

日本国内における 仮想通貨ウォレットの実態調査¹

栗田 青陽

株式会社メルカリ

DP2019-1

2019年03月14日

<<要旨>>

金融庁が設置した「仮想通貨交換業等に関する研究会」（以下、研究会）において、仮想通貨カストディ業務について、「決済に関連するサービスとして、一定の規制を設けた上で、業務の適正かつ確実な遂行を確保していく必要があると考えられる」という報告がなされた。

仮想通貨カストディ業務には様々な形態のものが想定されるなかで、イノベーションに配慮しつつ、異なるリスクレベルに応じて適切な規制を課していくために、国内の仮想通貨カストディ業務の実態を把握することには一定の重要性があると考えられる。

仮想通貨カストディにあたる業務の範囲は本調査の段階では明確に定められていないが、本調査では、国内における仮想通貨ウォレット提供者にヒアリングを行い、実態を調査した。

本ディスカッションペーパーの内容は執筆者の個人的見解であり、所属する組織及びCryptoassets Governance Task Forceとしての公式見解を示すものではありません。

¹ 本調査の実施に際し、多大なご協力を頂いた仮想通貨ウォレット提供者の皆様にご感謝申し上げます。アンダーソン・毛利・友常法律事務所の河合健、長瀬威志の各氏には貴重なご助言を頂いた。楠正憲、佐藤雅史、島岡政基、須賀祐治、菅原謙一、中島博敬、林達也の各氏、ならびにCryptoassets Governance Task Force Security Working Groupの参加者の方々からは多くの有益なコメントを頂いた。ここに記して感謝申し上げます。

1. はじめに

2018年3月8日に金融庁が設置し、2018年12月14日まで全11回にわたって開かれた「仮想通貨交換業等に関する研究会」²において、仮想通貨カストディ業務に対する規制の必要性が検討された。

同研究会の報告書³（以下、報告書）によると、仮想通貨カストディ業務とは、「仮想通貨の売買等は行わないが、顧客の仮想通貨を管理し、顧客の指図に基づき顧客が指定する先のアドレスに仮想通貨を移転させる業務」とされ、業務を行う上では、「サイバー攻撃による顧客の仮想通貨の流出リスク、業者の破綻リスク、マネーロンダリング・テロ資金供与のリスク等、仮想通貨交換業と共通のリスクがあると考えられること」、および「仮想通貨カストディ業務を行う業者についても、マネーロンダリング・テロ資金供与規制の対象にすることを各国に求める旨の改訂 FATF 勧告が採択されたこと」から、「仮想通貨交換業者に求められる対応のうち、顧客の仮想通貨の管理について求められる以下のような対応と同様の対応を求めることが適当と考えられる」とされている。

- 登録制
- 内部管理体制の整備
- 業者の仮想通貨と顧客の仮想通貨の分別管理
- 分別管理監査、財務諸表監査
- 仮想通貨流出時の対応方針の策定・公表、弁済原資の保持
- 顧客の仮想通貨の返還請求権を優先弁済の対象とすること
- 利用者保護や業務の適正かつ確実な遂行に支障を及ぼすおそれがあると認められる仮想通貨を取り扱わないこと
- 顧客の本人確認、疑わしい取引の行政当局への届出

また、「仮想通貨カストディ業務には様々な形態のものが想定されるところ、異なるリスクレベルに応じて適切な規制を課していくためにも、規制対象となる業務の範囲を明確にしておくことが重要」という意見があった。

加えて、報告書のおわりには、「引き続き、取引の実態を適切に把握していくとともに、イノベーションに配慮しつつ、利用者保護を確保していく観点から、リスクの高低等に応じて規制の柔構造化を図ることを含め、必要に応じて更なる検討・対応を行っていくことが重要である」と記載されている。

そこで、国内における仮想通貨ウォレット提供者⁴に対してヒアリングを行い、実態を調査した。

² <https://www.fsa.go.jp/news/30/singi/kasoukenkyuukai.html>

³ <https://www.fsa.go.jp/news/30/singi/20181221.html>

⁴ カストディはウォレットと呼ばれる場合もあるが、本紙では、研究会において規制の必要があるとされたカストディよりも広い概念としてウォレットを使用する。

2. 定義

2.1 ウォレット

研究会の第9回配布資料⁵では以下の4種類のウォレットが挙げられている。

1. オンラインウォレット
2. ソフトウェアウォレット
3. ハードウェアウォレット
4. ペーパーウォレット

1.のオンラインウォレットとは、事業者が秘密鍵を管理し、顧客が事業者に対して仮想通貨の移転を指示するサービスとして提供されるウォレットである。

2.のソフトウェアウォレットとは、利用者の所有するデバイス上で動作し、デバイス内で秘密鍵を管理するソフトウェアである。

3.のハードウェアウォレットとは、利用者の所有するハードウェアで秘密鍵を管理し、パーソナルコンピューター等に接続して操作を行うハードウェアである。

4.のペーパーウォレットとは、利用者の所有する紙等の非電子的媒体に秘密鍵の文字列そのものが記録されたものである。

2.2 カストディ

報告書において規制の対象にすべきとされているカストディは、「顧客の仮想通貨を管理し、顧客の指図に基づき顧客が指定する先のアドレスに仮想通貨を移転させる業務」とされている。また、顧客の仮想通貨の管理の方法としては、「顧客の仮想通貨アドレスに対応した（仮想通貨の移転に必要な）秘密鍵を業者が管理する方法」と「顧客の仮想通貨アドレスから、業者が秘密鍵を管理する業者の仮想通貨アドレスに、仮想通貨の移転を受けて管理する方法」が例として挙げられている。このことから、ウォレットについては、規制の対象となるカストディに含まれる可能性があるものと考えられる。

⁵ <https://www.fsa.go.jp/news/30/singi/20181112-3.pdf>

3. オンラインウォレットの事業の例

様々な形態のサービスが存在すると思われるオンラインウォレットの事業の例を挙げる。現状国内でサービスを提供しているものだけではなく、海外で提供されている事業を含む。ただし、ここに挙げられていない事業も存在する可能性がある。

3.1 送金サービス

仮想通貨において資金移動業に似た役割を果たす事業者の提供するサービスである。事業者が用意した口座に対して利用者が入出金・他の利用者の口座への移転を指示する。

ブロックチェーン上でトランザクションを発行すると、発行の都度手数料がかかる。また、日本最大のカード決済総合サービスであるCAFISが1秒あたり平均270件以上の決済を処理している⁶のに対して、ビットコインは1秒あたり7トランザクションの処理が仕様上の上限とされており、同時に多数のユーザーがトランザクションを発行するとすぐに処理が滞る。この処理時間を短縮しようとするするとトランザクション発行手数料が高騰する。

