

論 説

暗号資産（仮想通貨）の税務調査と税務執行上の課題

—ブロックチェーン分析と損益計算の重要性—

東洋大学法学部教授
泉 純也

◆SUMMARY◆

本稿は、当校が令和7年2月14日に開催した「税務研究会」において、泉純也准教授（講演当時）が「分散型デジタル社会における税務執行上の課題—暗号資産・NFT等のデジタルトークンに対する税務調査の問題と納税環境の整備—」と題して行った講演の内容を基に、論説として加筆したものである。

暗号資産の匿名性と分散性がもたらす税務執行上の問題は、海外CEX、DEX及びプライベートウォレットを利用している場合、特に深刻化する。暗号資産に係る既存の情報収集制度は、これらの前では有效地に機能しない。また、暗号資産の損益計算の困難性は、調査選定のみならず課税処分ができない事態を生じさせる。

本稿は、国税庁が直面している暗号資産に係る税務執行上の問題とその要因を明らかにした上で、暗号資産を取り巻く納税環境の整備や調査手法の開発等の必要性を説く論説であり、税務執行当局に対して、課税の適正性と公平性を確保するための具体策の検討を促すものである。

（令和7年5月29日税務大学校ホームページ掲載）

（税大ジャーナル編集部）

本内容については、全て執筆者の個人的見解であり、税務大学校、国税庁あるいは国税不服審判所等の公式見解を示すものではありません。

目 次	
I はじめに	60
II 匿名性・分散性と税務執行上の問題	61
1 スーパータックスヘイブンとしての暗号資産の特徴	61
2 暗号資産の匿名性	63
3 匿名性がもたらす税務執行上の問題	65
4 暗号資産の分散性	67
5 分散性がもたらす税務執行上の問題	69
6 CARF とその限界	71
7 日本における状況と国税庁が直面する問題	76
III ブロックチェーン分析：期待と限界	81
1 ブロックチェーン分析とは	81
2 ブロックチェーン分析を利用した大規模選定	84
3 ブロックチェーン分析：期待と限界	85
IV 損益計算の困難性と税務執行上の問題	86
1 暗号資産の損益計算の手順と重要性	86
2 暗号資産の損益計算に必要な知識やスキル	87
3 暗号資産の損益計算の困難性	88
4 問題への対処方法とその困難性	94
V 結びに代えて	98

I はじめに

分散型台帳技術及び暗号技術に基づくデジタル資産⁽¹⁾、とりわけこれらの技術によって発行管理されている電子証票であるトーケン⁽²⁾の代表格である暗号資産⁽³⁾は、世界初の暗号資産であるビットコインが 2009 年に誕生して以来、その後の成長と普及により、各国の政策立案者にとって、マネーロンダリングのみならず課税の文脈においても種々の重要かつユニークな問題を提起している。これは、中央集権的機関の不存在（分散性）、匿名性、ボラティリティの高さ、金融商品や無形資産等の性格を併せ持つハイブリッド性、基盤となるテクノロジーの進化

⁽¹⁾ デジタル資産とは、何らかの権利の表章の有無にかかわらず、デジタル又は電子的に表現されたあらゆる資産であると理解しておく。See UK LAW COMMISSION, DIGITAL ASSETS: FINAL REPORT ix (2022).

⁽²⁾ トーケンとは、デジタル資産の一種であり、通常、デジタル上又は物理的に存在する他の何かを表すものと説明される。UK LAW COMMISSION, SMART LEGAL CONTRACTS ADVICE TO GOVERNMENT viii (2021).

⁽³⁾ 暗号資産とは、日本法の文脈では資金決済法 2 条 14 項の暗号資産を指すが、一般的には、より広い意味を持つ概念である。CARF の暗号資産の定義については後記注(41)参照。

の急速性といった暗号資産の特徴に起因する⁽⁴⁾。

本稿の目的は、暗号資産に係る税務執行、特に所得税の税務調査の場面において税務当局が直面する問題及びその要因を明らかにし、暗号資産に関する納税環境の整備や調査手法の開発等の必要性を説くことにある。具体的には、暗号資産の匿名性と分散性が引き起こす税務執行上の問題として、①税務当局がブロックチェーン上のトランザクションを把握していても当事者の特定ができない、また、特定の納税者が保有し、取引している暗号資産を把握できないという問題と、②税務当局が金融機関等の仲介者から利用者の情報を把握するような既存の枠組みが機能不全に陥る可能性があるという問題を取り上げる。その上で、日本においても暗号資産の匿名性と分散性により、納税者が本人確認をせずに利用できる中央集権型の暗号資産取引所（以下、暗号資産取引所を「取引所」といい、中央集権型の取引所を「CEX」（Centralized Exchange）という）のうち海外に所在する海外CEX、非中央集権型の取引所であるDEX（Decentralized Exchange：分散型取引所）、後述するプライベートウォレットを利用している場合に税務執行上の問題が深刻化すること及び既存の情報収集制度はいずれも課税当局への情報提供等に係る義務を課しうる国・地域内に当該義務を負担する「者」が存在する場合にしか有効に機能しないことを指摘する。このような考察を経て、暗号資産の匿名性と分散性に起因する税務執行上の問題に対処するために、暗号資産の追跡可能性・透明性に加えて仮名性を生かした調査手法であるブロックチェーン分析に着目し、国税庁においては、高性能な分析ツールを開発又は利用し、国税調査官をトレーニングする必要があることを論じる。

また、最も重要な税務執行上の問題として、国税庁が納税者に帰属するCEXの口座やプライベートウォレットを把握できるとしても、効率的な調査選定ができないのみならず、課税処分をすることもできない事態が起こりうることを指摘する。かかる問題は損益計算の困難性という暗号資産のユニークな特徴によってもたらされる。そこで、その困難性の要因を明らかにした上で、国税庁は、性能等が税務調査に最適な損益計算ソフトを開発又は利用し、国税調査官をトレーニングする必要があることを論じる。

なお、本稿における暗号資産やブロックチェーンに関する記述は、ビットコインやイーサなど一般的な暗号資産に係るものを念頭に置いており、例外的なものがあることを否定するものではない。

本稿の作成に当たって、Chainalysis Japan株式会社の内田雅彦日本代表、小川大輔氏、重川隼飛氏より、多くの有益な助言と資料をご提供いただきましたことに深く感謝申し上げます。また、藤本剛平税理士、暗号資産損益計算ソフトであるクリプトーチの開発者の方にも、貴重なご見解とご指摘を賜りましたことを、心より御礼申し上げます。

II 匿名性・分散性と税務執行上の問題

1 スーパータックスヘイブンとしての暗号資産の特徴

暗号資産について、従来のタックスヘイブンにおいて最も重要な次の2つの特徴を備えてい

(4) See OECD, TAXING VIRTUAL CURRENCIES: AN OVERVIEW OF TAX TREATMENTS AND EMERGING TAX POLICY ISSUES 7, 41, 54 (2020); OECD, ADDRESSING THE TAX CHALLENGES OF THE DIGITAL ECONOMY, ACTION 1 - 2015 FINAL REPORT, OECD/G20 BASE EROSION AND PROFIT SHIFTING PROJECT 44 (2015).

ることを指摘する見解がある⁽⁵⁾。

①源泉地国課税の対象外

暗号資産は、オンライン上のウォレットとして知られるサイバー空間の口座に保管され、運用される国・地域が存在しないことから、源泉地国課税の対象にはならない。

②匿名性

暗号資産の口座は匿名で運用されている。利用者はビットコインの購入やマイニング、取引を行うために、身元を特定する情報を一切提供することなく、オンライン上のウォレットをいくつでも開設することができる。

さらに、上記見解は、次のとおり、仲介役の金融機関の不存在に注目する。

③仲介役の金融機関の不存在

ビットコインやその他の暗号資産には、脱税者にとって、従来のタックスヘイブンにはない、より大きな利点がある。ビットコインは、仲介役の金融機関の存在に依存しておらず、コンピュータ同士が直接的につながり、データを送受信するネットワークモデルであるピアツーピアで交換（利用者同士が直接交換）可能である。

このことから、ビットコインは、国際的な脱税防止体制の発展の影響を受けない、具体的には、FATCA（外国口座税務コンプライアンス法）の整備などにより⁽⁶⁾、情報申告や源泉徴収などの点において、税務当局の代理人としての役割を担い、徴税の新たな担い手となっている金融機関が蚊帳の外に置かれるため、暗号資産はスーパータックスヘイブンとなる可能性を秘めていると指摘する⁽⁷⁾。

ただし、現在では、上記見解は、暗号資産は伝統的なタックスヘイブンよりも効果的に機能するものではなく、おそらくは機能できないことが徐々に明らかになったという結論に達している⁽⁸⁾。このような結論は、上記②と③に関して、ブロックチェーン技術は、理論上、金融資産の取引において仲介者に頼ることなしに広範囲に分散された疑似的な匿名性を有するシステムを提供できる可能性を持っているが、現実には、暗号資産の市場の大半は仲介者不在でも分散型でもなく、（ブロックチェーン分析（後記Ⅲ参照）や従来の金融仲介機関を通じて利用者の身元が把握されるなどブロックチェーン経済は透明性があることから）匿名でもないことが判明したことを論拠としているようである。

しかしながら、暗号資産の匿名性と分散性は、技術の進歩や両者における相互補完などにより、一定の範囲と程度で確保されているし、今後もそのような状況が続く可能性は否定できない。国際的な脱税防止体制が有効に機能しないケースも想定されるほか、規制（後記6のCARF）

⁽⁵⁾ Omri Y. Marian, *Are Cryptocurrencies 'Super' Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 42 (2013).

⁽⁶⁾ FATCAとこれを範とした CRS の導入により、オフショアを拠点とした脱税が減少した、あるいは少なくとも著しく複雑化したという重要な実証的証拠があるとする見解として、Omri Y. Marian, *Not 'Super Tax Havens' After All*, UC IRVINE SCH. OF L. RSCH. PAPER No. 2025-01, forthcoming in INTERNATIONAL ISSUES IN THE TAXATION OF CRYPTOASSETS (Editora Revista dos Tribunais, 2025), at 7, <https://ssrn.com/abstract=5096107> 参照。なお、本稿で引用する URL の最終閲覧日は 2025 年 3 月 25 日である。

⁽⁷⁾ Marian, *supra* note (5), at 42.

⁽⁸⁾ Marian, *supra* note (6), at 8.

や執行体制の強化により、これらの影響を受けない国・地域又は新種の技術やサービスへの納税者の逃避を招来する可能性もある。もっとも、本稿の問題関心は、上記見解の妥当性や暗号資産のスーパータックスハイブン該当性ではなく、暗号資産の匿名性と分散性が引き起こす税務執行上の問題である。以下、このような観点から考察を進める。

2 暗号資産の匿名性

上記②の暗号資産の匿名性⁽⁹⁾について、一般に、暗号資産には一定の匿名性があると認識されている。ここでの認識は、暗号資産は、身元を明らかにすることなく、取引や保有を行うことができるように設計されているというものである。

暗号資産を自由に取引する際、通常、ウォレットを利用する。ウォレットとは、秘密鍵を保管し、トランザクションの署名・作成をしてネットワークにブロードキャストするためのツール（例：ソフトウェアウォレット、ハードウェアウォレット、ペーパーウォレット）である。また、ウォレットは、ブロックチェーン等にアクセスし、トーケンの残高やトランザクション履歴を確認するためのインターフェースを提供している。暗号資産の管理や保護に関してサードパーティのサービスに依存せずに、利用者自身がトランザクションの署名・作成に必要な秘密鍵を管理し、暗号資産を自ら管理するためのウォレットはプライベートウォレット（ノンカストディアルウォレット又はアンホステッドウォレット）と呼ばれる。本稿でいうウォレットとは、主としてこのプライベートウォレット、とりわけ本人確認をせずに利用できる海外事業者が提供するものを想定している。トランザクションとは、ブロックチェーン上における暗号資産の移転や後述するスマートコントラクトの操作を実行するアクションである。本稿では、暗号資産の移転に係るトランザクションの背後にある取引（交換取引や貸借取引など）とは別の概念として用いる。

ウォレットを作る際、秘密鍵がランダムに生成され、これに対応する公開鍵が暗号化アルゴリズムによって生成され、この公開鍵からアドレス（暗号資産の送受信やブロックチェーン上のアカウントの識別に使用される英数字の文字列）が作られる。秘密鍵は、ブロックチェーン上の特定のアドレスに関連づけられた暗号資産を、利用者が管理するためのランダムに生成された英数字の文字列であり、いわばパスワードのようなものである。これを紛失すると暗号資産へのアクセスができなくなるし、窃取されるとウォレットで管理している暗号資産が抜き取られる可能性がある。秘密鍵は、トランザクションへの署名、保有する暗号資産へのアクセスなどの際に使用され、暗号資産の保有者ないし処分権を証明するような役割も有する⁽¹⁰⁾。公開鍵によって暗号化された情報は、対応する秘密鍵を持つ者だけが復号できる仕組みとなっているため、公開鍵はアドレスの生成やトランザクションの検証などに使用される。

利用者が保有する暗号資産を移転する場合、例えば、送付元である自身のアドレス、送付先

(9) 暗号資産の匿名性や追跡困難性について、具体的な手法の説明を交えて検討する宇根正志「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—」金融研究 38 卷 3 号(2019)129 頁は、匿名性を「特定の取引にかかる当事者の属性を推定することの難しさの度合い」、追跡困難性を「特定のユーザーによる複数の取引やその流れを把握すること（取引の追跡）の難しさの度合い」と定義する。

(10) 「Not your keys, not your coins(cryptos)」と表現される所以である。See David G.W. Birch, *Not Your Keys, Not Your Coins? Whatever*, FORBES (Oct. 15, 2021, 7:03 AM, updated Mar. 9, 2022, 8:36 AM), <https://www.forbes.com/sites/davidbirch/2021/10/15/not-your-keys-not-your-coins-whatever/>.

のアドレス、送付する暗号資産の数量に係るデータをネットワークにブロードキャストする。ブロードキャストされたデータは、利用者の秘密鍵でデジタル署名され、対応する公開鍵を利用して、正当な秘密鍵の保有者による署名であること、十分な残高を保有していること、同一の nonce (number used once。一度だけ使用される数値であり、トランザクションの一意性を保証するために利用される) が既に実行済みでないことが検証される。これにより、二重払いの防止や、既に実行されたトランザクションとの重複の回避が可能となる。

暗号資産は一般的に非中央集権で運用されており、上記の検証はマイナーやバリデータなどと呼ばれるノードにより行われる。ノードとは、ブロックチェーンネットワークの基本的な構成要素であり、トランザクションの共有やデータの保存、ブロックの検証などの役割を担うソフトウェアを実行するデバイスである。ただし、ブロックの検証を行わないノードも存在する。

上記の検証作業を通じて新しい暗号資産が発行される。暗号資産は政府や金融機関など身元確認を行う中央集権的機関によって直接管理されていないことが通常であり、その発行はプロトコルに従い自動的に行われる。このため、暗号資産には分散性があるといわれる。このような分散性は、匿名で取引を可能にする基盤を提供し、暗号資産の匿名性を補完する。他方、暗号資産の匿名性により、利用者はプライバシー侵害や追跡のリスクを恐れずにネットワークに参加できるようになるし、特定の利用者が何らかの理由で参加を排除されるリスクは減少する。これにより、ネットワークの分散度合いが高まり、システムの堅牢性や検閲耐性が強化される。このように暗号資産の匿名性と分散性は相互に関連している。

ウォレットを生成し、暗号資産を送付する過程で、利用者が自身の身元に関する情報や身分証の類をブロックチェーン等に提供することはない。秘密鍵、公開鍵、アドレスもそのような情報と直接に関連づけられていない。暗号資産のトランザクションはブロックチェーン上に公開記録されるが、トランザクションはそれを実行している者の身元に関する情報ではなくウォレットアドレス（英数字の文字列）のみに関連づけられている。このため、暗号資産は仮名性を備えている。

以上のとおり、暗号資産の利用に当たって、利用者が自身の身元に関する情報を提供する必要はないこと、秘密鍵や公開鍵等にかような情報が関連づけられていないこと、ブロックチェーン上に利用者の情報が記録されていないことが暗号資産の匿名性を提供する基盤となっている⁽¹¹⁾。ただし、暗号資産の匿名性は絶対的なものではなく相対的なものにすぎない。利用者は公開鍵やアドレスといった自身の身元と結びついていない識別子を公開しており、これによって第三者は特定のアドレスに関連づけられたトランザクションを把握することができるため、

⁽¹¹⁾ Sergio Avalos, *Challenges That Cryptoasset Anonymity Creates for Tax Administrations*, 9 J. TAX ADMIN. 66, 72 (2024).

仮名取引が行われているようなものである（暗号資産の仮名性）⁽¹²⁾⁽¹³⁾。また、ブロックチェーンに記録されている情報は基本的に公開されており、誰でも追跡可能であるから（暗号資産の追跡可能性・透明性）、当該情報（オンチェーン情報）と、ブロックチェーンに記録されていない情報（オフチェーン情報）、特に CEX やショップなどが保有する利用者の身元に関する情報が関連づけられて、ウォレットの保有者の身元が特定されることがありうる。このように暗号資産の追跡可能性や透明性は匿名性とは別の性質であるが、仮名性と併せて利用されて、匿名性が破られることもありうる（後記Ⅲのブロックチェーン分析参照）。

3 匿名性がもたらす税務執行上の問題

上記で示したような暗号資産の匿名性がもたらす税務執行上の問題として、次の点が注目される⁽¹⁴⁾。

- ・ ブロックチェーン上のトランザクションを把握していても当事者の特定ができない。
- ・ 特定の納税者が保有し、取引している暗号資産を把握できない。

上記のとおり、ブロックチェーン上のトランザクションに係る当事者を特定し、接触することができなかつたり、特定の納税者が取引をしている暗号資産を把握できないとすれば、税務当局は、暗号資産取引の当事者について、自国における納税義務が発生しているか、損益額はいくらになるのかを把握することができない。自国の居住者に係る暗号資産の利用や税務コンプライアンスの実態も把握できない。ただし、個人を特定するまでに至るかという問題はあるが、少なくともビットコインについては、利用者の IP アドレスを特定し、地理的な場所にリンクさせることはできるようである⁽¹⁵⁾。

また、上記のような問題は、税務当局に捕捉されないことを奇貨として納税者が暗号資産取引から生じた所得を適正に確定申告しない、どこの国でも課税できないという事態につながる

(12) 暗号資産の匿名性は現金よりも低いものの、利用者にとっては、高額な資金を迅速かつグローバルにやりとりできるという利便性があり、特定の場面では暗号資産の方が使い勝手がよい場合がある。一方、税務当局からすると、暗号資産はブロックチェーン上にトランザクション履歴が記録されるため、追跡可能性が高いという利点がある。暗号資産と現金の匿名性の比較について、藤岡祐治「通貨の匿名性が課税に与える影響」金子宏=中里実編『租税法と民法』(有斐閣、2018)201-203 頁。なお、現金の匿名性に対する課税の議論について、藤岡祐治「現金の流動性と匿名性に対する課税」論究ジュリ 29 号(2019)207 頁参照。

(13) Avalos, *supra* note (11), at 73.

(14) 当事者の租税属性が把握できないことは、課税関係の検討場面で種々の問題を提起することについて、泉綱也「DeFi における暗号資産等のトークンの移転と課税—ブロックチェーン・スマートコントラクトを利用した分散型デジタル社会—」税法 589 号(2023)185-188 頁参照。

(15) Andreas Thiemann, *Cryptocurrencies: An Empirical View from a Tax Perspective*, 9 J. TAX ADMIN. 88, 91, 93-94 (2024).

