ✓ リスク評価の計画を立案し、関係機関や利害関係者を特定する
- ✓ 利用可能な情報を徹底的にレビューし、リスクベースの戦略立案に活用できるよう包括的な分析を行う
- ✓ データの収集と分析、評価結果の文書化とその維持管理、当局報告等の手順を規定する
- ✓ リスク・コンプライアンス対応プログラムの一部として拡散金融対応を実施することも可能

● 包括的かつ具体的な検証
- ✓ 利用可能な情報を徹底的にレビューし、リスクベースの戦略立案に活用できるよう包括的な分析を行う
- ✓ 商品・サービス、取引形態、顧客属性、地理的要因等多面的な観点から脆弱性を特定する
- ✓ 国のリスク評価や標的型金融制裁の違反等の事例、及び、顧客受入時と継続的顧客管理において収集した顧客情報、輸出規制対象商品等に関連する取引記録等を分析に活用する

- ✓ 顧客受入時と継続的顧客管理、取引モニタリング/スクリーニング、監査や当局検査の指摘内容等を分析に活用する
- ✓ リスク低減に必要なリソース配分の優先順位付けに有用な情報を提供する
- ✓ 国連安保理専門家パネルの報告書で確認された違反、非実施、回避の方法、傾向、類型、他国のリスク評価、その他事例等をリスク評価の目的や範囲を定めるための予備的な分析に活用する

④ 国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）

- 法規制等の整備
  - ✓ 拡散金融に対抗する規制体系を整備する
  - ✓ 拡散金融に対抗する政策方針、行動計画を策定する
  - ✓ 特定のセクターや顧客を対象に、包括的な検証なく取引を制限することは不適切
- 体制・手順の整備
  - ✓ 制裁の実施及び責任を有する所管省庁を特定する
  - ✓ 金融機関、DNFBPs、VASPs を含む全ての関係機関に対し、制裁の指定が適時に通知するための体制を構築する
  - ✓ 既存のマネロン・テロ資金供与対策の体制や枠組みを活用する

⑤ 金融機関等による標的型金融制裁への対応

- 体制・手順の整備
  - ✓ リスクを管理・軽減するための方針・計画・手続きを策定・実施・見直しを行う
  - ✓ 既存のマネロン・テロ資金供与対策の体制や枠組みを活用する
  - ✓ リスク・コンプライアンス対応プログラムの一部として拡散金融対応を実施することも可能
  - ✓ 内部統制の構築と維持（定期的な有効性検証等）
- 人材の確保・育成
  - ✓ 研修プログラムの開発、運営
- 顧客管理
  - ✓ ビジネスの特性、規模、地理的要因、市場、顧客プロファイル、取引量・金額等の観点からリスクを特定する
  - ✓ 顧客の受入プロセス、顧客情報の維持管理、スクリーニングの実施、及びこれらの見直し
  - ✓ 実質的支配者の特定やビジネス様態等に関する情報収集
  - ✓ コルレス先の管理
  - ✓ 特定のセクターや顧客を対象に、包括的な検証なく取引を制限することは不適切
- IT システムの活用
  - ✓ AI 等を活用した技術やソフトウェアへの投資
- リスクベースアプローチ
  - ✓ リスクが低い金融機関等は簡素な顧客管理も許容される

⑥ その他企業（貿易会社等）による標的型金融制裁への対応

- 体制・手順の整備
  - ✓ 内部統制の構築と維持（定期的な有効性検証等）

✓ 実質的支配者の特定やビジネス様態等に関する情報収集

⑦ 国の金融機関等に対する拡散金融対策の監督・アウトリーチ

- リスク評価の要求
  - ✓ 金融機関等に対し、拡散金融リスクの特定・評価を要求する
- 体制整備の要求
  - ✓ 金融機関等に対し、拡散金融リスクを管理し軽減するために相応の措置をとることを要求する
  - ✓ 経営層の主体的な関与を求める
- 監督・監視
  - ✓ 定期的に異なる業種や個々の事業者のリスクレベルを体系的に特定・評価し、そのレベルに応じた体制が構築されているかを考慮する
  - ✓ 継続的な監督・監視のため、内外から入手可能な情報を活用し、リスク評価を最新化する
  - ✓ マネロン・テロ資金供与リスクとの相違を認識する（ML/TF リスクと異なる部署が対応している可能性、異なる商品に焦点を当てる必要がある可能性 等）
  - ✓ 金融機関の及び各業態が直面するリスク、それぞれの能力・経験、対象となる金融制裁の義務等を考慮する
  - ✓ 取引フィルタリング/モニタリングの精度を確認する（アラートの陽性/偽陽性の割合）
  - ✓ 指摘内容についてのフォローアップを行う
  - ✓ 規制違反に対し広範な規制・監督上の措置を有する（行政処分、営業停止等）
- アウトリーチ
  - ✓ 標的型金融制裁に係る法規制についてのガイダンスやプラクティスの提供
  - ✓ 金融機関等に対して、定期的な研修等の普及啓発を行う
  - ✓ 民間セクターから必要に応じてアクセス可能なサポートの提供
- リスクベースアプローチ
  - ✓ 民間セクターの取組みだけでは低減できない高リスク領域に対する規制・監督措置の強化（特定の取引の制限、ガイダンス、テーマ別検査等）
  - ✓ リスクが低い金融機関等は監督・監視等の措置を簡素化することも許容される

⑧国のその他企業（貿易会社等）に対する拡散金融対策の監督・アウトリーチ

- 監督・監視
  - ✓ 継続的な監督・監視のため、内外から入手可能な情報を活用し、リスク評価を最新化する
  - ✓ 指摘内容についてのフォローアップを行う
  - ✓ 規制違反に対し広範な規制・監督上の措置を有する（行政処分、営業停止等）
- アウトリーチ
  - ✓ 標的型金融制裁に係る法規制についてのガイダンスやベストプラクティスの提供
  - ✓ 民間セクターから必要に応じてアクセス可能なサポートの提供
- リスクベースアプローチ
  - ✓ 民間セクターの取組みだけでは低減できない高リスク領域に対する規制・監督措置

の強化（特定の取引の制限、ガイダンス、テーマ別検査等）
⑨国の拡散金融機関対策に係る組織・体制（組織間の連携、調整等の観点を含む）
● 関係所管、民間部門、他国との情報共有・連携 ✓ 核拡散資金対策に関与している全ての関連省庁の協調・情報共有の枠組みを構築する（監督官庁、輸出入管理当局、税関、国境管理、情報機関等） ✓ 国と民間セクターが効果的かつ継続的に情報共有や対話を行う ✓ リスク評価の経験を有する国や直面するリスクの性質が類似する国と連携する

２．調査結果のとりまとめ方法

まず、「２．（１）調査対象文献」の各文献より把握できた日本を含む各国の「脅威」「取組み」「脆弱性」の内容について、①～⑬の各調査観点に沿って整理した（「３．調査結果（１）～（４）」）。

次に、UN Security Council “Report of the expert panel assisting the committee overseeing its sanctions against the Democratic People’s Republic of Korea（2020～2022）”（以下、「（北朝鮮制裁）専門家パネル報告書」）より把握できた北朝鮮による拡散金融に係る「脅威」「脆弱性」の内容について、①及び⑩～⑬の各調査観点に沿って整理した（「３．調査結果（５）」）。

最後に、これらを踏まえ、今後の我が国における拡散金融の取組みにおいて参考となり得る各国の取組み事例、及び、専門家パネル報告書の勧告事項等を抽出し、「４．まとめ」に整理した。

3．調査結果

（1）日本

①　拡散金融の主体、協力者

一般社団法人安全保障貿易センターが公表する外為法違反事例[4]、及び、警察庁が公表する対北朝鮮措置に係る事件一覧[5]より、不正輸出に伴う行政処分をうけた事例における、主な取引相手国（仕向地、経由地）を以下の図表 5 に整理した。

図表 5：不正輸出の取引相手国（下線は、2018 年以降に処分された事例における仕向地/経由地）

分類	内容
仕向地	北朝鮮、中華人民共和国、大韓民国、ミャンマー連邦、タイ王国、シンガポール共和国、マレーシア、イラン・イスラム共和国、フィリピン、インドネシア、米国、東ドイツ（ドイツ民主共和国)、ポーランド
経由地	香港、中華人民共和国、中華人民共和国（大連)、大韓民国、大韓民国（釜山)、シンガポール共和国、マレーシア、台湾、イラン・イスラム共和国

また、行政処分をうけた法人や個人の業種や属性について、主なものを類型化して抽出すると以下のとおり（下線は、2018 年以降に処分された事例における業種や属性)。

- 貿易会社（化学品、建築材、PC、海産物、日用品、機会装置、自動車 等）
- 製造業
- 産業廃棄物運搬業
- 運送業
- 会社役員
- 元会社役員
- 北朝鮮旅行者
- 無職少年
- EC サイト運営会社
- 卸売業
- 旅行代理店
- 日朝友好協会関係者

[4] https://www.cistec.or.jp/export/ihanjirei/index.html

[5] https://www.npa.go.jp/bureau/security/publications/kaiko_to_tenbou/R3/shiryou.pdf

また、経済産業省は、輸出管理不備等のケースも含め、外為法違反として何らかの行政処分（制裁、警告、口頭注意、報告書等）をうけた企業の傾向を外為法違反事例分析[6]として公表している。これによると、外為法違反事例の仕向け地や主体（企業規模等）には、以下のような傾向が見て取れる。

- 仕向地
  - ✓ アジア向けが 57%と最多
  - ✓ 次いで、先進国の多い地域である欧州及び北米がともに 20%
- 主体（企業規模等）
  - ✓ CP 届出別でみると、CP 届出企業以外の割合が高い（65%）
  - ✓ 資本金別でみると、3 億円以下が過半（56%）を占める
  - ✓ 従業員別でみると、300 人超と 300 人以下で約半々の割合

② 国のリスクアセスメント（リスクの特定・評価）

日本における資金情報機関（FIU）である JAFIC（警察庁刑事局犯罪対策部組織犯罪対策第一課犯罪収益移転防止対策室）は、国内のマネー・ローンダリング及びテロ資金供与のリスクを特定・評価する報告書（NRA：犯罪収益移転危険度調査書）を平成 26 年より毎年作成し公表している。

FATF “Anti-money laundering and counter-terrorist financing measures JAPAN Mutual Evaluation Report（2021）”（以下、「第 4 次審査報告書」）においては、国によるリスク評価の手法について、以下のような指摘がなされたところ、令和 3 年度版以降は、これらの指摘事項を念頭に分析・記載の充実化が図られている。

- クロスボーダーのリスクを含め、日本経済を取り巻く広範なリスクの理解を深める必要がある
- 疑わしい取引の届出に加え、法執行機関や独立した情報源から得られる追加の情報を活用する必要がある
- 脅威や脆弱性へのフォーカスを増やす必要がある

なお、2023 年 3 月末現在、日本では拡散金融に特化した NRA は策定されていない。

③ 金融機関等のリスクアセスメント（リスクの特定・評価）

第 4 次審査報告書において、日本の民間セクターの企業は、国のリスク評価（犯罪収益移転危険度調査書）やその他の評価結果を認識しているとされている。

拡散金融ついても、金融機関は、制裁逃れの可能性が高く注意を要すべき輸出品目を認識しており、年間約 1200 件から 1700 件の拡散金融に係る疑わしい取引の届出を実施してい

[6] https://www.meti.go.jp/policy/anpo/gaitameho_document/ihanjireigaitamehou3.pdf

ることが評価されている。

他方、金融庁監督下以外の金融機関、およびDNFBPsは、リスク評価の実施が、犯罪収益移転防止法の規定にもとづく努力義務であり、リスク評価を最新に保つことを保証するには不十分であると評価された。

④　国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）

「外国為替及び外国貿易法（外為法）」や「関税法」による対外取引の規制、「国際テロリスト財産凍結法」による居住者間取引の規制、「テロ資金提供処罰法」による資金等の提供等に係る規制、その他、「特定船舶入港禁止法」や「貨物検査特別措置法」等の輸送・運搬等に係る規制等により措置している。

第 4 次審査報告書において、これらの標的型金融制裁に関連する法規制や運用に関し、主に以下のような点が指摘された。

- 国際テロリスト財産凍結法は、大量破壊兵器関連計画等関係者を措置できない点
  - 将来的に日本の居住者が制裁対象に指定された場合、対外取引を規制する外為法で対処できない
  - 国際テロリスト財産凍結法は、従来、国際テロリストを対象としており、大量破壊兵器関連計画等関係者を規制できない
- 外為法における「支払等」の定義が明確ではない点
  - FATF が要求する「資金その他の資産の移転、転換、処分または移動の禁止」の措置を講じる上でギャップがとなる可能性がある
- テロ資金提供処罰法は、規制対象としてカバーできる資金供与活動が限定的である点
- 国連による制裁対象のリストアップから官報公示までにタイムラグがある点[7]

これらの指摘内容（及び、その他マネロン等全般や刑罰に係る指摘内容等）を踏まえ、国際テロリスト財産凍結法を始めとした関係法令の改正案が、「FATF 勧告対応法案」として取りまとめられ、国会の審議を経て 2022 年 12 月に成立・公布された。

図表 6：FATF 勧告対応法案で改正された法律の概要

法律	主な内容
国際テロリスト財産凍結法	● 拡散金融への対応（居住者間取引に係る資産凍結）

[7] 但し、国連による制裁対象先の約 1/3 は、独自制裁により先行して対象指定済であり、北朝鮮が関与する資金又は物品の移転の全般的な禁止が実施されている。また、対象の指定の効力が日本国内で発生する前に金融機関等に対して連絡する仕組みがある等の点からギャップは限定的であるとされた

