

仮想通貨およびVASPに対するリスクベースのアプローチのための ガイダンス更新案に対する日本暗号資産ビジネス協会のコメント

第1 日本暗号資産ビジネス協会について

日本暗号資産ビジネス協会（以下、「当協会」という。）は、暗号資産に関連するビジネスに従事する事業者及びビジネス参入を検討する事業者が、人的ネットワークを形成し、それぞれの専門領域の知見を持ち寄り、お互いに高めていくためのプラットフォームである。当協会は、来るべき自立・分散型の協調社会における社会基盤となることが期待されるブロックチェーン、とりわけその原動力となる暗号資産の可能性を拓く礎となり、暗号資産交換業又は暗号資産若しくはその他のブロックチェーン上のデジタル資産に関するビジネスに対する社会の理解を深め、暗号資産関連ビジネスに対して関心を抱く者及び団体への教育環境を提供し、日本における暗号資産ビジネスの持続的な発展を期することを目的とする。当協会の会員数は100社であり、多数のVASPのほか、銀行、証券会社、通信事業者、システム会社、法律事務所、監査法人、インターネットメディア等、多くの関連事業者が会員となっている。当協会は2016年に設立された一般社団法人であり、継続的に暗号資産ビジネスに関する勉強会を開催しているほか、仮想通貨及びVASPに関する日本の法制に関して多くの提言を行ってきた。

当協会は、AML/CFTへの効果的な取り組みによる暗号資産ビジネスの健全化を支持しており、FATFが公表したDraft updated Guidance for a risk-based approach to virtual assets and VASPsについて、意見を提出する機会が与えられたことに感謝する。当協会による意見は以下のとおりである。

第2 ガイダンス全体に対する意見

1. Virtual Asset の意義

Virtual Asset (VA) は、これまでの金融商品と異なるデジタルな価値であり、送金や交換を含め、あらゆる取引をP2Pで行うことができるという革新的な性質である。

このようなVAの登場によって、これまでは金融機関を通じてしか金融サービスにアクセスできなかった個人が、P2P取引を通じてダイレクトに金融サービスにアクセスをすることができるようになった。金融機関の運営に必要な様々なコストが個人に転嫁されなくなるため、個人はより低いコストで送金、交換、融資といった金融サービスを利用することができる。

これにより、銀行口座を持たない人たちが金融サービスを享受できるという金融包摂¹の観点から有益であるだけでなく、銀行口座を保有している個人にも、コストの低い効率的な金融サービスという大きな利益をもたらすことになる。

2. 規制の民主的正統性について

VAに対してその特性に沿った規制が必要であることはVA業界においても基本的に賛同している。もっとも、AML/CFTという目的だけでなくあらゆる規制が正統化されるわけではな

¹ 2010年にソウルで開催されたG20サミットの首脳宣言では、金融包摂が世界的なアジェンダの主要な柱として認識され、具体的な金融包摂行動計画も承認された (<http://www.g20.utoronto.ca/2010/g20seoul.pdf>)。

い。

ごく一般的に言えば、規制を正統化するためには、手続の適切性に加え、規制内容の合理性も必要であると考ええる。

手続的の適切性の観点からは、規制導入プロセスにおいて根拠となるデータが示された上で、民主的に利害関係者の意見が反映されるプロセスが必要であることが求められる。また、規制内容の合理性の観点からは、規制目的が正当であることに加えて、規制目的を達成するための手段が合理的であるかどうか、権利や自由の制約によって失われる利益と得られる利益の比較衡量が適切に行われているかどうかを慎重に検討する必要がある。

特に、VA 及び P2P 取引に対する規制は、金融機関に対する業規制を超えて、利用者個人の財産権やプライバシー権を制約するという側面を強く持っていることに留意すべきである。例えば、利用者個人が VA を保有する場合、これを VASP から引き出すことは当該利用者の権利であって、禁止することは当該利用者の財産的権利を直接に制約することになる。当該利用者に犯罪に関わる疑惑などがあれば、現金の引き出し同様に制限されることはあるであろうが、そうした合理的理由なしに当該利用者の権利を制約することはできないと考えられる。また、P2P 取引を可視化しようとする試みは、個人の資金使途を通じた私生活上のプライバシーや、適法なデモや取材・報道などの表現の自由に関する活動に係る資金移動に対してまでも政府から干渉されるおそれの高い行為であり、単に P2P 取引を行ったというだけで干渉することは許容されるべきではない。

このように、個人の権利や自由を制約する規制を導入する場合、本来は、各加盟国の法体系において、どのような規制が許容されるかなどの観点から、選挙で選ばれた代表者による民主的な議論が必要である。しかしながら、FATF において合意が確定した場合、当該合意は条約ではないにもかかわらず、mutual evaluation の仕組みを通じて、国際的な金融ネットワークに参加し続けるために合意に沿った規制を導入せざるを得ず、各国の立法機関における議論の余地がほぼなくなってしまう。このため、FATF において合意を確定させる前に民主的正統性を確保することが必要であると考ええる。

