諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究

その４

調査項目③－２　暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究

令和４年 12 月 23 日

有限責任 あずさ監査法人

KPMG

目次

1 はじめに 3
2 暗号資産等の定義 4
3 暗号資産等の生態系 6
4 ML/TF 観点での暗号資産悪用手口 11
5 暗号資産の ML/TF リスク 14
5.1 暗号資産そのものに内在するリスク 15
5.1.1 記帳方法に関するリスク 15
5.1.2 暗号資産の定義に関するリスク 20
5.2 暗号資産交換業者に関するリスク 26
5.2.1 暗号資産交換業者の定義のリスク 27
5.2.2 暗号資産交換業者のリスク 29
5.3 ネットワーク連携に関するリスク 30
5.4 P2P 取引に関するリスク 34
5.4.1 リスクの概要 34
5.4.2 DeFi 36
5.4.3 秘匿性を高めるサービス 37
5.4.4 リスクへの対処の方向性 38
5.5 法域に関するリスク 38
6 規制・監督上の課題 41
6.1 規制・監督当局に求められる事項 41
6.2 規制・ガイドライン 42
6.2.1 各国法規制：EU 43
6.2.2 各国法規制：フランス 48
6.2.3 各国法規制：ドイツ 50
6.2.4 各国法規制：ノルウェー 53
6.2.5 各国法規制：オーストラリア 54
6.2.6 各国法規制：カナダ 56
6.2.7 各国法規制：韓国 60
6.2.8 各国法規制（まとめ） 64
6.3 改善・制裁措置 64
6.4 モニタリング 66
6.5 コミュニケーション 67
6.5.1 アウトリーチ・官民連携 67
6.5.2 国際協力 68
6.6 リスク評価・調査分析 69
6.6.1 事業者のリスク評価の活用 71
6.6.2 無登録・無許可事業者の特定 72

6.6.3 主体者の特定 72
6.7 インフラ 73
6.7.1 人材育成 73
6.7.2 テクノロジー 74
6.7.3 外部専門家 74
6.8 分析手法 75
6.8.1 市場動向調査 75
6.8.2 規制対象となる暗号資産交換業者のリスク分析 77
6.8.3 トラベルルールについて 78
Appendix 82
Appendix I: 参考文献リスト 82

1 はじめに

本報告書は、有限責任 あずさ監査法人が、金融庁から委託を受けた「諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究」の調査研究結果をまとめたものである。調査対象は、

調査項目① 諸外国におけるマネロン情報の共有制度と個人情報保護法制

調査項目② 当局マネロン検査のフォローアップを外部適格コンサルタントに委託する手法（英）の事例研究

調査項目③ 海外当局のマネロンリスク分析手法やデジタル技術の活用状況

- デジタル技術等を活用した先進的なリスク分析手法の事例研究
- 暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究

と多岐にわたることから、報告書を以下のように 4 分冊構成とした。

分冊	タイトル	内容
第一分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究 その１	調査項目① 諸外国におけるマネロン情報の共有制度と個人情報保護法制
第二分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究 その２	調査項目② 当局マネロン検査のフォローアップを外部適格コンサルタントに委託する手法（英）の事例研究
第三分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究 その３	調査項目③－１ デジタル技術等を活用した先進的なリスク分析手法の事例研究
第四分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究 その４	調査項目③－２ 暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究

本報告書は、第四分冊であり、調査項目③ 海外当局のマネロンリスク分析手法やデジタル技術の活用状況のうち、暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究についてとりまとめたものである。本報告書は、2022 年 12 月 23 日現在で入手可能な情報に基づいている。

KPMG

2 暗号資産等の定義

本稿における暗号資産および暗号資産交換業者の定義は FATF の「Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers」に基づき[1]、以下のとおりとする。

暗号資産：デジタルで取引、移転可能であり、決済あるいは投資目的で利用可能なデジタル上の価値（既存の FATF 勧告でカバーされる法定通貨、有価証券その他の金融資産をデジタル表現したものは含まない）

FATF は、暗号技術に基づかないデジタル資産もあり得るとの前提で、暗号資産（Crypto Asset）ではなく、あえて VA; Virtual Asset（すなわち仮想資産）という言葉を用いている。わが国の金融制度上では、暗号資産は、資金決済法によれば、

一　物品を購入し、若しくは借り受け、または役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入および売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨および外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの

二　不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの

と定義[2]されており、概ね FATF の定義と整合的であることがわかる。

関連して、OECD においても暗号資産を共通報告基準（CRS）に取り込むべく暗号資産に係る報告制度（CARF）が公表されている。ここでは暗号資産は「Crypto-Asset」と称されているが、その定義は、（報告基準の対象となる）「関連暗号資産は、FATF 勧告の範疇に入る」[3]と明記されている。

次にバーゼル銀行監督委員会では、「Cryptoasset」の定義は「主に暗号技術と分散記帳もしくは同様のテクノロジーに依拠した民間のデジタル資産」[4]とされており、この定義は（FATF の定義が）暗号技術、分散記帳技術に依拠するものに限っていない点でわずかな違いがある[5]としている。ただし、この Cryptoasset に対する取り組みは、「Cryptoasset とその関連サービスの成長が、金融安定上の潜在的なリスクを高めており、Cryptoasset によっては、高い価格変動性を有し、流動性リスク、信用リスク、市場リスク、（不正、サイバーリスクも含めた）オペレーショナルリスク、ML/TF リスク、および法的ならびにレピュテーショナルリスクをもたらし得る。」との懸念に基づくものであり、定義上のテクニカルな相違点、あるいは暗号資産、仮想資産の用語の違いは、本稿の考察にあたって特段の支障とならないと思われる。このようなことから、本稿では、FATF の定義に準拠しつつ、用語としては「暗号資産」あるいは適宜略称として VA を以降で使用することとする。

次に、暗号資産交換業者の定義を以下のとおりとする。

---

[1] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org) (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf)

[2] 資金決済に関する法律　第 2 条第 5 項

[3] Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, OECD　AML/KYC obligations. (https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf)

[4] Second consultation on the prudential treatment of cryptoasset exposures, June 2022, Basel Committee on Banking Supervision (https://www.bis.org/bcbs/publ/d533.pdf)

[5] FSI Insights on policy implementation No 31, Supervising cryptoassets for anti-money laundering, April 2021 (https://www.bis.org/fsi/publ/insights31.pdf)

暗号資産交換業者：以下の行為、業務のいずれかを他の自然人、法人のために業として行う自然人または法人（既存の FATF 勧告でカバーされる者を除く）

i. 暗号資産と法定通貨の交換
ii. 暗号資産同士の交換
iii. 暗号資産の移転
iv. 暗号資産の保管・管理、または暗号資産の管理を可能とする方法
v. 暗号資産の発行や販売への参加および金融サービスの提供

FATF の定義上の言語は、VASP; Virtual Asset Service Provider であり、特に交換に限らず一連のサービス提供を行う事業者として位置付けている。一方、わが国の資金決済法によれば、暗号資産交換業とは、以下のいずれかを業として行うことと定義[6]されており、交換業と称しているものの FATF 同様、交換以外の業も含めていることがわかる。

一　暗号資産の売買または他の暗号資産との交換
二　前号に掲げる行為の媒介、取次ぎまたは代理
三　その行う前二号に掲げる行為に関して、利用者の金銭の管理をすること。
四　他人のために暗号資産の管理をすること（当該管理を業として行うことにつき他の法律に特別の規定のある場合を除く。）。

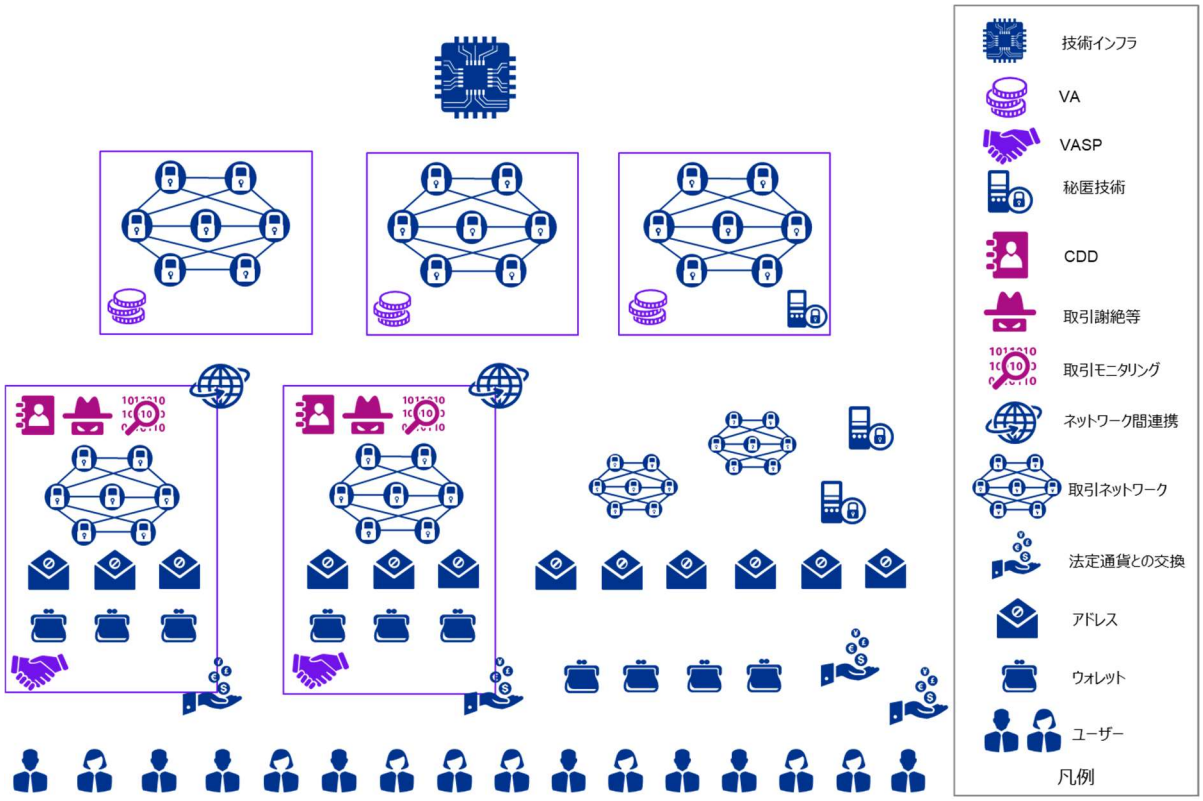
本稿においては、暗号資産の定義と同様、FATF の定義に準拠しつつ、用語としては「暗号資産交換業者」あるいは適宜略称として VASP を以降で使用することとする。

[6] 資金決済に関する法律　第二条 7

3 暗号資産等の生態系

暗号資産は、いわゆるサトシナカモト論文[7]によって、中央集権的な組織の関与を排除した Peer-to-peer（以下 P2P）に基づく電子的な通貨として紹介され、2009 年から運用が開始されたビットコインをその嚆矢[8]とする。リバタリアン的な設計思想に対する一種の熱狂と呼ぶべき社会現象も伴い、技術的にはゼロダウンタイムが実現できているとして、基盤であるブロックチェーン技術に対する一定の評価がなされている一方で、不正アクセスによる巨額の資産流出や、乱高下する資産価値、マイニングによる電力大量消費の地球環境に与える影響等の問題もはらみつつ、暗号資産は、今や無視できない相応の経済的地位を確保するに至っている。2022 年 10 月 29 日時点で、暗号資産を代表する仮想通貨の数は 21,555、取引所の数は 521、時価総額は 1,003,346,912,999.495 ドル（約 1 兆ドル）に上る。大手暗号資産交換業者の破綻およびその後の市場の動揺を経て、12 月 4 日時点での仮想通貨の数は 21,924、取引所の数は 528、時価総額は 854,677,652,021 ドル（約 0.85 兆ドル）となっている[9]。

本セクションでは、暗号資産や暗号資産に関連する様々な技術要素や主体（一旦、監督・規制主体は除外する）を取り巻く環境を生態系（以下エコシステム）的に整理したい。この整理は、以降の考察において示される論点が、どの部分に該当し、どのような主体が関与するのかを明確にすることを目的とするものである。



暗号資産のエコシステム

[7] “Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto”（https://bitcoin.org/bitcoin.pdf）

[8] これ以前にも同様のデジタル上の通貨の構想、商業的な試みはいくつか見られたが、一定の支持の下で社会に定着するに至ったのはビットコインが初と言ってよい。

[9] 仮想通貨価格、チャート、時価総額 | CoinMarketCap (https://coinmarketcap.com/ja/)

ユーザー

まず、決済、投資、もしくはその他の自らの目的で、何らかの暗号資産を保有、交換、売却する主体としてユーザーが定義される。ユーザーは①総合的なサービスを提供する暗号資産交換業者が提供する口座を保有するか、②オープンソースのウォレットサービスを利用する等して暗号資産のネットワークに直接・間接にアクセスすることができる。

ウォレット

ウォレットは、総合的な関連サービスを提供する一般的な暗号資産交換業者の顧客（口座保有者）の立場として、当該業者から割り振られる場合、メタマスクなどのオープンソースのサービスやその他のウォレットサービスを利用する場合が想定される。ユーザーが、異なる暗号資産交換業者の口座を開設する等して複数のウォレットを保有したり、複数のウォレットをたばねて管理したりするのは、もちろん自由であり、ウォレット自体は暗号資産の分散台帳の外で管理される。

アドレス

ユーザーが暗号資産交換業者の口座を保有する場合は、当該暗号資産交換業者から見れば当該ユーザーすなわち顧客に対しては、パブリックブロックチェーン上のアドレスではなく、当該業者によって内部的な識別子が割り振られるのが一般的である。一方、ユーザーが自ら、オープンソースのサービスその他のウォレットサービスを利用する場合は、当該ウォレットの仕様によって、自由にパブリックブロックチェーン上のアドレスを設定することが可能である。このアドレスは、基本的に当該暗号資産の分散台帳上のノードとして識別されるものであるが、前者のような場合は、あくまで当該暗号資産交換業者が提供する販売所や取引所における内部的な識別子と位置付けられるケースもあり、この場合、暗号資産全体のパブリックブロックチェーン上のアドレスとしては識別されない。

法定通貨との交換

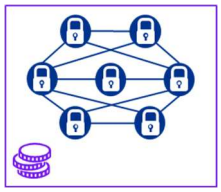
ユーザーが暗号資産を購入するためには、暗号資産交換業者が提供する総合的なサービスを利用することが一般的である。すなわち暗号資産交換業者が提示する当該業者の銀行口座に法定通貨を送金することで、当該ユーザーの口座上、当該法定通貨が現金資産と認識され、これを原資に販売所、交換所で、暗号資産を購入するという流れである。売却はこの逆で、販売所、交換所で売却して得た現金資産をあらかじめ登録していたユーザー自身の銀行口座への送金を依頼することが想定される。このような暗号資産交換業者の銀行口座とユーザー自身の銀行口座間の送金の他、暗号資産交換業者が提供する ATM で入金、出金を可能とするケースも想定される。

取引ネットワーク

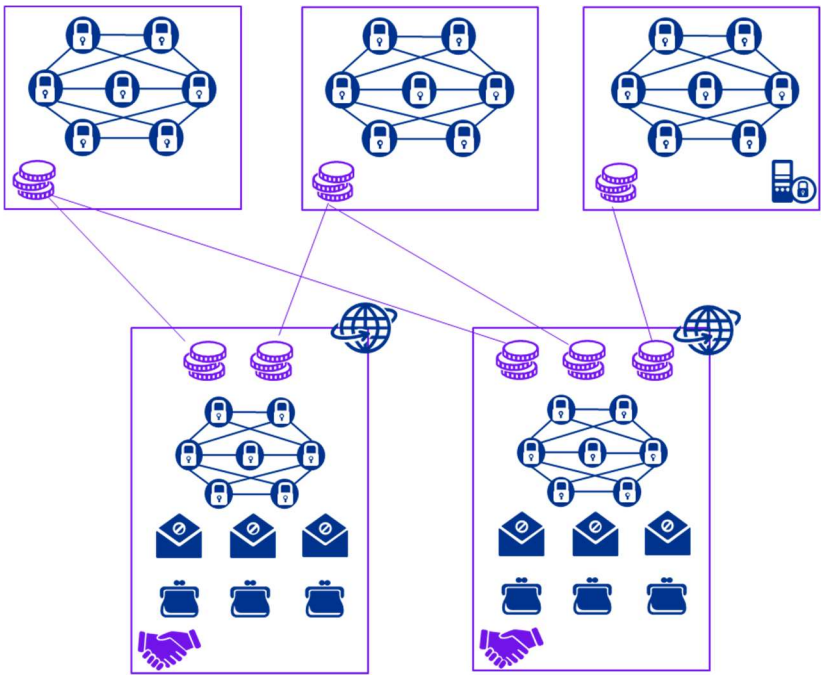
取引ネットワークは多様な意味合いを含む。①暗号資産の基盤となるブロックチェーン等の分散台帳、②暗号資

産交換業者自身がその顧客に対して提供するクローズドな取引ネットワーク、および③オープンソースで提供される各種ネットワーク等がこれに該当する。

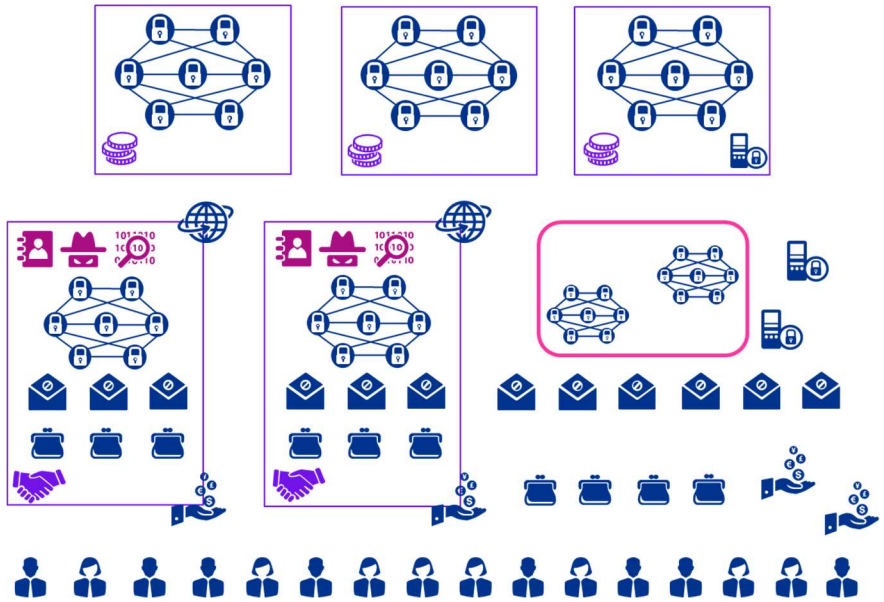
①については、暗号資産は、たとえばビットコインのようなコインのブランドとして、ユーザーから認識されるもの（後述の  ）と、分散台帳、すなわちパブリックブロックチェーンとしての取引ネットワーク  の２つの意味合いを持つものととらえることができる。（下図）



②については、暗号資産交換業者（後述の  ）自身がその顧客に対して提供する販売所、交換所は、当該業者内での閉じられた市場であり、これは暗号資産そのもののパブリックブロックチェーンとは別個に提供される暗号資産交換業者内のクローズドな取引ネットワーク（ブロックチェーンとは限らない）である。暗号資産交換業者は、販売所、取引所として顧客に提供可能な暗号資産を示し、ユーザーがクローズドなネットワークを通じて売買を行う。取り扱う暗号資産は暗号資産交換業者によって異なり得る。（下図）



③については、オープンソースでの売り買いマッチングサービスがツール、あるいは事業サービスとして（事業者としてのビジネス提供の性質を有するものから、あくまでオープンソースのシステム、ツールとしての性質を有するものまで位置づけは様々である）提供されているネットワークも存在する（下図　　）。悪意を持つユーザーに利用されることを想定したダークネット上の取引所もこれに含まれる。



ネットワーク間連携

暗号資産交換業者は、口座保有者に対して、暗号資産の売買の場を提供する販売所、交換所を開設しており、これらの取引は、直接に、あるいは間接的に、外部に存在する該当暗号資産のパブリックな分散台帳との連携がなされ、その取引が当該台帳に記帳される。

秘匿技術

暗号資産に関連する技術として取引の秘匿性を高めることを目的としたものが提供されている。ここでの秘匿性は、必ずしも ML/TF 目的等での悪意の秘匿を意味するものではない。パブリック型ブロックチェーンの性質上、アドレスがすべて公開されるということは、当該アドレスが行った過去の取引全てが全世界に知られてしまうことに他ならず、プライバシーの観点から、これを保護したいというニーズは合法である限り正当なものである。

暗号資産（VA）

暗号資産は、デジタルで取引、移転可能であり、決済あるいは投資目的で利用可能なデジタル上の価値（既存の FATF 勧告でカバーされる法定通貨、有価証券その他の金融資産をデジタル表現したものは含まない）のことである。ビットコインのような仮想通貨から始まり、その後、ステーブルコイン、NFT 等の様々な形態のデジタル資産が登場している。

暗号資産交換業者（VASP）

暗号資産交換業者という呼称から想像するよりも、その実態は極めて多様である。暗号資産の該当性判断と同様、FATF は、事業者の名称、技術要素、運営モデル、記帳方法その他の特徴によらず、提供される金融サービスの本質的な内容に応じて該当性を判断すべきとしている。たとえば、既述のウォレット、取引ネットワーク等の機能を提供するソフトウェアプログラムは暗号資産交換業者には該当しないが、当該プログラムを作成、所有、運営する主体が存在しており、その活動が定義に該当するのであれば、その主体者は暗号資産交換業者となり得る。活動が定義に該当するとは、既述の定義にあるような行為、業務のいずれかを、他の自然人、法人のために、「業として」（すなわち定期的に頻繁に）、「行う」（すなわち、既述の定義の i.～v.の行為、業務を行う）ことを指す[10]。

暗号資産交換業者に該当するのであれば、その業務範囲に応じて、AML/CFT にかかる以下の 3 つの措置[11]が義務付けられているべきである。

暗号資産交換業者に求められる AML/CFT 固有のコンプライアンス要素

技術インフラ

暗号資産そのものの開発、運用を容易にするための技術インフラも提供されている。イーサリアムはその典型例であり、テザー(USDT)、USD コイン(USDC)、バイナンスコイン(BNB)といったイーサリアム自体として提供するイーサ（ETH）やイーサリアムクラシック（ETC）以外の暗号資産の基盤ともなっている。

以上が、まず暗号資産や暗号資産に関連する様々な技術要素や主体を取り巻く環境、あるいはエコシステムの包括的な概観である。ただし、エコシステムと言っても、安定的、循環的なものではなく、時に爆発的、破壊的とも言えるような急激に変化、進化を遂げている状況にある、ということを理解する必要がある。引き続き、技術要素、主体、提供サービス等の進展に注視して、環境全体を捉え直す不断の努力が求められる。

匿名化、P2P 等に関する技術革新や、ステーブルコイン、NFT に代表されるような適用範囲拡大が引き続いて進展すると予想されていることも踏まえると、暗号資産に関連する ML/TF リスク[12]は、常にダイナミックに捉え直していく必要がある。

[10] SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, FATF, JULY 2021.

[11] さらにいえば、後述の 3 つの措置の基盤となる、教育研修、リスク評価、記録の保存、有効性の検証等の要素も求められるが、本稿では割愛する。

[12] 暗号資産にまつわるサイバーセキュリティ、消費者・利用者保護も無視できないリスクであるが、本稿では考察の対象外とし、ML/TF リスクを主な考察対象としてとりあげる。

4 ML/TF 観点での暗号資産悪用手口

暗号資産は、金融サービスの革新をもたらす一方で、中央集権的な主体者の介在を前提としないサービス形態、クロスボーダーの価値移転の迅速性・容易性等によって、ML/TF を企図する勢力に対して、不法行為の新たな機会を与えるものであることが懸念されている。

実際の手口として暗号資産が悪用される局面は以下の３つに代表され、犯罪行為者にとって暗号資産は、不法資金の金融システムへの導入、レイヤリング、統合の重要な手段の一つとして利用されている。

- ✓ 麻薬その他の化学物質等、政府機関によって製造、所有、使用を規制されている規制物資の不法な輸送・移転に伴う支払
- ✓ 上記の支払の資金の出所を隠匿するためのレイヤリング
- ✓ 不正、詐欺、ランサムウェア、恐喝に関連する支払

FATF 報告書「Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing」[13]によれば、主な手口は以下のように整理できる。

【取引の規模や頻度の観点からの主な手口】
- 記録や報告が必要となる閾値を下回る少額での多数取引
- 短期間での多額の複数取引（特にランサムウェア身代金等取引の際に顕著であり、新規口座や長期間不稼働であった口座等が利用される）
- 顧客の居住地や業務地とは異なる法域、AML/CFT 規制がない、もしくは脆弱な複数の法域の複数 VASP への短期間での送金
- 取引所への暗号資産の預け入れと、その後一切の取引がないままの引き出し、合理的な説明がつかない複数暗号資産への交換、プライベートウォレットへの短期間での引き出し
- 窃盗、不正が疑われる資金の受け入れ（窃盗資金を保有していると特定されたアドレス、もしくは当該アドレスに関連付けられたアドレスへの預け入れ）

【取引パターンの観点からの主な手口】
- 口座開設と同時に、当該顧客属性につり合わない多額の預け入れ
- 口座開設と同時に、多額の預け入れ、さらに同預け入れを担保とした限度額いっぱいの借り入れを実施し、これらを資金とした多額の取引と、短期間での全額引き出しまたは送金
- 多数の暗号資産、口座をまたぐ取引であり、合理的な説明がつかないもの
- 一定の期間内の頻繁な資金移動
- 不特定多数のウォレットからの少額資金移動後、他のウォレットへの全額転送もしくは法定通貨交換
- 極端に高い手数料、価格変動に伴う損失が想定されるにもかかわらず、合理的な説明がつかない暗号資産と法定通貨間の交換
- 合理的な説明がつかない、法定通貨と暗号資産、あるいは暗号資産同士の多額の交換

【秘匿性の観点からの主な手口】
- 追加的なコストが発生するにもかかわらず、秘匿性を高める機能を有する暗号資産の取引を選好する
- P2P の交換ウェブサイト上で、未登録、未許可の VASP として運営している者は、顧客から高額な手数料

[13] FATF Report, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020 (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf)

をとり、高額の暗号資産を移転する
- P2P 交換所でのウォレットからの多頻度あるいは多額の暗号資産の引き出し
- ミキシングサービス、P2P 交換所を運営する VASP の利用が関連付けられるような行動パターンを示すウォレットとの間の暗号資産の移転
- 既知のウォレットとダークネットでの市場間の不法資金の流れを隠す目的でミキシングサービスを利用する
- 疑わしいと特定された、ダークネット市場、ミキシングサービス、ギャンブリングサイト、ランサムウェア等の不法行為等に関連付けられる暗号資産アドレスで資金を出し入れする
- アンホステッド・ウォレット、ペーパーウォレット等を介してクロスボーダーで暗号資産を移転する
- 匿名プロキシその他の技術を用いて本人を特定できないドメインネームで VASP に口座開設する
- ダークネットその他の匿名コミュニケーションを許容するソフトウェアに関連付けられた IP アドレスを用いて VASP サービスを利用する
- 同一 IP アドレス（もしくは MAC アドレス）によって管理される多数の暗号資産ウォレット（口座名義はそれぞれ異なる）を利用する
- 不正、ねずみ講等の詐欺スキームに関連して設計が適切に文書化されていない暗号資産を利用する
- CDD プロセスが脆弱もしくは不在とされる VASP の口座との資金移転
- 高手数料にもかかわらず、犯罪行為が多い等の高リスク地域での、あるいは、ミュールとしての利用、あるいは詐欺被害が疑われるような暗号資産 ATM の利用

【発信者、受信者の観点からの主な手口】
- 口座ごとに定められた取引上限額、引出上限を解消するため異なる口座を開設する
- 認証されていない IP アドレス、経済制裁法域からの IP アドレス、既に疑わしいと認定された IP アドレスから発せられる取引
- 同一 IP アドレスが、同一 VASP に対して頻繁に口座を開設しようとする
- 法人顧客の場合、登記とは異なる法域もしくはドメイン登録プロセスが脆弱な法域のインターネットドメインからの口座開設
- 不完全、不十分な KYC 情報、もしくは顧客が KYC 文書や資金源に関する照会を拒否する
- 発信者、受信者が、取引、資金源、相手との関係について、知識がないもしくは、不正確な情報を提供する
- 偽造文書、編集された写真や本人確認資料を提供する
- 他のアカウントと同一 IP アドレス、フラッシュクッキー
- 顧客の属性に関連する IP アドレスと、取引が発せられた取引の IP アドレス間の相違
- 不法行為にひもづけられた暗号資産アドレス
- ミュール、もしくは詐欺被害者で、犯罪者に指示されたが、暗号資産技術やオンラインウォレットの知識に乏しい
- プラットフォームユーザーの平均年齢より著しく高齢の顧客が、口座を開設し、多数の取引を開始する
- 金融属性、背景から裏付けられないような多額の暗号資産を購入する
- email アドレス、IP アドレス、その他の情報を頻繁に変更する
- 同日中に異なる IP アドレスから VASP に取引を求める

【資金や財産の源泉の観点からの主な手口】

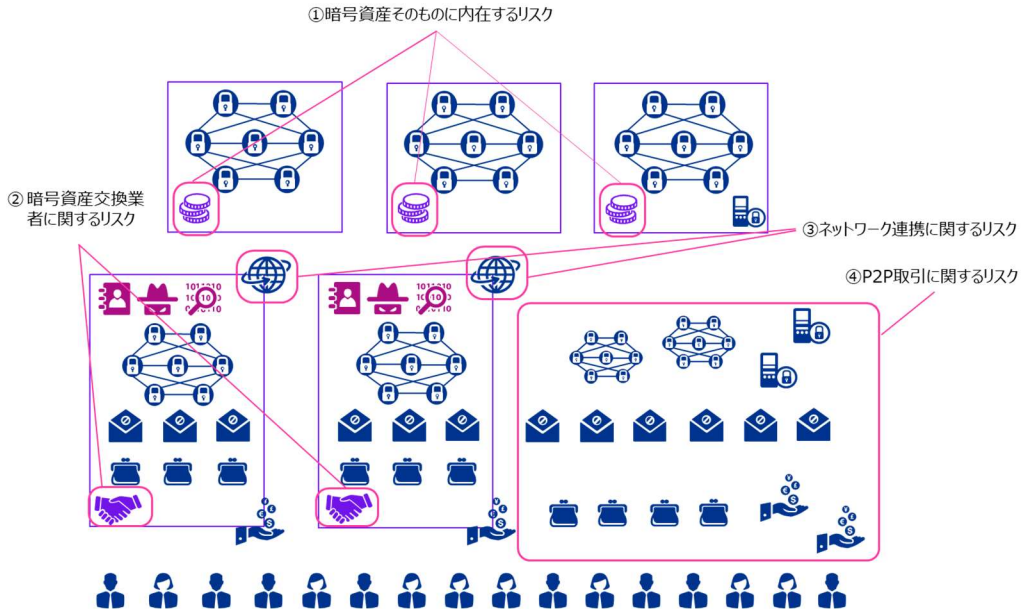
- 不正、恐喝、ランサムウェアスキーム、経済制裁対象者の住所、ダークネット市場、その他の不法ウェブサイトに関連付けられる暗号資産アドレスや銀行カード
- オンラインギャンブリングサービスとの暗号資産取引
- 暗号資産アドレスや口座への入金の資金源が不明で著しく高額
- シェルカンパニー等、経営実態のない企業の利用や、投資家名が入手できない ICO への払い込み等、資金源や資金の所有者に関する情報が不透明、不十分
- 暗号資産購入に係るクレジットカード、プリペイドカードからのオンライン支払の後、即座に引き出される
- 顧客の資金が、サードパーティミキシングサービス、ウォレットから送られている
- AML/CFT コントロールが欠如している VASP から暗号資産が送られた後引き出される

