

研究報告書

～web3ウォレットのルール形成について～

2025年6月

web3ウォレット(アンホステッドウォレット)の
ルール形成に関する研究チーム

役割	氏名	所属	職位等	その他
研究共同 責任者	田村次朗	慶應義塾大学	KGRI特任教授、 名誉教授	
	渕川和彦	慶應義塾大学	法学部准教授	
座長	河合健	アンダーソン・ 毛利・友常法律 事務所外国法 共同事業	パートナー弁護士	
監修	川崎ひでと	自由民主党	衆議院議員	自民党デジタル 社会推進本部 web3PT 前事務局長
メンバー	白石陽介	MZ Web3 Fund	ジェネラルパートナ ー	日本暗号資産ビ ジネス協会 副会長
	舘林俊平	KDDI株式会社	オープンイノベー ション推進本部 副本部長	
	黒田千春	KDDI株式会社	渉外・広報本部 政策調整部 レギュラトリーエキ スパート	
	増島雅和	森・濱田松本 法律事務所外国 法共同事業	パートナー弁護士 /弁理士	
	佐野史明	弁護士法人片岡 総合法律事務所	パートナー弁護士	
	吉田世博	株式会社Hash Port	代表取締役CEO	日本暗号資産 ビジネス協会 理事
	堀田昂慈	株式会社Hash Port	取締役CAO、 弁護士	
	大場昌寛	株式会社Hash Port	法務Gマネージャ ー、弁護士	

後援団体：日本暗号資産ビジネス協会

目次

はじめに.....	5
エグゼクティブサマリ.....	6
第1章 web3産業とその構成要素.....	6
第2章 web3ウォレットの技術と展望.....	6
第3章 日本国内におけるweb3ウォレット事業者のニーズと課題.....	6
第4章 web3ウォレットを取り巻くルールに関する現状と展望.....	7
第5章 DeFiの法規制とweb3ウォレットのDeFi接続に関する法的論点.....	7
第6章 経済法的視点からのweb3規制枠組みに関する考察.....	7
第1章 web3産業とその構成要素.....	9
1 web3産業の概要.....	9
2 web3産業の構造.....	11
3 web3を構成する技術的要素.....	12
4 web3を構成する要素の今後の展望.....	14
第2章 web3ウォレットの技術と展望.....	15
1 web3ウォレットとは.....	15
2 web3ウォレットの技術分類と特徴.....	16
3 ホステッドウォレットとアンホステッドウォレットの比較と展望.....	18
第3章 日本国内におけるweb3ウォレット事業者のニーズと課題.....	21
1 web3ウォレットのビジネスモデルと日本市場の動き.....	21
2 web3ウォレット事業者に求められるサービス・機能.....	22
3 web3ウォレット事業者の事業展開上のニーズ.....	24
4 法律や制度に関する課題.....	24
5 ウォレット事業者の課題解決に向けた具体的な提案.....	25
第4章 web3ウォレットを取り巻くルールに関する現状と展望.....	27
1 web3ウォレットを取り巻く法規制.....	27
2 web3ウォレットと暗号資産交換業等の該当性.....	28
3 web3ウォレットに望まれるルール整備.....	29
4 小括.....	30
第5章 DeFiの法規制とweb3ウォレットのDeFi接続に関する法的論点.....	32
1 DeFiとは.....	32
2 DeFiサービスに対する従来の金融規制の適用可能性.....	34

3 DeFiサービスに接続するweb3ウォレットに対する従来の金融規制の適用可能性	37
4 DeFiサービス/web3ウォレットに対する規制のあるべき方向性	39
第6章 経済法的視点からのweb3規制枠組みに関する考察	45
1 web3規制と経済法	45
2 経済法的視点からのweb3規制枠組み	45
3 web3に関する金融規制の課題	46
4 終わりに	47

はじめに

近年、日本国内においてもweb3と呼ばれる新たなテクノロジーの潮流が着実に広がりを見せ、一般の利用者が日常的にそのサービスに触れる時代が到来しつつある。そのような中、2017年に当時の「仮想通貨交換業」への規制として初めて導入されたルールについては、今まさにその制度設計の抜本的な見直しが議論されており(金融庁令和7年(2025年)4月10日「『暗号資産に関連する制度のあり方等の検証』ディスカッション・ペーパー」参照)、事業者がユーザの暗号資産を預かり、売買や交換の依頼に応じるサービスについては時代に対応したルール形成が進められている。

他方、MetaMaskに代表されるユーザ自身が暗号資産の管理を行うためのツールであるウォレットサービスの領域については、同サービスが全世界で3,000万以上の月間アクティブユーザ(MAU)を抱えるに至っており、日本国内においても多くの利用者が存在していると言われている。しかしながら、かかる利用の実態に比して、当該サービスを対象とした法規制や政策に関する議論は、量的にも質的にも甚だ不十分であるのが現状である。

こうした状況を踏まえ、本研究会においては、web3の根幹を成すインフラであり、ユーザとweb3エコシステムとをつなぐ要として機能する「ウォレット」(=「web3ウォレット」)に着目し、その法的性質、現在の規制上の位置づけ、さらには今後あるべき政策的対応の方向性について、実務的な観点もふまえた検討を加えていくこととした。

このように、web3の理念をふまえつつ、web3ウォレットに関する我が国における制度整備の在り方を展望することが本研究の目的である。

エグゼクティブサマリ

第1章 web3産業とその構成要素

web3は、非中央集権型のテクノロジースタックを基盤とする新たなビジネスモデルおよび社会的モデルであり、ユーザがデジタル資産やデータを自ら所有・管理できる「価値のインターネット」を実現するものである。従来のWeb1.0(“Read-only”型)・Web2.0(“Read&Write”型)を経て、web3(Web3.0)は“Read&Write&Own/Join”型の所有と参加を核とした新たな経済圏を形成している。

web3産業は、多層レイヤー構造から成り、各レイヤーが相互に補完し合いながらエコシステム全体の進化と成長を支えている

web3のエコシステムを支える技術的要素として、スマートコントラクト、Ethereum Virtual Machine (EVM)、Externally Owned Account(EOA)、インターオペラビリティ、Decentralized Physical Infrastructure Network(DePIN)などがある。

web3ウォレットは、web3を構成する要素の中でも中核をなすものであり、資産管理のみならず、デジタルIDの管理としての役割や、分散型アプリケーション(DApps)や分散型金融(DeFi)へのアクセスゲートウェイの役割まで担うものとして不可欠な存在である。

第2章 web3ウォレットの技術と展望

web3ウォレットの技術的方式については、現在、事業者が秘密鍵を管理する「ホステッド型」と、ユーザ自身が秘密鍵管理する「アンホステッド型」に分類されており、それぞれに利便性とセキュリティのトレードオフがある。

また、技術的には、インターネットに常時接続されている「ホットウォレット」とインターネットには接続していない「コールドウォレット」の区分も存在するほか、新たに登場したアカウントアブストラクション(AA)型ウォレットにも注目が集まっている。

今後は、各方式の共存と選択肢の多様化を図りつつ、ユーザ教育・技術革新・規制との調和を進めることで、安全で使いやすいweb3環境の実現が期待されている。

第3章 日本国内におけるweb3ウォレット事業者のニーズと課題

web3ウォレットのビジネスモデルには、トランザクション手数料モデル、サブスクリプションモデル、ステーキングモデル、アフィリエイト・広告モデルなどがあり、日本では大手プラットフォームも続々と参入中である。

オンランプ・オフランプ(法定通貨へのシームレスな接続)の実装その他の金融プラットフォームとの連携が、マスアダプションの鍵とされる。

また、ユーザの信頼を得るためには、高度なセキュリティ設計(例:秘密鍵のバックアップ)、複数チェーン対応、わかりやすいUI/UXが重要となる。

法規制面では、交換・媒介の定義の曖昧さや税の重さ、プライバシー・知的財産の保護・法制度の国際的整合性といった課題が存在している。

web3ウォレット事業の発展には、ルールの特明確化、税制の見直し、スタートアップ支援、そして国際的な制度整合が必要不可欠である。

第4章 web3ウォレットを取り巻くルールに関する現状と展望

現在の資金決済法においては、他人の暗号資産や電子決済手段を業として管理する場合等に、暗号資産交換業や電子決済手段等取引業の登録が必要とされ、それぞれコールドウォレットでの保管や信託義務、AML/CFT対応が義務付けられる。

他人の資産を管理しない場合であっても、ウォレットサービスが暗号資産の売買・交換を媒介していると判断される場合、暗号資産交換業の規制対象となる可能性がある。

金融庁のガイドラインでは、一定の行為は売買・交換の媒介に該当しないと整理されているが、媒介に該当する行為を行う場合の負担が重い。そのため、現状では、事業者が暗号資産交換業者や電子決済手段等取引業者と提携したとしても暗号資産と法定通貨との交換機能の実装が難しい。これらの課題に対し、金融審議会では暗号資産及び電子決済手段の仲介制度の創設が提案され、新たな仲介業（電子決済手段・暗号資産サービス仲介業）が資金決済法改正により実現することとなった。これにより、web3ウォレット上での取引連携や暗号資産、電子決済手段の直接入出庫が実現し、ユーザ体験が向上することが期待される。

暗号資産業者や電子決済手段等取引業者との連携が進むことで、web3の普及が進むと考えられるが、web3の本質である自己主権型のモデルとの両立をどのように図るか、特に分散型金融(DeFi)の位置づけは現時点においても明確ではなく、この点が今後のルール形成において重要な論点となる。

第5章 DeFiの法規制とweb3ウォレットのDeFi接続に関する法的論点

DeFiは、従来の金融機関や金融仲介業者を介さずにブロックチェーンとスマートコントラクトを活用し、貸付けや交換といった金融サービスを提供する新たな仕組みである。取引の透明性や自律性が高く、利用者はweb3ウォレットを通じて直接サービスを利用可能である一方、利用者保護やセキュリティ面では課題も残る。DeFiの技術アーキテクチャは3層からなり、各種プロトコルやトークン、分散型サイトを組み合わせて構築されている。

現行の金融規制は、暗号資産交換業者のような中央集権的仲介者を前提としており、DeFiの非中央集権的な構造には必ずしも適合していない。例えば、分散型取引所(DEX)やステーキング、レンディングの提供・利用方法によっては、暗号資産交換業等への該当性が問題となるが、いかなる提供・利用方法であれば現行規制が適用になるのかは明確ではない。

国際的には、IOSCOなどがDeFiへの規制の共通原則を提唱しており、「同一活動・同一リスク・同一規制成果」の原則を通じて、リスクに応じた柔軟かつ技術に即した対応が求められているが、現時点においても共通合意の形成には至っていない。今後は、アジャイルガバナンスの観点から、既存の枠組みにとらわれず、DeFiやweb3ウォレットに適した新たな規制体系の検討が求められる。

第6章 経済法的視点からのweb3規制枠組みに関する考察

web3市場は、DeFi、NFT、メタバースなどの急速な技術革新を背景に、国内外で急成長している。一方で、法規制が未整備なことにより、行政のケースバイケースの判断によって競争機会が損なわれることのないよう、早急な制度整備が求められている。

web3には、デジタルプラットフォームとしての性質から、独占禁止法その他の既存の経済法の枠組みが適用されうる領域が存在する。これらの規制は、過剰な干渉を避けつつ、グローバルな規制環境に適合する必要がある。

また、金融規制の面では、DeFiの法的取扱いが課題となっており、ゲートウェイとなるアンホステッドウォレットの法的取扱いも不透明である。加えて、セキュリティ対策や課税ルールの整備も必要とされている。

競争の本質であるイノベーションと公正かつ自由な競争を両立させるために、経済法を通じて、産学官の連携の上に柔軟かつ国際的整合性のある法規制の設計がなされることが不可欠である。

第1章 web3産業とその構成要素

1 web3産業の概要

本研究において、web3(Web3.0)とは非中央集権型のテクノロジースタックを基盤とする新たなビジネスモデルおよび社会的モデルを指すものとする。この概念は、ブロックチェーン技術に基づき、デジタル資産の所有やトランザクション管理をユーザ自身が直接担う仕組みを特徴としている。このような構造は、透明性、効率性、信頼性を向上させることで、従来のインターネットでは実現が困難であった持続可能なデジタル経済を可能にすると考えられている。

【図1-1】インターネットの歴史的発展



この進化により、インターネットは単なる情報流通の基盤から、価値の創造、保有、交換を促進する「価値のインターネット」へと変貌を遂げている。背景には、インターネットの歴史的発展が存在しており、以下のとおり、それぞれの時代でビジネスモデルおよび価値観に大きな変革が生じてきた。

(1) Web1.0

1990年代におけるインターネットは、静的なウェブページが中心であり、企業が一方的に情報を提供する「Read-only」型メディアとして機能していた。この時期における主なビジネスモデルは、広告収益およびサブスクリプションモデルに基づいており、ニュースサイトやポータルサイトがその代表例である。利用者は主に情報収集を目的としてインターネットを利用し、アクセス可能な情報量の拡大そのものに価値が見出されていた。

(2) Web2.0

2000年代に入り、インターネットは双方向性を有する「Read&Write」型プラットフォームへと進化した。Web2.0の特徴は、ユーザがコンテンツ生成および共有の主体と

なりうる点にあり、SNS(ソーシャルネットワーキングサービス)やブログ、動画共有プラットフォームが普及した。この時期の代表的なプラットフォームにはFacebook、YouTube、Twitter(現時点ではX)などが含まれる。

この進化により、企業はユーザの生成したデータを活用することで広告モデルを高度化し、個人化されたマーケティングが可能となった。また、ユーザは単なる情報消費者からコンテンツの生産もできる者へと変貌し、デジタル空間における社会的つながりが新たな価値として認識されるようになった。しかしながら、プライバシー侵害やデータ独占といった課題も顕在化した。

(3) web3(Web3.0)

2020年代において本格化したweb3は、"Read&Write&Own/Join"型のインターネットとして定義される。この進化を可能にしたのが、ブロックチェーン技術およびトークンエコノミーである。これにより、ユーザはデータやデジタル資産を直接保有し、分散型エコシステムに参加できるようになった。

web3の進展は、分散型金融(DeFi)、非代替性トークン(NFT)、メタバースといった領域で顕著である。例えば、DeFi市場は2024年末時点で総資産(TVL)が1,400億ドルを超える規模に達している(注1)。DeFiは「分散台帳技術(一般的にはパブリックかつパーミッションレス型のブロックチェーン)に基づき、仲介者を必要としないことを企図した金融サービスや商品を提供するもの」とされており(注2)、暗号資産の売買や交換などのCEX(Centralized Exchange、日本でいう暗号資産交換業)と同様の機能にとどまらず、貸付やデリバティブ、保険商品など様々な金融商品を提供している。

また、NFT市場では、従来のデジタルコンテンツ分野を超えて、実物資産(RWA: Real World Asset)との結びつきのあるデジタル資産が伸長しており、いわゆる所有権のデジタル化や取引の効率化に寄与している。

