# FATF 第 4 次対日審査結果報告書

# （IO.4 該当箇所）

2021 年 8 月

（仮訳）

## 概要

### *主な評価結果*

大規模銀行（より高いリスクを有する金融機関として認識されているグローバルなシステム上重要な銀行（GSIB）等）及び一定数の資金移動業者を含む一定数の金融機関は、マネロン・テロ資金供与リスクについて適切な理解を有している。その他の金融機関においては、自らのマネロン・テロ資金供与リスクの理解が限定的である。金融機関がマネロン・テロ資金供与リスクについて限定的な理解しか有していない場合、金融機関のリスクベース・アプローチ（以下、RBA）の適用に直接的な影響を及ぼす。このような金融機関は、最近導入・変更された AML/CFT に係る義務について十分な理解を有しておらず、これらの新しい義務を履行するための明確な期限を設定していない。指定非金融事業者及び職業専門家（以下、DNFBPs）は、マネロン・テロ資金供与リスクや AML/CFT に係る義務について低いレベルの理解しか有していない。暗号資産交換業者は、暗号資産取引に関連する犯罪リスクについて一般的な知識を有し、基本的な AML/CFT に係る義務を実施している。疑わしい取引の届出の総件数（年ベース）は増加傾向にあるところ、疑わしい取引の届出の大部分は金融分野からのものであり、暗号資産交換業者の届出の実績も良いが、全体的にみて、疑わしい取引の届出は、基本的な類型や疑わしい取引の参考事例を参照して提出されている傾向がある。また、特定のマネロン・テロ資金供与リスクに直面している一部の DNFBPs を含め、全ての DNFBPs が、疑わしい取引の届出義務の対象になっているわけではない。

## *遵守状況と有効性の全体的な水準*

### *予防的措置（Chapter 5; IO.4；R.9-23）*

大規模銀行（より高いリスクを有するとされているGSIB等）及び一定数の資金移動業者を含む一定数の金融機関は、マネロン・テロ資金供与リスクについて適切な理解を有している。その他の金融機関は、自らのマネロン・テロ資金供与リスクの理解がまだ限定的である。一定数の金融機関は、自らのリスク評価を開始しているが、その他の金融機関は、リスクに基づいた低減措置を適用していない。これらの金融機関は、継続的顧客管理、取引モニタリング、実質的支配者の確認・検証等の、最近導入・変更された義務について、十分な理解を有していない。これらの金融機関は、AML/CFTの枠組みや取組を強化する必要があるとの一般的な認識は有しているが、新たな義務を履行するための明確な期限は設定していない。

年間の疑わしい取引の届出の総件数は増加傾向にある。届出の大部分は金融分野によるもので、三分の一は大規模銀行によるものであるが、FIU（JAFIC）のガイダンスに基づく基本的な類型や疑わしい取引の参考事例を参照したものである。

暗号資産交換業者は、2017年以降、登録義務が課されており、AML/CFT目的で規制・監督されている。暗号資産交換業者は、暗号資産取引に関連する犯罪のリスクについて一般的な知識を有する。テロ資金供与リスクの理解は概して限定的である。 暗号資産交換業者は、基本的なAML/CFTに係る義務を実施する傾向があるが、一般に、自らのリスク応じた低減措置や、厳格な顧客管理措置（EDD）又は特定の顧客管理措置（CDD）の適用について、この業種に特有なリスクに則した方針を定めていない。一定数の暗号資産交換業者は、顧客の本人確認のために厳格な措置を適用している。

暗号資産交換業者の疑わしい取引の届出は、2017年以降顕著に増加しているが、これは、主にFIU（JAFIC）と日本暗号資産取引業協会（JVCEA）が共同で行った一連の啓発活動やガイダンスの結果である。

DNFBPsは、マネロン・テロ資金供与リスクについて、低いレベルの理解しか有していないが、北朝鮮に関連する業務のリスクや、最近の事案から金の密輸に係るリスクについては、一般的に認識している。DNFBPsは、主に顧客の本人確認

及び顧客が暴力団の構成員・関係者でない旨の確認といった、基本的な AML/CFT に係る予防的措置の適用に留まっている。また、全ての DNFBPs が、実質的支配者の概念に関する明確な理解があるわけではない。制裁者リストとの照合や高リスク国リストとの照合は、主に顧客が通常の取引形態や属性から逸脱した場合のみ実施されている。

全ての DNFBPs が、疑わしい取引の届出義務の対象になっているわけではない。届出義務が課されている DNFBP セクターにおいて、ある程度のマネロン・テロ資金供与リスクに直面していると認識された分野も含め、届出のレベルは低い。

### *優先して取り組むべき行動*

日本は、以下に取り組むべきである。

金融機関、暗号資産交換業者、DNFBPs が AML/CFT に係る義務を理解し、適時かつ効果的な方法でこれらの義務を導入・実施するようにする。これらにおいては、事業者ごとのリスク評価の導入・実施、リスクベースでの継続的な顧客管理、取引のモニタリング、資産凍結措置の実施、実質的支配者情報の収集と保持を優先する。

# 第５章　予防的措置

## 5.1 主な評価結果及び勧告事項

### *主な評価結果*

大規模銀行（より高いリスクを有するとされている GSIB 等）及び一定数の資金移動業者を含む一定数の金融機関は、マネロン・テロ資金供与リスクについて適切な理解を有している。その他の金融機関は、自らのマネロン・テロ資金供与リスクの理解がまだ限定的である。一般に、これらの金融機関は、主に犯罪収益移転危険度調査書（以下、NRA）の評価に基づく、監督当局が指摘するリスクカテゴリーについて、例えこれらのリスクが自らの業務に関連しない場合であっても参照している。金融機関は、現金取引を介するもののほかは、前提犯罪とマネロンとの関連性や、犯罪収益がどのように銀行システムに侵入するかについて、深く理解していない。