【法域の観点からの主な手口】

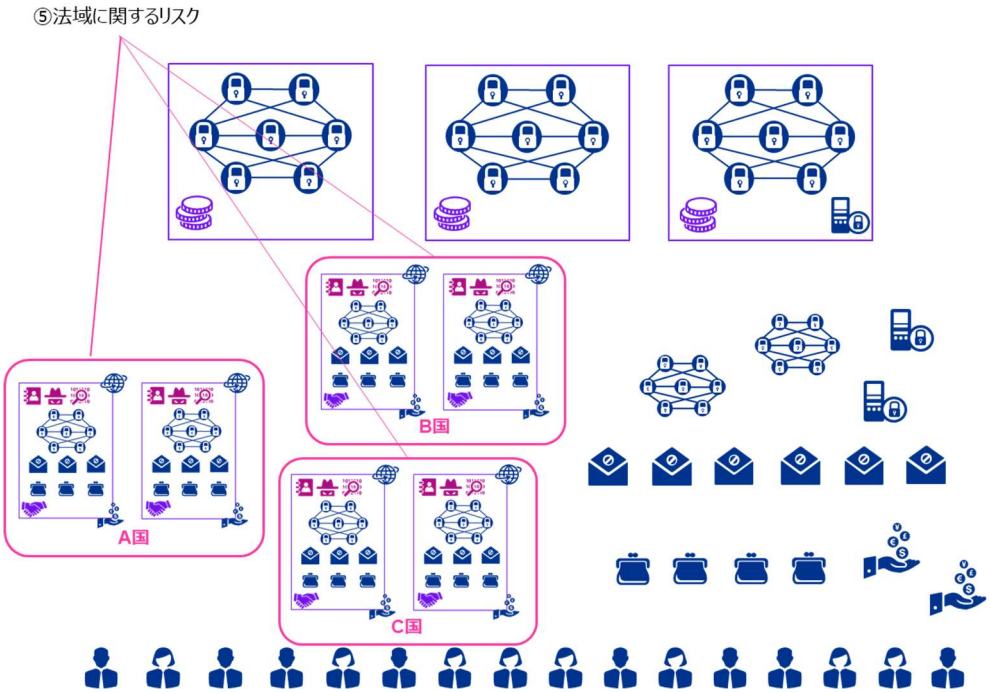
- 顧客の資金が、未登録の交換所との入出金に関連付けられる
- 顧客が、AML 規制が欠如もしくは不適切な法域の暗号資産交換所や不正な資金移動業者を利用している
- 顧客が暗号資産規制のない法域で運営している VASP へ送金する
- 顧客が、暗号資産関連規制のない法域に事務所を移転・開設する

5 暗号資産の ML/TF リスク

前セクションの悪用手口を基に、暗号資産の ML/TF リスク[14]を整理すると、①暗号資産そのものに内在するリスク、②暗号資産交換業者に関するリスク、③ネットワーク連携に関するリスク、④P2P 取引に関するリスク、⑤法域に関するリスクに分類[15]できる。このうち①～④は下図のように位置付けられる。



⑤はこのようなエコシステムの中で法域ごとのサブ・エコシステムが存在し、それらの間の格差・相違点という形で示すことができる。



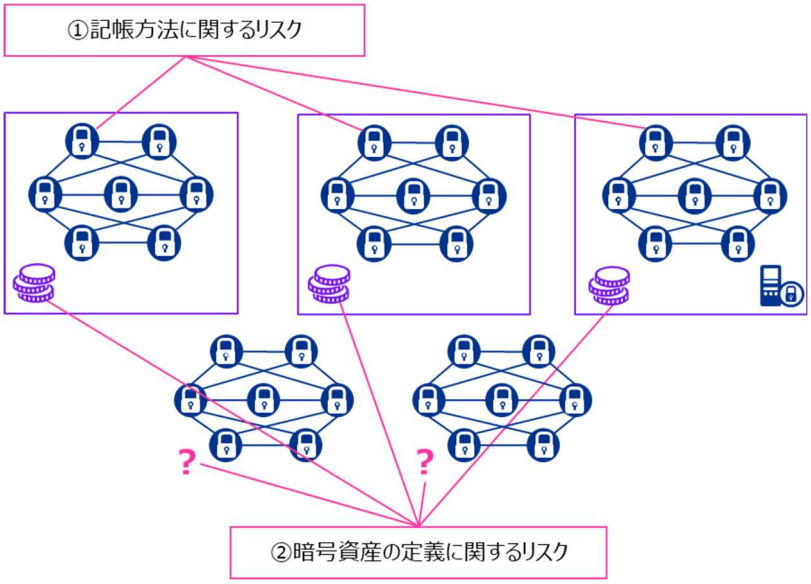
[14] 暗号資産の ML/TF リスクは、一般的にはリスクを被る主体によって多様に整理することができるが、本稿の趣旨に照らし、特に、規制・監督当局が留意すべきという観点で、金融システム全体に与えるリスクとして取り扱う。

[15] わが国においては、金融庁より「疑わしい取引の参考事例（暗号資産交換業者）」が公表されているが、これらの事例も、このリスク分類のいずれかに整理できる。

以下、それぞれのリスク別に考察を進める。

5.1 暗号資産そのものに内在するリスク

暗号資産そのものに内在するリスクは、①記帳方法に関するリスク、②暗号資産の定義に関するリスクに分けられる。前者は、暗号資産のベースとなる分散記帳技術自体に秘匿性[16]を増大させる要素が備わっていること、後者は新商品・サービスが次々と提供されており、これによって暗号資産の定義の射程があいまいになることに関するリスクである。



5.1.1 記帳方法に関するリスク

暗号資産はブロックチェーンという分散記帳技術（以下 DLT; Distributed Ledger Technology）を基盤としており、暗号資産取引の記帳方法は、「UTXO モデル」と「アカウントモデル」に大別される。モデルの違いによって、ML/TF リスクがどのように異なるのか、それぞれどのような対応が求められるかを以下に整理する。ここでは UTXO モデルの代表例としてビットコインと、アカウントモデルの代表例としてイーサリアムを取り上げる。

5.1.1.1 UTXO モデル（ビットコイン）

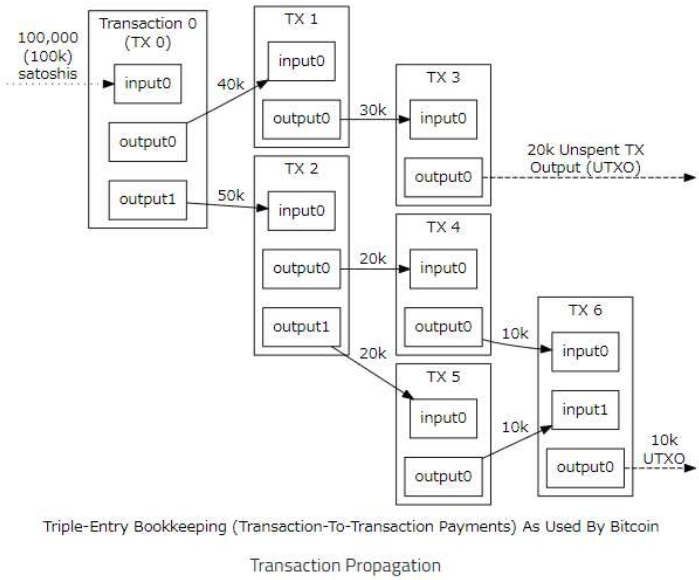
ビットコインとは、その名を冠する仮想通貨そのものであると同時に、その取引を支えるブロックチェーン基盤としての意味合いも含む。すなわち、ビットコインという基盤は、ビットコインという仮想通貨を流通させることを（少なくとも創設当初においては）単一の目的として構築されたものであると言うことができる。取引はトークンと呼ばれる価値の単位をやり取りすることで行われ、アドレス間のトランザクション（移動データ）としてブロックチェーンに記録される。

ユーザーはウォレットを用いて、秘密鍵、公開鍵を、さらにアドレスを生成し、このアドレスがトークンに紐づけられることによって、ウォレット上で当該トークンを保有していると認識することができる。

[16] 本章において秘匿性とは、その取引の真の主体者をわからなくする匿名性に加え、その取引の真の目的をわからなくすることもあわせたものと定義する。

トークンは分割できない仕組み[17]となっており、取引の際には、①当初保有していたトークンを費消し、②相手のアドレスを指定したトークン（送金用）と③自分のアドレスを指定したトークン（おつり用）の２つのトークンを新たに生成する。②③の金額の合計は①の費消されたトークンの金額以下とすることが仕様上求められており、この差額が、マイニング手数料[18]と認識される。

ユーザーが利用するウォレットにもよるが、取引の秘匿性を高めるため[19]、一般的に取引の都度異なるアドレスを設定する仕様となっており、この場合、上記の例で言えば、①の当初保有していたトークンでのアドレスと、③のおつり用のアドレス（さらに言えばおつり取引におけるインプットアドレスとアウトプットアドレス）は同じではない。



Bitcoin Developer Guides より（Block Chain — Bitcoin）

このような取引の結果としてのユーザー自身の保有残高は、ブロックチェーン上のすべてのトークンのうち、自分のものと認識されるアドレス宛の未使用トークン（UTXO; Unspent Transaction Output）の金額の合計を計算することによって得られる[20]。これが UTXO モデルと呼ばれる所以である。

既述のとおり、このユーザーは複数のアドレスを有しているが、これをウォレット上合算することで、最終的にユーザ

---

[17] 法定通貨としての紙幣をイメージすると、五千円を支払うのに一万円札を半分に切って渡しても決済できないのは明らかであり、一万円を渡して五千円をおつりとして受領することを想像するとわかりやすい。ただし紙幣の例では、五千円札一枚と一万円札一枚がもともと存在していることが前提であるが、UTXO の場合は、厳密には、最初の一万円のみがトークンとして存在しており、これが支払いとともに費消（消滅）し、代わりに五千円が二枚新たに生成され、一枚を受取人に渡し、もう一枚をおつりとして手元に残すということになる。

[18] ブロックチェーンを生成するための計算処理を行い、ビットコインの取引を承認したマイナーに支払われる手数料を指す。

[19] 必ずしも ML/TF 目的等での悪意の秘匿を意味するものではない。パブリック型のブロックチェーンの性質上、アドレスがすべて公開されるということは、当該アドレスと個人情報が一旦関連付けられてしまえば、当人が行った過去の取引全てが全世界に知られてしまうことに他ならず、これを保護したいというニーズは合法である限り正当なものである。

[20] 先の法定通貨の例に戻れば、自分の現金残高は、手元で保有する紙幣（つまり未使用のもの）を合計すればよいのと同じである。ただし、暗号資産は、物理的に手元にあるという概念がない。一方でブロックチェーン上には創設以来のすべての取引のアドレスが記録されている。これは現実世界において、個々の紙幣が発行されて以来、点々流通する過程で、これを入手したすべての人物の名前（アドレス）が、当該紙幣上に時系列で記載されているようなものである。そのような世の中に流通するすべての紙幣のうち、最後に自分の名前が記載されているものの紙幣の金額を合計することが、すなわち、このようにブロックチェーン上のすべての取引のうち自分のアドレス宛となっている未使用トークン（UXTO）を計算することと同義である。

ーの保有残高を知ることができる。ウォレットはブロックチェーンの外のデバイスに存在することから、ブロックチェーン上では、当該ユーザーに関連する複数のアドレスが存在するだけであり、それが同一人物によって紐づけられていることを確認できるのは、このウォレットを保有するユーザー自身のみであるということが確保される仕組みである。

5.1.1.2　アカウントモデル（イーサリアム）

次にアカウントモデルの代表であるイーサリアムについて解説する。イーサリアムはビットコイン同様、仮想通貨であると同時に、ブロックチェーン基盤としての意味合いも含む。イーサリアムは、大学を中退した 19 歳の若者、ヴィタリック・ブテリンが発表したホワイトペーパー[21]で構想されたものである。資金移動に特化したビットコインと大きく異なるのは、仮想通貨を流通させることのみを目的とせず、分散型アプリケーションやスマートコントラクトを構築するための汎用的なブロックチェーンプラットフォームとして設計されている点である。この点で、単一通貨流通を目的とした取引中心のデータモデルであるビットコインとは大きく異なっており、より広範な適用領域を想定したうえでのデータモデルを検討した結果の一つとして、契約主体の残高をアカウントとして直接表現する（取引はアカウント間の移動として認識する）ことを選択したものと推察される。

イーサリアムの開発者向け文書[22]では、アカウントは、nonce, balance, codeHash, storageRoot の 4 つのフィールドを持っており、balance は当該アドレスによって保有される数量（すなわち残高）を示すと定義されている。

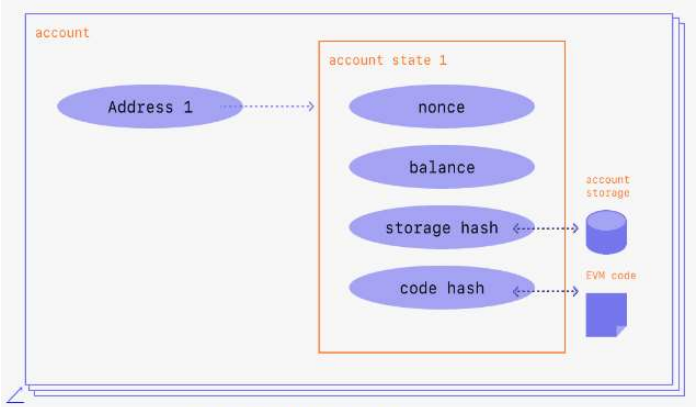


Diagram adapted from Ethereum EVM illustrated

アカウントモデルは直感的にも理解しやすい[23]。また、テザー(USDT)、USD コイン(USDC)、バイナンスコイン(BNB)といったイーサリアム以外の仮想通貨だけでなく、分散型アプリケーションやスマートコントラクトの基盤を活用し、DeFi や NFT 等の新たな金融サービス[24]も数多く開発、運用されている。アカウントモデルの場合、暗号資産保有者が利用することになるウォレットは、アカウント利用の利便性を享受するため、アドレスを変えない仕様となっていることが一般的である。

UTXO モデルとの主な違いは、おつり取引が発生しないこと、残高把握は UTXO のような負荷のかかる計算を

[21] このペーパーは 2014 年に公表されて以降、イーサリアムの開発コミュニティによって更新、管理されている。(https://ethereum.org/en/whitepaper/)
[22] Ethereum accounts | ethereum.org (https://ethereum.org/en/developers/docs/accounts/)
[23] UTXO モデルを紙幣にたとえるとすると、アカウントモデルは預金口座にたとえることができる。
[24] 金融サービス以外にも、婚姻届出、キャラクター育成ゲーム等のサービスが提供されており、分散型アプリケーションやスマートコントラクトに基づく汎用的ブロックチェーンプラットフォームとしてのイーサリアムの適用範囲は幅広い。

要しないことの二点である。一方で、手数料が発生することは同じである。[25]

5.1.1.3　UTXO モデルとアカウントモデルの ML/TF リスク比較

UTXO モデル、アカウントモデルそれぞれの記帳方法の違いによる ML/TF リスクを、①固有リスク、これに対処するための②リスク低減策、さらにその結果としての③残存リスクと三段階にわけて考察する。

① 固有リスクに関しては、おつりの存在と取引ごとにアドレスを自由に変えられることとの関係性において整理することができる。

アカウントモデルの世界から見ると発生し得ないおつりが、UTXO モデルでは、不可避的に発生する。このおつりについては以下の問題が存在する。すなわち、手数料が個々の取引としてではなく、取引の差額として認識されるため、①決済の原資となるべく費消したトークンの金額と、②支払のためのトークン＋③おつりトークンの金額が一致しないこと、①のトークンのアドレスに対し、③のおつりを受け取るアドレスを変えることが一般的な実務となっていることから、そもそも、おつりトークンであることが判別困難であること、さらにそのような判別困難な取引が不可避的に発生することによって決済ネットワークの相当部分を占めてしまうことの二点である。これに比して、アカウントモデルは、そもそもおつりが存在しないこと、かつアカウント利用の利便性から同一アカウント、同一アドレスの繰り返し利用が、UTXO モデルに比べてより一般的となっていることが特徴と言える。ネットワーク全体として取引の透明性が高い方が、不自然な取引を特定しやすいという観点から、記帳方式そのものに内在する ML/TF の固有リスクは、アカウントモデルに比べて UTXO モデルの方が大きいということが言える。

② このような固有リスクに対するリスク低減策としては分析ツールの活用が考えられる。

パブリック型ブロックチェーンは、一般に匿名性が高いと言われるが、厳密には疑似匿名性であり、取引の宛先がアドレスという識別子で管理され、そのブロックチェーンが創設された時から現在までのすべての取引がブロックチェーン上で公開されている。

このような公開ブロックチェーン上の取引履歴を活用したデータ解析ツールが注目されている。たとえば FATF が実施した暗号資産および暗号資産交換業者に関する調査「Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs」[26]では、Chainalysis, CipherTrace, Coinfirm, Elliptic, Merkle Science, Scorechain, TRM Labs の 7 社のブロックチェーン分析企業による分析データが活用されている。今回の調査の一環として実施したブロックチェーン分析企業および暗号資産交換事業者へのヒアリングでは、おつり取引であること、そのおつりがどの取引に基づくものなのか、異なるアドレスの複数取引が同一ウォレットないしは同一ユーザーによるものなのかの特定は、ある程度の確度を以て可能になってきているようである。具体的には、大量の取引の中から一定の特徴量を把握することによって一群の取引をグループ化するクラスタリング分析やノード間の通信に用いる IP アドレス情報等を活用したネットワークのプロトコル分析によって、秘匿性を下げ

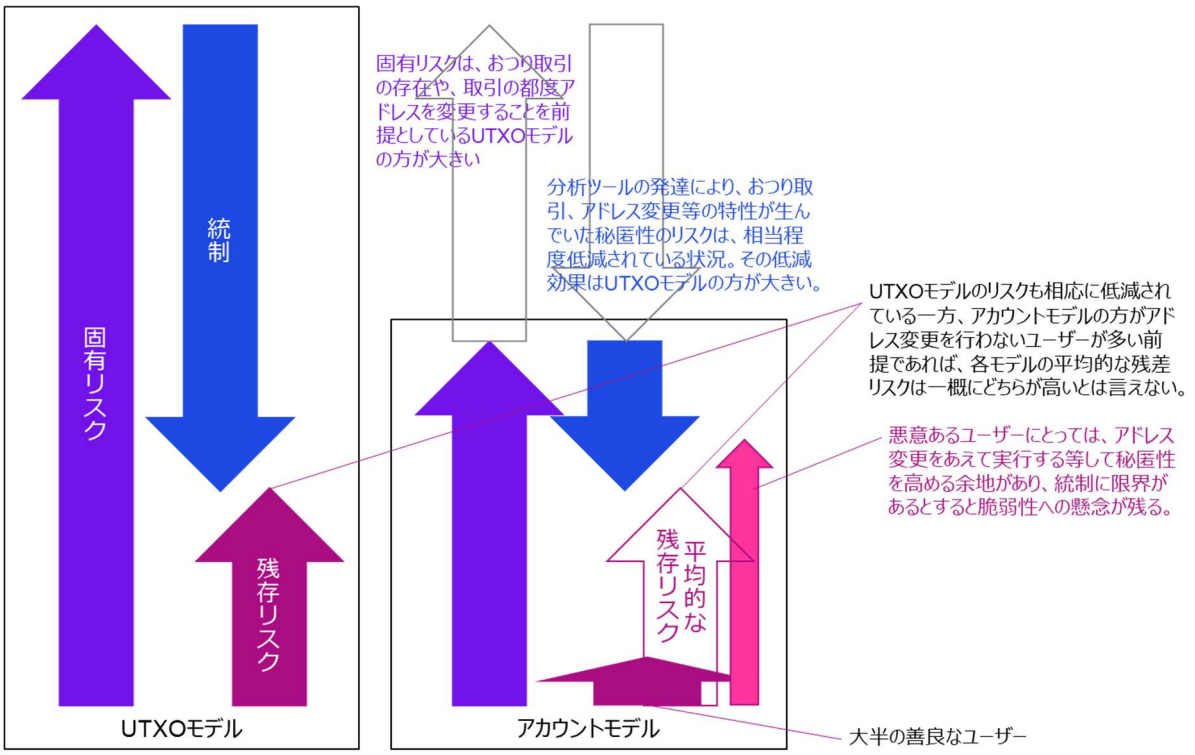
[25] なおイーサリアムのプラットフォームを利用した暗号資産、NFT 等には、取引手数料に加えてイーサリアムのスマートコントラクトの利用料も付加される。この二つを合わせた手数料がいわゆるガス代である。このような取引が増えるとイーサリアム全体のネットワークに負荷がかかり送金スピードが落ちることから、これを回避するためにガス代という手数料を課してコントロールする仕様となっていると言われている。これによってたとえば DDoS 攻撃を防ぎやすいといったメリットもある一方で、NFT 人気が過熱した際のガス代高騰が問題となることもある。ガス代あるいはそのヴォラティリティの高騰は、価格発見機能等の流動性リスクの問題をはらむが、ガス代の受取人はマイナーないしはバリデーターであることは明らかであり、本稿では ML/TF リスクとしての要素は小さいものと整理し考察の対象外とする。

[26] Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs, FATF, July 2021. (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html)

られる効果が確認されているとのことである[27]。

一見、邪魔とも思えるおつり取引も、データアナリティクスの観点からは、実はおつり取引としての性質や、原取引との関係性を検出するに足る貴重な情報源となり得るということを示唆している。すなわち、固有リスクとして、アカウントモデルの方が取引の透明性が高いと一旦整理したものの、実は、むしろアカウントモデルの方が、取引の性質を把握する情報量に乏しいということもできる。

③　上記①②を整理して残存リスクについて最後に考察する。



上図のとおり、固有リスクは UTXO モデルの方が大きいが、同時に統制も強い（分析ツールの導入効果が大きい）と考えられ、残存リスクについての相対的な多寡の判断は難しい。ただし、これはアカウントモデルの一般的なユーザー層（同一アカウントに同一アドレスを紐づけており、アドレスを頻繁に変更しない）を想定した平均的なリスク属性である。アカウントモデルでは、アドレス変更ができないわけではなく、悪意あるユーザーは、アカウントモデルの利便性よりも秘匿性を優先させようと思えば、アドレスを都度変更することによって、ML/TF を敢行しやすいという点に着目すると、アカウントモデルの方が残存リスクは大きいと考えることもできる。アカウントモデルを適用しているイーサリアムは、分散アプリケーション、スマートコントラクトといったより広範なプラットフォームとして、既に多くの暗号資産で利用されており、アカウントモデルに基づく暗号資産の利用を認めない措置をとることは現実的ではない。分析手法の一層の高度化に期待する他、ウォレットサービスプロバイダへの統制を強めるといったこと等が想定される。当面はこのような記帳方式の違い等によるリスクプロファイル、顕在事象等の情報を注視していく必要がある。

なお、ここまでの考察は、実は、ユーザーが暗号資産のブロックチェーンネットワークに対し、一ノードとして、いわば素の P2P で（すなわち unhosted wallet で）参加するという前提に立ったものである。大半のユーザーは、一

[27] このような分析ツールについては、「6.8 分析手法」において考察する。

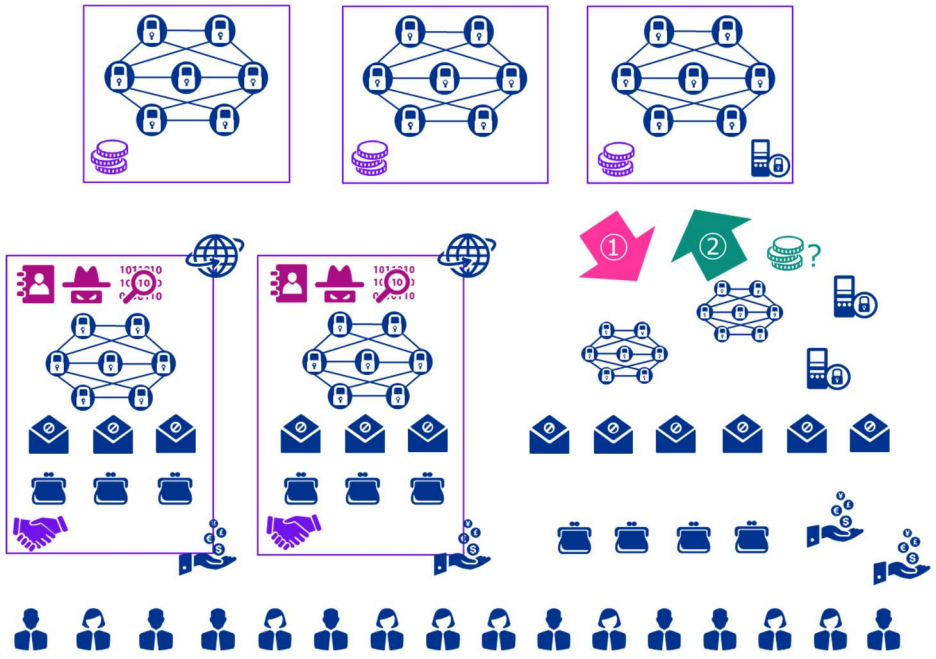
般的な暗号資産交換業者で口座を開設し、当該業者が提供する販売所、もしくは取引所で取引を実施するものであり、当該ユーザーの取引は、暗号資産交換業者が具備する AML/CFT 管理体制の下で、適切に取引時確認、取引モニタリングの対象となっており、これが適切に行われる限り、上記のモデルの違い、アドレス変更可能性といった要素の ML/TF リスクへの影響はほぼないと考えられる。

このような P2P での取引と、暗号資産交換業者が提供する販売所、取引所での取引とは、それぞれのネットワークが異なることから、その連携上のリスクが存在する。これについては、「5.3 ネットワーク連携に関するリスク」において考察する。

5.1.2 暗号資産の定義に関するリスク

暗号資産の ML/TF リスクに関して、従来は、規制下にある伝統的な金融システムとの間で発生する暗号資産に関連する活動として捉えてきた。しかしながら、暗号資産関連市場では、様々な新商品・サービス、ビジネスモデルが次々と生まれ、これにともなってその活動、相互作用も多岐にわたっている。たとえば、秘匿機能を有する仮想通貨、ミキサー、分散プラットフォーム、分散取引所、プライバシーウォレット等の商品、サービスは、資金の流れの透明性を減少させ、ICO 等の新たなビジネスモデルは ML/TF リスクだけでなく、不正や相場操縦のリスクも伴う。

このような観点で、暗号資産の定義は、技術要素に対して中立であり、かつ関連する金融資産が FATF 基準でカバーされないということがないように拡張的である必要があると FATF は述べている[28]。すなわち、加速度的に発展する暗号資産市場において、新たな新商品・サービス、ビジネスモデルが登場することで、それまでの暗号資産の定義にはまらない、ないしはその定義をあいまいにさせるような要素が発生することが暗号資産の定義に関するリスク（下図①の矢印 ➡）として存在し、これに対しては、特定の技術にしばられることなく、幅広に、かつ拡張的に暗号資産の定義を適用し、FATF 基準でカバーされないような金融資産が存在する余地をなくすという措置（下図②の矢印 ➡）が必要であるということである。



[28] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org) (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf)

このリスクについて、当局として対処すべき方向性としては、主に以下のようなことが考えられる。これについては「6 規制・監督上の課題」にて取り上げる。

- 規制・ガイドライン：暗号資産の定義の明確化、暗号資産交換業者が取り扱うべき暗号資産の範囲の明確化とこれらの適時の更新
- 改善・制裁措置：規制に照らして許容できない暗号資産や関連サービス事業者に対する厳格な措置
- コミュニケーション：当局が期待する事項の暗号資産交換業者への徹底と、民間とのリスク・コミュニケーション促進、グローバルな動向把握に資する各国当局との連携
- リスク評価・調査分析：市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査
- インフラ：上記各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用

本セクションでは、このような代表例として、ステーブルコイン、NFT、ICO を取り上げて、定義の拡大性についての論点を整理する。

5.1.2.1 ステーブルコイン

ステーブルコインは、価格変動性が高く、決済に利用というよりはむしろ投機対象としての性格が強い、従来の仮想通貨に対するアンチテーゼとして登場したと言ってよい。ステーブルコインは、「特定の資産、もしくはそのプール、バスケットの価値に連動して安定的な価値を維持する暗号資産」[29]というのが本来あるべきものとしての定義と考えられるが、後述するように、実態としてはこの定義から乖離したものがステーブルコインとして市場に存在している。

まず、主要法定通貨のバスケットと連動して決まる仕組みとして、2019 年にフェイスブック社が「Libra」発行を宣言[30]すると、ステーブルコインは一躍脚光を浴びることとなった。ステーブルコインは金融包摂に資する、中央集権的管理コストが低減される、プライバシーが確保される、グローバルな資金移動が迅速かつ安価で実現する等として前向きに評価される一方で、特に、金融当局からは、①金融安定、②利用者保護、③ML/TF リスクの観点での懸念が表明されてきた。

①に関しては、金融当局が、金融安定という政策目的を達成するための手段として通貨を位置付けている一方、ステーブルコインの登場によって、政策目的達成の手段としての有効性が阻害され、金融危機等のリスクが高まるという懸念である。2020 年 10 月、FSB はいわゆるグローバルステーブルコイン（GSC）に関する規制・監督に関する勧告文書を公表し、2022 年にはその見直しを実施している。この中で FSB は、国際標準の監督指針の導入、グローバルな協力体制の構築、仲介業者等への規律の徹底、インフラや破綻計画の明確化や透明性、払戻しの権利の確保などについて言及している。これらすべてが具備されていない場合は、GSC を許可すべきではないとしている[31]。

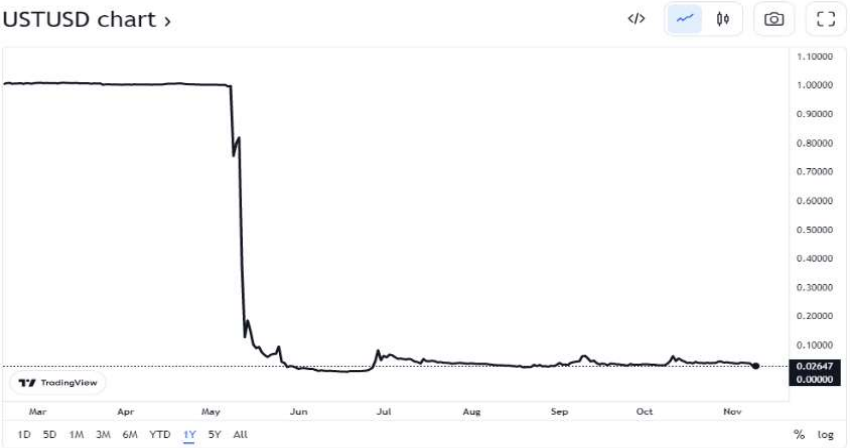
②の利用者保護に関する懸念は、ステーブルと標榜しているにもかかわらず、実際はステーブルでなかった（価格下落損失を被った）という事例が相次いだ、という観点である。ステーブルコインがその定義通り、特定の資産等に連動して安定的な価値を維持する方法としては、①裏付け資産型（裏付けとなる資産を確保することによ

[29] Crypto-assets and Global “Stablecoins” - Financial Stability Board (fsb.org) (https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/)
[30] Libra LIBRA whitepapers - whitepaper.io (https://whitepaper.io/document/475/libra-1-whitepaper)
[31] Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Consultative report (https://www.fsb.org/2022/10/review-of-the-fsb-high-level-recommendations-of-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-consultative-report/)

