KPMG Newsletter

KPMG Insight

Topic ⑤

暗号資産に関するマネロン等のリスク
および対応のポイント

Vol. 67

July 2024

暗号資産に関するマネロン等のリスクおよび対応のポイント

あずさ監査法人
金融統轄事業部　金融アドバイザリー事業部　AML・CFTアドバイザリー部
流 良和／マネジャー

流 良和
Yoshikazu Nagare

マネー・ローンダリングおよびテロ資金供与防止対策（AML/CFT）は、幅広い業態の事業者にとって重要なテーマとなっています。近年では、預金取扱金融機関等における対策が強化されるに従い、犯罪者等が代替手段として暗号資産等の従来にはなかったサービスを悪用し、マネー・ローンダリング等を敢行するケースが見られます。特に暗号資産は、ランサムウェア攻撃による身代金支払い、テロ組織への資金提供、北朝鮮による拡散金融等の手段として悪用されています。また、預金取扱金融機関等においても、顧客または振込相手先等に暗号資産交換業者が存在する場合、間接的にマネー・ローンダリング等の機会を提供する可能性もあります。本稿では、AML/CFTを推進するうえで前提となる暗号資産および関連する技術のリスク、また暗号資産交換業者、預金取扱金融機関等における対応のポイントについて解説します。
なお、本文の内容については、筆者の私見であることをあらかじめお断りいたします。

☑ POINT 1

暗号資産取引は財産的価値の移転に利用可能な性質があること、また匿名性を高めるための技術もあることから、マネー・ローンダリングやテロ資金供与を企図する犯罪者にとって魅力的なサービスとなっている。また、態勢整備不備を起因とした事案では、当局より巨額の制裁金が暗号資産交換業者に課されたケースも認められる。各事業者は対応の前提として、このようなリスクが存在することを理解しておく必要がある。

☑ POINT 2

暗号資産交換業者には、FATFが提唱するトラベルルール等、法規制への対応はもとより、自社のリスク評価を踏まえた態勢整備が求められる。特に、規制外のP2P取引についてリスクが高いとされているため、暗号資産ウォレットの入出庫にあたってのリスクを踏まえた取引モニタリング・制限等を検討することが有用である。

☑ POINT 3

預金取扱金融機関等も、暗号資産のリスクを踏まえた対応が必要である。特に、暗号資産交換業者に振込入金専用口座（バーチャル口座等）を提供する場合は、当該事業者の態勢整備状況の確認をすることが考えられる。このほか、自行顧客の振込相手先が暗号資産交換業者である場合のリスクを踏まえた対応も求められる。

Ⅰ 暗号資産取引に関するリスク・法規制の状況

AML/CFTの重要性が高まるなか、近年は預金取扱金融機関等において対策の強化が実施されてきました。一方で、暗号資産取引は事業者が関わることなく、利用者間で価値の移転をすることも可能であるため、マネー・ローンダリングやテロ資金供与を企図する犯罪者にとっても利便性の高い性質があります。

ここでは、このような性質に起因するリスクのほか、各事業者が準拠する必要のある法規制等について解説いたします。

• 暗号資産の性質

（1）資金決済・保管機能

暗号資産には、資金決済に関する法律（以下、「資金決済法」という）の定義のとおり、財産的価値の移転に利用可能な性質があり、これを売買・交換または保管等する事業者のことを「暗号資産交換業者」と言います（図表1参照）。

また、海外では、暗号資産を購入・売却することが可能なATMが設置されている国・地域もあり、銀行口座を使用せずとも価値の移転が可能な場合もあります。

（2）暗号資産のリスクが高い理由

このような利便性がある一方で、暗号資産には、マネー・ローンダリング等のリスクを高める要因も存在します。

① 匿名性を高める技術

資産の匿名性が高い場合、マネー・ローンダリング等が行われた際に、その追跡が困難となるリスクがあります。

この点について、暗号資産は移転記録がブロックチェーン上で記録・公開されることで、取引の追跡が可能ですが、その追跡を困難とする技術も存在します。国家公安委員会「犯罪収益移転危険度調査書」[1]（以下、「NRA」という）では、当該技術として以下のようなものが挙げられています。

