テロ資金供与リスク評価に関する調査

調査報告書

令和８年３月

株式会社NTTデータ経営研究所

目次

１．本調査の目的と概要

（1）背景と目的

テロ資金供与リスクとは、テロ行為の実行資金、テロ組織の活動資金等のために、資金や場所等を収集・提供等する行為を指す。

テロ資金供与対策にかかる国際基準は、金融活動作業部会（以下、「FATF」という。）[1]において、2001 年の米国同時多発テロ事件を契機として、同年以降に決定・公表されてきた。これらの基準は、テロ資金供与の捜査・起訴の実効性を確保するとともに、国連安全保障理事会決議に基づく義務を遵守するため、タリバーン、アル・カーイダ及び ISIL 等のテロリストに対する経済制裁（資産凍結等の金融制裁措置）の実施を各国に求めている。

現在までのところ、日本国内において、国際連合安全保障理事会が指定するテロリスト等によるテロ行為は確認されていないが、過去には、爆弾テロ未遂等で国際手配されていた者の不法出入国の繰り返しなど、イスラム過激派組織のネットワークが我が国にも及んでいることなどを踏まえ、必要なテロ資金供与対策を講じることが不可欠である。

政府では、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、「テロ資金等提供罪の捜査・訴追」の項目として、「重大複雑なテロ資金供与の更なる捜査・訴追のため、タスクフォースの枠組みや各種通達に基づいて、関係省庁が連携し、態勢整備も含め捜査・訴追の執行を強化する」とされるとともに、捜査・訴追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、2022 年 5 月 18 日に公表された「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」では、国連安保理決議に基づく資産凍結対象に日本人や国内居住者は含まれていないものの、国内で資金が集められ、海外に送金される可能性は否定できず、テロ資金供与リスクの適切な把握が重要とされている。こうした状況を踏まえ、政府としては、テロ資金供与対策の取組を着実に進めていく必要がある。

そして、第 4 次対日相互審査によると、当局は、高リスク国・地域又はその周辺で活動する非営利団体が一定数存在しているにもかかわらず、これらの団体におけるテロ資金供与リスクの実態や脆弱性について、十分な理解や分析を行えていない状況にあると指摘されてきた。

加えて、金融機関や DNFBPs においても、テロ資金供与リスクの把握は不可欠である。FATF による第 4 次対日相互審査では、日本における国内又は国境を越えたテロ資金供与リスクに関する具体的な情報や分析がなされていないとの指摘があった。このことは、当局

---

[1] 1989 年のアルシュ・サミット経済宣言を受け、マネロン対策の国際基準策定・履行を担う多国間枠組みとして設立

[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）

によるテロ資金供与リスクの理解が不十分であることを示しており、金融機関等が適切なリスク評価を行う上での障壁となっている。リスク評価の基礎となる情報が欠如している現状においては、政府が主導して、業態別・セクター別のテロ資金供与リスク評価を策定することが求められる。

一方、国際的にみると、各国においても、これまで G7 各国やオーストラリア・NZ・韓国等の国々でテロ資金供与に関するリスク評価書が策定・公表されているところ。また、FATF をはじめとした国際機関は、リスク評価のガイダンスや最新事例に関する報告書を公表し、各国の対応を促している。

こうした他国のテロ資金供与評価書や国際機関が有する情報等を踏まえつつ、NPO のテロ資金供与リスクも含めた日本に相応しいテロ資金供与リスク評価を行う必要がある。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顧客管理や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、テロ資金供与対策の更なる対策の高度化に向け、世界的なリスクの潮流を反映しつつ日本独自の環境に即したテロ資金供与リスク評価を実現するため、他国のテロ資金供与リスク評価書や国内関係機関が有する情報等を調査・分析する。

（2）調査概要

FATF のテロ資金供与対策に関するガイダンス[3]、及び日本を含む 9 か国・地域のリスク評価書、国連安全保障理事会のレポート等を対象に文献調査を行った。

（3）実施スケジュール

本調査は、2026 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] Comprehensive Update on Terrorist Financing Risks（2025）
Terrorist Financing Risk Assessment Guidance （2019）

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

No	国／機関	文献名称	発行機関
1	日本	犯罪収益移転危険度調査書（令和 7 年/2025 年版）	国家公安委員会
		Anti-money laundering and counter-terrorist financing measures - Japan Mutual Evaluation Report（2021）	FATF
		Anti-money laundering and counter-terrorist financing measures - Follow Up Report Japan-2023（2023）	FATF
		内外情勢の回顧と展望（令和 8 年/2026 年版）	公安調査庁
		警察白書（令和 7 年）	国家公安委員会
2	FATF	Comprehensive Update on Terrorist Financing Risks（2025）	FATF
		Terrorist Financing Risk Assessment Guidance（2019）	FATF
		Best Practices on Combating the Abuse of Non-Profit Organisations（2023）	FATF
3	米国	National Terrorist Financing Risk Assessment（2024）	US Treasury
4	英国	UK National risk assessment of money laundering and terrorist financing（2025）	HM Treasury
5	カナダ	Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada（2023）	Department of Finance

6	ドイツ	National risk assessment of Germany（2018-2019）	Federal Ministry of Finance
7	オーストラリア	Terrorism financing in Australia national risk assessment （2024）	AUSTRAC
8	ニュージーランド	National Risk Assessment（2024）	NZ Police Financial Intelligence Unit
9	香港	Money Laundering and Terrorist Financing Risk Assessment Report （2022）	Financial Services and the Treasury Bureau
10	マレーシア	NATIONAL RISK ASSESSMENT on Money Laundering and Terrorism Financing（2023）	Bank Negara Malaysia
11	国際連合	36th Analytical Support and Sanctions Monitoring Team Report（2025.7）	UN Security Council

（2）調査手法

FATF ガイダンス[4]によると、テロ資金供与のリスクは、「脅威」、「脆弱性」、「発生可能性と結果」の三つの要素の関数としてとらえることができる。これは、テロリスト又はテロ組織を目的とする資金又はその他の資産が、正当又は不正な資金・資産の形態を問わず、ある法域において、又は当該法域を通じて、調達、移転、保管、又は使用されるリスクを意味するとし、当該資金その他の資産が当初合法的又は非合法的に取得されたか否かは問わないとされている。

「脅威」、「脆弱性」、「発生可能性と結果」それぞれの概念は、以下のとおり定義されている（図表 2）。

図表 2：「脅威」「脆弱性」「発生可能性と結果」の定義

項目	定義
脅威	● テロ目的のために資金又はその他の資産（正当な出所か不正な出所かを問わない）を調達、移転、保管、又は使用することにより、害を及

[4] Comprehensive Update on Terrorist Financing Risks（2025）
Terrorist Financing Risk Assessment Guidance （2019）

	ぼす可能性を有する個人又は集団を指す。 ● 国内又は国際的なテロ組織及びその支援者、これらの組織が保有・管理する資金、並びに過去・現在・将来のテロ資金供与活動が含まれるほか、テロ組織に共感・同調する個人や集団も含まれ得る。
脆弱性	● 脅威によって悪用され得る要素、又はその活動を支援・助長し得る要素を指す。 ● 特定の業界、金融商品、又はサービスの種類に固有の特性であって、テロ資金供与の観点から魅力的となり得るものが含まれる。 ● また、テロ資金供与対策のために特別に設計された措置の不備や、より広く AML/CFT 体制や内部統制における弱点、さらにはテロ資金供与者が資金やその他の資産を調達・移転する機会に影響を与え得る法域特有の状況的要因（例：大規模なインフォーマル経済、国境管理の脆弱性等）も含まれ得る。 ● なお、マネー・ローンダリングとテロ資金供与の双方において共通して悪用される脆弱性が存在する場合もある。
発生可能性と結果	● テロ資金供与の脅威が実際に顕在化する可能性及び、顕在化した場合に生じ得る影響又は被害を指す。 ● これには、テロ行為そのものが国内の金融システムや金融機関、さらには制度面に与える影響に加え、より広く経済及び社会全体に及ぼす影響が含まれる。特に、テロ資金供与に伴う結果は、マネー・ローンダリングやその他の金融犯罪（例：租税詐欺等）と比較して、より深刻なものとなる可能性が高い点に留意する必要がある。この点は、各国が特定された脅威にどのように対応するかに影響を与える。

本調査では、この定義を準用し、各文献より国内外のテロ資金供与における「脅威」と「脆弱性」を特定し、「発生可能性と結果」を踏まえ、国内の「脆弱性」を中心にとりまとめを行った。

１．調査項目

FATF ガイダンス[5]で示された先述のリスク評価の考え方（「脅威」、「脆弱性」、「発生可能性と結果」）及び、テロ資金供与のリスクに影響を与える要因や各国の実例等を踏まえ、調査のフレームワークを以下のとおり整理した。（図表 3）。

[5] Comprehensive Update on Terrorist Financing Risks（2025）
Terrorist Financing Risk Assessment Guidance （2019）

図表 3：調査項目

大分類	小分類	調査項目
①脅威	①-1.テロ資金供与の主体	①-1-1.テロ組織、テロリスト ※日本のみ「国内固有の団体」の調査を実施
		①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団
	①-2.テロ資金供与のための活動	①-2-1.(テロ資金供与の主体による)資金獲得のための活動
		①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法
		①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等
②脆弱性	②-1.文化･経済･社会･産業構造	②-1-1.国・地域に固有の文化的背景や社会・経済構造
	②-2.法・制度	②-2-1.テロ資金供与を防止するための法的枠組み
	②-3.監督､アウトリーチ	②-3-1.金融当局等の監督・アウトリーチ
		②-3-2.NPO の規制、監督・アウトリーチ
		②-3-3.その他セクターの規制当局の監督･アウトリーチ
	②-4.関連セクターの活動・対応	②-4-1.金融機関等(DNFBPs 含)の活動･対応
		②-4-2.NPO の活動・対応
		②-4-3.その他セクターの活動・対応
③発生可能性と結果	③-1.発生可能性	③-1-1.テロ資金供与の脅威が顕在化する可能性
	③-2.結果	③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

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等の「①脅威」「②脆弱性」「③発生可能性と結果」の内容について、①-1-1～③-2-1 の各調査観点に沿って整理した（「３．調査結果（１）～（11)」)。

次に、各国において、業態別・セクター別の切り口でテロ資金供与リスクがどのように評価されているかを比較・整理した（「３．調査結果（12)」)。

最後にこれらを踏まえ、今後、我が国においてテロ資金供与リスクを特定・評価するにあ

たり、参考となり得る各国の事例や取り組みを抽出し、以下の観点から「4．まとめ」に整理した。

A）グローバルな脅威と脆弱性の共通

日本と経済規模や金融システムの成熟度が類似する G7 諸国（米国・英国・ドイツ・カナダ）や、地政学・経済的な結びつきが強いアジア・オセアニア地域（オーストラリア・ニュージーランド・香港・マレーシア）との比較を通じ、国境を越えて波及する共通のリスク。

B）日本固有の文脈への適用可能性

諸外国の脅威や脆弱性が、日本の文化・経済・社会、産業構造、法規制、実務慣行等の文脈に照らし合わせ、そのまま適用可能な要素、調整を要する要素、及び日本特有の事情を踏まえ新たに考慮すべき要素。

３．調査結果

（1）日本

日本では、国家公安委員会が、マネロン・テロ資金供与の危険度を分析し、「犯罪収益移転危険度調査書」として毎年公表している。リスクの特定・評価においては、日本をとりまくマネロン等の「脅威」と「脆弱性」を特定し、また、それらの「影響」として、移転され得る犯罪収益の大きさ、組織的な犯罪を助長する危険性や健全な経済活動に与える影響等を踏まえて、「取引形態」、「国・地域」及び「顧客」並びに「商品・サービス」の観点から、危険度に影響を与える要因を特定している。また、当該要因ごとに、

- マネー・ローンダリング等に悪用される固有の危険性
- マネー・ローンダリング事犯
- 疑わしい取引の届出状況
- 危険度を低減させるためにとられている措置（特定事業者に対する法令上の義務、所管行政庁による特定事業者に対する指導・監督、業界団体又は特定事業者による自主的な取組等）

に関する状況等を分析し、多角的・総合的に危険度が評価されている。

なお、業態別・セクター別の評価は、「第５　商品・サービスの危険度」において、主にマネロンの観点から分析されている。テロ資金供与のリスク評価は、独立した章（第７　テロ資金供与に関する危険度）で分析され、業態別・セクター別の評価は明示されていない。

本調査では、「犯罪収益移転危険度調査書」のほか、図表 1：調査対象文献に記載の文献を対象に、「①脅威」「②脆弱性」「③発生可能性と結果」に関する調査を実施した。

①脅威

①-1-1.テロ組織、テロリスト、国内固有の団体等

日本におけるテロ組織・テロリスト等の脅威として、国際的な過激派組織及び国内固有の団体等が特定されている。それぞれの活動実態と脅威の動向は以下の通りである。

1. 国際テロ組織（イスラム過激派等）

ISIL（イラク・レバントのイスラム国）や AQ（アルカイダ）等のイスラム過激派は、国際社会において依然として活発な活動が確認されており、テロ資金供与リスクにおける主要な脅威として位置付けられている。

現在までのところ、日本国内において国際連合安全保障理事会が決議等に基づき指定するテロリストによるテロ行為は確認されておらず、資産凍結対象となる日本人や国内居住者も把握されていない。

但し、日本への敵対的動向として、以下のような事例が指摘されている。

- ISIL の関連組織である ISIL-K のメディアにおいて、我が国の国旗が批判対象として掲載される事案が発生している。
- AQ の関連組織である「インド亜大陸のアルカイダ」（AQIS）は、機関誌等において我が国製品を不買運動の対象に加えるなど、批判的な認識を強めている。
- AQ の幹部が過去、我が国所在の米国大使館を破壊する計画に関与していたと供述するなど、我が国やその権益が標的となる懸念は払拭できない。

以上のほか、テロ組織・団体としては日本赤軍及び「よど号」グループがあげられる。

- 日本赤軍及び「よど号」グループ

日本赤軍は「解散」を宣言しているものの、過去のテロ事件を称賛する姿勢を崩しておらず、組織の本質を隠蔽した形だけの解散であると評価される。現在も 7 人の構成員が国際指名手配中である。「よど号」グループは、北朝鮮に留まっているメンバーやその妻の一部に、日本人拉致容疑で逮捕状が発付されている。

2. 国内固有の団体

オウム真理教は、過去に無差別大量殺人行為である地下鉄サリン事件、松本サリン事件を引き起こし、現在も当該団体と同一性を有する「Aleph」、「山田らの集団」、「ひかりの輪」の 3 団体を中心に活動を継続している。これら 3 団体は依然として麻原彰晃（松本智津夫）の影響下にあり、過去の無差別大量殺人行為に及んだ当時の危険な体質を保持している。教団名を隠した巧妙な勧誘活動を若い世代に対して展開しており、SNS 等の活用も確認されている。

また、我が国の公安情勢に脅威となる国内団体として過激派・右翼団体等が挙げられる。過激各派は、暴力革命による共産主義社会の実現を掲げ、多数の不法行為を引き起こした組織であり、現在もなお危険な体質を有している。右翼団体等は、理想とする社会変革を実現するために最も効果的かつ実現可能な手段として暴力行為を容認する傾向が強く、過去に殺人等を含め多くの事件を引き起こしている。過去の事件の首謀者を顕彰する行事や、旧日本軍の銃剣術を取り入れた「教練」と称する訓練を継続しており、引き続き警戒が必要な危険性を保持している。

3. 北朝鮮関連

警察は、拉致容疑事案 13 件を北朝鮮によるものと判断して、北朝鮮工作員等 10 人に対して逮捕状の発付を得て国際手配を行っている。また、過去には、大韓航空機爆破事件（1987 年）等、工作員によるテロを世界各地で引き起こしており、その際には日本人を装うなど、我が国との関連性が高い手法も確認されている。

４．ローン・オフェンダーの台頭

特定のテロ組織等と関わりのないままに過激化した個人、いわゆるローン・オフェンダーによる事件や社会一般に対する恨み、不安等を背景として不特定多数の者に対して危害を加える事件が繰り返し発生しており、新たな脅威となっている。それらの背景には、インターネットを通じて容易に銃砲・爆発物の製造方法等に関する情報が入手可能であることが指摘されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

特定のテロ組織に直接所属せずとも、その思想に共鳴し、あるいは支援を行う個人や集団の存在は、現代のテロ資金供与対策において看過できない脅威となっている。我が国における主な動向は以下の通りである。

- 過激思想に影響を受けた国内居住者

  日本においても、インターネット上で ISIL 等への支持を表明する者や、組織関係者と連絡を取り合っていると称する者の存在が確認されている。過激思想を介して緩やかにつながるイスラム過激派組織のネットワークは我が国にも及んでおり、こうした同調者によるテロ発生の可能性は否定できない。

- 外国人戦闘員（FTF）及びその家族

  ISIL の旧支配地域を離れた外国人戦闘員やその家族が、母国又は第三国へ渡航しテロを引き起こす危険性が指摘されている。収容施設や難民キャンプにおいてさらなる過激化が進む可能性も懸念事項として挙げられる。

- 紛争地域への渡航者及び外国人コミュニティ

  紛争地域へ渡航する個人は、それ自体がテロ資金供与を行う主体となる懸念が存在する。また、イスラム過激派等が国内の外国人コミュニティに潜伏し、当該コミュニティが資金調達等の活動に悪用される可能性は否定できない。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

テロ組織やテロリスト等による資金獲得の手法は、その出所の多様性と巧妙な偽装性に特徴がある。主要な活動形態は以下の通りである。

- 犯罪行為による資金獲得

  テロ組織は、麻薬密売、詐欺、身代金目的の誘拐等の重大な犯罪行為を資金源としている。AQ の関連組織であるアル・シャバブ等の支配地域を有する組織においては、その地域内における取引等に対して独自に課税を行うことで組織的に資金を徴収している。

- 合法的活動への偽装と個人支援

  テロ資金は、団体や企業等による正当な商業取引を装って獲得されるケースがある。外国人戦闘員（FTF）等に対して、その家族や知人が人道的支援等を名目に金銭的支援を行う形態も確認されている。

● 先端技術・プラットフォームの悪用

- SNS 及びクラウドファンディングの利用

  近年、SNS やクラウドファンディング、モバイルアプリの利用が増加しており、過激主義を助長する動画や寄附を呼びかける動画を併用することで、広範囲から効率的に資金を集める手法が定着している。

- 暗号資産による寄附の募集

  ISIL-K の関連メディア「ホラサンの声（Voice of Khurasan）」等において、匿名性の高い暗号資産（モネロ等）による資金提供を呼びかけ、実際に数万米ドル単位の資金を調達した事例が報告されている。

- オンラインツールの活用

  オウム真理教（Aleph）のように、施設外の在家信者に対し、ネットワーク通信を用いたオンライン配信を通じて指導を行い、組織の維持・活動の活性化を図る動きも見られる。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

テロ組織等への資金供与は、既存の金融システムを悪用するのみならず、伝統的な価値移転システムや先端技術、さらには物品の不正輸出など、極めて多様な経路で行われている。その主な特徴と手法は以下の通りである。

● 取引の秘匿性

テロ資金供与に関係する取引は、マネー・ローンダリングと比較して少額・断片的な形態をとる傾向がある。このため、金融機関等が日常的に取り扱う膨大な取引の中に紛れてしまい、検知が困難であるという脆弱性を有している。

● 送金経路

資金はテロ組織の支配地域内に所在する金融機関へ直接送金されることもあるが、イラク、シリア、ソマリアといった高リスク国へ直接送らず、トルコ等の周辺国を経由する事例が確認されている。また、中東や北アフリカ、インド亜大陸で一般的に利用されている「ハワラ」などの非公式な価値移転システムや、現金の直接受け渡しといった伝統的な手法も、ISIL 等により広く利用され続けている。

● 先端技術の悪用（暗号資産）

ISIL-K 等の組織は、関連メディアを通じて匿名性の高い暗号資産（モネロ等）による資金提供を呼びかけている。従来の犯罪行為（身代金目的の誘拐等）から、暗号資産を利用した支持者からの寄附へと資金調達の手段が移行しつつある現状がうかがえる。

国内におけるテロ資金供与が疑われる事案は以下のとおり。

● 輸出における虚偽申告

中古貨物船の輸出先が実際はイランであるところ、アラブ首長国連邦（UAE）の企業に輸出するという虚偽の申告書類を税関に提出したとして、大阪市の船舶売買仲介会社が、関税法違反の疑いで書類送検をうけた事例。

- 不正口座を利用した資金移転

第三者に利用させる目的で不正に開設された口座に、国際手配中の日本赤軍メンバーを支援する国内団体からの入金があり、その全額が外国で引き出されていた事例が確認されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

テロ組織や国内固有の団体は、その活動を維持・拡大させるための基盤として、既存の社会インフラや先端技術を巧妙に悪用している。特にデジタルプラットフォームの活用は、資金調達のみならず、組織の運営や宣伝においても重要な役割を果たしている。

- SNS 及びデジタルプラットフォームの活用

テロ等資金調達において、SNS、クラウドファンディング、及びモバイルアプリの利用が増加傾向にある。これらのプラットフォーム上では、過激主義を助長したり、寄附を直接呼び掛けたりする動画が効果的に用いられている。

- オンラインツールによる組織運営の高度化

オウム真理教（Aleph）は、在家の構成員に対する指導や修行の場を施設外へ移す動きを見せており、ウェブサイトでの説法掲載や、車両内からネットワーク通信を用いた行事のオンライン配信を実施している。また、ISIL-K 系のメディアは、オンライン誌の発行を通じて支持者へ資金提供を呼び掛けるだけでなく、安全な通信手段の確保や AI 技術の活用に関する助言を行うなど、組織運営の高度化を図っている。

- 先端技術の積極的な採用意図

テロ組織側には、暗号資産を用いた資金調達に加え、AI 技術等の先端技術をテロ活動に積極的に活用しようとする意図がうかがえる。これらは、従来の物理的な拠点に依存しない形での資金獲得や情報伝達を可能にしており、対策側にとっての新たな障壁となっている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

- 国際金融・貿易センターとしての立ち位置

地域的・世界的な金融センターとしての役割に照らすと、日本は国際的な貿易や金融取引の量、頻度、範囲が大きい。こうした大規模かつ複雑な取引環境そのものが、テロ資金供与の脅威に対する構造的な脆弱性となっている。また、テロやテロ資金供与の脅威にさらされている東南アジアや中東の諸国との間で、量・質ともに重要な取

引を行っている実態がある。

- 特定の製品需要と人的要因に係るリスク

  紛争地域やその周辺において、テロリストやテロ組織による日本製品、特に中古車に対する強い需要が存在することがリスク要因として挙げられる。人的交流の側面では、日本人による紛争地への渡航や帰国は限定的であるものの、ISIL に共感するイスラム過激派とみられる者が少人数ながら国内に存在することが指摘されており、注意を要する。

②-2-1.テロ資金供与を防止するための法的枠組み

日本におけるテロ資金供与防止の法的枠組みは、組織的犯罪処罰法、犯罪収益移転防止法、テロ資金提供処罰法、外為法などの複数の法律によって構成されている。近年、国際的な要請に応えるための法改正が進められている。

- 組織的犯罪処罰法及び犯罪収益移転防止法による規制

  組織的犯罪処罰法において、テロ資金提供罪等を前提犯罪と定めて、テロ資金そのものを犯罪収益として規定している。また、犯罪収益移転防止法に基づき、テロ資金の疑いがある財産に係る取引を「疑わしい取引の届出」の対象としており、警察庁は、安保理決議等に基づく資産凍結対象者リストの改正の都度、特定事業者に対して取引時確認義務の履行や届出の徹底を要請している。

- テロ資金提供処罰法（公衆等脅迫目的の犯罪行為のための資金の提供等の処罰に関する法律）

  殺人や航空機強取等の「公衆等脅迫目的の犯罪行為」を実行しようとする者への資金・利益提供行為等に対する罰則を規定している。2022 年 12 月の改正により、法定刑の引き上げ、条約特定犯罪における意図要件の明確化、及び法人に対する抑止力のある刑事制裁の導入が図られた。

- 外国為替及び外国貿易法（外為法）並びに国際テロリスト等財産凍結法

  安保理決議等に基づき、対象となる個人・団体に対する資産凍結等の措置を実施している。FATF 第四次対日相互審査では、資産凍結措置を「遅滞なく」実施できていないとの指摘があったが、行政手続きの改正により 24 時間以内に実施する体制が整えられた。

- 関税法

  貨物及び「支払手段（銀行券、小切手等）」の越境運搬についての申告制度を導入している。

②-3-1.金融当局等の監督・アウトリーチ

テロリスト等に対する資産凍結措置を実効的なものとするため、金融当局及び関係行政機関は、対象者の指定情報の迅速な周知や、制度の理解を深めるためのアウトリーチ活動を

展開している。

- 金融機関に対する資産凍結情報の周知体制

  官報により制裁対象者が公告された際、国家公安委員会の要請に基づき、財務省は直ちにその内容を国内の金融機関へ電子メールで通知するとともに、同省のウェブサイトに掲載する体制をとっている。

- 特定非金融業者（DNFBPs）へのアウトリーチ

  国家公安委員会は、全ての DNFBPs の監督機関及び自主規制機関（日本弁護士連合会、日本暗号資産取引業協会等）に対し、書面による通知を行い、傘下の会員等への情報共有を要請している。

②-3-2.NPO の規制、監督・アウトリーチ

非営利団体（NPO）セクターについては、その活動の善意や透明性を悪用しようとするテロ資金供与の脅威から保護するため、所管行政庁によるリスクベースの監督と継続的なアウトリーチが実施されている。

日本国内において、非営利団体がテロ資金供与に悪用されたとして摘発された事例は、現時点で確認されていない。一方で、海外（特にテロ組織が活動する地域やその周辺）で活動する団体については、現地のテロ組織による脅威にさらされる可能性が指摘されている。

日本の非営利団体は法人種別ごとに異なる法制度を有しているが、各所管行政庁はそれぞれの枠組みに基づき、監督・指導を実施している。例えば、内閣府では「特定非営利活動法人のテロ資金供与対策のためのガイダンス」を策定し、資金の透明性確保やリスク管理体制の構築を促している。当該ガイダンスは、FATF 勧告 8 に基づく国際的な要請や情勢の変化を踏まえ継続的に更新されており、最新版は令和 7 年（2025 年）6 月に公表されている。NPO 法人を主対象としているが、非営利団体全般の対策強化に資する内容として、関係者への啓発・支援に活用されている。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-2.NPO の活動・対応

日本における非営利団体（NPO）は、テロ資金供与に悪用される危険度を自ら把握し、適切なリスク管理を行うことが求められている。

リスクが相対的に高いとされる団体の特徴は以下のとおり。

- テロ行為が行われている地域やその周辺で活動している非営利団体

意図せずテロ組織の資金調達等に利用される懸念がある。

- 相当量の資金を取り扱い、外国への送金や現地での現金取扱いを頻繁に行っている非営利団体

  資金の流れの不透明さからリスクが高まると考えられる。

- 休眠状態にあるなど、法人としての実体が不明確な非営利団体

  テロ組織による隠れ蓑として悪用される危険性が指摘されている。

上記のような特性を有する団体は、リスクベース・アプローチに基づく、確認や体制の整備が必要とされる。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

我が国においては、テロ資金供与に関する法令上の措置等が整備されており、他国と比較してテロ資金供与リスクは相対的に低いと評価される状況にある。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

（2）FATF

①脅威

①-1-1.テロ組織、テロリスト

テロ資金供与の直接の脅威主体として、国際的な過激派組織や武装組織が特定されている。それぞれの活動実態と脅威の動向は以下の通りである。

- アルカイダ（AQ）

  以前は中央評議会（Majlis al-Shura）が戦略的・財務的決定を下す中央集権型であったが、現在は分散型モデルへと移行しており、AQIM（イスラム・マグレブ諸国のアルカイダ）、AQAP（アラビア半島のアルカイダ）、JNIM（イスラムとムスリムの支援団）、AQIS（インド亜大陸のアルカイダ）、アル・シャバブなどの地域支部が、独自に資金調達と活動を展開している。

- ISIL（イスラム国）

  シリア・イラクでの領土支配を失った後、現在は地域の資金調達活動への依存を強めており、世界各地に分散した地域財務局（Regional Financial Offices）（al-Karrar, al-Furqan, al-Siddiq など）を通じて、資金の収集と再分配を行っている。支配地域内の石油や金などの天然資源を収入源として利用するほか、東南アジアではハワラ業者や自己資金など多様な手法を用いている。アフガニスタンを拠点とする ISIL-K は、欧州や中央アジアにおいても深刻な脅威となっており、独自のメディア部門（Voice of Khorasan）を通じたプロパガンダにより、国際的な寄付を募り、攻撃資金としている。

- アル・シャバブ

  ソマリア及び東アフリカで活動し、構造化された財務部門を保持している。領土支配を通じた「税金」徴収（車両、物資、家畜等）や恐喝によって多額の収益を得ており、収益の約 30%を投資に回していると推定される。

- ADF（連合民主軍）

  コンゴ民主共和国及びウガンダで活動し、中央で資金調達と支出を調整。金の不法採掘や木材密売、誘拐を主な資金源とする。

- ASWJ（アフル・スンナ・ワル・ジャマー）

  モザンビークで活動し、ルビー採掘や漁業活動の収益を運営費に充てている。

- ISWAP（イスラム国西アフリカ州）

  ナイジェリア等で活動。農作物の販売や漁業の「許可証」発行など、地域社会に深く根ざした課税システムを構築している。

- PKK（クルディスタン労働党）

  地域マネージャーが資金運営を監督し、季節労働者からの強制徴収や不動産業者への恐喝を行っている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

テロ組織を支える人的基盤は、従来の組織的なネットワークに留まらず、イデオロギーに共鳴する個人や、地理的・血縁的な繋がりを悪用されたコミュニティへと拡散している。特に、インターネットや SNS を通じた過激化の進展により、組織と直接の接点を持たない自己活性型の主体が深刻な脅威として指摘されている。

- 外国人テロ戦闘員（FTF）及び帰還者

  テロ行為や訓練への参加、あるいはその準備・実施を目的として、自国又は居住国を離れて他国（紛争地域等）へ渡航する個人を指す。ISIL の衰退後も、アフリカ（ソマリア等）やアフガニスタン、シリアへの継続的な渡航や、拘束キャンプでの維持、さらには自国への帰還・再統合に伴う資金需要が依然として存在する。紛争地域から戻った帰還者や別の地域へ移動した移転者は、潜在的な脅威及び新たな資金流入ルートの分析対象として重要視されている。

- ディアスポラ（移住先の同胞コミュニティ）

  紛争地域等にルーツを持つ移住先のコミュニティであり、母国や地域のテロ組織にとって主要な資金源の一つとなっている。例えば、ISIL-K は中央アジアやロシア語圏のディアスポラを標的とし、多言語でプロパガンダを展開して寄付を募っている。PKK（クルディスタン労働党）のように、欧州等のコミュニティや企業から寄附名目で資金を収集し、時には強要や脅迫が伴うケースも報告されている。

- オンラインで過激化した個人及び単独犯（ローンアクター）

  SNS や暗号化メッセージアプリ、オンラインゲームを通じて過激思想に触れ、特定の組織に属さず活動を開始する自己活性型のテロリストが増加している。これらの主体は、個人の給与、貯蓄、社会保障給付といった自己資金で活動を完結させることが多く、少額かつ日常的な取引に紛れるため、金融システムにおける検知が極めて困難である。

- 青少年及び未成年者

  過激思想の影響を受ける層の若年化が顕著であり、欧州ではテロ容疑での逮捕者の 5 人に 1 人が法律上の未成年者となっている。オンラインゲーム内でのチャットや AI を用いた精巧なプロパガンダを通じて勧誘され、保護者の金融リソースが知らない間に流用されるリスクも指摘されている。

- NPO（非営利団体）及び偽装 NPO

  慈善、宗教、教育等の正当な活動を行う NPO が、テロ組織の資金調達の隠れみのとして悪用される、あるいは善意の寄付が意図せず転用される事例が確認されている。最初からテロ支援を目的に設立された偽装 NPO も存在し、東アジアでは人道支援を装う団体がテロ資金供与のプラットフォームとして機能している例がある。

- 支援者や同調者

テロ組織の思想に共鳴し、活動を支援する者として、小口資金提供者や親族・知人、仲介活動を行う者があげられる。小口資金提供者は、世界中に存在し、SNS 上の慈善活動を装ったキャンペーンに同調し、暗号資産やモバイルマネー等を用いて少額寄付を行っている。親族・知人は、FTF やローンアクターの家族が、意図的あるいは無自覚に、口座の提供や生活費・渡航費の支援、借入の肩代わりを通じて活動を支えている実態がある。また、資金の移動・保管、武器調達、戦闘員募集、渡航の段取りなど、テロ活動を実効的に支えるネットワーク構築に深く関与する仲介活動を行う者の存在も指摘されている。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

テロ組織及びテロリストによる資金獲得活動は、領土支配を背景とした「国家模倣型」の徴収から、個人の日常生活に埋没した「マイクロファイナンス型」まで、極めて広範かつ多層的に展開されている。特に、合法的な経済活動や公的制度の悪用が巧妙化しており、検知を困難にさせている。

1. 天然資源及び一次産業の搾取・支配

大規模な領土や支配地域を持つ組織は、その地域の資源を組織的な収益源として活用している。

- エネルギー資源

  ISIL による石油・ガスの生産・取引や、AQAP 及びフーシ派による港湾・石油インフラの支配を通じた収益確保が報告されている。

- 貴金属・宝石

  サヘル地域（ISGS、JNIM 等）や中央アフリカ（ADF）において、金の不法採掘やルビーの密売が重要な原資となっている。

- 農業・家畜・林業

  ソマリアのアル・シャバブによる農産物・家畜への課税や、ナイジェリアにおける漁業・農作物の販売許可証発行による組織的な収益化が見られる。

- 木材・木炭

  コンゴ民主共和国の ADF 及び ISIL 系組織による希少木材（ローズウッド等）の不法伐採や、アル・シャバブによる木炭密輸ネットワークを通じた多額の収益が確認されている。