そこで、少額の取引が頻繁に発生する用途のために、事業者が送金サービスを提供する場合がある。事業者のデータベース上で利用者の口座残高が付け替えられるため、高速に、かつトランザクション発行手数料を必要とせずに送金できる。

利用者間で取引が発生する投げ銭⁷やフリーマーケットのために事業者が送金サービスを提供している事例がある。



図3-1 Monappy⁸内の投げ銭が可能な画像投稿サービス⁹

⁶ CAFISによると（https://solution.cafis.jp/about/img/monthly_data.pdf）、2017年度末の月間処理件数は7億1,726万件であり、1秒あたりの処理件数は平均約277件である。

⁷ 物品・サービスの売買などに依らない、個人間における少額の寄附行為を指す。

⁸ <http://monappy.jp/>

⁹ Monappyは2018年9月に顧客資産の45.8%を保管していたホットウォレットから当時の価値で1,500万円程度の仮想通貨(93078.7316 mona)が不正に出金される事件が発生し、2019年2月時点ではサービスを停止している（<https://link.medium.com/uBgrvGYxSU>）。当時の円に換算した不正出金発生前の預かり総額は3,000万円程度であったと考えられる。



図3-2 Monappy内のフリーマーケット
で販売されていたお米

事業者が提供する送金サービスでは、トランザクションの発行手数料が削減されるだけでなく、利用者が送金相手のウォレットのアドレスを知らなくても、サービス上のアカウント名に対して送金ができる利点もある。Twitter上のボット（自動応答プログラム）アカウントとの対話形式のインターフェースで提供されるチップボットと呼ばれる送金サービスは、Twitter上でチップを送る手段として利用されている。

以下に、この種類のオンラインウォレットである@tipmona¹⁰を利用する際の画面を図で示しながら、具体的な仕組みを説明する。なお、Twitter上での対話形式であり、新しい投稿が古い投稿よりも上に表示されるため、図中において、対話は下から上の順に進行している。

入金とは、図3-3のように、ユーザーはボットアカウントに対して「deposit」というコマンドを送信する。応答として、ボットアカウントは入金を受け付けるアドレスを送信する。ユーザーがこのアドレスに対してブロックチェーン上で送金を行うと、その金額がユーザーの残高となる。

depositされた仮想通貨は、ウォレット事業者によって管理された状態になっている。



図3-3 入金

¹⁰ <https://twitter.com/tipmona>

図3-4のように、チップボットに対して「balance」コマンドを送信すると、応答としてボットアカウントは現在の残高を送信する。



図3-4 残高の確認

図3-5は送金の様子である。「tip」コマンドと合わせて、送金先のTwitterアカウントと数量を指定すると、コマンドの指示に従い、指定した数量が指定したTwitterアカウントに移動する。ボットアカウントは残高の移動があったことを送金者と送金先のTwitterアカウントに通知する。

この場合の暗号資産の移動は、チップボットを提供している事業者のデータベース上で行われるものであり、ブロックチェーンネットワーク上での実際の送金はこの時点では行われていない。



図3-5 送金

ユーザーが仮想通貨を引き出すには、図3-6のように「withdraw」コマンドを送信して、数量と引き出し先のアドレスを指定する。これにより、チップボットはブロックチェーン上で送金トランザクションを作成し、利用者がトランザクションの様子を確認できるWebサービスのURLを送信する。



図3-6 出金

仮想通貨は小数点以下の単位で取り扱うことが可能であることから、「0.114114（いいよいいよ）」や「0.315(最高)」、「39（サンキュー）」、「0.8888（パチパチパチパチ:拍手の音）」等、金額に意味を込めて送ることも行われている。

3.2 一般利用者向けの暗号資産保管サービス

送金機能を提供する場合もあるが、送金サービスが送金を主な用途としているのに対して、より保管の目的が強く、利用するたびに必要な金額を入金するというよりは、他所で仮想通貨が必要になった場合に引き出し元となるウォレットサービスである。

3.3 機関・資産家向けの暗号資産保管・管理サービス

いわゆる金融機関が行うカストディに近い機能を提供するサービスが考えられる。

仮想通貨交換業者や機関投資家、資産家等、大きな額の暗号資産を保管・管理する。

また、顧客の代理人として、仮想通貨のトレードや、投資性を有するICOトークンの受渡決済、議決権等のトークンに付随する権利の行使、税務処理などを行う業務を担うことや、海外の同様の事業者と連携し、国境を越えた暗号資産への投資を受託することも考えられる。

現在日本国内にこのようなサービスを提供する事業者は存在しない。

海外においてはCoinbase Custody¹¹等があり、最低で百万米国ドル以上の仮想通貨の残高を必要とするなど、大きな額の仮想通貨を預かることを前提としている。

¹¹ <https://custody.coinbase.com/>

| | |
|---|---|
| <p>IMPLEMENTATION FEE</p> <p>\$0 - \$10,000 <small>DEPENDING ON USE-CASE</small></p> | <p>PRICING INCLUDES</p> <ul style="list-style-type: none"> ✓ Segregated cold storage ✓ Regulated Custody ✓ Industry-leading insurance ✓ Audited statements & financials ✓ Dedicated coverage ✓ SLAs on fund transfers |
| <p>CUSTODY FEE</p> <p>50 bps <small>ANNUALIZED</small></p> | <p>COMING SOON</p> <ul style="list-style-type: none"> ✓ Multi-user accounts ✓ ERC20 support ✓ Staking |
| <p>MINIMUM BALANCE</p> <p>\$1,000,000</p> | |

[SIGN UP](#)
[SIGN IN WITH COINBASE](#)

図3-7 Coinbase Custody の価格表

適格投資家のみを対象とするICOトークンや移転規制等の制限のあるトークンは、トークンが自由に移転できた場合に、その制限が実効性を持たないことを懸念されているが、事業者が投資家の資格を保証して購入を代行し、事業者の口座に紐づけて管理することで、その制限の実効性を担保できる可能性がある。

3.4 トークンエコノミーサービスに付随するオンラインウォレットサービス

トークンエコノミーサービスの明確な定義はないが、一般にブロックチェーンを活用して電子的にトークン（証票）を発行し、サービス内にトークンの経済循環を構築するものであると考えられる。

具体的には、サービスに貢献した利用者に対してインセンティブとしてトークンを付与し、サービスの利用やサービス内における利用者間の取引にトークンを必要とするなどの形態が考えられる。

トークンの利用価値によっては価格が付き、仮想通貨として流通するものがある。

トークンは、スマートコントラクトと呼ばれる、ブロックチェーン上で自律的に動作するプログラムに記述されたルールに従って発行される。特定の事業者がトークンを発行し、管理を行う場合もあるが、特定の管理者がいない場合もある。また、発行したトークンを用いて資金調達が行われる場合もある。

