業種別委員会研究資料第2号

「Web3.0 関連企業における監査受嘱上の課題に関する研究資料」の概要（第2回）

公認会計士 髙山（たかやま） 朋也（ともや）

1. はじめに

日本公認会計士協会は、2023年11月20日に業種別委員会研究資料第2号「Web3.0 関連企業における監査受嘱上の課題に関する研究資料」（以下「本研究資料」という。）を公表した。本研究資料の概要を2回に分けて解説する。第1回目では、本研究資料の「はじめに」及び「第1部」の説明として、トークンの法律上の定義及びトークンの類型の整理、本研究資料の公表の経緯、Web3.0 企業の監査受嘱上の留意事項、トークンの発行に係る監査上の課題等の解説を行った[1]。第2回目の本稿では「第2部」の説明として、トークンの保有及び発行に関する論点のうち、「第1部」で取り扱っていないその他のトークン等の保有及び発行に関連する論点について解説する[2]。具体的には、自己の発行した資金決済に関する法律（以下「資金決済法」という。）上の暗号資産の保有、資金決済法上の暗号資産を財又はサービスの対価として受領するケース、未上場トークンの保有、NFT（Non-Fungible Token）、SAFT（Simple Agreement for Future Tokens）及びその他実務上の検討課題について、事例も含め解説する。

2. トークン保有に係る監査上の課題

（1）自己の発行した資金決済法上の暗号資産の保有

① 論点整理の考え方及び寄せられたコメント

自己が発行した資金決済法上の暗号資産の保有に関する会計処理は、第1回目で解説した資金決済法上の暗号資産の発行時の会計処理と同様に、企業会計基準委員会（以下「ASBJ」という。）が公表している実務対応報告第38号「資金決済法における暗号資産の会計処理等に関する当面の取扱い」（以下「実務対応報告第38号」という。）の適用範囲外である。そのため、会計基準等の定めは明らかではなく、ASBJは、2022年3月15日に「資金決済法上の暗号資産又は金融商品取引法上の電子記録移転権利に該当するICOトークンの発行及び保有に係る会計処理に関する論点の整理」（以下「論点整理」という。）を公表し、第38項及び第39項において、自己の発行したICOトークンを自己に割り当てた場合及び第三者から取得した自己発行のICOトークンの会計処理の考え方を、以下の通り紹介している。

論点	考え方
自己に割り当てた自己発行ICOトークンの会計処理[3]	以下の2つの方法が示され、前者の方法を取る考え方が示されている。 ・第三者が介在しない内部取引として会計処理の対象としない方法 ・会計処理の対象として会計上の資産及び負債（発行者が何らかの義務を負担している場合）を計上する方法

1 会計情報2024年3月号の記事を参照。

2 本研究資料は2023年9月に公表された公開草案に寄せられたコメントを踏まえて公表されたものであるが、内容面で大幅な見直しは行われていない。本稿では2023年11月号掲載の公開草案の解説記事から若干の変更を行っており、主な変更点に下線を付している。

3 2023年度税制改正要望において金融庁と経済産業省の共同要望として「ブロックチェーン技術を活用した起業等への阻害要因を除去し、Web3 推進に向けた環境整備を図る観点から、法人が発行した暗号資産のうち、当該法人以外の者に割り当てられることなく、当該法人が継続して保有しているものについては、期末時価評価課税の対象外とすること」が要望として出されていることを受け、ASBJに対して、自己に割り当てた自己発行ICOトークンの会計処理について質問が寄せられた。これを受けて、2022年11月7日開催の第490回企業会計基準委員会にて、自己に割り当てた自己発行ICOトークンの会計処理について審議が行われた。論点整理で紹介した考え方のいずれを採用すべきか結論は出していないが、いずれの場合も時価評価しないという考え方が示された。

