ステーブルコインの健全な発展に向けた分析
調査研究報告書

令和7年3月

デロイト トーマツ コンサルティング合同会社

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、米ジョージタウン大学・松尾真一郎研究教授、立命館大学・上原哲太郎教授から有益な助言やコメントをいただいたほか、日本銀行、デジタル庁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・助言をいただきました
- また、アドレス分析のChainalysis社、Elliptic社、TRM Labs社の分析レポートを参照し、個別にヒアリングさせて頂いた内容を一部掲載させていただきました
- 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デロイト トーマツ コンサルティング合同会社に帰します

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ありません
- 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ります

ステーブルコインが市場で存在感を増す中で、不正利用等懸念が報告されています
本研究は、今後の健全な発展に向け実態を把握することを目的としています

研究の背景・目的

■ ステーブルコインが、従来の暗号資産が抱える価格変動リスクを回避し、迅速かつ低コストな送金や決済を実現できる点が強みとされており、個人、企業、機関投資家等による利用が急速に拡大[*1]しつつある。その利用範囲は暗号資産取引の決済に留まらず、国際送金、B2Bクロスボーダー取引、デジタル決済、Eコマース等、多岐にわたって導入が進展している[*2]。

*1 時価総額2,100億ドル超規模(25年1月時点)、最もシェアの高いTether（USDT）は全暗号資産のうち時価総額3位と無視できない規模

*2 決済手段として主流ではないが、既存決済ネットワーク（決済国際ブランド等）と接続することで利便性を高める等一部国・地域で普及が進みつつある

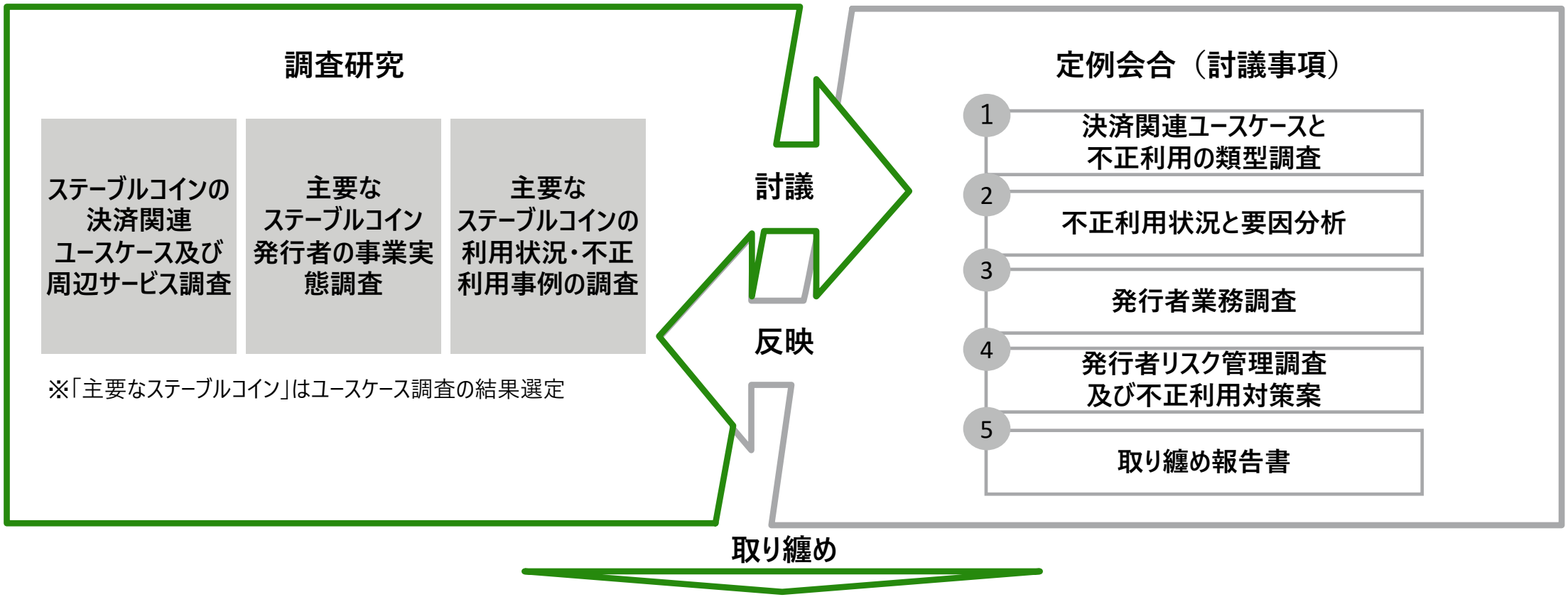
■ 一方で、匿名性や即時性を悪用する形で、一部のステーブルコインの不正利用が拡大しているとの民間分析会社による報告もある等、特にAML/CFTの観点から懸念も指摘されており、国際的にも問題意識が高まっている。また、FSBからは、不正利用に限定せずとも、ステーブルコインの利用拡大は、金融安定にもたらすリスクを含有することも指摘されている。そこで、本研究は、ステーブルコインの多様な決済利用の実態把握とその潜在的リスクを分析しつつ、ステーブルコインがもたらす新たな機会を最大限に活かすための知見を提供することを目的とする。

