【金融庁ブロックチェーン国際共同研究プロジェクト】

金融庁　御中

「分散型金融システムにおけるオンチェーン／オフチェーンデータを活用した実態把握に関する研究」 研究結果報告書

令和５年６月

株式会社クニエ

研究の目的・背景

- 分散型金融システムにおいては、利用者保護や金融犯罪防止、金融安定等の観点から多くの課題が指摘されており、技術革新による果実を享受するためには、これらのリスクを低減することが欠かせない。各種リスクへの対応を検討するに当たっては、客観的かつ信頼できるデータを活用したリスク評価が重要になると考えられるが、FSBやFATF等の報告書においてデータギャップの問題が指摘されているように、DeFiやP2Pを含む分散型金融システムの実態把握に必要なデータの不足が指摘されており、必ずしも十分なリスク評価が行うことが出来ていないとの指摘もある。

- そこで、本調査研究では、金融庁の「ブロックチェーン国際共同研究」の一環として、 DeFiやP2Pを含む分散型金融システムのオンチェーン／オフチェーンデータを活用した実態把握に関する調査を実施する。分散型金融システムにおいては、ブロックチェーン上の取引記録などのオンチェーンデータに加えて、IPアドレスやウェブトラフィック、制裁関連情報などのオフチェーンデータとブロックチェーンアドレスを紐づけることで、より深度あるデータが入手可能となる。当該オンチェーン／オフチェーンデータについて、公知情報やブロックチェーン分析ツール、専門家によるリサーチなどにより調査を行いデータの取得可否を含めた実態を把握し、今後の政策対応を検討する上で有益な視座を提供することを目的に、本調査研究を実施する。

※今回利用したブロックチェーン分析ツール等で解析が行えるアドレス・取引は全体のごく一部に留まっており、必ずしも分散型金融システム全体のデータを分析したものではないことに留意。（詳細は後述）

謝辞・免責事項

謝辞

- 本報告書作成にあたっては、京都大学・岩下直行教授、早稲田大学・佐古和恵教授、米ジョージタウン大学・松尾真一郎研究教授から有益な助言やコメントを得た。また、デジタル庁・日本銀行のオブザーバー及び金融庁のご担当者からも有益な示唆・助言をいただいた。
- もっとも、本報告書に関する内容の誤りは、すべて受託者である株式会社クニエに帰する。

免責事項

- 本報告書の内容は金融庁の公式見解を示すものではない。
- 本報告書で記載している過去または現在の事実以外の内容については、本稿執筆時点で入手可能な情報に基づいた見通しであり、実際の動向等は種々の不確定要因によって変動する可能性がある。

目次

用語集

※ 本報告書中の一部の用語については、定まった定義が必ずしも存在せず、また分析ツール会社間でも定義に差異がある。これらの用語については、今回採用したブロックチェーン分析ツールの定義も踏まえて規定したものであることに留意。

用語	定義
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism マネー・ローンダリング及びテロ資金供与対策
DeFi	Decentralized Finance スマートコントラクトを活用して提供される金融サービスの総称
DEX	Decentralized Exchange 分散型取引所（DeFiの一類型）
EOA	Externally Owned Account 外部所有アカウント：秘密鍵で管理され、ネイティブトークンや他のトークンの送受信およびスマートコントラクトのデプロイ・実行ができるEthereumブロックチェーン上のアカウント
FATF	Financial Action Task Force 金融活動作業部会
FSB	Financial Stability Board 金融安定理事会
KYC	Know Your Customer 顧客確認のプログラム
P2P	Peer to Peer (Transaction) アンホステッド・ウォレットを用いた取引（当報告書では、アンホステッド・ウォレット間の取引とする）
TVL	Total Value Locked DeFiに預けられた（スマートコントラクトにロックされた）暗号資産の総額
VASP	Virtual Asset Service Provider 暗号資産の交換やホステッド・ウォレットなどを提供している業者

用語集

用語	定義
オンチェーンデータ	• ブロックチェーン上で取得できるデータ（アドレス、取引履歴、残高、その他スマートコントラクトの状態など）
オフチェーンデータ	• オンチェーンデータ以外のデータ ※当報告書では、Ethereumブロックチェーンのレイヤー2（Arbitrumなど）はオフチェーンデータとする
BCエクスプローラー	• 当報告書では、Webサイトで公開されているブロックチェーンデータ分析サイトを指す。（Etherscan、Dune Analyticsなど）
暗号資産関連データベース	• 当報告書では、Webサイトで公開されている暗号資産マーケット情報サイトを指す。（CoinGecko、Coinmarketcapなど）
ブロックチェーン分析ツール	• ブロックチェーン分析会社が提供する分析ツール • オンチェーンデータの照会・検索、ブロックチェーン分析会社が特定した一部のアドレスのカテゴリ名やアカウント名などの情報、高リスクアドレスの取引などのデータが取得できる
高リスクアドレス	• 当報告書では、特定のブロックチェーン分析会社が下記の情報を基にリスク値を100段階で計算し、80以上のスコアになったものを「高リスクアドレス」とする ➢ 詐欺やハッキングに使用されたアドレス ➢ 公的機関の制裁リストに掲示されたアドレス ➢ 他のブロックチェーン分析会社からの情報 ➢ ブロックチェーン会社内部の調査情報 ➢ Open Source Intel (OSINT)からの情報
高リスク取引	• 取引の送信側または受信側、あるいはその両方が高リスクアドレスの取引
スマートコントラクト	• ブロックチェーンに書き込まれ、トランザクションを通して機能が呼び出された際に自動的に実行されるルールを定めたプログラム

用語集

用語	定義
トークンコントラクト	• スマートコントラクトのうち、ERC-20規格などに準拠するトークン（USDC/USDT等）の発行量・所有者・残高などを管理するもの • トークンの送金に伴い所有者・残高などが更新される※1
オラクルコントラクト	• スマートコントラクトのうち、オフチェーンの外部データを取得するためのデータフィードを行うもの • 主に価格オラクルとして外部の市場価格や利率を取得するために使用されている※2
コントラクトアカウント	• デプロイされたスマートコントラクトのアカウント • EOAや他のコントラクトアカウントからのメッセージ受信に応答してスマートコントラクトが実行される※3
トランザクション	• EOAによって開始されるデジタル化された署名付きのアクション • Ethereumにおいてはトークンの送金、スマートコントラクトのデプロイ、またはスマートコントラクトの機能の呼び出しを行う※4
ブロック	• ブロックチェーン内の１つ前のブロックのハッシュ（暗号学的ダイジェスト）とトランザクションを含むデータ • Ethereumブロックチェーン上でランダムに選択されたバリデータによりブロックが生成される※5
ブリッジ	• クロスチェーンブリッジとも呼ばれ、異なるブロックチェーンを相互に接続してトークンなどを送信する方法を提供する機能・サービスの総称 • 異なるブロックチェーン間で送信するトークンが異なる場合は、一般に、ブリッジに送信元ブロックチェーンのトークンをロック（凍結）し、送信先ブロックチェーンのトークンに交換して送信する※6
ホステッド・ウォレット	• VASP等が提供するウォレット • 利用者は秘密鍵の管理をVASP等（ウォレット管理者）に委託しており、利用者の暗号資産の移転取引等をVASPが介入して実行することができる
アンホステッド・ウォレット	• VASPなどを通さず、利用者が秘密鍵を直接管理するウォレットで、利用者は一般に暗号資産の移転取引等を直接実行できる

※1：Ethereum.org ERC-20 TOKEN STANDARD https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
※2：Ethereum.org ORACLES https://ethereum.org/en/developers/docs/oracles/
※3：Ethereum.org ETHEREUM ACCOUNTS https://ethereum.org/en/developers/docs/accounts/
※4：Ethereum.org TRANSACTIONS https://ethereum.org/en/developers/docs/transactions/
※5：Ethereum.org BLOCKS https://ethereum.org/en/developers/docs/blocks/
※6：Ethereum.org BRIDGES https://ethereum.org/en/developers/docs/bridges/

第１章　分散型金融システムにおけるデータ分析の必要性

第１章 分散型金融システムにおけるデータ分析の必要性

- 本章では、金融当局の観点から分散型金融システムの実態把握において必要とされるデータの類型と、その取得可能性について整理を行う。特に、FSB報告書やFATF報告書で指摘されているデータギャップに関する指摘などを整理の起点とする。
- 本章は次のように構成される。
  - 1-1では、FSB報告書で指摘されているデータギャップの要因と利用可能／不可能なデータ及び追加取得すべきデータ例を説明する。
  - 1-2では、FATF報告書で指摘されているブロックチェーン分析会社によるP2P取引の実態調査結果、AML/CFTの暗号資産関連データの特定におけるレッドフラッグのデータ例を説明する。

1-1. FSB報告書におけるデータギャップ問題

（１）FSB報告書の指摘

- DeFiの金融安定上のリスク等について指摘した報告書（2023年2月公表）において、DeFiを含む暗号資産市場におけるデータの透明性及び一貫性の欠如の問題を指摘している。（下記表を参照）
- 今後、基準設定主体（SSBs）及び規制当局と協働し て、DeFiとの相互連関性を測定及び監視するために データギャップを埋めるアプローチを検討するとしている。

表1-1-1　FSB報告書におけるデータギャップ要因

データギャップ要因	具体的内容
分散型台帳上で利用可能な膨大な量のデータの集約と分析の難しさ	• 公開ブロックチェーンから得られるデータは、ある面では透明で不変である一方で、一般的にはその膨大な量の影響で収集と分析が困難である。
公開台帳上の情報が匿名である	• ウォレットレベルの取引データにはアクセス可能だが、ウォレット所有者の身元に関するデータがないため、脆弱性の評価が非常に困難である。 • 様々なプライバシー強化技術（ウォレットミキサー/タンブラー/匿名性強化暗号資産など）が存在し、特定のユーザーによって取引の透明性を曖昧にすることができる。
オフチェーンデータの多さ	• DeFiを含む暗号資産市場におけるデータにはオフチェーンデータが多く存在することから、オンチェーンデータだけでは、市場の活動全体をイメージすることが難しい。
規制に基づく一貫したデータの報告義務がない	• 暗号資産エコシステムの一部が、現時点では規制の枠外にある、または規制を遵守していないため、一貫性のある信頼できるデータを作成し報告する義務がない、または義務を遵守していない。
データプロバイダによるデータ操作の可能性	• 一部のデータプロバイダが、それぞれのプラットフォームをより重要なものに見せ、追加の取引件数または投資を引き付けるために、データを操作するインセンティブを受ける可能性がある。取引・融資プラットフォームに対する市場のインセンティブは、既存の規制の枠組みを逸脱し、または遵守せずに行動する参加者と相まって、市場操作やデータ改ざんのリスクを増大させる。

出典：FSB, The Financial Stability Risks of Decentralized Finance, February 2023, https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/

1-1. FSB報告書におけるデータギャップ問題

（２）FSB報告書の指摘（データ例）

- FSBが指摘する、利用可能／不可能なデータは以下のとおり。
- 本調査研究は、これらの指摘も踏まえて取得することが望ましいデータセットを特定し、ブロックチェーン分析ツールを用いて各々のデータの取得可否及びその信頼度を検証する。

表1-1-2-1　裏付資産のない暗号資産のデータギャップ

伝達チャネル	利用可能なデータ	利用できないデータ
資産効果	・暗号資産の時価総額 ・取引件数 ・実現ボラティリティ ・地域ごとの普及状況	・暗号資産に投資をしている世帯の割合 ・家計資産に対する割合 ・暗号資産保有の世帯間の偏り ・暗号資産の保有者
市場信頼性	・暗号資産のリテールの保有割合 ・暗号資産関連のインフラ（取引プラットフォーム、ウォレット提供者等）にアクセスできるユーザー数	・不正取引被害総額
金融機関へのエクスポージャー	・暗号資産の機関投資家の保有割合 ・暗号資産への投資割合 ・暗号資産関連サービスを提供している主要な金融サービス提供者数 ・暗号資産のデリバティブマーケットの規模 ・暗号資産のデリバティブ契約の建玉 ・暗号資産と他の資産クラスとの相関 ・取引規模ごとの取引件数分布	・暗号資産に投資しているファンドの保有割合と運用資産残高（スポット、デリバティブ、エコシステム、投資家の属性ごと） ・銀行セクターへのエクスポージャー ・暗号資産の保有/サービス提供にかかる金融機関による報告
決済利用	・価格とデルタ (1w, 1m, 3m, 6m, 1y, ...) ・取引件数 ・暗号資産決済サービスの提供者数 ・主要な暗号資産取引所の市場占有割合	・取引数と額 ・支払人と受取人の法域 ・取引形態（例えば、送金、電子商取引、貿易） ・採用されている暗号資産の種類 ・法定通貨としての受け入れ状況

出典：FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

1-1. FSB報告書におけるデータギャップ問題

（２）FSB報告書の指摘（データ例）

表1-1-2-2　ステーブルコインのデータギャップ

伝達チャネル	利用可能なデータ	利用できないデータ	追加すべきデータ（有識者の指摘事項）
資産効果	・ステーブルコインの時価総額 ・取引件数 ・実現ボラティリティ	・ステーブルコインの保有者	・ステーブルコインの発行主体とVASPとの取引関係
市場信頼性	・ステーブルコインのリテールの保有割合 ・ステーブルコインのインフラ（取引プラットフォーム、ウォレット提供者等）にアクセスできるユーザー数	・不正取引被害総額	・凍結対象アドレス ・凍結対象額合計
金融機関へのエクスポージャー	・ステーブルコインの機関投資家の保有割合 ・ステーブルコインへの投資割合 ・ステーブルコイン関連サービスを提供している主要な金融サービス提供者数 ・米国MMFと比較したステーブルコインの市場規模	・ステーブルコインに投資しているETFの保有割合や残高（スポット、デリバティブ、エコシステム、投資家の属性ごと） ・銀行セクターへのエクスポージャー ・規制市場に投資している裏付資産 ・裏付資産の流動性 ・裏付資産の構成の詳細 ・暗号資産の保有/サービス提供にかかる金融機関による報告	・機関投資家や金融機関の暗号資産取引実態（大口ユーザーが選好する暗号資産／ステーブルコインの種別など）
決済利用	・価格 ・取引件数 ・ステーブルコイン決済サービスの提供者数	・取引数と額 ・支払人と受取人の法域 ・取引形態（例えば、送金、電子商取引、貿易） ・ステーブルコインの取引プラットフォームでの利用方法 ・ステーブルコインの用途の内訳	－

出典：FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

1-1. FSB報告書におけるデータギャップ問題

（２）FSB報告書の指摘（データ例）

表1-1-2-3　DeFiのデータギャップ

伝達チャネル	利用可能なデータ	利用できないデータ	追加すべきデータ（有識者の指摘事項）
資産効果	・TVL ・DEXの取引件数 ・ウォレットの成長率 ・ガバナンストークンの時価総額と取引件数 ・DeFiレンディングの取引件数と貸出金利 ・DeFiレンディングと取引所の流動性プールの利用率 ・DeFiの利回りと利益	・リテールと機関投資家の参加者割合 ・DAppsの数 ・DeFi内のエンティティ（DeFiと伝統的な金融機関とのリンク） ・レバレッジ ・ガバナンストークンの保有者情報（どの程度分散されているか。例えば、ガバナンストークンが集中しているエンティティは開発者であると推測可能。）	・TVL（主要DeFiプロトコルのTVLベースのマーケットシェア） ・ステーブルコインの時価総額 ・主要DeFi間の連関度合い（DEX-Lending等） ・クロスチェーンブリッジのロックされているトークン総額 ・クロスチェーンブリッジのVASPとの取引関係 ・TVL等の尺度でオラクルのマーケットシェア ・レンディングプロトコルの担保種別に応じた担保比率、レバレッジ比率、リハイポセケーションの実態 ・トレジャリープロトコルからの主な送金先アドレス
市場信頼性	・DeFi関連のインフラ（取引プラットフォーム、ウォレット提供者等）にアクセスできるユーザー数	・不正取引被害総額 ・裏付資産のない暗号資産とステーブルコインの取引割合	・ガバナンストークンの集中度 ・DeFiプロトコルの集中度 ・DeFi関連のハッキング被害総額、件数
金融機関への エクスポージャー	・機関投資家の保有割合 ・暗号資産の資産割合 ・暗号資産関連サービスを提供している主要な金融サービス提供者数 ・デリバティブマーケットの規模 ・デリバティブ契約の建玉 ・暗号資産と他の資産クラスとの相関 ・取引規模ごとの取引件数分布	・暗号資産に投資しているETFの保有割合や残高	・担保としてスマートコントラクトにロックされたトークンを活用した伝統的金融資産への投資額
決済利用	・価格（DOT, UNI, LINK） ・デルタ（1w, 1m, 3m, 6m, 1y）	・取引数と額 ・支払人と受取人の法域 ・取引形態（例えば、送金、電子商取引、貿易）	–

出典：FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

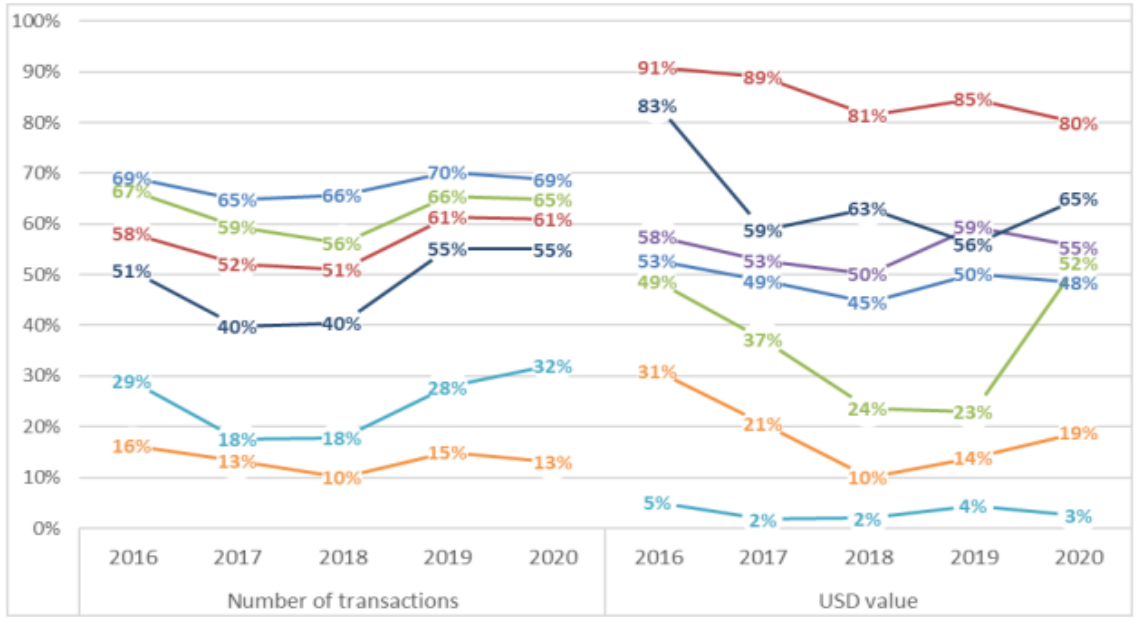
1-2. FATF報告書におけるデータギャップ問題

（１）FATF報告書の指摘（P2P取引）

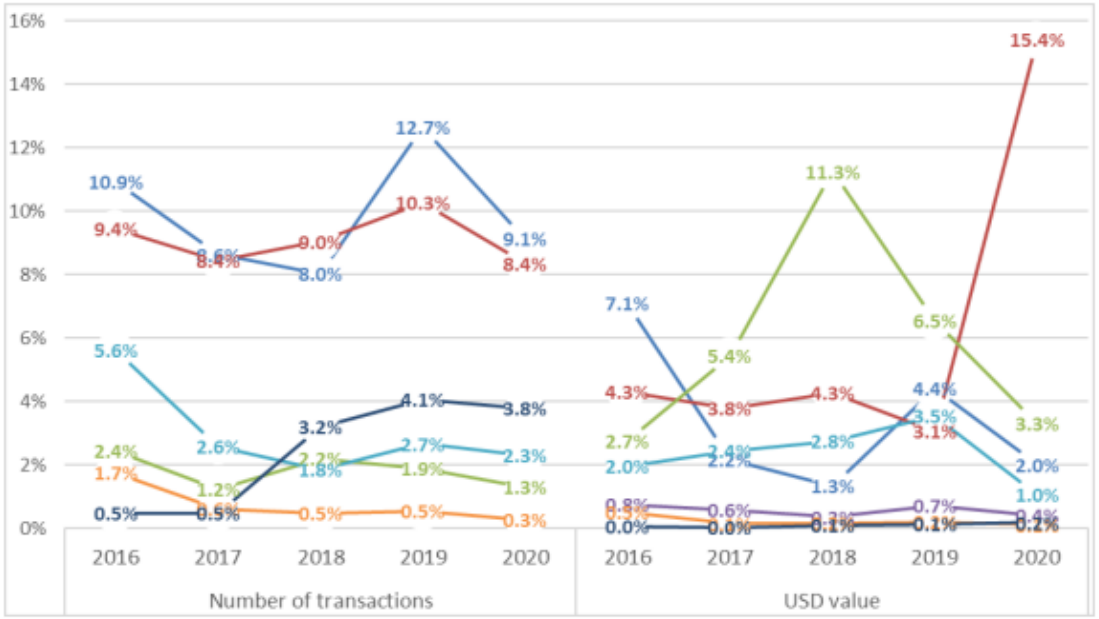
- 2021年7月のFATF報告書では、複数のブロックチェーン分析会社によるP2P取引の実態調査結果（P2P取引の全体に占める割合等）に大きな結果のばらつきがあったことが報告されている。
- 2016年から2020年にかけてVASPを介さずに発生したビットコイン取引の割合について、取引件数では4社が40～70%との分析に対して、2社は10%~32%と分析している。また、取引額（米ドル）について、各社の分析結果が2%～91%と大きなばらつきが存在している（Graph 2）
- 2016年～2020年の間に確認された不正なビットコイン取引の割合は、取引件数では0.3%～12.7%、取引額（米ドル）では0%～15.4%のばらつきが存在している（Graph 3）

図1-2-1　FATF報告書のP2P取引・不正取引実態調査結果の例

Graph 2: Proportion of bitcoin transactions which occur without a VASP between 2016-2020 (left: number of transactions;12 right: USD value13)



Graph 3: Proportion of identified illicit bitcoin transactions between 2016-2020 (left: number of transactions[15]; right: USD value[16])



出典：FATF, Second 12-Month Review of the Revised FATF Standards on Virtual Assets/VASPs, July 2021, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html

1-2. FATF報告書におけるデータギャップ問題

（２）FATF報告書の指摘（AML/CFT関連）

- 2020年9月のFATF報告書では、マネーロンダリング、テロ資金提供者、その他の犯罪者が規制された金融システムの外側でデジタル的に資産を取得、移動、保管できるだけでなく、資金の出所や行き先を難解にし、報告主体が疑わしい活動を適時に特定することが難しいこと指摘している。
- 上記の指摘も踏まえて、VASPなどを含む報告主体が、暗号資産に関連する潜在的なMLおよびTF活動を特定し報告する事を支援する為、暗号資産に関連するML/TFのレッドフラッグに関するレポートを発表している。

表1-2-2　AML/CFTにおける暗号資産関連データ特定の問題

レッドフラッグ	具体的内容
取引に関するレッドフラッグ（取引の規模及び頻度）	• 記録管理や報告の閾値に満たない金額での暗号資産取引（交換や送金など） • 複数の高額取引を24時間以内など短時間で連続して取引する場合 • 新しく作成されたアカウントまたは非アクティブだったアカウントに対して複数の高額取引を行う場合　など
取引パターンに関するレッドフラッグ	• 新規ユーザが暗号資産の全残高を取引するか、暗号資産を引き出してプラットフォームから全残高送金する場合 • 特定の期間（1日、1週間、1か月など）に複数の人が同じ暗号資産アカウントに頻繁に送金する場合　など
匿名性に関するレッドフラッグ	• ミキシング、タンブリングサービスやP2Pプラットフォームを利用したことがあるwalletとの間で暗号資産がやり取りされた場合 • ダークネットマーケットプレイス、疑わしいギャンブルサイト、違法行為（ランサムウェアなど）や盗難報告など、既知の疑わしい情報源への直接的・間接的な関連を含む、暗号資産アドレスまたはwalletからの入金や出金をする場合 • 顧客管理（CDD）や本人確認（KYC）プロセスがないもしくは不十分なVASPからの資金授受を行う場合　など
送信者または受信者に関するレッドフラッグ	• ユーザの暗号資産アドレスが違法行為に関連する公開掲示板に表示されている場合 • 過去に犯罪に関与したことがあり、公開されている情報を通じて法執行機関に知られているユーザ　など
資金の源泉に関するレッドフラッグ	• 詐欺・恐喝、ランサムウェアスキーム、制裁対象のアドレス、ダークネットマーケットプレイス、またはその他の違法なWebサイトに関連する暗号資産アドレスでの取引 • オンラインギャンブルサービス経由の暗号資産取引　など
地理的リスクに関するレッドフラッグ	• ユーザの資金が、ユーザまたは取引所が所在する法域に登録されていない取引所から送金された場合 • 注意が必要な法域の暗号資産取引所を利用している場合（暗号資産事業体へのAML/CFT対策が不十分であることによるリスク）など

出典：FATF, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

第２章　オンチェーン／オフチェーンデータのマッピング

第２章 オンチェーン／オフチェーンデータのマッピング

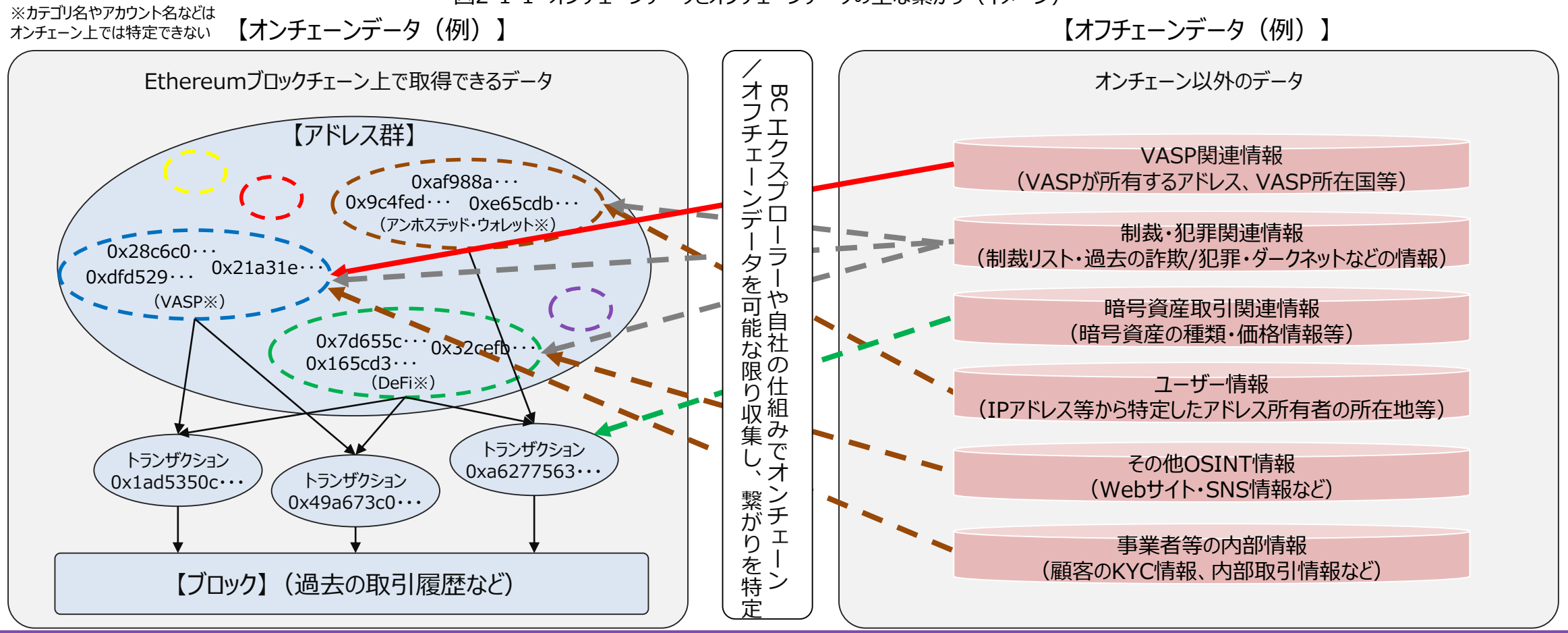
- 分散型金融システムにおけるデータ分析を行うためには、オンチェーンで取得できるウォレットアドレスやトランザクションIDといった数字・文字のランダムな羅列だけでは限界があり、これらのオンチェーンデータと、ウォレットの所有者などのブロックチェーン外のデータ（オフチェーンデータ）を結びつけて取引関係等の実態を把握していく必要がある。そこで、本章では、オンチェーン／オフチェーンデータの概要と構成要素の整理、また両データのマッピングを試みた。
- 具体的には、Ethereumブロックチェーン上で取得できるオンチェーンデータと、それ以外のオフチェーンデータについて、その要素と繋がりについて整理した。これを踏まえ、オンチェーン／オフチェーンデータの全体像のマッピングを行った。
- 本章は次のように構成される。
  - 2-1では、オンチェーン／オフチェーンデータの構成要素について説明する。
  - 2-2では、オンチェーン／オフチェーンデータのマッピングについて説明する。

2-1. オンチェーン／オフチェーンデータの繋がりと構成要素

（１）オンチェーン／オフチェーンデータの接続

- ブロックチェーン分析会社は一般に、オープンソース及び独自のツール・ノウハウを活用してオンチェーンデータとオフチェーンデータの双方を収集し、関連するアドレスのグループ化やアドレスへのラベル付け（例えば特定のVASPが管理しているアドレスの一群に対して当該VASPのアカウント名を付与するなど）、アドレスのリスクスコア算出などを行なっている。
- 下記は、ブロックチェーン分析ツール会社が収集している各種データと、それらの繋がりの一端を示したイメージ図である。

図2-1-1　オンチェーンデータとオフチェーンデータの主な繋がり（イメージ）



2-1. オンチェーン／オフチェーンデータの繋がりと構成要素

（２）オフチェーンデータの要素

- オンチェーンデータに紐づくオフチェーンデータの要素は以下が考えられる。（オンチェーンデータは用語集で定義しているため説明は省略）

  ※ 本ページでは各データの取得可能性は論じておらず、表は一般に存在すると考えられるオンチェーンデータのうち主要なものを抽出したもの。

- 各々のオフチェーンデータとオンチェーンデータとの関係は、後述のマッピング図で示す。

表2-1-2 オフチェーンデータの主な構成要素（１／２）

区分	データ要素		データ内容
オフチェーンデータ	トークン取引価格		• VASP等が提供する各種暗号資産等の取引価格
	利用者情報	ホステッド・ウォレット	• 利用者のIPアドレス、KYC情報（氏名・住所・生年月日・クレジットカード情報など）、取引履歴、ウォレットの秘密鍵、Webトラフィックデータなど
		アンホステッド・ウォレット	• Metamask等のウォレットの利用者情報として、利用者のIPアドレス、ウォレットの秘密鍵、Webトラフィックデータなど
		DeFiユーザーインターフェース	• DeFi等の利用者情報として、インターフェース経由での利用者のIPアドレス、Webトラフィックデータなど
	ブロックチェーン外の取引情報		• VASP内の帳簿の付け替えなどを通じた顧客間の暗号資産の移転など、ブロックチェーン外での取引情報など
	ガバナンス投票者情報		• DeFi・DAO等におけるガバナンス投票関連の情報として、投票者の素性（Discord等におけるユーザー名など）など
	ノードやAPIなどのインフラサービス利用者情報		• EthereumノードやEthereumブロックチェーンのAPIサービスを利用するインフラサービス利用者の情報として、利用者のIPアドレス、KYC情報（氏名・住所・生年月日・クレジットカード情報など）、API呼出数など
	Githubのソースコード・パラメータなど		• Github（プログラムなどを保存・公開できるソフトウェア開発プラットフォーム）などで掲示されているスマートコントラクトのソースコード、パラメータなど
	ステーブルコイン発行裏付け準備金情報		• ステーブルコイン発行の裏付け資産となる銀行預金や国債などを管理する金融機関名や資産の種類、金額など

2-1. オンチェーン／オフチェーンデータの繋がりと構成要素

（２）オフチェーンデータの要素

表2-1-2　オフチェーンデータの主な構成要素（２／２）

区分	データ要素	データ内容
オフチェーンデータ	バリデータ情報	• バリデータの情報として、バリデータノードのIPアドレス、秘密鍵など
	ステーキング情報	• バリデータのステーキング情報として、ステーキングサービスを利用する出資者や金額などの情報
	レイヤー2の取引情報	• レイヤー2で実行された取引情報として、利用者のアドレスや送信アドレス、送金額など （本調査研究ではレイヤー2はオフチェーンデータとして定義する）
	ブリッジのノード情報	• ブリッジの管理者が運営するノードの情報として、IPアドレスや秘密鍵など
	ブリッジにロックしたトークン情報	• ブリッジにロックしたトークンの情報として、ロックしたトークンの種類、金額など

