安心・安全な暗号資産取引基盤（SSVATF）の提案

才所 敏明[*1]　　辻井 重男[*2]　　櫻井 幸一[*3]

概要：暗号資産は，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，様々の犯罪での利用が急増し，大きな社会課題となっている．原因は，ビットコインに限らず多くの暗号資産がプライバシーや個人情報の保護の観点から利用者の強い匿名性を確保可能な仕組みを採用していることにある．
OECD 下の政府間会合である金融活動作業部会（FATF : Financial Action Task Force）では，2019 年には FATF 勧告（FATF Standards）として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を策定，2021 年にはその内容を更に改定し，暗号資産のさまざまの犯罪での利用を防止・抑止するための対策を，各国へ要請している．
本稿では，暗号資産が社会に与える脅威・弊害を防止・抑止する対策としての現状の FATF 勧告・トラベルルールの課題を指摘し，そのような課題克服を目指した安心・安全で公正・公平な暗号資産移転が可能となる暗号資産取引基盤（SSVATF : Secure and Safe Virtual Asset Transfer Framework）構想を提案する．

キーワード：暗号資産，マネーロンダリング，テロ資金供与，決済手段，匿名性，特定・追跡性，FATF，トラベルルール，暗号資産関連事業者，暗号資産取引基盤，SSVATF，W3C，DID，VC，VP，本人確認基盤，身元確認，当人確認，NAF

Proposal of Secure and Safe Virtual Asset Transfer Framework (SSVATF)

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

Abstract: Cryptocurrency assets have become a major social issue due to the rapid increase in their use in various crimes such as money laundering, terrorist financing, and settlement methods for fraudulent and illegal transactions. The cause is that many crypto assets, not limited to Bitcoin, have adopted a mechanism that can ensure strong anonymity of users from the viewpoint of protection of privacy and personal information.
In order to prevent and deter the use of crypto assets for various crimes, the Financial Action Task Force (FATF) under the OECD, announced the 2019 FATF Recommendations (FATF Standards) that defines the role of VASP (Virtual Asset Service Provider). VASP should confirm, record, and share the user information between VASPs. It is called the travel rule. In 2021, the travel rule was further revised, requesting each country to take measures to prevent and deter the use of crypto assets in various crimes.
This paper points out the issues of the current FATF recommendations and travel rules as measures to prevent and deter the threats and harmful effects of crypto assets on society. Furthermore, we propose the SSVATF (Secure and Safe Virtual Asset Transfer Framework) that enables safe, secure, fair and equitable crypto asset transfer with the aim of overcoming the issues pointed out.

Keywords: CryptoAssets, Money Laundering, Terrorist Financing, Anonymity, Specifiability / Traceability, FATF, Travel Rule, Virtual Asset Service Provider，VASP，Secure and Safe Virtual Asset Transfer Framework, SSVATF, W3C, DID, VC, VP，National Authentication Framework，NAF

1. はじめに

2009 年に運用が開始されたビットコイン([38])以来，数多くの暗号資産が登場し，CoinMarketCap ([53])によると，2022 年 8 月には 20436 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 8 月には$1084B と推定されている．

一方，暗号資産は，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，様々の犯罪での利用も急増し，大きな社会課題となっている．2021 年の FATF のレポート([24])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 2020 年の取引総額を約$383B，当時のビットコインの評価額を約$15000 で試算すると，ビットコインだけでも違法な取引による資産移転総額は$0.8B～$58.9B に上ると推定されている．

暗号資産の様々の犯罪での利用の急増は，ビットコイン

*1　（株）IT 企画　http://advanced-it.co.jp/
mail：toshiaki.saisho@advanced-it.co.jp
中央大学研究開発機構
(株)ZenmuTech
*2　中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp
*3　九州大学大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所
mail：sakurai@inf.kyushu-u.ac.jp
【 論文原稿：上記*の文字書式「隠し文字」 】

に限らず多くの暗号資産がプライバシーや個人情報の保護の観点から利用者の強い匿名性を確保可能な仕組みを採用していることにある．このことが犯罪捜査機関・金融情報調査機関による利用者の特定・追跡を困難とし，犯罪での利用には都合の良い資産移転の仕組みとなっているのが現状である．

このような暗号資産の課題克服を目指し，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，2019 年には FATF 勧告（FATF Standards）として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を策定，2021 年にはその内容を更に改定し，各国へ暗号資産のさまざまの犯罪での利用を防止・抑止するための対策を要請している．

