仮想通貨交換業者におけるマネロン・テロ資金供与対策のあるべき姿

国際的要請も高まるなかで、リスク管理態勢の整備は急務

金融庁監督局総務課
仮想通貨モニタリングチーム
モニタリング管理官
岡田　瞳

マネー・ローンダリングおよびテロ資金供与対策（ＡＭＬ／ＣＦＴ）への要請がますます高まるなか、仮想通貨交換業者においても、犯罪収益移転防止法（犯収法）の遵守に係る一律の対応にとどまらず、自らが直面するマネロンおよびテロ資金供与（ＭＬ／ＦＴ）リスクについて特定・評価し、リスクに見合った低減措置を講じるなど、有効なＭＬ／ＦＴリスク管理態勢の整備が求められる。

なぜ資金決済法と犯収法が改正されたのか

２０１５年６月に発出されたＧ７エルマウ・サミット首脳宣言は、テロ資金供与対策に関連し、「仮想通貨およびその他の新たな支払手段の適切な規制を含め、すべての金融の流れの透明性拡大を確保するためにさらなる行動を取る」ことを明示した。本宣言に呼応し、ＡＭＬ／ＣＦＴに係る政府間会合であるＦＡＴＦ（Financial Action Task Force：金融活動作業部会）は同月、仮想通貨に係るリスクベース・アプローチ（ＲＢＡ）のガイダンスを発出し、仮想通貨と法定通貨の交換について登録・免許制を課すことや、顧客の本人確認や疑わしい取引の届出・記録保存義務等のＡＭＬ／ＣＦＴ規制を課すことを求めた。

このようなＡＭＬ／ＣＦＴに係る国際的な要請のほか、わが国においては、取引量において14年当時世界最大規模であった仮想通貨取引所の破綻もあるなかで、利用者保護や的確なＡＭＬ／ＣＦＴ実施等の観点から法整備が行われ、16年５月に資金決済法および犯収法が改正された（17年４月施行）。

仮想通貨交換業者が講ずるべきＡＭＬ／ＣＦＴ

では、仮想通貨交換業者にはどのようなＡＭＬ／ＣＦＴが求められるのか。犯収法は仮想通貨交換業者にも一定の対応を義務付けている。しかし、①仮想通貨がＭＬ／ＦＴに利用されるおそれ（注）、②次々と編み出される新たなＭＬ／ＦＴ手法、③ＡＭＬ／ＣＦＴへの国際的な目線の高まり、④国内外の金融機関等がＭＬ／ＦＴリスク管理のなかで仮想通貨交換業者を含む顧客の体制や、場合によってはその実効性等も精査している状況、⑤実効的な対策整備に後れを取る金融機関が犯罪者等の標

的とされるおそれ――などをふまえれば、法令上の規定を遵守するための一律の対応だけでは十分とは言えない。すなわち、仮想通貨交換業者は、自らが直面しているリスクを適時・適切に特定・評価し、そのリスクに見合った低減措置を講じる（ＲＢＡ）などＭＬ／ＦＴリスク管理態勢を整備し、時々刻々と変化するリスクについて機動的に対応することが求められる。

その観点から、仮想通貨交換業者においても、金融庁が今年２月６日に公表した「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」（以下、ガイドライン）をふまえるほか、たとえば、前述のＦＡＴＦによるガイダンスや他国当局による報告書等を参考に、ＭＬ／ＦＴリスク管理態勢を整備することが強く求められる。

以下では、ガイドラインの内容のうち、実効性のある態勢整備の大前提となるＲＢＡについて仮想通貨交換業者が留意すべき事項を概説するが、ガイドライン上の「Ⅲ管理態勢とその有効性の検証・見直し」に記載されている事項についても、リスクや業務規模・特性をふまえて対応することが重要である。

リスクの特定・評価におけるポイント

仮想通貨交換業者が適切なリスク低減策を講じるためには、営業地域の地理的特性や事業環境・経営戦略のあり方など、自らの個別具体的な特性を考慮する必要がある。そのうえで、国家公安委員会が公表する「犯罪収益移転危険度調査書」（以下、調査書）の内容を勘案しつつ、自社における⑴商品・サービス、⑵取引形態、⑶顧客属性、⑷国・地域――などのリスクを包括的かつ具体的に特定し、その特定したリスクの高低を適切に評価することが求められる。