このように、web3は新たな経済圏の形成を促進し、社会の基盤となりうる多様なユースケースを提供している。

【図1-2】web3の普及した未来

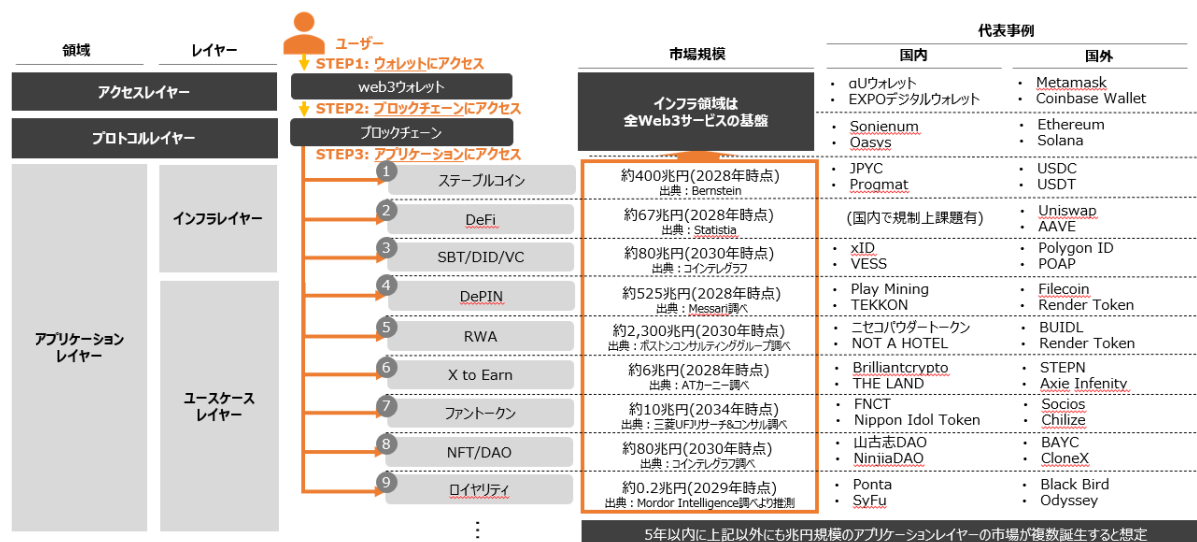
金銭的価値/非金銭的価値の両方がデジタル化されて活発に流通する			
金銭的価値/非金銭的価値の両方がデジタル化される		ボーダーレスな価値移転がスムーズになる	
- 証券や不動産などの金銭的価値に加え、コンテンツや活動履歴などの非金銭的価値の共創・保存・交換が容易に - 仲介者を介さず、誰でも自由に、プログラム制御で効率的に価値の保存・交換できるようになった		- ブロックチェーンを介することで、プラットフォームや国境を跨ぐ価値移転が低コストで実現可能になった。 - ブロックチェーンによるトランザクションの透明性で取引のモニタリングコストが大幅に低減した	
効率的で安定した価値の流動性が確立される		価値の共創を促すインセンティブ設計が可能になる	
- プログラム(スマートコントラクト)に基づいた取引の実行が容易となるため、取引にかかる時間が縮減された - 人を介在させることなく、複雑な価値の移転が非中央集権的に行えるため、価値の流動性が高まった		- トークンを活用してサービスに関わる人々に経済的インセンティブを付与することが容易になった - ブロックチェーンの比中央集権制によって、管理者不在での長期の価値保存が可能になった	

出典：https://www.meti.go.jp/shingikai/sankoshin/shin_kijiku/pdf/010_03_01.pdf

2 web3産業の構造

web3産業は複数の機能的レイヤー(階層)で構成され、それぞれが特定の役割を果たすことで全体として効率的に機能している。このレイヤー構造は、技術基盤のスケラビリティを高めるとともに、エコシステム全体の発展を促進する。

【図1-3】web3産業のレイヤー構造



(1) アクセスレイヤー

このレイヤーは、ユーザがweb3エコシステムに接続するためのインターフェースを提供する。具体例として、海外ではMetaMask(Consensys)やCoinbase Wallet(Coinbase)、国内ではαUウォレット(KDDI)といったウォレットが挙げられる。これらは分散型取引所(Decentralized Exchange、DEX)やNFTマーケットプレイス、DAO(分散型自律組織)へのアクセスゲートウェイとして機能する。

(2) プロトコルレイヤー

プロトコルレイヤーは、ブロックチェーンネットワークやスマートコントラクトの標準を定義し、データ管理およびトランザクション処理を支える基盤を提供する。例えば、Ethereumはその汎用性によりDeFiやNFTの主要なプラットフォームとして機能している。

(3) アプリケーションレイヤー

(a) インフラレイヤー

ステーブルコインや分散型ID、分散型ストレージネットワークなど、web3アプリケーションの運用を支える技術インフラを提供する。このレイヤーは、持続可能でスケラブルなエコシステムを実現するために重要である。

(b) ユースケースレイヤー

ファントークンやNFT、DAOなど、web3技術を利用した実際のアプリケーションやサービスを提供するレイヤーである。これらは、ユーザエクスペリエンスを向上させるだけでなく、新しい社会的および経済的価値を創出する。

このように、各レイヤーが独立して機能しながらも、相互に補完し合うことで、web3エコシステム全体が進化と成長を遂げている。今後、技術革新とユーザ体験の向上により、さらに多様なユースケースが生まれることが想定されている。

3 web3を構成する技術的要素

web3のエコシステムを支える技術的要素は、分散型の構造を実現するための基盤として極めて重要である。その全体像を理解するには、ブロックチェーン技術を中核としたインフラストラクチャ、相互運用性を確保するプロトコル、分散型データ管理、そしてそれらを支えるスマートコントラクトなど、さまざまな要素がどのように連携しているかを知る必要がある。

まず、web3の構成要素は単一の技術に限定されるものではなく、多層的な仕組みから成り立っている。これには、ブロックチェーンプラットフォーム(例: Ethereum、Polkadot、Solana)、それらの上で動作するプロトコル(例: ERC-20やERC-721のようなトークン標準)、および分散型アプリケーション(DApps)を含む。これらの要素が連携することで、従来の中央集権的なサービスを超えた分散型インフラが構築されている。

例えば、Ethereum Virtual Machine(EVM)は、分散型アプリケーションを実行するための主要な仮想環境であり、Ethereumやその他のEVM互換チェーンにおいてスマートコントラクトを動作させる基盤技術である。同様に、Externally Owned Account(EOA)は、ユーザがブロックチェーンにアクセスするための主要なインターフェースを構成する技術であり、ウォレットや取引を通じて資産を管理する上で不可欠である。

また、これらの技術が機能するためには、ブロックチェーン間での相互運用性(インターオペラビリティ)を確保する仕組みが必要不可欠である。Polkadotのようなプロトコルは、異なるチェーン間でデータや資産を安全に移動させるためのフレームワークを提供しており、web3のエコシステム全体の拡張性を大幅に向上させている。

さらに、分散型ストレージ(例: Filecoin、Arweave)や分散型計算リソース(例: Render)のようなDePIN(分散型物理ネットワーク)が、中央集権型のクラウドサービスに代わるインフラとして注目されている。これらの技術により、ユーザは自らのデータを完全にコントロールできると同時に、コストの削減やデータの耐久性の向上が可能となる。

以下に、これらの中でも特に重要な役割を果たしているスマートコントラクトやEVMを中心に、具体的な機能について記載する。

(1) スマートコントラクト

スマートコントラクトは、web3の中核技術として位置付けられる。これにより、契約や取引がコード化され、自動的に実行される仕組みが提供される。スマートコントラクトは、透明性と信頼性を保証し、仲介者を排除することでコスト削減を実現する。

たとえば、Uniswapでは、スマートコントラクトを利用してユーザ間の資産交換を完全に自動化している。この技術は、分散型金融だけでなく、サプライチェーン管理やデジタル証明書の発行といった幅広い分野での応用が期待されている。

(2) EVM(Ethereum Virtual Machine)

EVMは、Ethereum上でスマートコントラクトを実行する仮想マシンであり、web3エコシステムを構成する代表的な技術の1つである。この技術により、プログラムが信頼性と透明性を保持したまま分散型の環境で実行される。EVMは、Ethereumだけでなく、PolygonやBinance Smart Chainなどの多くのブロックチェーンで採用されており、相互運用性の確保に寄与している。

EVMの最大の利点は、その汎用性と拡張性にある。同一のスマートコントラクトコードが複数のEVM互換ブロックチェーンで動作するため、開発者は効率的に分散型アプリケーションを構築できる。この技術基盤は、分散型金融(DeFi)や非代替性トークン(NFT)の市場拡大を支える鍵である。

一方で、EVMのパフォーマンスやスケーラビリティに関する課題も指摘されている。これを克服するため、Ethereum 2.0やLayer 2ソリューションといった技術的進化が進行中である。

(3) EOA(Externally Owned Account)

EOAは、ユーザがブロックチェーンネットワークにアクセスするためのアカウント制御技術であり、秘密鍵によって制御される。この技術は、デジタル資産の送受やスマートコントラクトの呼び出しといった基本操作を可能にする。

EOAは、スマートコントラクトとのインタラクションを通じて、分散型金融やNFTのトランザクションを可能にする。例えば、ユーザがウォレットを介して分散型取引所(DEX)でトークンを取引する場合、EOAが中心的な役割を果たす。この仕組みにより、ユーザ自身と分散化された取引所での取引が可能となり、中央集権的な管理者を介さずに取引を完了できる点が、web3の特徴と言える。

しかしながら、秘密鍵の管理がユーザ自身の責任であるため、その優位性はリテラシーに左右される側面が強く、セキュリティリスクも伴う。この点に関しては、マルチシグウォレットやMPC(マルチパーティ計算)などの新しい技術が課題解決に向けた方向性を示している。

(4) インターオペラビリティ

インターオペラビリティは、web3エコシステムが拡大する上で欠かせない要素である。これにより、異なるブロックチェーン間でデータや資産の移動が可能となる。具体的には、PolkadotやCOSMOSといったプロジェクトが、相互運用性を実現するためのプロトコルを提供している。

インターオペラビリティが実現することで、分散型アプリケーションはより多くのユーザとネットワークに対応できるようになり、エコシステム全体の一体感が高まる。また、この技術は、分散型金融における流動性の向上やNFT市場の拡大をもたらす可能性がある。

一方で、異なるブロックチェーン間のセキュリティやパフォーマンスの差異が課題となっている。これを克服するための新しいソリューションの開発が期待される。

(5) DePIN(Decentralized Physical Infrastructure Network:分散型物理ネットワーク)

分散型ストレージ(例:Filecoin、Arweave)や分散型計算リソース(例:Render)は、web3エコシステムの基盤技術として重要である。これらの技術により、データと計算リソースが中央集権的なサーバから分散化され、ユーザ間で共有される。

分散型ストレージは、データの耐久性や透明性を向上させる一方で、データ保存のコスト削減にも寄与している。また、分散型計算リソースは、人工知能モデルのトレーニングや大規模データ処理を効率的に行うためのリソースを提供している。

これらの技術は、金融、医療、教育といったさまざまな分野での応用が進んでおり、web3が従来の中央集権型インフラを超える可能性を示している。

4 web3を構成する要素の今後の展望

web3を構成するこれらの技術要素は、それぞれが独立して機能するだけでなく、相互に補完し合いながらエコシステム全体を進化させている。この中で特に重要なのは、インターオペラビリティとスマートコントラクトの組み合わせである。これにより、異なるネットワーク間での資産の移動やデータ共有が円滑に行われ、ユーザ体験が向上する。

今後は、技術の成熟とともに、さらなる課題解決が進むと予想される。例えば、EVMのスケラビリティや分散型ストレージのコスト効率の改善が挙げられる。また、Layer 2 ソリューションの導入により、トランザクション処理速度の向上と手数料の削減が実現しつつある。さらに、クロスチェーンプロトコルの進化により、異なるブロックチェーン間での相互運用性が強化され、データや資産の移動がよりシームレスになることが期待される。他にも、ユーザが直面するセキュリティリスクを低減するため、秘密鍵管理の代替ソリューションとしてマルチパーティ計算(MPC)やソーシャルリカバリー型のウォレット設計が進展している。

web3の技術的進化は、単なるインフラの変革にとどまらず、社会的および経済的な変革をもたらす可能性を秘めている。その際に、web3ウォレットは、ユーザがweb3を利用する際の起点として、ユーザ体験を根本から変える鍵となると考えられる。web3ウォレットは、資産の管理のみならず、デジタルアイデンティティの管理や分散型アプリケーションへのアクセスゲートウェイとしての役割を果たしており、今後のweb3エコシステムの発展において不可欠な存在である。

(注1)DeFiLlama Total Value Locked (<https://defillama.com/>)

(注2)FSB「Assessment of Risks to Financial Stability from Crypto-assets」(February 2022)

第2章 web3ウォレットの技術と展望

1 web3ウォレットとは

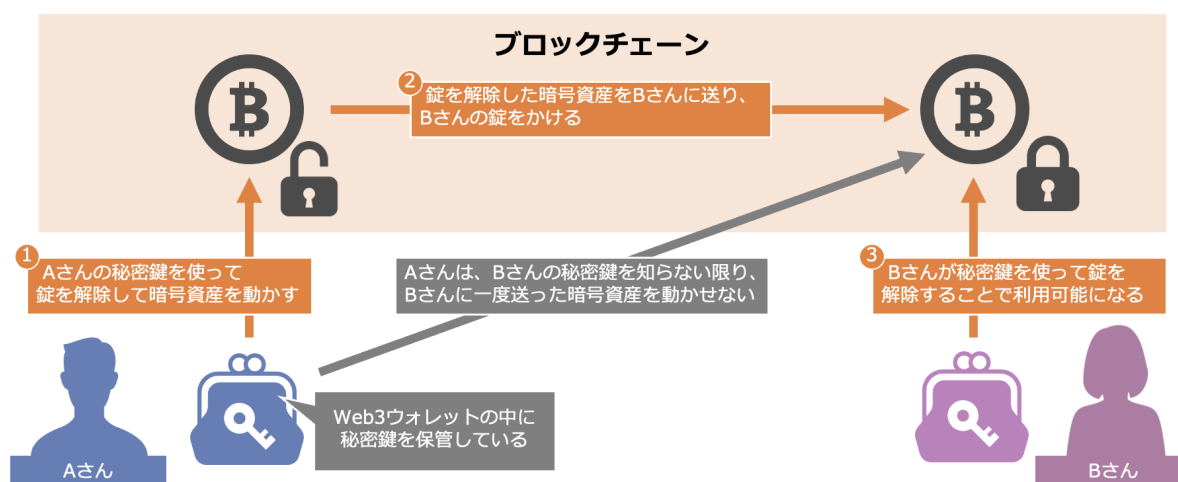
(1)web3ウォレットの概要

web3ウォレットは、ブロックチェーンの世界においてデジタル資産を管理・取引するためのツールである。第1章で述べたとおり、web3ウォレットは、ユーザがweb3エコシステムに接続するためのインターフェースとなることから、web3エコシステムの発展において不可欠な存在である。

実際には、デジタル資産の取引記録はブロックチェーン上に保存されるため、web3ウォレット自体が資産を保持しているわけではない。ブロックチェーン上のデジタル資産を操作するための機能を提供するのがweb3ウォレットの役割である。現在広く利用されている方式は、「秘密鍵」と呼ばれる文字列を使用するEOA(Externally Owned Account)方式であるため、以下ではEOA方式を前提に解説していく。