2-1. オンチェーン／オフチェーンデータの繋がりと構成要素

（３）オンチェーン／オフチェーンデータの接続ポイント

- オンチェーンデータとオフチェーンデータの間には一般にウォレットやインターフェース等の結節点が存在。表は主要な接続ポイントを示すもの。

※ 各々の接続ポイントとオンチェーンデータ／オフチェーンデータとの関係は、後述のマッピング図で示す。

表2-1-3　オンチェーン／オフチェーンの接続ポイント例

接続ポイント		説明（繋がりの具体例）
外部オラクル		• VASPが提供する暗号資産価格等ををオラクルプロバイダがブロックチェーン内のプロトコル（DeFi等）に提供する
ウォレット	ホステッド・ウォレット	• VASP（ホステッド・ウォレット提供者）が顧客情報や秘密鍵を管理し、顧客はVASPに指図することで当該ウォレットからトークンの送金などを行う
	アンホステッド・ウォレット	• ソフトウェア企業（ウォレット提供者）が提供するウォレットを利用し、利用者が直接秘密鍵を管理する形でトークンの送金などを行う
ユーザーインターフェース		• DeFi等がWebサイトやスマートフォンアプリなどのユーザーインターフェースを運営し、利用者がサービスを直接利用する
ノード	スマートコントラクト開発者のノード	• スマートコントラクトの開発者が、GitHub上のソースコードを元にスマートコントラクトをブロックチェーン上にデプロイする（ウォレットからのデプロイも可能な場合あり）
	ステーブルコイン運営者のノード	• ステーブルコインの運営者が、管理者権限によりステーブルコインの発行や焼却を行う
	バリデータのノード	• バリデータが、参加費用の預入やクライアントの登録によりブロックチェーンのコンセンサスに参加し、ブロックの生成・承認を行う
	レイヤー2オペレータのノード	• レイヤー2オペレータが、レイヤー2のブロックチェーンでトランザクションを実行し、結果をレイヤー1のメインチェーンに転送する
	ブリッジ管理者のノード	• ブリッジの管理者が、利用者が異なるブロックチェーン間で相互にやりとりするトークンなどを送信・検証する

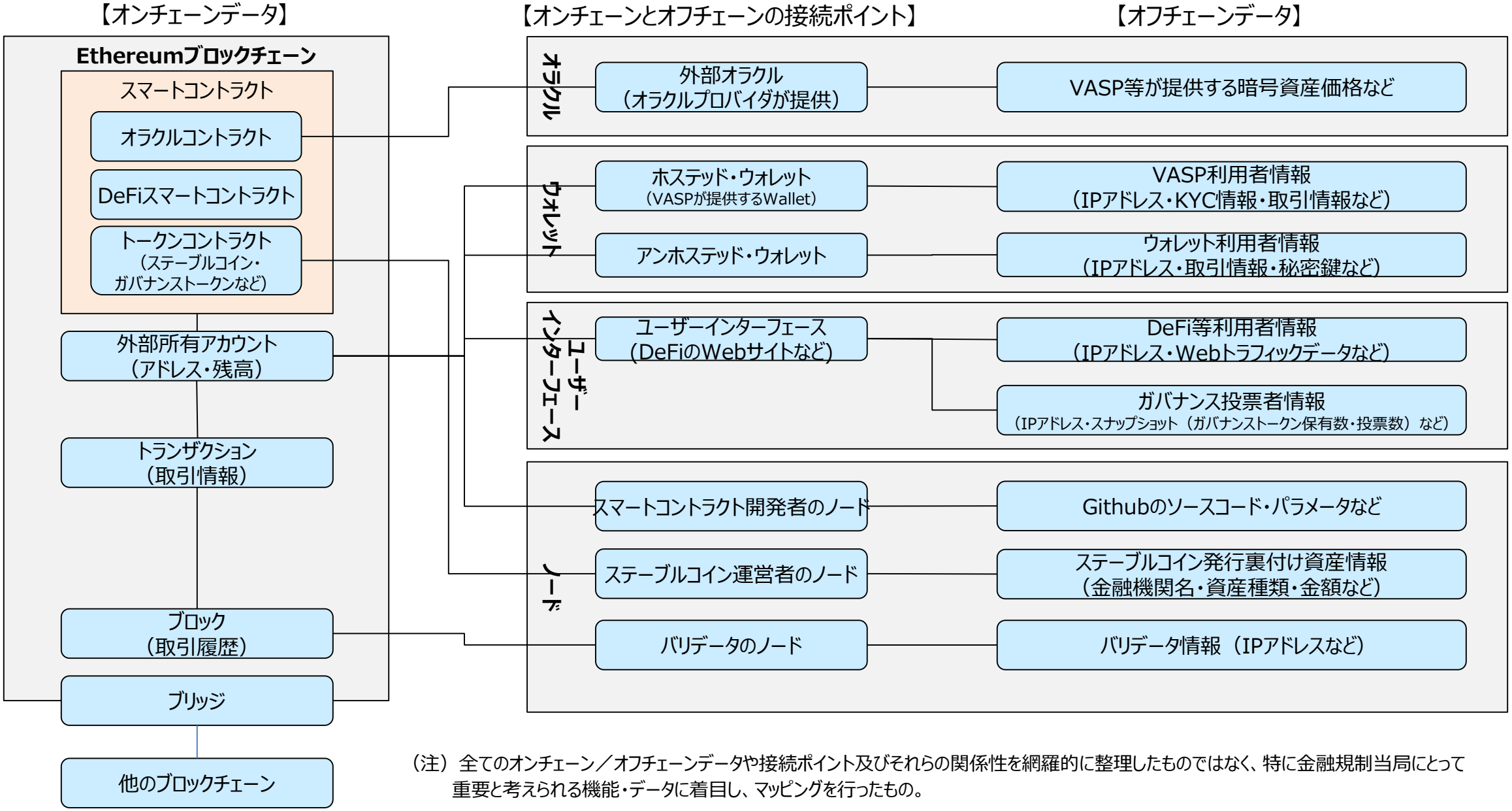
2-2. オンチェーン／オフチェーンデータのマッピング

（１）オンチェーン／オフチェーンデータのマッピング

- Ethereumブロックチェーンのオンチェーン／オフチェーンデータの主要な構成要素を抽出・マッピングし、以下の3点を可視化した。
  - オンチェーンデータ・接続ポイント・オフチェーンデータの主な構成要素と全体分類
  - オンチェーンデータ・接続ポイント・オフチェーンデータ間の繋がり
  - オフチェーンデータの管理者（オフチェーンデータを管理する組織や人物）　※詳細版にのみ記載

2-2. オンチェーン／オフチェーンデータのマッピング

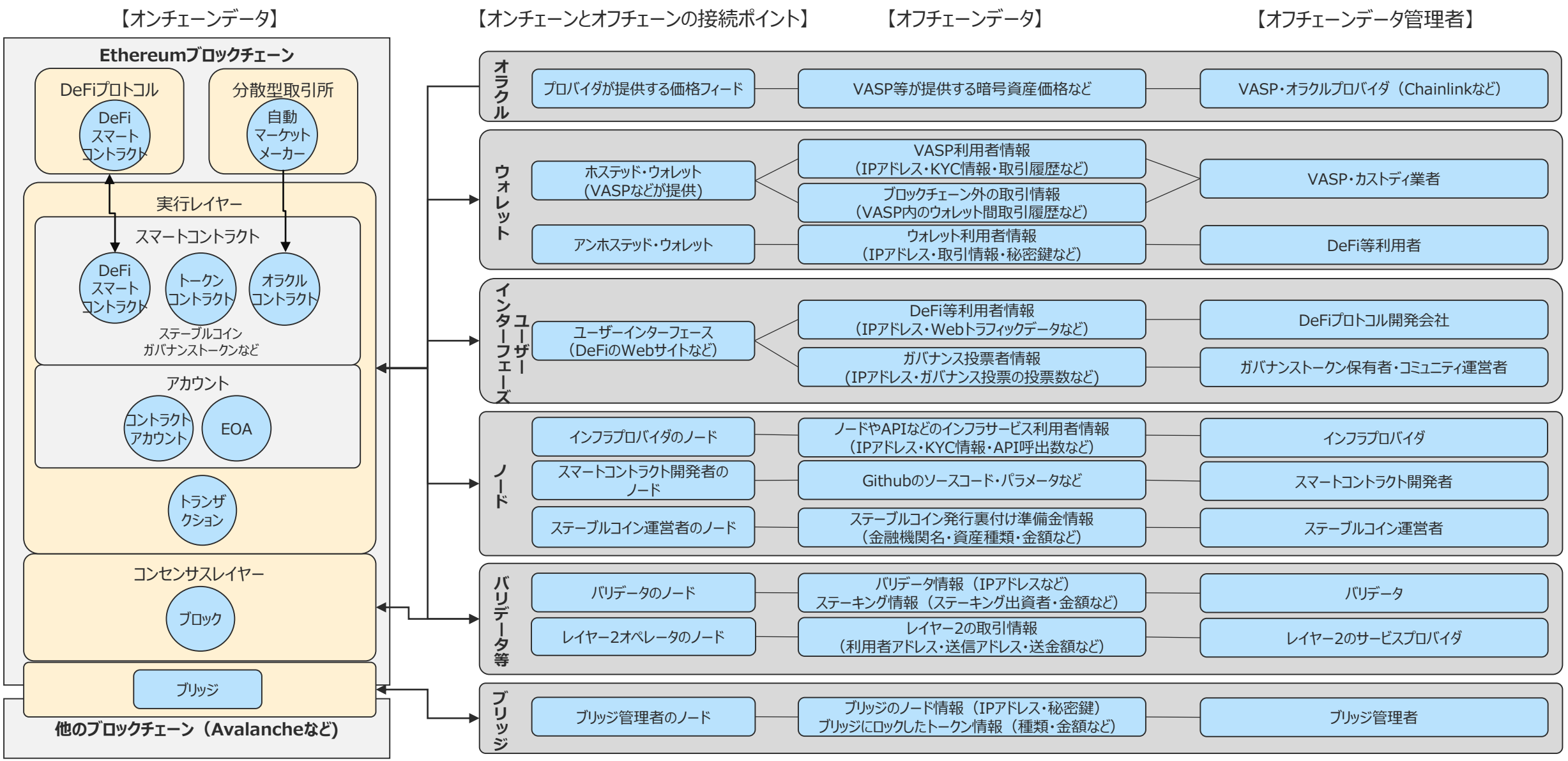
図2-2-1　オンチェーン／オフチェーンデータのマッピング（概要版）



（注）全てのオンチェーン／オフチェーンデータや接続ポイント及びそれらの関係性を網羅的に整理したものではなく、特に金融規制当局にとって重要と考えられる機能・データに着目し、マッピングを行ったもの。

2-2. オンチェーン／オフチェーンデータのマッピング（詳細）

図2-2-2　オンチェーン／オフチェーンデータのマッピング（詳細版）



第３章　分散型金融システムの実態把握に必要なデータの調査検討

第３章 分散型金融システムの実態把握に必要なデータの調査検討

- 本章では、前章までのオンチェーン／オフチェーンデータ及び接続ポイントに関する整理を踏まえ、これらデータの取得元として有用と考えられるデータソースと本調査研究のデータ分析で活用したデータソースの範囲、データ調査方法について詳述する。
- 本章は次のように構成される。
  - 3-1では、分散型金融システムの実態把握に有用と考えられる各種データソースを整理した上で、本調査研究で実際に活用したデータソースの範囲を示す。
  - 3-2では、データ分析に際して用いた調査方法の概要について説明する。
  - 3-3では、今回のデータ分析において多用した、ブロックチェーン分析ツールの概要について説明する。

3-1. 各種データソースと本調査研究のスコープ

- 表に記載の通り様々なデータソースが存在するが、オンチェーン／オフチェーンの違いに加えて、データの信頼性や取得可能性、アクセシビリティ（無料で利用可能か）は区々。各々のデータの特性を理解しつつ、規制目的に応じてデータ分析を進めていく必要。
- 本調査研究においては、監督上の対応等により入手可能なデータとは異なる性質のデータを取得できる可能性がある「BC（ブロックチェーン）エクスプローラー」、「暗号資産関連データベース」、「ブロックチェーン分析ツール会社（分析ツール・リサーチャー）」を活用してデータ分析等を実施。

表3-1　各種データソースと本調査研究のスコープ

データソース	事業者等（内部情報）	事業者等（開示情報）	BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール会社
概要	報告徴求等で得られるデータ	上場企業が法定開示を行なった情報等	Etherscanなどから入手できるブロックチェーンのアカウントや取引関連データ	Coingecko等のWebサイトから取得できる暗号資産価格等のデータ	ブロックチェーン分析ツール／リサーチャーから得られるデータ
公開／非公開	非公開	公開	公開	公開	非公開
オンチェーン／オフチェーン	オフチェーン	オフチェーン	オンチェーン	（多くは）オフチェーン	オンチェーンとオフチェーンの組合わせ
データの信頼性	高	高	高	中（VASPの申告ベースでの情報が多い）	中～低？（※）
VASP	○	△（非上場企業の場合はデータの範囲や信頼度が落ちる可能性）	△（大手VASPに関しては一定の情報あり）	○～△（一部入手困難なVASPあり）	○～△（分析ツール会社の能力に依存）
（無登録もしくは規制要件が不十分な法域に所在する）VASP	×	×	△～×	○～△（一部入手困難なVASPあり）	○～△（分析ツール会社の能力に依存）
DeFi	△～×（VASPとして規制されるDeFiについては取得可能性あり）	×（一部DeFiは自発的に情報開示を行うことも）	△（コントラクトアドレス等に関するデータ取得可能）	△（DEX等に関するデータを取得可能）	○～△（分析ツール会社の能力に依存）
アンホステッド・ウォレット（含P2P）	△（VASP-アンホステッド・ウォレット関連データは取得可能性あり）	×	△～×（一部のアンホステッド・ウォレットは取得可能性あり）	×	△（分析ツール会社の能力に依存するが、精度は高くないか）

本調査研究のスコープ

※ブロックチェーン分析ツールの機能・特性は区々であり、取得できるデータの範囲や信頼度も様々であることに留意。

3-2. 調査方法

（1）概要

- 各々のデータソースから取得できるデータと本調査研究の方法は以下のとおり。

表3-2-1　本調査研究で活用したデータソースと調査方法

データソース		取得できるデータ	本調査研究の調査方法
BC（ブロックチェーン）エクスプローラー		• ブロックチェーンアドレスやトランザクションなどのオンチェーンデータ • 一部のアドレスに付与されたカテゴリ名/アカウント名（VASPやDeFiなど）などのオフチェーンデータ	• 公開Webサイトを参照して取得できるデータを調査 • データソース例 ➢ Etherscan ➢ Dune Analytics　など
暗号資産関連データベース		• 暗号資産価格、市場価格チャート、時価総額など • 主要な暗号資産取引業者やDeFiに関する取引量等のデータ、最新ニュースなど	• 公開Webサイトを参照して取得できるデータを調査 • データソース例 ➢ CoinGecko ➢ Coinmarketcap
ブロックチェーン分析会社	分析ツール	• ブロックチェーン分析会社が提供する分析ツールから取得できるデータ （アドレス保有者のカテゴリ・アカウント名、制裁・過去犯罪履歴によるリスクスコアなど）	• 2社のブロックチェーン分析会社ツールを利用してデータを調査 （1社のデータに依存するリスクを回避）
	専門家リサーチ	• ブロックチェーン分析会社の専門家によるリサーチ結果データ （オンチェーンデータと自社データベースなどを組み合わせることで、複雑な条件に合致するデータなどを抽出することが可能）	• ブロックチェーン分析会社（1社）にリサーチを委託して必要なデータを取得

3-2. 調査方法

（２）分析対象とするデータ候補

- 表に記載の通り、取得可能と考えられるデータは各手段によって異なる。一方で、①BCエクスプローラーから取得できる情報の多くは③、④にも取り込まれていること等を踏まえ、②③④を主に活用してデータ分析を実施した。
- ブロックチェーン分析ツールは複数の会社と契約することで、１つの会社の（我々では信頼性の検証が困難な）データに依存するリスクを低減することを試みた。

表3-2-2　取得可能なデータの具体例

		①BCエクスプローラー	②暗号資産関連データベース	③ブロックチェーン分析ツール	④専門家によるリサーチ
主な特徴		• ブロックチェーン内のデータを検索・照会ができるWebサイト（Etherscanなど） • 一部の主要なVASPやDeFiは、アカウント名からアドレスが取得できる	• 暗号資産の市場価格をリアルタイムで提供するWebサイト	• ブロックチェーン会社が有償で提供する分析ツール • 事業者や捜査当局、金融当局向けに、特定のエンティティやアドレス等のリスク表示や高リスクアドレス取引のアラート検知機能を提供	• ブロックチェーン分析会社の専門家が、自社の分析ツールやデータベースの情報を活用して詳細なリサーチを行うもの
分析対象とするデータ候補	オンチェーンデータ	• ブロック情報（ブロック番号・取引件数など） • アカウント情報（アドレス・トークン別残高など） • 取引情報（取引時刻・取引件数・取引量など） ※データは1件毎に取得できる（全体の統計情報などは取得できない）	• 主なDeFiのTVL・トークン発行量 • 主な分散型取引所の取引情報（直近24時間取引高・トークンペア数/ペア別の取引高など）	• アカウント情報（アドレス・トークン別残高など） • 取引情報（直近24時間取引高・初回/最終取引日・取引日・取引件数・取引量など） • アカウント取引相手の図表示 • （複数アカウントを跨る取引を連結して表示）など	• 複雑な検索条件による取引の集計（少額取引、同じ相手に短時間に複数回送金、不正アドレス利用者など） • 匿名性の高いサービスのアドレス • トークン凍結アドレス・取引量　など
	オフチェーンデータ	• 一部のアドレスのアカウント名（アドレスを公開している一部のVASPやDeFiなど）	• VASP毎のトークン価格一覧 • トークン価格の推移チャート（1日から全期間まで） • トークンの時価総額の推移チャート • 最新の暗号資産関連ニュース • 主要トークンの概要（創立者・特徴など）	• 識別できたアドレスのカテゴリ名(VASPやウォレットなどの種類)・アカウント名 • アドレスのリスク値 制裁リストや過去の犯罪利用などからリスク値を分析会社が自己判定 • アカウント情報 （企業情報、各国ライセンス保有、KYC実施レベル、最新トピック等）など	• カテゴリやアカウント別の取引の集計(VASPやP2P取引など) • VASP情報の集計（ライセンス無登録やKYC未実施など） • ハッキング被害件数・被害額 • 不正アドレスの集計（制裁リスト・詐欺恐喝・犯罪利用・ダークネットなど） • VASP利用者数　など

3-3. ブロックチェーン分析ツールの概要

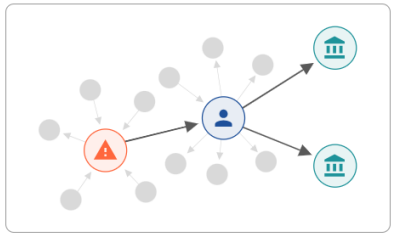
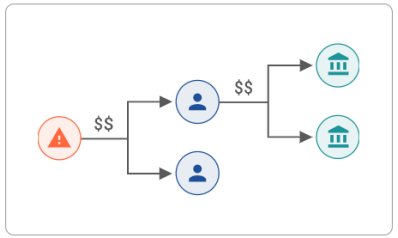
- 分析ツールは一般に民間企業により有償で提供されるソフトウェアで、オンチェーンデータとオフチェーンデータを組み合わせて、クラスタリング技術等によりカテゴリ名やアカウント名などの特定及び該当アドレスのリスクスコアの判定等を行うもの。主にVASPや機関投資家、捜査当局などが、高リスクアドレスとの取引検知や調査対象アドレスのアカウント名の特定、特定のインシデント（暗号資産の窃取等）に関連する取引の追跡等の目的で利用している。
- 以下の表は、今回利用した分析ツールが提供するデータ等を整理したもの（ツールにより得られる情報やその精度、範囲は区々であることに留意）

表3-3 ブロックチェーン分析ツールの概要（１／２）

項目	提供されるデータ･サービス	具体的な内容	備考
ブロックチェーンデータの表示･検索	エンティティ情報	• VASP：保有アドレス、アカウント名、法人が在籍する国名、現在の稼働状況、サービス内容、設立時期、CEO名、概要説明、連絡先、eメールアドレス、オフィス設置国、電話番号など • DeFi／ウォレット：アドレス、アカウント名、トークン別の残高、直近24時間取引高、送信／受信総額、初回／最終稼働日など	• 自社でアドレスにラベリングしたカテゴリ名やアカウント名等が取得できる
	エンティティの取引情報	• VASPのトークン別の取引量、日次の損益額、資産価値の推移、VASPが管理するアドレス毎の残高･取引額、取引履歴など	• 対象はVASPのみ
	エンティティのリスク情報	• ライセンス登録国、AML/KYCの実施状況など	• 対象はVASPのみ
	アドレスのリスクレベル･リスクスコア	• リスクレベル：危険･高･中･低の4段階で表示（危険：リスクスコア80～100、高：リスクスコア50～79など） • リスクスコア：100段階で計算したリスク値 ※リスク判定の情報：過去に詐欺や犯罪などで使用されたアドレス、制裁対象アドレスなど	• リスクレベルの分類、リスクスコアの数値は分析ツールによって異なる
	アドレスに関連する高リスク取引の内容	• 高リスク取引と判断した理由（脅迫･マルウェア･ミキシング･ダークネット･フィッシング･ランサムウェアなど） • 取引件数、金額（USD･ETHなど）、取引件数のグラフ表示 • 取引履歴（取引日時･取引ハッシュ番号･送信者アドレス･受信者アドレス･金額など） • 上記についてブロックチェーン別、期間指定などで表示できる	
	高リスクアドレスの一覧表示	• リスクスコアの高い順からアドレスを表示（アドレス毎の表示画面にリンク）	

3-3. ブロックチェーン分析ツールの概要

表3-3 ブロックチェーン分析ツールの概要（２／２）

項目	提供されるデータ･サービス	具体的な内容	備考
ブロックチェーンデータの表示･検索	トランザクショングラフ	• 対象アドレスの受信／送信別の取引履歴、送信／受信先のカテゴリ名／アカウント名、トークン、金額を1画面に描画してトランザクションの繋がりを可視化する • 高リスクアドレスと関連する取引は赤表示で区別される • 指定したアドレスについて、前後の複数の取引を関連付けて自動的に描画する 【トランザクションの描画イメージ】 	• 該当のアイコン（アドレス）をクリックすると、そのアドレスを中心とした送信/受信取引先とトークン名･金額などが表示される
	エンティティ関連ニュース	• エンティティに関連するネットニュースなど（各ニュースサイトの記事を抜粋）	
トレース機能	トランザクション自動トレース	• 指定したアドレスについて、指定した期間に実行した複数の取引を自動的に連続で描画する 【自動トレースの描画イメージ】 	• アドレスと期間を指定して実行すると、対象期間内の取引状況が連続で表示される
アラート検知	指定アドレス取引の自動検知	• 高リスクアドレスなど指定したアドレスの取引を自動検知してアラート通知する機能	• 事前にアドレスを指定することで、取引発生時に自動検知される
制裁リスト	各国制裁リストの表示	• 米国OFACや英国･EUなどの制裁リストで公表された情報（対象者名･制裁内容など）を表示する	
その他	ブロックチェーンアドレスの記録	• 一度検索したアドレスを記録し、次の検索時にアドレス入力を不要とする機能	

第４章　データ分析結果

第４章 データ分析結果

- 本章では、前章までで指摘したデータを分析ツールやリサーチャー等を活用して可能な限り取得し、実際に分析を行なった結果を示す。
- 本章は次のように構成される。
  - 4-1では、データ分析を実施した範囲とデータ分析の限界（分析対象困難なアドレス・取引が多く存在する点）について述べる。
  - 4-2では、リサーチャーから取得したデータの信頼性を考察するため、他社ツールとの定量比較を実施した結果を報告する。
  - 4-3では、FSB報告書の指摘も踏まえ、VASP、レンディング事業者、ステーブルコイン、DeFiのデータ取得可能性及び金融安定の観点に着目したデータ分析結果を示す。
  - 4-4では、FATF報告書の指摘も踏まえ、VASP、レンディング事業者、アンホステッド・ウォレット（P2P含む）、AML/CFT関連のデータ取得可能性、高リスク取引の分布とその分析結果を示す。

4-1. データ分析の範囲とその限界

- 本調査研究における調査対象範囲は、今回使用したブロックチェーン分析会社がアカウント名等を特定したアドレスの取引データに限定。その結果、データ分析結果も、これらのデータに限定して行なった局所的なものであることに留意（分散型金融システム全体のデータを分析したものではない）

表4-1-1-1　オンチェーン／オフチェーンデータの調査対象範囲

項目	説明	補足
データの調査対象範囲	• 2022年のEthereumブロックチェーン上の取引データのうち、ブロックチェーン分析会社がカテゴリ名（VASP・DeFiなど）またはアカウント名（VASP名など）などを特定した一部のアドレスを調査対象として、そのアドレスから送受信されるトランザクションデータを集計した	• カテゴリ名またはアカウント名を特定した取引件数は全体の4～33%であり、全体を示すものではない • 分析会社のカテゴリ名などの分類が誤っていた場合には、データも正確性を欠くものとなる

図4-1-1　取引データの調査対象範囲

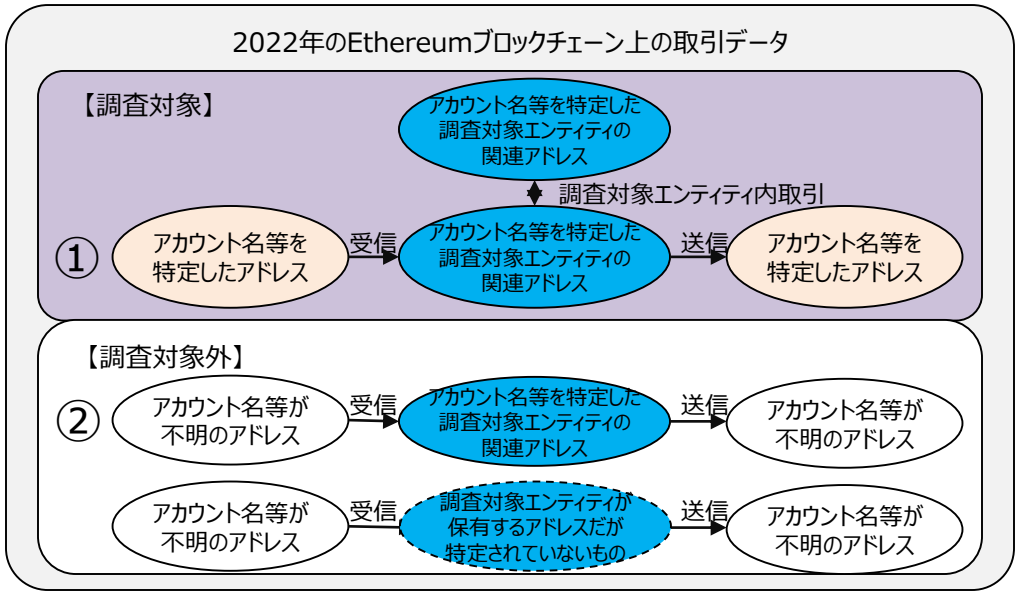


表4-1-1-2　調査対象エンティティの取引件数（リサーチャーから取得したデータ）

調査対象	調査対象から他の取引相手に送受信した取引件数			参考：①＋②とEthereum全体取引件数との比率※
	①取引相手のアカウント名等を特定	②取引相手のアカウント名等が不明	①＋②	
暗号資産交換業者A	3,381,239件（13%）	22,397,649件（87%）	25,778,888件	6.3%
暗号資産交換業者B	1,293,983件（4%）	34,175,484件（96%）	35,469,467件	8.7%
レンディング事業者	144,457件（33%）	297,820件（67%）	442,277件	0.1%
アンホステッド・ウォレット	5,772,973件（18%）	26,097,100件（82%）	31,870,073件	7.8%

※「①＋②」は、調査対象のアカウント名等が特定されたアドレスに関する取引件数であり、例えばアンホステッド・ウォレットの取引であっても、調査対象のアカウント名が特定されていないものは含まれない
※Ethereum全体の2022年取引件数：約4.09億件

4-2. 取得したデータの信頼性評価

（１）リサーチ結果と他社ツールの比較：VASP関連の取引件数・取引金額には一定の信頼性

- アドレス保有数は、2社で約20~2,200倍と顕著な差がある。これは、2社の情報収集リソースやラベル付けの手法が異なっているためと考えられる。
- 取引件数・取引金額は、2社の差が約50～150%程度であり大きな差はないため、データに一定の信頼性が見られると考えられる。

  →上記の結果から、例えば、②は現在ほとんど使用されていない調査対象エンティティ関連アドレスを含んでいる可能性が考えられる。

表4-2-1　調査結果と他社ツールの比較（取引件数・取引金額）

大項目	小項目		①ブロックチェーン分析会社A リサーチ結果	②ブロックチェーン分析会社B ツール情報	②÷①	備考
暗号資産交換業者A	アドレス保有数		21,834	8,066,565	36945.0%	顕著な差（370倍）
	取引件数	受信	9,310,372	14,369,476	154.3%	
		送信	14,269,851	12,135,550	85.0%	
	取引金額(M$)	受信	314,321	344,649	109.6%	
		送信	311,188	340,245	109.3%	
暗号資産交換業者B	アドレス保有数		14,220	31,755,943	223318.9%	顕著な差（2,233倍）
	取引件数	受信	15,717,777	7,425,815	47.2%	
		送信	18,752,632	13,616,799	72.6%	
	取引金額(M$)	受信	250,914	265,435	105.8%	
		送信	252,892	255,632	101.1%	
レンディング事業者	アドレス保有数		15,730	306,442	1948.1%	顕著な差（19倍）
	取引件数	受信	109,391	127,706	116.7%	
		送信	205,940	202,160	98.2%	
	取引金額(M$)	受信	13,785	16,092	116.7%	
		送信	11,725	16,288	138.9%	

※取引金額の算出は2023年4月時点のレートを使用

4-2. 取得したデータの信頼性評価

（2）リサーチ結果と他社ツールの比較：調査対象エンティティ・取引相手によりデータの信頼性は区々

- 送信・受信共にVASPが絡む高リスク取引は2社で大きな差がないため、データに一定の信頼性が見られると考えられる。
- VASPとDeFi/アンホステッド・ウォレットとの高リスク取引件数／アドレス数は、2社で最大約3倍の差がある。これは、分析会社によってDeFi/アンホステッド・ウォレットの識別率や高リスクアドレスの判定方法に違いがあると考えられる。

表4-2-2　調査結果と他社ツールの比較（高リスクアドレスの取引件数）（１／２）

調査対象	区分	取引相手	送信/受信	高リスク取引件数（アドレス数）※			備考
				①ブロックチェーン分析会社Aリサーチ結果	②ブロックチェーン分析会社Bツール情報	②÷①	
暗号資産交換業者A	アドレス数	–	–	85アドレス	–	–	
	取引件数	暗号資産交換業者A間	–	2,184,570件 （29アドレス）	2,184,443件 （17アドレス）	99.9% (58.6%)	アドレス数は約2倍異なるが、取引件数は概ね同じ
		暗号資産交換業者B	暗号資産交換業者Aが受信	88,988件 （18アドレス）	88,983件 （16アドレス）	100.0% (88.9%)	
			暗号資産交換業者Aが送信	59,102件 （18アドレス）	59,102件 （18アドレス）	100.0% (100.0%)	
		その他VASP	暗号資産交換業者Aが受信	173,577件 （115アドレス）	172,891件 （99アドレス）	99.6% (86.1%)	
			暗号資産交換業者Aが送信	133,483件 （398アドレス）	116,634件 （136アドレス）	87.4% (34.2%)	アドレス数は約3倍異なるが、取引件数は概ね同じ
		DeFi	暗号資産交換業者Aが受信	30,158件 （262アドレス）	9,954件 （132アドレス）	33.0% (38.8%)	アドレス数は約3倍異なり、取引件数も約3倍異なる
			暗号資産交換業者Aが送信	3,465件 （37アドレス）	3,383件 （21アドレス）	96.4% (82.3%)	
		アンホステッド・ウォレット	暗号資産交換業者Aが受信	11,565件 （55アドレス）	10,561件 （32アドレス）	91.3% (58.2%)	アドレス数は約2倍異なるが、取引件数は概ね同じ
			暗号資産交換業者Aが送信	25,622件 （131アドレス）	19,561件 （58アドレス）	76.3% (44.3%)	アドレス数は約2倍異なるが、取引件数の差は小さい

※アドレス数は送信側・受信側の両方のアドレスの合計、②は①の高リスク取引件数・アドレス数のうちブロックチェーン分析会社Bのツールで高リスクのものを集計

4-2. 取得したデータの信頼性評価

（3）リサーチ結果と他社ツールの比較：取引相手によりデータの信頼性は区々

- アンホステッド・ウォレットの高リスク取引件数／アドレス数は2社で顕著な差がある。これは、分析会社によってアンホステッド・ウォレットの識別率及び高リスクアドレスの判定方法に大きな違いがあると考えられる。