⑴商品・サービス

①取扱仮想通貨

一般的に、仮想通貨の性質に伴うリスクは以下が考えられる。

・匿名性（資金源／取引等の犯罪性の検知や追跡が困難）

・即時移転性（当局等が検知する前にさらなる資金移転・犯罪利用が可能）

・遠隔取引可能性（高リスクな地域や顧客が取引に関与する機会が増加）

・直接取引可能性（第三者または当局による検知・介入機会が減少）

こうした性質については、調査書においても仮想通貨に関連して言及されているが、仮想通貨交換業者においては、以下にあげるような具体的内容にも踏み込んで検討すべきである。

■仮想通貨の種類や種類ごとの性質

ビットコインをはじめとする仮想通貨は、現時点で千数百種類を超え、その性質はそれぞれ異なる。たとえば、ＮＥＭのブロック組成間隔は約１分と言われており、ビットコインよりも急速なレイヤリングが可能である。また、DashやMonero、Zcashのように、後述するミキシング技術やゼロ知識証明（移転元／移転先と金額を隠匿）といった匿名化機能を実装した匿名性の高い仮想通貨も存在する。

■ＭＬ／ＦＴリスクを高める匿名化技術やサービス

犯罪者は次にあげるような技術やサービスを併用することで、取引の追跡をさらに困難にすることが可能である。

●Tor（The Onion Router）

発信元のコンピュータと送信先のコンピュータとの間で直接通信が行われる一般的な通信と違い、発信元コンピュータから世界中にある複数のノードを経由（発信元コンピュータとノード間および経由したノード間の通信は暗号化）して、送信先のコンピュータと通信が行われる。これにより、発信元コンピュータの地理的所在の特定を困難にする。

●ミキシング技術

取引を、複数の他者による取引と混合し一つに集約した後、各々の移転先に再分配することにより、移転元とのつながりを不明瞭にする技術。本技術を用いた匿名化サービスは「ミキサー」と呼ばれ、企業等の第三者が仲介しサービスを提供するほか、Ｐ２Ｐでミキシングを行うこともできる。

●仮想通貨同士の交換ができる口座開設不要なオンライン・サービス

自らが保有する仮想通貨を匿名性の高い通貨に交換し、任意のアドレスに移転が可能。ミキシング技術の一つとしてもとらえられている。

以上のように、ひと口に仮想通貨と言ってもそのＭＬ／ＦＴリスクは多様であること、また、匿名化技術等により取引のＭＬ／ＦＴリスクが高まることに留意すべきである。仮想通貨交換業者は、取り扱う通貨や取引に伴うＭＬ／ＦＴリスクをそれぞれ特定し評価することが求められる。

②サービス

仮想通貨交換業者は通常、顧客との間で仮想通貨の売買や他仮想通貨との交換を行っているほか、これらの媒介、取次または代理などを行っている。こうしたサービスのＭＬ／ＦＴリスクの特定にあたっては、自社が顧客に対しどのようなサービスを提供しているのか網羅的に洗い出す必要がある。そもそも、リスクの特定・評価は適切なリスク低減措置を講じるために行うものであるため、犯収法上の特定業務に含まれていないからといって、仮想通貨交換業としてのサービス提供を行っていない顧客に対するウォレットサービス（仮想通貨の保管・移動）を、リスク特定・評価の対象から外すべきではない。また、特定取引ではないということのみをもって、一律にリスクが低いと評価することも適切ではない。犯罪収益が自社のサービスを通じて移転されるリスクがある限りは適切に当該サービスのリスクを特定・評価する必要がある。

⑵取引形態

仮想通貨交換業の取引形態は、その大半が非対面で行われている。一般的に非対面取引は、他人になりすますことを企図する者を看破する手段が限定され本人確認の精度が低下することから、対面取引よりも高リスクとされている。しかし、しっかりとした顧客管理を行っている金融機関等の口座に紐付く場合の非対面での仮想通貨取引と、現金を用いた対面での仮想通貨取引とを比較すれば、後者のほうがリスクが高いとも考えられる。このように、銀行口座入金、コンビニ入金、ペイジー入金の入金方法や、顧客が口座を有する金融機関等の顧客管理の程度等によってリスクが異なることから、取引形態に関連して、入金方法も勘案すべきであろう。