本論文では，暗号資産が社会に与える脅威・弊害を防止・抑止する対策としての現状の FATF 勧告・トラベルルールの課題を指摘し，そのような課題克服を目指した安心・安全で公正・公平な暗号資産移転が可能となる安心・安全な暗号資産取引基盤（SSVATF : Secure and Safe Virtual Asset Transfer Framework）構想を提案する．

2. FATF 勧告とその課題

2.1 トラベルルール

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が成立，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」を改定し，暗号資産の提供者と受取者の特定・追跡に必要な個人情報の確認・保存を VASP へ課した（詳細は 2.2 参照）．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([23])．

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 利用者間のトランザクションのみを対象とした規定であることであった．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．2019 年 10 月に発表された Europol のレポート([28])でも，このトラベルルールの問題が指摘されている．

2021 年 10 月，FATF はトラベルルールを改定した（[21], [22]）．しかし，改定されたトラベルルールで新たに追加された Unhosted Wallet への対応は，暗号資産移転を実施する提供者又は受取者の一方が VASP 利用者の場合のみであった．

暗号資産の犯罪利用の防止・抑止を目指し，調査・捜査機関が利用者の特定・追跡を可能とするよう導入されたトラベルルールであるが，現在の内容では，Unhosted Wallet 間の暗号資産移転においては利用者の特定・追跡は依然として困難な状況である．

2.2 トラベルルールの具体的内容（現状）

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
⑤トランザクション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

また，2021 年の改定で対象となった VASP 利用者と暗号資産移転を行う Unhosted Wallet の利用者に対しても，VASP はトラベルルールが規定している提供者および受取者の情報の確認・保存が求められている．

2.3 トラベルルールの課題

(1)不正・不法な利用者の特定・追跡の仕組み

FATF の 2019 年のトラベルルールは VASP に対し，VASP 利用者間の暗号資産の移転を対象とし，利用者の特定・追跡のための情報収集・確認・保存を求めた規定であり，2021 年の改定トラベルルールは，VASP 利用者と Unhosted Wallet 利用者間の暗号資産移転を対象とし，VASP に対し同様の要件を定めた規定である．

一般に暗号資産の移転には，図 1 のように大きく 4 種のパターンに分類できる．FATF の現在のトラベルルールが VASP に対し利用者の特定・追跡のための情報収集・確認・保存を求めているのは，黄色でマーク（実線で表示）した移転パターンであり，赤色でマーク（点線で表示）した移転パターンである Unhosted Wallet 利用者間の暗号資産の移転は対象から外れている．現在のトラベルルールでは，このパターンの不審な暗号資産の移転を検知しても，犯罪捜査機関や金融情報調査機関がその利用者を特定・追跡する

ことは困難である．

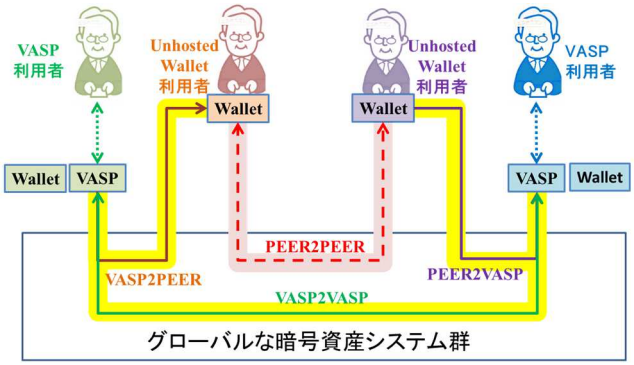

図１　暗号資産の移転パターン

ビットコインのトランザクションを分析したレポート([20])では，2020 年のビットコイン・トランザクションの内，61%が Unhosted Wallet 間（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おり，このように暗号資産の主要な移転パターンである Unhosted Wallet 利用者間の暗号資産移転について規定されていない FATF の現状のトラベルルールでは，たとえ各国が厳密に順守したとしても，多くの場合，不審な暗号資産の移転を検知しても利用者の特定･追跡は難しく，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，様々の犯罪での利用の急増という大きな社会課題の克服には程遠いと言わざるを得ない．

(2)利用者の個人情報の VASP 間での共有

FATF トラベルルールによると，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（図２）．VASP の個人情報の収集・確認・保管には様々のリスクが発生し，また通信相手の 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([25],[26])．

トラベルルールは，従来の金融機関と同様の利用者の確実な特定・追跡性を保証する仕組みを，VASP にも適用することを目指している．しかし，利用者の観点から望まれる，暗号資産システムと同程度の匿名性の確保と，調査・捜査機関の観点から望まれる，犯罪利用を防止・抑止するための利用者の特定・追跡性の確保，の両立を目指した仕組みが望ましい．

