様式第九（第４条関係）

新事業活動に関する規制について規定する法律及び法律に基づく命令の規定に係る照会書

令和６年９月１２日

内閣総理大臣 岸田 文雄 殿
経済産業大臣 齋藤 健　 殿

東京都中央区日本橋茅場町２－１２－１０
一般社団法人ジャパン・コンテンツ・ブロックチェーン・イニシアティブ
代表理事　伊藤　佑介

産業競争力強化法第７条第１項の規定に基づき、実施しようとする新事業活動及びこれに関連する事業活動に関する規制について規定する法律及び法律に基づく命令の規定の解釈並びに当該新事業活動及びこれに関連する事業活動に対する当該規定の適用の有無について、確認を求めます。

記

１．新事業活動及びこれに関連する事業活動の目標

当法人は、ブロックチェーン（以下「ＢＣ」という）等の先端技術を基点として日本のコンテンツ業界のデジタルトランスフォーメーションを業界横断で加速させることを目的とする一般社団法人であり、コンテンツの流通市場の拡大及び知的財産権等の権利保護に関する提言・施策を通じて、コンテンツ業界の健全かつ持続可能な更なる発展を推進するための事業を行なっている業界団体である（なお、２０２４年２月末時点で、コンテンツ業界関連企業を中心とする加盟企業が７０社である）。

ＢＣを活用したサービス（以下「ＢＣサービス」という）のマスアダプテーションのためには、ＮＦＴや暗号資産などのＢＣ上の記録（以下「ＢＣ資産」という）を移転するための秘密鍵（以下「ＢＣ秘密鍵」という）の管理に係る課題を解決することが必要不可欠である。即ち、ＢＣ秘密鍵は一般に複雑で長い文字列であるところ、特にＢＣサービスのユーザー（以下、単に「ユーザー」という）が個人である場合、これを自己で管理することは、その管理負担やＢＣ秘密鍵を紛失した場合のリスク等から忌避される一方、ＢＣサービスを提供する事業者（以下「ＢＣ事業者」という）がユーザーのＢＣ秘密鍵を管理することは、かかる管理機能（以下「ウォレット機能」）の開発・構築自体のほか、資金決済に関する法律（以下「資金決済法」という）上の規制対象となる場合にはその遵守のための体制構築などに相当程度のコストを要することから、必ずしも容易に実現できる解決手段とはならない。

そこで、当法人は、ＢＣ秘密鍵の管理に関して、ユーザー及びＢＣ事業者の双方にとって、負担が小さく、かつ、安全性の高い仕組みを構築するためのサービスとして「ＰａｓｓＷａｌｌｅｔ（パスウォレット）」を提供することを予定している。このＰａｓｓＷａｌｌｅｔの提供を通じて、ＢＣ秘密鍵の管理に係る課題を解決することによりＢＣサービスのマスアダプテーションを促進し、コンテンツ業界の更なる発展に資することを事業活動の目標としている。

２．新事業活動及びこれに関連する事業活動により生産性の向上又は新たな需要の獲得が見込まれる理由

「新たな役務の開発又は提供」に該当する。

（１）生産性の向上

ＢＣ事業者自身が、自社のＢＣサービスのための独自のウォレット機能を開発・構築するためには、相当程度のコストを要するが、ＰａｓｓＷａｌｌｅｔをＢＣ事業者が導入した場合、ＢＣ事業者において、より少ないコストでのウォレット機能の実装が可能となる点で生産性が向上する。

（２）新たな需要の獲得

ユーザー自身にＢＣ秘密鍵の管理負担をかけることなく、マス向けのＢＣサービスを提供したいと考えるＢＣ事業者は多数存在するものの、ＢＣ事業者自身によるウォレット機能の開発・構築のコストから、これを断念する場合がある。ＰａｓｓＷａｌｌｅｔの提供は、このようなＢＣ事業者からの新たな需要の獲得が見込まれる。