表4-2-3　調査結果と他社ツールの比較（高リスクアドレスの取引件数）（２／２）

調査対象	区分	取引相手	送信/受信	高リスク取引件数（アドレス数）※			備考
				①ブロックチェーン分析会社Aリサーチ結果	②ブロックチェーン分析会社Bツール情報	②÷①	
暗号資産交換業者B	アドレス数	–	–	8アドレス	–	–	
	取引件数	暗号資産交換業者B間	–	694,838件 （8アドレス）	694,838件 （8アドレス）	100.0% （100.0%）	
		暗号資産交換業者A	（暗号資産交換業者A－暗号資産交換業者Bの取引件数と同じ）				
		その他VASP	暗号資産交換業者Bが受信	45,792件 （56アドレス）	45,744件 （55アドレス）	100.0% （98.2%）	
			暗号資産交換業者Bが送信	51,716件 （211アドレス）	47,144件 （57アドレス）	91.2% （27.0%）	アドレス数は約4倍異なるが、取引件数は概ね同じ
		DeFi	暗号資産交換業者Bが受信	4,039件 （102アドレス）	2,464件 （60アドレス）	61.0% （58.8%）	アドレス数は約2倍異なり、取引件数も約2倍異なる
			暗号資産交換業者Bが送信	361件 （14アドレス）	356件 （10アドレス）	98.6% （71.4%）	
		アンホステッド・ウォレット	暗号資産交換業者Bが受信	3,467件 （31アドレス）	3,264件 （21アドレス）	94.1% （67.7%）	アドレス数は約1.5倍異なるが、取引件数は概ね同じ
			暗号資産交換業者Bが送信	22,259件 （105アドレス）	20,157件 （39アドレス）	90.6% （37.1%）	アドレス数は約3倍異なるが、取引件数は概ね同じ
アンホステッド・ウォレット	アドレス数	–	–	291アドレス	–	–	
	取引件数	アンホステッド・ウォレット間（P2P取引）	–	425,882件 （291アドレス）	15,349件 （55アドレス）	3.6% （18.9%）	顕著な差（取引件数28倍、アドレス数5.3倍）

※アドレス数は送信側・受信側の両方のアドレスの合計、②は①の高リスク取引件数・アドレス数のうちブロックチェーン分析会社Bのツールで高リスクのものを集計

4-2. 取得したデータの信頼性評価

（4）Key Findings

表4-2-4　Key Findings

Key Findings		内容	補足
ブロックチェーン分析ツールの限界	取引相手を特定できるケースはごく一部に留まる	• 調査対象（VASP等）の関連アドレスとの間で行われた全取引のうち、取引相手が特定されたもの（送信／受信先アドレスのカテゴリやアカウント名等が特定できたもの）はごく一部に留まり、今回の分析対象とできたのは、取引全体のごく一部に過ぎない。 • 理由としては、カテゴリやアカウントを識別できるだけの十分な情報の取得が困難（例：過去１回しか取引が行われていないアドレス）、分析ツール会社のキャパシティ不足（IPアドレスやウェブトラフィック、制裁関連情報など、アドレスを識別するために必要なオフチェーンデータを十分入手できていない）、等が考えられる。	• 他社の分析ツールではより多くのカウンターパーティが特定された可能性がある。但し、不十分なデータに基づいて識別している可能性もあり、識別率のみで分析会社の優劣を判断することは困難。
	分析ツール会社間で顕著な差が見られるデータが存在	• VASP間の取引件数・金額など2社の違いが僅かで一定の信頼性を与えて良いと思われるデータ区分が存在する一方で、VASPの保有アドレス数やDeFi/アンホステッド・ウォレット関連の取引など、分析ツール会社の間で顕著な差が見られる結果になった。 • 相対的にVASP関連の取引の信頼度が高い結果となっているのは、一定規模以上の取引が集中するVASPの方が、個人等が保有し散発的な取引が多いと考えられるアンホステッド・ウォレット関連（P2P含む）等に比べて識別が容易である可能性が考えられる。 • その他、ラベル付けの手法（ヒューリスティックベース：経験則などに基づくものや独自のアルゴリズムなど）の違い	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

- FSB報告書の指摘について、各種ツールや専門家リサーチによるデータ取得可能性の調査の結果、報告書で利用可能とされているデータの一部は本調査研究の手法ではデータが取得が困難であること、また利用できないとされるデータの一部を取得できる可能性があること（取得が限定的なものを含む）等が確認された。
- 当調査結果は、あくまで今回使用した分析ツールや専門家リサーチの結果に基づく局所的な整理であることに留意。

（１）裏付資産のない暗号資産のデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-1　裏付資産のない暗号資産のデータ取得可能性（１／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
裏付資産のない暗号資産	資産効果	利用可能なデータ	暗号資産の時価総額	△ 主な暗号資産は取得できる	△ 主な暗号資産は取得できる	× データ取得が困難	△ 主な暗号資産は取得できる	暗号資産関連データベース等が時価総額を公開している暗号資産が対象
			取引件数	△ 暗号資産発行体の取引データから1件毎に取得できる（集計は困難）	× データ取得が困難	△ 暗号資産発行体の取引データから1件毎に取得できる（集計は困難）	〇 暗号資産発行体の取引データから取得できる	ブロックチェーン分析会社が裏付資産のない暗号資産と特定したアドレスが対象
			実現ボラティリティ	× データ取得が困難	▲ 価格変動データは取得でき、当該データから計算できる可能性	× データ取得が困難	－ （調査対象外）	
			地域ごとの普及状況	× データ取得が困難	× データ取得が困難	▲ 主なVASPのライセンス登録国と利用できる暗号資産のデータは取得でき、当該データから取得できる可能性	－ （調査対象外）	今回利用しなかったブロックチェーン分析会社で、地域ごとの普及状況に関する報告書を出している先も存在

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（１）裏付資産のない暗号資産のデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-1　裏付資産のない暗号資産のデータ取得可能性（２／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				備考
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
裏付資産のない暗号資産	資産効果	利用できないデータ	暗号資産に投資をしている世帯の割合	× データ取得が困難	× データ取得が困難	× データ取得が困難	－（調査対象外）	
			家計資産に対する割合	× データ取得が困難	× データ取得が困難	× データ取得が困難	－（調査対象外）	
			暗号資産保有の世帯間の偏り	× データ取得が困難	× データ取得が困難	× データ取得が困難	－（調査対象外）	
			暗号資産の保有者	▲ アドレスのアカウント名を特定した一部に限られる	× データ取得が困難	▲ アドレスのアカウント名を特定した一部に限られる	▲ アドレスのアカウント名を特定した一部に限られる	大手取引所や著名投資家や制裁対象者など、一定の類型のユーザーは特定されている
	市場信頼性	利用可能なデータ	暗号資産のリテールの保有割合	▲ アドレスのアカウント名等を特定した一部に限られるため、割合の算出までは困難	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られるため、割合の算出までは困難	ブロックチェーン分析会社がアカウント名等を特定したアドレスが対象
			暗号資産関連のインフラ（取引プラットフォーム、ウォレット提供者等）にアクセスできるユーザー数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－（調査対象外）	プラットフォーマーやウォレット提供者が内部データとしては保有している可能性
		利用できないデータ	不正取引被害総額	× データ取得が困難	× データ取得が困難	▲ 一部の不正事案は特定されているが、総額の算出は困難	▲ 一部の不正事案は特定されているが、総額の算出は困難	ブロックチェーン分析会社が不正取引と特定したアドレスが対象

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（１）裏付資産のない暗号資産のデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-1　裏付資産のない暗号資産のデータ取得可能性（３／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				備考
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
裏付資産のない暗号資産	金融機関へのエクスポージャー	利用可能なデータ	暗号資産の機関投資家の保有割合	▲ 機関投資家の保有が特定されたアドレスに限られ、全体の割合算出は困難	× データ取得が困難	▲ 機関投資家の保有が特定されたアドレスに限られ、全体の割合算出は困難	▲ 機関投資家の保有が特定されたアドレスに限られ、全体の割合算出は困難	
			暗号資産への投資割合	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			暗号資産関連サービスを提供している主要な金融サービス提供者数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	各国の登録事業者情報等を通じて相当程度の把握は可能と考えられる
			暗号資産のデリバティブマーケットの規模	× データ取得が困難	△ 主な暗号資産は取得できる	× データ取得が困難	△ 主な暗号資産は取得できる	
			暗号資産のデリバティブ契約の建玉	× データ取得が困難	△ 主な暗号資産は取得できる	× データ取得が困難	△ 主な暗号資産は取得できる	
			暗号資産と他の資産クラスとの相関	× データ取得が困難	〇 暗号資産の価格データから計算可能	× データ取得が困難	－ （調査対象外）	
			取引規模ごとの取引件数分布	▲ アドレスのアカウント名等を特定した一部に限られ、分布の把握までは困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られ、分布の把握までは困難	▲ アドレスのアカウント名等を特定した一部に限られ、分布の把握までは困難	ブロックチェーン分析会社が金融機関と特定したアドレスが対象

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（１）裏付資産のない暗号資産のデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-1　裏付資産のない暗号資産のデータ取得可能性（４／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
裏付資産のない暗号資産	金融機関へのエクスポージャー	利用できないデータ	暗号資産に投資しているファンドの保有割合と運用資産残高（スポット、デリバティブ、エコシステム、投資家の属性ごと）	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			銀行セクターへのエクスポージャー	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			暗号資産の保有/サービス提供にかかる金融機関による報告	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（１）裏付資産のない暗号資産のデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-1　裏付資産のない暗号資産のデータ取得可能性（５／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
裏付資産のない暗号資産	決済利用	利用可能なデータ	価格とデルタ (1w, 1m, 3m, 6m, 1y, ...)	× データ取得が困難	△ 主なトークン価格と推移が取得できる	× データ取得が困難	△ 主なトークン価格と推移が取得できる	
			取引件数	▲ 決済サービス関連アドレスと特定した一部に限られる	× データ取得が困難	▲ 決済サービス関連アドレスと特定した一部に限られる	▲ 決済サービス関連アドレスと特定した一部に限られる	ブロックチェーン分析会社が決済サービスと特定したアドレスが対象
			暗号資産決済サービスの提供者数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	登録事業者に関する一定の公知情報は存在
			主要な暗号資産取引所の市場占有割合	× データ取得が困難	〇 主要なVASPの暗号資産ペア別取引高から市場占有率が算出できる可能性	× データ取得が困難	〇 主要なVASPの暗号資産ペア別取引高から市場占有率が算出できる可能性	暗号資産関連データベースで直近24時間取引高などが取得できる
		利用できないデータ	取引数と額	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が決済サービスと特定したアドレスが対象
			支払人と受取人の法域	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等と法域を特定した一部（VASPなど）に限られる	▲ アドレスのアカウント名等と法域を特定した一部（VASPなど）に限られる	ブロックチェーン分析会社がアカウント名等と法域を特定したアドレスが対象
			取引形態（例えば、送金、電子商取引、貿易）	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			採用されている暗号資産の種類	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			法定通貨としての受け入れ状況	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（２）ステーブルコインのデータ取得可能性

【データ調査結果の凡例】
○：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-2　ステーブルコインのデータ取得可能性（１／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				備考
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
ステーブルコイン	資産効果	利用可能なデータ	ステーブルコインの時価総額	○ （ペッグされた法定通貨と等価との前提）	△ 主なステーブルコインは取得できる	× データ取得が困難	○ （ペッグされた法定通貨と等価との前提）	暗号資産関連データベース等が時価総額を公開しているステーブルコインが対象
			取引件数	△ ステーブルコイン発行体の取引データから1件毎に取得できる（集計は困難）	× データ取得が困難	△ ステーブルコイン発行体の取引データから1件毎に取得できる（集計は困難）	○ ステーブルコイン発行体の取引データから取得できる	ブロックチェーン分析会社がステーブルコインと特定したアドレスが対象
			実現ボラティリティ	× データ取得が困難	▲ 価格変動データは取得でき、当該データから計算できる可能性	× データ取得が困難	－ （調査対象外）	
		利用できないデータ	ステーブルコインの保有者	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社がアカウント名等を特定したアドレスが対象
		追加すべきデータ	ステーブルコインの発行主体とVASPとの取引関係	△ エクスプローラー上で識別されたVASPに限定して1件毎に取得できる（集計は困難）	× データ取得が困難	△ 分析ツールで識別されたVASPに限定して1件毎に取得できる（集計は困難）	△ 分析ツールで識別されたVASPに限定して一定数が取得できる	ブロックチェーン分析会社がVASPと特定したアドレスが対象

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（２）ステーブルコインのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-2　ステーブルコインのデータ取得可能性（２／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
ステーブルコイン	市場信頼性	利用可能なデータ	ステーブルコインのリテールの保有割合	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社がアカウント名等を特定したアドレスが対象
			ステーブルコインのインフラ（取引プラットフォーム、ウォレット提供者等）にアクセスできるユーザー数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	プラットフォーマーやウォレット提供者が内部データとしては保有している可能性
		利用できないデータ	不正取引被害総額	△ 過去に不正な取引を行ったアドレスの取引データから1件毎に取得できる（集計は困難）	× データ取得が困難	△ 過去に不正な取引を行ったアドレスの取引データから1件毎に取得できる（集計は困難）	〇 過去に不正な取引を行ったアドレスの取引データから取得できる	ブロックチェーン分析会社が過去に不正な取引を行ったアドレスと特定したものが対象
		追加すべきデータ	凍結対象アドレス／凍結対象額合計	△ ステーブルコイン発行体の取引データから1件毎に取得できる（集計は困難）	× データ取得が困難	× データ取得が困難	〇 ステーブルコイン発行体の取引データから取得できる	ステーブルコイン発行体のトランザクションの結果が「Blocked」となった取引のアドレスと取引量を集計

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（２）ステーブルコインのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-2　ステーブルコインのデータ取得可能性（３／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				備考
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
ステーブルコイン	金融機関へのエクスポージャー	利用可能なデータ	ステーブルコインの機関投資家の保有割合	▲ 機関投資家の保有が特定されたアドレスに限られ、全体の割合算出は困難	× データ取得が困難	▲ 機関投資家の保有が特定されたアドレスに限られ、全体の割合算出は困難	▲ 機関投資家の保有が特定されたアドレスに限られ、全体の割合算出は困難	
			ステーブルコインへの投資割合	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			ステーブルコイン関連サービスを提供している主要な金融サービス提供者数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	各国の登録事業者情報等を通じて相当程度の把握は可能と考えられる
			米国MMFと比較したステーブルコインの市場規模	× データ取得が困難	△ ステーブルコインの市場規模は取得できる 米国MMFの市場規模は取得が困難	× データ取得が困難	〇 ステーブルコイン・米国MMFの市場規模が取得できる	
		利用できないデータ	ステーブルコインに投資しているETFの保有割合や残高（スポット、デリバティブ、エコシステム、投資家の属性ごと）	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			銀行セクターへのエクスポージャー	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			規制市場に投資している裏付資産・裏付資産の流動性・裏付資産の構成の詳細	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（２）ステーブルコインのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-2　ステーブルコインのデータ取得可能性（４／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
ステーブルコイン	金融機関へのエクスポージャー	利用できないデータ	暗号資産の保有/サービス提供にかかる金融機関による報告	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
		追加すべきデータ	機関投資家や金融機関の暗号資産取引実態（大口ユーザーが選好する暗号資産／ステーブルコインの種別など）	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が機関投資家や金融機関と特定したアドレスが対象
	決済利用	利用可能なデータ	価格	× データ取得が困難	× データ取得が困難	× データ取得が困難	〇 決済サービスのサイトなどから決済で利用するトークン価格が取得できる	決済で利用される場合のトークン価格の取得可能性について調査
			取引件数	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が決済サービスと特定したアドレスが対象
			ステーブルコイン決済サービスの提供者数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（２）ステーブルコインのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-2　ステーブルコインのデータ取得可能性（５／５）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
ステーブルコイン	決済利用	利用できないデータ	取引額	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が決済サービスと特定したアドレスが対象
			支払人と受取人の法域	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等と法域を特定した一部（VASPなど）に限られる	▲ アドレスのアカウント名等と法域を特定した一部（VASPなど）に限られる	ブロックチェーン分析会社がアカウント名等と法域を特定したアドレスが対象
			取引形態（例えば、送金、電子商取引、貿易）	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			ステーブルコインの取引プラットフォームでの利用方法	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			ステーブルコインの用途の内訳	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（３）DeFiのデータ取得可能性

【データ調査結果の凡例】
○：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-3　DeFiのデータ取得可能性（１／６）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
DeFi	資産効果	利用可能なデータ	TVL	× データ取得が困難	△ 主なDeFiは取得できる	× データ取得が困難	△ 主なDeFiは取得できる	暗号資産関連データベース等がデータを公開しているDeFiが対象
			DEXの取引件数	▲ DEXと特定したアドレスの取引が1件毎に取得できるが、取引件数の集計は困難	× データ取得が困難	▲ DEXと特定したアドレスの取引が1件毎に取得できるが、取引件数の集計は困難	△ DEXと特定したアドレスの取引データが一定数は取得できる	ブロックチェーン分析会社がDEXと特定したアドレスが対象
			ウォレットの成長率	× データ取得が困難	× データ取得が困難	▲ アンホステッド・ウォレットと特定した一部のアドレスの取引が1件毎に取得できる（過去の取引データは取得可能）	▲ アンホステッド・ウォレットと特定した一部のアドレスの取引について、過去からの推移データが取得可能	DeFiを利用するアンホステッド・ウォレットの取引件数・金額の推移のデータ取得可能性を調査
			ガバナンストークンの時価総額と取引件数	△ 主なトークンの時価総額は取得できる 取引件数は1件毎に取得できる（集計は困難）	△ 主なトークンの時価総額は取得できる 取引件数は取得が困難	△ 主なトークンの時価総額は取得が困難 取引件数は1件毎に取得できる（集計は困難）	○ 主なトークンの時価総額・取引件数が取得できる	暗号資産関連データベース等が時価総額を公開している主なガバナンストークンが対象
			DeFiレンディングの取引件数と貸出金利	× データ取得が困難	× データ取得が困難	× データ取得が困難	▲ 一部のDeFiは取得できる	当該DeFiレンディングサービスのウェブサイトから取得できる可能性あり
			DeFiレンディングと取引所の流動性プールの利用率	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			DeFiの利回りと利益	× データ取得が困難	△ DeFiの利回りは取得できる 利益は取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（３）DeFiのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-3　DeFiのデータ取得可能性（２／６）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
DeFi	資産効果	利用できないデータ	リテールと機関投資家の参加者割合	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社がアカウント名等を特定したアドレスが対象
			DAppsの数	× データ取得が困難	× データ取得が困難	× データ取得が困難	▲ 主なDAppsは特定されており、一定の数を集計することは可能と考えられるが、リサーチコストは大きい	一部のBCエクスプローラー（DappRadarなど）でデータが取得できる
			DeFi内のエンティティ（DeFiと伝統的な金融機関とのリンク）	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が金融機関と特定したアドレスが対象
			レバレッジ	▲ 一部のDeFiは取得できる	× データ取得が困難	× データ取得が困難	▲ 一部のDeFiは取得できる	DeFi全体の負債額/資産額等のデータの取得可能性を調査
			ガバナンストークンの保有者情報（どの程度分散されているか。例えば、ガバナンストークンが集中しているエンティティは開発者であると推測可能。）	▲ 保有者アドレスのアカウント名等を特定した一部に限られる アドレス別のトークン保有数の分散状況は取得できる	× データ取得が困難	× データ取得が困難	▲ 保有者アドレスのアカウント名等を特定した一部に限られる アドレス別のトークン保有数の分散状況は取得できる	ブロックチェーン分析会社がアカウント名等を特定したアドレスが対象

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（３）DeFiのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-3　DeFiのデータ取得可能性（３／６）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
DeFi	資産効果	追加すべきデータ	TVL（主要DeFiプロトコルのTVLベースのマーケットシェア）	× データ取得が困難	△ 主なDeFiは取得できる	× データ取得が困難	△ 主なDeFiは取得できる	暗号資産関連データベース等がデータを公開しているDeFiが対象
			ステーブルコインの時価総額	△ 主なステーブルコインは取得できる	△ 主なステーブルコインは取得できる	× データ取得が困難	△ 主なステーブルコインは取得できる	暗号資産関連データベース等が時価総額を公開しているステーブルコインが対象
			主要DeFi間の連関度合い（DEX-Lending等）	△ 主なDeFi間の取引データは1件毎に取得できる（集計は困難）	× データ取得が困難	△ 主なDeFi間の取引データは1件毎に取得できる（集計は困難）	〇 主なDeFi間の取引データが取得できる	
			クロスチェーンブリッジのロックされているトークン総額	△ 主なブリッジは取得できる	× データ取得が困難	× データ取得が困難	△ 主なブリッジは取得できる	ブロックチェーン分析会社がブリッジと特定したアドレスが対象
			クロスチェーンブリッジのVASPとの取引関係	△ 主なDeFiとブリッジ間の取引データは1件毎に取得できる（集計は困難）	× データ取得が困難	× データ取得が困難	△ ブリッジやVASPと特定したアドレスの取引データが一定数は取得できる	ブロックチェーン分析会社がVASPと特定したアドレスが対象
			TVL等の尺度でオラクルのマーケットシェア	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			レンディングプロトコルの担保種別に応じた担保比率、レバレッジ比率、リハイポセケーションの実態	▲ 一部のDeFiは取得できる	× データ取得が困難	× データ取得が困難	▲ 一部のDeFiは取得できる	
			トレジャリープロトコルからの主な送金先アドレス	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社がトレジャリープロトコルと特定したアドレスが対象

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（３）DeFiのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-3　DeFiのデータ取得可能性（４／６）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				備考
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
DeFi	市場信頼性	利用可能なデータ	DeFi関連のインフラ（取引プラットフォーム、ウォレット提供者等）にアクセスできるユーザー数	× データ取得が困難	× データ取得が困難	× データ取得が困難	× データ取得が困難	ステーブルコイン運営者からの情報提供が必要と考えられる
		利用できないデータ	不正取引被害総額	× データ取得が困難	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が不正取引と特定したアドレスが対象
			裏付資産のない暗号資産とステーブルコインの取引割合	△ 主な暗号資産とステーブルコインの取引データは1件毎に取得できる（集計は困難）	× データ取得が困難	△ 主な暗号資産とステーブルコインの取引データは1件毎に取得できる（集計は困難）	△ 主な暗号資産とステーブルコインの取引データは一定数が取得できる	ブロックチェーン分析会社が裏付資産のない暗号資産やステーブルコインと特定したアドレスが対象
		追加すべきデータ	ガバナンストークンの集中度	△ 主なガバナンストークンの取引データは1件毎に取得できる（集計は困難）	× データ取得が困難	× データ取得が困難	△ 主なガバナンストークンの取引データが取得できる	ブロックチェーン分析会社がガバナンストークンと特定したアドレスが対象
			DeFiプロトコルの集中度	× データ取得が困難	× データ取得が困難	× データ取得が困難	△ 主なDeFi別の取引件数・金額が取得できる	ブロックチェーン分析会社がDeFiプロトコルと特定したアドレスが対象
			DeFi関連のハッキング被害総額、件数	× データ取得が困難	× データ取得が困難	× データ取得が困難	△ 主なハッキング事件の被害総額、件数が取得できる	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（３）DeFiのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-3　DeFiのデータ取得可能性（５／６）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
DeFi	金融機関へのエクスポージャー	利用可能なデータ	機関投資家の保有割合	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が機関投資家と特定したアドレスが対象
			暗号資産の資産割合	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	金融機関が保有する暗号資産割合の取得が困難
			暗号資産関連サービスを提供している主要な金融サービス提供者数	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
			デリバティブマーケットの規模	× データ取得が困難	△ 主なDeFiは取得できる	× データ取得が困難	－ （調査対象外）	
			デリバティブ契約の建玉	× データ取得が困難	△ 主なDeFiは取得できる	× データ取得が困難	－ （調査対象外）	
			暗号資産と他の資産クラスとの相関	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	金融機関の資産における暗号資産に関するデータの取得が困難
			取引規模ごとの取引件数分布	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が金融機関と特定したアドレスが対象
		利用できないデータ	暗号資産に投資しているETFの保有割合や残高	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	
		追加すべきデータ	担保としてスマートコントラクトにロックされたトークンを活用した伝統的金融資産への投資額	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	

4-3. 金融安定関連のデータ分析結果
4-3-1. FSB報告書が指摘するデータの取得可能性

（３）DeFiのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-3-1-3　DeFiのデータ取得可能性（６／６）

種別	伝達チャネル	データ区分	調査対象データ	データ取得可能性の調査結果				備考
				BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
DeFi	決済利用	利用可能なデータ	価格（DOT, UNI, LINK）	× データ取得が困難	△ 主なトークン価格が取得できる	× データ取得が困難	△ 主なトークン価格が取得できる	決済で利用される主なトークン価格の取得可能性について調査
			デルタ (1w, 1m, 3m, 6m, 1y)	× データ取得が困難	△ 主なトークン価格の増減が取得できる	× データ取得が困難	△ 主なトークン価格の増減が取得できる	
		利用できないデータ	取引件数と金額	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が決済サービスと特定したアドレスが対象
			支払人と受取人の法域	× データ取得が困難	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等と法域を特定した一部（VASPなど）に限られる	ブロックチェーン分析会社がアカウント名等を特定したアドレスが対象
			取引形態（例えば、送金、電子商取引、貿易）	× データ取得が困難	× データ取得が困難	× データ取得が困難	－ （調査対象外）	取引形態に関するデータは取得が困難

4-3. 金融安定関連のデータ分析結果
4-3-2. リサーチ調査項目

- 本章では、以下の4つの調査項目について、VASPやレンディング事業者などのカテゴリ別にアドレス保有者数や取引件数・金額など具体的な調査項目を設定し、ブロックチェーン分析会社の専門家によるリサーチを行った。
- リサーチ結果は、データを整理のうえ表やグラフに整理し、結果から見られる傾向や特徴について考察を行った。

表4-3-2 リサーチ調査項目

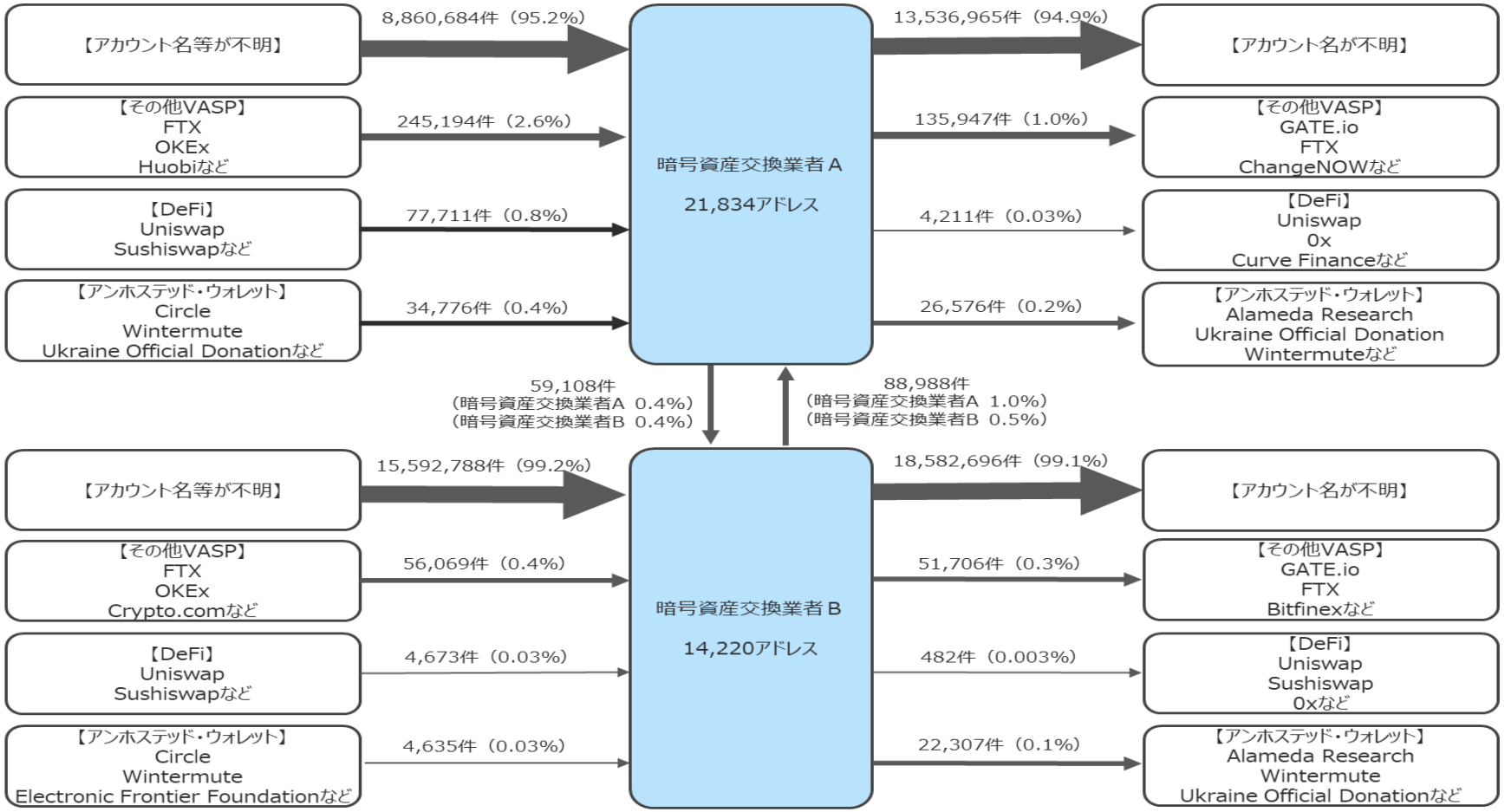
調査項目	調査内容	補足
主なVASPの取引件数の傾向	• 主な暗号資産取引業者２社について、受信・自業者内・送信の３つに分けて取引件数、取引金額を調査した。 • ①カテゴリ別、②トークン別、③カテゴリ別のうちDeFi内訳の３つについて調査した。	• アカウントのカテゴリ名やアカウント名は、ブロックチェーン分析会社が定義した分類を使用した。 • DeFiのサービス種別は、Webの公開情報を参考にして弊社で定義した。 • 取引金額は2023年4月時点のトークン価格等のレートを使用した。
主なレンディング事業者の取引件数の傾向	• 主なレンディング事業者１社について、受信・自業者内・送信の３つに分けて取引件数、取引金額を調査した。 • ①カテゴリ別、②トークン別、③カテゴリ別のうちDeFi内訳の３つについて調査した。	
ステーブルコイン関連データ	• 主要なステーブルコイン3種類（USDC・USDC・DAI）について、送金実態や凍結対象データなどを調査委した。	
DeFi関連データ	• 主なDeFiプロジェクト（Uniswap・Maker・Aave）について、DeFiの規模やガバナンストークン保有者数、担保比率やリハイポセケーション（担保流用）の実態などを調査した。 • DeFi全体の実態調査として、クロスチェーン・ブリッジ利用状況、ハッキング被害の実態、金融機関との連携、特定のオラクルサービスへの集中度合いなどについて調査した。	

4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP

（1）主なVASP：暗号資産交換業者A/暗号資産交換業者Bの取引件数の概要

- 識別できた取引の中では、VASP間での取引が多く、取引所等の密接な連関が示唆されている。加えて、VASPとDeFi、VASPとステーブルコイン発行主体・投資会社等との取引も確認でき（定義上、アンホステッドウォレットに含まれる）、これらの間で密接な取引関係が存在している可能性がある。
- アカウント名等が不明なアドレスとの取引件数が95%以上を占めており、今回の分析結果が必ずしもVASP関連の全体の傾向を示すものではないことを認識しておく必要がある。