可能性がある⁽¹⁶⁾。さらに、税務当局における租税回避スキームを追跡・把握する能力を妨げるため、脱税のみならず、租税回避をも助長するという指摘もある⁽¹⁷⁾。

もっとも、税務当局にとって朗報であるのは、政府や第三者情報を提供する立場にある中央集権的機関を介さずに金融取引を行う方法を提供するという暗号資産の当初の構想に反し、暗号資産の取引では、利用者の情報を収集し、税務当局に提供する役割を果たしうる中央集権的機関が中核的な存在となったことである⁽¹⁸⁾。暗号資産の仕組み自体は匿名性を提供するものであるが、多くの利用者は、顧客に身分証を提出させて氏名や住所等を確認する本人確認手続 (KYC : Know Your Customer) を実施している CEX を通じて暗号資産を取引又は保有しており、暗号資産の匿名性を享受していない。利用者が CEX を通じて取引等を行うのは、アクセスしやすい、ユーザーインターフェースがよい、匿名性に関心がない、自身で責任を負うこと回避したい、簡単に法定通貨と交換したい、他人にトランザクション履歴を追跡されるのを避けたい⁽¹⁹⁾などの理由によるものと推察される。

しかしながら、このことによって、税務当局が暗号資産の匿名性を完全に克服できるわけではない。一部の海外 CEX、DEX、プライベートウォレットなど、利用者が本人確認を求められることなく暗号資産を取引できる場所やツールがあり、これらが依然として暗号資産の匿名性を支えているからである。実際、暗号資産の世界では、日々、身元不明な利用者が国境を超えて、暗号資産の交換、貸借、運用等を行っている。

2023 年の暗号資産市場の調査によると、取引量の約 90%が上位 10 の取引所によって占め

(16) 暗号資産の税務執行が困難であることを認識した上で、暗号資産の課税に係る最も根本的な問題は暗号資産の匿名性であることを指摘するものとして、Katherine Baer et al., *Crypto Poses Significant Tax Problems—and They Could Get Worse*, IMF BLOG (July 5, 2023), <https://www.imf.org/en/Blogs/Articles/2023/07/05/crypto-poses-significant-tax-problems-and-they-could-get-worse> 参照。See also Thomas Slattery, *Taking a Bit Out of Crime: Bitcoin and Cross-Border Tax Evasion*, 39 BROOK. J. INT'L L. 829 (2014); James Alm et al., *New Technologies and the Evolution of Tax Compliance*, 39 VA. TAX REV. 287,330-331 (2020).

(17) Vincent Ooi, *Report on the Challenges Which Digital Assets Pose for Tax Systems with a Special Focus on Developing Countries*, prepared for the United Nations Committee of Experts on International Cooperation in Tax Matters (26th Session), commissioned by the International Tax and Development Cooperation Branch, Financing for Sustainable Development Office, United Nations Department of Economic and Social Affairs (Mar. 7, 2023), at 26, <https://financing.desa.un.org/sites/default/files/2023-03/Report%20Challenges%20of%20Digital%20Assets%20for%20Tax%20Systems.pdf>.

(18) See Katherine Baer et al., *Taxing Cryptocurrencies*, 39 OXFORD REV. ECON. POL'Y 478, 491 (2023). 同論文の概要等について、増井良啓「Baer et al. (2023) Taxing Cryptocurrencies」J-TaxNotes ブログ (2024.11.20)(<https://ymastax.blogspot.com/2024/11/baer-et-al-2023-taxing-cryptocurrencies.html>) 参照。

(19) 例えば、取引相手など自分の身元を認識している相手方に対して、決済等のために自分のウォレットアドレスを提供した場合、ブロックチェーンのトランザクション履歴を追跡され、当該アドレスに紐づくトランザクションが相手方に知られる可能性があることに抵抗を感じる個人や事業者も少なくないであろう。他方、CEXを介した場合、その内部の取引はブロックチェーンに直接的には記録されないため、外部から取引を追跡することは困難である。ただし、CEXはこれらの情報を管理しており、税務当局等に対して提供する可能性がある。参考として、Awa Sun Yin, *How Centralized Exchanges Became the Most Common Crypto Mixers*, NASDAQ (Oct. 23, 2023, 11:18 AM), <https://www.nasdaq.com/articles/how-centralized-exchanges-became-the-most-common-crypto-mixers> 参照。

られていた。その中で DEX は Uniswap の 1 つだけであり、その市場シェアはわずか 3 %にとどまった⁽²⁰⁾。他方、最近では、DEX と CEX の取引高比率が過去最高の 20%に達したというデータがあり、このことはユーザーが DEX の透明性、セキュリティ及び強化された資産管理に魅力を感じていることを反映したものであって、CEX に対する規制当局の監視が厳しくなる中、規制の厳しい地域のトレーダーが DEX の提供する自由なアクセスを求める傾向が強まっているという見解も示されている⁽²¹⁾。

さらに、必ずしも脱税が動機でないにせよ⁽²²⁾、例えば、次のような暗号資産の匿名性を高めるツール等を意図的に利用している者もいる。

- ・ トランザクションの詳細を隠匿するよう設計された暗号資産（プライバシーコイン⁽²³⁾）
- ・ 異なる利用者のトランザクションを混ぜ合わせることで資金の出所の追跡を困難にするミキサーとランプラー⁽²⁴⁾
- ・ 異なる種類の暗号資産に交換を繰り返し、異なるブロックチェーン間を行き来することで追跡を困難にするチェーンホッピング

当初、犯罪者は、違法取引に関するやりとりをビットコインで行うだけで安心感を得ていたが、その後、いくつかの法執行機関がブロックチェーン分析を利用することで犯罪捜査に成功した結果、ビットコインは、匿名性や追跡不可能性とはかけ離れたものであることが明らかになつた。そこで、暗号資産は、匿名性を高めるサービスと併用されて、犯罪に利用されるようになったといわれる⁽²⁵⁾。

4 暗号資産の分散性

暗号資産について、スーパータックスヘイブンとなる可能性を秘めていることを示した前記 1 の見解は、③仲介役の金融機関の不存在に着目していた。このような特徴は、中央集権的に運用されるものではないという意味における暗号資産の分散性といい換えることができる。暗号資産の文脈では、分散性という語は、ネットワーク、記録管理、ガバナンスや意思決定が分散しているという意味で用いられることがあり、このような分散性の要素が金融機関その他の

⁽²⁰⁾ EUROPEAN SECURITIES AND MARKETS AUTHORITY, CRYPTO ASSETS: MARKET STRUCTURES AND EU RELEVANCE, ESMA50-524821-3153 (Apr. 10, 2024).

⁽²¹⁾ Bitcoinworld, *DEX-to-CEX Volume Ratio Reaches Record 20%, Reflecting Growing Decentralized Adoption*, BINANCE SQUARE (Jan. 8, 2024), <https://www.binance.com/en/square/post/18663110436361>.

⁽²²⁾ See Nathan J. Richman, *Practitioners See No Rush to Add Cryptocurrency to Badges of Fraud*, 160 TAX NOTES Fed. 1327, 1329 (2018).

⁽²³⁾ プライバシーコインについては、多くの CEX が規制当局の指導に従ってその取扱いを廃止している。EUROPOL, CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCES 7 (2023)。このことに加えて、プライバシーコインについては、流通量が限定的であること、投機目的で購入されるケースが多く、利用者がプライバシー機能を必ずしも活用していないこと、さらに永続的なプライバシー保護を保証するものではないことを考慮すると、税務執行上の重大な問題を引き起こす可能性は高くないとの見解がある。See Marian, *supra* note (5), at 22-23.

⁽²⁴⁾ ミキサーを利用して、ICO に関する収益を隠匿した脱税事件として、United States v. Elmaani, No. 20 Cr. 661 (CM), 2023 U.S. Dist. LEXIS 59357 (S.D.N.Y. Apr. 4, 2023) 参照。

⁽²⁵⁾ EUROPOL, *supra* note (23), at 19.

仲介者に頼らないエコシステムを構築しているという見方もできよう⁽²⁶⁾。

分散型台帳とは複数のノードに分散されたデータの集合体であり、その整合性は分散型台帳を通じて情報を記録する分散型台帳技術によって確保される。分散型台帳技術により、ノードは、信頼できるデータを得るのに中央集権的な機関に依存することなく、ネットワークのノード全体で一貫した状態変更又は更新を提案、検証、記録することが可能となる⁽²⁷⁾。より具体的には、分散型台帳では、合意された方法ないし合意のためのプロセスとしてのコンセンサスメカニズムを通じて、台帳への情報やデータの追加がノードによって承認され、即時的に世界中に存在する（しゅう）他のノードに同期する。ネットワークは中央集権的機関を介さずに、ピアツーピア方式で運営されている。ネットワークの運営（と場合によっては意思決定）は、事前に定められたプロトコルやコンセンサスメカニズムを通じて実行され、権限とデータはネットワーク内の多数のノードに分散されている。

このような分散型台帳は、单一障害点の除去、改ざん耐性のほか、実行されたトランザクションやプログラムが公開されることからくる透明性や事後検証の容易さ（暗号資産の追跡可能性・透明性）という種々の利点を有する⁽²⁸⁾。

前述のとおり、暗号資産の取引では、利用者の情報を収集する役割を果たしうる中央集権的機関が中核的な役割を果たすようになった。他方、暗号資産の分散性は、利用者同士のピアツーピア取引を促進する分散型金融システムを提供する DeFi (Decentralized Finance: 分散型金融) の登場によってより強固なものとなったという別の潮流も観察しうる⁽²⁹⁾。

暗号資産の利用者の一部は、手元の暗号資産を運用する際に DeFi を利用している。DeFi とは、銀行、証券会社、CEX のような中央集権的な管理者が存在しない分散型金融システムないし金融アプリケーションの総称であり⁽³⁰⁾、中央に金融機関等が管理者として存在する CeFi (Centralized Finance) や伝統的な金融市場等を指す TradFi (Traditional Finance)⁽³¹⁾と対比して用いられる用語である。ネットワーク上でデータを記録し、共有する分散型技術の 1 つであるブロックチェーン技術に基づく分散型金融システムでは、仲介者や中央集権化されたプ

(26) 暗号資産の分散性については、ノードの分布、コンセンサスアルゴリズムによる合意形成のあり方、権限の分散など種々の考慮要素を検討する必要がある。参考として、FSB, DECENTRALISED FINANCIAL TECHNOLOGIES: REPORT ON FINANCIAL STABILITY, REGULATORY AND GOVERNANCE IMPLICATIONS 1-4(2019)は、金融サービスの分散化とは、伝統的に金融サービスの提供に関与してきた 1 つ以上の仲介機関や中央集権的なプロセスの排除又は役割縮小を指し、場合によっては伝統的な仲介業者からのリスクテイクの分散化を意味し、一般に、①意思決定の分散化、②リスクテイクの分散化、③記録管理の分散化の形態をとると説明している。

(27) *Id. at 26.*

(28) デジタル・分散型金融への対応のあり方等に関する研究会「中間論点整理」(2021)2-3 頁。

(29) 初期の DeFi プロジェクトの 1 つは 2015 年にローンチした MakerDAO といわれることがある。See e.g., Jakub, *History of DeFi – From Inception to 2021 and Beyond*, FINEMATICS (Jan. 4, 2021), <https://finematics.com/history-of-defi-explained/>.

(30) 株式会社クニエ「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結果報告書」(2022)7 頁 (https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_ja.pdf)。See also FSB, THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE 4(2023), <https://www.fsb.org/wp-content/uploads/P160223.pdf>.

(31) IOSCO, DECENTRALIZED FINANCE REPORT 8-9(2022).

ロセスの必要性を低減又は排除したピアツーピアの金融取引が可能となる。主として、誰でも許可を得ることなく自由に参加できるパブリック型ないしパーミッションレス型のブロックチェーン上でスマートコントラクトを活用して構築される分散化された金融サービスは DeFi と称されている。

分散型台帳によっては、スマートコントラクトを搭載し、一定の条件を満たした場合にプロセスが自動的に実行される仕組みを採用している⁽³²⁾。スマートコントラクトとは、一般に、「ある条件で作動するプログラムをブロックチェーンに登録し、条件が満たされた際に自動的に作動させ、その結果をブロックチェーンに自動的に記録する仕組み」であり、いわば「自動化された手段を用いて契約を強制的に執行する仕組み」といわれる⁽³³⁾（ただし、スマートコントラクト外で当事者間の契約がない場合に、契約を執行するという表現が適切ではないケースもあるかもしれない）。

また、「自然人及び法人に送金の許諾をするときと異なり、スマートコントラクトは、基本的にプログラムが公開されており、特定の処理しかできないことを実行前に検証することができる、第三者のエージェンシーリスクを一切勘定することなくエスクロー処理を実装することができる」ものであると説明される⁽³⁴⁾。契約内容や取引履歴、所有権等を管理しながら、条件が整ったときに自動的に契約内容を実行し、その結果をブロックチェーン上に記録するプログラムであるスマートコントラクトは、分散型台帳（ブロックチェーン）と共に DeFi の分散性ないし管理者不在の仕組みを支える重要なツールである⁽³⁵⁾。

5 分散性がもたらす税務執行上の問題

税務当局にとって、暗号資産の分散性は、納税者の情報が集積するインフォメーションハブや源泉地国の課税権を確保するための源泉徴収代理人のような者に依拠できないという問題を引き起こす。本稿では、分散型の金融システムにおいては、税務当局が金融機関等の仲介者から利用者の情報を収集するような既存の枠組みが機能不全に陥る可能性があることに注目する。

伝統的な金融システムでは、仲介者である金融機関は租税制度の中で2つの役割を演じてきた。所得の稼得者や資産の保有者の居住地国に CRS (Common Reporting Standard : 共通報告基準) などに基づいて情報を提供する「情報保有者」としての役割と、源泉地国の課税権を確保するための「源泉徴収代理人」としての役割である。しかしながら、DeFi エコシステムでは、取引当事者をマッチングさせるような仲介者は存在せず、仲介業務の多くがアルゴリズムベースで行われる⁽³⁶⁾。このような場合、上記のような役割を演じる者が不存在か、そのような

(32) デジタル・分散型金融への対応のあり方等に関する研究会・前掲注(28)2-3 頁。

(33) 北條真史=鳩貝淳一郎「暗号資産における分散型金融—自律的な金融サービスの登場とガバナンスの模索—」日銀レビューNo.21-J-3(2021)1 頁及び 8 頁の脚注(2)。

(34) 落合涉悟「ゼロ知識証明を用いたトークン匿名授受システムの概要と介入余地分析」アコードタックスレビュー17=18 号掲載予定。

(35) 谷口栄治「DeFi(分散型金融)の拡大と指摘される金融リスク」リサーチ・フォーカス No.2022-009(2022)3 頁(<https://www.jri.co.jp/MediaLibrary/file/report/researchfocus/pdf/13468.pdf>)。

(36) See Bob Michel & Tatiana Falcão, *OECD (2022) Public Consultation on the Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard: Comments by B. Michel and T. Falcão* 9(2022), <http://dx.doi.org/10.2139/ssrn.4266327>.

者の特定が困難となり、法的管轄も不明確なものとなり⁽³⁷⁾、円滑な税務執行が立ち行かなくなる可能性がある。

補足すると、暗号資産のシステム自体は匿名性を提供するものであるが、ピアツーピア方式では不特定多数の利用者間での取引は進まず、流動性の確保等が課題となる。そのため、取引を仲介・促進する役割を果たすサービスの需要が高まるが、このようなサービスを提供する事業者が、本人確認規制やマネーロンダリング・テロ資金供与規制に従って利用者の情報を収集する中央集権的機関であると、暗号資産の匿名性は減退する。

一方、DeFi の中心的な存在である DEX は、スマートコントラクトを介して利用者間の取引を実現し、仲介者を介在させない仕組みやサービスを提供している。DEX は、通常、利用者の身元に関する情報を収集しない。もっとも、DEX の開発や運営等に関与する「者」が存在することは通常であるし、DEX が提供しているのは「仲介業務」であると理解することもできる。しかし、その目指すところは、利用者の暗号資産を管理したり、権利義務の帰属主体となりうる「者」を介在させることなく、上記のようなサービスを提供することにある。

このように DEX は、暗号資産の匿名性を維持しつつ、その取引を活発化させるものであるが、DEX を利用したトランザクション履歴はブロックチェーン上に記録されるため、税務当局を含む外部の者がこれを確認することは可能である。この意味で暗号資産の追跡可能性と透明性が維持されている。この点については、CEX の内部で行われた取引はオフチェーンで管理され、直接的にはブロックチェーンに記録されていないため、暗号資産の追跡可能性や透明性が損なわれていることと対比して理解しておくべきである。

振り返れば、金融システムの文脈に限らず、従来、税務当局は、情報提供者や源泉徴収義務者としての役割を果たすことを期待できる企業、金融機関、役所などの中央集権的機関を、納税者の税務コンプライアンスを確保するために利用してきた。分散型のシステムは、このような税務当局が中央集権的機関に依存する構造を機能不全に陥らせる可能性を有している⁽³⁸⁾。

「仲介業務を担う」者が存在しないだけでなく、税務当局が依拠できる「者」、責任を持って役割を果たすことができる「者」が存在しない完全な分散型のシステムの前で、既存の税制は見直しを求められる。

この点について、筆者は別稿において、分散型デジタル社会、とりわけ中央集権的機関がおらず（取引に権利義務や納税義務の帰属主体が介在せず）、トラストレスで匿名性が確保されているような分散化が進んだ環境下でグローバルに価値の移転が繰り返される世界がもたらす課税上の問題を取り上げた。また、税制との関係において注目されるかかる社会の基盤となるブロックチェーンや人間による介入なしに、コード化された通りの操作を実行することで取引を処理するスマートコントラクトがもたらす影響等を考察した⁽³⁹⁾。これに対し、本稿では主として税務調査を中心とした執行上の問題を考察するものである。

(37) デジタル・分散型金融への対応のあり方等に関する研究会「事務局説明資料」6 頁(2022.6.20) (<https://www.fsa.go.jp/singi/digital/siryou/20220620/jimukyoku.pdf>)は DeFi の技術・性質がもたらす規制上の問題点等として、①規制遵守の責任を負う者の特定が困難、②DeFi のグローバルな性質から適用される法的管轄が不明確、③違法行為、マネーロンダリング、テロ資金供与又は制裁措置の回避を誘引、④金融安定に対するリスクの存在があるとしている。

(38) Avalos, *supra* note (11), at 67.