2. 犯罪行為や強制的な徴収

テロ組織等による組織犯罪ネットワークとの連携や、住民・企業への恐喝が常態化している。

- 税名目の恐喝

支配地域や影響下にあるコミュニティにおいて、「ザカート（喜捨）」、「道路税」、「保護料」といった名目での強制徴収が行われている。

- 身代金目的の誘拐

  外国人や地元住民を拉致し、解放と引き換えに数百万ドル単位の身代金を得る行為が、サヘル地域やフィリピン等で継続している。

- 密売・不正取引

  薬物、武器、人身売買、文化遺産（古美術品）の略奪・売買、さらには日常品（タバコ、燃料等）の密輸ルートの支配も重要な収益源である。

- 小規模犯罪・詐欺

  銀行強盗、家畜の略奪に加え、欧州等のローンアクターによる税金や社会保障給付の不正受給、還付金詐欺などの経済犯罪も報告されている。

3. 自己資金や公的制度の悪用

組織に属さない単独犯や小規模セルにおいて、追跡が困難な資金獲得手法が多用されている。

- 合法的な個人的所得

  個人の給与、貯蓄、あるいは親族・友人からの個人的な支援が、特に低コストな攻撃（ローンウルフ型）の主たる原資となっている。

- 公的な社会保障給付

  失業手当、子供手当、障害手当などの政府給付金を、渡航したテロ戦闘員（FTF）やその家族が継続受給し、活動資金に充てる脆弱性が指摘されている。

- 融資の悪用

  消費者ローン、学生ローン、クレジットカードのキャッシングなどを、返済の意図なく最大限引き出し、渡航や攻撃準備に充てる手法が確認されている。

4. 合法的な経済活動・寄付の悪用

- 実業への投資・運営

  不動産、建設、レストラン、ガソリンスタンド、中古車販売などの実業を営み、そこからの利益を活動資金に充てている。アル・シャバブは収益の約 30%を投資に回していると推定される。

- 寄付・クラウドファンディング

  SNS や人道支援を装ったウェブサイトを通じ、世界中から少額の寄付を募っている実態がみられる。

- NPO の悪用

  正当な NPO の資金流用や、最初から資金集めのために設立された偽装 NPO による活動が確認されている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

テロ資金の移動手法は、伝統的な銀行送金や現金の物理的運搬に加え、暗号資産やモバイルマネー、さらにはオンライン上の新技術を悪用した手法へと急速に拡大している。

1. 伝統的な金融サービス

- 銀行送金（Wire Transfers）

  迅速かつ容易に世界中へ送金可能であるため、依然として主要なルートの一つである。監視を逃れるために送金額を少額（1万ドル未満等）に分割するスマーフィングや、最終的な受益者の特定を困難にするネステッド・アカウント（入れ子状の口座）が悪用されている。

- 資金移動サービス（MVTS）

  銀行サービスが制限されている地域や紛争地への主要な送金手段であり、身分証明書の偽装や共謀した代理人を介してテロ組織へ資金が流れる。現金集約的で非公式な性質を持つため匿名性が高く、テロ組織にとって魅力的なチャネルとなっている。

- ハワラ及び非規制資金移動サービス（HOSSP）

  正規の金融システムを介さない地下銀行であり、中東、アフリカ、南アジアで広く普及している。書類上の記録が残らず匿名性が極めて高いため、ISIL-K などの組織が国際的な資金移動や収集に多用している。近年はブロックチェーン技術を統合し、デジタル化を進める動きも確認されている。

2. 物理的な移転及び貿易の悪用

- 現金の物理的な密輸

  テロ資金の移動において依然として支配的な方法であり、アフリカ、中東、東南アジアで広く報告されている。家畜や農産物、その他の商品の中に現金を隠匿して国境を越える手法に加え、近年ではドローン等の技術デバイスを用いた輸送も報告されている。

- 貿易を利用したテロ資金供与（TBTF）

  商品の価格を不当に操作するインボイス不正（過小・過大請求）を通じて、合法的商取引を装い価値を移転させる。具体例として、カナダからレバノンへの盗難車・高級車輸出を通じてヒズボラに資金が提供されている事例が挙げられる。

- 貴金属・宝石及び現物支給

  金や宝石を代替通貨として利用し、公式な銀行システムをバイパスして物理的に運搬・換金する。不動産投資を通じた価値の保存・移転や、家畜（牛など）を用いた支払いも行われている。

3. デジタル技術及び新興決済手段の悪用

- 暗号資産

  ビットコインに加え、USDT（テザー）などのステーブルコインへのシフトが顕著である。Monero（モネロ）等の秘匿性の高い通貨の利用や、P2P 取引、ミキシングサービスを悪用して追跡を困難にさせている。

- モバイルマネー

  サハラ以南のアフリカ等で、ハワラと連携して規制外の国境を越えた送金に悪用されている。PayPal 等の P2P 決済サービス、SNS 上のチップ機能やライブ配信の「投げ銭」機能も少額寄付の収集に活用されている。

- クレジットカード

  匿名での国際的な資金移動が可能なオープンループ型のプリペイドカードが悪用されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

テロ組織及びその支援者は、法執行機関による検知を回避し、継続的かつ効率的に資金を調達・移動させるため、合法的な経済活動の基盤や、最新のデジタルプラットフォームを巧妙に悪用している。

1. 法人等

- 法人（フロント会社、シェルカンパニー等）

  実質的支配者を隠蔽するために、複雑な法的構造が悪用されている。不動産、建設、貿易（中古車等）、レストラン、ガソリンスタンド等の実業を行うフロント会社が、資金の洗浄や隠匿、あるいは合法的な収益とテロ資金を混在させる基盤として利用されている。

- 非営利団体（NPO）

  慈善、宗教、教育目的の団体が、テロ組織によって資金調達の「フロント」として悪用されるほか、管理体制が脆弱な組織は資金転用のプラットフォームとなるリスクにさらされている。最初からテロ支援の目的で設立された偽装 NPO も存在し、人道支援を装って寄付を募る事例が報告されている。

2. デジタルプラットフォーム

- SNS

  Facebook、X（旧 Twitter）、Instagram、TikTok 等が、寄付呼びかけの拡散や、寄付用サイトへのリンク・QR コードの掲示に利用されている。

● メッセージングサービス

Telegram や WhatsApp などの暗号化されたチャットアプリが、資金移動の指示や暗号資産ウォレットアドレスの共有、ハワラ業者との連絡手段として不可欠な基盤となっている。

● クラウドファンディング・プラットフォーム

公開型のプラットフォームや独自のプラットフォームが、戦闘員の家族支援や武装費用などの特定プロジェクトへの資金募集に利用されている。

● オンラインゲーム

ゲーム内チャットが連絡手段として、ゲーム内通貨の譲渡・売却が金融規制を回避した価値移動手段として悪用されており、特に若年層へのアプローチ基盤となっている。

● EC プラットフォーム

EC サイト（衣類・音楽販売等）が、物品販売を装った資金獲得手段として利用されるケースもある。

3. 公的制度

● 社会保障制度

社会保障給付をテロ戦闘員やその家族が受給し、活動の原資とするケースがある。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

テロ資金供与のリスクは、各国の地理的条件、経済発展の段階、社会構造、及び文化的な慣習と密接に関連している。これらの要因は、テロ組織が資金を調達・移動させるための隙間、すなわち脆弱性として機能することが指摘されている。

1. 地理的・社会的な要因

● 紛争地域との近接性

紛争地域やテロ組織が活発に活動する国と国境を接している、あるいは地理的に近い場合、資金、物資、戦闘員の輸送経路として悪用されるリスクが極めて高い。

● 特定のコミュニティ、ディアスポラとの繋がり

紛争地域にルーツを持つ民族や大規模な難民コミュニティが存在する場合、コミュニティ内の思想的同調者による寄付や、家族支援を目的とした送金ネットワークがテロ資金供与に利用される脆弱性がある。

● 国境管理の脆弱性

広大で監視の行き届かない国境線は、現金の密輸や、金、農産物、家畜といった現物資産の秘密裏の移動を容易にする。

2. 経済構造や金融インフラの特性

- 高い現金依存度と非公式経済の規模

  多額の現金を基盤とする経済や、地下銀行等の規制が届かない非公式セクターが大規模に存在する場合、金融システムの監視網を回避した資金移動が可能となる。

- 非公式送金システム（ハワラ等）の普及

  銀行サービスへのアクセスが限られている地域では、文化的・歴史的にハワラ等が生活に根付いており、これがテロ組織の国際的な資金収集・移動のインフラとして悪用されている。

- 低い金融包摂率とモバイルマネーの普及

  伝統的な銀行口座の普及が遅れる一方でモバイルマネーが急速に普及した地域では、エージェントの管理体制が脆弱な場合、偽名アカウントを通じた資金移動の隙を生む。

- 国際的な金融・貿易ハブとしての立ち位置

  開放的な経済を持ち、膨大な資産移動や複雑な商取引が行われる環境は、テロ資金を通常の経済活動の中に紛れ込ませるための隠れみのとなる。

3. 不安定な統治機構

- 政治・行政の不全

  政治的不安や行政能力の限定的な地域では、テロ組織が地域社会を実効支配し、独自の課税や資源搾取を行う「空白地帯」が生じやすい。

- 天然資源の管理態勢の脆弱性

  石油、金、宝石などの資源が豊富でありながら採掘・取引の規制が脆弱な場合、テロ組織がサプライチェーンを支配・恐喝し、巨額の継続的収益を得る基盤となる。

4. デジタル化

- デジタル化の進展

  デジタル化が進んだ社会では、SNS やオンラインゲームが生活の一部となっており、特に IT リテラシーの高い若年層が物理的な国境を越えた勧誘や小口資金提供のターゲットとなりやすい。

②-2-1.テロ資金供与を防止するための法的枠組み

テロ資金供与を効果的に防止・抑制するためには、国際基準（FATF 勧告）に準拠した強固な法的枠組みの構築が不可欠である。不十分な法整備は、テロリストによる金融システムの悪用や、訴追の失敗を招く重大な脆弱性となる。

②-3-1.金融当局等の監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-3-2.NPO の規制、監督・アウトリーチ

非営利団体（NPO）セクターに対する規制と監督は、正当な NPO 活動を不当に妨げたり阻害したりすることなく、テロ資金供与への悪用を防止するバランスの取れたアプローチが求められる。

1. リスクベース・アプローチ（RBA）の適用

- ターゲットを絞った規制

  全ての NPO を一律に規制するのではなく、FATF の定義に該当し、かつテロ資金供与への悪用のリスクが高い NPO を特定して保護する法的枠組みが必要である。
- リスク評価の実施

  国家のリスク評価結果に基づき、テロリストによる資金流用や組織の悪用（偽装 NPO 等）を防ぐための適切な措置を講じることが求められる。
- 比例原則の遵守

  監督・監視措置は、対象のリスクの程度に比例して実施されるべきである。

2. 実効的な監督

- 専門性の確保

  規制当局は、不審な行動を特定するためのテロ資金供与に関する専門知識を備える必要がある。
- 税務データの活用

  税務当局が保有する財務諸表や活動報告書などのデータは、NPO の背景や資金の流れを把握するための重要な情報源として活用されるべきである。

3. アウトリーチ

- ベストプラクティスの共有

  当局は NPO に対し、テロリストによる悪用の手口や、寄付者及び現地協力者のデューデリジェンス方法等についてのガイダンスを提供すべきである。
- セクターとの対話

  NPO と共同で、リスク評価の作業部会を開催することも有効である。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-2.NPO の活動・対応

非営利団体（NPO）がテロ悪用の脅威から自組織を保護し、セクターの健全性を維持するためには、外部の規制に依拠するだけでなく、自主的なガバナンスの強化とリスクベースの内部管理措置を講じることが重要である。

1. ガバナンスの強化と内部統制の整備

- ガバナンス体制

  定款や規約に基づく透明性の高い組織運営、理事会による活動の積極的な監視、及び財務・人事方針の策定が基盤となる。

- リスクベースでの内部管理

  画一的な管理ではなく、組織の規模や活動地域、特定の資金調達リスクに応じた、的を絞った比例原則に基づく措置を設計・実施すべきである。

2. 関係者に対するデューデリジェンス

- パートナー及び寄付者の検証

  契約締結前に、公開情報の検索や選定基準の活用を通じて、パートナー組織や寄付者の評判・実態を確認する。

- 対象を絞ったスクリーニング

  高リスクな状況下においては、職員やパートナーに対し、制裁リストを用いたスクリーニングを実施することが推奨される。

- 受益者の実在確認

  支援が意図した通りに届けられているかを確保するため、サービス提供時に受益者の実在や適格性を確認する手順を確立する。

3. 資金の管理

- 厳格な財務記録の保持

  運営全般における収入・支出の完全な記録を保持し、可能な限り正規の金融システムを通じて取引を実行することで、透明性と追跡可能性を確保する。

- 資金移動の承認プロセス

  支払いや送金の決定に最低 2 名の承認を要する原則の導入や、年間予算の承認プロセスの構築を通じて、資金の流用や濫用を防止する。

- プロジェクトの監視

  活動目的と範囲を明確に定義し、詳細な予算管理と定期的な現地訪問・報告を通じ

て、リソースが当初の目的通りに使用されているかを直接的に管理・統制する。

- 透明性の高い募金活動

  SNS やクラウドファンディングを利用する際は、活動実態と報告書の整合性を保ち、不透明な資金収集を避けることで寄付者や金融機関の信頼を維持する。

4. 外部との連携資金使途の管理

- 金融機関との対話

  自組織の対策状況を正しく理解させるための対話を促進し、不当なデリスキング（取引拒絶）を回避するための信頼関係を構築する。

- 連合組織の活用

  支部組織や連合組織への加盟を通じて、知識共有や専門性の向上を図り、行動規範の遵守を通じた説明責任を果たすことが有効である。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

テロ資金供与の脅威が顕在化する可能性は、伝統的な手法の固執と新技術による加速、さらには地政学的な構造変化により、以前に増して複雑かつ高い水準で推移している。

1. 手口の高度化と技術的要因による加速

現金やハワラといった伝統的な送金チャネルは依然として支配的であり、今後も継続される可能性が高い。これら伝統的チャネルと暗号資産やモバイルアプリ等のデジタル技術の組み合わせが加速しており、資金移動の検知をより困難にさせている。

また、テロ組織の分散化に伴い、自己資金（給与、社会保障給付等）や小規模犯罪に基づくマイクロファイナンス戦略を用いる組織や、ローンアクター、小規模セルが増加している。これらの活動は日常的な金融活動に紛れるため、事前検知のハードルが極めて高くなっている。

2. 特定地域における地理的な脅威の拡大

アフガニスタンを拠点とする ISIL-K は、ロシア語や多言語によるプロパガンダを通じて欧州や中央アジア等へ脅威を拡大させており、最も深刻な懸念の一つとなっている。また、サハラ以南のアフリカ（特にサヘル地域）が世界のテロの震源地として浮上しており、現地の天然資源搾取や非公式経済に依存した強固な資金基盤を有している。

3. 社会的・動機的要因の変化

デジタルネイティブ世代がオンラインゲームや SNS を通じて過激化するリスクが高まっており、AI を用いた精巧なプロパガンダがこの傾向をさらに助長する可能性がある。実際に、欧州でのテロ逮捕者の 5 人に 1 人が未成年者であるなど、脅威の若年化が顕著である。さらに、政治的な分極化を背景とした、民族的・人種的に動機付けられたテロ（EoRMT）の増加が指摘されている。

4. 複合的なリスクの結びつき

テロ資金供与と薬物、武器、人身売買等の組織犯罪ネットワークとの結びつきが強化されており、特に現金依存度の高い地域でリスクを定着させる要因となっている。また、気候変動に起因する食料不安や資源不足が深刻な地域では、テロ組織が略奪や課税を行う機会が増え、地域社会の脆弱性を利用した資金獲得の脅威が顕在化しやすくなっている。さらに、テロ組織が活動する地域との金融・貿易上の結びつきが存在する場合、国内のリスクが低くとも資金の通過点として悪用される可能性を常に孕んでいる。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

テロ資金供与がもたらす影響は、単なる経済的損失に留まらず、国家の安全保障、金融システムの健全性、そして人道活動の根幹を揺るがす深刻なものである。テロ資金供与は直接的にテロ活動を支援することを目的としているため、社会に与える実害の性質がマネー・ローンダリングや脱税よりも深刻であると想定される。

（3）米国

米国では、財務省が FATF の方針に基づいて、基本的には米国をとりまく「脅威」、「脆弱性」、「結果」の 3 つの要素を合成してリスクを評価している。「脅威」について、米国の NRA において特徴的である要素は、テロ組織やそのファシリテーター、及び米国の金融システムを悪用しようとする過激化した個人が含まれる点である。「脆弱性」については、特定の金融商品、規制・監督・執行における弱点、あるいはテロ資金調達者に機会を与える固有の状況等を指している。「結果」については、流通する資金の量が多いほどテロ資金供与に及ぼす影響も大きくなる傾向がある一方で、少額の資金でも壊滅な人的被害をもたらし得る、という特性があることに言及している。

また、米国においてはこの「脅威」、「脆弱性」、及び「結果」の要素に加えて、規制・監督・執行等の「軽減措置」の効果を考慮に入れた後の総合的な判断として、リスク評価を位置づけている。

本調査では、図表 1：調査対象文献に記載の文献を対象に、「①脅威」「②脆弱性」「③発生可能性と結果」に関する調査を実施した。

①脅威

米国内におけるテロ資金供与の主体は、高度に組織化された外国テロ組織（FTO）から、特定の組織に属さない国内の個人に至るまで多岐にわたり、その形態は複雑化・分散化の傾向にある。米国内及び国際的な安全保障に対する脅威として、以下の組織・個人が特定されている。

①-1-1.テロ組織、テロリスト

主に国内過激主義者（DVE：Domestic Violent Extremists）と外国テロ組織（FTO：Foreign Terrorist Organizations）に二分される。

- 国内過激主義者（DVE）

  米国内を拠点とし、外国のテロ組織からの直接の指示やインスピレーションを受けずに、政治的・社会的目標のために不法な暴力行為を行う個人である。米国にとって最も差し迫ったテロ脅威の一つとされる。その中には、「人種・民族的に動機付けられた過激主義者（RMVE）」と呼ばれる、DVE の中で最も懸念されるカテゴリーが存在し、特に白人至上主義を信奉する者が、宗教・文化施設や政府機関を一貫して標的としている。その他には、「反政府・反権力過激主義者（AGAAVE）」や、特定の政党や派閥に関連するとみなされる個人・団体への暴力を企てる者や、米軍・法執行機関を標的にする民兵過激主義者（MVE）が含まれる。
- 外国テロ組織

- ISIS（イラク・レバントのイスラム国）

  主要指導者の喪失後、階層を抑えた緩やかなネットワーク構造（アフィリエイト）へ移行しているが、依然として地域的・世界的な脅威であり、特に ISIL-K は外部作戦能力を保持している。
- アルカイダ（AQ）

  指導部の損失により分散化が進んでいるものの、アフリカのアル・シャバブや AQIM などの支部を通じて、依然として強力な脅威となっている。
- ヒズボラ

  洗練されたグローバルな資金調達ネットワークと軍事能力を維持し、国内外で米国の利益を脅かしている。
- ハマス及びパレスチナ・イスラム聖戦（PIJ）

  ハマスは 2023 年 10 月のイスラエル攻撃を首謀し、ガザ地区を拠点に活動している。PIJ はイランの支援を受けるテロ代理組織として、ハマスの攻撃以降、米国の要員や同盟国を脅かす存在として再浮上している。
- その他

  ロシアを拠点とする白人至上主義組織「ロシア帝国運動（RIM）」や、シリアのアルカイダ関連組織「ハヤト・タハリール・アル・シャーム（HTS）」などが指定されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

組織に直接属さないものの、思想的な共鳴や専門的なスキルの提供を通じてテロ活動を支える主体として、以下のものが挙げられる。

- 外国の暴力ジハード主義思想に影響を受けた個人

  外国のテロ組織から個別の指示は受けていないが、主に外国のジハード主義的信念に触発された米国内の個人である。組織に属さず、銃器や車両を用いた低コストのローンウルフ型の攻撃を行う特徴がある。SNS 等を通じてオンライン上で過激思想に染まり、予兆の検知が困難な攻撃を実行しようとする個人の存在が確認されている。
- 非公式な資金移転ネットワークを提供する主体

  武器調達、勧誘、資金移転などのサービスを提供する専門的なネットワークである。トルコ、イラク、アフリカなどに拠点を置き、ハワラや暗号資産等を駆使して ISIS-K やアル・シャバブ等の資金移動を支えている。
- ディアスポラ（移住先の同胞コミュニティ）

  世界各地に居住するレバノン系ディアスポラなどのコミュニティにおいて、ヒズボラ等の組織に共感し、個別に資金提供を行うメンバーが存在する。
- 偽装 NPO 及び寄付者

人道支援を装い、ハマスや PIJ 等への資金移動の導管として機能する団体の運営者が存在する（例：Al-Ansar Charity Association）。また、クラウドファンディング等を通じ、人道目的と誤認して、あるいは意図的にテロの大義のために資金を提供する個人（意図的又は無意識の寄付者）が世界中に存在する。

● 加速主義（アクセレラショニズム）の信奉者

社会の不安定化や人種戦争の誘発を目的として、エネルギー、通信、公衆衛生などの重要インフラへの攻撃を推奨・支援する RMVE の一群である。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

テロ組織は、その活動維持及び拡大のため、犯罪行為による収益獲得のみならず、合法的な経済活動や国家からの支援を巧妙に組み合わせた多角的な資金獲得スキームを構築している。

● 犯罪行為による資金獲得

- 恐喝・徴税及び誘拐・身代金

ISIS-K や ISIS-Somalia は、地域の企業や金融機関への恐喝を通じて多額の収益を得ている。また、アル・シャバブはソマリア国内において、検問所での通行税徴収や不動産への違法な課税など、組織的な恐喝を行っている。ハマスもガザ地区の統治権力を利用し、地元住民を恐喝することで相当な収益を上げている。身代金目的の誘拐も、ISIS の各支部（特に ISIS-K や ISIS-Somalia）及びアル・シャバブにとって重要な資金源となっている。

- 密輸（石油・木炭等）及び麻薬・武器取引

アル・シャバブは、国連で禁止されている木炭の違法輸出ネットワークを運営し、ペルシャ湾諸国へ出荷することで収益を得ている。ヒズボラは、イランのイスラム革命防衛隊（IRGC-QF）と協力し、原産地を偽装した複雑な石油密輸スキームを展開している。また、アル・シャバブはイエメンの武器密輸業者と連携しているほか、ヒズボラはグローバルな犯罪ネットワークを通じて麻薬取引や武器の密売に関与している。

- 資金洗浄・詐欺

DVE による薬物売買等の違法行為のほか、ヒズボラによる美術品、ダイヤモンド、高級品の取引を利用した大規模な資金洗浄ネットワークの構築が確認されている。

● 合法活動及び外部支援による資金獲得

正規の金融システムや商取引、公的支援を悪用した資金獲得も依然として大きな脅威となっている。

- 国家支援

ヒズボラはイラン政府から年間数億ドルの直接支援を受けているほか、ハマス

もイランから年間約 1 億ドルの支援を受けている。

- 投資ポートフォリオ、フロント企業及び事業収益

  ハマスは、アルジェリア、サウジアラビア、トルコ、UAE などの企業や資産に投資する、少なくとも 5 億ドル相当の高度な国際投資ポートフォリオを管理している。また、アル・シャバブは合法的事業を装う実業家の支援を受け、ヒズボラは不動産、建設、輸出入などの合法的な事業分野でフロント企業を運営し、多額の利益を上げていることが確認されている。

- 自己資金・寄付

  DVE の攻撃資金は、主に個人の貯蓄や給与などの合法的な自己資金で賄われている。ヒズボラは世界中のディアスポラからの寄付を集め、ISIS やハマスは SNS、暗号化アプリ、クラウドファンディングを通じて世界中の支持者から小口の寄付を広く募っている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

獲得されたテロ資金を組織や実行犯へ移転・提供する手法は、伝統的な金融システムから先端技術を用いたものまで多岐にわたる。テロ組織は、監視の目を逃れるためにこれらの手法を組み合わせ、資金移動の秘匿化を図っている。

- 銀行サービス及びコルレス銀行

  銀行サービスは、その規模と処理能力の高さから、依然としてテログループに悪用されている。ヒズボラ、ハマス、アル・シャバブなどの主要組織が、国際金融システムを利用して資金を移動させている実態があると報告されている。

- 資金移動業者（MSB）

  登録済みの MSB と未登録の MSB に二分されるが、いずれも銀行口座を持たない層へのサービス提供や海外送金の容易さが、テロ資金供与に対する脆弱性として悪用されている。特に、登録済みの MSB は ISIS 支持者による渡航資金の送金や、ヒズボラによる世界規模の資金移動に利用されている。一方で、未登録の MSB については、規制の網を逃れるために、ISIS やアルカイダ等のグループ自らが国際的な資金移動に利用しており、法執行機関による疑わしい取引の把握を困難にさせている。

- 暗号資産

  ISIS-K やハマスなどが利用を拡大させており、ビットコインに加えて、価格変動リスクを抑えられるステーブルコイン（テザーなど）の利用が増加している傾向にある。

- 現金及び現金の密輸

  現金は匿名性が高く電子的記録が残らないため、依然として主要な資金調達・移転の手段である。ISIS 支持者による渡航資金の直接運搬や、ヒズボラによるスーツケースに詰めた米ドルの空路運搬などの事例が確認されている。

● 伝統的・非公式な資金移転システム

主にハワラが伝統的かつ非公式な資金移転システムとして多用されており、ISISが紛争地や公的金融機関が機能していない地域での資金移動に多用しているほか、アル・シャバブも国際的な資金移動において利用を継続している。また、モバイルマネーも東アフリカや中央アフリカの地域でISISやアル・シャバブによって広く利用されており、携帯電話プラットフォームを通じて迅速な資金移動が行われている実態がある。

● 新興決済プラットフォーム及びその他

P2P 決済アプリが普及したことによって、モバイルやデスクトップを介した迅速な送金手段として悪用されており、さらに現金やハワラと組み合わされることで、資金追跡をより複雑にさせている。また、特殊な事例としてギフトカードをダークウェブ上で売却して現金化し、テロ活動を宣する目的で利用されるケースがある。ISIS支持者が軍資金としてギフトカードを提供した起訴事例も報告されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

テロ組織及びその支援者は、監視の回避や効率的な資金移動を実現するため、既存の法的枠組みや最新のデジタル技術を基盤とした多様なプラットフォームを組織的に悪用している。

● 法人（フロント会社、ペーパーカンパニー等）

テロ組織は、実態のある事業活動を隠れ蓑として利用している。アル・シャバブは、自ら登録したビジネスを、違法な木炭の密輸ネットワークの仲介に利用している。ヒズボラは、船舶の所有権やイラン産石油の供給源を隠蔽するために複雑なフロント会社網を構築しているほか、不動産や建設、高級品取引などの合法的事業セクターにおいてフロント会社を運営し、爆発物の原料となる肥料の調達にもこれらを活用しようとした事例が確認されている。さらに、特定のMSBが組織的なテロ支援の基盤となるケースも存在する。一例として、レバノンの経済学者が所有するMSB（CTEX社）が、ヒズボラへの米ドル資金提供のためのフロント会社として設立・運用されていた事例が挙げられる。

● NPO（テロ支援・協力組織、管理体制が脆弱な組織等）

人道支援を装った「偽装チャリティ」が、テロ組織（ISIS、アル・シャバブ、ハマス等）の資金洗浄や資金調達の導管として悪用されている。具体的な組織として、ガザの「Al-Ansar Charity Association」（ハマス・PIJに関連）、PIJが運営する「Muhjat Alquds Foundation」、ヒズボラを支援する環境団体「Green Without Borders」、及びMMIが設立した「World Human Care」などが、資金提供の基盤として特定されている。

● ソーシャルメディア及びメッセージングサービス

SNS は、DVE の過激化や攻撃の呼びかけに利用されるだけでなく、直接的な資金調達の場となっている。また、ISIS は Telegram 等の暗号化アプリを積極的に活用して寄付を募り、RMVE は「Terrorgram」と呼ばれる Telegram チャンネル網を通じてプロパガンダの共有や攻撃の称賛を行っている。ハマスもまた、SNS やメッセージアプリ上で寄付の勧誘を投稿している実態があることが報告されている。

● クラウドファンディングプラットフォーム及びオンラインゲームプラットフォーム

これらのプラットフォームは、匿名性、グローバルな到達範囲、及び送金の速さに着目され、多数のテロ組織が悪用している実態がある。特に DVE は訴訟費用や渡航費の調達に、ハマス支持者は人道支援を装った「ガザへの寄付」の収集に、オンラインクラウドファンディングを悪用した事例が確認されている。また、ISIS は、オンラインゲームプラットフォームを資金移動やコミュニケーションの場として利用することを試みていることが報告されている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

米国内におけるテロ資金供与対策の有効性を阻害する要因として、グローバルな金融・経済システムにおける米国の立ち位置や、憲法によって保護された個人の権利、さらには社会的な緊張状態といった、同国固有の背景が脆弱性として指摘されている。

● 国際金融・貿易における米国の役割と膨大な取引量

米国の銀行は、グローバルな金融システムで処理される大半の取引を促進する役割を担っている。また、同国の金融機関が提供するコルレス銀行サービスは、AML/CFT 体制が脆弱な法域の銀行とも接続している。これらの膨大な取引量そのものが、テロ関連取引の特定を極めて困難にしており、本質的なリスクが高い状態にあると評価されている。特にハマスやヒズボラ等の外国テロ組織にとって、米国は高度な金融システムと大規模な経済市場を有する「収益を生み出す場」として利用されている。これらを背景に、複雑な資金洗浄や投資、寄付収集が行われる脆弱性が存在している。

● 社会・政治的不満の深刻化と過激化の土壌

選挙、パンデミック、移民政策といった社会・政治的な不満が、DVE の脅威を煽る要因となっている。こうした国内の社会的緊張が、オンライン上での過激化や寄付収集を促進する背景として存在しており、過激化した個人（DVE や HVE を含む）の多くは、個人の貯蓄や給与といった合法的な手段による自己資金によっても攻撃資金を賄っている。これらの資金は通常の家計支出と区別がつかず、金融機関が事前に不審な取引として検知することを著しく困難にしている。

● 合衆国憲法による権利保護と法的限界

合衆国憲法修正第1条等で保護された表現や結社の自由に従事する個人の行為は、具体的な暴力行為と結びつかない限り合法である。多くのDVEは、許容される行為と違法行為の境界を熟知しており、金融活動と暴力を法的・論理的に結びつけることを困難にしている。

- 米国内での現金利用の匿名性

  匿名性、流動性、及びフットプリントの欠如を理由に、ISIS支持者等のテロ支持者は依然として現金を多用している。具体的には、海外渡航資金の運搬や、攻撃のための武器・材料の購入に現金が利用されており、規制された金融機関を介さない資金移動が監視を回避する手段となっていることが報告されている。

②-2-1.テロ資金供与を防止するための法的枠組み

米国におけるテロ資金供与対策の法的枠組みは、金融機関への義務付け、制裁措置、及び当局の権限強化を柱として構成されている。

- 銀行秘密法（BSA：Bank Secrecy Act）

  米国の金融機関（銀行、資金移動業者（MSB）、カジノ、暗号資産交換業者等）に対し、AML/CFTプログラムの構築、疑わしい取引の届出（SAR）、及び記録保持を義務付ける中核的な法律である。

- AML/CFT国家優先事項（FinCEN Priorities）

  金融犯罪取締ネットワーク（FinCEN）が発行する国家優先事項であり、国内外のテロ資金供与リスクを網羅し、金融機関がリスクベースの対策を講じる際の指針となっている。

- テロリスト資産凍結制度（OFAC等）

  外国資産管理局（OFAC）等による制裁指定を通じ、テロ組織やその支援者の資産を凍結し、米国金融システムから排除することを可能にしている。

- 疑わしい取引の届出（SAR）基準

  金融機関に対し、一定の敷居値（MSBは2,000ドル、その他は5,000ドル）を超える疑わしい取引の届出を義務付けており、テロ資金供与の探知において不可欠な役割を果たしている。

- パートナーの審査（USAID Vetting）

  国際開発庁（USAID）が、高リスク環境で活動する実施パートナー（NPO等）に対し、テロ組織への資金流用を防ぐための追加的な審査・評価措置を講じる枠組みを設けている。

- 法的限界及び制度上の脆弱性

  現金（特に米ドル）は匿名性が高く、電子的記録が残らないため、規制された金融機関を介さないキャッシュ・クーリエによる国境を越えた資金移動が監視回避の主要な手段であり続けている。

②-3-1.金融当局等の監督・アウトリーチ

当局による監督活動及び関係各所へのアウトリーチは、金融システムの透明性を維持し、テロ資金供与リスクを効果的に低減するための不可欠な要素となっている。

- 銀行セクターの監督とデリスキリング対策

  大手銀行は BSA を遵守し、高度なリスク緩和措置及びモニタリング体制を維持している。一方で、リスク過多を理由に銀行が特定の顧客（NPO 等）との取引を拒否するデリスキリングの問題に対し、当局はその影響を指摘している。金融包摂を維持しつつ、透明性を確保するための戦略を推進し、不透明なチャネルへの資金流出防止を図っている。

- 資金移動業者（MSB）への規制とモニタリング

  当局は MSB に対し、AML プログラムの構築、疑わしい取引の届出（SAR)、及び記録保持を厳格に義務付けている。2020 年から 2022 年の間に報告されたテロ資金供与関連の SAR のうち、約 72%が MSB によるものであり、当局のモニタリングにおいて MSB が極めて重要な役割を果たしていることが示されている。

- 暗号資産交換業者（VASP）への厳格な法執行

  米国で活動する VASP に対し、BSA に基づく登録と AML/CFT に関する義務を課している。例えば大手交換業者 Binance に対する過去最大規模の民事制裁金の賦課や創設者の起訴事例は、未登録業者やコンプライアンス違反に対する当局の監視と法執行の有効性を実証するものとなっている。

②-3-2.NPO の規制、監督・アウトリーチ

NPO セクターにおけるテロ資金供与リスクの低減に向けて、当局は規制のみならず、透明性の確保及び正規金融システムへのアクセス維持を目的としたアウトリーチを強化している。