図4-3-3-1　主なVASPの取引の概要



4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP（暗号資産交換業者A）

（２）主なVASP：暗号資産交換業者A　カテゴリ別

図4-3-3-2　暗号資産交換業者Aのカテゴリ別取引件数・金額

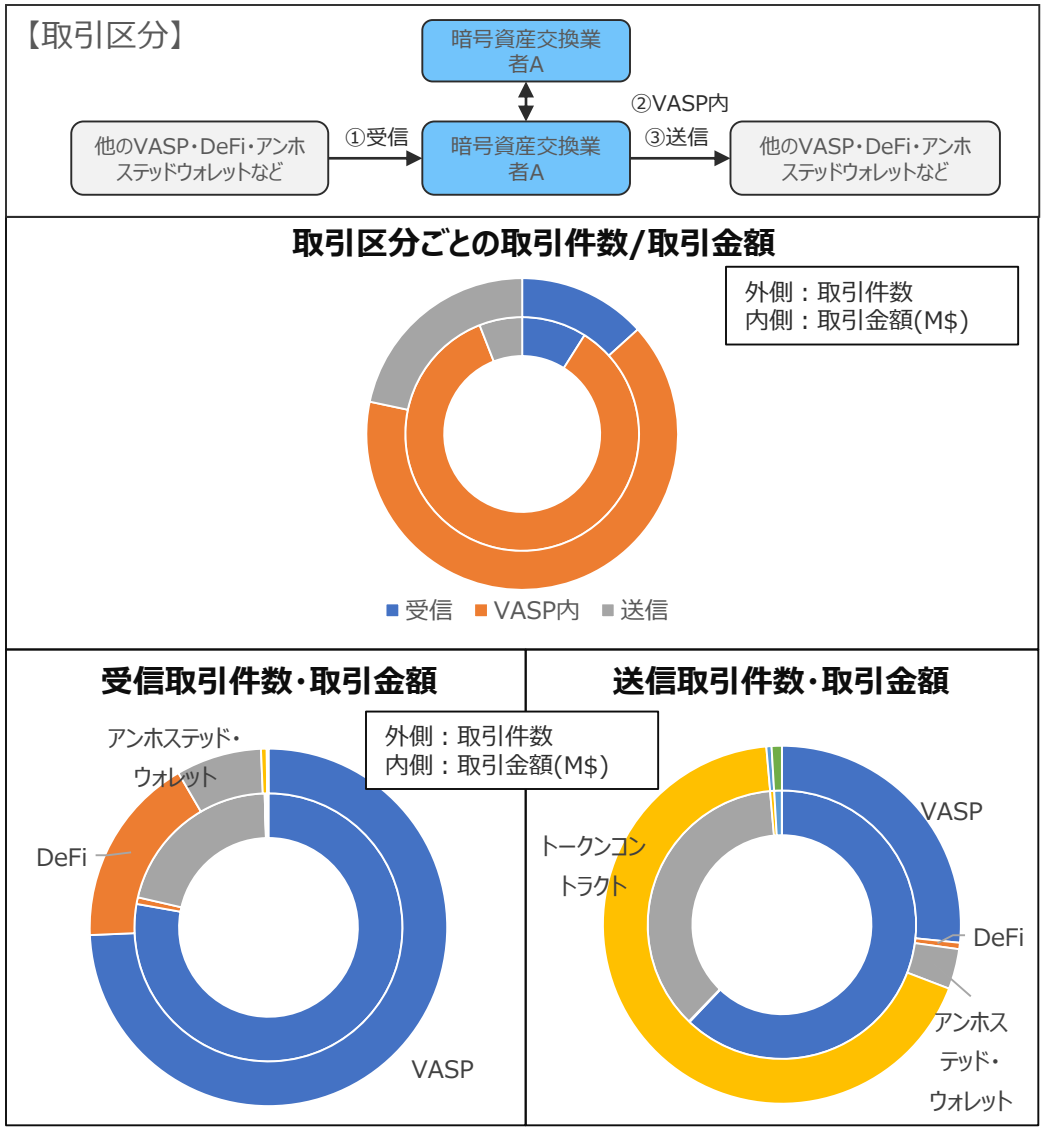


表4-3-3-2　暗号資産交換業者Aのカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	取引件数		取引金額	
		件数	件数比率	金額M$	件数比率
①受信	VASP	334,182	74.3%	51,239	77.8%
	DeFi	77,711	17.3%	528	0.8%
	アンホステッド・ウォレット	34,776	7.7%	13,791	20.9%
	トークンコントラクト	2,320	0.5%	27	0.0%
	ブリッジ（他チェーンへの送金）等	566	0.1%	148	0.2%
	その他	133	0.0%	123	0.2%
	合計	449,688	100.0%	65,856	100.0%
②VASP内	VASP	2,198,665	100.0%	625,406	100.0%
	合計	2,198,665	100.0%	625,406	100.0%
③送信	VASP	195,055	26.6%	27,079	62.1%
	DeFi	4,211	0.6%	46	0.1%
	アンホステッド・ウォレット	26,576	3.6%	15,873	36.4%
	トークンコントラクト	496,837	67.8%	217	0.5%
	ブリッジ（他チェーンへの送金）等	3,451	0.5%	398	0.9%
	その他	6,756	0.9%	0	0.0%
	合計	732,886	100.0%	43,613	100.0%

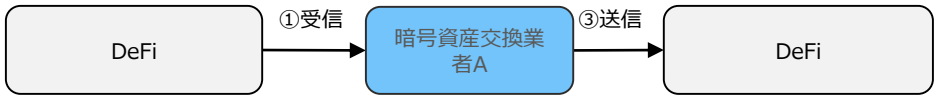
【考察】
- ②同一のVASP内の取引件数・金額が最も多い
  → 事業者内のウォレットの内部資金移動によるものが多いか
- ①受信は他のVASP、③送信はトークンコントラクト、VASPの取引件数が大半を占める一方で、DeFiやアンホステッド・ウォレットの取引も相当数認められる
  → トークンコントラクトはERC-20規格に準拠したトークンの転送（全体の62%がUSDTの転送など、但し取引金額は小さく、実際の送金（VASPなど別カテゴリでカウント）と一部ダブルカウントされている可能性）、DeFiはDEX利用、アンホステッド・ウォレットはその後のDeFi利用などが目的と考えられるか

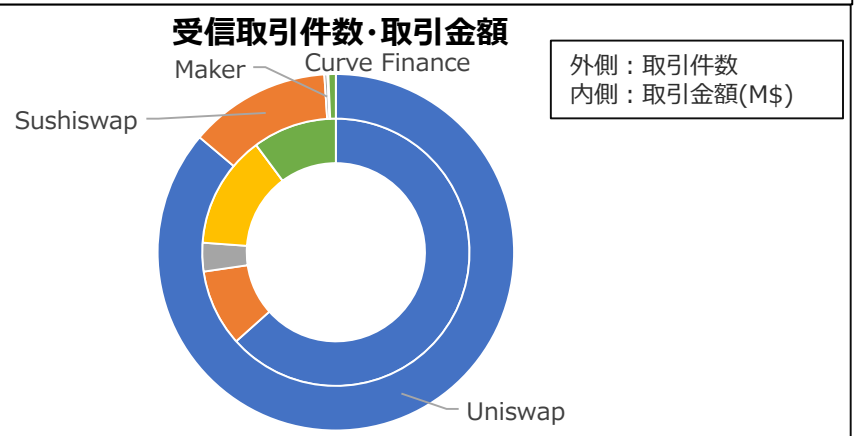
4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP（暗号資産交換業者A）

（３）主なVASP：暗号資産交換業者A　カテゴリ別のうちDeFi内訳

図4-3-3-3　暗号資産交換業者Aのカテゴリ別取引（うちDeFi）件数・金額

【取引区分】





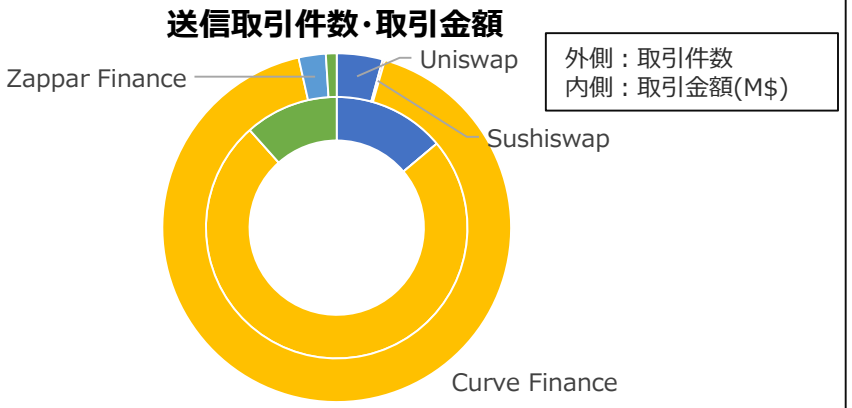


表4-3-3-3　暗号資産交換業者Aのカテゴリ別取引（うちDeFi）データ

カテゴリ名のうちDeFi内訳	サービス種別	①受信			③送信		
		取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
Uniswap	分散型取引所	66,954	86.2%	335	179	4.3%	6
Sushiswap	分散型取引所	9,955	12.8%	49	9	0.2%	0
Maker	ステーブルコイン発行	215	0.3%	18	0	0.0%	0
Curve Finance	分散型取引所	65	0.1%	72	3,875	92.0%	34
Zappar Finance	DeFiダッシュボード	1	0.0%	0	106	2.5%	0
その他	–	521	0.7%	54	42	1.0%	5
合計		77,711	100.0%	528	4,211	100.0%	46

【考察】

- DeFi全体では分散型取引所の取引件数・取引金額が多い（全体の95%以上）
  → 分散型取引所は暗号資産の交換やステーキングの送金が多いと考えられる
- 分散型取引所のうち、受信はUniswap、送信はCurve Financeの取引件数が多い
  → 理由は必ずしも定かではないが、①Uniswapは多種類のトークン交換（約800種類）、②Curve Financeはステーブルコイン交換等に活用されているか

4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP（暗号資産交換業者A）

（４）主なVASP：暗号資産交換業者A　トークン別

図4-3-3-4　暗号資産交換業者Aのトークン別取引件数・金額

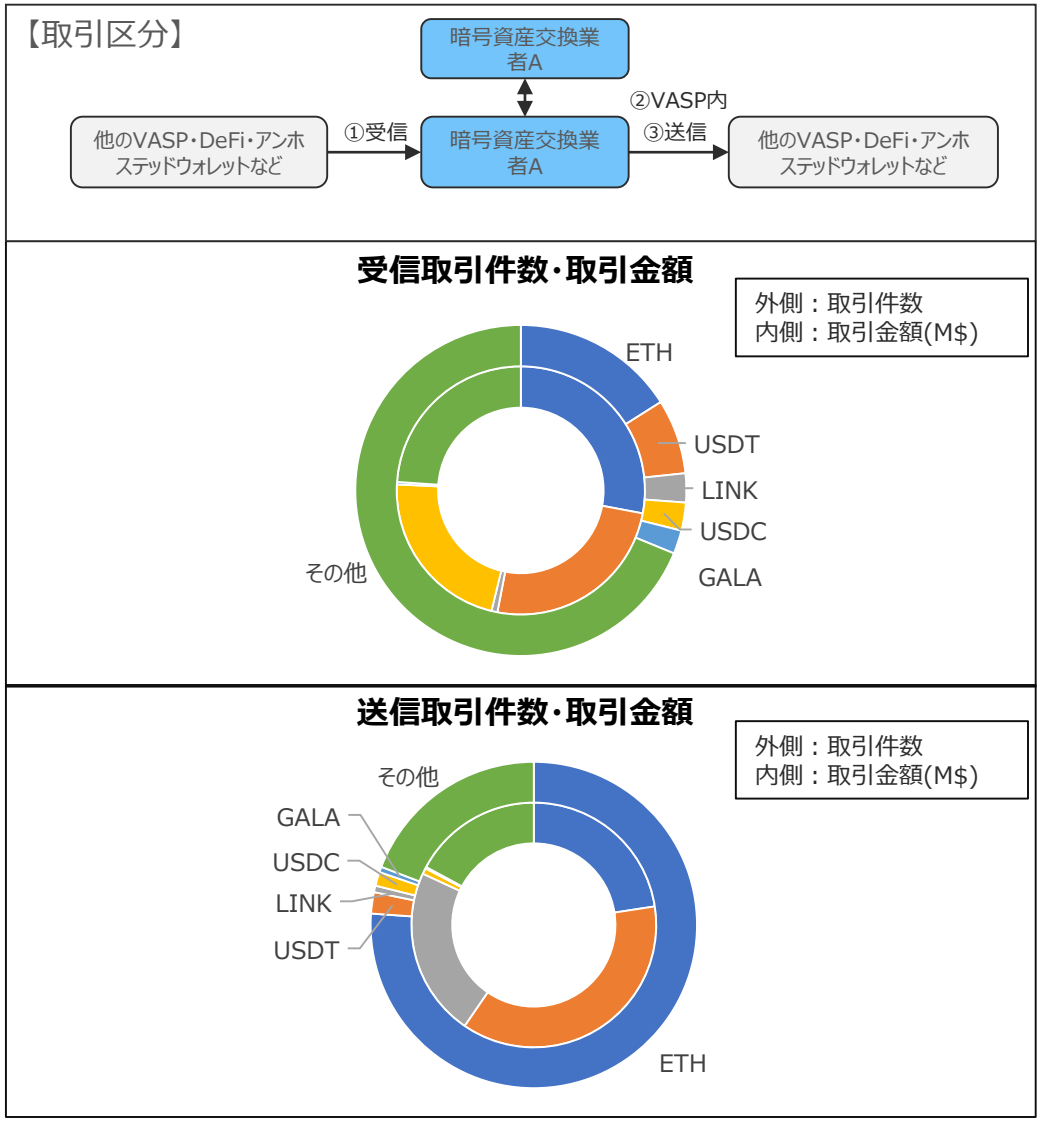


表4-3-3-4　暗号資産交換業者Aのトークン別取引データ

アカウントの利用トークン別	種別	①受信			②VASP内			③送信		
		取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
ETH	ネイティブトークン	72,095	16.0%	18,416	1,581,015	71.9%	196,040	557,875	76.1%	9,845
USDT	ステーブルコイン	32,849	7.3%	16,509	84,191	3.8%	164,185	15,463	2.1%	16,135
LINK	外部オラクル用	12,744	2.8%	513	15,317	0.7%	84,536	4,769	0.7%	9,736
USDC	ステーブルコイン	12,319	2.7%	14,470	18,349	0.8%	4,396	10,120	1.4%	336
GALA	ゲーム用	10,337	2.3%	208	11,500	0.5%	2,300	3,924	0.5%	89
その他	–	※309,344	68.8%	15,740	488,293	22.2%	173,949	140,735	19.2%	7,473
合計		449,688	100.0%	65,856	2,198,665	100.0%	625,406	732,886	100.0%	43,613

※①受信の「その他」は約1,100種類のトークンに対する取引件数

【考察】

- 全ての取引区分でETH・USDT・USDCの取引件数・金額が多い
  → 主要トークンとして、その他トークンとの交換等に利用されることが多いためと考えられる
- ①受信・②VASP内の取引件数・金額はETHが最も多く、③送信の取引件数はETH、取引金額はUSDTが最も多い。USDTは他と比べて取引１件あたりの金額が多い
  → 他のVASPとの資金移動にETHとUSDTを多く使用していると考えられる
- LINK（外部オラクルサービスChainlink利用トークン）の取引件数が多い
  → 外部オラクルサービスのChainlinkを利用するDeFiが多いためと考えられる
- GALA（Gala Gamesのゲーム利用トークン）の取引件数が多い
  → 当ゲーム利用のためと考えられる
  （Gala Games：23年5月時点　総供給量390億トークン、トークン保有者23万アドレス）

4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP（暗号資産交換業者B）

（５）主なVASP：暗号資産交換業者B　カテゴリ別

図4-3-3-5　暗号資産交換業者Bのカテゴリ別取引件数・金額

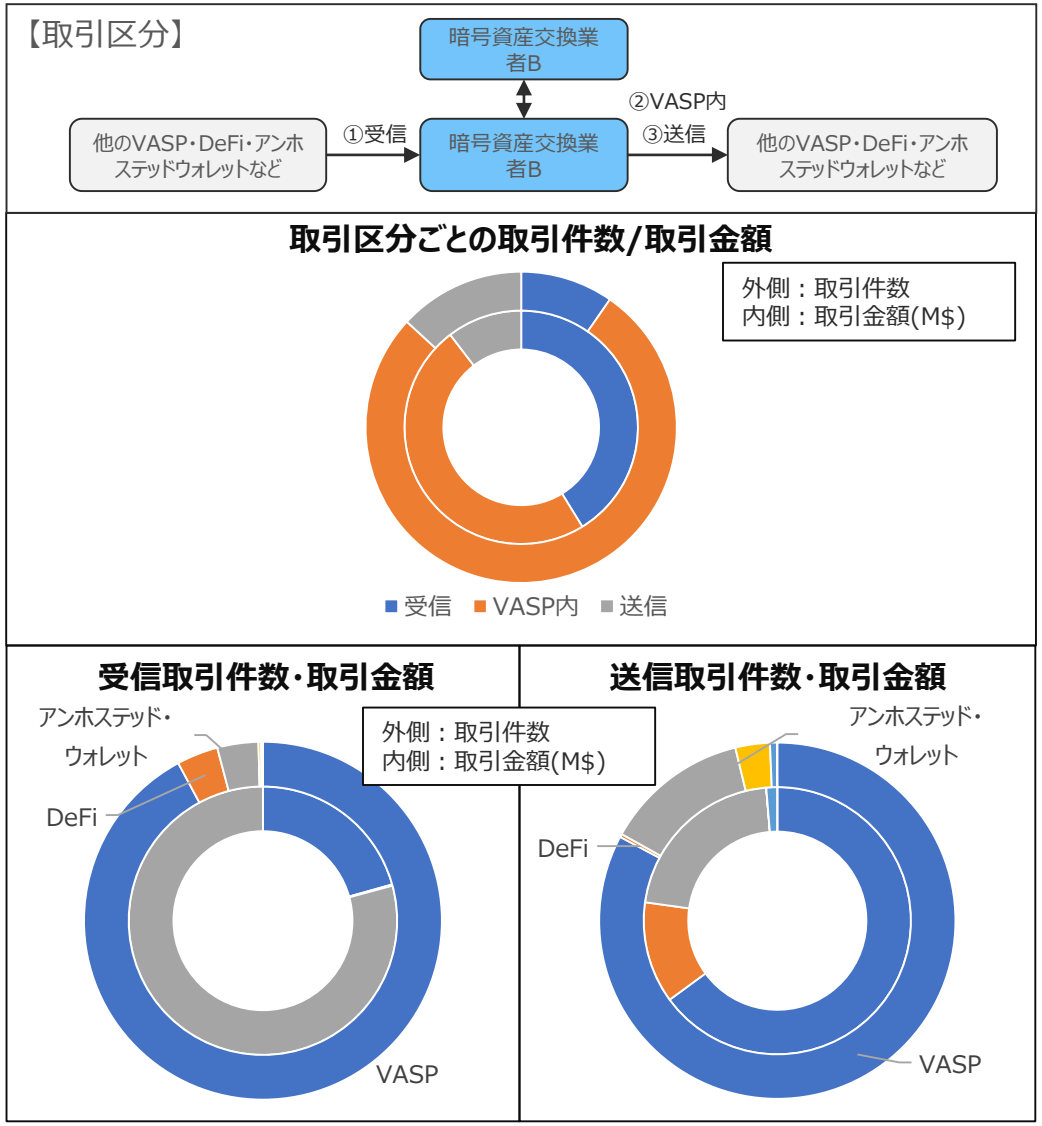


表4-3-3-5　暗号資産交換業者Bのカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	取引件数		取引金額	
		件数	件数比率	金額M$	件数比率
①受信	VASP	115,177	92.1%	17,190	20.6%
	DeFi	4,673	3.7%	123	0.1%
	アンホステッド・ウォレット	4,635	3.7%	65,944	79.2%
	トークンコントラクト	306	0.2%	0	0.0%
	ブリッジ（他チェーンへの送金）等	192	0.2%	1	0.0%
	その他	6	0.0%	0	0.0%
	合計	124,989	100.0%	83,259	100.0%
②VASP内	VASP	999,058	100.0%	97,707	100.0%
	合計	999,058	100.0%	97,707	100.0%
③送信	VASP	140,704	82.8%	13,655	64.9%
	DeFi	482	0.3%	2,583	12.3%
	アンホステッド・ウォレット	22,307	13.1%	4,514	21.5%
	トークンコントラクト	5,320	3.1%	1	0.0%
	ブリッジ（他チェーンへの送金）等	1,072	0.6%	279	1.3%
	その他	51	0.0%	0	0.0%
	合計	169,936	100.0%	21,032	100.0%

【考察】
- 取引区分は、②VASP内の取引件数が最も多い
  → VASP内のウォレットの内部資金移動によるものが多いか
- 自社内取引以外では、①受信、③送信とも他のVASPとの取引件数が大半を占める
  → 他の大手VASPとの資金移動が多いと考えられる
- 次に多いカテゴリは、①受信はDeFiとアンホステッド・ウォレット、③送信はアンホステッド・ウォレットである
  → DeFiは分散型取引所のトークン交換、アンホステッド・ウォレットはDeFi利用等が目的として考えられるか
- ①受信の取引金額は、アンホステッド・ウォレットが最も多い
  → DeFiサービスなどで利用した資金を、アンホステッド・ウォレットを経由してVASPのウォレットに移動する動きと考えられるか

4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP（暗号資産交換業者B）

（６）主なVASP：暗号資産交換業者B　カテゴリ別のうちDeFi内訳

図4-3-3-6　暗号資産交換業者Bのカテゴリ別取引（うちDeFi）件数・金額

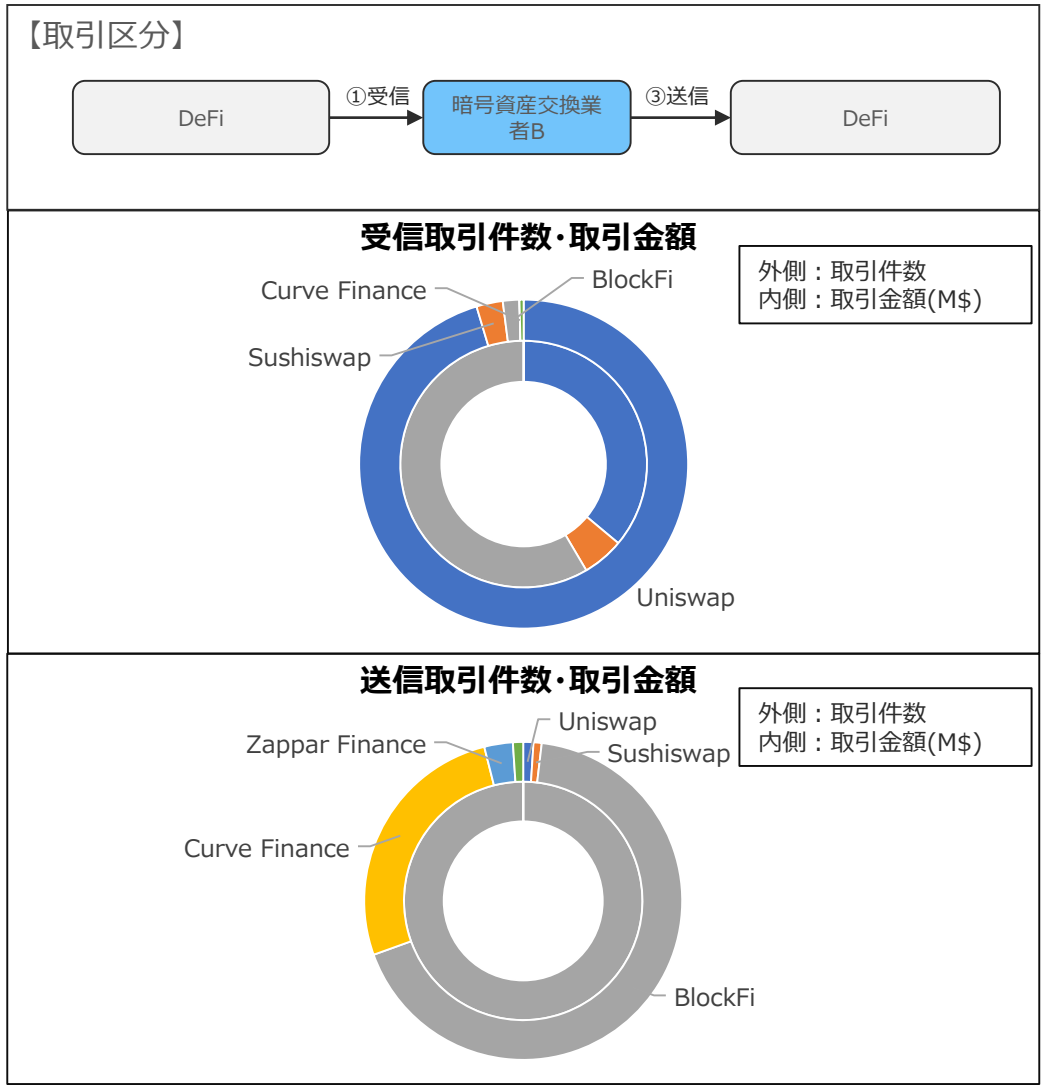


表4-3-3-6　暗号資産交換業者Bのカテゴリ別取引（うちDeFi）データ

カテゴリ名のうちDeFi内訳	サービス種別	①受信			③送信		
		取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
Uniswap	分散型取引所	4,457	95.4%	19	5	1.0%	0
Sushiswap	分散型取引所	121	2.6%	3	4	0.8%	0
BlockFi	レンディング事業者	76	1.6%	30	326	67.6%	2,583
Curve Finance	分散型取引所	0	0.0%	0	128	26.6%	0
Zappar Finance	DeFiダッシュボード	0	0.0%	0	14	2.9%	0
その他	–	19	0.4%	0	5	1.0%	0
合計		4,673	100.0%	52	482	100.0%	2,583

【考察】

- ①受信は分散型取引所、②送信はレンディング事業者の取引件数が多い
  → 分散型取引所は暗号資産の交換やステーキングの送金、レンディング事業者は暗号資産の貸出サービス利用によるものと考えられる
- 分散型取引所のうち、受信はUniswap、送信はCurve Financeの取引件数が多い
  → ①受信のUniswapは多種類のトークン交換（約800種類）、②送信のCurve Financeはステーブルコイン交換に活用されているか

4-3. 金融安定関連のデータ分析結果
4-3-3. 主なVASP（暗号資産交換業者B）

（7）主なVASP：暗号資産交換業者B トークン別

図4-3-3-7 暗号資産交換業者Bのトークン別取引件数・金額

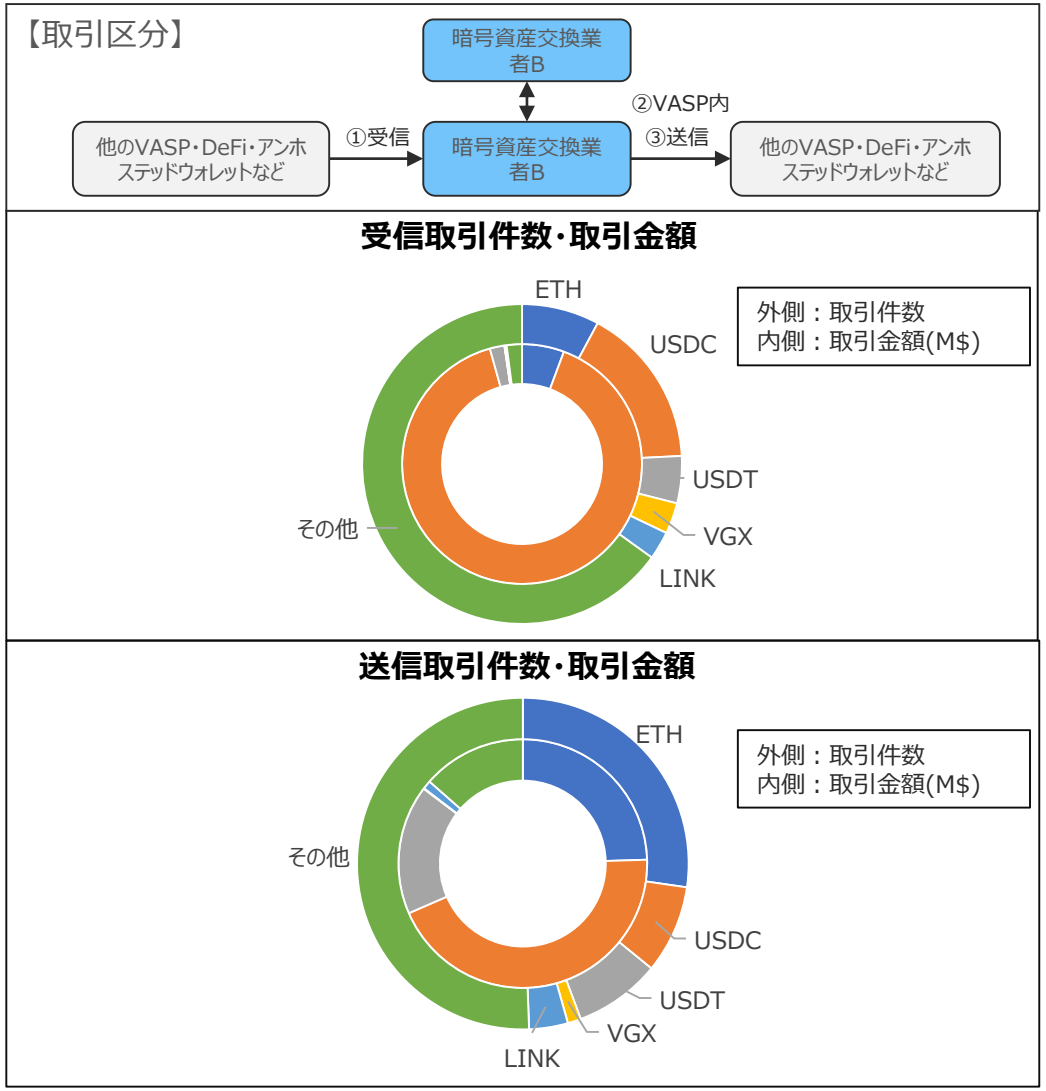


表4-3-3-7 暗号資産交換業者Bのトークン別取引データ

アカウントの利用トークン別	種別	①受信			②VASP内			③送信		
		取引件数	件数比率	取引金額 M$	取引件数	件数比率	取引金額 M$	取引件数	件数比率	取引金額 M$
ETH	ネイティブトークン	9,804	7.8%	4,723	848,157	84.9%	9,345	46,376	27.3%	5,155
USDC	ステーブルコイン	20,433	16.3%	74,866	45,016	4.5%	82,798	14,612	8.6%	9,249
USDT	ステーブルコイン	5,957	4.8%	1,636	16,371	1.6%	3,031	14,333	8.4%	3,541
VGX	VASP発行トークン	3,922	3.1%	47	3,411	0.3%	54	2,201	1.3%	14
LINK	外部オラクル用	3,563	2.9%	203	5,038	0.5%	391	6,424	3.8%	233
その他	–	※81,310	65.1%	1,713	81,065	8.1%	2,100	85,990	50.6%	2,845
合計	合計	124,989	100.0%	83,188	999,058	100.0%	97,719	169,936	100.0%	21,038

※①受信の「その他」は約600種類のトークンに対する取引件数

【考察】

- 全ての取引区分でETH・USDT・USDCの取引件数が多い
  → 主要トークンとして、その他トークンとの交換等に利用されることが多いためと考えられる
- VGX（VASPVoyagerが発行するトークン）の取引件数が多い
  → 主なVASP間の資金移動によるものと考えられる
  （23年5月時点：総供給量2.9億トークン、トークン保有者6,500アドレス）
- LINK（外部オラクルサービスChainlink利用トークン）の取引件数が多い
  → 外部オラクルサービスのChainlinkを利用するDeFiが多いためと考えられる

4-3. 金融安定関連のデータ分析結果
4-3-4. 主なレンディング事業者

（1）主なレンディング事業者：カテゴリ別

図4-3-4-1　レンディング事業者のカテゴリ別取引件数・金額

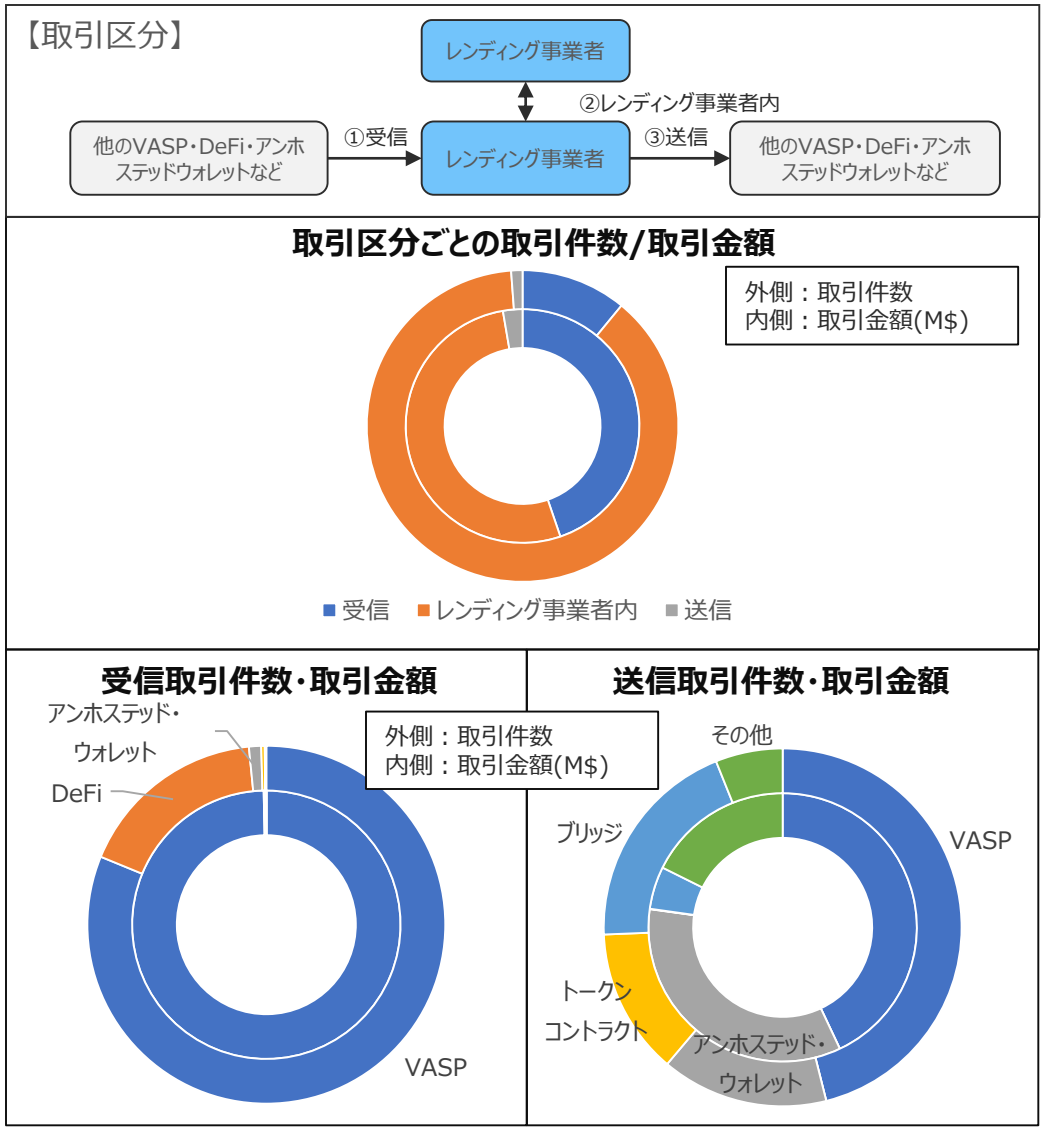


表4-3-4-1　レンディング事業者のカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	取引件数		取引金額	
		件数	件数比率	金額M$	件数比率
①受信	VASP	12,841	81.2%	6,807	99.7%
	DeFi	2,727	17.2%	6	0.1%
	アンホステッド・ウォレット	174	1.1%	15	0.2%
	トークンコントラクト	50	0.3%	0	0.0%
	ブリッジ（他チェーンへの送金）等	12	0.1%	0	0.0%
	その他	10	0.1%	0	0.0%
	合計	15,814	100.0%	6,828	100.0%
②レンディング事業者内	レンディング事業者	126,946	100.0%	8,015	100.0%
	合計	126,946	100.0%	8,015	100.0%
③送信	VASP	782	46.1%	177	43.0%
	DeFi	0	0.0%	0	0.0%
	アンホステッド・ウォレット	256	15.1%	141	34.2%
	トークンコントラクト	224	13.2%	0	0.0%
	ブリッジ（他チェーンへの送金）等	332	19.6%	21	5.1%
	その他	103	6.1%	73	17.6%
	合計	1,697	100.0%	412	100.0%