り、参照資産（法定通貨など）との価格の連動を図るもの）と②アルゴリズム型（アルゴリズムを用いて通貨の需給調整をすることにより、参照資産との価格の連動を図るもの）に大別される。

ところが①に関しては、たとえばテザー（USDT）は、価値に見合うドル建て資産が確保されていないのではないかと市場でうわさされ、ドル等価から乖離する状況が見られた。2019 年 4 月ニューヨーク州司法長官は、USDT の発行元が損失の穴埋めにテザーHD の準備資産を流用したとして裁判所に提訴し[32]、その後、アメリカの商品先物取引委員会（CFTC）は、テザー（Tether Holdings Limited, Tether Limited, Tether Operations Limited, および Tether International Limited の各社）に対して、十分な準備資産を保有していることについて、真実と異なる、ミスリーディングで、かつ重要情報を含まない情報公表を行ったとして 41 百万ドルの課徴金支払を命じた[33]。この期間に先立つ 2017 年後半から、USDT は十分な資産を用意していないのではないかとの憶測から、ドル等価から乖離する状況が見られた[34]。

同様に②に関しても、たとえば、テラ（UST）は、アルゴリズムが想定通りに機能せず、大幅な価格下落を招き、ほぼ無価値の状態で取引を終了した[35]。



[32] Attorney General James Announces Court Order Against “Crypto” Currency Company Under Investigation For Fraud (https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company)
[33] CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million | CFTC (https://www.cftc.gov/PressRoom/PressReleases/8450-21)
[34] Tether price today, USDT to USD live, marketcap and chart | CoinMarketCap (https://coinmarketcap.com/currencies/tether/)
[35] USTUSD Charts and Quotes — TradingView (https://www.tradingview.com/symbols/USTUSD/)

このように「ステーブルではない」ステーブルコインという形態が現に発生していることも各国金融当局の懸念するところであり、FATF もこの問題に対しては So-called、すなわち「いわゆる」ステーブルコインに関する問題として G20 に対して「FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins」と題する報告書[36]を提出している。バーゼルも同様の観点で、ステーブルコインを、以下のテスト基準を満たすものを Group A、満たさないものを Group B と分類する案[37]を提示している。

- 償還リスクのテスト：ストレス時においても、ペグされた値で償還できるだけの準備資産が確保されているか
- 価格差テスト：過去 1 年間で 10bp 以上の価格乖離が 3 回以内かどうか

このような動きを踏まえて、わが国でも世界に先駆ける形で法整備が行われた。すなわち 2022 年 6 月に成立した改正資金決済法[38]では、第 2 条第 5 項で「電子決済手段」が新たに定義され、当該手段は「電子機器その他の物に電子的方法により記録されている通貨建資産に限り」と整理されている。通貨建資産とは同条第 7 項にて、

> この法律において「通貨建資産」とは、本邦通貨若しくは外国通貨をもって表示され、または本邦通貨若しくは外国通貨をもって債務の履行、払戻しその他これらに準ずるもの（以下この項において「債務の履行等」という。）が行われることとされている資産をいう。この場合において、通貨建資産をもって債務の履行等が行われることとされている資産は、通貨建資産とみなす。

と規定されており、「法定通貨の価値と連動した価格（例： 1 コイン＝ 1 円）で発行され、発行価格と同額で償還を約するもの（およびこれに準ずるもの）」、すなわち裏付け資産型を電子決済手段として規律し、アルゴリズム型は電子決済手段ではなく、暗号資産型として、暗号資産や金融商品として規律するものとされている[39]。

さらに、「電子決済手段」の売買や交換、その媒介、管理などを行う行為は「電子決済手段等取引業」として（同条第 10 項）、改正法に基づく登録を取得することが求められる。電子決済手段等取引業者は、電子決済手段について利用者のものと自己のものの分別管理と、その管理の状況についての監査を受けることを義務付けられ（第 62 条の 14）、事業年度ごとの電子決済手段等取引業に関する報告書の作成と、当該報告書については、財務に関する書類、当該書類についての公認会計士または監査法人の監査報告書その他の内閣府令で定める書類の添付が義務付けられている（第 62 条の 19）。

③の ML/TF リスクについては、以下のように整理できる。

まずステーブルコインに対して指摘されている ML/TF リスクの懸念（たとえばグローバルな資金移転が容易、秘匿性が高い等）は、暗号資産全般に対するものと変わらない。ただし、ステーブルコインの特性に照らすと、①広範適用、②P2P 取引の 2 点について特に留意すべきと考えられる。

1 点目の広範適用（mass-adoption）について考察する。暗号資産は、相応の関心を集めているとはいえ、必ずしも社会に広く遍く利用が行きわたっているというわけではなく、投機対象としての性格が強い。一方で価格

---

[36] FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf)

[37] Second consultation on the prudential treatment of cryptoasset exposures, June 2022, Basel Committee on Banking Supervision 上記はいくつか示されているもののうち主要なテストのみを列挙したもの。(https://www.bis.org/bcbs/publ/d533.pdf)

[38] 改正資金決済法 (https://www.fsa.go.jp/common/diet/index.html)

[39] 説明資料　安定的かつ効率的な資金決済制度の構築を図るための 資金決済に関する法律等の一部を改正する法律案 (https://www.fsa.go.jp/common/diet/208/03/setsumei.pdf)

変動がないステーブルコインは、決済目的での広範適用が想定される。そうなると ML/TF の手段としての利用価値も同時に高まるため、「同じビジネス、同じリスクには同じルールを適用する」という原則[40]に基づけば、広範に決済に利用されている既存のサービスや同サービスを提供している事業者と同等のルールがステーブルコインや関連事業者に適用されるべきである。この点で、サービスの導入や、事業者の新規参入・立上げが目覚ましいステーブルコインに対しては、同等のルールが適用され得るのか、適用されたとして事業者が適切に遵守できるのかという課題がある。

わが国においては、既述のとおり、ステーブルコインは電子決済手段として資金決済法上位置付けられる。電子決済手段等取引業者は、犯罪収益移転防止法上の特定事業者とされ、AML/CFT 関連規制の遵守義務を負う形となっており、AML/CFT 制度面の手当てについては、整理ができていると考えられる。また、海外では、関連サービスの進化・分化に伴い、発行と仲介（カストディ、交換、トレーディング・プラットフォームの運営）それぞれの機能に求められるべき規律が異なるとして、それぞれに異なる規制を課す傾向があるが[41]、わが国においても、既述の改正資金決済法で、電子決済手段の仲介機能を担う電子決済手段等取引事業者が創設されており、電子決済手段においても発行と仲介の機能の違いに対応した規制が整備されている[42]。今後はその運用における実効性をどのように確保していくかを注視していく必要がある。

次に②の P2P に関する論点とは、AML/CFT 規制は、基本的に事業者単位で義務付けを行う構造となっているところ、当該規制が及ばない P2P 取引において広範適用が拡大するのではないかとの懸念である。この点に関して、ステーブルコインは、何らかの中央管理機能（開発者、監督者）を担う主体が想定され得る。この場合、開発者、監督者が金融機関ないしは暗号資産交換業者として規制されるべきであるということになる。このような包括的な事業者がいないような分散構造のサービスであったとしても、広範適用の過程において、顧客接点、交換、ウォレットサービス等のサービスを提供する事業者が何らかの形で関与することが想定される。このような事業者を AML/CFT 規制下に置くことで ML/TF リスクは抑えられるはずであり、規制すべき事業者が全くいないステーブルコインが広範適用されるというリスクは小さいのではないか、というのが現時点での FATF の見解[43]である。ただし、これは、何らかの形で関与している事業者が適切に AML/CFT 規制の対象になっていることが確保されていることが前提であり、この観点でも、既述の事業者の機能分化とそれに応じた柔軟、かつ過不足のない適切な法制度の構築は重要と考えられる。規制・監督の立場からは、ステーブルコインのサービス導入前に、リスクが十分分析され、未然に低減されていることを確保することが極めて重要である。事業者が何らかの形で関与しているのであれば、適切に暗号資産交換業者等として金融規制・監督の枠組みに取り込むべきという観点については、ステーブルコインに限らずすべての暗号資産に共通するものであり、暗号資産交換業者に関するリスクとして後述する。

5.1.2.2　NFT

NFT; Non Fungible Token は非代替性トークン等と訳される。トークンとは、分散台帳上の残高記録であり、電子情報処理組織を用いて移転することができる財産的価値のことである。トークンの代表例である仮想通貨

[40] 金融庁プレスリリース 2020 年 10 月 13 日 (https://www.fsa.go.jp/inter/fsf/20201016/201016_21.pdf)
[41] 金融庁 金融審議会「資金決済ワーキング・グループ」報告　2022 年 1 月 11 日 (https://www.fsa.go.jp/singi/singi_kinyu/tosin/20220111/houkoku.pdf)
[42] 暗号資産では、発行者は規制対象となっていないが、暗号資産交換業者が、仲介者として規制の対象となっている。
[43] FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf)

のように代替性を有するものがある一方、代替性がないものが NFT に分類される。NFT は、唯一性の証明をデジタル空間で実現でき、それゆえに、時に希少性を伴う、さらには、たとえばイーサリアムのスマートコントラクト機能等によってデジタル情報として手軽に取引しやすいという特徴を有する。VR アートや音楽コンテンツ、トレーディングカード、ゲームのキャラクターやアイテム、メタバース上の土地区画等が続々と NFT として登場し、時に高額取引が話題となることも多い。一方で、NFT のマーケットプレース上では、その本人性が定かではないもの、NFT によって裏付けされるコンテンツが盗品、偽造品、海賊版でないことが確認できないもの等が少なからず取引されているとも指摘されている。マーケットプレースを騙るフィッシングメールにより NFT のアカウントがハックされて、NFT の所有権が攻撃者に渡ってしまう事件も報告されている。

本セクションの主題である暗号資産の定義に関するリスクという観点では、以下のように整理される。

NFT は、デジタルデータの所有を主張する証であり、必ずしも決済あるいは投資目的で利用することを想定しているわけではない。この意味では NFT は暗号資産には該当しないが、その該当性は NFT といった名称によって判断されるべきではなく、実態上決済や投資目的で利用されているかどうかで判断されるべきであると FATF は指摘している[44]。したがって、その判断は、当該 NFT と、その機能に着目し、どのように利用されているのかを踏まえる必要がある。この点で、NFT の暗号資産への該当性、あるいは FATF 基準への該当性については、ケースバイケースで検討しなければならない。

ある分析業者の報告書[45]によれば、NFT はいわゆる wash trading という手口に悪用されている。すなわち、NFT の売り手となる一方、売り手自身であることを秘匿して買い手となるものである。多くの NFT 取引プラットフォームは本人確認の必要がなく、利用者として登録して自身のウォレットを示せば手軽に NFT の売買が可能となっている。買い手を装ったアドレスは、多いケースで 300 を超える場合もある。新たに買い手となって拠出した資金はいずれ何らかの形で回収する必要があるところ、取引上発生するガス代も含めると損失を被るケースもあるものの、何らかの形で売り逃げてかなりの資金を回収しているケースも確認されているとのことである。

5.1.2.3 ICO

ICO; Initial Coin Offering とは、資金調達をしたい事業者や事業プロジェクト実施者が、独自の仮想通貨（コイン）を発行し、資金を調達することである。発行者または発行者の依頼を受けた販売者は、法定通貨もしくは他の暗号資産と交換で、コインを提供する。通常、ICO はオンライン上のホワイトペーパーと呼ばれる文書で事業と ICO の内容が公表される。ホワイトペーパーには、たとえば調達した資金が、デジタルプラットフォーム、ソフトウェア、その他のプロジェクト開発に投下され、当該開発が完了したあかつきには、発行コインで、開発されたプラットフォーム、ソフトウェア等を利用することが可能となること等が謳われる。投資家は、プラットフォーム、ソフトウェア等の利用の他、暗号資産の取引プラットフォーム等のセカンダリー市場でコインを転売することで、投資リターンを得られるとの期待の下にコインを購入する。

ICO のリスクは、ホワイトペーパーで記載された事業計画通りに事業が進まず、プロジェクトが行き詰まったり、経営が破綻することによってコインの価格が下落、さらには無価値になってしまう投資リスク、そもそもホワイトペーパーに掲げたプロジェクトが実施されなかったり、約束されていた商品やサービスが実際には提供されないといった詐欺

[44] Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, FATF, July 2021.

[45] The 2022 Crypto Crime Report.pdf (chainalysis.com) (https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf)

リスクが考えられる。

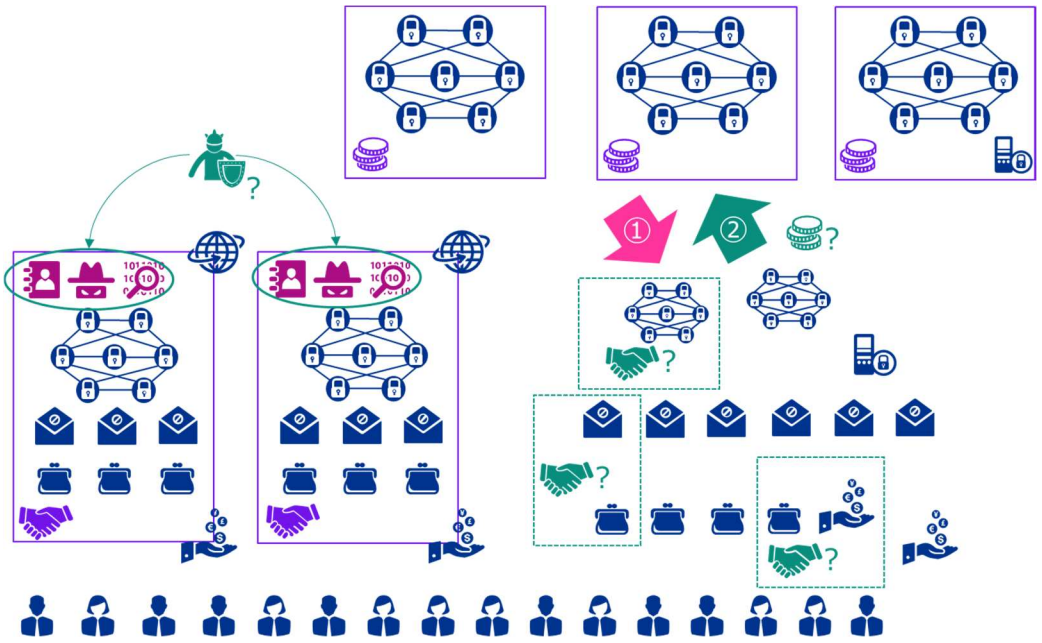
ここでは、ICO 対象となるデジタル資産が、①暗号資産かどうか、②「暗号資産の発行や販売への参加および金融サービスの提供」等の観点に照らして暗号資産交換事業者と特定できる事業者が存在するか、さらには、当該デジタル資産が、③有価証券に該当するか、④金融商品関連法令に照らして金融商品取引業者と特定できる事業者が存在するかがポイントとなる。[46]

わが国においては、既に 2017 年の段階で、金融庁が注意喚起[47]を行っており、ICO において発行される一定のトークンは資金決済法上の暗号資産に該当し、その交換等を業として行う事業者は内閣総理大臣（各財務局）への登録が必要になることを示している。

関連して、既述のようなリスクへの対策となり得る代替サービスとして、STO; Security Token Offering や IEO; Initial Exchange Offering 等が提供されている。前者は、ICO の対象となるコインを明示的に金融商品取引法規制の対象とし、同規制に基づいて資金調達を実施するものであり、後者は、ICO の対象となるコインを、規制に基づいて登録、認可済みの暗号資産交換事業者が、その責任において ICO プロジェクトを企図する企業と契約を交わし、暗号資産交換事業者の責任において、その顧客にコインを販売するものである。

5.2 暗号資産交換業者に関するリスク

暗号資産交換業者に関するリスクは、暗号資産などのエコシステムにおいてどの程度暗号資産交換業者を通して ML/TF のリスクをコントロールできるかという①暗号資産交換業者の定義のリスクと、特定された暗号資産交換業者間での②AML/CFT コントロールの格差のリスクに分けて考えることができる。



①のリスクは、加速度的に発展する暗号資産市場において、新たな商品・サービス、ビジネスモデルが登場する中で、何らかの形で関与している事業者を、暗号資産交換業者としてどこまで特定できるか（上図の　　）とい

[46] ②は「5.2 暗号資産交換業者に関するリスク」で触れる。③、④は本稿の対象外とする。

[47]「ICO（Initial Coin Offering）について ～利用者および事業者に対する注意喚起～」29.10.27 金融庁 (https://www.fsa.go.jp/policy/virtual_currency/06.pdf)

うことであり、②のリスクは、特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できるか（上図の  ）ということである。①は「5.2.1 暗号資産交換業者の定義のリスク」として、②は「5.2.2 暗号資産交換業者のリスク」として、それぞれ以下で考察する。

5.2.1 暗号資産交換業者の定義のリスク

暗号資産交換業者の定義のリスクについて、まず拡大する暗号資産関連の商品、サービス、テクノロジーに伴って同時並行的に進化する事業者としてのビジネスモデルを整理[48]する。本稿でも採用した FATF の暗号資産交換業者の定義では、以下の 5 つが整理されており、これが暗号資産交換業者のビジネスモデルを構成する機能と考えられる。

i. 暗号資産と法定通貨の交換
ii. 暗号資産同士の交換
iii. 暗号資産の移転
iv. 暗号資産の保管・管理、または暗号資産の管理を可能とする方法の提供
v. 暗号資産の発行や販売への参加および金融サービスの提供

このうち、i, ii は、暗号資産交換業という呼称にふさわしい機能といえ、一般に販売所、交換所として提供されている。販売所とは暗号資産交換業者が顧客の売買の相手方として取引を受けるものであり、売買価格スプレッドが事業者の収益となる。交換所とは、交換業者がトレーディング、マッチングのプラットフォームとなって顧客同士の売り買いの場を提供するもので、この場合は成立した取引について発生する一定の手数料が事業者の収益となる。さらに証拠金取引やアルゴリズムに基づいた取引機能を提供する事業者も存在する。このような高度な機能は、比較的熟練した投資家によって利用されることが一般的である。さらに、ユーザーが、暗号資産や法定通貨を受け取る際に、取引が成立するまでの間、当該資金の保管サービスを提供して、安全確実な取引執行を支援するエスクローサービスも存在する。

iii は i と ii とあわせて提供されることも多いサービスである。事業者は、現金、電信送金、クレジットカード、暗号資産等、様々な方法での支払を受け付ける。たとえば ATM サービスも、このカテゴリーに含まれる。2022 年 11 月段階で、暗号資産の ATM 設置台数は、全世界で 79 か国、38,821 台と公表しているウェブサイト[49]も存在する。

iv に関しては、暗号資産に対する何らかのコントロールを行使する能力を提供する事業者が、全て該当する。保管は、他人のために暗号資産、あるいは暗号資産にアクセスできる秘密鍵を保管するサービスを含み、管理は、他人のために、暗号資産を管理することを含む。コントロールとは、暗号資産を保有、取引、移転もしくは消費することができる能力と解される。たとえばウォレットサービスプロバイダが、このカテゴリーに含まれる。

v に関しては、ICO のセクションでも述べた通り、発行者による暗号資産の発行・販売に関して、参加もしくは何らかの金融サービスを提供する場合が該当する。これらには、買付注文の受付、再販売のための暗号資産購入、ブックビルディング、引受、マーケットメーキング、プレースメント・エージェント等の活動が含まれる。

一般的に想定される暗号資産交換業者は、顧客のために口座を開設し（ウォレットを提供し）、預かり資産の

[48] 本セクションの整理は、主に Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf) に基づく。
[49] Bitcoin ATM Map – Find Bitcoin ATM, Online Rates (https://coinatmradar.com/) このサイトでは、日本での設置台数は 3 台（うち東京 2、大阪 1）と表示されている。

管理を行い、暗号資産の移転、法定通貨との交換、暗号資産同士の交換を提供するとともに、時には ICO で発行された暗号資産の販売も行うことから、上記の i～v すべてを総合的に提供していることになる。一方で、既に述べた通り、急速に様々なサービスが登場しており、この場合は、必ずしも i～v すべてを総合的に提供するということではなく、むしろ i～v のいずれに該当するのかの判別も難しい業態や個別機能に特化したユニークなサービスも発生し得る。この点で、i～v の機能に該当するかどうかの判断は、テクノロジー中立で、かつ、拡張的でなければならない。この点を見誤ると、本来暗号資産交換業とみなすべき事業を見逃し、結果的に、規制・監督対象となるべき事業者不在のサービスが提供されるという事態になりかねない。これが暗号資産交換業者の定義のリスクである。

暗号資産交換業者を特定する際に確認すべき観点の例として FATF は以下を示している。

- ✓ 誰が当該サービス、資産の利用によって便益を受けるのか
- ✓ 誰が創設し、ルールを変更することができるのか
- ✓ 誰がオペレーションに影響を与えるような意思決定を行えるのか
- ✓ 誰が商品やサービスを作り上げ、商品化、サービス開始を推進したのか
- ✓ そのサービスの一環として受けられるデータを保有、管理する主体を相手方として継続的な業務関係を維持するのは誰か
- ✓ 誰がその商品、サービスの提供を終了させることができるのか

この例は網羅的ではなく、それぞれ固有の状況に鑑みて様々な観点を考慮して特定する必要がある、と FATF は強調している。

たとえば、ミキシング等の秘匿性を高める技術やこれを活用したサービス事業や、このような技術を組み込んだ暗号資産の存在がある。前者については、暗号資産の送金元と送金先の直接の関係性を秘匿するために、複数の送金先からの取引をプールして、別なアドレスから、最終送金先へ再配分するものであり、こういった行為自体は、暗号資産交換業の i～iii の定義に該当すると解釈される。後者については、そのような暗号資産を暗号資産交換業者が、適切なリスク評価（金融犯罪への悪用の可能性等）の下に、取扱可否を判断しているかどうかがポイントとなる。ミキシング等の秘匿性を高める技術については、「5.4 P2P 取引に関するリスク」にて解説する。

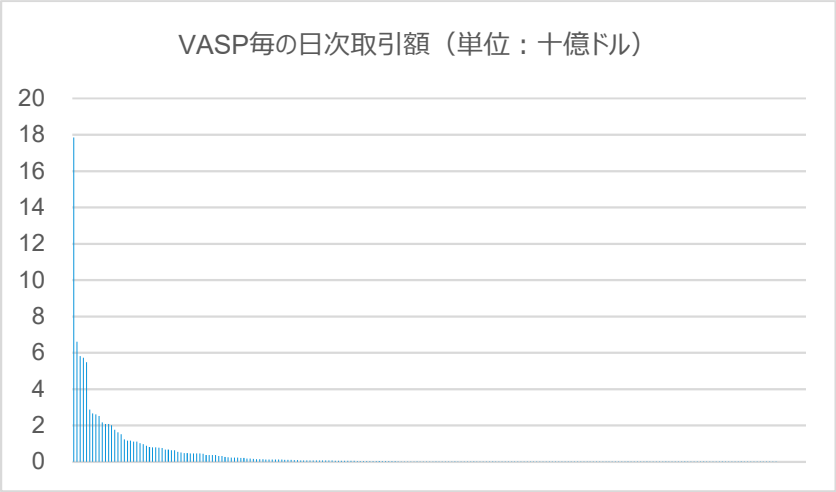
暗号資産交換業者の定義のリスクとは、新たな商品・サービス、ビジネスモデルが登場する中で、何らかの形で関与している事業者を、適切に暗号資産交換業者として特定できないリスクであり、このリスクについて、当局として対処すべき方向性としては、主に以下のようなことが考えられる。これについては「6 規制・監督上の課題」にて取り上げる。

- ・ 規制・ガイドライン：暗号資産交換業者の定義の明確化と適時の更新、およびこれに基づく厳正な免許・登録審査
- ・ 改善・制裁措置：無登録・無許可の事業者に対する厳格な措置
- ・ コミュニケーション：当局が期待する事項の暗号資産交換業者への徹底と、民間とのリスク・コミュニケーション促進、グローバルな動向把握に資する各国当局との連携
- ・ リスク評価：市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査
- ・ インフラ：上記各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用

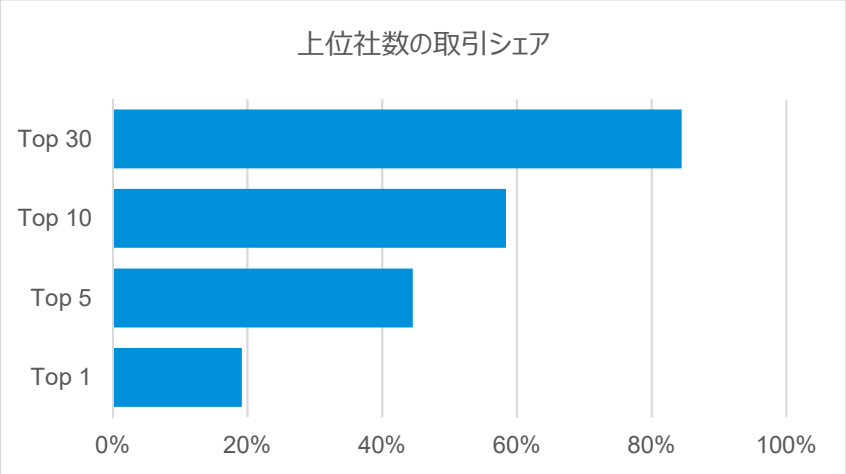
5.2.2 暗号資産交換業者のリスク

前セクションでは、急速に進化するサービスにおいて、本来、暗号資産交換業者として認識すべき対象があいまいになる点、いわばVASPの定義拡大問題に関して述べたが、本セクションは、一旦暗号資産交換業者として認識され、関連法規制の下に組み込まれたとしても、当該事業者が、適切に法規制を遵守できるかというリスクである。

まず、グローバルな暗号資産交換市場を見ると、一日24時間の取引量が入手可能な事業者233社の分布[50]を見ると以下のとおりである。



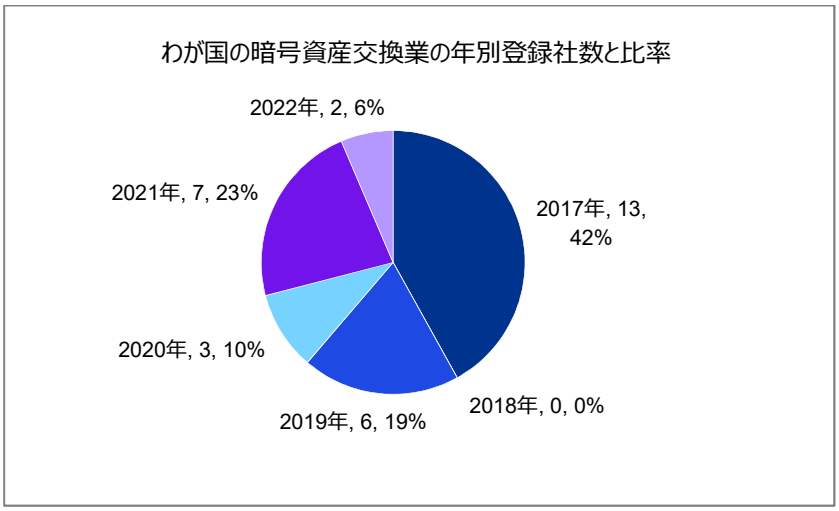
一部の大手が相当の取引シェアを占め、寡占的傾向を示しつつも、残りのシェアを多数の小規模事業者が競い合っているフラグメントな市場であることが見てとれる。



このような構造を持つ、金融市場は他でもしばしばみられ、たとえばわが国では、クレジットカード業界が該当する。ただし、多くの中小事業者は、実は、銀行などの金融機関、その他の事業で相応のプレゼンスを有する比較的大規模な企業グループの子会社であることが多い点が異なる。暗号資産市場は、ファンド投資に支えられるなどして立ち上がった単独のスタートアップ中心であり、かつ、新規参入、撤退が頻繁に起こっている。わが国におい

[50] 2022年11月15日時点のTop Cryptocurrency Exchanges Ranked By Volume | CoinMarketCap (https://coinmarketcap.com/rankings/exchanges/)をもとに集計したもの。

ても、2022 年 10 月 14 日現在の登録事業者 31 社の登録年次を見ると以下のとおりである[51]。



このような市場競争環境にある場合、成長性、収益性等の投資家の要請に応えつつ、一定のコンプライアンス要件を確保することは決して容易ではない。結果的に、当局が期待する要件に沿う形で AML/CFT 態勢が構築、運用できているかという観点では、相当の注意を払う必要があると考えられる。加えて、AML/CFT 要件とベクトルが真逆の、秘匿性を高めるニーズが市場に内在していることから、国としての AML/CFT 政策にそぐわない事業者が存在し得ることも否定できない。

暗号資産交換業者のリスクとは、特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できないリスクであり、このリスクについて、当局として対処すべき方向性としては、主に以下のようなことが考えられる。これについては「6 規制・監督上の課題」にて取り上げる。

- 改善・制裁措置：暗号資産交換業者に対する厳格な措置
- モニタリング：オン、オフ双方での事業者に対する効果的なモニタリング
- コミュニケーション：当局が期待する事項の暗号資産交換業者への徹底と、民間とのリスク・コミュニケーション促進、グローバルな動向把握に資する各国当局との連携
- リスク評価：市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査
- インフラ：上記各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用

5.3 ネットワーク連携に関するリスク

2009 年 1 月 3 日、最初のビットコイン取引がジェネシス・ブロックに記録されて以来、ブロックチェーンに組み込まれるブロックは常に増えてつながり続けており、2022 年 11 月 16 日の日本時間 14:48 時点でのブロック数は 767,385 個に上る。ブロックに含まれる個別取引に関する情報、すなわち取引日時、発信元アドレス、発信先アドレス、取引額等は誰もが見ようと思えば見ることができるパブリックな分散台帳に記帳されている。

このことは、今、手元にある現金（たとえば特定の千円紙幣）が、過去どのような経済主体を介して自分自身にたどりついたのかを追跡することが事実上不可能であることとはきわめて対照的である。また、預金口座同士の為替取引は、それぞれの銀行内であれば、取引モニタリングシステムを通して AML/CFT 目的での取引監視が可能であるが、銀行をまたぐ送金ネットワーク全体の監視は、顧客との守秘義務、個人情報保護の観点から難しい

[51] 金融庁　暗号資産交換業者登録一覧 (https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf) をもとに集計。

とされている。これらのことから、暗号資産については、ネットワーク全体の取引監視が、技術的には可能だという点は、きわめて特徴的であり、AML/CFT の観点から積極的に評価すべき性質を有すると言える。

もっとも、取引上識別されるアドレスと、それを実際に所有する自然人等の主体とを関連付けることが難しいという制約がある。これについては、暗号資産交換業者が CDD の義務を負うこと、もしくはトラベルルールを徹底するということでカバーされなければならないというのが FATF の基本的な考え方である。このセクションでは、このような制約がありつつも、ネットワーク全体の取引監視が適切に実現されるためには、どのような条件が整っているべきかを考察する。

まず、以下のような一連の取引を想定する。

取引①　暗号資産交換業者（VASP）V の顧客 A が V の販売所で 1BTC 購入
取引②　顧客 A が V の取引所で顧客 B より 1BTC 購入
取引③　顧客 A が購入した 2BTC を、外部者 X に送金するよう V に依頼

V は、分別管理の観点から、自己勘定と顧客勘定を設けて、それに関連したウォレットを保有していること、さらにセキュリティの観点から当該ウォレットは、それぞれホットウォレットとコールドウォレットを設け、ホットウォレットは常に同額を維持すること、顧客との取引で発生した自己ポジションは常にスクエアになるようにすることという方針を有しているものとする。この時、一連の取引、およびその結果としてそれぞれの経済主体の口座もしくはウォレットの残高の推移（状態 0～12）は以下のようなものとなる[52]。