- NPO セクターとの共同取組及び指導

  財務省は NPO セクターと協力し、デューデリジェンスの強化及びリスク緩和策に関する指導を実施している。その結果、この 10 年間で、当該セクターはテロ資金供与の脅威への対応において大きな進歩を遂げたと評価されている。2022 年のテロ資金対策法改正法（NTFRA）においても、米国政府は多くの慈善 NPO がデューデリジェンス及びガバナンスを含む内部リスク低減措置を継続的に適用していることを認識している。

- 人道支援の透明性確保及びアウトリーチ

  財務省は、人道支援に関わる制裁認可を標準化し、NPO が銀行システムへのアクセスを維持できるようアウトリーチを行っている。当該措置により、NPO が規制外の不透明なチャネル（ハワラ等）へ流れるリスクを抑制している。

● 高リスク環境下での審査

国際開発庁（USAID）は、テロ組織が活動する高リスク環境のパートナーに対し、厳格な審査及びリスク管理計画の策定を義務付けている。これにより、人道支援資金のテロ組織への流用を未然に防止する体制を構築している。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

新技術の台頭に伴う新たなテロ資金供与リスクに対し、当局は既存の枠組みを超えた監督体制の強化を図っている。

● 新技術及び暗号資産ミキシングへの監督強化

FinCEN は、国際的な暗号資産のミキシングを「主要なマネー・ローンダリングの懸念」として特定している。米国当局は、取引の透明性を向上させるため、記録保持及び報告を義務付ける規則案（NPRM）を提示しており、新たな技術的脅威に対応した監督・規制枠組みの構築を推進している。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

テロ資金供与リスクの低減に向けては、公的機関による監督のみならず、民間セクターによる自主的な管理体制の構築及びリスクベース・アプローチの適用が重要な役割を担っている。

● 銀行・MSB

米国の大手銀行及び大規模な資金移動業者（MSB）は、銀行秘密法（BSA）を厳格に遵守し、高度な内部管理体制を構築している。各機関は、洗練されたコンプライアンスプログラムを運用するとともに、最新の技術を用いたリスク緩和及び取引モニタリング手法を維持している。

● 暗号資産交換業者（VASP）

米国内の VASP は、AML プログラムの構築、不審な取引の報告（SAR）、及び制裁遵守の義務を負っている。また、法執行機関やブロックチェーン分析ベンダーと協力してテロ資金供与対策に取り組む事例（Binance 等）も存在する。

②-4-2.NPO の活動・対応

米国の NPO セクターにおいては、テロ資金供与のリスクを自主的に管理・低減するための取組みが広く浸透しており、セクター全体のレジリエンス向上に寄与している。

● 自主的なコンプライアンス対策の適用

多くの慈善 NPO は、デューデリジェンス、ガバナンス、透明性、説明責任、及びコンプライアンス対策を自主的に適用している。これらの自律的な取組みにより、米国の税制優遇を受ける慈善団体の大多数において、テロ資金供与に悪用されるリスクは大幅に緩和されている。

● 高リスク環境下における管理体制

紛争地域又はテロ組織が活動する地域などの高リスク環境で活動する NPO は、支援資金の転用を防止するため、強化された審査や内部的なリスク緩和措置を講じている。

②-4-3.その他セクターの活動・対応

金融及び NPO セクター以外の関連分野においても、デジタル技術の進展に伴うテロ資金供与リスクの変容に対応した取組みが進められている。

● ソーシャルメディア企業のモニタリング

SNS 企業は、自社プラットフォーム上における不正な資金調達の投稿を迅速に特定し、削除するための継続的かつ警戒的なモニタリングが必要とされている。

● 新技術・プラットフォームにおける課題と対応

クラウドファンディングやオンライン募金の多くは合法的な活動であるが、その匿名性、送金の速さ、及びグローバルな到達範囲がテロ資金供与に悪用されやすいという脆弱性が存在する。これらの膨大な合法の取引の中から、テロ資金に関連する不正な利用を的確に識別することは、当該セクターにおける依然として困難な課題となっている。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

テロ資金供与の脅威が現実の暴力行為として顕在化する可能性は、国内外の情勢変化、技術の進展、及び過激化プロセスの変容に伴い、極めて高い水準で推移している。

● DVE の持続的脅威

DVE による脅威は、予見可能な将来にわたって持続すると評価されている。特に人種・民族的に動機付けられた過激主義者（RMVE）は、宗教、文化、及び政府の標的に対して最も一貫した致死的又は非致死的な暴力の脅威を与えている。

● 外国テロ組織の脅威の持続と再浮上

海外における米国及びその利益に対する外国テロ組織（ISIS、アルカイダ等）の脅威は依然として持続している。2023 年 10 月のハマスによる攻撃は、テロの脅威がいかに迅速に再浮上し得るかを浮き彫りにした。

● 新技術の採用と適応によるリスク

SNS の普及により、テロ組織や過激派運動が、オンライン通信に支えられた、より拡散されたネットワーク構造へと移行している。これにより、個人の自己資金による小規模な攻撃が増えており、米国本土への主要なテロ脅威は、テロ組織からの直接的な指示を受けずに、オンラインで過激化し、警告がほとんどない状態で致死的な攻撃を企てる個人から生じている。これらの個人は、組織に属さないローンウルフとし

て活動することが多いため、事前の探知が困難であるため、金融機関や法執行機関による未然の防止が極めて困難になっている。

- 重要インフラへの攻撃意欲の増大

  DVE、特に社会の不安定化を狙う加速主義を推進する RMVE の間で、エネルギー、通信、及び公共保健などの重要インフラに対する物理的な攻撃を求める声が強まっている。実際に電力網を標的とした攻撃の陰謀により起訴・判決が出されている事例が報告されている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

テロ資金供与の脅威が現実の暴力行為又は組織的な活動として顕在化した場合、その影響は単なる物理的被害に留まらず、国家安全保障、経済システム、及び社会の根幹を揺るがす甚大な事態を招く恐れがある。

- 甚大な人的被害の発生

  テロリズムの実行には比較的少額の資金で足りる場合があるが、ひとたび攻撃が実行されれば、修復不可能な甚大な人的被害（致死的な暴力）をもたらす結果となる。

- 重要インフラの破壊及び経済的損失

  電力網、通信、及び公衆衛生等の重要インフラへの攻撃は、政府に数百万ドルの直接的な損害を与えるのみならず、数ヶ月にわたる停電等の機能不全を引き起こす可能性がある。これにより、市民生活の維持が困難となり、多額の復旧費用及び経済活動の停滞による二次的な損失が発生する。

- 社会的不安の増幅及び治安の悪化

  大規模な暴力やインフラ破壊は、市民の間に深刻な不安を広げ、人種戦争の誘発又は「大恐慌」にも比肩する経済的・社会的な混乱を招くことが企図されている。

- 国家安全保障への深刻な脅威

  洗練された金融基盤を有するテロ組織（ハマス等）の殺傷能力を過小評価することは、国家安全保障に深刻な結果をもたらすことが示されている。テロ組織が国家構造や既存の制度を掌握・制限することにより、当該地域又は関連セクターの国際金融システムへのアクセスが制限される。これは貧困対策や持続的な経済成長を長期的に阻害し、国際社会全体の発展に悪影響を及ぼすこととなる。

- 人道支援活動の阻害及び脆弱性の連鎖

  NPO や資金移動業者が正規の銀行システムから排除されると、資金が不透明な代替チャネル（未登録の送金等）へ流れることとなる。この結果、政府の監視能力が低下し、さらなるテロ資金供与のリスクを招くとともに、真に支援を必要とする地域への人道支援が阻害されるという悪循環が生じる。

（4）英国

英国では、法執行機関におけるリスク管理モデルである「MoRiLE モデル」の拡張版を採用しており、「脆弱性」、「規模」、「軽減策」の 3 つの領域を検証することによってリスクの特定・評価を行うとしている。

- 脆弱性の算定基準：①取引量と送金速度、②高リスク地域や個人（PEPs 等）への露出度、③所有権の匿名性レベル、④サービスの複雑さとアクセスしやすさ、の 4 点を評価要素としている。
- 規模の算定基準：各セクターがテロ資金供与に悪用される頻度を指す。これは、犯罪者がテロ資金供与の手段として好む度合いを反映している。
- 軽減策の算定基準：①法執行機関、②監督機関、③民間企業のそれぞれにおける能力（人員、法的権限、技術的解決策、プロセス等）がリスクをどの程度抑え込めているかを評価する。
- 評価の決定：数値的な計算結果は、法執行機関、監督機関、政府部門の専門家パネルによって調整され、最終的に「高」「中」「低」の格付けに変換される。
- 格付けの定義：最終的な格付けは、各セクターにおける典型的なビジネス活動におけるリスク露出を反映したものである。格付けの閾値は 2020 年版の NRA と同じ基準が維持されている。

また、英国におけるリスクスコア算出の詳細基準は、以下の通りである。

- 固有基準の考え方：「脆弱性」が高い（匿名性が高い、あるいは送金が速いなど）セクターであっても、実際に犯罪者に利用されている「規模」が小さければ、固有リスクは限定的とみなされる。逆に、脆弱性が低く見えても、犯罪者が大量に利用している場合はリスクが高まる。
- 軽減策の影響：英国の NRA における大きな特徴は、民間企業の対策能力が直接スコアに影響を与える点にある。たとえ銀行セクターのように脆弱性が高く、規模が大きくても、企業の管理体制や当局の監視が強力であれば、最終的なリスクスコアは抑制される仕組みになっている。
- 思想・組織別の考慮（テロ資金供与に特有の考え方）：セクション 4.13 において、テロリストの性質（組織のレベルや戦略的意図）によって利用するメカニズムが異なり、組織化のレベルが上がるほど資金移動が複雑かつ高額になり、リスク評価に影響を与えることが記述されている。

①脅威

①-1-1.テロ組織、テロリスト

英国におけるテロ資金供与の脅威は、依然としてイスラム過激主義、極右、及び北アイル

ランド関連テロといった多様な背景を持つ主体によって構成されている。2025 年のリスク評価によれば、これらの主体は組織の規模や活動形態に応じて異なる資金ニーズと調達手法を有している。また、組織的なテロリズムと単独犯によるテロリズムの対比についても強調されており、特に後者の「自己開始型／単独犯テロリスト（ローンアクター）」は近年の対テロ戦略（CONTEST）において主要な脅威とされている。

- イスラム過激主義テロ

  英国に対するテロ攻撃の約 67%を占め、依然として最大の脅威となっている。主に「ダーイシュ（Daesh：ISIL）」や「アルカイダ（Al-Qaida）」の思想に触発された個人又はグループによる活動が中心である。また、「ヒズボラ（Hizballah）」に関連して、資金供与に関与した疑いで経済制裁対象となっている個人が、制裁を回避するために英国の美術品ギャラリーやオークションハウスを介して取引を行っていた事例が確認されており、制裁回避のネットワークとしての側面が警戒されている。

- 極右テロ（Extreme Right-Wing Terrorism: ERWT）

  英国において 2 番目に大きな国内テロの脅威として位置づけられている。組織化された動きよりも、特定の組織に属さない個人（ローンウルフ型）による活動が目立つ傾向にある。一方で、「System Resistance Network（SRN）」や「Sonnenkreig Division」といった指定グループが、テロ資金の収集や過激派出版物の配布に関与した事例も報告されている。

- 北アイルランド関連テロ（Northern Ireland-Related Terrorism: NIRT）

  暴力的な「反体制派共和派（Dissident Republicans: DRs）」が主な脅威である。北アイルランドの脅威レベルは 2022 年 2 月以降「相当」を維持しており、攻撃の発生可能性が高い状態が続いている。DR の構成員は、武器調達のみならず、車両、燃料、旅費といった組織の運営・維持のために継続的な収入を必要としているが、その資金管理体制は必ずしも標準化されておらず、グループや個人ごとに分断されている実態がある。

- クルディスタン労働者党（PKK）

  英国国内において階層構造を持って活動しており、組織犯罪グループのメンバーでもある若年層ネットワークが、小口資金の収集や運搬を分担して行っている。これらの小口資金の総額は数百万ポンドに達する場合があり、その一部がトルコ政府に対する攻撃計画の資金源となっている証拠も確認されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

英国におけるテロ資金供与の脅威は、実行犯のみならず、それらを支える広範な支援ネットワークや、意図せずあるいは不注意に資金移動に関与する主体によって複雑化している。

- NPO・チャリティ団体（テロ資金供与への悪用）

  英国における NPO セクター全体のリスクは低いと評価されているが、テロ組織が

支配する地域や紛争地帯の近傍で活動する団体は、その地理的要因により悪用リスクが著しく高いとされている。慈善活動を装う支援者の事例として、シリアでの農場やビル建設といった「慈善プロジェクト」を名目に資金を集め、実際には ISIL の武器製造拠点の構築を企てたケース（Tarek Namouz 事件）が報告されている。

- 外国人テロ戦闘員

  英国から海外のテロ組織に参加するために渡航した個人、あるいはその家族や友人が主たる主体である。家族からの援助、オンライン寄付、給与、ローン等を原資とし、暗号資産、プリペイドカード、送金サービス等を用いて海外へ送金が行われる。

- ディアスポラ（移民コミュニティ）

  母国の家族等への送金のためにハワラなどの非公式資金移動サービスを頻繁に利用するコミュニティが、テロ資金供与に悪用されるリスクがある。特にクルディスタン労働者党などの組織が、コミュニティイベントやビジネスを通じて資金を収集する際に、これらのネットワークが利用される実態がある。

- オンライン上で過激化した個人・小グループ

  テロ組織から直接の指示を受けず、オンライン上の宣伝活動に触発されて活動するローンウルフ型の個人である。資金源は給与やローンなどの合法的なものが主であり、攻撃準備のための資金も少額であることから、金融システム上での探知が極めて困難である。

- クラウドファンディング・ソーシャルメディア利用者

  オンラインプラットフォームや SNS を通じて寄付を募る手法が、テロ組織やその同調者にとって魅力的な手段となっている。これらは地理的制限がなく、世界中の聴衆に迅速にアクセスできるため、悪用されるケースが増加している。

- マネーミュール（資金運び屋）としての学生

  特に中国人留学生などが、組織犯罪グループによってマネーミュールとして利用されるケースが増加している。少額の報酬や学費の割引といった誘因により、自身の銀行口座を犯罪資金の移動に貸し出すことがあり、これが間接的にテロ資金等の不透明な送金経路を支える基盤となっている。

- 専門的便宜供与者（Professional Enablers）

  会計士、弁護士、信託・会社サービスプロバイダー（TCSP）が、不注意又は意図的に、テロ組織の資金洗浄や複雑な法人構造の構築を支援することがある。彼らは専門知識を提供することで、組織犯罪やテロ資金の流れを隠蔽し、正当なビジネス取引に見せかける役割を果たす。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

英国におけるテロ資金の獲得手法は、伝統的な犯罪収益の利用から、一見して不審とは見なされにくい合法的な手段の悪用まで多岐にわたる。

● 合法的な活動（給与、融資、手当等）

英国国内で調達されるテロ資金の多くは、犯罪行為ではなく、給与、学生ローン、個人融資、国家による給付金などの合法的な手段によって調達されている。その他には、PKK による英国国内の家族向けイベント、ビジネス、コミュニティ行事を通じた資金の収集、慈善活動を装った「寄付ベースのクラウドファンディング」や、SNS、オンラインゲームのチャットルーム等を活用した寄付の募集が増加しており、特に極右テロにおいて多用される傾向がある。極右テロに関連する個人やグループが、過激派の出版物や関連グッズを販売することで活動資金を調達しているケースも報告されている。また、NPO への無利子ローンによる資金調達の事例も確認されており、一部のチャリティ団体が地域コミュニティから「無利子ローン」として現金を受け取り、これが実質的な資金提供や資金洗浄の隠れ蓑となる脆弱性が指摘されている。

● 非合法的な活動

北アイルランド関連テロや PKK などの組織は、タバコ密輸、燃料の不法転用、薬物取引、武器の密輸入、不法移民の支援、及び人身売買といった多岐にわたる組織犯罪を資金源としている。他には、反体制派共和主義者（DRs）や高リスク地域で活動する国際的なテロ組織は、地元企業や住民を恐喝することで、組織の運営費や個人的な利益を強制的に徴収している。特殊な手口としては紛争地域で略奪された骨董品や文化財を、偽造された来歴証明書とともに販売し、その収益をテロ資金に充てるリスクが存在することが報告されている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

英国におけるテロ資金の移転手法は、従来の現金や銀行送金といった伝統的な手段に加え、暗号資産や電子マネーといったデジタル技術を組み合わせた多層的なプロセスへと進化している。特に近年の国内テロ攻撃においては、多額の資金を必要としない低コストかつ低技術の手法が主流となっている。

● リテール銀行

給与や融資といった合法的な資金をテロ資金として移動させる際の、最初の接点として広く利用されている。近年の攻撃事案では、少額かつ単純な送金が中心であり、日常的な取引に紛れることで検知を困難にさせている。

● 電子マネー（EMI）及び電子決済サービス（PSP）

利便性とアクセスの良さから、迅速な小口送金の手段として利用が増加している。EMI や PSP の代理店が顧客審査（KYC）を十分に行わないケースがあり、規制の網を潜り抜ける脆弱性が指摘されている。

● 資金移動業者（MSBs）

銀行口座を持たない個人や、特定の紛争地域への送金において依然として主要な手段である。第三者の仲介業者を介在させることで、最終的な受益者（指定テロ組織

関係者等）を隠蔽して送金を行う事例も確認されている。

- 暗号資産

  国境を越えた迅速な資金移動に利用され、特に「オフランプ（法定通貨への換金）」の後に決済サービスを介して海外へ送金されるケースが多い。資金はハイリスク地域の境界付近にある口座やウォレットへ送られ、そこでプリペイドカードへのチャージや現金化が行われ、テロ組織の手に渡る。給与受取（銀行）から暗号資産の購入、海外決済サービスへの入金・送金、プリペイドカードへのチャージ、国境を越えた密輸といった、複数の手段を組み合わせた多層的なフローにより、資金の出所と使途の特定を極めて困難にさせていることが報告されている。

- 非公式資金移動システム（IVTS／ハワラ）、現金密輸やプリペイドカードの利用

  移民コミュニティ（ディアスポラ）による母国送金の手段として日常的に利用されており、公式な記録が残りにくい特性を持つ。PKK などの組織が、数百万ポンド規模の多額の資金を移動させる際に悪用する事例がある。また、現金密輸も依然として利用されており、申告義務のない 1 万ポンド未満の現金を、運び屋が物理的に海外へ持ち出す伝統的な手法は、現在も有効な手段として継続している。その他にも、英国内で合法的にチャージしたカードを高リスク地域の国境付近へ物理的に持ち込み、現地で現金化してテロ組織へ提供する手法が確認されている。

- 美術品・骨董品などの取引

  制裁対象となっているテロ支援者が、英国の美術品ギャラリーやオークションハウスを通じて高額取引を行い、制裁を回避して資金を移動・洗浄する事例がある。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

テロ資金供与の主体は、資金を効率的に獲得し、かつ当局の追跡を回避して送金するために、既存の合法的なインフラや新興のデジタルプラットフォームをテロ資金供与の基盤として巧妙に利用している。

- 寄付型クラウドファンディング・プラットフォーム

  寄付ベースのクラウドファンディングは、地理的制限なく世界中の聴衆に迅速にリーチできるため、テロ資金供与にとって魅力的な手段となっている。英国において、これらのプラットフォームの多くはマネー・ローンダリング規則（MLRs）の対象外であり、当局への疑わしい取引の届出（SARs）義務がないことから、情報把握における空白地帯となっている。

- ソーシャルメディア及びメッセージングアプリ

  特に極右テロにおいて、オンラインゲームのチャットルームやフォーラムに決済サービスのリンクが掲載され、資金提供の入り口として活用されている。クラウドファンディングと同様に MLRs の適用外であるため、英国政府は悪用の規模や類型に

関する包括的なデータを十分に保有できていない実態がある。

- 法人構造・フロント企業及び事業基盤

  アルカイダや ISIL 等のテロ組織は、高リスク地域において市場参入管理の不備を突き、ビジネスに実質的な利害関係を持つことで資金調達の基盤を構築している。これらの収益は、英国国内の事業体への投資やサービス提供に利用されることもある。

- 暗号資産エコシステム

  暗号資産は、特に共有ウォレットなどの形式でクラウドファンディングと組み合わせて利用される。法定通貨への換金を支える決済サービス事業者も、テロ資金の移動を支える重要な基盤の一部となっている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

英国が有する高度に開放された経済体系、国際金融ハブとしての地位、及び多様な移住者コミュニティ等の社会的特性は、テロ資金供与に対する固有の脆弱性を形成している。

- 国際金融ハブとしての開放性

  英国の経済・金融システムが高度に開放されていることは投資を呼び込む一因となる一方、テロリストや犯罪者が複雑な法人構造や金融サービスを悪用して資金を隠蔽又は移動させる隙を与えている。

- 現金取引を中心としたサービスの存在

  現金は価値移動において匿名性が高く、依然として主要なリスクである。送金業務を行う資金移動業者（MSB）は現金取引が中心であり、少額資金の取り扱いや第三国経由の送金により、テロ資金調達の疑念を回避しやすい構造にある。特に、郵便局を通じた銀行預金サービスが、本人確認の脆弱性を突いた組織犯罪やテロ資金の預け入れに利用されるリスクが指摘されている。また、1 万ポンド未満の現金持ち出しが申告不要である仕組みを悪用し、運び屋が物理的に資金を海外の高リスク地域近辺へ持ち出すことが比較的容易な構造となっている。

- ディアスポラ・コミュニティの経済活動

  英国には大規模な移住者コミュニティ（ディアスポラ）が存在し、母国への送金ニーズが非常に高い。この文化的な結びつきが、ハワラ（IVTS）等の非公式な送金ネットワークの利用を促進し、結果としてテロ資金が混入するリスクを高めている。

- 北アイルランド固有の政治的・歴史的背景

  北アイルランド関連テロにおいては、長年の歴史的背景から犯罪組織、準軍事組織、及びテロ支援者の境界が曖昧となっている。これにより、合法的なビジネスと組織犯罪が混在した資金調達構造が地域社会に根付いている。

- 高リスク地域・紛争地帯への地理的近接性及び地政学的な緊張と政治的背景

  英国の NPO セクター全体のリスクは低いと評価されているものの、紛争地域やテ

ロリストが支配する地域で活動する団体は、活動の近接性から、セクターの他の部分よりも著しく高いリスクに晒されている。北アイルランド以外の地域については、中東、ウクライナ、及び北アフリカ等における地政学的緊張の変化が、英国国内のテロ脅威レベルやテロ資金の流れに直接的な影響を及ぼしている。

②-2-1.テロ資金供与を防止するための法的枠組み

英国は、テロ資金供与対策として、刑罰（TACT 2000）、予防的規制（MLRs 2017）、及び機動的な制裁措置（SAMLA 2018）を組み合わせた、重層的な法的枠組みを構築している。特に近年の法改正により、暗号資産の押収権限の強化等、技術変化に対応した法的基盤の整備が進められている。主要な法的枠組みは、以下の通りである。

- 2000 年テロ対策法（TACT 2000）

  英国におけるテロ資金供与に関する主要な刑事罰を規定する基本法である。「テロ資産」を定義し、資金の収集、保持、提供、及び利用に関する主要な犯罪（セクション 15-18 等）を規定している。

- 2001 年反テロリズム・犯罪及び安全保障法（ATCSA 2001）

  金融機関等に対し、テロ資金供与に関連する可能性のある口座の開示や、一定期間の口座監視（アカウント・モニタリング）を求める命令等の法的ツールを規定している。法執行機関がテロ資産（現金含む）と疑われる資産を差し押さえ、没収するための権限を規定しており、これは国境を含むあらゆる場所で適用可能である。

- 2002 年犯罪収益法（POCA）

  英国全土に適用されるマネー・ローンダリング罪と、民事・刑事上の没収制度を規定している。税関当局（HMRC）を含む法執行機関は、犯罪収益と疑われる現金等を差し押さえる権限を有している。

- 2017 年マネー・ローンダリングマネー・ローンダリング・テロ資金供与・資金移動規則（MLRs 2017）

  銀行、カジノ、士業等の被規制セクターに対し、顧客管理（CDD）、記録保持、及びリスク評価の実施等を義務付ける主要な予防的規制である。実効性を高めるため、継続的な見直しと動的な改正が行われている。

- 2018 年制裁・マネー・ローンダリング法（SAMLA 2018）

  国際的な協力に基づき、テロに関与した個人や団体に対して資産凍結等の制裁を課す権限を政府に付与している。

- 2022 年経済犯罪（透明性及び執行）法（ECTEA 2022）

  制裁措置の適用を迅速化し、制裁回避を困難にすることを目的としている。「海外事業体登録制度」の創設や「説明のつかない富に関する命令」の強化が含まれる。

- 2023 年経済犯罪及び企業透明性法（ECCTA 2023）

  テロ資金に関連する暗号資産を、迅速かつ容易に捜索、差し押さえ、及び回収する

ための新たな権限を法執行機関に付与している。法人責任のリフォームや、民間企業間の情報共有を促進する規定を含んでいる。

- 対テロ戦略（CONTEST）

  英国政府のテロ対策全体戦略であり、テロ資金のフローを検知、理解、捜査、阻止、及び遮断するための運用指針を示している。「4 つの P」（予防：Prevent、保護：Protect、準備：Prepare、追及：Pursue）を横断的に機能させることで目的達成を図っている。

- 報告義務及び国境規制

  テロ資金供与の疑いがある場合、被規制部門の企業は英国金融情報機関（UKFIU）に対して疑わしい取引の届出を行う義務を負う。さらに、英国の国境を越えて 1 万ポンド（又は相当額）以上の現金を移動させる際、税関への申告が義務付けられている。

②-3-1.金融当局等の監督・アウトリーチ

英国の各監督機関は、被規制セクターにおけるテロ資金供与リスクの理解を深め、検知能力を向上させるため、積極的なアウトリーチ及び指導を行っている。

- 金融・士業等（DNFBPs）へのアウトリーチ及び情報共有

  金融行動監視機構（FCA）、税関当局（HMRC）、及び専門職団体監督局（OPBAS）等の監督機関は、被規制セクターに対し、最新の脅威情報や「レッドフラグ（警告指標）」を含む詳細なガイダンスを提供している。合同マネー・ローンダリング情報タスクフォース（JMLIT）等の官民連携枠組みを通じ、テロ資金供与の最新トレンドを民間部門と共有することで、企業の自主的な検知・報告能力の向上を図っている。

- 士業（法務・会計）向け監督基準の高度化

  OPBAS は、22 の専門職団体監督機関（PBS）を通じた指導の一貫性と質の向上を図るため、2023 年 1 月に「監督機関向けソースブック」を更新した。これにより、弁護士や会計士等の専門家に対する指導体制を強化し、専門知識が意図的又は不注意にテロ資金供与に悪用されるリスクの低減を推進している。

- リスクベースのアプローチの徹底

  監督当局は、JMLIT 等のプラットフォームを活用し、犯罪の傾向や手口に関するインテリジェンスを民間と共有することで、各企業が自らのリスク評価に基づいた実効性のある対策を講じるよう促している。

②-3-2.NPO の規制、監督・アウトリーチ

英国政府及び規制当局は、NPO セクターがテロ資金供与に悪用されるリスクを低減するため、多層的な監督及びアウトリーチ活動を展開している。

- NPO 向けガイダンス及びツールキットの提供

  英国内の NPO 規制当局（CCEW 等）は、NPO とその受託者に対し、内部管理体

制の構築やリスク軽減に資する詳細なガイダンス及び「ツールキット」を公開している。これらのリソースを通じて、各団体におけるテロ資金供与リスクへの理解浸透を図っている。

- トライ・セクター・グループ（TSG）を通じた戦略的対話

  政府、金融セクター、及び人道支援団体の 3 者で構成される TSG を通じ、官民の緊密な対話を継続している。テロ対策法や経済制裁措置を遵守しつつ、紛争地域等への合法的な人道支援を円滑に継続するための具体的な指針として、「対テロ法の下での活動」等のガイダンスを発行し、実務的な支援を行っている。

- リスクの多様性に応じた重点的啓発

  NPO セクター全体のリスクは低いと評価されている一方で、セクター内の多様性により、個々の団体が直面するリスクの種類やレベルは異なる。特に、テロ組織が支配する地域や紛争地帯の近傍で活動する団体に対しては、活動の近接性に伴う著しく高いリスクを認識させるための重点的なアウトリーチが行われている。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

金融・士業以外の特定セクターにおいても、テロ資金供与に悪用される脆弱性を低減するための監督及びアウトリーチ活動が展開されている。

- 非公式資金移転（IVTS／ハワラ）に対するアウトリーチ

  税関当局（HMRC）は、資金移動業者（MSBs）及びハワラ等の非公式資金移転システム（IVTS）に対する監督及び指導を強化している。未登録の非公式業者に対する取締りを徹底する一方で、登録済みの業者に対してはコンプライアンス遵守の働きかけを行い、リスクの高い送金ルートの透明化を促進している。

- 教育セクター（学校・大学）への働きかけ

  留学生等が組織犯罪グループによってマネーミュール（資金の運び屋）として利用されるリスクが高まっていることを受け、警察及び関係当局は学校又は大学に対する啓発活動を実施している。学生が意図せずテロ資金供与等の犯罪に加担することを防ぐため、教育機関を通じた直接的なアウトリーチが継続的に行われている。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

英国の金融セクター及び特定非金融事業者・職業（DNFBPs）は、テロ資金供与のリスクを低減させるため、ガバナンスの強化、官民連携、及びテクノロジーの活用を通じた多角的な対策を講じている。

- 銀行

  リテール・バンキング業界は、JMLIT 傘下の「テロ資金調達官民脅威対策グループ（TFPPTG)」を通じ、英国政府、法執行機関、及び監督当局との協働を継続している。特に 2020 年以降、事業・コンプライアンスの監督や関連法令・規則の変更へ

の対応を統括する「責任担当者」を設置したことで、業界の対応能力が向上している。また、金融データの活用は、テロ資金犯罪に限定されないテロ関連事件での有罪判決の獲得においても重要な役割を果たしている。

一方で、ホールセール・バンキング業界は相対的にリスクが低いと評価されているものの、2025 年のフォローアップレビューにおいて、CDD やガバナンス体制の進捗が確認された。しかしながら、依然としてリスクが過小評価され、あるいは取引モニタリングの改善が必要な領域も存在する。

- 電子マネー（EMI）及び決済サービス（PSP）

一部の電子マネー事業者（EMI）及び決済サービス事業者（PSP）は、TFPPTG に参加しており、2025 年にはさらなる参加企業の増加が見込まれている。当該セクターについては、金融行動監視機構（FCA）による監督上の優先事項として金融犯罪対策が掲げられており、一部の企業ではシステム・管理体制の大幅な改善が確認されている。

- 暗号資産サービスプロバイダー

「官民暗号資産フォーラム」を通じて、法執行機関や政府、及び監督当局とノウハウを共有し、既存及び新興の暗号資産に対する理解を深めている。一部の企業は、ブロックチェーン分析ツールを独自に活用し、暗号資産の出所や違法活動との関連性を特定する能力を強化している。

- 士業（法律・会計）

信託・会社サービスプロバイダー（TCSP）に関連するテロ資金供与のリスクスコアが「低」から「中」へ上昇したことを受け、当該セクターには適切なリスク評価及び管理措置の適用が求められている。また、会計サービス提供者は、会社設立業務等がテロ行為者・組織へ資金を提供する団体に悪用されるリスクを認識し、監督当局のリスク評価を考慮した対応を行っている。

②-4-2.NPO の活動・対応

英国の NPO セクターは、テロ資金供与に悪用されるリスクを最小化するため、自主的なリスク評価の実施や内部管理体制の強化を継続している。

- テロ資金供与リスクの自己評価と特定

NPO セクター全体のリスク評価は「低い」とされているが、一部の NPO は自らの活動が高リスク地域や紛争地帯に近接していることにより、テロ資金供与に悪用される潜在的なリスクがあることを明確に認識し、個別的なリスク評価を行っている。

- 受託者（Trustees）の責任と内部管理

海外で支援活動を展開する多くの慈善団体において、受託者は自らの責任を認識し、強固な財務管理体制を構築している。資金源の透明性を確保し、不正な資金の混

入を防止するための厳格な特定プロセスが運用されている。

- デューデリジェンス及びパートナー審査

最終的な受益者を特定し、下流の協力パートナー（パートナー団体等）を審査するための広範なデューデリジェンス・システムが備えられている。多くの NPO 及びその提携先は、活動の安全性を担保しつつ、不適切な資金流用を阻止するために高度なセキュリティシステムを導入している。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

英国におけるテロ資金供与の脅威が顕在化する可能性は、全体的なテロ脅威レベルの高止まり、金融システムの利用実態、及び攻撃形態の変容等を踏まえると、極めて高い水準にあると評価される。

- 全体的な脅威レベル及び発生可能性

北アイルランド関連を除く英国のテロ脅威レベルは、2022 年 2 月以降「相当（Substantial）」に維持されており、これは「攻撃が発生する可能性が高い（an attack is likely）」状況を意味している。

- 思想別・セクター別の顕在化傾向

2020 年以降のテロ資金供与捜査の大部分を「イスラム過激主義」が占めており、次いで「極右テロ」が約 4 分の 1 を占めている。リテール・バンキングにおいては、膨大な顧客基盤及び製品・サービスの遍在性から、国内のテロ資金供与に関与する可能性は「極めて高い（high likelihood）」と評価されている。2020 年以降、対テロ警察（CTP）により銀行口座から約 190 万ポンドが没収されており、これは銀行システムがテロ資金供与に実際に、かつ継続的に利用されている証左である。

- 攻撃の「低コスト化」に伴う発生の常態化

近年のテロ攻撃は低コストかつ単純な手法で行われる傾向にあり、準備資金も少額であることから、日常的な経済活動に紛れて資金供与が発生する事態が常態化している。特に、主要な脅威である単独犯は、自身の給与や融資等の合法的な源泉を原資とするため、資金調達そのものは頻繁に発生しているものの、その探知は極めて困難である。