(2)web3ウォレットの機能

【図2-1】web3ウォレットと秘密鍵の仕組み(EOA方式)



web3ウォレットは、単純化して言えば、上記概念図のように「秘密鍵」を保管するツールであり、一般的には、主に以下の3つの機能を提供している。

- ・ 秘密鍵の生成・管理: ユーザのデジタル資産を取り扱う際に必要な秘密鍵の生成・管理
- ・ 電子署名の作成: ブロックチェーン(データベース)上でデジタル資産の移転を行う取引(トランザクション)を有効化するための電子署名の作成
- ・ ブロックチェーンを活用したサービスへのアクセス窓口: 暗号資産取引所、DeFi(分散型金融)やNFTマーケットプレイスなどの、ブロックチェーンを活用したアプリケーションに接続するためのAPI接続やブラウザ提供

上記の各機能は、一般のユーザがweb3サービスを利用するために必要不可欠な機能である。現時点で既に無数のweb3サービスが世の中に存在しているが、web3ウォレットを持たない場合、それらのサービスの多くは利用することができない。その意味で

web3ウォレットはすべてのユーザがweb3サービスを利用する際のゲートウェイとなる存在といえる。

2 web3ウォレットの技術分類と特徴

web3ウォレットの技術モデルは複数あるが、主要な分類として以下の2分類がある。

(1) 誰が管理しているか(ホステッド／アンホステッド)

ユーザの秘密鍵をウォレットサービスの提供者が管理するタイプのウォレットを「ホステッドウォレット」と呼び、ウォレットサービスの提供者はユーザの秘密鍵に触れることができず、ユーザ自身が秘密鍵を自ら管理するタイプのウォレットを「アンホステッドウォレット」と呼ぶ。なお、ホステッドウォレットは「カストディアルウォレット」、アンホステッドウォレットは「ノンカストディアルウォレット」と呼ばれることもある。

なお、1(2)において、「web3ウォレットはすべてのユーザがweb3サービスを利用する際のゲートウェイとなる存在」であると述べた。しかし、ホステッドウォレットからは、様々な金融機能等を提供するDAppsと呼ばれる分散型アプリケーションには基本的にアクセスできず、分散型のソリューションのメリットを十分に享受することはできない。なぜなら、DAppsの利用にあたっては、当該暗号資産の管理に必要な秘密鍵をもって署名を行う必要があるところ、ホステッドウォレットにおいては秘密鍵をユーザがサービス提供者に預託している関係上、ユーザ自身による柔軟な署名が実現できないためである。

日本においては、一般的に、「ホステッドウォレット」の提供には暗号資産交換業の登録が必要とされている一方、「アンホステッドウォレット」の提供にはそのような登録は不要と理解されている(詳細は第4章参照)。

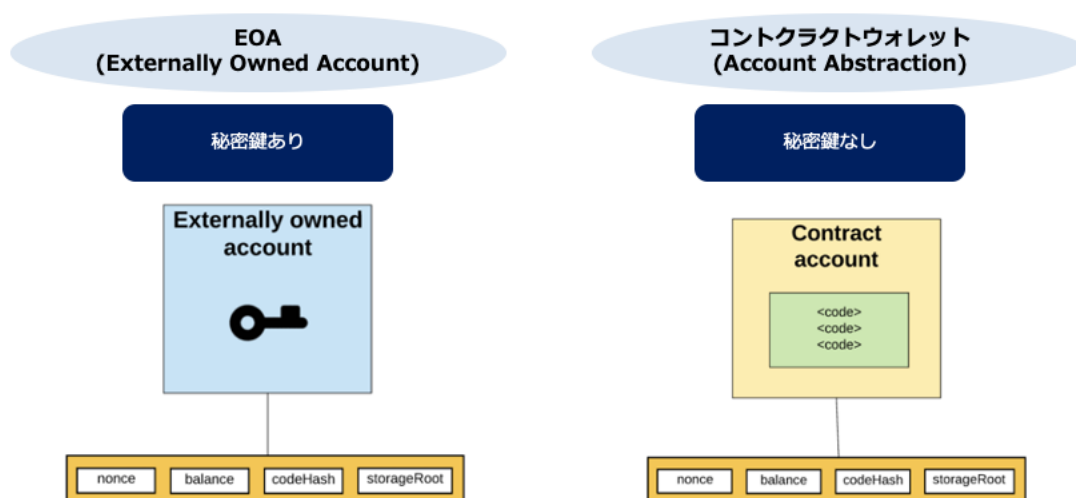
(参考) Account Abstraction(AA)

従来の秘密鍵を使用したEOA方式のウォレットに対し、スマートコントラクトでデジタル資産を管理する「コントラクトウォレット」を実現する技術も開発が進められている。

EOAは「Externally Owned Account」の略であり、ユーザがブロックチェーンの外から公開鍵・秘密鍵を使って管理出来ることを指している。ユーザが外部から秘密鍵を使ってウォレットの管理者であることを証明し、デジタル資産を管理する方式である。

コントラクトウォレットは秘密鍵が存在せず、スマートコントラクトによって制御されているウォレットである。ユーザは、コントラクトアカウントを用いることで、ブロックチェーン上のスマートコントラクト(Solidity等で自由にロジックを書けるEthereum等のブロックチェーン上で動くプログラム)を介して、デジタル資産を管理する。

【図2-2】



アカウントアブストラクション(AA)とは、コントラクトウォレットを実現する技術の一つである「アカウントアブストラクション(Account Abstraction:アカウントの抽象化)」のことであり、Ethereumの規格の一つであるERC-4337によって定義されている。「アカウントの抽象化」とは、アカウントタイプの詳細がEthereumなどのプロトコルからは見えないことを意味する。すべてのアカウントは単なるスマートコントラクトであり、ユーザは個々のアカウントをどのように管理および運用するかを自由に設計できる。

アカウントアブストラクション型のコントラクトウォレットが普及すると、ウォレットサービス提供者もユーザも秘密鍵の保持が不要になり、ユーザ自身が設定するパスワードや生体認証に依拠してブロックチェーン上の資産を取り扱うことができると期待されている。

なお、アカウントアブストラクション型のコントラクトウォレットが実装された場合の法的規制については、明確な結論は出ていない。

(2) インターネット接続されているか(ホット/コールド)

インターネットに接続されているウォレットを「ホットウォレット」、インターネットから隔離されたウォレットのことを「コールドウォレット」と呼ぶ。

ホットウォレットはインターネットに接続された状態で運用されるものであり、ユーザからの要求に従い直ちに取引が行える方式である。スムーズなユーザ体験を実現しやすいというメリットがある一方、インターネットに接続されていることからハッキングへの耐性が弱いというデメリットがある。

コールドウォレットは、インターネットから隔離された環境に秘密鍵を保管する方式である。インターネットを通じたハッキングの可能性が低く安全性が高いというメリットがある一方、秘密鍵を記録したハードウェア等が操作のプロセスにおいて必要であり、スムーズなユーザ体験の実現が困難というデメリットがある。

暗号資産の売買・交換サービスを提供している暗号資産交換業者は、ユーザの秘密鍵を預かるホステッドウォレットの方式で暗号資産の管理サービスを同時に提供していることが多く、ハッキング等による顧客資産の流出のリスクを低減するため、ホットウォ

レットでの管理は限定的な範囲でのみ使用が認められ、原則としてコールドウォレットによる管理が法律上求められている。

一方で、アプリ型のweb3ウォレット事業者は、一般的に、ユーザの秘密鍵を預からないアンホステッドウォレットの形式でサービスを提供しており、サービス提供者のシステムがハッキングされても直ちにユーザ資産が流出するリスクが低い。そのため、通常は利便性の高いホットウォレットのみの形で提供されている。

3 ホステッドウォレットとアンホステッドウォレットの比較と展望

前述のとおり、現在主流となっているEOA方式のweb3ウォレットは、ブロックチェーン上の資産を取り扱うために必要な秘密鍵を誰が管理するかによって「ホステッドウォレット」と「アンホステッドウォレット」の二種類に区別される。いずれもブロックチェーン上の資産管理を担うが、ユーザに要求されるリテラシーや生じうるリスクが大きく異なる。暗号資産の普及に伴い、秘密鍵の盗難やウォレット事業者へのハッキングなどのセキュリティリスクが顕在化していることから、ユーザ保護や規制整備の観点でも両者の比較・検討が必要と考えられるため、以下検討する。

(1)ホステッドウォレットとアンホステッドウォレットの特徴

(a) ホステッドウォレットの特徴

① 事業者による秘密鍵の管理

ホステッドウォレットは、ウォレット事業者がユーザの秘密鍵を管理するものである。ユーザは既存の金融サービスと同様にパスワードやメールアドレス等の認証でログインするだけで済み、秘密鍵そのものを意識する必要がなく、パスワード等を紛失した場合であっても復旧が可能であるため、ユーザのリテラシーに比較的依存しない。

② 集中管理に伴うハッキングリスクと対策

ホステッドウォレットは多数のユーザの大量の資産が一つの事業者に集積されるため、攻撃者がハッキングに成功すると大規模な資産流出が起きるリスクがある。そのため、日本では、暗号資産交換業者がホステッドウォレットを提供する際には、資金決済法に基づき、原則としてコールドウォレットで保管するなどの管理義務が定められている。

しかし、近年は、事業者内の権限を奪うソーシャルエンジニアリングの手口も増えるなど攻撃手法が巧妙化しており(注3)、コールドウォレットを利用していたとしてもハッキングされる事件が起きている。

そのため、事業者同士の情報共有や従業員教育の徹底などが強く求められる。また、技術の進展を踏まえ、そもそも法令で(安全とされる)「コールドウォレット」に該当するための現行の要件の妥当性やコールドウォレットかホットウォレットかという二元論でウォレットの安全性を測るのではなく、全体的なシステム設計やオペレーションを踏まえた安全性基準の策定についても再検討する必要があると考えられる。

③ 多様なweb3サービス(DApps等)の利用困難性

2(1)で述べたとおり、基本的にホステッドウォレットからDAppsへのアクセスはなされない。そのため、ユーザの意思に基づく多様なweb3サービスへの接続は通常困難であり、あくまでユーザが取引をする暗号資産交換業者が提供する限定的なサービスを利用することができるにとどまる。

(b) アンホステッドウォレット

① 自己管理と高い自由度

アンホステッドウォレットは、ユーザ自身が秘密鍵を保持し、ブロックチェーン上の資産の取り扱いにおいて第三者に依存しないこととなるため、口座凍結や資産の押収などのリスクが低く、また、匿名性が担保されるためプライバシーや検閲耐性が高い。web3の自己所有の概念にフィットするものである。一方で、秘密鍵を紛失した場合の復旧が困難であり、ユーザのセキュリティリテラシーに大きく依拠する。

② ウォレット事業者のサポートとセキュリティ対策

ユーザのセキュリティリテラシーには幅があるため、ウォレット事業者がセキュリティ関連のUI/UXを提供する例が増えている。例えば複数署名(マルチシグ)を用いた秘密鍵の分散管理や、秘密鍵のバックアップを支援する(ただし、事業者自身は秘密鍵に触れることはない)仕組みなどが挙げられる。しかし、こうしたサービスが十分でない場合、ユーザ個人の責任や知識不足によってハッキング等のリスクが高まりうる。

③ 多様なweb3サービス(DApps等)の利用可能性

アンホステッドウォレットでは、ホステッドウォレットとは異なり、DAppsに接続してこれを利用することができることから、ユーザの意思に基づく多様なweb3サービスにアクセスすることができる。

【図3】

	ホステッドウォレット	アンホステッドウォレット
メリット	① 事業者が秘密鍵を管理するためユーザのリテラシー負担が小さい ② 資金決済法等のレギュレーションに基づき、コールドウォレットなどで安全管理が行われる場合が多い ③ サポートや補償制度が整備されている場合があり、初心者にも安心感がある	① ユーザ自身が秘密鍵を保持するため検閲耐性やプライバシーが高い ② ブロックチェーン本来の「自己所有・自己管理」を実現 ③ 第三者による資産凍結のリスクが低い ④ 多様なweb3サービス(DApps等)へのアクセスが可能
デメリット	① 事業者へのハッキングや内部不正が成功すると資産が一括流出 ② 事業者倒産や破綻による資産喪失リスク ③ KYC等によってプライバシーが制限され、ユーザの取引活動が監視されうる ④ 多様なweb3サービス(DApps等)へのアクセスが通常困難	① 秘密鍵の紛失・盗難時の補償がなく自己責任が重い ② セキュリティ対策を誤ると資産を容易に喪失 ③ UI/UXが不十分な場合、ユーザの操作ミスを誘発する
法規制※	ウォレットサービス提供にライセンス必要	ウォレットサービス提供にライセンス不要

※法的整理の詳細については第4章参照

(2) 今後の展望

① 選択肢の確保

上記のとおり、ホステッドウォレットとアンホステッドウォレットはそれぞれに長所と短所があるため、いずれが優れているというものではない。web3のマスアダプションのためには、いずれもセキュリティ対策を向上させつつ選択肢として確保し、ユーザのリテラシー、リスク許容度や用途に応じて適切に選択される環境が整備されていくことが望ましい。

業界としても、ホステッドウォレット提供事業者におけるセキュリティ強化を進める一方で、アンホステッドウォレット提供事業者においても、マルチシグやユーザに対するセキュリティ教育などの充実により、リテラシーによるハードルを下げる取り組みを進めていくことが必要と考えられる。

ユーザにおいても、自らリテラシーを向上させ、ホステッドウォレットとアンホステッドウォレットを使い分けることでリスク分散をすることが有用と考えられる。

② 技術革新

アカウントアブストラクション(AA)などの新技術の開発が進められることにより、秘密鍵管理の負担を軽減しつつ安全性を高めることが可能となるため、積極的な技術開発とともに、世界標準の研究開発を進めていくことが望まれる。

③ 規制当局と業界の連携

上記①②の環境を整備するため、規制当局と業界が密に連携し、ユーザを保護しつつ技術革新を阻害しないよう柔軟な制度設計を行うことが求められる。また、規制内容を検討するにあたっては、第5章で述べるとおり、従来の金融規制の枠組みのみに固執することなく、様々な観点を取り入れて規制枠組みを検討していく必要があることにも留意が必要である。

(注3) <https://www.fsa.go.jp/news/r6/sonota/20241224-2/241224yousei.pdf>

第3章 日本国内におけるweb3ウォレット事業者のニーズと課題

1 web3ウォレットのビジネスモデルと日本市場の動き

(1) web3ウォレットの市場規模

web3ウォレットの競争は世界的にも活発化しており、世界最大手のアンホステッドウォレットであるMetaMaskは2024年1月時点で3,000万人のMAU(Monthly Active Users)を抱えている(注4)。

(2) web3ウォレットのビジネスモデル

web3ウォレットのビジネスモデルにはいくつかの種類がある。そのうち収益モデルの違いに着目した分類の代表的なものを紹介する。

(a) トランザクション手数料モデル

暗号資産の交換(スワップ)機能その他の取引機能を、自ら提供または提供する外部サービスへの接続機能を通じて手数料を徴収するモデルである。例えばMetaMaskは、暗号資産を交換(スワップ)する外部サービスへの接続機能を提供しており、その利用の際に一定の手数料を徴収している。なお、このようなサービスを提供するためには、アンホステッドウォレットであっても、その態様に応じ、暗号資産の売買もしくは交換またはそれらの媒介として、暗号資産交換業の登録が必要となる場合がありうる(詳細は第4章、第5章参照)。