取引①：VASP"V"の顧客AがVの販売所で1BTC購入

Wallet/口座	状態0	①-1顧客口座から見た取引	状態1	①-2 Vの勘定から見た取引	状態2	①-3カバー取引	状態3	①-4ウォレット調整取引	状態4
顧客A 口座	10	1	11		11		11		11
顧客B 口座	20		20		20		20		20
V 自己勘定	1,000		1,000	-1	999	1	1,000		1,000
同 Hot Wallet	50		50	-1	49	1	50		50
同 Cold Wallet	950		950		950		950		950
V 顧客勘定	2,000		2,000	1	2,001		2,001		2,001
同 Hot Wallet	100		100	1	101		101	-1	100
同 Cold Wallet	1,900		1,900		1,900		1,900	1	1,901
外部者X Wallet	80		80		80		80		80
外部者Y Wallet	40		40		40	-1	39		39

取引②：顧客AがVの取引所で顧客Bより1BTC購入　　取引③：顧客Aが購入した2BTCを、外部者Xに送金するようVに依頼

Wallet/口座	状態4	②-1顧客口座から見た取引	状態5	③-1送金取引	状態6	③-2顧客口座から見た取引	状態7	③-3ウォレット調整取引	状態8
顧客A 口座	11	1	12		12	-2	10		10
顧客B 口座	20	-1	19		19		19		19
V 自己勘定	1,000		1,000		1,000		1,000		1,000
同 Hot Wallet	50		50		50		50		50
同 Cold Wallet	950		950		950		950		950
V 顧客勘定	2,001		2,001		2,001		2,001		2,001
同 Hot Wallet	100		100	-2	98		98	2	100
同 Cold Wallet	1,901		1,901		1,901		1,901	-2	1,899
外部者X Wallet	80		80	2	82		82		82
外部者Y Wallet	39		39		39		39		39

一般に、販売所取引は顧客と交換業者との相対取引であり、取引所取引は取引所内の顧客同士の取引である。前者は、交換業者と顧客間のやりとりであるが、パブリックなブロックチェーン上認識されるのは、そのための V の自己勘定と顧客勘定間の振り替えと、それにともなって発生する自己勘定のポジション調整のためのカバー取

[52] 実際はより動的、かつ複雑な形で運営されていることが容易に推察される。ここでは経済実態としての取引と、ブロックチェーン上の取引がどのように乖離して見えるのかをわかりやすく俯瞰するための簡易的なモデルを想定した。

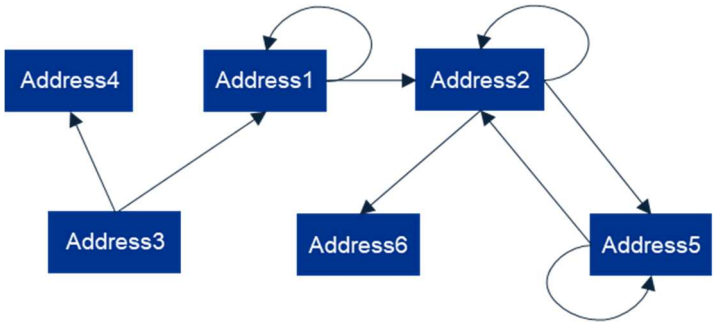
引[53]である。後者については、パブリックなブロックチェーン上の取引は発生せず、純粋に V の内部的な顧客口座間の付け替えで取引が完了するものと考えられる。

パブリックブロックチェーンで認識される取引のアドレスは、ウォレットで管理されており、これらの取引等は、図中の　　で示される部分で表される。一方、顧客として認識すべき取引や残高は、図中　　で示される部分であり、両者には乖離があることがわかる。V は、ウォレット間の資金移動と残高管理をしつつ、顧客に対しては、それを基にしてバーチャルな（顧客にとってはリアルな）取引、残高を記帳して、顧客に示しているという構図である。

次に、パブリックブロックチェーン上は、これらの取引がどのように認識されるかを以下の表に示す。

ウォレット所有者	ブロックチェーン上のアドレス	取引① VASP"V"の顧客AがVの販売所で1BTC購入				取引② 顧客AがVの取引所で顧客Bより1BTC購入	取引③ 顧客Aが購入した2BTを、外部者Xに送金するようVに依頼		
		①-1顧客口座から見た取引	①-2 Vの勘定から見た取引	①-3 カバー取引	①-4 ウォレット調整		③-1 送金取引	③-2顧客口座から見た取引	③-3 ウォレット調整
V自己勘定	Hot Wallet address1		OUT						
			IN						
				IN					
V顧客勘定	Hot Wallet address2		IN						
					OUT				
					IN				
							OUT		
									IN
	Cold Wallet address5				IN				
									OUT
									IN
外部者X	address6						IN		
外部者Y	address3			OUT					
	address4			IN					

ビットコインは UTXO モデルに基づくため、保有トークンと送金額が一致しなければ、おつり取引が発生すること、ウォレット所有者によっては、取引の都度、アドレスを変えることが可能である[54]ことを踏まえると、①～③のような簡単な取引例でも、上図のように 6 つのアドレスが登場することがわかる。ここで特徴的なのは、顧客 B に関連するアドレスは登場せず、顧客 B にかかる取引は、ブロックチェーン上では認識されないということである。さらに、この表は、それぞれのアドレスがどこのウォレットに関連しているのかを知っている前提で作成できるものであるが、パブリックチェーン上はアドレスのみが開示されているのみであり、以下のように見えることになる。

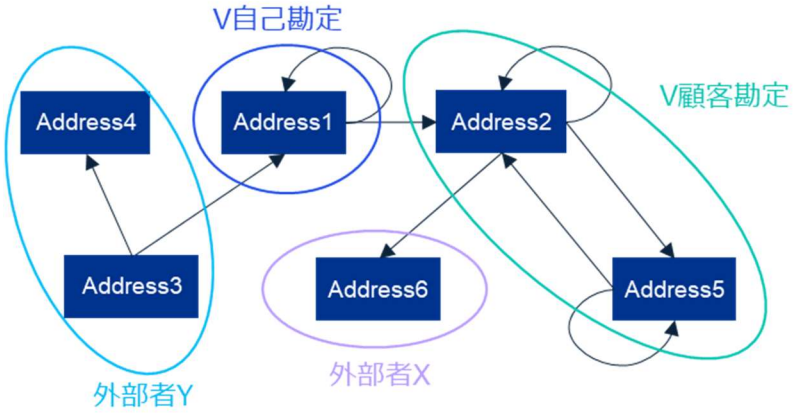


ここでは、たとえば、交換業者の内部的な取引である address1 と address2 の間の取引、対外的な送金取引である address2 と Address5 の間の取引や address4 に入るおつりの取引は、ブロックチェーン上はほぼ無差別に見える。同様に 6 つのアドレス間の取引を見ると、それらの関係性を本来の経済主体間の金融取引という

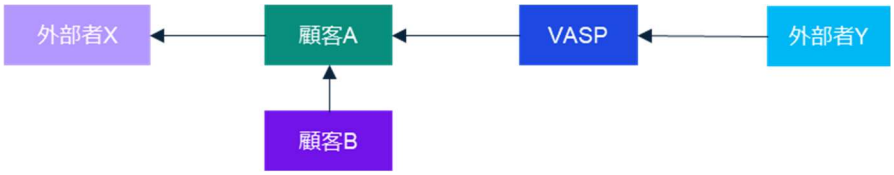
[53] この例では、簡単のために、顧客取引が発生する都度、バックトゥバックでカバー取引を実施している（①-4 および③-3 のウォレット調整取引）想定としたが、実務上は、顧客勘定を介する取引は他にも多数あり、手数料負担軽減の観点からも、一定期間を置いてマクロ的な調整を行っているものと考えられる。ポジション調整のためには、いわゆるカバー取引が必要であり、その相手方を上記の表上は外部者 Y とした。

[54] この例では、V は同一アドレスを繰り返し使用、外部者 Y は取引の都度異なるアドレスを発行していると想定した。

意味あいで理解することは極めて困難であることがわかる。この例では我々が全知全能的に背景情報を知っているから、実は以下のような主体、もしくはウォレット間での取引である、と初めて認識できるのである。さらに、V 顧客勘定のアドレスは、顧客 A 固有のものではなく、他の多くの顧客の多数の取引の宛先となっていることを考えると、パブリックチェーンの情報だけで顧客 A に関連する一連の取引を認識するのは難しい。

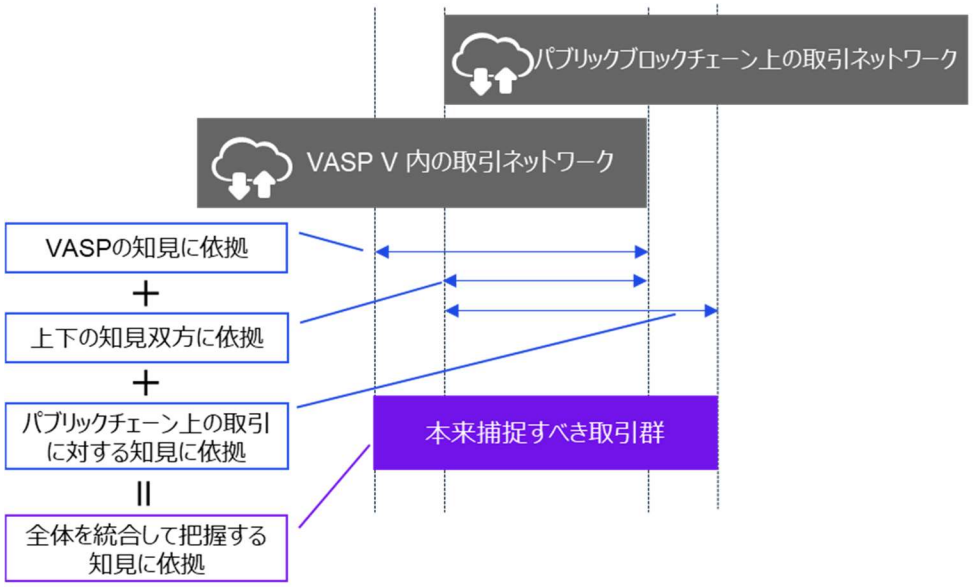


一方、V の立場からは、我々と同等レベルの背景情報をもって認識できる範囲は、V 自己勘定、V 顧客勘定、および顧客 A ウォレットのみである。特に顧客 A ウォレットのみのやり取りでは本来の顧客 A の取引は認識できず、V が保有する顧客 A との取引情報とあわせて把握する必要がある。さらに、ブロックチェーン上認識できない顧客 B の取引を認識できるのは、唯一 V のみである。結局、この例で、本来認識すべき根源的な金融取引は、以下のように比較的シンプルなものであるにもかかわらず、これらの全貌を、最も全知全能に近い形で理解できる（法規制的に言えば、理解すべき立場にある）のは交換業者 V 自身であって、パブリックなブロックチェーンのみからこれを推察することは容易ではないということになる。



このように、本来捕捉したい取引群に対して、取引そのものの情報を得られるという点では、パブリックなブロックチェーンを利用する暗号資産は、現金、預金取引といった伝統的な金融サービスと比較すると優位である一方、捕捉ネットワークやその取引や経済主体に関する知見[55]の保有者が分断されている。本来は、分断されている知見を統合して、全体像を把握すべきところ（下図）、情報、知見が異なるネットワークをまたがって存在するために正しくリスクを把握できない、というのが、ネットワーク連携のリスクである。

[55] 取引という情報に加えて、その取引の経済的意味合いも理解しているという意味あいで「知見」としている。



「全体を統合して把握する」ということは、暗号資産交換業者が、本セクションで整理したように、パブリックなブロックチェーンに、アドレス単位に記帳された取引の情報、自社内の販売所、取引所内で記帳された取引の情報、に加えて自社で知り得た当該取引に関する経済的意味合い、さらにはパブリックなブロックチェーンで観測・推測される各種の経済的意味合い[56]、これらすべてを包括的に把握、統合して初めて達成できることである。すなわち、FATF や各国当局の期待に沿うためには、暗号資産交換業者が、情報量、情報分析基盤、分析能力に加えて、ML/TF リスク低減への意欲等、相当レベルの熱量を投入する必要があるということであり、前セクションで整理した、暗号資産交換業者のリスク（規模、社歴、成長性、収益性等、多様な事業者すべてが、適切に法規制を遵守できるか）とあわせて留意すべき点である。

ネットワーク連携に関するリスクとは、パブリックブロックチェーン、事業者毎の取引所等、ネットワーク全体に関する情報・知見が分断されているために全体像が把握できないリスクであり、このリスクについて、当局として対処すべき方向性としては、主に以下のようなことが考えられる。これについては「6 規制・監督上の課題」にて取り上げる。

- コミュニケーション：当局が期待する事項の暗号資産交換業者への徹底と、民間とのリスク・コミュニケーション促進、グローバルな動向把握に資する各国当局との連携
- リスク評価・調査分析：市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査
- インフラ：上記各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用

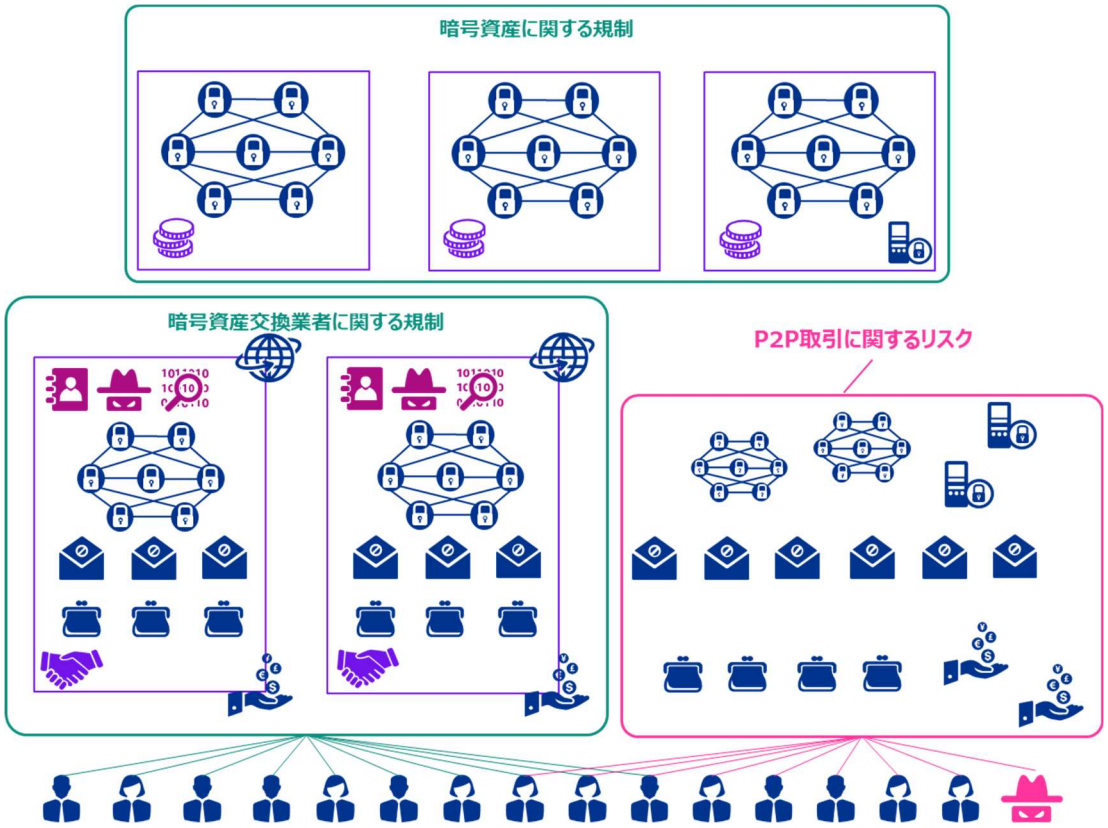
5.4 P2P 取引に関するリスク

5.4.1 リスクの概要

P2P 取引とは、暗号資産交換業者やその他の規制対象事業者の関与なく、あるいはそういった事業者が提供するサービスを利用することなく、暗号資産の移動等を実行する取引のことを指す。「5.2.1 暗号資産交換業者の定義のリスク」で示したような機能が進化した多様な暗号資産や関連サービスの利用により、ユーザーは、暗号資産交換業者や金融機関の助けを借りることなく取引が行えるようになり、多額の資金移動をグローバルに迅速

[56] 分析ツールや分析結果を提供しているブロックチェーン分析企業や当局、同業者、業界団体その他から得られる外部情報等がこれに該当する。

に実行したり、資金やその他の価値の移転、有価証券、コモディティ、デリバティブ等の金融活動を行ったりすることができる余地が広がっている。これらの商品、サービスの多くが、秘匿性を高める技術を伴ったり、機会をもたらしたりすることで、暗号資産交換業者が関与していたら可能なはずの真の受益者の特定を困難にし、ML/TF リスクを高めている。AML/CFT コンプライアンスの義務を有する暗号資産交換業者の関与なしでは、非対面でのクロスボーダー取引が容易に可能な世界において、顧客やその送金元、送金先の特定はできず、資金の流れを追跡することも難しいということである。（下図）



特に、この領域では、意図の有無にかかわらず不法を企図する者の金融システムへの参加、また、そのような者にも（これも意図の有無にかかわらず）便益を提供し得るサービス、ツールの提供といった機会を与えているリスクが高いとも言える。

FATF 勧告や、それに基づく各国 AML/CFT 規制は、取引を実行する個人に対してではなく、そのような取引主体の間を取り持つ事業者を対象としていることから、定義のとおり、P2P 取引は直接的にはそのような規制対象とはなりにくい。仮にプライベートウォレットを有する二者間で P2P 取引を行えば、それが、どのような不法取引であったとしても、これを防止、検知、対処することは難しい。

FATF の報告書「Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs」[57]によれば、2016 年～2020 年の間、暗号資産交換業者を介さない取引の比率は、件数ベースで 10～70%、金額ベースで 2～91%と、この調査に選定された分析企業 7 社によって大きく割れている。同様に不法取引と特定されたものの比率は、件数ベースで 0.3%～12.7%、金額ベースで 0.0%～15.4%と推定されている。7 社中、4 社については、不法取引と特定されたものを、さらに、暗号資産交換業者経由のものと経由

[57] Documents - Financial Action Task Force (FATF) (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html)

しないもの分けて分析がなされており、取引ベースでは暗号資産交換業者経由の取引が 1.7%～8.1%、経由しないものの取引が 3.6%～12.9%、金額ベースは前者が 0.0%～1.6%、後者が 0.1%～27.9%となっている。暗号資産の P2P 取引がどの程度行われているかについてのコンセンサスが得られている状態ではない、と言える。このような状況下、暗号資産交換業者に対する規制・監督だけでは不十分であることは明らかであり、規制・監督当局として、P2P 取引の ML/TF リスクに関する理解を深めるための市場動向やサービスの利用状況の把握は重要である。これに関して、FATF は、以下のように述べている。

「P2P 取引の顕著な増加は今のところ認められていないが、FATF 基準に基づき暗号資産交換業者に対する規制・監督を適切に実施する国が増加するにつれ、そのような規制や監督を逃れるために、より多くの暗号資産取引が P2P に移行する潜在的なリスクがある。仮に暗号資産交換業者の介在や法定通貨との交換なしに、P2P 取引が増加し、P2P での不法行為が暗号資産のエコシステムにおいて顕著となれば、FATF 基準の施行上の有効性に対する課題となり得る。したがって、P2P 取引にかかる ML/TF リスクについては、継続的かつフォワードルッキングにモニタリングされるべきである。」[58]

本セクションでは、以下、P2P 取引を可能にするサービスとしての DeFi、秘匿性を高めるサービスについて順に考察する。

5.4.2 DeFi

P2P 取引が行われる環境では、分散化されたアプリケーション（DApp; Decentralized or distributed application）が多く提供されている。たとえば、ブロックチェーン上で動くソフトウェアプログラムがこれに該当する。このプログラムは、他のプログラム、アプリケーション、あるいは暗号資産の移動等の実行を容易にしたり、支援したりする機能を有している。このようなアプリケーションやプラットフォームは分散記帳上で実行されているものの、暗号資産の生成・発行、DApp 機能や口座保有、手数料徴収のための UI 開発等の何らかの関与、コントロールを有する中央機構がしばしば存在する。DApp 自体はプログラムであったとしても、その処理を実行することで、手数料支払を求めるようプログラムされており、その最終的な受益者が、DApp の所有者、運用者、開発者、コミュニティとなっていることが想定される。

DApp のうち、特に暗号資産交換業者が提供するような金融サービスに該当するものが DeFi; Decentralised Finance と呼ばれる。DApp、DeFi アプリケーション自体は暗号資産交換業者には該当しないものの、既述のとおり所有、運営、その他、DApp、DeFi アプリケーションの取極めに関して何らかのコントロールないしは十分な影響力を行使する立場にある者が存在すれば、取極め自体がいかに自動化されていたとしても、暗号資産交換業者に該当する可能性が高い。ちなみに DeFi の一形態である DEX; Decentral EXchange（分散交換所）に関して、いくつかインターネット上の情報を見ると、創設者名、本部や開発チームの所在地、手数料体系等が開示されているものが多いが、中には不明なものも存在している。ただし後者についても問い合わせ先が Contact us、Help Center 等として掲示されており、何らかの運営主体の存在を示唆しており、全体としては暗号資産交換業者として特定されるべき可能性が高い主体が存在している状況がうかがえる。

DeFi サービス提供者が暗号資産交換業者の定義に該当するかどうかは、提供サービスがいかに自動化されていようが、拡張的に検討すべきと考えられる。各種管理機能、手数料徴収、利益処分等についてコントロール手段を維持し、もしくは十分な影響力を行使できるのであれば、暗号資産交換業者の義務を果たすべき立場にあ

[58] Documents - Financial Action Task Force (FATF) (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html)

る。

5.4.3 秘匿性を高めるサービス

P2P 取引空間上には、秘匿性を高めるための様々なサービスが提供されている。これらは、明らかに不法行為者を想定した悪意あるものや、そうではないもの、いずれか判然としないもの等が混然と提供されている。

これらの技術あるいはサービスには、ミキシング、タンブリング、分散プラットフォーム、分散ウォレット、さらには Tor に代表されるようなインターネット上の通信を匿名化するために IP パケットに重層的に暗号化を施すようなもの等が含まれる。また、単独機能として提供されるものもあれば、機能を暗号資産、ウォレットサービス等に組み込んでいるものもある。後者の例の暗号資産としては Dash、Monero、Zcash、Komodo 等が挙げられる。これらは AEC; Anomymity-Enhanced Cryptocurrency とも呼ばれる。

秘匿性を高めるサービスの代表的な例として、ミキシングが挙げられる。これは、複数の送金元からの取引をプールし、元の送金元の情報を秘匿して、新たな取引として再分配し、最終的な送金先へ暗号資産を送るものである。ミキシングサービス事業者が用意した中央集権的な取引プラットフォーム上で行うものと、ゼロ知識証明等の技術を用いて送金人や受取人、送金額といった情報を開示することなく、取引が正当に行われたことを証明するような分散型のものがある。前者は、結局何らかの中央集権的なプラットフォームに情報が存在することから、ミキシング事業者の持ち逃げ、ハッキング、サーバー障害等のリスクがあり、徐々に後者のタイプに移行する傾向にあったが、昨今では、後者も含めて当局がミキシング事業者に対して厳しい態度で臨んでいる。

たとえば、ミキシングサービスを提供する事業者が、捜査当局の強制捜査を受け、事実上の閉鎖に追い込まれたもの[59]、該当事業者のミキシングサービスが巨額のマネー・ローンダリングに悪用されたとして、経済制裁者に指定されたもの[60]等が挙げられる。

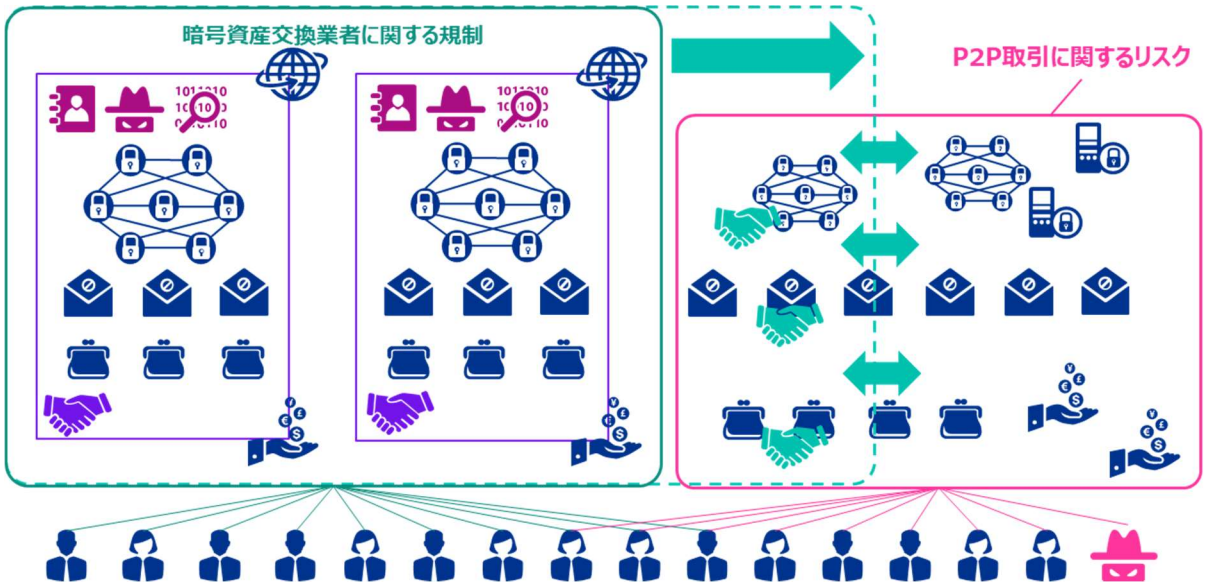
ミキシングは、暗号資産の取引上のアドレスを秘匿するものだが、インターネットプロトコルで秘匿性を高めるものも存在する。たとえば、ダークウェブは、Tor; The Onion Router や I2P; Invisible Internet Project といった特定のソフトウェアや技術を使わなければ接続できない領域で運用・公開されているウェブサイトである。麻薬、搾取個人情報、サイバー攻撃ツール等の不法取引の場を提供する取引ネットワークとして悪用されている。ある分析業者の報告書[61]によれば、これらの取引ネットワークでの収入は 2021 年の一年間で 21 億ドル相当に上り、前年よりも増加しているが、特定されている取引所は 2020 年よりも減少しており、不法取引関連（いわゆる Fraud shop）が 60 前後、麻薬関連が 80 弱となっている。取引所が閉鎖される際、従来は、顧客の預かり金はそのまま持ち逃げされることが多かったようだが、昨今は閉鎖を予告し、顧客に資金を引き出すよう案内するケースも増えている。これは無断で閉鎖すると、慌てた顧客が当局に通報し、足がつくことを恐れた結果、閉鎖時の行動パターンが変わってきたものと分析されている。また取引所間の競争もし烈で、お互いに情報リーク、DDoS 攻撃等を仕掛けて合っているという。活発に活動している顧客数は不法取引関連で 190 万人、麻薬関連で 120 万人とされている。

[59] Multi-million euro cryptocurrency laundering service Bestmixer.io taken down (https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down)
[60] U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (https://home.treasury.gov/news/press-releases/jy0916)
[61] The 2022 Crypto Crime Report.pdf (chainalysis.com) (https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf)

5.4.4 リスクへの対処の方向性

これまで見てきた P2P 取引に関するリスクへの対処の方向性としては、まず、P2P 取引の中で、拡張的に暗号資産交換業者を特定し、暗号資産交換業者に対する規制の対象領域を拡大することが重要である。（下図 ➡ ）

次に、それでもなお残る P2P 取引領域と暗号資産交換業者の顧客との取引について追跡性を確保することが必要である。（下図 ↔ ）この他、不法行為を働く、あるいは助長するようなサービスやその提供事業者については禁止、制裁等の措置をとることも考えられる。



P2P 取引に関するリスクとは、P2P の取引、サービスの多くが、秘匿性を高める技術を伴ったり、機会をもたらしたりすることで、暗号資産交換業者が関与していたら可能なはずの真の受益者の特定を困難にするリスクである。既述のとおり、FATF は「P2P 取引の顕著な増加は今のところ認められていない」としているが、P2P 取引が今後指数関数的に増加し、将来、取引のメインストリームに躍り出たとき、従来の仲介事業者を対象に規制をかけるアプローチが線形でしか進展しないとすると、ある時点からギャップが拡大するため、さらなる代替アプローチが必要ではないか、との懸念も示されている[62]。このリスクについて、当局として対処すべき方向性としては、主に以下のようなことが考えられる。これについては「6 規制・監督上の課題」にて取り上げる。

- 改善・制裁措置：無登録・無許可の事業者に対する厳格な措置
- コミュニケーション：当局が期待する事項の暗号資産交換業者への徹底と、民間とのリスク・コミュニケーション促進、グローバルな動向把握に資する各国当局との連携
- リスク評価・調査分析：市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査
- インフラ：上記各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用

5.5 法域に関するリスク

暗号資産市場のグローバルな広がりを考えると、一国のユーザーが決済や資金移転を検討するとき、海外の暗号資産や関連サービスが、どのように提供され、どのように利用され得るのかは重要なポイントである。たとえば、不

[62] Outcomes of neutral multi-stakeholder discussions of Blockchain Governance Initiative Network (https://bgin-global.org/pdf/FATFPresentation.pdf

法なユーザーは、自国の厳格な規制の結果制限を受けている AEC のような秘匿性の高い暗号資産、ミキシングサービス、ダークウェブを、海外事業者が提供するサービスとして利用すること等が想定される。すなわちそのようなサービスが利用可能であるということは、当該サービスの提供元の法域において、暗号資産、暗号資産交換業者に対する規制・監督が脆弱であるリスクがあるということに他ならない。各国の規制・監督に大きな差異が認められる場合、悪意あるユーザーにとっては、まさに規制アービトラージの格好の餌食になるということである。

一国のユーザーはネットを介して手軽にグローバルに提供される暗号資産や関連サービスを入手できる時代であり、自国の法規制上、利用が認められない暗号資産、および関連サービスがあったとしても、規制が異なる、もしくは脆弱な国から提供されるサービスを利用することができれば、自国の法規制の実効性に問題が生じる。

規制アービトラージが発生する要因は以下のようなものが考えられる。

- 暗号資産、暗号資産交換業者に関する規制が相対的に遅れている
- 暗号資産交換業者に対する監督が相対的に遅れている
- 暗号資産・暗号資産交換業者に関連した法執行が十分ではない
- 関連当局間での国際協力が積極的ではない

FATF が実施した 2 回の調査（12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers[63]）に基づいて、各国の規制の進展状況を整理すると次ページの通りである。

それぞれの選択肢や、母集団が異なるものの、相応の進展は認められる。ただし、二回目の調査回答国数がいまだ 128 か国にとどまっていること、対象国中でも関連規制施行済みの国は約半分にとどまっていることから、FATF 勧告に基づく暗号資産、暗号資産交換業者に関する規制はいまだ途上であることがうかがえる。

一方で、繰り返し述べている通り、暗号資産や関連サービスは、法域を超えて急速に進展、機能も多様化し、利用者も増えている。暗号資産のクロスボーダー性を勘案すれば、各国の足並みをそろえた法規制の整備は急務と言える。