金融機関がマネロン・テロ資金供与リスクについて限定的な理解しか有していない場合、金融機関の RBA の適用に直接的な影響を及ぼす。一定数の金融機関は、自らのリスク評価や、認識されたリスクに応じた低減措置を適用している。その他の金融機関は画一的な低減措置を適用し、顧客の本人確認、取引確認及び疑わしい取引の届出以上の措置は実施していない。

金融機関は、紛争地域への近接性に基づき、テロ資金供与リスクを理解しているようであり、金融セクターにおける他の類型のテロ資金供与については、報告も調査もされていない可能性を示している。金融機関は、イランや北朝鮮等のリスクの高い国々と関連のある取引については、特別な注意を払っている。

金融庁による 2018 年の AML/CFT に関する強制力のあるガイドラインは、金融機関による AML/CFT に係る義務の理解や履行を促進する一里塚であった。しかしながら、全ての金融機関について、自らのリスクに応じた効果的な AML/CFT 管理態勢（AML/CFT systems）を確保するため、この基準のレベルは引き上げられるべきである。

一定程度の金融機関は、基本的な AML/CFT に係る概念、とりわけ、実質的支配者の確認・検証、継続的顧客管理等の、最近導入・変更された義務について、まだ明確かつ一律の理解を有していない。基本的な取引モニタリングシステムは一定数の金融機関で既にある程度導入されており、取引スクリーニングシステムはほとんどの金融機関で導入されているが、どちらのシステムもその効果は限定的である。金融機関は、法律上・規制上・監督上の新たな義務を履行するために AML/CFT の枠組みや取組みを高度化する必要があるとの一般的な認識を有している。しかしながら、監督当局は、直接、対話を通じて監督している金融機関のみに対応期限を課している。その他の金融機関は、AML/CFT に係る義務の履行について独自の期限を定めているが、期限が延長される傾向にある。したがって、金融機関の顧客管理（CDD）の適時の改善や十分な AML/CFT に係る低減措置の適用に、深刻な懸念がある。

金融機関は、基本的な顧客の情報を収集しているが、このために金融機関の顧客に関する知識が限られており、かつ、この情報は通常更新されていない。金融機関は、顧客の特性に基づいた顧客リスク格付も、顧客属性等と取引記録との結び付けも行っていない。一定数の金融機関は、最近、新規顧客について完全な CDD を最近開始したところである。また、口座の売買や不正利用の蔓延は、金融機関が直面している深刻な問題である。これらの要素は全て、CDD の質、及び、有効性に更なる懸念を生じさせている。

金融機関は、いくつかの例外を除いて、リスクの高い顧客に対して適切な、厳格な顧客管理措置（EDD）を適用しておらず、多くの場合、EDD は、顧客の本人確認、及び、リスト照合に限定されている。

疑わしい取引の届出の総件数（年ベース）は増加傾向にあり、届出の大部分は金融セクターによるもので、三分の一は大規模銀行によるものであるが、これらは FIU（JAFIC）のガイダンスに基づいた基本的な類型・疑わしい取引の参考事例を参照したものである。

ほとんど全ての銀行は、AML/CFT に係る内部管理態勢、方針、手続を確立している。その他の金融機関は、より基本的な内部管理態勢を適用しており、そのほとんどはコンプライアンス部署の中に AML/CFT 管理機能を有している。

業界団体は、金融庁と協働して、AML/CFT に係る義務に関する金融機関の啓発や監督上の期待に係るコミュニケーションの役割を担っている。しかし、こうした取組みにもかかわらず、AML/CFT に係る措置に対する平均的な意識は依然として不十分である。

暗号資産交換業者は、登録義務制度が導入されており、2017 年以降、AML/CFT 目的で適切に規制・監督されている。今のところ 19 社の暗号資産交換業者が、登録されている。

暗号資産交換業者は、暗号資産取引に関連する犯罪のリスクについての一般的な知識を有する。テロ資金供与リスクの理解は概して限定的である。

暗号資産交換業者は、基本的な AML/CFT に係る義務を実施する傾向がある。一定数の暗号資産業者は、顧客の本人確認のために厳格な措置を適用している。一般的に、暗号資産交換業者は、自らのリスクに応じた低減措置や、厳格な顧客管理措置（EDD）又は特定の顧客管理措置（CDD）の適用について、当業態に特化した方針を有していない。

暗号資産交換業者の疑わしい取引の届出は、2017 年に義務が導入されて以降、900%以上（2018 年には７千件を超える届出）増加した。これは、主に FIU と、日本暗号資産取引業協会（JVCEA）が共同で行った一連の啓発活動やガイダンスの結果である。

暗号資産交換業者は、監督上の措置に従って、内部管理態勢を改善した。

## *勧告事項*

引続き、マネロン・テロ資金供与リスクに基づく金融機関のコンプライアンス文化の変化を促すための適切な啓発、及び、研修を実施し、監督当局も関与しつつ、マネロン・テロ資金供与リスク及び AML/CFT に係る義務のより良い理解のために支援すべきである。

全ての金融機関に対して、自らの業務、商品、サービス、及び顧客に応じた適切なリスク評価の策定を求めるべきである。

３メガバンク向けのベンチマークの基準に平仄が取れるよう、金融庁 AML/CFT ガイドラインを高度化するよう更新すべきである。適切な取引モニタリングシステムの必要性を強調し、適切な継続的顧客管理との関連性を明確にすべきである。

全ての金融機関が新たな法律上・規制上・監督上の義務を履行するための、規範的（prescriptive）かつ適切なスケジュールを設定すべきである。

金融機関において、取引記録を考慮に入れた包括的、かつ、変化する顧客のリスク特性に基づく、顧客情報の検証方法の改善、及び、継続的顧客管理措置の完全な履行がなされるようにすべきである。