■ 本調査研究では以下の項目に対して、机上調査および有識者ヒアリング等を実施した上で調査研究レポート（本書）を取り纏め、国際会議等で発信を想定する。主な読者をステーブルコインのステークホルダーとし、今後の新たな発行やユースケースの発展に向けた潜在的リスクへの対策の方向性を提示する。

- ステーブルコインの決済関連ユースケース及び周辺サービス調査
  主要なステーブルコインの利用実態に関する調査を行い、普及を促進する要因となる技術やサービスを特定する
- 主要なステーブルコインの利用状況・不正利用事例の調査
  不正の全体像や状況を体系的に整理し、これまでの対策方法のみでは防止困難な状況を調査する。調査はLayer2, 非管理型ウォレット、決済サービス等の動向整理を行う等技術レベルで実施する
- 主要なステーブルコイン発行者の事業実態調査
  発行者の事業実態として、資産管理（プロセス）・普及活動（提携先や周辺サービス等）を調査し、リスク管理体制を解明する

調査研究内容の調査状況を定例会合で報告・討議し、有識者アドバイスを調査に反映させ、報告書を取り纏めました

アプローチ



報告書目次

用語集

#	用語	定義
1	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じ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。スマートコントラクトは、ブロックチェーンネットワーク内のノードによって実行されます。すべてのノードが同じ実行結果を得る必要があり、実行結果はブロックチェーンに記録されます
2	分散型金融	➢ 金融サービスの提供における１つ以上の仲介者または集中型プロセスの必要性を削減または排除する可能性のあるテクノロジーを使って運営される一連の代替金融市場、商品、システム
3	分散アプリケーション (dapp)	➢ スマートコントラクトとフロントエンドユーザーインターフェイスを組み合わせた分散型ネットワーク上に構築されたアプリケーション
4	決済事業者	➢ 決済事業者とは、商取引において、資金の送金、決済、清算などのサービスを提供する企業や機関をいう。クレジットカード会社、電子マネー発行者、モバイル決済プロバイダー、銀行など伝統的な事業者のほか、暗号資産やステーブルコインを決済手段とする場合にその交換を仲介する事業者も含む。
5	アドレス分析事業者	➢ アドレス分析事業者とは、ブロックチェーンに記録されたデータを分析し、暗号資産取引のモニタリングや追跡に資する情報を提供することを専門とする事業者をいう。ブロックチェーン外に存在する公表情報を分析し、不正利用に使われたアドレス等を特定すること等に特化したサービスを提供する。
6	ウォレット事業者	➢ ウォレット事業者とは、暗号資産の保管、送受信、管理を行うためのサービスを提供する事業者をいう。ウォレットには、カストディアルウォレットとノンカストディアルウォレットに大別されるため、いずれのサービスを提供するのかによって事業に付随するリスクが異なる。
7	FATF	➢ Financial Action Task Force 金融活動作業部会
8	OFAC	➢ The Office of Foreign Assets Control 米国財務省の外国資産管理室
9	KYC	➢ Know Your Customer 顧客確認のプログラム
10	AML/CFT	➢ Anti Money Laundering and Combating the Financing of Terrorism マネー・ロンダリング及びテロ資金供与対策