【需要獲得見込み】

年間導入ＢＣ事業者数：５０社

年間利用ユーザー数：５００万人

１導入ＢＣ事業者あたりのサービス料：０円（当法人は、コンテンツ業界の発展に資する活動を行う業界団体であり、ＢＣサービスのマスアダプテーションを促進するために、ＰａｓｓＷａｌｌｅｔは無償で提供することを予定している）

３．新事業活動及びこれに関連する事業活動の内容

（１）事業実施主体

サービス提供事業者：当法人

サービス利用者：ユーザー及びＢＣ事業者

（２）事業概要

ＰａｓｓＷａｌｌｅｔは、端的には「当法人が設置・運営する認証サーバー（以下「当法人認証サーバー」という）とのＡＰＩ連携をＢＣ事業者に提供する」というものである。当法人認証サーバーとのＡＰＩ連携を含めた、下記一連の仕組みにより、ユーザーが保有するＢＣ資産に係るＢＣ秘密鍵が管理されることとなる。

なお、かかる仕組みにおいては、ユーザーが有するパソコンやスマートフォンなどのデバイスに広く標準実装されているパスキー機能（具体的には、その標準技術規格であるＦＩＤＯ２を用いたもの）を利用する。従前の認証方式であるパスワードを利用したユーザー認証においては、サービスのクライアント（本事業に即していうとユーザー側のこと）及びサーバー（本事業に即していうとＢＣ事業者側のこと）の双方において、ＩＤ及びパスワード情報を管理し、サーバーがクライアントから送付されるＩＤ及びパスワードを識別することによりユーザー認証を行っていたが、ＩＤ及びパスワード情報について、管理負担や情報漏洩リスクなどの問題点を有していた。一方、パスキー機能を利用したユーザー認証（以下「パスキー認証」という）においては、（ａ）クライアントが有するパスキー機能に係る認証器として機能するデバイス（以下「パスキー認証デバイス」という）に

おいて、クライアントの顔認証や指紋認証といった生体情報やＰＩＮコードなどのパターン情報を利用した本人認証（以下「生体・パターン認証」という）が行われた後、（ｂ）クライアント及びサーバー間でいわゆる公開鍵暗号方式に基づくユーザー認証が行われる。そのため、パスキー認証では、クライアントにおいては生体・パターン認証のみを行い、パスキー認証に必要となる秘密鍵（以下「パスキー秘密鍵」という）はパスキー認証デバイスにおいて生成・保存・使用されることから、パスワード等の情報管理が不要となる。また、パスキー秘密鍵については、サーバーに共有する必要がなく、かつ、サーバーに共有されるパスキー認証に係る公開鍵（以下「パスキー公開鍵」という）については、第三者に対してパスキー公開鍵のみが公開されたとしても当該第三者がユーザー認証を行うことができないため、サーバー側における管理負担や情報漏洩リスクが軽減される。なお、パスキー認証におけるパスキー秘密鍵及びパスキー公開鍵は、上記のとおり、クライアント及びサーバー間におけるユーザー認証に利用されるものであり、ＢＣ資産の移転に必要となるＢＣ秘密鍵やＢＣ秘密鍵に対応する公開鍵とは別物である（加えて、下記一連の仕組みにおいても、パスキー秘密鍵及びパスキー公開鍵は、ＢＣ秘密鍵の生成には利用されない）。また、パスキー秘密鍵は、パスキー機能の提供者（当法人及び事業者とは異なる者であり、当法人及び事業者はパスキー秘密鍵を取得しない）のクラウド上に、ユーザーのパスキー認証デバイス上でしか復号化できないようにエンドツーエンドで暗号化された状態で安全に保存されており、当該同一ユーザーによる認証を通じて異なるパスキー認証デバイス間で同期できる。そのため、ユーザーがパスキー認証デバイスの端末変更を行ったとしても、同期した新しいパスキー認証デバイスで同じパスキー秘密鍵を利用して引き続きパスキー認証を行うことができる。