(39) 泉・前掲注(14)159 頁以下。

6 CARF とその限界

OECD も暗号資産の台頭がもたらす問題の対応に取り組んでいる。上述のとおり、暗号資産は従来の仲介機関を介さずに移転や保有できるものであり、税務当局が暗号資産の取引等の状況を把握することは難しい。こうした状況により、税務当局はその管轄内で行われた課税に関する活動の把握が難しくなり、関連する納税義務が適切に履行されているかを確認することが困難になっている。このことは、CRS によってもたらされた世界的な課税の透明性の向上という成果が徐々に損なわれていくという重大なリスクをもたらす。また、個人が暗号資産についてプライベートウォレットで保有し、グローバルにそれを移転できることは、暗号資産が違法行為に利用されたり、納税義務を回避するために使用されるリスクをはらんでいる⁽⁴⁰⁾。

そこで、OECD は、2022 年から 2023 年にかけて、暗号資産取引に関する税務情報を、納税者の居住地国との間で、標準化された方法により、自動的に交換することで課税の透明性を確保する世界的な枠組みである CARF (Crypto-Asset Reporting Framework : 暗号資産等報告枠組み) を策定した。情報交換の対象となる税務情報には、暗号資産の残高情報は含まれていないものの、利用者や事業体に係る実質的支配者の氏名、住所・所在地、居住地国、納税者番号、生年月日、出生地のほか、報告対象となる暗号資産⁽⁴¹⁾の種類、法定通貨による購入や売却、

⁽⁴⁰⁾ See OECD, PUBLIC CONSULTATION DOCUMENT: CRYPTO-ASSET REPORTING FRAMEWORK AND AMENDMENTS TO THE COMMON REPORTING STANDARD 4-5(2022); OECD, INTERNATIONAL STANDARDS FOR AUTOMATIC EXCHANGE OF INFORMATION IN TAX MATTERS: CRYPTO-ASSET REPORTING FRAMEWORK AND 2023 UPDATE TO THE COMMON REPORTING STANDARD 11-12(2023).

⁽⁴¹⁾ CARF は暗号資産(Crypto-Asset)を「暗号化の方法により保護された分散型台帳又は類似の技術に依拠して取引の検証及び安全性の確保を行う価値のデジタル表現」と定義し、ここから中央銀行デジタル通貨、特定電子マネー商品（一定のステーブルコイン）、RCASP が支払や投資の目的として使用できないと適切に判断した暗号資産を除いたものを報告対象暗号資産 (Relevant Crypto-Asset) と定義している。「価値のデジタル表現」とは、暗号資産が価値に対する権利を表章しており、所有権 (ownership) 又は権利がデジタル方式で他者と取引可能、他者に移転可能であることを意味する。例えば、暗号技術に基づいて生成されたトークンで、個人が価値を保管し、支払を行うことを可能にするものであり、他者に対する会員資格の請求権や権利、財産権、その他の絶対的又は相対的な権利を表さないものは暗号資産である。さらに、個人又は事業体に対する会員資格の請求権や権利、財産権、その他の絶対的又は相対的な権利（例えば、所定の日付、価格、その他の事前に定められた要素で、金融資産や暗号資産を含む資産を購入又は売却するためのセキュリティトークン、デリバティブ契約又は権利）であり、デジタル方式で法定通貨又は他の暗号資産と交換可能な場合、これも暗号資産である。OECD, INTERNATIONAL STANDARDS *supra* note (40), at 22, 49. 具体的には、ビットコインなどの典型的な暗号資産だけでなく、法定通貨建のものも含むステーブルコイン、暗号資産の形態で発行されたデリバティブ、ファンジブルなトークンにとどまらないデジタル方式で他者と取引できる収集品、ゲーム、芸術作品、物理的な財産、金融関係の書類に対する権利を表章するような一定の NFT (実際に支払目的や投資目的で使用できる NFT) など、伝統的な金融仲介機関を介さずに分散型で保有及び移転できる資産を包含するものである。Id. at 13, 50-51. このような暗号資産それ自体の定義は、日本の資金決済法上の暗号資産の定義よりも広いものである。

暗号資産の交換、受領及び移転に係る暗号資産の名称、総額、総数量、件数などが含まれる⁽⁴²⁾。また、暗号資産の移転は、後述する RCASP が認識している限りにおいて、無償で暗号資産を配布する行為であるエアドロップ、暗号資産を運用等するステーキング⁽⁴³⁾、レンディングなどの取引タイプに分類される。CARF による情報交換は 2027 年から開始される予定であり、日本においても 2024（令和 6）年度税制改正で CARF に準拠した非居住者に係る暗号資産等取引情報の自動的交換のための報告制度（日本版 CARF）が導入された（2026 年から施行予定）（実特法 10 の 9 等）⁽⁴⁴⁾。

CARF の骨組みは、中央集権的な機関を情報提供者として想定し、顧客及び取引に関する情報を収集し、税務当局に対する報告義務を課すなどの点で CRS にならうものである。他方、そのような義務を課せられるプレーヤーは自動的情報交換制度の経験のない暗号資産サービスプロバイダーである⁽⁴⁵⁾。暗号資産の利用者の多くは、CEX を通じて取引や保有を行っているため、CARF は税務執行において相応の効果を発揮することが期待される。この場合であっても、

⁽⁴²⁾ OECD, PUBLIC CONSULTATION DOCUMENT, *supra* note (40), at 4-5; OECD, INTERNATIONAL STANDARDS *supra* note (40), at 11-12, 14, 18-19, 34-35. プライベートウォレットのアドレスに関わる問題については、後掲注(72)参照。

⁽⁴³⁾ ステーキングという用語は、特定のブロックチェーンや暗号資産等のシステムが分散型の合意を達成するため用いる POS (Proof of Stake) というコンセンサスメカニズムに由来する。POS では、バリデータはシステム内のスマートコントラクトに資本や価値を移転又はステーク（一種の預入れ）する。このステークされた価値は、担保として機能し、全体的なコンセンサスメカニズムやシステムセキュリティにとってマイナスとみなされるような事前に合意された特定の行動（不誠実な又は怠慢といえるような行動）をバリデータがとった場合にその全部又は一部がペナルティとして没収される。バリデータは、ネットワーク上でブロードキャストされた新しいブロックの有効性を検証し、場合によっては新しいブロックを生成し、それをブロードキャストする責任を負う。バリデータは、ブロックの提案や検証などのプロセス及びセキュリティへの貢献に対して報酬（多くの場合、新しい暗号資産等）を受け取る。ただし、最近では、ステーキングという用語が市場参加者によって、より広義で曖昧な意味で使用されるようになっている。ステークした参加者が積極的な貢献を一切行わない場合や、ステークされた資本や価値がリスクにさらされていない場合でも、単に報酬と引き換えに一定の資本や価値をスマートコントラクトに移転又はロックすることを指す場合がある。UK LAW COMMISSION, *supra* note (1), at xv; ETHEREUM.ORG, *Blocks* (last updated May 26, 2024), <https://ethereum.org/en/developers/docs/blocks/>.

⁽⁴⁴⁾ クロスボーダーの取引情報アクセスのためのものである CARF と異なり、法定調書など日本居住者の取引情報アクセスのための包括的な措置は講じられておらず、このままではバランスを大きく欠いてしまうため、CARF 実施のための制度を日本国内法に導入する場合、居住者についても同様の情報アクセスを可能にする仕組みを検討する必要があり、また事業者の負担の観点からは、別の制度の導入によるのではなく、CARF の枠組みの下、居住者・非居住者の区別なく扱う対応が考えられるという指摘がなされている。岡直樹「富裕層・暗号資産と税金（OECD の取り組みと展望）」東京財團研究所（2022.11.29）（https://www.tkfd.or.jp/research/detail.php?id=4117#_ftnref8）。なお、日本版 CARF では、暗号資産等取引を行っている日本の居住者も暗号資産交換業者等に氏名や住所等を記載した届出書を提出する義務があるが、この届出書は居住地国の特定手続に利用されるものであり、税務当局からの提供要請がないにもかかわらず、当該者に係る身元や暗号資産等取引の情報が当該交換業者等から税務当局に提供されるものではない。

⁽⁴⁵⁾ CARF が「Old Tricks for New Dogs」と表現される所以である。See Paul Foster Millen & Peter A. Cotorceanu, *Old Tricks for New Dogs: The OECD's Cryptoasset Reporting Framework*, 112 TAX NOTES INT'L 345, 345 (2023).

多くの利用者が税務当局に対する匿名性の確保にそれほど関心を持たない国・地域においては、CARF による捕捉を回避するために本人確認のない海外 CEX や DEX に大規模な移行が行われるような事態は生じない可能性がある。

CARFにおいて、顧客から提出された自己証明書の妥当性を確認し（デューデリジェンス）、税務当局に上記の報告義務を負うのは RCASP (Reporting Crypto-Asset Service Provider) と呼ばれる暗号資産サービスプロバイダーである。RCASP は、事業として、顧客のため又は顧客に代わって交換取引（報告の対象となる暗号資産と法定通貨との交換及び報告の対象となる暗号資産同士の交換）を実行する（effectuate）サービスを提供する個人又は事業体である。RCASP には交換取引の相手方又は仲介者として行動する者や取引プラットフォームを提供する者が含まれる。他方、単に、暗号資産の保管や移転に係るサービスを提供する者、ブロックチェーンのトランザクションの検証をする者（マイナーやバリデータ）、ソフトウェアやアプリケーションを作成又は販売する者は含まれない⁽⁴⁶⁾。純粋なカストディアンやウォレットサービスプロバイダーは RCASP に該当しないことになる⁽⁴⁷⁾。

個人又は事業体は、取引プラットフォームに対して支配力（control）を有し、又は十分に影響力（sufficient influence）を有している限りにおいて、当該プラットフォームを提供しているとみなされ、RCASP として報告義務を課せられる。このため、DEX と称している取引所の関係者が RCASP に該当すると認定されるケースもあると考えられる。上記の支配や十分な影響力の判断は 2012 年の FATF 勧告及び関連するガイダンスと整合的な方法により評価される⁽⁴⁸⁾。FATF 基準によれば DeFi アプリケーション（すなわちソフトウェアプログラム）は VASP に該当しない⁽⁴⁹⁾。ただし、上記の支配力や影響力の定義、該当者が存在する場合の適用のあり方は必ずしも明確ではなく、DEX によっては RCASP に該当しないように運営される可能性

⁽⁴⁶⁾ OECD, INTERNATIONAL STANDARDS, *supra* note (40), at 22, 53-54.

⁽⁴⁷⁾ Raffaele Russo et al., *Approval of the Cryptoasset Reporting Framework Is a Step in the Right Direction*, 108 TAX NOTES INT'L 567, 569 (2022).

⁽⁴⁸⁾ OECD, INTERNATIONAL STANDARDS, *supra* note (40), at 54, 68. CARF が手本としている FATF の勧告やガイダンスによれば、規制当局は、DeFi について、CARF の RCASP に相当する VASP (Virtual Asset Service Providers) に対応する主体を特定し、責任主体を捕捉するための規制枠組みを作る必要がある。もっとも、DeFi が分散化や分散型の看板を掲げていてもそれは名目的なものであるケースがある一方、DeFi のアレンジメントに対して支配力や影響力を行使しており、VASP に該当する個人又は事業体を特定することは困難を伴うケースもある。See FATF, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, 27-28, 31-32 (2021); FATF, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS/VASPs 27 (2024); FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 137-138 (2012, rev. 2023). なお、FATF の基準自体は技術中立の立場をとっているため、FATF は VASP の活動に係る基盤技術を規制しようとしているわけではなく、所定の活動を他の自然人又は法人に代わって事業として行うような技術の背後に存在する自然人又は法人を規制しようとしている。FATF, UPDATED GUIDANCE, *supra*, at 22, 24, 31-32.

⁽⁴⁹⁾ FATF, UPDATED GUIDANCE, *supra* note (48), at 27.

もあることから、より詳細な解釈・適用に関するガイダンスが待たれる⁽⁵⁰⁾。

併せて、結局、DeFi のアレンジメントに対して、支配力や影響力を行使する個人又は事業体を特定することは依然として困難であることが認識されていることも理解しておく必要がある。すなわち、多くの DeFi のアレンジメントは分散化を標榜しているものの、それは名目上のものにすぎないと考えられている。他方で、FATF 基準を DeFi のアレンジメントに適用する際には、特に規制上のアンカーポイントの特定のほか、DeFi プラットフォームの所在地、運営場所及び／又はライセンス取得や登録・届出の状況の特定に関して、依然として規制上の課題があると認識されている⁽⁵¹⁾。RCASP に該当しない者をあたかも該当するかのように当局が規制の圧力をかける事態も懸念される。

DEX の関係者の中に RCASP に該当する者が存在しない場合には、報告義務が課せられる主体が存在しないため、CARF は効果を発揮できない。これは暗号資産の分散性に関わる問題であるところ、DEX の分散性の程度について、分散性の意義や評価指標は複数存在しうることからすると、税務執行の文脈において単に抽象的な分散性の議論を取り上げるだけでは十分ではない。ここでは指摘にとどめるが、伝統的な金融機関と同様の役割を果たすべき又は果たすことが可能であると認められる者が DEX の関係者の中に存在するかどうかという観点から、規制の策定と執行の各場面で向き合うことになると考える。

また、暗号資産の利用者が、CARF に参加しない国⁽⁵²⁾の CEX を通じて取引を行っていたり、仲介者に依存する CARF による捕捉を回避するために CEX や DEX などの仲介サービスを利用せずに⁽⁵³⁾、RCASP に該当しないウォレットサービスプロバイダーが提供するプライベート

⁽⁵⁰⁾ See Raffaele Russo et al., *The EU DAC8: Tax Transparency in Sight for Cryptoassets*, 111 TAX NOTES INT'L 153, 158(2023); Peter A. Cotorceanu & Paul Foster Millen, *Old Tricks for New Dogs, Part II: The OECD's Cryptoasset Reporting Framework*, 114 TAX NOTES INT'L 203, 206 (2024); Noam Noked, *Ending the Crypto Tax Haven*, 15 Harv. Bus. L. Rev. 171, 194, 209 (2025). なお、DAO(Decentralized Autonomous Organization：分散型自律組織)自体は、パートナーシップ又はその他の法的アレンジメントとして、CARF の目的上、事業体とみなされる可能性がある。Id. at 194.

⁽⁵¹⁾ FATF, TARGETED UPDATE, *supra* note (48), at 27.

⁽⁵²⁾ 2025 年 3 月 25 日現在、68 の国・地域が 2027 年又は 2028 年に情報交換を開始するの間に合うようCARF を実施することを約束している。OECD, *Jurisdictions Committed to Implement the Crypto-Asset Reporting Framework (CARF) in Time to Commence Exchanges in 2027 or 2028 as Part of the Global Forum's CARF Commitment Process* (2025), <https://web-archive.oecd.org/tax/transparency/documents/commitments-carf.pdf>. 暗号資産取引量やウォレット保有数量が比較的多い発展途上国 (OECD 非加盟国)との関係で CARF の枠組みがうまく機能するかという問題が指摘されている。See Michel & Falcão, *supra* note (36), at 3-5. オフショアの CEX の利用が拡大する場合には、これらの CEX の所在地国が CARF に参加するかどうかが CARF の有効性を決定づける重要な要素となる。そして、CARF 参加国の拡大が国際的な暗号資産の透明性を高める 1 つの鍵となる。

⁽⁵³⁾ IRS は、取引に関する必要な情報にアクセスできる DeFi 参加者を、単に「人間とのやりとりではなく、ソフトウェアを通じてサービスを提供している」という理由だけで、情報申告制度の対象外とすることを認めないとする立場である。このような除外は、次のような意図しない影響をもたらす可能性があると考えているからである。

- ・情報申告制度は、納税者の収入に関する情報を IRS と納税者の双方にオーブンにすることで、納税者のコンプライアンス水準を向上させる効果があるが、この制度の実効性が低下する可能性がある。
- ・納税者にデジタル資産の取引方法を変更するインセンティブを与え、意図しない行動を促す恐れがある。

ウォレット⁽⁵⁴⁾を利用して取引を行っている場合にも CARF は有効に機能しない⁽⁵⁵⁾。注目すべきことに、本人確認を行わない又は行っていても他国の税務当局が情報交換を期待できないような CEX は、税務当局からするとブラックボックスであり、利用者の身元や取引内容に関する情報を把握する手段がかなり限定されるため、DEX よりも深刻な課題を提起する。一般に、CEX から外部のウォレットアドレスに暗号資産を送付する際、送付元アドレスは、利用者専用のアドレスではなく、CEX が管理する CEX のアドレスが使用される。また、利用者が CEX 内部で行った取引はブロックチェーンに記録されるのではなく、CEX の内部データベースで管理される。このため、ブロックチェーンの記録だけでは特定の利用者の取引内容を把握することができず、利用者や CEX の協力がない限り税務当局が取引内容を確認することはできない⁽⁵⁶⁾。この点で、CEX の内部取引は第三者からするとブラックボックスである⁽⁵⁷⁾。

これに対して、DEX では利用者の身元情報は収集されていないが、取引はスマートコントラクトを通じて行われ、そのトランザクションの記録はブロックチェーン上で公開される。この点で、透明性があり、税務当局もブロックチェーン上のデータを利用してトランザクションを追跡することが可能である。また、多くの DEX はオープンソースで開発されており、その仕組みやスマートコントラクトが公開されているため、DEX に関しては、取引のプロセスやトランザクションに関する内容を検討する際に有益な情報を比較的容易に入手することが可能である。

-
- ・自主的な納税の履行を阻害し、デジタル資産の取引に係る所得を適正に申告していない納税者を特定するための IRS の執行努力を妨げるリスクがある。

このような理由から、IRS は情報申告制度の適用範囲を広く確保する必要があると考えている。T.D. 10021, 89 Fed. Reg. 106928, Summary of Comments and Explanation of Revisions Part II.B.2 (Dec. 4, 2024).