研究結果サマリ

■ ステーブルコインは暗号資産との取引等が中心だが、決済関連ユースケースも昨今導入が進展している。主には、銀行口座保有率が低い、あるいは自国通貨のインフレ率が高い一部国において、自国通貨の代替としての価値保存や既存銀行ネットワークに代わる価値交換手段として活用されている。本邦においてもこのグローバルの環境変化に対して、規制当局・関係事業者・利用者各々の視点でどの様に対応していくべきかを引き続き検討していくことが重要である。

■ 国際的に問題意識が高まっているステーブルコインの不正利用については、民間分析会社の報告によると、「近年、制裁主体に関する大規模な取引の分析が進んだ結果であり、この分類に対するステーブルコインの利用割合が比較的高かったことが要因」（アドレス分析事業者）が実態であり、他分類では引続き暗号資産を直接利用する割合が高い。故に、ステーブルコインの利用拡大により不正が拡大したとは必ずしも言えない。むしろ、ステーブルコインそのものの管理体制だけでなく、背後にある暗号資産との瞬時交換性を捉えた全体像として把握する必要がある事を確認した。

■ ステーブルコインの不正利用への対応は発行者によるBlacklist機能の活用などが考えられるが、発行者が単独で出来ることには限界がありアドレス分析事業者や当局との協力体制が求められる。また、ステーブルコインは換金だけでなくモノやサービスへ交換出来る等、決済およびその周辺事業者やマーチャント等へアクターが拡大していることもあり、今後一層ステークホルダー全体で、各アクターの役割に応じた対策により網の目をきめ細かくすることが期待される。一方、関係者に対する規制やインセンティブ等の面で伝統的金融と比較して未整備な点（残課題）が多く、まだその環境整備に向けた取り組みは道半ばである。

■ 例えば事案発覚時、疑いがある場合にすぐに凍結する（その後疑いが解消されると解除する）、当局に相談してから凍結する等（複数アドレス分析事業者ヒアリング結果）、対応が一様でなくステーブルコインの瞬時に換金できる特性に鑑みると、よりリアルタイムな対策に向けた対応強化が求められる。また誰が見ても不正と認めるものが何かを明確にする必要があるのではないかとの論点も確認した。

■ また、ステーブルコインの不正利用に使用される技術は、盗難経路を隠蔽するMixingや複数チェーンをまたぐChain-hopping等、その手口は進化している。これら技術に対しての対策事例として、ステーブルコイン発行者がLayer2ブロックチェーンも含めて自社のBlacklistの効果を及ぼす仕組みや、アドレス分析事業者による機械学習等を活用したパターン分析、ウォレット事業者によるアラート機能による予防等、新たな技術に応じた対策を施すトレンドがあることを確認した。