例として、ビットコインは特定の管理者がいないトークンエコノミーであると考えられる。ビットコインの送金を検証し記録したマイナーには新規に発行されるビットコインがインセン

タイプとして付与される。送金を行う利用者はマイナーに手数料としてビットコインを支払う。

トークンエコノミーが事業者によるサービスとして提供される場合、利用者のトークンを管理するオンラインウォレット機能が付随する場合がある。海外の事例として、ブログサービスのsteemitがある。

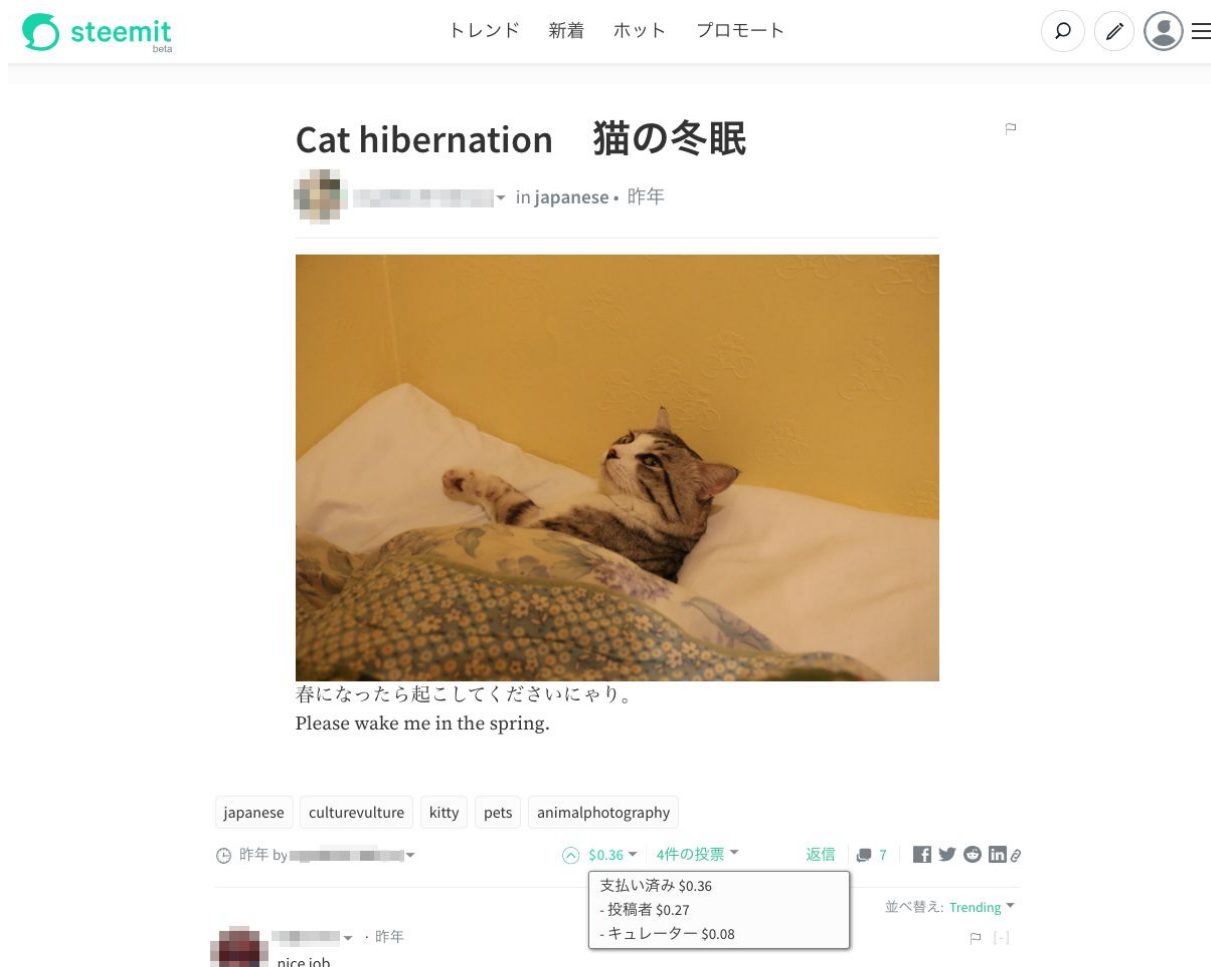


図3-8 steemitに投稿され0.36米ドル相当のトークンを獲得した記事

4人のフォロワー | 投稿1件 | 誰もフォローしていません

登録年月：2018年6月

ブログ コメント 返信 報酬

ウォレット 設定

残高 アクセス権 パスワード

STEEMやSTEEM POWERを購入する

STEEM

いつでもどこへでも送ることができる取引可能なトークンです。
SteemはパワーアップによってSTEEM POWERに変換できます。

0.000 STEEM

STEEM POWER

投稿への支払額の制御権を持ち、キュレーション報酬を得ることが可能になる、プラットフォームにおける影響力を持つトークンです。

現在のSTEEM POWERの一部は委託されたものです。委託は影響力の寄付や、新規ユーザーがSteemitでアクションを起こしやすくするために行われます。委託された額は変動する可能性があります。

0.101 STEEM
(+4.942 STEEM)

STEEM DOLLARS

Tradeable tokens that may be transferred anywhere at anytime.

\$0.000

貯蓄口座

引き出しに3日間の待ち時間が必要となる貯蓄口座です。

0.000 STEEM

\$0.000

推定アカウント価格

推定値はSteemの平均値に基いてUSドルで表されます。

\$0.03

図3-9 steemitにログインするとサービス上の口座の残高を確認することができる

Confirm Transfer From Savings

from

to

amount

0.000 STEEM

memo

request_id

Ok

キャンセル

図3-10 steemitのサービス上の口座残高を引き出すことができる

4. 国内ウォレットの実態についての調査

国内のオンラインウォレット提供者とソフトウェアウォレット提供者を対象に、利用実態や運営状況の実態について調査を行った。

オンラインウォレットは、それに付随する暗号資産を含めて提供者が管理していることから、利用実態については提供者によって把握されている。

ソフトウェアウォレットは、個人が所有するコンピューターやスマートフォンの中に鍵を保管することで仮想通貨を管理しているが、こうしたソフトウェアの中には、提供者によって利用状況の統計データが収集されているものがあり、こうした場合も利用実態が把握されている。

本調査は、ウォレット提供者に対して協力を呼びかけ、Google Formによるアンケート形式、対面・チャット・メール等による対話形式のヒアリング、あるいはこれらの両方の手段によって実施した。

調査は2018年12月から2019年2月にかけて実施した。

調査項目は別添資料のとおりである。ウォレット提供者の把握する統計データの種類・範囲や、サービスの形態がウォレットによって異なることが予想されたことや、答えにくい項目があることで寄せられる回答が減少することを避けることを目的として、すべて任意回答とした。また、より詳細な実態を調査するため、ウォレット提供者ごとに個別で追加の質問を行い、回答を得たものもある。

