# トラベルルール（FATF 勧告 16）の現状・課題・考察
## ― 暗号資産業界の健全な発展のために ―

才所 敏明 [1]　　櫻井 幸一 [2]　　辻井 重雄 [3]

**概要**：2009 年に運用が開始されたビットコイン以来，数多くの暗号資産が登場し，活発に取引されている一方，暗号資産の多くは強い匿名性が確保されており，マネーロンダリングやテロ資金供与，不正・不法な取引の決済手段等に活用されている．
このような暗号資産による不正・不法な資金移転を防止・抑止すべく，OECD 下の金融活動作業部会（FATF）は各国政府への勧告として，暗号資産関連事業者（VASP）へ利用者の特定・追跡を可能する情報の確認・記録および事業者間での共有を課すこと求めている．
本論文では，暗号資産の現状，FATF の 2019 年の勧告で規定したトラベルルール（VASP が確認・記録および共有すべき利用者情報の規定）およびその 2021 年の改定の内容，OpenVASP や TRISA 等のコンソーシアムを中心とした暗号資産業界の対応状況を報告・考察すると共に，トラベルルールの内容や暗号資産業界の対応の課題を指摘し，期待される安心・安全で公正・公平な暗号資産移転のあり方について考察する．

**キーワード**：暗号資産，匿名性，特定・追跡性，悪用対策，FATF，トラベルルール，Wallet，VASP，OpenVASP，TRISA，TRP，Travel Rule Protocol，IVMS101，interVASP Messaging Standards ，Unhosted Wallet，AOPP，Address Ownership Proof Protocol

# Current status, issues, and considerations of the Travel Rule (FATF Recommendation 16)
## - For the sound development of the virtual asset industry -

Toshiaki Saisho[†1]　　Kouichi Sakurai[†2]　　Shigeo Tsujii[†3]

***Abstract***: Since Bitcoin was started operation in 2009, many virtual assets have appeared and are being actively traded. On the other hand, most virtual assets have strong anonymity and are used for money laundering, terrorist financing, and settlement methods for fraudulent and illegal transactions.
The Financial Action Task Force (FATF) under the OECD has issued recommendations to governments of each country to prevent and deter fraudulent and illegal transfer of funds by such virtual assets. The recommendation requires governments to impose obligations on virtual asset service providers (VASPs) to confirm and record user information and share it among providers.
In this paper, we'll give the overview and the considerations on the current status of virtual assets, the Travel Rule defined in the FATF's 2019 recommendations, and their 2021 revisions. In addition, we'll give the overview and considerations on the response status of the virtual asset industry, such as the activities of consortia such as OpenVASP and TRISA. Furthermore, we'll point out issues regarding the content of Travel Rule and the response of the virtual asset industry, and finally we'll give considerations on the safe and secure and also fair and impartial transfer mechanism of virtual assets.

***Keywords***: Virtual Asset，Anonymity，Identifiability/Trackability，Abuse，FATF，Recommendation 16，Travel Rule，Wallet，VASP，OpenVASP，TRISA，TRP，Travel Rule Protocol，IVMS101，interVASP Messaging Standards ，Unhosted Wallet，AOPP，Address Ownership Proof Protocol

## 1. はじめに

暗号資産の元祖であるビットコインは Satoshi Nakamoto が 2008 年に投稿した論文([35])で公開され，2009 年に運用が開始された．以来，数多くの暗号資産が登場し，CoinMarketCap ([50])によると，2022 年 2 月には 17800 以上もの多数の暗号資産が登場し,活発な取引が行われている．暗号資産の時価の変動は大きいが，その中でも暗号資産総額は確実に増加し，2017 年 1 月には$17B であった資産総額が 2022 年 1 月には$2254B と推定されている．

一方，暗号資産の多くは，プライバシーや個人情報の確実な保護の観点から利用者の一定レベルの匿名性が確保されており，このことが利用者の特定・追跡を困難とし，マネーロンダリングやテロ資金供与，不正・不法な取引の決済手段等，暗号資産が様々の犯罪に活用され，犯罪・悪意の急増・氾濫を招く原因ともなっており，大きな社会課題となっている．2021 年の FATF のレポート([23])によると，2020 年の違法なビットコイン取引の割合は調査会社の判