下記一連の仕組みにおいては、当法人が指定する一定の技術的仕様に準拠する形でＢＣ事業者が開発するアプリで、パスキー認証デバイスにインストールされるもの（以下「事業者アプリ」という）も利用する。事業者アプリは、当法人認証サーバーに加えパスキー認証デバイスとＡＰＩ連携を行うほか、その他の機能（即ち、当法人認証サーバーとのＡＰＩ連携の前提として当法人が事業者アプリに求める技術的仕様）については下記も参考にされたい。

＜ＢＣ秘密鍵の管理に係る仕組み＞

（Ａ）ユーザー登録等

①パスキー認証デバイスを有するユーザーが、パスキー認証に関して、当法人認証サーバーとの関係でユーザー登録を行う。

②当法人認証サーバーが、ユーザーに係るパスキー公開鍵を取得する。

③当法人認証サーバーが、ユーザーに係るＩＤ（以下「ユーザー識別ＩＤ」という）を生成する（なお、生成されたユーザー識別ＩＤは、当法人認証サーバーにおいて管理される）。

（Ｂ）ＢＣ秘密鍵の生成・利用・削除

ユーザーによるＢＣ秘密鍵の利用の都度、以下のプロセスにより、ＢＣ秘密鍵の生成・削除が行われる。

④ユーザーが、パスキー認証デバイスにおける生体・パターン認証を行うことにより、当法人認証サーバーに対してパスキー認証を行う。

⑤事業者アプリと当法人認証サーバーとのＡＰＩ連携を通じて、当法人認証サーバーから（パスキー認証デバイス内の）事業者アプリに対してユーザー識別ＩＤが送信

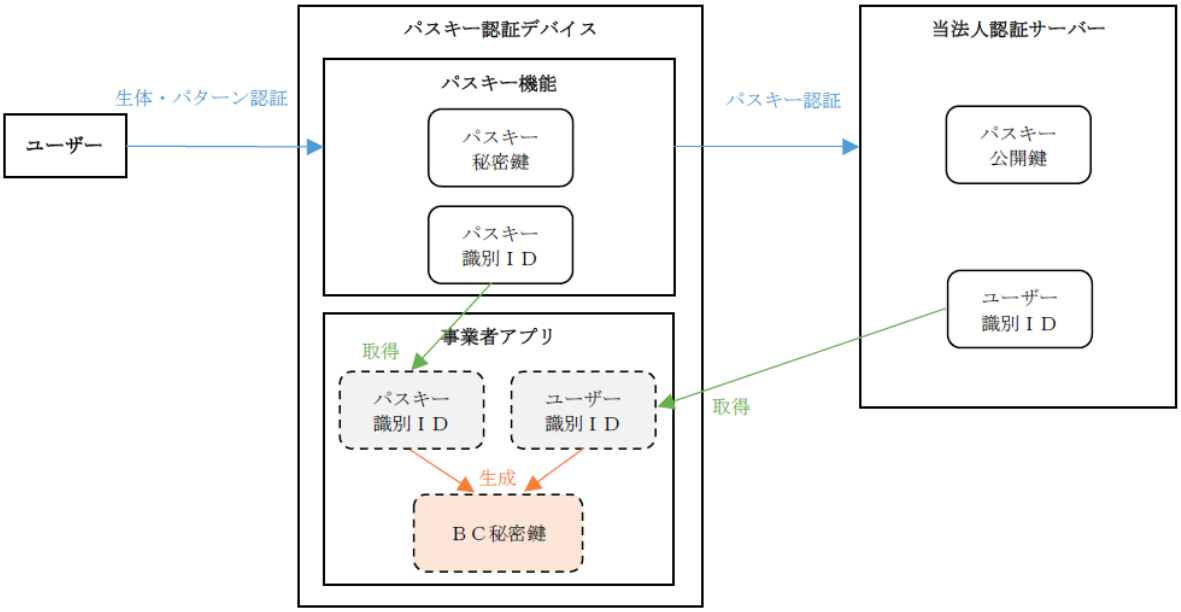
される（なお、ユーザー識別ＩＤは当法人認証サーバーにおいて管理され、ユーザーから当法人認証サーバーに対するパスキー認証がなくとも、当法人がユーザー識別ＩＤを把握・感知することができる状態にはあるが、ユーザーによるパスキー認証がある場合に限って当該ユーザーに係る事業者アプリに対してのみユーザー識別ＩＤを送信し、当法人としては、かかる様態以外でのユーザー識別ＩＤの利用を予定していない）。なお、ＢＣ事業者自体は、ユーザー識別ＩＤを取得しない。