(b) サブスクリプションモデル

高度なセキュリティ機能や管理機能等を月額課金で提供するモデルである。例えば、サブスクリプションサービスに加入すると、より高度なセキュリティや、優先サポート等が提供されるサービスがこれに当たる。

(c) ステーキングモデル

ステーキングサービスに接続し、ステーキングで発生する利息や報酬の一部を収益化するモデルである。ステーキング以外にも、レンディングなどのDeFiプロトコルに接続することも考えられる。

(d) アフィリエイト・広告モデル

主にweb3関連のサービスと提携し、広告収益やアフィリエイト収益を得るモデルである。例えば、NFT関連の広告やパートナーアプリの広告を掲載し、プロモーション収益を得るサービスや、DApps(分散型アプリケーション)の紹介プログラムを利用し、アフィリエイト収益を得るサービスがこれに当たる。

(3) 大手プラットフォームの参入

web3ウォレットは、暗号資産やNFT(非代替性トークン)の管理を行うツールであると同時に、分散型アプリケーション(DApps)や分散型金融(DeFi)、さらにはメタバース経済圏へのアクセスを支える中核的な存在である。その役割は、単なるデジタル資産の保管にとどまらず、ユーザのデジタルアイデンティティやトークンエコノミーへの参加を支える重要な基盤へと進化している。

現在、国内においては大手プラットフォームを中心にアンホステッドウォレット事業への参入が活発化しており、NTTドコモ(NTT Digital)、KDDI、LINE(LINE NEX T)、楽天(楽天ウォレット)など大手各社が参入してきている。他方で、メルカリ(メルコイン)は、ホステッドウォレットを通じてサービスを提供する形で、ビットコインを購入できるサービスの提供を開始してから1年で200万人以上のユーザを集め、大きな話題となった。これからweb3のゲートウェイであるweb3ウォレットをめぐる競争は、今後ますます加速化していくと考えられる。

なお、web3ウォレットのユーザ体験に大きな影響を与える要素の一つとして、オンライン・オフラインと呼ばれる法定通貨とのシームレスな交換が挙げられる。その意味で、すでに銀行口座の接続が完了しており、ユーザの金融サービス利用動線のハブとなっている決済サービスはweb3ウォレットと連携をしていく重要なチャンネルになっていくと考えられる。そのような金融プラットフォームとの連携は、web3ウォレットのマスアダプションを実現していくと同時に、web3そのもののマスアダプションも実現していくことが期待されている。

2 web3ウォレット事業者に求められるサービス・機能

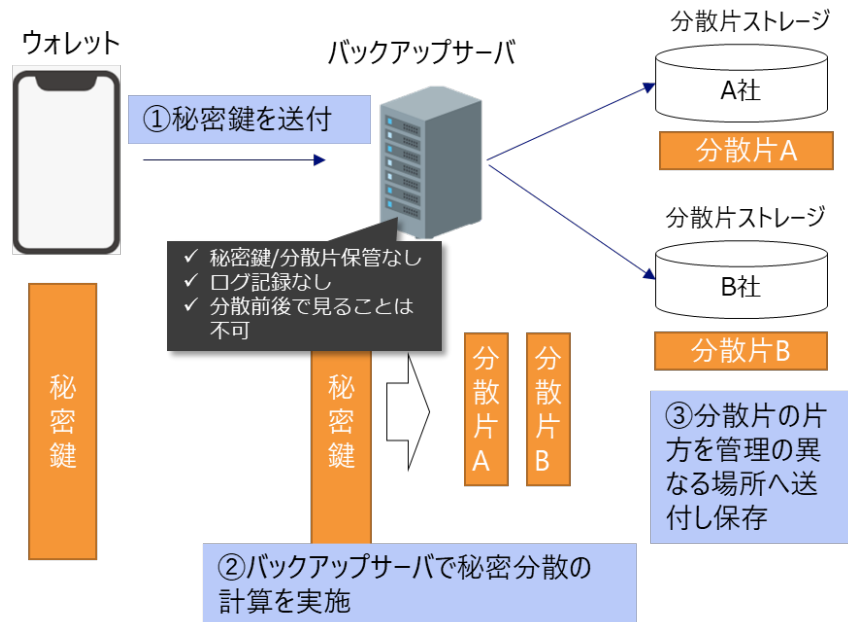
(1) 高度なセキュリティと信頼性

ユーザの資産を守るためのセキュリティは、web3ウォレットにおいて最も重要な要素の一つであり、特に秘密鍵の管理やハッキング対策の強化が求められている。

一般的に、ホステッドウォレットはウォレットの秘密鍵を事業者側で管理するため、ユーザはその事業者の一定の保証と顧客対応の中で利用を行うことができる。ID/パスワードを紛失してもアクセスを回復することができ、ブロックチェーンに関する知識がなくても利用が可能だが、事業者がハッキングされることにより一斉に資産を失うことや、一方的に出金が止められる等のリスクもある。

他方で、アンホステッドウォレットはユーザ自身が秘密鍵を保持、管理できるため、ハッキングやプラットフォーム障害等により資産が失われるリスクは低く、規制耐性も強いと考えられる。一方で利用と管理はユーザの自己責任に委ねられるため、ユーザが管理に必要なシードフレーズを忘れることで資産にアクセスできなくなる危険性がある他、フィッシングなどで資産が盗まれた際に補償を受けられない可能性が高い。そこで、アンホステッドウォレット事業者においては、事業者が秘密鍵に触れることなくユーザが秘密鍵をバックアップできる機能を提供するなどの模索がなされている。

事例：KDDIのアンホステッドウォレット「αU Wallet」では、ソーシャルIDを利用した秘密鍵のバックアップを導入し、初心者でも安全かつ容易に利用できる環境を整えている。



両ウォレットにはそれぞれ特性があることから、ウォレット事業者においては、利用シーンやユーザ自身の重視する点に応じて使い分けられる選択肢を提供するとともに、ユーザに情報提供をしっかりと行うことが重要である。

(2) 多様なブロックチェーン対応

web3エコシステムは、日本国内外で普及しているEthereumやSolana、Polygonなど、複数のブロックチェーン上で形成されている。そのため、多くのブロックチェーンに対応したウォレットが必要とされる。これにより、ユーザは異なるブロックチェーン上で発行されたNFTやトークンを一元的に管理・取引できるようになる。

(3) ユーザフレンドリーな操作性

初心者ユーザが増加する中、直感的な操作性を実現するUI/UX設計が求められる。技術用語を減らし、分かりやすいインターフェースを提供することが、web3ウォレットの普及における鍵となる。

事例：楽天ウォレットでは、暗号資産と楽天ポイントを組み合わせた独自機能を提供し、ユーザにとっての利便性を高めている。

3 web3ウォレット事業者の事業展開上のニーズ

web3ウォレットは金融、ゲームをはじめあらゆるweb3サービスを利用する際のID、決済、資産管理の基盤として機能するサービスであり、今後様々な用途に拡大していくことが見込まれる。また、事業会社が提供するウォレットは当該企業の本業や、経済圏と連携しweb2とweb3をつなぐゲートウェイとして新たなユーザ体験を広げる要になっていくと考えられる。ウォレット事業者には以下のような事業展開上のニーズがある。

(1) 暗号資産や電子決済手段と法定通貨の交換

現在、サービス提供者が暗号資産をサービス内に取り入れたい場合、暗号資産と法定通貨の交換は外部の暗号資産交換業者サービス内で行われている。しかし、例えばゲーム内で利用する暗号資産の購入、決済アプリを用いたステーブルコインによる送金等、多様な利用シーンを想定する場合、より実際の利用シーンに近い位置で法定通貨と暗号資産の交換が可能になることでユーザの利便性が向上し、利用の拡大や新たなアイデアによるサービスの創出が見込まれる。

(2) 多様なサービスへの接続

MetaMaskを始め海外事業者のウォレットは数千万人単位でユーザを獲得しており、ユーザはこれらのウォレットを利用して暗号資産の取得、交換から様々なサービスの接続までシームレスに利用できる環境となっている。日本国内においても先進層は既にこれらを利用していると見込まれ、国内事業者がこれと競争していくためには、一定の利用者保護のための規制は整備しながらも、海外事業者のサービスと同等以上の多様なサービスと連携、接続可能な自由度が確保されることが望まれる。

4 法律や制度に関する課題

web3ウォレット事業者にとって、法規制への対応は最も大きな課題の一つである。日本国内において、暗号資産や関連取引に関する制度整備が急速に進む一方で、web3ウォレット事業者に求められる要件は複雑かつ曖昧な部分も残されている。

(1) 暗号資産の交換にかかる仲介・媒介行為

資金決済法では、暗号資産の「売買」、「交換」、これらの「媒介」を業として行う行為は「暗号資産交換業」に該当する。そして、暗号資産交換業を行うにあたっては内閣総理大臣への登録が必要となる。

- 課題：アンホステッドウォレットそのものは、現状は基本的に暗号資産交換業の規制対象外ではあるが、ウォレット内でスワップ機能への接続を提供する場合や取引を促進する機能を持つ場合、どの機能が媒介行為とみなされるかについては議論がある。
- 例：MetaMaskのスワップ機能は、暗号資産の交換のP2P取引を実現するものだが、媒介行為に該当するかについては議論がある。但し、現時点において、金融規制当局が何らかの法執行を行っていることを示す公開情報はない。

本研究では、第4章、第5章において本論点をさらに深く検討する。

(2) 税制

日本の税制では、個人が暗号資産やNFT取引から得た利益は「雑所得」として分類され総合課税の対象となり、最高55%の税率が適用されうる。これは他国と比較して高水準であり、取引意欲の減退や市場縮小を招く要因となっているとの意見がある。

(3) その他の法的課題

(a) 個人情報保護法

web3ウォレットは分散型技術を活用する一方で、ユーザデータの管理に関する規制(個人情報保護法)との整合性が課題となっている。ブロックチェーン上の情報が「個人情報」とみなされる場合、その管理方法には課題を伴う。

(b) 知的財産権の保護

画像等のNFT化に関連するコンテンツの知的財産権が明確化されていないプロジェクトも多く、権利者と購入者の間でのトラブルが発生する可能性がある。これを解消するためには、NFTメタデータにライセンス情報を埋め込む標準化等が必要となる。

(4) 国による規制の不統一性

NFT、暗号資産ともに国や地域ごとに規制や許認可の制度が異なるため、ブロックチェーンを通じたデータの流通性は高い一方で、暗号資産やNFTを活用したプロジェクトの展開にはインバウンド、アウトバウンド共に法規制上の課題がある。

5 ウォレット事業者の課題解決に向けた具体的な提案

(1) 規制の柔軟化とガイドライン整備

web3ウォレットが暗号資産交換業に該当する条件を明確化し、アンホステッドウォレットとホステッドウォレットの区別をガイドラインに記載することが求められる。

(2) 税制の見直し

NFTや暗号資産取引に関する税制を再構築し、トークンの性質、利益の種類や取引規模等に応じた税率を導入することが求められる。

(3) 技術革新とユースケース拡大

ウォレット事業者は、生体認証や次世代のブロックチェーン技術を導入し、利便性と安全性を両立する新たなサービスを開発し続けている。また、NFTを活用したイベントチケットやメタバース内の資産管理など、新しいユースケースの創出が推進されている。規制当局においては、これらの発展を阻害することなくユーザ保護を進めていく必要がある。

(4) スタートアップ支援と国際整合性

新規事業者が規制の負担を軽減できるよう、特例措置や簡易登録制度を導入すべきである。また、欧州のMiCA規制など国際的な基準と整合する仕組みを構築し、日本市場の競争力を強化することが期待される。

日本国内におけるweb3ウォレット事業者は、技術革新と規制の変化の両面に対応し、web3サービスの中核であるウォレットの利便性と利用者の拡大を図っていく必要がある。特に、暗号資産に関連する交換・売買の媒介行為に対する規制の不明瞭さは海外ウォレットと比較した際の競争力獲得の障壁となる可能性がある。規制の明確化、税制の見直し、そして新たな技術とサービスの導入等が達成されることにより、web3ウォレットの次世代のデジタル経済を支える基盤としての地位を確立と多くのユーザへの普及が実現すると期待される。

(注4) <https://consensys.io/blog/metamask-reveals-55-surge-in-users-introduces-default-security-alerts-to>

第4章 web3ウォレットを取り巻くルールに関する現状と展望

1 web3ウォレットを取り巻く法規制

web3ウォレットは、web3エコシステム上で取引されるデジタル資産の管理やトランザクションの実行を行うことを可能にするアプリケーションやサービスであるため、これらウォレット上では、ユーザの保有するデジタル資産が管理されることになる。特に、web3サービス上では、NFTのミントやトランザクション実行に際してのガス代として暗号資産が必要となるほか、サービス利用時の決済手段として暗号資産やステーブルコイン(日本法上、ステーブルコインの多くは資金決済法上の「電子決済手段」に該当するため、以下ではステーブルコインを表す用語として「電子決済手段」を用いる。)が用いられることから、暗号資産や電子決済手段がweb3ウォレット上で管理される場面が想定される。国内法では、暗号資産や電子決済手段を「他人のために管理」することを業として行う場合(以下、かかる業務を総称して「カストディ業務」という。)は、資金決済法に基づく登録が必要となるため、以下では、これらの法規制の内容を概説する。

(1)暗号資産交換業

暗号資産交換業とは、①暗号資産の売買又は他の暗号資産との交換(資金決済第2条第15条第1号)、②①の行為の媒介、取次ぎ又は代理(同条第2号)、③①又は②の行為に関して利用者の金銭の管理をすること(同条第3号)、④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。)(同条第4号)のいずれかを業として行うことをいい、暗号資産のカストディ業務は④に該当する。

カストディ業務を営む暗号資産交換業者は、原則として利用者の暗号資産(に係る秘密鍵等)を、自己の保有する暗号資産とは異なるウォレット上で区分管理の上、当該ウォレットを常時インターネットに接続されていない環境下で保管(コールドウォレット管理)することが求められるほか、毎年、当該分別管理の状況につき監査を受ける等の規制に服することになる。なお、暗号資産交換業者は、利用者から預託を受けた暗号資産全量の5%を上限として、インターネットに接続されている環境下で管理(ホットウォレット管理)することが許されているが、かかる環境下で管理している暗号資産と同種同量の暗号資産(履行保証暗号資産と呼ばれる)を別途保有の上、コールドウォレットで管理することが求められる。

(2)電子決済手段等取引業

電子決済手段等取引業とは、①電子決済手段の売買又は他の暗号資産との交換(資金決済第2条第10条第1号)、②①の行為の媒介、取次ぎ又は代理(同条第2号)、③④他人のために電子決済手段の管理をすること(その内容等を勘案し、利用者の保護に欠けるおそれが少ないものとして内閣府令で定めるものを除く。)(同条第3号)のいずれかを業として行うことをいい、電子決済手段のカストディ業務は③に該当する(注5)。

カストディ業務を営む電子決済手段等取引業者は、原則として、利用者の電子決済手段を信託会社等に信託することが求められるが、当局の承認を受けることで、電子決済手段等取引業者が自己信託を行うことも可能である。なお、利用者の電子決済手