1 （株）IT 企画　Advanced IT Corporation　http://advanced-it.co.jp/
toshiaki.saisho@advanced-it.co.jp.
（株）ZenmuTech　https://zenmutech.com/
中央大学研究開発機構　https://www.chuo-u.ac.jp/research/rdi/
2 九州大学大学院システム情報科学研究院
https://www.isee.kyushu-u.ac.jp/
3 中央大学研究開発機構　https://www.chuo-u.ac.jp/research/rdi/
【 研究報告用原稿：上記*の文字書式「隠し文字」 】

断により大きく異なるが，トランザクション数では 0.3%～9.1%，金額ベースでは 0.2%～15.4%と報告されている．ビットコインの資産総額は暗号資産全体の資産総額の 1/3 程度を占めているので，違法なビットコイン取引による資産移転総額は$1.4B～$113B に上ると推定されている．

このような暗号資産業界の課題に対し，1989 年に設立されたマネーロンダリングやテロ資金調達等の監視を行う政府間会合である金融活動作業部会（FATF：Financial Action Task Force）が，発行する FATF 勧告（FATF Standards）内で暗号資産取引時の要件等を規定し各国へ対応を要請している．

本論文では，FATF が 2019 年の勧告で暗号資産関連事業者（VASP：Virtual Asset Service Provider）が確認・記録および共有すべき利用者情報を規定したトラベルルールおよびその 2021 年の改定の内容，OpenVASP や TRISA 等のコンソーシアムを中心とした暗号資産業界の対応状況を報告・考察すると共に，トラベルルールの内容や暗号資産業界の対応の課題を指摘し，期待される安心・安全で公正・公平な暗号資産移転のあり方について考察する．

## 2. FATF 勧告 16「トラベルルール」

### 2.1 トラベルルール策定に向けて

2015 年 6 月の G7 サミットにて，暗号資産およびその他の新たな支払手段に対する適切な規制の導入が宣言された．同月に早速，FATF が，各国の VASP に対して登録・免許制を課すと共に利用者の本人確認を義務付けることなどを各国政府に勧告した．日本では，FATF の勧告を受け，制度設計や資金決済法の改正が検討され，2016 年 5 月に改正資金決済法を成立させ，VASP の登録制がスタートした．

2018 年 7 月の G20 財務大臣・中央銀行総裁会合にて，FATF に対し既存の FATF 勧告をどのように暗号資産に適用するかを明確にするよう要請した．FATF は同年 10 月，FATF 勧告 15「新技術」を改訂し，VASP にはマネーロンダリング等の規制が課されなければならないことを規定した．

更に FATF は 2019 年 6 月，FATF 勧告 16「電信送金」を改訂し，暗号資産の提供者と受取者に関する情報の確認・保存を VASP へ課した．この改定された FATF 勧告 16 がトラベルルールと呼ばれている([22])．

### 2.2 トラベルルールの内容

資産の提供者が使用する VASP では，暗号資産の提供者と受取者に関する以下の情報の確認・保存が求められ，受取者が使用する VASP への電信送金に以下の情報を含めておくことが求められている．

①資産提供者の名前
②トランザクション（以降，TX と略記）の処理に利用される資産提供者のアカウント番号
③資産提供者の地理的な住所および国固有の個人識別番号等
④資産受取者の名前
⑤TX の処理に利用される資産受取者のアカウント番号

このような内容のトラベルルール順守のためには，VASP は以下の機能を実装し運用する必要がある．

(1)Wallet 利用者の認証（本人確認）
(2)VASP 間での資産提供者・受取者の情報交換
(3)利用者情報の保存

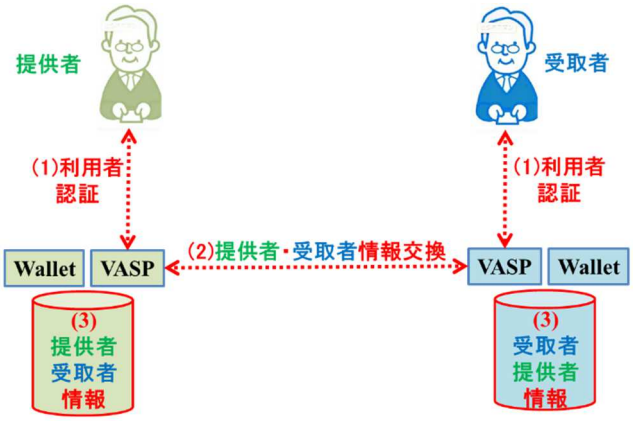


図 1　トラベルルールによる VASP への要請

### 2.3 トラベルルールの課題

(1)利用者の個人情報の VASP 間での交換

VASP は原則として暗号資産の取引時に利用者の個人情報を通信相手の VASP へ提供することが求められている．VASP は，通信相手の VASP が他国の場合，その国の個人情報の取扱いに関する規制を順守することが必要であり，また通信相手の VASP には自国の個人情報の取扱いに関する規制を順守させる必要がある([24],[25])．