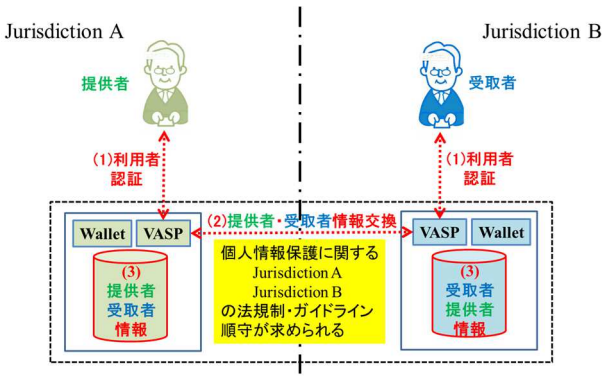

図２　VASP 間の利用者の個人情報の共有

3.　安心・安全な暗号資産取引基盤（SSVATF）

本章では，トラベルルールの課題の克服を目指して構想策定中の安心・安全な暗号資産取引基盤（SSVATF：Secure and Safe Virtual Asset Transfer Framework）について報告する．

3.1　構想策定基本方針

①VASP による利用者の確実な身元確認

トラベルルールでは，利用者の名前，住所，国固有の識別番号の収集・確認が求められているが，その具体的方法は各国に任されている．SSVATF では，各国で構築・運用が進められている本人確認基盤（NAF：National Authentication Framework，[12]）との連携により，確実な身元確認の枠組みの提案を目指している．

②資産移転における利用者の確実な匿名性の確保

SSVATF における暗号資産移転にかかわる手続き・情報交換においても，現行の暗号資産システムと同程度の利用者の確実な匿名性確保を目指している．その実現にあたっては，W3C で標準化が進められている DID（Decentralized Identifier，[36]）の活用を想定している．

③不正・不法な利用者の確実な特定・追跡

社会の安心・安全や公平・公正の維持には，暗号資産の不正・不法な利用の防止・抑止が不可欠である．利用者の匿名性の確保と同時に，犯罪捜査機関や金融情報調査時には，不正・不法な利用者の確実な特定・追跡性の確保を目指す．具体的には，確実な身元確認に基づき割り当てられる NAF-ID を連結可能匿名化により匿名 ID である DID と連携させ確実な匿名性を実現すると共に，必要な場合は，管理されている連結情報を利用し，DID から NAF-ID を特定し，身元情報を確認し追跡を可能とする仕組みを想定している．

④個人情報・プライバシー情報の開示先・範囲の最少化

トラベルルールでは，暗号資産移転時に個人情報・プライバシー情報を VASP 間で共有することになっているが，SSVATF では金融情報調査機関が報告を求める場合や犯罪捜査機関・金融情報調査機関の要請を受けた時点で，W3C で標準化が進められている VC（Verifiable Credential，[37]）/VP（Verifiable Presentation，[37]）を利

用し，必要な開示先に必要な情報のみを開示する仕組みを目指している．

⑤各種暗号資産システムとの連携

特定・追跡性が保証されない利用者が暗号資産システムの悪用を防ぐため，SSVATF で利用者の特定・追跡性の確実な確認した上で発行されたトランザクションには確認した VASP が署名を付与すると共に，暗号資産システム側では，その署名の確認により，特定・追跡性が保証された利用者かどうかの確認を可能とすることを想定している．暗号資産システムとの連携により，疑わしいトランザクションの利用者の特定・追跡を容易とし，さまざまの犯罪での暗号資産の悪用の防止・抑止を目指している．