⁽⁵⁴⁾ ただし、Metamask や Ledger などのウォレットプロバイダーも、顧客に対して交換サービスを提供している場合には RCASP とみなされる可能性がある。

⁽⁵⁵⁾ この辺りの議論について、Noked, *supra* note (50), at 191-197; Baer et al., *supra* note (18), at 492 参照。なお、CARF は暗号資産経済の大部分を捕捉することであること及び CARF が成功するかどうかは、立法の起草に関する問題ではなく、それを広く解釈し、執行するという政治的意志の問題であることを指摘するものとして、Marian, *supra* note (6), at 29 参照。堀治彦「暗号資産に関する税務情報交換制度に関する覚書」東北学院大学経営学論集 22 号 (2024) 10 頁は、CARF により、報告義務を持つ事業者が税務当局に報告を行ったとして、従来の国際的情報交換の枠組みと同様の機能を発揮できるか否かが注視されるべきであるとする。

⁽⁵⁶⁾ このような CEX 内部で行われている取引を把握することにより、税務当局は、暗号資産の課税対象であるキャピタルゲインの相当部分を捕捉できるという見解として、Thiemann, *supra* note (15), at 91 参照。

⁽⁵⁷⁾ ブロックチェーンゲームも同様にブラックボックスの性質を有する場合があるがここでは取り扱わない。ブロックチェーンゲームを利用した場合において、オフチェーン取引の履歴が取得できない問題を指摘するものとして、藤本剛平「暗号資産・NFT の税務計算の問題点—青色申告を中心に—」アコードタックスレビュー17=18 号掲載予定参照。ブロックチェーンゲームの課税関係について、泉絢也「ゲームプレイ・仮想空間における活動と所得課税—MMORPG に関する米国の議論を参考として—」アコードタックスレビュー17=18 号掲載予定参照。

7 日本における状況と国税庁が直面する問題

日本の暗号資産取引や税務執行の現状を踏まえて、国税庁が直面する税務執行上の問題を考察する。

(1) 暗号資産の利用者の増加

2023 年のメルカリ（メルコイン）の参入により暗号資産の国内口座数が飛躍的に増加し、2024 年 4 月末までに 1000 万を超えていた（ただし、稼働口座は約 600 万である）⁽⁵⁸⁾。同社によれば、メルカリのビットコイン取引サービスの暗号資産口座数は、口座数を公表している各暗号資産交換業者を超える水準に達している。さらに、利用者の 83% が暗号資産取引を初めて行う層であり、新たな層の顧客を開拓することに成功したとされる⁽⁵⁹⁾。

同社のサービスは、メルカリのアプリを使って簡単な操作だけで暗号資産を取引できる仕組みとなっている。不用品を売った売上金で暗号資産を購入できる、暗号資産の売却代金を使ってメルカリで買い物ができる、さらには暗号資産の積立てが可能であるといった特徴を備えており、初心者でも簡単に暗号資産取引を行うことができる。もともと、メルカリの利用者層は若年層に限らず全世代に広がっており、普段投資をしていない人でも気軽に暗号資産に投資ができる場を提供している。このため、今後も同社のサービスを通じて暗号資産取引の利用者が増加する可能性がある。

これにより、これまで収入が少ないと認められていたため確定申告を受けていたため確定申告をする必要がなかった人々が、暗号資産で利益を得ることで、確定申告をしなければならなくなるケースが増加する可能性がある。確定申告に不慣れで、取引の記録を適切に管理できない納税者においては、税金を申告しない、あるいは正しく計算できないといった事態が生じ、税務コンプライアンス違反のリスクが高まることが懸念される。

これに対して、国税庁としては、例えば、米国の Form1040 に見られるような暗号資産関係の収入の有無をセルフチェックさせる項目を確定申告書等に設けるほか⁽⁶⁰⁾、暗号資産の税務に関するガイド（FAQ 等）の充実化、これをベースにしたチャットボットサービスの提供、CEX 等への適正申告のための協力要請など、納税者が適正に申告を行うための環境を整備することが考えられる。加えて、税務調査による税務コンプライアンスの確保も重要である。その際、日本では顧客の本人確認手続を実施している国内 CEX が暗号資産取引の場を提供しており、市場で大きな役割を果たしているため、まずは国内 CEX を起点に調査を展開することが

⁽⁵⁸⁾ 一般社団法人日本暗号資産等取引業協会が公表している暗号資産取引月次データ(<https://jvcea.or.jp/about/statistics/>)参照。

⁽⁵⁹⁾ 株式会社メルコイン HP(https://about.mercoin.com/news/20240411_bitcoin2m/)。

⁽⁶⁰⁾ このようなチェックボックスによるナッジ的手法は、暗号資産の収入がある納税者が「収入がない」ことを意味する「いいえ」の項目にチェックを入れた場合、その申告漏れを「不注意による見落とし」から「積極的な隠蔽」に変える側面を有することについて、Haozheng Jiang & Henry Ordower, *Cryptocurrency Public Key Reporting: Using Embedded Technology to Aid Tax Compliance*, 185 TAX NOTES FED. 2119, 2125 (2024) 参照。

予想される⁽⁶¹⁾。

まず、税務調査の対象者を選定する調査選定の場面では、特定事業者等への報告の求め（通法 74 条の 7 の 2）や事業者等への協力要請（通法 74 の 12①）等を利用して⁽⁶²⁾国内 CEX から利用者の身元や取引履歴等の情報及び資料入手することが考えられる⁽⁶³⁾。特定事業者等への報告の求めを利用すると、例えば、国内 CEX に対して、「〇年〇月〇日～〇年〇月〇日の期間において、取引金額が■■■円以上の暗号資産取引を行っている顧客」の情報を報告させることができる。これは、特定の調査対象者を指定して情報を求めるなどを前提とせず、「取引金額が■■■円以上の暗号資産取引を行っている顧客」全員の情報の報告を求めるなどを可能とする制度である。他方、個別の税務調査の場面では、国税庁は、質問検査権（通法 74 の 2）に基づいて、調査対象者本人からだけではなく、その利用している国内 CEX から同人の取引情報等を入手することができる⁽⁶⁴⁾。

(61) 自身の身元に関する情報を保有する国内 CEX 等とのつながりを断ち、いわばスタンダロン状態で海外 CEX やプライベートウォレットを利用している納税者の暗号資産取引を捕捉することは非常に困難である。このような納税者は暗号資産のリテラシーが高く、一般的なマス層には含まれないため、税務執行上の取組の優先順位が低くなる可能性がある。しかしながら、このような納税者の税務コンプライアンスリスクは非常に高いため、決して放置されるべきではなく、専門部署による適正な対応が求められる。ただし、前記Ⅱ3 のとおり、そもそも自国の居住者に係る暗号資産の利用や税務コンプライアンスの実態を把握できない現状では、各層のリスクレベルや該当する納税者数を正確に把握して、税務執行上の取組の優先順位を効果的に設定することが難しいという根本的な問題が存在する。なお、国税庁が令和 6 年 11 月に公表した「令和 5 事務年度 所得税及び消費税調査等の状況」(https://www.nta.go.jp/information/release/kokuzeicho/2024/shotoku_shohi/pdf/shotoku_shohi.pdf)の資料では、暗号資産等取引を行っている個人に対する調査の 1 件当たりの追徴税額は 662 万円であり、所得税の実地調査全体の 275 万円という金額の 2.4 倍となっている。

(62) これらの規定の意義等について、野一色直人「国税通則法上の新たな情報照会手続の意義と法的課題」税法 582 号(2019)67 頁以下参照。

(63) 国内 CEX では、本人確認規制やマネーロンダリング・テロ資金供与規制を遵守し、最近では「利用者の依頼を受けて暗号資産の送付を行う暗号資産交換業者は、送付依頼人と受取人に関する一定の事項を、送付先となる受取人側の暗号資産交換業者に通知しなければならない」というトラベルルールの運用に取り組んでいる。このため、国税庁は、国内 CEX を通じて、その利用者に関する信頼できる情報を収集することができる。他方で、国内 CEX の規制強化に伴い、利用者が外部ウォレットや他の CEX との間で入出金を行う際に、取引目的や受取人の氏名・住所地等に関する情報の提供や、追加の本人確認手続などを求められる場合がある。この結果、利用者の手間や負担が増加している上、取引が完了するまでに時間も要するようになり、一部の利用者からは利便性が低下しているとの指摘もある。このような指摘もあるが、前記Ⅱ3 で述べたとおり、種々の理由から、多くの者は国内 CEX を利用するであろう。トラベルルールについて、安河内誠=後藤出「トラベルルールに対応する暗号資産業界団体の自主規制の概要」金財 73 卷 12 号(2022)38 頁以下、島幸明「暗号資産におけるトラベルルールと犯罪収益移転防止法等の改正」消費者法ニュース 135 号(2023)106 頁以下、JVCEA「トラベルルールに関するお知らせ」(<https://jvcea.or.jp/travelrule-info/>)参照。

(64) 財産債務調書の記載を端緒として調査を展開することも考られる。所定の要件を満たし、財産債務調書を提出する義務がある者は、同調書に暗号資産も記載することになることについて、泉絢也=藤本剛平『事例でわかる！NFT・暗号資産の税務〔第 2 版〕』(中央経済社、2023)246～253 頁参照。

(2) 海外 CEX、DEX、プライベートウォレットの利用がもたらす問題

しかしながら、このような調査手法によって、暗号資産の匿名性や分散性がもたらす税務執行上の問題を完全に克服できるわけではない。まず、メルカリで暗号資産取引の経験を積んだ利用者の一部が、暗号資産取引の世界のより深いところに足を踏み入れる可能性がある。海外 CEX や DEX の中には、国内 CEX と比べて、取り扱っている暗号資産の種類が多く、取引手数料が低い一方⁽⁶⁵⁾、逆に得られる報酬が高いものや、日本で提供されていない種々のサービスを提供するものが多く存在するため、利用者にとって魅力的に映るであろう。暗号資産を自分で管理し、DEX を利用するために、プライベートウォレットを作成する者も出てくる可能性もある。

また、日本ではオンラインカジノの利用者が増加しているところ⁽⁶⁶⁾、オンラインカジノでは決済手段として暗号資産が利用されており、暗号資産を管理するためにプライベートウォレットを利用している者も多いと推察される。

暗号資産は匿名で取引が可能であり、税務調査で取引を把握されない可能性があることが、一部の利用者を強く惹きつける可能性もある。そして、ネット上には、海外 CEX、DEX、プライベートウォレットの利用の仕方をわかりやすく解説するサイトが数多く存在する。このため、一般の人でも比較的容易にこれらにアクセスするための環境が整っているといえる。既に、暗号資産について一定の知識や経験を有する人々は、当たり前のように海外 CEX⁽⁶⁷⁾、DEX⁽⁶⁸⁾や海外事業者が提供するプライベートウォレットを利用している。

もともと、本人確認を行っている海外 CEX に日本の居住者が口座を保有している場合には、国税庁は、CARF を通じて身元や暗号資産取引に関する情報を一定程度、把握できる予定である。これは、次の①及び②を前提として、国税庁が暗号資産の匿名性の壁を乗り越えたことを意味する。

①納税者が中央集権型の取引所である CEX を選択したこと

②CARF という非居住者の暗号資産等の取引情報を国内 CEX 等が税務当局に報告し、各国

(65) MEDIXS FINANCE「海外仮想通貨取引所の安い手数料比較ランキング 国内との比較・手数料の種類を解説」(2025.1.15)(<https://achs.co.jp/crypto/fee-comparison-exchange/>)。

(66) 日本経済新聞電子版「違法オンラインカジノ 337 万人利用 賭け金競輪超え 1 兆円」(2025.3.13 10:06)(<https://www.nikkei.com/article/DGXZQOUE113ZF0R10C25A3000000/>)、木曾崇「最新オンラインカジノ参加率 2.8% と推計／国際カジノ研究所」YAHOO ニュース(2024.9.11 18:11)(<https://news.yahoo.co.jp/expert/articles/f563bf4097c3416a6a2e132daca8d4b513e28cdc>)参照。

(67) 日本の居住者における海外 CEX の利用状況の参考として、中嶋美彰「日本企業が暗号資産（トークン）を発行して資金調達を行う場合の現状と問題点」早稲田大学商学学術院経営管理研究科 2023 年度学位論文(2024)30 頁(https://waseda.repo.nii.ac.jp/record/2002088/files/57223061_202403.pdf) 参照。

(68) 日本における暗号資産活動のプラットフォームタイプ別のシェアは、CEX と様々な種類の DeFi プロトコルの間でほぼ均等に分散しているという調査結果がある。Chainalysis「The 2023 Geography of Cryptocurrency Report(日本語版)」(2023)63-64 頁(<https://go.chainalysis.com/2023-geo-report-japanese-download.html>)参照。また、Chainalysis「The 2022 Geography of Cryptocurrency Report(日本語版)」(2022) 59-61 頁(https://go.chainalysis.com/rs/503-FAP-074/images/2022%20Geography%20of%20Crypto%20Report_FINAL-JP%20%281%29.pdf)、CHAINALYSIS, THE 2024 GEOGRAPHY OF CRYPTO REPORT 127 (Oct. 2024), <https://go.chainalysis.com/2024-geography-of-cryptocurrency-report.html> も参照。

当局間で情報交換する制度が有効に機能したこと

よって、上記のいずれかの前提が崩れる場合には、依然として暗号資産の匿名性の壁が立ちはだかる。税務執行面から特に問題が深刻化するのは、本人確認を行っていない CEX、DEX、プライベートウォレットが利用されている場合である。国税庁がこれらを通じて行われた取引を捕捉できたとしても、そもそもそのような CEX の口座やウォレットについて、誰が管理しており、誰に帰属しているのかを把握することは困難であるし、特定の納税者がそのような CEX の口座やウォレットを保有していることを把握することも難しい⁽⁶⁹⁾。

より具体的に調査選定と個別の調査の場面を検討してみよう。調査選定の場面では、CARF 不参加国に所在し、本人確認手続を実施していない海外 CEX は、国税庁からするとより強固なブラックボックスであり、利用者の身元や取引内容に関する情報を把握することは難しい。ただし、後述するブロックチェーン分析により、このような海外 CEX を利用しているウォレットアドレスを把握することはありうるし、このようなウォレットについて税務コンプライアンスリスクが高いものとして調査選定時に注目することは考えられる。

プライベートウォレットについても、一般に、本人確認手続を実施せずに利用することが可能であり、これを提供する事業者は中央集権的な機関に該当するとしても RCASP には該当しない可能性があるため、CARF 以外のルートで各国から情報が提供されない限り、国税庁がプライベートウォレットの利用者の身元に関する情報を把握することは難しい。複数の取引候補の中から条件が合致する者を選び、様々な種類の暗号資産の売買ができるピアツーピア取引所 (Bybit などの CEX がサービスを提供するものや、Bisq など DEX と称して運営されているものがある)⁽⁷⁰⁾においては、利用者同士が直接メッセージをやりとりし、暗号資産、銀行振込、Amazon ギフト、PayPay、LINE Pay、Wise など多様な決済手段を使って暗号資産取引をすることも可能である。この場合も利用者の身元や取引内容に関する情報を把握することが難しい。

DEX も、そのトランザクションデータはブロックチェーン上に記録され、公開されているが、利用者の身元に関する情報を収集していないため、これを利用するプライベートウォレットのアドレスの管理者を特定することはできないし、日本の居住者によって管理されているものであるかもわからない。利用者からそのような情報を得ることができる中央集権的な機関も介在しておらず、他に身元を照会できる「者」は存在しない。もっとも、DEX のトランザクションのデータは容易に把握できるため、例えば、DEX で多額の報酬を得ているプライベートウォレットに係るアドレスを特定し、調査選定に活用することはありうる。

個別の調査の場面では、国税調査官が調査中の納税者（当然ながら身元は把握済み）の保有

(69) CEX の口座の真の保有者が誰であるかを認定することは、本人確認手続を実施している CEX の場合にも問題となりうる。一方で、本人確認手続を実施していない CEX の場合には、開設された口座の真の保有者の有力な候補となる口座開設者を形式的に認知できる書面やデータが存在しないため、真の保有者の認定は一層困難なものとなる。

(70) ピアツーピア取引所では、売り注文と買い注文をペアにしてプラットフォームの資産を管理するオーダーブックを使用せず、資金の保管や取引の処理に仲介業者を挟むことなく利用者同士で直接取引ができるし、利用可能な決済手段も多様であるが、メッセージのやりとりなど取引完了までに多少の手間や時間がかかる。Bybit 「安い手数料と高い安全性を提供する P2P 暗号資産取引所 15 選」(2022.2.5) (<https://learn.bitbybit.com/ja/bitbybit-p2p-guide/best-p2p-crypto-exchanges/>)。

する海外 CEX の口座やプライベートウォレットを把握したいと考えても、事実上照会する手立てがなく、把握することができないといったケースが想定される。暗号資産の譲渡原価は平均法で算出することが原則となっている（所法 48 の 2、所令 119 の 2）。このため、CEX の口座やプライベートウォレットが 1 つでも抜けていると、その口座やウォレットに係る損益を税額計算に反映できないだけでなく、他の口座やウォレットで行った暗号資産取引に係る税額計算全体に広範な影響を与える可能性があるため、極めて重要な問題である。もちろん、これは調査選定の場面でも問題となりうる。

もっとも、個別の調査の場面においては、調査官が納税者のパソコンやスマートフォン等のデバイスの中を確認し、利用している海外 CEX、DEX、ウォレット、これらにおける取引履歴等を確認するという従来の調査手法である現物確認調査（ブロックチェーン外で実施されるという意味ではオフチェーン調査）を利用する一定程度有効である。しかしながら、暗号資産の調査ではその効果は限定的になるのではないかと考える。

ウォレットに関連づけられた秘密鍵は暗号化されてデバイスのローカルストレージ内に保存される。このような場合に、ブラウザやアプリの起動、トランザクションの送信、残高の確認などの操作画面や操作方法を他人に見せるだけでは、秘密鍵が直接的に表示されることはない。ただし、誤ってシークレットリカバリーフレーズ（シードフレーズ、ニー モニックフレーズ）⁽⁷¹⁾や秘密鍵を表示する操作を行ってしまうリスクはゼロではない。これらの情報が流出してしまうと、そのウォレットに紐づけられている暗号資産が他人に抜き取られる可能性が出てくる。

いずれにしても、プライベートウォレットを利用している人の中には、秘密鍵を管理しているウォレットの画面や管理状況等を他人に見せることに抵抗を感じる人が少くないと考える。特に、ウォレットで多額の暗号資産を管理している場合にはその傾向は顕著であろう。このような事情から、調査官がデバイスの中を確認することを拒否する納税者がいても不思議ではない。そのような場合に、直ちに検査忌避（通法 128 二）に当たると断ずることはできない。

そもそも、ウォレットの利用状況を確認するために納税者のデバイスを直接確認することに躊躇する調査官もいるであろう。調査官が納税者にウォレットの画面操作を依頼して確認を行った数日後に、当該ウォレットに紐づく暗号資産が窃取された場合、その調査官に対して疑いの目が向けられる可能性があるからである。

少し整理すると、質問検査権による調査、特定事業者等の報告の求め、CARF はいずれも課税当局への情報提供等に係る義務を課しうる国・地域内に当該義務を負担すべき者が存在する場合にのみ有効に機能するものである。また、CARF の RCASP には、単に、暗号資産の保管や移転に係るサービスを提供するような純粋なウォレット提供事業者等は含まれない。このため、海外 CEX、特に CARF に参加していない国に所在する CEX、DEX、プライベートウォレットを利用して、匿名性を保ちながら、グローバルに暗号資産の取引・運用をしている納税者の情報を国税庁が把握することは難しく、上記で示したような調査選定及び個別の調査の場

⁽⁷¹⁾ 通常、ウォレットの使用開始時に示される複数のランダムな単語とその順序で構成される単語リストのことであり、ウォレットのログインパスワードとは異なるものであるが、ウォレットに紐づいている暗号資産にアクセスするために重要なものである。ウォレットの復元（リカバリー）のために用いられる。例えば、ウォレットのログインパスワードを忘れた場合のほか、複数のデバイスでウォレットを利用するために、あるいはデバイスの紛失又はパソコンやスマートフォンの買換えのために、新しいデバイスにウォレットを復元する場合に使用する。

面における問題が起こりうる。特定取引等の報告の求めや CARF を通じて、国税庁が利用者の身元を把握できるわけではないし、特定の納税者が利用している海外 CEX、DEX、プライベートウォレットを把握することも困難である。

これらの点を考慮すると、納税者が CEX の口座やプライベートウォレットの情報を国税庁に提出することを義務付ける又は納税者に提出を促すような制度を検討すべきであるといわざるをえない。

III ブロックチェーン分析：期待と限界

1 ブロックチェーン分析とは

暗号資産の匿名性と分散性に起因する税務執行上の問題に対処するために力を発揮する調査手法としてブロックチェーン分析を取り上げる。ブロックチェーン上のトランザクションを分析することで、エンティティ（ブロックチェーン取引に関与する特定可能な個人や組織等）間のパターン、関係性、活動を特定することができる点が注目される。

ブロックチェーン（誰でも許可を得ることなく自由に参加できるパブリックブロックチェーン）上に記録された暗号資産のトランザクションは、公開されているため誰でも確認できる。よって、ウォレットのアドレスがわかれば⁽⁷²⁾、そのアドレスに関連づけられた暗号資産のトランザクションや残高、あるいは同一人物によって管理されていることが想定される CEX の口座や他のウォレットを把握することができる。ブロックチェーン分析は、暗号資産の追跡可能性・透明性に加えて、仮名性を生かした調査手法である。

もちろん、ブロックチェーンには個人を特定する情報は記録されていない。しかしながら、法定通貨を暗号資産に交換するプロセス（オンラインプ）⁽⁷³⁾とその逆のプロセス（オフランプ）では、本人確認規制やマネーロンダリング・テロ資金供与規制に従って中央集権的な機関がサ

⁽⁷²⁾ CARF は、RCASP に利用者のプライベートウォレットのアドレスの報告を義務付けるものではない。当初の草案ではウォレットアドレスも報告対象であったが、業界からの要望により変更されたようである。代替策として、税務当局はフォローアップ要請を利用して、特定のウォレットアドレスに係る情報（5 年間以上、保存する義務あり）を追加で入手することが可能であるとされている。しかしながら、5 年以上保存義務では場合によっては更正の期間制限を徒過することになるし、結局、代替策が有效地に機能せずに、プライベートウォレットと分散型アプリケーションがもたらす課税の抜け穴を放置することになりはしないかといった問題がある。See OECD, INTERNATIONAL STANDARDS, *supra* note (40), at 14, 21, 35, 48; Roger Brown & Norman Hannawa, *Reporting Obligations of the OECD Crypto Asset Reporting Framework*, CHAINALYSIS (Oct. 25, 2022), <https://www.chainalysis.com/blog/oecd-crypto-asset-reporting-framework-reporting-obligations/>; Bob Michel, *EU Ambition for DAC8 Transparency on Crypto Is Cut Short by Failure to Think Outside the OECD Box*, TAX JUSTICE NETWORK (May 25, 2023), <https://taxjustice.net/2023/05/25/eu-ambition-for-dac8-transparency-on-crypto-is-cut-short-by-failure-to-think-outside-the-oecd-box/>.