4.1 調査対象

オンラインウォレット提供者3者とソフトウェアウォレット提供者2者に協力を依頼し、オンラインウォレット提供者2者、ソフトウェアウォレット提供者2者から回答があった。また、Twitterで広く協力を呼びかけたところ、オンラインウォレット提供者1者、ソフトウェアウォレット提供者3者から回答があった。

あわせて、オンラインウォレット提供者から3件、ソフトウェアウォレット提供者から5件の回答を得ることができた。なお、一般利用者向けの暗号資産保管サービスと、機関・資産家向けの暗号資産保管・管理サービスに該当するオンラインウォレット提供者からは回答を得ていない。

これらのウォレットを便宜的に以下の通り区分した。

- 送金サービスを提供するオンラインウォレット
(オンラインウォレットA、オンラインウォレットB)
- トークンエコノミーサービスを提供するオンラインウォレット
(オンラインウォレットC)
- Webで提供されるソフトウェアウォレット
(ソフトウェアウォレットA、ソフトウェアウォレットB)
- スマートフォンアプリケーションとして提供されるソフトウェアウォレット
(ソフトウェアウォレットC、ソフトウェアウォレットD、ソフトウェアウォレットE)

この各区分ごとに、どのようなウォレットかを説明する。

4.1.1 送金サービスを提供するオンラインウォレット (オンラインウォレットA、オンラインウォレットB)

オンラインウォレットAとオンラインウォレットBは、いずれもTwitter上のボット（自動応答プログラム）アカウントとの対話形式のインターフェースで提供されている、チップボットと呼ばれるサービスである。

4.1.2 トークンエコノミーサービスを提供するオンラインウォレット (オンラインウォレットC)

オンラインウォレットCはトークンエコノミーサービスをWebサービスとして提供する事業者が、Webサービスの機能の一部として提供しているウォレットである。

当該サービスの利用登録を行うと、Webサービス上にオンラインウォレットの口座が用意される。利用者はサービスに対してコンテンツを投稿し、投稿したコンテンツが他の利用者から高い評価を得ると、インセンティブとしてトークンが得られ、口座に残高が付与される。

この事業者はICOを行って資金を調達した。トークンは海外の取引所に上場しており、2019年2月時点でも取引が行われている。

4.1.3 Webで提供されるソフトウェアウォレット (ソフトウェアウォレットA、ソフトウェアウォレットB)

ソフトウェアウォレットAとソフトウェアウォレットBは、いずれもブラウザ上で動作するウォレットである。

サーバーはブラウザからのアクセスに対して、JavaScript等で実装されたブラウザ上で動作するウォレットプログラムを提供する。ブラウザ上で秘密鍵を生成するか、ユーザーがウォレットプログラムに対して自身の秘密鍵を入力することで利用が可能となる。秘密鍵はサーバーに送信されず、ブラウザを閉じることで削除される¹²。

図4-1は、ブラウザ上で動作するソフトウェアウォレットのもにゃ¹³にて、秘密鍵を導出するニーモニックコード（単語の列。乱数を人間が扱いやすくするために単語を使って表現したもの）を作成した画面である。このニーモニックコードをウォレットプログラムで処理することで秘密鍵が導出される。ユーザーはこのニーモニックコードを控えておくことで、秘密鍵そのものではなく、人間の読みやすい形でバックアップを取得することができる。

¹² ブラウザ内に秘密鍵が保管され、次回アクセス時に復元されるものもある。

¹³ <https://monya-wallet.github.io/>

<
パスフレーズ

- 英単語を正確に、紙に手書きしてください。
- 英単語のスクリーンショットを撮影・コピーしないでください。
- 他人に知れ渡ると、コインを盗まれる可能性があります。
- チェックボックスは確認のためにお使いください。

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐
6 ☐
7 ☐
8 ☐
9 ☐
10 ☐
11 ☐
12 ☐

次へ

図4-1 ニーモニックコードの作成

図4-2は、ユーザーがニーモニックコードを入力し、過去に作成した秘密鍵を復元する場合の画面である。

<
ウォレットの復元

単語を入力してください。候補を絞り込んだ場合、確定します。絞り込まない場合、画面下に候補が表示されます。

単語をリセット

次へ

図4-2 秘密鍵の復元

4.1.4 スマートフォンアプリケーションとして提供されるソフトウェアウォレット（ソフトウェアウォレットC、ソフトウェアウォレットD、ソフトウェアウォレットE）

ソフトウェアウォレットC、ソフトウェアウォレットD、ソフトウェアウォレットEは、スマートフォン用のアプリケーションとして動作するウォレットである。

アプリケーション内で秘密鍵を生成するか、ユーザーが秘密鍵を入力することで利用を開始する。秘密鍵は端末内に保存し、サーバーに秘密鍵の情報は送信されない。

この種類のウォレットの場合にも、通常は鍵のバックアップや復元の方法が提供されている。

ソフトウェアウォレットCはウォレット機能に加え、ブラウザ機能を備えている。このブラウザ機能は、通常のWebブラウジング機能に加え、Webアプリケーションから提示される未署名のトランザクションに秘密鍵を使って署名し、ブロックチェーンネットワークに送信する機能を有する。こうした機能はDApps（Decentralized Applications, 分散型アプリケーション）ブラウザと呼ばれる。

DAppsとは、ブロックチェーン上でスマートコントラクトプログラムによって実現されたアプリケーションそのもの、あるいはブロックチェーン上の記録に基づき動作するWebアプリケーション等を指す。DAppsブラウザは、ブロックチェーン上の記録に基づき動作するWebアプリケーションの閲覧と操作を行うためのブラウザである。図4-3は、分散型アプリケーション、DAppsブラウザ、ブロックチェーンの関係を示したものである。