- さまざまな手段を利用して暗号資産の送信アドレスと受信アドレスとのつながりを隠す「ミキサー」、「タンブラー」
- 複数の中間アドレスを経由し、暗号資産を少しずつ連続して新しいアドレスに移転する「ピールチェーン」
- 暗号資産を、記録されているブロックチェーンから、別のブロックチェーンに移動させる「チェーンホッピング」

実際に、北朝鮮とつながりがあるとされるサイバー犯罪グループが、これら技術を使用してマネー・ローンダリングを実施したことが指摘されています（これまでに数十億米ドルの暗号資産を犯罪行為により得たとも言われます）。この他、2023年には、当該グループにミキサーのサービスを提供していたとする事業者に対し、米国財務省外国資産管理室（OFAC）は制裁を課しています。

② P2P取引

暗号資産取引には、暗号資産交換業者を介して行うほか、直接利用者間で取引する方法があります。後者は、Peer to Peer（P2P）取引と言います。P2P取引を可能とする仕組みの一例として、DEXやアンホステッド・ウォレットがあります（図表2参照）。

暗号資産取引交換所は、各種AML/CFT

図表1 資金決済法上の定義

用語	定義
暗号資産	一　物品等を購入し、若しくは借り受け、又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及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、本邦通貨及び外国通貨、通貨建資産並びに電子決済手段（通貨建資産に該当するものを除く。）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
暗号資産交換業者	一　暗号資産の売買又は他の暗号資産との交換 二　前号に掲げる行為の媒介、取次ぎ又は代理 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）

出典：e-gov（資金決済に関する法律）を基にKPMG作成

図表2 P2P取引を可能とする仕組み

仕組み	説明
DEX	• 暗号資産取引を可能とする分散型取引所のことを指す（Decentralized Exchange の略称） • DEX では、P2P による暗号資産取引が可能 • 従来、金融サービスは、第三者（信用のある金融機関等）による管理・仲介がなされていた。DEX では、スマートコントラクト（条件が満たされた際に、自動的にプログラムを作動させる仕組み）により、第三者の関与なしの取引を実現する
アンホステッド・ウォレット	• 暗号資産を保管するウォレット（暗号資産を保管する財布のようなもの）のうち、暗号資産交換業者等がホスト（管理）しておらず、個人が管理しているものを指す • 暗号資産交換業者等がホスト（管理）しているウォレットと同様、暗号資産の保管のほか、個人間の送金等も可能

出所：KPMG作成

に関する法規制の対象となります。一方、図表2に挙げたような仕組みで取引される場合、暗号資産交換業者等による管理がなされていないために、そのような法規制の対象外となります。この場合、違法となる取引がなされていたとしても、誰にも検知されず、取引が実行されてしまう可能性があります。その点にリスクがあります（FATF*の関連ガイダンス2（パラグラフ44）には、実施した調査において、P2P取引は暗号資産交換業者を介した取引に比べて違法な取引の割合が高いことが記載されています）。

この点、暗号資産交換業者にとっても、たとえば犯罪者がアンホステッド・ウォレットに犯罪収益を入庫した後、出庫先を自社がホスト（管理）するウォレットとする等の場合には、間接的に取引に関与してしまうリスクもあります。

* Financial Action Task Force（金融活動作業部会）の略称。マネー・ローンダリング等対策の国際基準策定・履行を担っている。

③ 海外取引

暗号資産は、預金と同様に海外にも移転することが可能です。この点、規制等の対応が遅れている国・地域との取引は、リスクが高くなります。たとえば、トラベルルールの浸透状況に関し、FATFの関連ガイダンス[2]（パラグラフ16〜17）では以下のように述べられています。

- 2023年4月にトラベルルールの立法措置に関する調査を実施。結果、135法域中、トラベルルールに関する法律がすでに可決済であるのは35法域、立法手続き（法案のドラフトを公開、パブコメ募集中である等）に取組み中であるのは27法域であり、不十分な進捗状況
- トラベルルールの有効性は、グローバルでの一貫した取組みに依るため、当該領域の進捗の遅れにつき、深刻に懸念している

また、預金口座の場合には通常、海外の金融機関でも本人確認等がなされますが、暗号資産の場合には実施されないケースもあります。この点、NRAでは以下のようなリスクを述べています。