⑥（パスキー認証デバイス内において）事業者アプリとパスキー認証に係るアプリケーションとのＡＰＩ連携を通じて、事業者アプリがパスキー識別ＩＤを取得する（なお、このパスキー識別ＩＤは、パスキー秘密鍵に対して一意に生成されるＩＤであり、ユーザーが生体・パターン認証を行った場合に上記ＡＰＩ連携を通じて、事業者アプリにより取得される）。なお、当法人及びＢＣ事業者自体は、パスキー識別ＩＤを取得しない。

⑦（パスキー認証デバイス内の）事業者アプリにより、ユーザー識別ＩＤ及びパスキー識別ＩＤを基に、ＢＣ秘密鍵が生成される。

⑧ユーザーが、事業者アプリを通じて、ＢＣ秘密鍵を利用する（＝ユーザーが保有するＢＣ資産を移転する）。

⑨ユーザーによるＢＣ秘密鍵の利用後、事業者アプリから、ＢＣ秘密鍵、パスキー識別ＩＤ及びユーザー識別ＩＤの情報は削除される。なお、ＢＣ秘密鍵の生成・利用・削除の過程において、当法人及びＢＣ事業者自体は、ＢＣ秘密鍵を取得しない。



上記仕組みにおいては、ユーザーが保有するＢＣ資産を移転するに際して必要となる行為の中心は、パスキー認証（生体・パターン認証）であり、ユーザーにおいてＢＣ秘密鍵その他の情報を管理する必要はない。また、パスキー認証デバイスにおいてＢＣ秘密鍵の生成・利用・削除（ＢＣ秘密鍵の管理）が行われるため、ＢＣ事業者自身においてＢＣ秘密鍵の管理コストを要しないことに加え、事業者アプリの技術的仕様は当法人からＢＣ事業者に対して提示することから、ＢＣ事業者にとって、独自のウォレット機能を開発・構

築する場合に比べ、より少ないコストでのウォレット機能の実装が可能となると考えられる。

（３）新事業活動を実施する場所

一般社団法人ジャパン・コンテンツ・ブロックチェーン・イニシアティブの本社（東京都中央区日本橋茅場町２－１２－１０）

４．新事業活動及びこれに関連する事業活動の実施時期

本法律の解釈が明確になった時点で速やかに実施

５．解釈及び適用の有無の確認を求める規制について規定する法律及び法律に基づく命令の規定

資金決済に関する法律第二条

１５　この法律において「暗号資産交換業」とは、次に掲げる行為のいずれかを業として行うことをいい、「暗号資産の交換等」とは、第一号又は第二号に掲げる行為をいい、「暗号資産の管理」とは、第四号に掲げる行為をいう。

一　暗号資産の売買又は他の暗号資産との交換

二　前号に掲げる行為の媒介、取次ぎ又は代理

三　その行う前二号に掲げる行為に関して、利用者の金銭の管理をすること。

四　他人のために暗号資産の管理をすること（当該管理を業として行うことにつき他の法律に特別の規定のある場合を除く。）。

６．具体的な確認事項並びに規制について規定する法律及び法律に基づく命令の規定の解釈及び当該規定の適用の有無についての見解

（１）具体的な確認事項

当法人によるＰａｓｓＷａｌｌｅｔの提供及びＢＣ事業者による事業者アプリの提供が、資金決済法第２条第１５項第４号所定の「他人のために暗号資産の管理をすること」に該当するか否か。