外為法	● 金融機関、暗号資産交換業者等による資産凍結措置の態勢整備義務 ● ステーブルコイン取引への対応（資産凍結）
組織的犯罪処罰法	● マネロン罪の法定刑引上げ ● 犯罪収益等として没収可能な財産の範囲の改正
麻薬特例法	● マネロン罪の法定刑引上げ
テロ資金提供処罰法	● テロ資金等提供罪の強化
犯罪収益移転防止法	● 暗号資産等に係るトラベルルール・法律・会計等専門家の確認義務等に係る規定整備

（出所）内閣官房公表資料

⑤ 金融機関等による標的型金融制裁への対応

第 4 次審査報告書において、日本の金融機関は、北朝鮮やイランに関連する標的型金融制裁を遵守するため、自社の規模や特性に応じ、メガバンクはリスクベースとリストベースの組み合わせ、地方銀行はリストベースの対応を実施していることが多いと評価されている。また、年間約 1,200 件から 1,700 件の拡散金融に係る疑わしい取引の届出を行っており、拡散金融対策に対する一定の理解が窺える一方で、届出が多いということは、取引が多いことの証左でもあるため、効果的な資産凍結が実施されていない懸念があるとされている。

また、財務省と金融庁による検査・監督において、金融機関における標的型金融制裁の措置に関連した対応の不備が多く確認されている点を踏まえ、金融機関の対応や当局による監督措置の有効性について懸念があるとされている。

⑥ その他企業（貿易会社等）による標的型金融制裁への対応

第 4 次審査報告書において、当局によるリスクベースでのアウトリーチを通じ、貿易金融、保険、海運、漁業等、拡散金融に係るリスクの高いセクターの理解は良好であると評価されている。

また、①に記載の経済産業省による外為法違反事例分析によると、外為法違反企業全体の 65%が輸出管理内部規程（CP）を届出ていない企業が占めることや、CP を届出ていない企業は、届出ている企業と比較して自主通報の割合が低い（公的機関による指摘の割合が高い）傾向がみられる。

⑦ 国の金融機関等に対する拡散金融対策の監督・アウトリーチ

第 4 次審査報告書において、当局は金融機関および DNFBPs を含む拡散金融リスクの高いセクター、その他関連する業界団体等にアウトリーチを実施していると評価されている。また、アウトリーチの手法として、拡散金融に焦点を当てた「疑わしい取引の参考事例」を

追加する等の対応が指摘されている。

他方、⑤に記載のとおり、財務省と金融庁による検査・監督において、金融機関における標的型金融制裁の措置に関連した対応の不備が多く確認されている点を踏まえ、金融機関の対応や当局による監督措置の有効性について懸念があるとされている。具体的には、2018年に実施された検査において、対象の金融機関の約半数が外為法に関連した不備が発見されたことが指摘されている。

また、拡散金融対策の遵守について、DNFBPs を組織的に監督していないことが指摘されている。

⑧　国のその他企業（貿易会社等）に対する拡散金融対策の監督・アウトリーチ

⑥に記載のとおり、第 4 次審査報告書において、当局によるリスクベースでのアウトリーチを通じ、貿易金融、保険、海運、漁業等、拡散金融に係るリスクの高いセクターの理解は良好であると評価されている。

他方、テロ資金供与の訴追、対象を特定した金融制裁、及びテロ資金供与リスクに対処する必要のある NPO 等セクターへの支援に関しては不十分な点が存在するとされている。

⑨　国の拡散金融機関対策に係る組織・体制（組織間の連携、調整等の観点を含む）

第 4 次審査報告書において、関連する当局は北朝鮮関連の核拡散対策が国家安全保障上の最優先事項であると捉えており、これは民間セクターへの監督・アウトリーチや、北朝鮮との貿易に関する制限措置、違反に対する強力な対応措置等に反映されていると評価されている。北朝鮮関係の国連制裁に係る対応を協議する枠組みとして、外務省、警察庁、公安調査庁、国土交通省、財務省、経済産業省等の関係省庁が参加する国家安全保障会議（NSC）が整備されている。その他、警察が拡散金融違反の特定、抑止において有効な機能を果たしている点、財務省と金融庁による共同検査の枠組みが、財務省が有する北朝鮮関連の制裁回避の類型に関してのノウハウの活用に繋がっている点等が評価されている。

他方、商業・法人登記制度を所管する法務省の関わりが限定的である点、法執行の観点では良好な省庁間協力・連携が行われているも政策の策定のための協力・連携には改善の余地があると指摘されている。

⑩　国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）

第 4 次審査報告書において、日本の北朝鮮との地理的な近接性や、国際金融センターとしての役割の大きさ、国際貿易における重要性等の点から、拡散金融の観点で大きな脆弱性に晒されているとされている。①でも記載のとおり、実際に外為法違反事例の傾向として、アジア向けが 57%と最多であり、地理的な近接性や貿易関係の結びつきが拡散金融の脆弱性に影響を及ぼしていることが窺える。

⑪　拡散金融に利用される金融機関等と金融サービス

第 4 次審査報告書において、海運会社による運賃名目でのイランへの不正送金や、貿易金融、特に中国の特定地域に所在する自然人や法人が関与するクロスボーダー取引の脆弱性が指摘されている。

⑫　拡散金融に利用されるその他の産業と貿易等の形態や品目等

拡散金融に利用されるその他の産業や貿易、品目等の特徴を把握するため、①と同様に、一般社団法人安全保障貿易センターが公表する外為法違反事例、及び、警察庁が公表する対北朝鮮措置に係る事件一覧より、不正に輸出（輸入）された品目を抽出した（図表 7）。これを踏まえると、拡散金融に利用され得るリスクの高い貿易や品目の特徴は、①大量破壊兵器や武器等の研究、開発、生産、運搬等に利用され得る物品、すなわち、電子機器や産業機械、車両、化学材料等の輸出、②国内の政治体制の維持等に利用され得る奢侈品等の輸出、及び、③外貨獲得の手段になり得る制裁先の生産物等の輸入の 3 つに類型化される。なお、不正輸出（輸入）事件における最近の傾向としては、大型の産業機械や車両よりも、電子機器や機械部品、日用品等の取引に係る検挙事例が多くみられる。

図表 7：不正輸出事件における品目（下線は、2018 年以降に処分/検挙された事例における品目）

参照文献	分類	品目[8]
外為法違反事例（一般社団法人安全保障貿易センター）	輸出	【電子機器・電子部品】 サーボモーター、航空機搭載用赤外線カメラ、振動試験装置の制御用プログラム、IC、イメージ増強管、周波数変換器、数値制御工作機械（マシニングセンタ等）、数値制御装置付工作機械用自動プログラミング装置のコンピュータ、飛行安定装置ローレロン、中古パソコン、ゲルマニウムトランジスター、シンクロ・スコープ、シグナル・ジェネレーター、サンプリング・オシロスコープ、非磁性のスクーバ用ダブルバルブ、測定装置 【産業機械・産業機械部品】 炭素繊維製造装置の部分品となる不融化炉の炉殻、半導体製造装置「マスクアライナー」、誘導炉、熱交換器、工作機械、中古半導体製造装置、振動試験装置振動台付駆動コイル、直流安定化電源、直流磁化特性自記装置、凍結乾燥機、3 次元測定機、製造設備一式、磁気測定装置、小型円筒研削盤、大型金属工作機械及びその付属品、特殊なポンプ、鏡内目盛板「レクチル」、ジェットミル 【運搬・車両・車両部品】 大型タンクローリー、中古パワーショベル、自転車、中古自動車、

[8] 参照文献より確認できた品目を対象に、【　】の分類は NTT データ経営研究所にて実施

		高級中古車、自動車の中古タイヤ、トラックトラクタ（トラックの動力部分)、トラックトレーラー、自動車用スプリング、無人ヘリコプター 【化学・材料】 炭素繊維、硫化ナトリウム九水和物、高純度のダイフロン（フロン系液体)、フッ化水素酸、フッ化ナトリウム 【日用品・食品・奢侈品】 冷凍タラ、日用品、シャンプー、ガスコンロ、壁紙、カップ、漁網、粉ミルク、モザイクタイル、化粧品、ニット生地、缶コーヒー、たばこ、日本酒、スロットマシン、卓球用品、厨房用品、日用雑貨、家具、コーヒー、チョコレート、ファンデーション、ボウリング用品、みかん
対北朝鮮措置に係る事件一覧（警察庁)	輸出	【電子機器・電子部品】 サーボモーター、赤外線カメラ、ソナー、イメージ増強管、ゲルマニウムトランジスター製造設備、周波数変換器、ノート型 PC、中古 PC、サンプリング･オシロスコープ、ジェットミル、シグナル･ジェネレーター、シンクロ･スコープ、振動試験装置振動台付駆動コイル、測定装置、飛行安定装置、非磁性スクーバ用ダブルバルブ、三次元測定器 【産業機械・産業機械部品】 炭素繊維製造装置、大型金属工作機械、真空吸引加圧鋳造機、直流安定化電源、直流磁化特性自記装置、凍結乾燥機、半導体製造装置、噴霧乾燥器、ポンプ、工作機械、鏡内目盛板、真空ポンプ、プラズマエッチング装置を使用するためのプログラム 【運搬・車両・車両部品】 中古タイヤ、中古高級自動車、中古自動車、パワーショベル、タンクローリー、無人ヘリコプター 【化学・材料】 炭素繊維、ニッケルの粉、炭素繊維の成形品、銘木、フッ化水素酸、フロン液体 【日用品・食品・奢多品】 日用品、冷凍タラ、家具、壁紙、化粧品、粉ミルク、食品、食料品、スロットマシン、ニット生地、布地、ボウリング用品、粧品、清酒、タイル、たばこ、陶磁器製品、ピアノ 【武器】

		ライフルスコープ
	輸入	【日用品・食品】 ビール、食料品、アサリ、ウニ、サルトリイバラ、ショートパンツ、ステンレス継手、化粧品、松茸

⑬　拡散金融に利用されるその他の手段（サイバー攻撃等）

JAFIC が公表する「犯罪収益移転危険度調査書」において、北朝鮮の国家的関与がうかがわれるサイバー攻撃集団（「Lazarus（ラザルス）」）による日本の暗号資産関連事業者等を標的としたサイバー攻撃が行われていることが指摘されている。これらのサイバー攻撃集団は、搾取した暗号資産の移転に際し、ミキサーと呼ばれる技術を利用することでブロックチェーン上の取引履歴をかく乱し、追跡を困難にするとされ、欧米の複数の当局が、ミキシングサービスへの経済制裁措置も課している。

（2）米国

① 拡散金融の主体、協力者

図表 1 に示す文献にて、図表 8 に示す国を拡散金融に関する脅威国と評価している。また、図表 8 に示す脅威国における拡散金融の主体や協力者を図表 9 に示す。

図表 8：脅威国

脅威国	概要（評価の内容）
北朝鮮	● 世界、また米国に対して、最も複雑な PF の脅威である ● 核および弾道ミサイルの能力を向上させるために直接的に貢献する、高度な制裁回避スキームを継続的に運用し、歳入を増やしている
イラン	● イランが依然として中東地域の安定をさらに脅かす大量破壊兵器の能力を求めていることを懸念している ● イランの核拡散の脅威は、兵器用ウラン濃縮による潜在的な核の「ブレイクアウト能力」と弾道ミサイルの能力によって最も顕著に示されている
シリア	● 化学兵器の使用と化学兵器禁止機関に対するアサド政権の対応の欠如を脅威とみなしており、米国は、長年の国際規範に違反する化学兵器の使用など、シリア内戦におけるシリアのアサド政権に対する強固な制裁プログラムを維持している
中国	● 国家戦略の「軍民融合戦略」を通じて、中国の民間の研究開発と軍事・防衛産業部門との間の障壁をなくし、軍事力の近代化を進めている ● イランや北朝鮮等の制裁対象国のように収益を上げる活動をしているわけではないが、自国では生産できない米国発の技術を求めている
ロシア	● 通常兵器と核兵器の両方で優勢と思われる米国に対抗するため、軍事力の近代化を進めている ● イランや北朝鮮等の制裁対象国のように収益を上げる活動をしているわけではないが、自国では生産できない米国発の技術を求めている
パキスタン	● インドに対する脅威の認識から、核兵器と高度なミサイル能力を開発している ● 既存の核兵器および通常戦力を増強するために、米国由来の物品、技術、専門知識を求めている

図表 9　拡散金融の主体や協力者

脅威国	拡散金融の主体や協力者
北朝鮮	● 北朝鮮の国営企業や金融機関、ブローカー、エージェント、銀行代理店、第三国に拠点を置く外交官 ● 米国から機密性の高い物品やデュアルユース物品（民間用と軍事用の両方の用途を持つ品目）を取得するために米国の金融システムを利用する拡散金融行為者
イラン	● 不正な石油輸出を行う企業 ✓ イラン産原油を海外の顧客に不正に輸出して得た収益の一部はイランの軍事力増強のための資金となっている可能性がある
シリア	● シリア科学研究センター等の団体 ✓ シリア向けの特殊な機器を入手しており、米国の制裁と輸出規制に違反している ● レバノンやシリアに拠点を置く個人および企業 ✓ シリアの大量破壊兵器プログラムのために米国原産品を求めている ● シリア国外に拠点を置く科学技術材料の供給者 ● 機密性の高い技術やデュアルユース技術の取引に関与するプローカーや個人
中国	● 北朝鮮と違法な天然資源貿易を行う企業
ロシア	● ロシアの活動を支援する第三国企業 ● 北朝鮮と違法な天然資源貿易を行う企業
パキスタン	● パキスタン政府機関による核開発計画の実現に向けて、米国産の物品を販売し、米国の金融システムを利用する者 ● サウジアラビアや UAE などの第三国の個人や団体

② 国のリスクアセスメント（リスクの特定・評価）

財務省のテロ資金調達・金融犯罪局が、米国政府機関（NPFRA 作成に関与した機関を図表 10 に示す）と共に NPFRA（国家拡散資金リスク評価）を実施している（直近では 2022 年と 2018 年に実施）。