なお、取引形態の一つとして、仮想通貨ＡＴＭ（通常、ビットコインと法定通貨との交換を行う装置で「ＢＴＭ」とも呼ばれる）がある。ＢＴＭは銀行ＡＴＭと同様に一般の商業施設等に隣接して設置されるものであるが、英国においては薬物販売者が薬物売買で得た収益をＢＴＭでビットコインに交換する手口が多発し、警察が苦慮していると報道されている。ＢＴＭには非対面取引のみならず現金取引という要素が加わるためリスクが高く、今後は東京五輪等に向けて利用者増加も見込まれるなか、ハード面の投資を含めた相応の態勢整備が求められてしかるべきであろう。

⑶顧客属性

顧客の属性については、調査書に記載されているもののほか、前述の匿名化技術を利用する顧客もリスク特定・評価の対象となるであろう。もちろん、顧客は匿名化技術や匿名性の高い通貨を必ずしも不正目的のために利用しているわけではないが、相応の潜在的リスクはあると言える。後述のブロックチェーン解析ツールを用いず把握することが困難な場合であっても、こうした把握ができないからといってリスクの特定・評価の対象から外すのではなく、把握できないこと自体をリスクとしてとらえる必要がある。

⑷国・地域

国・地域については、調査書が記載する海外の国・地域（国際テロリストのおもな活動地域を含む）のみならず、国内にも目を向けるべきである。対面取引であれば店舗が所在する周辺環境、ＢＴＭの場合には設置場所のリスクを特定・評価することが考えられる。たとえば、都内であっても、オフィス街、繁華街、住宅街ではそれぞれＭＬ／ＦＴリスクが異なるはずである。なお、仮想通貨取引はデジタル空間で行われることから、アドレスの実際の所在を特定することは困難であろう。一方で、顧客属性と同様、ブロックチェ

ーン解析ツールの利用により、所在を一定程度特定できるパターンもあると考えられる。

以上、これらのリスク要素について、仮想通貨交換業者は自らが直面するＭＬ／ＦＴリスクを定量的かつ定性的に特定・評価すべきである。この点、たとえば、非対面取引、対面（現金）取引、ＢＴＭなど複数のビジネスを営んでいるのであれば、そのビジネスごとにリスクの特定・評価を行ったうえで総合的に勘案し、最終的に自社全体としてのリスクを評価することも可能である。

他業態よりも一歩進んだ低減措置を

以上のとおり、仮想通貨やその取引に伴うリスクをふまえれば、仮想通貨交換業者が直面する固有リスクは相応に高いと考えられ、他業態と同等の低減措置を講じたとしても、残存リスクが適切なレベルまで低減されるとは限らない。すなわち、仮想通貨交換業者は他業態よりも一歩進んだ低減措置を講じるべきである。

⑴顧客管理

仮想通貨交換業者は、取引関係の開始時、継続時、終了時の各段階において、個々の顧客や取引のリスクの程度に応じて、顧客情報や取引内容を調査し講ずべき低減措置を的確に判断・実施（顧客管理）する必要がある。この点において、前述のリスク特定・評価の結果、たとえばリスクの高い通貨に係る取引を行う顧客に対しては、顧客情報等の調査や低減措置の対象、頻度、内容を、その他の通貨に係る取引だけを行う顧客に対するものよりも強化するなど、厳格な顧客管理を実施するほか、こうした顧客管理を講ずることができない場合には当該通貨の取扱いに再考が求められる。

また、仮想通貨の売買等取引を国内外の同業他社と行う場合には、相手先におけるＭＬ／ＦＴリスク管理態勢を精査すべきである。

なお、外国為替及び外国貿易法では経済制裁措置を実施しており、経済制裁に係る支払いまたは支払いの受領が仮想通貨で行われる場合も、同法上の許可が必要となる。同法上、仮想通貨交換業者には、為替取引に該当しない仮想通貨交換取引に関する制裁対象に係るスクリーニング（制裁対象者リストとの照合等）は求められていないが、同法上の許可制の趣旨に鑑み、適切なＡＭＬ／ＣＦＴのリスク管理として当該スクリーニングを行う必要がある。一方で、ウォレットは必ずしも特定の自然人と結びつかないことから、所有者が制裁対象者等に該当するか否かの把握は困難であることに留意したい。