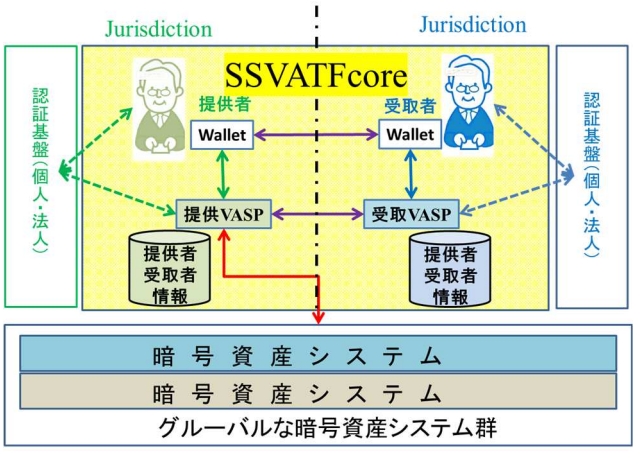

図３　SSVATF の位置づけ

3.2 SSVATF における暗号資産移転

2 人の利用者間で暗号資産の移転を行う際の，SSVATF における処理手順を図 4 に示している．

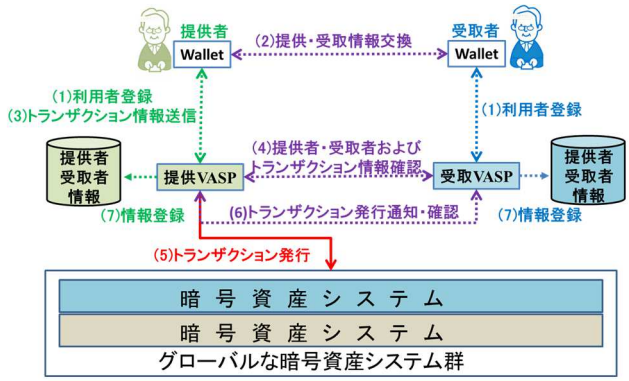

図４　SSVATF による暗号資産移転のための処理手順

3.2.1 利用者登録

暗号資産システム利用者は，SDIP（SSVATF DID Issuer for People）へ利用者固有の NAF-IDp（日本の場合は，個人番号を想定）を提示し，当人確認を受け，SSVATF 内の個人識別コード（DIDu）を入手する．

次に，利用者は使用する VASP へ，DIDu を提示し，DIDu の所有者であることを示し，暗号資産の取引に使用する利用者識別コード（DIDut）を入手する．利用者は必要に応じ新たな利用者識別コード DIDut を入手し使用する．

利用者登録後は，利用者は個人情報を開示する必要はなく，DIDut を利用し暗号資産の移転が可能となる．

また，VASP も同様に，組織の NAF-IDo（日本の場合は，法人番号を想定）を SDIO（SSVATF DID Issuer for Organization）へ提示し，組織として，また VASP としての確認を受け，SSVATF 内の組織識別コード（DIDo）を入手し，使用する．SSVATF 内で使用する DID は VDR（Verifiable Data Registry）に登録され，DID 所有者（個人，組織）の当人確認が可能である．

なお，SDIP，SDIO の機能は，NAF 内での提供，あるいは SSVATF 内の VASP が担うことも可能で，新たな役割の組織は必ずしも必要ではない．

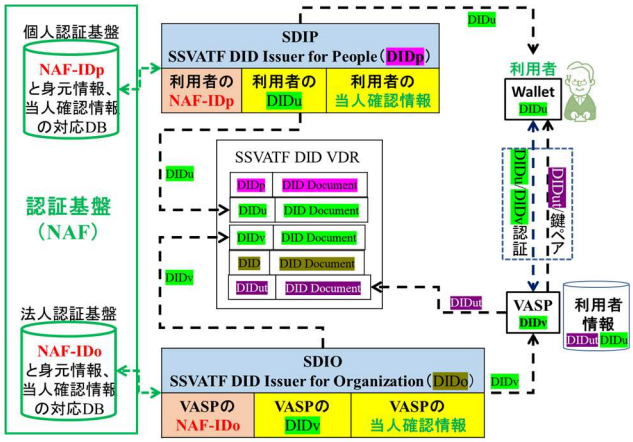

図５　SSVATF における利用者登録

3.2.2 利用者間情報交換（トランザクション構成）

暗号資産の提供者・受取者間では，暗号資産システムへ発行するトランザクション作成に必要な情報の交換を行う．トランザクション作成に必要な情報は暗号資産システムごとに異なるが，基本的には以下のような情報の交換を想定している．

提供者は，自身の利用者識別コード DIDst，受取者の利用者識別コード DIDrt，暗号資産の種類，提供用アドレス，提供額，その他のトランザクション作成に必要な情報，以上の情報全体への提供用アドレスの秘密鍵による署名，更に以上の情報全体への DIDst の秘密鍵による署名から構成される提供情報を受取者へ送信することを想定している．

受取者は，自身の DIDrt，提供者の DIDst，受取用アドレス，その他のトランザクション作成に必要な情報，以上の情報全体への受取用アドレスの秘密鍵による署名，更に以上の情報全体への DIDrt の秘密鍵による署名から構成される受取情報を提供者へ送信することを想定している．