金融機関の複雑な構造を踏まえつつ、金融機関が、CDD データと取引モニタリングを統合した、適切かつ包括的な、情報システムを導入することを確実に履行すべきである。その取引モニタリングは、金融機関の業務内容、特定されたリスク、並びに、顧客の取引パターン、及び、リスク特性に適合したものであり、また、適切な検知シナリオに基づく取引モニタリング・パラメータを有するものであるべきである。

AML/CFT 義務の新たに課されたカストディアル・ウォレット・サービスについて、適時に履行するようにすべきである

「トラベルルール」の解決策が開発された際には、暗号資産交換業者とカストディアル・ウォレット・サービス提供業者が、電信送金に係る義務の対象となるようにすべきである。

引続き、暗号資産交換業者のマネロン・テロ資金供与リスクに対する理解を改善させると共に、暗号資産に関連する全ての新しい技術開発（新たなビジネスモデ

ル、取扱候補の暗号資産及びその他の暗号資産に係るイノベーション等）が、マネロン・テロ資金供与リスクを勘案して分析されるようにすべきである。

暗号資産交換業者のコンプライアンス文化を継続的に強化するため、AML/CFT に係る義務の理解と実施に欠かせない指導やサポートを提供する。この際、各事業者のリスク評価及び当該評価に基づく全ての AML/CFT に係る義務の履行に重点が置かれるべきである。

暗号資産交換業者の特性に合わせた、より踏み込んだシナリオ設定に資するために、疑わしい取引の届出へ参考となる情報の提供を精緻化、そして調整すべきである。

本章において検討・評価された関連する有効性検証項目（IO）は、IO.4 である。有効性の評価に関連する勧告は、勧告９から 23、並びに 勧告１、６、15 及び 29 における関係する項目である。日本は、暗号資産交換業者に対して、金融機関と同様の取組みを行っている。しかしながら、暗号資産交換業者の固有の特性及び AML/CFT の枠組みが最近導入されたことに鑑み、暗号資産交換業者は、IO.4 において金融機関とは独立して評価されている（第１章、1.4.4 参照）。

審査団は、監督対象となる業態（obliged sectors、特定事業者の業態）について、各業態の重要性とマネロン・テロ資金供与リスクのレベルを考慮し、日本の文脈における相対的な重要性に基づき、順位付けした（第１章、1.4.3 で説明）。最終的に、審査団は、評価における考慮の重要度について、以下の結論を得た。

a) 最も重要：銀行

b) 重要：暗号資産交換業者、資金移動業者、信託会社、貸金業者、保険会社、金融商品取引業者、両替業者、不動産特定共同事業者、クレジットカード事業者、宅地建物取引業者、宝石・貴金属等取扱事業者、法律・会計専門家

c) やや重要：ファイナンスリース事業者、郵便物受取サービス業者、電話受付代行業者、及び電話転送サービス事業者

d) 重要性が低い：少額短期保険業者、短資業者、証券金融会社、特例業務届出者、商品先物取引業者、口座管理機関、電子債権記録機関、国債を取り扱う振替機関及び口座管理機関、並びに独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構

IO.4 における結論は、金融庁及び他の監督当局（財務省、経済産業省等）から

提出された文書（手続・手順書、統計、事例を含む）、金融庁・他の監督当局・関連当局（例えば、JAFIC）との面談、金融業者、暗号資産交換業者及び非金融業者からの民間事業者の代表とのインタビューに基づいている。金融業者には、大規模銀行及び比較的規模の小さな銀行、並びにその他の金融機関が含まれ、これらの先を合計すると資産ベースで当該市場の大部分を占める。

## 5.2. 有効性検証項目４（予防的措置）

### *5.2.1 マネロン・テロ資金供与リスクと AML/CFT に係る義務の理解*

*金融機関*

大規模銀行（より高いリスクを有するとされている GSIB 等）一定数の資金移動業者を含む一定数の金融機関は、マネロン・テロ資金供与リスク及び AML/CFT に係る義務について適切な理解を有している。その他の金融機関は、自らのマネロン・テロ資金供与リスクの理解がまだ限定的である。

金融機関は、マネロン・テロ資金供与リスクや AML/CFT に係る義務の履行に関する主要な参考先として、金融庁やその他の当局、特に NRA より得られた情報を利用する傾向がある。

金融機関は、一般に、国際的な電信送金や現金取引とともに、暴力団、北朝鮮、外国人顧客を、より高いリスクがあると位置付けている。銀行口座の不正利用の主な事例の一つとして、口座乗っ取り（フィッシング・詐欺）や口座売買（出国予定の一時滞在者によるもの）に関連する詐欺が挙げられる。密輸の危険があるため、金に関連する取引もまた、懸念のある領域である。これは、概ね NRA の結論と一致している（IO. 1 参照）。しかし、大部分の金融機関は、現金取引を介するもののほかは、前提犯罪とマネロンとの関連性や、どのように犯罪収益が金融システムに入り込むかについて、より深い理解を有していない。さらに、一定数の金融機関は、一定の特定の分野（例えば、閉鎖的なグループに属し、当該グループの会員であることにより本人確認が行われた顧客に対し、主にサービスを提供する銀行）に限定されているため、顧客基盤のリスクが低いとみなし、それゆえ、各顧客のリスク評価を実施していない。

金融機関は、紛争地域への近接性に基づき、テロ資金供与リスクを理解しているのみと見られ、金融セクターにおける他の類型のテロ資金供与については、報告

も調査もされていない可能性を示している。

大規模銀行（より高いリスクを有するとされている GSIB 等）及び一定数の資金移動業者を含む一定数の金融機関は、自らのリスクをより良く理解しているようであり、そのリスク評価に一定の具体的な要素又は指標（例えば、外国人顧客の国際送金の頻度、取引量等）を追加している。