また、12年10月に金融庁が公表した「犯罪収益移転防止法に関する留意事項について」をふまえ、仮想通貨交換業者においては、ほぼリアルタイムで第三者への移転等が可能という仮想通貨のリスク特性に鑑み、取引時確認完了前においては、全取引または出金・出コインなど一部取引の制限を含む適切な対応について検討する必要がある。

⑵取引モニタリング・フィルタリングおよびシステムの活用

ＩＴシステムと密接な関係にある仮想通貨交換業において実効的なＭＬ／ＦＴリスク管理態勢を整備するためには、とりわけ顧客スクリーニング、取引モニタリングまたはフィルタリングに係るシステム対応は当然であろう。こうしたシステムツールの一つには、おもにビットコインについてブロックチェーン上の公開情報を分析する「ブロックチェーン解析ツール」がある。このツールには、ウォレットの過去の取引実績（ダークウェブとの取引の有無等）に基づいて当該ウォレットのリスクを評価するものもあり、出コイン先ウォレットに対するアラート発出のほか、前述の外国との取引やミキサー等を使用する顧客についても一定の検知が可能と言われている。仮想通貨交換業者においては、強いリスク認識のもと、業務規模・特性等をふまえ、こうしたツールの早期導入の必要性を検討することが求められる。なお、導入を不要と判断した場合にはその理由について的確に説明できることが重要である。

なお、米当局は昨年7月、海外仮想通貨取引所ＢＴＣ－ｅに

対して同国の銀行秘密法および関連規制を適用し、1億100万ドルの罰金を命じた。仮想通貨交換業者がその事業のすべてまたは実質的な部分を米国内において行う場合、事業者は米国においてMoney Services Business（MSB）として登録をしなければならない。一般に、米国人顧客との取引状況、米ドル取引状況および米国内でのサーバー設置等を勘案し事業の実質的な部分が米国で行われているかの該当性が判断されるものと考えられるが、こうした判断基準を含む米国当局の動向には留意する必要がある。また、本事案では、有効的なML／FTリスク管理態勢の不備等の事例として、ミキサーや匿名性の高い仮想通貨のリスクに見合った低減措置が不十分であった旨も指摘されているところ、とりわけ非居住者との取引や海外に展開している仮想通貨交換業者はこうした海外当局による制裁リスクも勘案しシステム導入を検討すべきである。

(3)疑わしい取引の届出

犯罪者はさまざまなML手口を考案するため、複数のサービスを複数の取引形態で提供している場合、IPアドレス、取引パターン、顧客の挙動、言動など疑わしさを検知する場面やきっかけはそれぞれ異なることに留意したい。

なお、わが国においては一般的に、疑わしい取引の届出後も取引の追跡可能性を確保するなどの目的で当該取引の口座を凍結しないケースが見受けられる。しかし、仮想通貨については、取引履歴がブロックチェーン上で公開され取引追跡が可能であることや、その即時移転性に鑑みれば、明らかに疑わしいなどの場合には速やかな口座凍結を含む適切な対応を行える態勢を整備することが重要と考える。

＊　＊　＊

今後、金融庁としては、各社が実施するガイドライン上の「対応が求められる事項」等と現状とのギャップ分析の内容もふまえ、オンサイトも含む必要なモニタリングを実施し改善を促していくことが想定される。また、関連省庁や業界団体、他業態、個別仮想通貨交換業者のみならずシステムベンダー等や海外当局との対話を通じ、仮想通貨交換業に係るリスクおよびAML／CFTについて積極的に理解を深めるとともに情報収集し還元していきたい。

（注）たとえば、海外では、偽造パスポート・違法薬物・個人情報の売買や、犯罪の請負などが行われるダークウェブでの支払いのほか、資金洗浄プロセスのうち、「レイヤリング」（犯罪収益の出所を不透明にするための資金源からの分離）に仮想通貨が多用される事例が明らかになっている。

（本稿において意見にわたる部分は筆者の個人的な見解であり、所属する組織の見解を示すものではない。また、本文中にあげるリスク要素や低減措置、管理態勢の内容は一例にすぎず、これらに限定されない。）

おかだ　ひとみ
ニュージーランド オークランド大学政治学部卒。外資コンサルティング会社等を経て、14年6月金融庁入庁（金融証券検査官）。17年11月から現職を併任。