3. 規制導入プロセスの適切性

規制導入プロセスに関して、FATF は、PSCF という民間の意見を聴く場を設けることがある。トラベルルールを導入については 2019 年 5 月 6 日に議論が行われた。当日の議論においては、伝統的な金融機関に対しては有効でも、VA に対しては必ずしも効果的な規制ではないなどの理由で規制案に反対する声も多く上がった。一部の参加者からは「技術的には可能」という意見もあったが、「技術的に可能」であることは規制が合理的であることを裏付けるものではない。結果的に、トラベルルールについては同年 6 月にほぼ原案どおりの形で確定したが、PSCF での議論を踏まえて、FATF においてどのような検討が行われたのかについては明らかにされていない。

このように、FATF の規制はこれまで当局間のクローズドな会合で決められてきており、開示は非常に限定的である。PSCF での議事内容が公開されることはなく、Public consultation が行われても、提出された意見の内容やそれに対する FATF の回答が公開されることもない。このような手続は民主的であるとは言えないのではないか。

今回のガイダンス改訂については、その確定前に、この Public consultation で提出された意見の内容及びそれに対する FATF の見解の公表、VASP を含めた関係者から意見を聴くための Private Sector Consultative Forum の開催とその議事録並びに PSCF の内容を踏まえた FATF における再検討結果の公表を行うことを強く要望する。これらに加えて、民間の代表者らで構成されるワーキンググループを FATF 内に設置し、ドラフト策定段階から当該ワー

キンググループの意見を反映させるなど、継続的に民間の意見を反映させるための仕組みの構築を行うことを要望する。

4. 規制には明確性が必要であること

FATF 勧告をもとに各法域が立法する場合、VASP となるためにはライセンスや登録が必要となる。仮にライセンスなしに VASP として活動した場合、行政処分を受けるだけでなく、刑罰規程の対象となることが想定される。

そうであれば、FATF 勧告やガイダンスの要件は明確でなければならない。不明確なガイダンスを確定させることは、各法域に不明確な刑罰法規を導入させることにつながるおそれが高い。これはイノベーションを委縮させるだけでなく、不明確な刑罰法規の適用による人権侵害につながりうるものである。日本においても、刑罰法規の明確性は憲法上の要請として求められるが、これは FATF に加盟する多くの国における憲法上の要請でもあると考えられる。

5. 過剰な規制は意図しない結果をもたらすこと

上記 2. の観点から正統化できない規制が導入された場合、結果として、次々と生まれる新技術に対する実効性が乏しい内容となるおそれが高い。その結果、マネロン対策において鍵となる、規制に準拠しようとする健全な VASP の体力を不合理に疲弊・弱体化させることになりかねない。さらに、規制に準拠しようとしめない VASP が規制の緩い国に流れてしまい、結果として法執行機関による捜査や取引の追跡が困難になるおそれがある。

6. 規制当局側にも Reg Tech の推進など効率化が必要であること

暗号資産のトランザクションはパブリックなブロックチェーンに記録されるため、透明性がある一方で、トランザクション実行者の特定においては、KYC を実行している VASP が重要な役割を持つと考えられる。法執行機関からの VASP に対する照会は、暗号資産のトランザクションが公開されていることから、将来的には伝統的金融機関に対するもの以上に増えていく可能性がある。しかしながら、これらの照会対応は、上述の通り捜査の過程で重要な役割を担う規制に準拠した VASP に、多大なコストをかけさせ、弱体化させることに繋がる。現在の問題点として、同じ法域内でも地域ごとに存在する法執行機関から、フォーマットや方法の異なる照会が多数なされており、VASP 側の対応コストが増加している。また、旧来型の紙での照会がなされることや、WEB 報告システムがあっても使い勝手が悪く効率的ではないことなどにより、本来の捜査のための調査以外のところで VASP に多大な時間を割かせる法域がある。FATF は、VASP に対して捜査協力のためのリソース確保を求めるだけでなく、VASP が無駄なリソースを割かなくて済むよう、各法域が捜査機関に対し効率的な照会方法を求めることも検討し、見直しと改善を促すべきである（例えば、照会フォーマットの統一や、報告システムの改善、地域ごとの照会を集約する仕組みの導入など）。これにより、VASP による照会への回答もスムーズなものとなり、AML/CFT の観点からも効率性が上昇するはずである。

第 3 各パラグラフについての意見

1. パラグラフ 13 及びパラグラフ 22 について

日本を含めたいくつかの国は、FATF 勧告に従い VASP に対する厳格な規制制度を導入済みであるが、そうでない法域も多い。そして、租税制度におけるタックス・ヘイブンの存在と同様に、そのような法域における VASP が規制のセキュリティホールになっていることは