暗号資産の強い匿名性により様々の犯罪に活用され，犯罪・悪意の急増・氾濫を招く原因ともなっており，犯罪捜査のための利用者の特定・追跡性の保証のためには必要なことであろうが，他国の VASP に対しても取引時に利用者の個人情報を提供するのが適切かどうか，疑念が残る．

(2)VASP 経由の取引のみを対象

暗号資産の移転パターンを大きく分類すると，次図に示すパターンに分類できる．

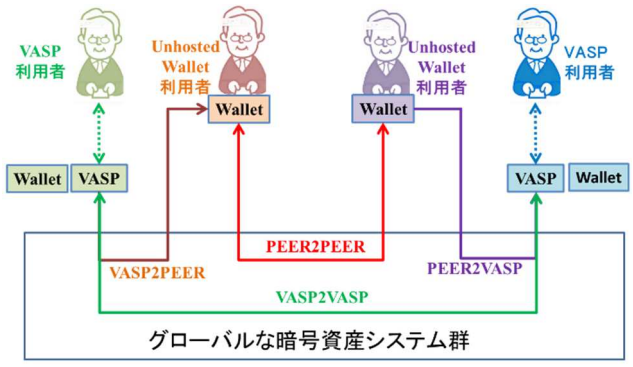


図 2　暗号資産の移転パターン

トラベルルールの対象は，図 2 の緑色の矢印で示した，VASP を利用する利用者間の暗号資産の移転のみである．

一般に暗号資産は VASP を通さず，直接利用者間で移転が可能なため，2019 年勧告のトラベルルールでは不正・不法な暗号資産の移転を検知してもその移転パターンが図 2 の緑色の矢印以外の場合は，利用者の特定・追跡は難しい．2019 年 10 月に発表された Europol のレポート([27])にても，このトラベルルールの問題が指摘されている．

## 3. 暗号資産業界のトラベルルールへの対応

トラベルルールにいろいろ課題はあるものの，その順守のための仕組みについて，システム開発ベンダーや VASP が検討に着手，まだ構想段階のものが多いが複数が提案・検討されている．以下に，VASP 間メッセージ交換方式の代表的な構想である OpenVASP([29])と TRISA([30])について，3.1 にて VASP 間の信頼性確認方式，3.2 にて各 VASP に期待される利用者の認証方式，3.3 にて VASP 利用者が暗号資産システムへ TX を発行するプロセス，それぞれの現状・比較・考察等をまとめている．

なお，VASP 間メッセージ交換のためのメッセージフロー（TRP：Travel Rule Protocol([31])）やメッセージ形式（IVMS101：interVASP Messaging Standards([32])）の標準化の議論も進められている．OpenVASP は，TRP および IVMS101 を，TRISA も IVMS101 の採用あるいは採用を予定している．

### 3.1 VASP 間の信頼性確認

#### 3.1.1 OpenVASP([29])

OpenVASP（Open Virtual Asset Service Provider）は，FATF のトラベルルールで求められている利用者情報の VASP 間での交換のためのオープンなプロトコルを確立することを目的として設立された組織である．

OpenVASP では，参加する VASP はイーサリアム上でスマートコントラクトを生成する．そのコントラクトアドレスが VASP Identity として使用し，その一部のデータを VASP の識別コード（VASP code）として使用する．VASP は VASP code に利用者に割り当てた固有のデータを追加し利用者の暗号資産アカウント番号（VAAN：Virtual Asset Account Number）を定義する．この VAAN が VASP 間のメッセージ交換に利用されている．メッセージには，トラベルルールで規定されている暗号資産の利用者（提供者および受取者）の個人情報も含まれている．

OpenVASP の基本原則の一つとして Decentralized Approach の採用がある．そのため，VASP が利用者の個人情報の交換を行う通信相手の VASP が信頼できるかどうかについては，VASP 自らの責任での確認が求められている．

通信相手の VASP が信頼できるかどうかの判断には，VASP がその法域（国）のしかるべき機関により認定・登録されているか，すでに信頼関係を構築できている VASP が通信相手の VASP を信頼しているか，等により信頼性を判断することが想定されている．なお，信頼性が確認できた通信相手の VASP は信頼できる VASP として登録され，次回以降の信頼性確認を省略できる仕組みとなっている．