その後，提供者はトランザクションを構成，関係者の署名等を収集の上，トランザクション，提供情報，受取情報から構成されるトランザクション発行情報を，提供者が使用する提供 VASP へ送信する．

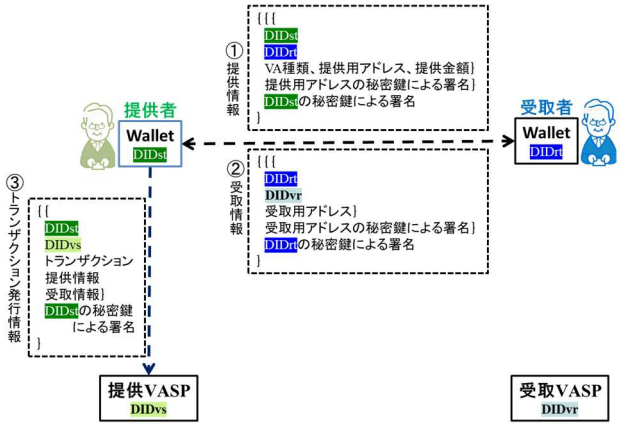

図６　利用者間情報交換（トランザクション構成）

3.2.3 VASP 間情報交換

トランザクション発行情報を受け取った提供 VASP は，トランザクションが適切に構成されていることを確認，更に関係する利用者が身元確認済利用者であることの確認，提供用アドレスや受取用アドレスがそれぞれ提供者および受取者のアドレスであることの確認等を行い，その上で受取 VASP へトランザクション発行情報を送信する．

なお，提供 VASP は受取 VASP へ情報を送信する前に，受取 VASP が信頼できるかどうかを，VASP DID VDR を使用し確認する．

提供 VASP よりトランザクション発行情報を受け取った受取 VASP は，まず提供 VASP が信頼できるかどうかを，VASP DID VDR を使用し確認する．その後，受取 VASP もトランザクションが適切に構成されていることを確認，更に関係する利用者が身元確認済利用者であることの確認，提供用アドレスや受取用アドレスがそれぞれ提供者および受取者のアドレスであることの確認等を行い，提供 VASP へ確認結果を通知する．

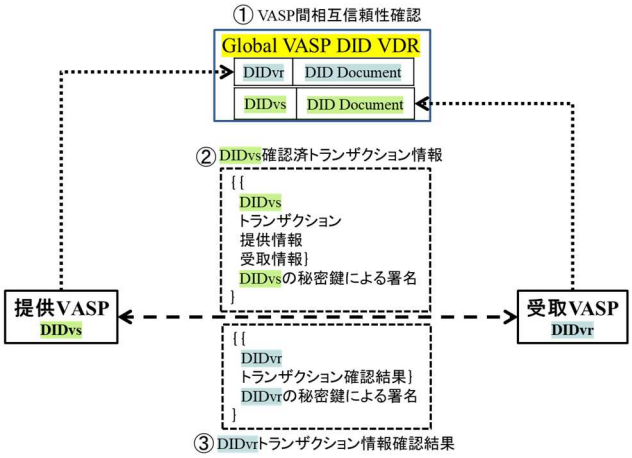

図７　VASP 間情報交換

3.2.4 トランザクション登録

提供 VASP は，受取 VASP の確認終了後，対応する暗号資産システムへ，提供 VASP の署名付きでトランザクションを発行する．

暗号資産システム側では，署名を付与した提供 VASP の信頼性の確認を含め，トランザクション承認処理を実施し，承認後，トランザクション ID を提供 VASP へ通知する．

提供 VASP は，そのトランザクション ID を受取 VASP へ連絡すると共に，登録トランザクション情報を登録する．受取 VASP もトランザクション ID の連絡を受けた後，登録トランザクション情報を登録する．