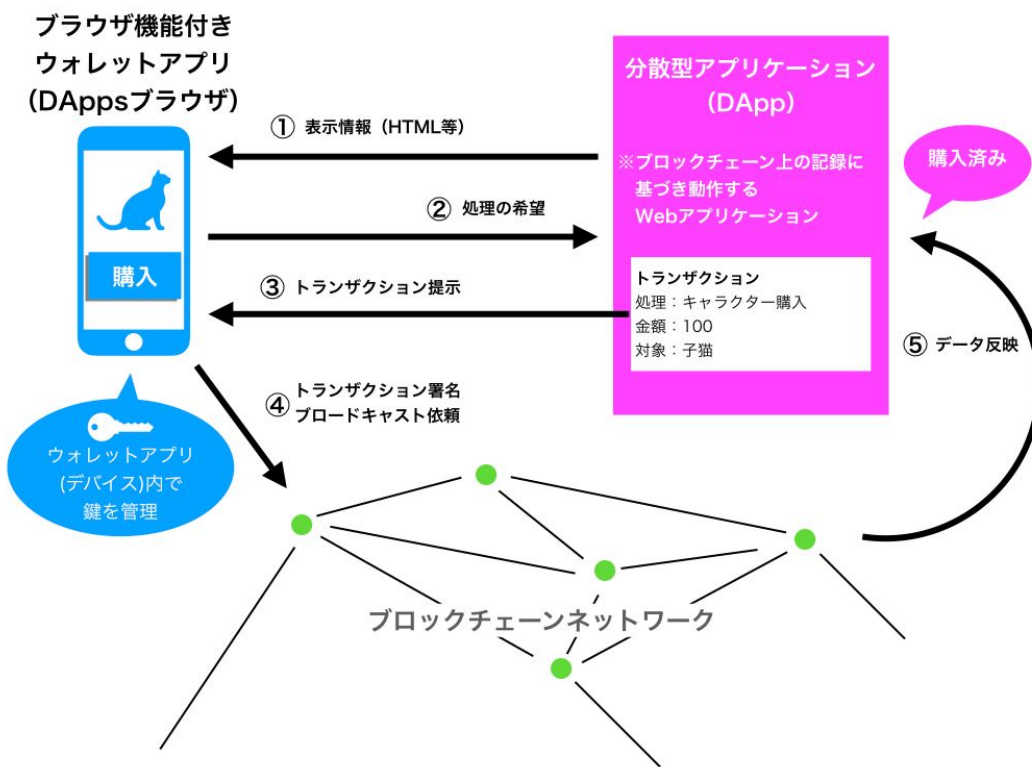


図4-3 DAppsブラウザの概念図

図4-4から図4-6はそれぞれ、DAppsブラウザを搭載する、スマートフォンアプリケーションウォレットのtokenPocket¹⁴を利用した図である。このアプリケーションを利用して分散型として提供されているWebサイトに接続し（図4-4）、ゲームキャラクターの猫を購入するトランザクションに署名を行い（図4-5）、ブロックチェーン上で個別の猫を表すユニークなトークンが自身のウォレットの鍵に紐付いた状態となったことがWebアプリケーションに反映された様子（図4-6）である。

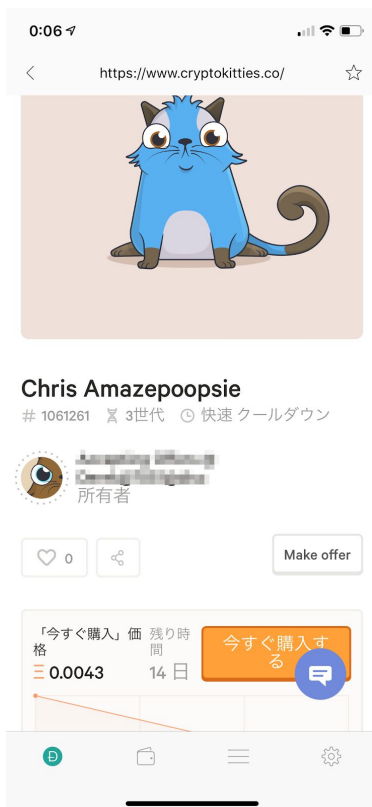


図4-4 閲覧

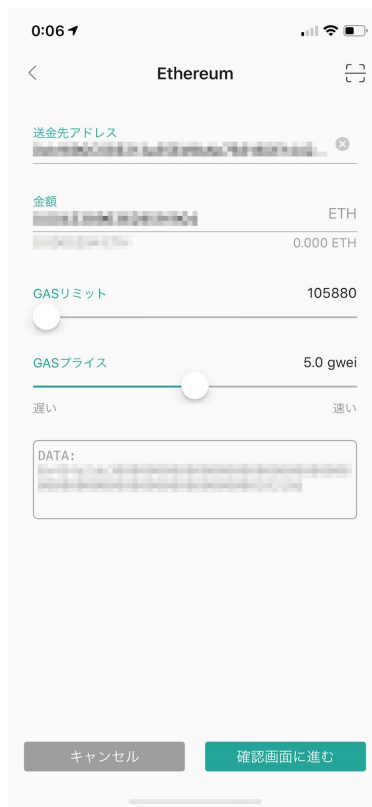


図4-5 署名



図4-6 反映

¹⁴ <https://tokenpocket.jp/>

4.2 調査結果

表4-1に、各ウォレットの預かり総額、高額な送金の規模、収入、支出、運営の状況（個人法人の別、報酬を得ている・支払っているか等）の回答を一覧にした。仮想通貨の額で回答があったものは2019年2月25日時点の時価¹⁵をもとに円に換算した。ただし高額な送金の規模は送金時点の時価から算出した。

表4-1 各ウォレット提供者の回答一覧

| 回答者 | 秘密鍵の管理場所 | 預かり総額 | 高額な送金の規模 | 収入（年間） | 支出（年間） | 運営の状況 |
|--------------|----------|-------------------|----------------------|--------------------|--------------------|----------------|
| オンラインウォレットA | ウォレット提供者 | 300万円程度 | 400万円程度 (通常数万円程度) | 収入なし | 48,000円 | 個人 (無報酬) |
| オンラインウォレットB | ウォレット提供者 | 40万円程度 | 7万円程度 | 数十円 (手数料) | 240,000円 | 個人 (無報酬) |
| オンラインウォレットC | ウォレット提供者 | 80万円程度 | 数千円程度 | 回答なし | 回答なし | 法人 15名程度 |
| ソフトウェアウォレットA | 利用者の端末 | 収集していない | 不明 | 収入なし | 240,000円 | 個人 (無報酬) |
| ソフトウェアウォレットB | 利用者の端末 | 収集していない | 不明 | 20万円 (寄付) | 48,000円 | 個人 (無報酬) |
| ソフトウェアウォレットC | 利用者の端末 | 6,500万円程度 | 30万円程度 | 55万円 (広告収入) | 60,000円 | 法人 6名 (無報酬) |
| ソフトウェアウォレットD | 利用者の端末 | 50億円程度 (累積入金額) | 数千万円程度 (取引所間) | 金額回答なし (収益源でない) | 回答なし | 法人 30名程度 |
| ソフトウェアウォレットE | 利用者の端末 | 1,000万円程度 | 数百万円程度 | 数百万円程度 (収益源でない) | 200万円程度 (SMS認証) | 法人 20名程度 |

4.2.1 預かり総額と送金の規模

顧客資産保護の観点や、犯罪収益移転防止法における特定取引の基準となる金額等の観点から、預かり金額の総額や、高額な送金の額について、リスクの実態を把握することに役立つと考えた。

