暗号資産等の利用拡大と利用者保護

投資対象として認識されつつある暗号資産について、当局が、金融商品の一種として位置づけ直す議論を進めている。暗号資産のリスクについて、一般投資家には交換業者が防護壁となることが期待されるが、ノンカストディアル・ウォレットの利用が広まることを見越したリスク対策を検討すべきである。

暗号資産保有の広まりと制度改正

暗号資産を保有する裾野が拡大しつつある。金融庁によれば[1]、国内の暗号資産交換業者（以下、交換業者）における、口座数は延べ1,200万口座を超え[2]、利用者預託金残高は5兆円を超えた（2025年1月末時点）。また、いわゆるステーブルコインについて、改正資金決済法の施行を受け、2025年3月にSBI VCトレード社が米ドル建てのUSDC[3]の取り扱いに係る登録を行い、8月にはJPYC社が電子決済手段を発行可能な資金移動業者として登録した。

海外に目を向けると、米国はトランプ政権への移行後、様々な暗号資産プロジェクトの進展を促進する政策への転換姿勢を明確にした。具体的には、証券取引委員会（SEC）が数多くの訴訟を取り下げ、また、連邦議会がステーブルコインの規制整備に関するGENIUS法を可決、トランプ大統領が7月18日に署名して成立させた。さらに、多種多様なデジタル商品について、米商品先物取引委員会（CFTC）とSECの権限を明確化するCLARITY法案を議会で審議している。これまで、暗号資産等に係る連邦法の整備で日本や欧州等に後れていた米国が、一気に巻き返そうとしているように見える。

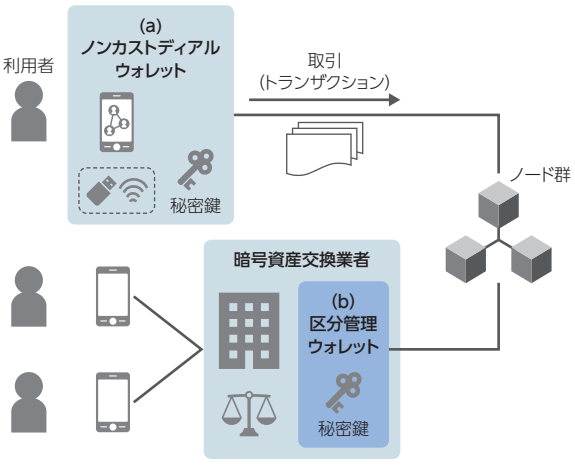
日本では米国の政策転換に先立ち、暗号資産に係る制度改正の議論が始まっている。これまで、資金決済法により規制されてきたが、国民の投資対象の一つとして認識が広まる反面、①情報開示・提供の充実、②無登録業者への対応、③投資運用等に係る不適切行為への対応、④価格形成・取引の公正性の確保にかかる喫緊の課題が生じたためとされる[4]。

暗号資産の扱いに伴うリスク

ここで、そもそも暗号資産はどのように扱われるのか、その基本的な仕組みについておさらいしておきたい。代表的なビットコインを例にとると、資産を移転するには「送信者のアドレス[5]から受信者のアドレスへある一定量の額面を移動させる[6]」というデータを送信者の秘密鍵で署名したもの（「取引」）をノード群に送付、承認を受ける[7]。そして、2009年のビットコイン草創期から手掛けるような「尖った」利用者は、アドレスと秘密鍵を格納する電子財布（ウォレット）を自らのコンピューターに作成／導入してきた。外部の業者に保管を委託しないことから、この電子財布はノンカストディアル・ウォレットとも呼ばれる（図表のa）。