【考察】

- 取引区分は、②レンディング事業者内の取引件数が最も多い
  → 自社サービス内のウォレットの内部資金移動によるものと考えられる
- 取引区分のうち、①受信の取引件数が、③送信よりも多い
  → ①受信は暗号資産の貸出サービス利用のため取引件数が多く、③送信は資金の引き出しのため取引件数が少ないと考えられる
- カテゴリ別では、①受信、③送信とも他のVASPとの取引件数が多い。次に多いカテゴリは、①受信はDeFi、③送信はカストディ業者等、アンホステッド・ウォレットである
  → 必ずしも背景は明らかではないが、例えば暗号資産のステーキングサービス利用などが活用目的として考えられるか

4-3. 金融安定関連のデータ分析結果
4-3-4. 主なレンディング事業者

（２）主なレンディング事業者：カテゴリ別のうちDeFi内訳

図4-3-4-2 レンディング事業者のカテゴリ別取引（うちDeFi）件数・金額

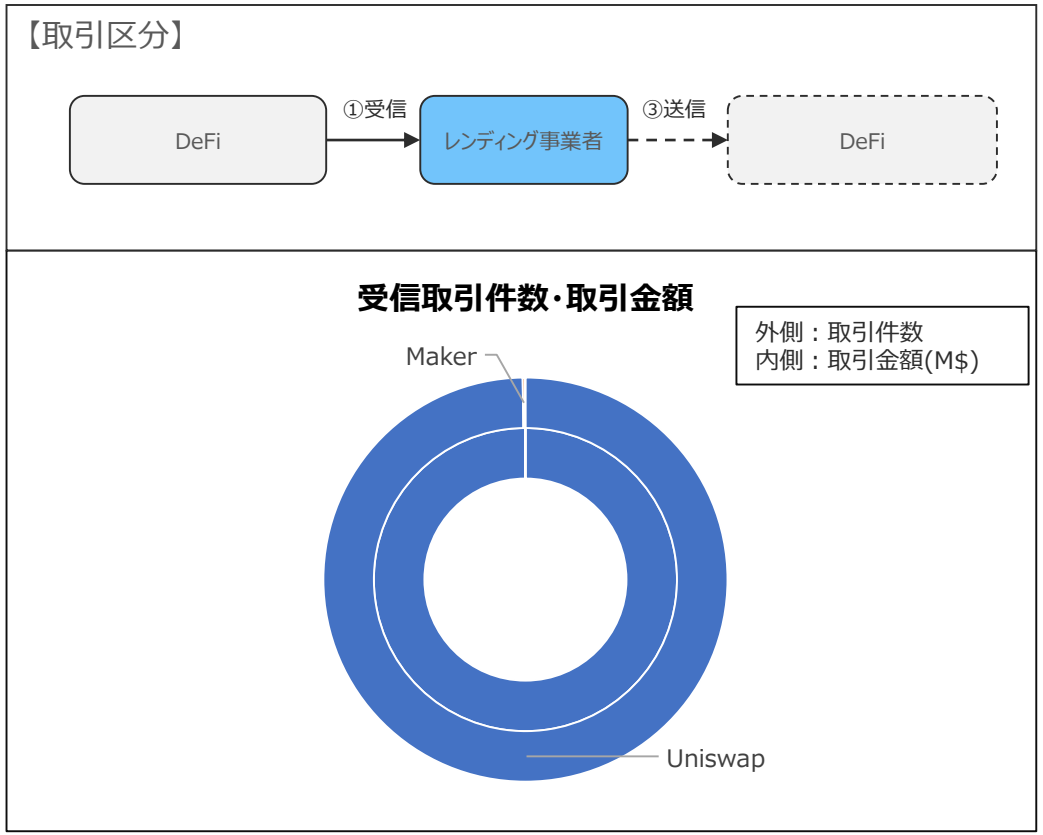


表4-3-4-2 レンディング事業者のカテゴリ別取引（うちDeFi）データ

カテゴリ名のうち DeFi内訳	サービス種別	①受信		
		取引件数	件数比率	取引金額 M$
Uniswap	分散型取引所	2,721	99.8%	6
Maker	ステーブルコイン発行	5	0.2%	0
Compound	レンディング	1	0.0%	0
合計		2,727	100.0%	6

※③送信は該当取引なし

【考察】

- ①受信は分散型取引所の取引が多い
  → 多種類のトークン交換と考えられる（約300種類）
- DeFiの①受信と②送信の取引件数が異なる
  → 分散型取引所の取引件数が多いことによるもの

4-3. 金融安定関連のデータ分析結果
4-3-4. 主なレンディング事業者

（３）主なレンディング事業者：トークン別

図4-3-4-3　レンディング事業者のトークン別取引件数・金額

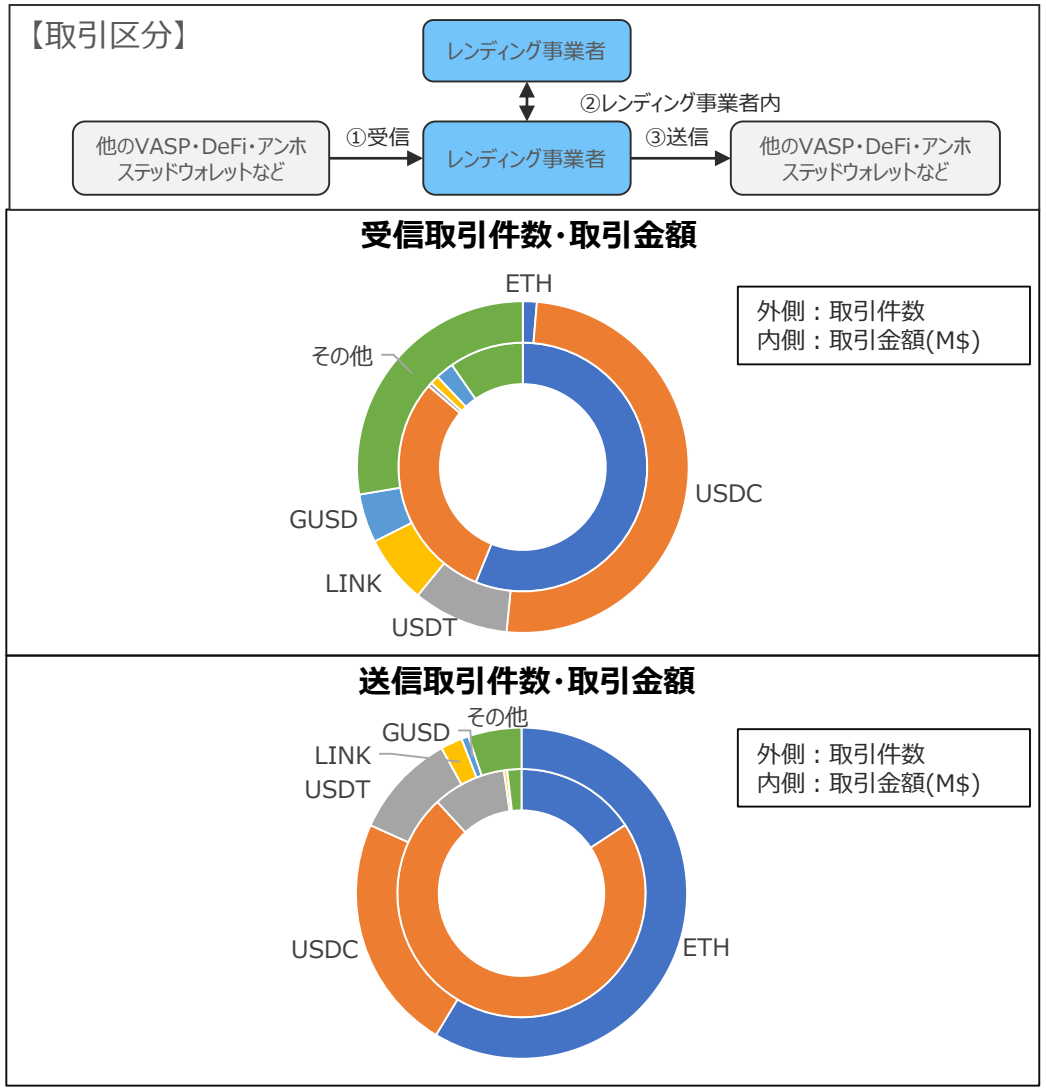


表4-3-4-3　レンディング事業者のトークン別取引データ

アカウントの利用トークン別	種別	①受信			②レンディング事業者内			③送信		
		取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
ETH	ネイティブトークン	215	1.4%	3,836	77,958	61.4%	2,346	995	58.6%	65
USDC	ステーブルコイン	7,941	50.2%	2,057	29,412	23.2%	3,784	392	23.1%	298
USDT	ステーブルコイン	1,478	9.3%	36	4,932	3.9%	994	174	10.3%	39
LINK	外部オラクル用	1,057	6.7%	78	2,614	2.1%	117	36	2.1%	2
GUSD	ステーブルコイン	750	4.7%	162	5,474	4.3%	476	12	0.7%	0
その他	–	※4,373	27.7%	659	6,556	5.2%	298	88	5.2%	8
合計		15,814	100.0%	6,828	126,946	100.0%	8,015	1,697	100.0%	412

※①受信の「その他」は約300種類のトークンに対する取引件数

【考察】

- 全ての取引区分でETH・USDT・USDCの取引件数が多い
  → 主要トークンとして、その他トークンとの交換等に利用されることが多いためと考えられる
- LINK（外部オラクルサービスChainlink利用トークン）の取引件数が多い
  → 外部オラクルサービスのChainlinkを利用するDeFiが多いためと考えられる
- GUSD（VASPGeminiが発行するトークン）の取引が多い
  → VASP内の資金移動によるもの
  （GUSD：23年5月時点　総供給量5.4億トークン、トークン保有者1.0万アドレス）

4-3. 金融安定関連のデータ分析結果
4-3-5. ステーブルコイン関連

- 今回調査した3種類のステーブルコイン間で若干の傾向は見られるものの、総体としてはDeFiでのステーブルコイン利用が圧倒的に多いことが確認された。
- アルゴリズム型ステーブルコインであるDAIではアドレス凍結の実例は確認できなかった（凍結機能が存在しない可能性）。
- アンホステッド・ウォレットは、送金先アドレスは多いが取引件数・金額はDeFiやVASPよりも少ないことが確認された。これは、DeFiやVASPの取引が特定の送金先（分散型交換所や大手VASPなど）に集中しているためと考えられる。

表4-3-5　ステーブルコインのデータ調査結果

カテゴリ	調査対象項目	調査対象データ	オンチェーンデータ調査結果			備考
			USDCステーブルコイン	USDTステーブルコイン	DAIステーブルコイン	
ステーブルコイン関連	ステーブルコインの送金実態（主なユースケース、送金規模など）	送金先アドレス	計2,057件 【内訳】 アンホステッド・ウォレット 1,020件 トークンコントラクト　698件 VASP　128件　など	計1,657件 【内訳】 アンホステッド・ウォレット 689件 トークンコントラクト　630件 VASP　151件　など	計899件 【内訳】 アンホステッド・ウォレット 321件 トークンコントラクト 311件 VASP 105件　など	
		上記アドレスの取引件数・取引額	796.6万件/14,021億USD 【内訳】 DeFi 405.9万件/7,514億USD VASP 195万件/11億USD アンホステッド・ウォレット 61.5万件/1,381億USD など	809.3万件/2,362億USD 【内訳】 VASP 510.9万件/26億USD DeFi 186.5万件/934億USD アンホステッド・ウォレット 18.8万件/215億USD など	127.2万件/5,095億USD 【内訳】 DeFi 64.8万件/4,282億USD VASP 19.3万件/0.8億USD アンホステッド・ウォレット 8.7万件/193億USD など	
	発行主体により凍結されたステーブルコインに関連するデータ（凍結対象アドレス、凍結額合計など）	凍結対象アドレス	159アドレス	858アドレス	–	2023年4月までの全件
		凍結額合計/アドレス毎の平均額	785.9万USD/21アドレス 平均37.4万USD	4.4億USD/777アドレス 平均56.7万USD	–	2023年4月までの全件

4-3. 金融安定関連のデータ分析結果
4-3-6. DeFi関連

（1）DeFi関連

表4-3-6-1　DeFiのデータ調査結果（1／2）

カテゴリ	調査対象項目	調査対象データ	オンチェーンデータ調査結果			備考
			Uniswap分散型取引所	Makerステーブルコイン発行	Aaveレンディング事業者	
DeFi関連	DeFi全体の規模（TVLやユーザー数、ステーブルコインの時価総額等）	DeFi毎のTVL	40.9億USD（UNI）	72.3億USD（DAI）	51.8億USD（AAVE）	2023/5時点
		トークン/ステーブルコインの保有者数	（ガバナンストークン欄に記載）	50.7万アドレス（DAI）	（ガバナンストークン欄に記載）	2023/5時点
		トークン/ステーブルコインの時価総額	29.4億USD（UNI）	49.8億USD（DAI）	9.4億USD（AAVE）	2023/5時点
	DeFiの脆弱性（ガバナンストークンやDeFiプロトコルの集中度等）	ガバナンストークン保有者アドレス数	37.0万アドレス（UNI）	9.5万アドレス（MKR）	16.1万アドレス（AAVE）	2023/5時点
		ガバナンストークン保有者アドレスの取引件数	送信：213.7万件 受信：210.5万件	送信：113.9万件 受信：112.1万件	送信：96.6万件 受信：102.0万件	
	特定のオラクルサービスへの集中度合い	DeFi毎のオラクルサービス利用動向	自プロジェクト内でオラクル機能を開発（TWAP：時間加重平均価格）	自プロジェクト内でオラクル機能を開発（オラクル価格フィード）	外部オラクルサービスを利用（Chainlink）	2023/4時点
	レンディング・プロトコル関連データ	担保種別に応じた担保比率	–	19種類 102%～5000%	10種類 125%～200%	2023/4時点
		レバレッジ比率 （レバレッジ比率＝総負債額/総資産額で算出）	–	6種類のトークンなど 96.6～99.9%	14種類のトークン 0.4～77.9%	2023/4時点

4-3. 金融安定関連のデータ分析結果
4-3-6. DeFi関連

（1）DeFi関連

表4-3-6-1　DeFiのデータ調査結果（2／2）

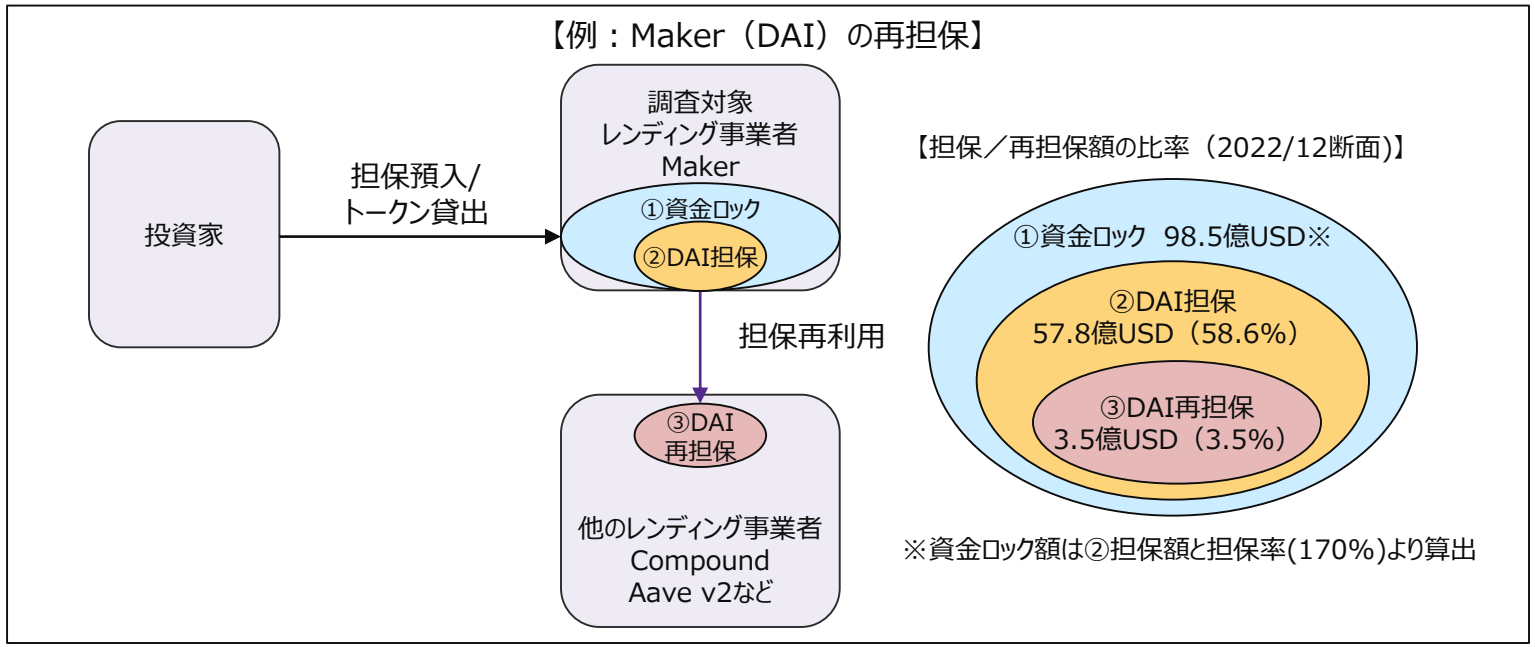
<table>
<tr><th>カテゴリ</th><th>調査対象項目</th><th>調査対象データ</th><th>データ調査結果
（オンチェーン／オフチェーン）</th><th>備考</th></tr>
<tr><td rowspan="8">DeFi関連</td><td rowspan="3">クロスチェーン・ブリッジの利用実態（ロックされているトークン総額、VASP等との取引関係など）</td><td>クロスチェーン・ブリッジのアドレス</td><td>18アドレス</td><td rowspan="3">【主なクロスチェーン・ブリッジ】 2023/4時点
<table><tr><th>クロスチェーン・ブリッジ</th><th>ロックされている金額</th></tr><tr><td>Polygon Bridges</td><td>33.0億USD</td></tr><tr><td>Arbitrum Bridges</td><td>22.9億USD</td></tr><tr><td>Avalanche Bridge</td><td>15.3億USD</td></tr><tr><td>Optimism Bridges</td><td>12.8億USD</td></tr><tr><td>Ronin Bridge</td><td>7.0億USD</td></tr></table></td></tr>
<tr><td>ロックされているトークン総額</td><td>95.0億USD</td></tr>
<tr><td>上記アドレスのVASPとの取引件数</td><td>1,027.0万件</td></tr>
<tr><td rowspan="2">DeFi関連のハッキング被害の実態（被害総額、件数など）</td><td>ハッキングされたDeFiの特定</td><td>ハッキング事件10件発生</td><td>2022年発生分</td></tr>
<tr><td>ハッキング総額</td><td>24.9億USD</td><td>2022年発生分</td></tr>
<tr><td rowspan="2">伝統的金融セクターとDeFiの連携の実態（担保としてスマートコントラクトにロックされたトークンを活用した伝統的金融資産への投資額など）</td><td>金融機関の保有アドレス</td><td>155アドレス</td><td>ブロックチェーン分析業者の保有情報</td></tr>
<tr><td>金融機関とDeFiとの連携取引件数</td><td>13,252件</td><td></td></tr>
<tr><td>特定のオラクルサービスへの集中度合い</td><td>外部オラクルサービスと利用DeFi数</td><td>・Chainlink：263プロジェクトが利用
・TWAP（Uniswapが提供）
：78プロジェクトが利用
・Chronicle：2プロジェクトが利用</td><td></td></tr>
<tr><td>DEX関連データ（例：主要トークンペアの流動性、DEXと取引関係が深いエンティティ）</td><td>主要トークンペアの流動性</td><td>・主要なトークンペア：31ペア（Uniswap：WETH・USDC・USDT・DAI・MATICなど）
・プールしているTVL総額：101.3億ドル</td><td></td></tr>
</table>

4-3. 金融安定関連のデータ分析結果
4-3-6. DeFi関連

（２）リハイポセケーション（担保流用）

表4-3-6-2　DeFi（リハイポセケーション）のデータ調査結果

カテゴリ	調査対象項目	調査対象データ	ブロックチェーン分析会社リサーチ結果				
			データソース	データ取得方法	Uniswap	Maker	Aave
DeFi関連	レンディング・プロトコル関連データ	リハイポセケーション（担保流用）の実態	Etherscan Dune Analytics 自社データベース	調査対象のレンディング事業者の担保を、他のレンディング事業者に再利用した貸出残高を取得 （2022/12時点） ※担保対象は自社発行トークンのみ （DAI/AAVE）	（対象外）	計34,682万USD 【内訳】 Compound 25,686万USD Aave v2 7,765万USD Aave v1 475万USD　など	計16.3万USD 【内訳】 Maker　14.8万USD Euler Finance 1.5万USD　など



※再担保額は2022/12断面の値

Maker（DAIトークン）		Aave（AAVEトークン）	
再担保先	③再担保USD	再担保先	再担保USD
Compound	256,862,012	Maker	147,935
Aave v2	77,652,885	Euler Finance	14,611
Aave v1	4,748,882	Idle Cash	535
Euler Finance	3,807,531	合計	163,081
DyDx	1,613,278		
Cream Finance	1,401,051		
Yearn Finance	662,674		
Idle Cash	70,541		
合計	346,818,854		

出典：Dai Stats https://daistats.com/#/

4-3. 金融安定関連のデータ分析結果
4-3-7. 主なFindings

表4-3-7　主なFindings

主なFindings	内容
金融安定上の影響評価に有益と考えられるデータは一定程度入手可能	• VASPなど各エンティティ間の取引関係やDeFiにおけるリハイポセケーションの実態など、今回の初期的なデータ分析において、更なるリスク分析・評価に向けた端緒となるようなデータが一定程度提示できたとも考えられる。 • FSB報告書の指摘によるデータの取得可能性について、FSBが利用可能としたデータが本調査研究では取得が困難だったケースが確認された一方で、FSBが利用できないとしたデータが本調査研究で取得が可能と考えられるもの（但し一部のデータは限定的）があることも確認された。
複数のデータソースを活用した分析の必要性と、専門家によるリサーチの有効性	• データソースによって取得できるデータの種別やその信頼度は区々。例えば、BCエクスプローラーはブロックチェーン上の取引や残高に関するデータが取得できる一方でトークン価格は取得が困難。他方、暗号資産関連データベースは暗号資産の価格などマーケットデータは取得できるが、ブロックチェーン上の取引などは取得が困難。ブロックチェーン分析ツールは主にリスクの高いVASPの情報収集や高リスク取引のトレースなどを目的としており、ステーブルコインやDeFi関連のデータ取得が一部困難であった（他の分析ツールではステーブルコインやDeFi関連のデータが取得できる可能性） • 分析ツールでデータ取得が困難な調査項目について、専門家によるリサーチでは多くのデータ取得が可能（但し一部のデータ限定的）であることが確認された。 • 監督上の対応を通じたデータ取得など、本調査研究で活用したデータソース以外のソースも存在するところ（P.29）、金融当局として、複数のデータソースへのアクセシビリティを確保し、金融安定上のインプリケーションをモニタリングすることが必要とも考えられる。
既存金融システムとの相互連関性の分析に資するデータは入手困難	• 金融機関のエクスポージャーや決済利用の実態といった観点では、今回の調査結果からは多くのデータは入手できなかった。背景として、これらの取引実態を把握するには公知情報からでは入手困難なオフチェーンデータ（金融機関がデジタル資産を預けているカストディアンに関する情報や、EC等での決済利用にかかる取引・価格データなど）が必要であることが考えられ、現状でこれらのデータはブロックチェーン分析会社も多くは保有していない可能性がある。 • 他方、（今回の調査対象外とした）監督上の対応（金融機関への報告徴求等）によりデータを取得できる可能性はあり、当局はモニタリング能力の強化に向けて様々な手法を模索していくことが望ましいと考えられる。

4-4. AML/CFT関連のデータ分析結果
4-4-1. FATF報告書が指摘するデータの取得可能性

- FATF報告書の指摘について、各種ツールや専門家リサーチによる調査の結果、調査対象としたデータのうち、法定通貨との換金や暗号資産ATM/キオスクなど一部のデータは取得が難しいものの、取得可能なデータも一定数存在することが確認された。
- 当調査結果は、あくまで今回使用した分析ツールや専門家リサーチの結果に基づく局所的な整理であることに留意。

【データ調査結果の凡例】
○：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

（１）VASPのデータ取得可能性

表4-4-1-1　VASPのデータ取得可能性（１／２）

カテゴリ	調査対象項目	調査対象データ	データ取得可能性の調査結果				備考
			BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	
暗号資産交換業者(VASP)関連	主要VASPの関連ウォレットアドレスの取引動向の調査（集中／分散管理等の管理実態やグループ内取引の状況把握を含む）	主要VASPが保有するグループ内アドレス	△ VASPと特定したアドレスが一定数は取得できる	× データ取得が困難	△ VASPと特定したアドレスが一定数は取得できる	△ VASPと特定したアドレスが一定数は取得できる	ブロックチェーン分析会社がVASPと特定したアドレスが対象
		上記アドレスの取引件数・取引額	△ VASPと特定したアドレスの取引データが1件毎に取得できる（集計は困難）	× データ取得が困難	△ VASPと特定したアドレスの取引データが1件毎に取得できる（集計は困難）	△ VASPと特定したアドレスの取引データが一定数は取得できる	
	主要VASPと関連する主体（機関投資家・金融機関など）とその取引実態	機関投資家・金融機関のアドレス	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社が機関投資家等と特定したアドレスが対象
	VASP-DeFi/アンホステッド・ウォレット間の取引実態	DeFiのアドレス	△ DeFiと特定したアドレスが一定数は取得できる	× データ取得が困難	△ DeFiと特定したアドレスが一定数は取得できる	△ DeFiと特定したアドレスが一定数は取得できる	ブロックチェーン分析会社がDeFiやアンホステッド・ウォレットと特定したアドレスが対象
		アンホステッド・ウォレットのアドレス	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	
		上記アドレスの取引件数・取引額	△ DeFiやアンホステッド・ウォレットと特定したアドレスの取引データが1件頃に取得できる（集計は困難）	× データ取得が困難	△ DeFiやアンホステッド・ウォレットと特定したアドレスの取引データが1件頃に取得できる（集計は困難）	△ DeFiやアンホステッド・ウォレットと特定したアドレスの取引データが一定数は取得できる	

4-4. AML/CFT関連のデータ分析結果
4-4-1. FATF報告書が指摘するデータの取得可能性

（１）VASPのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-4-1-1　VASPのデータ取得可能性（２／２）

カテゴリ	調査対象項目	調査対象データ	データ取得可能性の調査結果				
			BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
暗号資産交換業者（VASP）関連	高リスクと考えられるVASP関連ウォレットアドレス・取引の特定	高リスクと判断されたアドレス（過去に犯罪に利用されたアドレスなど）	× データ取得が困難	× データ取得が困難	△ VASPと特定した高リスクアドレスが一定数は取得できる	△ VASPと特定した高リスクアドレスが一定数は取得できる	ブロックチェーン分析会社が高リスクと判断したアドレスが対象
		上記アドレスの取引件数・取引額	× データ取得が困難	× データ取得が困難	△ 特定したアドレスの取引データが1件毎に取得できる（集計は困難）	△ 特定したアドレスの取引データが一定数は取得できる	
	（無登録もしくは規制要件が不十分な法域に所在する）VASPの所在地・地域別傾向	無登録VASPのアドレス	× データ取得が困難	× データ取得が困難	▲ VASPと特定したアドレスが一定数は取得できるが、無登録VASPの詳細な検索は困難	△ VASPと特定したアドレスが一定数は取得できる	ブロックチェーン分析会社が自社データベースに保有しているVASP登録情報に依存する
		無登録VASPの所在地・地域別傾向	× データ取得が困難	× データ取得が困難	△ 特定したVASPの所在地が一定数は取得できる	△ 特定したVASPの所在地が一定数は取得できる	

4-4. AML/CFT関連のデータ分析結果
4-4-1. FATF報告書が指摘するデータの取得可能性

（２）アンホステッド・ウォレットのデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-4-1-2　アンホステッド・ウォレットのデータ取得可能性

カテゴリ	調査対象項目	調査対象データ	データ取得可能性の調査結果				
			BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
アンホステッド・ウォレット（含P2P）関連	P2P取引実態	アンホステッド・ウォレットのアドレス	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社がアンホステッド・ウォレットと特定したアドレスが対象
		P2P取引総額の取引件数・取引額	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	
		不正取引の占める比率	× データ取得が困難	× データ取得が困難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	
	PET（ミキシングサービスなど）の利用実態	ミキシングサービスの取引件数・取引額	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難難	▲ アドレスのアカウント名等を特定した一部に限られる	▲ アドレスのアカウント名等を特定した一部に限られる	ブロックチェーン分析会社がミキシングサービスと特定したアドレスが対象

4-4. AML/CFT関連のデータ分析結果
4-4-1. FATF報告書が指摘するデータの取得可能性

（３）AML/CFT関連のデータ取得可能性

【データ調査結果の凡例】
〇：データが全て取得できる
△：データが概ね取得できるが一部は困難
▲：データが一部取得できるが限定的
×：データが全く取得できない
－：今回の調査対象外

表4-4-1-3　AML/CFT関連のデータ取得可能性

カテゴリ	調査対象項目	調査対象データ	データ取得可能性の調査結果				
			BCエクスプローラー	暗号資産関連データベース	ブロックチェーン分析ツール	専門家によるリサーチ	備考
AML/CFT関連	大量の法定通貨を暗号資産に大量に変換する場合	暗号資産と法定通貨の交換を行っているユーザ（アカウント）のアドレス	× データ取得が困難	× データ取得が困難	× データ取得が困難	× データ取得が困難	法定通貨の交換は主にVASPが行っており、監督当局によるデータ取得の可能性がある
	盗まれた資金を保有していると特定された暗号資産アドレスや不正に入金されたと疑われる資金を受け取る場合	不正利用されているアドレス	▲ アドレスのアカウント名等を特定したごく一部に限られる	× データ取得が困難	△ 対象のアドレスが一定数は取得できる（1件毎に取得できるが集計は困難）	△ 対象のアドレスが一定数は取得できる	ブロックチェーン分析会社が不正利用と特定したアドレスが対象
		上記アドレスの取引相手のアドレス	▲ アドレスのアカウント名等を特定したごく一部に限られる	× データ取得が困難	△ 対象のアドレスが一定数は取得できる（1件毎に取得できるが集計は困難）	△ 対象のアドレスが一定数は取得できる	
	顧客管理（CDD）や本人確認（KYC）プロセスがないもしくは不十分なVASPからの資金授受を行う場合	VASPの加入時にCDD/KYCプロセスがないと思われるVASPの特定	× データ取得が困難	× データ取得が困難	▲ 該当条件のVASPが一定数は取得できるが検索は困難	△ 該当条件のVASPが一定数は取得できる	ブロックチェーン分析会社が自社データベースに保有しているVASP登録情報に依存する
	犯罪行為が増加するリスクが高い場所で暗号資産ATM/キオスクを利用する場合	暗号資産ATM/キオスクを利用したアドレス	× データ取得が困難	× データ取得が困難	× データ取得が困難	× データ取得が困難	暗号資産ATM/キオスクのデータ取得は困難
	詐欺・恐喝、ランサムウェアスキーム、制裁対象のアドレス、ダークネットマーケットプレイス、またはその他の違法なWebサイトに関連する暗号資産アドレスでの取引	違法なWebサイトに関連する暗号資産アドレス	▲ アドレスのアカウント名等を特定した一部に限られる	× データ取得が困難	△ 対象のアドレスが一定数は取得できる（1件毎に取得できるが集計は困難）	△ 対象のアドレスが一定数は取得できる	ブロックチェーン分析会社が詐欺・恐喝等と特定したアドレスが対象