金融機関の AML/CFT に係る義務の理解は、限定的なようである。取引モニタリングシステムの利用と組み合わされた継続的顧客管理の考えに関する明確かつ一律の理解の確立について、課題がある。これらの義務は、犯罪収益移転防止法の改正や 2018 年２月に適用された強制力のある金融庁 AML/CFT ガイドライン（第 1 章参照）を通じて、最近日本の法制度に適用された。基本的な取引モニタリングシステムは一定数の金融機関で既にある程度導入されており、取引スクリーニングシステムはほとんどの金融機関で導入されているが、どちらのシステムもその効果は限定的であり、非常に高い割合で誤検知が見られる。既に取引モニタリングシステムを導入している大部分の金融機関は、独自のツールを開発しているが、異なるツール間で複雑性や有効性にばらつきがあり、また、それ以外の金融機関には手動で管理を行っているものもある。

金融機関は、新たな義務を履行するためには、AML/CFT の枠組みや取組みを強化する必要があるとの一般的な認識を有している。しかし、これらのギャップに対処するために監督当局により課された明確な期限はなく、金融セクターの変化に対する取組みの遅さを考えると、直接金融庁と緊密な対話を行っていない金融機関が、どの程度、自らの施策においてギャップを速やかに理解・評価しているのかは不明である（IO.3 参照）。

2018 年の金融庁 AML/CFT ガイドライン（第 1 章参照）は、金融庁所管の金融機関が AML/CFT に係る義務を履行するための大きな一歩であったが、一定の改善が必要である。金融庁 AML/CFT ガイドラインは、全ての金融機関に共通の最低基準を設定し、所管金融機関における適切な AML/CFT の枠組みの履行を要求している。しかし、全ての金融機関における自らのリスクに応じた効果的な AML/CFT 管理態勢（AML/CFT systems）を確保するために、基準のレベルを引き上げる必要がある。金融庁マネーローンダリング・テロ資金供与対策企画室は、2018 年５月に、ガイドラインのプリンシプル・ベースの指示を統合した AML/CFT に係る一連の義務が記載された「３メガバンク向け AML/CFT ベンチマーク」を発出し、メガバンクが海外のグローバルなシステム上重要な金融機関（G-SIFIs）の国際的な AML/CFT に係る基準を満たすことを要求している。これらのベンチマーク

は、金融機関毎の複雑な特性に配慮しつつ、２つの異なる基準が存在するという状態を回避するため、金融庁 AML/CFT ガイドラインにリスクに応じた形で統合されるべきである。

業界団体は、金融庁と協働して、会議、セミナー、研修活動を通じて、AML/CFT に係る義務に係る金融機関の啓発や監督上の期待に係るコミュニケーションの橋渡しの役割を担っている（IO.3 参照）。しかし、こうした取組みにもかかわらず、AML/CFT に係る措置に関する認識レベルは依然として不十分である（いくつかの金融機関を除く。第 336 及び第 339 パラグラフ参照）。

### *暗号資産交換業者*

暗号資産交換業者は、暗号資産取引に関連するリスク（追跡可能性の欠如、即時移転可能性、国境を越えた移転の容易さ、匿名化技術を含む技術革新の速度等）について一般的な知識を有する。過去数年間において日本に影響を及ぼした大規模な暗号資産流出事件（例えば、Mt Gox、コインチェック、Zaif）は、市場の脆弱性についての認識を引き上げる重要な事件であったが、こうした認識は、AML/CFT よりも消費者保護の観点によるものであった。したがって、暗号資産交換業者は、セクター固有のマネロン・テロ資金供与リスクよりも、暗号資産取引に係る消費者保護リスクにより焦点を当てている、と審査団は判断した。

一般に、暗号資産交換業者は、NRA に挙げられているリスク要素以外に、自らが取り扱っている暗号資産の種類（匿名・非匿名）等の、多数の主なリスク要素を追加している。これは、当該セクターが率先して固有のリスク特性を判断している前向きな的な兆候である。

2017 年に暗号資産交換業者の AML/CFT に係る義務が導入された（第 1 章参照）。JVCEA（5.2.6 参照）は、コンプライアンス文化をまだ改善させる必要があると認識していた。JVCEA は、金融庁と協力して、会員を対象に月次で AML/CFT 勉強会を開催している（6.2.6 参照）。2018 年にいくつかの暗号資産交換業者に対して発出された業務改善命令を受けて、暗号資産交換業者は、現在、ほとんどの事例において、経営陣レベルで AML/CFT の問題に対処しており、金融業界出身の AML/CFT オフィサーを雇っている。

現状、暗号資産交換業者は、顧客・ユーザの特定、制裁者及び反社リストとの照合、NRA に基づくよりリスクの高い要素の特定及び疑わしい取引の届出等の基本的な AML/CFT に係る義務を理解している。

資金決済法における暗号資産交換業者の定義の範囲のために、AML/CFT に係る義務は、暗号資産交換業者が提供するカストディアル・ウォレット・サービスには適用されない。しかし、このギャップを埋めるために資金決済法が 2019 年５月に改正され、オンサイト審査後の 2020 年５月１日に施行された。

### *5.2.2. リスク低減措置の適用*

#### *金融機関*

金融機関がマネロン・テロ資金供与リスクについて限定的な理解しか有していない場合、金融機関の RBA の適用に直接的な影響を及ぼす。一定数の金融機関は、自らのリスク評価や、認識されたリスクに応じた低減措置を適用している。その他の金融機関は、リスクに応じて十分に調整することなしに、画一的な低減措置を適用している。一般に、金融機関は、単なる法令等遵守への取組みに留まっており、例えこれらのリスクが自らの業務に関連しない場合であっても、監督当局によって指摘された基本的なリスクカテゴリー（主に NRA の結論に基づくもの）を参照している。実際、2018 年の「マネー・ローンダリング及びテロ資金供与対策の現状と課題」（「現状と課題」）で評価されたように、2018 年８月時点では必ずしも全ての金融機関に RBA が浸透しているわけではなく、単なる顧客の本人確認、取引の確認、及び、疑わしい取引の届出のみならず、より有効性の高いリスク低減措置の実施が問題となった。