以上の処理により，トランザクションの登録手続きが完了し，以降，VASP は登録利用者情報および登録トランザクション情報を管理する．

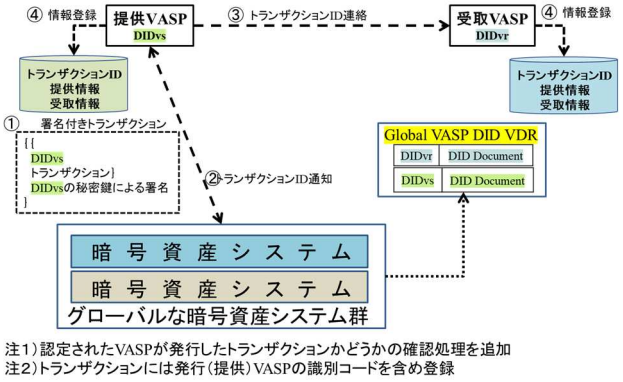

図８　トランザクション登録方式―１
（VASP 組織識別コードによる利用者の特定・追跡）

3.2.5 不審なトランザクションの調査・捜査

SSVATF では暗号資産システムにてトランザクションを発行した VASP の DIDvs が登録されていることを前提としており，不審なトランザクションの調査・捜査が必要な場合，調査・捜査機関は暗号資産システムのブロックチェーンよりそのトランザクションを発行した VASP の DIDvs を特定する．

調査・捜査対象のトランザクションを発行した DIDvs に対応する DID Document よりそのトランザクションを発行した VASP を特定・追跡し，その上で，その VASP に調査・捜査対象のトランザクション ID に対応する登録トランザクション情報の開示を求める．VASP は開示要請が合法的なものであれば開示に応じ，調査・捜査機関はそのトランザクションの提供者の利用者識別コード DIDst や受取者の利用者識別コード DIDrt を特定することができる．更に，DIDst および DIDrt に対応する DID Document よりそれぞれの VASP を特定・追跡し，VASP の協力を得，提供者および受取者の NAF-ID と連結された個人識別コード DIDs および DIDr 入手する．

調査・捜査機関は，入手した DIDs，DIDr から SDIP の協力により，提供者および受取者のそれぞれの NAF-IDp を入手でき，その NAF-IDp から認証基盤（NAF）の協力により，提供者および受取者の身元情報を入手，調査・捜査が可能となることを想定している．

3.3 SSVATF 考察

本節では，前節で記載した SSVATF における暗号資産移転の仕組みについて，3.1 節で述べた構想策定基本方針の観

点から考察する．

①VASP による利用者の確実な身元確認

SSVATF では，身元確認は各国の認証基盤 NAF の身元確認結果を利用する．VASP が直接身元確認を行わないことにより，利用者の個人情報の入手・確認・管理を不要とし，更に各国の制度として構築・運用されている信頼できる認証基盤を利用することにより，利用者が確実な身元確認済であることを確認でき，必要な場合の利用者の特定・追跡も可能となる．

②資産移転における確実な匿名性の確保

SSVATF で取り扱う情報は，利用する暗号資産システムのトランザクション発行に必要な情報を含め，利用者は利用者識別コード DIDut で表現され，一定の匿名性を確保している．

③不正・不法な利用者の確実な特定・追跡

暗号資産システムのブロックチェーンに登録されている不審なトランザクションの調査・捜査は，トランザクション・データに含まれるそのトランザクションを登録した VASP の DIDvs からその VASP を特定でき，その VASP が管理するトランザクション情報から利用者（提供者および受取者）の DIDst，DIDrt を確認でき，その DIDst，DIDrt から発行した VASP を特定でき，その VASP が DIDst，DIDrt 発行に利用した個人識別コード DIDs，DIDr を発行した SDIP を特定でき，更にその SDIP が管理する個人識別コード DIDs, DIDr のそれぞれに対応する NAF-IDp を特定でき，最終的にその NAF-IDp を利用し認証基盤 NAF から利用者の名前や住所等の身元情報を確認することができ，必要な場合の利用者の特定・追跡性が確保されている．

以上のような連結可能匿名化の連鎖をさかのぼるには，それぞれ連結可能情報を管理する事業者・組織の協力が不可欠であり，合法的な捜査・調査が大前提である．しかし，海外の事業者・組織の協力を得るには，一般にはその国の調査・捜査機関経由の要請となり，法体系の異なる海外の利用者の特定・追跡には各国間の調査・捜査に関する協力が必要である．

④個人情報・プライバシー情報の開示先・範囲の最少化

SSVATF における暗号資産移転のフェーズでは，個人情報・プライバシー情報は一切取り扱わず，原則開示も必要ない．しかし，各国の規制やガイドラインにより移転資産額・移転先（海外）等に応じ，しかるべき機関・組織へ個人情報・プライバシー情報を含め資産移転内容の報告をする義務が発生する場合もある．

個人情報・プライバシー情報を含む暗号資産移転の報告を求められる場合も，報告者（提供者または受取者）は，認証基盤から発行される VC（Verifiable Credential）の選択開示による身元情報，および暗号資産移転にかかわる情報を暗号化し報告先のみが内容を復号できる VP（Verifiable Presentation）の発行により，個人情報・プライバシー情報の開示先・範囲の最少化は実現できるものと想定している．なお，報告先が，暗号資産の移転にかかわる VASP 経由の報告を求める場合も，VC/VP の利用により，個人情報・プライバシー情報の開示先・範囲の最少化は実現できるものと想定している．