図表 10　NPFRA 作成に関与した米国政府機関

米国政府機関		2018 年	2022 年
商務省	産業安全保障局	○	○
国防総省	国防総省政策担当次官事務所		○
国土安全保障省	大量破壊兵器対策/戦略、計画、	○	○

	政策局		
	調査局		○
	政策局	○	
	米国移民税関捜査局	○	
	情報分析局	○	
司法省	刑事局	○	○
	連邦捜査局	○	○
	国家安全保障局	○	○
国務省	国際安全保障・不拡散局	○	○
	経済商務局	○	
財務省	テロ・金融情報局	○	○
	金融犯罪取締ネットワーク	○	○
	外国資産管理局	○	○
	情報分析局	○	○
	テロ資金調達・金融犯罪局		○
連邦機能規制当局	―	○	
国防総合大学	―	○	
国家情報長官官房	国家拡散防止センター	○	

③　金融機関等のリスクアセスメント（リスクの特定・評価）

米国の金融機関及びその他の米国企業は、FATF 基準の改正に沿った国内の AML/CFT フレームワークにより、北朝鮮及びイランに関するリスク評価を既に実施しており、当該リスクを軽減している。

④　国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）

米国政府は、拡散金融の国家安全保障への影響を考慮し、法律や規制等（大量破壊兵器拡散に関する大統領令 13382 および、北朝鮮、イラン、シリア、ロシアに対する国別制裁権限を含む）を組み合わせて、主に以下 2 点に関する取組を実施しており、制裁措置の違反に対して、民事および刑事上の制裁を科すことができる。

- 大量破壊兵器部品および関連物質の追跡と管理
- 拡散ネットワークが米国の銀行やその他の金融サービスプロバイダーにアクセスし、米国製造事業者から拡散関連部品を購入することを防止

北朝鮮やイラン、シリア等の脅威国に対する個別の取組みを図表 11 に示す。

図表 11　脅威国への個別の取組み内容

脅威国	取組み内容
北朝鮮	● 2020 年 9 月に国務省、財務省、商務省が「北朝鮮弾道ミサイル調達アドバイザリー」を発表
イラン	● 2017 年 2 月、OFAC はイランの弾道ミサイル調達に関わる複数のネットワークと支援者を指定 ● 2019 年 9 月、OFAC は、イランの海運または石油部門と取引する者が最終的にイスラム革命防衛隊に支援を提供する可能性があるリスクを強調するガイダンスを発表 ● 2020 年 9 月、国務省、財務省、商務省は、イランの核、ミサイル、通常兵器活動に対する最も広範な制裁と輸出管理制限を発表し、大統領令 13382 と 13949 に基づき、個人と団体を指定 ● 2021 年 7 月、商務省は、レバノンとイランに所在する 4 人の個人と企業を、適切なライセンスを取得せずにイランへの米国原産品の輸出に関与したとして、輸出管理規則の事業者リストへ追加
シリア	● 2014 年と 2015 年に起きた、シリア政府による自国民への塩素ガス攻撃を受けて、個人や団体を個別制裁対象に指定 ● 2017 年 4 月のアサド政権によるサリン攻撃を受けて、OFAC は、シリア科学研究センターの職員 271 名を指定
中国・ロシア	● 2021 年 1 月、商務省は、中国、キューバ、ロシア、ベネズエラの軍事エンドユーザーを支援する米国技術および米国人が行う特定の活動、ならびに特定の種類の兵器運搬システム、生産施設、メンテナンス、修理、オーバーホールを含む無許可大量破壊兵器プログラムに関する規制を発表
パキスタン	● 2019 年、商務省は、パキスタンの米国輸出規制違反に特に焦点を当てた輸出業者向けデューデリジェンス・ガイドを発表 ● 2021 年 11 月、パキスタンの安全保障されていない核活動や弾道ミサイル計画に貢献したとして、中国とパキスタンで活動する 16 の団体と個人を指定

⑤　金融機関等による標的型金融制裁への対応

まず、米国の金融機関における課題（脆弱性）として、以下 3 点が指摘されている。

- 内部関係者の共謀、または銀行自身の AML/CFT コンプライアンスプログラム内のシステム上の欠陥が一部存在する
- 海外の金融機関の顧客に代わって取引を清算する際、貿易金融におけるドル精算等特定の種類の取引では、取引に関する基礎情報が不足している可能性がある

- 米国の金融機関は PF に関する理解が十分ではない（PF がマネー・ローンダリングやテロ資金供与等の違法な金融活動とどのように異なるのかを理解できていない）

次に、金融機関等による対応として、金融機関や BSA の下で AML プログラムの要件を持つ事業体は、顧客デューディリジェンス、取引監視、疑わしい活動報告の提出等の BSA 要件を適切に実施しており、リスクを軽減している。

また、顧客管理規則（CDD 規則）に則り、対象となる金融機関は下記を実施している。

- 口座を開設する企業の受益者の身元を特定し、確認する
- 法人の株式の持分を 25%以上所有する個人、及び経営を通じて法人を支配する個人を特定し、本人確認をする必要がある
- 顧客のリスクプロファイルを作成するため、顧客の性質と目的を理解する
- 疑わしい取引を特定・報告するために、継続的なモニタリングやリスクに応じた顧客情報の維持・更新を実施する

また、米国の金融機関には、特定の高リスクの外国コルレス銀行に対して、強化されたデューディリジェンスの実施が求められている。

- 外国コルレス銀行が、他の外国銀行の入れ子口座を維持しているかどうかの確認
- 上場していない外国コルレス銀行に関する受益者情報の収集
- 外国シェル銀行のコルレス口座を維持することを禁止

⑥　その他企業（貿易会社等）による標的型金融制裁への対応

米国の金融機関及びその他の米国企業は、FATF 基準の改正に沿った国内の AML/CFT フレームワークにより、北朝鮮及びイランに関するリスク評価を既に実施しており、当該リスクを軽減している。

⑦　国の金融機関等に対する拡散金融対策の監督・アウトリーチ

米国は、ガイダンス（FATF の PF リスクアセスメントガイダンス等）や官民の情報共有メカニズム（以下に例を記載）を通じて民間部門との関与を深め、民間部門による PF 防止のためのリスクベースアプローチを支援している。

（官民の情報共有メカニズムの例）

- 銀行機密保護法アドバイザリーグループ
- FinCEN が管理する米国愛国者法 第 314 条 (a) と第 314 条 (b) の情報共有規定

また、FinCEN の取り組みは下記のとおり。

- 2016 年 5 月 11 日、BSA 規則の一部を改正し、金融の透明性を向上させて、脅威者が企業を悪用して不正な活動を偽装することを防止するため「CDD 規則」を発行

- 2017 年 11 月、北朝鮮の PF 活動にかかる勧告を発行（“Advisory on North Korea’s Use of the International Financial System”）
  - ✓ 北朝鮮の PF 活動と米国の金融システムの関与方法を詳述
- 2018 年 10 月、イランの PF 活動にかかる勧告を発行（“Advisory on the Iranian Regime’s Illicit and Malign Activities and Attempts to Exploit the Financial System”）
  - ✓ イランに関する違法な可能性がある取引をより適切に検知し、外国の金融機関が米国制裁の義務をより理解して、イランの違法な取引がもたらすリスクに対処することを支援する勧告

さらに、2020 年 4 月、国務省、財務省、国土安全保障省、司法省は北朝鮮のサイバー脅威に関するガイダンスを発表し、北朝鮮の悪質なサイバー活動と、北朝鮮が外交政策の目的を果たすために金融機関や他の民間セクターをターゲットにしていることを周知した。

⑧ 国のその他企業（貿易会社等）に対する拡散金融対策の監督・アウトリーチ

米国内外で設立された法人の実質的支配者情報へのアクセスの欠如は、大量破壊兵器拡散の資金調達を含む様々な金融犯罪の抑止、混乱、捜査における重大な脆弱性と評価されている。

財務省やその他の米国政府機関は、金融機関からの潜在的な PF ネットワークに関する報告を支援するために、ターゲットとなる情報を共有している。米国政府機関のその他の取組みは以下のとおりである。

- 2020 年 5 月、財務省、国務省、米国沿岸警備隊は、海運業、エネルギー、金属セクター、および関連コミュニティに対する制裁勧告を発表し、海運セクターを含む主要セクターにおける不正資金脅威の防止に関するアドバイスを業界に提供
- 2020 年、マネー・ローンダリング防止法の一環として、特定の法人の設立時（非米国法人の場合は、米国で事業を行うために州に登録する時）および所有者の変更時に、受益者情報の収集を義務付ける規制を策定
- 2020 年、国務省は旗籍を持つ国に対し、不審船に関する情報共有のための情報共有協定「レジストリ情報共有コンパクト」に参加することを奨励

⑨ 国の拡散金融機関対策に係る組織・体制（組織間の連携、調整等の観点を含む）

米国は、PF ネットワークが複数の法域を跨いで運営されていることを背景に、より強固なグローバル CPF 体制の構築に向けて、2018 年から 2019 年にかけて、FATF 基準の更新と PF リスクの軽減に関する新しいガイダンスの採択を支持する等、様々な多国間フォーラムを通じて同盟国や他のパートナー国と協力することを積極的に目指している。

また、外国政府や外国金融機関と連携し、拡散金融に関する議論を実施している。

⑩　国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）

米国の経済・社会・産業構造等に係る脆弱性として、「米国金融システムの規模の大きさ」、「国際的な決済システムにおける米ドルの重要度の高さ」、「拡散関連技術の生産における米国製造業者の技術力の高さ」の 3 点が挙げられる。

- 米国金融システムの規模の大きさ
  - ✓ 多くの PF ネットワークは、米ドルで価格設定され取引される商品を売買する必要があるため（海運セクターでは、米ドルベースのグローバルなシステムに完全統合されている）、米国金融システムとの接点を必要としている
- 決済システムにおける米ドルの重要度の高さ
  - ✓ クロスボーダー融資、国際債務証券、外国為替取引量、外貨準備、貿易インボイス、SWIFT 支払い等に占める米ドルの割合は世界全体の 40%以上である
- 拡散関連技術（二重用途品を含む）の生産における米国製造業者の技術の高さ
  - ✓ 軍事利用の可能性がある部品等の高度な製造技術を有している米国や西ヨーロッパ諸国は、大量破壊兵器能力の開発を望む国の優先調達先となる

⑪　拡散金融に利用される金融機関等と金融サービス

拡散金融に利用される脆弱性がある金融機関等と金融サービスとして、「コルレス銀行」、「仮想資産の採掘・取引」、「貿易金融」の 3 点が挙げられる。

- コルレス銀行
  - ✓ フロント企業やシェル企業等の不透明な法人格を作り、コルレス銀行を通じて、一見合法的な商取引を米国の金融システム上で実施している
- 仮想資産の組織的な採掘や取引
  - ✓ PF ネットワークが、大量破壊兵器や弾道ミサイルのプログラムに必要な資金や技術等を調達するために仮想資産を使用したという証拠は確認できていないが、仮想資産は、収益創出や国境を越えた資産の移動に不可欠な役割を果たす
  - ✓ 仮想資産等の新たな金融分野には、強力な AML／CFT 規制・監督が不足し、当該事業者は FATF が要求する AML／CFT 義務を十分に認識しておらず、悪質なサイバー活動や、仮想資産の不正使用の可能性がある
- 貿易金融
  - ✓ 貿易金融は、銀行による貨物検査等が実施されないため、文書詐欺や偽造に対して脆弱になる可能性がある

⑫　拡散金融に利用されるその他の産業と貿易等の形態や品目等

拡散金融に利用されるその他の産業と貿易等の形態や品目等として、主に北朝鮮とイラン、シリアが利用している手法等を図表 12 に示す。

図表 12　拡散金融に利用されるその他の産業と貿易等の形態や品目等

脅威国	拡散金融に利用されるその他の産業と貿易等の形態や品目等
北朝鮮	● フロント企業、シェル企業の悪用 ✓ 第三国の個人や企業（制裁回避のスキームへの意図的な参加や、北朝鮮の PF ネットワークに利用されるコンプライアンス上の欠陥がある）を利用した取引を実施 ✓ 北朝鮮が利用するフロント企業、シェル企業、銀行代理店、企業向けサービス業者の多くは中国に拠点を置いているほか、中国の銀行を利用して、北朝鮮政府に代わって不正資金を移動している。拠点は特に、中国遼寧省の大連市、丹東市、錦州市、瀋陽市、と香港 ✓ 海運、貿易、繊維、衣料、漁業や海洋事業者はフロント企業としてリストアップされている ● 海洋事業者による不正な輸出入 ✓ 違法な天然資源取引や兵器製造に必要な米国産商品を密輸 ✓ 関連当局の監視を逃れるために、商品の不正な輸出入の際には、船舶 ID ロンダリング、フラグホッピング、AIS 操作等を用いている ✓ 商品のラベリングや貨物の統合・再梱包等によって、北朝鮮への配送を隠ぺい ✓ 「キャッチオール」規制の対象となるような物品を調達 ● 外交官の悪用 ✓ 第三国に合法的に滞在している北朝鮮外交官が政府を代表して取引を実施している
イラン	● 海洋事業者による不正な輸出入 ✓ 違法な天然資源取引や兵器製造に必要な米国産商品を密輸 ✓ 関連当局の監視を逃れるために、商品の不正な輸出入の際には、船舶 ID ロンダリング、フラグホッピング、AIS 操作等を用いている ✓ 不正な石油輸出（イラン産原油を海外の顧客に秘密裏に輸送するスキームが確認）を行っている ● フロント企業、シェル企業の悪用 ● 両替所の悪用 ● イラン中央銀行を含む高官を利用した不正取引の隠蔽
シリア	● 海洋事業者による不正な輸出入 ✓ 違法な天然資源取引や兵器製造に必要な米国産商品を密輸