ほとんどの金融機関は、新規顧客について、その属性を総合的に評価し顧客リスク格付を付すための適切な顧客管理（CDD）の仕組みを整備しているが、既存顧客については情報更新手続の途上である。一定数の金融機関は、CDD のためのツールを導入し始めたが、情報更新手続は進行中である（5.2.3 参照）。よりリスクの高いリスクカテゴリーは、主に、NRA に分析・記載されているリスク要因（IO.1 参照）に基づいて設定されている。顧客のリスク特性は、主にリスト照合に焦点を当てている。顧客に関する情報は、取引関係の構築の際に取得した基本的な情報に限定され、かつ、この情報は大抵の場合、更新されていない。顧客の取引先や関係会社を検出し、これらを名寄せしたりグループとしてリスクを評価し、取引をモニタリングする仕組みはない。自主的に分析した顧客のリスク特性を、グループ内の異なる法人間で共有している金融グループは少ない。

一定数の金融機関が自らの業務に関連するリスクを限定的にしか理解していないことを踏まえると、これらの金融機関が金融庁 AML/CFT ガイドライン（第１章

1.4.5 参照）が明記する RBA の基本をどの程度理解し、リスクに応じた低減措置を実施しているかについては懸念がある。

### *暗号資産交換業者*

日本における取扱い暗号資産のマネロン・テロ資金供与リスクを低減・管理するために、暗号資産交換業者は、金融庁及び JVCEA に、取扱い暗号資産を追加する等変更する場合、事前に報告しなければならない。取扱候補の暗号資産は、暗号資産交換業者による評価に基づいて、また必要に応じて、当該暗号資産の適法性及び技術的側面を検証する第三者を通じて、検討される。ある暗号資産はギャンブル目的で使用された履歴があることから、最近取扱いが拒否された。暗号資産交換業者が金融庁及び/又は JVCEA の指導に反した場合、金融庁は、当該業者に対する行政処分を課す最終的な権限を有する。

さらに、日本の全登録暗号資産交換業者に適用される自主規制規則（6.2.6 参照）は、匿名性暗号資産の取扱いを禁じている。これらの暗号資産は、追跡可能性がなく、ダークネットでの取引媒体の大宗を占め、高リスクであると考えられている。

AML/CFT に係る予防的措置に関しては、暗号資産交換業者は、金融機関の場合と同様（上記参照）に、基本的な義務を画一的に適用し、自らのリスクに合わせて調整しない傾向がある。

## *5.2.3. 顧客管理措置（CDD）の適用及び記録保存義務*

### *金融機関*

金融機関は、実質的支配者の確認・検証や、取引モニタリングシステムと組み合せた継続的顧客管理等の顧客管理措置（CDD）の導入に、大きなギャップを有しているようである。情報更新とリスク評価の見直しが実施されていない多くの既存口座が存在している。

取引関係の構築に当たって、潜在的な顧客が、制裁及び反社リストに該当する場合や必要な情報が不足している場合には、金融機関により取引が謝絶される。金融機関は、日本における他の事業者と同じく、暴力団・反社会的勢力関係者との関係を排除しなければならない（IO.1 参照）。金融機関がアクセス可能な、固有

かつ公式の（暴力団）リストは存在しない。基本的に、金融機関は、自らの情報と警察庁や都道府県警察を含むその他の情報源、サービス提供会社からのデータに基づいて作成した独自のリストを有している。当該リストは、金融機関により継続的に更新されることが必要であり、その正確性や確度の確保については課題がある。

既存顧客が反社リストに該当した場合、又は、既存顧客が暴力団員である、もしくは、暴力団員に関連していると疑われる場合、口座の活動は厳格な調査と管理により取引に制限が加えられる。組織犯罪に関連する口座解約の手続には、長期間を要するようである。

金融機関は、取引関係の構築に当たって、顧客の住所等の基本的な顧客情報を収集・検証しようとしているだけのようである。口座開設のための写真付の身分証は、標準的なリスクの顧客にとっては必須とはならない。金融機関は、2016 年に義務化されるまで、収集した基本的な顧客情報を更新しなかった。さらに、この新たな義務は体系的かつ適時に、既存及び新規の顧客に適用されていない傾向がある。

実質的支配者に関する情報は、顧客の申告に基づいて収集されることが多いが、これは不十分な検証方法である。日本は、近年、有益な検証手段となる可能性のある、公証人主導の実質的支配者の登録制度を創設したが、いくつかの制約が確認されている（IO. 5 参照)。

金融機関は、口座の売買や不正利用の蔓延に係る問題に直面している（5.2.1 参照)。口座の不正利用の容易性とその拡大は、金融機関が直面する主要なリスクの一つとして認識されているが、適用される顧客管理措置（CDD）の質と有効性に更なる懸念を生じさせている。

継続的顧客管理について、金融機関は、金融庁 AML/CFT ガイドラインの規定に従い、正確かつ適切な顧客情報を保つためのシステムの構築を開始している。しかしながら、継続的顧客管理措置は、収集された顧客情報の更新及びリスト照合に限定されているように見られる。

この手法に従って継続的顧客管理に係る措置を実施しても、金融機関が、顧客の特性と業務内容を結びつけ、予測される顧客の取引パターンからの逸脱の可能性を検知できるようにはならない。この弱点に対処し、継続的顧客管理に係る義務の履行の有効性を改善するためには、監督当局からの説明、又は、指導が必要と思われる（IO. 3 参照)。2019 年の「現状と課題」にあるように、一定数の金