#### 3.1.2 TRISA([30])

トラベルルール情報共有アライアンス(TRISA：Travel Rule Information Sharing Alliance)は，OpenVASP と異なり，信頼できる第 3 者機関 TRISA CA（Certificate Authority）の存在を前提とした，通信相手の VASP の信頼性確認が相互に可能な PKI ベースの仕組みを採用している．具体的には，VASP の実在性の確認や法域（国）における認可された VASP であることの確認等は，TRISA CA への登録申請時に VASP が提出する情報により，TRISA CA が検証する．確認がとれた VASP へ TRISA CA が公開鍵証明書を発行し，その証明書が VASP 間の相互の信頼性確認に使用される．

#### 3.1.3 比較・考察

VASP 間の信頼性確認について，OpenVASP と TRISA の対応を整理したのが次図である．

| 機能 | OpenVASP | TRISA |
|---|---|---|
| VASP登録時の信頼性確認 | 規定せず（各国政府の認定時の審査に期待） | TRISA CAによる登録時の審査 |
| VASP間通信時の信頼性確認 | 初回は各国の認定情報、業界の信頼度評価等で確認（信頼できるVASPはスマートコントラクトに登録） | TRISA CA発行の証明書（SSL/TLS） |

図 3　VASP 間信頼性確認方式の比較

OpenVASP が採用する VASP ごとの信頼性の確認は，個々の VASP の負担となるが，VASP の信頼性を審査する中央管理組織は不要となる．このような Decentralized Approach が適切に機能するには，各国の VASP 認定・登録の審査基準の統一，VASP の責任ある確認作業の実施，が前提となろう．

TRISA が採用している PKI ベースの Centralized Approach の場合は，通信相手の VASP の信頼性確認は TRISA CA 発行の証明書の確認のみで済み，確認作業は不要となる．

### 3.2 利用者の認証

下図に示すように，利用者の認証（KYC）に必要な機能の実現方式については，OpenVASP，TRISA 共に一切規定していない．

| 機能 | OpenVASP | TRISA |
|---|---|---|
| 登録時の利用者認証<br>身元確認<br>身元情報の登録・管理<br>当人確認情報の登録・管理 | 規定せず<br>①VASPが個々の手順に従ってKYCを実施<br>②VASPのKYCの適切さは、各国のVASP審査時の確認に期待 | |
| 利用時の利用者認証<br>当人確認 | | |

図 4　利用者認証方式の比較

一般に，身元確認方法や当人確認方法は，各国の制度や

IT 環境により異なるため，規定されていないものと考えられる．VASP は各国で個々に整備・運用されている制度により登録・認定されていることが前提であり，身元確認方法・当人確認方法の適切さおよび身元情報・当人確認情報の登録・管理の適切さは，各国の制度による審査に期待しているものと想定される．

しかし，各国・各 VASP 独自の方式による利用者認証方式であっても，利用者の特定・追跡性を一定レベル確保する必要があり，利用者認証方式の信頼性に関する基準・規定等が必要と考えられる．