- 特定ルート及び新技術の悪用可能性

高リスク地域への送金や、ハワラ等の非公式送金システムにおいて、PKK 等の組織が数百万ポンド規模の資金を移動させる事案が継続的に発生している。これらの伝統的な手法に加え、暗号資産やクラウドファンディングを通じた資金提供の試行

が増加しており、特に海外テロ組織への小口送金における利用頻度が高まっている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

テロ資金供与の顕在化は、単なる経済犯罪の枠を超え、国家安全保障、社会の安定、及び国際的な金融秩序に対して深刻かつ多層的な被害をもたらす。英国政府は、テロ資金供与を「被害者のいない犯罪」ではなく、凶悪な行為の手段を提供するものであると位置づけている。

- 国家安全保障及び公衆の安全への直接的脅威

  テロ資金の流入は、危険なグループが攻撃を計画・実行することを容易にし、英国のコミュニティの安全と幸福を直接的に脅かす結果を招く。また、北アイルランド関連テロ等に見られる恐喝、密輸、及び詐欺等の資金獲得活動は、地域社会における国家の正当な権威を損ない、法の支配を形骸化させる。

- テロ組織の存続及び運営基盤の維持

  資金はテロ攻撃の準備費用のみならず、メンバーの生活費、組織の基盤維持、プロパガンダの拡散、及び過激化のための教育活動等に利用される。これによりテロ組織の存続・拡大が助長され、長期的な脅威が維持されることとなる。

- 経済的信頼、金融システムの完全性への損害及び国際的な制裁体制の実効性低下

  テロリストによる金融システムの悪用は、経済全体への信頼を損ない、英国の国際的な金融ハブとしてのレピュテーションに傷をつけることにつながる。さらに、専門的便宜供与者（美術品ディーラーや弁護士等）を介した資金洗浄や制裁回避が行われることで、国際的な対テロ制裁体制の有効性が損なわれ、世界的な安全保障の弱体化を招く恐れがある。

- 社会不安と過激思想の拡散

  オンラインゲームや SNS を通じた少額の資金提供（クラウドファンディング等）は、それ自体がプロパガンダの一部として機能し、若年層を含む一般市民の過激化を促進する影響を持つ。

（5）カナダ

カナダでは、財務省（Department of Finance Canada）が、カナダ金融取引・報告分析センター（FINTRAC)、王立カナダ騎馬警察（RCMP）及びカナダ保安情報局（CSIS）等の関係機関と協働してマネロン・テロ資金供与の危険度を分析し、その結果を公表している。

リスクの特定・評価においては、「脅威（Threats）」、「固有の脆弱性（Inherent Vulnerabilities)」及び「結果・影響（Consequences)」の 3 つの要素の関数としてリスクを捉えるアプローチを採用している。具体的には、テロ資金供与の「脅威アクター」が、経済セクターや金融商品が持つ「脆弱性」を悪用する「可能性」を評価し、それに社会や経済へもたらされる「結果」を重ね合わせることで、多角的に固有リスクを算出している。

「脅威」の評価においては、国連やカナダが懸念を抱くテロリストグループ及び外国人戦闘員による脅威を対象とし、以下の 6 つの基準に基づき分析が行われている。

- 洗練度：当局に探知されることなく、持続的、長期的かつ大規模なテロ資金供与活動を国内で実施するための知識、専門性及び全体的な洗練度
- 能力：国内でテロ資金供与活動を実施するためのネットワーク、リソース及び全体的な能力の規模
- 資金供与の範囲：脅威アクターが国内及び世界中に有している支持者や同調者のネットワークの広さ
- 推定資金調達額：国内におけるテロ資金供与活動の推定金額
- 手法の多様化：国内での資金の収集、集約、送金、使用に関連する手法の多様性と複雑さ
- 資金の疑わしい使途：国内外で調達された資金が、国内外のカナダの国益に反して使用されると疑われる程度

また、「固有の脆弱性」の評価においては、33 の経済セクター及び金融商品を対象として、テロ資金供与等に悪用されやすい特徴を以下の 5 つの基準から評価している。

- 固有の特性：セクターの経済的重要度、運営構造の複雑さ、他セクターとの統合度、並びに事業の範囲及びアクセスの容易さ
- 商品・サービスの性質：商品やサービスの性質と範囲、並びにそれらに関連する取引の量、速度及び頻度
- 顧客関係の性質：顧客関係が単発の取引ベースか継続的か、直接的か間接的か、及び高リスク顧客やビジネスへのばく露の程度
- 地理的範囲：高リスク管轄区域（国・地域）や懸念される場所へのばく露の程度
- 提供チャネルの性質：商品やサービスの提供が、どの程度の匿名性（非対面取引や第三者の利用等）及び複雑さ（複数の仲介者の介在等）を伴って行われるか

①脅威

①-1-1.テロ組織、テロリスト

カナダにおけるテロ組織・テロリストの脅威として、テロ組織及びテロリストの存在と活動が確認された。それぞれの活動実態と脅威の動向は以下の通りである。

- アルカイダ・コア及び系列グループ

  アフガニスタンを拠点とする中核組織に加え、アラビア半島のアルカイダやイスラム・マグレブ諸国のアルカイダなどのネットワークが活動している。主な資金調達方法には、身代金目的の誘拐、石油・ガスなどの支配地域の資産に対する課税、及び寄付を受け取るための慈善団体の利用が含まれる。ただし、カナダ国内における募金活動は限定的であり、その手法も単純なものに留まっている。

- アル・シャバブ

  ソマリアにおけるイスラム国家樹立を目指すアルカイダの公式支部である。同組織は、支配下にある企業やインフラ、家畜に対する課税をはじめ、国際送金、オンラインを通じた勧誘、慈善キャンペーンからの資金転用など、高度かつ多様な資金調達能力を維持している。

- アリアン・ストライク・フォース

  人種戦争の引き起こしを目指すネオナチ組織であり、化学兵器の製造や自爆テロ計画に関与したことが確認されている。

- アトムヴァッフェン・ディヴィジョン（Atomwaffen Division：AWD）

  米国で設立された国際的なネオナチ・テロ組織であり、社会崩壊を目指して人種・宗教グループに対する暴力を呼びかけている。また、武器の扱いや格闘訓練を行う「憎悪キャンプ（hate camps）」を開催している。

- ザ・ベース（The Base）

  社会崩壊と白人至上主義国家の設立を掲げるネオナチ組織である。テロ攻撃に関するマニュアルや爆弾製造方法を配布するとともに、武器及び軍事戦術の訓練キャンプを組織している。

- ブラッド＆オナー（B&H）及びコンバット 18（C18）

  武装部門である C18 を含む国際的なネオナチ・ネットワークであり、殺人や爆撃事件を実行している。

- ISIL

  超国家的なイスラム国家樹立を目指すジハード主義グループである。支配地域と収入源は減少したものの、依然として国外の同調者からの資金提供を受けており、カナダ国内においては過激派渡航者への支援活動を行っている。

- ハマス

  ガザ及び西岸地区を拠点とし、慈善団体、学校、クリニックなどを含む広範な「ダワ（Dawa）」ネットワークを通じて高度な資金調達を行っている。ただし、カナダ国

内におけるネットワークは小規模であり、組織化の程度も以前と比較して低下している。

- ヒズボラ

  レバノンを拠点とし、イランから多大な支援を受ける一方で、広範な犯罪的資金調達能力を有している。カナダ国内には確立された募金ネットワークが存在し、慈善団体や非営利団体を通じた多様な手法によって資金を集めている。

- インド国内の独立国家樹立を支持する過激派グループ

  ババール・カルサ・インターナショナルや国際シーク青年連盟などがこれに含まれる。カナダを含む数カ国で資金調達を行っている疑いがあるものの、カナダ国内におけるネットワークは縮小傾向にある。

- ロシア帝国運動（Russian Imperial Movement：RIM）

  ロシアを拠点とする民族主義グループであり、欧米のネオナチ組織に対して準軍事訓練を提供しているほか、爆弾テロ計画の支援や紛争地域への戦闘員派遣を行っている。

- スリー・パーセンターズ

  分散型の反政府民兵組織であり、米連邦政府のビルやイスラム教徒のコミュニティを標的とした爆破計画に関与している。

- プラウド・ボーイズ

  政治的暴力を振るうネオファシスト組織であり、2021 年 1 月に発生した米連邦議会議事堂襲撃事件において中心的な役割を果たした。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

カナダにおけるテロ資金供与の脅威として、特定のテロ組織やテロリスト本人だけでなく、これらを支援し、あるいは同調する以下の個人や集団の活動が確認された。

- カナダ人過激派渡航者（Canadian Extremist Travelers: CETs）

  海外でのテロ活動（戦闘、訓練、資金調達等）に参加する、又はそれを試みるカナダにゆかりのある個人である。帰国後は、国内において新たな志願者の勧誘、資金調達、あるいはテロ攻撃の計画や実行の主体となるリスクが指摘されている。また、海外で拘束された CET の釈放資金を募る活動が行われていることも報告されている。

- 単独犯（Lone Actors）

  特定のテロ組織のメンバーではないものの、オンライン上の過激なプロパガンダに同調し、独力で攻撃を準備及び実行する個人である。主に雇用収入や家族からの送金等の合法的な個人資産を、武器購入や装備の調達に使用する傾向がある。さらに、自らの活動にとどまらず、他の同調者へ資金を転送する事例も確認されている。

- ディアスポラ内の個人・グループ

  カナダの多文化社会における固有の脆弱性を突かれ、テロ組織による資金搾取の

対象となる可能性のあるコミュニティである。母国の紛争地域に残された家族の安全を確保するための「人道支援」や「家族送金」という名目で、意図せず、あるいは脅迫を受けた結果として、テロ組織へ資金を流出させる主体が含まれている。

- 過激化した個人

  オンラインのプロパガンダや SNS を通じたリクルート活動の影響により過激化した個人である。テロ組織の思想に強く同調しており、自ら戦闘員として渡航することを企図したり、組織を財政的に支えたりする意思を持つ者がこれに該当する。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

カナダにおけるテロ資金供与の主体は、テロ活動を維持・実行するために、以下のような多様な手法を用いて資金を獲得していることが確認された。

- 合法的収益（個人資金）

  単独犯やカナダ人過激派渡航者は、主に自身の雇用収入や家族からの送金といった合法的な個人資産を利用している。これらの資金は、攻撃の準備、武器や装備の購入、及び渡航費に充てられている。

- 寄付、募金、及びクラウドファンディング

  戸別訪問、寄付箱の設置、慈善イベントの開催といった対面での活動に加え、SNS やウェブサイトを通じたオンラインのクラウドファンディングが資金調達に利用されている。ISIL の同調者をはじめ、ヒズボラ、アル・シャバブ、及び IMVE（イデオロギーに裏打ちされた暴力的な過激主義）グループが、世界的な支援者ネットワークを通じて資金を収集している実態が確認されている。

- 国家による直接支援

  ヒズボラなどの一部のテロ組織は、イラン政府などの国家から多大な財政的、軍事的、及びロジスティクス上の支援を直接的に受けている。

- 支配地域における資源搾取、課税、及び徴収

  テロ組織は国外の支配地域において、組織的な資金獲得を行っている。具体的には、アルカイダによる石油・ガス等の支配地域資産への課税や、アル・シャバブによる地元企業、交通インフラ、日用品への課税、及び一般市民からの家畜の徴収などが挙げられる。

- 身代金目的の誘拐

  アルカイダの中核及びその関連組織（AQAP、AQIM 等）にとって、身代金目的の誘拐は依然として主要な資金源の一つとして維持されている。

- 犯罪活動による収益

  テロ資金供与の主体は、自動車盗難や各種詐欺（クレジットカード詐欺、福祉詐欺、学生ローン詐欺、ビザ・パスポート詐欺等）を通じて不法な利益を生成している。さらに、クレジットカードのバストアウト（計画的倒産）スキームや、不正なローンを

通じた資金調達も確認されている。

- 人道支援資金及び組織活動の流用（NPO/慈善団体）

  貧困救済、教育、宗教振興などの人道目的で集められた資金が、組織の内部関係者や海外のパートナーを通じてテロ活動へ転用されるケースが存在する。これには、ハマスの「ダワ」ネットワークや、アル・シャバブ、ヒズボラに同情的な団体が関与していることが指摘されている。

- 会費、物販、及び事業収益との混蔵

  組織化された過激派グループにおいては、会費の徴収やグッズ販売による資金調達が行われている。また、テロ活動に関与する個人が支配する合法的なビジネスの収益に犯罪収益を混同させることで、資金源を隠蔽しつつ獲得する手法が用いられている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

カナダにおけるテロ資金供与の主体は、獲得した資金や物資をテロ組織等へ提供するため、以下のような多様な移転手法を悪用していることが確認されている。

- 銀行を通じた国際送金

  海外のテロ組織や個人に資金を送るための主要な移転手法の一つである。個人又は法人の銀行口座を利用し、テロ活動に関連する高リスク地域へ国際送金が行われる。

- 国内送金（Domestic Wires）

  カナダ国内で資金を移動させたり、収集した寄付金（現金やウェブベース）を海外送金前に一つの口座に集約（集計）したりするために使用される。

- 資金移動業者（MSB）による海外送金

  銀行と並んで頻繁に利用される資金移転の手段である。特に世界展開する大手 MSB や、特定の国・地域への送金に特化した小規模 MSB が、高リスク地域への送金手段として使用される。

- 非公式な価値移転システム（IVTS）

  従来の銀行システムの外側で行われる非公式なネットワークである。小規模な独立系 MSB の運営者が、海外の IVTS 運営者とつながりを持ち、これを通じて資金を移動させることがある。

- 現金密輸及び現金運び屋

  国境を越えて物理的な現金を密輸する、あるいは個人が「運び屋」として海外へ現金を運搬する手法である。当局の検知を避けるための主要な海外移転手法の一つとして位置づけられている。

- 暗号資産

  ビットコイン等の暗号資産が利用される。特に匿名性を高める「プライバシーコイ

ン」は、資金移動の秘匿化を目的とするテロ資金供与主体にとって魅力的であるとされている。

- E メール送金

  送金者と受取人の間での資金移転に使用される。特に IMVE（イデオロギーに裏打ちされた暴力的な過激主義）の単独犯などが、資金を送受信する際によく見られる手法である。

- 物資・商品の直接提供

  電子機器などの高価値商品を個人が直接懸念地域へ持ち込み、現地で売却してその代金をテロ活動に充てる、あるいは商品を直接テロ組織に届ける手法である。

- 貿易ベースのスキーム

  ビジネス口座を用いた輸出入取引を装い、国境を越えて資金や物資を移動させる手法である。

- 支払処理会社

  MVE（暴力的な過激主義）ネットワークに関連する個人が、国際的なネットワークの各拠点へ資金を送る際に利用されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

カナダにおいて、テロ資金供与の主体が資金獲得やテロ組織への資金提供を行うにあたり、以下のような制度、基盤、及びプラットフォームがインフラとして悪用されていることが確認されている。

- 法人（フロント会社、シェル会社、民間企業）

  民間企業、特に非公開会社は、テロ組織や個人への資金移動の「フロント（隠れ蓑）」として悪用される。これらは正当なビジネスを装ってテロ資金を移動させたり、合法的な事業収益と不法な資金を混同させたりするために利用される。また、貿易ベースのスキームにおいて、高リスク地域への送金や物資提供の基盤となる。

- 非営利団体（NPO）及び登録慈善団体

  慈善団体は、その社会的な信頼、多額の資金へのアクセス、及び現金中心の性質から、テロ資金供与に悪用される脆弱な基盤となっている。具体的な悪用形態には、内部関係者による資金の流用、テロ組織による組織の乗っ取り、偽の慈善活動を掲げた「偽装団体」の設立などが含まれる。

- ソーシャルメディア及びオンラインプラットフォーム

  ソーシャルメディアが、資金調達の呼びかけや、特定の個人・大義への支援を募る基盤として利用されている。これらはウェブベースの寄付を集めるための強力なプラットフォームとして機能する。

- クラウドファンディング・プラットフォーム

インターネットを通じたクラウドファンディングは、特に IMVE（イデオロギーに裏打ちされた暴力的な過激主義）に関与する個人や組織によって、多数の支持者から小口資金を集めるための重要な基盤として利用されている。政府は、このプラットフォームの悪用を新たなリスクとして特定し、監視を強めている。

- 明示信託

  信託が持つ「実質的支配者」を隠蔽できる性質が悪用される。カナダ国内から海外、あるいは海外から国内へのテロ資金のフローを促進するための複雑な法的構造として利用されるリスクがある。

- サイバー犯罪・詐欺エコシステム

  クレジットカード詐欺、福祉詐欺、学生ローン詐欺、ビザ・パスポート詐欺などが、テロ資金を生成するための犯罪インフラとして機能している。特にクレジットカードのバストアウト（計画的倒産）スキームやスキミングが、テロ活動の資金源確保のために悪用されている。

- ダークウェブ及びオンラインマーケットプレイス

  アルファベイ（AlphaBay）やハンサ（Hansa）などのダークウェブ上のマーケットプレイスは、テロ組織や犯罪者が暗号資産を用いて、武器、偽造文書、マルウェア、毒劇物などのテロ活動に必要な物資を調達するための基盤（エコシステム）となっていた。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

カナダにおいて、テロ資金供与の脆弱性を生み出している国・地域に固有の文化的背景、地理的条件、及び社会・経済・産業構造として、以下の要素が確認されている。

- テロリスクが高い地域との地理的、経済的、文化・社会的な近接性

  カナダは多文化・多民族国家であり、多くの住民が海外に家族やコミュニティの強い絆を有している。しかしながら、特定のディアスポラ（離散民族集団）がテロ支援目的で搾取される可能性があり、母国の家族の安全確保や人道支援という名目で、意図せず、あるいは脅迫を受けてテロ組織に資金を送付してしまう脆弱性が存在する。具体的には、アフガニスタン、レバノン、パレスチナ自治区、ソマリア、シリア、イエメンなど、テロ組織が活動する地域が資金の主な送付先として特定されている。

- 政治的安定性と民主主義的価値観

  カナダは安定した民主主義国家であり、強固な公的機関と司法制度を有している。一方で、開かれた民主主義社会において保証されている自由や、被告人を保護するための法的・手続き的な防護策自体が、テロ資金供与主体によって悪用される可能性のある固有の脆弱性として認識されている。

- 地理的広大さと国境管理の強度

カナダは世界第 2 位の広大な国土と 20 万 km 以上の海岸線を有し、アメリカとは世界最長の国境（約 8,800km）を共有している。この地理的な広大さゆえに、陸路、空路、海路を用いた国境を越える不法な活動（バルク現金の密輸や物資の移動など）を網羅的に検知・捕捉することは、極めて困難な挑戦となっている。

- 現金依存度と地下経済

  カナダにおける地下経済活動は GDP の約 2.7%（2018 年時点で 612 億ドル）に達しており、隠蔽された活動の土壌となっている。カジノ、NPO、ホワイトラベル ATM[6] などの現金集約型セクターは、テロ資金の配置段階において依然として脆弱である。特に、装甲車会社による現金管理サービスは、銀行システム外で多額の現金をプール・移動させるため、資金の源泉特定を困難にするリスクが指摘されている。

- 国際金融・貿易における立ち位置

  カナダは世界最大級の成熟した金融システムを有するとともに、GDP の 65%以上を占める高度に発達した国際貿易システムを擁している。この貿易の活発さと、アメリカや中国等の主要経済圏との強固な結びつきは、貿易ベースのテロ資金供与（TB-TF）スキームを通じて不法な資金や物資を隠蔽・移動させる機会をテロ資金供与主体に提供している。

- 規制の適用が限定的な分野・取引の存在

  テロ資金供与防止法（PCMLTFA）の適用外、あるいは適用が不十分な分野が脆弱性として残存している。具体的には、非公開法人や特定の信託、規制外の住宅ローン貸付人、及び過去の裁判判決により法規制が機能していない状態にある弁護士等の法的専門職が挙げられる。

②-2-1.テロ資金供与を防止するための法的枠組み

カナダにおいて、テロ資金供与を防止・抑止するための法的枠組み及び制度的基盤として、以下の体制が整備されている。

- テロ資金供与対策の主要な法的枠組み

  カナダのテロ資金供与対策（ATF）の枠組みは、主に犯罪収益（マネー・ローンダリング）及びテロ資金供与防止法（PCMLTFA）と刑法によって規定されている。PCMLTFA は、特定の金融機関や事業者に対して、顧客確認、記録保存、及び遵守プログラムの策定を義務付けている。

- 疑わしい取引報告と情報収集制度

  PCMLTFA は、疑わしい金融取引、多額のクロスボーダー現金移動、及び特定の規定された取引に関する義務的な報告システムを構築している。報告主体はテロ資

[6] 銀行法の対象となる金融機関ではなく、通常、銀行・信用組合業界外の個人や中小企業によって運営されている ATM

金供与リスクを特定し、強化された顧客デューデリジェンス（EDD）や取引の継続的監視を通じて、当該リスクを軽減する措置を講じる義務を負っている。

- 法執行機関の体制と財務捜査能力

  王立カナダ騎馬警察（RCMP）、カナダ安全保障情報局（CSIS）、及びカナダ国境サービス庁（CBSA）が、カナダ金融取引報告分析センター（FINTRAC）からの情報提供を受け、テロ資金供与やその他の重大犯罪に関する財務捜査を実施している。また、連邦検察局（PPSC）は、これらの金融犯罪を法の及ぶ最大限の範囲で訴追する役割を担っている。

- テロリスト資産のリスト化と凍結制度

  刑法及び国連テロ防止決議の履行規則に基づき、テロリストの資産を凍結するための強固なリスト化のプロセスが存在している。このプロセスは公共安全省及びグローバル連携省が主導しており、現在 113 のテロ関連団体・個人がリスト化されている。政府が訴追した刑事事件において差し押さえ・没収された資産の管理については、公共サービス・調達省（PSPC）が担っている。

- 制度の監視・監査及び国際的な立ち位置

  カナダ議会は、法律の規定により、5 年ごとに PCMLTFA 及び対策体制全体の包括的な見直しを行うことが義務付けられている。さらにカナダは、FATF（金融活動作業部会）の創設メンバーとして、国際的な FATF 基準の策定に積極的に関与しているほか、グローバル連携省（GAC）主導のもとで他国への能力構築支援も行っている。

  なお、高額現金の携帯輸入等に関する具体的な税関規制（申告義務のある金額の基準や手続き等）については、本調査対象文献における特段の記載は確認されていない。

②-3-1.金融当局等の監督・アウトリーチ

カナダにおいて、テロ資金供与対策を実効的なものとするため、金融当局等による監督及びアウトリーチ活動が以下の通り実施されている。

- FINTRAC の監督権限と行政罰（AMPs）による法執行

  カナダの金融情報ユニット（FIU）兼規制当局である FINTRAC（カナダ金融取引報告分析センター）は、PCMLTFA に基づき、報告主体に課される本人確認、記録保存、及び報告といった義務の遵守状況を監督している。具体的には、リスクベースのアプローチによる検査を実施し、不遵守が疑われる場合には詳細な精査を行っている。また、報告主体が義務を遵守していない場合には行政通貨罰を課す権限を有しており、この措置は単なる制裁としてだけでなく、セクター全体におけるコンプライアンス文化の定着を促す手段として機能している。

- OSFI による連邦金融機関の監督

金融機関監督庁（OSFI）は、連邦規制下にある銀行、保険会社、及び信託会社に対して監督を行っている。これらの機関に対する AML/ATF コントロールの有効性については、健全性規制の枠組みの中で継続的に評価及び監督が実施されている。

- ガイダンス・指標（Red Flags）の提供を通じたアウトリーチ

  FINTRAC は、民間部門におけるテロ資金供与の検知及び報告能力を向上させるため、報告主体に対する積極的なアウトリーチを行っている。具体的には、法解釈や指針に加え、テロ資金供与の指標（Red Flags）などの実務的なガイダンス資料を定期的に発行し、更新を続けている。

- 関係当局への金融インテリジェンス開示

  FINTRAC は、収集した金融情報を分析し、それがテロ資金供与や国家安全保障に対する脅威に関連すると判断した場合、RCMP（王立カナダ騎馬警察）、CSIS（カナダ安全保障情報局）、CBSA（カナダ国境サービス庁）等の関係法執行機関及び情報機関に対して情報開示を行っている。

- 官民連携を通じた情報交換

  特定の重大犯罪や脅威（人身売買、スキャム、テロ資金等）に対処するため、官民連携プロジェクトが推進されている。当局が民間部門と最新の脅威情報を共有することにより、報告主体からのより質の高い疑わしい取引報告（STR）の提供や、テロ資金供与活動の早期検知が実現されている。

②-3-2.NPO の規制、監督・アウトリーチ

カナダにおいて、非営利団体（NPO）や慈善団体がテロ資金供与に悪用されるリスクを軽減するため、規制当局による以下の監督及びアウトリーチ活動が実施されている。

- NPO に関連する法規制及び税務当局の役割

  カナダ歳入庁（CRA）は、所得税法に基づき、慈善団体の登録及びその管理・運営が法的に適切な目的（貧困救済、教育、宗教振興等）に合致しているかを監視している。特に、テロ資金供与のリスクが疑われる慈善団体を検知し、テロ活動への悪用を未然に防止するための法的措置を講じる中核的な役割を担っている。

- NPO 規制当局による監督・監査活動

  CRA は、リスクベース・アプローチに基づく監督を実施しており、とりわけ紛争地域やテロ組織が活動する高リスク地域で活動している慈善団体、あるいはそれらに関連する個人・団体と繋がりのある慈善団体に対して、重点的な監査及び監督を行っている。

- 当局の権限、専門性、及び関連当局との情報共有

  CRA は、王立カナダ騎馬警察（RCMP）や FINTRAC 等の他の関係機関と密接に連携し、テロ資金供与の疑いがある慈善活動に対する財務捜査や分析を実施している。また、疑わしい事実が確認された場合には、慈善団体としての登録取り消しを含

む厳格な行政処分を執行する権限を有している。

- アウトリーチ及びガイダンスの提供

  規制当局は、報告主体や一般公衆に対して、テロ資金供与の手法及び最新のトレンドに関する報告書並びにガイダンスを提供している。これらの情報提供を通じて、NPO を含むセクターが自らの直面するリスクを適切に評価し、必要な管理措置を講じることができるよう支援を行っている。

- 国際的な能力構築への貢献

  カナダは国内の対策にとどまらず、グローバル連携省（GAC）が主導するプログラムを通じ、テロ資金供与対策の法的・制度的枠組みが脆弱な他国に対して、専門知識の共有や監督能力向上のための資金援助を行うなど、国際的な能力構築にも貢献している。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

カナダにおいて、金融機関や NPO 以外のセクターにおけるテロ資金供与リスクに対応するため、関係当局等による以下の監督及びアウトリーチ活動が実施されている。

- 非公式な資金移動システム（IVTS）への対応

  非公式なネットワークは、伝統的な銀行システムの外側で運営されているが、カナダではこれらの一部が「代替送金 MSB」や「小規模独立系 MSB」として規制対象に含まれている。当局は、これらの業者が高リスク地域への資金移動に悪用される脆弱性を深く認識しており、継続的な監視を行っている。

- クラウドファンディング・プラットフォームへの監督拡大

  カナダ政府は、クラウドファンディング・プラットフォームの悪用を「新たなリスク」として特定している。この脆弱性に対応するため、2022 年 4 月に同プラットフォーム及び関連する決済サービスプロバイダーをテロ資金供与防止法（PCMLTFA）の規制対象に新たに追加する制度改正を行った。

- 貿易・輸出入セクター（貿易ベースの TF 対策）

  カナダ国境サービス庁（CBSA）等の当局は、輸出入業者、貨物運送業者、及び通関業者が貿易ベースのテロ資金供与（TB-TF）に悪用されるリスクを評価している。さらに、2019 年予算において、貿易ベースのマネー・ローンダリングや貿易詐欺に対処するための能力構築及び専門知識の強化に向けて資金が投じられた。

- 天然資源（違法漁業）セクターの評価

  2015 年版以降のリスク評価において、新たな脅威として「違法漁業」が評価対象に加えられた。カナダ環境・気候変動省や水産海洋省が中心となり、これら天然資源の不法な搾取が犯罪収益の生成や組織犯罪、さらにはテロリズムに関連する可能性について、継続的な監視及び評価に関与している。

- 当局によるリスクベース・アウトリーチ

FINTRAC は、既存の報告主体のみならず、これまで規制の適用が限定的であったセクターに対しても、固有のリスク情報を統合したガイダンス資料を継続的に提供している。これにより、カナダ経済のセクター全体において、テロ資金供与リスクを特定し、それを軽減するための管理措置の実効性を高めることを目指している。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

- 預金取扱金融機関（銀行）

  預金取扱金融機関（国内銀行：D-SIBs）の固有の脆弱性評価は、「非常に高い（Very High）」と評価されている。連邦規制下の銀行等に対しては、金融機関監督庁（OSFI）が AML/ATF の遵守管理フレームワークの適切性を監督しており、ガバナンスの欠幼が機関の健全性に与える影響を継続的に評価している。

- 資金移動業者

  資金移動業者（代替送金 MSB）の固有の脆弱性評価は、「非常に高い（Very High）」と評価されている。非公式な価値移転システム（IVTS）などの代替送金業者は、伝統的な銀行システムの外側で運営されており、テロ組織が活動する高リスク地域への送金を可能にする。これらは小規模で目立たないビジネスであるため、テロ資金の送信や集約に悪用される極めて高いリスクを有している。

- 暗号資産

  暗号資産セクターの固有の脆弱性評価は、「高い（High）」と評価されている。ビットコインや匿名性を高める「プライバシーコイン」がテロ資金の移動に使用されるリスクがある。2021 年 6 月の規制改正により、暗号資産を扱う業者は顧客管理や記録保持が義務付けられたが、依然としてピアツーピア（P2P）等の非規制チャンネルを介した国境を越えた迅速な資金移動に関する脆弱性が指摘されている。電子決済手段（ステーブルコイン）調査対象文献において、電子決済手段やステーブルコインに関する特段の記載は確認されない。

- 前払式支払手段(プリペイド型決済サービス)

  オープンループ・プリペイドカードの固有の脆弱性評価は、「中程度（Medium）」と評価されている。国内外で高い流動性を持ち、匿名での現金チャージが可能な場合があることから、他国でロードしたカードを用いてカナダ国内で現金を引き出すなどのテロ資金移動に悪用されるリスクがある。

- クレジットカード

  本項目における固有の脆弱性評価に関する明記はない。ただし、テロ資金獲得の脅威の文脈において、クレジットカードのバストアウト（計画的倒産）スキームやクレジットカード詐欺等の犯罪活動が、テロ活動の資金源確保のために悪用されている事実が確認されている。

- 保険

ML/TF の脆弱性として、「高い（High）」と評価されている。規制下の生命保険会社は、銀行と同様に OSFI による AML/ATF の健全性・ガバナンス監督の対象となっている。

- 証券

ML/TF の脆弱性として、証券業者（ディーラー）の固有の脆弱性評価は、「高い（High）」と評価されている。主に ML のレイヤリング（資金洗浄の層化）段階での利用が懸念されている。

- 信託

信託・ローン会社の固有の脆弱性評価は、「高い（High）」と評価されている。連邦規制下の信託会社は OSFI による監督対象である一方、テロ資金供与防止法の適用が限定的な特定の信託が存在し、脆弱性として残っている。また、明示信託（Express Trusts）は、信託の実質的支配者を隠蔽できる性質が悪用され、テロ資金のフローを促進するための複雑な法的構造として利用されるリスクがある。

- 金銭貸付

ML/TF の脆弱性として、「高い（High）」と評価されている。特に「規制外住宅ローン貸付業者」（住宅ローン専業会社（MFC）、モーゲージ投資会社（MIC）、シンジケートローン、民間法人や個人などの非規制の貸手を含む）のテロ資金供与に関する脆弱性については、住宅ローンなどの融資が、テロ活動の資金を調達（アクセス）するための手段として利用されるリスクや、業者が借り手から犯罪収益である資金を返済として受け取るリスク、意図的か無意識的かを問わず、業者側が犯罪収益を用いて融資（資金提供）を行ってしまうリスクが指摘されている。

- 不動産

不動産業の固有の脆弱性評価は、「高い（High）」と評価されている。他の報告主体と同様に、PCMLTFA に基づく顧客確認等の共通義務が課されている。

- 宝石・貴金属

貴金属・宝石商の固有の脆弱性評価は、「高い（High）」と評価されている。他の報告主体と同様に、PCMLTFA に基づく顧客確認等の共通義務が課されている。

- 法律・会計関係サービス（TCSP）

弁護士等の法律専門家の固有の脆弱性評価は、「高い（High）」と評価されている。信託口座の開設、法人や法的信託の設立、不動産や証券などの高額取引の実行に関する専門知識を有しており、これらが（意図的か否かにかかわらず）悪用されるリスクがある。なお、裁判判決により法規制が機能していない状態[7]にある弁護士等の法的専門職の存在が挙げられている。

[7] 過去の裁判所の判決及び関連する差止命令の結果として、カナダの「犯罪収益移転防止及びテロ資金供与対策法（PCMLTFA）」の中で法律専門職に適用される規定が機能していない状態となっている。

また、会計や会社サービス事業者（Company Service Providers: CSP）の固有の脆弱性評価は、いずれも「中程度（Medium）」と評価されている。会計士に関しては、財務や税務のアドバイス、法人や信託の設立支援などの専門知識を提供しており、富裕層、PEP、現金集約型のビジネスなどを顧客に持つことがリスクとされている。また、会社サービス事業者に関しては、国内及びオフショアの法人設立サービスを提供しており、違法なスキームの一部として法人を迅速に設立することを容易にするリスクがある。なお、会社サービス事業者が設立に関与する「企業」自体の脆弱性は、テロ組織への資金移動のフロント（隠れ蓑）として利用される可能性を踏まえ、「極めて高い（Very High）」と評価されている。

- カジノ

  カジノの固有の脆弱性評価は、「高い（High）」と評価されている。地下経済の存在や現金への依存度が高く、カジノ等の現金集約型セクターは、テロ資金の配置段階において依然として脆弱であると指摘されている。他の報告主体と同様に、PCMLTFAに基づく顧客確認等の共通義務が課されている。