SSVATF では，利用者の個人情報・プライバシー情報の開示先・範囲の最少化には，W3C で標準化が進められている DID([36])，VC/VP([37])の利用を想定している．

⑤各種暗号資産システムとの連携

VASP がトランザクションに付与する署名で，SSVATF の VASP が発行したトランザクションであること，利用者の本人確認と利用者の特定・追跡のための情報保存を行った上でのトランザクションであることを，暗号資産システムのトランザクション承認の条件の一つに加えられることを想定している．

また，トランザクションを発行した VASP の識別コード DIDos をブロックチェーンのトランザクション・データに加えられることを想定している．不審なトランザクションを検知した場合，そのトランザクションの情報から発行した VASP を特定し，その VASP の情報から利用者の特定・追跡を可能とするためである．

なお，トランザクション・データに発行した VASP の識別コード DIDos を加えることが難しい場合は，次図のように，Global トランザクション ID VDR へ必要情報を登録，犯罪捜査機関や金融情報調査機関がアクセス可能とすることにより，利用者の特定・追跡が可能である．

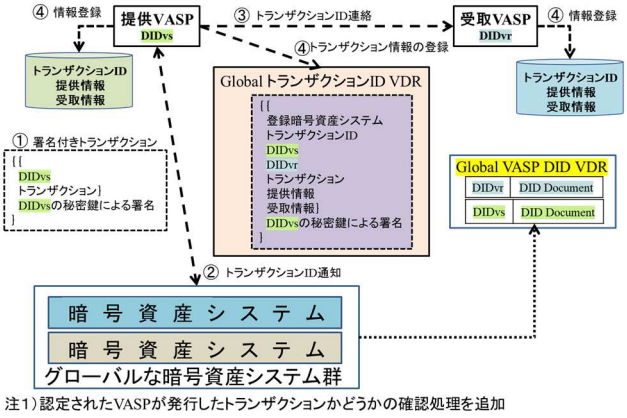

図９　トランザクション登録方式―２
（トランザクション ID による利用者の特定・追跡）

4. おわりに

暗号資産の悪用の急増，安心・安全な社会への脅威の増大，その対応策としての FATF トラベルルールの課題を憂慮し，安心・安全で公正・公平な暗号資産の利活用環境を構築するための仕組み SSVATF を提案した．

SSVATF はまだ構想段階であり詳細仕様を詰める必要があるが，その実現は開発技術面よりも社会実装面の課題が多い．

その一つの課題は，そもそも SSVATF が FATF トラベルルールに準拠していないこと，である．FATF トラベルルールでは従来の金融機関と同様，実名・住所等の個人情報の確認・保存を規定しているが，SSVATF では，個人情報・プライバシー情報の保護を重視し，VASP における利用者情報の確認・保存においても仮名である DID のみを使用する仕組みである．今後，トラベルルールにおける個人情報・プライバシー情報の扱いに関する各国の議論の推移を当面は見守りたいが，長期的に改定の可能性が無いようであれば，トラベルルールに準拠しつつ，VASP における個人情報・プライバシー情報の保護の仕組みを強化した SSVATF も検討し，SSVATF の社会実装を目指したい．

もう一つの課題は，暗号資産業界の負担増への理解，である．暗号資産は従来の金融サービスに比べ様々の利点があり，具体的には利用者の強い匿名性と取引・送金の低コスト等がある．しかし，そのための犯罪の増加やその対策のための社会コストは甚大で，その犯罪被害や対策コスト負担を社会に押し付けている状況は放置されるべきではない．暗号資産業界としての適切な対応により社会への負担を早期に軽減させることが求められている．

暗号資産業界が，単にサービス事業者と利用者の観点のみではなく，安心・安全で公正・公平な社会を維持可能な，社会的責任を果たしうる自律可能な健全な業界として，発展を期待したい．

謝辞　本研究の一部は，一般財団法人テレコム先端技術研究支援センターの研究助成を受けている．

参考文献

[1] 才所敏明，櫻井幸一，辻井重男，“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　―”，第 97 回コンピュータセキュリティ研究会（CSEC97）

[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（２）”，第 94 回コンピュータセキュリティ研究会（CSEC94）

[3] 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（ICSS54）．

[4] 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）．

[5] 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）．

[6] 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．

[7] 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）

[8] 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）．

[9] 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.