ソフトウェアウォレットA、ソフトウェアウォレットBは利用者の残高や送金について情報を取得していないとの回答であった。それ以外ウォレットについて、預かり総額は40万円程度から50億円程度までと幅があり、それぞれの中で高額な送金の規模も、数万円から数千万円程度までの幅があった。

以下に個別のウォレットについての分析を記載する。

¹⁵ 時価はCoinMarketCap (<https://coinmarketcap.com/>) および三菱UFJリサーチ&コンサルティングの公表仲値 (http://www.murc-kawasesubai.jp/fx/past_3month.php) を参考にしている。

4.2.1.1 オンラインウォレットA

オンラインウォレットAにおける高額な送金の規模を見ると、2019年2月25日時点の預かり総額である300万円程度を上回る、400万円程度の送金が行われている。この送金にあたっては、必要な額の仮想通貨が入金された後に、送金が行われたものであり、常に高額な残高が保持されていたわけではない。

送金者本人にこの送金について確認することができたが、送金の理由としてはコミュニティの盛り上げに貢献したサービス運営者・開発者に対するお礼とのことであった。他にも数百万円程度の送金が行われた実績があるが、同様にサービス運営者・開発者に対するお礼であった。

これらは例外的に大きな金額が送金された事例であり、通常は高額な送金でも数万円程度である。

鍵の管理や流出時の対応方針、弁済資金の確保等については、管理方法はホットウォレットのみであり、弁済資金は保有しておらず、流出時は無保証としている。

4.2.1.2 オンラインウォレットB

オンラインウォレットBについては、預かり総額は40万円程度である。また、高額な送金の規模は数万円程度であり、最高でも当時の価値で7万円程度であった。

鍵の管理や流出時の対応方針、弁済資金の確保等については、管理方法はホットウォレットとコールドウォレットを併用し、出金に対応するための自己資金はホットウォレット、顧客資産は全額コールドウォレットである。このため、ホットウォレットからの流出については自己資金で弁済可能とのことであった。

4.2.1.3 オンラインウォレットC

オンラインウォレットCの預かり総額は、一時的な価格変動によって200万円程度まで上昇することもあったが、2019年2月6日時点の価値で80万円程度であった。1日あたり3,000円程度（2019年2月6日時点の価値）のトークンがマイニングによって新規に発行され、トークンエコノミーのインセンティブとして、顧客に分配されている。

顧客は、インセンティブとして分配されたトークンを、当該サービスの他の利用者に送金することが可能となっているが、1回あたりの送金額は最大で数千円程度に制限されている。

なお、このウォレットを提供するトークンエコノミーサービス事業者はICOを実施したが、ICOで販売されたトークンは、Ethereumと呼ばれるパブリックブロックチェーン上で発行され、流通し、交換所で取引されている。しかし、当該サービスにおいてインセンティブとして分配されるトークンは、流通しているトークンとは別に、事業者自身が管理するプライベートブロックチェーン上で発行しているトークンである。顧客は当該サービス内で得たトークンを、顧客が自身で鍵を管理するウォレットに引き出したり、交換所に送金して取引することはできない。また、顧客がICOや交換所での取引によって取得したトークンを、サービス内に預け入れることも出来ない。

このため、顧客の資産であるトークンと事業者の資産は完全に分離して管理されているとのことであった。

ただし、将来的にはプライベートブロックチェーン上で発行しているトークンをパブリックチェーン上で流通するトークンと交換し、顧客が引き出しや預け入れを行う予定である。そこで、ウォレットの預かり総額やサービス内での送金額は、流通するトークンの時価から算出している。

資金流出時の対応方針については、現段階では仕組みとして流出の恐れがないため、決めていないとのことであった。プライベートブロックチェーン上で発行しているトークンは、不正アクセス等によりサービス外に流出する心配がない。仮に不正アクセス等により、プライベートブロックチェーン上で不正な取引が記録された場合でも、事業者の意思でプライベートブロックチェーンのハードフォークを行い、取引履歴を修正することが可能である。

ただし、現在の預かり総額程度であれば、自己資金で弁済が可能であるとのことであった。

4.2.1.4 ソフトウェアウォレットA

利用状況の統計データを収集しておらず、利用実態は把握されていない。

4.2.1.5 ソフトウェアウォレットB

利用状況の統計データを収集しておらず、利用実態は把握されていない。

4.2.1.6 ソフトウェアウォレットC

ソフトウェアウォレットCは預かり総額が6,500万円程度で、高額な送金は30万円程度である。

ソフトウェアウォレットCに残高のあるユーザーについて、残高の平均は7万円程度、中央値は800円程度（2018年12月7日時点）となっている。

4.2.1.7 ソフトウェアウォレットD

ソフトウェアウォレットDは預かり総額は公開できないとのことであったが、累積入金額は50億円程度とのことであった。

数千万円程度の送金実績も多いとのことであり、これについて、より詳しく聞き取りを行ったところ、「こうした高額な送受金は利用者自身の仮想通貨交換所の口座との間で行われているとみられる」とのことであり、「ユーザー間の送金が頻繁に行われているわけではない」とのことであった。

4.2.1.8 ソフトウェアウォレットE

ソフトウェアウォレットEについては、預かり総額は1,000万円程度である。また、高額な送金の規模は数百万円程度である。

4.2.2 収入、支出、運営の状況

ウォレット事業を規制の対象とすることを考えた場合に、ウォレットサービスの収益性を把握することが、実態に即した適切な規制の内容を検討することに役立つと考え、収入、支出、運営の状況（個人か法人か、報酬、従業員数等）について質問した。

回答を総合してみると、ウォレットは収益化された事業ではないことが伺える。

個人によって運営されているものが多く、収入を得ていないものや、サーバー利用料等の費用も自己負担のものが多かった。また、法人で運営している場合も、調査時点では収益源として位置づけられてはいないとの回答が多かった。

回答の内容によって、ウォレットを便宜的に以下の通り区分した。

- ボランティアの個人によって運営されているウォレット
(オンラインウォレットA、オンラインウォレットB、ソフトウェアウォレットA、ソフトウェアウォレットB)
- 法人によって人員の報酬無しで運営されているウォレット
(ソフトウェアウォレットC)
- 法人によって、他の事業によって人員の報酬を負担している状態で運営されているウォレット
(ソフトウェアウォレットD、ソフトウェアウォレットE)
- その他のウォレット
(オンラインウォレットC)

この各区分ごとに、収入、支出、運営の状況を説明する。

4.2.2.1 ボランティアの個人によって運営されているウォレット

(オンラインウォレットA、オンラインウォレットB、ソフトウェアウォレットA、ソフトウェアウォレットB)

これらのウォレットは個人によって報酬なしで運営されている。支出はサーバー費用等があるが、ソフトウェアウォレットBを除いて収入より支出が大きく、そうした費用を運営者が自己負担している。また、ソフトウェアウォレットBも収入はユーザーからの寄付によるものであり、寄付が集まらなければ運営者が負担する前提であると考えられる。