⁽⁷³⁾ オンランプ又はオフランプに含まれるかどうかに関わらず、税務当局としては、暗号資産を他の財産やサービスと交換するためのサービスを提供しているプラットフォーム等を情報源として着目して、調査を展開することが考えられる。具体例として、CEX、DEX、ウォレット、暗号資産 ATM、暗号資産デビットカード、ピアツーピアプラットフォーム、ブロックチェーンゲーム、Crypto Faucets（簡単なタスクやアクティビティ等の報酬として、少額の暗号資産を配付するオンラインプラットフォーム又はアプリケーション）、オンラインカジノ、財・サービスの提供サイトなどを挙げることができる。

ービスを提供していることが多い⁽⁷⁴⁾。このため、これらのプロセスは、ブロックチェーン上の活動と現実世界の身元を結びつける上で重要な接点である（一般に、DEX は暗号資産と法定通貨との交換サービスを提供していないことに留意）。このような状況は、法定通貨と比較して、何らかの対価として暗号資産を受け取る機会は少なく、また、暗号資産での支払が可能な場面は限られており、暗号資産の多くが主として支払手段以外の用途を持たないことによって維持されている⁽⁷⁵⁾。例えば、「①本人確認を行っていない CEX の口座やウォレットアドレス」が「②国内 CEX その他の本人確認を行っている CEX 等」と一度でもブロックチェーン上でトランザクションのやりとり（トーカンの送受信等）をしていて、かつ、①と②が同一人物によって管理されていると認定されるのであれば、①を管理している者の身元を特定できることになる。他に同一人物によって管理されていることが想定される CEX の口座やウォレットも把握できる。

国税庁は、調査選定の場面においては国内 CEX に一定の条件に合致する日本の納税者の情報を照会することで、また、個別の調査の場面においては国内 CEX に対して調査対象者の情報を照会することで、[1]「国内 CEX の口座」を把握できる。そこから特定の口座が[2]「海外 CEX やプライベートウォレット」と暗号資産のやりとりをしていることを確認した上で、ブロックチェーン分析によって、[1]と[2]が同一人物によって管理している兆候を把握できれば、[2]を管理している者の身元を特定できるし、他に同一人物によって管理されていることが想定される海外 CEX の口座やウォレットも把握できる。よって、ブロックチェーン分析は、調査選定や個別の調査の場面の双方において有効な調査手法である。

より意図的に暗号資産の匿名性を高めるツール等が利用されている場合にもブロックチェーン分析が有効に機能する。例えば、次のような場合にも、ブロックチェーンを分析することで、トランザクションや資金の流れの追跡、CEX の口座やプライベートウォレットの管理者の解明につながる可能性がある⁽⁷⁶⁾。

- ・ A というウォレットから B というウォレットに暗号資産を移動する際に、追跡を困難にするために、複数のプライベートウォレットを中間に挟んでいる場合
- ・ 様々な利用者の暗号資産を混ぜ合わせ、資金の出所や所有者をわかりにくくするミキシングサービスを利用している場合
- ・ 異なるブロックチェーンネットワーク間の資産移転をファシリテートするサービスやプロトコルを利用しておらず、トランザクションの流れが複雑化されている場合
- ・ 高度な暗号化技術を使用してトランザクションの詳細を隠す機能が備わった Monero や

(74) よって、査察部門において、警察庁の犯罪収益移転防止対策室が外国の金融情報機関(Financial Intelligence Unit)から得たマネーロンダリング及びテロ資金供与に関する疑わしい取引報告に係る情報を入手することも考えられる。

(75) ただし、高所得国における典型的な暗号資産の納税者は暗号資産を投資資産として保有し、支払手段としての使用は付隨的なものにすぎない一方、低所得国における暗号資産の納税者は、通貨代替として利用しているという見方もある。Bob Michel & Tatiana Falcão, *Cryptoization Through Currency Substitution: Tax Policy Options for Low-Income Countries*, 108 TAX NOTES INT'L 973, 975 (Nov. 21, 2022).

(76) Chainalysis「日本における暗号資産のマネーロンダリング—日本の視点から見たグローバルの共通問題—」(2024.11.21)(<https://www.chainalysis.com/blog/crypto-money-laundering-japan-japanese/>)。

Zcashなどのプライバシーコインが使われている場合

現時点では、税務当局は民間企業が提供するブロックチェーン分析ツールに頼らざるを得ないであろう⁽⁷⁷⁾。このような分析は、一般に公開されている（無料で使用できる）サイトやサービスを利用して行うことも可能であるが、例えば、ブロックチェーン分析会社として著名なChainalysisが提供している暗号資産のトランザクションを追跡するリアクターというツールを使うことで、より精度の高い分析が可能となる。リアクターに特定のウォレットアドレスを入力すると、そのアドレスと関連性のある複数のウォレットアドレスを1つのグループとしてまとめたクラスタが保有するアドレス群を認識できる。これらのアドレスがどのようなエンティティ（個人、組織、CEX、団体など）につながっているのかを確認したり、トランザクションの流れをグラフ化し、資金がどのような経路でどこに渡ったのかを明らかにしたりできる⁽⁷⁸⁾。すなわち、リアクターを使うと、次のことが可能となる。

- ①ウォレットアドレスの関連づけ（クラスタリング）
- ②クラスタ情報の把握（クラスタが保有するアドレス、クラスタ全体の資金量や取引の流れ、CEXや詐欺・マネーロンダリングに関与する組織などクラスタのカテゴリ）
- ③クラスタがどのようなエンティティと結びついているかというエンティティとの関連づけ（例えば、このウォレットアドレスは海外のA取引所であるなどChainalysisが認識しているエンティティのウォレットアドレスの情報により分析の確実性と効率性が向上）

また、リアクターは、取引の流れやクラスタ間のつながりをヴィジュアル化することで、資金がどのように移動しているかを視覚的に理解せるものであり、資金の最終移転先や保管先を突き止めたい場合にも有効なツールである。

参考として、「Bitcoin Jesus」という異名を持つロジャー＝バーが米国の国籍離脱税（Exit Tax）の脱税や虚偽の確定申告書の提出等の罪で起訴された事件の起訴状等によると、IRS（米国内国歳入庁）は、バー及びバーの企業に関連するアドレスを特定し、それらをクラスタリングすることで、バーのビットコインの保有状況を追跡した。バーは、法律事務所と鑑定人に対してビットコインの正確な保有数量を隠匿し、虚偽又は誤解を招く情報を提供していたが、クラスタ分析と他の証拠を組み合せることで、同氏に関連する4つの主要なビットコインアドレスのクラスタが特定された。その結果、IRSは、2014年2月3日時点で、バーが、直接又は自

(77) 米国財務省の担当官は、制裁逃れを含む違法行為にデジタル資産を利用する行為者の身元を特定するのに、民間のブロックチェーン分析企業との契約に大きく依存していること及び分析ツールの改善とツール数の増加により、制裁逃れの行為者やこれを促進する者に対する調査のための証拠収集能力が強化されたことを述べている。U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Economic Sanctions: Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets*, GAO-24-106178 (Dec. 13, 2023), <https://www.gao.gov/products/gao-24-106178>.

(78) アンカーテクノロジーズ株式会社 HP(<https://anchor-u.com/product/chainalysis/>)。ヒューリスティックを使用してアドレスをクラスタリングするリアクターの仕組みについて、United States v. Sterlinggov, 719 F. Supp. 3d 65, 71-77 (D.D.C. 2024)参照。

身の企業を通じて、約 13 万ビットコインを保有していたことを突き止めた⁽⁷⁹⁾。

また、米国で、初期のビットコイン投資家が、取得価額の水増し、複数ウォレット、対面取引、ミキサーなどを駆使して、暗号資産取引による 100 万ドル以上の利益の過少申告・無申告による逋脱の罪で 2 年の実刑判決を受けたという事件（暗号資産のみを理由とする脱税で刑事訴追された初めての事件）がある。この事件においても、IRS は Chainalysis のリアクターを使って納税者の資金の流れを追跡することに成功した。この納税者は、複数のウォレットを通じてビットコインを移転し、対面でのピアツーピア取引を行い、ミキサーを利用するなどしていたが、IRS の捜査官は Chainalysis のツールやデータを活用し、取引開始から処分までの流れを追跡し、日付、評価額、取引相手などの詳細を特定することに成功した⁽⁸⁰⁾。

2 ブロックチェーン分析を利用した大規模選定

ブロックチェーンに公開されている膨大な情報を最大限活用することで、大規模な調査選定に役立てることができる可能性がある。（国内 CEX ではなく）ブロックチェーン上に記録されている情報を起点として分析を行い、国内 CEX の口座と一度でもトランザクションのやりとりをしている海外 CEX の口座やウォレットアドレスをリストアップし、調査選定に利用するといった具合である。

しかしながら、リストアップされた口座やウォレットアドレスがその国内 CEX の利用者によって管理されていると直ちに断ることはできない。また、海外 CEX やプライベートウォレットと一度でもトランザクションのやりとりがある国内 CEX の口座について、コンプライアンスリスクが高いとしてやみくもに調査することは効率的ではない。効率性の観点からは、コンプライアンスリスクの高い国内 CEX の口座をフィルタリングする必要がある。

このような状況で活躍を期待されるのが Chainalysis のデータソリューションズというブロックチェーンデータの集計・フィルタリングを行うツールである。これは、ブロックチェーンのデータをシステム的に検索・集計し、目的に沿った条件に合致する取引やアドレスを特定することで、詳細な調査を行うべき対象を絞り込むためのツールである。例えば、調査選定の場面において、データソリューションズを用いて、DEX から取得したウォレットアドレスを一定の条件を設定してフィルタリングし、税務コンプライアンスリスクの高いアドレスを抽出することで調査優先度の高いウォレットを絞り込む。その後、絞り込まれたウォレットに紐づくブロックチェーン上のトランザクションについてリアクターを用いて追跡・分析し、日本の納

⁽⁷⁹⁾ See United States v. Roger Keith Ver , No. 2:24-cr-00103-MWF (C.D. Cal. indictment filed Feb. 15, 2024), <https://storage.courtlistener.com/recap/gov.uscourts.cacd.915322/gov.uscourts.cacd.915322.1.0.pdf>; U.S. ATTORNEY'S OFFICE, C.D. CAL., *Early Bitcoin Investor Known as 'Bitcoin Jesus' Indicted for Allegedly Committing Tax Fraud and Causing \$48 Million Loss to IRS* (Apr. 30, 2024), <https://www.justice.gov/usao-cdca/pr/early-bitcoin-investor-known-bitcoin-jesus-indicted-allegedly-committing-tax-fraud-and>.

⁽⁸⁰⁾ See U.S. DEP'T OF JUSTICE, *Early Bitcoin Investor Sentenced for Filing Tax Returns that Falsely Reported His Cryptocurrency Gains* (Dec. 27, 2024), <https://www.justice.gov/opa/pr/early-bitcoin-investor-sentenced-filing-tax-returns-falsely-reported-his-cryptocurrency>. Chainalysis 「Chainalysis in Action—米国における画期的な事例が暗号資産関連の脱税検査の先例に—」(2025.1.27) (<https://www.chainalysis.com/blog/case-sets-precedent-for-crypto-tax-fraud-investigations-japanese/>) 参照。

税者に該当する可能性がある者を特定することが考えられる。

さらに、暗号資産に関する税務調査のデータや税務当局の調査経験が蓄積されることにより、不正取引や過少申告の兆候を類型化できる可能性がある。AI（人工知能）を活用することのほか、各国の税務当局と知見やデータを共有することも有益である。

筆者が Chainalysis Japan 株式会社の方々にインタビューしたところによれば、これらのツールを活用することで次のようなことも可能になるようである。

- ・ 国内 CEX の口座を起点として、ブロックチェーン上、不適正な税務処理が想定される異常なパターンのトランザクションを抽出すること
- ・ プライベートウォレットに含み益のある暗号資産が蓄積されている場合において、これらがどこかに送付されたときにアラートを発する仕組みを構築すること

3 ブロックチェーン分析：期待と限界

このように、調査選定や個別の税務調査の場面において、税務当局が暗号資産の匿名性と分散性による税務執行上の課題に直面する際、ブロックチェーン分析は有効な手法となりうる。ブロックチェーンに公開されているアドレスやトランザクションの情報を分析して、本人確認を行っている CEX 等と結びつけることにより、匿名性や分散性を克服する試みである。

しかしながら、国内や海外の CEX 等のいずれに結びつけるにしても、CEX 等で本人確認が行われていることが必須である。この意味で、本人確認を行っている CEX 等からの情報に依存する特定事業者等に対する報告の求めや CARF と同様に、ブロックチェーン分析を駆使するとしても、税務当局は暗号資産の匿名性や分散性が税務執行にもたらす問題を完全に乗り越えることができるわけではない。

要するに、ブロックチェーン分析それ自体は、本人確認を行っていない CEX の口座やプライベートウォレットの管理者が誰であるのかを明らかにするものではない。このため、納税者が、本人確認を行っている CEX 等とのつながりを一切持たない形で本人確認を行っていない CEX の口座やプライベートウォレットを利用している場合には、そのような口座やウォレットの管理者を特定することはできない。この意味で、ブロックチェーン分析にも限界があるといえる。このことは、少なくとも現時点においては、CEX 等が本人確認手続を実施し、納税者がそのような CEX 等を利用していることが、暗号資産に対する適正な税務執行を確保する上で極めて重要であることを示している。

しかしながら、ブロックチェーン分析により、①「本人確認を行っていない CEX の口座やウォレットアドレス」が RCASP に限らず②「国内 CEX その他の本人確認を行っている CEX 等」と一度でもトランザクションのやりとりをしている場合、①を管理している者の身元を特定できる可能性がある。

また、そのアドレスに関連づけられた暗号資産のトランザクションや残高、あるいは同一人物によって管理されている CEX の口座やウォレットを把握することができる。このようなクラスタリングは、上記のような身元の特定の機会を増加させることにつながる。

さらに、DEX におけるトランザクション等はブロックチェーン上に記録されているから、特定のウォレットアドレスが DEX で、いつ、どのような取引をどの程度の規模で行っているかという点も把握できる。

以上のようなブロックチェーン分析は、税務当局からすれば、税務調査における強力な武器

となりうる⁽⁸¹⁾。CARF を含む国内外の規制強化に伴い、税務執行の場面において、ブロックチェーン分析の存在感は一層顕著になると予想される。よって、日本においても、暗号資産の匿名性や分散性が引き起こす税務執行上の問題に対峙するために、国税庁は高性能なブロックチェーン分析ツールを積極的かつ効果的に活用するとともに、そのために国税調査官のトレーニングを強化する必要がある⁽⁸²⁾。

IV 損益計算の困難性と税務執行上の問題

国税庁が暗号資産に関して、調査選定を効率的に行い、また、課税処分を適正に行うためには、暗号資産取引に係る損益の計算を一定の精度で行うことが必須である。しかしながら、暗号資産の損益計算は驚くほど難しい。この損益計算の困難性は、暗号資産に特有のものであり、暗号資産の匿名性や分散性が引き起こすものとは別に、現在、国税庁が直面している暗号資産に係る最も重要な税務執行上の問題である。

1 暗号資産の損益計算の手順と重要性

暗号資産取引に係る所得税は、まず、暗号資産の損益を計算し、これを基に、所得税法の規定に従って税額を計算することで算出される。この際、暗号資産取引の損益を適正（できる限り正確）に計算することが極めて重要である⁽⁸³⁾。暗号資産の損益計算は、一般に、CEX やウォレットなどから取引やトランザクションのデータを取得し、暗号資産の損益計算ソフトに取り込むことで行われる⁽⁸⁴⁾。この場合の損益計算の手順を簡単に示すと次のようになる⁽⁸⁵⁾。

(81) 課税のみならず、徴収の場面でも有益であることはいうまでもない。

(82) 現在のところ、ブロックチェーン分析は、犯罪捜査の場面で成果を上げているようである。例えば、警察庁サイバー特別捜査部と埼玉県警など 9 府県警の合同捜査本部は、秘匿性が高いとされる暗号資産 Monero を悪用しマネーロンダリングを図っていたグループについて、Monero の流れを追跡して容疑者を特定した。日本経済新聞朝刊「クレカ不正か、首謀者摘発 警察庁など 仮想通貨追跡、被害 1 億円」(2024.10.22)参照。また、暗号資産所得の申告除外者を特定するプロジェクトの一環として、IRS の不正取締局は、IRS の職員に対して、600 以上のブロックチェーン分析ツールのライセンスを取得している。IRS の犯罪捜査部門は、デジタル資産のコンプライアンス違反に対処するために分析ツールを活用し、ブロックチェーン分析企業と組んで、デジタル資産を利用して所得を隠匿することで脱税を図っている可能性のある個人を特定することに成功している一方、民事調査部門における努力は間接的で無視できる程度にすぎず、改善の余地があるという。TIGTA, VIRTUAL CURRENCY TAX COMPLIANCE ENFORCEMENT CAN BE IMPROVED, Rep. No. 2024-300-030, at 9, 14 (July 10, 2024). See also Nathan J. Richman, *There May Be Much to Learn From Trials of 'Bitcoin Jesus'*, 184 TAX NOTES FED. 124, 126 (2024).