4-4. AML/CFT関連のデータ分析結果
4-4-2. リサーチ調査項目

- 本章では、4つの調査項目について、VASPやレンディング事業者などのカテゴリ別に取引件数・金額や疑わしい取引の利用実態など具体的な調査項目を設定し、ブロックチェーン分析会社の専門家によるリサーチを行った。
- リサーチ結果は、データを整理のうえ表やグラフに整理し、結果から見られる傾向や特徴について考察を行った。

表4-4-2 リサーチ調査項目

調査項目	調査内容	補足
主なVASPの高リスク取引比率の傾向	• 主な暗号資産取引業者２社について、受信・自業者内・送信の３つに分けて取引件数、取引金額、高リスク取引件数をカテゴリ別に調査した。	• アカウントのカテゴリ名やアカウント名は、ブロックチェーン分析会社が定義した分類を使用した。 • 取引金額の算出は、2023年4月時点のトークン価格等のレートを使用した。
主なレンディング事業者の高リスク取引比率の傾向	• 主なレンディング事業者１社について、受信・自業者内・送信の３つに分けて取引件数、取引金額、高リスク取引件数をカテゴリ別に調査した。	
アンホステッド・ウォレットの高リスク取引比率の傾向	• アンホステッド・ウォレットについて、受信・P2P（アンホステッド・ウォレット内）・送信の３つに分けて取引件数、取引金額、高リスク取引件数をカテゴリ別、カテゴリ別のうちDeFiの内訳、トークン別に調査した。	
AML/CFT関連データ	• 疑わしい取引の実態調査として、少額取引や連続した高額取引の実態、ミキシングサービス、詐欺・恐喝や制裁対象アドレス、オンラインギャンブルサービスなど高リスクアドレスの取引を調査した。 • 所在する法域に登録されていない無登録VASPの所在地や地域別傾向などを調査した。	

4-4. AML/CFT関連のデータ分析結果
4-4-3. 主なVASP

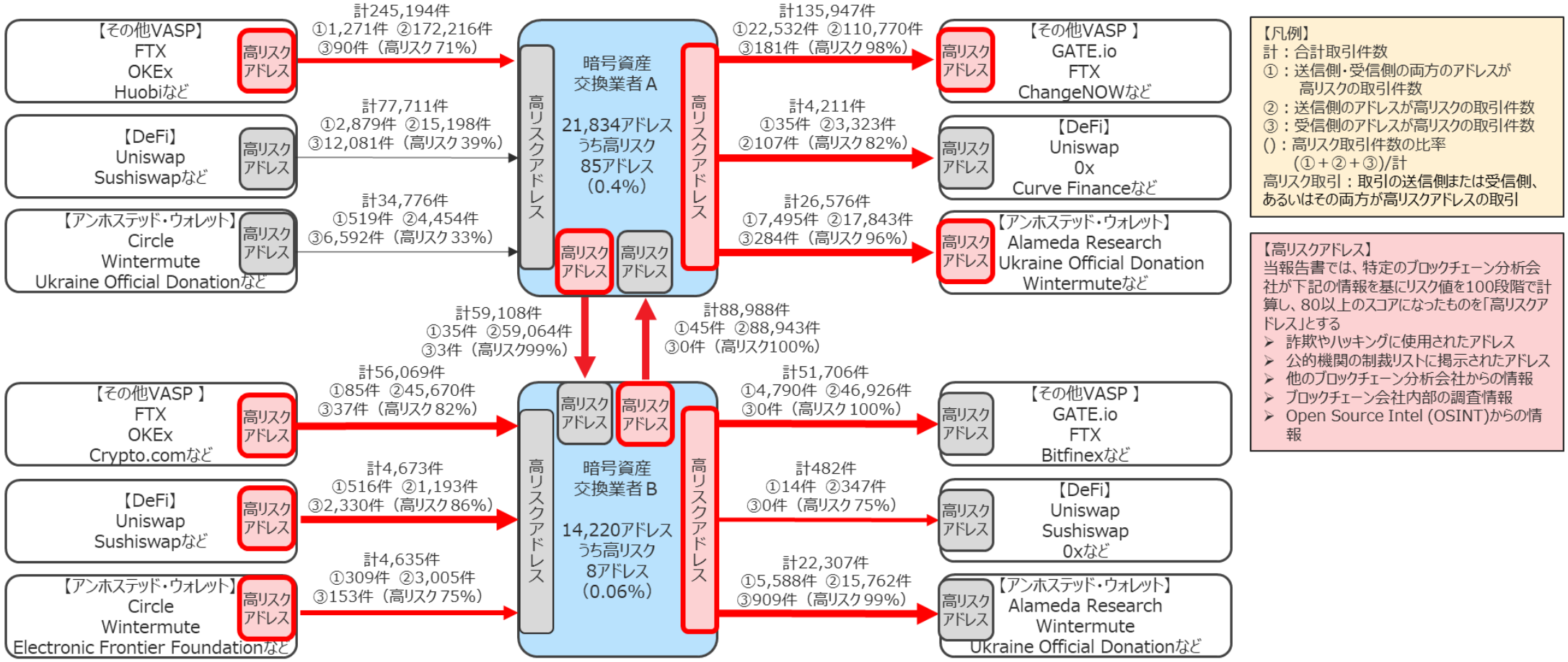
（1）主なVASP：主要暗号資産交換業者2社（A・B）の高リスク取引の概要

- 高リスク取引は主にA・B及びその他VASPからの送信（VASPの管理する高リスクアドレスからのトークン移転）であり、いずれも70%以上の比率になっている。

  ※ ただし、高リスクアドレス・取引の定義上、VASPの関連取引は「高リスク」と分類されるものが多くなっているものと考えられ（VASPが管理する少数のアドレスで多数の送受信が行われており、それらのアドレスは高リスクと分類されやすい）、実態を反映しているかについては精査が必要（詳細は次頁以降に記載）。

- DeFiやアンホステッド・ウォレット（一部の大口事業者やファンド含む）との取引も、相当数の高リスク取引を確認した。

図4-4-3-1　主なVASPの高リスク取引の概要



4-4. AML/CFT関連のデータ分析結果
4-4-3. 主なVASP（暗号資産交換業者A）

（２）主なVASP：暗号資産交換業者A　カテゴリ別

図4-4-3-2　暗号資産交換業者Aのカテゴリ別取引件数・金額

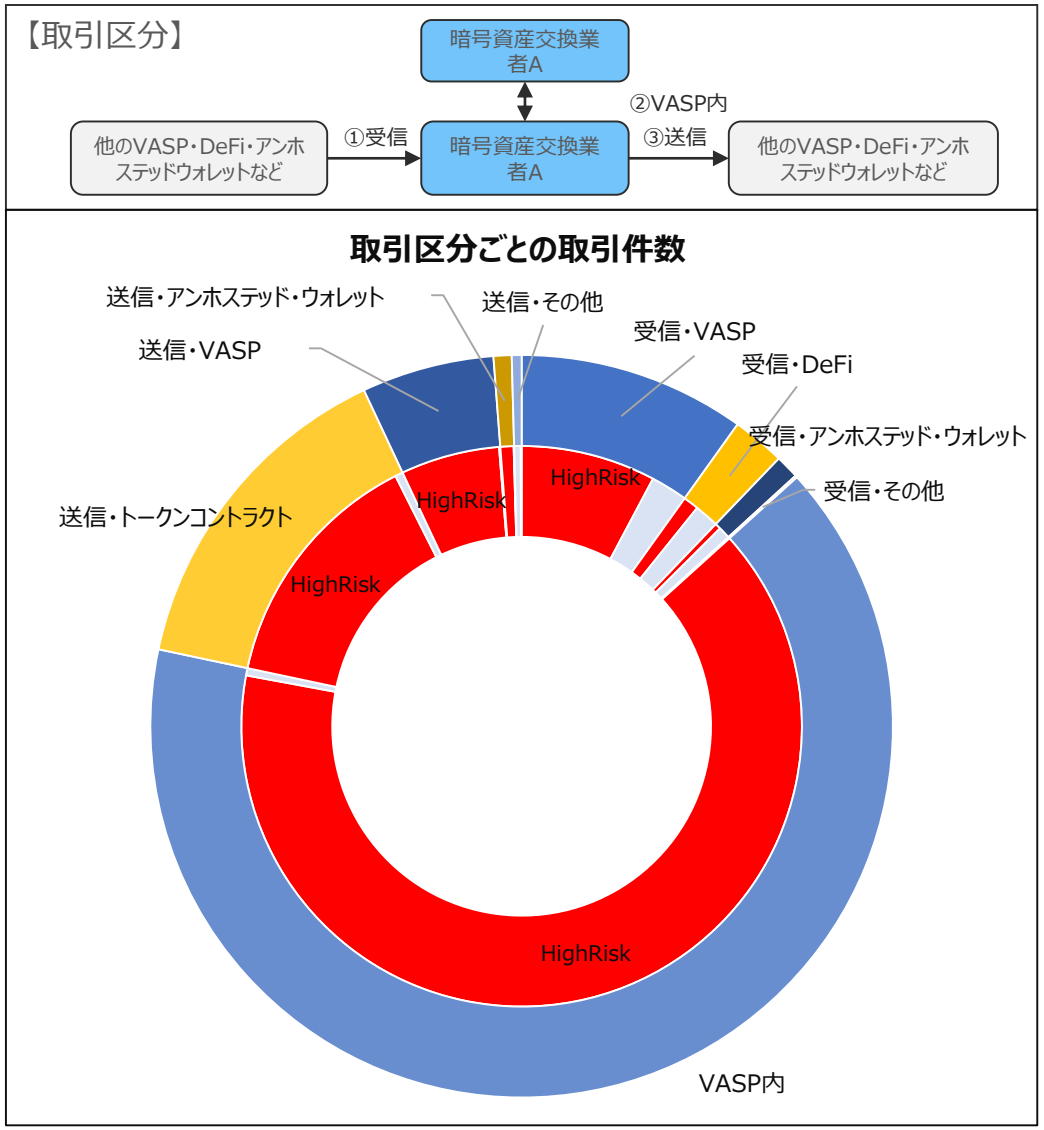


表4-4-3-2　暗号資産交換業者Aのカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	取引件数		うち高リスク取引		取引金額	
		件数	件数比率	件数	高リスク比率	金額M$	件数比率
①受信	VASP	334,182	74.3%	262,565	78.6%	51,239	77.8%
	DeFi	77,711	17.3%	30,158	38.8%	528	0.8%
	アンホステッド・ウォレット	34,776	7.7%	11,565	33.3%	13,791	20.9%
	トークンコントラクト	2,320	0.5%	1,864	80.3%	27	0.0%
	ブリッジ（他チェーンへの送金）等	566	0.1%	146	25.8%	148	0.2%
	その他	133	0.0%	42	31.6%	123	0.2%
	合計	449,688	100.0%	306,340	68.1%	65,856	100.0%
②VASP内	VASP	2,198,665	100.0%	2,184,570	99.4%	625,406	100.0%
	合計	2,198,665	100.0%	2,184,570	99.4%	625,406	100.0%
③送信	VASP	195,055	26.6%	192,585	98.7%	27,079	62.1%
	DeFi	4,211	0.6%	3,465	82.3%	46	0.1%
	アンホステッド・ウォレット	26,576	3.6%	25,622	96.4%	15,873	36.4%
	トークンコントラクト	496,837	67.8%	481,607	96.9%	217	0.5%
	ブリッジ（他チェーンへの送金）等	3,451	0.5%	3,117	90.3%	398	0.9%
	その他	6,756	0.9%	6,157	91.1%	0	0.0%
	合計	732,886	100.0%	712,553	97.2%	43,613	100.0%

【考察】

- 高リスク取引は、②VASP内の比率が最も高い
  → VASP内の取引が、特定の高リスクアドレス（5アドレス）への送金に集中している
  取引量の多い一部アドレスが、詐欺や犯罪に利用された実績に基づき「高リスク」と判定され、当該アドレスと関連する全ての取引が「高リスク」と分類されている可能性（実際は問題無い取引が大半である可能性も）
- 次に③送信、①受信の順に比率が高い
  → ②VASP内と同じく、VASPの特定の高リスクアドレスの取引件数が多いことが考えられる

4-4. AML/CFT関連のデータ分析結果
4-4-3. 主なVASP（暗号資産交換業者B）

（３）主なVASP：暗号資産交換業者B　カテゴリ別

図4-4-3-3 暗号資産交換業者Bのカテゴリ別取引件数・金額

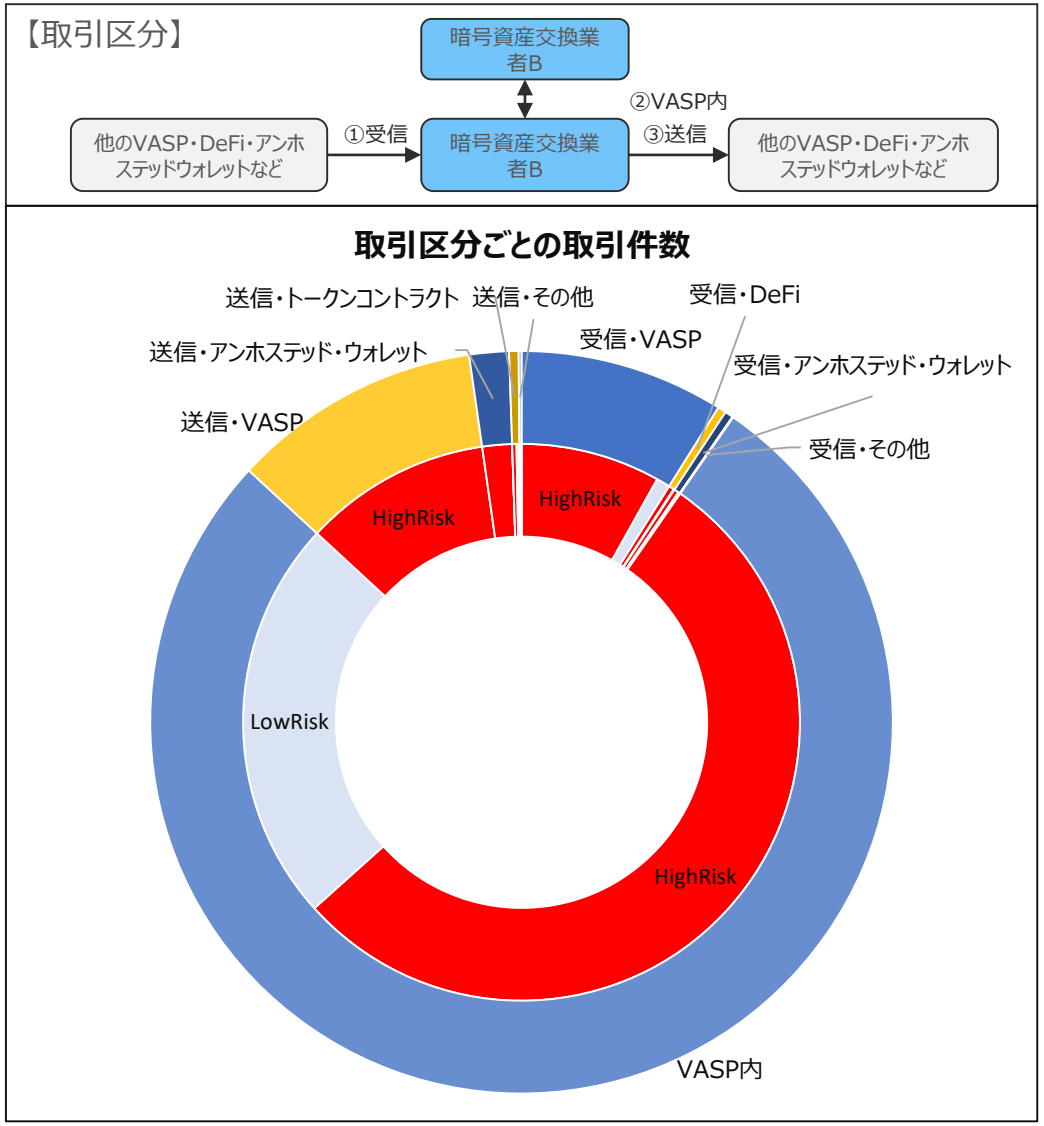


表4-4-3-3　暗号資産交換業者Bのカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	取引件数		うち高リスク取引		取引金額	
		件数	件数比率	件数	高リスク比率	金額M$	件数比率
①受信	VASP	115,177	92.1%	104,894	91.1%	17,190	20.6%
	DeFi	4,673	3.7%	4,039	86.4%	123	0.1%
	アンホステッド・ウォレット	4,635	3.7%	3,467	74.8%	65,944	79.2%
	トークンコントラクト	306	0.2%	304	99.3%	0	0.0%
	ブリッジ（他チェーンへの送金）等	192	0.2%	30	15.6%	1	0.0%
	その他	6	0.0%	6	100.0%	0	0.0%
	合計	124,989	100.0%	112,740	90.2%	83,259	100.0%
②VASP内	VASP	999,058	100.0%	694,838	69.5%	97,707	100.0%
	合計	999,058	100.0%	694,838	69.5%	97,707	100.0%
③送信	VASP	140,704	82.8%	140,704	100.0%	13,655	64.9%
	DeFi	482	0.3%	361	74.9%	2,583	12.3%
	アンホステッド・ウォレット	22,307	13.1%	22,259	99.8%	4,514	21.5%
	トークンコントラクト	5,320	3.1%	3,179	59.8%	1	0.0%
	ブリッジ（他チェーンへの送金）等	1,072	0.6%	1,072	100.0%	279	1.3%
	その他	51	0.0%	34	66.7%	0	0.0%
	合計	169,936	100.0%	167,609	98.6%	21,032	100.0%

【考察】

- 高リスク取引は、③送信の比率が最も高い
  → ③送信は、VASPの特定の高リスクアドレス（8アドレス）からの取引件数が多いことが考えられる
  取引量の多い一部アドレスが、詐欺や犯罪に利用された実績に基づき「高リスク」と判定され、当該アドレスと関連する全ての取引が「高リスク」と分類されている可能性
- 次に①受信、②VASPの順に比率が高い
  → ③送金と同じく、VASPの特定の高リスクアドレスの取引件数が多いことが考えられる

4-4. AML/CFT関連のデータ分析結果
4-4-4. 主なレンディング事業者

（1）主なレンディング事業者：カテゴリ別

図4-4-4-1　レンディング事業者のカテゴリ別取引件数・金額

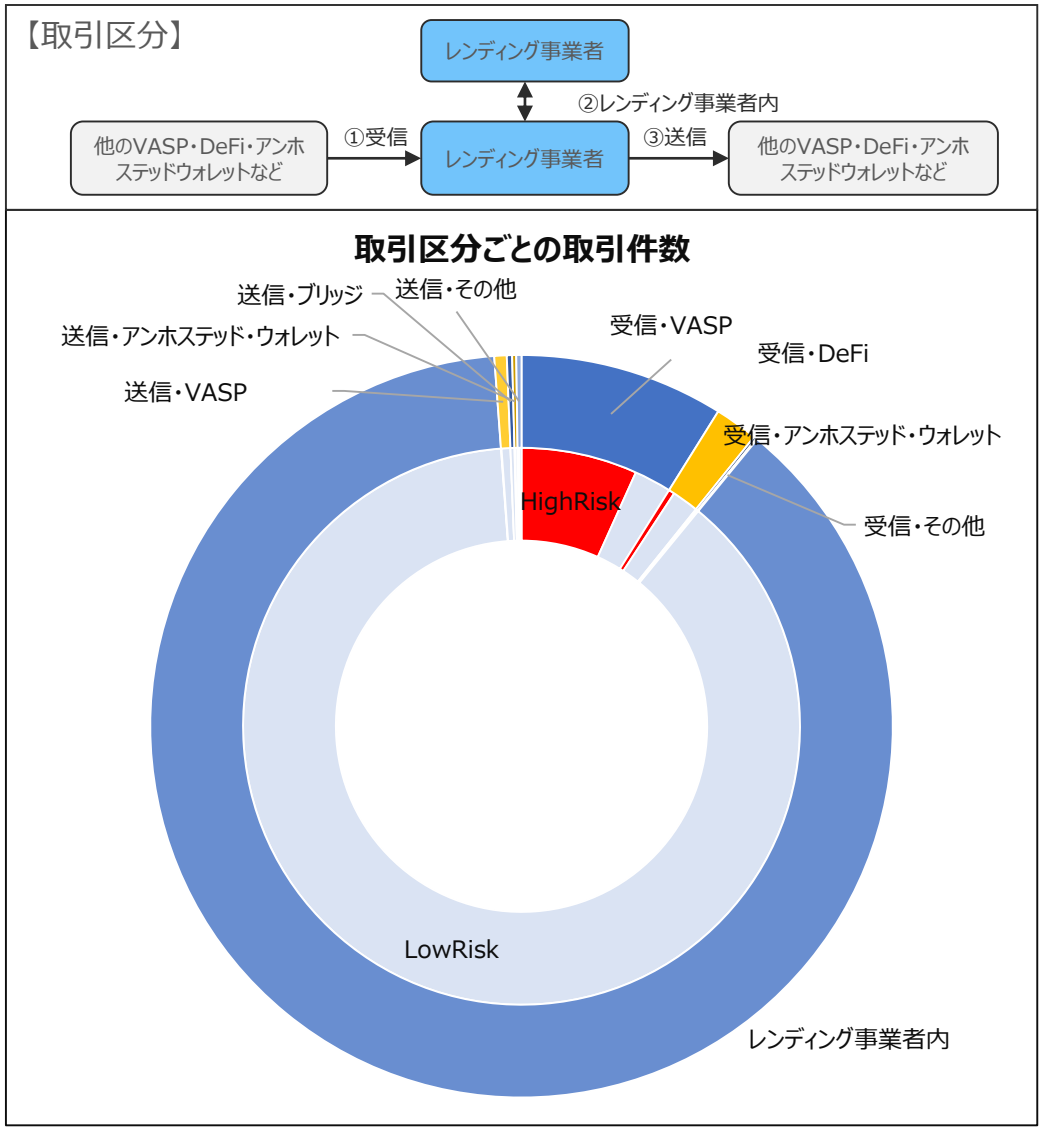


表4-4-4-1　レンディング事業者のカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	取引件数		うち高リスク取引		取引金額	
		件数	件数比率	件数	高リスク比率	金額M$	件数比率
①受信	VASP	12,841	81.2%	9,733	75.8%	6,807	99.7%
	DeFi	2,727	17.2%	501	18.4%	6	0.1%
	アンホステッド・ウォレット	174	1.1%	146	83.9%	15	0.2%
	トークンコントラクト	50	0.3%	40	80.0%	0	0.0%
	ブリッジ（他チェーンへの送金）等	12	0.1%	4	33.3%	0	0.0%
	その他	10	0.1%	9	90.0%	0	0.0%
	合計	15,814	100.0%	10,433	66.0%	6,828	100.0%
②レンディング事業者内	レンディング事業者	126,946	100.0%	0	0.0%	8,015	100.0%
	合計	126,946	100.0%	0	0.0%	8,015	100.0%
③送信	VASP	782	46.1%	40	5.1%	177	43.0%
	DeFi	0	0.0%	0	0.0%	0	0.0%
	アンホステッド・ウォレット	256	15.1%	62	24.2%	141	34.2%
	トークンコントラクト	224	13.2%	125	55.8%	0	0.0%
	ブリッジ（他チェーンへの送金）等	332	19.6%	0	0.0%	21	5.1%
	その他	103	6.1%	4	3.9%	73	17.6%
	合計	1,697	100.0%	231	13.6%	412	100.0%

【考察】

- 高リスク取引は、①受信の比率が最も高い。カテゴリ別では他のVASP、アンホステッド・ウォレット、トークンコントラクトの比率が高い
  → VASPとトークンコントラクトは、取引件数が多いアドレスが詐欺や犯罪に利用されやすいのではないかと考えられる。
  アンホステッド・ウォレットは、特定の高リスクアドレスからの送金が多いことが考えられるか
- ②レンディング事業者内は、高リスク取引が0件である
  → レンディング事業者のアドレスは、VASP等に比べて取引件数が少ないため、詐欺や犯罪に利用されにくいのではないかと考えられる

4-4. AML/CFT関連のデータ分析結果
4-4-5. アンホステッド・ウォレット

※MEV（最大抽出可能価値）ボット:
Ethereumブロックチェーンの待機中の取引プール（mempool）を分析して、フロントランニングなどで価値を取得する自動実行ソフトウェア

（1）アンホステッド・ウォレット：カテゴリ別

図4-4-5-1　アンホステッド・ウォレットのカテゴリ別取引件数・金額

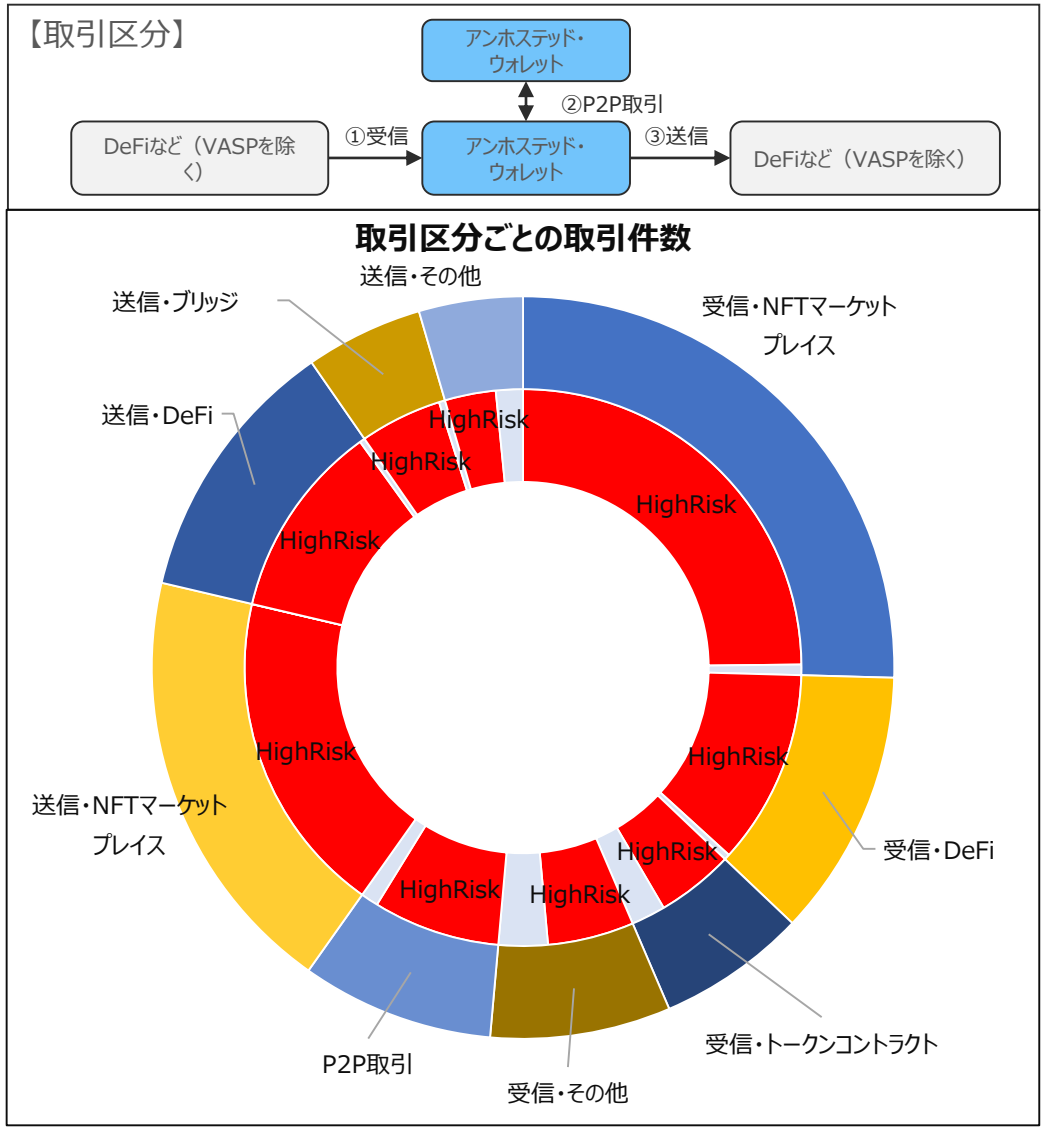


表4-4-5-1　アンホステッド・ウォレットのカテゴリ別取引データ

取引区分	アカウントのカテゴリ別	アドレス数	取引件数		うち高リスク取引		取引金額	
			件数	件数比率	件数	高リスク比率	金額M$	金額比率
①受信	NFTマーケットプレイス	190	1,468,421	49.5%	1,433,197	97.6%	152	0.2%
	DeFi	8,752	672,335	22.7%	653,168	97.1%	30,537	44.9%
	トークンコントラクト	1,753	373,899	12.6%	259,006	69.3%	22,378	32.9%
	ブリッジ（他チェーンへの送金）等	895	271,589	9.1%	265,744	97.8%	10,179	15.0%
	MEVボット※	103	152,869	5.2%	11,550	7.6%	989	1.5%
	その他	549	29,174	1.0%	11,861	40.7%	3,818	5.6%
	合計	12,242	2,968,287	100.0%	2,634,526	88.8%	68,053	100.0%
②P2P取引	P2P取引	5,989	484,394	100.0%	425,882	87.9%	28,967	100.0%
	合計	5,989	484,394	100.0%	425,882	87.9%	28,967	100.0%
③送信	NFTマーケットプレイス	77	1,088,944	46.9%	1,088,322	99.9%	1,083	2.1%
	DeFi	4,799	674,524	29.1%	656,787	97.4%	22,876	44.0%
	トークンコントラクト	1,361	248,009	10.7%	160,917	64.9%	16,077	30.9%
	ブリッジ（他チェーンへの送金）等	500	295,673	12.7%	275,222	93.1%	10,149	19.5%
	MEVボット※	27	3,963	0.2%	2,834	71.5%	344	0.7%
	その他	329	9,179	0.4%	7,087	77.2%	1,498	2.9%
	合計	7,093	2,320,292	100.0%	2,191,169	94.4%	52,027	100.0%

【考察】

- 高リスク取引は、③送信の比率が最も高い。カテゴリ別では他のVASP、アンホステッド・ウォレット、ブリッジの比率が高い
  → VASPとブリッジは、取引件数が多いアドレスが詐欺や犯罪に利用されやすいのではないかと考えられる。
  アンホステッド・ウォレットは、特定の高リスクアドレスの取引件数が多いことが考えられるか
- 次に①受信、②P2P取引の順に比率が高い
  → ③送金と同じく、特定の高リスクアドレスの取引件数が多いことが考えられるか