融機関は、顧客管理措置（CDD）や取引モニタリング、取引フィルタリング・スクリーニングについて、統合されたITシステムの活用・設計・導入を検討しているところである（以下参照）。しかし、これらのITシステムは、ほとんどの場合まだ導入されておらず、既に導入されている場合でも、その効果は限定的である（既に顧客のリスク特性に基づいて敷居値を調整した取引モニタリングシステムを導入しているメガバンクと一定数の地銀についても、非常に高い割合の誤検知等の多くの課題に直面している）。

取引モニタリングに関しては、疑わしい取引を識別するために、顧客の特性及び取引パターンに注目する、適切な取引モニタリングシステムを整備しているのは、非常に限られた数の金融機関のようである。これらの金融機関は、一般に、自らのリスクを十分に理解している金融機関である（例えば、資金移動業者と一定数の銀行。上記参照）。

一般に、適用されているリスク低減措置は、制裁者及び反社リストとの照合に限定されている。場合によっては、これらの措置は国際的な電信送金にしか適用されていない。

しかし、金融庁AML/CFTガイドラインの指示に従い、一定数の金融機関においては、基本的な取引モニタリングシステムが整備されている。現在導入されているITツールの有効性は、大量のアラートが発生し、誤検知の平均比率が最大99%にのぼっていることからすると、不十分である。このことは、検知の指標が、単に、基本的なトリガー基準（シナリオ）及び敷居値に関連しているだけで、不適切に設定されていること示している。これらには、取引のパターンやマネロン・テロ資金供与の手法の検知シナリオが含まれるべきである。これらの要因は、金融機関が基本的なもの以外の疑わしい取引パターンを検知する能力を制限している（この点は翻って、金融機関及び国のリスク評価、及び、理解に影響を及ぼしている。IO.1 参照）。さらに、大量の誤検知を手作業でチェックする非常に時間のかかる作業は、金融機関が AML/CFT の枠組みを改善するための経営資源の活用に制約を加えている。

一定数の金融機関は、取引モニタリングシステムを導入する過程にあるが、このようなシステムをまだ導入していない金融機関も多くある。信用組合等の小規模な預金取扱金融機関の11%が、手作業で取引をモニタリングできるものと判断して、IT ツールを全く導入していない。これは、業務量が少なく、顧客基盤はリスクが低いものとみなしているためである。一定数の業界団体は、会員金融機関がスケールメリットを得られるように、共同化された取引モニタリングシス

テムを開発しているところである。これらのプロジェクトは進行中であるため、現時点では有効性を評価することはできない。しかし、関係する小規模の銀行による AML/CFT に係る義務の履行を改善するために役立つツールとなりうる。

最後に、金融機関は、継続的顧客管理及び取引モニタリングについて確認されたギャップへの対応について、監督当局から一般的な期限を設定されていない（IO.3 参照)。金融機関は、一般に独自の期限を設定しているが、期限が延長されることが多い。銀行は、既存顧客に対する顧客管理措置（CDD）の実施のため優先順位付けを始めているが、銀行が顧客に関して限られた情報しか持っていない場合には、RBA を適用することが困難であることが分かっている。その結果、金融機関が顧客に関する理解を改善し、適切な AML/CFT に係る低減措置を適時に適用することが容易ではなく、それが重大な懸念となっている。

金融機関は、法律に従い、１万円（79.19 ユーロ、96.3 米ドル）の敷居値を超えた業務に関する記録を保持しているようであり、通常、（過去 12 ヶ月間の取引に係る要請については)、約３～５営業日で求められた情報を捜査当局に提供することができる。関係する金融機関の記録保存方法によっては、より過去に遡る一般的でない、又は、より複雑な取引の情報提供要請について、より多くの時間がかかる可能性がある。実際、監督当局によって課された記録保存に係る標準的な形式はなく、通常は犯罪収益移転防止法に従って７年間保存されている様々な情報（例えば、顧客に係る書類一式、当座預金取引等）は、それぞれ異なる方法及び場所で保存されている可能性があり、必要となる関連記録の作成をより困難にしている。

暗号資産交換業者は、顧客・ユーザの確認・検証、制裁者及び反社リストとの照合を中心とした、基本的な顧客管理措置（CDD）に係る義務を実施しているようである。顧客・ユーザの確認・検証には、通常、顧客・ユーザがどこからアクセスしているかを知るための IP アドレスの確認、及び、当該アドレスが顧客・ユーザによって提供された他の情報（居住地又は職業に関する情報等）と一貫性があるかの確認が含まれる。IP アドレスに伴う地理的位置情報は、分散型台帳技術分析ツール（distributed ledger technology analytical tools）を使用して特定することができる。金融機関の場合と同様に（上記参照）、継続的顧客管理及び取引モニタリングは、暗号資産交換業者においてまだ完全には実施されていない。暗号資産交換業者は、顧客・ユーザの情報及び取引記録を保存しているようであり、法執行当局からの要求に応じて情報を提供することができる。

### *5.2.4. 厳格な顧客管理措置（EDD）の適用*

*金融機関*

ほとんどの金融機関は、外国人等のリスクの高い顧客に対して、適切な厳格な顧客管理措置（EDD）を適用していないようであり、通常 EDD は、本人であることの確認（例えば、金融機関は、リスクの高い顧客については、口座開設にあたって写真付の身分証明書のみを受け入れる）及びリスト照合に限定されている（5.2.3 参照）。リスクの高い顧客に関する厳格な業務規程（operational rules）はなく、また、追加的又は厳格な低減措置の実施を担保するためのエスカレーション手続も存在しない。