### 3.3 VASP 利用者の TX 発行プロセス

OpenVASP および TRISA では，VASP 利用者の TX 発行プロセスを下図のように想定している．

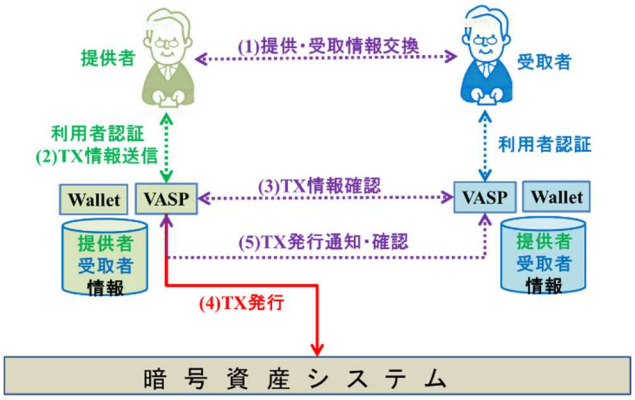


図 5　VASP 利用者の TX 発行プロセス

TX 発行プロセスにおけるトラベルルール対応のための情報交換について，OpenVASP，TRISA の両方式を比較したのが次図である．

| 機能 | OpenVASP | TRISA |
|---|---|---|
| (1)提供・受取情報交換<br>（提供者←→受取者） | 規定せず<br>＊受取者のVAAN | 規定せず<br>＊受取者のVASP |
| (2)TX情報送信<br>（提供者→VASP） | 金額、提供アドレス、<br>受取者のVAAN | 金額、アドレス、<br>受取者のVASP |
| (3)TX情報確認<br>（VASP←→VASP） | →金額、提供者情報、<br>受取者情報（＊）<br>←（＊）に加え、<br>受取アドレス | →金額、アドレス、<br>提供者情報<br>←受取者情報 |
| (4)TX発行<br>（VASP←→<br>暗号資産システム） | →TX<br>←TXID | →TX（VASP署名）<br>←TXID |
| (5)TX発行通知・確認<br>（VASP←→VASP） | →（＊）に加え、<br>提供アドレス、TXID<br>←受信データをそのまま | →TXID |

図 6　TX 発行プロセスにおける情報交換方式の比較

(1) 提供・受取情報交換（提供者＜＝＞受取者）

TX 作成に必要な情報の交換を行うフェーズであるが，それに加え，受取者は利用する VASP を提供者へ通知する．

OpenVASP では，VASP の識別情報（VASP code）が含まれている受取者のアカウント番号 VAAN を，TRISA では規定はないが，TRISA CA が発行する受取者の VASP の識別コードや VASP 証明書の通知を想定しているものと考えられる．

(2)TX 情報送信（提供者＝＞VASP）

提供者が発行する TX 情報の他に，受取者が利用する VASP の情報を含め送信する．

(3)TX 情報確認（VASP＜＝＞VASP）

**3.1** で記載した OpenVASP，TRISA それぞれの方法による VASP 間の信頼性確認後，トラベルルールに規定された提供者の情報，受取者の情報を相互に通知する．

(4)TX 発行（VASP＜＝＞暗号資産システム）

OpenVASP，TRISA 共に，暗号資産システムへの影響を与えないよう，従来の TX のみによる資産移転の承認依頼を行う方式である．

なお，TRISA では，TX へ発行元の VASP の署名を付与することも検討されている．VASP 署名の付与により，正規の VASP により発行された TX であること，トラベルルールに規定された情報の確認・管理が保証された TX であることを，暗号資産システム側で検証することへの期待があるものと想定される．

(5)TX 発行通知・確認（VASP＜＝＞VASP）

TX が発行された後は，OpenVASP，TRISA 共に，受取者の VASP へ TXID を通知する．

## 4. FATF によるトラベルルール改定

2019 年 6 月の FATF 勧告に含まれているトラベルルールの最大の課題は，トラベルルールが VASP 利用者間の TX のみを対象とした規定であることである．いわゆる Unhosted Wallet への対応が考慮されていなかった点にあった．

筆者らも，2019 年版トラベルルールの不十分さ・課題を指摘しつつ，安心・安全な暗号資産移転基盤の可能性を検討してきた([1])．

2021 年 10 月，FATF はトラベルルールを改定した([20], [21])．改定されたトラベルルールで新たに追加された主な規定は次の 2 点である．

(1) Unhosted Wallet への対応

FATF は各国に対し，VASP へ Unhosted Wallet（個人管理の Wallet）との暗号資産移転の精査を可能とする仕組みを課すこと，を要求している．もちろん，Unhosted Wallet を使用する提供者または受取者の情報の確認・管理も求めている．

本規定を各国の VASP が順守することにより，図 2 に示す暗号資産の移転パターンのうち，VASP2PEER および PEER2VASP の移転パターンも少なくともトラベルルールの規定対象として，不正・不法な暗号資産移転の監視対象とすることが可能となる．

しかし，今回の改定においても，図 2 に示す暗号資産の移転パターンのうちの，PERR2PEER の移転パターンは依

然として対象から外れている．

(2) 金融分野の新たな製品・サービスへの対応

FATF は各国に対し，金融分野の新たな製品やサービスの，マネーロンダリングやテロ資金供与および不正・不法な取引の決済手段等，暗号資産が様々の犯罪に活用されるリスクを特定・評価し，市場投入前にリスクを管理・軽減する適切な対策を事業者にとらせること，を要求している．