論点	考え方
第三者から取得した自己発行ICOトークンの会計処理	以下の2つの方法が示され、前者の方法のうち、関連する負債の消滅の認識を行い、当該負債の計上金額と取得したICOトークンの取得原価が異なる場合には、差額を損益として処理する考え方が示されている。 ・関連する負債の消滅又は控除として取り扱う方法（関連する負債の消滅の認識を行う方法又は関連する負債の消滅の認識は行わず、ICOトークンの取得原価をもって関連する負債から控除して表示する方法） ・資産として取り扱う方法

論点整理に対しては、第三者から取得した自己発行トークンを再度売却した場合の取扱いなど、様々な論点に対するコメントが寄せられた。また、発行者が負う義務の性質や発行後に第三者から取得する目的などを踏まえて更なる分析が必要であるという意見もあった。

② 監査上の課題

トークンの発行時と同様に、監査人は、識別された保有者や発行者の権利及び義務が、ホワイトペーパーやその他の契約、法律専門家による見解書などによって裏付けられることや、識別された権利及び義務に基づく経営者による会計判断が適切であることを検討する。

また、監査人は、企業が発行したトークンを自己が保有していることに対して、自己で保有していることの理由を理解し、その理由が企業の事業戦略に従ったものであるかどうかを評価し、何らかの理由により、企業が意図しない保有が生じている場合には、監査上追加で識別すべきリスクがないか、監査計画に影響がないか検討する。

(2) 資金決済法上の暗号資産を財又はサービスの対価として受領するケース

企業は、財又はサービスの対価として暗号資産を受領することがあり、例えば、以下のようなケースが考えられる。

・IEO（Initial Exchange Offering）において暗号資産交換業者に報酬として現金以外に新規上場の暗号資産で支払われるケース
・自社が発行したNFTを通常の営業活動として販売するに当たって、当該NFTに表章されている権利を引き渡す対価として暗号資産を受領するケース

企業会計基準第29号「収益認識に関する会計基準」（以下「収益認識会計基準」という。）は、資金決済法における定義を満たす暗号資産及び金融商品取引業等に関する内閣府令における定義を満たす電子記録移転有価証券表示権利等に関連する取引については、収益認識会計基準の適用範囲から除外しているが（収益認識会計基準第3項(7)、第108-2項）、暗号資産そのものの売買ではなく、財又はサービスの対価として暗号資産を受け取る場合は、当該収益について収益認識会計基準に従って検討が行われている実務がある。

この場合、収益認識会計基準に定める5つのステップ（契約の識別、履行義務の識別、取引価格の算定、履行義務への取引価格の配分、履行義務の充足による収益の認識）に従って会計処理を検討するにあたり、監査人は、具体的な履行義務の識別、いつの時点で収益を認識するのか、いつの時点の市場価格で収益を測定するのか等の点に関して、契約や事実関係に基づく整理を企業に説明を求めることになる。

なお、収益認識会計基準第59項に基づき、現金以外の対価を時価により算定することから、実務対応報告第38号第5項及び第6項に記載のとおり、対価として受領する暗号資産に活発な市場が存在する場合には、収益認識時の暗号資産の市場価格に基づく価額より取引価格を算定している実務がある。

(3) 上場していないトークン等の保有

企業は暗号資産取引所に上場していない、例えば、以下のようなトークンを取得することがある。

・暗号資産取引所における将来の上場を前提として相対取引で取得するトークン
・暗号資産プロジェクトの初期フェーズにおけるプライベートセールを通じて取得するトークン
・ハードフォーク（プロトコルの後方互換性・前方互換性のない大規模なアップデートによるブロックチェーンの分岐（スプリット）により保有する暗号資産が異なる種類の暗号資産に分裂する事象）等により取得するトークン

監査人は、トークンが資金決済法に規定する暗号資産に該当するかどうかについて、企業による検討を確認する。暗号資産該当性は、法律の解釈を伴う場合もあるため、監査人は、法律専門家による見解書の入手やその検討を行うことも考えられる。監査人は、企業がトークンを取得する目的や合理性も併せて検討する。