(83) 暗号資産に関する税務処理の 95%は、収入を計算し、さまざまなカテゴリーに仕分けすることに費やされ、残りの 5%は、それぞれのカテゴリーに対する課税上の取扱いや税率を決定することに費やされるという見解として、Kirk D. Phillips, THE CRYPTO TAX BLUEPRINT: HOW TO AVOID EXPENSIVE CRYPTO TAX MISTAKES & AUDIT-PROOF YOUR TAX RETURN 9 (2023)参照。

(84) 暗号資産の取引数が極端に少ない場合には損益計算ソフトを使わずに損益計算をすることが可能だが、そのようなケースは検討の対象外とする。

(85) 暗号資産の税額計算や損益計算の流れを比較的詳細に解説するものとして、藤本剛平「暗号資産(仮想通貨)の税金計算までの流れと所得区分」税通 80 卷 2 号(2025)62-66 頁、泉=藤本・前掲注(64)448-450 頁参照。

- ①CEX で行った取引のデータや、DEX やプライベートウォレットで行った取引のトランザクションデータを取得等（API 連携の準備や CSV データの取得等）し、
- ②上記①で取得したデータを損益計算ソフトに取り込み、
- ③損益計算ソフトが示す確認を要する取引（数量エラー（ポジション不足の取引）、未対応のトークン、価格データ未取得のトークン⁽⁸⁶⁾ や年末数量不一致（残高不一致）⁽⁸⁷⁾ の問題を随時解決しながら、並行して、
- ④取引タイプ等を中心に取引の内容を確認し、取引金額、損益計上の有無やタイミング等を判断（損益取引か、貸借取引かの判断を含む）し、損益を確定

暗号資産取引に係る収入として、暗号資産の譲渡や交換、マイニング、ステーキング、レンディング、流動性供給といった様々な取引タイプに係る報酬、これらに係る必要経費として、暗号資産の譲渡原価や手数料の比重がそれぞれ大きい。このため、上記の手順を経ることによって暗号資産取引に係る収入や必要経費の多くがカバーされ、損益計算の結果はほぼ所得金額に直結することになる。

上記④の後に、損益計算の結果に基づいて課税関係を検討することになるが、暗号資産の損益計算の際に、どのような取引タイプが課税イベント（含み損益に対する課税の契機となる事象）になるか、暗号資産による支払が必要経費になるかなどの税務処理も加味して行うことが通常である。したがって、暗号資産に係る所得税額の計算過程においては、暗号資産取引の損益計算の比重が極めて大きいといえる。

これまで考察してきた税務調査の観点からみても、暗号資産取引の損益計算は重要である。ブロックチェーン分析により、同一人物によって管理されている CEX の口座やウォレットアドレス、あるいは適正に申告していないことが疑われる不審な口座やウォレットアドレスを抽出することができたとしても、申告漏れ所得金額や税額を推算するためには、結局、暗号資産の損益計算が必要となる。同様に、調査官において、調査対象者である納税者が申告していない CEX の口座やウォレットアドレスを把握したとしても、申告漏れ所得金額や税額を算出するためには、やはり、暗号資産の損益計算が必須となる。このように、調査選定と個別の調査の場面の双方で、暗号資産の損益計算の重要性が際立つ。

なお、暗号資産の会計処理のルールが固まっていないため、税法に基づく損益計算を実施している側面があることから、暗号資産の損益計算はドメスティックな性格が強いこと及び損益計算を請け負う者が税理士ではない場合に税理士法違反の問題が出てくることに注意が必要である。

2 暗号資産の損益計算に必要な知識やスキル

暗号資産の損益計算を適正に行うには、税法に関するもの以外にも、程度の差こそあれ、資金決済法などの関連法令やガイドライン、暗号資産・ブロックチェーン・関連ビジネスなどに

⁽⁸⁶⁾ 例えば、クリプタクト「未分類取引の確認と解消方法」(2025.2.19 15:08) (<https://support.cryptact.com/hc/ja/articles/360002460672-%E6%9C%AA%E5%88%86%E9%A1%9E%E5%8F%96%E5%BC%95%E3%81%AE%E7%A2%BA%E8%AA%8D%E3%81%A8%E8%A7%A3%E6%B6%88%E6%96%B9%E6%B3%95>)。

⁽⁸⁷⁾ 実務においては、③の年末数量不一致を解消するための調整処理を行うことがある。

に関する知識のほか、各種データ等の取得方法、ブロックチェーンエクスプローラーや損益計算ソフトの操作等に関するスキルが求められる。これらは、一般の税理士にとって一種の参入障壁となっている。

補足すると、ブロックチェーンのトランザクションを追跡したり、暗号資産の残高を確認したりする際に、Etherscanなどのブロックチェーンエクスプローラーを利用することがある。ブロックチェーンエクスプローラーは、ブロックチェーン上のオンチェーンアクティビティを検索等するためのユーザーフレンドリーなインターフェースを提供しており、トランザクション履歴の確認、ウォレットアドレスの検索と残高確認、ブロック情報の確認などのために利用されている。一般の暗号資産利用者がトランザクション履歴を確認する場合、ブロックチェーンエクスプローラーなどのサービスを利用することが通常である。

しかしながら、後記3及び4の考察を踏まえると、現時点では、国税庁が、複数の海外CEX、DEX、プライベートウォレットを利用している納税者に係る暗号資産の損益計算を1つの誤りもなく正確に行うことは相当難しく、やや現実的ではない。

3 暗号資産の損益計算の困難性

民間企業が提供する暗号資産の損益計算ソフトを利用したとしても、一般に、暗号資産の損益計算は難しく、海外CEX、DEX、プライベートウォレットを複数利用している場合、「正確に」計算することは困難である。また、少なくとも日本においては、複数のCEXとプライベートウォレット等を利用する事例や複雑な取引をしている事例に係る損益計算に対応できる税理士は限られている。納税者からすると種々の損益計算コストが暗号資産の利益を上回るケースもある。

これに対して、国内CEXでは取引履歴の提供等のインターフェースが整備されており、DEXやウォレットを利用している場合でもトランザクションの記録はブロックチェーン上で公開されているため、これらを入手することで暗号資産の損益計算を正確に行うことが可能ではないかと疑問に思う者もいるであろう。確かに、前記2で示した知識やスキルをある程度有していれば、国内CEXのみを利用し、暗号資産を月に数回程度、売買しているようなケースの損益計算を行うことは難しくない。

しかしながら、海外CEX、DEX、プライベートウォレットを利用している場合には、データの取得や取込みが困難であるという問題に遭遇する可能性がある。また、DEXやプライベートウォレットを利用している場合には、ブロックチェーンエクスプローラー等を用いたトランザクションの分析が必要となるため、損益計算の難易度が上がる。このようなケースでは「正確な」損益計算を行うことは不可能なことが多いというのが暗号資産にある程度精通している税理士や国税調査官に共通する理解であろう。

さらに、暗号資産の損益計算の①～④の各段階において、次のような問題が存在しており、このことが暗号資産の損益計算を一層困難なものにしている。なお、次に示す問題は、納税者が複数のDEXやプライベートウォレットを利用している場合にはさらに深刻化する。

①CEXの取引データやブロックチェーン上のトランザクションデータを取得等(API連携の準備やCSVデータの取得等)

「CEXやブロックチェーンごとにデータの取得方法等が異なる場合」がある。「海外CEXや

DEX によっては、日本語のサポートがなく、日本の税法に基づく損益計算にも対応していない場合」もある。このような場合には、データの取得等に手間取る可能性がある。

より深刻なのは「データを取得できない場合」があるという問題である。その要因として次のようなものがある⁽⁸⁸⁾。

- ・ 特定の CEX やサービスでは、API 連携や CSV ダウンロードに対応していない、あるいは特定のトランザクションデータが含まれていない、日本の総平均法に対応していないなど、取引等のデータの取得に係るサービスやサポートが十分ではない。
- ・ ブロックチェーンエクスプローラーの精度が低かったり、ブロックチェーンエクスプローラーに不具合がある。
- ・ CEX 等の破綻その他の理由によるサービス終了に伴い、過去の取引データの取得が不能となっている。
- ・ 海外 CEX では過去の取引データの取得可能期間が限定されていることも珍しくない。その場合は、サポートに連絡し、データの送付を受ける必要がある。ただし、通常とはデータの形式が異なる場合も多く、損益計算ソフトに取り込むために利用者自身でデータを加工する必要が生じる⁽⁸⁹⁾。

②上記①のデータを損益計算ソフトに取り込み（データの取り込みや API 連携）

「データを適切に損益計算ソフトに取り込むことができない場合」がある。例えば、損益計算ソフトが新たにリリースされた又はマイナーなブロックチェーン、取引所、サービス又はプロトコル（規格や技術仕様）に対応していないことがある。これは、各ブロックチェーンやサービスは独自のルールと仕様に基づいており、これらの非互換性が損益計算ソフト側の対応を困難にしていること、あるいは、一部のブロックチェーンは API やデータ提供の仕組みを備えているが、これらの仕様は統一されておらず、外部ソフトウェアがトランザクションデータを一貫性のあるフォーマットで容易に取得できるような標準化が進んでいないことを背景とする。技術革新のスピードが速く、新しいプロトコルや多様なトークン規格が次々に提案され、導入されるため、費用対効果やリソースの限界等の問題から損益計算ソフト側の対応が追いついていないという側面もある⁽⁹⁰⁾。

また、取引タイプに着目すると、例えば、異なるブロックチェーンネットワーク間で暗号資産の移転を可能にするプロセスであるブリッジ⁽⁹¹⁾や DEX への流動性供給⁽⁹²⁾に係るトランザク

⁽⁸⁸⁾ CEX の本人確認手続が厳格化され、利用者において完了した本人確認手続のレベルに応じて、過去の取引データへのアクセスが制限される場合もあるが、この場合は本人確認手続のレベルを進めて完了することにより、データへのアクセスが可能となる。

⁽⁸⁹⁾ 藤本・前掲注⁽⁸⁵⁾ 63 頁参照。

⁽⁹⁰⁾ オープンソース、モジュール設計、コンポーザビリティ（分散型アプリケーションやプロトコルがシームレスに連携して動作する性質）により、開発者はゼロから開発することなく、既存のプロトコルやコードを活用し、効率的かつ迅速に新しいブロックチェーンやサービスを構築することが可能であり、このような背景から新しいブロックチェーンやサービスを作ることが比較的容易となっている。

⁽⁹¹⁾ COINBASE, *What Is Bridging in Crypto?*, <https://www.coinbase.com/learn/wallet/what-is-bridging-in-crypto>.

⁽⁹²⁾ 流動性供給の意義や課税関係について、泉・前掲注⁽¹⁴⁾159 頁以下参照。

ションについて、損益計算ソフトが取引タイプや損益判定を正確に実行できない、判定の精度が粗いなど、損益計算ソフトにおける仕様上の制約に直面することがある。トランザクションデータの統一様式が存在しないため、異なるブロックチェーンやサービス間でのデータ統合が難しいという課題もある。

なお、国内のものに限らず⁽⁹³⁾、暗号資産の損益計算ソフトについて、同一のデータを取り込んで利用するソフトによって損益計算の結果が異なる場合があることに注意が必要である⁽⁹⁴⁾。

③損益計算ソフトが示した確認を要する取引や年末数量不一致の問題を解消

「確認を要する取引（数量エラー（ポジション不足の取引）、未対応のトークン、価格データ未取得のトークン）や年末数量不一致（損益計算ソフト等で算出された理論上の年末数量と、CEX やウォレットから提示された年末数量の不一致）の問題を解消することが難しい場合」がある。例えば、ビットコインを 3BTC 譲渡するトランザクションが存在するが、その譲渡時点で、データ上は 2BTC しか保有していないとして、損益計算ソフトにおいて数量エラーが表示される場合がある。このような数量エラーは、すべての取引データが正確に登録されていない又は登録できない場合、保有していない通貨を売却しようとするトランザクションが登録され

⁽⁹³⁾ 米国でも同様の問題があることについて、Matthew Foreman et al., *Common Sense Recommendations for the Application of Tax Law to Digital Assets*, U. OF COLO. L. LEGAL STUD. RSCH. PAPER No. 23-22, WAYNE STATE U. L. SCH. LEGAL STUD. RSCH. PAPER No. 2023-22, UC IRVINE SCH. OF L. LEGAL STUD. RSCH. PAPER No. 2024-01, SAINT LOUIS U. LEGAL STUD. RSCH. PAPER No. 2023-14, CARDOZO L. LEGAL STUD. RSCH. PAPER No. 2024-06, ARIZ. ST. U. SANDRA DAY O'CONNOR C. OF L. LEGAL STUD. RSCH. PAPER No. 4576425, 4-5 (2023), <https://ssrn.com/abstract=4576425>.

⁽⁹⁴⁾ 損益計算ソフトによって損益計算の結果が異なるのは、取引タイプごとの損益処理の相違、対応している CEX やブロックチェーンの種類や取り込み精度、利用している暗号資産の時価の相違等に起因するものと思われる。藤本・前掲注⁽⁵⁷⁾は、時価に関して、次のような問題点を指摘する。

- ・一見したところ、同一名称のトークンに見えるがコントラクトアドレスが異なることもあるところ、価格サイトに表示されているトークンの時価は単一のコントラクトアドレスに紐づくトークンの時価が示されているため、たとえ同一名称であっても異なるコントラクトアドレスである以上、これらは厳密には異なるトークンであり、暗号資産の価格サイトで取得できる時価が正しいとはいえない。
- ・DEX に暗号資産を流動性供給した際に受領する LP トークンは、流動性供給した暗号資産の時価及びプールされている暗号資産の在庫量に基づいてその価格が決まることから、その時価の把握を後日行うことは困難である。暗号資産の価格サイトにも LP トークンごとの時価情報は掲載されていないため、時価の取得ができない。

上記のコントラクトアドレスとは、スマートコントラクトがブロックチェーン上にデプロイされた際に割り当てられる固有の識別子である。例えば、DEX は、ブロックチェーン上にデプロイされたスマートコントラクトを通じてサービスを提供する。DEX に暗号資産を送付する際、利用者は、送付元として自身のプライベートウォレット(外部所有アカウント)、送付先として DEX のコントラクトアドレスを指定することで、DEX とのやりとりを実行する。外部所有アカウント(Externally Owned Account、EOA)とは、スマートコントラクトが管理するコントラクトアカウントと異なり、いわば「人」が管理し、秘密鍵によって制御されるアカウントである。

なお、藤本・前掲論文は、暗号資産の損益計算の結果を複式簿記に落とし込むことの難しさや、取引データを取得できなかった場合における青色申告承認の取消しの可能性の問題を論じている。

ている場合、前年度から保有する暗号資産の繰越処理が正確に行われていない場合、トランザクションが二重に登録されている場合などに発生するが、納税者がその原因を解明できないこともある。

また、理論上は、「年初に保有していた暗号資産の数量」と「その年中に入手した暗号資産の数量」の合計から、「その年中に手放した暗号資産の数量」を引いた分が「年末の暗号資産の数量」となるはずである。しかしながら、実際には、損益計算ソフト等で算出された理論上の年末数量と、CEX のサイト、ブロックチェーンエクスプローラー、ウォレット等で表示される年末数量が一致しないことが珍しくない。年末数量不一致の原因としては、損益計算ソフトに取り込んだ CEX やウォレットの取引等のデータに欠落や誤りがあることが考えられる。このような欠落や誤りの原因は、納税者側のヒューマンエラーによる場合もあるが、容易には特定できないことが多い。

いずれも、納税者以外の第三者が解明することは非常に難しいし、場合によっては納税者も完全には解明できないことがある。なお、ブロックチェーンの記録には、スマートコントラクトとやりとりしたもの⁽⁹⁵⁾、悪意のある第三者が勝手に無価値又は少額のトークン（いわゆる詐欺コインなど）を送りつけてきたもの、トランザクションが失敗したものなどが含まれる。このため、納税者からすると身に覚えのないトランザクションや、自身の意思で操作したのか判

⁽⁹⁵⁾ 例えば、Dan, *Why is Transaction Value Showing 0 ETH on Etherscan?*, ETHEREUM STACK EXCHANGE (Sept. 21, 2023, 10:31 PM), <https://ethereum.stackexchange.com/questions/154783/why-is-transaction-value-showing-0-eth-on-etherscan> では、約 0.12ETH を送付した際のトランザクションを Etherscan で確認したところ、その Value が 0ETH と表示されている理由がわからないという質問が投稿されている。この 0ETH という表示は、表示されているトランザクションが、他のウォレットに直接 ETH を送付するものではなく、スマートコントラクトの関数を呼び出すものであることを示している。このようなケースでは、ETH の移転は、スマートコントラクトの実行ロジックの一部として自動的にトリガーされ、スマートコントラクトの内部トランザクションとして記録される。このため、Etherscan の「Internal Transactions」のタブを確認すると、スマートコントラクト内部で約 0.12ETH の移転処理が実行されたことを確認できる。

なお、イーサリアムブロックチェーンにおいて、外部トランザクションは、外部所有アカウントから発信され、他の外部アカウントやスマートコントラクトに対してトークンの移転や操作（スマートコントラクトの関数の呼び出し）を行うトランザクションである。このトランザクションは、外部所有アカウントの秘密鍵を使用したデジタル署名によって認証され、ネットワーク上でブロードキャストされ、ブロックチェーンに記録される。他方、内部トランザクションには、外部トランザクションのように固有のトランザクションハッシュが割り振られることはなく、ブロックチェーンに直接的にログとして記録されることはない。しかし、内部取引のトランザクションレコードのデコードをサポートしているブロックチェーンエクスプローラーであれば表示される。また、内部トランザクションの結果としてトークンの移転やスマートコントラクトの状態変化が発生し、それらの結果はブロックチェーン上で更新され、場合によってはイベントログに間接的に記録される。See GEEKSFORGEEKS, *What Are ETH Internal Transactions?* (Sept. 19, 2024), <https://www.geeksforgeeks.org/what-are-eth-internal-transactions/>; GeeksforGeeks, *Normal Transactions vs. Internal Transactions in Etherscan* (Sept. 19, 2024), <https://www.geeksforgeeks.org/normal-transactions-vs-internal-transactions-in-etherscan/>; Moralis Blog, *Ethereum Logs and Events – What Are Event Logs on the Ethereum Network?* (Dec. 31, 2022), <https://developers.moralis.com/ethereum-logs-and-events-what-are-event-logs-on-the-ethereum-network/>; METAMASK, *Internal Transactions*, <https://support.metamask.io/more-web3/learn/internal-transactions/>.