現状の暗号資産システムが不正・不法な利用を防止・抑止する仕組み無しに社会に投入され，対策が後手に回っていることへの反省からの各国への要請と考えられる．

## 5. 2021 年版トラベルルールへの対応

暗号資産業界は 2019 年版トラベルルールへの対応が中心で，2021 年版トラベルルーへの対応はまだこれから，という状況である．

ところで，スイスでは金融規制を担当する政府機関である金融市場監督局（FINMA）が 2019 年 8 月より，Unhosted Wallet との間の暗号資産の移転は，VASP は提供者および受取者の身元を確認し，Unhosted Wallet/暗号資産アドレスの所有権を確認した場合にのみ可能，という規制を行っている．この FINMA 規制順守のために AOPP（Address Ownership Proof Protocol）([33])が開発された．

このような経緯で開発された AOPP を，2021 年版トラベルルール対応に利用することが検討されている．以下，AOPP の概要を示す．

### 5.1 AOPP ([33])

2021 年版トラベルルールで VASP に要求される Unhosted Wallet への対応は，単に **2.2** に記載している 2019 年のトラベルルールで規定された提供者・受取者の情報確認・管理のみでは済まない．VASP が管理する Hosted Wallet の場合は，暗号資産が割り付けられているアドレスの所有者がその Hosted Wallet の所有者であることを VASP は容易に確認できるが，Unhosted Wallet の場合はその所有者が指定したアドレスが Unhosted Wallet の所有者のアドレスかどうかを確認する別途の仕組みが必要となる．

AOPP は，Unhosted Wallet が指定した暗号資産アドレスの所有確認のためのプロトコルである．VASP から Unhosted Wallet へ何らかのメッセージを送信，Unhosted Wallet はそのメッセージへ指定したアドレスに対応する秘密鍵で署名し VASP へ返送，VASP は指定されたアドレスに対応する公開鍵で署名検証しそのアドレスの所有（秘密鍵の所有）を確認する，という仕組みである．

VASP にとっては 2019 年のトラベルルール対応の仕組みへ AOPP の追加により 2021 年のトラベルルールへの対応が可能となるが，Unhosted Wallet 利用者は AOPP へ対応する Wallet が必要となる．

## 6. 安心・安全で公平・公正な暗号資産移転の仕組み実現上の課題

本章では、暗号資産の課題、FATF の勧告の内容・課題、暗号資産業界の対応・課題を踏まえ、筆者らが期待する安心・安全で公平・公正な暗号資産移転の観点から課題を整理し考察する．

(1)利用者の特定・追跡の仕組み上の課題

FATF は，利用者の特定・追跡のための情報収集・確認・記録を VASP に期待し，VASP 間での情報共有を期待している．VASP およびシステム開発ベンダーは，FATF の勧告を順守するための技術開発・標準化等を進めている．

しかし，VASP を利用しない Unhosted Wallet 利用者の特定・追跡については規定されていない．CipherTrace のレポート([19])によると，ビットコインの 2020 年のトランザクションの内，61%が PEER2PEER のトランザクションであり，資産移転総額の 80%が PEER2PEER のトランザクションで移転が行われている．つまり，最新の FATF トラベルルーでも，多くの資産移転が規制の対象外となっており，マネーロンダリングやテロ資金供与，不正・不法な取引の決済等の検知・防止の観点からは大きな問題である．早期の FATF での検討，暗号資産業界の対応が望まれる．

(2)利用者の匿名性確保上の課題

FATF は VASP に利用者の身元確認を期待している．つまり，VASP に対する利用者の匿名性は完全に失われることになる．特定・追跡性と両立可能な一定レベルの匿名性を保証する仕組みの検討・導入が望まれる．

(3)個人情報の海外移転上の課題

FATF は，暗号資産移転時に利用者情報（個人情報）の関連する VASP 間での共有を期待している．海外の VASP も含めたこのような個人情報の VASP 間での拡散が適切かどうか，疑念が残る．利用者の個人情報の VASP 間共有を必要としない利用者の特定・追跡性の確保の仕組みが望まれる．

(4)暗号資産システム側の対応の課題

暗号資産の課題に対し，暗号資産システム開発・運用関係者の検討は進んでいない．ビットコインでは，トラベルルール対応に向けた BIP（Bitcoin Improvement Proposal）検討の動きはあるが，未だ提案されていない．今後，暗号資産システム開発・運用関係者による課題克服策の検討・提案を期待したい．

## 7. おわりに

暗号資産の課題は，強い匿名性が確保されているがゆえに，利用者の特定・追跡を困難とし，マネーロンダリングやテロ資金供与，不正・不法な取引の決済手段等，暗号資産が様々の犯罪に活用され，社会の犯罪・悪意を誘発する要因となっていることである．