	✓ 関連当局の監視を逃れるために、商品の不正な輸出入の際には、船舶 ID ロンダリング、フラグホッピング、AIS 操作等を用いている

⑬ 拡散金融に利用されるその他の手段（サイバー攻撃等）

制裁回避を実施する国家やグループは、ビットコイン等の既存の仮想資産を利用しており、一部の国家等は制裁逃回避のために、中央銀行デジタル通貨やステーブルコインの開発に取り組んでいる。また、資金調達のために、中央銀行や民間銀行等の伝統的な金融セクターに加え、仮想資産等の新興的な金融セクターも標的としたサイバー攻撃を実施している。

なお、朝鮮人民軍偵察総局等の北朝鮮のサイバー攻撃組織は、以下の目的の達成に向け、金融機関だけではなくその他の民間企業もターゲットとしたサイバー攻撃を実施している。

- 重要インフラの破壊
- 政権に批判的な人物への攻撃、
- 金融詐欺とマネー・ローンダリング
- コンピュータとネットワークシステムの攻撃による仮想資産生成（暗号ジャック等）

米国政府は、「伝統的な金融セクターと、仮想資産等の金融セクターの両方において、コンプライアンス文化を浸透させ、強固なサイバーセキュリティ規制を構築することは、大量破壊兵器拡散を直接支援するさまざまな不正な金融活動の防止と検知に役立つため、今後も米国政府の優先事項であり続ける」と評価している。

（3）英国

① 拡散金融の主体、協力者

英国は図表 13 に示す国を拡散金融に関する脅威国と評価している。

図表 13：脅威国

脅威国	概要（評価の内容）
北朝鮮	● 北朝鮮の石炭輸出は依然として、核・弾道ミサイル計画の資金調達の最も効果的な手段の 1 つである ● 北朝鮮の大使館と外交官は、国連安保理制裁に違反して、外交外の手段で収入を得たり、北朝鮮企業のビジネス機会を特定したり、正式な金融システムへのアクセスを支援するといった PF 活動を行っていることが知られている
イラン	● イランは、北朝鮮が行っている活動に比べれば規模は小さいものの、核兵器プログラムのための資金を得るために、同じような活動を多く行っている ● イラン経済の不透明さ、およびそれによってもたらされる不法金融リスクは、イランで事業を行おうとする英国の企業にとって大きなリスクと金融コストを生む ● イランの拡散者は合法的な手段で CBRN 拡散を財政的に支援する機会が少なくなっているため、この資金を得るために非合法な手段に注力することになっている ● 北朝鮮の行為者と同様に、英国の銀行口座を持つイラン人個人が英国外の無関係な第三者から支払を受領し、その後英国内の口座から英国企業に支払いが行われる例もある
シリア	● 化学兵器に関する自律的な制裁体制、The Chemical Weapons（Sanctions） （EU Exit） Regulations 2019 を実施している。シリアとロシアの個人と団体がこの体制で指定されている ● 石油とその他の石油化学製品を外国、特に中国とシリアに販売することは、イラン政権にとって重要な拡散資金収入を生み出している
ロシア	● 化学兵器に関する自律的な制裁体制、The Chemical Weapons（Sanctions） （EU Exit） Regulations 2019 を実施している。シリアとロシアの個人と団体がこの体制で指定されている

また、図表 14 に示す国を拡散金融の協力国と評価している。

図表 14：拡散金融の協力国

脅威国	概要（評価の内容）
中国	● PF 活動についてイランと北朝鮮が大きく取り上げられているが、中国を含む国家が世界の PF で果たしている役割は過小評価されるべきではない ● 2021 年 3 月の専門家パネルの報告書では、中国管轄区への石炭の「少なくとも 400 件の輸送」があり、そのほとんどが寧波-舟山地域に向かい、北朝鮮船舶が石炭の積み降ろしを続けている ● 石油とその他の石油化学製品を外国、特に中国とシリアに販売することは、イラン政権にとって重要な拡散資金収入を生み出している ● 北朝鮮のフロント企業やその代理人はしばしば中国の遼寧省を経由して出荷を行うが、これは支払いの構造、及びコルレス銀行の関係性が中国の金融機関との間で維持されていることを意味する

② 国のリスクアセスメント（リスクの特定・評価）

英国では、2021 年 9 月に“National risk assessment of proliferation financing”（「NRA-PF」）が公表されている。本ドキュメントは英国の政府、民間セクター、学界の幅広いパートナーからの情報をもとに、2020 年 12 月に更新された“National risk assessment of money laundering and terrorist financing 2020”（「ML/TF NRA」）を補完するものとして、英国財務省（HM Treasury）が公表している。

なお、NRA-PF については、英国における PF 分野に関する新たな脅威とリスクを反映するため、定期的に更新される予定である。

③ 金融機関等のリスクアセスメント（リスクの特定・評価）

2021 年 9 月に公表された NRA-PF 内において、財務省は民間部門に対して ML/TF リスク評価と同様の枠組みで PF リスク評価を求めることを計画している旨が明記された。

その後 2022 年 9 月に ML/TF 規則が改正され、規制の対象となる各事業者は PF リスク評価を作成する、ML/TF リスク評価に組み込むことが求められている。

④ 国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）

英国は、PF がもたらす脅威と戦うために、強固な規制的枠組みを有している。主な焦点は、北朝鮮、イラン、及び化学兵器活動に対する英国および国連の制裁制度の実施である。

制裁措置は、英国の司法権下にある者、英国人が英国外で行った行動、英国で設立された企業に適用される。国連が課す措置の下での義務は、関連する国連安保理決議、並びに制裁及びアンチ・マネー・ローンダリング法（SAMLA）の下で実施される CPF 制裁など、関連する CPF 措置が定められている。

英国は30年近くにわたり、マネー・ローンダリング防止を目的とした規制を設けてきた。これらは、FATFが定めた国際基準やEUの複数のマネー・ローンダリング指令に沿って発展し、近年の最も大幅な改訂は2017年6月で、欧州第4次マネー・ローンダリング指令と資金移動規制を反映したものである。

2002年犯罪収益法（POCA）には、英国全土で適用されるマネー・ローンダリング犯罪が対象とされている。さらに、2017年犯罪財政法（CFA）によって、POCA、2000年テロリズム法（TA）、2001年反テロリズム、犯罪及び安全保障法（ATCSA）が改正されている。これらの改正は、法執行機関や検察機関が汚職・犯罪資金を特定し、英国内で隠匿、使用、移動しようとする者から回収できるようにするための追加権限を提供している。なお、テロ犯罪防止・治安法はCBRNの開発、調達、使用に関連する犯罪も含まれている。

⑤　金融機関等による標的型金融制裁への対応

英国では、法律で定められた制裁対応に加え、各金融機関において送金先の地域に応じてリスクベースの対応を取っているように見受けられる。例えば、英国ではイランとの貿易は違法ではないことに加え、イランの関係者への制裁も対象を絞っているものの、金融機関の中には、輸出業者がイランに商品を輸出する際の支払いや、イランの事業体が関与する金融取引を促進することに抵抗を感じる事業者も一定存在している。

他方、金融機関等による標的型金融制裁が関与する脆弱性としては以下 2 点が指摘されている

- 北朝鮮大使館の外交官受け入れに関する要件[9]について、大手銀行では認識されていると想定されるが、他の銀行では理解が不足している可能性がある
- トラスト又は企業サービスプロバイダー[10]（TCSP）を利用して、銀行取引や信用履歴が残っている「シェルフカンパニー」[11]を購入し、信頼できる企業であるかのように見せかけたり、企業の実質的所有者の匿名性を高めたりする可能性がある

⑥　その他企業（貿易会社等）による標的型金融制裁への対応

英国のその他企業（貿易会社等）は米国のイランに対する域外適用を意識して活動していることが窺える。多くの英国企業は米国に大きなエクスポージャーを有している中で、米国による既存の制裁はかなり広範囲に及んでいることが要因である。そのため、たとえ英国で認められている事業であっても、イランとの取引に抵抗を感じる企業も一定存在している。

他方、フロント企業を利用した取引に関連した脆弱性については、以下の2点を指摘の上、併せて取引に関与する当事者及びその関係する事業体に対する制裁措置チェックの重要性

---

[9] 銀行口座の提供に関連する国連安全保障理事会決議の要件

[10] 日本には存在しないものの、いわゆる会社秘書役と呼ばれる事業。主に会社の設立等日本の司法書士、行政書士が行うような業務を行う

[11]売却目的で設立された企業

について明記している。

- 航空機部品の購入に関連し、英国、ドバイ、マレーシア、英領ヴァージン諸島（BVI）にフロント企業を設立し、最終的にシンガポールやマレーシアの企業からイランに横流しを行う不正調達ネットワークが存在していた
- 北朝鮮のフロント企業やその代理人はしばしば中国の遼寧省を経由して出荷を行っている

⑦　国の金融機関等に対する拡散金融対策の監督・アウトリーチ

英国は、国連安全保障理事会や金融活動作業部会（FATF）などの場で、核拡散金融に取り組む国際的な取り組みを推進する上で、主導的な役割を担うなど、当局主導の基、監督・アウトリーチの実施体制が整備されている。

例えば、金融機関（FI）及び指定非金融業・専門職（DNFBPs）の監督当局は、リスクベースの検査、デスクベースのレビュー、及び規制対象部門のモニタリングの一環として制裁順守を監視している。当局からの検査、監督を基に、事業者が自らのリスク評価の際に考慮することを当局は期待している。

金融制裁（CP に関連するものを含む）については、2016 年に金融機構監督局（OFSI）を設立することで、金融制裁の遵守の確保と監視のためのリソースの集約を行った。英国では OFSI が金融制裁を主導し、他の機関や政府部門からのサポートを得ながら、英国で金融制裁が適切に実施されることを保証している。2019-2020 年、OFSI は 9 億 8234 万ポンドに相当する金融制裁違反の可能性に関する 140 件の報告を受けている

また、OFSI は、AML 監督者フォーラム（AMLSF）を通じて、金融行為規制機構（FCA）（専門機関アンチ・マネー・ローンダリング監督局（OPBAS）を含む）、歳入税関庁（HMRC）及び専門機関監督者等の AML/CFT 監督者と、規制対象者への OFSI ガイダンスの周知等の問題について緊密に協力している。加えて、OFSI は、金融機関等が自らのコンプライアンス責任を果たすのに役立つガイダンスやアラートの提供も行っている。

⑧　国のその他企業（貿易会社等）に対する拡散金融対策の監督・アウトリーチ

英国は、厳格な輸出管理を適用することで、拡散の行為者が CBRN 関連物質を調達する機会を制限している。オーストラリア・グループ[12]やワッセナー・アレンジメント[13]のような国際的な制度に準拠した独自の輸出管理制度を採用し、二重使用品目や機密品目の取引

---

[12] この枠組は、オーストラリアが議長国を務めていることから「オーストラリア・グループ（Australia Group：AG）」と呼ばれる。化学及び生物兵器開発・製造に使用し得る関連汎用品及び技術の輸出管理を通じて、化学・生物兵器の拡散を防止することを目的とし、年 1 回（1994 年までは年 2 回）主にパリで総会を開催している。

[13] 通常兵器の輸出管理に関する、国際的な申し合わせである。42 ヶ国が協定を結んでいる https://www.mofa.go.jp/mofaj/gaiko/arms/wa/index.html

が国際安全保障に脅威を与えないように努めている。

他方、英国経済全体における PF の理解が不十分な場合、PF 関係者が果たす役割に対する認識が不足し、コンプライアンスチェックが行われなくなる点について指摘しており、監督・アウトリーチに関連した脆弱性が存在している。

⑨　国の拡散金融機関対策に係る組織・体制（組織間の連携、調整等の観点を含む）

⑦で述べたように、OFSI が金融制裁を主導し、他の機関や政府部門からのサポートを得ながら、英国で金融制裁が適切に実施されることを保証している。OFSI は国際的パートナー、同盟国と協力しており、定期的に米国や欧州の国々と情報交換（ベストプラクティスの共有、共通の優先事項の特定等）を実施している。

その他にも、国際的な CP と武器管理問題に関する専門知識と政策決定を一カ所に集約しすることを目的に、国防省（MOD）内に「拡散防止・武器管理センター（CPACC)」を 2016 年に設立している。これには、外務英連邦開発省（FCDO)、MOD、国際貿易省（DIT)、ビジネス・エネルギー・産業戦略省（BEIS）の職員が参画している。

⑩　国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）

英国の経済・社会・産業構造に関連した脆弱性について以下の 4 点が指摘されている。

- 世界における英国の金融システムの重要性
  - ✓ 英国の金融システムは、世界の金融システムにおけるその役割と、英国経済の開放性・透明性から、特に PF の脅威の影響を受けやすい
  - ✓ 英国経済の規模、開放性、及び最大の金融サービス輸出国である点は、英国の競争力にとって大きな利点であることに加え、特にロンドンが外国人投資家にとって魅力的である。ただし、同時に、世界の金融システムにおける英国の重要な役割を利用しようとする拡散的な行為に対して脆弱な国となっている
- 会社設立の容易性
  - ✓ もし、ある事業体が不正な活動のために使用されていることが取引中に発覚した場合、迅速に撤退し、今後の取引で同じ活動を行うための新しい事業体を設立しすぐに置き換えることができる
  - ✓ 登記所は英国の企業の透明性を確保する上で重要な役割を担っていたが、信頼できる企業のように見せかける等悪用する主体にとっても魅力的なものである ※より正確な情報を提供するため、登記所の権限を強化する計画が進行中
- 王室属領（CDs)、海外領土（OTs）
  - ✓ CDs、OTs の金融センターは PF 目的で法人設立や金融システムへのアクセスのために利用される
- 低利益率の事業者の存在
  - ✓ 一部の事業が非常に薄い利益率で運営されているため、注文を断る意欲を制限