トークンの期末における評価方法については、実務対応報告第38号を参考にしている実務も見られる。実務対応報告第38号第6項に従い、活発な市場が存在しない場合には、取得原価又は期末における処分見込額のいずれか低い方をもって貸借対照表価額とすることとされ、取得価額をもって貸借対照表価額とする実務や備忘価額まで減額する実務が見られる。

3. NFT

(1) 概要及び利用事例

本稿執筆時点（2024年2月9日）ではNFTに関する固

有の法規制はなく、トークンがそれぞれに固有の権利を表章し非代替的な性質を持ち、金融商品取引法や資金決済法等の既存の金融規制が適用されないトークンが一般的にNFTと認識されている。法規制上の定義はなく、会計基準等の明確な定めはないことから、NTFが表章する権利や発行者、一次保有者及び二次保有者などの取引当事者間の権利及び義務等の実態を踏まえ、既存の会計基準等に照らした検討を実施する必要がある。そのため、NFTがどのような権利を表章しているのか、取引当事者間でどのような権利及び義務があるのか等を利用規約や譲渡契約等で明確にすることが会計処理を行うために必要となる。

NFTの利用事例としては、例えば以下のようなものが挙げられる。

- デジタルコンテンツの流通のために、デジタルアートの閲覧権をNFTに表章する事例や、メタバースと呼ばれる仮想空間上に構築された土地を利用する権利をNFTとして表章する事例
- ゲームアイテムをNFT化して流通させ、独自トークンの発行と組み合わせてゲーム内で独自の経済圏を作る取り組みはGameFiと呼ばれる。
- イベントの参加権や施設の利用権等をNFTに表章する事例

NFTは流通市場が多数存在しており、二次流通市場においてNFTが転々流通することが想定されることも特徴となっている。

（2）NFT発行

①　自己発行NFTの一次流通

企業が発行したNFTを販売する会計処理の決定においては、収益認識会計基準の適用範囲となるかの検討が必要になる。NFTが金融商品取引法や資金決済法等の金融規制の適用を受けない場合、収益認識会計基準に従って処理される事例が見られる。

収益認識会計基準の適用範囲となった場合、履行義務の識別が課題となる事例が見受けられる。例えば、NFTの保有者に対してトークンの受け渡し後においても様々な権利（例えば、NFT保有者にイベントへの入場権利を与えるケース）を付している事例がある。このように顧客に約束した財又はサービスが複数ある場合には、企業は、別個の財又はサービスかどうかを評価し、別個であれば、それぞれの履行義務を識別し、取引価格の配分及びそれぞれの履行義務の充足する時点又は期間の検討を行うことになる。

企業がこの検討を適切に行うための前提として、発行者及び保有者の権利及び義務が利用規約や譲渡契約等において具体的に明記されることが必要となる。

②　二次流通ロイヤリティの収受を含むNFTの自己発行

NFTの二次流通市場で第三者間での売買が行われた際に、売買代金の一定割合を発行者が受領する事例が見受けられる。このような二次流通ロイヤリティの会計処理にあたって、企業は、二次流通ロイヤリティは発行者のどのような財又はサービスの提供に基づいた対価なのか、誰から受領するものなのか（第三者間の売買における販売者から受領するものなのか、購入者から受領するものなのか）を利用規約や二次流通市場の販売サイトにおいて明確化することが必要となる。収益認識会計基準第127項に基づき、個々の契約の実態とそれに係る顧客の合理的な期待を分析することが必要な場合もある。