暗号資産の課題克服は道半ばである．最新の FATF の勧

告（2021 年版トラベルルール）でも，PEER2PEER の暗号資産移転についての対策は含まれておらず，一方，暗号資産業界はまだ VASP2VASP の暗号資産移転に対する 2019 年版トラベルルールへの対応に苦心しており，2021 年版への対応検討はこれからという状況である．暗号資産の課題克服という社会のニーズに応えるべく，暗号資産に関する規制の再検討および暗号資産業界のより精力的な対応が求められている．

このような状況を踏まえ，期待される安心・安全で公平・公正な暗号資産移転の仕組み実現上の課題について整理・考察した．

筆者らは，上記課題を念頭に置きつつ，暗号資産業界の健全な発展のために，安心・安全で公平・公正な暗号資産移転の仕組みに関する研究を推進する予定である．

## 参考文献

[1] 才所敏明, 辻井重男, 櫻井幸一,“ビットコイン利用者の特定・追跡の仕組みに関する考察（２）”, 第 94 回コンピュータセキュリティ研究会（CSEC）
[2] 才所敏明, 辻井重男, 櫻井幸一,“ビットコイン利用者の特定・追跡の仕組みに関する考察”, 第 54 回情報通信システムセキュリティ研究会（ICSS）.
[3] 才所敏明，辻井重男，櫻井幸一,“暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察”, 暗号と情報セキュリティシンポジューム（SCIS2021）.
[4] 才所敏明，辻井重男，櫻井幸一,“暗号資産の匿名性要件の整理と対応レベルの比較”, コンピュータセキュリティシンポジューム（CSS2020）.
[5] 才所敏明，辻井重男，櫻井幸一,“暗号資産台帳の匿名性と特定・追跡性についての考察”, 2020 年電子情報通信学会ソサイエティ大会.
[6] 才所敏明，辻井重男，櫻井幸一,“DAG 技術ベースの暗号資産の匿名性に関する考察”, 暗号と情報セキュリティシンポジューム（SCIS2020）
[7] 才所敏明，辻井重男，櫻井幸一，”匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察 ”, コンピュータセキュリティシンポジューム 2019（CSS2019）.
[8] 才所敏明，辻井重男，櫻井幸一，” 暗号仮想通貨における匿名化技術の現状と展望 ”, 情報処理学会第 81 回全国大会, 2019.
[9] 才所敏明，辻井重男，櫻井幸一，” 仮想通貨の匿名性の現状と課題”，暗号と情報セキュリティシンポジューム（SCIS2019）.
[10] 才所敏明，辻井重男,“インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立”, 暗号と情報セキュリティシンポジューム（SCIS2021）.
[11] 才所敏明，辻井重男,“インターネット時代の本人確認基盤に関する考察－ NAF から GAF へ －”, コンピュータセキュリティシンポジューム 2020（CSS2020）.
[12] 才所敏明,“NAFJP における本人確認方法に関する考察 － National Authentication Framework in Japan －”, コンピュータセキュリティシンポジューム 2019（CSS2019）.
[13] 才所敏明，辻井重男,“日本における本人確認基盤（NAFJA）の考察 － National Authentication Framework in Japan －”, 情報処理学会・第 85 回コンピュータセキュリティ研究発表会，2019.
[14] 穴田啓晃，櫻井幸一,“ブロックチェーンの暗号論的要素技術の分類”, SCIS2018.
[15] 宇根正志,“暗号資産における取引の追跡困難性と匿名性：研究動向と課題”, 金融研究/2019.7. http://www.imes.boj.or.jp/research/papers/japanese/kk38-3-4.pdf
[16] Chainalysis,“The 2022 Crypto Crime Report” https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf
[17] Sean Foley, Jonathan R. Karlsen, Tālis J. Putniņš,“Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?”, 2019. https://academic.oup.com/rfs/article/32/5/1798/5427781
[18] CipherTrace,“CipherTrace Geographic Risk Report:VASP KYC by Jurisdiction”, 2020. https://ciphertrace.com/wp-content/uploads/2020/10/CipherTrace-2020-Geographic-Risk-Report-100120.pdf
[19] CipherTrace,“Cryptocurrency Crime and Anti-Money Laundering Report, May 2021”, 2021. https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-may-2021/
[20] FATF,“INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION（FATF Recommendations 2012（Updated October 2021））”, 2021. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
[21] FATF,“Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers”, 2021. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
[22] FATF,“Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers”, 2019. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.htmll
[23] FATF,“SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS”, 2021. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf
[24] GRC World Forums,“The AML “travel rule”: a new challenge for VASPs and GDPR”, 2020. https://www.grcworldforums.com/financial-crime/the-aml-travel-rule-a-new-challenge-for-vasps-and-gdpr/236.article
[25] European Commission ,“What rules apply if my organisation transfers data outside the EU?”. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en
[26] EUR-Lex,“DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU”, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
[27] EUROPOL,“INTERNET ORGANISED CRIME THREAT ASSESSMENT”, 2019.