- 取引に利用されるウォレットが、本人確認等の措置が義務化されていない国・地域に所在する暗号資産交換業者や、個人の取得・管理に係るものである場合には、取引により移転した暗号資産の所有者を特定することは困難となる

犯罪者等はAML/CFTの対策が劣っている国・地域等を標的に、マネー・ローンダリング等を行う傾向があると考えられます。そのため、上記のような状況にもリスクがあるものと思われます。

- **法規制等**

（1）主な法令

暗号資産交換業者に関する規制として、マネー・ローンダリング等防止の観点から、日本においてもAML/CFT関連法令が施行されています。主な法令と暗号資産に特に関する義務等は以下のとおりです。

- **犯罪による収益の移転防止に関する法律（以下、「犯収法」という）**
  暗号資産交換業者につき、特定事業者として指定（第2条）。また、実施すべき事項として、取引時確認（第4条）、トラベルルール（第10条の5）等を規定
- **外国為替および外国貿易法**
  暗号資産移転時における顧客の本人確認（第18条の6）等を規定
- **資金決済に関する法律**
  暗号資産交換業者を定義（第2条）のうえ、登録の要件（第63条の2）等を規定。そのうえで、当局による立入検査（第63条の15）、業務改善命令（第63条の16）および登録の取消し等（第63条の17）の実施等を規定

上記のように各種義務が課されるとともに、態勢不備があった場合には、当局による処分がなされる可能性もある点、配意が必要であるものと思われます。

（2）トラベルルール

日本では、前掲のとおりトラベルルールの適用開始のため、犯収法を改正、2023年6月より施行しました。内容としては、暗号資産交換業者が顧客の暗号資産等を移転する際に、送付人・受取人の情報を通知する義務を定めるものとなります（図表3参照）。加えて、暗号資産交換業者は、トラベルルール遵守の前提として、顧客の情報の取得・通知事項の記録・保存等が必要となります。

図表3　トラベルルール上、通知が必要となる事項

	自然人	法人
送付人情報	• 氏名 • 住居または顧客識別番号等 • ブロックチェーンアドレスまたは当該アドレスを特定できる番号	• 名称 • 本店または主たる事務所の所在地または顧客識別番号等 • ブロックチェーンアドレスまたは当該アドレスを特定できる番号
受取人情報	• 氏名 • ブロックチェーンアドレスまたは当該アドレスを特定できる番号	• 名称 • ブロックチェーンアドレスまたは当該アドレスを特定できる番号

出典：金融庁資料（暗号資産・電子決済手段等の移転に係る通知義務（トラベルルール））を基にKPMG作成
https://www.fsa.go.jp/news/r4/sonota/20230526-2/00.pdf

（3）規制等に違反した場合のリスク

各種法規制等に違反した場合、前章I.(2).①節「暗号資産の性質」に記載のように、当局より処分される可能性があります。過去にマネー・ローンダリング等に関連し、処分が行われた事例としては、以下のようなケースが存在します。

- 取引時確認の不備、疑わしい取引の届け出要否の判断が適切になされていない、また利用者情報の管理態勢等に不備がある等の事由により、業務停止命令等の処分がなされたケース
- 犯収法に定める取引時確認や、確認記録の作成を行っていないといった、法令違反行為等が認められたために、業務改善命令がなされたケース

これらのケースでは、直接犯罪等に関与したという情報は見られませんでしたが、取引時確認・確認記録の作成等が行われていないことをもって業務停止命令等がなされていることから、しっかりとした態勢整備自体が当局より求められているものと考えられます。なお、トラベルルールについての処分事例は見受けられませんでしたが、同様に対応する必要があるものと思われます。

このほか、海外における事例となりますが、近年では大手暗号資産交換業者に対し、AML/CFT関連規制に違反したことを事由に、数千億円相当の罰金が米国当局から課されている事案もあります。態勢の不備が大きなリスクにつながる可能性もある点、配意が必要なものと思われます。