各国間規制アービトラージの機会が早急に解消される状況にないとすると、AML/CFT 規制が脆弱もしくは存在しない法域の暗号資産交換業者の問題は深刻であり、各国においてそのような業者に関連し得る取引に関する具体的な措置をとる必要がある。

2020 年

分類	状況	FATF	FATF 地域体	合計
VASP 規制	施行済	24	8	32
	施行検討中	9	4	13
VASP 禁止	罰則付きで禁止	1	2	3
	施行検討中	2	0	2
未決定	VASP への対応未定	2	2	4
合計		38	16	54

[63] 一回目は 2020 年 6 月（https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf）、二回目は 2021 年 7 月（https://www.bis.org/bcbs/publ/d533.pdf）

2021 年

分類	状況	FATF	FATF 地域体	合計
施行済み	VASP 規制	27	25	52
	VASP 禁止	1	5	6
施行検討中	VASP 規制	7	19	26
	VASP 禁止	0	0	0
方針決定済施行未着手	VASP 規制	1	5	6
	VASP 禁止	1	5	6
方針検討中		1	31	32
合計		38	90	128

法域に関するリスクとは、規制が異なる、もしくは脆弱な法域から提供されるサービスを一国のユーザーが利用することで、自国の法規制の実効性に問題が生じるリスクであり、このリスクについて、当局として対処すべき方向性としては、主に以下のようなことが考えられる。これについては「6 規制・監督上の課題」にて取り上げる。

- 改善・制裁措置：無登録・無許可の事業者に対する厳格な措置
- コミュニケーション：グローバルな動向把握に資する各国当局との連携
- リスク評価・調査分析：市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査
- インフラ：上記各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用

6 規制・監督上の課題

6.1 規制・監督当局に求められる事項

暗号資産に限らず、一般的なリスクベースの金融監督は以下のようなフレームワーク[64]で整理することができる。

特に、FATF も指摘しているように、ルールベースからリスクベースへの転換は、各国とも苦慮している中、あるべきリスクベース監督の姿として、特に留意すべき事項は、以下のとおりである[65]。

1. リスクの理解	① 対象事業者に対する ML/TF リスク評価のスコープと目的を明確にすること ② リスク評価のプロセスを確立し運用すること ③ リスクの特定と理解のために必要な情報を特定すること ④ 上記リスクの理解を常に最新のものに保つこと
2. リスクベースの監督	① 監督上の戦略を明確にし、特定されたリスクに対処すること ② リスクに応じて監督の態勢、頻度、集中、重点項目を柔軟に設定すること ③ 適切なツールを用いてオン・オフのバランスの取れた監督を実施すること ④ 事業者に対し、リスクに見合った適切な改善措置や制裁措置をとること ⑤ 監督としてのリスクベースアプローチの有効性を検証すること ⑥ 国内関連省庁や海外当局との連携を図ること
3. 横断的な課題	① 施策を執行するために必要なリソースを確保すること（要員確保、研修等） ② リスクの迅速な把握、情報収集・蓄積・分析を効果的・効率的に実施するためのテクノロジー(SupTech)の活用 ③ 民間セクターとの連携・対話を強化すること ④ 外部専門家等のサードパーティの活用

このような一般的な監督・規制当局のリスクベースのフレームワークに対して、「5 暗号資産の ML/TF リスク」で考察したそれぞれのリスクが、どのように関連付けられるかを整理すると、以下のようになる。

[64] FATF Guidance on Risk-Based Supervision (https://www.fatf-gafi.org/content/dam/fatf/documents/Guidance-Risk-Based-Supervision.pdf.coredownload.pdf)を基に KPMG が整理した例

[65] 同上

リスクの分類		規制・ガイドライン	改善・制裁措置	モニタリング	コミュニケーション	リスク評価	インフラ
暗号資産そのものに内在するリスク		✓	✓		✓	✓	✓
暗号資産交換業者に関するリスク	暗号資産交換業者の定義のリスク	✓	✓		✓	✓	✓
	暗号資産交換業者のリスク		✓	✓	✓	✓	✓
ネットワーク連携に関するリスク					✓	✓	✓
P2P 取引に関するリスク			✓		✓	✓	✓
法域に関するリスク			✓		✓	✓	✓

以下、図の右側で示した対応の分類項目ごとに、整理を進める。

6.2 規制・ガイドライン

規制・ガイドラインに関連付けられるべきリスクは以下の通りである。

リスクの分類		リスクの説明
暗号資産そのものに内在するリスク		新たな商品・サービス、ビジネスモデルが登場することで、それまでの暗号資産の定義にはまらない、ないしはその定義をあいまいにさせるような要素が発生するリスク
暗号資産交換業者に関するリスク	暗号資産交換業者の定義のリスク	新たな商品・サービス、ビジネスモデルが登場する中で、何らかの形で関与している事業者を、適切に暗号資産交換業者として特定できないリスク

このリスクに対して、規制・監督当局は、暗号資産および暗号資産交換事業者の定義の明確化、暗号資産交換業者が取り扱うべき暗号資産の範囲の明確化とこれらの適時の更新、厳正な免許・登録審査等を、規制・ガイドラインとして示すことが求められる。

審査にあたっては、暗号資産交換業者が AML/CFT 義務を適切に履行できるかを含めて適切な評価基準を定め、免許・登録の前に、事業の内容（暗号資産、取引、想定顧客、販売チャネル等）に応じた方針、手続、組織体制を含めた AML/CFT プログラムが適切であることを見極める必要がある。その過程で、犯罪者あるいはその近親者が、暗号資産交換業者に対する所有、実質的支配、利益処分、経営機能の保有等に関与することのないことを確保しなければならない。

暗号資産に関するエコシステムは、急速に進展しており、この中で、暗号資産や暗号資産交換業者となるべき事業者を特定することは極めて重要である。この観点で、暗号資産、暗号資産交換業者の定義は拡張的である必要がある。たとえばステーブルコイン、ウォレットサービスプロバイダ等の取扱等がこれに含まれる。

このような観点で、海外各国（EU、フランス、ドイツ、ノルウェー、オーストラリア、カナダ、韓国）について、監督当局、関連法令、暗号資産および暗号資産交換業者の位置づけ、暗号資産交換業者に求める主な AML/CFT 要件、直近の規制・市場動向を以降のセクションで整理する。

なお、暗号資産や関連するサービス動向については幅広に情報収集、調査することも求められ、これについては、「6.6 リスク評価・調査分析」にて考察する。さらに、無登録・無許可事業者による暗号資産に関する行為について、禁止、制限等の措置をとることも求められ、これについては「6.3 改善・制裁措置」にて考察する。

6.2.1 **各国法規制：EU**

6.2.1.1 EU 体系について

EU は、欧州連合条約（EU 条約）をはじめとする EU の基本条約によって設立、運営される国際機関である。基本条約によって加盟国の主権の一部が EU へ移譲され、主権が移譲された政策分野においては、加盟国に代わって EU が権限を行使する。そのため、EU の法体系は、国際法とも、また加盟国の国内法とも異なる独自の体系となっている[66]。

また、欧州経済地域（EEA; European Economic Area）協定は、アイスランド、リヒテンシュタイン、ノルウェーを EU 域内市場に取り込み、もの、サービス、人、資本の移動の自由、統一関連政策(競争、運輸、エネルギー、経済・金融協力)を保証するものであり、EU 加盟国と同じ規則と条件が EEA 内のすべてのビジネスに適用され、域内市場に関する EU の法律は、EEA 加盟国の法律の一部となる[67]。

EU において、一次法である基本条約を根拠に制定される法令である二次法には、規則（Regulation）、指令（Directive）、決定（Decision）、勧告（Recommendation）、意見（Opinion）があり、加盟国の国内法との関係や法的拘束力がそれぞれ異なる。本パートに関連する、規則および指令については以下の通りである。[68]

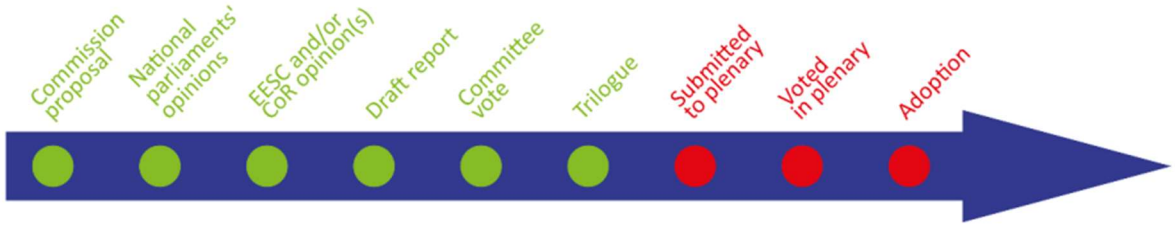
- 規則（Regulation）
  加盟国の国内法に優先して、加盟国の政府や企業、個人に直接適用される。そのため、加盟国の国内立法を必要とせず、加盟国の政府等に対して直接的な法的拘束力を及ぼす。
- 指令（Directive）
  加盟国の政府に対して直接的な法的拘束力を及ぼす。指令には政策目標と実施期限が定められ、指令が採択されると、各加盟国は、期限内に政策目標を達成するために国内立法等の措置を取ることが求められる。ただし、どのような措置を取るかは各加盟国に委ねられる。企業や個人には直接適用されない。

6.2.1.2 関連法令

暗号資産関連については、2022 年 6 月、暗号資産、暗号資産発行者および暗号資産交換業者に対する規制法案である Market in Crypt-Assets (MiCA)が EU 理事会と EU 議会で暫定合意された[69]。EU 加盟国を直接、統一的に規律する暗号資産関連のルールが確立され、既存の EU 法でカバーされていない暗号資産も規制されることになる。時期は未定であるが、施行とともに EU 加盟国、EEA 加盟国において、既存の国内法

[66] EU（欧州連合）-EU 法について｜国立国会図書館 (https://rnavi.ndl.go.jp/jp/politics/eu-law.html)
[67] European Economic Area (EEA) Agreement (https://trade.ec.europa.eu/access-to-markets/en/content/european-economic-area-eea-agreement)
[68] EU（欧州連合）-EU 法について｜国立国会図書館 (https://rnavi.ndl.go.jp/jp/politics/eu-law.html)
[69] Digital finance: agreement reached on European crypto-assets regulation (MiCA) (https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/)

に優先して MiCA が適用されることとなる。MiCA 制定までの流れは以下のとおりである。



2022 年 6 月 30 日に EU 理事会と議会が暫定合意、10 月 5 日に常任代表委員会承認、10 月 10 日に EU 経済委員会承認後は、今後 EU 議会本会議で、その後欧州評議会で投票が行われる[70]。

AML/CFT については　EU AML 指令[71]によって AML 規制の枠組みが示され、EU 加盟各国が指令の遵守のために各国の国内法等で措置をとっている。

6.2.1.3　監督当局

MiCA においては、EU 加盟各国の所管官庁 (NCAs; national competent authorities)が MiCA 規則に規定された機能および義務を遂行し、EBA および ESMA に情報連携する枠組みとなっている[72]。

AML/CFT に関しては、EU 加盟各国の所管当局がそれぞれの国で AML 規制・監督を行うが、EU レベルにおいては、それぞれ銀行、証券、保険・企業年金を担当する欧州銀行監督機構 (EBA; European Banking Authority)、欧州証券市場局 (ESMA; European Securities and Markets Authority)、欧州保険・企業年金監督局（EIOPA; European Insurance and Occupational Pensions Authority）の三機関からなる、欧州監督当局(ESAs; European Supervisory Authorities) が、AML 規制を所管する[73]。

6.2.1.4　暗号資産および暗号資産交換業者の位置づけ

MiCA の規制案において、規制の趣旨として、暗号資産の分野で採択されるいかなる法律も、具体的で将来性があり、そしてイノベーションやテクノロジーの発展のペースに追いつけるようにするべきであり、現在 EU の金融サービスに係る法律でカバーされていないものも含めて全ての暗号資産を含めるように、暗号資産はできるだけ広義に定義すべきである、と説明されている。このため、暗号資産、暗号資産交換業については、FATF での定義に則って Article 3 の 1 の以下の各号において定められている[74]。

(2)　暗号資産（Crypto-asset）とは、分散記帳技術や同様のテクノロジーを用いて、電子的に移転および保管可能なデジタル上の価値表現である。

---

[70] European parliament briefing eu legislation in progress - Markets in crypto-assets (MiCA) (https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf)

[71] 現在は、Fifth Money Laundering Directive が適用されており、改正案としての Sixth Money Laundering Directive も示されている。

[72] European parliament briefing eu legislation in progress – Markets in crypto-assets (MiCA) (https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf)

[73] EU context of anti-money laundering and countering the financing of terrorism (44uropa.eu) (https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en)

[74] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA) (https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf)

(8) 暗号資産交換業者（Crypto-asset service provider）とは、以下の一つもしくは複数の暗号資産サービスを業として第三者に提供する者である。

(9) 暗号資産サービスとは、暗号資産にかかる以下のサービス[75]をいう。

(a) 第三者のための暗号資産のカストディおよび管理
(b) 暗号資産交換プラットフォームの運営
(c) 暗号資産の法定通貨との交換
(d) 暗号資産同士の交換
(e) 第三者のための暗号資産取引指示の執行
(f) 暗号資産のプレースメント
(g) 第三者のための暗号資産取引指示の受付と発信
(h) 暗号資産に関する助言の提供

暗号資産交換業者はEU内での業務提供のために、現状は、加盟国それぞれの当局による許可（Authorization）が必要であるが、MiCAにおいては以下の2つのオプションが提示されている。

Option 1（オプトイン制度）：EU法準拠を表明して許可を得た暗号資産交換業者は、EUパスポート制度の便益を受け、EU(およびEEA)域内全域での業務提供が許可される。意思表明をしない場合は、引き続き域内で無許可事業者となるか、もしくは、当該国のみの固有制度の規制対象事業者となる。

Option 2（全面適用）：全ての暗号資産交換業者は、EU法に準拠して許可を得る必要があり、この場合は、EUパスポート制度の便益を受け、EU(およびEEA)域内全域での業務提供が許可される。暗号資産に係る各国固有の規制はなくなる。

ステーブルコインについては、MiCA上は、資産裏付け型トークン（Asset-referenced token）、電子マネートークン（e-money token）として、以下のように定義されている。

- 資産裏付け型トークン：法定通貨、その他のコモディティもしくは暗号資産、あるいはその組み合わせによって裏付けられて安定的な価値を提供する暗号資産
- 電子マネートークン：法定通貨に裏付けられて安定的な価値を維持し、交換手段として用いられる暗号資産

なお、「いわゆる」アルゴリズム型ステーブルコイン[76]は、資産裏付け型トークンとみなされるべきではない、と整理されている。

また、NFTは、暗号資産の定義に該当する場合以外は、金融規制対象外とされる。ただし、18ヶ月以内に、EU委員会は、包括的な評価を準備し、必要と認められる場合には、NFTのための制度を創設し、そのような新しい市場の新たなリスクに対処するための具体的、比例的かつ水平的な立法提案を作成する任務を負う、とされている。

[75] 「2 暗号資産等の定義」で示したFATFのi～vの定義に沿ったものとなっている。
[76] 暗号資産に対する需要に応じて供給を増減させる手順によって安定的な価値を維持しようとするもの。

さらに、規制を遵守しない暗号資産交換業者については EBA に公表を義務付ける予定としている[77]。

6.2.1.5　暗号資産交換業者に求める主な AML/CFT 要件

MiCA においては、暗号資産交換業者およびその経営陣が、EU AML 指令に基づく各国の AML/CFT 法規制に違反した場合は、各国当局は当該免許を取り消す権限を有すべきことが規定されている。

EU AML 指令において、暗号資産交換業者を含む規制対象事業者（Obliged entity）に求められる AML/CFT の主な義務は以下の通りである[78]。

- リスク評価
- CDD（EDD、継続的顧客管理、実質的支配者）
- コルレスリレーションシップ[79]
- PEPs
- 疑わしい取引の届出
- 記録の保存
- 方針・手続
- 経済制裁

また、MiCA においては、AML 上ハイリスク、および税務上非協力的として EU リストに記載されている法域所在の親会社によって設立された暗号資産交換業者については、EU の AML の枠組の中でより厳格な確認が求められることが予定されている[80]。

さらに、2022 年 6 月には、資金移転に適用される現行トラベルルール（Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006[81]、以下 EU トラベルルール規則という。）を踏まえ、これを暗号資産の移転に適用する規制案「Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets」（以下暗号資産トラベルルール規則案という。）[82]について、理事会と議会が暫定合意に達し、その適用は MiCA

---

77 Digital finance: agreement reached on European crypto-assets regulation (MiCA) (https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/)

78 EUR-Lex - 02015L0849-20210630 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L0849-20210630#tocId3)

79 コルレスバンキングについては、FATF 勧告 13 では、海外コルレスバンキングおよび「同様の関係」において、相手方金融機関等の DD を適切に実施（相手方との関係確立においては、上級管理職の承認を要することを含む）することが求められている。EU AML 指令では、コルレスリレーションシップとして Article 3(7)で同様に定義され、Article 19 にて同様の DD 義務等が規定されている。FATF 解釈ノートでは、資金移転等も FATF 勧告 13 における「同様の関係」の例として示されており、Updated Guidance でも VASP を介した顧客の暗号資産の移転で同様の特徴を有する場合は、これに該当し、相手方金融機関、あるいは VASP の DD を適切に実施すべきことが明記されている（同ガイダンス 166）。

80 Digital finance: agreement reached on European crypto-assets regulation (MiCA) (https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/)

81 EUR-Lex - 32015R0847 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0847)

82 Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (https://data.consilium.europa.eu/doc/document/ST-14259-2021-INIT/en/pdf)

の施行のタイムラインと合わせることが公表された[83]。

このように EU においては、暗号資産向けのトラベルルールは未制定、未施行の状態ではあるが、規制案は、以下の通り、概ね FATF 勧告[84]の趣旨に沿った内容となっている。

論点	FATF 要件	EU
制度化	FATF 勧告 16 に関して、（自主規制団体ではなく）国の制度として暗号資産に関するトラベルルールの規制・監督の枠組を定めるべき（INR15-7(b)）[85]	規則改正案は策定済み。 暫定合意に至っているが、未制定、未施行。 （以下は施行した場合を記載）
閾値[86]	1,000USD/EUR 超（INR16-5）[87]	1,000EUR 超（ただし、関連がある複数取引の合計を超える場合も含む）（規則案前文(22)）
VASP の関与	非規制対象者（アンホステッド・ウォレット）と暗号資産交換業者間の取引も FATF 勧告 16 が適用される。（Updated Guidance 179）[88]	左記準拠。VASP が一つでも関与する限り、アンホステッド・ウォレットとの移転も適用される。（規則案前文(29)）
発信側 VASP	送金人の正確な情報（氏名、口座番号、住所（もしくは何らかの識別子、生年月日、出生地）および受取人の正確な情報（氏名、口座番号）が取引情報に含まれていることを確保すること(INR16 6,7,11, UG Annex A 9(b)) [89]	左記準拠（規則案 Article 14-1, 2, 3, 5）。閾値以内の取引の取扱も準拠（規則案 Article 5-2(b), 6-2(b)）。
	上記は、取引の事前もしくは同時に実施すること(UG 185)	左記準拠（規則案 Article 14-4）
	上記情報を受信側暗号資産交換業者もしくは金融機関（存在する場合）に直ちに、かつ安全に送信すること(UG Annex 9(b))	左記準拠（規則案 Article 14-2）
	関連記録を保存すること(INR13)	左記準拠（規則案 Article 21）
	これらが準拠できない場合は送金を認めないこと(INR16-14)	左記準拠（規則案 Article 14-7）
受信側 VASP	送金人、受取人それぞれについて必要な情報が欠落している取引を特定すること（リアルタイムもしくは事後のいずれか適宜に）(INR16-19)	左記準拠（規則案 Article 16-1, 2）
	取引を受け付ける前に受取人の本人性を検証し、記録を保存すること(INR16-20)	左記準拠（規則案 Article 7-5-(a), 16-4(a), 21）
	必要情報が欠落している取引について、いつ執行、拒否、差し止めし、どのようにフォローアップするかについてリスクベースでの方針・手続を有すること(INR16-21)	左記準拠（規則案 Article 17）

83 Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers (https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/)

84 FATF 勧告の暗号資産のトラベルルール要件は、FATF 勧告 15、16、およびこれらの解釈ノート、および Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers の Annex A 等にまとめられている。本稿では、発信側 VASP および受信側 VASP が負う、取引に含まれるべき情報の確認義務を中心に整理する。

85 FATF の Updated guidance には、電信送金に関する FATF 勧告 16 および同解釈ノートは、暗号資産の移転に関する VASP の同様のサービスにも適用されること（同ガイダンス 175）、全ての暗号資産の移転は海外電信送金と同様に取り扱うべきこと（同ガイダンス 179）が明記されている。

86 ここで言う閾値は、正確性について検証したうえで情報を通知することが求められる取引額の最小値を言う。

87 厳密には、①各国は 1,000USD/EUR を上回らない範囲で閾値を定めることができ、閾値以下の取引については、送金人氏名、受取人氏名、およびそれぞれの暗号資産ウォレットアドレスまたは取引固有の参照番号の情報を収集する（検証までは求められない）ことが求められる。（UG 191）

88 すなわち、発信側 VASP にとっては、受取人側に該当 VASP が存在しない場合でも、情報確認等の義務が遵守できないときには送金できないこと、受信側 VASP にとっては、発信側 VASP が存在しない場合でも、必要情報が欠落している取引の特定と、受取人の本人性の検証、およびリスクに応じた対応が求められる、ということを意味する。なお相手方 VASP が存在し、かつ無届事業者等の場合の取扱は、トラベルルールではなく、FATF 勧告 13 で求められる相手事業者に対する DD の一環として対応すべきこと、と位置付けられる。

89 当該義務は既述の閾値を超える場合に適用される。閾値を超えない取引については、送金人、受取人の氏名、送金人の氏名、口座番号、もしくは取引参照番号の確認（検証までは求められない）が求められる（INR16-12）。もっとも閾値を超えない場合であっても ML/TF の疑いがある場合は、表記載の義務が適用される（INR16-5(a)）。

6.2.2 **各国法規制：フランス**

6.2.2.1 監督当局

金融市場庁（AMF; Autorité des Marchés Financiers）が所管する PACTE 法にて暗号資産および暗号資産交換業者を規律[90]。また、AMF は中央銀行の独立管理機関で銀行および保険部門を監督する健全性監督破綻処理機構（ACPR; Autorité de Contrôle Prudentiel et de Résolution）と協力して AML/CFT 規制の監督を行う体系となっている[91]。

6.2.2.2 関連法令

- 企業成長と変革行動計画法（Las Loi PACTE; Le Plan d'Action pour la Croissance et la Transformation des Entreprises）
- 通貨金融法典（Code Monétaire et Financier）

2019 年 5 月に施行された PACTE 法にて暗号資産および暗号資産交換業者の規制の枠組みを確立。また、2020 年 12 月の法令第 2020-1544 によって、PACTE 法に加え、通貨金融法典によって定められたフランスの AML/CFT 規制が暗号資産交換業者にも適用された[92]。

6.2.2.3 暗号資産の位置づけ

AMF は PACTE 法にて、暗号資産[93]を、「ICO の際に発行されるトークンと、欧州法[94]で定義されているビットコインなどの仮想通貨 (Virtual Currency)とで構成され、金融商品はこの枠組みからは除外される」と定義している[95]。

なお、2020 年 1 月の時点で、フランス銀行の第一副総裁が、「ステーブルコインについては新しく枠組みを作るのではなく、PACTE 法や EU の規制などの既存の規制枠組みの中で適応させていくのが良いと考えている」と述べており[96]、現段階においてステーブルコインに対して法規制面で特段の手当てをしている事実は確認できなかった。

---

90 Loi PACTE : des mesures structurantes pour l'AMF et les acteurs qu'elle régule (https://www.amf-france.org/fr/actualites-publications/actualites/loi-pacte-des-mesures-structurantes-pour-lamf-et-les-acteurs-quelle-regule)

91 Obtaining a DASP registration/optional licensing (https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#Focus_on_digital_asset_services)

92 Ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques (https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000042645365/)

93 法律上の用語は actifs numériques すなわちデジタル資産となっているが、実質的には本稿での暗号資産と同義であるため、暗号資産と表記した。同様に、原語ではデジタル資産サービス、デジタル資産サービス業者と訳されるところ、これらについてもそれぞれ暗号資産交換業、暗号資産交換業者とした。

94 Fifth Money Laundering Directive によって、仮想通貨は「中央銀行や公的機関によって発行もしくは保証されていない価値のデジタル表現として EU の AML 規則によって定義され、必ずしも法的に確立された通貨に裏付けされているわけではなく、通貨やお金の法的地位を持っていないが、交換手段として自然人または法人によって受け入れられ、電子的に転送、保存、取引することができるもの」と定義されている。

95 Towards a new regime for crypto-assets in France | AMF (https://www.amf-france.org/en/news-publications/news/towards-new-regime-crypto-assets-france)

96 Stablecoins: a good or a bad solution to improve our payment systems? (https://www.banque-france.fr/en/intervention/stablecoins-good-or-bad-solution-improve-our-payment-systems)

6.2.2.4　暗号資産交換業者

通貨金融法の第 L.54-10-2 条に記載されている下記の暗号資産交換業の少なくとも 1 つを提供する場合、暗号資産交換業者とみなされる[97]。

1. 顧客のための暗号資産の保管
2. 法定通貨での暗号資産の売買
3. 暗号資産と他の暗号資産の交換
4. 顧客の代理での暗号資産の売買注文
5. 暗号資産ポートフォリオの管理
6. 暗号資産の投資家へのアドバイス
7. 暗号資産の転売目的の引受行為
8. 暗号資産の保証販売代理業（guaranteed placement）（暗号資産の発行者に代わって購入者を探し、購入を約束することによって最低額を保証すること)
9. 暗号資産の無保証販売代理業（non-guaranteed placement）(購入金額を保証することなく、暗号資産の発行者に代わって購入者を探す行為)
10. 暗号資産の取引プラットフォームの運営

このうち、1. 暗号資産の保管、2. 法定通貨での暗号資産の売買、3. 暗号資産と他の暗号資産の交換、10. 暗号資産の取引プラットフォームの運営をフランスで提供する場合は AMF での登録が必須となる[98]。

6.2.2.5　暗号資産交換業者に求める主な AML/CFT 要件

2020 年 12 月 9 日の法令第 2020-1544 号[99]により、暗号資産交換業者は AML/CFT および資産凍結に関するすべての義務を履行しなければならないとされている[100]。

具体的には通貨・金融法の L. 561-2 のサブセクションの規定を遵守しなければならないとされているが、AMF が暗号資産交換業者の登録・許可の際に評価する主な項目について例を下記の通り挙げている[101]。

- 顧客のリスク分類
- 顧客との関係の分類
- CDD（真の受益者、EDD 等を含む）
- 疑わしい取引の届出
- 内部統制の整備と AML/CFT 規制遵守の責任者の任命
- 資産凍結措置の遵守

---

97 Obtaining a DASP registration/optional licensing（https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#Focus_on_digital_asset_services) (FATF の i～v の定義と概ね同義と考えられる)

98 上記資料には、登録された暗号資産交換業者のリストが記載されている。また、制度上は登録ではなく、許可(agrément optionnel 英語で optional licensing)を取得することもできるとされているが、同資料では、許可を取得した暗号資産交換業者はいない、と記載されている。

99 Ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques - Légifrance (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042636234)

100 Obtaining a DASP registration/optional licensing (https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#Focus_on_digital_asset_services)

101 AMF clarifications regarding the main measures to be implemented by digital assets service providers (https://www.amf-france.org/sites/default/files/private/2021-07/aml-cft-regulations.pdf)

- TRACFIN（フランスの FIU）による義務の遵守
- リスクベースで組織としての AML/CFT 体制の構築

フランスは EU 加盟国として、EU AML 指令に準拠した AML/CFT 規制となっている。なお、同国独自の暗号資産向けトラベルルールは適用されておらず、EU の規則案の制定待ちという状況である。

6.2.2.6 直近の規制・市場動向

2022 年 5 月 AMF は、資産運用会社に対し、暗号資産の形を含む有価証券のロシア関係者への販売、および暗号資産ウォレットのロシア関係者への提供の禁止を通達[102]

2022 年 6 月 MiCA（「6.2.1 各国法規制：EU」を参照）が欧州議会、理事会、委員会の三者間において合意されたことについて、AMF は、声明[103]にて、当該合意を歓迎すること、MiCA がフランスの PACTE 法の規制枠組みに取って代わるものになる予定であること、ただし施行までは、関係各位、業界団体と連携をとって移行を支援していくことを公表した。MiCA と同時に施行される予定のトラベルルール規制案について、フランスにおいて独自の手当てはなされておらず、状況としては EU にて記載のとおりと推察される。

2022 年 9 月 デジタル資産サービス業者 2 社が AMF によって登録リストから除外された。（1 社はサービスの停止により、1 社は登録要件の不遵守による） [104]

6.2.3 **各国法規制：ドイツ**

6.2.3.1 監督当局

金融規制当局 である BaFin(Bundesanstalt für Finanzdienstleistungsaufsicht)が所管する銀行法(KWG; Kreditwesengesetz)にて暗号資産交換業者を定義・規律。

6.2.3.2 関連法令

- 銀行法 Kreditwesengesetz（KWG）
- マネー・ローンダリング防止法 Geldwäschegesetz（GWG）

KWG にて暗号資産および暗号資産交換業者を定義し、暗号資産交換業者を金融サービス機関として位置付けることで、GWG にて他の金融機関同様、ALM/CFT の観点でも規律される仕組み。

6.2.3.3 暗号資産の位置づけ

KWG Section1-(11)-11 にて、暗号資産を「中央銀行または公的機関によって発行もしくは保証されておらず、法定通貨として機能しない、あらゆる価値のデジタル表現で、支払いや交換、投資目的で一般に受け入れら

---

[102] War in Ukraine: the AMF alerts asset management companies (https://www.amf-france.org/en/news-publications/news/war-ukraine-amf-alerts-asset-management-companies)

[103] Crypto-asset markets: Agreement reached on the European Crypto-Assets regulation (MiCA) (https://www.amf-france.org/en/news-publications/news/crypto-asset-markets-agreement-reached-european-crypto-assets-regulation-mica)

[104] Obtaining a DASP registration/optional licensing (https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#Focus_on_digital_asset_services)

れ、電子的に移転、蓄積、取引がされるもの（ただし決済サービス監督法で定義する電子マネーは除く）」と定義し、金融商品の一つとして位置付けている。

なお、同条項では、決済サービス監督法（ZAG）Section1-(2)-3 における電子マネー、または Section2-(1)-10 の要件を満たす、または Section2-(1)-11 に従って決済取引にのみ使用される金銭的価値は暗号資産ではないと規定されている。ZAG においては電子マネーを発行する事業者に対して、財務管理、流動性管理等を義務付けており、本来の意味でのステーブルコインおよびその発行者も、ZAG に基づく規制・監督を受けるものと解釈される。

6.2.3.4　暗号資産交換業者

KWG において金融サービス事業者は、金融商品の売買の手配（例：投資仲介）他人の口座のための他人の名前での金融商品の取得および販売（例：契約仲介）、意思決定権を持つ他者のために金融商品に投資された個々の資産の管理（例：金融ポートフォリオ管理）等を行うもの、と Section1-(1a)にて定義されており、既述の通り暗号資産は金融商品と整理されたことから、暗号資産についての投資仲介、契約仲介、金融ポートフォリオ管理等を行う者は金融サービス事業者として位置付けられる[105]。さらに同条項で、暗号資産または暗号資産の保管および移転のために使用される秘密鍵を、他人のために保管、管理、保護する（暗号カストディビジネス）者も、金融サービス事業者として定義されており、いわゆる暗号資産交換業者はこれらに該当すると解釈される[106]。