4-4. AML/CFT関連のデータ分析結果
4-4-5. アンホステッド・ウォレット

（２）アンホステッド・ウォレット：カテゴリ別のうちDeFi内訳

図4-4-5-2　アンホステッド・ウォレットのカテゴリ別取引（うちDeFi）件数・金額

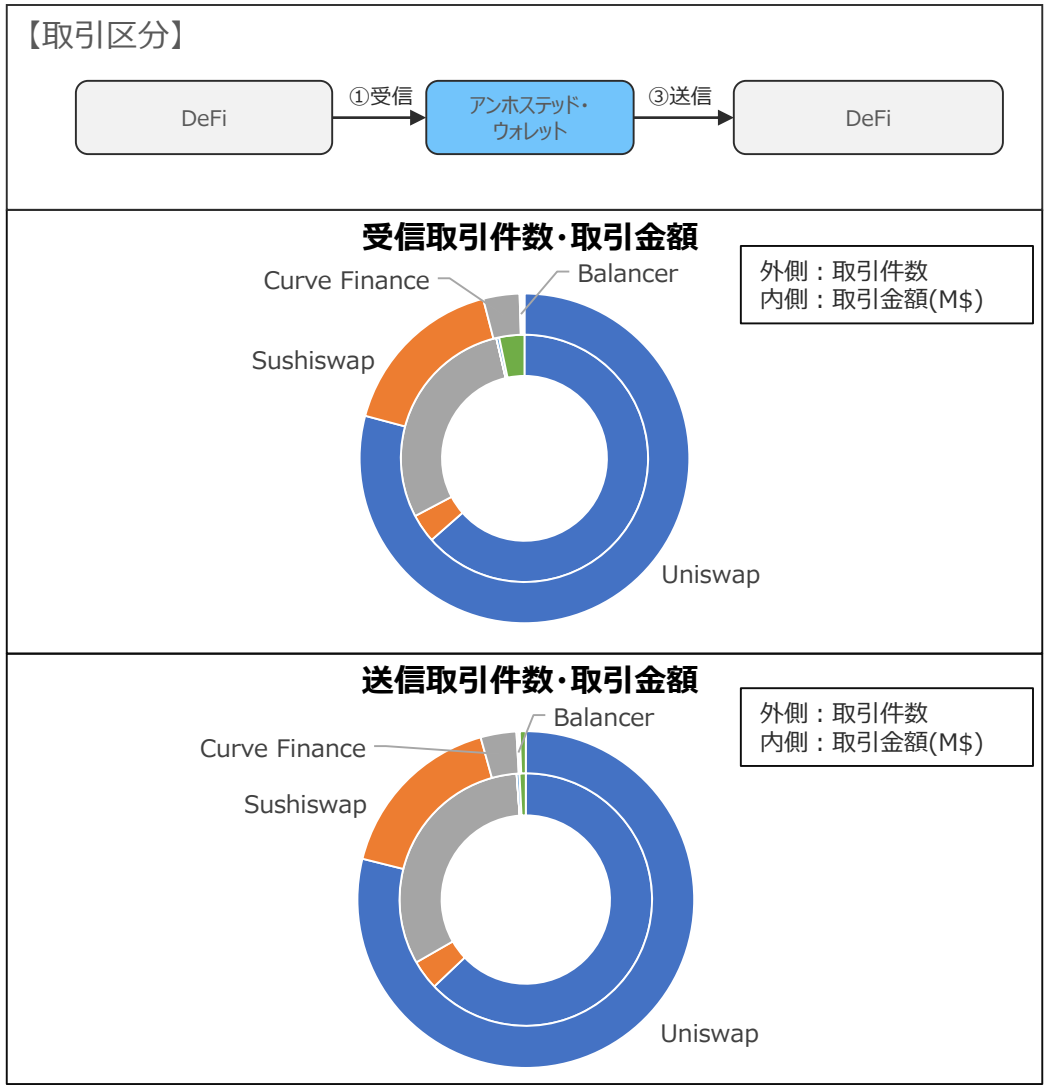


表4-4-5-2　アンホステッド・ウォレットのカテゴリ別取引（うちDeFi）データ

カテゴリ名のうちDeFi内訳	サービス種別	①受信			③送信		
		取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
Uniswap	分散型取引所	532,196	79.2%	19,400	532,203	78.9%	14,393
Sushiswap	分散型取引所	113,024	16.8%	1,144	113,155	16.8%	869
Curve Finance	分散型取引所	23,941	3.6%	8,874	23,170	3.4%	7,348
Balancer	分散型取引所	1,279	0.2%	3	1,288	0.2%	2
mStable	ステーブルコイン発行	897	0.1%	114	837	0.1%	81
その他	–	998	0.1%	1,002	3,871	0.6%	183
合計	合計	672,335	100.0%	30,537	674,524	100.0%	22,876

【考察】

- ①受信、②送信とも分散型取引所の取引件数が多い
  → 暗号資産の交換や流動性提供、ステーキングの送金が多いと考えられる
- 分散型取引所のうち、①受信、②送信ともUniswapの取引が多い
  → Uniswapは多種類トークン交換と考えられる（約700種類）
- ①受信、②送信の取引件数がDeFi毎にほぼ同じである
  → 詳細は精査が必要だが、例えば分散型取引所で交換したトークンをアンホステッド・ウォレットに送金するような動きが考えられるか

4-4. AML/CFT関連のデータ分析結果
4-4-5. アンホステッド・ウォレット

（３）アンホステッド・ウォレット：トークン別

図4-4-5-3　アンホステッド・ウォレットのトークン別取引件数・金額

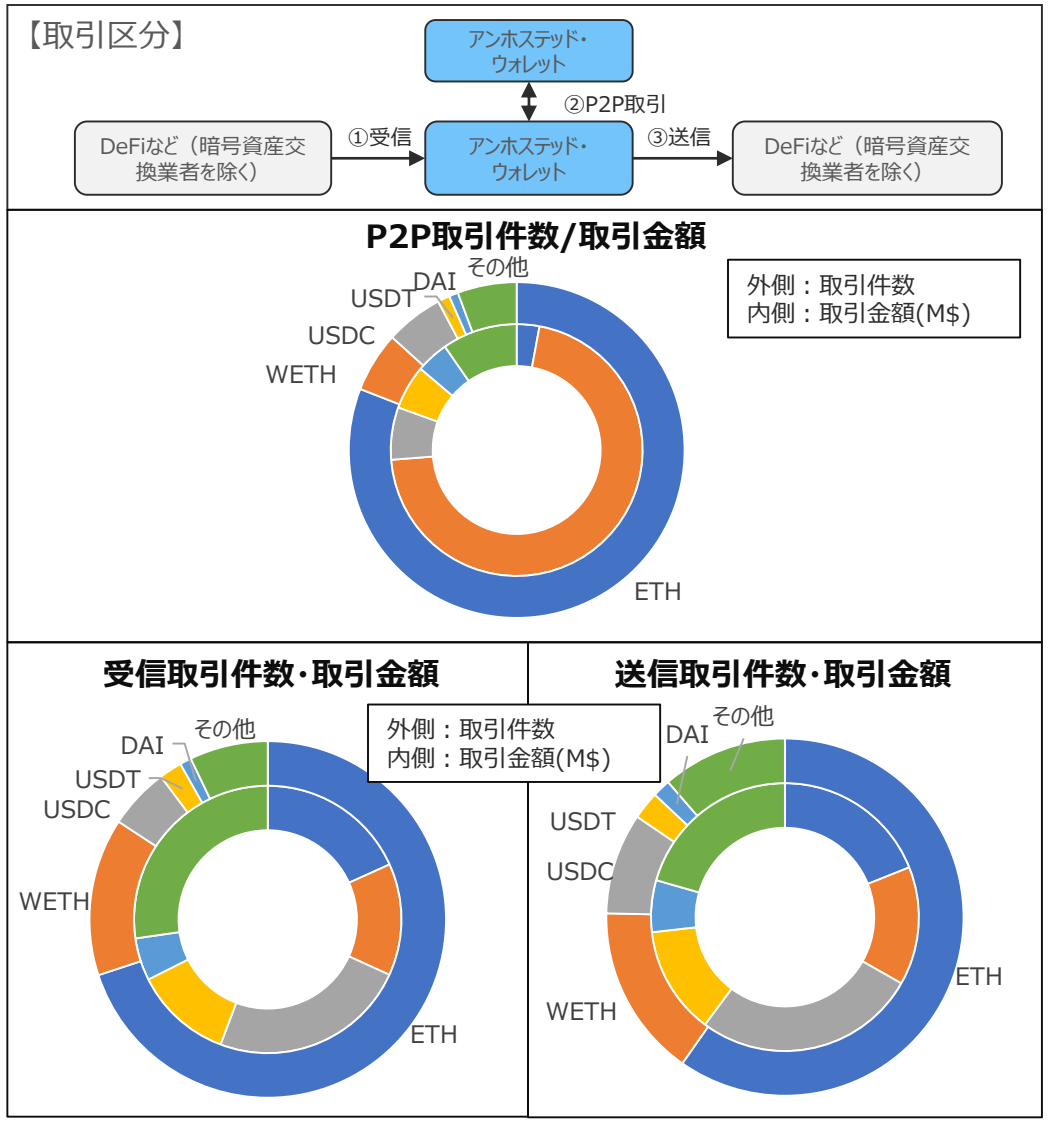


表4-4-5-3　アンホステッド・ウォレットのトークン別取引データ

アカウントの利用トークン別	種別	①受信			②P2P取引			③送信		
		取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
ETH	ネイティブトークン	2,076,058	69.9%	12,420	391,975	80.9%	843	1,386,001	59.7%	9,853
WETH	ネイティブトークン	424,295	14.3%	9,219	28,025	5.8%	20,524	362,035	15.6%	7,439
USDC	ステーブルコイン	164,494	5.5%	16,299	26,908	5.6%	1,952	212,593	9.2%	14,020
USDT	ステーブルコイン	61,740	2.1%	8,053	5,655	1.2%	1,642	58,577	2.5%	6,769
DAI	ステーブルコイン	30,959	1.0%	3,503	4,241	0.9%	1,209	37,793	1.6%	3,255
その他	–	※210,741	7.1%	18,559	27,590	5.7%	2,797	※263,293	11.3%	10,691
合計		2,968,287	100.0%	68,053	484,394	100.0%	28,967	2,320,292	100.0%	52,027

※①受信の「その他」は約800種類、③送信の「その他」は約700種類のトークンに対する取引件数

【考察】

- 全ての取引区分でETH・WETH（ETHと1対1でペッグされたトークン）の取引件数が多い
  次にUSDC・USDT・DAIなどのステーブルコインの取引が多い
  → 他のトークンとの交換（金額確定など）に利用されるためと考えられる
- 暗号資産交換業者やレンディング事業者では取引件数が上位にないWETHの取引件数・金額が多い
  → WETHはETHをDeFiやNFTサービス等で利用しやすいようにERC-20規格に準拠したトークンであり、DeFi等の利用が多いためと考えられる

4-4. AML/CFT関連のデータ分析結果
4-4-6. AML/CFT関連

（１）盗まれた資金の保有者に関連したアドレス数

図4-4-6-1　盗まれた資金の保有者に関連したカテゴリ別アドレス数

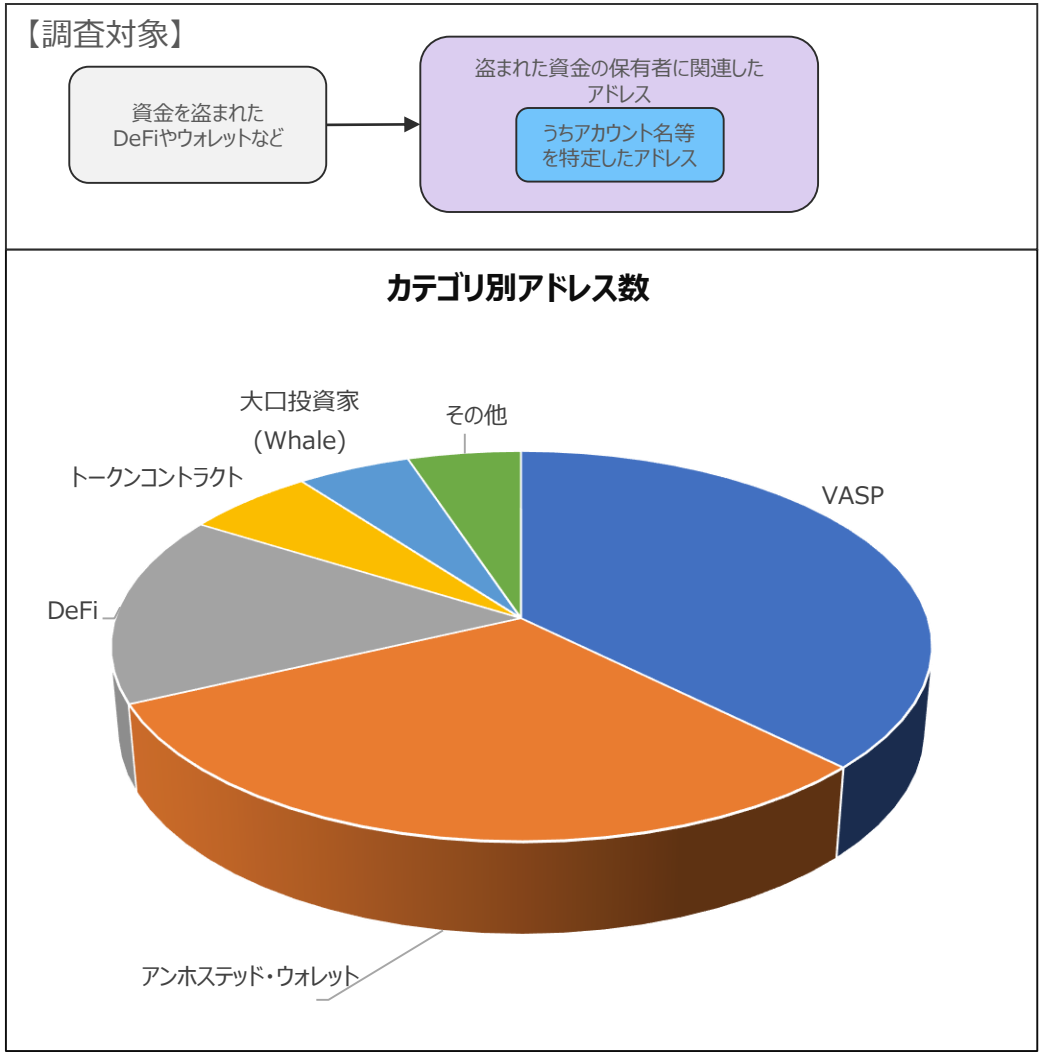


表4-4-6-1　盗まれた資金の保有者に関連したカテゴリ別アドレスデータ

アカウントのカテゴリ別	アドレス数	比率
VASP	1,567	37.4%
アンホステッド・ウォレット	1,285	30.7%
DeFi	662	15.8%
トークンコントラクト	246	5.9%
大口投資家(Whale)	216	5.2%
その他	215	5.1%
合計	4,191	100.0%

アカウント名などの特定有無	アドレス数	比率
アカウント名等を特定	4,191	2.6%
アカウント名等が不明	158,918	97.4%
合計	163,109	100.0%

【考察】

- 盗まれた資金の保有者に関連したアドレスのうち、アカウント名が特定できたものは全体の3%に留まる。
  → ブロックチェーン分析会社のデータベースによりアドレスが特定できていても、殆どのアカウント名が特定できていない状況であり、オフチェーン情報などからのアカウントの特定が極めて難しいと考えられる。
- 特定できたアドレスについては、VASPのアドレスが最も多い。次にアンホステッド・ウォレットが多い。
  → VASP、アンホステッド・ウォレットは、過去に犯罪や詐欺に使用されたアドレスが多いことが考えられる。ただし、VASPは相対的に識別が容易であるとも考えられるため、全体の傾向を必ずしも示したものではない可能性

※「盗まれた資金の保有者に関連したアドレス」は、ブロックチェーン分析会社が保有する既知の攻撃者に関するデータを使用した

（２）ミキシングサービスを利用したアドレス数

図4-4-6-2　ミキシングサービスを利用したカテゴリ別アドレス数

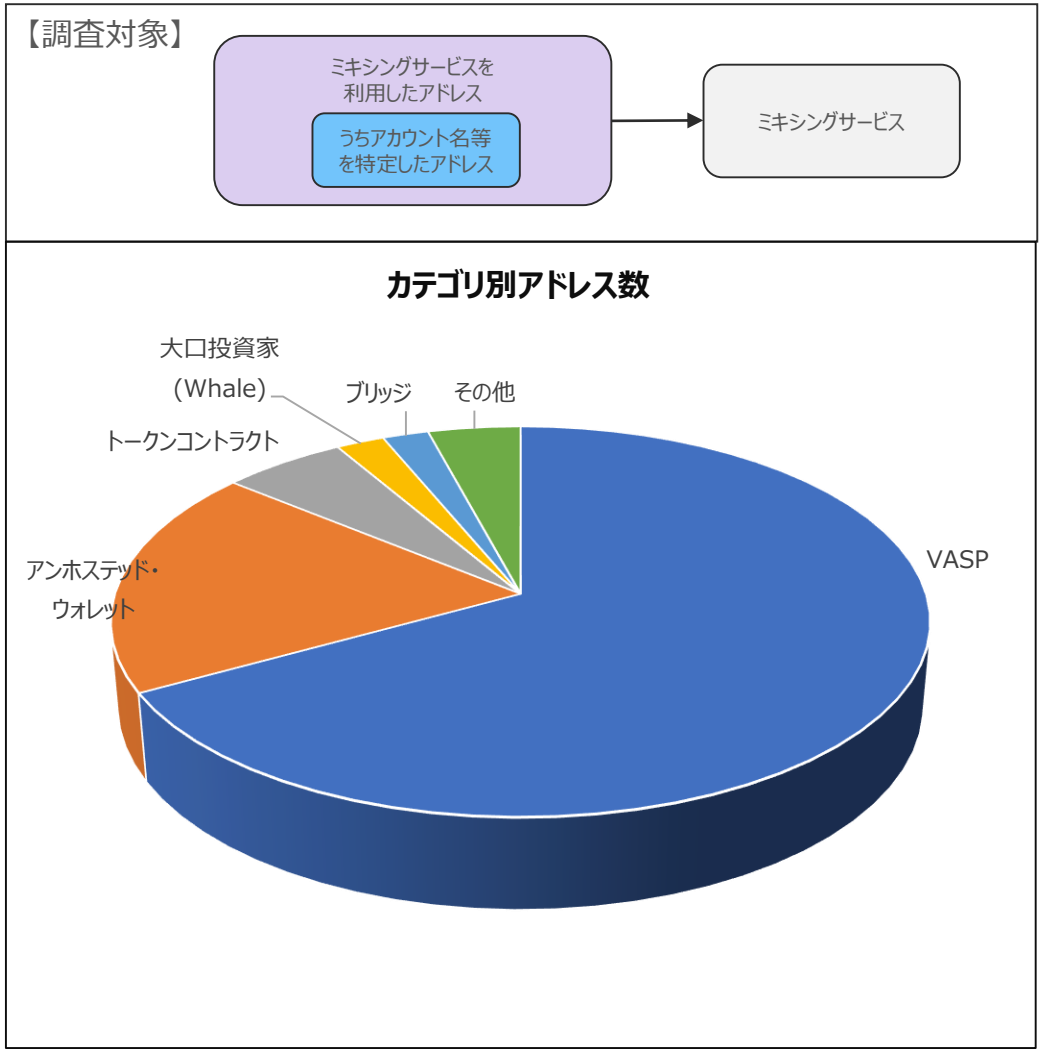


表4-4-6-2　ミキシングサービスを利用したカテゴリ別アドレスデータ

アカウントのカテゴリ別	アドレス数	比率
VASP	22,257	67.0%
アンホステッド・ウォレット	6,304	19.0%
トークンコントラクト	1,866	5.6%
大口投資家(Whale)	727	2.2%
ブリッジ（他チェーンへの送金）等	692	2.1%
その他	1,390	4.2%
合計	33,236	100.0%

アカウント名などの特定有無	アドレス数	比率
アカウント名等を特定	33,236	0.4%
アカウント名等が不明	9,001,940	99.6%
合計	9,035,176	100.0%

【考察】

- 識別されたミキシングサービス関連アドレスの大半はTornado Cash関連。
- ミキシングサービスを利用したアドレスのうち、アカウント名が特定できたものは全体の0.4%。
  → オンチェーンの取引情報からの調査によりミキシングサービスを利用したアドレスが特定できていても、殆どのアカウント名が特定できていない状況であり、オフチェーン情報などからのアカウントの特定が極めて難しいと考えられる。
- カテゴリ別は、VASPのアドレスが最も多い。次にアンホステッド・ウォレットが多い。
  → VASPのユーザーもしくはアンホステッド・ウォレット所有者が、何らかの目的（ML含む）でミキシングサービスを活用している可能性。

（３）詐欺・恐喝、ランサムウェア、制裁対象アドレス、ダークネットマーケットプレイスなどに関連付けられたアドレスの取引件数・金額

図4-4-6-3　詐欺・恐喝などに関連付けられたアドレスのカテゴリ別取引件数・金額

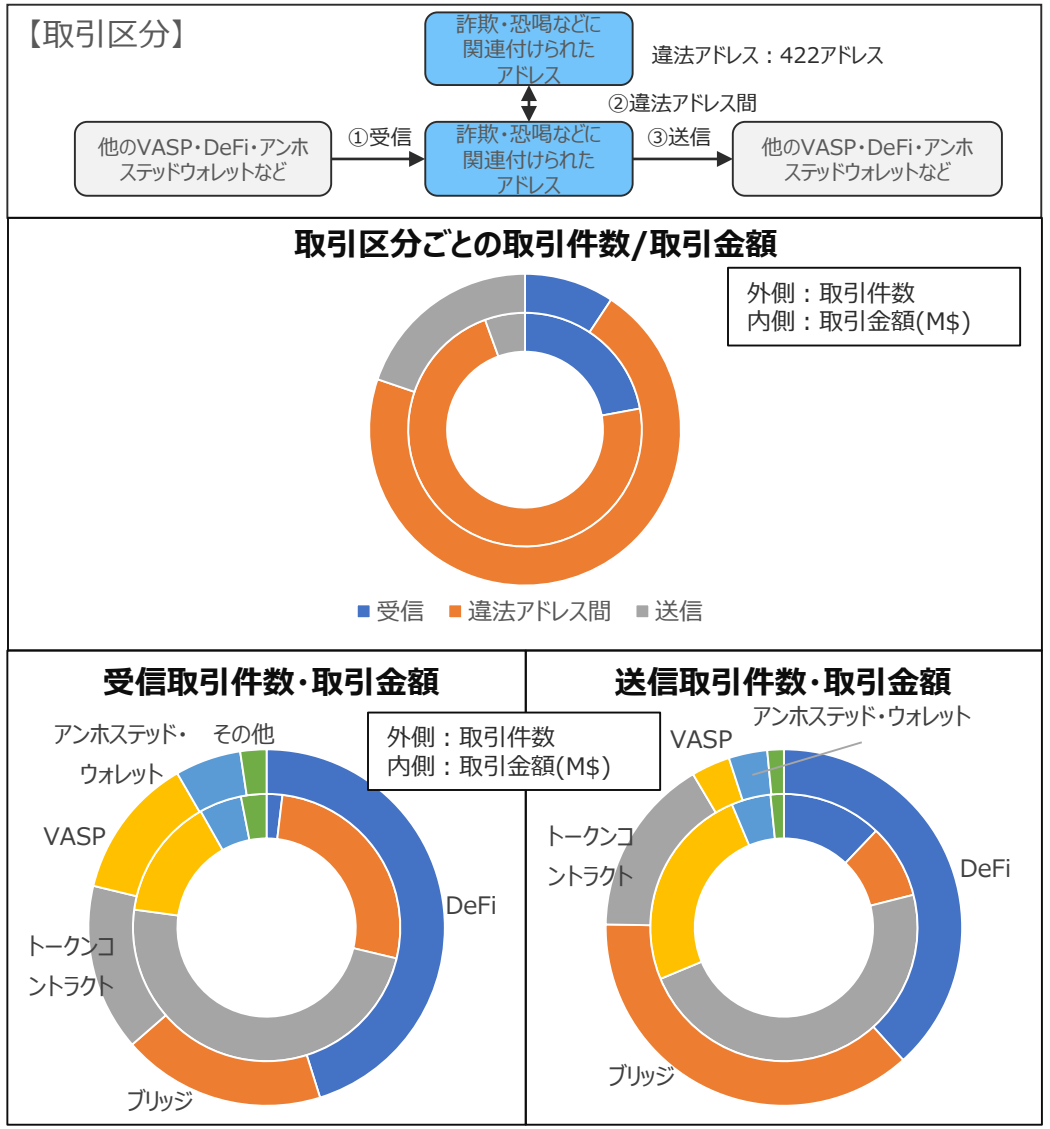


表4-4-6-3　詐欺・恐喝などに関連付けられたアドレスのカテゴリ別取引データ

アカウントのカテゴリ別	①受信			②違法アドレス間			③送信		
	取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
DeFi	5,496	45.1%	23				9,902	38.3%	37
ブリッジ（他チェーンへの送金）等	2,246	18.5%	323				9,544	36.9%	27
トークンコントラクト	1,846	15.2%	584				4,187	16.2%	144
VASP	1,568	12.9%	177				910	3.5%	75
アンホステッド・ウォレット	728	6.0%	62				903	3.5%	14
その他	289	2.4%	37				386	1.5%	5
合計	12,173	100.0%	1,206	92,730	100.0%	3,945	25,832	100.0%	303

アカウント名などの特定有無	①受信			③送信		
	取引件数	件数比率	取引金額M$	取引件数	件数比率	取引金額M$
アカウント名等を特定	25,832	14.3%	303	12,173	13.7%	1,206
アカウント名等が不明	154,762	85.7%	3,002	76,399	86.3%	2,267
合計	180,594	100.0%	3,305	88,572	100.0%	3,472

【考察】

- ②違法アドレス間の取引件数・金額が最も多い
  → ミキシングサービスなどで、取引が特定されないように多数の内部取引をダミーで実行していることが考えられる
- カテゴリ別の取引件数は、①受信・③送信ともDeFiが最も多い。取引金額は、トークンコントラクトが最も多い
  → DeFiは①受信、③送信ともUniswapなどの分散型取引所によるトークン交換、トークンコントラクトはトークン転送（主にWETHなど）によるものと考えられる

（４）オンラインギャンブルサービスから送金されたアドレスの取引件数・金額

図4-4-6-4　オンラインギャンブルサービスから送金されたカテゴリ別取引件数・金額

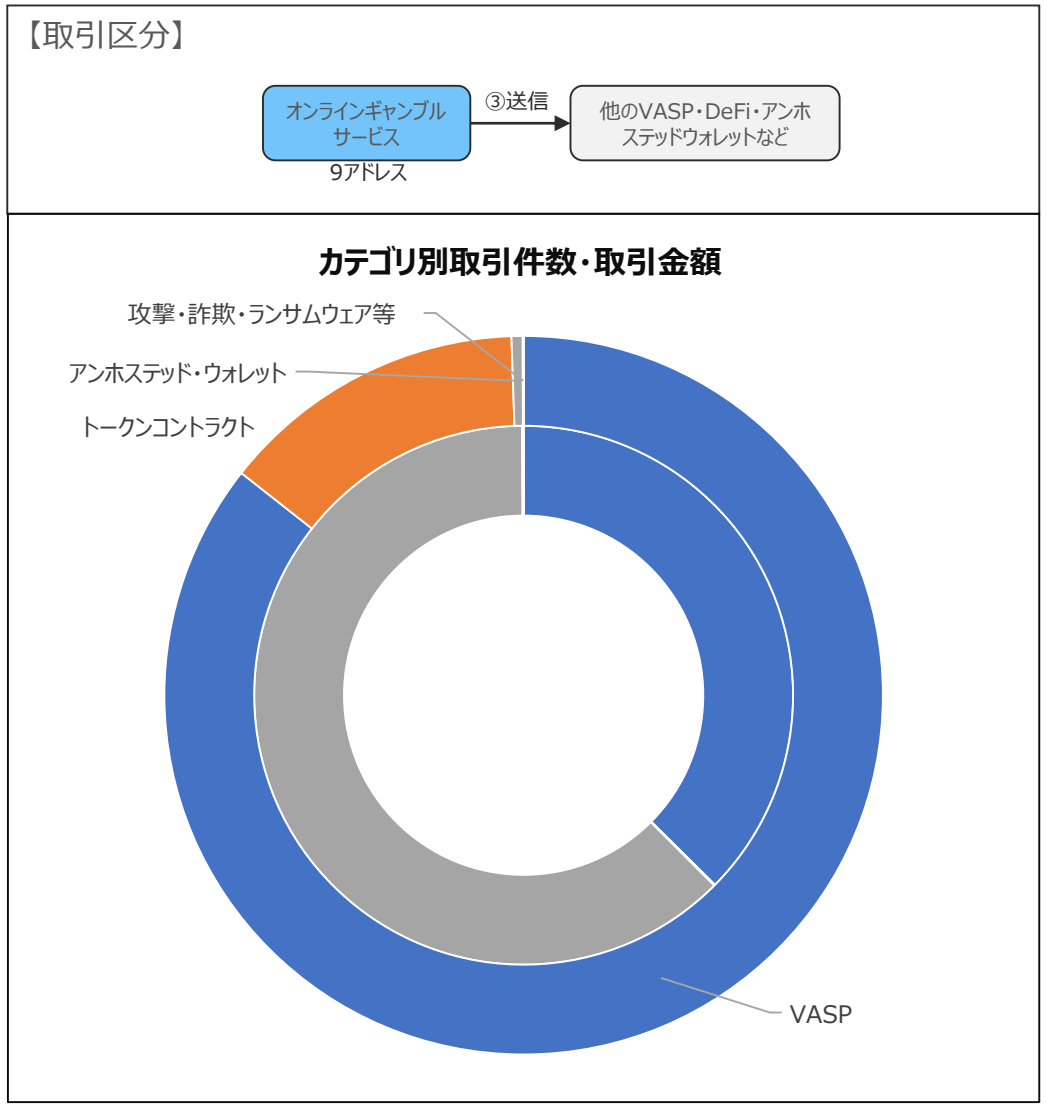


表4-4-6-4　オンラインギャンブルサービスから送金されたカテゴリ別取引データ

アカウントのカテゴリ別	③送信		
	取引件数	件数比率	取引金額M$
VASP	24,495	85.6%	8
トークンコントラクト	3,961	13.8%	0
アンホステッド・ウォレット	143	0.5%	13
攻撃・詐欺・ランサムウェア等	12	0.0%	0
合計	28,611	100.0%	21

アカウント名などの特定有無	③送信		
	取引件数	件数比率	取引金額M$
アカウント名等を特定	28,611	7.4%	21
アカウント名等が不明	357,354	92.6%	874
合計	385,965	100.0%	895

【考察】

- カテゴリ別は、VASPが最も多い
  → 大手VASPのウォレットをオンラインギャンブルサービスの送金先に利用することが多いと考えられる
- 次に多いのは、トークンコントラクトである
  → ステーブルコイン（USDCやDAIなど）の送金のためと考えられる

（５）ミキシングサービスから送金されたアドレスの取引件数・金額

図4-4-6-5　ミキシングサービスから送金されたカテゴリ別取引件数・金額

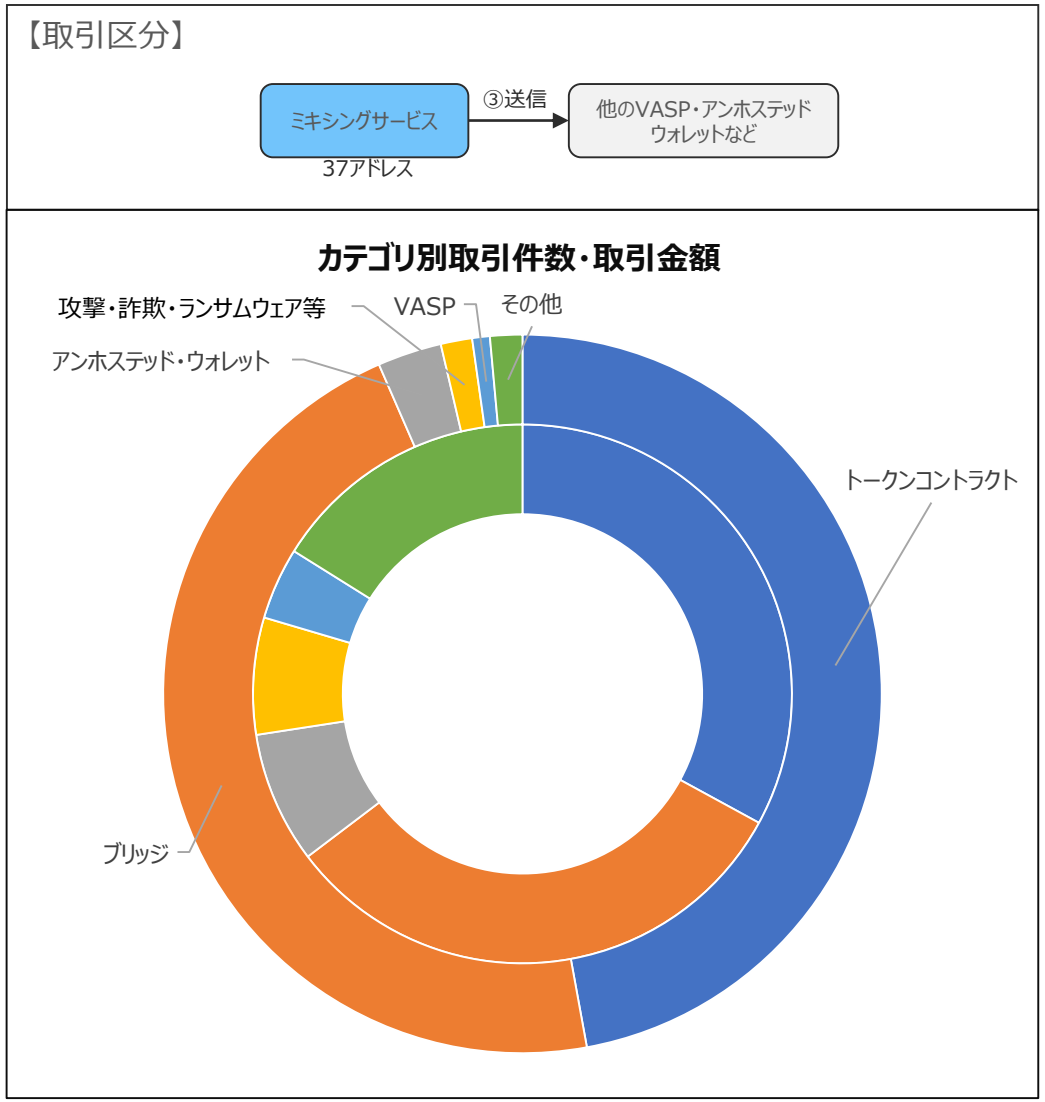


表4-4-6-5　ミキシングサービスから送金されたカテゴリ別取引データ

アカウントのカテゴリ別	③送信		
	取引件数	件数比率	取引金額M$
トークンコントラクト	9,341	47.1%	22
ブリッジ（他チェーンへの送金）等	9,183	46.3%	22
アンホステッド・ウォレット	572	2.9%	5
攻撃・詐欺・ランサムウェア等	280	1.4%	5
VASP	157	0.8%	3
その他	287	1.4%	11
合計	19,820	100.0%	68