段の信託を受けた信託会社等又は自己信託を行った電子決済手段等取引業者は、原則として利用者の電子決済手段をコールドウォレット上で分別管理することが求められるほか、電子決済手段等取引業者は、当該信託保全の状況につき監査を受けなければならない。

(3) AML/CFT

暗号資産交換業者及び電子決済手段等取引業者(以下「暗号資産交換業者等」という。)は、犯収法上の特定事業者として、利用者の取引時確認を行う必要があるほか、利用者の取引がマネー・ローンダリングやテロ資金供与に利用されるリスク(以下「ML/FTリスク」という。)を低減するための必要な措置等を講じることが求められる。このような措置の一環として、暗号資産交換業者等は、利用者から指図を受けて利用者の暗号資産や電子決済手段(以下「暗号資産等」という。)を他の暗号資産交換業者等の管理するアドレスに送付する場合は、送付人や受取人等の情報を当該他の暗号資産交換業者等に通知する義務(いわゆるトラベルルール)を負う。また、後述するアンホステッドウォレットとの間で暗号資産等の移転(入出庫)を行う場合は、当該ウォレット保有者の名義を確認の上、当該移転取引のリスク評価等を行うことが求められる。さらに、暗号資産交換業者等は、外為法に基づき、利用者による暗号資産等の取引が制裁対象取引に該当しないかの確認等を行うことが義務付けられる。

2 web3ウォレットと暗号資産交換業等の該当性

(1) カストディ業務の該当性

カストディ業務を営むものとして暗号資産交換業等に該当するか否かは、「主体的に利用者の暗号資産の移転を行い得る状態」の有無によって判断される(金融庁事務ガイドライン)。かかる判断基準が採用されたのは、ある事業者が利用者の暗号資産等を自由に移転できる状況にあるならば、当該事業者の行為に起因して、暗号資産等が外部に流出したり、マネー・ローンダリング等に利用されるリスクが認められるが、利用者の暗号資産等を事業者が移転できないのであれば、これらリスクが限定されており、規制を及ぼす必要性に乏しいからである。

例えば、事業者単独で(あるいは他の関係事業者と共同して)利用者の暗号資産等を移転でき得るだけの秘密鍵を保有する場合には、当該「状態」にあるものとして暗号資産交換業等に該当する。ユーザの秘密鍵をウォレットサービスの提供者が管理する「ホステッドウォレット」については、ウォレットサービス提供者が秘密鍵を用いて利用者の暗号資産等を移転でき得る状態にあるため、カストディ業務に該当する一方、サービス提供者が利用者の秘密鍵にアクセスできずユーザ自身が秘密鍵を管理する「アンホステッドウォレット」については、サービス提供者は利用者の暗号資産等を移転でき得る状態にないため、カストディ業務に該当しない。

(2) 媒介の該当性

後記3のとおり、web3ウォレットは、デジタル資産等の管理にとどまらず、web3サービスへのアクセスゲートウェイとしての重要な役割を担っているため、法定通貨と暗号資産等の交換機能(いわゆるオンランプ／オフランプ機能)の実装が期待されている。そのため、web3ウォレットのUI(User Interface)上で、提携する暗号資産交換業者

等の営む販売所や取引所サービスにおける取引画面等に遷移できるリンクを設けたうえで、当該暗号資産交換業者等のサービスの概要や利用ガイドを表示することによって、暗号資産等と法定通貨の交換を促す画面等を設けることが考えられる。かかるweb3ウォレット上の画面表示が、暗号資産交換業者等とユーザ間の暗号資産等の売買の成立に尽力していると評価されてしまうと、web3ウォレット提供者の行為が暗号資産等の売買の「媒介」を行っているとして暗号資産交換業等に該当することになるが、ウォレット提供者は暗号資産交換業等の登録を有していないケースも多いため、実務的には「媒介」に至らない程度の表示を模索することになる。

この点につき、令和6年9月6日に「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)が改正され、暗号資産交換業者等による暗号資産等の売買等の媒介の範囲及びその該当性の明確化が図られるに至っている。例えば、ウェブサイト上において、暗号資産交換業者等の業務内容について説明を行うことや、暗号資産交換業者等のサイトへの単なるリンクの設定や暗号資産交換業者等から提供を受けた商品案内等のコンテンツの転載のみを行うことは、単に顧客を紹介するものとして「媒介」には当たらないとされており(ただし、リンクの設定やコンテンツの転載にとどまらず、独自の見解として商品等を推奨・説明する場合には「媒介」に当たることがありうる(同ガイドラインⅠ-1-2-2②(注2)c。))、かかる限度で暗号資産交換業等のサービスを紹介する画面等をweb3ウォレット上に表示したとしても、直ちに暗号資産交換業等に該当するものではないと考えられる。

3 web3ウォレットに望まれるルール整備

(1)現状の課題

web3が、ブロックチェーン技術及びトークンエコノミーの形成を裏付けとして、エコシステムに参加するユーザ自身がデータやデジタル資産を自ら保有管理するビジネスあるいは社会モデルである以上、web3ウォレットの機能も、自ずとユーザ自身が秘密鍵を管理できるウォレット(アンホステッドウォレット)が指向されるものと思われる。

そして、web3ウォレットは、デジタル資産等の管理にとどまらず、web3サービスへのアクセスゲートウェイとしての重要な役割を担っており、法定通貨とデジタル資産の交換機能(いわゆるオンランプ／オフランプ機能)であったり、分散型金融(DeFi)その他の分散型アプリケーションに接続する機能の実装が期待されている(なお、分散型金融(DeFi)及びDeFiへの接続機能の法的論点等については第5章を参照)。

しかし、上記2のとおり、同タイプのweb3ウォレットを提供する事業者の行為はカストディ業務に該当せず、現状、資金決済法や犯収法上の各種規制は適用されない一方で、暗号資産交換業等に該当する行為を行うことはできないため、①暗号資産やステーブルコインを法定通貨に交換する機能を自ら提供することは事実上困難といえる。また、アンホステッドウォレット間で行われる取引(P2P取引とも呼ばれる)は、前記2で述べたAML/CFT規制が適用されず、匿名性が高いため、②一般的にML/FTリスクが高いと解されており、web3ウォレットが既存の金融サービス(TradFi)から敬遠される可能性も孕んでいる。

以上のようなweb3ウォレットに関する現状の課題(ペインポイント)に対しては、以下に述べる①新たな仲介制度の創設と、②既存の決済・金融サービスとの連携・接続を図ることが解決の糸口となりうるように思われる。

(2) 新たな仲介制度の創設

2025年1月22日に公表された「金融審議会 資金決済制度等に関するワーキング・グループ 報告」(14頁以下)では、ゲームアプリやアンホステッドウォレット等をウェブ上で提供する事業者が利用者に対して暗号資産交換業者等を紹介する場面等を念頭に、利用者の財産の預託を受けることなく、暗号資産等の売買等の媒介のみを業として行う者については、特定の暗号資産交換業者等に所属することを前提に、財務要件やAML/CFT規制を課さない簡易な仲介制度を創設することが提案された。そして、本年6月6日に国会で成立した資金決済法改正において、1年以内に電子決済手段・暗号資産サービス仲介業を導入することになった。

アンホステッドウォレットタイプのweb3ウォレットを提供する事業者は、かかる新たな仲介制度を活用することによって、上記2(2)のような「媒介」に至らない紹介行為を超えた機能提供(つまり、媒介行為)ができる可能性がある。

例えば、所属する暗号資産交換業者の販売所や取引所サービスとweb3ウォレットをAPIで連携することによって、当該web3ウォレットのアプリ画面上にて暗号資産等の取引の受発注を行い、かつ、web3ウォレットを用いた暗号資産等の入出庫が可能になる等、シームレスなユーザ体験を実現することが可能になる。

(3) CeFiとの連携・接続

第3章で述べたとおり、国内においては大手プラットフォーマーを中心にweb3サービスへの参入が活発化しており、web3ウォレットは、これらプラットフォーマーが提供するポイント、電子マネー、クレジットカード等の既存の決済・金融サービスとの連携・接続を行うための重要なハブとなりうる。

これら既存サービスとweb3ウォレットが接続することにより、web3サービス及びデジタル資産が広く大衆に普及(マスアダプション)することが期待できる。また、上記(2)で述べた所属先の暗号資産交換業者等のほか、クレジットカード会社や資金移動業者等の既存の金融サービス提供者が、web3ウォレット(アンホステッドウォレット)ユーザの取引時確認を実施し、制裁対象ウォレットのフィルタリングやブロックチェーン解析ツールを用いる等によりML/FTリスクが適切に評価されれば、web3サービスに内包される全てのML/FTリスクを排除することはできないにせよ、web3ウォレットユーザを介したリスク・コントロールが一定可能になると思われる。すなわち、web3ウォレットが中央集権的な金融サービス(CeFi: Centralized Finance)と接続すればするほど、(金融事業者を介した)複眼的なリスク評価が可能となる結果、ML/FTリスクを低減できる度合も相対的に増すものと考えられる。

4 小括

このように、web3ウォレットがCeFiとの連携を図ることによって、安心・安全なサービスの提供が可能になるほか、新たな仲介制度は、暗号資産交換業者等を通じた暗号資産等の法定通貨(又は他の暗号資産等)との交換を実現しやすくする制度として、web3ウォレットとCeFiの連携をさらに加速させることが期待される。他方で、web3の本質は中央集権的要素(トラストポイントとも呼ばれる)を介さないことによる自己主権型のサービスを展開できる点にあるため、かかるコンセプトを実現するべくweb3領域で完結するサービスをどのように構築するのか、特に、分散型金融(DeFi)をどのように評価し利用すべきかの問いを避けて通ることはできない(第5章に続く)。

(注5)資金決済第2条第10条第4号に規定する業務は、電子決済手段に関連しないため、省略している。

第5章 DeFiの法規制とweb3ウォレットのDeFi接続に関する法的論点

1 DeFiとは

(1) イントロダクション

分散型金融(DeFi、Decentralized Finance)とは、伝統的な金融仲介業者を介することなく、分散台帳技術(DLT)を活用して暗号資産などのデジタル資産の貸付けや投資、交換などの金融サービスを提供する新たな金融サービスを総称する言葉である。伝統的な仲介業者による事務処理に替えて、DeFiではこれらの事務処理ロジックをコード化したソフトウェアプログラム、すなわちスマートコントラクトによってトランザクションを自動処理する。これにより利用者は、仲介業者とやり取りすることなく、ソフトウェアプログラムを通じて、自らの資産を運用することができる。

DeFiに対置される用語としてTradiFiやCeFiといった用語がある。TradiFiは銀行や証券会社などの伝統的な金融サービス業者を仲介者として成立する金融サービスを示す概念であり、ブロックチェーンとの関わりのない金融サービスが念頭に置かれている。これに対してCeFiは、こうした伝統的な金融サービス業者に加え、ブロックチェーンのエコシステムの中で金融仲介サービスを提供する事業者が存在することによって成立する金融サービスを含む概念である。たとえば、暗号資産交換業者は、利用者に対してウォレット(ホステッドウォレット)を提供することによりカストディ業務を提供し、利用者の暗号資産の売買・交換需要に対して、自らまたは他の利用者の保有する暗号資産や法定通貨と売買・交換ないしそのマッチング業務を提供する。これら暗号資産交換業者のサーバで中央集権的に行われる事務処理を伴う金融サービスはCeFiと呼ばれる。

これに対してDeFiは、取引のすべてがブロックチェーンの分散台帳上に記録され、分散台帳上で実行される金融サービスを示す概念である。EVM互換ブロックチェーンにおいては、取引はスマートコントラクトによる処理がなされることになり、EVMの特性である、いったん設置されたスマートコントラクトのコードは変更が困難であるという性質により、改竄耐性が確保されることとなる。すなわち、技術により、金融規制に基づく態勢整備がなされるCeFiとは異なる形で、サービスのセキュリティと透明性を高めている。

本章では、EVM互換のブロックチェーンを基本的に念頭に置きながら、DeFiの金融サービスとしての主要な特徴とそのアーキテクチャを説明する。そのうえで、DeFiサービスに対するCeFiを念頭に置いた現状の金融規制の適用可能性の検討を経て、これに対する入り口となるweb3ウォレットとそのサービスに対する金融規制の適用可能性を検討する。以上を踏まえて、国際金融組織におけるDeFiサービスに対する規制動向を概説し、結びとしてあるべきDeFiに対するルールについて言及する。

(2) DeFiの金融サービスとしての主要な特徴

DeFiはブロックチェーン上に設置され、そのすべてが分散台帳に記録されたうえで実行されることになる。この分散台帳の記録とコントラクトの実行(すなわち台帳記録の更新)の処理は、多数のバリデータ(更新処理の確認者)の報酬をめぐる競争により担われている。この点は、金融サービス事業者が集中的に取引を管理する(つまり、帳簿

(アカウント)の記録と更新を行う)CeFiとは大きく異なる。CeFiにおいては、取引が集中的に管理されることから大規模化と寡占化が進んできたために、大きすぎてつぶすことができない結果、競争が潜在的にゆがめられているとの批判もある中、より分散化された新たな金融取引手段として登場してきたのがDeFiである。

また、DeFiにおいては、利用者は、インターネットを通じて世界中から提供されるコントラクトのうち、どのコントラクトを利用するか、自ら選択することができる。様々なエンジニアが開発した複数のコントラクトを組み合わせることで、より特徴のある、または複雑な取引条件にも対応することが可能である。そしてDeFiでは、これらのすべてを、利用者がカストディ業者を介さずに、自らが管理するweb3ウォレットから直接行うことができる高い自由度が確保されている。サービスの多様性や自由度の高さ、金融サービス事業者が取引データを囲われることなく金融取引を実現することができることがDeFiの大きな特徴である。このデータ自己主権の維持といった特性は、インターネット上で自律分散的に価値をやりとりすることができるweb3の表れとして、これまでの金融取引では実現することができなかった新たな価値であり、DeFiがポジティブなイノベーションとして捉えられるべき重要な特性といえる。

加えて、スマートコントラクトはいったん設置すれば以後変更することが困難であるため、コントラクトコードをよくレビューして意図したとおりに動作することを確認できれば、分散台帳のすべての記録と更新が記録され、誰でもこれを閲覧することができる。そのため、DeFiは、CeFiに比べて透明性の高い金融サービスであると評価することができる。そしてこの特性は、FTXやCelsiusといったCeFiが外部から見た不透明性のゆえに大規模な破綻を見たことを経験したことを踏まえると、DeFiが持つ強みとしての側面も持つ。

一方で、カストディ業者をはじめとする仲介業者が存在しないこととの裏表の関係として、DeFiには利用者保護の手段が組み込まれていない場合もあり、犯罪行為や不正行為、コントラクトのバグによる利用者の損失や金融秩序の侵害に対して脆弱性を抱えている。様々なコントラクトを組み合わせる生成されるDeFiサービスにつき、事前にそのすべてをレビューし安全性を評価することが現実的に利用者に期待できるのか、そもそもエンジニアではない利用者にコードをレビューして評価することが可能なのかといった点は、課題となりうる。また、利用者の保護という観点からは、サービスのセキュリティ(特に完全性)が確保されていないリスクについては自己責任の問題として整理することができるとしても、悪意のある利用者がDeFiを用いてマネー・ローンダリングを試みたり、利用者の意図にかかわらず悪意のあるコントラクトによって利用者のデジタル資産がテロの資金源とされたりすることは、利用者の保護の問題とは別に抑止されなければならない。そのためのメカニズムが現状まだ実装されていない点に、DeFiが解決しなければならない課題があるといえる。