（２）当法人の考え

金融庁「事務ガイドライン（第三分冊：金融会社関係）（１６　暗号資産交換業者関係）」（以下「事務ガイドライン」という）のⅠ－１－２－２において、以下のとおり記載されている。

> ③　法第２条第１５項第４号に規定する「他人のために暗号資産の管理をすること」に該当するか否かについては、個別事例ごとに実態に即して実質的に判断するべきであるが、利用者の関与なく、単独又は関係事業者と共同して、利用者の暗号資産を移転でき得るだけの秘密鍵を保有する場合など、事業者が主体的に利用者の暗号資産の移転を行い得る状態にある場合には、同号に規定する暗号資産の管理に該当する。
>
> 〔略〕
>
> （注２）上記③の「主体的に利用者の暗号資産の移転を行い得る状態」に該当するか否かについては、個別事例ごとに実態に即して実質的に判断するべきであるが、例えば、以下のような場合は、「主体的に利用者の暗号資産の移転を行い得る状態」には該当しないものと考えられる。

・事業者が、単独又は関係事業者と共同しても、利用者の暗号資産を移転するために必要な秘密鍵の一部を保有するにとどまり、事業者が単独又は関係事業者と共同して保有する秘密鍵のみでは利用者の暗号資産を移転することができない場合。
・事業者が利用者の暗号資産を移転することができ得る数の秘密鍵を保有する場合であっても、その保有する秘密鍵が暗号化されており、事業者が当該暗号化された秘密鍵を復号するために必要な情報を保有していない場合。

また、令和元年資金決済法等改正に係る政令・内閣府令案等に関して実施されたパブリックコメントに係る金融庁の令和２年４月３日付「コメントの概要及びコメントに対する金融庁の考え方」（以下「本パブコメ回答（令和元年資金決済法等改正）」という）のＮｏ９乃至１２、１６、１７及び１８、並びに、「事務ガイドライン（第三分冊：金融会社関係）」（１６　暗号資産交換業者関係）の一部改正（案）に関して実施されたパブリックコメントに係る金融庁の令和５年３月２４日付「コメントの概要及びコメントに対する金融庁の考え方」（以下「本パブコメ回答（事務ガイドライン改正）」といい、「本パブコメ回答（令和元年資金決済法等改正）」と併せて「本パブコメ回答」という）のＮｏ４４において、金融庁の考え方として、以下のとおり記載されている。

＜本パブコメ回答（令和元年資金決済法等改正）Ｎｏ９＞
個別事例ごとに実態に即して実質的に判断されるべきものではありますが、事業者が利用者の暗号資産を移転するために必要な秘密鍵を一切保有していない場合には、当該事業者は、主体的に利用者の暗号資産の移転を行い得る状態にないと考えられますので、基本的には、資金決済法第２条第７項第４号〔注：現行資金決済法の第２条第１５項第４項のこと。以下同じ〕に規定する「他人のために暗号資産の管理をすること」に該当しないと考えられます。

＜本パブコメ回答（令和元年資金決済法等改正）Ｎｏ１０～１２＞
個別事例ごとに実態に即して実質的に判断されるべきものではありますが、事業者が利用者の暗号資産を移転するために必要な秘密鍵の一部を保有するにとどまり、事業者の保有する秘密鍵のみでは利用者の暗号資産を移転することができない場合には、当該事業者は、主体的に利用者の暗号資産の移転を行い得る状態にないと考えられますので、基本的には、資金決済法第２条第７項第４号に規定する「他人のために暗号資産の管理をすること」に該当しないと考えられます。