6.2.3.5　暗号資産交換業者に求める主な AML/CFT 要件

暗号資産交換業者は、GwG で求められる AML/CFT 要件を、他の金融サービス機関と同様のレベルで遵守する義務を有する。ドイツは EU 加盟国として、EU AML 指令に準拠した AML/CFT 規制となっている。さらに、暗号資産に関するトラベルルールについては、これを GWG に盛り込む施行令（Ordinance）KryptoWTransferV; Kryptowertetransferverordnung（英訳は、Ordinance on enhanced due diligence when transferring crypto assets）[107]が成立し、2021 年 10 月に施行された。この法的手当ては、EU での新たな規制が適用されるまでの措置と位置付けられている。KryptoWTransferV は、顧客の暗号資産の移転に関与する暗号資産交換業者は、資金移転に適用される現行の EU トラベルルール規則の関連条文で規定される義務を適宜負うこととしている。

ドイツのトラベルルールに関しては、EU と同様、以下の通り、概ね FATF 勧告 の趣旨に沿った内容となっている。なお、ドイツは EU に先んじて暗号資産に関するトラベルルールを施行済みであるが、移行期間中である。

105　金融サービス事業は KWG Section32 に基づく許可制となっている。

106　KWG においては、暗号資産交換業者（VASP）に該当する包括的な定義はないが、これらを総合すると、FATF の VASP の定義 i～v を網羅しているものと考えられる。

107　KryptoWTransferV - Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (https://www.gesetze-im-internet.de/kryptowtransferv/BJNR446500021.html)

論点	FATF 要件	ドイツ
制度化	FATF 勧告 16 に関して、（自主規制団体ではなく）国の制度として暗号資産に関するトラベルルールの規制・監督の枠組を定めるべき（INR15 7(b)）	KryptoWTransferV によって施行済み[108]。
閾値	1,000USD/EUR 超（INR16-5）	1,000EUR 超（関連がある複数取引の合計を超える場合も含む）（EU トラベルルール規則 Article 2-5(c), Article 6-2）
VASP の関与	非規制対象者（アンホステッド・ウォレット）と暗号資産交換業者間の取引も FATF 勧告 16 が適用される（Updated Guidance 179）	左記準拠（KryptoWTransferV§4(1)(2)）
発信側 VASP	送金人の正確な情報（氏名、口座番号、住所（もしくは何らかの識別子、生年月日、出生地）および受取人の正確な情報（氏名、口座番号）が取引情報に含まれていることを確保すること(INR16 6,7,11, UG Annex A 9(b)	左記準拠[109]（EU トラベルルール規則 Article 4-1,2）また、閾値以下でも少なくとも支払人と受取人の名前、口座番号が必要（ただし検証の必要はなし）（ EU トラベルルール規則 Article 5-2(b),3 Article 6-2,3）
	上記は、取引の事前もしくは同時に実施すること(UG 185)	左記準拠（EU トラベルルール規則 Article 4-4）
	上記情報を受信側暗号資産交換業者もしくは金融機関（存在する場合）に直ちに、かつ安全に送信すること(UG Annex 9(b)	左記準拠（EU トラベルルール規則 Article 4-2）
	関連記録を保存すること(INR13)	左記準拠（EU トラベルルール規則 Article 16）
	これらが準拠できない場合は送金を認めないこと(INR16-14)	左記準拠（EU トラベルルール規則 Article 4-6）
受信側 VASP	送金人、受取人それぞれについて必要な情報が欠落している取引を特定すること（リアルタイムもしくは事後のいずれか適宜に）(INR16-19)	左記準拠（EU トラベルルール規則 Article 7-1, 2）
	取引を受け付ける前に受取人の本人性を検証し、記録を保存すること(INR16-20)	左記準拠（EU トラベルルール規則 Article 7-5(a), 16）
	必要情報が欠落している取引について、いつ執行、拒否、差し止めし、どのようにフォローアップするかについてリスクベースでの方針・手続を有すること(INR16-21)	左記準拠（EU トラベルルール規則 Article 8）

6.2.3.6 直近の規制・市場動向

2020 年 1 月　暗号資産カストディ業を金融サービス業に追加

2020 年 10 月　老舗銀行 BVDH が欧州初のユーロ建てステーブルコイン EURB を発行

2020 年 10 月　ドイツ連邦財務省は暗号資産に係る所得税のガイドラインのドラフトを公表

2021 年 4 月　Binance が発行した株式トークンは、有価証券に該当するにも関わらず、法令上求められる目論見書を公表していないとして BaFin が警告文を公表[110]

2022 年 10 月　BaFin は暗号資産交換業者 Coinbase に対し、年次検査においてリスク管理体制および外部委託管理に関する KWG 上の違反が認められたとして体制改善の命令を発出[111]

---

108 なお、同規制の義務履行が困難な場合は相応の理由があれば、最大 24 か月の猶予期間が与えられている。BaFin - Aktuelles - Kryptotransferverordnung: BaFin veröffentlicht neues Formular (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2021/meldung_2021_11_23_Formular_Kryptotransferverordnung.html)

109 厳密には当規則は暗号資産固有の事情を踏まえていないため、確認情報は住所、個人の公的識別番号等とされており、暗号資産固有の識別子といった概念は明確には示されていない。

110 Binance Deutschland GmbH & Co. KG: Hinreichend begründeter Verdacht für fehlende Prospekte (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2021/meldung_210428_binance_deutschland.html)

111 Coinbase Germany GmbH: BaFin ordnet Sicherstellung einer ordnungsgemäßen Geschäftsorganisation an (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/meldung_2022_11_08_Coinbase_Germany.html)

6.2.4 **各国法規制：ノルウェー**

6.2.4.1 監督当局

ノルウェーの金融規制・監督当局は、ノルウェー金融監督庁（FSAN; Finanstilsynet）である。AML 法は財務省（Finansdepartementet）が所管し、規制対象となる業種ごとに監督官庁が存在する。対象事業のほとんどが FSAN の監督下にある。また、FIU は Økokrim （ノルウェーの経済・環境犯罪捜査・起訴機関）の一部門が担っている。

6.2.4.2 関連法令

包括的な金融規制法としての金融企業法（Finansforetaksloven; Lov om Finansforetak og Finanskonsern）の他、証券取引法金融商品関連で証券取引法（Verdipapirhandelloven; Lov om verdipapirhandel）が存在する。また AML 関連では、AML 法[112]（Hvitvaskingsloven; Lov om Tiltak Mot Hvitvasking og Terrorfinansiering）が規定されている。

6.2.4.3 暗号資産の位置づけ

現段階において、AML 法改正によって、仮想通貨（Virtual Currency）関連事業は別途規則で定めることができる旨が規定され、これに基づいて AML 規則（Hvitvaskingsforskriften; Forskrift om tiltak mot hvitvasking og terrorfinansiering）において、仮想通貨とは、「中央銀行や公的機関が発行しておらず、必ずしも公的通貨と連動しておらず、貨幣や通貨の法的地位を持たないが、決済手段として受け入れられ、電子的手段で送金、保管、取引できるデジタル価値表現」と定義されている[113]。これ以外、金融企業法、証券取引法等において包括的に暗号資産、仮想通貨を定義しているものは確認されず、金融企業法の電子マネーの定義や証券取引法の金融商品の定義に該当すると認められる場合は、それぞれの法律による規制を受けるものと解釈される。

6.2.4.4 暗号資産交換業者

暗号資産の定義と同様、暗号資産交換業者を包括的に定義する法は定められておらず、AML 規制にて仮想通貨サービス（Virtual Currency Services）を対象として定義・規律されている。

すなわち、仮想通貨サービス事業者の定義は、仮想通貨と法定通貨の交換サービスを提供する事業者、仮想通貨のカストディサービスを提供する事業者とされ、これらの事業者は、AML 法の規制対象事業者となり、免許が必要であることが同規則にて定められている[114]。

---

112 Act relating to Measures to Combat Money Laundering and Terrorist Financing (https://lovdata.no/dokument/NLE/lov/2018-06-01-23)

113 Regulations relating to Measures to Combat Money Laundering and Terrorist Financing Section 1-3 (2) (https://www.finanstilsynet.no/globalassets/laws-and-regulations/regulations/aml-regulations-of-14-september-2018.pdf)

114 同 Section 1-3 (1), (3), (4)。FATF の定義との比較では、対象が仮想通貨に限られている他、「v. 暗号資産の発行や販売への参加および金融サービスの提供」が明示的に含まれていない。

6.2.4.5　暗号資産交換業者に求める主な AML/CFT 要件

上記の通り、仮想通貨サービス事業者は、AML 法上の規制対象事業者であり、他の金融機関同様の AML/CFT の義務を負う。

ノルウェーは EU 加盟国ではないが、欧州経済領域（EEA）メンバー国[115]として、EU　AML 指令に準拠した AML/CFT 規制となっている。なお、同国独自の暗号資産向けトラベルルールは適用されておらず、EU の規則案の制定待ちという状況である。

6.2.4.6　直近の規制・市場動向

2022 年 4 月　ノルウェーは EU からの第 5 次制裁パッケージを採択し、ウクライナの安全を脅かす行為に関する制限措置の規則の改正に関する規則を発行し、ロシアにおける特定の預金の受領および暗号資産に関するサービスの実行を禁止[116]

2022 年 5 月　中央銀行であるノルウェー銀行が金融インフラレポート 2022 を公表[117]し、暗号資産について以下のように取りまとめた。

- EU、EEA レベルで MiCA を中心に検討が進んでいるものの、規制上対応すべきことは多い
- ステーブルコインのリスクへの対処を目的とした国際的に多くの規制的イニシアチブに引続き注目していく
- ノルウェーとしても欧州での MiCA 成立に協力しているが、各国施行までに相応の時間を要する

2022 年 10 月　ノルウェー財務大臣が、仮想通貨マイニングも含むデータセンターに対する電力料金優遇措置について、昨今の事情に鑑みて中止すべきと発言したと報道された。

2022 年 10 月　ノルウェーがメタバース上での税務署開設を計画していると報道された。

6.2.5 **各国法規制：オーストラリア**

6.2.5.1　監督当局

オーストラリアの金融規制・監督当局 は、オーストラリア証券投資委員会（ASIC）およびオーストラリア健全性規制庁（APRA）である[118]。AML 当局は AUSTRAC (Australian Transaction Reports and Analysis Center)である。

6.2.5.2　関連法令

ASIC 所管関連法として、会社法 (Corporations Act 2001)、証券投資委員会法（ASIC; Australian Securities and Investments Commission Act 2001)、APRA 所管関連法として、Banking Act 1959、

---

115 Ten facts about the EEA (https://www.norway.no/en/missions/eu/ten-facts-about-the-eea2/)

116 Forskrift om endring i forskrift om restriktive tiltak vedrørende handlinger som undergraver eller truer Ukrainas territorielle integritet, suverenitet, uavhengighet og stabilitet (https://lovdata.no/dokument/LTI/forskrift/2022-04-29-658)

117 Financial Infrastructure Report 2022 (norges-bank.no) (https://www.norges-bank.no/en/news-events/news-publications/Reports/Financial-Infrastructure-Report/financial-infrastructure-2022/)

118 ASIC が金融サービス業の許可、APRA が預金受入機関の許可権限を有する。

AML 関連法として AML/CFT 法(AML/CFT Act; Anti-Money Laundering and Counter-Terrorism Financing Act 2006)が存在する。

6.2.5.3 暗号資産の位置づけ

現段階において、暗号資産を包括的に定義した法律はないものと思われる。

唯一、AML/CFT 法§5 において「デジタル通貨」が以下の通り定義されている[119]。

(a) 以下のような価値のデジタル表現

(i) 交換の媒体、経済的価値の貯蔵、または記帳単位として機能し、
(ii) 政府機関、または政府機関の権限の下で発行されるものではなく、
(iii) (口座の借方記入を含む) 金銭と交換可能であり、商品またはサービスの供給の対価として使用され、かつ、
(iv) 利用が制限されることなく、公衆の利用に供されるもの、もしくは、

(b) AML/CFT 規則によってデジタル通貨であると宣言された交換、デジタルプロセス、またはクレジットの手段

現段階において、ASIC は暗号資産に関する案内文書[120]をウェブサイトに公開しており、暗号資産とみなされるものが、どのような場合に会社法、もしくは証券投資委員会法上の金融資産に該当するかを解説している。たとえば、ICO を用いた投資管理スキーム、有価証券、デリバティブ等に該当すれば、会社法の適用を受ける可能性が高いこと等が示されている。

6.2.5.4 暗号資産交換業者

暗号資産と同様、暗号資産交換業者についても、現段階において、包括的に定義した法律はないものと思われる。唯一、デジタル通貨交換プロバイダー(DCE: Digital Currency Exchange Provider)が AUSTRAC によって以下の通り定義されている[121]：

「デジタル通貨交換業の一環として、デジタル通貨と法定通貨の交換を行う自然人もしくは法人」

デジタル通貨交換プロバイダーは、AUSTRAC への登録が必要である。

既述の ASIC の暗号資産に関する案内文書によれば、金融商品に該当する暗号資産に関して、助言、ディーリング、保険の提供、その他の仲介関連サービスを提供する場合や、取引所を運営する場合は、国内法の適用を受ける可能性が高く、この場合は、オーストラリア金融サービス（AFS）からライセンスを取得する必要があること等が示されている。

6.2.5.5 暗号資産交換業者に求める主な AML/CFT 要件

既述のデジタル通貨交換プロバイダーおよび、金融商品に該当する暗号資産に関して金融サービス業に該当する場合は、AML/CFT 法の適用を受け、一般的な金融機関と同様、リスク評価、CDD、取引モニタリング（疑

[119] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (https://www.legislation.gov.au/Details/C2022C00179)
[120] Crypto-assets (https://asic.gov.au/regulatory-resources/digital-transformation/crypto-assets/)
[121] Digital currency exchange providers (https://www.austrac.gov.au/business/industry-specific-guidance/digital-currency-exchange-providers) FATF の i～v の定義に照らして網羅的ではない状況と言える。

わしい取引の届出含む）、記録の保存、その他の義務を負う。

2022 年 11 月現在、暗号資産に対するトラベルルールは存在せず、規制案も示されていない。

6.2.5.6 直近の規制・市場動向

2018 年 4 月　AML/CFT 法でデジタル通貨、デジタル通貨交換プロバイダーが定義された。

2021 年 10 月　豪上院に設置されたテクノロジーおよび金融センターとしてのオーストラリアに関する特別委員会が報告書[122]を公表、レポートを発行し、暗号資産に関して以下を勧告。

- AUSTRAC のみでの規制ではなく、適切に設計された免許制度を確立すべき
- デジタル資産のカストディ、預託サービスに対する規制を確立すべき
- 変化する暗号資産トークンの定義と分類明確化（ステーブルコイン含む）が必要
- 分散型自律機関への法的取極めの明確化が必要
- トラベルルール適用等の AML/CFT 規則の改正が必要
- 税制改革が必要
- CBDC 取組方針の明確化が必要

2022 年 3 月　政府は、上記報告書に基本的に同意し、このうち 1 と 2 に関して以下の内容のコンサルテーションペーパーを公表して意見を募集[123]。

- 暗号資産を会社法第 764 A 条に基づく金融商品と定義すること
- 従来のデジタル通貨交換プロバイダーを AML 規制ではなく金融規制下の暗号資産セカンダリーサービスプロバイダーと再定義し、免許制度とすること

2022 年 4 月　APRA は規制対象である預金受入機関の暗号資産リスク軽減を目的とし、規制対象機関向けに中期ポリシーロードマップを策定。ロードマップでは対象機関の暗号資産関連活動において期待する包括的なリスク管理対策を提示、および政策の方向性等を明確化[124]。

6.2.6 **各国法規制：カナダ**

6.2.6.1 監督当局

カナダの金融規制・監督は、金融機関監督庁（OSFI; Office of the Superintendent of Financial Institutions）が、連邦規制下の商業銀行等を監督する一方、証券会社等は州法に基づくものであり、州政府が監督[125]するという構造となっている。後者については、連邦レベルでは州政府監督当局を総合調整する機関としてカナダ証券管理局（CSA; Canadian Securities Administrators）が、自主規制機関として投資業

---

122 Parliament of Australia Committee on Financial Technology and Regulatory Technology - Final report (https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report)

123 Crypto asset secondary service providers: Licensing and custody requirements (https://treasury.gov.au/consultation/c2022-259046)

124 APRA: Crypto-assets: Risk management expectations and policy roadmap (https://www.apra.gov.au/crypto-assets-risk-management-expectations-and-policy-roadmap)

125 たとえば最大の州であるオンタリオでは、Security Act, R.S.O. 199, C, S,5 （https://www.ontario.ca/laws/statute/90s05）が証券法で、Ontario Securities Commission（https://www.osc.ca/en）が所管当局である。

規制機構（IIROC; Investment Industry Regulatory Organization of Canada）が存在する。

AML 規制当局は、カナダ金融取引報告分析センター（FINTRAC; Financial Transactions and Reports Analysis Centre of Canada）である。

6.2.6.2 関連法令

商業銀行は銀行法（Bank Act 1991, c. 46）、証券会社は既述のとおり州ごとの証券法が根拠法令である。銀行法上の規制対象事業者は免許制、州証券法の規制対象事業者は届出制に基づく。

AML/CFT は、PCMTFA; Proceeds of Crime (Money Laundering) and Terrorist Financing Act[126]が根拠法である。

6.2.6.3 暗号資産の位置づけ

銀行法あるいは証券関連法において、包括的に暗号資産を定義したものは存在しないと思われる。

ただし、AML/CFT 法である、PCMLTFA において、仮想通貨（Virtual currency）については、別途規制を定めることができると規定され、これに基づいて同法規則（PCMLTFR; Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations[127]）において、以下のように定義されている。

(a) 支払または投資の目的で使用できる、法定通貨ではなく、資金または資金と交換できる別の仮想通貨と容易に交換できる価値のデジタル表現、または

(b) 個人または団体が価値のデジタル表現にアクセスできるようにする暗号化システムの秘密鍵

一方、CSA は 2020 年 1 月 16 日にガイダンス[128]を公表し、もし、その暗号資産（Crypto asset）が、有価証券、デリバティブもしくはコモディティに該当し、当該暗号資産がプラットフォーム上で取引されるなら、そのようなプラットフォームは証券法の規制対象となる、との解釈を示した。

6.2.6.4 暗号資産交換業者

暗号資産と同様、暗号資産交換業者についても、現段階において、包括的に定義した法律はないものと思われる。

AML 法である PCMLTFA においては、仮想通貨の取扱（dealing）をカナダにおいて業として提供する者（同法 5(h)(iv), (h.1)(iv)）は同法の対象となる、とのみ規定されている。さらに同法規則である PCMLTFR においては、クラウドファンディングプラットフォームサービスを他人のために資金や仮想通貨を発行するためのプラットフ

126 Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) (https://lois-laws.justice.gc.ca/eng/acts/P-24.501/FullText.html#h-398215)

127 Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (https://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/index.html)

128 CSA Staff Notice 21-327 Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets (https://www.osc.ca/sites/default/files/pdfs/irps/csa_20200116_21-327_trading-crypto-assets.pdf)

ォームを提供、維持する者と定義し（同規則 1(2)）同法適用対象事業者となることが示されている[129]。

なお、CSA は既述のガイダンスにおいて、いくつかのプラットフォーム事業者は、デリバティブもしくは有価証券ではない暗号資産のみを取り扱っていることから、証券規制の対象ではないと考えているようだが、そのような暗号資産を通じて、プラットフォームは何らかの契約上の権利もしくは請求権をユーザーに提供していると考えられるため、その場合は、一般論として証券規制対象であると CSA は結論付けている、としている。

6.2.6.5　暗号資産交換業者に求める主な AML/CFT 要件

2021 年 6 月の PCMLTFA、および PCMLTFR の改正により、既述の仮想通貨取引を提供する事業者は、同法および同規則等で定める AML/CFT 要件の遵守義務を有する。主な要件は以下の通り。

- 大口仮想通貨取引の報告
- 疑わしい取引の届出
- CDD（PEPs、継続的顧客管理含む）
- 記録の保存
- 仮想通貨に関するトラベルルール
- コンプライアンスプログラムの実践

この中で、仮想通貨に関する大口取引の報告、およびトラベルルールが義務付けられたことが特徴と言える[130]。トラベルルールに関しては、PCMLTFA 9.5 において、電信資金移転（electric fund transfer）について、事業者は必要情報の確保、そのための対応措置を義務付けており、これに基づき PCMLTFR 124.1 および関連条項において仮想通貨移転に関する要件が定められている。既述の通り、カナダにおいては暗号資産交換業者という定義がないことから、PCMLTFR 124.1 においては、仮想通貨に関して記録の保存を PCMLTFR によって義務付けられている金融機関（financial entity）、資金移動業者（money services business）もしくは外国送金業者（foreign money services business）を対象として暗号資産に関するトラベルルールが適用されるという形をとっている。内容については、以下の通り、必ずしも FATF 要件準拠と言い切れず、不明確な部分も残している。

[129] このようにカナダにおける暗号資産交換業者の定義は、仮想通貨に限られていること、dealing という整理で包括的に定義されていること、クラウドファンディングプラットフォームについてはアドホックに定義されていること等から、FATF の i～v の定義との対応関係を整理することが難しく、必ずしも明確な定義となっているわけではないと言える。

[130] Regulatory amendments in force as of June 1, 2021 (https://fintrac-canafe.gc.ca/notices-avis/2021-06-01-eng)

論点	FATF 要件	カナダ
制度化	FATF 勧告 16 に関して、（自主規制団体ではなく）国の制度として暗号資産に関するトラベルルールの規制・監督の枠組を定めるべき（INR15 7(b)）	PCMLTFA および PCMLTFR として施行済み。
閾値	1,000USD/EUR 超（INR16-5）	CAD1,000（PCMLTFR 12(r)等[131]）
VASP の関与	非規制対象者（アンホステッド・ウォレット）と暗号資産交換業者間の取引も FATF 勧告 16 が適用される（Updated Guidance 179）	不明確。（下記発信側 VASP の要件参照）
発信側 VASP	送金人の正確な情報（氏名、口座番号、住所（もしくは何らかの識別子、生年月日、出生地）および受取人の正確な情報（氏名、口座番号）が取引情報に含まれていることを確保すること(INR16 6,7,11, UG Annex A 9(b)	一部準拠（PCMLTFR 124.1(1)(a)）。必要情報は網羅しているが、FATF が求める正確な情報の確保、すなわち検証を行うことは明示されていない。
	上記は、取引の事前もしくは同時に実施すること(UG 185)	左記準拠（PCMLTFR 124.1(1)(a)）
	上記情報を受信側暗号資産交換業者もしくは金融機関（存在する場合）に直ちに、かつ安全に送信すること(UG Annex 9(b)	左記のように VASP もしくは金融機関が存在する場合に情報を送信するとの規定はなく、単に発信側 VASP は移転取引に必要情報を含めることとされている。
	関連記録を保存すること(INR13)	左記準拠（PCMLTFR 12 等）[132]
	これらが準拠できない場合は送金を認めないこと(INR16-14)	上記のとおり、関連情報を取引に含めることが規定されているが、左記趣旨での明示規定はない。
受信側 VASP	送金人、受取人それぞれについて必要な情報が欠落している取引を特定すること（リアルタイムもしくは事後のいずれか適宜に）(INR16-19)	必要情報が受信情報に含まれていることについて合理的な措置をとることが規定されている（PCMLTFR 124.1(1)(b)）が、左記趣旨での明示はない。
	取引を受け付ける前に受取人の本人性を検証し、記録を保存すること(INR16-20)	一般的な事業者の義務として顧客の本人性を検証することが求められている（PCMLTFR Part2 等）が、トラベルルールとして左記趣旨での明示規定はない。
	必要情報が欠落している取引について、いつ執行、拒否、差し止めし、どのようにフォローアップするかについてリスクベースでの方針・手続を有すること(INR16-21)	左記準拠（PCMLTFR124.1(2)）

6.2.6.6 直近の規制・市場動向

2021 年 12 月　オンタリオ州証券委員会がバイナンスは州の証券規制上、無届事業者であり、有価証券、デリバティブの取引は住民に提供できないと警告[133]

2022 年 6 月　CSA は Business Plan 2022-2025[134]を公表し、その中で「暗号資産取引プラットフォームに対して、より包括的な規制体系を構築していくこと、ステーブルコインについては規制の方向性について引き続き監視、評価を継続すること」を表明

2022 年 8 月　CSA は、州当局に届出申請を行った暗号資産取引プラットフォーム事業者三社の社名を公表し、他の事業者について、届出の用意をしない事業者にはしかるべき措置をとる、との警告を

131 既述の通り、暗号資産に関するトラベルルールは、仮想通貨に関する記録の保存を義務付けられている事業者を対象としており、この閾値は、トラベルルールではなく、それぞれの事業者に対する一般的な記録の保存義務として定められているものである。閾値以下の取引についての特段の取り決めはなされておらず、FATF 要件とのギャップが存在すると考えられる。

132 上記の通り、トラベルルールとして記録の保存に関する規定があるわけではなく、より一般的な記録の保存が求められている事業者に対するトラベルルール規定という形をとっている。

133 Binance is not registered in Ontario (https://www.osc.ca/en/news-events/news/binance-not-registered-ontario)

134 2022_2025CSA_BusinessPlan.pdf (https://www.securities-administrators.ca/wp-content/uploads/2022/10/2022_2025CSA_BusinessPlan.pdf)

公表[135]

2022 年 11 月　オンタリオ州証券委員会が、無届の事業者 11 社を公表[136]

2022 年 11 月　オンタリオ州証券委員会が投資家教育ウェブサイト GetSmarterAboutCrypto.ca を開設[137]

6.2.7 **各国法規制：韓国**

6.2.7.1　監督当局

韓国の金融規制・監督は、金融監督委員会（FSC; Financial Supervisory Commission）の下で執行機関として金融監督院（FSS; Financial Supervisory Service）が担い、ほぼすべての金融機関が同一の監督当局の管轄となっている。

AML 規制当局は、FSC 下の KoFIU; Korea Financial Intelligence Unit である。

6.2.7.2　関連法令

FSS 所管関連法として、銀行法（Banking Act）、資本市場統合法（FSCMA; Financial Investment Services and Capital Markets Act）が存在する。銀行法の下で銀行事業者は FSC による許可制、FSCMA の下で金融投資事業者は FCS による許可制もしくは届出制（事業の内容によって異なる）となっている。

AML/CFT 関連法は、マネー・ローンダリングを犯罪化する根拠法である犯罪収益法（POCA; Proceeds of Crime Act）および、KoFIU の権限や、金融機関の義務を規定する金融取引報告法（FTRA; Financial Transaction Reports Act）[138]が存在する。

6.2.7.3　暗号資産の位置づけ

銀行法あるいは FSCMA において、包括的に暗号資産を定義したものは存在しないと思われる。

ただし、AML/CFT 法である FTRA 第 2 条第 3 項において、暗号資産（Virtual asset）が以下のように定義されている[139]。

「経済的価値を有するものとして電子的に取引または移転することができる電子的証票。ただし以下を除く。

(a) 現金、商品、サービスなどとの交換ができず、発行者によって販売、利用が制限されている電子的な証票
(b) 「ゲーム産業振興に関する法律」第 32 条第 1 項第 7 号によるゲーム関連サービスの利用を通じて獲得した有形無形の商品
(c) 「電子金融取引法」第 2 条第 14 号による前払い電子支払手段および同条第 15 号による電子通貨

---

135 Canadian securities regulators expect commitments from crypto trading platforms pursuing registration (https://www.osc.ca/en/news-events/news/canadian-securities-regulators-expect-commitments-crypto-trading-platforms-pursuing-registration)

136 OSC investor warnings and alerts for October 25 – November 15, 2022 (https://www.osc.ca/en/news-events/news/osc-investor-warnings-and-alerts-october-25-november-15-2022)

137 Home - GetSmarterAboutCrypto.ca (https://getsmarteraboutcrypto.ca/)

138 특정금융거래정보의보고및이용등에관한법률 (https://www.law.go.kr/법령/특정금융거래정보의보고및이용등에관한법률)

139 Financial Transaction Reports Act ｜ FIU (https://www.kofiu.go.kr/eng/legislation/financial.do)

(d) 「株式・社債等の電子登録に関する法律」第 2 条第 4 号による電子登録株式等
(e) 「電子手形の発行および流通に関する法律」第 2 条第 2 号による電子手形
(f) 「商法」第 862 条による電子船荷証券
(g) その形態や特性を関して、大統領令によって規定される取引

6.2.7.4 暗号資産交換業者

暗号資産と同様、暗号資産交換業者についても、銀行法あるいは FSCMA レベルでの規定は確認できなかったが、AML/CFT 法である FTRA 第 2 条第 1 項において、暗号資産交換業者（Virtual asset service provider）とは、以下のような暗号資産に関わる業務を行う者として定義されている[140]。

(i) 暗号資産の売買
(ii) 暗号資産とその他の資産との交換
(iii) 大統領で定める暗号資産の移転
(iv) 暗号資産の保管・管理
(v) 上記(i)および(ii)にかかわる仲介・斡旋・代行
(vi) 暗号資産に関してマネー・ローンダリングおよびテロ資金供与のおそれがある、として大統領令で定めるその他の行為

上記によって定められた暗号資産交換業者は、KoFIU に事業を届出ることが求められるとともに、銀行、保険会社、証券会社等と同様、金融機関（Financial company）として FTRA に定められる AML/CFT 上の義務を負う。

なお暗号資産交換業者の届出制度は、FTRA の 2021 年 9 月の改正によって開始されたものであり、これに先立って FSC は、暗号資産交換業者 25 社に対し以下のような事前相談を実施したと公表した[141]。

- 対象となり得る 33 社のうち 25 社が事前相談を希望した。
- すべての届出要件を満たす暗号資産交換業者はいなかった。（ISMS 認証取得済が 19 社、実名確認済口座要件を満たしているのは 4 社にとどまった）

6.2.7.5 暗号資産交換業者に求める主な AML/CFT 要件

金融機関である暗号資産交換業者が負うべき FTRA 上の AML/CFT の義務は以下の通りである。

- 疑わしい取引の届出
- 大口現金取引の届出[142]
- 統括責任者の任命
- 方針手続の確立と実践

---

140 FATF の i～v に沿った定義と言える。
141 Press Releases - Financial Services Commission (https://fsc.go.kr/eng/pr010101/76393?srchCtgry=&curPage=&srchKey=cn&srchText=virtual%20asset&srchBeginDt=&srchEndDt=)
142 韓国においては暗号資産交換業者の顧客に対しては暗号資産のままでの移転を認めておらず、銀行口座を通じた現金での暗号資産交換業者の当該顧客口座との入出金のみ認められている。結果、暗号資産は大口現金取引の対象とはなっていない。

- 役職員の教育研修
- CDD[143]
- トラベルルール
- 記録の保存

なお、トラベルルールは、従来から国内為替、外国為替に適用されているものであり、大統領令 32028 号[144]による FTRA 改正に伴って、暗号資産にも適用されることとなり、半年の猶予期間を経て百万ウォン以上相当の取引を対象として 2022 年 3 月より施行された。韓国のトラベルルールについては世界的にも早い時期に制定・施行されたものの、以下に見る通り、現段階では、情報提供の内容も含め FATF 要件との差異がかなり見受けられる状況となっている。