する要因となり、行為者からのアプローチのリスクを負ってしまう

⑪　拡散金融に利用される金融機関等と金融サービス

拡散金融に利用される金融機関等と金融サービスについては、以下 2 点が指摘されている。

- 海上保険（再保険）
  - ✓ 海上保険のうち、特に元受保険者がアジアにある場合の再保険についてはリスクが高い
  - ✓ 再保険についてはコルレス銀行のリスクとやや類似しており、英国の保険会社は最初の引受プロセスから切り離されているため、元受保険会社が行ったデューディリジェンスや制裁措置の審査について、限られた範囲でしか知ることができない
  - ✓ 例えば、ロンドンの保険会社は、船舶が制裁活動に関与していたことが判明した場合、保険サービスを遡及的に停止するいわゆる制裁条項に頼ることが多い。しかし、情報の把握は顧客が提供した情報に大きく依存しており、例えば核拡散に敏感な品目が虚偽の書類によって隠されていないことを確認するために、保険会社が出荷を積極的に調査することは現実的ではない
- 英国の金融システム
  - ✓ 拡散関連の活動や行為者に関連する支払いは、英国の金融システムまたは英国に本社を置く金融機関の海外支店／子会社と相互に作用する可能性がある
  - ✓ 海外支店/子会社がアジアのように、活発な PF ネットワークが存在する、あるいは拡散国の間で取引があるため国に存在する場合、直接的に、またはコンプライアンス管理が不十分な現地国営銀行とのリンクを通じて、PF 活動を促進する可能性がある

⑫　拡散金融に利用されるその他の産業と貿易等の形態や品目等

拡散金融に利用されるその他の産業と貿易等の形態や品目等については、以下 3 点が指摘されている。

- 海運部門
  - ✓ 海運部門と海運関連保険は、拡散する行為者に頻繁に狙われている
  - ✓ 保険契約時点で船舶、所有会社が指定されず、その際の制裁チェックで北朝鮮関連であることが確認できなかった事例も確認されている
- 中堅の防衛関連下請け業者とデュアルユース品セクター
  - ✓ 行為者からのアプローチのリスクが高い先は、中堅の防衛関連下請け業者と二重使用品セクターである
  - ✓ 中堅企業は拡散リスクと供給者の輸出管理およびその他の義務（例えば化学兵

器法に基づく義務）についての認識が低い可能性がある

- 高等教育・研究セクター
  - ✓ 英国の学術機関に対する海外からの資金提供の増大は、特に CBRN に関連する研究の場合、拡散の野心を持つ国家からの潜在的な圧力に対して脆弱なものとなっている
  - ✓ なお、政府は大学、資金提供団体、産業界と協力し、敵対的な干渉から保護するための取り組みを行っている

⑬ 拡散金融に利用されるその他の手段（サイバー攻撃等）

拡散金融に利用されるその他の手段については、以下 3 点が指摘されている。

- 北朝鮮の PF 関連のサイバー犯罪活動
  - ✓ 世界中に及び、国際的な金融機関、中央銀行、取引所などの暗号通貨事業者からの窃盗やそれを通じた資金洗浄も含まれている
- イランの暗号資産活用
  - ✓ イランは代替金融システムの一部として運用するための中央銀行デジタル通貨の立ち上げを検討、加えて、暗号通貨の採掘を通じて資金を調達している
- 参加者を隠すために作られたフロント企業ネットワークの活用
  - ✓ エンドユーザーや拡散行為者の活動を隠しながら、軍事用物品の調達ネットワークを活用し、イラン人等が規制品目等を調達している

（4）豪州

① 拡散金融の主体、協力者

豪州は拡散金融の主体として、下記を列挙している。

- デュアルユース商品（民間用と軍事用の両方の用途を持つ品目）の調達、及び制裁を回避するために、豪州の金融サービスやインフラを使用する主体
- 拡散金融の促進、及び制裁を回避するために、豪州を拠点とする企業の構造を利用する主体
- 拡散金融の促進、及び制裁を回避するために、豪州または第三国の国民を利用する主体
- 豪州市民を利用して、拡散金融を実施する懸念がある行為者に向けて、機密性の高い技術や知識を調達または輸出する主体
- 拡散金融の促進、及び制裁を回避するために、指定非金融業者及び職業専門家（DNFBPs）を利用する主体

② 国のリスクアセスメント（リスクの特定・評価）

豪州連邦政府の金融情報機関（FIU）である豪州取引報告分析センター（AUSTRAC）は、FATF やその他の国際機関のリスク評価手法に関するガイダンスや報告書に従って、国家拡散金融リスク評価（以下、NPFRA）を作成し、2022 年 12 月 14 日に初公表した。

NPFRA には政府、及び民間分野の幅広い関係者の知識を基に、拡散金融リスクとその対策、及び取り組みの改善点における最新かつ統合的な全体像が描かれている。

AUSTRAC は、豪州の拡散金融リスクを下記のように評価している。

- 北朝鮮とイランに対する金融制裁の義務違反や不履行のリスクは低い
  - ✓ 業界調査の結果、最もリスクの高い主体（大量の国際取引を実施する、または貿易金融商品を提供する企業等）において、北朝鮮とイランに対する金融制裁の義務に高い理解と遵守が見られている
- 金融制裁の潜在的な回避のリスクは中程度
  - ✓ 金融制裁の回避を促進、または回避を可能にする脆弱性が存在する
  - ✓ 金融機関による疑わしい取引の検知や当局による捜査活動を困難にする脆弱性が存在する

③ 金融機関等のリスクアセスメント（リスクの特定・評価）

豪州銀行協会は、2021 年に金融機関等における制裁実施に関する好取組事例を含むガイドラインを発表している。AUSTRAC と豪州制裁局は、当該ガイドラインの作成を支援した。

④　国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）

豪州には下記 2 つの制裁制度がある。

- 包括的な制裁制度
  - ✓ 1945 年の国連憲章とその後の関連法のもとで、国連安保理の金融制裁、及び北朝鮮とイランに対する制裁を豪州の法律として統合したもの
- 北朝鮮とイランに対する独自の制裁制度

制裁制度は、豪州外務貿易省内の豪州制裁局にて管理されている。同局では主に下記を実施している。

- 政府機関、個人、企業、その他の団体を含む対象の団体に、制裁制度に関するガイダンスを提供する
- 制裁許可の申請と発行処理を実施する
- 個人、企業、その他の組織と連携し、法律遵守の推進と法律違反の防止を支援する
- 他の政府機関と連携し、制裁制度の遵守状況を監視する
- 違反が疑われる場合、法執行機関による是正措置や強制措置を支援する

豪州では、制裁制度のほか、拡散金融対策に関連する AML/CFT 法体系も整備されている。適用対象は、豪州の居住者だけではなく、豪州を拠点とする事業者、または海外にある豪州企業の子会社も含まれる。

また、豪州は 2018 年以降、国際的なパートナーと連携し、北朝鮮を発着とする物品の出荷を監視・抑止している。さらに、不審な活動をしている船舶の旗国に対して、外交的な働きかけを行い、国連の専門家パネルに情報を提供して調査に協力している。

⑤　金融機関等による標的型金融制裁への対応

豪州では、指定されたサービスを提供する 17,000 を超える事業者（デジタル通貨取引所の運営業者含む）は、AML/CFT 法に基づいて、疑わしい取引等の情報を AUSTRAC に報告している。また、拡散金融のコンプライアンス機能を有する金融機関では、下記のような取り組みを実施している。

- 金融制裁リストに対するスクリーニング
- 豪州の制裁制度に照らし合わせたスクリーニング
- 指定団体との関連やリンク先を特定するためのネットワーク分析
- 北朝鮮、及び北朝鮮国民とのすべての取引の禁止
- イラン、及びイラン国民とのすべての取引の禁止
- その他拡散金融に懸念がある国とのすべての取引の禁止
- 拡散金融リスク指標とレッドフラッグに対するスクリーニング
- 拡散金融が懸念される主体とのビジネスに対するデューディリジェンスの強化

- 拡散金融が懸念される地域でのビジネスに対するデューディリジェンスの強化

なお、デジタル通貨取引所に関する FATF のトラベルルールは未導入となっている。

⑥ その他企業（貿易会社等）による標的型金融制裁への対応

豪州では、輸出者や物品の所有者、またはその代理人は、豪州から輸出される全ての物品について、積み替え港や最終目的地等、物品と輸出取引に関する情報が記載された「輸出申告書」を豪州国境警備隊に報告する必要がある。

⑦ 国の金融機関等に対する拡散金融対策の監督・アウトリーチ

豪州制裁局は下記を提供し、業界が制裁義務を理解し、遵守することを支援している。

- AUSTRAC に登録したユーザーに、豪州の制裁制度やリストの変更にかかる最新情報を電子メールで配信する
- AUSTRAC に登録したユーザーがアクセスできるポータルサイト
  - ✓ ユーザーは一般的な問い合わせ、制裁許可の申請、制裁制度が自社のケースにどのように適用されるかの評価を要求する等が可能
- 制裁を受けた個人、及び団体を検索可能な統合リスト
- 北朝鮮やイランを含む豪州の制裁制度や関連する規制にかかるトレーニングやガイダンス資料
- AML/CFT への期待や制裁措置の遵守に関する様々なオンライン資料やガイドライン

しかしながら、現在の政府による拡散金融にかかるアウトリーチ、情報提供、トレーニング等は、主に北朝鮮とイランを想定するものであり、その他の国・地域の関与の可能性を含む広範な脅威に対するものではない。

また、下記の脆弱性も指摘されている。

- DNFBPs に対する直接的な制裁遵守の監督、及び AML/CFT における管理の欠如
  - ✓ 弁護士、会計士、トラスト・アンド・カンパニー・サービスプロバイダー（TCSPs）など、主要な DNFBPs は、AUSTRAC によって規制されておらず、AUSTRAC への報告義務がない
- 事業登録において、最終的な受益者情報の登録が必須ではない（但し、近代化事業登録プログラム（⑨参照）を推進中）
- 信託に関する州または連邦レベルの透明性メカニズムが存在しない

⑧ 国のその他企業（貿易会社等）に対する拡散金融対策の監督・アウトリーチ

上記⑦と同様

⑨　国の拡散金融機関対策に係る組織・体制（組織間の連携、調整等の観点を含む）

拡散金融対策における体制整備、及び実施について、下記機関は連携して情報共有等を実施している。

- 豪州取引報告分析センター（AUSTRAC）
- 豪州国境警備隊（ABF）
- 豪州連邦警察（AFP）
- 連邦検察庁長官（The Commonwealth Director of Public Prosecutions）
- 国防省の国防輸出管理局（DEC）
- 豪州外務貿易省（DFAT）
- 国家情報コミュニティ（NIC）

また、NIC に属する機関の間では、情報共有の取り決めを確立し、拡散金融に関する情報交換、拡散金融行為者の活動を監視し、排除するために協調している。

現在、豪州は、豪州事業登録簿（ABR）と、30 以上ある豪州証券投資委員会（ASIC）の登録簿を 1 か所に統合する予定（近代化事業登録プログラム）を推進している。本プログラムにおいて、既に豪州事業登録サービス（ABRS）が設立されており、企業役員の身元や豪州企業との関係を確認する「取締役識別番号」制度が導入されている。

⑩　国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）

豪州は、下記の脆弱性を認識している。

- 北朝鮮による拡散金融活動に対して脆弱なアジア地域との貿易が盛んである
  - ✓ アジアの一部地域は、北朝鮮との地理的な近接性、制裁遵守と金融犯罪に対する制度におけるギャップ、政治的なシンパシーや文化的な繋がりから、北朝鮮による拡散金融活動に対して脆弱である
  - ✓ 黄海や東シナ海の一部で、石油や石炭等の物資の瀬取りが行われている
  - ✓ 中国との貿易自体はリスクにはならないが、中国は、北朝鮮への規制された物品や密輸品の出入りの経路となっている
- デュアルユース商品、及び核拡散に敏感な商品等を輸出している
  - ✓ 資源採掘、自動車、航空宇宙、テクノロジーといった産業からの輸出含む
- 北朝鮮への輸出が禁止されている金属やその他商品について、拡散金融に懸念がある者による資源転用の可能性がある
  - ✓ 2022 年 1 月時点で、豪州には 350 以上の鉱山があり、世界的にも鉱物の主要輸出国となっている。豪州の鉱業に関する専門知識や技術、生産する鉱物は、北朝

鮮やイランに関心を持たれる可能性がある
  - ✓ 豪州の鉱山企業は、北朝鮮やイランの鉱山企業と合弁企業を設立し、これらの国々に技術的な専門知識や収入を得る機会を提供する可能性がある
- 一部の業界、主に中小企業の間で、拡散金融のリスクエクスポージャーや違法行為の指標に対する認識が低い

⑪ 拡散金融に利用される金融機関等と金融サービス

拡散金融の行為者は、活動に関する資金の確保や支払いのために、国内外の大手銀行を利用することが多く、一部、送金業者や外国為替業者を利用することもある。豪州が認識する金融機関や金融サービスにおけるリスクを図表 15 に示す。

図表 15：金融機関や金融サービスにおけるリスク

分類	リスク
全体	● 拡散金融は、マネー・ローンダリングのスキームを模倣したスキームで実施されることから、金融機関等が、拡散金融における資金調達や制裁回避行為と従来のマネー・ローンダリング行為を区別することが困難である
大規模な金融機関（事業を国際的に展開している）	● 取り扱う金融取引の量が多く、特に、取り決めが複雑かつ、複数の当事者や管轄区域が関与する貿易金融は、拡散金融に関連する活動の特定を困難にする
小規模な金融機関（貿易金融商品や、迅速かつ効率的な国際送金を提供しない）	● デューディリジェンスのプロセスが弱く、拡散金融リスクを認識していない ● 拡散金融の活動を特定するためのプロセスを整備していない
送金業者、外国為替業者、デジタル通貨取引	● デジタル通貨取引所 ✓ FATF のトラベルルールが未導入である