②-4-2.NPO の活動・対応

カナダにおいて、非営利団体（NPO）や慈善団体がテロ資金供与に悪用される固有の脆弱性及び活動・対応状況について、以下の事実が確認されている。

- NPO セクターのテロ資金供与リスク評価

  カナダにおける NPO セクター（特に登録慈善団体）は、テロ資金供与に対して「高い（High）」固有の脆弱性を有すると評価されている。この要因として、セクターの規模が大きく、多額の資金へのアクセスが可能であること、及び現金集約的な性質を持つことが挙げられている。特にテロ資金供与の観点から最大の懸念とされているのは、テロの脅威が活発な地域や紛争地において活動する、あるいはテロ運動が支持を求めて標的とするコミュニティ内で活動する「サービス提供型」の NPO（教育、社会福祉、医療、開発、住宅供給等）である。

- テロ資金供与の悪用手法

  NPO を悪用する主な手法として、以下の 3 点が確認されている。

  - 流用：NPO セクターにおいて最も一般的に観察される手法である。災害救助、貧困救済、教育、宗教振興などの人道プログラムのために集められた資金が、組織の内部関係者や海外のパートナーを通じて、テロ活動へと転用されるリスクが存在する。
  - テロ組織による組織の浸透・乗っ取り：テロ組織に関連する個人が、かつては合法であった組織の理事会や財務部門を管理・掌握し、テロ支援のために当該組織を利用・悪用するリスクが指摘されている。

- プログラムの悪用と勧誘支援：NPO が資金提供を行う人道プログラムが、物資等の配送段階においてテロ組織を支援するように操作されるケースや、NPO の施設及び活動自体がテロの勧誘活動を促進・支援する環境として悪用されるケースが存在する。

● セクター内の脆弱性要因

個別の団体における脆弱性要因として、脆弱なガバナンス構造や不透明な資金管理が、資金源の特定を困難にする要因となっている。NPO が十分なデューデリジェンスを実施しなかったり、パートナー組織や第三者（エージェント）へ送金した後にリソースの最終使途を適切に管理しなかったりする場合、資金がテロ支援に転用されるリスクが高まると指摘されている。

②-4-3.その他セクターの活動・対応

カナダにおいて、金融機関や DNFBPs、NPO 以外のその他のセクターにおいても、テロ資金供与に対する固有の脆弱性が評価されており、各セクターにおける活動・対応状況やリスクの性質について以下の事実が確認されている。

● 輸入・輸出会社（貿易ベースのテロ資金供与）

輸入・輸出会社の固有の脆弱性評価は「高い（High）」と評価されている。これらの事業者は、貿易ベースのテロ資金供与（TB-TF）のフロントとして悪用される脆弱性を有している。具体的には、不透明な取引が可能な経済特区（SEZ）を利用したり、商品の虚偽記載や多重請求等の手法を通じて、テロ組織が活動する高リスク地域へ資金や物資を移転させるリスクが指摘されている。

● 非規制の住宅ローン貸付

非規制の住宅ローン貸付人の固有の脆弱性評価は「高い（High）」と評価されている。住宅ローンという金融形態を介して、テロ活動資金へのアクセスや、資金のレイヤリング（資金洗浄の段階）に悪用される可能性がある。特に、シェルカンパニーやノミニー（名義人）構造を用いた複雑なスキームを通じて、テロ資金の源泉を秘匿するリスクが指摘されている。

● 装甲車会社

装甲車会社の固有の脆弱性評価は「高い（High）」と評価されている。これらの事業者は、銀行システム外での多額の現金管理を行い、中央の法人口座へのプーリングを通じて現金集約型ビジネスからの資金移動を担うため、テロ資金の源泉特定を困難にするリスクを有している。

● ホワイトラベル ATM

ホワイトラベル ATM の固有の脆弱性評価は「高い（High）」と評価されている。これらは銀行以外の独立系業者によって運営されており、監視の不十分な場所に設置されることが多い。そのため、不法な現金の投入や、盗難カードを用いた現金引き

出しといった、資金洗浄及びテロ資金供与における「配置（Placement）」段階の脆弱性を持つと分析されている。

- 貨物運送業者・通関業者

  貨物運送業者及び通関業者の固有の脆弱性評価は「中程度（Medium）」と評価されている。これらの業者は直接的に資金を扱うわけではないものの、複雑な物流網に関する専門知識を悪用し、虚偽の説明を付与することによってテロ資金に関連する物資や価値の移動を円滑化させる「隠れた仲介者」として機能するリスクが認められている。

- クラウドファンディング・プラットフォーム

  クラウドファンディング・プラットフォームは、「新たなリスク」として特定されており、2022 年 4 月に規制対象に追加された。特に、IMVE（イデオロギーに裏打ちされた暴力的な過激主義）に関与する個人や組織が、オンラインを通じて多数の支持者から小口資金を集めるための重要な基盤として悪用している実態が確認されている。

- 天然資源（違法漁業）

  天然資源（違法漁業）セクターの脅威評価は「中程度（Medium）」とされており、2015 年版以降の新たな脅威として位置づけられている。違法漁業によって得られた収益がテロ組織への資金提供につながる可能性について、関係当局が監視の対象としている。また、これらの活動は組織的かつ多国籍な性格を持つことがある点が特徴として挙げられている。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

カナダ国内には、様々なテロ組織に対して資金を調達し、収集し、及び送金している疑いのあるネットワークが存在しているが、カナダにおける既存の制度の強みもあり、テロ組織が強固な基盤を築いている世界の他の地域と比較すると、テロ資金供与の脅威は顕著ではないと評価されている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

カナダにおいて、テロ資金供与の脅威が顕在化（マネー・ローンダリングの結果も含む）した場合、社会、経済、及び政治の広範な領域に対して甚大かつ多面的な影響を及ぼすことが評価されている。具体的に生じ得る影響や被害は以下の通りである。

- テロ活動の維持と直接的被害

  テロ資金供与は、国内外におけるテロリストの活動を根本的に支え、持続させる機能を持つ。その直接的な結果として、カナダ国内又は海外においてテロ攻撃が引き起こされ、人命の喪失や甚大な物理的破壊をもたらす可能性がある。

● 社会的な影響

社会への波及効果として、犯罪活動の増加や、犯罪者への社会的・経済的権力の集中が懸念される。さらに、精神的トラウマから身体的暴力に至るまでの被害の拡大、収監率の上昇、及び公的・民間機関に対する社会的な信頼の低下が生じるリスクが指摘されている。

● 経済的な影響

経済面においては、消費、貯蓄、投資などに歪みが生じ、経済成長に対して悪影響を及ぼす。これに伴い、国内外からの投資の減少、不法な資本流入の増加と正当な資本流出の増加が引き起こされる。また、民間セクターにおける不公正な競争や市場価格の歪み、銀行の流動性や健全性の問題（金融システムの完全性への悪影響）が生じ、さらにはカナダ経済全体及び特定セクター（特に金融セクター）に対する評判の低下を招く可能性がある。

● 政治的な影響

政治・制度的側面への影響として、公的機関及び「法の支配（Rule of law）」の浸食が挙げられる。国が不法な資金移動の「安全な避難所（Safe haven）」と見なされることで、さらなる犯罪を誘引する危険性が増大する。加えて、国際社会におけるカナダの信頼と影響力の喪失、地下経済化による政府収入の減少、さらにはテロ資金供与に対処する政府の能力に対する国民の否定的評価が生じることが指摘されている。

（6）ドイツ

ドイツのリスク評価は、主管機関である財務省のもと、35 の連邦及び州機関が参加している。4 つの作業部会を設置し、14 カ月にわたって作業を実施した。既存の「分野別リスク評価」や、欧州委員会による「超国家的リスク評価」を統合して評価している。

分野別リスク評価の手法は以下の通り。

- 世界銀行が開発した「国家リスク評価実施手法」を採用しつつ、当局の定性的情報の活用を強化し、国内要件に適合するよう更新。
- FATF 勧告 1 に基づくリスクベース・アプローチの要件に準拠し、ML/TF それぞれに対する脅威と脆弱性から構成される。
- 脅威とは、犯罪形態やテロ活動資金調達に関連して、危害を引き起こす一定の潜在的可能性又は可能性を有する活動を指す。
- 脆弱性とは、ML/TF の防止・対策における現行の防衛メカニズムにおける欠陥又は不明確性を意味する。

①脅威

テロ組織がドイツで資金調達活動を行う脅威は「中程度から高い」と評価されている。主な主体は以下の通りである。

①-1-1.テロ組織、テロリスト

- イスラム過激派組織（IS、アルカイダ等）

  ドイツにおける最大の脅威であり、IS（いわゆる「イスラム国」）やアルカイダなどのグローバルなジハード主義グループが、ドイツ国内での攻撃や、そのための資金調達・勧誘活動に従事している。IS はオンラインを通じて個別の実行犯を勧誘しており、2016 年のベルリンでのトラック突入テロ事件では、実行犯と IS メンバーとの接触が確認されている。

- サラフィー主義グループ

  ドイツ国内で活動する大小のサラフィー主義グループは、過激化の土壌となり、シリアやイラクなどの紛争地へ向かう外国人テロ戦闘員（FTF）の勧誘や、テロキャンプへの参加費の調達に関与している。

- 外国に拠点を置くテロ組織

  クルド労働者党（PKK）などの組織は、ドイツ国内の同調者を通じて資金を収集している。特に、出張などの機会を利用した「臨時運び屋」による現金の国外持ち出しが確認されている。

- 右翼過激派

  過去の国家社会主義地下組織（NSU）のような大規模な組織は近年確認されていないものの、ローンウルフ型や小規模グループによる脅威が存在する。これらは、テ

ロの目的を達成するために必ずしも多額の資金を必要としない傾向がある。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

組織に直接属さない個人や、人道的活動を装った支援活動も重要な脅威となっている。

- 個人主義的ジハード

  組織と直接的な繋がりを持たず、ジハード主義思想に触発されて過激化した個人やごく小規模なグループである。彼らは、就労収入や公的扶助、貯蓄などの合法的な資金源を利用して攻撃を準備しており、ごく少額の資金でテロを敢行できるため、資金流からの検知が極めて困難である。

- ディアスポラ及び同調者

  ドイツ国内に居住する外国テロ組織の同調者や特定のコミュニティは、出身国の組織を支援するための寄付金の源泉となっている。

- 非営利団体（NPO）の悪用

  ドイツで一般的な登録団体（e.V.）[8]の形式をとるNPOが、人道的目的を装って寄付金を募り、その資金を間接的にテロ組織へ還流させている事例がある。また、テロ組織の支配下にあるNPOや、正当なNPOの悪用を通じた国際的な資金移動も懸念されている。

- 外国人テロ戦闘員（FTF）とその家族

  紛争地域から帰還した戦闘員や、現地へ渡航した女性などが、ドイツ国内に潜伏してテロ組織の代理人として活動したり、過激化を促進するための構造を構築したりするリスクがある。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

ドイツ国内において、テロ資金供与の主体が資金を獲得する手段は、合法的な源泉から不法な犯罪収益まで多岐にわたる。

- 合法的な資金源

  個人の給与所得、預貯金、及び公的扶助（社会保障手当等）が、テロ活動を支える主要かつ実質的な資金源となっている。また、親族からの支援や金融機関からの借入れが、紛争地域への渡航資金などに充てられる事例も確認されている。

- 不法な資金源（犯罪収益）

  窃盗、強盗、盗品等関与、薬物密売に加え、各種詐欺（保険詐欺、インターネットを通じた詐欺等）などの刑事犯罪を通じて資金が獲得されている。特に、過激化した個人が渡航やテロ準備のために、こうした犯罪行為を厭わない傾向が認められる。

- 寄付金及び支援金

[8] “eingetragener Verein”の略

ドイツ国内のディアスポラや同調者から募る寄付金は、外国テロ組織の活動基盤を維持するための重要な源泉である。

- 事業・投資

  不動産投資や飲食業などの事業運営を通じて、中長期的に安定した資金流を確保し、組織構造を定着させようとする動きも懸念されている。また特定の商品を投機対象とした株式取引（デリバティブ利用など）による資金稼ぎも存在する。

- 他国による支援

  限定的ではあるが、他国が個人の過激化を促進する構造を構築するために資金を提供している可能性も指摘されている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

獲得された資金をテロ組織や活動拠点へ移転・供与する手法としては、既存の金融システムを回避する手段が好まれる傾向にある。

- 非公式資金移転サービス

  特にハワラが多用されており、銀行システムが未発達な地域や、追跡を逃れたい場合に、信頼関係に基づいたネットワークを通じて多額の資金が移動されている。

- 現金運び屋（キャッシュ・クーリエ）

  専門的な運び屋だけでなく、出張者などの「臨時運び屋」が、監視を潜り抜けて現金を国外へ持ち出す手法が確認されている。また、テロキャンプへの参加者が「参加費」として数千ドルを直接持参する事例もある。

- 正規の金融システム及び送金サービス

  多額の資金移動には、依然として既存の銀行システムや、資金移動業者が利用されることがある。

- 物品による提供（現物供与）

  衣類、医薬品、軍事機器、車両などの現物収集・輸送も、直接的な資金供与に代わる重要な支援形態となっている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

テロ資金の獲得・提供を容易にしている背景には、ドイツの経済・法的特性や技術的プラットフォームが存在する。

- 現金主導の経済特性

  ドイツ経済は高い現金依存度を有しており、これが取引の匿名性を高め、テロ資金の隠匿や移動を容易にするリスク要因となっている。

- 法的組織形態（NPO 及び法人）

  ドイツの登録団体（e.V.）制度は設立が比較的容易であり、これを隠れ蓑にした

NPO が人道的活動を装って資金を募り、テロ組織へ還流させる基盤となっている。

また、最低資本金の制約が少ない「有限会社（GmbH）」なども、資金洗浄やテロ資金供与の手段として悪用されやすい。

- オンラインプラットフォーム

IS（「イスラム国」）等の組織は、SNS やメッセージングアプリを継続的に運用しており、これらが個人の勧誘や、自己過激化した「ローンウルフ」による資金調達の呼びかけ、活動の調整を行うプラットフォームとして機能している。

②脆弱性

ドイツにおけるテロ資金供与（TF）のリスクを増大させている脆弱性として、以下の固有の背景が挙げられる。

②-1-1.国・地域に固有の文化的背景や社会・経済構造

- 経済的魅力とグローバルな相互接続性

ドイツは欧州単一市場の中核を担い、世界有数の輸出国であることから、経済的な魅力が極めて高い。その経済構造はグローバルレベルで深く相互接続しており、こうした国際的な繋がりが、本質的に高いクロスボーダー・リスクを生み出す要因となっている。

- 現金主導の経済特性

ドイツ経済の顕著な特徴として、決済手段における現金への高い依存度が挙げられる。この現金中心の文化は、取引の匿名性を高める選択肢を広げており、テロ資金供与の潜在的な脅威を増幅させる主要なリスクとして機能している。実際に、テロ資金供与や資金洗浄の多くが依然として現金に依存している実態が確認されている。

- 地理的・人口統計学的要因とディアスポラ

ドイツは欧州の中心部に位置し、隣接国が多いという地理的特性に加え、多様な国籍の移民や大規模なディアスポラ・コミュニティを有している。外国のテロ組織が、ドイツ国内に居住するこれらの同調者やディアスポラを悪用し、人道的目的を装った寄付金の募集や、組織の構造維持・活動のための資金源として利用している実態がある。

- 移民と移動の管理における脆弱性

紛争地域（シリア、イラク等）からの帰還者や、移民の流れに紛れてテロ組織のメンバーや代理人が入国するリスクが指摘されている。こうした人の移動は、テロ組織がドイツ国内に活動拠点を構築したり、過激化を促進したりするための資金流入を伴うことが多く、社会構造上の脆弱性となっている。

- 法制度及び NPO の構造的特徴

ドイツの登録団体（e.V.）等の法的組織形態は、その設立の容易さから、人道的目的を装って資金を募るテロ支援団体に悪用されやすい側面がある。正規の非営利団

体（NPO）が意図せず悪用されるケースもあり、慈善活動という文化的・社会的基盤がテロ資金移転の隠れ蓑となっている。

②-2-1.テロ資金供与を防止するための法的枠組み

ドイツにおけるテロ資金供与対策（CFT）の法的枠組みは、国際的な基準である金融活動作業部会（FATF）の勧告、及び欧州連合（EU）の資金洗浄防止指令を国内法に反映させる形で構築されている。

- マネー・ローンダリング法

  ドイツの CFT 予防体制の中核となる法律である。第 4 次 EU 資金洗浄防止指令を国内法化した改正マネー・ローンダリング法が 2017 年 6 月に施行され、リスクベース・アプローチが強化された。特定事業者（金融機関、弁護士、公証人、不動産業者等）に対し、顧客管理や、国家リスク評価の反映を含むリスク管理体制の構築を義務付けている。

- 刑法

  ドイツではテロリズムに関する独立した刑法典は存在せず、一般刑法の中にテロ関連規定を組み込んでいる。

  - 第 76 条（財産没収）

    特定の重大犯罪（テロ資金供与を含む）の疑いがある場合、個別の犯罪事実が完全に立証されなくとも、状況証拠から不法な源泉であると裁判所が確信した場合に資産を没収できる制度が導入され、テロ組織の資金基盤を剥奪する手段となっている。

  - 第 89a 条（国家を危険にさらす重大な暴力犯罪の準備）・第 89b 条（国家を危険に陥れる重大な暴力犯罪を犯す目的でのテロ組織との接触）

    重大な暴力的行為の準備や、そのための接触行為を処罰対象としている。

  - 第 89c 条（テロ資金供与）

    テロ活動を支援する目的での資金提供を直接罰する規定である。

  - 第 129a 条（テロ組織の結成）・第 129b 条（国外の犯罪組織及びテロ組織）

    国内及び国外のテロ組織の結成、参加、及び支援を処罰する。

- 対外経済取引・支配法

  第 18 条に基づき、国連や EU による対テロ経済制裁（資産凍結等）への違反が処罰される。

- 透明性登録簿

  法人の実質的支配者を特定するための登録制度が構築されている。これにより、法人がテロ資金の隠匿先として悪用されるリスクの低減を図っている。

- 税関検査

  税関検査は EU 税関法典（UCC）（EU 規則第 952/2013 号）に基づき、原則とし

てリスクベース・アプローチの対象となる。同法第 46 条（2）は、税関検査は主に国内レベル、EU レベル、及び可能な場合には国際レベルで策定された基準によるリスク分析に基づいて行わなければならないと規定している。

- 非公式送金の禁止

  連邦金融監督庁（BaFin）の認可を受けない送金サービス（ハワラ等）の運営は禁止されており、決済サービス監督法（ZAG）等を通じて規制されている。

②-3-1.金融当局等の監督・アウトリーチ

ドイツの金融セクターにおけるテロ資金供与対策の監督は、連邦金融監督庁（BaFin）が中心的な役割を担っている。

- リスクベースの監督体制

  BaFin は、銀行、保険、証券などの金融機関に対し、リスクベース・アプローチに基づく監督を行っている。定期的な立ち入り検査や書面監査を通じて、マネー・ローンダリング法に基づく義務（顧客の本人確認、リスク管理体制の構築、疑わしい取引の届出等）の遵守状況を監視している。

- アウトリーチ活動と指針の提供

  BaFin は、解釈・適用指針を公表し、金融機関がテロ資金供与リスクを正しく理解し、実効的な対策を講じるための具体的なガイドラインを提供している。また、説明会等を通じて、最新のテロ資金供与の手口や制裁対象リストに関する情報の周知を図っている。

- 疑わしい取引の届出の質的向上

  金融情報ユニット（FIU）との連携により、報告の質を向上させるためのフィードバックを金融機関に行っている。これにより、テロ資金供与に関連する可能性のある資金流の早期検知を促している。

②-3-2.NPO の規制、監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

指定非金融業者・職業（DNFBPs）を含む非金融セクターの監督は、ドイツの連邦制に基づき、各連邦州の権限当局によって行われている。

- 監督主体の分散と連携

  不動産業者、高額商品、カジノ、弁護士、公証人、会計士などの非金融セクターの監督主体は、ドイツ全土で約 300 の当局に分散している。

- 金融情報ユニット（FIU）

  DNFBPs セクターにおける AML/CFT の有効性を高めるため、同セクターの監督

に対する追加的な支援を提供することを目的としている。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

- 預金取扱金融機関（銀行）

  銀行セクター全体として、テロ資金供与リスクは「中・高（medium-high)」と評価されている。特に当座預金は、国内外への送金が容易であることから、テロ組織の活動資金や生活費の管理に悪用されるリスクが最も高い製品とされている。大手銀行や外国銀行の支店は、その国際的なネットワークや顧客基盤の広さから、クロスボーダーの資金移動に対する高度なモニタリング体制の構築が義務付けられている。

- 資金移動業者

  国際的な現金送金業務は、テロ資金供与への感受性が極めて高く、リスクは「高（high)」と評価されている。既存の銀行口座を介さない取引や、非公式なハワラ送金との接点になりやすいため、BaFin による厳格なライセンス管理と監督が行われている。

- 暗号資産

  暗号資産がテロ資金調達に利用されるリスクは、現時点では低いと評価されているが、取引の匿名性と迅速な国境を越える移動の可能性が懸念されている。EU 指令に基づき、法定通貨との交換業者を AML/CFT 規制の対象に加え、当局による監視を可能にする法的整備が進められている。

- 前払式支払手段(プリペイド型決済サービス)

  当該分野がマネー・ローンダリングやテロ資金供与に悪用される脅威は、関係公的機関により全体として低いと評価されている。プリペイドカード、電子バウチャー、デジタルウォレット等が該当する。現金でチャージ可能な匿名性や、世界中で利用できる利便性から、テロ活動の準備段階における資金手段としてのリスクを高める。銀行口座と比較して発行体による顧客の財務状況把握が困難であるため、取引パターンに基づいた異常検知に重点を置いた対応がなされている。

- 保険

  全体的なテロ資金供与リスクに関する言及はないが、マネー・ローンダリングに悪用されるリスクについては、関係公的機関が全体として中程度から低いと評価している。ただし、このリスクは増加する傾向にあると想定されている。テロ資金供与リスクが高い商品として、銀行類似商品（元本保証型)、保険料返還型傷害保険、養老保険及び繰延年金保険等が挙げられる。

  「顧客確認」の原則に基づき、保険事業者は顧客の財務的背景を確認することが求められているが、多くの保険会社は、顧客に職業の申告を常に求めていない。この情報は、マネー・ローンダリング防止目的ではなく、主に保険対象となるリスクに関連して収集されるためである。

保険会社は法律上、IT ベースのモニタリングを提供する必要がない。そのため、顧客のキャッシュフローを完全に把握できず、疑わしい取引の報告を妨げる可能性がある。

- 証券

全体的なテロ資金供与リスクに関する言及はないが、マネー・ローンダリングに悪用されるリスクについては、関係公的機関が全体として中程度と評価している。特に不動産ファンドの脆弱性が高い。

リテール投資信託は登録簿の保持が義務付けられていないため、多くの資産運用会社は個人顧客の身元を把握していない。現時点で全ての資産運用会社が個別のマネー・ローンダリングリスクを十分に認識しているかは不明である。

- 信託

信託によるテロ資金供与リスクは低と評価されている。信託を用いた資金管理は、資金の真の所有者を隠すために悪用されるリスクがあるため、信託管理人はマネー・ローンダリング防止法の対象者とされている。これらの専門職のサービスを利用することは、資金洗浄の代替手段となり得る。

- 不動産

ドイツの不動産セクターにおけるテロ資金供与リスクは中程度と評価される。不動産は高額な取引額と安定した価値という特性から、マネー・ローンダリング及びテロ資金供与活動の影響を受けやすく、リスクの高いセクターとなっている。

- 宝石・貴金属

ドイツの高い現金依存度を背景に、現金による高額購入がテロ資金供与の手段となりやすく、テロ資金供与リスクは中程度と評価されている。取引額が大きいため、一般的に犯罪収益を合法的に洗浄するのにも適している。

- 法律・会計関係サービス（TCSP）

ドイツのマネー・ローンダリング防止法に基づく対象者（法律・自由職業分野）は、監査人、税理士、弁護士、公証人である。テロ資金供与リスクは、これら 4 つの専門職において中程度から低程度と評価されている。特に監査人及び税理士は業務遂行過程において、企業組織の構造及び財務状況に関する詳細な知見を得ることができ、収入源と実質的所有者の両方を明確に把握できる立場にある。このため、企業内の異常を検知するのに最も適した義務履行主体となる。

- カジノ

カジノ等のギャンブル業界はマネー・ローンダリング脅威が極めて高いと評価されているが、テロ資金供与の脅威は低いと見なされている。オフラインギャンブルでは現金で支払われることが多く、高額取引と、高い資金処理量が特徴である。オンラインギャンブルは、ギャンブルに内在するリスクに加え、インターネット取引特有のリスクをさらに増幅させる。

②-4-2.NPO の活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

NRA の方法論に基づき、テロ組織によるドイツ国内でのテロ資金調達活動の脅威は中程度から高いと評価されている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

（7）オーストラリア

オーストラリアでは、オーストラリア取引報告・分析センター（AUSTRAC）が主体となり、国内の法執行機関、情報機関及び規制当局など 50 以上の関係機関と連携してテロ資金供与のリスクを分析し、「オーストラリアにおけるテロ資金供与国家リスク評価書（Terrorism financing in Australia national risk assessment）」として公表している。

リスクの特定・評価においては、「脅威（Threats）」、「固有の脆弱性（Inherent Vulnerabilities）」及び「結果・影響（Consequences）」の 3 つの要素の関数としてリスクを捉えるアプローチを採用している。具体的には、リスクを「発生可能性 × 結果・影響」と定義する考え方に基づき、総合的な固有リスクを算出している。

「発生可能性（Likelihood）」の評価にあたっては、「脅威」と「脆弱性」を掛け合わせたマトリックスを用いており、それぞれの評価基準は以下の通りである。

- 脅威：当局が調査した事例に基づき、特定のチャネルや手法がテロ資金供与に悪用される「規模や頻度」を推定している。評価にあたっては、テロリストによる過去の悪用実績、実行グループの能力（ネットワーク規模や専門性）と意図、及び現在のセキュリティ環境（当該手法を用いるグループの活動状況）が考慮される。
- 脆弱性：テロ資金供与を容易にする構造的な弱点を指し、以下の 5 つの観点から評価されている。
  - 収益性：当該チャネルを通じて調達・移動・保管し得る資金の量（規模）
  - アクセス性：コストの低さや、高リスク地域へ資金を移転する際の障壁の少なさ
  - 使いやすさ：利用に際して必要となる専門知識や技術的スキルの水準
  - 検知の難易度：報告事業者が不正を可視化・検知し、当局に報告できる体制の有無
  - 分断・阻止の難易度：捜査当局が当該チャネルを調査し、犯罪を阻止し得る能力

「結果・影響（Consequence）」の評価については、資金が海外に流出する性質上、手法ごとの正確な測定が困難であることから、チャネル別の個別評価ではなく、国家レベルでの総合評価として扱われている。評価基準には、資金が「組織運営費（プロパガンダ、給与等）」か「直接的な作戦費（武器購入、攻撃準備等）」のいずれに使用されるかという「資金の用途」と、政府への信頼低下や社会の分断、金融システム全体への悪影響を測定する「政治的・社会的・経済的損害」が含まれる。

また、現在のリスクレベルに加え、今後 3 年間でリスクがどのように推移するかという「見通し（Outlook）」も評価に組み込まれている。将来の予測軌道は、「増加（Increase）」、「減少（Decrease）」、「安定（Stable）」、「流動的（Dynamic）」の 4 つに分類され、多角的な分析が行われている。

①脅威

①-1-1.テロ組織、テロリスト

オーストラリアにおけるテロ組織・テロリストの脅威として、テロ組織及びテロリストの存在と活動が確認された。それぞれの活動実態と脅威の動向は以下の通りである。

- イスラム国（IS/ISIL）及びアルカイダ（al-Qa'ida）

  オーストラリアからの資金提供の可能性が最も高いグループとして特定されている。これら組織の海外におけるネットワークや能力は大幅に低下しているものの、その暴力的な過激主義は依然として国内の少数の個人に影響を与え続けている。

- ハマス（Hamas）及びヒズボラ（Hizballah）

  オーストラリアからの資金提供先となるリスクが、高いグループである。特にハマス・イスラエル紛争以降、人道支援目的で送付された資金がハマスによって搾取されたり、暴力的に徴収されたりする脆弱性が懸念されている。

- 宗教的動機に基づく暴力的な過激主義者（RMVE）

  宗教的な解釈に基づき、特定の社会・政治・法的システムを達成又は反対するために暴力を支持する主体である。ISIL 等の思想に同調する者のほか、2022 年のクイーンズランド州ウィアンビラでの攻撃（Wieambilla attack）に見られるようなキリスト教系の過激主義もこれに含まれる。

- 思想的動機に基づく暴力的な過激主義者（IMVE）

  政治的な目的の達成や不満への対応として暴力を支持する主体である。特に「国家主義的・人種主義的な過激主義」が脅威とされており、白人至上主義的な「人種戦争」とそれに続く白人国家の樹立を信奉するグループが含まれている。

- ジェマ・イスラミア

  アルカイダに連帯する東南アジアの組織である。将来の暴力行為に備え、地域内において勧誘、訓練、及び準備活動を継続しているとされている。

- アル・ヌスラ戦線

  シリアを拠点とするアルカイダ系の組織である。関連するケーススタディにおいて、人道支援活動家を装いながら同組織に加入した疑いのあるオーストラリア人の事例が報告されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

オーストラリアにおけるテロ資金供与の脅威として、特定のテロ組織やテロリスト本人だけでなく、これらを支援し、あるいは同調する以下の個人や集団の活動が確認された。

- 単独犯

  オーストラリアにおいてテロ攻撃を行う可能性が最も高い主体である。自己資金で活動し、検知可能な財務的要素を欠くことが多いという特徴を持つ。攻撃準備のために武器や戦術装備を現金で購入したり、個人の貯蓄や資産を活動資金に充てたり

する傾向がある。

- 支持者

  テロ実行犯に対して、武器の直接提供や少額の現金を渡すなどの支援を行う個人である。善意の寄付を装って国内外のテロ活動に資金を提供するほか、海外の戦闘地域へ渡航しようとする者に対して、少額の送金を行う事例も確認されている。

- オンライン上の推進者・勧誘者

  SNS、メッセージングアプリ、及びクラウドファンディングを統合した「オンライン資金調達エコシステム」を活用する者である。オンライン上で過激な思想を広めて支持者と繋がり、少額の寄付を募ることで、ネットワークの拡大やリソースの増強を図っている。

- 外国テロ戦闘員（Foreign Terrorist Fighters: FTFs）

  海外の紛争に参加するためにオーストラリアを出国した個人である。ISIL の衰退等によりその数は激減したものの、過激な思想を保持したまま帰国した場合、安全保障上の持続的な脅威となることが懸念されている。

- 高リスク・テロリスト受刑者

  刑期満了を迎え釈放されるテロ犯である。コミュニティに対する持続的な脅威とみなされており、法に基づく継続拘留命令や拡張監視命令の対象となる。

- 不当な慈善活動の推進者

  テロ組織の同調者、支持者、親族、又は関係者である。人道支援を装った偽のキャンペーンを立ち上げ、オーストラリアのドナー（寄付者）を標的にして、最終的に海外のテロ組織へ資金を流出させる主体として活動している。

- 第三者の仲介者及び「ミュール（運び屋）」

  資金の最終的な受益者を隠蔽する目的で、送金を代行する個人である。犯罪歴のない個人が、特定の思想に基づき、自身の銀行口座をテロ関連の資金調達に使用させるケースも確認されている。

- ディアスポラ及び特定のコミュニティ

  海外の紛争や地政学的緊張に強く反応し、人道支援という名目で、意図せず（又は強要により）テロ組織への資金流出に関与する可能性のある集団である。特に、紛争地域に根ざした小規模 NPO などを通じて支援を行う際に、その脆弱性が顕在化すると指摘されている。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

オーストラリアにおけるテロ資金供与の主体は、テロ活動を維持・実行するために、以下のような多様な手法を用いて資金を獲得していることが確認された。

- 自己資金

  オーストラリアにおけるテロ資金供与の主要な形態として位置づけられている。

資金は個人の貯蓄、給与、資産の売却をはじめ、クレジットカード、ローン、福祉給付金、さらには年金（スーパーアニュエーション）などから捻出されている。取引額は一般的に数百ドルから数千ドルといった低額に留まる傾向がある。

- ソーシャルメディア、クラウドファンディングを通じた募金

「オンライン資金調達エコシステム」を活用し、国内外の支持者から小口の寄付を募る手法である。これには、人道支援を装った「偽装慈善募金」が含まれており、善意の寄付者が意図せずテロ組織を支援してしまうリスクが指摘されている。

- 登録慈善団体及び合法的な NPO による資金の流用

公的な信頼や多額の資金へのアクセスが悪用される手法である。善意で活動する NPO が、海外の紛争地域や高リスク地域でのプロジェクト実施に際し、現地のパートナーや第三者を通じて意図せず資金をテロ活動へ転用される（流用される）ケースが存在する。

- グループの会費

特に思想的動機に基づく暴力的な過激主義者（IMVE）グループ、とりわけ国家主義的・人種主義的な過激主義を掲げるグループにおいて、活動資金を維持するための重要な源泉として確認されている。

- 犯罪活動及び詐欺

詐欺やその他の犯罪活動を通じて資金を獲得する手法である。調査のケーススタディにおいては、政府のプログラムに対する詐欺によってテロ資金を捻出した実例が挙げられている。

- 合法的な事業及びフロント企業

外形上は合法的なビジネスを装い、その収益をテロ支援に充てる手法である。複雑な企業ネットワークを構築し、複数の国の銀行口座を利用することで資金源を隠蔽しながらテロ活動を支える事例が報告されている。

- 国内外の富裕な個人寄付者

オーストラリア国内、あるいは国外の富裕な個人支持者からの直接的な資金提供である。これらは大規模なテロ組織を支えるための重要な資金源となり得ると評価されている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

オーストラリアにおいて、テロ資金供与の主体がテロ組織等へ資金を提供するにあたり、以下のような多様な移転手法やチャネルが悪用されていることが確認されている。

- 銀行システム

国内外の資金移動に最も頻繁に利用される信頼性の高いチャネルである。取引口座や電子資金送金が、迅速かつ容易に資金を収集・保管・移動できる手段として悪用されている。特に大手銀行は、広範な顧客基盤と国際的なネットワークを有している