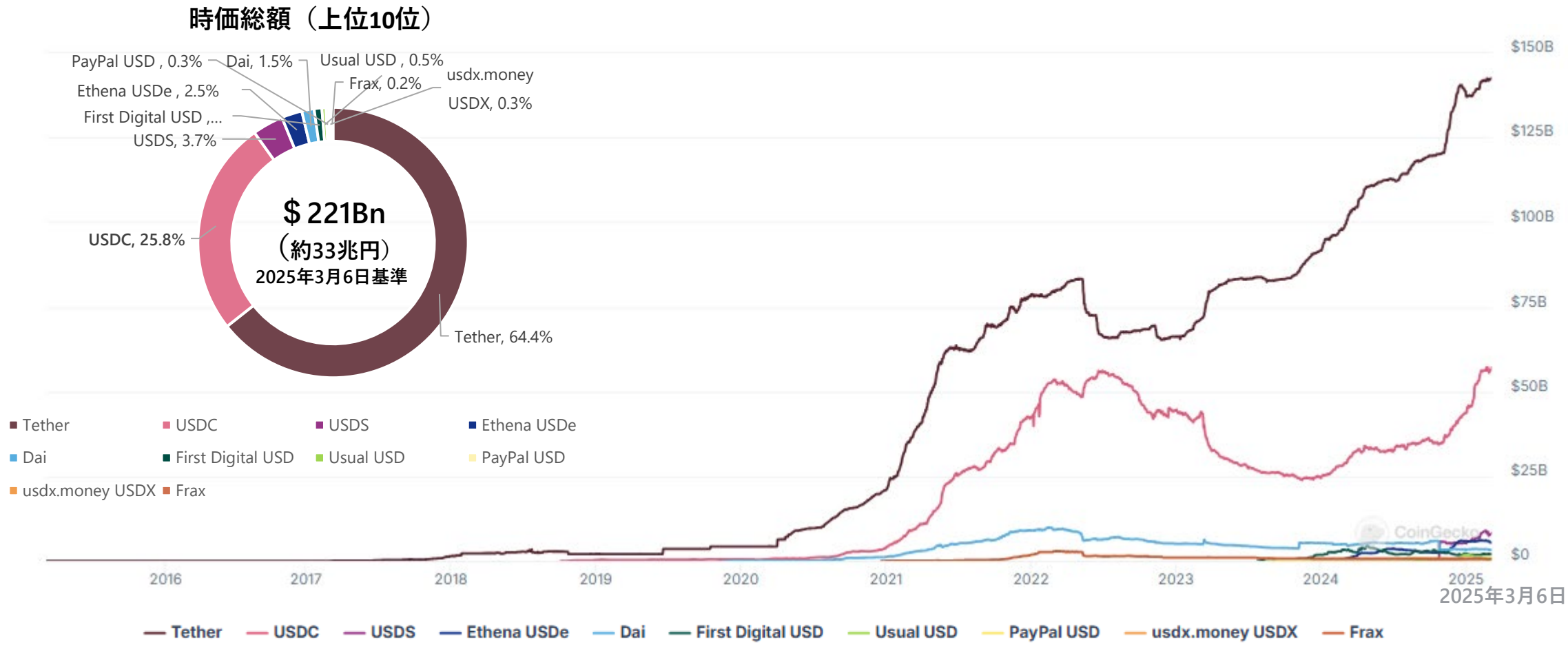
■ USDT/USDCを対象としたステーブルコイン発行者の実態把握では、資産管理やリスク管理等過去顕在化した課題は適宜アップデートされていることを確認した。ステーブルコインが健全に新たな機会を創出するためには、これら先行者の知見を活かすことが重要である。

■ また、参考として本研究期間中に発生した直近事案について、経緯・対応・追跡状況(3/7時点)を補足した。一部凍結事実等で効果があがって事が確認できる一方で、過去発覚事案の課題が関係者全体で共有される事により対策できた事象もある。今後、ステーブルコインの健全な発展に向けて、報告書で提示する「主要アクターとリスク評価」の残課題をTODOリストとし、未熟な業界を成熟させるべく、関係者が引き続き協力を推し進めていくべきと考える。

1. ステーブルコインの決済関連ユースケース及び周辺サービス調査
1.1 ステーブルコインの概況と主要ステーブルコイン

昨年12月にステーブルコイン時価総額が初めて2,000億ドルを超え、連続で増加
USDTが高いシェアを保持しています（続いてUSDC、利回り付きトークンUSDeが急上昇）

主要ステーブルコインの時価総額



【参考】：「Stablecoins by Market Capitalization」（CoinGecko）_2025年3月時点確認、「Top USD Stablecoin Coins Market Cap Chart」（CoinGecko）_2025年3月時点確認