⑫ 拡散金融に利用されるその他の産業と貿易等の形態や品目等

拡散金融の行為者は、下記のような手段を用いて活動を偽装する。

- フロント企業やシェル企業を利用する
- 商品を偽装する
- 様々なサプライヤーから部品や付属部品を調達する
- 商品の最終仕向け先を隠すために、積み替え拠点を利用する
- 商品の管理基準値または報告基準値を基準値ちょうどで輸出する

- 実際に商品を取引する地域から物理的に離れた地域における金融サービスまたは取引を利用する（例えば、オーストラリアに籍を置く企業が、オフショア事業拠点から商品を出荷し、支払いを受けるためにオフショア事業拠点の金融サービスを活用する）

実際に確認されたケースの一例として、下記が挙げられる。

- 韓国出身の豪州市民は、オフショア銀行口座と豪州を拠点とする一連のフロント企業を利用して、石炭、黒鉛、銅鉱石、金、原油（北朝鮮に代わって、イランのガソリンを購入することを含む）、ミサイル、ミサイル関連技術等の様々な商品について、北朝鮮との取引を仲介した
- ニューサウスウェールズ州在住の夫婦は、合弁企業を設立し、ニッケル合金をイランに調達・供給した
  - ✓ 合弁企業は、英国を拠点にする企業からニッケル合金を調達。ニッケル合金は、英国からイランが所有するドバイの企業に輸送されて、その後イランのバンダル・アッバースに送られた
  - ✓ 本ケースについて、ニッケル合金が違法な目的で使用されたわけではないことが証拠により判明した。しかしながら、本ケースは、合弁企業が豪州の企業や金融構造から物理的に距離を置くことは、制裁回避行為の隠蔽に役立つことを実証した

また、特に親密または文化的な繋がりを持つ顧客層にサービスを提供する事業者は、顧客に対するデューディリジェンスが不十分であり（事業者が認識している顧客イメージと、顧客の実態にギャップがあるケース等）、拡散金融に利用される可能性がある。

⑬ 拡散金融に利用されるその他の手段（サイバー攻撃等）

NPFRA では、大規模な金融サービス部門とデジタル通貨取引所に対するサイバー攻撃の可能性があることを指摘している。AUSTRAC は、上記に対して適切なサイバーセキュリティ対策の実施を推奨している。

サイバー攻撃等は、下記図表 16 の脅威国によって実施される可能性があることを指摘している。

図表 16：サイバー攻撃等を実施する脅威国

脅威国	内容
北朝鮮	● 金融機関含む組織に、様々な悪意のあるサイバー攻撃を実施 ✓ 国連の専門家パネルによると、これらの活動は、北朝鮮の大量破壊兵器の重要な収入源になっているとのこと

脅威国	内容
イラン	● 金融機関に対してサイバー攻撃を実施 ✓ ただし、サイバー攻撃によって、ハッカーが金銭的な利益を得たか、金融制裁の回避を促進できたかは明らかになっていない ● イラン政府は、中央銀行デジタル通貨の開発を検討しており、米国の制裁を回避するために使用される可能性がある

（5）北朝鮮制裁専門委員会専門家パネル報告書

① 拡散金融の主体、協力者

図表 1 に占める専門家パネル報告書（2020～2022）が分析、指摘している拡散金融の主体を図表 17 に、協力者等を図表 18 に示す。

図表 17：拡散金融の主体

主体	概要
軍需産業部（Munitions Industry Department）	● 軍需産業部に所属する情報技術労働者は、音声フィッシングハッキングアプリケーションを販売し、複数の海外サーバーとインターネットプロトコルアドレスを運用することで外貨を取得 ● 軍需産業部に所属する情報技術労働者は、中国の大連に拠点がある企業と共に、マネー・ローンダリングに関与
偵察局（Reconnaissance General Bureau）	● 偵察局に所属するサイバー攻撃部隊（Kimsuky, Lazarus Group, BlueNoroff, Stonefly 等）が、機微情報の窃取のために、防衛関連企業へのマルウェアの配布や政府機関に対する DDoS 攻撃等のサイバー攻撃を実施 ● 2015 年以降、BeagleBoyz は、ATM や SWIFT 端末、金融機関の決済システムサーバーへのサイバー攻撃を通じて、約 20 億ドルを窃取。また、暗号資産取引所へのサイバー攻撃も実施 ● 2016 年にバングラデシュ中央銀行に対するサイバー攻撃を行った BlueNoroff は、「Snatchcrypto キャンペーン」と称し、サイバー攻撃の対象を銀行から、世界中の暗号通貨とスマートコントラクトを扱う企業にターゲットを変更 ● 2020 年の傾向として、Kimsuky, Lazarus は、世界各国（イスラエル島）の防衛産業に対してサイバー攻撃を実施し、軍事技術への不正アクセスに加え、金銭の窃取に利用できる情報へのアクセスを試みていた
人民武力省 デパートメント 53（Ministry of the People's Armed Forces, Department 53）	● 平壌に本部を置く兵器取引団体であり、少なくとも、2019 年～2021 年の機関に、ロシアから通信機器や電子部品等を入手 ● 2021 年後半から、北朝鮮労働者を雇用し、コンゴにおける多数の建設プロジェクト（病院や集合住宅等）に直接関与 ● 下部組織とフロント企業を所有し、コンゴ、モザンビーク、

主体	概要
	シリア・アラブ共和国、タンザニア連合共和国、ロシア連邦および中国に公認部隊（代表部）を設置している可能性がある
Haegumgang Trading Corporation	● 人民武力省傘下の兵器取引団体であり、2021 年 6 月に同社はナイジェリアへ350万ドル相当の軍事関連装備の売却を仲介する予定であった
朝鮮民主主義共和国大使館	● 大使館敷地内にあるホテル等外交施設の商用利用が確認されていた
海外で活動する北朝鮮資本の金融機関	—
国家が支援/運営するサイバー犯罪集団（Lazarus 等）	—
北朝鮮の商社や国防科学院	● 外貨獲得及び、兵器開発を支援するために、特に、中東諸国（シリア・アラブ共和国やイラン・イスラム共和国など）との間で、軍需物資を輸出入している可能性がある
北朝鮮の軍需代理店	● アフリカや東南アジアで兵器を販売しようとしている可能性がある

図表 18：拡散金融の協力者等

協力者	概要
スリランカ	● 2022 年 2 月、スリランカの閣僚が 1983～2009 年のスリランカ内戦中に北朝鮮より兵器を購入したことを認めた
赤道ギニア	● 国連の指定企業の北朝鮮の Korea Mining Development Trading Corporation と赤道ギニアの間に 2022 年初頭の時点で継続的な関係が構築
コンゴ民主共和国	● 北朝鮮による金採掘や大統領府への軍事訓練、武器売却の関与が疑われる
エリトリア	● 北朝鮮と武器関連の協力関係が疑われる
イラン	● 北朝鮮外交官による金や現金の密輸を支援していることが疑われる
ミャンマー	● 北朝鮮と弾道ミサイルの開発等を含む軍事的な協力関係が疑われる
北朝鮮労働者の雇用（IT、医療、建設、ケー	● アラブ首長国連邦 ● アルジェリア

協力者	概要
タリング、スポーツ等の分野）を受け入れている国	● カタール ● カンボジア ● コンゴ ● コードジボワール ● セネガル ● トーゴ ● ナイジェリア ● ベトナム ● ラオス ● ロシア連邦
中国企業	● XinXin Green Work Research & Development Co. Ltd.、Taizhou Yifeng Transportation Co., Ltd.などの中国企業が、北朝鮮原産の石炭の不正調達に関与 ● Jinzhao Art Museum145 などの中国企業が、北朝鮮の制裁先企業である Mansudae Art Studio と美術品等の取引を実施していたことが疑われる
東欧のサイバー犯罪集団（Trickbot グループ）	―
北朝鮮と学術交流を実施する海外の大学	● 金日成総合大学のウェブサイトに「姉妹校」として記載されている、4 つの大学（キューバ、インドネシア、シリア・アラブ共和国、ベトナムに 1 つずつ）は 2012 年から 2016 年の間に、同大学と協力協定を締結したとのこと ● ただし、4 つの大学は、同大学との交流プログラムの範囲は「法律、語学、観光、教育」に限られていると説明し、制裁違反は確認されなかった
北朝鮮に船舶を提供する主体	―

⑩　国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）

北朝鮮は、第三国の団体に漁業権を売却し、北朝鮮の海域での操業を許可していることが指摘されている。なお、4～5 ヶ月間の漁業権は、約 200,000 人民元（30,867 ドル）から 300,000 人民元（46,301 ドル）で販売されているとのことである。

また、北朝鮮領海、及び EEZ 内や中国領海では、船舶間輸送が実施されており、新しい規制回避の手法と評価されている。主な場所は下記のとおりである。

- 北朝鮮領海及び EEZ 内：南浦の南西 50 ㎞にある Ch'o-do Iskabd

- 中国領海内：Dongyin Island や Sansha Bay

⑪ 拡散金融に利用される金融機関等と金融サービス

北朝鮮が、拡散金融に利用する金融機関等と金融サービスとして、下記が指摘されている。

- NFT の利用
  - ✓ 収益創出とマネー・ローンダリングの両方の手段として、NFT の利用が増加
- オフショア口座の管理
  - ✓ 駐ロシア北朝鮮大使館の商業参事官課の三等書記官である、Hang Jang Su 氏がロシア連邦の銀行口座を所持、管理
  - ✓ 北朝鮮の FOREIGN TRADE BANK の代表者が中国の銀行口座を所持、管理
- 暗号資産サービスプロバイダー
  - ✓ 北朝鮮は、KYC に関する情報を十分に収集していないサービスをサイバー攻撃の標的としている
  - ✓ 暗号通貨を管理するグローバルな規制メカニズムが存在しないことを理由に、北朝鮮による暗号通貨取引所等を標的としたサイバー攻撃によって盗まれた資金の追跡が困難となっている
- 現金や金の利用
  - ✓ 北朝鮮の外交官が、協力国の外交ルートを通じて現金や金を密輸している

⑫ 拡散金融に利用されるその他の産業と貿易等の形態や品目等

北朝鮮は、図表 19 に示す手法を拡散金融に利用している。また、図表 20 に示す品目を不正に輸出または輸入していることが指摘されている。

図表 19：拡散金融に利用される手法

手法	概要
船舶の偽装、改造	—
第三国との合弁企業の設立	● 北朝鮮は制裁回避の目的で中国企業との合弁企業や協力団体の設立を続けている ● 合弁事業、オフショア口座、シェル企業、仮想資産（暗号通貨など）の利用を通じて国際金融システムへのアクセスを続けている
フロント企業の利用	● 北朝鮮の FOREIGN TRADE BANK のフロント企業が、2017 年以降に、200 万ドル相当の楽器と部品をロシアの企業へ輸出 ● 北朝鮮の MANSUDAE OVERSEAS PROJECT GROUP OF COMPANIES のフロント企業（Corman Construction）

手法	概要
	が、セネガルのダカールにおける複数の建設プロジェクトを通じて、収益を得ている ● 船舶や奢侈品の購入に、契約書に記載されていないサードパーティーの企業を利用し、支払を難解にする
シェル企業の利用	● 北朝鮮への石油の不正な船舶間輸送に関与する事業者はシェル企業(ペーパーカンパニー)を使用している ● ペーパーカンパニーを活用して受益者情報を難読化し、海外の企業と合弁会社を設立
船舶の自動識別システム（AIS）信号の未送信や、偽造した AIS 信号の送信	● 偽造した AIS 信号を送信している船舶は、特に中国の寧波-舟山水域で石炭を移送している
1 回の往復航海で、石炭の輸出と人道支援物資の輸入の実施	● 北朝鮮の船舶は、中国海域で石炭を降ろすと同時に、人道支援物資を積む
不動産賃貸	● ブルガリアの首都ソフィアにある北朝鮮が保有する不動産を、ブルガリアの企業が賃貸契約していた
北朝鮮国民の海外出稼ぎ労働	● 北朝鮮の海外労働者は、複数の国に滞在を続け、IT、建設、電子工学、農業分野で収入を得ている ● 北朝鮮国民が、東南アジアのいくつかの国で、レストランを営業していた可能性がある ● 北朝鮮の医療従事者 3 人と翻訳者 3 人がエクアドルのピンチャ州で働いていた
北朝鮮による不正な金融活動	● 東アジア及び東南アジア諸国に集中している。不透明な企業登録プロセスにより、コンプライアンスと顧客管理手続きが脆弱である
北朝鮮の銀行代理店の運営	● 北朝鮮の銀行代理店は、ロシアで 6、中国で 22、インドネシアとシンガポールで 1 ずつ、運営している可能性がある

図表 20：拡散金融に利用される品目等

形態	品目	概要
輸入	石油製品	下記手法で、石油製品を輸入している ● 一部を改造した貨物船 ● 複数（3 隻以上）の船舶による多段階の石油の積み替え

形態	品目	概要
		● 不正な船舶 ID の送信、他の船舶への偽装 ● 中国等の外国籍の大型船舶の利用 ● 海上で受渡用の中間船として追跡や識別が難しい小型船の利用
輸出	石炭	● 中国領海での石炭の積み下ろしを実施している ✓ 北朝鮮籍船は、2020 年 1～9 月にかけて 400 回、計 250 万トンの石炭を輸送。岐路に、中国から人道物資を輸送している ✓ 2021 年 2 月から 5 月に、北朝鮮の船舶から中国の寧波-舟山地域に少なくとも 41 回の輸送が行われ、北朝鮮を原産地とする 364,000 トンの石炭が輸出された ● 船舶 ID の操作（別の船舶との識別情報の交換等）、使い捨ての船舶 ID の利用
	美術品	● 北朝鮮の美術工房である Mansudae(万寿台)アートスタジオ所属の芸術家の作品が、韓国の美術展に展示された ● Mansudae アートスタジオで制作された美術品がベトナムのレストランで販売されている
	天然砂	● 北朝鮮の様々な種類の天然砂が、大量に中国の港に出荷されている
	ステンレス鋼、バルブ、ポンプ、ボールベアリング	● ステンレス鋼は、弾道ミサイルの計画に用いられるとされる
	鉱物資源、鉄、繊維製品	―
その他取引	現金と金	● 2020 年に北朝鮮による現金及び金の密輸にイラン人が関与 ● 北朝鮮の外交官が、協力国の外交ルートを通じて現金や金を密輸