PEPs については、厳格な顧客管理措置（EDD）の適用に技術的限界があるが、これは主に国内 PEPs と国際機関 PEPs の概念が国レベルで認識されていないためである（TC 附属書 R.12 参照）。

コルレス銀行業務については、金融機関は、新たな関係の構築を慎重に検証し、コルレス先の信頼性を適切に評価しているようである。いずれにせよ、コルレス銀行業務は、主要銀行・中規模銀行に限定されている一方で、小規模銀行は、大手銀行等に本サービスの提供を委託している。

金融機関は、定期的に、リストベースの手法を通じて、テロ資金供与に関連する制裁者リストについて取引スクリーニングを実施している。この手法には、第三者の自動スクリーニングソフトウェアが含まれる。一般に、日本の当局の認識は、大規模金融機関が、（Wolfsberg Group 等の）国際的なグループの取組みを遵守していることを拠り所としている。財務省は、国連安全保障理事会によるリストの更新について、更新の日、又は、速やかに、更新情報を金融機関に直接送付している（IO.10 参照）。

日本の当局が、北朝鮮及び北朝鮮と関連のある者や法人に対する支払いを禁止していることから、金融機関は、イランや北朝鮮等のリスクの高い国々と関連のある取引について、特別な注意を払っている（IO. 11 参照）。また、金融機関は、北朝鮮に面する日本の西海岸（九州地域）の港湾等の、これら２つの高リスク国に隣接する地域に関連する外為送金や業務（operations）にも、より一層の注意を払っている。外国と取引する顧客を有する一定数の金融機関は、主に北朝鮮を中心とした高リスク国への輸出に主に用いられる瀬取りを考慮に入れている。

*暗号資産交換業者*

暗号資産交換業者は、高リスク顧客に対して、厳格な又は特定の措置を適用していないようである。特に、暗号資産交換業者は、顧客・ユーザが（国内 PEPs を含む）PEPs であるかどうかを特定するために必要な仕組みを有していないが、これは金融機関についても強調されている規制上の制約も要因となっている。

勧告 16・電信送金において、暗号資産交換業者は、「トラベルルール」問題に対処するための技術的解決策を見つける必要性を認識している。JVCEA は、このセクターでの取組みを調整し、各国の同じ問題意識を持つ業界団体とグローバルに協働している。

暗号資産交換業者は、顧客・ユーザに関し、テロ資金供与に係る制裁者リストとの照合を行っている。一定数の暗号資産交換業者は、暗号資産取引のスピード及び不可逆性のために、顧客・ユーザがこれらのリストに該当しても、取引の発生を防ぐことができない可能性のあることを認識している。一定数の暗号資産交換業者の中は、トラベルルールの適用に関係する可能性のあるこの問題に既に対処しているが、その他の業者は解決策の策定を検討中である（勧告 15. 7. b）。

暗号資産交換業者は、一般に、よりリスクの高い国を認識しているが、リスクを低減するために取られている措置は不明確である。一定数の暗号資産交換業者は、口座開設段階において、顧客・ユーザのプロファイルに応じて、リスクのより高い国が関連する取引を禁止することを検討するべきではないか。

### *5.2.5. 届出義務及び内報の禁止*

*金融機関*

金融機関は、一般に、疑わしい取引又は疑わしい可能性のある取引を検知したときに疑わしい取引の届出を行っている。金融庁は、金融機関の疑わしい取引の届出をモニタリングしており、疑わしい取引が金融庁に提出されると、それらを分析のために JAFIC に転送する（IO.6 参照）。検知されてから、金融機関が疑わしい取引の届出までに要する期間は、問題ない合理的なレベルである（平均 17 日）。

疑わしい取引の届出の総件数（年ベース）は増加しており、過去５年間（2014 から 2018 年）で年間約 40 万件となっている。金融機関は、届出全体の 96%を占め

る。疑わしい取引の届出の三分の一は、大規模銀行によるものであり、金融庁が実施した 2018 年度の AML/CFT に関する調査によると、信用金庫や信用組合等の比較的小さなリスクにさらされている銀行の 22%が、年度中に全く届出を行っていない。疑わしい取引の届出の大部分は、基本的な犯罪類型と疑わしい取引の参考事例に関するものであり、主に FIU （JAFIC）が銀行セクターに示したものである（IO.6「疑わしい取引の参考事例」参照）。入手可能なデータによると（IO.6、表 3.3 参照）、疑わしい取引の届出の大部分は、FIU の指針に記載されている基本的な犯罪類型に基づいている。仮に適切な取引モニタリングツールが既に導入されており、より洗練された疑わしい取引の参考事例等を踏まえて、より精巧なシナリオを考慮していれば、検知される疑いの範囲と届出に含まれる情報の内容という両方の点で、届出が改善される可能性がある。このことは、金融機関によるリスクのより良い理解と組み合わさって、疑わしい活動の特定及び分析の継続的な改善につながるであろう。このことはまた、国レベルでのリスク全体のより良い理解にもつながるであろう（IO.1 参照）。

金融機関は、紛争地域やテロ資金供与リスクが高い地域に関連する取引を含む事案等の、テロ資金供与に関連する疑わしい取引の届出を行っている。JAFIC は、これらの疑わしい取引の届出のうち、テロ資金供与が関与する可能性のある状況を特定している（IO.6 参照）。しかし、JAFIC 及び警察庁によるテロ資金供与に関連する疑わしい取引の届出の調査の質は概ね高い一方（IO.9 参照）、疑わしい取引の届出自体は、比較的基本的な検知事例を含む傾向がある。したがって、テロ資金供与にさらされている可能性について金融機関への更なる啓発や追加の疑わしい取引の参考事例及びシナリオの提供により、金融機関によるテロ資金供与の潜在的リスクのある取引の検知を支援し、複雑なテロ資金供与の手法の防止に寄与する必要がある。