過去の事案から、ステーブルコインは、安定通貨等による裏付けやリスク管理高度化等が重要と示唆しており、分散金融には引き続き伝統的金融の知見が求められている状況です

【参考】Terraショック

概要と教訓	【発生時期】：2022年5月7日～9日 ■ アルゴリズム型ステーブルコインの脆弱性を露呈し、市場全体に大きな影響 以下の経緯によってUSTのドルペグが崩壊 • Anchor Protocol（USTの高利回り運用プラットフォーム）の金利引き下げを受けて、大口投資家がUSTを大量に売却し、USTの価格が1ドルを割り始め、パニック売りが拡大 • USTの価格が下落すると、ペグ維持のためUSTが大量にLUNAに交換され。LUNAの供給量が急増し、価格が暴落（数日で99%以上下落） • これが「デススパイラル」を引き起こし、USTの価値も回復不可能になり、信用不安が波及し、仮想通貨市場全体に影響を与える事となった
対象	■ アルゴリズム型ステーブルコインであるTerra USD（UST）とTerraのネイティブトークンであるLUNA • 【価格安定の仕組み】：USTの価格が1ドルを上回ると、LUNAをバーンしてUSTを発行し、供給量を増やして価格調整。1ドルを下回ると、USTをバーンしてLUNAを発行し、供給量を減らして価格を調整する仕組み
被害	■ Defi Protcolに端を欲したUSTの下落が、アルゴリズムを破綻させ、価格ペッグが崩壊。以下のステークホルダーに対して連鎖的に被害を及ぼした • 【個人投資家】：USTとLUNAの保有者は99%以上の価値を失う • 【仮想通貨取引所】：Binance、FTX、Coinbase等がLUNAの上場廃止を強いられる • 【DeFi】：Terra上のプロジェクト（Anchor Protocol等）が崩壊 • 【仮想通貨市場全体】：BTCやイーサリアムも連鎖的に下落

【参考】SVB（Silicon Valley Bank）の破綻

概要と教訓	【発生時期】：2023年3月11日～13日 ■ ステーブルコインの安定のために、伝統的金融の知見を取り入れ、裏付け資産に関するリスク管理の高度化が必要である 以下の経緯によってUSDC、DAI等のドルペグが崩壊 • FRBの利上げを受けて、SVBの資産（米国債等）の価値が大きく下落。預金流出用に伴い流動性が枯渇し、2023年3月10日に破綻 • 預け入れた資金が凍結される懸念からUSDCが暴落。CEXはUSDCの大量流入を受けUSDCの交換を一時停止。DEXでの取引は急増し、USDCは一時0.87ドルまで下落、連動する形でDAIも0.89ドルまで下落 • 3月12日、米財務省・FRB・FDICがSVBの預金全額保護を発表したことで、USDCは急速に値を戻し1ドルを回復
対象	■ 法定通貨担保型のステーブルコインであるUSDCと暗号資産担保型のステーブルコインであるDAI • 【USDC】：準備金（約400億ドル）のうち、33億ドルがSVBへ預金 • 【DAI】：USDCを大量に担保に使用
被害	■ SVBに準備金を預けていたUSDCやUSDCを担保としていたDAIは破綻後、大きく値を崩し、以下のステークホルダーに対して連鎖的に被害を及ぼした • 【USDC保有投資家】：ドルペッグが外れ、一時0.87ドルまで値を下げる • 【DAI保有投資家】：USDCの下落に連動して一時0.89ドルまで値が下がる • 【暗号資産取引所】：CoinbaseとBinanceは、3月10～12日までUSDCの交換を停止