北朝鮮の船舶は、継続してその出所を偽装しており、船主、運航者、商品取引者に対する更なるデューディリジェンスが必要であると指摘されている。

上記の現状を踏まえて、専門家パネルは加盟国に対して、石油等の不正な輸入に係る貨物船等に関する勧告を実施している。主な勧告を図表 21 に示す。

図表 21：加盟国への勧告

分類	勧告内容
北朝鮮による石油等の不正な輸入に関する勧告	● 改造等をした貨物船による精製石油の輸入について加盟国の海事当局が認識し、同国貨物船が自国の港等に寄港した際には必要な船舶検査を行うこと ● 船舶修理工場及び、関連する船舶ブローカーに対し、北朝鮮による欺瞞的行為と、それを支援する貨物船が北朝鮮に輸出される場合の影響等に関する情報を周知すること
北朝鮮船舶による船舶 ID 改ざん等への対応に向けた勧告	● 加盟国と船舶登録機関が、船舶の ID ロンダリングまたは改ざんの検出事例に関する情報（以下に一例を記載）を広く周知すること ✓ 偽装 ID を送信した登録船舶の ID ✓ 他の船舶に ID を利用された可能性のある登録船舶の ID ✓ 不正な ID を送信した船舶登録者の名前 ✓ 登録が抹消された船舶のリスト ● 海上移動業務識別コード(MMSI 番号)の不正使用の疑いが検出された場合、当該船舶等を特定、調査し、調査結果を他の海事当局やパネルに共有すること ● 船舶の識別子の有効性に疑いがある場合、港やその他関連する海事当局は、その港の管轄水域に侵入する該当する船舶の履歴を確認すること ● 加盟国は北朝鮮及び、北朝鮮に関連する船舶が操業している可能性がある海域で、疑わしい船舶識別子を発信している船舶を監視、及び調査すること ● 北朝鮮の漁業許可証を取得した船舶が、その活動と身元を不明瞭にするために用いる方法を特定し、その不正操業を防止するために警戒を行うこと
北朝鮮による船舶取得に関する勧告	● 引き渡しの際の AIS の完全監視、制限された航行条件への適合確認のための船舶検査、受取人との船舶引渡しの確認などを行うこと ● 船舶の売主に対し、船舶の最終目的地とエンドユーザー（所有者)、関連ブローカーの身元、過去の取引記録を含む情報を確認すること

分類	勧告内容
	● 船舶売却時に、船舶が北朝鮮または同国の関係者にいかなる形でも譲渡されないこと、買い手が北朝鮮の制裁違反を助長しないこと、および、そのような場合に買い手が責任を負うことを保証する確認書を買主から入手すること ● 船舶の譲渡後、船舶の安全保障理事会決議違反の可能性がある場合、売主、買主、ブローカーがそれぞれの当局に報告すること
貿易関連措置に関する勧告	● 北朝鮮および大韓民国（それぞれ KP および KR）の国別コードの誤用を防ぐため、適切な措置を講じること ● 禁止品目リストを活用し、輸出入管理リストを合理化すること ● 加盟国の税関当局が、特に制裁対象国の近隣で当該商品を扱う場合等に備え、管轄区域内の取引業者に禁止品目リストを共有すること ● 贅沢品や高級品を輸出する事業体や個人等に対し、北朝鮮への転売を防止する契約条項を含めることを奨励すること ● 精製石油の船舶間移送を行う当事者に対し、船長または担当乗務員が、関連する旗国登録機関に、事象の通知、関係船舶の船舶識別番号、移送材料と量、移送の開始・停止の日時、移送場所を示す電子メールを送信する権限を与えること ● 船舶間転送を行う船舶に対して適切な原産地証明チェックを可能にする管理手段の導入を検討すること ● 北朝鮮に出入りする個人の荷物を含む貨物の検査に警戒を払うこと ● 指定団体の美術品の移転に関する警戒を行うこと ● 船会社および運送会社に対し、積み替えのリスクを念頭に置き、荷受人の確認のためのシステムを提供するよう奨励すること ● 船主、船舶管理者、運航者が輸送に関して KYC 及び KYCV(Know your couterparty's vessel：取引先の船舶に関する理解)を引き続き強化すること ● 旗国登録機関は、自国船籍に加入を希望する全ての申請者に対して、船舶の外観（船首、船尾の甲板）及び、船舶識別装置が設置された船舶の内部の最新の写真を添付するほか、登録されたプロファイルとは異なる AIS 信号を発信する船舶への連絡や、AIS ステータスを監視する専任の担当者を確保すること

分類	勧告内容
	● 船舶登録機関に登録しようとしている全ての法人は、受益所有者情報を開示すること ● 船級協会は、定期的安全検査の一環として、各船舶にタイプ A の AIS システムが搭載されていることを証明すること ● 加盟国は、制裁対象国との取引を監視するために、国連貿易開発会議（UNCTAD）が開発した税関管理システム「ASYCUDA システム[14]」を使用すること（推奨）

専門家パネルは、実態を把握するために、加盟国、団体や個人に問い合わせを実施している。しかしながら、2021 年 9 月の報告書では、加盟国の全体的な回答率は 50%未満で、団体や個人の回答率はさらに低いと述べている。専門家パネルは、加盟国、団体や個人が、関連する安全保障理事会決議を遵守し、専門家パネルからの問い合わせにタイムリーに回答する必要があることを指摘している。

⑬ 拡散金融に利用されるその他の手段（サイバー攻撃等）

北朝鮮は、資金確保のために、サイバー攻撃等を実施している。主なサイバー攻撃等を図表 22 に示す。

図表 22：サイバー攻撃等

標的・手法	内容
暗号通貨取引所等を標的としたサイバー攻撃による資金の窃取	● 2020 年 9 月、暗号通貨取引所に対するハッキングにより、約 2 億 8100 万ドル相当の暗号通貨が窃取された ● 暗号通貨取引所や投資会社に対する 7 回の侵入を通じて、2021 年に合計 4 億ドル相当の暗号通貨を盗み出した ● 2022 年 3 月下旬、Lazarus Group が、ノンファンジブルトークン（NFT ゲーム）Axie Infinity を支える Ronin ネットワークをハッキングし、17 万 3600 イーサ（ETH）と 2550 万ドル相当の USD コインを盗んだ ● 2022 年 6 月下旬、Lazarus Group が「Horizon Bridge」へ不正ハッキングにより総額 1 億ドル相当の複数種類のトークンを窃取した。流出したそれらの暗号資産は、犯行後に DEX（分散型取引所）ユニスワップ（Uniswap）でイーサリアムに交換された

[14] https://asycudaorg/en/

標的・手法	内容
	● マルウェアに感染したアプリケーションを配布するために、合法的に見えるウェブサイトと会社名（Celas Limited）を使用
貨物物流会社に対する情報および資金の窃取	● 南アフリカの貨物物流会社に対してマルウェアによる攻撃を行い、物品の輸送経路等から制裁回避のための知見を得つつ、ランサムウェアによる収入を得ることも可能にしている
製薬会社を標的としたサイバー攻撃	● 北朝鮮と関連があるとされる者が、COVID-19 ワクチンを開発している製薬会社にサイバー攻撃を実施した
防衛企業等を標的としたサイバー攻撃	● 2020 年、Lazarus Group はロシアの防衛、エネルギー、情報技術部門に対して、「ThreatNeedle」と呼ばれるサイバー攻撃を実施。ドイツの防衛企業 2 社に対しても、偽の求人票を当該企業の従業員に送り付けて、サイバー攻撃を実施した
スピアフィッシングの実施	● 北朝鮮は、下記方法で、スピアフィッシング（フィッシング詐欺の一種）を実施している可能性がある ✓ フィッシングメッセージを送信・追跡するために、電子メールのマスマーケティングプラットフォームを利用する ✓ ニュース記事への関連リンクや添付ファイル（悪意のないもの）を使用して接触を開始する ✓ 一般的なクラウドベースのファイル共有プラットフォームで悪意のあるファイルを共有する ✓ 暗号資産取引所のサポート担当者にコールド・コーリングを実施する

北朝鮮は、サイバー攻撃等で窃取した仮想資産を下記の手法で資金洗浄している。

- 2017 年～2019 年ハッキングで得た暗号資産を「ピール・チェーン」と呼ばれる数千もの小規模取引で不明瞭な状態とした
- 北朝鮮は、2019 年～2020 年 11 月までに窃取した約 3 億 1,640 万ドルの仮想資産を、中国のブローカーを通じて資金洗浄を行った

上記を踏まえて、専門家パネルは加盟国に対して、北朝鮮によるサイバー攻撃や資金調達への対応に向けた勧告を実施している。主な勧告を図表 23 に示す。

図表 23：加盟国への勧告

分類	勧告内容
活動が不透明な企業の登録規制強化	● 制裁回避活動に匿名性を与える可能性がある企業の登録に関する規制に引き続き対処すること

分類	勧告内容
外国への投資等を行う企業へのデューディリジェンス強化	● 特にサハラ砂漠以南のアフリカにおける自治体の融資、補助金、外国直接投資を伴うプロジェクトの請負業者と下請業者に対するデューディリジェンスを強化すること
教育・訓練	● 経営者からパートタイム従業員まで、あらゆるレベルの個人に対して適切な教育、訓練、情報共有、助言のための資料を採用するよう助言すること
サイバー衛生強化	● 暗号通貨取引所へのアクセスを試みる全ての暗号通貨取引者に対し、取引時の二要素認証などのサイバー衛生強化に適切な注意を払うこと
事件の速やかな情報開示	● 盗まれた資産の回収の見込みを高めるため、サイバー攻撃を受けた企業は、できるだけ早く適切な法的機関に報告し、事件の公表を行い、ブロックチェーン分析会社など、事件に関連する機関と連携すること
暗号資産事業者へのKYC厳格化	● 暗号資産サービスプロバイダー登録の手続きを厳格化するための法制化を検討すること
暗号資産事業者へのFATF勧告の適用	● 暗号資産サービスプロバイダーに対しマネー・ローンダリング防止とテロ資金対策の要件を課すことにより、大量破壊兵器拡散のための資金調達を防止しようとする、仮想資産に関する金融活動作業部会の指針をできるだけ早く実施すること
加盟国間の連携強化	● 拡大するサイバー犯罪の情報及び経済的脅威に対処するため、協力の強化、対話の促進、情報共有を強化すること

４．まとめ

「図表 4：FATF ガイダンスを踏まえた取組みのポイント」及び「３．調査結果」を踏まえ、日本を取り巻く脅威環境や日本の現在の取組みにおける課題（脆弱性）等を念頭に、

（１）今後日本における拡散金融対策の参考となり得る各国の取組み、及び

（２）専門家パネルによる勧告のうち日本が取組みを強化すべきと考えられる事項

を整理した。

（１）日本における拡散金融対策の参考となり得る各国の取組み事例

「図表 4：FATF ガイダンスを踏まえた取組みのポイント」及び「３．調査結果（１）～（４）」を踏まえ、日本の取組みにおける課題（脆弱性）等を念頭に、今後日本における拡散金融対策の参考となり得る各国の取組み事例等を整理した（調査項目②～⑨）。

調査項目	日本における拡散金融対策の参考となり得る各国の取組事例
②国のリスクアセスメント（リスクの特定・評価）	● PF に特化した NRA の策定・公表（米、英、豪） ✓ 米、英、豪は、従来の ML/TF の NRA を補完するものとして、PF（拡散金融）に特化した PF-NRA を策定・公表している ✓ FATF ガイダンスでは、PF のリスクについて、マネロン・テロ資金供与リスクとの相違を認識しつつ、定期的に特定、評価することが求められている ✧ 日本では PF に特化した NRA は策定されていない ● 政府機関横断的な情報収集・分析（英） ✓ FATF ガイダンスでは、政府機関は情報を有する関係機関と連携し、PF のリスクを包括的かつ具体的に検証することが求められている ✓ 英国では、民間セクターや学界等とも連携するなど、PF-NRA の策定において、政府機関横断的に情報を収集・分析している
③金融機関等のリスクアセスメント（リスクの特定・評価）	● 当局による金融機関等に対する PF リスク評価の実施要請 （英） ✓ 英国では、民間部門に対して ML/TF リスク評価と同様の枠組みで PF リスク評価（新たに PF リスク評価を作成するか、既存の ML/TF リスク評価へ組込む必要がある）の実施を要請している ✓ FATF ガイダンスでは、金融機関や DNFBPs は、体制や手順を整備して、定期的に PF のリスクを特定、評価することが求められている