明らかである。そうした法域があり続ける限り、導入済みの国に対して規制強化を求めることは、規制に準拠する VASP の競争力が低下し、規制に準拠しない VASP がより多くの利益を得るという意図しない結果をもたらすことになるおそれが高い。したがって、現状において優先してリソースを割くべきなのは、既に導入済みの国に対して規制の更なる厳格化を求めることではなく、規制未導入の国に対して規制の導入を強く働きかけることであると考え。このことは、パラグラフ 22c)において各国に対して求められている Level Playing Field の実現のためにも必須であると考え。

2. パラグラフ 16 について

中央銀行発行のデジタル通貨は一律適用除外とされているが、FATF 非加盟国におけるデジタル通貨の取り扱いや、中央銀行による任意のデジタル形式のアセット発行の可能性を考慮すべきである。中央銀行が発行するものであっても、VA と全く同等のことが行われる場合には、パラグラフ 22.c)の Level-playing field の観点からも VA と同様に取り扱われるべきと考える。

3. パラグラフ 19 について

パラグラフ 19 では、「Virtual Assets Red Flag Indicators of ML/TF」を引用して、より広範な犯罪行為のために VA がますます主流になっているとしている。しかし、同報告書には統計データは載っておらず、また例として出されているものに対しても金額を書いていないものもあり、同報告書から犯罪行為のために VA が主流になっているエビデンスは見取れない。むしろ、近時公表された元 CIA の Director of Intelligence によるレポートは、様々な根拠を示したうえで、ビットコインが違法な金融取引に利用されているという一般的な議論は著しく誇張されていることを指摘している²。また、代表的なブロックチェーン分析企業である Chainalysis の近時のレポートは、仮想資産を利用した犯罪行為は減少傾向にあり、2020 年に行われた仮想資産の取引全体のうち 0.34%のみが犯罪に関わるものであったと指摘している³。SWIFT が BAE システムズに依頼して作成された 2020 年 9 月のレポートにおいても、仮想資産を使ったロンダリングが確認されているケースは、従来の方法でロンダリングされた現金の量に比べて、比較的小さいと指摘している⁴。

本ガイダンスは FATF 内で何らかのデータ及び判断基準に基づいて書かれているはずであるため、それらの統計データを公開し、リンク等で示すべきである。

4. パラグラフ 21 及びパラグラフ 28 について

「金融機関がリスクベース・アプローチを適切に適用し、適切に目標を絞ったリスクアセスメントをすることなく、VASP セクター内の顧客関係を一律に打ち切ったり排除したりしないことが重要である」とある。しかしながら、実際には銀行による de-risking によって、銀行と VASP との取引関係はこのガイダンスからは程遠い状態にある。加盟各国において、実態調査と積極的な改善措置をとることが必要と考える。

5. パラグラフ 31 及び 155、167 について

² Michael Morell “An Analysis of Bitcoin’s Use in Illicit Finance” Crypto Council for Innovation, April 6,2021,

https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf

³ “The 2021 Crypto Crime Report” Chainalysis, February 16, 2021, <https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets>

⁴ “New Report Reveals How Cyber Attackers ‘Cash out’ Following Large-Scale Heists.” BAE Systems, September 2, 2020, <https://www.baesystems.com/en-financialservices/insights/news/report-reveals-how-cyber-attackers-cash-out-following-heists>

匿名性の高い取引を促進する VA やサービスがより高い ML/TF リスクをもたらすことが指摘されているが、他方でプライバシー保護の要請が高まっており、金融取引においても匿名化への対応が社会的に求められることが予想される。消費者がプライバシーを守りたい場合、現金取引を行うことは可能であるが、VA についてのみ一切、匿名取引が認められないとすることはバランスを失するようと思われる。

こうした匿名化された金融サービスにおいては、取引開始時の KYC や KYC に基づくリスク評価は可能である。しかし、個々の取引については取引内容の一部が匿名化されるため、サービス提供事業者であっても、トラベルルールの実施が困難なことも考えられる。

したがって、あらゆる取引にトラベルルールを適用すべきではない。匿名サービスを提供する場合にも、VASP におけるリスク低減措置として、例えば匿名取引が可能な金額に制限を設けることや、サービス全体における包括的なブラックアドレスのフィルタリングなどの手段をとることも可能と考えられる。そのようなリスク低減措置ができていない場合には、一定範囲においてトラベルルールの例外とすることが必要と考える。パラグラフ 167 では 1000 米ドル/ユーロ未満の取引についてもトラベルルールの実施を求めているが、他のリスク低減措置が取られている場合にはトラベルルールの実施を必須とすべきではないと考える。

6. パラグラフ 35 及び 36 について

パラグラフ 34 で確認されているように、FATF 勧告は個人と金融システムの間の中介者に義務を課すものであって、現金や VA の P2P 取引に適用されるものではない。