(2) 基本的なリファレンスアーキテクチャ

DeFiの技術アーキテクチャは、以下の3つのレイヤーから構成されると考えられる。

(a) 決済レイヤー

このレイヤーは、取引を実行し、取引後のデジタル資産の残高を更新する機能を提供する。コントラクトに基づく取引がブロックチェーンネットワークに配信され、バリデータによる合意が成立すると取引が実行される。このレイヤーを機能させるためには、バリデータに報酬としてネイティブトークン(例:ETH、SOL)が必要となる。

(b) アプリケーションレイヤー

このレイヤーは、スマートコントラクトを通じて実装される様々なアプリケーションによって構成される。アプリケーションレイヤーをさらに細かく見ると、同レイヤーはさらに3つのサブレイヤーから構成されている。

①デジタルトークン(ステーブルコインやセキュリティトークンなどを含む広い意味でのcryptoassets):ステーブルコインやセキュリティトークンなど、価値移転のためのトークン。USDTのような代替性トークン(FT)とNFTのような非代替性トークン(NFT)が存在する。

②DeFiプロトコル:金融サービス機能を提供するプロトコルで、主にレンディング、デリバティブ、分散型取引所(DEX)に分類される。

③DeFiコンポジション:複数のDeFiプロトコルを組み合わせ、新たな金融サービスを提供。例えば、DEXアグリゲータは最適な取引レートを提供するDEXを選定し、イールドアグリゲータは資産を最適なDeFiプロトコルに自動分配して利回りを最大化する。

(c) インターフェースレイヤー

利用者向けの画面インターフェースを提供する。サービス提供者のサーバから配信される場合や、web3サイトを通じて分散型の形態で提供される場合がある。

web3サイトは、IPFSなどの分散型ファイル共有プロトコルを用いて実装され、ブロックチェーン技術とスマートコントラクトを利用してサービス提供者とユーザ間のデータのやりとりを実現する。

2 DeFiサービスに対する従来の金融規制の適用可能性

(1) 問題の所在

日本に限らず世界中の金融規制は、これまでTradFiすなわち金融サービスを管理・運営する特定の事業者が存在することを前提に、金融サービス事業者に対して規制を課す形の法体系を採用している。そして、暗号資産に関する規制として各国においてこの十年ほどの間に導入されている規制も、CeFiすなわち暗号資産交換業者等(世界的にはVirtual Asset Service Provider: VASPと呼ばれる。)が存在することを前提として、そのVASPに対する規制体系を構築するものであったといえる。つまり、現在の金融規制は、説明したようなDeFiの技術アーキテクチャを想定した法体系になっていない。

しかし、金融規制体系がDeFiを想定していないという事実は、DeFiが既存の金融規制に服しないことを直ちに意味するものではない。あるイノベティブなサービスが、想定をしていない規制体系のスコープにたまたま入ってしまうことはしばしばみられ、その場合、伝統的なサービスに対する規制がイノベティブなサービスに対して適用される。イノベティブなサービスは、伝統的なサービスと異なる価値観を実現するものであるにもかかわらず、その価値観を共有しない規制体系をそのまま適用すれば、イノベーションが目指す価値の実現が困難となるため、適時適切に規制の見直しを検討しなければならない。

以下では、代表的なDeFiアプリケーションである分散型取引所(DEX)、レンディングおよび運用の一種であるステーキングを取り上げて、それぞれに対して日本の現行の金融規制が適用されるものであるかどうかを検証する。

(2) DEX

DEX(分散型取引所)とは、一般に、ブロックチェーン技術を活用し、スマートコントラクトを用いて、第三者を介さずに利用者間で直接暗号資産等の取引をすることができる取引所をいう。

DEXにまつわる暗号資産交換業等(電子決済手段等取引業を含む。以下同じ。)該当性については、先述したDeFiアーキテクチャに照らすと、以下の3点での議論が必要になる。

(a) DeFiアプリケーションの開発者は暗号資産交換業等に該当するか

(b) DeFiアプリケーションを利用して流動性プールを提供する者は暗号資産交換業等に該当するか

(c) 利用者によるDeFiアプリケーションへのアクセスを容易にするためのインターフェースを提供する者は暗号資産交換業等に該当するか

(a) DeFiアプリケーションの開発者の暗号資産交換業等該当性

DEXは、技術的にいえば、第三者を介さずに利用者間で直接暗号資産等の交換をすることができるスマートコントラクトの機能そのものといえる。先述したDeFiアーキテクチャでいうところのアプリケーションレイヤーに属するものであり、これはソフトウェア開発という技術レイヤーに属するものである。つまり、スマートコントラクトの機能をブロックチェーン上に設置し、このツールをインターネット空間上に置くこと自体は、必ずしも暗号資産等の売買等やその媒介等に該当するものではないと考えられる。

なお、報道によれば、米国においては、米国証券取引委員会(SEC)がUniswapが証券取引所及び証券ブローカー・ディーラーとして機能しているとして証券法違反の疑いで開発者であるUniswap Labsに対する調査を行っていたが、これを終了したとのことである(注6)。

(b) 流動性プールの提供者の暗号資産交換業該当性

DEXに対して流動性を提供する者、つまりDEXによるP2P取引において、利用者による暗号資産等の交換需要に応じるために交換先の暗号資産等を大量に預け入れておく、交換取引の相手方は、暗号資産交換業者等に該当するか。

この点、利用者は流動性プールを利用して暗号資産等の交換を行うという事実を鑑みれば、流動性プールの提供者は、暗号資産等の交換又はその媒介を行っていると評価される可能性がある。

そうすると、流動性プールの提供者は、それが業として行われるものである限り、暗号資産等の交換又は媒介を業として行う者として暗号資産交換業等に該当するという帰結になる。この「業として」という要件は、反復継続性と対公衆性といった総合的な事情を加味して個別具体的に判断されるものとされているが、流動性プールの提供者については、単なる個別のP2P取引という側面を超えて広く公衆を相手としている面は否めず、現行規制とその運用に照らすと、流動性プールの提供者は、形式的には暗号資産交換業等に該当していると判断される可能性はあると思われる。

流動性プールの提供者が暗号資産交換業者等に該当するという結論は、現行法による限り、流動性プールの提供者は暗号資産交換業等の登録をしなければプールの提供ができないということを帰結する。しかしながら、暗号資産交換業等は、もともとDEXにおける流動性プールの提供者を念頭に規制を設計したものではないため、流

動性プールの提供者に暗号資産交換業等の登録を求めるという帰結は、対応不可能な規制をプールの提供者に適用すること(つまり、事実上サービスを禁止すること)を意味するため、これが望ましい結論なのかについては疑問の余地がある。

このように、我が国の暗号資産規制体系は、その設計に当たり伝統的な金融サービスとはその基本的な構造が異なるDEXを想定していないため、DEXの流動性プールの提供者につき、偶発的に規制対象に取り込んでしまっている可能性がある。

(c) DeFiアプリケーションへのアクセスを容易にするインターフェース提供者に対する暗号資産交換業等該当性

DEXのスマートコントラクトをインターネット上に設置するに留まらず、利用者をDEXに誘導して暗号資産等の取引を行わせるインターフェースを提供する場合、暗号資産等の交換の媒介を行うものとして、暗号資産交換業等の登録を受ける必要が生じる可能性がある。

この点、金融庁は、無登録で暗号資産交換業を行う者に対して警告書を発出し、その旨を公表しているが(注7)、DEXプラットフォームの代表例であるUniswapに関しては、Uniswap Labsが日本語で暗号資産等の取引が可能なインターフェース(ウェブサイトやアプリケーション)を提供しているにもかかわらず無登録暗号資産交換業者であるとする警告書を発出していない。すなわち、金融庁によって資金決済法が適正に執行されていることを前提とするのであれば、Uniswap LabsのようにDeFiアプリケーションのみならず、DEXのインターフェースの提供者の行為についても、暗号資産等の交換の媒介にまでは至らず、暗号資産交換業等の登録を要しないと整理している可能性がある。

(2) ステーキング

ステーキングとは、典型的にはブロックチェーンの運用やセキュリティを支援するために一定量のトークンをロックアップし、その報酬として追加的にトークンを受け取ることができる仕組みのことをいう。ステーキングによってブロックチェーンのトランザクションを検証し、ブロックチェーン上の記録の整合性を確保することができるようになっているものが典型である。

トークンをロックしたことの報酬として一定のトークンを受け取ることができる仕組みは、技術的にはスマートコントラクトにより実装することができる。そのようなスマートコントラクトを開発してインターネット空間上に置き、サービス提供者がこれを使うことができる状態に置くこと自体は、DEXにおける議論と同様、先述したDeFiのリファレンスアーキテクチャにおけるDeFiアプリケーションの開発行為に過ぎず、これがなんらかの金融規制に抵触することはないと考えられる。

他方、ステーキングの仕組みに利用者のアクセスを容易にするサービスは、これが暗号資産等のカストディとして暗号資産交換業等又は集団投資スキームの提供として金融商品取引業に該当しないかが論点となる。

この点、ステーキングには様々なモデルがあるため、その具体的な内容に応じて個別具体的に判断することになるが、たとえば、ロックアップされた暗号資産を移転することができる秘密鍵が利用者に留保されるような仕様になっている場合には、暗号資産等のカストディにも集団投資スキームの提供にも該当しないと考えうる。

(3) レンディング

DeFiにおけるレンディングとは、一般に、銀行や仲介者を必要とせずに暗号資産等の貸し借りを行うことができるローンサービスをいう。

DeFiレンディングについても、DeFiのリファレンスアーキテクチャをベースに規制の適否を検討することになり、DeFiアプリケーションを開発し、インターネット上に設置するのみでは金融規制の適用はないと考えられる。他方で、利用者がDeFiアプリケーションにアクセスできるサービスを開発してこれを利用者に提供した場合、貸金業法の適用があるかどうか問題となる。

この点、貸金業法は「金銭」の貸付けを対象としており、「暗号資産」の貸付けは、個別事例ごとの実態に即した実質的な判断が必要になるものと考えられるものの、一般的には貸金業に該当しないと考えられている(注9)。他方、ステーブルコイン(電子決済手段)については、金銭と同一の経済的利益を有すると考えられることから、貸金業への該当性につき慎重な検討を要するものと考えられる。

3 DeFiサービスに接続するweb3ウォレットに対する従来の金融規制の適用可能性

(1) 問題の所在

web3ウォレットは、利用者がウォレットにデジタル資産を保管し、DeFiを利用できるようにするという意味で、web3ウォレットはDeFiへの接続の入り口(ゲートウェイ)であると位置づけることができる。

web3ウォレット事業者は、一般的に、アプリ提供プラットフォーム(AppStoreやGoogle Playなど)を通じてweb3ウォレットアプリを利用者に提供している。

こうしたweb3ウォレット事業者の行為に対して、金融規制、特にDeFiが提供する金融サービスに対する仲介規制が適用されるかを検討する。

(2) DeFiサービスに接続することの媒介該当性

事業者が暗号資産等の交換等の媒介を行う場合には、当該事業者は暗号資産交換業等の登録を受ける必要がある。

現行の媒介規制については第4章で述べたところであり、従来の議論は資金決済法上の暗号資産交換業者のサービスへの接続が中心であったが、以下ではweb3ウォレットからDeFiへの接続についても規制の対象となるかについて検討を行う。

(a) DEXへの接続について

web3ウォレット事業者が、web3ウォレットをDEXに接続してウォレット上で暗号資産等の交換を行うことができるようなサービスを利用者に提供した場合、暗号資産等の交換の媒介を行うものとして、暗号資産交換業等の登録が必要になる可能性がある。

なお、第4章で述べたとおり、暗号資産等の売買等の媒介のみを業として行う仲介制度が創設されることとなったが、いわゆる所属制が採用されることから、暗号資産交換業登録を有しないDEXへの媒介は仲介制度の対象外となる。したがって、DEX

への接続が暗号資産等の交換の媒介にあたる場合、所属先の暗号資産交換業者がないため上記仲介制度に基づく登録を受けることができないことから、従来の暗号資産交換業登録が必要となる。媒介のみを行う事業者に従来の暗号資産交換業登録を要求すると規制対応コストとの見合いで経済的にそのようなサービスの提供者は現れないことが、仲介制度を創設することとなった背景にあることを考えると、DEXへの媒介が暗号資産交換業に該当するものとされると、DEXへの媒介サービスの提供は我が国ではできないということになってしまう。

web3ウォレットからDEXに接続するサービスには様々な実装方法が考えられる。そこで、以下では具体的な実装例に照らして、各行為が暗号資産等の交換の媒介に該当するかを個別に検討する。

① DEXへ接続できるリンクのweb3ウォレット上での掲載

web3ウォレット上で、特定のDEXを特段推奨することなく、単に複数のDEXのリストを掲載するという実装が考えられる。この場合、利用者において、リストからDEXを選択するとサービスサイトに遷移し、同サイトにおいて利用者自らがDEXを利用した交換を行うものであれば、ウォレット上でのリンクの掲載はDEXの紹介にとどまる。したがって、暗号資産交換業等の登録が不要になるものと考えられる。

② DEXへのインターフェースをユーザがweb3ウォレット内に組み込める仕様の提供

既存のDEXサービスをユーザがweb3ウォレット上に表示することができるようにすることで、利用者がweb3ウォレットから暗号資産等の交換を行うことができるようにする実装が考えられる。Googleが提供するウェブブラウザ「Chrome」における拡張機能(extention)のような実装である。ユーザは、ChromeでMetamaskの拡張機能を利用することができ、これによりChrome上でMetamaskから接続されるDEXを利用することができることになるが、これによってGoogleが暗号資産等の交換の媒介をしているものと評価されたことはない。そうであるとする、web3ウォレットにサードパーティ製サービスの拡張機能を表示することができる機能を付し、web3ウォレット事業者以外の者が拡張機能としてDEXへの接続サービスを提供する場合、利用者がその拡張機能を自らインストールしてweb3ウォレット上で暗号資産等の交換ができるとしても、web3ウォレット事業者は暗号資産等の交換の媒介をするものではないと考えられる。

③ DEXへのインターフェースとなるミニアプリの組み込み

web3ウォレット事業者がミニアプリの組み込み機能を提供し、DEXサービスの提供者のミニアプリを組み込んでユーザに提供する実装が考えられる。

この場合、②と異なりミニアプリのインストール自体はweb3ウォレット事業者側で行われた形でユーザに提供されるものの、ユーザが実際にサービスを利用するにあたってはDEXサービスの提供者(ミニアプリの提供者)を明確に認識し、利用規約等に同意して利用を開始することとなる。そうすると、利用開始後の個別のDEXサービス利用に関しては、web3ウォレット事業者において一切関知しないこととされている場合には、web3ウォレット事業者としては「場」を提供しているのみであり、暗号資産等の交換の媒介には至らないとの評価もありうると考えられる。

④ DEXへのインターフェースを自ら提供する行為

端的にweb3ウォレットから直接DEXに接続し、暗号資産等の交換を行うことを可能とする実装もありうる。この場合、web3ウォレットから直接暗号資産等の交換が可能となるユーザ導線が用意されるため、現在の規制枠組みを前提とすると、web3ウ