	✧ 日本では、DNFBPs におけるリスク評価が不足している可能性がある（犯収法による努力義務に留まる）。また、金融機関においても、NRA が PF に関する詳細な分析を提供していない（②のとおり、PF に特化した NRA は策定されていない）ため、PF への理解が不足している可能性がある ● 業界団体による支援（豪） ✓ FATF ガイダンスでは、金融機関等は利用可能な情報を徹底的にレビューし、リスクベースの戦略に活用することが求められている ✓ 豪州では、金融機関等の取組みを支援するために、業界団体（銀行協会）が制裁実施に関する好事例を含むガイドラインを策定・公表している
④国による標的型金融制裁の制度・運用（法的な枠組みや国の運用に関する観点）	● 実効的・多層的な法規制やルールの整備（米） ✓ 米国では、法律、規制、大統領令、ガイダンス、調達基準などの様々なルールや罰則措置を組み合わせて、標的型金融制裁を実効化している ✧ 日本では、FATF 勧告対応法案において、拡散金融対策を強化する法規制の整備が進められているが、業界団体によるガイダンスや調達基準、自主規制等、いわゆるソフトローと呼ばれるようなルールや行動規範等は必ずしも定着していない ● 体制・手順の整備（各国） ✓ FATF ガイダンスでは、金融機関等に対し、制裁の指定が適時に通知するための体制の構築が求められている ✧ 日本では、国連による制裁対象のリストアップから官報公示までにタイムラグが存在する ● 国際的なパートナーと連携した手順の整備（豪） ✓ 豪州では、国際的なパートーシップを重視し、パートナーと連携した輸出入管理を実施している（専門家パネルへの情報提供も積極的に実施）
⑤金融機関等による標的型金融制裁への対応	● 金融機関等における顧客管理の徹底（米） ✓ 米国の金融機関は、BSA（銀行秘密法）や CDD 規則に基づき、顧客デューディリジェンス、取引監視、疑わしい活動報告等を適切に実施し、リスクを軽減している ✧ 日本では、金融機関における標的型金融制裁の措置に関連した対応の不備が多く確認されている

⑥その他企業(貿易会社等)による標的型金融制裁への対応	● 民間セクターにおける域外制裁への理解と対応の促進（英） ✓ 多くの英国企業は、米国の主要制裁や域外制裁に該当する可能性を踏まえ活動している ● 民間セクターにおける輸出規制の遵守（豪） ✓ 豪州から物品を輸出する際、輸出者や物品の所有者、またはその代理人は、輸出申告書を豪州国境警備隊に報告している ✧ 日本では、輸出管理内部規程（CP）を届出ていない企業による外為法違反事例が多い
⑦国の金融機関等に対する拡散金融対策の監督・アウトリーチ	● リスクベースアプローチの支援（米） ✓ FATF ガイダンスでは、リスクベースアプローチに基づき、各業態が直面するリスク、及び、各業態の能力・経験等も踏まえた監督・アウトリーチが求められている ✓ 米国では、FATF PF リスクアセスメントガイダンスや銀行機密保護法アドバイザリーグループ（BSAAG）等の官民情報共有メカニズムを通じて民間部門との関与を深め、民間部門自身による PF 防止のためのリスクベースアプローチを支援している ● 拡散金融対策に関するガイダンスの公表（米、英、豪） ✓ FATF ガイダンスでは、標的型金融制裁に係る法規制についてのガイダンスやプラクティス、トレーニング機会の提供が求められている ✓ 米国では、2020 年 4 月、国務省、財務省、国土安全保障省、司法省は DPRK サイバー脅威に関するガイダンスを発表している ✓ 英国金融機構監督局(OFSI)は制裁に関するガイダンスやアラートを提供している ✓ 豪州制裁局は金融業界が制裁義務を理解、履行するために、制裁を受けた個人及び団体の検索が可能な統合されたリスト、北朝鮮及びイランを含む豪州の制裁制度、関連する規制にかかるトレーニングやガイダンス資料等を提供している
⑧国のその他企業(貿易会社等)に対する拡散金融対策の監督・アウトリーチ	● 業界へのアドバイスの提供（米） ✓ FATF ガイダンスでは、標的型金融制裁に係る法規制についてのガイダンスやプラクティス、トレーニング機会の提供が求められている ✓ 財務省、国務省、米国沿岸警備隊は、海運業、エネルギー、金属セクター、および関連コミュニティに対する制裁勧告を発表し、海運セクターを含む主要セクターにおける不正資金脅威の

	防止に関するアドバイスを業界に提供している
⑨国の拡散金融機関対策に係る組織・体制(組織間の連携、調整等の観点を含む)	● 国内当局間の連携（英） ✓ FATF ガイダンスでは、核拡散資金対策に関与している全ての関連省庁（監督官庁、輸出入管理当局、税関、国境管理、情報機関等）の協調・情報共有の枠組みの構築が求められている ✓ 英国では、CPACC を設立し、FCDO、MOD、DIT、BEIS の職員を集め、国際的な CP と武器管理問題に関する専門知識と政策決定を一カ所に集約している ● 他国との協力、連携（米、豪） ✓ FATF ガイダンスでは、PF リスク評価の経験を有する国や直面するリスクの性質が類似する国との連携が推奨されている ✓ PF ネットワークが複数法域に跨り運営されるため、米国では強固なグローバル CPF 体制構築に向け、様々な多国間フォーラムを通じて、同盟国や他パートナー国と協力体制を整備している ✓ 米国では、外国政府パートナーや外国金融機関と連携し、PF の類型と傾向をより広範に議論している ✓ 豪州は NIC に属する機関の間で、情報共有の取り決めを確立し、拡散金融に関する情報交換、拡散金融行為者の活動を監視し、排除するために協調している

（2）日本が取組みを強化すべきと考えられる事項（専門家パネル勧告より）

「3．調査結果（1）及び、(5)」を踏まえ、北朝鮮による脅威を念頭に、専門家パネルによる勧告のうち、日本が取組みを強化すべきと考えられる事項を図表 24 に整理した（調査項目①、⑩～⑬)。

図表 24　専門家パネルによる勧告（日本が取組みを強化すべきと考えられる事項）

調査項目	勧告の内容
①拡散金融の主体、協力者	● 活動が不透明な企業の登録規制強化 ✓ 制裁回避活動に匿名性を与える可能性がある企業の登録に関する規制に引き続き対処すること ✧ 日本は、商業・法人登記制度を所管する法務省の関わりが限定的である点を FATF により指摘されている ✧ 日本では、貿易業や製造業を営む法人、個人による不正輸出事例が見られる

	● 外国への投資等を行う企業へのデューディリジェンス強化 ✓ 特にサハラ砂漠以南のアフリカにおける自治体の融資､補助金､外国直接投資を伴うプロジェクトの請負業者と下請業者に対するデューディリジェンスを強化すること ✧ 北朝鮮と武器や軍事関連の協力関係が疑われる国や、北朝鮮労働者の受入れを行う国がサハラ以南のアフリカに多く存在する
⑩国の経済・社会・産業構造（輸出入、地政学的要因等の観点を含む）	【北朝鮮による石油等の不正な輸入に関する勧告】 ● 北朝鮮船舶寄港時の船舶検査 ✓ 偽装、改造をした貨物船による精製石油の輸入について加盟国の海事当局が認識し、同国貨物船が自国の港等に寄港した際には必要な船舶検査を行うこと ✧ 日本の周辺海域において、偽装、改造した船舶による瀬取が行われている実態がある ● 船舶関連企業（修理工場や船舶ブローカー等）への北朝鮮による不正な輸入等の周知啓発 ✓ 船舶修理工場及び、関連する船舶ブローカーに対し、北朝鮮による欺瞞的行為と、それを支援する貨物船が北朝鮮に輸出される場合の影響等に関する情報を周知すること ✧ 日本でも、ソナーやシンクロ・スコープ、周波数変換器等、船舶に関連する部品の不正輸出の実態がある 【北朝鮮船舶による船舶 ID 改ざん等への対応に向けた勧告】 ● 船舶 ID の改ざんや MMSI 番号の不正使用等の検出事例の調査、共有 ✓ 加盟国と船舶登録機関が、船舶の ID ロンダリングまたは改ざんの検出事例に関する情報(偽装 ID を送信した登録船舶の ID、他の船舶に ID を利用された可能性のある登録船舶の ID 等)を広く周知すること ✧ 船舶 ID の改ざんや MMSI 番号を不正使用した船舶を利用した不正な輸出入の実態がある ● 疑わしい船舶 ID を発信する船舶の監視、調査 ✓ 船舶の識別子の有効性に疑いがある場合、港やその他関連する海事当局は、その港の管轄水域に侵入する該当する船舶の履歴を確認すること ✓ 加盟国は北朝鮮及び、北朝鮮に関連する船舶が操業している可

	能性がある海域で、疑わしい船舶識別子を発信している船舶を監視、及び調査すること ✧ 船舶 ID の改ざんや MMSI 番号を不正使用した船舶を利用した不正な輸出入の実態がある ● 漁業許可証の取得船舶による不正操業の防止 ✓ 北朝鮮の漁業許可証を取得した船舶が、その活動と身元を不明瞭にするために用いる方法を特定し、その不正操業を防止するために警戒を行うこと ✧ 北朝鮮の漁業許可証を取得した船舶が、身元を偽装する等して不正な輸出入を敢行する実態がある 【北朝鮮による船舶取得に関する勧告】 ● 引き渡しの際の AIS（自動船舶識別装置）の監視 ✓ 引き渡しの際の AIS の完全監視、制限された航行条件への適合確認のための船舶検査、受取人との船舶引渡しの確認などを行うこと ● 船舶売主に対する、船舶の最終目的地とエンドユーザー、関連ブローカーの身元、過去の取引記録等の確認 ● 船舶の譲渡後、安全保障理事会決議違反の可能性がある場合、売主・買主、ブローカーによる当局への報告
⑪拡散金融に利用される金融機関等と金融サービス	【暗号資産業者に関する勧告】 ● 暗号資産事業者への KYC 厳格化 ✓ 暗号資産サービスプロバイダー登録の手続きを厳格化するための法制化を検討すること ✧ 暗号資産取引の匿名性や即時性、越境性等の性質により、北朝鮮により拡散金融に利用されている実態がある ✧ 日本でも、北朝鮮の国家的関与がうかがわれるサイバー攻撃集団（「Lazarus（ラザルス）」）による暗号資産関連事業者等を標的としたサイバー攻撃が行われていると指摘されている ● 暗号資産事業者への FATF 勧告の適用強化 ✓ 暗号資産サービスプロバイダーに対しマネー・ローンダリング防止とテロ資金対策の要件を課すことにより、大量破壊兵器拡散のための資金調達を防止しようとする、仮想資産に関する金融活動作業部会の指針をできるだけ早く実施すること ✧ 暗号資産取引の匿名性や即時性、越境性等の性質により、

	北朝鮮により拡散金融に利用されている実態がある ✧ 日本でも、北朝鮮の国家的関与がうかがわれるサイバー攻撃集団（「Lazarus（ラザルス）」）による暗号資産関連事業者等を標的としたサイバー攻撃が行われていると指摘されている ● サイバー衛生強化 ✓ 暗号通貨取引所へのアクセスを試みる全ての暗号資産業者に対し、取引時の二要素認証などのサイバー衛生強化に適切な注意を払うこと ✧ サイバー攻撃は北朝鮮による資金確保の主たる手段となっている 【金融機関を含む全企業に共通的な勧告】 ● 従業員に対する拡散金融に関する教育・訓練 ✓ 経営者からパートタイム従業員等のあらゆるレベルの個人に対して適切な教育、訓練、情報共有、助言のための資料を採用するよう助言すること
⑫拡散金融に利用されるその他の産業と貿易等の形態や品目等	【貿易関連措置に関する勧告】 ● 国別コードの誤用防止 ✓ 北朝鮮および大韓民国（それぞれ KP および KR）の国別コードの誤用を防ぐため、適切な措置を講じること ✧ 国別コードも誤用により、北朝鮮による不正な輸出入を見逃した事例が確認されている ● 禁止品目リストの活用や共有 ✓ 禁止品目リストを活用し、輸出入管理リストを合理化すること ✓ 加盟国の税関当局が、特に制裁対象国の近隣で当該商品を扱う場合等に備え、管轄区域内の取引業者に禁止品目リストを共有すること ● 北朝鮮への贅沢品等の物資の移転防止、貨物の検査 ✓ 贅沢品や高級品を輸出する事業体や個人等に対し、北朝鮮への転売を防止する契約条項を含めることを奨励すること ✓ 指定団体の美術品の移転に関する警戒を行うこと ✓ 北朝鮮に出入りする個人の荷物を含む貨物の検査に警戒を払うこと

	【その他船舶関連の勧告】 ● 精製石油の船舶間移送を行う当事者に対し、船長または担当乗務員が、関連する旗国登録機関に、事象の通知、関係船舶の船舶識別番号、移送材料と量、移送の開始・停止の日時、移送場所を示す電子メールを送信する権限を与えること ● 船舶間転送を行う船舶に対して適切な原産地証明チェックを可能にする管理手段の導入を検討すること ● 船会社および運送会社に対し、積み替えのリスクを念頭に置き、荷受人の確認のためのシステムを提供するよう奨励すること ● 船主、船舶管理者、運航者が輸送に関して KYC 及び KYCV（Know your counterparty's vessel：取引先の船舶に関する理解）を引き続き強化すること　等 【金融機関を含む全企業に共通的な勧告】 ● 従業員に対する拡散金融に関する教育・訓練 ✓ 経営者からパートタイム従業員等のあらゆるレベルの個人に対して適切な教育、訓練、情報共有、助言のための資料を採用するよう助言すること
⑬拡散金融に利用されるその他の手段（サイバー攻撃等）	● サイバー攻撃事件の速やかな情報開示 ✓ 盗まれた資産の回収の見込みを高めるため、サイバー攻撃を受けた企業は、できるだけ早く適切な法的機関に報告し、事件の公表を行い、ブロックチェーン分析会社など、事件に関連する機関と連携すること ✧ サイバー攻撃は北朝鮮による資金確保の主たる手段となっている ● 加盟国間の連携強化 ✓ 拡大するサイバー犯罪の情報及び経済的脅威に対処するため、協力の強化、対話の促進、情報共有を強化すること ✧ サイバー攻撃は北朝鮮による資金確保の主たる手段となっている

以上