Ⅱ 暗号資産交換業者等における対応のポイント

各事業者には、暗号資産取引のリスクを踏まえたAML/CFT態勢構築が求められます。本章では、まず暗号資産交換業者における対応のポイントについて述べます。

• 全社的リスク評価の実施

暗号資産取引全般として、前章に挙げたリスクが存在します。一方で、事業内容等により、個々の事業者の抱えるリスクの種類や大きさは異なるため、リスクベースでの対応が必要となります。この点、金融庁「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」[3]（以下、「金融庁ガイドライン」という）では、各事業者に対して、4つの評価軸（自社の商品・サービス、顧客属性、取引形態、国・地域）のリスクを特定・評価のうえ、低減措置を検討・実施することを求めております。

これらリスク評価の実施にあたっては、たとえば商品・サービスならば、すべての取扱商品（取引可能な暗号資産の銘柄等）を対象にする等、網羅的なリスクの特定・評価が求められます。つまり、上記4つの評価軸別に暗号資産の特性を踏まえることが必要となるものと考えられます。一例としては、想定される取引の局面ごとに、どのようなリスクがあるかを評価することが挙げられます（図表4参照）。

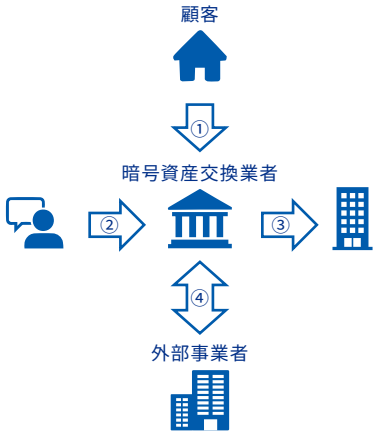
• リスク低減措置の実施

リスク評価の結果を踏まえ、現状の態勢に不足がある場合には、追加のリスク低減措置を講じる必要が生じます。この点、前掲図表4の①～④の局面別に、たとえば以下のような取組みが実施されているか、また高度化の余地が無いかなどを検討することも考えられます。

① 顧客受入/継続時

- KYCによる顧客の氏名や実質的支配者情報等の取得。また、当該情報を用い

図表４ リスク評価



①	顧客受入／継続時	• 自社の顧客が反社会的勢力である等、不芳な属性であるリスク • アカウントが譲渡・売買等されるリスク
②③共通	入庫／出庫時	• 匿名性の高い暗号資産取引を行うリスク • 不芳な入庫元／出庫先と取引をするリスク（資産凍結対象者等、入庫元／出庫先自体が不芳な場合） • 規制下に置かれていない先と取引をするリスク（アンホステッドウォレット、または規制が整備されていない国の暗号資産交換業者を利用する者等が入庫元／出庫先である場合）
④	外部事業者との取引／接続時	• 暗号資産の調達先等がマネー・ローンダリング等に関わったことにより、自社も風評被害を受けるリスク

出所：KPMG作成

たスクリーニングを実施（反社会的勢力等に該当しないかの確認）
- 取引モニタリングにより、これまでの態様と異なる取引を検知（アカウントが不正に譲渡等されていないかを確認）

② ③ 入庫/出庫時
- 取引可能な暗号資産の銘柄を限定（たとえば、暗号資産交換業協会でグリーンリストとして公表されているか、取引を匿名化する仕組みの有無等が挙げられる）
- 入庫元/出庫先のリスクに応じて取引制限等を実施（児童虐待と関連するサイト等への入出庫は禁止する等）
- 上記に関連し、アンホステッド・ウォレットや高リスク国・地域との関連があるアカウントや相手先との入出庫が見られる場合には、より厳格に取引モニタリングを実施。そのうえで不審な取引が見られる場合には、疑わしい取引の届け出、または取引制限等の実施を検討

④ 外部事業者との取引/接続時
- 暗号資産の調達先となる外部事業者に対し、必要に応じ質問票等を用いて態勢確認を実施（たとえば、AML/CFTに関する方針・手続きの有無、KYC/取引モニタリング/スクリーニングの実施内容等を確認する等）

Ⅲ 預金取扱金融機関等における対応のポイント

預金取扱金融機関等も、顧客または顧客の振込相手先等に暗号資産交換業者が存在する場合には、間接的にマネー・ローンダリング等に関わってしまう可能性があります（暗号資産交換業者の顧客が、マネー・ローンダリングを実施する場合等）。その場合、決済の場を提供していたことや、提携先として自社の名前が公表されることにより、自社にも責任が問われてしまう、また風評被害等が及ぶことが考えられます。このため、リスクに応じた対応が求められます。ここでは、そのような対応のポイントについて述べます。