ただし、ウォレットは発展途上かつ多種多様であり、導入にはITスキルの高さが求められてきた。加えて、利

図表　2通りのウォレット



（出所）各種情報を基に野村総合研究所作成

NOTE

1) 金融庁「ディスカッション・ペーパー『暗号資産に関連する制度のあり方等の検証』」(2025年4月)。
2) 個人口座と法人口座の両方を含め、同一人が複数の交換業者で口座を開設している場合には複数の口座としてカウントされている(上記1)の脚注9より)。
3) 米ドル建ステーブルコインの一つ。日本では外国電子決済手段として扱われる。
4) 1)と同じ。
5) 送信元や受信先に紐づく、文字と数字の長い連なり。
6) アンドレアス・M・アントノプロス著、今井崇也・鳩貝淳一郎訳(2016)「ビットコインとブロックチェーン」NTT出版より引用。
7) ある送信者の取引が承認(ブロックに追加)された後、さらにブロックが追加されていくことで当該取引が取り消される可能性が低くなる(確実性が高まる)。
8) ブロックチェーン技術の制約や限界については、松尾真一郎ほか(2024)「Web3の未解決問題」(日経BP)が詳しい。
9) 特定の個人や組織、もしくは最終受益者。
10) トランザクションのプライバシーを高める技術が開発されているが、他方で、法執行機関から見た透明性の確保が課題となっており、部分的な開示機能を持つ方式が提案されている。また、トランザクションとは直接関係しないが、フランスでウォレット技術会社の経営者等が身代金誘拐に遭い、大怪我を負う事案が生じた。
11) ただし、交換業者の口座から利用者のウォレットへの移転(出庫)や、その逆(入庫)の際には外部から個別の取引として観察可能である。
12) また、ステーキングなどの新たな収益サービスの提供についても各種のリスク説明が求められている。
13) チェーン上での他の暗号資産等との交換や担保付貸借等には別途、高度な金融知識やトレーディング技術が求められる。

用時に、大まかにみて、次の3つのリスクに対峙することになる[8]。(1)保管リスク:ブロックチェーンは、従来の金融情報システムでいうところの勘定系をそのまま表に出しているとも喩えられ、もし秘密鍵が漏えいすれば資産が流出しかねない。(2)プライバシー・リスク:取引をノード群に公開するため、ウォレットのアドレスと実利用者[9]の関係が悪意ある第三者に特定されれば、個人情報や企業秘密の漏えいや、強盗や誘拐、恐喝等に遭うおそれを高める[10]。(3)未成熟リスク:技術開発や制度整備の歴史が20年弱と浅く、承認速度や順序の問題、また、特定の人や組織からの強い影響力や弊害の有無をどう判定するかなど、未だ社会実験的な段階にある。

上記のリスクについて、大多数の一般利用者には交換業者が防護壁となることが期待されてきた。具体的には、(1)について、利用者から預託された財産を、交換業者の財産と分別してまとめて管理のうえ、利用者からの注文の総量に応じた必要な取引に、区分管理ウォレット用の秘密鍵で署名する(図表のb)。また、サイバー攻撃に伴う被害額について、これまでの国内事案では交換業者による弁済で利用者への波及が防がれてきた。

(2)について、利用者が交換業者の口座内で注文する限り、外部から個々の約定や残高を観察できない。また、他の交換業者の口座への資産移転について、交換業者のウォレットでまとめて処理するので、利用者分は観察が難しい[11]。

(3)について、交換業者が新たな暗号資産を扱うには、国内では海外より慎重な審査プロセスがあるとされる[12]。また、様々なブロックチェーンをどう区分するか、成熟度を判別するか、国内外で議論されているところである。

ノンカストディアルの利用の広まりと利用者保護

それでは、暗号資産のリスクをあまり心配しなくてよいのか。筆者はそうでもないと感じている。まず、一連の制度改正が、結果として、暗号を保有する裾野の更なる拡大につながる可能性がある。また、ウォレットの使い勝手が改善すれば、ウォレット保有者のすそ野が拡大し、交換業者から暗号資産を自らのウォレットに移転(出庫)するなどして、いわゆるWeb3的なサービスの利用を含めて、ノード群に取引を送信する場面が増える可能性がある[13]。

実際、ウォレットの利用者認証ではITプラットフォーマーとのサービス連携による簡便化が進む。また、送信者と受信者の長いアドレス(英数字列)を間違えずに入力する手間もQRコード活用により緩和されつつある。さらに、冒頭に触れたJPYC社はステーブルコインを、交換業者を経由せず、利用者のウォレットに直接発行するサービス形態である。

上記の一連の変化から、交換業者を通した保護下にある「こちら」の世界と、すべてに自己責任が問われる「あちら」の世界が近づくようであれば、暗号資産の扱いに伴うリスクへの対策や一般利用者への注意喚起等を、誰がどのような立場からどのように行いうるのかなど、検討を進めておくべきではないだろうか。

Writer's Profile

片山 謙 Ken Katayama
金融イノベーション研究部
シニアチーフリサーチャー
専門はデジタル資産
focus@nri.co.jp