もともと VA は現金同様、P2P 取引を想定したものであるから、顧客が VA を用いて P2P 取引を行ったとしても、それだけで疑わしいと判断することはできない。現金の使用と同様に、例えば不自然に多額の取引や、多数回の取引がなされている場合に限定してリスクが高いものと評価すべきと考える。

パラグラフ 35 の最後の一文について、VASP が関与しない P2P 取引に対しても「ブロックチェーン分析によって P2P 取引の可視性を高める」ことを VASP に求める趣旨であれば過度な求めであり、プライバシー保護の観点からも顧客の私生活上の支払等に干渉することは問題であると考えられる。

なお、VA の設計や開発の段階で ML/TF リスクを考慮する必要があるとの指摘もあるが、開発行為自体は VASP の定義に該当しないため、このガイダンスの対象範囲外と思われる。VA の設計や開発に関する標準をどのように定めるかについては、実際に VA の設計を行っている複数の参加者を含めて、例えば ISO などを中心に議論をすべきと考える。

7. パラグラフ 38 について

FATF は VA を「a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes」と定義している。しかしながら、どのような digital representation であっても投資対象とすることは可能であるため、この定義では全てのデジタル形式のデータが VA に該当しうることになり、実効性がない。VA に該当する要件をより明確にすべきである。

8. パラグラフ 42 及び 78 について

パラグラフ 78 において、「certain virtual items」も VA の定義に含まれることが示唆されているが、以下の特徴を有する Non Fungible Token (“NFT”)は FATF の目的である AML/CFT の観点からリスクが低いと考えられることから、VA に該当しないことを明確にすべきである。

①取引履歴がブロックチェーン上に履歴が残ること

- ②1つ1つが唯一性を持つこと（容易に特定が可能であること）
- ③一般的に発行数が有限で、大量購入/大量売却が難しいこと

9. パラグラフ 54 及び 55 について

このガイダンスによると、VASP からの委託を受けてマルチシグネチャの一部の署名を代行するサービスを提供する事業者も、VASP に該当しかねない。しかしながら、VASP としてはセキュリティの向上など、有意義な目的のためにこうした事業者に委託を行うものである。また、委託元となる VASP が VASP に求められる対策を実施することができ、委託契約に基づき委託先を管理することもできる。こうした委託先事業者まで VASP に該当させることは過剰な規制であり、委託元の VASP を適切に規制することによってリスク低減を図るべきであると考えられる。

10. パラグラフ 55 について

パラグラフ 55 によると、あるサービスプロバイダーがマルチシグの秘密鍵を一部でも管理していれば、取引を行うために他者が保有する秘密鍵を必要とする場合でも、当該サービスプロバイダーが VASP に該当することになる。

これによれば、例えばユーザーが自力で回復不能な場合にのみ署名を提供する Decentralized Digital Identity のサービス提供者までもが一律にカストディアンとみなされることとなり、イノベーションを著しく阻害する結果となる。

VASP の定義はパラグラフ 47 記載のとおりであり、”Safekeeping and/or administration of virtual assets”という文言の枠内で解釈されるべきである。例えば、仮想資産を移転できるのは 2 of 3 のマルチシグであれば 2 本以上の秘密鍵を保有している者であるから、その者が他人のために当該秘密鍵を管理しているのであれば VASP に該当する。これに対し、1 本だけの秘密鍵を保有している者は VASP には該当しないことになる。パラグラフ 55 に従うと、顧客が単独で仮想資産を移転できる場合にも、一部の秘密鍵を保有していれば VASP に該当することになるが、当該業者の意思とは無関係に仮想資産が動いてしまうのであれば”Safekeeping” や”administration”に該当しないことは明らかである。パラグラフ 55 の原文は、定義の拡張解釈を超えて、定義の書き換えになっているため、修正すべきである。

なお、ガイダンス案の定義に従うと、全てのブロックは採掘者（miners）の保有する鍵による署名を必要とするために採掘者も VASP に該当してしまい、採掘者は VASP に該当しないという整理と不整合となる。鍵を必要とするかどうかでなく、当該トランザクションの形式など、技術的な仕様の指定によってカストディアンかどうかを定義するべきである。

11. パラグラフ 55、57-60、62、64、65、69、72、75、91、178 について

これらのパラグラフにおいて、「facilitate」という用語によって、規制対象が曖昧なまま拡張されている。「facilitate」というだけで VASP に該当するというのはあまりにも広範かつ曖昧過ぎる。FATF の Glossary でも facilitate という用語は定義されていないため、この用語は削除すべきと考える。「補助的な役割」である場合には VASP に該当しないとのガイダンスもあり、整合性が取れていないように思われる。