監査人は、二次流通ロイヤリティの裏付けとなる監査証拠の入手可能性に留意する必要がある。二次流通プラットフォーム上での第三者間のNFT売買に伴うNFTの受渡及び代金決済並びにNFTの発行者への二次流通手数料の支払いがブロックチェーン上に記録される場合がある。一方、二次流通プラットフォームの利用者がNFTを当該プラットフォームに預託し、オフチェーンでNFTの売買、受渡及び代金決済並びに二次流通手数料の支払いが行われる場合もある。このようにNFT関連取引の記録方法には様々なケースが存在することから、監査人は、発行者がNFTの出品を許可した二次流通プラットフォームそれぞれについて、取引の記録方法や入手可能な監査証拠を理解し、監査の実施可能性を検討することが必要となる。ブロックチェーン上の取引履歴だけでは二次流通ロイヤリティが第三者間の実在する売買取引に基づくものであることを裏付けることができない場合には、二次流通プラットフォーム上のデータベースに記録された取引履歴の入手が必要となる場合も想定される。

（3）NFT保有

①　保有するNFTの法的性質に基づく会計上の取扱いの検討

他社の発行したNFTを保有する企業は、NFTが表章する権利及びNFTの保有目的を考慮して会計処理を検討することになると考えられる。企業会計基準第9号「棚卸資産の評価に関する会計基準」（以下「棚卸資産評価会計基準」という。）第3項の棚卸資産の定義に該当すると判断し棚卸資産として計上する事例と、「財務諸表等の用語、様式及び作成方法に関する規則」第27条（無形固定資産の範囲）に列挙されたいずれかの項目の権利を表章する目的で保有するトークンと判断し、無形固定資産として計上する事例が見られる。そのため、会計処理の判断にあたりNFTがどのような権利を表章するものであるか、発行者との契約書等で明確にされていることが必要となる。

他社の発行したNFTを棚卸資産として計上した場合、期末における正味売却価額が取得原価よりも下落している場合には、当該正味売却価額を貸借対照表価額とし、その差額は費用として処理される（棚卸資産評価会計基準第7項）。市場価格が観察できない時は、期末前後での販売実績に基づく価額等、合理的に算定された価格を売価とする（棚卸資産評価会計基準第8項）。NFTはその非代替的な性質から、参考となる市場価格を観察でき

なかったり、NFT市場は黎明期にあり十分な流動性があるとは言えないことから、正味売却価額の見積りが困難となる場合がある。

他社の発行したNFTを無形固定資産として計上した場合、例えば定額法で償却を行う際には、耐用年数の合理的な見積りが問題となる。ブロックチェーン上で記録される場合にはトークン自体は技術的にはほぼ永続的に存在し得るものと考えられるが、NFTをどの程度の期間ビジネスで利用するかについての実績が乏しいことから、耐用年数の見積りを合理的に説明することが難しい事例が見受けられる。また、NFTを利用したビジネスは、収益性やライフサイクル等のデータの蓄積も十分でなく詳細な中長期計画を立てることができず、固定資産の減損会計の適用に当たり、割引前将来キャッシュ・フローの見積りを合理的に説明することが難しい事例が見受けられる。回収可能価額の算定に正味売却価額を利用する場合には、棚卸資産の場合と同様に、正味売却価額の見積りが困難となる場合がある。

② 自己の発行したNFT

上記2.（1）①で述べた自己に割り当てた自己発行ICOトークンの会計と同様の論点が生じると考えられる。

4. SAFT等

（1）概要及び利用事例

諸外国におけるトークン関連の資金調達事例では、以下の通り、SAFT等の形態が見られる。我が国においてはSAFT等を通じた資金調達事例は見られないが、国内企業が運営する在外ファンド等を通じてSAFT等へ投資する事例は見受けられる。

① SAFT

将来発行が予定されるトークンの割安購入権

② SAFTE（Simple Agreement for Future Tokens or Equity）

将来発行が予定されるトークンの割安購入又は発行体株式への転換を選択できる権利

③ SAFE（Simple Agreement for Future Equity）

あらかじめ定められた金額を支払うことで、将来の新株発行時に所定の転換価額に基づき当該新株に転換できる権利であり、将来発行が予定されるトークンの有償又は無償での配布を受ける権利であるトークンワラントを組み合わせた形式の契約も見られる。