論点	FATF 要件	韓国
制度化	FATF 勧告 16 に関して、（自主規制団体ではなく）国の制度として暗号資産に関するトラベルルールの規制・監督の枠組を定めるべき（INR15 7(b)）	FTRA 改正に伴って施行済み。
閾値	1,000USD/EUR 超（INR16-5）	100 万ウォン（FTRA5-3 および大統領令 32028 号 10-10）[145]
VASP の関与	非規制対象者（アンホステッド・ウォレット）と暗号資産交換業者間の取引も FATF 勧告 16 が適用される（Updated Guidance 179）	大統領令（10-10）には VASP が他の VASP に対して情報を提供すべきことが規定されているのみであり、発信側 VASP のアンホステッド・ウォレットへの、あるいはアンホステッド・ウォレットから受信側 VASP への取引は規制対象外と解釈される。
発信側 VASP	送金人の正確な情報（氏名、口座番号、住所（もしくは何らかの識別子、生年月日、出生地）および受取人の正確な情報（氏名、口座番号）が取引情報に含まれていることを確保すること(INR16 6,7,11, UG Annex A 9(b)	受信側 VASP に送るべき情報として、大統領令には、送金人および受取人の氏名および暗号資産アドレスとのみ規定されており、左記とはギャップがある[146]。さらに FATF が求める正確な情報の確保（検証を含む）も定められていない。
	上記は、取引の事前もしくは同時に実施すること(UG 185)	左記準拠（大統領令 10-10-4）
	上記情報を受信側暗号資産交換業者もしくは金融機関（存在する場合）に直ちに、かつ安全に送信すること(UG Annex 9(b)	送金と同時に情報を提供することは規定されている（同上）が、直ちに、かつ安全に送信することの規定はない。
	関連記録を保存すること(INR13)	左記遵守。（FTRA5-4-3）
	これらが準拠できない場合は送金を認めないこと(INR16-14)	上記の通り、送金時に情報を提供することが求められているのみであり、左記に関する規定はない。
受信側 VASP	送金人、受取人それぞれについて必要な情報が欠落している取引を特定すること（リアルタイムもしくは事後のいずれか適宜に）(INR16-19)	韓国の暗号資産トラベルルールは発信側 VASP に送金時に含めるべき必要情報の提供を求めるものであり、左記に関する規定はない。
	取引を受け付ける前に受取人の本人性を検証し、記録を保存すること(INR16-20)	同上。
	必要情報が欠落している取引について、いつ執行、拒否、差し止めし、どのようにフォローアップするかについてリスクベースでの方針・手続を有すること(INR16-21)	同上。

143 FTRA において、暗号資産交換業者向けに第 6、7、8 条を特別に規定し、KoFIU への報告事項を定めている。

144 특정금융거래정보의보고및이용등에관한법률시행령 (https://www.law.go.kr/법령/특정금융거래정보의보고및이용등에관한법률시행령)

145 100 万ウォンは 2022 年 12 月 16 日現在で 800 ドル弱であり、FATF 要件と概ね整合的である。ただし、閾値を超える場合に求められる情報の取り扱いを規定するものであり、閾値以下の取引についての特段の取り決めはなされておらず、FATF 要件とのギャップが存在すると考えられる。

146 一般規定として、顧客の本人性を検証することは記載されている（FTRA5-2 等）が、これが本トラベルルールにおいて受取人に関する情報も含めてどのようにカバーされるのかは不明である。

韓国のトラベルルールは、アンホステッド・ウォレットとの取引については規制対象とはなっていない等、FATF 要件と照らしても、ギャップが認められる状況だが、以下のように業界の自主的な取組も進められている。

KoFIU の企画関連局の局長は以下の趣旨のプレス・リリース[147]を 2022 年 3 月 5 日に公表している。

- 現在、各暗号資産事業者が推進している暗号資産の個人ウォレットへの振替の事前登録制度は、マネー・ローンダリング等を防止するために業界が自主的に推進している案件である。
- 海外の暗号資産交換業者の場合、韓国とは異なり、トラベルルールは必須ではなく、実質的に実施の準備ができていない。このため、業界との協議の上、トラベルルールのない海外の暗号資産交換業者への暗号資産の移転は、マネー・ローンダリングのリスクを低減するために、送金者と受取人が同一であることが確認され、当該暗号資産交換業者のマネー・ローンダリングのリスクが低いと評価された場合に限り実施される。

このプレス・リリースは、韓国においては、アンホステッド・ウォレットとの取引は業界の自主的な取組によって、顧客自身の個人ウォレットへの振替のみに限ること、海外の暗号資産交換業者へ移転する場合も、送金人と受取人が同一の場合に限ること、についての当局の期待を述べたものと考えられる。

さらに、KoFIU は、暗号資産交換業者と行った会合の内容について、暗号資産検査部門の課長名で、2022 年 11 月 16 日にプレス・リリース[148]を公表し、事業者は、経済制裁対象者に対するブラックリストおよび、送金人と受取人が同一であると検証されたホワイトリスト双方の管理によって取引の透明性が高まっている、と述べている。

6.2.7.6 直近の規制・市場動向

2017 年 9 月 FSC が ICO を全面的に禁止することを発表

2022 年 3 月 デジタル資産基本法制定、ICO 許可、暗号資産収益の非課税枠拡大、ゲーム P2E の緩和などを公約に掲げた尹錫悦候補が大統領に当選

2022 年 5 月 韓国人が創業した Terraform Labs によるステーブルコイン TerraUSD やカバナンストークン Luna が暴落、検察関係者が同創業者に対し逮捕状を出状したとメディアが報道

2022 年 5 月 政府がいわゆるデジタル資産基本法を検討していると複数のメディアが報道

2022 年 6 月 大手仮想通貨取引所数社が、トラベルルールに準拠するために、プライバシー機能（MinbleWinble extension block）を実装したライトコイン（LTC）の取扱をやめた、とメディアが報道

2022 年 8 月 FSC がデジタル資産に関する官民連携のタスクフォースの第一回会議を開催したと公表

2022 年 8 月 FSC 委員長が、デジタル資産法案については、タスクフォースを通して、ブロックチェーンの開発、

147 문서뷰어 (https://www.korea.kr/docViewer/skin/doc.html?fn=0b928865cfea09cf95141ec4a268b453&rs=/docViewer/result/2022.05/02/0b928865cfea09cf95141ec4a268b453)

148 문서뷰어 (https://www.korea.kr/docViewer/skin/doc.html?fn=0b928865cfea09cf95141ec4a268b453&rs=/docViewer/result/2022.05/02/0b928865cfea09cf95141ec4a268b453)

投資家保護、市場安定のバランスをとりながら検討すると述べた、とメディアが報道

2022 年 8 月　FIU が特金法上未登録の暗号資産交換業者 16 社を捜査機関に通報し全登録事業者に対し当該業者との取引停止を指示したと公表[149]

6.2.8 各国法規制（まとめ）

以上、各国法規制のうち、特に差異が認められる暗号資産のトラベルルールに関して、簡単にまとめると以下のようになる。

論点	FATF 要件	EU	フランス	ドイツ	ノルウェー	豪	カナダ	韓国
制度化	FATF 勧告 16 に関して、（自主規制団体ではなく）国の制度として暗号資産に関するトラベルルールの規制・監督の枠組を定めるべき（INR15 7(b)）	案策定未施行	案策定未施行	施行済み	案策定未施行	未施行	施行済み	施行済み
閾値	1,000USD/EUR 超（INR16-5）	(〇)	(〇)	〇	(〇)	×	△	△
VASP の関与	非規制対象者（アンホステッド・ウォレット）と暗号資産交換業者間の取引も FATF 勧告 16 が適用される（Updated Guidance 179）	(〇)	(〇)	〇	(〇)	×	△	△
発信側 VASP	送金人の正確な情報（氏名、口座番号、住所（もしくは何らかの識別子、生年月日、出生地）および受取人の正確な情報（氏名、口座番号）が取引情報に含まれていることを確保すること(INR16 6,7,11, UG Annex A 9(b)	(〇)	(〇)	〇	(〇)	×	△	△
	上記は、取引の事前もしくは同時に実施すること(UG 185)	(〇)	(〇)	〇	(〇)	×	〇	〇
	上記情報を受信側暗号資産交換業者もしくは金融機関（存在する場合）に直ちに、かつ安全に送信すること(UG Annex 9(b)	(〇)	(〇)	〇	(〇)	×	△	△
	関連記録を保存すること(INR13)	(〇)	(〇)	〇	(〇)	×	〇	〇
	これらが準拠できない場合は送金を認めないこと(INR16-14)	(〇)	(〇)	〇	(〇)	×	△	△
受信側 VASP	送金人、受取人それぞれについて必要な情報が欠落している取引を特定すること（リアルタイムもしくは事後のいずれか適宜に）(INR16-19)	(〇)	(〇)	〇	(〇)	×	△	△
	取引を受け付ける前に受取人の本人性を検証し、記録を保存すること(INR16-20)	(〇)	(〇)	〇	(〇)	×	△	△
	必要情報が欠落している取引について、いつ執行、拒否、差し止めし、どのようにフォローアップするかについてリスクベースでの方針・手続を有すること(INR16-21)	(〇)	(〇)	〇	(〇)	×	〇	△

凡例　〇　FATF 要件準拠
(〇)　法案は策定され、制定・施行を待つ状況にあり、施行された場合 FATF 要件準拠
△　FATF 要件を十分満たしていない要素がある
×　法案も策定されておらず未施行で FATF 要件を満たしていない

6.3 改善・制裁措置

改善・制裁措置に関連付けられるべきリスクは以下の通りである。

[149] What's New (https://www.kofiu.go.kr/eng/notification/notice_view.do)

リスクの分類		リスクの説明
暗号資産そのものに内在するリスク		新たな新商品・サービス、ビジネスモデルが登場することで、それまでの暗号資産の定義にはまらない、ないしはその定義をあいまいにさせるような要素が発生するリスク
暗号資産交換業者に関するリスク	暗号資産交換業者のリスク	特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できないリスク
ネットワーク連携に関するリスク		パブリックブロックチェーン、事業者毎の取引所等、ネットワーク全体に関する情報・知見が分断されているために全体像が把握できないリスク
P2P 取引に関するリスク		P2P の取引、サービスの多くが、秘匿性を高める技術を伴ったり、機会をもたらしたりすることで、暗号資産交換業者が関与していたら可能なはずの真の受益者の特定を困難にするリスク
法域に関するリスク		規制が異なる、もしくは脆弱な国から提供されるサービスを一国のユーザーが利用することで、自国の法規制の実効性に問題が生じるリスク

このリスクに対して、規制・監督当局は、暗号資産交換業者や無登録・無許可の事業者に対する厳格な措置をとることが求められる。

暗号資産交換業者に対しては、オン・オフ双方でのモニタリング（「6.4 モニタリング」を参照）等を通じて検出されたリスクや脆弱性に対して、適切にフォローアップし、事業者の改善措置が堅確であり、再発がないかどうかを評価する必要がある。規制不遵守に対しては、警告、勧告、命令、合意、行政措置、罰則、課徴金、免許の制限、一次停止、取消等、不遵守の度合いに応じた様々な手段が用意され、適用されることが期待される。また事業者だけではなくその経営陣に対しても適宜の処分が求められる。

暗号資産交換業者に対する直近での処分事例は以下の通りである。

- 2022 年 9 月 28 日、フランスの金融当局 AMF が、検査を通じて検出された AML/CFT 上の不備を理由に、デジタルアセットサービスプロバイダーである BYKEP SAS の事業者登録を取り消したと公表[150]
- 2022 年 10 月 11 日、米国の財務省が仮想通貨交換所の Bittrex に対して、経済制裁コンプライアンスにおいて、AML および疑わしい取引の届出上の違反があったとして OFAC への 24 百万ドル、FinCEN への 29 百万ドルの和解金支払を公表[151]

無登録・無許可の事業者に対しては、当局が、これを特定し、適宜に対応することが求められる。直近の事例は以下の通りである。

- 2022 年 8 月 8 日、米国の OFAC は、仮想通貨ミキサー事業者である Tornade Cash が、2019 年の設立以来、ラザルスグループによって盗まれた 455 百万ドルも含め、合計 70 億ドルにのぼるマネー・ローンダリングに利用されたとして、同社を制裁リストに加えたと公表[152]

[150] L'AMF et l'ACPR annoncent la radiation du PSAN BYKEP SAS https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lamf-et-lacpr-annoncent-la-radiation-du-psan-bykep-sas

[151] Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc. https://home.treasury.gov/news/press-releases/jy1006

[152] U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (https://home.treasury.gov/news/press-releases/jy0916)

- 2022 年 8 月 12 日、オランダの AML 当局である FIOD は、Tornado Cash における犯罪収益隠蔽およびマネー・ローンダリングほう助に関与した容疑で 29 才の男性を逮捕したと公表[153]
- 2022 年 8 月 18 日、韓国の AML 当局である KoFIU は、同国の規制上求められる登録義務違反であるとして、海外暗号資産サービスプロバイダ 16 社の社名を無登録事業者として公表[154]
- 2022 年 11 月 25 日、イギリスの金融当局 FCA が、無許可事業者として Crypto Renewed の社名等を公表し、注意を喚起[155]

なお、オランダの逮捕事案については、容疑者はプライバシー保護の手段としてコードを書いただけで、犯罪者がこのオープンソースコードを悪用したのであり、逮捕は行き過ぎではないかとの憶測報道もなされている。暗号資産、暗号資産交換事業者の範囲が、テクノロジーの進展とともに拡大、ないしはあいまいになる性質を有していることに伴う難しさの一端を示しているとも言える。

暗号資産に関するエコシステムの動向を適時適切に把握するためには、様々な情報を収集し、分析することが求められ、これについては、「6.6 リスク評価・調査分析」において考察する。

6.4 モニタリング

モニタリング（オン・オフ）に関連付けられるべきリスクは以下の通りである。

リスクの分類		リスクの説明
暗号資産交換業者に関するリスク	暗号資産交換業者のリスク	特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できないリスク

このリスクに対して、規制・監督当局は、オン、オフ双方での事業者に対する効果的なモニタリングを実施する必要がある。FATF 勧告に基づいた暗号資産交換業者が遵守すべき以下の AML/CFT 要件がモニタリングの主な対象となる。

項目	FATF 勧告	暗号資産固有に考慮すべき点
CDD	R10	・ 一見取引（ATM サービスや P2P 取引） ・ EDD（暗号資産交換業者への規制が脆弱、欠落している法域、P2P 取引、秘匿性を高める技術要素、サービス）
記録の保存	R11	・ ブロックチェーン等の分散記帳固有の情報（ウォレットアドレス、ユーザーコード等）
PEPs	R12	–
コルレスバンキング	R13	・ 暗号資産交換業者への規制が脆弱、欠落している法域
資金移動サービス	R14	・ 資金移動業者との連携
ニューテクノロジー	R15	・ 新商品、ビジネス、デリバリーメカニズムの開発（AEC、ミキサー、プライバシーウォレット等の秘匿性を高める技術
電子送金	R16	・ トラベルルール（送金人・受取人情報の通知義務、経済制裁スクリーニング、相手方 VASP の DD）
疑わしい取引とティッピングオフ	R20, 21	・ デジタル特有の識別子（デバイス ID、IP アドレス、タイムスタンプ、ウォレットアドレス、取引ハッシュ値等）

[153] Arrest of suspected developer of Tornado Cash (https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/)
[154] KoFIU Cautions Virtual Asset Users against Unregistered Virtual Asset Service Providers (https://www.fsc.go.kr/eng/pr010101/78319)
[155] FCA Crypto Renewed (https://www.fca.org.uk/news/warnings/crypto-renewed)

次々と開発される商品、サービス、新規参入・撤退の激しい業界という特徴を有する業態を対象とするということは、規制・監督当局としてのモニタリングも、以下のようにダイナミックに対応する必要があるということを意味している。

- オンサイト・モニタリング、オフサイト・モニタリング間の関係の動的な見直し（リスクの高い状況が出来すればオンサイトを重視する、前回オンサイトでリスク低と認められた先はオフサイト中心とする等）
- オンサイト・モニタリングの頻度の見直し（リスク事象に応じた定期モニタリングと臨時モニタリングの適宜の切替、許可数、顧客数、取引量等の情報を活用した頻度の動的な調整等）
- モニタリング深度の見直し（リスクに応じた徴求情報やモニタリングスコープ、手法 – サンプリング基準、ヒアリング対象等 – の調整等）

より効果的かつ効率的なモニタリングを実現するためには、暗号資産交換業者自身が実施しているリスク評価の活用等も含めて、当局としてのリスク評価・調査分析の強化やテクノロジーを活用したデータドリブンアプローチの適用も必要であり、これについては、それぞれ「6.6 リスク評価・調査分析」、「6.8 分析手法」にて整理する。

また、モニタリングを通じて得られた情報については、適宜、暗号資産交換業者のリスクベースアプローチの品質高度化のために、暗号資産交換業者とのコミュニケーションに活用すべきである。これについては、「6.5 コミュニケーション」にて整理する。

6.5 コミュニケーション

コミュニケーション（アウトリーチ・官民連携）に関連付けられるべきリスクは以下の通りである。

リスクの分類		リスクの説明
暗号資産そのものに内在するリスク		新たな新商品・サービス、ビジネスモデルが登場することで、それまでの暗号資産の定義にはまらない、ないしはその定義をあいまいにさせるような要素が発生するリスク
暗号資産交換業者に関するリスク	暗号資産交換業者の定義のリスク	新たな新商品・サービス、ビジネスモデルが登場する中で、何らかの形で関与している事業者を、適切に暗号資産交換業者として特定できないリスク
	暗号資産交換業者のリスク	特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できないリスク
ネットワーク連携に関するリスク		パブリックブロックチェーン、事業者毎の取引所等、ネットワーク全体に関する情報・知見が分断されているために全体像が把握できないリスク
P2P 取引に関するリスク		P2P の取引、サービスの多くが、秘匿性を高める技術を伴ったり、機会をもたらしたりすることで、暗号資産交換業者が関与していたら可能なはずの真の受益者の特定を困難にするリスク
法域に関するリスク		規制が異なる、もしくは脆弱な法域から提供されるサービスを一国のユーザーが利用することで、自国の法規制の実効性に問題が生じるリスク

このリスクに対して、規制・監督当局は、アウトリーチ・官民連携、および国際協力それぞれの促進が必要である。

6.5.1 アウトリーチ・官民連携

規制・監督当局は、アウトリーチ・官民連携として、当局が期待する要件の暗号資産交換業者への徹底と、民間とのリスク・コミュニケーション促進を行う必要がある。

監督当局は、リスク評価や、モニタリングを通じて得た情報、気づきについて、守秘義務を遵守したうえで、暗号資産関連の民間セクターに対したコミュニケーションを通して、情報発信を行うことが期待される。個別のモニタリングを通じて知り得た発見事項、見解、さらにはそれを踏まえた事業者が具備すべき AML/CFT コンプライアンスのフレームワークについての当局としての期待を適切に伝えることが重要である。グローバルにもリスクベースアプローチの適用は、官民ともに途上の段階にあると FATF も指摘しており、また、リスクベースアプローチの本質からも、「これさえあれば」といった即効性のある正解としてフレームワークが提示できるものではないため、継続的に、課題と対応について振り返り、その時点での先行事例、実務を共有し、品質向上を図る、継続的な取組としてコミュニケーションを位置付ける必要がある。

共有すべき情報の例は以下の通りである。

- 官民双方のリスク評価内容
- 暗号資産の取組（資金移動、交換所、発行等）毎の、ML/TF の手口、手法
- 疑わしい取引その他の事業者からの報告についての品質や有用性についてのフィードバック
- 暗号資産に関する行動や暗号資産交換業者の取引に関連する疑わしい取引についての指標
- 求められる守秘性を確保した上での、特定の情報
- 経済制裁、資産凍結等に関する情報

このようなコミュニケーション促進のために、自主規制団体の存在とその役割は重要である。ただし、あくまで監督、モニタリングの主体は当局であり、自主規制団体ではない。自主規制団体は、暗号資産交換業者とのコミュニケーション促進、情報共有、アウトリーチに関して、監督当局を補佐することができる。

また、新たな商品、サービス、販売チャネル、技術要素、事業形態が次々と進展する暗号資産関連エコシステムにおいては、暗号資産あるいは暗号資産交換業者というスコープのみに囚われず、そのような新たな展開が影響を及ぼし得る様々な金融業態、事業者、関連当局（あるいは同当局内の部門）との連携も重要である。たとえば銀行、クレジットカード、保険、資金移動等が、暗号資産もしくは分散技術を活用した新たなビジネスに展開する局面を例にとれば、その際に、想定していない規制アービトラージの機会があってはならないし、逆に当局としての判断が情報分断等のために適切でない、ないしは時間がかかる等によって民間の健全な金融サービス発展を阻害するようなことがあってはならない。

顧客や市場に直接対峙し、その結果として様々な変化の予兆をもたらすような情報は、まず民間事業者から入る可能性が高い。この点でも、官民連携は重要であり、グローバルには、この連携をより緊密に、継続的に、かつ組織体系立てて対応するものとして PPP; Public Private Partnership と呼ばれる取組に注目が集まっている。これは定期的な会合というよりは、常設機関に近く、単なる当局が期待する要件の伝達や ML/TF の手口の共有といったことにとどまらず、より具体的な共通課題について実質的な議論や、個別事業者単独では対応することの難しい先進的なテクノロジー適用に向けた調査研究や実証実験の実施等が取り組まれている[156]。

6.5.2 国際協力

規制・監督当局は、国際協力の一環として、規制・監督当局は、グローバルな動向把握に資する各国当局との

[156] PPP の海外事例については、たとえば、国立研究開発法人新エネルギー・産業技術総合開発機構の 2020 年度成果報告書「規制の精緻化に向けたデジタル技術の開発／マネー・ローンダリング対策に係る調査」を参照。

連携が求められる。

各国当局が連携するメリットは以下のように整理できる。

- 登録・許可プロセスや結果を共有することで、自国における暗号資産交換業者の登録・許可、無登録・無許可事業者の特定・対処の有効性、効率性を向上させることができる。
- 暗号資産関連の活動のクロスボーダー性に鑑みて、一国単独での監督・規制には限界があり、各国当局の協力は不可欠である。
- 法域間の AML/CFT 規制の進展度合いの相違による脆弱性、欠落（サンライズ問題）は、金融システムを悪用する勢力にとっては、規制アービトラージの機会となるため、これを排除するために、国際協力を通して、当局間の足並み統一が促進される。
- 多国籍に活動する暗号資産交換業者の包括的な監督に資する。
- 暗号資産交換業者の破綻等のリスク事象における、国際的な市場の混乱の回避に資する。

特にトラベルルールの導入は、緒に就いたばかりであり、国際協力を通じて得た情報を基に、一国の金融システムとして、あるいは同国内の暗号資産交換業者として、適時適切にリスク低減策をとれるような状態となっていることが望ましい。たとえばトラベルルール導入等の規制の進展状況に応じて相手法域、事業者のリスクに応じた CDD の実施や取引条件の設定等が想定される。

なお、サンライズ問題は民間セクターにおける深刻な競争上の懸念をもたらす。すなわち、トラベルルールを徹底する重要性は論を俟たないものの、トラベルルール導入の時期について法域によって疎行性が生じれば、先に導入された法域の事業者は、導入のための先行負担、ルール導入に伴う利用者負担という課題が生じる。規制に無自覚なユーザーが、たとえばルール未導入の海外法域の事業者によって、自国において無登録、無届のまま提供されるサービスを利用することも考えられる。自国の正当な事業者にとっては、収益機会の逸失、規制対応の負担増、一国の金融システムとしても、ルール導入の実効性に疑義が生じるという事態が懸念される。このような規制アービトラージが発生しないように、規制・監督当局は、海外当局のトラベルルール導入のスピード、海外事業者の対応状況を、国際協力を通じて積極的に情報収集し、共有することが求められるほか、アウトリーチ、官民連携を通じて、事業者の負担や制度の実効性を慎重に見極める必要がある。関連して、ユーザーの取引活動状況や、無登録事業者の監視等のモニタリングを通じて、ユーザー・事業者への広報活動、場合によっては厳格な制裁措置等が求められる。いずれにしてもサンライズ問題は、一国の金融システムにおける金融犯罪に対するインテグリティの問題であると同時に、暗号資産に関する、さらに言えば Web3.0 に対する国家戦略の一環でのバランスを考慮した総合的な意思決定と対処が求められる。

6.6 リスク評価・調査分析

リスク評価・調査分析に関連付けられるべきリスクは以下の通りである。

リスクの分類		リスクの説明
暗号資産そのものに内在するリスク		新たな新商品・サービス、ビジネスモデルが登場することで、それまでの暗号資産の定義にはまらない、ないしはその定義をあいまいにさせるような要素が発生するリスク
暗号資産交換業者に関するリスク	暗号資産交換業者の定義のリスク	新たな新商品・サービス、ビジネスモデルが登場する中で、何らかの形で関与している事業者を、適切に暗号資産交換業者として特定できないリスク

リスクの分類		リスクの説明
	暗号資産交換業者のリスク	特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できないリスク
ネットワーク連携に関するリスク		パブリックブロックチェーン、事業者毎の取引所等、ネットワーク全体に関する情報・知見が分断されているために全体像が把握できないリスク
P2P 取引に関するリスク		P2P の取引、サービスの多くが、秘匿性を高める技術を伴ったり、機会をもたらしたりすることで、暗号資産交換業者が関与していたら可能なはずの真の受益者の特定を困難にするリスク
法域に関するリスク		規制が異なる、もしくは脆弱な法域から提供されるサービスを一国のユーザーが利用することで、自国の法規制の実効性に問題が生じるリスク

このリスクに対して、規制・監督当局は、市場動向、技術動向等に関するリスクベースかつフォワード・ルッキングな調査分析を実施することが求められる。ここまで整理してきたように、暗号資産のエコシステムは、暗号資産や関連するサービスが急速に進展し、それを提供する事業者も拡大、もしくは Web3.0 の進展とともに自動化、P2P 化されることに伴って主体者の特定が困難になるという特性に留意する必要がある。これが 5.1.2、5.2.1 で示した暗号資産や暗号資産交換業者の定義のリスクであり、定義の矮小化やあいまい化を排除するために、幅広にエコシステム全体についてのリスク評価、調査分析を実施することが重要である。

FATF の「Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers」[157]は、リスク評価のために考慮すべき情報の例として以下を挙げている。

暗号資産に関する要素

a. 暗号資産移転の件数と総額、発行された暗号資産の価値と価格変動性、暗号資産の時価総額、流通総額、ユーザーの法域数、法域毎のユーザー数、決済における暗号資産毎、法域毎のシェア、クロスボーダー取引に利用される度合い
b. 暗号資産と法定通貨、暗号資産同士の交換に伴う潜在的な ML/TF リスク、暗号資産ベースの取引チャネル・プラットフォーム同士、や法定通貨ベースの取引チャネル・プラットフォーム、デジタルサービス・プラットフォーム間のやりとりの度合い
c. 暗号資産決済チャネル・システムの態様とスコープ（オープンなのかクローズドループなのか、マイクロ・ペイメントなのかガバメントから個人なのか等）
d. (1)暗号資産交換業者とその他の規制対象事業者間、(2)暗号資産交換業者を含む規制対象事業者と非規制事業者間、(3)非規制事業者間（P2P）それぞれにおいて、a に関する不法行為との関連性 （ダークネット市場、ランサムウェア、ハッキング等）
e. 暗号資産資金移転における秘匿性を高める技術の利用（AEC、ミキシングサービス、ウォレットアドレスのクラスタリング、プライバシーウォレット等）および秘匿性を抑制する技術（ブロックチェーン分析ツールを利用したウォレットアドレスのリスク評価等）
f. 取引や行動を不透明にし、暗号資産交換業者の CDD その他の AML/CFT 関連対策の実効性を損なわしめるような Tor、I2P その他の秘匿性を高めるソフトウェアによるインターネットプロトコルの秘匿性の度合い
g. 事業規模、顧客基盤、ステークホルダー、発行者や、各種取組に関する（そのような存在がいれば）中央管理主体のクロスボーダー活動の重要性

暗号資産交換業者に関する要素

[157] Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf)

a. 法域内に存在する暗号資産交換業者、および法域内のユーザーに提供されるサービスの数と種類とそれぞれの取引件数と金額
b. 暗号資産事業者の AML/CFT プログラムの洗練度（暗号資産や暗号資産交換業者の活動をモニタリングする適切な監視ツールの存在の有無、責任者、担当者が暗号資産に関するコンプライアンスについての適切な知識、専門性を有しているか等）
c. 暗号資産交換業者のユーザー基盤の規模と種類（ユーザーやその行動に関するデータに対する暗号資産交換業者のアクセス－当該事業者内に限らず、可能であればプラットフォームをまたぐ統合的なデータ等）
d. 暗号資産交換業者が提供する暗号資産口座の特性と範囲（少額貯蓄、預金口座を持てない層向けの少額決済口座等）
e. 事業者（暗号資産交換事業者に限らず、暗号資産活動や、暗号資産関連商品、サービスを提供するその他の規制対象事業者も含めて）によるリスク低減に向けた措置（取引や口座残高に関する制限等）
f. 暗号資産交換業者が完全非対面（プラットフォームベースでの交換所等）か、対面チャネル（個人ユーザー間取引、ATM 取引等）を含むか
g. 暗号資産交換業者が関与する法域に関する潜在的な ML/TF リスクや経済制裁リスク
h. 暗号資産交換業者がトラベルルールを適用しているか否か、サンライズ問題にどのように効果的に対処しているか
i. 非規制事業者（規制対象事業者が関与しないアンホステッド・ウォレット、関連規制が存在しない法域の暗号資産交換業者等）との取引や導入間もない P2P 取引に関する取引に関して収集される情報が、プライバシー保護関連規制と整合的か
j. 暗号資産交換業者の CDD その他の AML/CFT 措置を阻害し得る AEC、ミキシング内在機能等の特定の種類の暗号資産、あるいは暗号資産にユニークな機能を提供している、もしくは提供しようとしているか
k. 暗号資産交換業者が、取引執行に利用可能なスマートコントラクトとの連携もしくは当該スマートコントラクトの経営に関与しているか

このように考慮すべき情報は多岐にわたり、対象とする暗号資産のエコシステムもダイナミックに変化していることから、規制・監督当局が実施するリスク評価は重要であるとともに困難を伴う。下記に検討すべき主なポイントを例示し、それぞれ整理[158]を行う。

6.6.1 事業者のリスク評価の活用

事業者自身にも ML/TF に関するリスク評価を実施することが求められるが、異なる事業者間であっても、同様の商品、サービスは整合的なリスク評価となっているべきことが期待される。さらには、各事業者のリスク評価書の総体が、国としてのリスク評価の相当部分に該当する要素として、有効に活用されなくてはならない。事業者のリスク評価はあくまで、それぞれの事業者の事業戦略やリスク特性に応じて自律的に作成されるべきである一方、リスク評価のための必要な要素や各種計数は共通するものも少なからず含まれる。特に当局は、多くの事業者のリスク評価書を入手できる立場にあるが、個々の事業者のモニタリングのみに活用するのではなく、これを網羅的に精査し、事業者全体のベンチマーク化を図って、特徴あるサブグループを特定したり、個々の事業者の相対的な位置関係を俯瞰したり、さらにはセクター総体としてのリスク評価に統合したりすること等も期待される。ただし、数多

158 以下の整理は、FATF の Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers をベースとしたものである。

くのリスク評価書を人の目で手分けして確認し、複数の担当がそれぞれの目で見た結果を横断的、かつ整合的に統合することは困難も伴う。これについては、「6.8 分析手法」で述べる。

6.6.2 無登録・無許可事業者の特定

「0 改善・制裁措置」で述べた通り、無登録・無許可事業者を特定することもリスク評価・調査分析の一環として対応することが期待される。そのためには、様々なツールやリソースの導入の検討や情報の活用が求められる。たとえば、

a. ブロックチェーン等の分散台帳の分析ツール
b. 無登録・無許可の事業者による広告、販促を特定するためのウェブ・スクレーピングやその他のオープンソース情報の活用
c. コミュニケーション（アウトリーチ、官民連携）を通した、暗号資産コミュニティでの動向に関する情報
d. FIU その他の捜査関連情報
e. 許可申請、取消等を通して得られた非公開情報
f. 国際協力の過程で海外当局から得られた捜査関係その他の情報