4.2.2.2 法人によって人員の報酬なしで運営されているウォレット

(ソフトウェアウォレットC)

ソフトウェアウォレットCは当該ソフトウェアウォレットの開発に副業として取り組む個人のグループが立ち上げた株式会社によって運営されている。全員が役員で、報酬は配当のみとなっているが、現時点で配当はなく無報酬である。

具体的な収益化の目処は立っていないとの回答であるが、ブロックチェーンとその利用者の接点となるウォレットサービスは、将来的に何らかの形でビジネスモデルを構築できる可能性があると考え、長期的な視野で取り組んでいるとのことであった。

年間で55万円の収入があるが、これは「4.3.2 ソフトウェアウォレットCおよびソフトウェアウォレットEの収入源について」で別途とりあげるアフィリエイト広告による収入である。

4.2.2.3 法人によって、他の事業によって人員の報酬を負担している状態で運営されているウォレット (ソフトウェアウォレットD、ソフトウェアウォレットE)

ソフトウェアウォレットDは30名程度の法人で、ソフトウェアウォレットEは20名程度の法人である。両社とも、開発および運営にあたる人員はボランティアではないが、ウォレットサービス自体は現状では収益源となるような事業ではないとの回答であった。

ソフトウェアウォレットDは、ウォレットサービスは仮想通貨関連のサービスを総合的にユーザーへ提供するための一環であり、その他のサービスのビジネス基盤構築という位置づけとのことであった。収入や費用についての具体的な回答は得られなかった。

ソフトウェアウォレットEは、ウォレットサービスを仮想通貨関連のサービスを総合的にユーザーへ提供するための一環と位置づけている。数百万円程度の収入があるが、これは「4.3.2 ソフトウェアウォレットCおよびソフトウェアウォレットEの収入源について」で別途とりあげるエアドロップの引き受けによる収入である。費用は、利用登録時にSMS認証を必要としており、そのシステムの利用に200万円程度がかかっている。

4.2.2.4 その他のウォレット（オンラインウォレットC）

オンラインウォレットCは法人であり、合計15名で運営している。ICOによって当時の価値で4.3億円程度の資金調達を行った。現時点の収入と支出については回答を得られなかった。

4.2.3 規制に対する意見・見解等

ウォレット事業に対する規制について、当事者であるウォレット提供者らの意見に参考にできるものがある可能性があると考え、規制に対する意見や見解について質問した。

まず、オンラインウォレット提供者からは、「取扱額の大小等に関わらず一律の規制が行われることを懸念している」、「リスクに見合った規制をかけるべき」といった回答があった。一般論であることを前提とした上で、「仮にスタートアップの規模の企業が規制の対象となった場合、対応する人員の確保が難しいことや、かかるコスト負担が大きいことから、事業運営を行うことが難しくなるのではないかと回答した提供者もあった。また、現在仮想通貨交換業者に求められている対応のうち、顧客の仮想通貨の管理について求められるレベルが、仮想通貨交換業者と同様の水準であった場合、「自身が運営するサービスは廃止に追い込まれる。また、他の多くのサービスについても同様に廃止に追い込まれるだろうと考える」という回答もあった。「仮想通貨交換業者の想定するリスクレベルと、カストディが想定すべきリスクレベルが異なるため、同等の規制とすることには賛成しかねる」といった回答や、「顧客に取引所の口座を登録させ、入出金を当該口座間のみに限定した場合は規制を緩和できるのではないかと」、「預かり資産額や取引額に上限を設定した場合は規制を緩和できるのではないかと」といった回答を行う提供者もあった。「システム要件のチェックリストなどが必要ではないか」という回答もあった。

調査時期が研究会においてウォレットの規制について検討が進められている最中であつたところ、ソフトウェアウォレット提供者からも、「ウォレット提供者が顧客の鍵を管理していないソフトウェアウォレットは規制の対象外としてほしい」といった回答があった。中には、オープンソースソフトウェアのソースコードの公開が禁止されることや、公開が禁止されたソースコードが開発者の意図しない形でP2Pネットワーク上で流通した場合に開発者の責任が問われることを懸念する声もあった。

一方で、規制に対して懸念を示す意見ばかりではなく、ソフトウェアウォレット提供者からの回答の中に、新たなソフトウェアウォレット提供者に対する規制として、顧客の本人確認等を実施するといった基準を設け、基準を満たしたソフトウェアウォレット提供者については、顧客に対して分散型取引所等へのアクセスや操作の機能を提供することを認めるといったことも、検討できるのではないかと意見があった。

分散型取引所とは、ブロックチェーンを活用して実現された仮想通貨交換所の総称である。分散型取引所のサービスは様々ではあるが、自律的に動作し、誰でも利用でき、利用者が資金を預ける必要がなく、利用者同士がブロックチェーン上で自身のウォレットの鍵を使って署名を行うことで仮想通貨を直接交換できるなどの特色や機能を備えることが多い。利用者にとっては資金を預ける必要がないため、事業者に預けた資金が流出するリスクが無いなどのメリットがある。ただし、匿名で仮想通貨の売買が行われるため、マネーロンダリングに利用されるリスクは依然として残る。

そこで、分散型取引所に代わって、ソフトウェアウォレット提供者が一定の基準を満たすことで、顧客に分散型取引所等へのアクセスや操作を行う機能の提供を認めることも考えられるのではないかと、という意見であった。また、このような規制が実現した場合、積極的に基準を満たし、サービスを提供していきたいとのことであった。

4.3 ウォレットごとの追加調査とその結果

オンラインウォレットCの提供者はトークンエコノミーサービスを提供するためにオンラインウォレット機能を提供している。しかし、トークンエコノミーサービスの提供にあたって、オンラインウォレット機能の提供は必ずしも必要ではないとも考えられたため、オンラインウォレット機能を提供する必要性について、オンラインウォレットCの提供者に追加で質問を行った。

また、ウォレットを取り巻くビジネス環境の実態把握のため、年間で55万円の収入があったソフトウェアウォレットCの提供者と、年間で数百万程度の収入があるソフトウェアウォレットEの提供者から、実際の収入源となっているビジネスモデルや、過去に持ちかけられた収入源となりうるビジネスモデルについて、追加で質問を行った。

4.3.1 トークンエコノミーサービスにオンラインウォレット機能を内包する必要性について

オンラインウォレットCの提供者は、将来のサービス提供計画として、サービスがブロックチェーン上で動作すること、顧客が自身で管理する鍵を使ってサービスを利用すること、インセンティブとして分配されるトークンを直接顧客が鍵を管理するウォレットに付与することを予定している。

