

様式第十三（第4条関係）

新事業活動に関する確認の求めに対する回答の内容の公表

1. 確認の求めを行った年月日
令和6年9月12日

2. 回答を行った年月日
令和6年10月8日

3. 新事業活動に係る事業の概要

本照会を行う事業者（以下「照会者」という。）は、ブロックチェーンを活用したサービスを提供する事業者（以下「BC事業者」という。）に対して、NFTや暗号資産などのブロックチェーン上の記録（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。）の管理方法として、照会者が設置及び運営する認証サーバー（以下「照会者認証サーバー」という。）とのAPI連携を提供するサービス（以下「本サービス」という。）を提供することを検討している。具体的な内容は以下のとおり。

（1）ユーザー登録

- ・BC事業者のユーザーが、パスキー機能を利用した認証（以下「パスキー認証」という。）（注）に関して、照会者認証サーバーとの関係でユーザー登録を行う。

（注）パスキー認証においては、（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きユーザー認証（パスキー認証デバイスにおいて保管されるパスキー認証用の秘密鍵（以下「パスキー秘密鍵」という。）とサーバーで保管されるパスキー認証用の公開鍵（以下「パスキー公開鍵」という。）による認証）が行われる。パスキー秘密鍵は、パスキー機能の提供者（照会者及びBC事業者とは異なる者であり、照会者及びBC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。

- ・照会者認証サーバーが、ユーザーに係るパスキー公開鍵を取得する。
- ・照会者認証サーバーが、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、照会者認証サーバーにおいて管理される）。

（2）BC秘密鍵の利用方法

- ・ユーザーが、パスキー認証デバイスにおいて生体・パターン認証を行うことにより、照会者認証サーバーに対してパスキー認証を行う。
- ・BC事業者が提供するアプリ（以下「事業者アプリ」という。）と照会者認証サーバーとのAPI連携を通じて、照会者認証サーバーから（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は照会者認証サーバーにおいて管理され、ユーザーから照会者認証サーバーに対するパスキー認証がなくとも、照会者がユーザー識別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、照会者としては、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。

- ・(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できる)。なお、照会者及びBC事業者自体は、パスキー識別IDを取得しない。
- ・(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。
- ・ユーザーが、事業者アプリを通じて、BC秘密鍵を利用して、ユーザーが保有するBC資産の移転を行う。
- ・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の情報が削除される。なお、BC秘密鍵の生成・利用・削除の過程において、照会者及びBC事業者自体は、BC秘密鍵を取得しない。

4. 確認の求めの内容

照会者による本サービスの提供及びBC事業者による事業者アプリの提供が、資金決済に関する法律第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。

5. 確認の求めに対する回答の内容

資金決済に関する法律第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しているが、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と判断している。

本照会に対する判断については次のとおりであるが、照会書で確認できる事実内容を前提としており、その内容に変更がある場合、又は新たな事実が認められる場合には、判断が変わる可能性がある。

本サービスにおいては、

- ・照会者及びBC事業者は、BC秘密鍵を取得しない
- ・BC秘密鍵は、ユーザー識別ID及びパスキー識別IDを基に、ユーザーのパスキー認証デバイス内で生成されるところ、照会者はユーザー識別IDを照会者認証サーバーにおいて管理し、ユーザーから照会者認証サーバーに対するパスキー認証がなくとも、照会者がユーザー識別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を送信することとしており、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
- ・仮に照会者がユーザー識別IDを利用したとしても、照会者はパスキー識別IDを取得しないことからBC秘密鍵を生成することはできない
- ・BC事業者は、ユーザー識別ID及びパスキー識別IDの双方を取得しないことからBC秘密鍵を生成することはできず、また照会者と共同したとしてもBC秘密鍵を生成することはできない

とされており、照会者及びBC事業者においては、単独又はお互いに共同したとしても、主体的に利用者の暗号資産の移転を行い得る状態にはないと考えられる。

以上から、照会者による本サービスの提供及びBC事業者による事業者アプリの提供は、資金決済に関する法律第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」には該当しないものと考えられる。

(記載要領)

「3. 新事業活動に係る事業の概要」、「4. 確認の求めの内容」及び「5. 確認の求めに対する回答の内容」中、事業者の事業上の秘密に該当する部分については、これを公表の対象として記載しない。