（2）SAFT等の発行

上述のように我が国においては、SAFT等を通じた資金調達の事例は見られないが、今後のWeb3.0 ビジネスの多様化の中で、第1回目で解説したWeb3.0 企業の監査受嘱上の留意事項等を考慮して実務上の検討が必要となることも考えられる。

この場合、第1回目の「3.Web3.0 企業の監査受嘱上の留意事項」にて解説した事項を検討することが必要になると考えられる。

（3）SAFT等の保有

① SAFE

保有するSAFEの会計処理を検討する場合には、SAFEの法的性質やデリバティブに該当するかどうかの検討が必要と考えられる。SAFEは将来発行される株式に自動的に転換される性質を有しており、SAFEの保有者がSAFEの発行者に対して新株を発行させることはできないと考えられている。そのため、以下の商品に該当するかどうかを、個別に検討した上であるべき会計処理を検討する必要があると考えられる。

- 「株式会社に対して行使することにより当該株式会社の株式の交付を受けることができる権利」である新株予約権（会社法第2条第21号）
- 金融商品取引法第2条第1項及び第2項（第1号及び第2号を除く。）に規定する有価証券
- 会計制度委員会報告第14号「金融商品会計に関する実務指針」（以下「金融商品会計に関する実務指針」という。）第6項で定めるデリバティブ

② SAFT

SAFTについても、会計処理の入り口として、その法的性質の検討が必要と考えられる。SAFTの条件は実務上多様な設計が行われていることが想定されるが、米国では、いわゆるHoweyテスト[4]によりSAFTが米国証券法の証券に該当するケースがあるものと考えられる。また、SAFTは、将来のトークン発行が所定の日までに行われない場合には調達資金を出資者に返還する条項が付される場合があるが、このような返還義務も会計処理の判断において考慮する必要があると考えられる。さらに、金融商品会計に関する実務指針第6項で定めるデリバティブの定義に該当するかどうかの検討も必要と考えられる。

5. その他実務の検討

（1）暗号資産の発行体株式の評価

非上場会社が資金決済法上の暗号資産の発行者となる場合、トークン発行に係る会計処理に課題が生じる場合がある[5]。そのため、実質価額の算定に基づく当該非上場

4 Howeyテストは、本研究資料の第1回目の解説の脚注3を参照。
5 トークン発行に係る会計処理の課題は、本研究資料の第1回目の解説の「4．トークン発行に係る監査上の課題」参照。

株式の減損処理要否の判定が困難になるケースが考えられる。

(2) 資金決済法上の暗号資産の貸付及び借入

企業が第三者と行う暗号資産の貸付及び借入に係る会計上の取扱いを明示した会計基準等はない。実務対応報告第38号第14項及び第15項並びに第55項及び第56項において、暗号資産交換業者が預託者から預かった資金決済法上の暗号資産について、暗号資産の私法上の位置づけが明確ではないものの、自己が保有する暗号資産との同質性を重視し、その時点の時価による資産として計上することとされている。これらを参考に、暗号資産の貸付は貸付暗号資産として資産に計上し、暗号資産の借入は借入暗号資産として負債に計上している実務が見られる。

なお、実務対応報告38号において、暗号資産の貸付としての資産や借入としての負債に関する規定はないことから、信用リスクの評価も含めこれらの事後測定（時価評価等）に関する会計上の取扱いが明らかではない点に留意する必要がある。

(3) 資金決済法上の暗号資産以外のトークン等を第三者から預かる場合

上記(2)で解説した通り、実務対応報告第38号は預託者から預かった資金決済法上の暗号資産の会計処理を定めるが、資金決済法上の暗号資産以外のトークン等（NFTなど）を第三者から預かる場合は実務対応報告第38号の適用対象外となる。そのため、ASBJから公表されている討議資料「財務会計の概念フレームワーク」（以下「概念フレームワーク」という。）における資産の定義に照らして、結果として資産として計上しないこととしている実務が見られる。