アカウント名などの特定有無	③送信		
	取引件数	件数比率	取引金額M$
アカウント名等を特定	19,820	11.7%	68
アカウント名等が不明	148,879	88.3%	2,491
合計	168,699	100.0%	2,560

【考察】

- カテゴリ別は、トークンコントラクトが最も多い
  → ミキシングサービスを利用するための送金（主にWETHなど）に使われていると考えられる
- 次に多いのは、ブリッジ（他チェーンへの送金）等である
  → Ethereumブロックチェーンでミキシングした資金を、他のブロックチェーンに送金することが考えられる

（６）AML/CFT関連

表4-4-6-6　AML/CFTのデータ調査結果（１／５）

カテゴリ	調査対象項目	調査対象データ	リサーチ結果				監督下にある事業者が、保有するデータと調査可能性
			データソース	データ取得方法	データ取得結果①※	データ取得結果②※	
AML/CFT取引に関するレッドフラッグ	0.1ETH（約2.5万円）未満での暗号資産取引（交換や送金など、記録管理や報告の閾値回避行動と仮定）	ユーザ（アカウント）のアドレス	Etherscan 自社データベース	0.1ETH（約2.5万円）未満の少額取引を送信したアドレスを取得する	65,482アドレス 【内訳】VASP 42,889 アンホステッド・ウォレット 11,362	27,013,172アドレス	VASPは利用者のアドレスとCDD/EDD情報を紐つけて保管しており、左記との組合わせにより、より確度の高い、疑わしい取引の絞り込みや届出が可能か
		上記アドレスの取引件数・取引額	Etherscan 自社データベース	上記アドレスの取引件数・金額を取得する	件数：69,669,928件 金額：46.1億USD	件数：167,267,783件 金額：91.4億USD	
	複数の高額取引を24時間以内など短時間で連続して取引する場合	ユーザ（アカウント）のアドレス	Etherscan 自社データベース	同じ送信者が24時間以内に10ETH（約1.8万USD）以上の取引を送信したアドレスを取得する	3,351アドレス 【内訳】VASP 1,436 アンホステッド・ウォレット 846	59,127アドレス	
		上記アドレスの取引件数・取引額	Etherscan 自社データベース	上記アドレスの取引件数・金額を取得する	件数：2,631,151件 金額：8,109億USD	件数：3,874,440件 金額：12,027億USD	
		上記アドレスの取引頻度	Etherscan 自社データベース	上記の取引について、時間別の取引件数の比率を取得する	1時間以内：88.4% 1-12時間：10.1% 13-24時間：1.5%	－	
	新しく作成されたアカウントまたは非アクティブだったアカウントに対して複数の高額取引を行う場合	ユーザ（アカウント）のアドレス	Etherscan 自社データベース	アドレスの最初の入金から24時間以内に10ETH以上の取引を送信したアドレスを取得する	703アドレス 【内訳】 アンホステッド・ウォレット 335 VASP 151	213,668アドレス	
		上記アドレスの取引件数・取引額	Etherscan 自社データベース	上記アドレスの取引件数・金額を取得する	件数：2,164件 金額：8.85億USD	件数：259,264件 金額：745.6億USD	
		上記アドレスの一定期間内の取引頻度	Etherscan 自社データベース	上記の取引について時間別の取引件数の比率を取得する	1時間以内：36.5% 1-12時間：57.5% 13-24時間：6.0%	－	
		上記アドレスの取引件数	Etherscan 自社データベース	上記の取引について時間別の取引件数を取得する	1時間以内：813件 1-12時間：1,280件 13-24時間：132件		

※データ取得結果①：ブロックチェーン分析会社がカテゴリ名やアカウント名を特定したアドレスにおける調査結果　※データ取得結果②：今回調査で取得したデータ全量（カテゴリ名などを特定していないアドレスを含む）

（６）AML/CFT関連

表4-4-6-6　AML/CFTのデータ調査結果（２／５）

カテゴリ	調査対象項目	調査対象データ	リサーチ結果				監督下にある事業者が、保有するデータと調査可能性
			データソース	データ取得方法	データ取得結果①※	データ取得結果②※	
AML/CFT取引に関するレッドフラッグ	暗号資産を複数のVASPに即時に転送する場合	ユーザ（アカウント）の特定	Etherscan 自社データベース	複数のVASPに送信するウォレットを取得する	997アドレス 【内訳】 アンホステッド・ウォレット　731 VASP 200	1,086アドレス	VASPは利用者のアドレスとCDD/EDD情報を紐つけて保管しており、左記との組合わせにより、より確度の高い、疑わしい取引の絞り込みや届出が可能か
		VASP等の特定	Etherscan 自社データベース	上記のウォレットが送信するVASPを特定する	9,268アドレス	－	
	盗まれた資金を保有していると特定された暗号資産アドレスや盗まれた資金の保有者に関連した暗号資産アドレスから、不正に入金されたと疑われる資金を受け取る場合	不正利用されているアドレス	Etherscan 自社データベース	既知の攻撃者のアドレスを取得する	422アドレス	－	－
		上記アドレスの取引相手のアドレス	Etherscan 自社データベース	既知の攻撃者に送信するウォレットを取得する	4,191アドレス 【内訳】VASP 1,567 アンホステッド・ウォレット 1,285	163,109アドレス	VASPは利用者のアドレスとCDD/EDD情報を紐つけて保管しており、左記との組合わせにより、より確度の高い、疑わしい取引の絞り込みや届出が可能か
AML/CFT取引パターンに関するレッドフラッグ	新規ユーザが暗号資産の全残高を取引するか、暗号資産を引き出してプラットフォームから全残高送金する場合	新規ユーザのアカウント	Etherscan 自社データベース	VASPの新規ユーザを取得する	137アドレス	57,415アドレス	
		上記アカウントが行う全残高取引	Etherscan 自社データベース	ユーザの残高を計算し、残高を空にする取引を取得する	175件	75,993件	
	特定の期間（1日、1週間、1か月など）に複数の人が同じ暗号資産アカウントに頻繁に送金する場合	ユーザ（アカウント）のアドレス	Etherscan 自社データベース	複数のアドレスから繰り返し送金されている同じアドレスを取得する	106アドレス 【内訳】詐欺・攻撃者　28 VASP 23 アンホステッド・ウォレット　12	25,543アドレス	
		上記アドレスの取引件数・取引額	Etherscan 自社データベース	上記アドレスの取引件数・金額を取得する	件数：21,338件 金額：5,087万USD	件数：1,688,075件 金額：14.6億USD	
		上記アドレスの取引頻度	Etherscan 自社データベース	上記の取引について、時間別の取引件数の比率を取得する	1時間以内：44.3% 24時間以内：54.7% 1日-30日：1.0%	－	

※データ取得結果①：ブロックチェーン分析会社がカテゴリ名やアカウント名を特定したアドレスにおける調査結果　※データ取得結果②：今回調査で取得したデータ全量（カテゴリ名などを特定していないアドレスを含む）

（６）AML/CFT関連

表4-4-6-6　AML/CFTのデータ調査結果（３／５）

カテゴリ	調査対象項目	調査対象データ	リサーチ結果				監督下にある事業者が、保有するデータと調査可能性
			データソース	データ取得方法	データ取得結果①※	データ取得結果②※	
AML/CFT匿名性に関するレッドフラッグ	ミキシング、タンブリングサービスやP2Pプラットフォームを運営するVASPを利用したことがあるwalletとの間で暗号資産がやり取りされた場合	ミキシング、タンブリングサービスやP2Pプラットフォームを運営するVASPのアドレス	Etherscan 自社データベース	ミキシングサービスを利用したVASPのアドレスを取得する	116アドレス	–	VASPは利用者のアドレスとCDD/EDD情報を紐つけて保管しており、左記との組合わせにより、より確度の高い、疑わしい取引の絞り込みや届出が可能か
		ミキシングサービス等と取引を行ったwallet（ユーザアカウント）などのアドレス	Etherscan 自社データベース	ミキシングサービス等を取引を行ったホステッド/アンホステッド・ウォレットなどのアドレスを取得する	33,236アドレス 【内訳】VASP 22,257 アンホステッド・ウォレット 6,304	9,035,176アドレス	
	ミキシング、タンブリングサービスを利用する取引の場合（当該walletアドレスとダークネットマーケットプレイスとの間の不正な資金の流れを隠蔽する意図を示唆している）	ミキシング、タンブリングサービスを利用した取引を行ったアドレス	Etherscan 自社データベース	ミキシングサービスのアドレスを取得する	37アドレス ※全てTornado Cash関連他社ツールでは他にRailgunがある ※OFAC制裁リストは90アドレス(うち重なりは26アドレス)	–	
	ダークネットマーケットプレイス、ミキシング/タンブリングサービス、疑わしいギャンブルサイト、違法行為（ランサムウェアなど）や盗難報告など、既知の疑わしい情報源への直接的・間接的な関連を含む、暗号資産アドレスまたはwalletからの入金や出金をする場合	既知の疑わしい情報源を特定するデータ	Etherscan、DappRadar、IC3、CISA、OFAC 自社データベース	DappRadar、IC3、CISA、OFACからダークネットにリンクする不正ウォレットアドレスを取得する	12アドレス ※ダークネットWEBのURLとそれに紐づくアドレスを特定	–	
		上記疑わしい情報源と取引を行ったアドレス	Etherscan、DappRadar、IC3、CISA、OFAC 自社データベース	上記の不正アドレスと取引を行ったアドレスを取得する	送信：38アドレス/50件 受信：4アドレス/5件	送信：38アドレス/50件 受信：143アドレス/193件	

※データ取得結果①：ブロックチェーン分析会社がカテゴリ名やアカウント名を特定したアドレスにおける調査結果　※データ取得結果②：今回調査で取得したデータ全量（カテゴリ名などを特定していないアドレスを含む）

（６）AML/CFT関連

表4-4-6-6　AML/CFTのデータ調査結果（４／５）

カテゴリ	調査対象項目	調査対象データ	リサーチ結果				監督下にある事業者が、保有するデータと調査可能性
			データソース	データ取得方法	データ取得結果①※	データ取得結果②※	
AML/CFT匿名性に関するレッドフラッグ	顧客管理（CDD）や本人確認（KYC）プロセスがないもしくは不十分なVASPからの資金授受を行う場合	VASPの加入時にCDD/KYCプロセスがないと思われるVASPの特定	Etherscan 自社データベース	VASPの加入時にCDD/KYCプロセスがないと思われるVASPのアドレスを取得する	788アドレス ※分散型でない、且つ所在地に登録されていないVASPのアドレスを取得	－	VASP自身が、取引相手VASPのデューデリを実施する過程で、無登録VASPと判明した事例があれば、当局等へ情報も可能か
AML/CFT送信者または受信者に関するレッドフラッグ	ユーザの暗号資産アドレスが違法行為に関連する公開掲示板に表示されている場合	不正取引を行ったアドレス	Etherscan, Reddit Bulletin Board, Darknet forums & marketplaces 自社データベース	DappRadar、Reddit掲示板、ダークネットフォーラムからダークネットにリンクする不正ウォレットアドレスを取得する	12アドレス	－	VASP自身が、顧客による不公正取引を発見した場合、疑わしい取引の届出等により当局へ情報提供
	過去に犯罪に関与したことがあり、公開されている情報を通じて法執行機関に知られているユーザ	不正取引を行ったアドレス	Etherscan, IC3, CISA, OFAC 自社データベース	IC3、CISA、OFACに公開されている制裁アドレスを収集する	送信：50アドレス/61件 受信：61アドレス/74件	送信：629アドレス/2,224件 受信：311アドレス/580件	
AML/CFT資金の源泉に関するレッドフラッグ	詐欺・恐喝、ランサムウェアスキーム、制裁対象のアドレス、ダークネットマーケットプレイス、またはその他の違法なWebサイトに関連する暗号資産アドレスでの取引	違法なWebサイトに関連する暗号資産アドレス	CISO OFAC , Threat Intelligence (Darknet), CISA, IC3 , CSAM Data (Hades) 自社データベース	詐欺・恐喝、ランサムウェアスキーム、制裁対象のアドレス、ダークネットマーケットプレイス、またはその他の違法なWebサイトに関連付けられたアドレスを特定する	送信：2,407アドレス 117,650件 受信：142アドレス 14,357件	送信：56,235アドレス /264,817件 受信：172アドレス/ 91,344件	
	オンラインギャンブルサービス経由の暗号資産取引	オンラインギャンブルサービスを利用したユーザのアドレス	Etherscan Word Cloud, ETHplorer.io 自社データベース	オンラインギャンブルサービスのアドレスを特定し、そのアドレスを利用した取引のアドレスを取得する	送信：ギャンブル 7アドレス ユーザ 257アドレス 取引 28,742件 受信：ギャンブル 2アドレス ユーザ 2アドレス 取引 3件	送信：ギャンブル 13アドレス ユーザ 102,392アドレス 取引 386,225件 受信：ギャンブル 11アドレス ユーザ 113,524アドレス 取引 627,912件	

※データ取得結果①：ブロックチェーン分析会社がカテゴリ名やアカウント名を特定したアドレスにおける調査結果　※データ取得結果②：今回調査で取得したデータ全量（カテゴリ名などを特定していないアドレスを含む）

（６）AML/CFT関連

表4-4-6-6　AML/CFTのデータ調査結果（５／５）

カテゴリ	調査対象項目	調査対象データ	リサーチ結果				監督下にある事業者が、保有するデータと調査可能性
			データソース	データ取得方法	データ取得結果①※	データ取得結果②※	
AML/CFT資金の源泉に関するレッドフラッグ	サードパーティのミキシングサービスまたはwalletタンブラーから直接調達されたユーザの資金	ミキシング、タンブリングサービスを利用した取引を行ったアドレス	Etherscan 自社データベース	ミキシングサービスから送金されたアドレスを取得する	ミキシング 37アドレス 送金先 769アドレス 取引 19,820件	送金先 53,268アドレス 取引 168,699件	VASP自身が、顧客によるこれら利用を発見した場合、疑わしい取引の届出等により当局へ情報提供が可能
	詐欺/不正なアドレスから大部分の収益が発生しているユーザ	不正取引を行ったアドレス	Etherscan 自社データベース	既知の詐欺/不正アドレスから送金されたアドレスを取得する	詐欺/不正 147アドレス 送金先 59アドレス 取引 1,121件	【全件】 詐欺/不正　1,142アドレス 送金先 1,186アドレス 取引 4,742件	
AML/CFT地理的リスクに関するレッドフラッグ	ユーザの資金が、ユーザまたは取引所が所在する法域に登録されていない取引所から送金された場合	所在する法域に登録されていない取引所のアドレス	Etherscan 自社データベース	所在する法域に登録されていないVASPからユーザに送金された取引のVASPのアドレスを取得する	139アドレス	–	VASPは利用者のアドレスとCDD/EDD情報を紐つけて保管しており、左記との組合わせにより、より確度の高い、疑わしい取引の絞り込みや届出が可能か
		所在する法域に登録されていない取引所から送金されたユーザのアドレス	Etherscan 自社データベース	所在する法域に登録されていないVASPからユーザに送金した取引のユーザのアドレスを取得する	8,275アドレス 内訳：VASP（ホステッド・ウォレット含む）8,266、その他　9	–	
	注意が必要な法域の暗号資産取引所を利用している場合（暗号資産事業体へのAML/CFT対策が不十分であることによるリスク）	注意が必要な法域の特定	Etherscan、OFAC、 自社データベース	OFAC制裁国リスト・米国軍事輸出禁止国リストの対象国を取得する	49ヶ国・地域※ ①OFAC制裁国リスト　25 ②米国軍事輸出禁止国リスト24（①と②は重複を含む）	–	• 同上 • VASP自身は、自社の定める高リスク国等と、ツール側の設定に差異がないか確認の上、活用が必要。

※【注意が必要な法域】 49ヶ国・地域
①OFAC制裁国リスト　25ヶ国・地域　https://ofac.treasury.gov/sanctions-programs-and-country-information
アフガニスタン、バルカン、ベラルーシ、ミャンマー、中央アフリカ、中国、キューバ、北朝鮮、コンゴ、エチオピア、香港、イラン、イラク、レバノン、リビア、マリ、ニカラグア、ソマリア、南スーダン、スーダン、シリア、ロシア、ベネズエラ、イエメン、ジンバブエ
②米国軍事輸出禁止国リスト　24ヶ国・地域　https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.1
ベラルーシ、ミャンマー、中国、キューバ、イラン、北朝鮮、シリア、ベネズエラ、アフガニスタン、カンボジア、中央アフリカ、キプロス、コンゴ、エチオピア、エリトリア、ハイチ、イラク、レバノン、リビア、ロシア、ソマリア、南スーダン、スーダン、ジンバブエ

※データ取得結果①：ブロックチェーン分析会社がカテゴリ名やアカウント名を特定したアドレスにおける調査結果　※データ取得結果②：今回調査で取得したデータ全量（カテゴリ名などを特定していないアドレスを含む）

4-4. AML/CFT関連のデータ分析結果
4-4-7. 主なFindings

表4-4-7　主なFindings

主なFindings	内容
分析ツールと比較した際のリサーチの一定の有用性	• FATF報告書の指摘によるデータの取得可能性について、本調査研究で調査対象としたAML/CFT関連データのうち、分析ツールではデータ取得が困難なものが多いが、専門家によるリサーチでは多くの調査項目でデータ取得が可能であった。AML/CFT関連の実態把握を行う際には、分析ツールに加えて、専門家によるリサーチを行うことも有効と考えられる。 • 但し、本調査研究でも取得が難しいデータが一定数存在することが確認されたため、監督による情報提供なども含めてデータ取得の可能性について明らかにしていくことが今後必要であると考える。
高リスク判定の困難さ	• 高リスクアドレス・取引の定義上、VASP関連取引は「高リスク」と分類されるものが多い結果となっている（取引件数の極めて多いVASP関連アドレスが「高リスク」とラベリングされている）が、当該アドレスに関連する取引の多くは通常の取引である可能性が高く、今回の調査結果を持って一概に結論を出すことは困難。 • アカウントが特定できていないアドレスの多くはアンホステッド・ウォレットであるとも考えられるが、リスクの様態は不明であり、P2P等の正確な実態把握（取引量など）やリスク評価は極めて難しいと考えられる。
VASP、アンホステッド・ウォレット（含P2P）、DeFi間の密接な相互連関	• VASP間の取引に限らず、VASP・アンホステッド・ウォレット（P2P含む）・DeFiの間で密接な取引関係が存在しており、（定義の難しさはあるものの）高リスク取引も相当数確認された。 • 多くの法域で規制対象外となっているP2Pや高度に分散化されたDeFiのML/TF/PFリスクを低減するためには、上述のアンホステッド・ウォレットやP2Pのデータ分析の困難性も加味すると、規制上の対応が相対的に容易であるVASPへのコントロールの強化（VASP-アンホステッド・ウォレット間の取引に対するEDD等）が有効である可能性。
データ及びデータ分析の信頼性を向上させるための取組みの必要性	• 本調査研究の結果、Ethereumブロックチェーンのデータのうち、ブロックチェーン分析会社がカテゴリ名やアカウント名を特定した対象が全体の約1割程度に留まっており、必ずしも分散型金融システム全体のデータを分析できていないことが確認された。 • また、特定したカテゴリ名やアカウント名、および高リスク取引の判定は全てブロックチェーン分析会社からの情報に依存しており、アカウント名等の特定やリスクスコアの算出は分析会社が独自に行っているため、分析会社ごとに内容が異なることが考えられる。 • よって、実態調査などを行う場合は、複数の分析会社による調査結果の比較など、1社のデータに依存しないなどデータの信頼性を高める工夫が必要と考えられる。

第５章　おわりに

第５章 おわりに

（１）データ分析を実施しての気づき

- 金融当局として分析ツール・リサーチャーを適確に使いこなすには一定の訓練が必要。現時点でのツールの限界も理解しておく必要（モニタリング力を大幅に向上させるようなsilver bulletではない）。
  - ツール及びリサーチャーから得られたデータのサニタイズ（例：外れ値の除去）やコンテクストの理解（例：トークンコントラクト関連の取引は実際のトークンの移転ではなく、ステーブルコイン等のアドレス（EOA）間の移転に伴うスマートコントラクトの挙動であること）が必要。
  - ツール会社、ソリューションは区々で（捜査当局向けに特化したものや、当局ではなく事業者が主に活用するものも）、用途にあったツールの選定、ツールの全体像の把握、最新技術動向の収集などが必要。
- 他方、規制監督対象となっていない先（DeFi、P2Pなど）も含め、暗号資産市場における相互連関（VASP-アンホステッド・ウォレット-DeFi間の繋がり等）や不正取引の実態を把握する上で有益な視座が得られる可能性もあり、今後ツールの識別率や精度が向上していく可能性も加味すると、ツール・リサーチャーの活用は模索していくべきか。

（２）初期的な金融規制上のインプリケーション

- 規制対象主体（VASP）とその他（アンホステッド・ウォレット・P2P・（完全に分散された）DeFi）の密接な関係を考慮すると、VASPに対するコントロールを強化することで、間接的にP2P等の規制対象外のアクティビティのリスクも低減できる可能性。
- DeFiやERC-20関連（ステーブルコイン等）のトークンコントラクト、ブリッジなど、スマートコントラクト関連の取引がイーサリアム上では多い。ハッキング等も多発しており、セキュリティの向上が大きな課題か。
- 犯罪に関与しているとみられるアドレスの特定は可能でも、実際の所有者等を識別するのは容易ではない（今回の調査研究で使用した分析ツールは犯罪捜査を目的としていないが、専門の分析ツールを活用すれば異なる結果となる可能性はある）。

付録

付録1. 研究文献で活用されているデータ分析手法

（１）研究文献のデータ分析手法

- ブロックチェーンの実態把握のため、オンチェーン／オフチェーンデータを分析した主な研究文献を調査し、そのデータ分析手法を調査した。
- 調査の結果、ブロックチェーンアドレスの複数アカウントの管理者や疑わしい取引の特定などを目的として、アドレスのクラスタリングやグラフ理論・機械学習を活用した複数の分析手法が確認された。
- 但し、研究の結果は全体傾向の把握や一部の対象アドレスの特定などであり、公開されているオンチェーン／オフチェーンデータからの分析ではブロックチェーンの実態把握に限界があると考えられる。

表A-1-1　研究文献のデータ分析手法

データの区別	データ分析手法	分析手法の概要	調査結果
オンチェーンデータ分析	クラスタリング	• ブロックチェーンのアドレスなどをデータ分析手法によりグループ分けすることで、目的とするデータを大まかなグループに分類する	• ブロックチェーンアドレスのクラスタリングに関する研究として以下3件を確認した ➢ トランザクションの入力に現れるアドレス ➢ アドレス再利用・エアドロップ（トークンの配布）などの取引パターンによるアドレスの分類 ➢ ブルームフィルタ（確率的データ構造）によるアドレスの特徴付け　など
	グラフ理論	• ノード（頂点）、エッジ（ノードを結ぶ線）の集合で構成される数学の理論を応用し、ノードをブロックチェーンアドレス、エッジをトランザクションとしてその集中度などの関係性からノードやエッジの特徴を分析する	• グラフ理論がブロックチェーンアドレスのクラスタリングやトランザクションの傾向分析などで研究されていることを確認した
	機械学習	• サンプルデータに基づいてモデルを構築し、明示的にプログラムされることなく予測(判定）を行う • 学習方法の違いにより、複数のアルゴリズムが存在する （教師あり学習、教師なし学習、強化学習など）	• 機械学習のうち、以下3件の分析手法が違法アドレスの検出などで研究されていることを確認した ➢ ランダムフォレスト ➢ サポートベクターマシン ➢ XGBoost
	その他	• 上記以外のオンチェーンデータの分析方法について調査する	• スマートコントラクトのコードと取引ログの分析事例1件を確認した （ポンジスキームと疑われる挙動を分析して検出ツールで調査）
オフチェーンデータ分析	公開データのスクリーニング	• 公開されているオフチェーンデータを用いて、ブロックチェーンの分析に有効なデータの選別を行う	• 以下のデータ分析事例3件を確認した ➢ Twitterの「Whale Alert」とBitcoinの価格上昇を紐付け ➢ 公開のブロックチェーン投稿サイトから犯罪行為関連アドレスを洗い出し ➢ 学術データベース、ジャーナル誌を検索して市場操作手法を調査　など

付録1. 研究文献で活用されているデータ分析手法

（２）研究文献の調査結果

表A-1-2　研究文献の調査結果（１／５）

No.	出所	文献名	概要	オンチェーンデータ分析				オフチェーンデータ分析
				クラスタリング	グラフ理論	機械学習	その他	
1-1	The Journal of Finance Volume 75, Issue 4	Is Bitcoin Really Untethered?	• Bitcoinの価格上昇に対するTether（USDT：米ドルにペッグされたステーブルコイン）との関係について、2014年10月～2018年3月のブロックチェーンデータを分析 • Tetherの発行により、Bitcoin価格の市場操作が行われたと推測されることを報告	○ トランザクションの入力に現れるアドレスをグループ分け				
1-2	Finance Research Letters Volume 49	The Intraday Bitcoin Response to Tether Minting and Burning Events: Asymmetry, Investor Sentiment, and “Whale Alerts” on Twitter	• Tetherが発行された2014年10月～2021年1月までのブロックチェーンデータを分析し、Tetherの発行に対するBitcoinの反応を調査 • 調査の結果、Tetherの発行イベントが「Whale Alert」により高額取引がほぼリアルタイムでTwitterに通知され、投資家の前向きな感情によりBitcoinの価格が上昇していたことを報告					○ Whale AlertのTwitter発表とBitcoinの価格上昇を分析
2	Financial Cryptography and Data Security 2020	Address Clustering Heuristics for Ethereum	• アドレス再利用やエアドロップ等の取引パターンからEthereumアドレスをクラスタリングし、複数のアカウントを管理している可能性が高いエンティティを分析 • Ethereumアドレスの約18%がクラスター化でき、複数アドレスを管理する34万以上のエンティティを特定	○ アドレス再利用、エアドロップなどの取引パターンからアドレスをグループ分け				

付録1. 研究文献で活用されているデータ分析手法

（２）研究文献の調査結果

表A-1-2　研究文献の調査結果（２／５）

No.	出所	文献名	概要	オンチェーンデータ分析				オフチェーンデータ分析
				クラスタリング	グラフ理論	機械学習	その他	
3	2021 IEEE International Conference on Decentralized Applications and Infrastructures	Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users	• グラフ理論を用いた機械学習によりEthereumアドレスの関連付けによるユーザー特定方法を研究 • ユーザーのプロファイリングは、ノード埋め込み手法が優れていることを説明	○ アドレスのクラスタリングによるユーザー特定方法を研究	○ データ分析にグラフ分析（ノード埋め込み手法）を活用	○ データ分析に機械学習を活用		
4	30th USENIX Security Symposium	Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain	• Ethereumのフロントランニング攻撃（マイナーがブロック生成時に取引を故意に入れ替えて利益を得る攻撃）の行動を効率的に測定する手法を研究 • 約20万件の攻撃取引、1.5千件の攻撃者アカウント、ボット、利益額などを特定	○ ブルームフィルタ（確率的データ構造）を用いて攻撃者のアドレスをグループ分け				
5	IEEE INFOCOM 2018 - IEEE Conference on Computer Communications	Understanding Ethereum via Graph Analysis	• Ethereumのトランザクションデータから、グラフ理論による分析でセキュリティ問題に対するアプローチを実施 ➢ ①攻撃フォレンジック：悪意のあるスマートコントラクトの攻撃者アカウントの検出 ➢ ②異常検出：呼び出されない多数のスマートコントラクトを作成するアカウントの検出 ➢ ③非匿名化：ノードに関するコメントなどの情報から重要なキーワードを抽出		○ マネーフロー/スマートコントラクト作成/スマートコントラクト呼出をグラフ理論で分析			

付録1. 研究文献で活用されているデータ分析手法

（２）研究文献の調査結果

表A-1-2　研究文献の調査結果（３／５）

No.	出所	文献名	概要	オンチェーンデータ分析				オフチェーンデータ分析
				クラスタリング	グラフ理論	機械学習	その他	
6	FC 2019: Financial Cryptography and Data Security	Measuring Ethereum-based ERC20 Token Networks	• Ethereumの上位1,000種類のトークン転送とトークン所有者の関係をグラフ理論で分析 • トークン転送の大部分は取引所などに集中するが、多くのトークン所有者はトークンを全く移動させないことがわかった		○ トークン転送とトークン所有者をグラフ理論で分析			
7	WWW '20: Proceedings of The Web Conference 2020	Measurements, Analyses, and Insights on the Entire Ethereum Blockchain Network	• Ethereumのユーザーやトランザクション、スマートコントラクト、トークン転送などの相互作用をグラフ理論で分析し、SNSやWebとの類似点・相違点を研究 • トランザクションの分布はSNSなどと異なることを説明		○ 取引やトークン転送などの関連性をグラフ理論で分析			
8	Financial Cryptography and Data Security 2023 Accepted papers	Understanding Polkadot Through Graph Analysis: Transaction Model, Network Properties, and Insights	• Polkadotブロックチェーンのユーザートランザクションをモデル化し、取引アクショングラフで分析 • Binanceの権力集中やネイティブトークンの大半が2%のユーザーで占められている実態を検出		○ ユーザー取引の集中度をグラフ理論で分析			
9	Web Information Systems Engineering – WISE 2019	Detecting Fraudulent Accounts on Blockchain: A Supervised Approach	• 悪意のあるアクターの不正アカウントを検出する目的で、3つの機械学習の分析手法を比較 • ランダムフォレストが再現率と偽陽性率で最良の結果を得た			○ ランダムフォレスト、サポートベクターマシン、XGBoostの3つの手法を比較		

【機械学習のアルゴリズム】
- ランダムフォレスト：
  並列に学習した複数の決定木に予測を行わせ、最終的な出力を多数決や平均で決定するアルゴリズム
- サポートベクターマシン：
  ２つのクラスのデータ群を分割するような境界線などを決定することで分類や回帰を行うアルゴリズム
- XGBoost：
  勾配ブースティングと呼ばれるアンサンブル学習（性能の高くない手法を複数用いて総合的に結果を出力する方法）と決定木（条件分岐によって問題を解く手法）を組み合わせたアルゴリズム

付録1. 研究文献で活用されているデータ分析手法

（２）研究文献の調査結果

表A-1-2　研究文献の調査結果（４／５）

No.	出所	文献名	概要	オンチェーンデータ分析				オフチェーンデータ分析
				クラスタリング	グラフ理論	機械学習	その他	
10	Expert Systems with Applications Volume 150	Detection of illicit accounts over the Ethereum Blockchain	• Ethereumコミュニティ（Etherscam DB）によって違法行為のフラグが立てられた約2千のアドレスと正常なアドレスを基に、XGBoostを用いて取引履歴から違法行為を検出 • 10回の交差検証にて平均96%の精度を達成			○ データ分析にXGBoostを利用		○ EtherscamDBの情報をEthereumアカウントに紐づけ
11	Future Generation Computer Systems Volume 102	Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact	• Ethereum上のポンジスキーム（投資詐欺）を調査し、挙動と影響を分析 • ポンジスキームと疑われる挙動について、検証ツールを用いてスマートコントラクトのコードと取引ログを分析し、184のポンジスキームを特定した				○ スマートコントラクトのコードと取引ログを分析し、ポンジスキームを特定	
12	ICIS 2021 - International Conference on Information Systems	Cryptocurrency Market Manipulation: A Systematic Literature Review	• 暗号資産の市場操作について、7つの学術データベースと3つの有力ジャーナル誌をキーワード検索 • 分析により7つの主要な市場操作方法（Pump&Dump、資金洗浄、オーダーブック、ステーブルコイン、フロントランニング、インサイダー取引、DDOS攻撃）を特定					○ 学術データベース、有力ジャーナル誌をキーワード検索して傾向を分析

付録1. 研究文献で活用されているデータ分析手法

（２）研究文献の調査結果

表A-1-2　研究文献の調査結果（５／５）

No.	出所	文献名	概要	オンチェーンデータ分析				オフチェーンデータ分析
				クラスタリング	グラフ理論	機械学習	その他	
13	Financial Cryptography and Data Security 2023 Accepted papers	Short paper: DeFi Deception—Uncovering the prevalence of rug pulls in cryptocurrency projects	• DeFiの持ち逃げ詐欺（rug pull）に関する詐欺実行までの期間と手法を分析し、詐欺の傾向を調査 • 2022年後半以降、詐欺がIDO（DEXのトークン発行による資金調達）、NFTなどの新サービス以降により持ち逃げ詐欺が減少している					○ Bitcointalk（ディスカッションフォーラム）、マーケットサイトの情報を分析