12. パラグラフ 56-57 について

(1) パラグラフ 57 によると、DApp の所有者／運営者が、顧客に代わって業として VA の交換または移転を行っているため、VASP の定義に該当する可能性があるとのことである。しかしながら、DApp の所有者／運営者という概念が不明確である。何を指して「所有」「運

営」というのか不明である場合、DAppに関わる全ての者がVASPに該当するということになりかねない。また、スマートコントラクトは誰でもパブリックブロックチェーン上に展開することができ、その後は誰でも利用可能となるため、全ての者をVASPに該当するということに実効性もない。

分散化されたアプリケーションであるDAppによって実行される個々のトランザクションは、ブロックチェーン上に展開されたスマートコントラクトを通じて実行されるものであり、DAppの「所有者／運営者」なるものが顧客に代わって又は顧客のために取引を行うものではない。これらの取引は、unhosted walletsを利用した個人間のVAの移転取引と同じように、P2P取引と位置付けられるものであり、金融規制の対象となる仲介機関は存在しない。パラグラフ34では、P2P取引はFATF勧告の対象ではないとされており、これと同様の整理となるものと考えられる。

(2) DAppが、たとえばイーサリアムネットワーク上のスマートコントラクトとして構築されている場合、当該DAppは基本的に改変できないコンピュータプログラムであり、イーサリアムネットワークが動き続ける限り自動で稼働し続ける。したがって、「運営」という概念は当てはまらない。また、DAppは通常、誰でもソースコードを見ることができ、コピーが可能であるため、「所有」という概念も当てはまらないものと考えられる。

(3) ガイダンス案にあるように、DAppにおいても、開発者等がDAppについて一定のadministrative keyを保有する場合はある。このようなadministrative keyの保持は、スマートコントラクトに重大なバグの存在が判明した際にバグを修正するために必要なものである。いかなるソフトウェアの開発においてもバグの発生を完全には防げないことは明らかであり、ソフトウェアリリース後のバグの修正は、開発者にとって必須の作業である。バグの修正等のために必要な範囲でのadministrative keyの保持をすることも開発行為の一環であり、そのみをもってVASPに該当するということとはできない。これは、administrative keyがDAppの機能のバージョンアップのために保有される場合についても同様である。これらの行為はソフトウェア開発の一環であり、顧客に代わって又は顧客のためにVAの取引を行っているわけではない。したがって、パラグラフ68にあるとおり、VASPの定義に該当しない。

これに対して、たとえばadministrative keyでユーザーの資産にアクセスすることが可能であるような場合や、個々の取引の成否に介入できるような場合には、VASPの定義に該当する可能性があると思われる。

以上を踏まえると、administrative key保有者がVASPに該当するかどうかについては、administrative keyの権限の内容、権限行使のための条件や権限行使の頻度等を総合的に考慮して、顧客のために又は顧客に代わって業としてVAの交換または移転を行っているかどうかを基準に判断すべきである。

(4) また、DAppの利用に関してユーザーが支払う手数料の一部が特定のアドレスに送金されることになったとしても、その事実のみで送金先のアドレスの所有者が当該ユーザーのために取引を行ったことにはならない。例えば、当該アドレスの所有者がDAppに関し何ら特別な権限を持っておらず、当該取引の成否に一切関与していない場合、VASPの定義に該当するとは言えない。手数料等の利益が生じていることは、当該手数料の受領者がDAppに何らかの関与をしていることを推測させる事実にはなるであろうが、そのみをもって受領者がVASPだということとはできないことは明確にすべきである。

(5) 上記の観点から、開発行為を超えて DApp に関与する一定の者が VASP に該当する場合であっても、DApp のサービスに関わるのは非常にコンパクトな組織または個人であることが想定される。そうしたあらゆる自然人または法人を予め把握したうえで規制することは現実的に困難であり、イノベーションや金融包摂の阻害となることが懸念される。これに対して、DApp の規模が大きくなること自体は捕捉が可能であり、その関与者が VASP に該当する場合には、その規模に応じた規制を敷くべきである。

また、仮に DApp に関与する事業者が VASP に該当する場合であっても、VASP と KYC プロバイダを分離することが許容されるべきである。これにより、DApp のコントラクト内で KYC プロバイダのコントラクトを呼び出し、フィルタリングやモニタリングを KYC プロバイダに委託することが可能となり、規制の実効性や実施効率の向上が期待できる。この場合、VASP に該当する者が KYC プロバイダにフィルタリング及びモニタリング業務やトラベルルール対応業務を委託し、これらの業務を KYC プロバイダ側で実施することとなる。

1 3. パラグラフ 58 について

58 b)において、“issuance”という単語があるが、仮想通貨の発行自体は exchange や transfer には該当しない。例えば、Bitcoin のマイニングを行った者や、Bitcoin をハードフォークさせて Bitcoin 保有者にフォークしたコインを付与した者は、“issuance”には関わっているが、顧客に代わって業として VA の交換または移転を行ったとはいえない。いかなる場合に VA の発行に関するサービスが VASP に該当するのかを明確にすべきである。