概念フレームワークでは、「資産とは、過去の取引又は事象の結果として、報告主体が支配している経済的資源をいう。」とされている。一般的に、トークン等（NFTなど）は、売却等によりキャッシュ（又は暗号資産）の獲得に貢献する便益の源泉であるため「経済的資源」に該当すると考えられるため、資産として計上が必要か否かを決定するに当たっては、顧客から預かったトークン等（NFTなど）を暗号資産交換業者が支配しているかが論点となると考えられる。概念フレームワークでは、支配とは「所有権の有無にかかわらず、報告主体が経済的資源を利用し、そこから生み出される便益を享受できる状態をいう。」とされている。よって、報告主体である暗号資産交換業者と預託者との預託の合意の内容を検討し、暗号資産交換業者が支配を有しているかを検討することで、会計処理を決定することが考えられる。支配の検討においては、NFTは、実務対応報告第38号第55項で示されている「現金と同様に個別性がなく」という資金決済法上の暗号資産の特徴を一般的に有しない点も考慮することが考えられる。

(4) 重要な会計方針等の開示

企業会計基準第24号「会計方針の開示、会計上の変更及び誤謬の訂正に関する会計基準」第4-3項では、特定の会計事象等に対して適用し得る具体的な会計基準等の定めが存在しない場合を「会計基準等の定めが明らかでない場合」と定義した上で、同第4-2項において、当該事項が重要な会計方針に該当する場合、財務諸表を作成するための基礎となる事項を財務諸表利用者が理解するために、採用した会計処理の原則及び手続の概要を示すことを求めている。Web3.0 ビジネスは、我が国において過去に事例のないものがあり、今後も既存の会計基準等が想定していないケースが発生するものと考えられることから、重要な会計方針等の開示は今後の会計実務において留意すべき事項である。

6. ブロックチェーンに関連する監査上の論点

(1) 秘密鍵の管理体制

暗号資産等のトークンの所有者は、保有する秘密鍵を用いて電子署名を行うことによって、ブロックチェーン上でトークンの移転を行うことが可能になる。サイバー攻撃等により秘密鍵が外部に流出し、企業が保管するトークンの不正流出事件が過去何度も生じていることから、サイバー攻撃等による暗号資産の不正流出リスクが識別される。また、企業の内部者が秘密鍵に容易にアクセスできる場合には、内部者によって企業が保管するトークンの不正流出が行われるリスクが高まることになる。そのため、監査人は、トークンの発行や保有を行う企業の監査を受嘱する際には、企業による堅牢な秘密鍵の管理体制が整備・運用されていることを確かめる必要がある。秘密鍵の管理体制の評価においては、例えば、以下の点を検討する必要がある。

① アクセスセキュリティ

企業は、秘密鍵の生成から、保管、利用、廃棄までの秘密鍵のライフサイクルにおいて、秘密鍵への不正アクセスを防止するため、職務分掌や物理的・論理的アクセスコントロールを整備・運用することが求められる。また、ホットウォレットでの保管を制限するとともに、サイバーセキュリティ体制を構築することが求められる。

② マルチシグ

企業は、送金を実行する際に複数の秘密鍵による電子署名を必要とするマルチシグ技術やそれに代替する内部統制（例えば、秘密分散技術により秘密鍵を複数に分割、秘密鍵へのアクセスに多段階認証を必要とする情報処理統制等）を整備することが求められる。

③ バックアップ

不測の事態によって秘密鍵を紛失したり、秘密鍵へのアクセスが出来ない状況下で秘密鍵情報を復元できなく

なると、トークンの移動ができず、実質的にトークンに対する権利を失った状態になる。そのため、企業は秘密鍵のバックアップ体制を整備・運用することが求められる。バックアップの保管場所は、秘密鍵と同様に、不正アクセスを防止するための厳重なセキュリティ対策が求められることに留意する。