ため、テロ資金供与に対して高い脆弱性に晒されている。

- 送金サービス

  銀行網が未発達な高リスク地域への送金に好んで利用されるチャネルである。登録された正規業者のほか、法規制を回避しようとする主体による「未登録業者」の利用も確認されている。さらに、ハワラ（Hawala）やオフセッティング（帳消し決済）といったインフォーマルな価値移転手法も、その匿名性の高さから悪用されている。

- 非銀行系オンライン決済サービス（OPSPs）

  SNS やクラウドファンディングと連携し、低額の送金を迅速に行うために利用される。第三者が決済に介在することによって取引の透明性が低下し、法執行当局による追跡や資産の凍結を困難にするという脆弱性が指摘されている。

- 電子通貨

  とりわけ思想的動機に基づく過激主義者（IMVE）の間で利用が増加しているチャネルである。匿名性の高い「プライバシーコイン」やミキシングサービスが、資金源や目的地の隠蔽を図るために悪用されている。また、ビットコインやステーブルコインを用いて、海外のテロ組織へ直接的に小口送金を行う事例も検出されている。

- 現金交換及び現金密輸

  国内における現金交換は、当局の監視を避ける目的で、支持者から集めた現金を直接手渡したり、銀行や送金業者へ預け入れる前にプールしたりするために使用されている。一方、国外への現金密輸は、国境を越えて物理的な現金を持ち出す手法であり、とりわけ正規の金融システムが遮断されている地域への価値移転手段として利用されている。

- 外貨両替及びプリペイドカード

  海外への渡航やオフショア送金の前段階として、現金を外貨に両替する手法が用いられる。また、プリペイドカード（保存価値カード）についても、匿名性が極めて高く、国内外で流動性を持つ特性があるため、価値移転の有効な手段として悪用され得ることが確認されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

オーストラリアにおいて、テロ資金供与の主体が資金獲得やテロ組織への資金提供を行うにあたり、以下のような制度、基盤、及びプラットフォームがインフラとして悪用されていることが確認されている。

- オンライン資金調達エコシステム

  SNS、メッセージングアプリ、クラウドファンディング、及びコンテンツホスティングを統合したネットワークである。各プラットフォームが密接に連携し、過激派の募集、宣伝、及び少額寄付の収集を低コストで行うための不可欠な基盤となってい

る。

- ソーシャルメディア・コンテンツ配信プラットフォーム

  SNS に加え、ライブ配信、動画ホスティング、及びサブスクリプション型プラットフォームが、チップ（投げ銭）やグッズ販売を通じた収益化に広く利用されている。また、これらは過激なプロパガンダの拡散や、クライストチャーチ事件等に見られるような攻撃のライブ配信の基盤としても悪用されている。

- メッセージングサービス（Telegram 等）

  特に Telegram が、オーストラリアの過激派にとって極めて重要な役割を果たしている。その暗号化機能により当局の監視を回避しつつ、送金指示やデジタル通貨のウォレットアドレスの共有、並びに実際の資金使途に関する隠密な議論を行う場として提供されている。

- クラウドファンディング・プラットフォーム

  多数のドナーから迅速に資金を集めるための重要な基盤である。大手プラットフォームが利用規約や規制を強化した結果、Hatreon や Wesearchr といった「過激主義に寛容なサイト」へ資金調達活動がシフトしている傾向が確認されている。

- 登録慈善団体及び合法的 NPO

  これらの団体が有する公的な信頼と多額の資金へのアクセスが、意図的又は不本意な資金流用の基盤として悪用されている。特に、宗教的 NPO の中には法的な報告義務が免除されている「基本宗教慈善団体」が存在しており、これが制度上の脆弱性となっていると指摘されている。

- 合法的なビジネス及びフロント企業

  国際貿易や現金集約型ビジネスを装い、国際送金に対して「正当性のベール」を着せるための基盤として利用されている。シェル企業などの複雑な所有構造を利用して実質的支配者を隠蔽し、資金源の追跡を困難にする手法が用いられている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

オーストラリアにおいて、テロ資金供与の脆弱性を生み出している国・地域に固有の文化的背景、地理的条件、及び社会・経済構造として、以下の要素が確認されている。

- 地理的・社会的な近接性と地域リスク

  オーストラリアは物理的には孤立した大陸であるものの、東南アジア諸国との地理的・経済的な近接性、及び中東等の紛争地域との文化・社会的な繋がりがリスク要因となっている。海外での紛争や地政学的な緊張に対する国内コミュニティの反応が、テロ組織への小規模な資金流出を誘発する一因となっている。

- 政治的安定性と社会的分断のリスク

  基本的には高度に安定した民主主義国家であるが、テロ資金供与の脅威が顕在化

した場合、民主主義的規範の浸食や社会の分断（コミュニティ間の不和）を引き起こすといった社会的被害（社会的害）をもたらす可能性があると評価されている。

- 現金依存度とデジタル化の状況

  経済全体のデジタル化が進行し、現金の全体的な使用率は低下しているものの、テロ資金供与における「現金」の固有リスクは依然として「高（High）」と評価されている。これは、現金が極めて高い匿名性を持ち、小口の正当な取引に紛れやすいためである。

- 規制の適用が限定的な分野

  現在、弁護士、会計士、不動産業などの特定の非金融セクター（DNFBPs）がAML/CTF 法の規制対象外に置かれている。この規制のギャップがオーストラリアの制度上の大きな脆弱性として特定されており、これらの分野が法人の複雑な構造化や不透明な価値移転に悪用されるリスクが指摘されている。

- 国際金融・貿易における立ち位置

  オーストラリアは洗練された金融システムを持ち、世界経済と深く結びついているため、国内外における迅速な資金移動が容易な環境にある。主要な銀行は強固な監視体制を構築している一方で、その膨大な取引量自体が、低額かつ合法的な取引に紛れ込むテロ資金の検知を困難にする要因となっている。

②-2-1.テロ資金供与を防止するための法的枠組み

オーストラリアにおいて、テロ資金供与を防止及び抑止するための法的枠組み並びに制度的基盤として、以下の体制が整備されている。

- テロ資金供与の犯罪化

  1995 年連邦刑法の 103 節において、テロ行為、テロ組織、個々のテロリストへの資金提供が広く犯罪化されている。直接的であるか間接的であるかを問わず、また資金が特定のテロ行為に実際に使用されなかった場合であっても処罰の対象となる。なお、テロ資金供与罪に対する最高刑は、無期懲役（最長）又は多額の罰金と定められている。また、テロ組織への加入や訓練に関連する資金提供についても厳格に処罰される法的枠組みとなっている。

- 法執行機関の捜査能力（AFP & JCTTs）

  オーストラリア連邦警察(AFP)及び州警察から成る合同テロ対策チーム(JCTTs)が中心となり、テロ資金の流れを遮断するための捜査を実施している。同チームは高度な財務分析能力を有しており、資金源を特定してテロ活動を未然に阻止することに重点を置いている。

- テロリストの資産凍結制度

  国連憲章法（Charter of the United Nations Act 1945）及び自主制裁法（Autonomous Sanctions Act 2011）に基づき、テロリストや組織の資産を即時に凍結する制度を有

している。外務貿易省（DFAT）が管理する「統合リスト」に掲載されることにより、金融機関は対象者との全取引を即座に停止する義務を負う。

- AUSTRAC の規制・監督活動

  AUSTRAC がオーストラリアの金融情報ユニット（FIU）兼規制当局として、AML/CTF 法に基づき数千に及ぶ報告主体を監督している。AUSTRAC は、疑わしい取引報告（SMRs）の分析結果を法執行機関へ提供し、テロ資金供与の兆候を早期に検知する中核的な役割を担っている。

- 情報共有メカニズム（FINTEL Alliance）

  金融機関、法執行機関、及び規制当局がリアルタイムで情報を共有する「FINTEL Alliance」という仕組みが存在する。これにより、法規制の枠組みを超えた官民一体の対応が制度化されている。

②-3-1.金融当局等の監督・アウトリーチ

オーストラリアにおいて、金融システムをテロ資金供与から保護し、制度の実効性を高めるため、金融当局等による以下の監督及びアウトリーチ活動が実施されている。

- AUSTRAC の権限と役割

  AUSTRAC はオーストラリアの主要な AML/CTF 規制当局であり、金融システムをテロ資金供与から守るための広範な監督権限を有している。具体的には、数千の報告主体（金融機関、送金業者、カジノ等）を登録及び監督し、コンプライアンスの遵守を確保する役割を担っている。

- リスクベースの監督手法

  セクターごとのリスクプロファイルに応じた監督が実施されている。特に、テロ資金供与リスクが「高」と評価された主要銀行や送金セクターに対しては、より集中的な監督活動が行われている。さらに、不遵守に対しては強制的な法執行アクションを行う権限を行使する体制となっている。

- FINTEL Alliance（官民連携）

  AUSTRAC が設立した「FINTEL Alliance」は、法執行機関、インテリジェンス機関、及び主要な民間金融機関がほぼリアルタイムで情報を共有するプラットフォームとして機能している。この枠組み[9]を通じて、テロ資金供与の複雑なパターンを共同で特定し、分析することが可能となっている。

- ガイダンス・指標の定期的な提供

  AUSTRAC は報告主体に対して、テロ資金供与に関する指標やセクター別のリスク評価書を定期的に提供している。これにより、民間企業が自律的にテロ資金の疑わ

[9] FINTEL Alliance 内部に設立された、テロ資金供与対策や国家安全保障上の脅威に特化した作業部会として「国家安全保障ワーキンググループ」が存在し、テロ資金供与に係る情報共有がされている。

しい取引（SMRs）を検知し、報告する能力を継続的に向上させている。

- 関連当局間の専門性共有

  AUSTRAC の金融インテリジェンス専門家は、オーストラリア連邦警察（AFP）やオーストラリア保安情報機構（ASIO）などの合同テロ対策チーム（JCTTs）と緊密に連携している。金融データの解析等を通じて、テロリストのネットワークを特定・解明するための高度な専門性を提供し、法執行当局の捜査を直接的に支援している。

②-3-2.NPO の規制、監督・アウトリーチ

オーストラリアにおいて、非営利団体（NPO）や慈善団体がテロ資金供与に悪用されるリスクを軽減するため、規制当局等による以下の監督及びアウトリーチ活動が実施されている。

- 規制当局（ACNC）の役割

  オーストラリア慈善・非営利団体委員会（ACNC）は、慈善団体が国内外の活動においてテロ資金供与リスクを特定し、軽減できるようガイダンスを提供している。また、ガバナンス、財務報告、記録保存などの法的義務に関する不遵守を継続的に監視・管理する役割を担っている。

- 連邦及び州・準州による多層的監督

  慈善団体は連邦レベルで監督される一方、各州・準州も独自の規制を課すという多層的な監督構造が存在している。この多層構造により、規制当局間における可視性、能力、及びリソースに不一致が生じており、登録を取り消された団体が別の管轄区へ移動して活動を継続するリスクが指摘されている。

- 外部行動基準

  慈善団体が海外で活動し、又は海外へ資金を送る際に遵守すべき基準として「外部行動基準」が設けられている。同基準は、適切な財務管理を維持し、資金がテロ活動に転用されることを防ぐための法的義務を課しており、ACNC は本基準に関する教育活動を継続的に実施している。

- 宗教団体に対する規制上のギャップ

  「基本宗教慈善団体」に分類される組織は、ACNC のガバナンス基準の遵守や財務報告の提出を免除されており、規制上の可視性に欠けるというギャップが存在している。ただし、当該団体であっても、海外への資金移動を伴う場合には外部行動基準の遵守が求められる。

- 当局間の連携とアウトリーチ活動

  連邦レベルと州・準州レベルの規制当局が相互に連携し、セクター全体のガバナンス向上や、脆弱な NPO に対するアウトリーチを強化している。さらに、AUSTRAC は NPO の代表団体や報告主体に対して、高リスクと評価される NPO への適切な対

応を促すための実務的なガイダンスや指標（インジケーター）を提供している。

- リスクベースのセクター評価

  当局は FATF（金融活動作業部会）の基準に基づき、テロ資金供与に悪用される可能性が高い NPO のサブセットを特定し、評価を実施している。AUSTRAC と ACNC は 2024 年に最新のリスク評価レポートを発行する予定であり、この評価には未登録 NPO がもたらすリスクも調査対象として含まれている。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

オーストラリアにおいて、金融機関や NPO 以外のセクターにおけるテロ資金供与リスクに対応するため、関係当局等による以下の監督活動及び法制度改革に向けた取り組みが進められている。

- 暗号資産（デジタル通貨）交換業者への監督

  同セクターは 2018 年より AUSTRAC の規制対象となっており、登録、顧客確認、記録保持、及び疑わしい取引の報告が義務付けられている。AUSTRAC は専用の分析チームとブロックチェーン追跡ツールを導入しており、ガイダンスの提供や取引監視を通じた監督を行っている。

- 未規制セクター（弁護士、会計士、不動産業等）への改革

  現在、弁護士、会計士、不動産業などのセクターは AML/CTF 法の対象外となっており、国際基準（FATF 勧告）に対するオーストラリアの制度上の脆弱性として指摘されている。これに対し、政府はこれらの分野を規制対象に含めるための法改正案を開発中であり、これが実現すれば監督体制が大幅に強化されると見込まれている。

- 独立送金業者（ハワラ等を含む）の管理

  ハワラや現金宅配便といった非公式な価値移転手法を用いる業者を含む、すべての送金業者は、AUSTRAC の「送金セクター登録簿」への登録が義務付けられている。AUSTRAC は、未登録業者の利用がもたらす危険性を訴えるコミュニティ・キャンペーンを 11 言語で実施するなど、積極的なアウトリーチ活動を展開している。

- オンライン資金調達（クラウドファンディング等）への対応

  クラウドファンディング等のプラットフォームは、現在「オンライン資金調達エコシステム」の一部として、高いテロ資金供与リスクを有すると評価されている。これに対応するため、当局はこれらのプラットフォームに対する AML/CTF 規制の適用可能性について検討を進めている。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

- 預金取扱金融機関（銀行）

  銀行セクターの固有リスクは「高（High）」と評価されている。主要銀行はテロ資金供与リスクを深く理解し、洗練された監視システムと AML/CTF 体制を構築して

いる。しかしながら、膨大な顧客基盤と現金取引インフラを有しているゆえに、合法的な取引の中に紛れ込む低額のテロ資金供与を完全に検知することには、依然として脆弱性が残っていると分析されている。

- 資金移動業者

  送金サービスの固有リスクは「高（High）」と評価されている。同セクターには、送金ネットワークプロバイダー（RNP）が加盟店の AML/CTF プログラムに対して責任を持つ構造が存在する。一方で、セクター全体を通してみると、プログラムの実効性や検知能力にはばらつきがあり、一部の業者においては不審な動きを報告する意欲や能力が低いことが課題として指摘されている。

- 暗号資産

  デジタル通貨交換業の固有リスクは「高（High）」と評価されている。法定通貨との交換を行う業者は、顧客確認や報告義務を概ね良好に遵守していることが確認されている。しかし、セクター自体が比較的新しいため、自らの製品や顧客をデフォルトで低リスクであると過小評価する傾向が見られ、テロ資金供与リスクへの理解が不十分な場合があることが弱点とされている。

- 前払式支払手段(プリペイド型決済サービス)

  本セクター固有の活動・対応に関する詳細な記載はない。ただし、プリペイドカード（保存価値カード）は匿名性が極めて高く、国内外で流動性を持つという特性から、価値移転の手段として悪用され得ることが確認されている。

- クレジットカード

  本セクター固有の活動・対応に関する詳細な記載はない。ただし、単独犯等のテロ資金獲得の活動において、クレジットカードが自己資金の主要な捻出元のひとつとして利用されている事実が確認されている。

- 不動産

  現在、不動産業は AML/CTF 法の規制対象外となっており、国際基準（FATF 勧告）に対するオーストラリアの制度上の脆弱性として特定されている。法人の構造化や価値移転に悪用されるリスクが指摘されており、政府は規制対象に含めるための法改正案を開発中である。

- 法律・会計関係サービス（TCSP）

  現在、弁護士や会計士等の法的・会計的専門職セクターは AML/CTF 法の規制対象外となっており、不動産と同様にオーストラリアの制度上の脆弱性として特定されている。これらは複雑な所有構造の構築や価値移転に悪用されるリスクがある。

- カジノ

  カジノは、AUSTRAC の監督下において AML/CTF 法の適用を受ける報告主体として位置づけられている。銀行等と同様に、顧客確認、1 万ドル以上の現金取引報告、疑わしい取引報告（SMR）、及び記録保持等の義務が課されている。

②-4-2.NPO の活動・対応

オーストラリアにおいて、非営利団体（NPO）や慈善団体がテロ資金供与に悪用される固有の脆弱性及び活動・対応状況について、以下の事実が確認されている。

- NPO セクターのテロ資金供与リスク評価

  NPO セクターの固有リスクは「中（Medium）」と評価されている。この評価は 2017 年のセクター別リスク評価以降、概ね安定している。善意の寄付を募る能力や、多額の資金へのアクセスが可能である点が、テロ資金供与主体にとっての魅力となっている。

- テロ資金供与の悪用手法

  NPO を悪用する主な手法として、以下の 2 点が確認されている。なお、確認されている多くの事例は、宗教的動機に基づく暴力的な過激主義者（RMVE）に関連する海外への資金流出である。一方、思想的動機に基づく暴力的な過激主義者（IMVE）については、合法的な NPO との繋がりは確認されているものの、現時点において暴力活動への資金提供には至っていないと分析されている。

  - 流用：善意で設立された団体が、海外でのプロジェクト実施時に、不十分な管理下で現地のパートナー等を通じて意図せず資金を転用されるケース。
  - 偽装：最初からテロ支援を目的として設立され、人道支援の「正面（フロント）」を装って資金を収集・移動させるケース。

- セクター内の脆弱性要因

  個別の団体における脆弱性要因として、テロ資金供与リスクへの理解不足、関係者（職員、パートナー、受益者等）に対する不十分なデューデリジェンス、不透明な資金サイクルの管理、及び高リスク地域での活動が挙げられている。

- 規制上の課題と対応状況

  多くの NPO はガバナンスを自己評価に依存しており、独立した外部監視が不十分であることが指摘されている。また、大部分の NPO は AML/CTF 法の対象外であり、AUSTRAC への報告義務がないため、不審な活動の検知を金融機関に依存せざるを得ないという構造的な課題が存在する。

  また、当局は、NPO セクター全体ではなく、テロ資金供与リスクに最も晒されやすい NPO のサブセットを特定し、標的を絞ったアウトリーチを実施している。具体的には、オーストラリア慈善・非営利団体委員会（ACNC）による外部行動基準の教育や、AUSTRAC による指標の提供が継続的に行われている。

②-4-3.その他セクターの活動・対応

オーストラリアにおいて、金融機関や NPO 以外のその他のセクターにおいても、テロ資金供与に対する固有の脆弱性が評価されており、各分野における活動・対応状況やリスクの

性質について以下の事実が確認されている。

- オンライン資金調達エコシステム（SNS、クラウドファンディング等）

  固有リスクは「高（High）」と評価されている。過激主義者が支持者と繋がり、小口の寄付を募るための不可欠な基盤として機能している。またう、人道支援を装った「偽装慈善募金」により、善意の寄付者が意図せずテロ組織を支援してしまうリスクが存在し、2016 年以降、関連製品の普及に伴い上昇していると分析されている。

- 国内の現金交換業

  固有リスクは「高（High）」と評価されている。匿名性が極めて高く、ローンアクターによる武器や装備の購入、グループの会費支払、あるいは銀行送金前の資金プールに悪用されることが確認されている。低額な取引が多いため、正規の経済圏に混じっても疑念を抱かれにくいという脆弱性を持つ。

- サイバー犯罪（ランサムウェア、暗号資産窃取）

  固有リスクは「中〜高（Medium-High）」と評価されており、新たな脅威として特定されている。サイバーエクストーション（サイバー恐喝）やクリプトジャッキング（暗号資産の窃取）により、当局による追跡を回避しながらテロ活動を支えるリソースを生成するリスクが指摘されている。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

オーストラリアにおいて、テロ資金供与の脅威が顕在化する可能性について、以下の評価及び分析がなされている。

- 脅威環境の変化と単独犯の台頭

  ISIL 等の大規模な国際テロ組織の能力低下に伴い、高度に組織化されたテロ攻撃の発生可能性は相対的に低下している。一方で、過激な思想に影響を受けた単独犯や小規模なグループによる、単純かつ事前計画の少ない攻撃の脅威が顕在化しやすくなっている。これらの攻撃は実行に要する資金が少額（数百ドル程度）で済むため、既存の金融監視網で検知する前に脅威が顕在化する可能性が高いと評価されている。

- 自己資金調達による検知の困難性

  オーストラリア国内で計画されるテロ攻撃の大部分は、個人の貯蓄や給与、福祉給付金などの自己資金によって賄われている。合法的な収入源からの少額支出は、日常的な経済活動と区別がつかないため、金融インテリジェンスのみによって脅威の顕在化を事前に予測・阻止することは極めて困難であると指摘されている。

- イデオロギーの多様化によるリスクの拡散

  宗教的動機に基づく暴力的な過激主義（RMVE）に加え、国家主義的・人種主義的な過激主義をはじめとする思想的動機に基づく暴力的な過激主義（IMVE）が台頭している。脅威の主体が多様化したことで、従来の監視対象とは異なる新たなコミュニ

ティや層からテロ資金供与活動が突発的に顕在化する可能性が生じている。

- テロ資金の共有源としての継続的リスク

  オーストラリアは依然として、海外のテロ組織や紛争地域に対して資金を供給し得る国としての性質を帯びている。特に、海外の紛争（中東情勢など）に呼応する形で、人道支援を装った偽装募金や、意図しない資金流出を通じて、海外におけるテロの脅威を顕在化させる資金的基盤を提供する可能性が継続して存在している。

- オンライン環境と新興技術の悪用

  オンライン資金調達エコシステム（クラウドファンディングや SNS）や暗号資産（デジタル通貨）の普及により、テロ資金供与の手法がより分散化・匿名化している。これにより、国境を越えた小口資金の迅速な移動が容易になり、当局の規制や監視をすり抜けて資金調達の脅威が顕在化する可能性が高まっていると分析されている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

オーストラリアにおいて、テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害について、以下の通り評価及び分析がなされている。

- 国家安全保障及び治安への影響

  資金提供がテロ攻撃に直接結びついた場合、その被害は極めて深刻となる。オーストラリアでは多くのテロ計画が未然に阻止されているものの、事案が顕在化した場合は国家の安全保障上の重大な脅威となる。

- 資金の使途による直接的な影響

  作戦目的での資金利用は、テロ攻撃の実行、人命の損失、物理的な破壊といった直接的かつ深刻な被害に直結する。一方、組織運営目的での利用においては、宣伝、勧誘、ネットワークの維持等を通じて、将来のテロ遂行能力や組織の回復力を高める結果を招くと評価されている。

- 政治的及び社会的な影響

  テロ資金供与の発生は、政府に対する国民の信頼の失墜、民主主義的規範の浸食、及び社会の分断（コミュニティ間の不和）を引き起こす可能性がある。また、オーストラリアの対策が国際的な基準に達していないと見なされた場合には、外交的な摩擦が生じるリスクも指摘されている。

- 経済的な影響

  オーストラリアにおけるテロ資金供与は小規模かつ低額な傾向があるため、経済全体への直接的なマクロ的影響は無視できる程度であると評価されている。しかしながら、事案に関与した金融機関や NPO 等の個別組織は、評判の失墜（レピュテーション・リスク）、規制対応コストの増大、及び公的信頼の喪失といった深刻な経済的打撃を受ける懸念がある。

（8）ニュージーランド

ニュージーランド（以下、「NZ」とする。）では、リスク評価は「脅威評価（犯罪類型）」と「セクター別脆弱性評価」の 2 軸で構成される。これらが相互に影響し合い、最終的な ML/TF リスクを決定する。

- 脅威の算定基準：犯罪の「量」と「価値」に基づき、「最大のリスク」「より小さいリスク」「低リスク」に分類される。（例：詐欺や薬物等の高頻度かつ高額な犯罪は「最大のリスク」、低頻度かつ少額の犯罪は「低リスク」に分類される。）
- 脆弱性の評価に関する考え方：セクター別の脆弱性は、「資金の出入り」や「規模」「複雑性」の要素によって構成される。「資金の出入り」については、預け入れ、引き出し、国内外の送金サービスの有無、「規模」と「複雑性」については、利用の容易さ、他セクターへのゲートウェイ機能、取引の量と速度が考慮される。また、各セクターの脆弱性を高める要素として、①犯罪者の能力、②当該セクターに関連する没収資産の価値、③犯罪者による実際の利用状況を考慮するとしている。一方で、セクターの脆弱性の軽減要因としては、①疑わしい取引の届出の質、②AML/CFT に関するコンプライアンス遵守レベル、③顧客モニタリングのレベルが考慮される。

また、NZ 政府のテロ資金供与リスク評価に関する独自の尺度として、NZ 国内ではテロ発生自体のリスクが低いと評価されていることから、NRA におけるテロ資金供与リスク評価の考え方において統一的に「高リスク」とする基準については言及がない。（ML リスクについては「高リスク」と評価している領域もある。）

NZ におけるテロ資金供与リスクの考え方は、以下の可能性を意味すると定義されている。

- 極めて低い：「可能性が低い」
- 低：「現実的な可能性がある」
- 中：「実行可能であり、起こり得る」

セクター別の ML/TF リスク評価については、銀行、送金サービス、及びクレジットカードの 3 セクターにおいて、「ML/TF リスク：高」と評価されている。その背景には、各セクターがテロ資金供与に悪用され得る脆弱性を主に評価しているものと解釈されるものの、上述の通り全体的な考え方に関する指針のようなものは NRA の中に記載されていないため、推測の域を出ないことに留意が必要である。

①脅威

①-1-1.テロ組織、テロリスト

NZ におけるテロの脅威は、単独実行犯から国際的な組織まで多岐にわたる。2024 年のリスク評価において特定された主要な主体は以下の通りである。

- 自己資金型の単独実行犯

  NZ におけるテロの主な懸念事項は、組織に属さない単独の実行犯である。過去 5

年間に国内で発生した 2 件の攻撃はいずれも、自己資金によって賄われた単独犯によるものであった。これらの攻撃は短期間で計画され、ナイフ、車両、銃器、又は斧といった、限られた資金で調達可能な手段を用いて実行されるという特徴がある。

- 国際的なテロ組織（Da'esh/ISIL、Al Qaeda）

  アルカイダの支部から派生したダーイッシュ（ISIL/ISIS）等の国際的なテロ組織に対し、NZ 国内の個人が直接又は間接的に資金支援を行うリスクが認識されている。特に ISIS については、テロ資金の管理又は所有に暗号資産を利用している事実が確認されている。

- その他の国際指定組織（Hezbollah、Hamas）

  ヒズボラやハマスへの資金提供の可能性が指摘されている。ハマスについては、2024 年 2 月に組織全体がテロ組織として指定された。現時点で NZ からの直接的な資金提供は確認されていないものの、パレスチナとの間で行われる資金移動は、テロ資金供与の観点から精査の対象となっている。

- 極右・白人至上主義団体（Extreme Right-wing）

  世界的に台頭している白人至上主義や反移民感情に基づく極右過激主義は、NZ においても重大な脅威として浮上している。具体例として、NZ 政府は「アメリカン・プラウド・ボーイズ（American Proud Boys）」をテロ団体として指定している。

- 国内法に基づく指定団体

  NZ 政府は、国連安保理決議 1373 を補完するため国連指定外の 22 の団体をリスト化し、監視の対象としている。

- ISIS に感化された主体

  組織との直接的な繋がりはなくとも、思想的な影響を受けた主体による脅威も存在する。具体例として、2021 年にオークランドで発生したテロ攻撃の実行犯は、ISIS に感化された主体であったと特定されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

NZ 国内には、直接的なテロ実行犯のみならず、思想的共鳴、人道支援の仮装、又は無意識的な関与等を通じて、テロ活動を支える多様な主体が存在する。

- オンラインで過激化した同調者

  インターネットや過激派フォーラムでの情報交換を通じて過激化した NZ 国内の個人が、海外の過激思想を有するグループに対して寄付又は送金を行うリスクが指摘されている。これらの主体は、特定の組織に属さずとも、オンライン上の交流を通じて資金提供に至る傾向がある。

- ディアスポラ（移住者コミュニティ）

  世界各地のテロ資金調達者が、NZ 国内に存在する特定のディアスポラ・コミュニティを利用し、テロ活動を支援するための資金を調達又は移動させている実態が認

識されている。

- 偽装 NPO の設立者及び運営者

  ドナー（寄付者）を欺くために、実態を伴わない「偽の NPO（Sham NPOs）」を設立し、人道支援活動を装いながら、収集した資金をテロ組織への供給源とする主体が存在する。

- 無意識の支援者（NPO/NGO の寄付者等）

  人道支援を目的として特定の紛争地域へ送金を行う慈善団体又はその寄付者が、現地の複雑な状況により、意図せずテロ組織への資金提供の回廊となってしまうリスクが特定されている。

- 外国人戦闘員の支援者

  紛争地域へ渡航した人物が現地の ATM で現金を引き出す行為、又は当該人物が保有する海外口座に対し、NZ 国内から資金を供給する支援者の存在が報告されている。

- 極右・白人至上主義への寄付者

  思想的な背景に基づく支援主体として、極右・白人至上主義団体への寄付者が挙げられる。具体的事例として、クライストチャーチのテロ攻撃の実行犯は、攻撃前に海外の極右・反移民団体又は個人に対して 14 件の寄付を行っていたことが確認されている。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

テロ資金供与の主体が活動資金を獲得する手法は、合法的な経済活動から組織的な犯罪行為に至るまで極めて多岐にわたる。NZ における主な資金獲得活動は以下の通りである。

- 合法的なソースによる自己資金調達

  NZ を含む多くの国において、テロ資金の主要な調達方法は合法的なソースであると特定されている。具体的には、個人の所得、個人資産の売却、クレジットカード、ローン、政府からの福利厚生の支払、年金、又は退職金等が挙げられる。

  また、予期せぬ多額の資金流入として相続が利用されるケースがある。具体的事例として、クライストチャーチのテロ攻撃の実行犯は、自身の生活費及び攻撃の準備費用を相続による収入によって賄っていた事実が確認されている。

- 寄付の募集

  第三者からの寄付の勧誘又は収集を通じて資金を獲得する手法は依然として利用されている。これには、人道支援、慈善活動、宗教、文化、教育、社会、又は親睦等を目的として掲げた活動が含まれる。ドナー（寄付者）を欺いて資金を拠出させるために、実態のない NPO を設立し、多額の寄付金にアクセスするリスクも指摘されている。

- 物品の販売等の経済活動

特定の組織を象徴する物品の販売が資金源となるケースもある。NZ 国内において、テロ団体として指定された「アメリカン・プラウド・ボーイズ」の関連グッズを個人が購入していた例が確認されており、これが組織の活動を支える資金源となっている可能性がある。

- 犯罪行為による収益の獲得

テロリスト又はテロ組織が、資金を調達する目的で詐欺又は薬物犯罪等の犯罪に従事する可能性が強く認識されている。これらの犯罪から得られた収益は、直接的又は間接的にテロ活動の原資となる。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

テロ資金を目的の組織や地域へ移転させる手法は、既存の金融システムを悪用するものから、規制を回避するインフォーマルな手段まで多岐にわたる。

- 銀行システムによる電信送金、及びオンラインバンキングの遠隔操作

銀行セクターは、国内外の広範な資金移動を可能にするサービスを提供しており、テロ資金供与において最も脆弱なセクターの一つとして特定されている。事実、高リスク地域への送金の半分以上が銀行セクターを経由して行われている。

また、NZ 国内で正当に開設された口座に対し、シリア等の高リスク地域からオンラインバンキングを通じてアクセスし、資金を管理又は移動させる手法も特定されている。

- 資金移動サービス（MVTS／レミッタンス）

国際的な資金移動の回廊として日常的に利用されており、特にテロ資金供与に特徴的な「少額・多頻度」の取引において多用される傾向にある。具体例として、パレスチナ向け送金の 60%がこのセクターを利用していたことが確認されている。

- 暗号資産

ビットコイン等の暗号資産は、その匿名性と高速な国際送金機能により、過激派団体への寄付又は資金移動に利用されている。ISIS が暗号資産を所有及び管理している可能性も当局により指摘されている。

- 現金の密輸・物理的運搬

銀行システムの監視を回避する目的で、現金、貴金属、又は宝石等の高価値商品を、物理的に国境を越えて運ぶ手法が取られる。NZ からイラクへ数万ドルの現金を物理的に持ち出そうとした事例も報告されている。

- プリペイド式旅行カード及び紛争地域での ATM 引き出し

国内で現金又は電子的にチャージしたカードを、海外へ郵送又は携帯する手法である。これらのカードは疑わしい取引の届出義務の対象外となることが多く、現地の ATM で匿名且つ継続的に現金を引き出すことを可能にしている。

NZ 国内で発行され、持ち出されたデビットカード、クレジットカード、又はプリ

ペイドカードを用い、イラク等の紛争地域又は高リスク地域の ATM から直接現金を引き出す手法が確認されている。

- 非公式な資金移動システム（ハワラ等）

  SWIFT 等の正式な銀行メッセージングシステムを介さず、業者間の相殺によって資金を移動させる手法である。パキスタン又はイラン等の特定の回廊において、その利用が確認されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

テロ資金の獲得及び移転を円滑化させるために悪用される制度的基盤又はデジタルプラットフォームは、その匿名性や国際的な利便性を背景に多様化している。

- 法人及び法的構成物（シェルカンパニー等）

  法人又は信託等の法的構造は、真の受益者の特定を困難にし、金融システムへのアクセスを容易にするため、テロ資金供与に悪用される可能性が高い。これらは資産の出所を隠蔽し、正当な経済活動を装うための有力な手段となっている。