1 4. パラグラフ 62 について

“Providing the functions outlined in the definition should be the determining factor rather than a categorization as a lawyer.”とあるが、前記のとおり VASP に該当するか否かは加盟国の刑罰法規の適用の有無を決定する基準となることから、法律解釈としてとらえるべきである。このようなガイダンスは、「法の支配」を破壊し、恣意的な解釈を許す結果になるため、適切でない。

また、VASP の定義に“helps/promotes”という文言はなく、“any provider that helps/promotes customers hold or use their VAs”を VASP に該当するというのは拡張解釈を超えた定義の書き換えである。

1 5. パラグラフ 63-64 について

パラグラフ 63 によると、VASP の定義に自分が当事者ではないスマートコントラクトを管理する者が含まれる可能性がある。しかしながら、「スマートコントラクトの管理」という概念が曖昧であり、国ごとに異なる恣意的な運用がなされる懸念がある。

通常スマートコントラクトには、ソフトウェアとして役務提供するスマートコントラクトと、当該コントラクトにアクセスするための入り口としての proxy contract と呼ばれるコントラクトが存在する。このように二重構造として設計、展開される理由は、万が一、コードにバグが発生したなどの際にプロキシコントラクトから後ろのスマートコントラクトを切り離すなどの、緊急対応を可能とするためである。したがって、開発者が proxy contract の更新権限すら放棄した場合、利用者に著しく悪影響となるだけでなく、こうしたスマートコントラクトが放置されることで悪意を持ち資金洗浄などに用いられる可能性が結果として高まることも懸念される。このようなエマージェンシーに対応するため、後続のスマートコントラクトを切り離す処置などの適切な管理権限を持ったスマートコントラクトを開発することこそが安全性に直結するものであると思料する。また、こうしたスマートコントラ

クトへの一定の権限付与という事実のみによって、当該権限を有する者を VASP に該当すると解釈することは適切ではないと考える。

1 6. パラグラフ 64 及び 65 について

これらのガイダンスによると、企業が独自パブリックブロックチェーンを開発する行為も「発行者による暗号資産の提供・販売に関連する金融サービスへの参加・提供」として VASP とみなされる可能性がある。しかしながら、「参加」の定義がなく、規制対象が曖昧かつ広範である。また、「facilitate」という VASP の定義に存在しない用語も使われており、より曖昧に規制対象が拡張されている。規制対象を明確化する必要があることについては前述のとおりである。

現実的にも、どのような企業体であれ、パブリックブロックチェーンの利用者を全て捕捉することは困難と思われる。また過剰な規制はイノベーション及び金融包摂の阻害につながる。パラグラフ 68 において明示されているように、ブロックチェーン自体の開発者については、それが VA の発行に関わるものとしても、VASP の定義から除外すべきである。そのうえで、仮想資産の販売や交換（いわゆる ICO）を広く大衆に対して行う主体についてのみ、VASP 該当性を肯定すれば足りると思われる。

1 7. パラグラフ 74 について

「VASP かどうかを機能に基づいて決定する」とあるが、unhosted wallets が VASP に該当しないとされているように、ソフトウェアの開発行為は P2P での取引を可能にするものであっても VASP には該当しないと考えられる。「交換、転送、保管、管理、制御及び発行に至らないものだけが VASP ではない」という記述はこうした整理と矛盾するため、修正が必要と考える。

1 8. パラグラフ 75 について

このパラグラフによれば、現在運用されているほとんどの仕組みは、たとえ P2P プラットフォームに分類されるものであっても、製品の開発と発売のいずれかの段階で、その製品に関与する一部の当事者が存在する可能性があり、当該当事者は VASP に該当することになる。しかしながら、ソフトウェアの開発や販売行為自体のみを行う主体は VASP には該当しないのであるから、上記は過剰な拡大解釈であり、修正が必要と考える。

また、「検索サービス」が取引に介在しなくても VASP に該当するとされているが、「検索サービス」がどのような要件を満たした場合に VASP に該当するのかを明確にすべきである。

1 9. パラグラフ 91 全体について

パラグラフ 91 は、VASP 間の取引と P2P 取引の分断を推進する内容となっている。このような分断には、例えば①金融包摂を阻害する、②P2P 取引のコア部分の開発コミュニティの開発・運用に VA のセキュリティは依存しており、産業としてのセキュリティが不安定になるリスクがある、③ユーザー個人の権利を著しく制約すること等の負の側面がある。