JAFIC は、主要な銀行に対して、その疑わしい取引の届出に係る方針を直接フィードバックしている。

内報を防止するための標準的な措置は存在しないが、2018 年度の金融庁の AML/CFT に関する調査によると、銀行の 73%が内報を防止するための社内規程（通常、疑わしい取引の届出マニュアル内に記載）を有している。その他の金融機関は主に、職員に対し、疑わしい取引の届出に関して内報を行わないように指導するための研修に依存している。

*暗号資産交換業者*

暗号資産交換業者は、2017 年から疑わしい取引の届出義務の対象となっている。2017 年は 669 件、2018 年は 7,096 件の届出があった。この増加は、主に、FIU（JAFIC）が、暗号資産に関する疑わしい取引の届出内容の改善に係る法執行当局からの要請に応じて開催した一連の啓発研修やアウトリーチの成果である。また、要請事項を明確にするための指針も公表した。2019 年４月には、金融庁と JAFIC が共同で、匿名化技術（ミキサー、タンブラー等）を用いたいくつかのマネロンの手法を対象とした、疑わしい取引の参考事例を作成・推進した。

暗号資産交換業者によって届出がなされた疑わしい取引の大部分は、架空の名前を使用した取引やなりすましを含む顧客情報に関連する問題に基づいていた。これは、金融機関（5.2.3 参照）について強調されているように、日本で適用されている本人確認の制度に関し、更なる懸念を提起している。金融機関（上記参照）について言及されたものと同様に、疑わしい可能性のある取引の検知・届出に用いられた参考事例は、かなり基本的かつ汎用的なのではないか。取引モニタリングシステムは、こうした参考事例も勘案し暗号資産交換業者によって開発される必要があり、また、届出を改善するための重要な一歩である。

### *5.2.6. 内部統制及び AML/CFT に係る義務の履行を妨げる法律上・規制上の義務*

日本では、AML/CFT に係る義務の履行を妨げる法律上又は規制上の義務は存在しない。

*金融機関*

ほとんど全ての銀行は、金融庁 AML/CFT ガイドラインに沿った AML/CFT の内部管理態勢、方針、手続を構築している。その他の金融機関は、より基本的な内部管理態勢を適用しており、そのほとんどはコンプライアンス部署の中に AML/CFT 管理機能を有している。

金融庁が実施した 2018 年度の AML/CFT に関する調査によれば、銀行の 99%が第２線に AML/CFT を担当する部署を有しており、93%が AML/CFT 監査を含む独立し

た内部監査部門を設置し、少なくとも年１回は研修を実施している。

銀行グループについては、グループ全体の方針や内部管理態勢が定められている場合があるが、通常、海外に支店や子会社を有する場合は当てはまらない。

金融グループの場合、方針及び手続は、一般に、グループの法人ごとに異なり、グループの全ての法人内で同じ AML/CFT に係る義務を確保しているものではない。

*暗号資産交換業者*

暗号資産交換業者は、AML/CFT に係る内部管理態勢を構築する義務を負っており、金融機関について要求されたものと同様の AML/CFT に係るガバナンス体制を整備している（TC 附属書 c.18.1 参照）。これは、コインチェックの暗号資産流出事件（IO.3, 6.2.3 参照）に基づき 2018 年に実施された立入検査において金融庁が主に焦点を当てた分野であった。これらの検査は、暗号資産交換業者の急速な事業拡大に対応していなかった内部管理態勢に主な弱点があることを明らかにした。例えば、評価の結果が取締役会に報告されていなかったり、経営陣が事業の性質・発展に合わせて人員を増やしたり、システムの能力を見直したりすることがなかったことが挙げられる。

## IO.4 に係る結論

一定数の金融機関（大規模銀行及び一定数の資金移動業者を含む）は、マネロン・テロ資金供与リスクについて適切な理解を有している。その他の特定事業者（金融機関、暗号資産交換業者、DNFBPs）は、自らのマネロン・テロ資金供与リスクの理解がまだ限定的である。金融機関は、AML/CFT に係る義務についてより良い認識を有しているものの、これらの義務の履行については金融機関によってばらつきがある。一定数の金融機関は、自身のリスク評価や、認識されたリスクに応じた低減措置を適用し始めているものの、その他の金融機関は画一的な低減措置を適用し、顧客の本人確認及び基本的な取引スクリーニング以上のことは実施していない。加えて、金融機関は、一般に、継続的顧客管理や実質的支配者の確認・検証等の最近導入・変更された義務の概念についての理解が限定的であることや、新たな義務を履行する期限を設定していないために、これらの義務を十分に履行していない。取引モニタリングシステムは、既に導入されている場合でも、大幅に強化され、新しい顧客管理（CDD）ツールと統合される必要がある。

また、強制力のある金融庁 AML/CFT ガイドラインで求められている義務も、リスクに見合った、全ての金融機関における効果的な AML/CFT 管理態勢（AML/CFT systems）を確保するために強化、高度化される必要がある。

他の特定事業者（暗号資産交換業者や DNFBPs）は、AML/CFT に係る義務の履行についてまだ初期段階である。疑わしい取引の届出は、特に 暗号資産交換業者について増加しているものの、基本的な類型や疑わしい取引の参考事例に基づいている。全ての DNFBPs が、疑わしい取引の届出義務の対象になっているわけではない。

地域における最も重要な金融ハブの一つとしての日本の役割、日本の状況における金融セクターの重要性、重大なマネロン・テロ資金供与リスクにさらされている銀行や固有のマネロン・テロ資金供与リスクを有する暗号資産交換業者分野の出現を考慮すると、IO.4 については、いまだ大幅な改善（major improvements）が必要である。

日本は、IO.4 に関して、中程度のレベル（moderate level）の有効性を有すると評価される。

（以上）