ウォレット自体が暗号資産の交換を媒介する機能を有しているものと評価される可能性がある。

しかしながら、Uniswap LabsはUniswapに接続可能なUniswap Walletを日本語で提供しており、また、Consensys社も代表的なweb3ウォレットアプリケーションであるMetamaskを通じてDEXを利用するサービスを展開しているが、金融庁はこれまでのところ無登録暗号資産交換業者であるとする警告書を発出していない。このような現状を踏まえると、金融庁はDEXに接続可能なweb3ウォレット提供者の行為については、(特定の交換のみを積極的に推奨したりしない限り、)暗号資産等の交換の媒介にまでは至らず暗号資産交換業等の登録を要しないと整理している、あるいは、現時点においては規制を適用する必要性は必ずしも高くないと整理している可能性がある。

日本国内の事業者が提供する主要なweb3ウォレットにおいて同様のサービスを展開している例はまだ見当たらないが、金融庁が上記のとおり整理している場合には、国内事業者によるサービス展開がなされた場合でも同様の整理がなされるべきと考えられる(競争政策上の観点からも、国内事業者か海外事業者かによって法解釈や法適用が異なることは望ましくないと考えられる。この点については、第6章参照。)

なお、報道によると、米国証券取引委員会(SEC)は、Metamaskを通じたデジタル資産の交換機能の提供が証券法に違反するとしてConsensys社に対し訴訟を提起していたが、この訴訟を取り下げることで基本合意に達したとのことである(注8)。米国が、DEXへの接続を提供する代表的なweb3ウォレットであるMetamaskを提供する同社のサービスを容認する方針へと進んでいることは、我が国においても注目すべきといえる。

(c) ステーキングサービスとの接続について

web3ウォレットをステーキングサービスへの接続に関して、上記2(3)に記載の通り、ステーキングサービスが暗号資産等のカストディ又は集団投資スキームの提供に該当しない場合は、基本的には業規制に服するものではないと思われる。

(d) レンディングサービスとの接続について

暗号資産の貸付けは一般に貸金業に該当しないものとされていることからすれば、その媒介も貸金業に該当するものではないから、web3ウォレットを暗号資産を対象とするレンディングサービスに接続させることについては、実装方法の如何を問わず、貸金業には該当しないものと考えられる。

他方で、ステーブルコイン(電子決済手段)の貸付けを対象とするレンディングサービスとの接続に関しては、「金銭」の貸付の媒介に該当するか否かについて検討を要する。仮にステーブルコインが「金銭」とみなされる場合には、DEXの場合と同様の場合分けに基づいて媒介該当性を検討することになると考えられる。

4 DeFiサービス/web3ウォレットに対する規制のあるべき方向性

(1) 現在の状況と検討の方針

本研究時点においては、DeFiの規制についてはDeFiサービスに接続可能なweb3ウォレットに対する規制の方向性について、国際的に統一的な整理はなされていない。これまでのところ、各国における証券市場を規制する政府機関から構成される国際団体

であるIOSCO(International Organization for Securities Commissions)が2023年12月に公表したDeFiに関する政策勧告の最終報告書(以下「DeFi最終報告」という、注10)や、EUの主要な暗号資産規制(MiCA)の下でルールを設定する予定のEU機関であるEuropean Securities and Markets Authority(ESMA)が2023年11月に公表したEUにおける分散型金融:発展とリスクと題する報告書(注11)が公表されているほか、日本国内でも金融庁の委託により株式会社クニエが実施した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が実施されるなどしている(注12)が、統一的な整理には至っていないという状況である。

そこで、本報告においては、代表的な報告書であるIOSCOのDeFi最終報告の概要に触れつつ、DeFiに対する規制のあるべき方向性、更にはDeFiサービスに接続可能なweb3ウォレットに対する規制の方向性について検討を行う。

(2) IOSCOによる最終報告

DeFi最終報告は、DeFiが既存の金融規制体系の想定していない形で金融サービスを提供するものであることに鑑み、各国の規制機関がDeFiに対して、どのような目的のもと、誰の、どのような行為を、どのような形で規律していけばよいのかにつき、一定の共通の目線を提供することによって、各国の規制機関の活動を支援することを目的とするものである。

IOSCOがDeFi最終報告において採用しているDeFiに対する規制スタンスは、以下のように要約することができる。

(a) 同一活動、同一リスク、同一規制成果の原則が適用される

DeFiに対しても、金融規制の原則である同一活動、同一リスクに対しては同一の規制ないし同一の規制成果が期待される規制体系が適用されるとの原則が適用される。具体的に適用される規制体系は、既存の規制体系であるのか、新たな規制体系であるかは問わないが、現行の規制体系によってアドレスしようとしているリスク種別に対して、同等程度にリスク軽減の成果が発揮されるように規制が及ぼされるべきである。適切な規制対応を決定するためにはまず、DeFiのサービスをよく分析しなければならない。

(b) DeFiにも規制対象となる責任者が存在する

DeFiが仲介業者を介することなく利用者が金融サービスにアクセスする手段を提供するものであったとしても、これが金融ソリューションとして提供されている以上は、必ずそのサービスを管理している、もしくは少なくともそのサービスに対して十分な影響力を保持している事業者、団体または個人がいるはずであるとの考えのもと、まずそれが誰に当たるのかを特定し、これを責任者として規制対象とするべきである。

(c) 規制成果の達成

既存の金融規制の適用の方法であれ、新たな規制体系を準備するものであれ、規制成果のレベルにおいて、IOSCOが定める共通基準と整合性がとれるように、DeFiに対する規制対応を実施しなければならない。規制成果の達成という観点から、適用される規制は、投資者保護のための規制とマーケットインテグリティ規制が含まれることになる。

(d) 責任者に対する利益相反の管理

DeFiの責任者に対する規制に当たっては、DeFiの責任者の利益相反関係を特定し、これを適切に管理するための規制体系を設計し、適用しなければならない。

(e) 重要なリスク管理

そのDeFiサービスに関する重要なリスクを特定し、そのリスクを責任者に管理させるような規制体系を設計し、適用しなければならない。管理対象となる重要なリスクには、オペレーショナルリスクやテクノロジーリスクが含まなければならない。

(f) 十分なディスクロージャー

DeFiサービスの責任者に対して、提供するDeFiサービスに関する包括的かつ明確な開示を要請し、利用者に対して適切かつ正確な情報を提供することで、投資者保護とマーケットインテグリティの確保を促進しなければならない。

(g) 適切な法執行

規制当局は、DeFiサービスないし責任者に対する、適切な検査・監督、モニタリング及び法執行の権限を確保しなければならない。適切な法執行のために、規制当局は、自組織の技術知識やデータ、ツール等をレビューし、組織に必要なケイパビリティを導入し訓練する必要がある。

(h) 国境を越えた情報共有と協力

規制当局は、国内外の関連する他の規制当局者との間で協力し、DeFiサービスや責任者に関する情報を積極的に共有しなければならない。

(i) TradiFiやCefiとの相互連動性

規制当局は、DeFiサービスの分析に当たっては、DeFiにとどまらないクリプトプロダクト市場全体への波及やこれとの相互連動性、さらにはTradiFi市場へのリスクの伝播といったものを考慮しなければならない。投資者の保護の観点及びマーケットインテグリティの確保の観点から、DeFiサービスが及ぼすTradiFiを含むCeFi全体へのマクロ的な影響を分析し、必要なモニタリング体制を整備しなければならない。

(3) DeFiに対するあるべき規制の方向性

IOSCOのDeFi最終報告の概要は上記のとおりであるが、IOSCOのようなもととTradiFiを対象としていた監督者団体の報告は既存の金融規制の体系の発想内でDeFi規制を検討しがちである。DeFiのルール体系を検討するにあたっては、まずもってDeFiの技術アーキテクチャをよく理解する必要した上で、テクノロジーガバナンスの体系によって規制されるべきではないかについても、中立かつ公正に検討する必要がある。

テクノロジーガバナンスの体系とは、経済活動の付加価値の創造メカニズムが、インターネット空間におけるデータプロセッシングに多くを依拠するサイバー・フィジカル空間(CPS)の一体運用に移行しつつあるとの事実認識のもと、国家統治の構造自体をトランスフォームしていこうとする我が国のイニシアティブ「ガバナンスイノベーション」の哲学をバックボーンとする、データと最新技術のガバナンスのための新たな体系である。政府が上から規制を押し付けるリバイアサン型の規制体系は、むしろ民間の方が最新の技術情報とデータを持ち合わせている現在の状況になじまず、情報劣位にある政府当局からスマートでない規制を押し付けることにより、最新の技術やデータ収集から得られる価値創造、ひいては国富の獲得が妨げられる結果となるとの考えのもと、政府と民間が一体となって、それぞれ役割を分担しながら、日々刻々と変化・発展していく技術の動向を見ながら、アジャイルにルール形成をしていく必要があるとの立場をとる。我

が国では、Society5.0を実現することを目標として、2019年からこのような新たなガバナンスモデルの研究と開発に着手し、経済産業省からアジャイルガバナンスの実装に向けた4つの報告書がこれまで公表されている(注11)(そのうち1つは本研究時点でパブリックコメント中)。

そして、最先端テクノロジーの分野では、アジャイルガバナンスの価値観をベースにしたルールメイキングも次々に実施されている。たとえばBig Techによる大規模プラットフォームの透明性や取引の公正性を確保するために制定された「特定デジタルプラットフォームの透明性および公正性の向上に関する法律」、寡占体制にあるモバイルOS分野におけるBig Tech事業者のアプリ開発事業者に対する競争制限的な措置の是正を目指す「スマートフォンにおいて利用される特定ソフトウェアに係る強制促進に関する法律」などは立法レベルでアジャイルガバナンスが実装された例であり、総務省と経済産業省が所管する「AI事業者ガイドライン」やデジタル庁が所管する「データガバナンスガイドライン」などは、急速に発展する生成AIや国境を超えるデータ流通に対し、事業者が新しいパラダイムにどのように適応し、何を規律として活動をしていくべきかをガイドラインとして取りまとめたものである。

ブロックチェーンという革新的な技術をベースに、これまでの伝統的な金融サービスとは異なる技術アーキテクチャのもと、伝統的な金融サービスとは異なる新たな価値を提供するDeFiの規律をどのように定めるかというアジェンダは、まさにこのテクノロジーガバナンスの系譜に連なるものであるといえよう。

金融規制は、IOSCOのようなグローバルな監督者団体がユニラテラルなルールメイキングをしがちな分野であるが、金融規制の体系は決してDeFiにアプローチするための唯一のツールではない。特に、ブロックチェーンを機能させるためのバリデーションの活動やスマートコントラクトを通じたアプリケーションの開発・設置は純粋なコンピュータエンジニアリングの領域であって、金融機関に対して情報システムを提供するベンダーの立場と異ならない。金融当局者は、自らの持つ最新技術やこれを応用するビジネスの最新現場の情報獲得活動には限界があると認め、いずれの領域をテクノロジーガバナンスの規制体系にゆだねるのか、いずれの領域において金融規制が実効性を持つのかということを、民間事業者とディスカッションするオープンな姿勢が求められる。その上で、金融規制が実効性を持つと考えられる領域を定義し、その領域におけるスマートなルールの構築を目指すべきであろう。

なお、DeFiに対するルールの開発に当たっては、以下の点に留意する必要がある。

(a) 同一活動、同一リスク、同一規制の原則の適用に当たっての留意事項

本章で詳述した通り、DeFiとCeFiは、基盤とする技術においてアーキテクチャレベルで異なる。技術アーキテクチャが異なるということは、同じ目的を達成する金融サービスを開発しようとしても、その強みと脆弱性の発現の仕方が全く異なるということである。例えば、オペレーショナルリスク一つをとっても、CeFiはシステムの運用者である金融機関や委託先事業者の担当者が過ちを犯すリスクといった、人間を起点としたリスクの発現形態をとることが多いのに対し、いったんスマートコントラクトを設置すれば自動的に執行されるDeFiにおいては、こうしたリスクは極小である。DeFiにおいては、むしろ正しくDeFiアプリケーションが開発されているのかであるとか、その検証体制が適切であるかであるとか、運用そのものよりも技術開発における適切性の管理が重要である。

このようなリスクが全く異なるDeFiに対して、CeFiの規制体系を機械的にあてはめたり、CeFiの規制体系の改正によって対応したりしようとすると、本当に必要な規制を見過ごし、不要な規制を課してしまうおそれがある。

(b) 内外のイコールフットイング

金融規制は、利用者が国内外にいると否とを問わず国内でサービスを提供する事業者と、国内居住者に対してサービスを提供する外国事業者に適用されると一般に考えられている。他方、ブロックチェーンを活用したDeFiにおいては国境が存在しない。そのため、DeFiに対する金融規制を立案する際には、国内居住者に対してサービスを提供する外国事業者と国内でサービスを提供する事業者とは執行のレベルに至るまで同等の取り扱いがなされなければならない。現状、金融監督においては、国内事業者に対しては立入検査を含め厳格に金融規制の適用がなされているが、国内法に違反する外国事業者に対しては執行力のない警告書を発状するに留まり実効的なサンクションを課すことはなされていない。この現状は、国内からのサービス提供を行わず、海外からサービスを提供することで規制の潜脱を実質的に許容していると評価されるおそれがある。

今後仮にDeFiに関して規制を及ぼす場合、実質的に見て現状のように国内事業者のみが真面目に対応しうるような規制体系となった場合、上記のようなDeFiの特性に鑑みると、現状よりも更に事業者の海外退避を促進することとなることが懸念される。

したがって、仮にDeFi接続の分野において規制を課すということであれば、国際協調も含め、海外事業者に対しても同様の規制が実効的に課されることが担保される規制体系とすることが求められよう。

(c) 我が国のデジタル戦略と整合性をもった規制戦略

我が国には、デジタル時代の到来を踏まえてサイバー・フィジカル空間を一体運用することによって国富を増進するとの明確な国家戦略が存在する。政府はこの国家戦略のもと一丸となって、ガバナンスイノベーションに邁進し、規制のデジタル化、生成AIの活用を促進している。web3もまたそれに連なる形で国家戦略として推進しているところ、web3の重要な要素であるDeFiについても戦略的なルールメイキングが必要である。

統合的なweb3戦略の一環としてDeFiのルールメイキングに取り組むのであれば、金融規制を担当する省庁のみではなく、より広い利害関係者が参加する形で議論が行われる必要がある。したがって、これまでの金融規制の立案手法や過程にとらわれることは必ずしも適切ではないと考えられる。

デジタル規制がどのように構築されるべきか、そのルールメイクの新手法に関する知恵とノウハウは、金融規制当局の外にも蓄積されている。外部に蓄積された知恵とノウハウもフル活用して、DeFiに関する革新的なルールメイキングを実現し、これを世界に発信していくことが、次世代の金融立国のあるべき姿を世界に示していくことにつながるはずである。

(4) DeFiサービスに接続可能なweb3ウォレットに対するあるべき規制の方向性

上述のとおり、DeFiに対するあるべき規制の方向性については、従来の金融規制の枠組みにとらわれることなく、様々な観点から検討を進める必要がある。然れば、そのようなDeFiサービスに接続可能なweb3ウォレットに対する規制についても、現行の法