④　外部委託先管理

トークンを保有する企業が、秘密鍵の管理やトークンの保管に企業外部の第三者を利用する場合や、外部SaaS（Software as a Service）のウォレットシステムを利用している場合、企業は当該外部委託先の秘密鍵管理等に関連する内部統制が整備・運用されているか評価することが求められる。監査人は、監査基準委員会報告書402「業務を委託している企業の監査上の考慮事項」に従い、例えば、利用規約や使用に関する契約を確認することで、当該外部委託先の業務を理解する必要がある。また、外部委託先の内部統制の整備・運用状況を評価するため、例えば、受託業務に係る内部統制の保証報告書を入手し、検討することが考えられる。

（2）スマートコントラクト[6]の検証

企業が新たに暗号資産やNFTを発行する場合に、トークンに関する仕様を定義したスマートコントラクトをブロックチェーンに配置し利用することが一般的である。スマートコントラクトの利用例は、以下のようなものがある。

・トークンの生成・移転及び焼却（バーン）等使用不可能とする処理や取引履歴のブロックチェーンへの記録を行う。
・一定条件下で取引参加者間でのNFTと暗号資産の交換を自動実行する決済機能

スマートコントラクトは、トークン発行に関わる基礎的な機能だけでなく、複数のプログラムを組み合わせることで発行数量の制限や指定したアドレスの取引停止といったトークンの流通を制御する特権的機能や、特権の保有者を変更する機能、さらには事後的にロジックを追加変更するための拡張性を備えることも可能である。

監査人は、自動化されたプログラムとして継続的に意図した通りに運用されているかという観点から、スマートコントラクトが情報処理統制として有効に運用されていることを確認する。監査人は、スマートコントラクトに不正流出や規制当局の要請等に備えた安全措置のための機能が組み込まれているかについても確認する。

監査人は、スマートコントラクトの開発・変更に関する内部統制の整備・運用状況を評価することで、スマートコントラクトの開発・変更過程で不具合や脆弱性の混入リスクへの対応が出来ているか確認することになる。監査人は、信頼できる第三者機関によって実施されたコードレビューの結果を入手し、異常が発見されていないことを確かめる等の方法を取ることも考えられる。監査人は、トークンの発行や特権的機能を利用するための秘密鍵へのアクセスコントロールが整備・運用されているか検証することで、特権の利用による不正なトークン発行やスマートコントラクトのロジック改ざんリスクへの対応ができているか確認する。

なお、スマートコントラクトは、通常、解読が困難なバイトコード等の形式でブロックチェーン上に配置されるため、監査人が企業からソースコードを入手し検証に利用する場合には、それがブロックチェーンに配置されたものと同一であるかにも留意する。

（3）監査証拠として利用するブロックチェーンの記録の信頼性の評価

トークンの発行や保有を行う企業を監査する際には、ブロックチェーン上の情報を監査証拠として利用することになる。ブロックチェーンのネットワークの参加者が相互に監視し合うことによりブロックチェーン上の記録は改ざんされにくい仕組みになっていると認識されているが、監査人はブロックチェーンの記録を監査証拠として利用するために、ブロックチェーンの信頼性及びブロックチェーンから情報を取得するためのプログラムの信頼性を評価する必要がある。

①　ブロックチェーンの信頼性の評価

ブロックチェーンネットワークに参加するコンピュータ（又は参加者）をノードというが、コンセンサスアルゴリズムに参加するノードに特に制限がない場合を「パブリック型ブロックチェーン」という。これに対して、非パブリック型ブロックチェーンとは、参加するノードが制限されている場合のうち、複数の組織体に限定されていれば「コンソーシアム型ブロックチェーン」といい、一つの企業や組織に限定されていれば「プライベート型ブロックチェーン」ということが多い。非パブリック型ブロックチェーンの場合には、発行に関係するシステムやブロックチェーンの理解に当たり、保証業務実務指針3701「非パブリック型のブロックチェーンを活用した受託業務に係る内部統制の保証報告書に関する実務指針」を参照されたい。