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
[28] Financial Crimes Enforcement Network，“Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets”, DEPARTMENT OF THE TREASURY, 2020. https://public-inspection.federalregister.gov/2020-28437.pdf
[29] David Riegelnig，“OpenVASP: An Open Protocol to Implement FATF’s Travel Rule for Virtual Assets”, 2019. https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf?cache=1
[30] TRISA，“Travel Rule Information Sharing Architecture for Virtual Asset Service Providers”, 2020. https://trisa.io/trisa-whitepaper/
[31] OpenVASP，“Travel Rule Protocol”，2021. https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/7c38b8c98ca7bc57bf368f98d5825699fa4f85e2/core/specification.md
[32] Joint Working Group on interVASP Messaging Standards，“interVASP Messaging Standards”. https://intervasp.org/
[33] 21 Analytics，“Address Ownership Proof Protocol (AOPP). https://aopp.group/index.html
[34] Thomas Hardjono，“Attestation Infrastructures for Private Wallets”，2021. https://arxiv.org/abs/2102.12473
[35] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf
[36] Mastering Bitcoin https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
[37] Stefano Bistarelli，Ivan Mercanti，Francesco Santini, "An Analysis of Non-standard Transactions", 2019. https://www.frontiersin.org/articles/10.3389/fbloc.2019.00007/full
[38] Monero：Privacy in the blockchain　v1.0 https://eprint.iacr.org/2018/535.pdf
[39] Zero to Monero: First Edition https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
[40] Mastering Monero https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf
[41] Zcash Protocol Specification https://www.btrade.co.kr/btrade_res/20180507145055652.pdf
[42] Grin Whitepaper https://www.allcryptowhitepapers.com/grin-whitepaper/
[43] Serguei Popov，“The Tangle”，April 30, 2018. Version 1.4.3. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
[44] Anton Churyumov，“Byteball: A Decentralized System for Storage and Transferof Value”，2016. https://obyte.org/Byteball.pdf
[45] Colin LeMahieu，“Nano: A Feeless Distributed Cryptocurrency Network”，2018. https://nano.org/en/whitepaper
[46] Leemon Baird, Mance Harmon, Paul Madsen，“Hedera: A Public Hashgraph Network & Governing Council”，2019. https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf
[47] AIDos Kuneen − A Blockless and Anonymous Cryptocurrency for the Post-Quantum Era −，AIDos Developer & AIDos Foundation，2018. http://www.aIDoskuneen.com/files/adk_whitepaper.pdf
[48] DERO PROJECT WHITE PAPER，2018. https://dero.io/attachment/Whitepaper.pdf
[49] Tangram: An Introduction，2018. https://tangrams.io/wp-content/uploads/2018/12/Tangram_An_Introduction-2018-12-19-03-27.pdf
[50] CoinMarketCap，https://coinmarketcap.com/ja/all/views/all/
[51] Nicolas van Saberhagen, "CryptoNote v2.0", 2013. https://cryptonote.org/whitepaper.pdf
[52] Andrew Poelstra，“Mimblewimble”，2016. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[53] Gregory Maxwell，“CoinJoin: Bitcoin privacy for the real world”，2013. https://bitcointalk.org/index.php?topic=279249.0
[54] Gregory Maxwell，Andrew Poelstra，”Borromean Ring Signature”，2015. https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
[55] SHEN NOETHER，“RING CONFIDENTIAL TRANSACTIONS”，2015. https://eprint.iacr.org/2015/1098.pdf
[56] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer, “From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again”，2011. https://eprint.iacr.org/2011/443
[57] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, “Pinocchio: Nearly Practical Verifiable Computation”，2013. https://eprint.iacr.org/2013/279
[58] Christina Garman，Matthew Green，Ian Miers，” Accountable Privacy for Decentralized Anonymous Payments”，2016. https://eprint.iacr.org/2016/061.pdf