[10] 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）．

[11] 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）．

[12] 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）．

[13] 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）．

[14] 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（CSEC85），2019.

[15] 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.

[16] 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

[17] Chainalysis，“The 2022 Crypto Crime Report”
https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

[18] 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

[19] 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

[20] CipherTrace，“Cryptocurrency Crime and Anti-Money Laundering Report, May 2021”，2021.
https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-may-2021/

[21] 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

[22] 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

[23] 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

[24] 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

[25] 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
[26] 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
[27] 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
[28] EUROPOL, “INTERNET ORGANISED CRIME THREAT ASSESSMENT”, 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
[29] 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
[30] 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
[31] TRISA, “Travel Rule Information Sharing Architecture for Virtual Asset Service Providers”, 2020. https://trisa.io/trisa-whitepaper/
[32] OpenVASP, “Travel Rule Protocol”, 2021. https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/7c38b8c98ca7bc57bf368f98d5825699fa4f85e2/core/specification.md
[33] Joint Working Group on interVASP Messaging Standards, “interVASP Messaging Standards”. https://intervasp.org/
[34] 21 Analytics, “Address Ownership Proof Protocol (AOPP). https://aopp.group/index.html
[35] Thomas Hardjono, “Attestation Infrastructures for Private Wallets”, 2021. https://arxiv.org/abs/2102.12473
[36] W3C, “Decentralized Identifiers (DIDs) v1.0”, 2022. https://www.w3.org/TR/did-core/
[37] W3C, “Verifiable Credentials Data Model v1.1”, 2022. https://www.w3.org/TR/vc-data-model/
[38] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf
[39] Mastering Bitcoin https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
[40] Stefano Bistarelli, Ivan Mercanti, Francesco Santini, "An Analysis of Non-standard Transactions", 2019. https://www.frontiersin.org/articles/10.3389/fbloc.2019.00007/full
[41] Monero : Privacy in the blockchain v1.0 https://eprint.iacr.org/2018/535.pdf
[42] Zero to Monero: First Edition https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
[43] Mastering Monero https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf
[44] Zcash Protocol Specification https://www.btrade.co.kr/btrade_res/20180507145055652.pdf
[45] Grin Whitepaper https://www.allcryptowhitepapers.com/grin-whitepaper/
[46] Serguei Popov, “The Tangle”, April 30, 2018. Version 1.4.3. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
[47] Anton Churyumov, “Byteball: A Decentralized System for Storage and Transferof Value”, 2016. https://obyte.org/Byteball.pdf
[48] Colin LeMahieu, “Nano: A Feeless Distributed Cryptocurrency Network”, 2018. https://nano.org/en/whitepaper
[49] Leemon Baird, Mance Harmon, Paul Madsen, “Hedera: A Public Hashgraph Network & Governing Council”, 2019. https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf
[50] 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
[51] DERO PROJECT WHITE PAPER, 2018. https://dero.io/attachment/Whitepaper.pdf
[52] Tangram: An Introduction, 2018. https://tangrams.io/wp-content/uploads/2018/12/Tangram_An_Introduction-2018-12-19-03-27.pdf
[53] CoinMarketCap, https://coinmarketcap.com/ja/all/views/all/
[54] data.bitcoinity.org, https://data.bitcoinity.org/markets/volume/30d?c=e&t=b
[55] yahoo finance, https://finance.yahoo.com/
[56] Nicolas van Saberhagen, "CryptoNote v2.0", 2013. https://cryptonote.org/whitepaper.pdf
[57] Andrew Poelstra, “Mimblewimble”, 2016. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[58] Gregory Maxwell, “CoinJoin: Bitcoin privacy for the real world”, 2013. https://bitcointalk.org/index.php?topic=279249.0
[59] Gregory Maxwell, Andrew Poelstra, ”Borromean Ring Signature”, 2015. https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
[60] SHEN NOETHER, “RING CONFIDENTIAL TRANSACTIONS”, 2015. https://eprint.iacr.org/2015/1098.pdf
[61] 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
[62] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, “Pinocchio: Nearly Practical Verifiable Computation”, 2013. https://eprint.iacr.org/2013/279
[63] Christina Garman, Matthew Green, Ian Miers, ” Accountable Privacy for Decentralized Anonymous Payments”, 2016. https://eprint.iacr.org/2016/061.pdf

【 この位置に改ページを入れ, 以降のページを印刷対象外とする 】