しかし、現段階では、ほとんどの処理をWebアプリケーションとして行っている。これは、現状のブロックチェーンでのサービス開発には課題が多いことから、ブロックチェーンの発展途上段階での課題の抽出と解消を目的としたものであるとのことであった。

ブロックチェーン上で顧客が自身で管理する鍵を使って行う処理を、Webアプリケーションの処理として行うには、Webアプリケーションが顧客に代わって鍵を管理する必要があるため、オンラインウォレット機能が必要となる。

なお、現段階でのブロックチェーンでのサービス開発における課題とは、以下のようなものとのことであった。

1. ユーザーにとって利用する敷居が高い
2. ブロックチェーンの処理能力が低い
3. スマートコントラクトプログラムは後から変更することができない

1. のユーザーにとって利用する敷居が高い件については、利用者が鍵管理やDappsブラウザ等の専用ブラウザを使用することに慣れておらず、専用ブラウザの普及展開までの期間は、サービス提供者がオンラインウォレットとして利用者の口座を用意して鍵を管理し、通常のWebサービス等と同様に、専門知識がなくても利用できるようにする必要があるとのことであった。

2. のブロックチェーンの処理能力が低い件については、ブロックチェーンにおいて一定時間内に処理できる上限が決まっており、同時に多数のユーザーが利用するとすぐに処理が滞る。この処理時間を短縮しようとする処理手数料が高騰する。こうしたスケーラビリティ問題と呼ばれる課題を解決するための研究が行われているものの、現時点ではWebアプリケーションで処理しているとのことであった。

3. のスマートコントラクトプログラムは後から変更することができない件については、ブロックチェーン上で処理を行うには、ブロックチェーン上にプログラムを設置する必要があるが、ひとたび設置したブロックチェーン上のプログラムは更新することができない。このサービス提供者は、現時点ではサービスの機能やアルゴリズムに改善点があるため、プログラムの改善が可能なWebアプリケーションで実装しているとのことであった。また、2. に記載したスケーラビリティ問題の解決策が、ブロックチェーン自体の後方互換性のないアップデートによって実現される可能性もあるといわれていることもあり、現時点ではブロックチェーン上にプログラムを設置することを避けているのも理由であるとのことであった。

上記のとおり、利用者に対するブロックチェーン技術の普及、ブロックチェーン自体の開発の進展、事業者のサービス開発の進展といった、複合的な要因から、オンラインウォレット機能の提供が必要とされている。

4.3.2 ソフトウェアウォレットCおよびソフトウェアウォレットEの収入源について

ウォレットを取り巻くビジネス環境の実態把握のため、年間で55万円の収入があったソフトウェアウォレットCの提供者と、年間で数百万程度の収入があるソフトウェアウォレットEの提供者から、実際の収入源となっているビジネスモデルや、過去に持ちかけられた収入源となりうるビジネスモデルについて、ヒアリングすることができた。

4.3.2.1 アフィリエイト広告

ソフトウェアウォレットCの収入源は、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と提携し、ユーザーをサービスへ誘導した場合に得られるアフィリエイト広告の報酬である。

ソフトウェアウォレットCはDAppsブラウザであるため、ブロックチェーンを活用したWebアプリケーションへ利用者を誘導するアフィリエイト広告が行いやすい。

4.3.2.2 エアドロップ（仮想通貨の配布）

エアドロップとは、仮想通貨を無償で配布することである。仮想通貨の発行者や開発者によって行われることが多い。エアドロップは、発行者や開発者によって認知の拡大や、新規利用者の獲得など、さまざまな目的によって行われることがある。

仮想通貨発行者から、ウォレット提供者に対して、広告宣伝のためウォレットのユーザーに対する仮想通貨のエアドロップ（配布）と、発行者の仮想通貨やプロジェクトの告知等を依頼されることがある。

ソフトウェアウォレットEの数百万円程度の収入源はエアドロップである。数十万円程度の提示金額の依頼を年間で複数引き受けているとのことであった。ただし、仮想通貨の価格が低迷してからは依頼がないとのことである。

ソフトウェアウォレットCの提供者もエアドロップの依頼を受けたことがあり、その提示金額は100万円程度（提示された仮想通貨の当時の価値）であったが、良い条件ではなかったため引き受けなかったとのことである。エアドロップによる広告宣伝は必ずしも魅力的な内容とは限らず、支持できない発行者またはプロジェクトからの依頼である場合や、ユーザーにとって不快になり得るような告知を行うことが条件になっていることがあるとのことである。

5. おわりに

カストディ規制の対象には、小規模な送金サービス、機関投資家向けの大規模な暗号資産保管・管理サービス、トークンエコノミーサービス等、様々なサービスが含まれる可能性があるものの、規模、取引内容、事業形態等によってリスクの内容や大きさはそれぞれ異なると考えられる。

今回の調査結果によると、ウォレットサービスは、現状では必ずしも収益性が高い事業とはいえない。規制によって国内におけるサービス提供が困難となると考えるウォレット提供者も存在した。なお、既存のウォレットサービスが規制への対応が困難であることを理由として終了した場合、利用者は規制の及ばない海外のウォレットサービスに流出することも考えられる。

また、トークンエコノミーサービス提供者に対する調査から、ブロックチェーンを活用したイノベーションを試みる場合に、オンラインウォレット機能の提供が重要な役割を果たすことも明らかになった。

マネーロンダリング・テロ資金供与に利用されるリスクを低減しつつ、イノベーションを阻害することのないように、事業やサービスの性質を踏まえたリスクに応じた規制とすることが肝要と考えられる。

国内ウォレットの実態についての調査 質問項目

| | |
|----|---|
| 1 | 名前（ハンドルネーム可） |
| 2 | 連絡先 |
| 3 | サービスの名称やURL等 |
| 4 | ユーザーの各アカウントにはどの程度の暗号資産が預けられているか（平均、中央値） |
| 5 | 全体でどの程度の額を預かっているか |
| 6 | ユーザー間で高額なやり取りが行われることがあるか、あるとすればどの程度の額か |
| 7 | 運営として、サービスから収入があるか。あるとすればどの程度の額か |
| 8 | 個人・法人・ボランティア等の運営形態、運営に携わる人数 |
| 9 | 運営費用（サーバー費用や割いている時間、人件費等）にどの程度かけているか |
| 10 | 会計処理を行ったり、顧客資産を分別管理したりしているか |
| 11 | 資金流出時の対応方針は決めてるか、返済資金確保が義務付けられた場合確保可能か |
| 12 | どのようなセキュリティ対策を行っているか（ホットウォレット・コールドウォレット管理等） |
| 13 | ウォレット業者に対する規制についての意見等 |
| 14 | 回答を公開可能な範囲（公開可、匿名で公開可、非公開を希望） |
| 15 | その他、必要に応じて追加の聞き取りを実施 |