断がつかないトランザクションが存在することも珍しくない。これらは直接的には損益計算に影響を与えない場合が多いが、確認を要する取引の迅速な解明を妨げる一因となっている。

④取引タイプ等を中心に取引の内容を確認し、取引金額、損益計上の有無やタイミング等を判断し、損益を確定

「損益計上の有無やタイミング等を判断することが難しい場合」がある。その要因として次のようなものがある。

- ・取引タイプが多様でそれぞれ損益処理が異なる。

暗号資産取引には、エアドロップ、マイニング、ステーキング、レンディング、流動性供給、ラップ・アンラップ、信用取引、レバレッジ、デリバティブなど様々な取引タイプが存在する。これらは、その性質や見解の相違等により、損益処理（損益計上の有無やタイミング）が異なりうる。暗号資産はボラティリティが大きいため、どの時点を損益計上すべきタイミングと考えるかによって損益額が大きく変動することに注意が必要である。また、その処理方法が確立していないものもある。他方、ブロックチェーンに記録されるトランザクションの基本系は、暗号資産の「移転」であり、一般的には、いつ、どのアドレスからどのアドレスにどの種類の暗号資産がどの程度送付されたかがわかるにすぎない。ここでいう「移転」とは、アドレス間における暗号資産の送付や受領のみならず、暗号資産の供給量が変化するミント（生成）やバーン（破棄）も含む意味での「移転」を指す。

図表に簡記したとおり、暗号資産の送付又は受領のトランザクションが発生している場合、その背後にある取引タイプや取引目的として想定されるものは多岐にわたる。しかしながら、ブロックチェーン上に記録されているトランザクションのみをもって直ちに損益取引か、貸借取引か、損益取引である場合にいつの時点でどのくらいの損益を計上すべきかを明確に又は直ちに判断することが難しい場合がある。ただし、ブロックチェーンエクスプローラーを利用して、そのトランザクションの前後関係や後述するイベントログを分析し、呼び出されているスマートコントラクトの関数や付随データを検討することにより、一定の精度で背後にある取引タイプや取引目的を判定又は推定できる場合もある⁽⁹⁶⁾。しかしながら、取引内容が複雑である場合や分析に必要なデータが不足している場合には、取引の詳細を把握することは難しい。結局、納税者が備忘記録や資料を適切に保管していることが税務コンプライアンスの観点から重要である。

図表：トランザクション別取引タイプと注意点

トランザクション	想定される取引タイプ等	注意点
[1]暗号資産の送付	単なる資金移動、ブロックチェーンゲームへの送付、法定通貨と交換、提供された財・サービスの対価の支払、贈与、ステーキ	・[1]のトランザクションのすべてが損益取引となるわけではない。ウォレットアドレス A から、ウォレットアドレス B にトークンが移転するトランザクションが起きている場合、それが単なる資金移動（両

⁽⁹⁶⁾ 開発事業者の目線として、藤本剛平ほか「座談会 現場目線で語りつくす暗号資産の税務上の問題と未来」税弘 70 卷 10 号(2022)139～149 頁〔斎藤岳発言〕参照。

	シグ、レンディング（貸付側の貸付時、借入側の返済時）、詐欺による窃取、バーンなど	ウォレットアドレスを同一人物が管理しているケースなど ⁽⁹⁷⁾ であるときには損益に影響はないが、法定通貨との交換等であるときは影響がある。
[2] 暗号資産を送付し、暗号資産等のトークンを受領（ただし、送付と受領にタイムラグがある場合もあり）	暗号資産同士の交換、NFT ⁽⁹⁸⁾ の購入、流動性供給、ラップ・アンラップ、流動性ステーキング、レンディング（貸付側がスマートコントラクトに送付し、代わりにトークンを受領又はその逆）、ICO・IEO・IDO ⁽⁹⁹⁾ など	<ul style="list-style-type: none"> ・[2]のトランザクションのすべてが損益取引となるわけではない。暗号資産同士の交換や暗号資産と NFT の交換が行われているように見えるトランザクションであっても、流動性供給やラップ・アンラップについては、損益処理をすることが妥当でないという立場も示されている⁽¹⁰⁰⁾。 ・1つのトランザクションだけではどのように処理すべきかを適切に判断ができない場合がある。例えば、IEO や NFT オークションにおいて入札のために暗号資産を送付したが、取引が成立しなかったときは、時間を置いてそれが戻ってくる。この場合、それぞれ別のトランザクションが記録されるが、いずれも損益処理は行わない。他方、取引が成立したときは、暗号資産の送付のトランザクションとは別に、時間を置いて、トークンの受領のトランザクションが発生し、損益処理を行う。いずれの場合も、実務上、損益計上のタイミングが問題になっている。
[3] 暗号資産の受領	マイニング報酬、ステーキング報酬、エアドロップ、贈与（受贈側）、レン	<ul style="list-style-type: none"> ・[3]のトランザクションのすべてが損益取引となるわけではない。 ・悪意のある第三者から無価値又は少額の

⁽⁹⁷⁾ 例えば、登録した自己保有のウォレット間のトランザクションは損益に反映させないなどの対応を損益計算ソフト側が対応していると、損益計算の手間が省ける。

⁽⁹⁸⁾ NFT とは、ブロックチェーン上で発行される唯一無二（非代替・ノンファンジブル）のデジタルトークンのこと。一般的に、NFT はそれぞれが一意の識別番号又は文字列（ぞれぞれに固有のトークン ID）を与えられており、これによって、たとえ同一のクリエイターが制作した同一コレクション内の NFT であったとしても、当該 NFT と他の NFT とが区別されるためノンファンジブルといわれる。

⁽⁹⁹⁾ ICO(Initial Coin Offering)とは、暗号資産を新規発行・販売して行う資金調達のことであり、CEX を通じて発行・販売する場合を IEO(Initial Exchange Offering)、DEX を通じて発行・販売する場合をIDO(Initial DEX Offering)という。

⁽¹⁰⁰⁾ ラップ・アンラップの意義や課税関係について、泉・前掲注⁽¹⁴⁾159 頁以下参照。なお、流動性供給の課税上の取扱いについては、上村和紀「DeFi（分散型金融）の税務上の取扱いについての一考察」税大論叢 113 号（2024）72-73 頁も参照。

	ディング（借入側の借入時、貸付側の返済受領時）、過大に見積もられたトランザクション手数料の払戻し、提供した財・サービスの対価として受領、詐欺師等からの暗号資産やNFTの受領など	暗号資産やNFTが勝手に送られてくる場合があり、ブロックチェーンのトランザクションのデータを検討する際にその検討や処理に時間を要する場合がある。
--	--	--

- 複数チェーン間の資産移動⁽¹⁰¹⁾、関連するトークンの送付と受領にタイムラグのある取引⁽¹⁰²⁾が絡むと、取引が複雑化し、損益計算処理が困難になる。

また、例えば、次のような理由から「損益計算が煩雑になる場合」がある。

- 納税者が、プログラムやボット、あるいはサードパーティの提供するサービスを利用して、暗号資産を自動で売買（事前に設定した条件やアルゴリズムに基づき、暗号資産の売買を自動的に実行）して大量の取引を行っている。ただし、取引自体は単純なので、損益計算ソフトへの取り込みの可否の問題に慣れんするという見方もありうる。
- トランザクションを実行する場合、ネットワーク利用のための手数料等を暗号資産で支払うことが通常であるが、所得税法の計算規定に合わせて損益計算しようとすると、これを利益（所得）の控除項目として取り扱うべきか否かの判断が必要となる。
- 所得税法の計算規定に合わせて総平均法を適用して計算する場合、過去の取引に遡って取得価額等を算定する必要があり、ケースによっては、非常に煩雑な計算を強いられる。他方、暗号資産を購入、売却、種類の異なる暗号資産と交換しようとする際に一時的に必要なこれらの暗号資産以外の暗号資産を取得する場合と信用取引に係る取得の場合における暗号資産の評価方法は、通常の総平均法や移動平均法ではなく、個別法となり、管理が煩雑となる（所法119の2、119の7）⁽¹⁰³⁾。

4 問題への対処方法とその困難性

上記①の段階で生じる「データを取得できない場合」、上記②の段階で生じる「データを適切に損益計算ソフトに取り込むことができない場合」、上記③の段階で生じる「確認を要する取引や年末数量不一致の問題を解消することが難しい場合」、上記④の段階で生じる「損益計上の有

(101) それぞれのチェーンで記録されるトランザクションが独立しており、全体の履歴を一貫して追跡することが難しい場合がある。

(102) どのタイミングで課税イベントが生じると考えるかにもよるが、ラップ・アンラップや流動性供給、ICOなど、トークンの送付と受領の間にタイムラグが生じる取引では、両トランザクションを適切に紐づけることができず、正確な損益計算が困難になることがある。

(103) 個別法を適用すべき場合であっても、実際には、個別法を適用していない納税者や個別法での計算結果を利用者に提供していない事業者も存在するようである。参考として、泉絢也「法人税法における暗号資産税制の問題点（1）一期末時価評価課税の改正提言」千葉商大論叢60巻1号(2022)77-81頁参照。

無やタイミング等を判断することが難しい場合」という問題への対処方法を検討してみたい。

このうち、「損益計上の有無やタイミング等を判断することが難しい場合」があるという問題を解決又は緩和するために、法令や国税庁の通達・FAQ等で手当てすることが考えられる。

また、上記問題の多くは、納税者が適切な備忘記録や証拠資料を自ら作成すること、定期的にデータをダウンロードしてバックアップを取ること、毎月損益計算を行うことなどにより、一定程度は対応できる可能性があるものと考える⁽¹⁰⁴⁾。もっとも、DEXやプライベートウォレットで様々なタイプの取引、多種類の暗号資産の取引をしている場合において、手動で記録を作成・保存することは能力や費用の観点から現実的ではない（暗号資産取引の大規模・高頻度・多様性という特徴）。

前記3で述べたとおり、ブロックチェーン上には、納税者からすると身に覚えのない、自身の意思で操作したか判断しがたいトランザクションが存在することが珍しくないため、備忘記録等を有する納税者であっても損益計算の際に戸惑うことがある。納税者が、適正申告のために、取引所、ウォレット、損益計算ソフト、顧問税理士を慎重に選択することも肝要であるが、少なくとも国内に関する限り、高性能な損益計算ソフトや暗号資産の損益計算に精通している顧問税理士の選択肢は決して多くないというのが現状である。

取引所、損益計算ソフト、ブロックチェーンエクスプローラー側の仕様等の問題については、アップデートやリリースを待つことも考えられるが、これには時間を要する。このため、更正・決定や申告に係る期限を徒過してしまう可能性があり、暫定的に手動対応が必要な場合は残る。しかも、次々に新しいブロックチェーン等が出現するので根本的な解決には至らない。

また、損益計算のためにブロックチェーンエクスプローラーを利用するにしてもいくつかの問題がある。特に、ブロックチェーンエクスプローラーは、通常、スマートコントラクト内部で発生するトークンの移転その他のアクティビティに関するイベントログ⁽¹⁰⁵⁾を利用して、トークンの移転等の履歴を追跡し、表示している。ただし、トークンが、広く使用されている標準規格に準拠していない又はブロックチェーンエクスプローラーによってサポートされていないため、ブロックチェーンエクスプローラーがイベントログを適切に解析できない場合、イベントログが出力されない場合、あるいはブロックチェーンエクスプローラーにバグがあるなどの場合には、その表示するトランザクションの履歴に欠落や誤りが生じることがある（データの不完全性・不正確性）⁽¹⁰⁶⁾。このようにブロックチェーンエクスプローラーは便利なツールで

⁽¹⁰⁴⁾適正申告のための納税者が記録しておくべき取引の例や記録すべき内容については、泉=藤本・前掲注(64)439頁参照。

⁽¹⁰⁵⁾イベントログとは、暗号資産の移転など特定のアクションや機能が実行された際にスマートコントラクトによって発行されるものであり、例えば「Transfer」などのイベント名や送信者と受信者のアドレス、移転した暗号資産の数量などが記録されたデータのこと。スマートコントラクトの内部で何が起きたかを追跡したい場合や特定のイベントに反応したい場合などに役立つ。See DUNE, *Event Logs*, <https://docs.dune.com/data-catalog/evm/ethereum/decoded/event-logs/>; Teck Yuan Lee, *Event Logs*, Etherscan (last updated Dec. 18, 2023), <https://info.etherscan.com/what-is-event-logs/>.

⁽¹⁰⁶⁾See e.g., Lucas Santoni, *Counting Crypto: The Problem of Auditable On-Chain Transaction Data*, CRYPTIO BLOG (Feb. 8, 2023), <https://blog.cryptio.co/counting-crypto-the-unique-challenge-of-retrieving-auditable-transaction-histories-from-chains>; BITQUERY, *What Are Internal Transactions & How to Get Them?*, <https://docs.bitquery.io/docs/API-Blog/what-are-internal-transactions-how-to-get-them/>.

ある一方、これを利用してもデータの不完全性や不正確性といった課題に直面することがある。

そこで、ブロックチェーンのブロックデータやステート（状態）データを取得し、独自にデータの分析や、ブロックとトランザクションの検証を実行するノード⁽¹⁰⁷⁾を利用又は自ら構築することにより、ブロックチェーンの生データを取得して適切な処理を施し、それを基にカスタムファイルを作成するなどして損益計算ソフトに取り込むことが考えられる。ただし、納税者や国税庁が自らノードを構築する場合には、適切なスペックのハードウェア、技術的な知識、さらに初期費用や維持費用が必要となるため、これが汎用的な解決策となりうるかは疑問である。

最近では、ブロックチェーンエクスプローラーではなくノードからトランザクションデータを取得したり、イベントログを解析したりすることで、トランザクションの取得や取引タイプの判定の精度を高めている損益計算ソフトも開発・リリースされつつあるため、結局、国税庁もそのような損益計算ソフトを利用することになる可能性がある（そうなると、税務調査を見据えて、納税者においても高性能な損益計算ソフトを利用しようとする動きが出てくることが予想される）。

もっとも、ブロックチェーンのデータを取得したとしても、納税者や損益計算ソフトの対応が不十分である場合には、国税庁は次のような問題に直面する可能性がある。

- ・ブラックボックスである海外 CEX の取引データを取得することができない。
- ・暗号資産の取引内容を把握することができない。
- ・損益計算の正確性を確保することができない。

取引当事者ではない国税庁にとって、これらの問題は、納税者が直面するものよりもはるかに大きい可能性がある。結局、次のような事実に複数当てはまるケースでは、国税庁が独力で（適切な資料を保存等している納税者、性能・仕様・インターフェースが税務調査に適している損益計算ソフト、暗号資産の損益計算に精通している税理士が存在しない中で）精度の高い損益計算を行うことはかなり難しいといえよう。

- ・海外 CEX、DEX、プライベートウォレットを複数利用している。
- ・納税者が適切な記録や資料を保管していないか、税務調査に協力的ではなく積極的に資料を提示等しない。
- ・正確なトランザクションデータを取得できない又は損益計算ソフトが対応していないブロックチェーンに係る暗号資産を取引している。
- ・様々なタイプの取引、多種類の暗号資産の取引を行っている⁽¹⁰⁸⁾。
- ・暗号資産の損益計算等に精通した税理士が関与していない⁽¹⁰⁹⁾。

場合によっては、次のような事態が生じうる。

⁽¹⁰⁷⁾ イーサリアムブロックチェーンにおけるフルノード及びアーカイブノードの説明について、ETHEREUM.ORG, *Nodes and Clients* (last updated Oct. 9, 2024), <https://ethereum.org/en/developers/docs/nodes-and-clients/>; ETHEREUM.ORG, *Ethereum Archive Node* (last updated Oct. 24, 2023), <https://ethereum.org/en/developers/docs/nodes-and-clients/archive-nodes/>参照。

⁽¹⁰⁸⁾ NFT など暗号資産以外のトークンも取引をしているとさらに損益計算の難易度が上がる可能性があるが、ここでは指摘をするととどめる。

⁽¹⁰⁹⁾ このような税理士は希少であるし、仮にそのような税理士が関与していても税務調査に対してどのような対応をとるかはケースによって異なる。

- ・税務調査に最適な損益計算ソフトを利用しない限り、費用や時間の面で効率性の悪い調査選定⁽¹¹⁰⁾や実地調査を強いられる。
- ・納税者が行った損益計算の正確性について、国税庁は、細部まで検証することはできず、その計算結果を受け入れざるをえない。
- ・個別の税務調査の場面で調査官が苦労して損益計算を行ったが、結局、調査官の損益計算が正確であり、納税者の計算が不正確であるとは断定できないか、両者共に自身が行っている損益計算の正確性に確信を持てない。
- ・以上から、課税処分を行おうとしても、訴訟において処分を維持できる証拠を収集・確保できない、修正申告の提出があったとしても更正の予知（通法 65①、66①等）があったといえるのかという問題が生じる。

結論として、これまでの考察を踏まえると、暗号資産の損益計算の問題への対応策として、次のような取り組みが有効であると考える。

第1に、納税者（や税理士）に対して、適正申告のために、取引又は利用する暗号資産等についての理解と選択、備忘記録や証拠資料の作成、データの定期的なダウンロードとバックアップの徹底などを働きかけることである。

第2に、国税庁が、暗号資産の損益計算のユニークさと困難性、現状の問題を十分に理解し、税務調査に最適な損益計算ソフトを開発又は利用し、これを十分に活用することである。最適な損益計算ソフトは、膨大なトランザクションやイベントログをシンプルな操作で効率的に分析し、損益取引等の高精度な判定（推定）を行う性能・仕様・インターフェースを持つものを想定する。このようなツールを活用した上で、国税調査官に対するトレーニングを実施し、これを適切に運用できる体制を構築することが、暗号資産取引における適正な税務執行を確保するための有力な方策である。

このような努力の営みを怠ると、税務執行上、大きな問題が生じる可能性がある。実際、国内 CEX のみで暗号資産を取引している場合の損益計算はさほど難しくないが、それでも「暗号資産」、「暗号資産の損益計算」と聞いただけで、ほとんど損益計算の正確性の検証や法的論点の検討をせずに、当初申告の内容や納税者又は税理士の説明を調査官がそのまま受け入れる事例が発生しているようである⁽¹¹¹⁾。また、膨大な取引の記録をデータではなく、あえて紙で提出しようとするを考える納税者や税理士もいるし、暗号資産の損益計算ソフトを利用して、所得税の確定申告を行っているにもかかわらず、損益計算ソフトのデータを税務署に渡さないように納税者に指示している税理士もいるようである（膨大な数の取引を行っている場合には税務当局による損益計算作業は困難を極める）。よって、暗号資産取引に係る資料の保管や提出

(110) なお、調査選定の場面においては、課税庁が把握したウォレットアドレス等に紐づくトランザクションに係る損益計算額を推計する必要があるから、国税庁にとって損益計算の効率性は正確性とともに重要な課題である。

(111) 紳税者が試算していた暗号資産の損益額よりもかなり低い金額を国税調査官が提示してきた事例もあるようであるが、暗号資産の損益計算は難しいため、納税者による損益の試算が正しいかを検証する余地はある。泉絢也「暗号資産 難易度が上がる損益計算 調査官の能力向上に課題大」週刊エコノミスト 103巻3号(2025)26~27頁。

方法等について、より実効性のあるルールの制定を検討すべきである⁽¹¹²⁾。

なお、国税庁は、伝統的な取引と異なり、暗号資産の場合には、「データを取得できない場合」、「データを適切に損益計算ソフトに取り込むことができない場合」、「確認を要する取引や年末数量不一致の問題を解消することができない場合」があること理解し、組織で十分に共有しておかないと、税務調査のアプローチや進行管理を含む様々な場面で適切な対応をとることはできないことに留意する必要がある。

V 結びに代えて

本稿では、暗号資産の匿名性・分散性及び損益計算の困難性がもたらす税務執行上の問題を考察した。

第Ⅱ章では、暗号資産の匿名性・分散性が引き起こす税務執行上の問題を明らかにした。

暗号資産の匿名性により、税務当局は、ブロックチェーン上のトランザクションを把握していても当事者を特定することができない、あるいは特定の納税者が保有し、取引している暗号資産も把握できないという問題が生じる。このことは、暗号資産取引の当事者について、自国における納税義務が発生しているか、発生している場合に所得金額はいくらになるのかを把握することができず、自国の居住者に係る暗号資産の利用や税務コンプライアンスの実態も把握できない⁽¹¹³⁾、などの事態を引き起こす。

暗号資産の分散性により、税務当局が依拠できる情報提出義務者や源泉徴収義務者としての役割を果たす企業、金融機関、役所などの中央集権的機関を活用する既存の税務執行枠組みは機能不全に陥るという問題が生じる。完全な分散型のシステムでは、「仲介業務を担う者」が存在せず、税務当局が依拠できる「者」も不在であることに起因する。暗号資産の取引では中央集権型の取引所である CEX が中核的な役割を果たすようになったことは、暗号資産の匿名性や分散性を減退させた。他方、DeFi、とりわけ DEX の登場によって、仲介者を介さないピアツーピアの取引が促進された結果、暗号資産の分散性はより強固なものとなり、このことが暗号資産の匿名性を補完することとなった。暗号資産の匿名性と分散性は相互に関連しつつ発展を遂げている。