- ノミニー（名義人）制度

  信託・会社サービスプロバイダー（TCSP）が提供する名義取締役（ノミニー・ディレクター）等のサービスが不正な取引に悪用されるリスクが指摘されている。

- 非営利組織（NPO）及び人道支援団体

  NPO は、紛争地域又は高リスク地域へ資金を送るための回廊として悪用されるリスクを有する。これには、テロ組織が善意のドナーを欺くために慈善活動を仮装して設立する偽装 NPO も含まれる。

- デジタルプラットフォーム

  クラウドファンディング・プラットフォームは、国境を越えて資金を獲得・移動させるための現代的なツールとして明示されており、疑わしい取引の届出（SAR）においても頻出するテーマとなっている。

  また、SNS 及びメッセージングサービスも、資金の募集、過激思想の拡散、同調者の獲得に悪用されている。SNS を通じたロマンス詐欺や投資詐欺がテロ資金源となる可能性について指摘されている。

  オンライン・過激派フォーラムも、世界中の個人が思想を共有し過激化する場となっており、特定の組織への寄付や支援に繋がるリスクがあると認識されている。

- オンライン決済及び経済エコシステム

  オンラインカジノ及びギャンブルプラットフォームは、犯罪収益の洗浄のみならず、プリペイドカード等でチャージした資金を移動させる手法として利用される。

  また、フィッシング又は身分盗用といったサイバー詐欺を通じて、テロ活動や兵器開発の資金を調達するリスクが認識されている。

Facebook や Trade Me といった電子商取引及びマーケットプレイスを通じた詐欺、又は指定テロ団体の関連グッズ販売が、活動資金を支える基盤として悪用されている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

NZ におけるテロ資金供与のリスクを増大させる要因として、国及び地域に固有の地理的、経済的、並びに社会的な背景に基づく脆弱性が特定されている。

- 地理的条件と国境管理

  NZ は他国と陸上の国境を接しておらず、高リスク管轄区域とも地理的に離隔している。このため、伝統的な組織的テロの脅威は比較的低いとされる一方、物理的な現金の密輸、又は高価値物品の持ち出しに対する警戒は国境において継続されている。

- 国際金融・貿易システムへの高度な統合

  NZ の経済は世界金融システムと密接に統合されており、毎日多額の国際送金が実行されている。この高度な接続性は、テロリスト又はその同調者が NZ 国内から海外の過激派組織へ、銀行送金、資金移動サービス、又は暗号資産等を通じて容易に資金を移動させることを可能にする脆弱性となっている。

- デジタル化とオンライン接続性

  世界的なデジタル接続の進展に伴い、NZ 国内の個人がオンライン上で海外の過激派グループと接触し、過激化するリスクが高まっている。これにより、インターネットを介した小口の寄付、又は SNS 及びクラウドファンディングを通じた支援が容易になっている。

- 現金依存度と匿名性

  一方で現金は高い匿名性を有しており、依然として犯罪経済において重要な役割を果たしている。特に国内の薬物市場は現金主導であり、これらの犯罪収益がテロ組織の資金源に転用される可能性が懸念されている。また、テロ活動支援を目的とした、数万ドルの現金を物理的に持ち出そうとする試みも確認されている。

- ビジネスの容易性

  NZ は「ビジネス環境の容易さ」や「起業の容易さ」で世界 1 位（世界銀行 2020 年調査）にランクされており、法人の設立が極めて容易である。この制度的な利便性は、実態のない会社（シェルカンパニー）等の設立を通じた、テロ資金又は拡散金融の隠蔽に悪用されるリスクとして認識されている。

  また、このビジネスにおける好環境、NZ の政治的安定性及び清廉な評判は、設立された法人等に「信頼性の外装」を与えるため、テロ資金を隠匿しようとする主体にとって魅力的な要素となっている。

- ディアスポラ（移住者）コミュニティの存在

世界各地のテロ資金調達者が、NZ 国内のディアスポラ・コミュニティを利用して資金を調達又は移動させている実態が認識されている。また、紛争地域への人道支援を目的とした慈善活動が、結果としてテロ組織への資金提供に繋がるリスクも指摘されている。

②-2-1.テロ資金供与を防止するための法的枠組み

NZ におけるテロ資金供与を防止するための法的基盤は、国内の金融システムの完全性を維持し、犯罪に対して敵対的な環境を構築することを主眼としている。

- AML/CFT 制度の目的

  NZ におけるテロ資金供与対策は、「マネー・ローンダリング及びテロ資金供与対策法 2009（AML/CFT 法）」等の法律を基盤としている。本制度は、金融システムの完全性を維持し、犯罪活動を抑制する環境を確保することにより、NZ 国民の幸福を向上させることを目的としている。

- 監督当局の指定

  AML/CFT 法に基づき、特定のセクターにおける報告義務機関の遵守状況を監視するため、以下の 3 つの機関が監督当局として指定されている。

  - ニュージーランド準備銀行（RBNZ）：銀行等の監督
  - 金融市場庁（FMA）：証券業者等の監督
  - 内務省（DIA）：カジノ、送金業者、及び貴金属ディーラー等の監督

- 報告義務機関の役割

  報告義務機関は、AML/CFT 法に基づき、自らの事業に及ぼすリスクを理解する義務を負う。また、特定されたリスクを適切に管理及び軽減するためのプログラム（方針、手続き、並びに管理措置）を整備することが法的に義務付けられている。

- 国境を跨ぐ現金の持ち出しに関する規制

  物理的な現金の移動によるリスクを抑制するため、国境現金報告（Border Cash Reports: BCRs）義務が課されている。金融インテリジェンスユニット（FIU）は、これらの報告を分析の情報源として活用しており、実際に薬物犯罪（55 件）又は詐欺（172 件）等の調査において重要な役割を果たしている。

②-3-1.金融当局等の監督・アウトリーチ

NZ における AML/CFT の監督体制は、報告義務機関の業種に応じ、ニュージーランド準備銀行、金融市場庁、及び内務省の 3 当局によって分担されている。各当局は、各セクターのリスク特性に応じたモニタリング、指導、並びに法執行を実施している。

- 銀行セクターにおける教育・啓発活動

  銀行セクターにおいては、詐欺等の犯罪急増に対応するため、オンラインバンキングを通じたガイダンスの提供や、メディアを活用した教育キャンペーン等の防止策

が強化されている。RBNZ は、銀行セクターに対し 2017 年から導入された規定取引報告（PTR）の遵守状況を監視しており、不適切な報告を行っていた銀行に対し正式な警告を行うとともに、システム設計の改善に向けたフィードバックを継続的に実施している。

- 送金セクター（MVTS）への監督と法執行

  DIA は、テロ資金供与に悪用されやすい送金業者（MVTS）セクターに対し、厳格な監督を行っている。2014 年以降、送金業者に対して 25 件の公式警告を発出したほか、2017 年以降には 4 件の民事訴訟、及び重大な違反に対する 2 件の刑事訴追を実施し、セクター全体のコンプライアンス向上を図っている。

- 暗号資産サービスプロバイダー（VASP）への対応

  新興セクターである VASP に対し、DIA は強力な執行措置を講じている。具体的には、AML/CFT 方針や本人確認基準（IDCOP）、並びに継続的な顧客管理（CDD）が不十分であった事業者に対し、事業停止を含む措置を実施した事例がある。また、急速に変化する技術動向に対応するため、主要なステークホルダーとの継続的な関与を維持している。

- 特定セクターへの関与強化と今後の課題

  一部のセクターにおいては、依然としてリスク認識の向上や監督の余地が残されている。

  第一に、会計士セクターにおいては、疑わしい取引の届出（SAR）の提出割合が低い現状を受け、当局は AML/CFT 法上の義務についての理解を深めるための密接な関与が必要であるとしている。

  第二に、現金輸送及び両替セクターに対しては、現金が犯罪収益の主要な媒体となっていることから、現金輸送セクターとのエンゲージメント深化や、両替セクターにおける報告の質の改善に向けたガイダンスの提供が課題として指摘されている。

②-3-2.NPO の規制、監督・アウトリーチ

NZ における NPO セクターは、その規模の大きさと国際的な活動実態から、テロ資金供与リスクに対する適切な規制及び監督が重視されている。

- NPO セクターの定義及び規模

  NZ における NPO は、FATF の定義に基づき、慈善、宗教、文化、教育、又は社会等の目的で資金の調達及び支出を行う団体を指す。NZ 国内には 28,970 の登録慈善団体が存在し、2023 年 6 月期において 810 億ドルの資産及び 240 億ドルの収入を計上しており、経済的に極めて大きな規模を有している。

- 主な監督当局（Charities Services）

  慈善団体セクターの健全性を維持するための監督及び調査を担う主な機関は、慈善団体サービス局（Charities Services）である。当該当局の調査活動は主に苦情ベー

スで実施されており、国内事案に焦点を当てている。テロ資金供与対策に特化した体制ではないものの、その活動はNPOセクターの誠実さを維持し、不正を防止する上で重要な役割を果たしていると評価されている。

- 登録審査及びリスク評価

  すべての慈善団体は登録時に審査を受け、リスク格付けが行われる。ただし、現行の格付け要素には海外活動の実態やテロ資金供与リスクへの曝露が含まれていない点が、今後の課題として指摘されている。

- 継続的な監視及び行政監督

  主に以下の3つの観点に基づいて、NZ当局は継続的な監視及び行政監督を行っている。

  - 監査及び監視

    会計原則の遵守を確認するための継続的な監査が実施されている。これには、寄付者の特定や、海外への支出が団体の本来の活動目的に合致しているかの確認も含まれる。

  - 多角的な監督

    学校、又は寄付者が税額控除を受けられる団体については、教育省（Ministry of Education）等の関連機関による追加の監視が行われている。

  - 不適切な活動への対応

    関連当事者への不適切な貸付等の資金流用、管理体制の不備、虚偽の身分証を用いた登録試行、又は税務回避を目的とした「棚上げ慈善団体（shelf charities）」の登録試行等に対し、厳格な調査が実施されている。

- アウトリーチ及び今後の改善策

  海外で活動するNPOに対し、年次報告プロセスの中で報告要件を強化することが、リスクの理解及び透明性の向上に寄与すると分析されている。当局は、これらのセクターに対し、テロ資金供与に関する認識向上のためのアウトリーチを継続する必要性を強調している。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

内務省等の監督当局は、金融機関以外の特定非金融業者及び職業的専門家（DNFBPs）に対しても、リスクに基づいた監督及び法執行活動を展開している。各セクターにおける主な監督実績は以下の通りである。

- 不動産セクター

  不動産セクターにおいては、AMLプログラムの欠陥に関連して5件の法執行活動が行われた。このうち、計5件の公式警告（3件は公表、2件は非公表）が発出されており、現在も複数の団体において是正措置が継続中である。

- 弁護士及び法務代行業

2019 年以降、AML/CFT 法上の義務を遵守していなかった 6 つの法律事務所に対し、監督当局より公式警告が発出された。法的な専門知識を有するセクターであっても、制度の適切な運用が厳格に求められている実態が示されている。

- 会計士セクター

2018 年から 2023 年の間に、複数の継続的な違反が確認された 1 社に対し、非公表の公式警告が発出された。当該事案においては、CDD の不備、政治的要人（PEPs）の確認漏れ、又は独立監査義務の不履行等が指摘されている。

- カジノセクター

カジノセクターでは、重大な義務違反に対する高額な制裁金が課された事例が報告されている。2024 年 2 月、リスク評価、AML プログラムの維持、及び取引モニタリング等の義務違反により、あるカジノに対し民事訴訟が提起された。同年 9 月、当該カジノ側が違反を認めたことを受け、416 万ドルの罰金支払いが命じられた。

- 信託・会社サービスプロバイダー（TCSP）

DIA は、会社設立又はノミニー（名義人）サービスを提供する TCSP、法律事務所、及び会計事務所を対象にテーマ別調査を実施した。調査の結果、多くの業者が海外の仲介者に依存せず自ら CDD を実施している良好な事例が確認された。一方で、DIA が把握していない業者が依然として存在する懸念も指摘されており、引き続き監視体制の強化が求められている。

②-4-1.金融機関等（DNFBPs 含）の活動・対応

マネー・ローンダリング及びテロ資金供与のリスクを軽減するために、銀行、資金移動業者、暗号資産、及び DNFBP（弁護士、会計士、不動産等）の各セクターが、主に疑わしい取引の届出の強化を含む、多角的かつ強固な規制措置を講じている。

- 銀行

銀行セクターは NZ 国内の疑わしい取引の届出の大部分を占め、2023 年には 12,233 件を提出した。報告理由は詐欺収益の疑いや多額の現金預金、急激な資金移動など多岐にわたる。また、警察、税関、内国歳入局、及び主要銀行（ANZ, Westpac 等）が参加する「金融犯罪防止ネットワーク（FCPN）」を通じて、情報のサイロ化を防ぎ、インテリジェンスを共有する取り組みを行っている。

- 資金移動業者

特に大手国際資金移動業者は、取引の多くを「疑わしい」として報告（セクター報告の約 80%を占める）するほど、強固な内部統制とスクリーニングを運用している。

- 暗号資産

自動化された技術をリスク軽減の主要ツールとして活用しており、新たな規制やプロセスの変更に対してもシステム改修を通じて迅速に対応する体制をとっている。

- 士業セクター

弁護士や不動産業者は、不動産取引等において顧客の身元や資産の源泉を確認する法的義務を負い、不透明なオフショア資金等の流入を阻止する防波堤として機能している。

- カジノ

  大手カジノ（SkyCity）は全ての「ジャンケット（カジノツアー）」を廃止し、2025年半ばまでに現金取引の匿名性排除の義務化を予定している。

- セクター共通の取組

  報告義務機関は 2017 年以降、1,000 ドル以上の国際電信送金及び 1 万ドル以上の現金取引を FIU に自動報告するシステム（PTR）を構築・維持している。

②-4-2.NPO の活動・対応

NZ において、NPO は、AML/CFT 法上の報告義務を有する機関には該当しない。しかし、慈善信託法、所得税法、及び 2005 年慈善団体法（Charities Act 2005）に基づき、テロ資金供与リスクを軽減するための以下の活動及び対応を行っている。

- ドナー（寄付者）の特定及び確認

  慈善団体は、会計原則の遵守及びリスク管理の一環として、寄付者の身元を特定し、その資金源を確認する活動を求められている。これにより、不透明な資金が団体に流入することを未然に防ぐ体制を構築している。

- 資金使途の監視及び整合性の確保

  特に海外の紛争地域等へ送金を行う際、その支出が団体の本来の慈善目的に合致しているか、又はテロ組織等に流用されていないかを監視及び確認する対応を行っている。これは、NPO が意図せず TF の回廊として悪用されることを防ぐための重要な措置である。

- 年次報告書の提出による透明性の確保

  すべての登録慈善団体は、監督当局である慈善団体サービス局（Charities Services）に対し、財務情報及び活動内容を含む年次報告書を提出する義務を負っている。このプロセスを通じて、団体の活動実績と資金の流れの透明性が確保されている。

- 登録審査への対応

  慈善団体として登録を受ける際、当局によるリスク格付けのための審査を受け、団体の目的や運営体制の正当性を証明する必要がある。この審査への対応は、団体自らが健全なガバナンスを有していることを示す機会となっている。

- 記録保存及び監査への協力

  監督当局や税務当局による監査に対し、資金の流れや活動実績を示す記録を保持し、必要に応じて調査に協力する体制を維持している。

- 海外活動に関する報告強化への対応

  現在の課題として、海外で活動する NPO に対し、年次報告プロセスの中でより詳

細な報告を求める方針が示されている。これを受け、セクター全体で報告の質を向上させ、海外送金に伴うテロ資金供与リスクに対する透明性をさらに高める対応が期待されている。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

NZ におけるテロ資金供与の脅威が現実のものとなる可能性については、過去の事例及び現在の国際情勢を踏まえ、以下の通り評価されている。

- テロ資金供与リスクの総合格付け

  NZ におけるテロ資金供与リスクは「低 (Low)」と評価されている 。この評価は、2019 年の前回評価から「変更なし（Unchanged)」とされている。

- 「低（Low)」リスクの定義

  本 NRA における「低」とは、「現実的な可能性がある（a realistic possibility)」ことを意味する。これは、「実行可能であり、起こり得る」と定義される「中(Medium)」、又は「可能性が低い」とされる「極めて低（Very Low)」との比較において、一定の警戒を要する水準として位置付けられている。

- 脅威の顕在化に関する現状分析

  過去 5 年間に NZ 国内で 2 件のテロ攻撃（2019 年クライストチャーチ、及び 2021 年オークランド）が発生しており、いずれも自己資金型の単独犯によるものであった。この事実は、テロ資金供与の脅威が単なる仮定ではなく、依然として現実のものであることを示している。

- 国内脅威と国際脅威の分離評価

  国内テロに関する資金供与の脅威は比較的低いとされている一方、海外のテロ活動を支援するための資金移動については、より高い警戒が必要であると認識されている。

- 今後の見通し

  NZ におけるテロの脅威見通しは今後も大きく変わらず、主にオンラインで過激化した単独実行犯が主要な懸念であり続ける可能性が高いと分析されている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

NZ において、テロ資金供与リスクが顕在化した場合、その影響は単なる経済的損失に留まらず、社会基盤や国際的地位を揺るがす「壊滅的」なものになると定義されている。

- 壊滅的な人命及び社会被害

国内外の経験から、テロリズムがもたらす帰結は「壊滅的」であると表現されている。これには、人命の喪失、並びに地域社会の安全及び安心に対する深刻な侵害が含まれる。

- 国家の評判（レピュテーション）の失墜

  NZ がテロ資金の調達又は移動の拠点として悪用された場合、国際的な評判が著しく損なわれる。これは、政治的・経済的に安定している国という評判に依拠している NZ のビジネス環境に対し、極めて深刻な悪影響を及ぼすことが懸念されている。

- 金融システムの完全性への脅威

  テロ資金供与に金融システムが利用されることは、当該システムの完全性を根本から揺るがす事態である。これは、NZ の金融インフラが犯罪に対して脆弱であることを露呈させ、国内外からの信頼を失墜させることに繋がる。

- NPO セクターへの信頼失墜

  NPO セクターがテロ組織に悪用された場合、寄付者の信頼及び確信に重大な影響を及ぼす。その結果として、本来の「善意の活動」に必要な資金が集まらなくなるという二次的被害が生じるリスクが指摘されている。

- 国際協力関係の毀損

  国際的な制裁（資産凍結等）を適切に実施できなかった場合、他国との信頼関係、共同捜査体制、又はインテリジェンスの共有に支障をきたす可能性がある。これは、国際社会と連携してテロに立ち向かう NZ の外交的立場を弱体化させる恐れがある。

（9）香港

リスク評価を行う「マネー・ローンダリング及びテロ資金供与評価運営委員会」は、金融サービス・財務局（FSTB）が議長を務め、警察、税関、金融管理局（HKMA）、証券先物委員会（SFC）、信託・会社サービスプロバイダー（TCSP）の監督機関や税務局（IRD）などの各分野の当局で構成される。リスク評価においては、2016 年から 2020 年までの 5 年間を対象とし、9,000 件以上の捜査・有罪判決・没収事例などの定量的データを活用している。さらに、法規制の更新を踏まえた現状分析と、ステークホルダーとの合意形成・対策案を策定のうえ、強化されたリスク軽減策を踏まえ、評価を更新した。

評価基準としては、世界銀行の「国家リスク評価ツール」を採用しつつ、2013 年～2021 年に発行された最新の FATF ガイダンスを参照している。

脅威と脆弱性をもとに、入手可能な定量的・定性的情報に基づき、「低・中低・中・中高・高」の格付けを割り当てている。また、評価結果をリスクレベル別のヒートマップとして視覚化し、重点的に対処すべき領域を特定している。

①脅威

①-1-1.テロ組織、テロリスト

香港国内において、組織的なテロ活動やそれに関連する資金供与が直接的に確認された事例は限定的である。

- 国際テロ組織の活動

  香港においてアルカイダ、イスラム国（ISIL）等のイスラム過激派による活動の兆候は確認されていないが、ソーシャルメディアによる宣伝が市民に影響を与える可能性を考慮し、警戒態勢を敷いている。

- 域外テロ組織の関与

  香港の高度な金融システムを背景に、域外のテロ活動を支援するための資金供与事案が発生する潜在的な脅威が指摘されている。しかし、現在までに香港国内においてテロ資金供与による起訴や有罪判決に至った確定事例は存在しない。

- 国内の過激派

  2019 年の社会不安[10]は、2020 年 6 月の「国家安全維持法」の施行により沈静化し、社会秩序は回復した。一方で、国内の過激派による潜在的な脅威や、それに関連する限定的な資金提供活動の兆候については、引き続き注視が必要な領域として監視されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

[10] 香港民主化デモ

支援者や同調者による活動については、主に個人による合法的資金の流用や、国外への送金リスクが中心となっている。

- 組織に属さない個人

  個人の合法的な所得をテロ活動に転用する「自己資金調達」は、国際的にも高まっている懸念事項であり、香港においても重要な分析対象となっている。

- 域内の外国人

  香港には約39万人の外国人家庭内労働者を含む多くの外国人労働者が居住しており、その中にはテロの被害を受けている地域の出身者も含まれる。これらの労働者が母国へ送金する際、意図せず、あるいは同調を通じてテロ資金に流用されるリスクが懸念されており、規制当局は銀行や資金移動業者（MSO）を通じた監視を強化している。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

- テロ組織による活動の傾向

  支配地域における恐喝、石油販売、課税、違法取引といった組織的な手法を多用する。非営利団体（NPO）からの拠出、個人支援者からの寄付、合法的な銀行システムへの投資も含まれる。資金は現金運び屋、ハワラ、送金サービス、銀行振込、暗号資産を通じて移動される。

- 極右過激派による活動の傾向

  個人から小規模組織、国境を越える大規模な組織に至るまで、規模やレベルが異なる幅広い主体が関与している。これらのグループの資金源は、クラウドファンディング、寄付、会費、商業活動といった合法的な活動から、犯罪収益の供与といった違法な活動まで多岐にわたる。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

- 自己資金調達

  最も一般的な資金獲得方法は、個人の給与、貯蓄、又は事業収益といった合法的な資金の流用である。特に、香港に居住する特定の外国人労働者コミュニティにおいて、少額の生活余剰金を母国の団体や個人へ送金するケースが潜在的なリスクとして特定されている。

- 銀行システム及び資金移動業者

  依然として従来の銀行送金や、資金移動業者を通じた電信送金が主要な手段である。特に、テロの脅威が高い地域への送金において、親族への送金を装う手法が警戒されている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォ

ーム等

- クラウドファンディング

  クラウドファンディングサイトを利用し、特定のキャンペーンや政治的活動を名目に不特定多数から資金を募る行為が見られる。これらは資金の出所を分散させ、監視を逃れるための効果的なツールとなっている。

- 暗号資産サービスプロバイダー（VASP）

  ビットコイン等の暗号資産を用いた送金は、その匿名性と国境を越える迅速性から、新たな脅威として位置づけられている。香港政府は VASP に対するライセンス制度を導入し、トラベル・ルールの適用等を通じてこのチャネルの透明性確保に努めている。

- 非正規の金融システム

  正規の金融システムを介さないハワラ等の伝統的な金融システムが、特定の外国人コミュニティ内で利用されることがあり、これが規制当局の追跡を逃れる手段として機能している。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

- 国際金融・貿易・物流ハブとしての開放性

  香港は、資本の自由な移動が保障された開放的な経済体制であり、世界有数の金融、貿易、物流のハブである。膨大な件数かつ高額なクロスボーダー取引が日常的に行われており、その中からテロ組織に関連する微細な疑わしい取引を特定することは、構造的に困難を伴う。この利便性と流動性が、意図せずテロ資金供与に悪用される潜在的な脆弱性となっている。

- 多文化社会と外国人労働者コミュニティ

  香港には約 39 万人に及ぶ外国人家庭内労働者が居住しており、その多くは東南アジア諸国（フィリピン、インドネシア等）の出身である。これらの出身国の中には、過激派組織の活動やテロの脅威に直面している地域が含まれる。

- 地理的・政治的特性

  中国本土への出入口としての機能や、東南アジア諸国との地理的な近接性は、ヒト・モノ・カネの活発な往来を促進する一方、地域的な過激思想の流入や、周辺国でのテロ事案に連動した資金移動が発生しやすい環境を形成している。

②-2-1.テロ資金供与を防止するための法的枠組み

香港は、国際基準である金融活動作業部会（FATF）の勧告に準拠し、テロ資金供与を効果的に検知・抑止するための強固かつ包括的な法的枠組みを構築している。これらの法的枠組みは、2019 年の FATF による第 4 次相互審査において高く評価されている。

● 国際連合（テロ防止措置）条例（UNATMO）

香港におけるテロ資金供与対策の中核となる法律である。国連安全保障理事会決議第 1373 号及びテロ資金供与阻止条約を国内法化したもので、テロ資金供与行為そのものの犯罪化、テロリストの資産凍結、及びテロリストに関連する財産の取り扱い禁止を規定している。2018 年の改正により、テロ行為の準備や参加を目的とした渡航資金の提供も犯罪化されるなど、国際的な脅威の変化に応じた強化が図られている。第 12 条では、テロリストの財産であるとの認識や疑いがある場合、すべての個人・法人は当局への報告が義務付けられている。

● マネー・ローンダリング及びテロ資金供与対策条例（AMLO）

金融機関及び特定非金融機関（DNFBPs）に対する規制の根拠法である。顧客身元確認（CDD）や記録保存、疑わしい取引のモニタリング体制の構築を義務付けており、違反した場合には刑事罰や監督上の制裁が科される。この条例に基づき、各監督当局はリスクベース・アプローチを用いた監督を行っている。

● 組織的及び重大犯罪条例（OSCO）

テロ組織の資産没収に関する規定が整備されており、テロ資金の源泉となる犯罪収益の遮断において実効性を担保している。

● 物理的通貨及び無記名譲渡証券の越境移動に関する条例（R32）

旅行者が香港に到着する際に、条例に定める指定管理地点を通過し、かつ多額の無記名譲渡証券（総額 12 万香港ドル超）を所持している者は、税関職員に対し書面による申告を行うことが義務付けられている。

②-3-1.金融当局等の監督・アウトリーチ

● リスクベースの監督

香港金融管理局（HKMA）、証券先物委員会（SFC）、保険業監理局（IA）等は、各事業者のリスクプロファイルに応じたオンサイト・オフサイトモニタリングを実施している。これには、テロリスト名簿との照合プロセスや、疑わしい取引報告（STR）の質に関する検証が含まれる。

● 民間セクターの指導

当局は、国際的なテロ資金供与のトレンドや新たな制裁対象者リストに関する通達を随時発行している。また、業界団体と連携したセミナーを定期的に開催し、民間セクターの意識向上を図っている。

②-3-2.NPO の規制、監督・アウトリーチ

● ガイドラインの公表

慈善団体向けにテロ資金対策専用のガイドラインを公表し、NPO に対しテロリスト又はテロ関連組織の指定名称への注意喚起を行っている。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

- 海事

  海事局は、国連による監視リストに掲載されている船舶から香港水域への入港を求められた場合、経済発展貿易局（CEDB）及び法執行機関（特に香港税関）と連携して対応している。また、疑わしい船舶の香港への入港を拒否している。

- 専門職

  弁護士、公認会計士、不動産業者、信託・会社サービスプロバイダー（TCSP）の各セクターに対し、それぞれの監督当局（香港法学会、香港公認会計士協会、会社登録所等）が AML/CFT 規制の遵守状況を監督している。

- 貴金属・宝石商（DPMS）

  2020 年に「貴金属・宝石取引業者向けマネー・ローンダリング及びテロ資金供与対策ガイドライン補足」を発行し、情報提供を行っている。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

セクターごとのリスク評価はマネー・ローンダリングリスクのみ評価されており、テロ資金供与リスクは本文献では評価されていない。

- 預金取扱金融機関(銀行)

  銀行セクターのマネー・ローンダリング脅威レベルと脆弱性レベルは、それぞれ「高」及び「中～高」と評価されており、セクター全体のマネー・ローンダリングリスクレベルは「高」と評価されている。

  香港は依然としてアジア太平洋地域における主要な国際金融・貿易ハブであると同時に有力な資産管理センターであり、銀行部門は本質的にマネー・ローンダリングに対して脆弱である。当局との密接な連携の下、疑わしい取引報告の提出や、官民情報共有プラットフォーム（FMLIT）を通じたインテリジェンスの活用を積極的に行い、潜在的なテロ資金の流入を監視している。

- 資金移動業者

  国内外の犯罪活動に起因する中程度から高いマネー・ローンダリング脅威に依然として晒されている。資金移動業者による疑わしい取引報告の提出件数は、銀行及び電子マネー事業者免許取得者に次いで 3 番目に多い。クロスボーダー送金の主要な担い手である資金移動業者は、免許更新時にテロ資金供与のスクリーニング能力の証明が求められる。

- 暗号資産

  従来の送金手段よりも高い匿名性と分散性を可能とするため、マネー・ローンダリング及びテロ資金供与リスクに脆弱である。当セクターのマネー・ローンダリングリスクは、中程度と評価される。暗号資産サービスプロバイダー（VASP）に対する免

許制度が導入されており、プロバイダーは当局による報告・監視・審査の対象となる。

- 前払式支払手段(プリペイド型決済サービス)

1回当たりの決済額が少額であるため、当セクターにおけるマネー・ローンダリングの脆弱性は中程度と評価される。香港金融管理局は、免許取得者に対し、AML/CFTに関する統制上の不備や法令・規制要件違反を是正させるため、一連の監督・執行措置を適用する。これには、事業又は活動に対する制限、又は条件付き許可、外部監査人によるAML/CFT統制に関する報告書の作成要求、是正命令、罰金、及び「決済システム及びプリペイド式電子マネーに関する条例（PSSVFO)」に基づく戒告が含まれる。

- クレジットカード

全体として、セクター別のマネー・ローンダリングリスクは低水準を維持している。犯罪者がクレジットカード申込書に偽造書類を添付し、顧客確認（CDD）テストを通過した事例は存在するが、香港ではこうした事例はごく限られている。

- 保険

保険セクターのマネー・ローンダリングリスクは全体として中低レベルと評価される。特に投資連動型又は現金価値積立機能を備えた長期保険商品においてリスクが顕著である。マネー・ローンダリング事案における保険が占める金額の割合は低いが、香港の保険市場がグローバルな性質を持つことを考慮すると、同セクターは越境的なマネー・ローンダリングの脅威に晒されている。

- 証券

証券セクターにおけるマネー・ローンダリングの脅威レベルと脆弱性レベルはともに中程度と評価されており、同セクターのマネー・ローンダリングリスクは中程度と評価される。証券セクターから提出された疑わしい取引報告の件数、及びマネー・ローンダリング調査・有罪判決件数は依然として低い水準にあるものの、中国本土との強固な経済的結びつきや世界的な株式取引センターであることが、マネー・ローンダリングリスクを高めている。

- 金銭貸付

当セクターのマネー・ローンダリング事案に占める割合は低く、リスクは全体として中程度から低いと評価される。いわゆる高利貸しと呼ばれる違法貸金業者が、債務返済不能となった借り手の銀行口座を掌握し、高利貸し活動やその他の組織犯罪からの資金回収に利用する事例が報告されている。

- 不動産

当セクターにおけるマネー・ローンダリングの脅威と脆弱性は、いずれも中低と評価されることを踏まえ、当セクターのマネー・ローンダリングリスクは中低と評価される。不動産仲介業者は、主に不動産取引や富裕層の売買対象としての不動産を通じて、潜在的なマネー・ローンダリング活動に晒されている。

● 宝石・貴金属

当セクターのマネー・ローンダリング脅威レベルと脆弱性レベルはそれぞれ中～低程度と中程度と評価される。これらを総合すると、マネー・ローンダリングリスクは中程度と評価される。一定額以上の現金取引を行う業者に対しては監視が強化されている。

● ファイナンスリース

ファイナンスリース契約は借手が資金を受け取るのではなく、あくまで資金の使用権を得るにとどまり、当該資金の法的・受益的権利はリース事業者に留保されるため、リスクは低い。

● 法律・会計関係サービス（TCSP）

マネー・ローンダリングの脅威及び脆弱性はいずれも中低と評価されていることから、当セクターのマネー・ローンダリングリスクは中低と評価される。

犯罪収益は不動産を含む様々な資産形態に変換される可能性があるため、不動産取引に関わる弁護士が意図的・非意図的にマネー・ローンダリングに関与する潜在的な脅威が生じうる。

信託・会社サービス事業に従事する会計専門家は、監査業務からの独立性を維持する必要性から、一般的に別個の法人を通じて事業を行う。したがって、彼らも TCSP に関連するマネー・ローンダリング脅威の対象となる。

②-4-2.NPO の活動・対応

NPO や慈善団体がテロ資金供与に悪用されたり、テロ組織を支持・容認したりしているという事例は確認されていない。NPO セクター固有のテロ資金供与の脆弱性は「低」と評価されており、現時点ではテロ資金調達や移動に悪用されている明白な兆候は見られない。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

香港はテロ資金供与リスクが中～低レベルと評価され、脅威と脆弱性の両方が中～低レベルと評価されている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

香港政府は、「香港は世界で最も安全な都市の一つ」であり、「世界で最も開放的な経済圏の一つ」と評しており、テロ資金供与の活動に悪用されることは、香港の金融システムの健全性に対する国際的な信頼を損ない、経済的な競争力に悪影響を及ぼすリスクがある。

（10）マレーシア

マレーシアでは、マレーシア中央銀行（Bank Negara Malaysia）が議長及び事務局を務める「マネー・ローンダリング対策国家調整委員会（NCC)」が主体となり、各省庁や法執行機関、規制当局と連携してマネロン・テロ資金供与のリスクを分析し、「国家リスク評価書（National Risk Assessment: NRA)」として公表している。

リスクの評価にあたっては、マネー・ローンダリングとテロ資金供与に対して共通の評価手法を採用しており、分析は「脅威リスク評価（Threat Risk Assessment)」と「セクター別リスク評価（Sectoral Risk Assessment)」の二つのアプローチで構成されている。

これら二種類のリスクレベルを決定するため、以下の二つの軸を用いたマトリクス（二次元表）による評価が行われている。具体的には、対象となる犯罪やセクターが元来有しているリスクの大きさと、それに対する対策の有効性を掛け合わせることで、最終的なリスクレベルを導出している。