• リスクの特定・評価

暗号資産はNRA（第5.1（8））にも、そのリスクについて触れられています。この点、金融庁ガイドライン（Ⅱ-2（1）①）を踏まえ、リスクの特定・評価の対象として、暗号資産交換業者を含めることも必要と思われます。

評価にあたっては、暗号資産交換業者の顧客取引に間接的に関与する場合のリスクを踏まえ、実施することが考えられます。この点、たとえば暗号資産交換業者に対し、当該事業者の顧客アカウントへのチャージ機能等を提供する場合（振込入金専用口座等の提供）のリスクを分析のうえ、対応を検討する等が挙げられます（自社が知らないまま、間接的にサービスがマネー・ローンダリング等に悪用されるリスク）。

• リスク低減措置

暗号資産交換業者が顧客、または顧客の振込相手先等が暗号資産交換業者である場合、間接的にマネー・ローンダリング等に関わる可能性があります。ここでは、対応ごとに考えられるリスク低減措置を説明します。

（1）暗号資産交換業者が顧客である場合の対応

前掲の暗号資産交換業者の顧客アカウントへのチャージ機能等を提供する場合、NRA（第5.1（1）ウ（ウ））においても以下のように記載されているように、暗号資産交換業者の態勢を確認することが対応のポイントとなります（Ⅱ.④節「外部事業者との取引／接続時」で挙げたもののほか、たとえばAML/CFTに関するリスク評価や内部監査の実施状況等を確認することも考えられます）。

- 特殊詐欺や不正送金等による犯罪収益を振込入金専用口座を経由して入金したあと、暗号資産を購入し、即時に購入した暗号資産を出金するといった手口が多数認められることから、暗号資産交換業者へ振込入金専用口座を提供する一部の預金取扱金融機関においては、暗号資産交換業者のマネー・ローンダリング等リスク管理態勢を確認するための質問状の発出（中略）等の対策を実施

（2）暗号資産交換業者への振込時の対応

近時の事案として、特殊詐欺の被害金が暗号資産交換業者あてに送金される事例が多発しており、以下の対策が金融機関に求められています（警察庁「暗号資産交換業者への不正送金対策の強化に関する金融機関への要請について」[4]（以下、「警察庁要請」という））。

- 振込名義変更による暗号資産交換業者等への送金停止等
- 暗号資産交換業者等への不正な送金への監視強化

上記については、一般社団法人全国銀行協会等に対して、会員等への周知の要請がなされている（警察庁要請の「1.経緯」参照）ことから、すでに取組みをしている金融機関も多数あるものと思われますが、自社に直接取引が無い場合にも対応が求められる点には配意が必要であるものと思われます。

以上、暗号資産に関するリスク、またその対応のポイントを紹介しました。暗号資産は、近年決済手段および投資対象としても認知され、幅広く使用される一方で、暗号資産に関連するマネー・ローンダリン

グ等の事案も多数見られます。この点、各事業者へのAML/CFTに関する役割期待も高まってきており、各種法規制の整備が行われています。もし、AML/CFTの態勢に不備がある場合、自社が犯罪に加担してしまう、または態勢不備を事由とした処分等のリスクもあります。

　このため、AML/CFT態勢の高度化を進めることが、今後さらに各事業者に求められるものと思われます。

1 国家公安委員会「犯罪収益移転危険度調査書」2023年12月
https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk051207.pdf

2 FATF「TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS」2023年6月
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

3 金融庁「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」2021年11月
https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf

4 警察庁「暗号資産交換業者への不正送金対策の強化に関する金融機関への要請について」2024年2月
https://www.npa.go.jp/bureau/cyber/koho/news/20240206.html

関連情報

ウェブサイトでは、マネー・ローンダリング、テロ資金供与および拡散金融対策関連サービス等を紹介しています。

https://kpmg.com/jp/ja/home/services/advisory/sectors-markets/financial-services/aml-cft.html

本稿に関するご質問等は、
以下の担当者までお願いいたします。

有限責任 あずさ監査法人
流 良和／マネジャー
☎ 03-3548-5125（代表電話）
✉ yoshikazu.nagare@jp.kpmg.com

KPMGジャパン
kpmg.com/jp