他方で、2020 年 6 月の FATF 文書「12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS/VASPS」において、「2019 年 6 月以降、匿名の peer-to-peer 取引の数と金額が、実質的に異なる ML/TF リスクを提示するほど変化したことを示す証拠は不十分でした。」「さらなる検討が必要である」とされている。同月の FATF 文書「FATF Report to G20 on So-called Stablecoins」では、so-called stablecoin に関して、mass-adopted され

たと仮定した場合には ML/TF の重大な脆弱性を提起するとしているが、他方で、改正 FATF 基準は現金取引と同様に一定レベルでは匿名性のある決済についてのリスク許容度を有しているとされている。2020 年 9 月の FATF 文書「VIRTUAL ASSETS RED FLAG INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING」においては、P2P 取引について何も触れていない。これらのレポートの公表後、どのような検討が行われて認識が変化したかについて公開されるべきと考える。また、何らかの統計的推測値を内部で持っている場合はそちらも公開されるべきと考える。

20. パラグラフ 91a)について

VASP が通貨取引報告書(Currency Transaction Report: CTR)を当局に提出することに関する記載がある。従来の法定通貨の取引においては、法執行機関は法定通貨の当該トランザクションについての情報は CTR で提示されるか自ら照会しない限り知り得ないが、暗号資産のトランザクションはパブリックなブロックチェーンに記録されるため、法執行機関は CTR のような報告がなくとも確認できる状況にある。前述の元 CIA の Director によるレポートは、仮想資産のブロックチェーンを分析することは非常に効果的な犯罪対策と情報収集のためのツールとなるにもかかわらず、法執行機関などに十分に活用されていないことが指摘している⁵。当局は、このような仮想資産の特性を踏まえて Reg Tech を推進するなど効率化を図ることが望まれる。

21. パラグラフ 91c)について

Unhosted wallets を利用する者との取引制限は、ユーザーの権利を著しく制約するものであり、また金融包摂を著しく阻害する。ML/FT リスクの低減という目的を考慮しても、失われる権利・利益との均衡を失っており、過剰な規制であると考え。VASP からの VA 流出等の損害を避けたい利用者は unhosted wallets を使用するという正当なインセンティブがあり、単に unhosted wallets を使用しているというだけで取引から排除する必要性はないと考える。

22. パラグラフ 122 について

パラグラフ 122 によると、アルゴリズム型を含めたステーブルコインについて、その公開前に VASP 同等のライセンス又は登録制による規制を行うべきとされている。しかしながら、アルゴリズムの開発がいかなる理由で、どの時点で VASP に該当するかは明らかではない。パラグラフ 68 において、ソフトウェアの開発自体は規制対象ではないと明示されているとおり、アルゴリズムミックステーブルコインの開発者個人は、仮想資産を顧客に代わって又は顧客のために交換したり、管理したりしない限り、VASP には該当しないことを明確にすべきである。

23. パラグラフ 135 について

冒頭において、「前述のとおり、VA は、犯罪者、マネーロンダラー、テロリストの資金提供者、その他の不正行為者により悪用されやすい特定の特徴を有しています。」とあるが、どのパラグラフを引用しているのか不明である。いずれにしても、どのような検討が行われてそのような認識に至ったか、明らかにされるべきである。

2020 年の BBC 等による報道 (<https://www.bbc.com/news/uk-54226107>) では、リークされたごく一部の文書だけみても、VASP 以外の金融機関を通じて VA 全体の時価総額にも匹敵す

⁵ Michael Morell・前掲注 2 参照

る約2兆ドルの疑わしい取引が行われたことが明らかになった。これらと比較せずに、VAを特に悪用されやすいと言えるかについては再検討が必要である。

24. パラグラフ 152 以下について

VASP に対して、ガイダンスに記載されている内容のトラベルルールの実施を直ちに要求することの合理性については、以下のとおり疑問がある。

まず、トラベルルールのうち、VASP が一定額以上の仮想資産送金にあたって送金人・受取人の情報を取得することについては、基本的に合理的な内容であると考えられる。この場合、自己の顧客については正確な情報を取得できるが、自己の顧客以外の情報については、自己の顧客から申告ベースで情報を取得することになる。現状、VASP においては、自己の顧客の情報のみを取得している場合が多いため、送金先又は送金元の情報を取得することにより、AML/CFT の観点からは大きく前進することになる。また、送金先又は送金元の情報の取得については、顧客との間の契約改訂やシステム更改は必要であるものの、他の VASP と個人データを共有する必要がないため、比較的早期に対応することが可能である。

これに対して、トラベルルールのうち、取得した個人データを他の VASP と共有する部分については、①共有する情報のデータフォーマットを統一する必要があること、②安全かつ効率的な共通の通信手段が確保されていないこと、③送金先の VASP において個人データが適切に保護されるかどうかの確認が難しいこと、④各国の個人データ保護に関する規制要件を満たす必要があることなどの課題がある。これらの課題をクリアするためには、各国における制度整備や、各国 VASP が使用に合意する共通ルールや共通システムの開発など、時間的・経済的コストを要することは明らかである。