- 内在リスク（Inherent Risk)：当該犯罪や特定のセクター自体が、その性質上、元々持っているリスクの大きさを指す。
- 管理措置（Control Measures)：リスクを低減・軽減させるために講じられている規制や監督、法執行機関による対策、及び報告事業者の取組などが、どの程度有効に機能しているかを分析する。評価にあたっては、その有効性の程度に応じて「強力（Strong)」、「許容範囲（Acceptable)」、「限定的（Marginal)」、「脆弱（Weak)」といった区分で判定が行われる。

①脅威

①-1-1.テロ組織、テロリスト

マレーシアにおけるテロ組織・テロリストの脅威として、テロ組織及びテロリストの存在と活動が確認された。それぞれの活動実態と脅威の動向は以下の通りである。

- イスラム国（IS）及び系列組織

  イスラム国（IS）の崩壊、地域内における IS 系列組織（IS-affiliated groups）に対する軍事作戦の強化、及び国内における著名な IS 指導者の不在又は死亡により、テロ及びテロ資金供与のリスクは残存している（低減傾向にある)。
- 適応能力を持つテロ組織（将来のリスク）

  テロ組織は変化する環境に適応する能力を有しており、その脅威は決して固定的ではないと分析されている。このため、テロの展望については引き続き「慎重な」見通しが維持されている。さらに、長期化する国際紛争が、地域へのテロやテロ資金供与の波及（spillover）を引き起こす潜在的なリスクについても指摘されている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

マレーシア国内におけるテロ資金供与事案は、多くの場合、支持者や同調者によって実行されている。これらは組織的な活動というよりも、個人の思想的な共感に基づく傾向がある。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

マレーシアにおけるテロ資金供与の主体は、テロ活動を維持・実行するために、以下のような多様な手法を用いて資金を獲得していることが確認された。

- 自己資金による賄い（Self-financing）

  マレーシア国内におけるテロ資金供与事案の大部分は、個人の雇用所得（給与）や個人的な貯蓄を原資とする自己資金で賄われている。

- 支持者・同調者による寄付・集金

  組織的なスキームではなく、思想に共鳴する個々の支持者や同調者、あるいは小規模な集団や団体が、地域的又は広域的な目的のために資金を出し合ったり、集めたりしている。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

マレーシアにおいて、テロ資金供与の主体がテロ組織等へ資金を提供するにあたり、以下のような多様な移転手法やチャネルが悪用されていることが確認されている。

- 銀行送金

  マレーシア国外へ不法な資金が流出する際の最も主要な経路である。テロ資金供与においても、送金業者（MSB）と並んで主要な送金チャネルとして利用されている。

- 送金サービス

  銀行システムと同様に、不法な収益を国外へ移動させるための主要なチャネルである。マレーシアのテロ資金供与リスク評価において、銀行セクターと並び中程度のネットリスクに分類される主要な送金手段である。

- 物理的な現金の密輸

  広大な海岸線や多数の入国地点といった地理的脆弱性を悪用し、物理的に国境を越えて現金を運び出す方法である。汚職や密輸に関連する資金移動として指摘されている。

- 専門的イネブラーを介した資金の構造化

  弁護士、会社秘書役、信託会社などの専門職を介し、実質的支配者を隠蔽するための複雑な法人構造を利用して資金を移動・隠蔽する方法である。高度な資金洗浄・テロ資金供与の手段として注視されている。

- ミュール口座の悪用

  第三者の口座（マネーミュール）を利用し、資金の真の出所や最終的な送金先を不明確にすることで、法執行機関による追跡を困難にする手法である。詐欺などの高リ

スク犯罪で顕著な手法だが、資金移動のリスク・ドライバーとして位置づけられている。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

マレーシアにおいて、テロ資金供与の主体が資金獲得やテロ組織への資金提供を行うにあたり、オンラインプラットフォームがインフラとして悪用されていることが確認されている。

- オンラインプラットフォーム

  詐欺などの高リスク犯罪において、勧誘やプロパガンダ、資金獲得の場として広く悪用されている。特にサイバーを媒介とした詐欺等の犯罪において、これらのデジタルプラットフォームが活動の主要な基盤となっている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

マレーシアにおいて、テロ資金供与の脆弱性を生み出している国・地域に固有の地理的条件として、以下の要素が確認されている。

- 地理的条件・脆弱性（黄金の三角地帯への近接性）

  マレーシアは「黄金の三角地帯（Golden Triangle)」[11]に地理的に近接している。このため、薬物密輸の供給、消費、及び中継地としての脆弱性を有しており、これが国内の主要犯罪（薬物密輸：固有リスク「高」）の背景となっている。また、地理的脆弱性として、広大な海岸線と多数の入国地点を有しており、物理的な現金の密輸が行われやすい物理的・地理的構造にあり、貨物の積替えを悪用した追跡回避が行われやすい点も脆弱性として指摘されている。

②-2-1.テロ資金供与を防止するための法的枠組み

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-3-1.金融当局等の監督・アウトリーチ

今回の調査対象文献からは、本項目に関する具体的な情報は確認されなかったが、当局による継続的な監督努力と執行アクションが、特定セクターのリスク低減に寄与したことが

[11] 東南アジアのタイ、ミャンマー、ラオスの３国の国境が接するメコン川流域の山岳地帯であり、かつては世界最大級のアヘン・ヘロイン生産地として知られていた。現在は各国による取締の強化や代替開発によりアヘン生産は減少したものの、ミャンマー北東部を中心に覚醒剤（メタンフェタミン）などの合成薬物の製造・密輸が続いている。また、周辺地域では観光やカジノ等の合法的な経済活動も行われている。

確認できた。特に送金サービス（MSB）セクターにおいては、監督能力の共有や連携を通じた強化された監督活動が実施された結果、セクター全体の管理態勢が改善されている。また、官民連携プラットフォームの活用により、法執行機関（LEAs）との情報共有が可能となっている。これに伴い、テロ資金供与に関する疑わしい取引届出（STRs）の質及び量の向上が図られている。

②-3-2.NPO の規制、監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

- 預金取扱金融機関（銀行）

  テロ資金供与リスクは「高」から「中程度に高い」へと低下した。この要因として、高リスク国からの顧客の減少やテロ資金供与に係る捜査の減少、情報収集の進展が挙げられる。また、官民連携によるテロ資金供与対策プラットフォームの確立により、疑わしい取引の届出の質と量が向上している。

- 資金移動業者

  不法な収益を国外へ移動させる主要なチャネルの一つとして位置づけられており、銀行セクターと並んで中程度のネットリスクに分類されている。監督能力の共有（連携）を通じて強化された監督活動が実施された結果、セクター全体の管理態勢の改善が見られる。

- 暗号資産

  デジタル資産交換業者（DAX）は「資本市場仲介者（CMIs)」に含まれ、固有リスクは「中程度 Medium)」と評価されている。

- 前払式支払手段(プリペイド型決済サービス)

  指定決済手段発行者（DPI Issuers）のテロ資金供与リスクは、預金取扱金融機関と同様に、前回の「高」から「中程度に高い」へ低下した。これは、監督能力の共有等によって業界全体の管理措置が改善され、監督活動が強化されたことによるものとされている。

- 保険

  保険のテロ資金供与リスクは「中程度」と評価されている。なお、保険仲立人（Intermediaries）のテロ資金供与（及びマネロン）リスクは、監督活動の改善により前回の「中程度に高い」から「中程度」へ低下した。

- 証券

証券会社等を含む資本市場仲介者（CMIs）のテロ資金供与リスクは「中程度」と評価されている。

- 金銭貸付

  貸金業のテロ資金供与リスクは「低」と評価されている。

- 不動産

  不動産業のテロ資金供与リスクは「低」と評価されている。

- 貴金属

  テロ資金供与リスクは「高」から「中程度に高い」へと低下した。この要因として、高リスク国からの顧客の減少が挙げられる。

- ファイナンスリース

  リース業のテロ資金供与リスクは「低」と評価されている。

- 法律・会計関係サービス（TCSP）

  弁護士、会社秘書役、信託会社などの専門的イネブラーのテロ資金供与リスクは「中程度」と評価されている。これらのセクターは、実質的支配者を隠蔽するための複雑な法人構造を利用した資金移動や隠蔽に関与するリスクがあり、高度なテロ資金供与の手段として注視されている。

- カジノ

  カジノのテロ資金供与リスクは「中程度」と評価されている。

②-4-2.NPO の活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

今回の評価期間中、マレーシアにおけるテロ及びテロ資金供与のリスクは低下したものの、テロ組織は活動環境の変化に適応する能力を有しており、その脅威は決して固定的ではないため、テロの展望については引き続き「慎重な」見通しが維持されている。また、長期化する国際紛争が地域へのテロやテロ資金供与の波及を誘発する潜在的な要因となり得ると分析されている。さらに、グローバルな相互依存関係の深化やマレーシア経済の開放性により、外国での前提犯罪に由来するマネー・ローンダリングの中継地、あるいは目的地となる可能性が高まる恐れがある。こうした背景から、法執行機関（LEA）、金融情報ユニット（FIU）、及び報告義務機関は、テロ及びテロ資金供与リスクに対して引き続き警戒を怠らないようにすべきであるとされている。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

（11）国際連合

①脅威

①-1-1.テロ組織、テロリスト

（制裁対象組織）

- アルカイダ

  調査対象文献における制裁対象。傘下組織は高い自律性を保ちながら活動しており、アフリカやシリアで支配地域を拡大し、活動資金の調達や勧誘を強化している。ガザ紛争を政治的に利用し、ローンアクターによる攻撃を扇動している。アラビア半島のアルカイダ（AQAP）は資金調達のためのクラウドファンディングを展開している。

- ISIL（Da’esh）

  調査対象文献における制裁対象。イスラム国西アフリカ州（ISWAP）、イスラム国大サハラ支部（ISGS）、ISIL 東南アジア（ISIL-SEA）などの分派が存在する。中東での活動は軍事的圧力により制約されている一方、作戦の重点をアフリカへと移している。

（関連組織）

- イスラムとムスリムの支持者（JNIM）

  サヘル地域で支配地域を拡大しており、ドローンや即席爆発装置を用いた高度な攻撃能力を保有している。

- ボコ・ハラム

  主にナイジェリアで活動する過激派集団。ISWAP が支配していた地域を奪取するなどの動きは見られるが、既存の勢力圏を超えて活動を拡大させる能力は限定的であると分析されている。

- アル・シャバブ

  ソマリア南部・中部で強固な戦闘力を維持しており、戦闘員数は 10,000～18,000 人と推定される。作戦資金の約 4 分の 1 を武器調達に充てており、イエメンのフーシ派やアラビア半島のアルカイダ（AQAP）との武器取引や訓練を通じた協力関係が報告されている。

- 東トルキスタン・イスラム運動（ETIM / TIP）

  シリアにおいて、前政権を打倒した HTS 連合の一部として活動する。「東トルキスタン独立」を支持する特定の民族グループから武器調達のための資金援助を受けているほか、シリア国内で中国民間人への嫌がらせや脅迫を行っている。

①-1-2.テロ組織、テロリストの支援者やそれらの者に同調する個人、集団

- ローンウルフ

ISIL は、様々なメディアを通じて定期的に多言語で発信を行っている。週刊誌「アル＝ナバ」では、外交問題からシャリーア法に至るまで幅広い議題を論じている。単独犯による攻撃を実行するよう読者に繰り返し呼びかけ、その実践的な手引きを提供している。その他の組織も、主に過激化・勧誘目的で人工知能を利用し、プロパガンダの拡散・強化を図っている。

①-2-1.(テロ資金供与の主体による)資金獲得のための活動

- 徴収・略奪

  アルカイダ、ISIL 及びその傘下組織は、支配地域において「ザカート（喜捨)」の名目での徴収、地元住民や企業に対する課税、及び恐喝を通じて資金を確保している。

- 誘拐・身代金要求

  西アフリカの ISGS は、直接的又は現地の犯罪ネットワークを通じて誘拐を実行し、身代金を獲得することで、戦闘員の勧誘や武装強化を図っている。ソマリアの ISIL は、軍事的圧力により企業からの資金集めが困難になったことを受け、50 ドルから 100 ドル程度の少額な身代金を即座に要求する誘拐へと手法を転換している。

①-2-2.(テロ資金供与の主体によるテロ組織等への)資金供与の方法

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

①-2-3.(テロ資金供与の主体による)資金獲得や資金提供を支える制度・基盤、プラットフォーム等

- クラウドファンディング

  AQAP は、ガザ・イスラエル紛争などの国際情勢を政治的に利用し、組織の資金補充を目的とした一連のクラウドファンディング・キャンペーンを展開している。

- ハワラ

  伝統的なハワラのほか、「クラウド・ハワラ」と呼ばれる、送金データをクラウド上に保存して物理的な証拠を残さないシステムや、パスワードを入力して両替所から現金を引き出す「セーフ・ドロップ・ボックス（Safe drop boxes)」といった新手法が採用されている。

- 暗号資産プラットフォーム

  ISIL-K は、Monero、KuCoin、MEXC、Huobi、Totalcoin といった多様な暗号資産・取引所を利用しており、その使用方法はますます複雑化している。また、異なる暗号資産間の交換を容易にする「Cash Now」アプリなどのツールが、工作員への現金支給を支える基盤となっている。

- メッセージングアプリ

Telegram 内の決済アプリ（@wallet）は、本人確認（KYC）プロセスが不要であるため、ISIL によって頻繁に利用されている。

②脆弱性

②-1-1.国・地域に固有の文化的背景や社会・経済構造

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-2-1.テロ資金供与を防止するための法的枠組み

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-3-1.金融当局等の監督・アウトリーチ

制裁措置の実施状況として、「渡航禁止」「資産凍結」「武器禁輸」に係る状況が報告されている。「渡航禁止」については、報告期間中、指定された個人の渡航に関する報告が19 件あり、全てアル・シャラー及びアナス・ハッタブの渡航に関するものとされている。「資産凍結」については、報告期間中の資産凍結免除要請の件数（4 件）のみが報告されている。「武器禁輸」については、ISIL とアルカイダの活動が確認されている。具体的には、両組織はともに、武装ドローンを含む無人航空機の専門家を勧誘することで無人航空機の専門知識を得ている。小型無人航空機は広く入手可能かつ安価であり、アルカイダと ISIL はネットワーク間で技術的専門知識を共有し、世界的な無人航空機の使用を可能にしている。

②-3-2.NPO の規制、監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-3-3.その他セクターの規制当局の監督・アウトリーチ

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-1.金融機関等(DNFBPs 含)の活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-2.NPO の活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

②-4-3.その他セクターの活動・対応

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③発生可能性と結果

③-1-1.テロ資金供与の脅威が顕在化する可能性

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

③-2-1.テロ資金供与の脅威が顕在化した場合に生じ得る影響や被害

今回の調査対象文献からは、本項目に関する有意な情報は確認されなかった。

４．まとめ

①脅威

①-1.テロ資金供与の主体

A）グローバルな脅威と脆弱性の共通性

全ての調査対象国において、ISIL 及びアルカイダやそれらの関連組織がテロ資金供与の主要な脅威として特定されている。また、米国・英国・カナダ・オーストラリア等では、極右過激主義が主要な国内脅威として台頭していると評価されている。

また、オンラインで過激化した個人、海外のテロ組織を支えるディアスポラ（移住者コミュニティ）についても、テロリストの支援者やそれらの者に同調する個人、集団として、テロ資金供与の脅威と捉えられている。

これらの脅威は、各国で程度の差はあるものの、グローバル化した社会・金融システムのもと、匿名性を保持したコミュニケーションと迅速な資金移動が容易になった環境の中で世界共通の脅威と捉えられており、日本においても同様のリスクが存在するものと考えられる。

B）日本固有の文脈への適用可能性

日本固有の団体として「オウム真理教（主要３団体）」等を考慮する必要がある。「オウム真理教（主要３団体）」等が SNS 等のオンラインツールを活用して、広宣・普及活動を行っている実態もみられており、日本においても、オンラインでの過激化に係る課題は存在すると考えられる。

また、過去のテロ事件の主体による影響力が現在にも残置している現状から、「オウム真理教（主要３団体）」等への同調を重点的に評価する必要があると考えられる。

①-2.テロ資金供与のための活動

A）グローバルな脅威と脆弱性の共通性

① 資金獲得活動における共通リスク

テロ資金の調達元として、世界各国の間で以下のような手法が共通して悪用されている。

- 合法的な収益（自己資金）の悪用

  特定の組織に属さない単独犯や同調者による、給与所得、預貯金、ローン、年金、公的給付金などの自己資金の流用が脅威となっている。これらは少額かつ日常的な取引に紛れるため、金融システム上での事前検知が極めて困難である。

- オンラインを通じた寄付

  人道支援や慈善活動を装い、SNS やクラウドファンディングを利用して世界中の不特定多数から小口の寄付を集める手法が各国で定着している。

- 犯罪収益の獲得と合法的ビジネスへの混蔵

詐欺、薬物取引、密輸などの違法な犯罪活動により収益を獲得し、不動産や飲食業等の合法的な事業の収益に混蔵させ隠蔽する手法が確認されている。

② 資金供与手法における共通リスク

調達した資金を高リスク地域やテロ組織へと移転させる手段として、各国で共通する脆弱性が確認されている。

- 銀行システム及び送金業者（MSB/MVTS）の悪用

  依然として主要な資金移動のチャネルであり、少額に分割した送金や、第三者を介在させて最終的な受益者を隠蔽する手法が悪用されている。

- 新興決済手段（暗号資産等）の悪用

  匿名性の高い暗号資産やステーブルコインが、国境を越えた迅速な価値移転手段として各国で利用拡大・警戒されている。

- 非公式資金移転（ハワラ等）と現金の物理的移転

  ハワラのような銀行システム外の非公式送金網や、国境を越えた物理的な現金の密輸、旅行用プリペイドカードの持ち出しなども、監視を回避手法として機能している。

③資金ネットワークを支える制度・基盤における共通リスク

テロ資金の獲得・移動を容易にするインフラとして、世界的に以下の基盤が悪用されている。

- オンライン・デジタルエコシステムの悪用

  SNS、暗号化メッセージングアプリ（Telegram 等）、クラウドファンディングサイト等が連携し、過激思想の拡散から小口寄付の収集、匿名での資金移動指示までを完結させる「オンライン資金調達エコシステム」が各国で脅威となっている。

- 複雑な法人構造と専門家の利用

  フロント企業やシェルカンパニー等を利用して実質的支配者を隠蔽し、これを弁護士や会計士、会社設立代行業者（TCSP）などの専門家（イネブラー）が支援する構造が各国で利用されている。

- 非営利団体（NPO）の悪用と偽装 NPO

  設立の容易さや社会的な信頼といった制度的・文化的脆弱性を突き、最初からテロ支援を目的とした「偽装 NPO」を立ち上げる事案や、正当な NPO の資金が意図せずテロ組織に流用されるリスクがある。

B）日本固有の文脈への適用可能性

日本固有の文脈へ適用可能な脅威として、諸外国でも主要な脅威となっている「合法的な

自己資金」や「オンライン・デジタルエコシステムの悪用」が挙げられる。特に、自己資金を少額に分割して送金する手口は、日常的な経済活動に埋没しやすく、検知と見極めが容易ではない。送金の手法として、高リスク国へ直接送金せず、トルコなど日本との取引が一定規模存在する周辺国を経由する事例も見られるため、日本においても送金経路の分析が重要と考えられる。また、クラウドファンディング、暗号資産を組み合わせた資金獲得や匿名送金の手法は、IT インフラが普及している日本においても脅威となりうる。IT の活用に関しては、「オンライン行事」の配信を通じた資金集めや、日本国内に居住する外国人をターゲットとした、外国語によるプロパガンダの拡散などをも考慮する必要があると考えられる。

一方で、欧米やアジア諸国で主要な脆弱性となっている、ハワラ等の地下銀行ネットワークや陸路等を用いた大規模な現金密輸に関しては、日本は島国であり、特定の移民コミュニティ（ディアスポラ等）に根ざした大規模な非公式金融インフラが諸外国ほど存在しないため、資金の供給源としてのリスクは存在するものの、これらの手法を通じたハブとしての脆弱性は限定的と考えられる。

また、日本特有の産業構造を背景とした「中古車」や「船舶」等の特定製品の無許可輸出・需要が、テロ組織の物資・資金源となるリスクを考慮する必要がある。

②脆弱性

②-1.文化・経済・社会・産業構造

A）グローバルな脅威と脆弱性の共通性

当該観点における脆弱性については、今回の調査対象国において、主に以下の 4 つの観点から分析が行われていた。

① 国際金融・貿易センターとしての開かれた経済環境や、膨大な取引量に起因する脆弱性：米国、英国、香港
② 高い現金依存度に起因する脆弱性：カナダ、ドイツ
③ 高リスク地域（紛争地等）との社会的・経済的結びつき（貿易関係、国内における当該地域出身のディアスポラの存在等）：カナダ、ドイツ、オーストラリア、香港
④ 広大な海岸線など、複数の入国地点の存在：マレーシア

これらは、各国独自の地理的・地政学的な状況、経済・産業構造の特性、あるいは歴史的・社会的な背景に起因するものであり、当該観点で、世界のあらゆる国・地域に共通の脆弱性は存在しないと考えられる。

B）日本固有の文脈への適用可能性

日本は、世界的に重要な金融・貿易の拠点であり、膨大な取引量を背景とした潜在的なリスクを有している。しかし、テロ資金供与に係る脆弱性の観点からは、以下の要因により他国の主要ハブとは異なる特性を有していると考えられる。

● 地理的・社会的要因によるリスクの抑制

紛争地域との地理的な隔絶に加え、当該地域との歴史的なビジネス及び人的結びつきが他国と比較して限定的である。このため、高リスク地域向けの送金需要や、ディアスポラ（移住先の同胞コミュニティ）を介した資金流入のリスクが、相対的に低水準に留まっていると考えられる。

● 非公式金融ネットワークの不在

中東や南アジア等の地域で生活に根付いているハワラ等の伝統的な非公式資金移動サービスが、国内において組織的なインフラとして殆ど存在しないと考えられる。

大規模な経済活動の中にテロ関連資金を紛れ込ませる等の方法から、海外への「資金供給源」として利用されるリスクは存在するものの、上述の地理的・社会的近接性や非公式ネットワークの普及度という観点に基づけば、ハブとしての脆弱性は限定的であると考えられる。

一方で、日本の経済・産業構造においては、武器に転用可能な製造物や中古車流通のルートの広範さとその透明性確保の難しさが、固有の脆弱性となり得ると考えられる。

②-2.法・制度

A）グローバルな脅威と脆弱性の共通性

各国の法制度を俯瞰すると、国境を越える資金移動と、技術革新に伴う新たなリスクへの対応が共通の課題となっている。

① 正規の金融システム外における資金移動の規制

多くの国で、正規の金融機関を介さない資金移動が最大の脆弱性と認識されている。

● 現金の越境規制

米国では、匿名性が高く電子記録が残らない現金による国境を越えた移動が、監視回避の主要手段となっている。日本、英国、ニュージーランド、香港などは、一定額以上の現金持ち出し・持ち込みに対して申告義務を課し、水際での捕捉を強化している。

● 非公式送金の規制

ハワラ等の公的な認可を受けない送金サービスがテロ資金の温床となるリスクが指摘されており、各国において厳格なライセンス管理と監督が実施されている。

② 技術革新への適応

技術の変化に対し、法執行機関の権限を拡大する動きが加速している。

● 暗号資産の押収

技術変化に伴い、暗号資産がテロ資金の隠匿や移動に利用されるリスクが高まっ

ており、迅速な押収・回収が課題となっている。

③ 法人の透明性確保

● 実質的支配者の透明性

法人の実質的支配者が不透明な場合、テロ資金の隠匿先として悪用されるリスクがある。例えば英国では、実質的支配者に関する登録簿の情報の一部を一般公開している。

B）日本固有の文脈への適用可能性

A）グローバルな脅威と脆弱性の共通性に記載の課題については日本においても同様であるため、引き続き FATF や各国の法規制等の動向の注視が必要と考えられる。

②-3.監督、アウトリーチ

A）グローバルな脅威と脆弱性の共通性

調査対象国・地域では、以下の 3 つのアウトリーチが共通のスタンダードとして確立されている。

① リスクベース・アプローチの徹底

全ての国・地域において、一律の規制ではなく、リスクの高いセクターや地域にリソースを重点的に配分するリスクベースの監督が主流となっている。

● 高リスクセクターへの集中

銀行、送金業者（MSB/MVTS）、暗号資産交換業者（VASP）に対し、重点的なモニタリングと指導が実施されている。

● ガイダンスの提供

当局が民間部門に対し、テロ資金供与が疑われる取引の特徴をまとめたガイダンスを提示し、検知能力の向上を図っている。

② 多層的な官民連携の構築

情報の非対称性を解消するため、当局と民間部門がリアルタイムに近い形で情報を共有する枠組みが強化されている。

● 官民情報共有プラットフォーム

英国の JMLIT やオーストラリアの FINTEL Alliance のように、法執行機関と主要金融機関が直接対話する場が設けられている。

● 迅速な周知体制

制裁対象者の指定情報を電子メールやウェブサイトを通じて即時に周知する体制が一般的である。

③ NPO セクターの保護と金融システムへのアクセス維持

NPO がテロ資金供与に悪用されるのを防ぐと同時に、善意の活動を阻害しないためのバランスが重視されている。

- ガイダンスによる自律的統制の促進

  各国は NPO 向けに専用のツールキットやリスク管理ガイドラインを提供している。

- デリスキリング対策

  NPO が正規の銀行システムから排除され、不透明なチャネル（ハワラ等）へ流れることを防ぐためのアウトリーチが行われている。

B）日本固有の文脈への適用可能性

- 新興プラットフォームへの対応

  カナダではクラウドファンディングを規制対象に追加している。日本でもオンラインでの資金調達が普及していることから、これらのプラットフォームへのアウトリーチや対策が必要と考えられる。

- 士業（DNFBPs）への監督強化

  英国の OPBAS のように、弁護士や会計士等の専門職団体に対する監督基準を高度化・統一する手法は、日本の特定非金融業者（DNFBPs）への監督の実効性を高める参考になると考えられる。

- 高リスク環境下の NPO 支援

  米国（USAID）や英国（TSG）のような紛争地域で活動する NPO に対する具体的な指導は、海外活動を行う日本の NPO に対するアウトリーチの参考となり得ると考えられる。

②-4.関連セクターの活動・対応

A）グローバルな脅威と脆弱性の共通性

調査対象である各国・地域では、主にテロ資金供与の少額化や多頻度化による、膨大な顧客基盤や取引数がもたらす検知の難しさが課題として認識されている。また、疑わしい取引に係る届出義務の有無など、国・地域ごとに規制の強度・範囲が異なることに起因する脆弱性が共通する。

- 金融機関及び DNFBPs における取組と課題

  膨大な顧客基盤や取引数と、それによるテロ資金供与リスクの高さに応じた IT システムや内部管理体制の構築が進んでいる。しかしながら、自らの顧客に対するリスクを低く評価する傾向があることが脆弱性として指摘されている。

  また、官民連携の枠組みの強化等の施策により、疑わしい取引の届出率の改善が進んでいる。一方で、金融機関の中でもリスク評価が低い業態や DNFBPs 等の一部のセクターにおいては、依然として疑わしい取引の届出率が低迷しているという課題

がある。また、一部の国・地域においては、疑わしい取引の届出義務を課されていないセクターが存在するため、テロ資金供与リスクの特定・把握が困難であるという課題も存在する。

- NPO セクターに関する取組と課題

  NPO におけるリスク管理体制強化や、資金使途（最終受益者）の透明化、提携パートナーや受益者に対するデューデリジェンスの実施等の促進を図る制度が整備されつつある一方で、高リスク国の近隣で活動する NPO がテロ資金供与に悪用される脆弱性があることは共通して認識されている。また、慈善団体を装った偽の NPO などにより、意図せずテロ資金供与に加担してしまう脆弱性や、金融機関がデリスキングを避けることによる脆弱性についても、調査対象である各国・地域の多くで共通している。

- その他セクターにおける取組と課題

  SNS 企業による不適切な投稿に対する取り締まりが強化されている一方で、オンラインゲームプラットフォームを利用した新しい連絡・資金移転の手法や、クラウドファンディング等の匿名性の高い資金調達方法の普及により、小口かつ多数の取引によるテロ資金供与のリスクが高まっている。

B）日本固有の文脈への適用可能性

日本国内においてもオンラインによる非対面取引の拡大や、暗号資産等の新技術の普及が見られる現状を考慮すると、日本独自のリスク指標を調整し、高度化する必要性があると考えられる。特に、日本国内においても SNS を通じた個人に対する勧誘活動やプロパガンダの拡散が行われている実態が確認されているため、プラットフォーム企業に対する自主的な対応の強化に関する更なる働きかけが必要である。また、日本の NPO も、関連省庁のガイダンス等を活用し、リスクベースの推進を行う余地がある。

また、日本国内においても金融機関と監督省庁間での官民連携の取組が拡充されつつある。したがって、先進的な諸外国の取組（特に英国等）を参考にした、より高度な情報連携及び情報分析サービスの提供や、民間事業者同士の情報連携の枠組みの整備等も見据えた制度設計を検討することで、日本におけるテロ資金供与対策の更なる高度化の余地がある。

③発生可能性と結果

③-1.発生可能性

A）グローバルな脅威と脆弱性の共通性

諸外国におけるテロ資金供与の発生可能性は、伝統的手法と新技術の結合、及び地政学的な変化により複雑化しており、以下のトレンドが国境を越えた共通のリスクとして特定されている。

- 合法的な資金を利用した単独犯の脅威の増加

米国、英国、オーストラリア、ニュージーランドの評価において共通して、高度に組織化されたテロ攻撃から、特定の組織に属さない単独犯や小規模グループによる攻撃へと脅威の性質が移行している。これらの実行犯は、自身の給与所得、ローン、福祉給付金等の「合法的な自己資金」を原資とした少額の資金移動をする特徴がある。このようなテロ組織との関係性が見えにくい協力者等による小口の資金移動は、既存の金融監視網において検知が容易ではなく、脅威が顕在化する可能性が高まっている。

- デジタル・新技術の悪用

  SNS、クラウドファンディング等のオンラインの資金調達エコシステムや暗号資産取引の普及により、テロ資金供与の手法がより分散化・匿名化している。これにより、国境を越えた小口資金の迅速な移動が容易になり、当局の規制や監視をすり抜けて資金調達の脅威が顕在化する可能性が高まっている。

- イデオロギーの多様化（極右・白人至上主義の台頭）

  従来のイスラム過激派による脅威が持続する一方で、米国、英国、オーストラリアを中心に、人種的・思想的動機に基づく暴力的な過激主義（極右・白人至上主義等）が台頭しており、新たなコミュニティから突発的に脅威が顕在化するリスクが拡大している。

- テロ資金の「供給源」としてのリスクの存在

  直接的なテロ攻撃の発生可能性が低いと評価される国（オーストラリア、ニュージーランド、マレーシア等）であっても、海外のテロ組織や紛争地域に対するテロ資金の「供給源」として機能してしまう脅威が存在している。特に、人道支援を装った偽装募金や意図しない資金流出、あるいは長期化する国際紛争の波及による顕在化が懸念されている。

B）日本固有の文脈への適用可能性

日本国内においてはテロ資金供与に関する法令上の措置等が整備されており、他国と比較してテロ資金供与リスクの発生可能性は相対的に低いと評価されている状況にある。しかしながら、諸外国にて顕在化している「合法的な自己資金を利用した単独犯の脅威」や「デジタル・新技術の悪用」は、日本においても顕在化する可能性はゼロではないと考えられる。

また、世界有数の国際金融・貿易センターである日本は、国内におけるテロ資金供与のリスクが発生可能性は低くとも、海外へのマネー・ローンダリングやテロ資金の「供給源」や「中継地」として意図せず悪用される可能性が考えられる。

なお、欧米や豪州で確認された「極右主義の台頭」については、日本の人口動態や社会的背景を踏まえると、直ちに同水準の発生可能性を見込む必要性は低いと考えられる。

③-2.結果

A）グローバルな脅威と脆弱性の共通性

諸外国におけるテロ資金供与の結果の発生に対する評価は、単なる物理的な攻撃・破壊活動による人命に対する危害や、社会・経済的な損失の発生にとどまらず、国家のレピュテーションや金融システムの安定性に対する毀損も射程に含めている。調査対象の国・地域における評価について、大きく分けて以下の 3 点に整理することができる。

- 国家安全保障に対する重大な脅威

  テロ資金供与リスクが顕在化しテロ事件が発生した場合、人命に対する危害や、重要なインフラ設備の破壊といった直接的な影響が生じ得る。これらは国家安全保障の根幹に関わる脅威である。少額な資金に基づく攻撃であっても、ひとたびテロ事件が発生すれば甚大な被害が発生する可能性がある。例えば数カ月間にわたって重要なインフラ設備の停止が生じた場合、国民の生活における安全性が脅かされるだけでなく、設備の復旧作業のために巨額の費用がかかるなどの二次被害も想定される。

  したがって、テロ資金供与自体を「被害者のいない犯罪」ではなく、凶悪な行為の手段を提供するものとして位置づけ、大規模な社会の混乱を防ぐ必要がある。

- 経済システムへの信頼低下

  日常的に利用する銀行や資金移動サービス等の金融・経済システムを通じた資金供与によってテロ事件が発生した場合、金融機関等の内部管理体制や監督機関の機能、及び権威に対する信頼が低下するおそれがある。

  それに伴い、国内外からの投資の減少や、不法な資本流入及び正当な資本流出の増加が引き起こされるなど、正常な経済活動に支障をきたすおそれがある。

- 社会の不安定化

  暴力的な手段による行動やテロ組織等によるプロパガンダや扇動は、社会に対する不安や混乱を招く。

B）日本固有の文脈への適用可能性

日本国内におけるテロ資金供与のリスクは、諸外国と比べて低く評価されているものの、テロ資金供与によるリスクが顕在化した場合は、諸外国と同様に社会心理的な影響や国際的な信用の失墜が懸念される。

日本という国家が安全性や信頼性の面で国内外から高い評価を維持していることを考慮すると、テロ事件に起因する日本社会の治安低下による混乱や、警察・規制当局及び金融機関等に対する信用の失墜は、重大かつ回復が困難な脅威になり得る。

以上