暗号資産の匿名性と分散性は、コンプライアンス意識の低い納税者に好都合な環境を用意するものといえるし、これまで築き上げてきた課税の透明性の向上を図る世界的な執行体制を脅

(112) ロンちゃん「仮想通貨で儲かったら税務調査された」note ブログ(2025.1.25 21:50) (https://note.com/glad_flax6331/n/nac793a6c14ed?sub_rt=share_pb)。あえて紙の資料を提出することを検討していること、国税調査官が暗号資産取引に詳しくなく、直接的に損益計算を行うスキルを十分に有していないこと、税理士に依頼しようとしても適切な税理士が見つからないことなど、このブログで取り上げられている内容は、筆者が複数の納税者から聞いた暗号資産に係る税務調査の内容や調査後の感想と多くの点で共通するところがある。なお、銀行の入出金の記録から概算で暗号資産の損益計算を行う税理士もいるようであるが、暗号資産を年末までにすべて法定通貨に換金していない場合には、そのような計算方法では正確な損益計算額を算出することは難しい一方、このようなケースでは国税調査官も正確な損益計算額を算出することに苦労することが予想される。

(113) よって、自国の居住者がどの程度、海外 CEX、DEX、プライベートウォレットを利用しているか、あるいは暗号資産のタックスギャップや自国の居住者が保有する暗号資産の含み益がどの程度かを推計することも難しい。なお、ウェブトラフィックを利用した推計の参考として、Thiemann, *supra* note (15)参照。

かす重大なリスクをもたらす。このような認識の下で、OECD は CARF を策定した。もっとも、CARF に参加しない国に所在する CEX、関係者の中に RCASP に該当する者が存在しない DEX、RCASP に該当しないウォレットサービスプロバイダーが提供するプライベートウォレットを利用した取引に対しては、CARF は必ずしも有効に機能しない。

日本においても暗号資産の匿名性と分散性により、本人確認を行っていない海外 CEX、DEX、プライベートウォレットが利用されている場合に税務執行上の問題が深刻化する。国税庁がこれらを通じて行われた取引を捕捉できたとしても、そもそもそのような CEX の口座やウォレットについて、誰が管理しており、誰に帰属しているのかを把握することは困難であるし、特定の納税者がそのような CEX の口座やウォレットを保有していることを把握することも難しい。

質問検査権による調査、特定事業者等の報告の求め、CARF はいずれも課税当局への情報提供等に係る義務を課しうる国・地域内に当該義務を負担する者が存在する場合にしか有効に機能しない。また、CARF の RCASP には、単に、暗号資産の保管や移転に係るサービスを提供するようなプライベートウォレット提供事業者等は含まれない。そうすると、海外 CEX、特に CARF に参加していない国に所在する CEX、DEX、プライベートウォレットを利用して、暗号資産の取引・運用をしている納税者の情報を国税庁が把握することは難しい。特定取引等の報告の求めや CARF を通じて、国税庁が利用者の身元を把握できるわけではないし、特定の納税者が利用している海外 CEX、DEX、プライベートウォレットを把握することも難しい。

第Ⅲ章では、暗号資産の匿名性と分散性に起因する税務執行上の問題に対処するために有効な調査手法としてブロックチェーン分析があり、国税庁においては、高性能なブロックチェーン分析ツールを積極的かつ効果的に活用し、調査官をトレーニングする必要性が高まっていることを指摘した。

もっとも、ブロックチェーン分析それ自体は、本人確認手続を実施していない CEX の口座やプライベートウォレットの管理者が誰であるのかを直接的に明らかにするものではないため、納税者が、本人確認を行っている CEX 等とのつながりを一切持たない形で利用している本人確認を行っていない CEX の口座やプライベートウォレットを割り出すことはできない。この意味で、ブロックチェーン分析にも限界がある。このことは、CEX 等が本人確認手続をしていることや納税者がそのような CEX 等を利用していることが、暗号資産に対する適正な税務執行を確保する上で重要なことを認識させるものである。

しかしながら、ブロックチェーン分析により、「①本人確認を行っていない CEX の口座やウォレットアドレス」が、RCASP に限らず「②本人確認を行っている CEX 等」と一度でもブロックチェーン上でトランザクションのやりとりをしている場合、①を管理している者を特定できる可能性がある。また、そのアドレスに関連づけられた暗号資産のトランザクションや残高、あるいは同一人物によって管理されていることが想定される CEX の口座やウォレットを把握することができる。このようなクラスタリングは、本人特定の機会を増加させるし、DEX での取引はブロックチェーン上に記録されているから、特定された人物が DEX で取引を行っていることを把握する端緒となりうる。ここでは、CEX の内部取引は外部から見るとブラックボックスであり、納税者や CEX の協力がない限り税務税当局が取引内容を確認することはできない一方、DEX では利用者の身元情報を収集しないが、取引そのものはスマートコントラクトを通じて行われ、トランザクションの記録はブロックチェーン上で公開されており税務当局も確認できることを想起すべきである。

第IV章では、暗号資産の匿名性や分散性が引き起こすものとは別に、現在、暗号資産の税務執行において、国税庁が直面している最も重要な税務執行上の問題として、暗号資産の損益計算の困難性により、国税庁において、調査選定を効率的に行うことができず、課税処分をすることもできない事態が起りうることを明らかにした。

損益計算ソフトを使ったとしても、一般に、暗号資産の損益計算は難しく、海外 CEX、DEX、プライベートウォレットを複数利用している場合、「正確に」計算することは困難である。この問題の根底には、「データを取得できない場合」がある、「データを適切に損益計算ソフトに取り込むことができない場合」がある、「確認を要する取引や年末数量不一致（損益計算ソフト等で算出された理論上の年末数量と CEX やウォレットから提示された年末数量の不一致）の問題を解消することが難しい場合」がある、「損益計上の有無やタイミング等を判断することが難しい場合」があるなど、多くの解決困難な要因が存在している。

ところで、暗号資産については次のような指摘がある。

- ・納税者は自らの取引状況を把握しているが（納税者自身が行っている取引であるから当然であるが）、他方で税務当局はその納税者の経済活動に関する情報を十分に把握できないという、「情報の非対称性」は厳然として存在し、このような「情報の非対称性」は、仮想空間における暗号資産の取引（投資を含む）による利益については、特に顕著である⁽¹¹⁴⁾。
- ・以前は、税務当局の課題は、「あなたが誰であるかは知っているが、あなたの取引（transactions）は知らない」ことだったが、暗号資産においては「あなたの取引（transactions）は知っているが、あなたが誰であるかは知らない」ことである⁽¹¹⁵⁾。

もつとも、これまでの考察を踏まえると、暗号資産の世界では次のようなケースが発生しうるため、税務当局はより困難な状況に直面しているというのが筆者の現状認識である。

- ①納税者においても取引や損益に関する証拠との距離が遠く、結局、納税者も税務当局も不完全な情報しか入手ないし認識できない（ある種の「情報の対称性」）。
- ②税務当局が、トランザクションデータを入手していても、取引主体の特定や取引内容の解明ができない。
- ③税務当局が、トランザクションデータを入手し、取引主体を特定できいても、損益計算を「正確に」行うことができない。

いずれにしても、暗号資産の匿名性・分散性、損益計算の困難性及びこれらが引き起こす税務執行上の問題に関するこれまでの考察を前提とすると、わが国における暗号資産の税務執行の適正性と公平性を確保するために、具体的な対応策の検討を急ぐ必要がある。

この点について、暗号資産の税金を適正に申告する際に必要となる要素のうち、納税者自身がコントロール可能なものに関しては、納税者に働きかけを行うことも考えられる。このようなものとして、例えば、取引又は利用する暗号資産、損益計算ソフト、CEX、ウォレット、税理士等の専門家、これらに加えて、取引又はトランザクションの履歴やデータ等の作成・保存、税情報へのアクセスがある。このような観点から、納税者に対して、適正申告のために、取引又は利用する暗号資産等についての理解と選択、備忘記録や証拠資料の作成、データの定期的

⁽¹¹⁴⁾ 大野雅人「EU の DAC8—暗号資産取引を対象とする税務当局間の自動的情報交換—」 フィナンシャルレビュー156号(2024)66頁。

⁽¹¹⁵⁾ Katherine Baer et al., *supra* note (18), at 490.

なダウンロードとバックアップの徹底などを働きかけることは、能力や費用の観点から制約があるという留保は付されるものの、有益である。

より重要な対応策として、税務調査に適したブロックチェーン分析ツール及び損益計算ソフトの積極的かつ効果的な活用、これらを駆使した調査手法の開発や国税調査官に対する専門的なトレーニングの推進が不可欠である。関係する専門の事業者との緊密な連携も欠かせない⁽¹¹⁶⁾。

加えて、国税庁の通達・FAQ の充実化、暗号資産の譲渡原価の算定方法等の簡便化、RCASP の定義の見直しを含む⁽¹¹⁷⁾CARF の改訂や CARF 参加国の拡大、国内の情報提供制度の拡充⁽¹¹⁸⁾といった方策も検討の対象となる。納税者が CEX の口座やプライベートウォレットの情報を国税庁に提出することを義務付ける又は納税者に提出を促すような方策も視界に入ってくる⁽¹¹⁹⁾。同時に、規制強化により、納税者が規制の緩い国・地域、プラットフォーム、ツールに逃避することがないかを注視し、対策を講じることも必要である⁽¹²⁰⁾。別の角度からの議論になる

⁽¹¹⁶⁾ 暗号資産の価格データの提供なども含めて、国税庁は民間企業に対して委託や協力を検討する必要がある。IRS は、デジタル資産取引について、コンプライアンス違反のリスクが高く、複雑なものであることを認識した上で、デジタルツールと分析機能を開発し、職員のトレーニングに注力するという方向性を示している。IRS, INFLATION REDUCTION ACT STRATEGIC OPERATING PLAN: FY2023–2031, at 76–77 (2023). *See also* U.S. DEP'T OF TREASURY & IRS, DIGITAL ASSET MARKETPLACE ANALYSIS, SAM.gov, Notice ID 23-326-OITA (June 12, 2023, updated July 25, 2023), <https://sam.gov/opp/c9ffa23337b244a6bd3c954755b1f433/view>.

⁽¹¹⁷⁾ 分散化に対して、ネットワークに存在し得る集中化の形態を特定することによって DeFi を「recentralise」することも考えられる。OECD, INSTITUTIONALISATION OF CRYPTO-ASSETS AND DEFI-TRADFI INTERCONNECTEDNESS 49(2022). 泉・前掲注(14)187 頁も参照。その際には、株式会社クニエ・前掲注(30)において行われているような各プロジェクトの構成要素やトラストポイント（利用者等が無条件にトラストせざるを得ない中央集権的要素）を個別具体的に分析する手法が有効であろう。

⁽¹¹⁸⁾ 情報申告の有用性について、米国では、誤った申告がなされる確率は情報申告が行われる場合に10%未満となるが、情報報告がほとんど、あるいはまったく行われない場合には55%となるという統計もある。IRS, *Publication 1415, Federal Tax Compliance Research: Tax Gap Estimates for Tax Years 2014-2016*, at 2 (rev. Oct. 2022), <https://www.irs.gov/pub/irs-pdf/p1415.pdf>.

⁽¹¹⁹⁾ 紳税者が自身の公開鍵を税務当局に報告すべき義務を課す必要性を説くものとして、Jiang & Ordower, *supra* note (60), at 2125 参照。

⁽¹²⁰⁾ 参照として、デンマーク税務当局が国内の CEX から暗号資産取引に係る顧客データを入手し、取り締まりを強化した後、投資家は海外取引所に逃避した。Hjalte Fejerskov Boas & Mona Barake, *Enforcing Taxes on Cryptocurrencies*, EU TAX OBSERVATORY WORKING PAPER No. 29 (Mar. 2025), at 18, https://www.taxobservatory.eu/www-site/uploads/2025/03/WP29_Enforcing-Taxes-on-Cryptocurrencies.pdf. また、インドが暗号資産取引に係る源泉所得税を導入したことをきっかけとして、投資家は海外取引所に逃避した。Vikash Gautam, *Impact Assessment of Tax Deducted at Source on the Indian Virtual Digital Asset Market*, ESYA CENTRE SPECIAL ISSUE No. 210 (Nov. 2023), <https://static1.squarespace.com/static/5bcef7b429f2cc38df3862f5/t/654c85514544360bd84a7f43/1699513682192/ESYA+CENTRE+-+IMPACT+ASSESSMENT+OF+TAX+DEDUCTED+AT+SOURCE+ON+THE+INDIAN+VIRTUAL+DIGITAL+ASSET+MARKET.pdf>.

が、暗号資産取引に係る所得に対し分離課税を導入する場合には⁽¹²¹⁾、本人確認が義務付けられた CEX を通じた取引のみに限定する、あるいはウォレットを利用して行った取引に係るもの を含めて一定の性能が確保されている損益計算ソフト等を用いて作成した損益計算データを 提出した場合に限定する（CARF とは異なる観点から、より厳しい義務が課されることに注意） など、適正な執行を確保するためにより抜本的な基盤整備を進めるべきである⁽¹²²⁾。

このように、新規性が高く、税務申告上の課題が多い暗号資産について、ひとり納税者に対して一方的に責任や負担を課すのではなく、暗号資産に係る税務執行上の問題とその要因を的確に把握し、暗号資産を取り巻く納税環境の整備を図ることが肝要である。同時に、テクノロジーの急速な発展がもたらす課題に対応するため、国税庁もまた高度なテクノロジーを活用した調査手法の開発等を推進することが求められる。

最後に、ここでは詳細な説明は割愛するが、本人確認を行っている取引所や商品・サービスの提供事業者と直接取引がないケースにおいても、SNS などを含むインターネットやブロックチェーン上に公開されている情報を活用することにより、税務当局が取引当事者を特定できる可能性があることに伴う問題を指摘しておく。この点については、自身が意図していない形で、また、自身の認識が及ばない範囲で、ブロックチェーンやインターネット上に残されていた様々なデジタルの足跡を分析され、課税情報として税務当局に利用されることに懸念や不安を抱く者もいるであろう。これは、一般に公開されている情報を用いた税務調査が、質問検査権の行使なしに無制限に認められるべきかという問題であって、AI 技術の活用とプライバシーの保護に関する議論とも接続するものである。今後、このような問題についてさらなる議論の深化が

⁽¹²¹⁾2024（令和 6）年 12 月の自由民主党＝公明党「令和 7 年度税制改正大綱」では、「検討事項」として、「暗号資産取引に係る課税については、一定の暗号資産を広く国民の資産形成に資する金融商品として業法の中で位置づけ、上場株式等をはじめとした課税の特例が設けられている他の金融商品と同等の投資家保護のための説明義務や適合性等の規制などの必要な法整備をするとともに、取引業者等による取引内容の税務当局への報告義務の整備等をすることを前提に、その見直しを検討する。」とされている。

⁽¹²²⁾匿名性が引き起こす税務執行上の問題に対しては様々なアプローチがありうる。例えば、Omri Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, 82 U.CHI. L. REV. DIALOGUE 53(2015)は、犯罪行為に有用となる暗号資産の特徴の 1 つとして匿名性を挙げた上で、暗号資産における価値移転プロセスの分散化という特徴に対してはコストを課さずに保護する一方、匿名性に対してはコストをかける規制手段を採用することを提案している。具体的には、暗号資産の利用者が販売業者や仲介業者に身元を開示しない場合には、暗号資産の取引税を当該業者に徴収させるような制度により脱税コストを内部化するというものである。Jiang & Ordower, *supra* note (60)は、納税者に対して公開鍵の IRS への報告を義務化することや、これと納税者番号を紐づけるデータベースを作成することを提案している。

望まれる⁽¹²³⁾。

(123)参考として、児童ポルノ受領の罪等で起訴された Gratkowski 氏が、特定のウェブサイトが管理するクラスタのいずれかのアドレスにビットコインを送金したことのある顧客に関するすべての情報を提供することを命じた米国の CEX である Coinbase への召喚令状とブロックチェーン分析が不当な検索や押収から身体、家屋、書類、所有物の安全を保障される人民の権利は侵害してはならないことなどを定める合衆国憲法修正 4 条に違反し、証拠として排除されるべきと主張した事件において、第 5 巡回区控訴裁判所は、Gratkowski 氏はビットコインブロックチェーン上の情報及び Coinbase 上のビットコイン取引記録に係る情報に対して、いずれもプライバシー上の利益を有していないと判断した。United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).

裁判所は、政府による検索が、合衆国憲法修正 4 条に基づく不当な検索から保護される個人の権利を侵害しているというためには、その人物が問題となっている対象に対して「合理的なプライバシーの期待」を有していなければならないところ、一般的に「自発的に第三者に与えた情報については、プライバシーを正当に期待する権利はない」と解されていることを確認した。その上で、ビットコインブロックチェーン上の情報の性質と情報開示の任意性が、同ブロックチェーン上の個人の情報にプライバシー権を見出すことに対して大きな影響を与えるとし、次の点を指摘した。Id. at 310-312.

- ・ビットコインブロックチェーンに記録される情報は、①ビットコインの送付数量、②送付者のビットコインアドレス、③受領者のビットコインアドレスに限定されていること
- ・ビットコインを通じた取引は「日常生活に浸透した又は不可欠な一部」ではないこと
- ・ビットコインの送受信には、ビットコインアドレスの保有者による「積極的な行為」が必要であること
- ・ビットコインの利用者は、ビットコインブロックチェーンに公開された情報が公開されないことを期待していないと考えられるため、「正当なプライバシーの期待」という主張は説得力を減じられること
- ・ビットコインの利用者は、他の送金手段を使用する人々よりも高いレベルのプライバシーを享受しているが、ビットコインのトランザクションはすべて公開されているブロックチェーンに記録されるることは周知の事実である。ビットコインの利用者は誰でもそのブロックチェーンにアクセスすることが可能であり、すべてのビットコインのアドレスとその送付履歴を確認できる。このような公開性があるため、ブロックチェーンを分析することでビットコインアドレスの保有者の身元を特定することが可能となっていること

また、裁判所は、Coinbase のビットコイン取引に対する Gratkowski 氏の合理的なプライバシーの期待について、同じように、情報の性質と開示の任意性は、Coinbase の記録にプライバシー上の利益を見出すことに対して大きなマイナス要因となるとした。その際、次の点を指摘している。Id. at 312-313.

- ・Coinbase の記録にアクセスしても、検査官には個人の暗号資産取引に関する情報のみが提供されるため、個人の生活の詳細が提供されるものではない。
- ・Coinbase 等の CEX を通じてビットコイン取引を行うには、利用者の「積極的な行為」を要する。ビットコイン利用者は、第三者の仲介者を介さずに取引を行うことで、高いレベルのプライバシーを維持する選択肢がある。しかし、そのためには技術的専門知識が必要であるため、ビットコイン利用者は、Coinbase のような仲介者を介して取引を行うことで、プライバシーをある程度犠牲にすることを選択する可能性がある。

このほか、IRS が発布した Coinbase に対する顧客情報提供の召喚状に対して、納税者からなされた合衆国憲法修正 4 条違反の主張を認めなかつた裁判例として、Zietzke v. United States, 426 F. Supp. 3d 758, 761 (W.D. Wash. 2019); Zietzke v. United States, No. 19-cv-03761-HSG (SK), 2020 U.S. Dist. LEXIS 8675 (N.D. Cal. Jan. 17, 2020)がある。See also Lee A. Sheppard, *The Sweeping Reach of the DeFi Broker Reporting Regulations*, 186 TAX NOTES FED. 1001, 1007 (2025).