監査人は、以下の通り、利用される暗号技術やコンセンサスアルゴリズム等の理解を通じて、ブロックチェーンの信頼性を評価することになる。

6　スマートコントラクトとは、参加者が相互にやり取りをする上で合意する一連のルールを含むデジタルコードを言う。事前に定義されたルールに合致すると、このコードにより自動的に合意が執行される。このスマートコントラクトコードは合意又は取引の実行を促進、承認及び執行し、その後、取引の結果がブロックチェーンに書き込まれる（本研究資料付録3.用語集No.10）。

a．利用される暗号技術の理解

ブロックチェーン上のデータ（ブロック情報）の真正性は、ハッシュ関数に依存している。ハッシュ関数の逆演算やハッシュ値の操作が可能になった場合、異なるブロックであるものの同一のハッシュ値を持つブロックを生成することができる可能性があり、過去のブロック情報の修正が可能となるリスクがある。また、ブロックチェーンにおけるトランザクションは、電子署名技術により証明される。電子署名の改ざんが可能になった場合、トランザクションの真正性が損なわれるリスクがある。

そのため、ブロックチェーンにおいて使用されている基盤技術を理解し、危殆化していないことを確かめることは、ブロックチェーンの信頼性について理解する上での前提となる。

b．コンセンサスアルゴリズムの理解

ブロックチェーンのネットワークにおいては、ネットワークに参加する各ノードが互いにデータを持ち合い、当該データが正しいデータか否かについて全体としての合意が形成される。この合意形成の仕組み、すなわち、コンセンサスアルゴリズムを理解することは、ブロックチェーンのネットワークそのものの信頼性についての理解を得ることや、どのようにトランザクションが確定データとしてブロックチェーンに記録されるかについての理解を行う上で有益である。コンセンサスアルゴリズムの理解には、以下を含む。

・コンセンサスアルゴリズム[7]の種類
・承認ノードの管理主体
・ブロックチェーンを維持するための必要なノード構成
・ファイナリティ[8]の条件
・コンセンサスアルゴリズムの変更に関する内部統制

参加者の多いパブリック型ブロックチェーンであれば、改ざんの可能性は低いと想定されるが、パブリック型ブロックチェーンであっても、参加者が少ないブロックチェーンであれば、51%攻撃[9]によって改ざんのリスクが高くなる。

② ブロックチェーンから情報を取得するためのプログラムの信頼性の評価

監査人はブロックチェーンから取引記録を入手する際に、監査人自らブロックチェーンノードを構築する場合があるが、監査人は、当該ブロックチェーンノードの信頼性を評価する必要がある。信頼性の評価には、プログラムが目的適合的にデザインされているか、プログラムが意図された通りに機能しているなどの検討が含まれる。

監査人は、各トークンのコミュニティ等が運営するWebサイト上のエクスプローラを利用してブロックチェーンの情報を取得する場合があるが、エクスプローラの信頼性を評価する必要がある。

以　上

7 コンセンサスアルゴリズムの代表的なものには、「Proof of Work（PoW）」、「Proof of Stake（PoS）」、「Practical Byzantine Fault Tolerance（PBFT）」といったものがある。PoW、PoSはパブリック型で利用されることが多い。プライベート型やコンソーシアム型で利用される代表的なコンセンサスアルゴリズムとしてPBFTが挙げられる。

8 トランザクションがブロックチェーン上のデータとして確定することを、「ファイナリティを得る」と表現する。PoWは構造上ファイナリティがなく、一定のブロック数を経過することで確定したものとみなされることが多い。PoS、PBFTには通常ファイナリティを与える仕組みが備わっている。

9 51%攻撃とは、悪意のある者が、ネットワーク全体の採掘に係る計算処理能力の50%超を支配して不正な取引を実行することをいう。