また、各国の VASP が適切な AML/CFT に係る措置をとっている場合、VASP 間での VA 送金のリスクは、VASP 以外との間の送金よりも低いとすることができる。しかしながら、VASP 以外を相手方とする取引において、相手方と個人データを共有することは困難であり、このガイダンス案でも求められていない（パラグラフ 180）。これは、リスクベース・アプローチに逆行する内容である。これに加え、個人データ共有のために必要となる時間及びコスト、個人データの漏洩等のリスクも加味すると、VASP 間での個人データの共有を現時点で一律に求めることの合理性には疑問がある。当局でも民間でもリソースは有限であり、効率的な対策が求められることからすれば、まずは送金先及び送金元の情報の取得及びその情報を用いたスクリーニングの実施など、効果的と考えられる規制を早期に実現することが望ましいのではないかと。

25. パラグラフ 156 について

パラグラフ 156 では、すべての VA 送金をクロスボーダー電信送金として扱うべきとされている。しかしながら、VA 送金を行う場合に、送金先が同じ国内の VASP であることが特定されている場合には、国内電信送金として扱うべきであることは明らかである。同一国内で行われる VA 送金であると特定されている場合には国内電信送金として扱うべき旨をガイダンスに明記すべきと考える。

26. Box4 及びパラグラフ 158 から 160 について

送金人及び受取人の名前、住所、国民識別番号、顧客識別番号又は生年月日及び出生地などは個人情報であり、その移転には各国における個人情報保護規制が適用される。トラベルルールを実施するためには、各国において個人情報の移転に関する統一的な法規制が導入されることが必要である。

27. パラグラフ 167 について

パラグラフ 167 では、1000 ドル未満の VA 移転であっても①送金人、受取人の名前及び②wallet アドレスを収集するべきとされている。

現在、日常生活の現金のやりとりについてはプライバシーが保たれているが、現金の使用は減少する傾向にある。これにより個人のプライバシーは限定されつつある。現状、電子的な通貨の中で実際にプライバシーが保たれていると市民が確信できる可能性のある技術はオープンソースで開発運用されている暗号通貨のみである。さらに self-sovereign な暗号通貨は TCP/IP のようなインターネットの基礎レイヤーとして期待されている。以上のことから例えば、一日の利用総額が特定の閾値を下回る場合は、現金と同様に、上記①及び②の情報収集義務の対象外とするような閾値を設けるべきと考える⁶。このような方法を認めない場合は、個人のプライバシー権を強く制約することになるため、それを正統化する根拠の詳細を明らかにすべきと考える。

また、VA のアプリケーションにおいて極小額の移転（例えば1セント）を同一のアプリケーションで同一人物に対して繰り返すマイクロアーニングアプリケーションが増えてきている。このような場合、一日ごとの総額に上限をつけた上で、例えば総額が一定の金額に達した場合に一つの移転とみなして①送金人、受取人の氏名及び②wallet アドレスを記録することを許容するべきと考える。

28. パラグラフ 176 について

「受取側の国の法域に規制がないとしても、送金元の事業者が、契約又は商慣習によって、受取側の国にトラベルルールの遵守を求めることができる」とあるが、現時点でそのような契約慣行や商慣習は存在せず、現実的ではない。VA 及び VASP に対する規制の統一性確保のためにも、トラベルルールを実施する場合には、実態に即した国際的統一商取引ルールの制定を行うことが必要になると考える。

29. パラグラフ 179 について

パラグラフ 179 では、unhosted wallets との間の VA 移転について、より高度な精査と制限を必要とする高リスクの取引として取り扱うよう求めることを検討すべきとされている。しかしながら、前述のとおり、たとえば VASP からの VA 流出等の損害を避けたい利用者は unhosted wallets を使用するという正当なインセンティブがあり、単に unhosted wallets を使用しているというだけで高リスクと判断すべきではない。

30. パラグラフ 246 及び 252 について

パラグラフ 246 では、VASP が適切なレベルの CDD を適用できない場合、取引を行わないことを求めている。他方でこの Guidance 全体において、①VA に関与する事業者は殆どが VASP であるとしたうえで、②self-hosted wallet との取引はリスクが高いとしているため、先進国から ID を持たない途上国の人への少額のトランザクションが殆どできなくなることが予想される。金融包摂と AML/CFT はトレードオフの関係に立つが、例えば一日1ドル以内のような極少額の取引はリスクが低いため、完全な CDD ではなくても（簡易的な ID 確

⁶ 前述のとおり、2020年6月の「FATF Report to G20 on So-called Stablecoins」においても、“Similar to other forms of payment(such as cash), there is a risk tolerance in the revised FATF Standards for a certain level of anonymous payments for virtual assets.”とされている。

認のみでも) 認めるべきと考える。

以上