等が想定される。

6.6.3 主体者の特定

「5.4 P2P 取引に関するリスク」に示したように、DeFi 等の P2P 取引について、暗号資産交換業者と特定し得る主体者を見極めることは重要だが困難を伴う。何らかの主体者の存在を特定するためには、注目すべき DeFi 等の取組が登場する都度、それぞれの状況に応じて、その構造、リスク特性を調査分析しなければならない。そのためにも、コミュニケーションの一環として DeFi コミュニティとの円滑なチャネルを確立・維持し、以下のような活動を行うことは重要である。

a. 暗号資産交換業者、P2P コミュニティの代表者等の民間セクターへのアウトリーチ
b. 当局内の人材に対する研修
c. プログラマーや開発者の協力を得つつ、P2P マーケット関連指標収集、リスク低減に資するブロックチェーン分析ツール、あるいは疑わしい行動やアンホステッド・ウォレットを特定するリスク手法等の開発を促進すること

このようにして主体者（もしくは主体者が存在しないこと）の特定ができた後に、そのリスク低減のために、以下の措置をとることが必要である。

a. 該当する P2P の活動に関する可視化
b. 特定のアンホステッド・ウォレットに関する暗号資産領域で活動する暗号資産交換業者やその他の事業者への集中的な監督
c. 暗号資産交換事業者に対し、同様に監督を受けている暗号資産交換業者またはその他の規制対象事業者とのみの取引を許容することの義務付け
d. 暗号資産交換事業者に対し、取引許容可能なアドレス等とのみ取引を許容することの義務付け
e. 非規制事業者との取引を許容するための追加的な AML/CFT 要件の提示（EDD やより厳格な記録の保存等）
f. 暗号資産交換業者が P2P 取引を行う顧客に対してリスクベースアプローチをとることの重要性を強調する

ガイダンスの提示

g. P2P 取引に関するリスクに対する意識醸成のための具体的な事例を含むガイダンス公表

関連して、「5.1.2.1 ステーブルコイン」で触れた通り、P2P 取引において広範適用されるような商品、サービスの登場の可能性については、継続的、かつフォワードルッキングに分析を行う必要がある。暗号資産のエコシステムの特性上、新技術をフォローし、リスクを把握することも重要である。暗号資産の決済、移転、発行、あるいは関連するテクノロジー革新等に対して常に目配りをしていくことが求められる。

このようにリスクベースの監督を実践する上で、リスク評価はその根幹となる要素であり、かつカバーすべき領域は広く、対象自体も常に変化し続ける。直近でも、海外の大手暗号資産交換業者の破綻が、市場に与える影響についてのリスク評価とその対処は喫緊の課題と考えられる。個社としての経営管理の問題に加えて、本邦法人のリングフェンスの問題、暗号資産エコシステムからの資金逃避に関連するリスク、その中で影響を受けるセクター（たとえば規制が脆弱、ないしは欠落している法域の事業者等）等、機動的な対応に資する情報の収集、分析は死活的に重要である。

6.7 インフラ

インフラ（テクノロジー・人材）に関連付けられるべきリスクは以下の通りである。

リスクの分類		リスクの説明
暗号資産そのものに内在するリスク		新たな新商品・サービス、ビジネスモデルが登場することで、それまでの暗号資産の定義にはまらない、ないしはその定義をあいまいにさせるような要素が発生するリスク
暗号資産交換業者に関するリスク	暗号資産交換業者の定義のリスク	新たな新商品・サービス、ビジネスモデルが登場する中で、何らかの形で関与している事業者を、適切に暗号資産交換業者として特定できないリスク
	暗号資産交換業者のリスク	特定された暗号資産交換業者が求められる AML/CFT 上の義務を適切に履行できないリスク
ネットワーク連携に関するリスク		パブリックブロックチェーン、事業者毎の取引所等、ネットワーク全体に関する情報・知見が分断されているために全体像が把握できないリスク
P2P 取引に関するリスク		P2P の取引、サービスの多くが、秘匿性を高める技術を伴ったり、機会をもたらしたりすることで、暗号資産交換業者が関与していたら可能なはずの真の受益者の特定を困難にするリスク
法域に関するリスク		規制が異なる、もしくは脆弱な法域から提供されるサービスを一国のユーザーが利用することで、自国の法規制の実効性に問題が生じるリスク

このリスクに対して、規制・監督当局は、各種施策を推進するために必要な人材、テクノロジー、外部専門家の活用が求められる[159]。

6.7.1 人材育成

当局は、幅広い暗号資産交換業者や、関連する暗号資産サービス、ビジネスを規制・監督するために必要な実務スキルと専門性を維持、向上させるための人材確保・育成に投資する必要がある。

特に、暗号資産交換業者のリスク評価の品質を評価し、その AML/CFT 方針、手続、および内部統制がリスク

[159] 以下の整理は、FATF の Guidance for a Risk-Based Approach Supervisors (https://www.fatf-gafi.org/media/fatf/documents/Risk-Based-Approach-Supervisors.pdf)をベースとしたものである。

評価を踏まえて適切、整合的、有効かつ効率的であることを見極めることができるように研修を受けることが求められる。最新テクノロジー、たとえばブロックチェーンやアナリティクス等についての知識習得も必要である。当局としてのリスク評価やモニタリングにおいては大量のデータに基づく分析や、定量的な仮説検証が求められるデータドリブンアプローチが適用される傾向にあり、この点でも、統計分析、データサイエンスに関する専門家を擁する必要がある。また Web3.0 での世界観に共鳴する暗号資産コミュニティ固有のカルチャー[160]をよく理解し、コミュニティ構成員とも信頼感をもってコミュニケーションがとれる人材の育成・投入も一層求められる。公式な会合、オフィス訪問ではなく、オンラインチャット、SNS での交流やカジュアルなミートアップでのつながりが重要視され、そこで交わされる口コミ情報が貴重なインテリジェンスとなることも多く、アミーゴベースで気軽に情報共有ができるネットワークの一員である必要がある。

6.7.2 テクノロジー

当局には事業者からの徴求情報をはじめとした多種多様、かつ大量の情報が蓄積されている。ただし、データの偏在、散在やデータ品質、活用上の課題があり、必ずしも有効活用されていると言える状況ではない。

一方でこれらの課題に対しては、データの収集、保管、分析、変換のための、いわゆる DX 関連ツールが活用可能な時代となっている。これらのツールを活用することで、当局として、既存のデータの活用、これまで有効に扱えていなかった外部データの取り込みとその分析が可能となり、リスク評価の高度化や、監督プロセスの効率化に資することが期待される。このような取組は SupTech と呼ばれる。

今後活用に値すると思われる分析手法等については、「6.8 分析手法」にて整理する。

6.7.3 外部専門家

規制・監督対象のビジネスにおける商品・サービスや販売チャネルの多様化、対象事業者の規模や複雑性の多様化、あるいは社会一般の DX 化の進展に伴い、規制・監督の効果的・効率的な活動を促進、維持するためには、内外のリソースを有効に活用することが求められる。外部委託によって、本来当局が担うべき規制・監督の責任を委託先に担わせることはできないが、適切なリソースの活用により、本来当局がコアとすべき活動に、内部リソースをより集中的に投下し、委託可能な部分（たとえば低リスク領域に関する業務）や、委託することが必要な領域（緊急性や専門性が高く、当局として恒常的にそのスキルを保有し続けたり、適時に内部調達したりすることが困難な業務[161]）等については、適宜外部リソースを活用するといった取組が必要である。

当局としての本来の独立性や、内部的に保持すべき専門性、能力を確保しつつ、効果的に外部リソースとのバランスを決定することが重要である。特に FinTech に代表されるように、金融商品、サービス、ビジネスモデルや IT 能力に関するイノベーションが進展し、民間セクターの洗練度が向上している状況において、IT 専門家、データサイエンティスト、その他の専門家を効果的に活用することが求められている。暗号資産のエコシステムに関しては、とりわけこの傾向が顕著である。

---

[160] たとえば、既存の権威的な勢力の存在、あるいは中央集権的な機構による個人情報の過度の管理に対しては批判的であり、個人的な自由や、それに伴う行動に関連する情報を、中央集権的な人的組織に預けて、他人の管理・監視にさらされるのではなく、自由な取引機会の創出や、個人情報の管理を分散テクノロジーやアルゴリズムによって実現させ、現状を改革して自己主権を確保しようとする世界観を有する傾向がある。

[161] たとえば本報告のその 2「当局マネロン検査のフォローアップを外部適格コンサルタントに委託する手法（英）の事例研究」を参照。

たとえば、民間セクターにおける分散記帳技術、AI 等の情報処理、分析手法、情報保管テクノロジーの急速な変化と革新は、AML/CFT に適用された当該テクノロジーの監督・監視の重要性を高めている。エンタープライズレベルでの IT システム構成、モニタリングシステム、あるいはそれらに適用されるパラメータや、外部ベンダーソリューションの理解なしには、有効なモニタリングは実現できない。

当局は、専門性を有する外部専門家の活用についての柔軟性を確保すべきである。外部専門家の活用においての留意点は以下の通りである。

- 委託候補選定の評価プロセス（競争力、実績、経験、利益相反等）
- データ保護
- 外部専門家が効果的、効率的かつ独立に求められた業務を担うために必要なコントロールの整備
- 課題が認められた場合のコミュニケーション手段の確立
- 成果物の品質に対する監督とモニタリング
- 機密情報へのアクセス許諾と管理

6.8 分析手法

本セクションでは、ここまで整理してきた暗号資産のリスクに対して、規制・監督当局が適切に対処するために役立つと考えられるリスク分析やモニタリング分析手法について整理する。

6.8.1 市場動向調査

6.8.1.1 ウェブ・スクレーピング／クローリング

「6.6 リスク評価・調査分析」で記載したように、当局として暗号資産や暗号資産交換業者の動向把握を含めたリスク評価を行うためには、多岐にわたる情報が必要である。一方で、ウェブ上には多種多様な情報が氾濫しており、これを取捨選択して効果的・効率的に活用することは容易ではない。

ウェブ上で公開される情報としては、幅広に暗号資産に関する市場情報を提供するもの[162]、各国の商品、サービス、事業者や規制動向をニュース形式で提供するもの[163]、その他、暗号資産取引の始め方や取引のヒント、あるいは、暗号資産、暗号資産交換業者の人気ランキングを掲載するもの等がある。これらは主に無料のオープンソース情報であるが、中にはプロの投資家向けに有料で分析ツールを提供するようなものもある[164]。また後述す

[162] たとえば、仮想通貨　市場情報、あるいは crypto asset market cap 等で検索すると、仮想通貨価格、チャート、時価総額 | CoinMarketCap、みんかぶ 暗号資産（みんなの仮想通貨）| 暗号資産の総合サイト (minkabu.jp)、Japan: most traded cryptocurrencies by spot trading volume 2022 | Statista、AssetMarketCap.org、All Crypto Prices and Market Cap on One Page — TradingView、Dune、CryptoQuant | Bitcoin: Summary, on-chain data analytics, ...等のウェブサイトがヒットする。あるいは DeFi に特化した DefiLlama - DeFi Dashboard 等も存在する。（アドホックに検索したものであり、それぞれのサイトの安全性、中立性、信頼性等を確認したり、推奨したりするものではない。以下、本セクションで例示するウェブサイト、ソリューション、サービスプロバイダ等も同様である。）

[163] 上記同様、関連キーサードで検索すると、CoinPost｜仮想通貨ビットコインニュース・投資情報、CoinPartner(コインパートナー) | あなたに寄り添う、暗号資産のパートナー (coinotaku.com)、仮想通貨・ビットコイン・メタバースのニュースサイト｜コインテレグラフ ジャパン (cointelegraph.com)、Crypto News: Latest Cryptocurrency News, Bitcoin News, Ethereum News and Price Data、crypto.news: Cryptocurrency News Today & Live Price Indexes、World news about cryptocurrency and blockchain technology from different sources (cryptonews.net)、CoinDesk: Bitcoin, Ethereum, Crypto News and Price Data 等のウェブサイトがヒットする。

[164] たとえば Nansen - Crypto, DeFi & NFT Analytics (https://www.nansen.ai/)

るネットワーク分析ツールプロバイダが公表する各種レポートや開催ウェビナーも有用である。

こういった情報に加えて、たとえばリスクの高い技術要素、暗号資産、無登録の事業者、さらには海外当局動向についても継続的にモニタリングする必要があることから、相応にリソースを配分して対応しなければいけないのは明らかである。FATF も複数の当局同士の連携は重要であると述べており、たとえば JAFIC や捜査機関との恒常的な連携の場の設定等についても検討の余地があると思われる。

さらにこのようなオープンソース情報のリサーチ、分析に資する技術要素として、FATF でも言及されているウェブ・スクレーピングやウェブ・クローリングが考えられる。スクレーピングは、特定のウェブページからテキストもしくは数値情報を切り出す技術であり、クローリングとは特定のウェブページではなく、一定の基準の下にウェブ上を巡回し基準に該当する URL をランダムに取得する技術である。いずれのツールも、ソリューションとしては既に市場に多く出回っており、最適な検索や情報収集・蓄積を行えるようにするための要件定義やパラメータ設定等の知見を、外部専門家を活用しながら蓄積しつつ、導入、運用する必要がある。

6.8.1.2　ネットワーク分析ツール

ネットワーク分析ツールは、既に「5.1.1 記帳方法に関するリスク」で整理した通り、暗号資産に関しては最も注目を集めている技術要素である。「5.3 ネットワーク連携に関するリスク」で記載した通り、銀行をまたぐ送金ネットワークでは実現が困難と考えられている取引ネットワーク全体の監視ができるというパブリックブロックチェーンが有する利点を活かして、たとえば以下のような局面に利用することができる。

- 一回の取引によって移転された暗号資産が、その後どのように転々流通していくかを把握する。
- 調査対象の取引が、金融犯罪のリスクにどれだけさらされているかを評価する。
- 活発な取引を示すノード主体の特性や素性を把握する。（たとえば暗号資産交換業者の評価、ミキサー的特質の抽出、ダークネットへのアクセスの有無）

留意しなければならないのは、相応の成果が得られているのは事実としても、上記に資する分析は、あくまで取引パターンといったブロックチェーン上の特徴量であったり、IP アドレスといったインターネット上のいわゆるデジタルフットプリント情報を利用したりすることによって得られる統計的な推定であるということである。「5.1.1.3UTXO モデルとアカウントモデルの ML/TF リスク比較」で記載した FATF の調査「Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers」でも、参考とした 7 社[165]の分析結果にはかなりの乖離があることが示されている。

推定は各社のノウハウであり、それぞれ様々なソリューションを提供している。代表的なソリューションは以下のようなものである。

- 特定のアドレス、ノードについてのリスクスコアを付与するもの（さらに踏み込んで white list や black list を提供するものも含む）
- 事業者の取引全体をモニタリングし、異常取引を検出するもの
- ネットワークで観測される脅威情報を提供するもの
- 調査対象の取引について、関連するネットワークを表示する等の分析環境を提示するもの

[165] ウェブ上で検索すると、この 7 社以外に、たとえば、AnChain.AI | The Guardians of Web3 Digital Assets、Uppsala Security | Home、Solidus Labs: The Crypto Market Integrity Platform といったツールがヒットする。

・　上記のサービスに加えて専門家による分析調査サービスを提供するもの

プロバイダーによってカバーする暗号資産の数は異なり、利用者はその目的に応じてプロバイダーやソリューションを選択する必要がある。従来の伝統的な預金取引では入手が難しかったネットワーク上の情報を得られる利点はあるが、「5.3 ネットワーク連携に関するリスク」でも述べた通り、この利点を最大限活かすためには、事業者であれ、当局であれ、自身が有する固有の情報・知見と、ソリューションが提供する情報とを総合的に勘案して取り組む必要がある。また、利用者同士の情報共有（このような利用者同士の情報連携を積極的に推進するプロバイダーが多い）も求められる。

このような観点で、これまでの、

・　法執行機関は届け出られた疑わしい取引の情報を所与とした捜査に注力する

・　金融規制当局は AML/CFT 規制の厳格化に注力する

・　金融機関等は自身のコンプライアンス強化に注力する

という、関係者が別々に AML/CFT に取り組むスタイルでは、ますます深刻化するマネロン・テロ資金供与等の金融犯罪を十分抑止できないとの共通認識がグローバルに高まっており、「6.5.1 アウトリーチ・官民連携」で述べた PPP の取組は極めて重要である。

6.8.2　規制対象となる暗号資産交換業者のリスク分析

前セクションは、主に外部から取得可能な情報について見てきたが、このセクションでは、規制・監督当局が保有する情報をどのように活用するのかについて考察する。

当局には、対象事業者からのオン・オフ双方のモニタリングを通じて、膨大な情報が蓄積されている。ただし、これらのデータの事業者とのやりとりはメールや表計算ソフトファイル等の手作業に頼っており、その分析も、担当者毎の知見に依拠する等、まだまだ活用の余地があると考えられる。

処理の自動化、取り扱うべきデータの品質確保や構造化、その処理の高度化として、RPA、クラウド、ネットワーク分析テクニック、BI、自然言語処理、AI 等を活用することによって、規制・監督として本来求められる判断業務に、より集中したり、当該判断を支援する情報を活用したりすることができる。たとえば暗号資産エコシステムにおけるリスクの傾向をいち早く特定する、事業者の特性を把握してグルーピングやベンチマークに基づいて相対評価（リスクレーティング等）をする、統合的に利用可能な構造化されたデータベースを活用しオン・オフのモニタリングに活用する、といったことが期待される。

対象を、データ、処理、操作の三領域に区分し、それぞれの現状（一般的に見られる傾向）、SupTech の方向性（上記テクノロジーを活用した適用領域）、暗号資産領域での例（暗号資産固有の特性を踏まえて想定される活用の例）を整理すると以下の通りとなる。

領域	現状	SupTech の方向性	暗号資産領域での例
データ	・内部データは、事業者ごとの情報、目的別の徴求資料が散在しがちな傾向 ・外部データはアドホックに収集	・内部データを横断的、整合的に構造化したデータベースの構築 ・データベース構築の前提としてのデータモデリング ・外部データのより広範な活用[166]と、内部データとの統合	・暗号資産交換業者の徴求データの整合的・統合的なレポジトリーの構築
処理	・メールベース、表計算ソフト（あるいは個々のファイル）ベース	・事業者とのやりとりをウェブベースとし、データ徴求のプラットフォームを提供することで、オペリスク軽減、徴求データ品質向上、ひいては事業者の対応負担軽減を図る	・報告徴求プラットフォームの構築 ・上記レポジトリーを踏まえた高度な分析ツールの導入
操作	・個別処理毎に人手で集計、分析 ・リスク評価書等の非構造データは各人の目視による査閲	・上記データベースを活用した分析ツール（BI、テキストマイニング、AI）の導入 ・上記に基づく、定量的なリスク評価モデル、非構造データのクラスタリング[167]により事業者の対応状況をベンチマーキング化	・リスク評価書の横断的な事業者評価や共通課題の抽出

なお、このような SupTech の取組は、業界団体、事業者との対話促進にも寄与する。たとえば上の表では報告徴求プラットフォームと例示したが、報告徴求に限らず、当局が関心を持っている特定領域についての分析結果や考察についてのフィードバックや、事業者が特定したリスク（事業者内に限らず市場で観測される様々な事象を含む）や課題の共有といった双方向でのコミュニケーションの場として活用することも考えられる。

6.8.3 トラベルルールについて

トラベルルールは暗号資産交換業者に求められる AML/CFT 要件であるが、その導入は、サンライズ問題や、必要とするソリューションの提供スコープ等、様々な制約がある等、個々の民間事業者だけで取り組むには課題が多いと思われるため、以下にソリューションの現状を整理し、トラベルルールの円滑、かつ有効な適用に資するためのポイントについて整理したい。

まずトラベルルール適用に向けては、複数の団体、機関がデータ交換のための規格を提唱[168]している。

これらは、暗号資産交換業者による業界ベースでのアライアンス、ベンダーや大手暗号資産交換事業者主導のネットワーク、ベンダーによる商業ベースでのソリューション等、様々な特徴、性質を有している。たとえば、複数の規格に対応したソリューションを複数提供しているベンダーも存在する。

これらの乱立する規格、ソリューションについて、暗号資産交換業者がどのような選択をとるのか、その選択が当該

166 たとえば、外部情報に対するウェブ・クローリングの活用による市場動向（新商品、新技術、ユーザー行動、無登録・無許可事業者等）の把握や、ネットワーク分析ツールの活用による P2P 動向の把握といったことが想定される。（「6.8.1 市場動向調査」を参照）

167 従来は担当者毎に精査していたために実現が難しかったものであるが、たとえば、事業者ごとの膨大なリスク評価書（非構造データ）を、テキストマイニング手法を活用して、類型化、相対評価、スコアリングし、業界横断的なベンチマーキングや時系列分析を定量的、かつ客観的に行うことが期待される。

168 ウェブ上でサーチしただけでも、OpenVASP（https://openvasp.org/）、Shyft（https://www.shyft.network/）、Sygna Protocol（https://www.sygna.io/jp/）、TransactID（https://www.netki.com/transactid）、TRISA（https://www.trisa.io/）、TRP（https://www.travelruleprotocol.org/）、TRUST（https://www.coinbase.com/ja/travelrule）、TR:Now（https://notabene.id/travel-rule-messaging-protocols/tr-now）、VeryfyVASP（https://verifyvasp.com/）等の規格ないしはソリューション（アルファベット順）が存在していることが確認できる。

業者だけではなく金融システム全体として AML/CFT の観点でどのような影響があるのか、そもそも暗号資産交換業者が選択する際の困難性は何か、といった課題が認められる。以下、相互運用性、システミックリスク、暗号資産交換業者のデューデリジェンスの観点毎に整理する。

6.8.3.1 相互運用性

トラベルルールの性質上、交換業者はなるべく広範囲なネットワークをカバーできるような規格ないしはソリューションを選定しようとする。いずれの規格、ソリューションも業界横断での専門家で構成される Joint Working Group[169]で開発、維持されている interVASP Messaging Standard（IVMS 101）に依拠しているが、現状、異なる規格を利用している暗号資産交換業者間のトラベルルールの適用は難しい。

規格間での連携や、異なる規格の間を取り持つソリューションの紹介等の動きもあるが、現時点では、相互運用性がどこまで図られるのかを見据えて、暗号資産交換業者が規格、ソリューションを選択することは極めて困難な状態である。大手事業者の中には、緊急避難的に複数の規格を採用するような動きも一部見られるが、すべての事業者がこのアプローチをとることはコスト的にも現実的ではない。

個々の事業者だけに判断を委ねるのではなく、業界団体、当局、あるいは海外も含めた規格団体やソリューションプロバイダ、海外当局との積極的な連携が期待される。

6.8.3.2 システミックリスク

各規格、ソリューションのサービス形態は様々である。

まず中央集権的なものなのか、分散処理に基づくものなのかの違いがある。中央集権的なものは、ベンダー主導のものが多い傾向にあるが、この場合は、ユーザーである暗号資産交換業者に対するサービスは一貫していて導入しやすいメリットもある一方で、暗号資産の移転に係る膨大な情報（加えて取引主体者の個人情報も含む）を、一企業のサーバー上の処理にどこまで依拠してよいのかという課題が生じる。一方で分散処理に基づくものであれば、純粋に規格のみ、ないしは API プログラムまで提供して、残りのプログラム開発を暗号資産交換業者に委ねるもの等、様々であり、暗号資産交換業者として対応すべき領域を見定めなければならない。これはそれぞれの規格、ソリューションが示す費用体系を理解したうえで、自社で追加負担すべきものもあわせたトータルコストを見極める必要があることを示している。また、分散処理に基づくような規格については、その主体者である団体の主体性、継続性、中立性といったガバナンスについても目配りが必要となる。

何より、これらの規格、ソリューションはまだテスト段階にあるものも含まれるだけでなく、運用が始まったものについても歴史が浅く、市場ストレス時においても問題なく決済ネットワークとして確実に機能し続けるかといったことについては、十分検証されていない。

このようなシステミックリスクを、当局、業界団体、規格団体、ソリューションベンダー、暗号資産交換業者それぞれが、どのように責任分担し得るのかについての議論はまだ十分尽くされていない状況と言える。

上記の要素を十分踏まえたうえで、暗号資産交換業者が自身の判断で適切に規格・ソリューションを選定することは極めて難しい状況にあり、当局、業界団体を交えて議論を尽くす必要がある。

[169] interVASP Messaging (https://intervasp.org/)

6.8.3.3　暗号資産交換業者のデューデリジェンス

これらの規格、ソリューションで対応できることは、暗号資産交換業者として対応すべきトラベルルールのすべてではない。その代表的なものは暗号資産交換業者に対するデューデリジェンスである。

規格、ソリューションによっては、まずネットワークの参加に際して一定の認証を実施するものや、参加希望する暗号資産交換業者に対して一定の審査を行うものもあるが、これは必ずしも、暗号資産交換業者として求められる相手方暗号資産交換業者のデューデリジェンスの全てを網羅するものではない。また、例えこのようなソリューションが全ての機能を網羅していたとしても、個別の暗号資産交換業者が担うべきデューデリジェンスの義務を代替するものではない。

これに関しては、暗号資産交換業者として、オープンソースでの情報検索[170]、ベンダーが提供する暗号資産交換業者データベースサービス、暗号資産交換業者に対するリスク評価サービス[171]を適宜利用する他、相手先暗号資産交換業者への直接のヒアリング等によって対応することが期待されているが、その実施・確認についてはいまだ十分な実務基準が確立されている状況ではない[172]。

当然のことながら、各国当局からも自国での登録・許可事業者名（あるいは無登録・無許可事業者）の名簿が公表されているが、さらに踏み込んで、グローバルな観点で、暗号資産交換業者等が容易にデジタルベースで取得、更新できるような標準的な VASP リストのデータ規格を当局同士の連携によって確立したり、あるいは業界団体がこの公的なリスクに加えて、事業者独自の追加情報等を付加して情報を広く開示したりする等の一層の工夫が期待される。

---

170 たとえば、「6.8.1 市場動向調査」で記載した市場情報提供ウェブサイトでも暗号資産交換業者についての一般的な情報は、どこまで検証できているかどうかは別にして、取得可能である。

171 たとえば、Notabene (https://app.notabene.id/network)、Ciphertrace https://ciphertrace.com/wp-content/uploads/2021/09/CipherTrace-Traveler-DS-20210908.pdf 等。

172 たとえばコルレスバンキングにおいては、CBDDQ、FCCQ（https://www.wolfsberg-principles.com/wolfsbergcb）といった質問状やそれに基づく確認実務が共有され、事実上の実務基準として定着している。暗号資産においても質問状の例（たとえば GDF Virtual Asset Due Diligence Questionnaire (https://www.gdf.io/gdf-virtual-asset-due-diligence-questionnaire/) などが示されつつある状況にある。（本文記載のとおり、このような質問状を利用して、デューデリジェンスの義務を負うのは個別の金融機関であることは論を俟たない。）また、規格によっては、参加要件として、一定の情報開示を求め、参加暗号資産交換業者同士のデューデリジェンスに資する枠組を提供しようとしているところも存在する。

本報告書は、金融庁の委託により有限責任 あずさ監査法人が実施した調査結果を取りまとめたものです。私たちは、調査時点で入手した情報に基づき本報告書を適時に取りまとめるよう努めておりますが、本調査報告書の内容は、本調査の対象に含まれない特定の個人や組織が置かれている状況に対応するものとは限らず、また、情報を受け取った時点およびそれ以降において、その情報の正確性や完全性を保証するものではありません。この調査報告書での KPMG の見解が常に規制当局の見解と一致することは保証できず、また、本調査報告書は法的見解を提供する、または保証意見を表明するものではございません。本報告書は委託者である金融庁に対してのみ提出したものであり、本報告書を閲覧あるいは本報告書のコピーを入手閲覧した第三者の本報告書の利用に対して、有限責任 あずさ監査法人は直接ないしは間接の責任を負うものではありません。

Appendix

Appendix I: 参考文献リスト

本稿（調査項目③の２　暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究）において参考とした文献の出典については、適宜本文中の脚注に示した。この他、執筆全般にあたっての、背景情報の理解等のために参考とした文献を以下に示す。（タイトル五十音順）

「アフター・ビットコイン」 中島真志　新潮社　2017 年 10 月

「アフター・ビットコイン２」 中島真志　新潮社　2020 年 6 月

「暗号技術入門　第 3 版」 結城浩　SB クリエイティブ　2015 年 8 月

「暗号資産における取引の追跡困難性と匿名性：研究動向と課題」 宇根正志　日本銀行金融研究所/金融研究 2019.7

「暗号資産交換所ビジネスの現状とモニタリングの方向性」 曽根康司　金融財政事情　2022 年 5 月

「暗号資産の現状と課題」 廉了　三菱 UFJ リサーチ&コンサルティング　2022 年 5 月

「暗号資産への FSB などの懸念と規制・監督の強化、各国の CBDC への取組み」 佐志田晶夫　日本証券経済研究所　2022 年 9 月

「Ethereum+Solidity 入門 Web3.0 を切り拓くブロックチェーンの思想と技術」Chris Dannen インプレス　2019 年 3 月

「NFT の教科書 ビジネス・ブロックチェーン・法律・会計まで デジタルデータが資産になる未来」 天羽健介　朝日新聞出版　2021 年 10 月

「NFT ビジネス見るだけノート」 増田 雅史　宝島社　2022 年 3 月

「仮想通貨に関する私法上・監督法上の 諸問題の検討」 金融法務研究会　2019 年 3 月

「仮想通貨の教科書」 アーヴィンド・ナラヤナン他　日経 BP　2016 年 12 月

「教養としての決済」 ゴットフリート・レイブラント他　東洋経済新報社　2022 年 8 月

「ステーブルコインと中央銀行デジタル通貨をめぐって」 淵田康之　野村資本市場研究所　2020 年 5 月

「ステーブルコインの検証と代案: FX のポジションを 担保にした「ポートフォリオ通貨」の構想」 リー・サンベック　明治学院大学国際学研究　2019 年 3 月

「世界で検討が進む CBDC の動向と 今後の方向性について」 国際通貨研究所　2021 年 3 月

「徹底理解ブロックチェーン　ゼロから着実にわかる次世代技術の原則」 Daniel Drescher 他　インプレス　2018 年 6 月

「電子的支払手段等の規律の在り方に関する意見書」 日本弁護士連合会　2022 年 3 月

「はじめてのブロックチェーン・アプリケーション Ethereum によるスマートコントラクト開発入門」 渡辺篤他　翔泳

社　2017 年 8 月

「ビットコインとブロックチェーン」 アンドレアス・M・アントノプロス　NTT 出版　2016 年 7 月

「ブロックチェーンを用いた金融取引のプライバシー保護と追跡可能性に関する調査研究」 金融庁　三菱総合研究所 2019 年 3 月

「ブロックチェーン・レボリューション」 クレイトン・クリステンセン他　ダイヤモンド社　2016 年 12 月

「分散型金融システムのトラストチェーンにおける技術リスクに関する研究」 金融庁　株式会社クニエ　2022 年 6 月

「メタバースと Web3」國光 宏尚　エムディエヌコーポレーション　2022 年 3 月

Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations, BGIN SR 001, November 11, 2021

Presentation slides at FATF's Private Sector Consultative Forum on virtual assets, BGIN, April 20, 2021

Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements, Fintech Note, September 2022, IMF

Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, Fintech Note, September 2022, IMF

Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations, Fintech Note, October 2021, IMF

Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2): Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework—Some Legal and Practical Considerations, Fintech Note, October 2021, IMF