＜本パブコメ回答（令和元年資金決済法等改正）Ｎｏ１６＞
個別事例ごとに実態に即して実質的に判断されるべきものではありますが、御質問のサービスを提供する事業者が、クラウドストレージ内に保管されている利用者の暗号資産を移転するために必要な秘密鍵にアクセスする権限を有していないなど、当該事業者が主体的に利用者の暗号資産の移転を行い得る状態にない場合には、基本的には、資金決済法第２条第７項第４号に規定する「他人のために暗号資産の管理をすること」に該当しないと考えられます。

＜本パブコメ回答（令和元年資金決済法等改正）Ｎｏ１７、１８＞
個別事例ごとに実態に即して実質的に判断されるべきものではありますが、御質問のサ

ービスを提供する事業者が、スマートコントラクト内に保管されている利用者の暗号資産を移転するために必要な秘密鍵にアクセスする権限を有しておらず、当該スマートコントラクトによる暗号資産の移転先を指定し、又は変更し得る権限を有していないなど、当該事業者が主体的に利用者の暗号資産の移転を行い得る状態にない場合には、基本的には、資金決済法第２条第７項第４号に規定する「他人のために暗号資産の管理をすること」に該当しないと考えられます。

＜本パブコメ回答（事務ガイドライン改正）Ｎｏ４４＞
個別事例ごとに実態に即して実質的に判断されるべきものではありますが、秘密鍵が一つしか存在しない、シングルシグ・シグネチャ方式の場合でも、秘密分散等の技術を用いて分散管理を行う場合において、事業者が利用者の暗号資産を移転するために必要な秘密鍵の一部を保有するにとどまり、事業者のみでは利用者の暗号資産を移転することができない場合には、当該事業者は、「主体的に利用者の暗号資産の移転を行い得る状態」にないと考えられます。

以上のとおり、事務ガイドライン及び本パブコメ回答においては、（あ）暗号資産を移転するために必要な秘密鍵を一切保有していない場合やその一部を保有するにとどまり当該一部の秘密鍵のみでは暗号資産を移転することができない場合、（い）秘密鍵を保有する場合であっても、その保有する秘密鍵が暗号化されており、事業者が当該暗号化された秘密鍵を復号するために必要な情報を保有していない場合、（う）秘密鍵にアクセスする権限を有していない場合など、「主体的に利用者の暗号資産の移転を行い得る状態にない場合」には、資金決済法第２条第１５項第４号所定の「他人のために暗号資産の管理をすること」に該当しないとの考え方が示されている。

この点、当法人によるＰａｓｓＷａｌｌｅｔの提供及びＢＣ事業者による事業者アプリの提供における当法人及びＢＣ事業者は、以下のとおり、上記（あ）～（う）のいずれの場合にも該当し（又は、これらの場合に類似し）、「主体的に利用者の暗号資産の移転を行い得る状態」ではないことから、当法人によるＰａｓｓＷａｌｌｅｔの提供及びＢＣ事業者による事業者アプリの提供は資金決済法第２条第１５項第４号所定の「他人のために暗号資産の管理をすること」に該当しないと考える。

・ユーザーのＢＣ秘密鍵の生成・利用・削除の過程において、当法人及びＢＣ事業者自体は、ユーザーのＢＣ秘密鍵を取得しない（ユーザーのＢＣ秘密鍵にアクセスすることもできない）（前記３．（２）⑨参照）。
・ユーザーのＢＣ秘密鍵は、ユーザー識別ＩＤ及びパスキー識別ＩＤを基に、ＢＣ秘密鍵が生成される（前記３．（２）⑨参照）ところ、当法人はパスキー識別ＩＤを取得せず、また、事業者はユーザー識別ＩＤ及びパスキー識別ＩＤを取得しない（前記３．（２）⑤及び⑥参照）ことから、当法人及びＢＣ事業者は、当該ユーザーのＢＣ秘密鍵を生成・復号することはできない。

７．その他
【特になし】