令上の文言に当てはめうるからと言って拙速に従来の金融規制を適用することのみによって方向性を決定すべきものではないと考えられる。

現在の我が国の暗号資産交換業にかかる規制は、利用者の暗号資産の保管・交換・法定通貨の入出金を垂直統合して引き受ける事業者に対する規制として実施されてきたものであるが、web3ウォレットやDeFiは、そのうち保管機能と交換機能について交換機能を提供する事業者の手から離すことを実現するものであり、そもそもの前提が変容しているといえよう。

かかる変容は、ブロックチェーンを中心とした技術の進展により生じているものであることから、web3ウォレットに対する規制についても、前記(3)で示した観点等を踏まえながら、丁寧に検討していくことが求められる。

(注6) <https://coinpost.jp/?p=597897>

(注7) 国内業者: https://www.fsa.go.jp/policy/virtual_currency/kasoutsukamutouroku.j.pdf

海外業者: https://www.fsa.go.jp/policy/virtual_currency/angoushisanmutouroku.pdf

(注8) <https://coinpost.jp/?p=598575>

(注9) 2020年4月3日付金融庁パブコメ36番参照

(注10) IOSCO「[Final Report with Policy Recommendation for Decentralized Finance \(DeFi\)](#)」参照

(注11) <https://www.meti.go.jp/press/2022/08/20220808001/20220808001.html>

(注12) https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf

(注13) https://www.fsa.go.jp/policy/bgin/ResearchPaper_gunie_ja.pdf

第6章 経済法的視点からのweb3規制枠組みに関する考察

1 web3規制と経済法

web3に関する技術的進化は目まぐるしく、web3を利用した分散型金融(DeFi)や非代替性トークン(NFT)、メタバースに関する取引に関する法規制の整備が喫緊の課題となっている。イノベーションは競争の本質的な要素であることから(注14)、web3技術のイノベーションによる競争の結果として、革新的なサービスが新たに提供され、日本社会全体にその成果が還元されることが期待される(注15)。また、法規制のルールが策定されないために、行政によるケースバイケースの判断に委ねられることにより、web3事業者の競争の機会が実質的に奪われてしまうことのないようにする必要がある(注16)。その上で、実務家や技術者、研究者そして官庁との密な対話を通じたweb3法規制の方向性の議論が行われる必要がある。

web3のグローバル市場は2021年の5兆円から、2027年には約13倍の67兆円に成長し、日本国内のweb3関連市場については、2021年の約0.1兆円から、2027年には、約20倍の約2.4兆円まで成長することが予測されている(注17)。このようにweb3は黎明期にある産業であり、ML/FT(Money Laundering/ Financing of Terrorism)リスクの防止、価格カルテル及び競争者排除の禁止等の市場基盤・市場秩序を維持する法規制を構築した上で、積極過誤(false positive)に陥ることの無いように配慮しながら、事業者のイノベーションを活発に促進することが望ましい。

この点、特にDeFiの分野においては、国内外の金融規制の検討が進展しつつあり、イノベーションを促進しながらも、国際的な金融規制から逸脱したり、諸外国から取り残されたりすることの無いように法規制の在り方を検討する必要がある(注18)。そこで、第6章では、経済法的な視点から、金融規制の現状と課題について考察を行うべく、まず第2節で経済法的視点からのweb3規制枠組みを検討する。そして第3節においてweb3に関する金融規制の現状と課題を明らかにする。

2 経済法的視点からのweb3規制枠組み

経済法上、web3それ自体を直接規制する枠組みは現在のところ存在しない。しかし、web3は異なるネットワーク間における資産の移動又はデータの共有を可能とするものであり、デジタルプラットフォームとして機能する。このため、web3に対しては、デジタルプラットフォーム市場、モバイルエコシステムをはじめとしたデジタル経済分野を規制する法規制の枠組みが適用されうる。

デジタル経済分野を規制する法規制として、具体的には、私的独占、不当な取引制限、不公正な取引方法の3本柱とする①独占禁止法(注19)の他、②取引透明化法(注20)、③スマホソフトウェア競争促進法(注21)が挙げられる。共同規制(あるいはアジャイル・ガバナンス)として位置づけられる②取引透明化法は、として、一定規模(注22)以上の特定デジタルプラットフォーム提供者(注23)に対して、提供条件等を開示することを義務付けており、特定デジタルプラットフォーム提供者は、毎年度、苦情の処理及び紛争の解決に関する事項、提供情報等の開示の状況に関する事項等を記した報告書を経済産業大臣に提出しなければならない(取引透明化法9条)。また、経済産業大臣は、特定デジタルプラットフォーム提供者について特定デジタルプラットフォームの透明性及び公正性を阻害する行

為があり、その事実が独禁法19条の規定に違反していると認めるときは、公取委に対し、同法の規定に従い適当な措置をとるべきことを求めることができる(取引透明化法13条)。

事前規制として位置づけられる②スマホソフトウェア競争促進法は、基本動作ソフトウェア(OS)、アプリストア、ブラウザ、検索エンジン等の特定ソフトウェアを提供する一定規模(注24)以上の指定事業者に対して、自己優遇等の行為を禁止し、違反行為が認められた場合には、排除措置命令及び違反行為に係る商品又は役務の売上額20%の課徴金が課すことができる。

このようにデジタル経済分野における経済法上の規制は、一定規模以上の指定事業者に対する「事前規制」としてのスマホソフトウェア競争促進法、広く一般的に規制が及ぶ「事後規制」としての独禁法、そして自主的に取引の透明性及び公正性の向上に取り組み「共同規制」としての取引透明化法から構成されており、相互に補完する法律となっている。web3もデジタルプラットフォーム市場を構成し、一定規模以上の事業者が該当する場合には上記の法律の規制に服することになる(注25)。

取引透明化法の「共同規制」ないしスマホソフトウェア競争促進法の「事前規制」は、GAMAM(Google, Amazon, Meta, Apple, Microsoft)をはじめとする巨大IT企業が事業活動を行うデジタルプラットフォーム市場およびデジタルエコシステムという新たな経済実態に対応するべく制定されたものである。これらの法律は、諸外国、特にEU、英国の法制度、法執行を念頭に置きながら、従来の日本の法規制にはみられない新たな法体系の規制として導入されたものである。両法の成立過程からもみられるように、新たな経済実態に対する法規制を検討する上で、日本法としての法体系を維持しつつも、諸外国の法規制及び法執行を踏まえながらグローバルな法秩序から隔絶することの無いよう、迅速かつ適切に、法規制を設計する必要があると思われる。その際には、過剰規制(false positive)に陥り、イノベーションを阻害することの無いように、そして、国際的な法規制の動向から取り残されることで国際経済分野における事業活動の妨げにならないよう、留意する必要があると思われる。

黎明期にある我が国web3市場において、取引透明化法やスマホソフトウェア競争促進法に該当するような事業者はまだ見受けられない。しかし、独占的なweb3事業者が現れた場合には、スタートアップ事業者も含めて、競争が活発に行われる上で、経済法は重要な役割を果たすものといえよう。

3 web3に関する金融規制の課題

銀行及び証券会社を金融サービス業者としての仲介者として成立する従来型のTradFiに対してCeFiは、伝統的な金融サービスに加えて、ブロックチェーンネットワークを利用した金融サービスを提供することが可能となっている。

今日web3の技術的な進展とともに、インターオペラビリティとスマートコントラクトを組み合わせたことが可能となっており、特にweb3を構成するweb3ウォレットは、異なるネットワーク間における資産の移動やデータ共有の円滑化が期待されている。web3ウォレットは分散型金融DeFiを支える中核的な存在であり、大手のプラットフォーム事業者も参入が行われている。ホステッドウォレットに関しては暗号資産交換業の登録が必要とされ、この場合、ハッキング等による顧客資産の流出防止の観点からホットウォレットとコールドウォレットを組み合わせた管理が法律上求められている。他方、アンホステッドウォレットに関しては暗号資産交換業の登録は基本的に不要と解されており、アプリ型web3ウォレット事業者については、ユーザの秘密鍵を預からないアンホステッドウォレット形式にてサービ

スを提供しており、利便性の高いホットウォレットの形で提供されている。アンホステッドウォレットに関する暗号資産交換業の登録について、どのような場合に登録が必要であるかに関しては行政官庁のガイドライン、あるいは法規制により整理される必要があると思われる。

特にアンホステッドウォレットに関して「暗号資産交換業」の「媒介」「仲介」に該当し、暗号資産管理事業者として登録が必要なのか否かについて不明確であるという点が課題として残されている。さらに、暗号資産やNFT取引から得られた個人の利益に関して「雑所得」として最高55%の税率が適用されている。web3というアーキテクチャを前提とした新たな市場については、国際的な比較法的な視点も踏まえた上で、我が国のweb3市場が国内外で魅力のある市場となるように法規制を設計する必要がある。

また、セキュリティとプライバシーに関する保護も重要となる。2024年5月にDMMビットコインでは、480億円相当のビットコインが流出し、2025年2月には、Bybitでは、15億ドル(約2250億円)が流出したことが報告されている。ハッキングの手口も巧妙化しており、顧客資産の流出防止のためのセキュリティ向上が急務となっている。個人情報保護の観点からは個人情報保護法との整合性、NFTに関する知的財産権法上の取扱いを明確化する必要がある。

また、アンホステッドウォレット市場を考えた場合、グローバルな市場において独占的なシェアを獲得しつつある海外web3事業者(注26)が現れ始めている。我が国におけるアンホステッドウォレット市場の問題が縦割り行政の狭間に陥ることで法規制のルールが策定されず、行政によるケースバイケースの判断に委ねられないよう留意する必要がある。特に、我が国におけるアンホステッドウォレット市場において法規制のルールが策定されないことにより、国内web3事業者が海外web3事業者とレベルプレイングフィールドに立つことができず、競争の機会を逸するおそれがある。アンホステッドウォレットをはじめとしたweb3技術は急速に進展するものであり、過剰規制(false positive)(行政指導による事実上の過剰規制を含む)がイノベーションを阻害すると同時に、国際的な法規制の動向から逸脱することもまた、国内web3事業者にとって競争の機会を奪うことにつながりかねない。アンホステッドウォレット市場をはじめとしたweb3市場において、国内ユーザがイノベーションと競争の利益を逸することのないようことを注意しなければならない(注27)。

4 終わりに

昨今、web3を利用したDeFi、NFT、メタバースに関する市場は急激に拡大しつつある。イノベーションは競争の本質であり、web3を巡る市場の秩序を維持しつつ、イノベーションを通じて競争を促進する必要がある。その際には、過剰規制によるイノベーションの阻害に留意しつつ、国際的な法規制の動向から取り残されないようにする必要がある。また、国内のweb3事業者のイノベーションと競争を阻害しないよう、web3の法規制の枠組みを構築する必要がある。

経済法では、デジタルプラットフォームとしてのweb3に関して、事前規制としてのスマホソフトウェア競争促進法、共同規制(アジャイルガバナンス)による取引透明化法、そして事後規制として独占禁止法が適用される。経済法に関しては事業活動の規制法という側面だけでなく、競争を促進する側面があることが改めて認識されるべきであろう。特にweb3に関するスタートアップ事業者等が独占的な事業者により不当に排除されたり、事業活動が妨害されたりすることがないよう、経済法を通じてweb3市場の公正かつ自由な競争秩序が維持促進されるべきである。

また、web3に関する金融規制については、従来型のホステッド型ウォレットだけでなく、利便性が高いとされるアンホステッドウォレットが活用されることが期待されるところ、セキュリティとプライバシーの保護が今後ますます重要となってくる。そして、我が国におけるアンホステッドウォレット市場において適切な法規制のルールを実現することにより、国内web3事業者が海外web3事業者との競争の機会が与えられるようにすることで、国内ユーザがイノベーションと競争の利益を享受しうることが期待される。web3に関する金融規制に関しては、産学官が密に連携した上で、実態に即した法規制が実現されるべきである。

(注14) J.A.シュンペーター『経済発展の理論(初版)』192-193頁(日本経済出版、2020)、小田切『イノベーション時代の競争政策』1-3頁(有斐閣、2016)参照。

(注15) ビジネスだけでなく、ヘルスケアや環境といった社会的な課題の解決も期待されている。大植拓真『Web3時代のAI戦略』104-219頁(日経BP、2022)。

(注16) キャス・サンスティーン、エイドリアン・ヴァーミュール『法とリヴァイアサン』41頁(勁草書房、2024)参照。

(注17) A.T.カーニー「Web3があたえるインパクト」4頁(日本経済新聞出版、2021)参照。

(注18) なお、NFTに関する法制についてゲーム産業に焦点をあてて整理したものとして、松本恒雄監修『NFTゲーム・ブロックチェーンゲームの法制』(商事法務、2022)がある。また、メタバースにおける商標との法的問題について取り扱ったものとして、青木博通『インターネット・メタバースと商標の保護』(勁草書房、2024)がある。

(注19) 「私的独占の禁止及び公正取引の確保に関する法律」(昭和22年法律第54号)。

(注20) 「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」(令和2年法律第38号)。

(注21) 「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」(令和6年法律第58号)。2024年6月に成立し、2025年に施行される。

(注22) 取引透明化法4条1項にいう「規模」とは、デジタルプラットフォーム提供者による商品等の提供の事業については、国内売上高4000億円、商品等提供利用者及びデジタルプラットフォーム提供者によるソフトウェアの提供及び権利の販売の事業については、国内売上高2000億円、デジタルプラットフォーム提供者による広告表示する役務の提供に係る国内売上高1000億円、商品等提供利用者による広告表示枠における広告素材を広告として表示する役務の提供に係る国内売上高500億円であるとされている(「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律第四条第一項の事業の区分及び規模を定める政令」(政令第17号))。

(注23) 特定デジタルプラットフォーム提供者として指定されている「総合物販のオンラインモール運営事業者」として、アマゾンジャパン合同会社、楽天グループ株式会社、LINEヤフー株式会社、「アプリストア運営事業者」として、Apple Inc.及びiTunes株式会社、Google LLC、「広告仲介型デジタルプラットフォームの運営事業者」として、Google LLCがそれぞれ指定されている。

(注24) スマートソフトウェア競争法3条1項にいう「規模」とは、国内向けに提供されている「基本動作ソフトウェア」、「アプリストア」、「ブラウザ」、「検索エンジン」をそれぞれ月1回以上利用するスマートフォンの利用者数の平均が4000万人であるとされている(「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律第三条第一項の事業の規模を定める政令」(政令第376号))。

(注25) この他、公取委は、生成AIに関する報告書(公取委「生成AIを巡る競争」(令和6年10月2日))を出しており、実態調査を始めている。また、フィンテックに関しても

実態調査(公取委「家計簿サービス等に関する実態調査報告書」(令和2年4月21日)、公取委「QR コード等を用いたキャッシュレス決済に関する実態調査報告書」(令和2年4月21日)公取委「フィンテックを活用したサービスに関するフォローアップ調査報告書」(令和5年3月1日))を行っている。

(注26)例えば、イーサリアムチェーンを基盤にした暗号資産のウォレットであるMetaMaskやビットコイン、イーサリアム等の暗号資産のウォレットであるTrust Wallet等が有力なWebウォレットとして挙げられる。

(注27)デジタル経済のAI及び基盤モデルを巡る市場の規制の文脈において、適切な介入の必要を説くものとして、Ariel Ezrachi「介入すべきか否か、それが問題だ」日本経済法学会年報45号82-83頁(2024)がある。

以上