【参考】：「分散型金融システムのトラストチェーンにおける技術リスクに関する研究　研究結果報告書」（クニエ）_2025年3月時点確認

【参考】：「Potential Points of Failure for Stablecoins」（BGIN）_2025年3月時点確認

2025年3月6日時点では、USDT・USDCが突出して大きな時価総額です

主要ステーブルコイン一覧（2025.3.6時価総額）

#	コイン	発行年	発行会社	累型	時価総額	裏付資産	特徴
1	**USDT**	2014	Tether Limited /英領ヴァージン諸島	法定通貨担保型	**約142.6 B＄（≒21.1兆円）**	米ドル及び現金等物、CP等	➢ 最大のシェアを持つステーブルコイン
2	**USDC**	2018	Centre Consortium (Circle/Coinbase PJ)/米国	法定通貨担保型	**約57.1 B＄（≒8.5兆円）**	米ドル及び現金同等物	➢ USDTに次ぐ市場シェアを保持するステーブルコイン ➢ 月次で準備金の監査レポートが公開される
3	**USDS**	2024	Sky（旧MakerDAO）/米国	暗号資産担保型	約8.2 B＄（≒1.2兆円）	暗号資産、SC・米ドル及び現金同等物	➢ USDS ネットワークへの流動性提供者に、準備金から得られる収益の一部を分配することでインセンティブを与える
4	**USDE**	2024	Ethena Labs /米国	戦略担保型合成ドル	約5.4 B＄（≒8,000億円）	暗号資産、デリバティブ	➢ 暗号資産デリバティブを活用した合成ステーブルコインで法定通貨の裏付けがない ➢ スマートコントラクトで自律的に運用される
5	**DAI**	2017	MakerDAO /米国	暗号資産担保型	約3.3 B＄（≒4,900億円）	暗号資産	➢ 暗号資産（ETHやWBTC）を担保に発行される ➢ スマートコントラクトで担保資産とDAI発行を管理される
参考	**PYUSD**	2023	PayPalとPaxos Trust Company /米国	法定通貨担保型	約0.8B＄（≒1,200億円）	米ドル及び現金同等物	➢ 米国大手決済事業者が発行したステーブルコインで、PayPalのエコシステム内での利用も可能 ➢ 米国のNYDFSの規制の下で運営されている
参考	**BUSD**	2019	BinanceとPaxos Trust Company	法定通貨担保型	約0.3 B＄（≒450億円）	米ドル及び現金同等物	➢ 2022年には約3兆円を超える時価総額であったが、23年8月に「BUSD」の取扱いを段階的終了を発表以降大幅減少
参考	**EURI**	2024	Banking Circle S.A.	銀行預金型	約0.03 B＄（≒45億円）	EUR及び現金同等物	➢ EU仮想通貨規制「暗号資産市場規制（MiCA）」に準拠した初の銀行発行ステーブルコイン

【参考】：「Top Stablecoins by Market Cap」（CoinGecko），「Cryptocurrency Prices, Charts And Market Capitalizations」（CoinMarketCap）__2025年3月時点

ステーブルコインの種類では、法定通貨担保型が主流で、USDT、USDCが該当します
昨今、戦略担保型合成ドル等利回り付きステーブルコインも出て来ています

ステーブルコインの種類

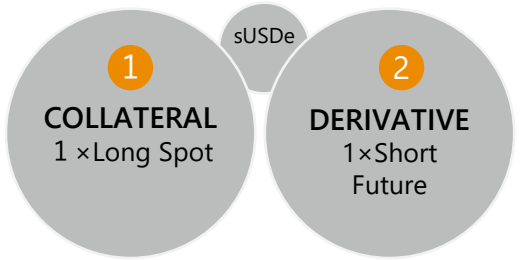
	概要	主要ステーブルコイン例
法定通貨担保型	➢ 発行されたステーブルコインの価値と同額の法定通貨、高流動性資産を担保とする ➢ 価格安定性が高く、信頼性が高いが、中央集権的である	➢ USDT（Tether） ➢ USDC（USDC） ➢ FDUSD（First Digital USD） ➢ PYUSD（Paypal USD） ➢ BUSD（Binance-Peg BUSD）
銀行発行型	➢ 銀行が発行主体となり、法定通貨の価値を裏付けとして発行されるステーブルコイン ➢ 価格安定性が高く、法定通貨と同様の信頼性があるが、中央集権的である	➢ EURI（Eurite）
暗号資産担保型	➢ 複数の暗号資産を預け入れ、その担保を超える額でコインを発行します（超過担保） ➢ 透明性は高いが、暗号資産の価格変動により、担保の価値が急落するリスク有	➢ USDS（USDS） ➢ DAI（Dai）
無担保 アルゴリズム型	➢ 特定の資産を担保せず、アルゴリズムと市場操作で価値を維持するコイン ➢ 担保不要で柔軟性は高いが、アルゴリズムの設計に依存し、信頼性が低く崩壊リスクが高い	➢ UST（Terra USD）
戦略担保型合成ドル Strategy-backed synthetic dollars	➢ 暗号資産とデリバティブを組合わせ価格変動をリスクを相殺する仕組みを内包するコイン ➢ 高利回りを狙えるも、市場の流動性やボラティリティに依存する為リスクが高い	➢ USDE（Ethena USDe）

戦略担保型合成ドルの代表USDEは、担保資産であるETHのステーキングとデリバティブを組み合わせることで、ユーザーに安定した価値と利回りを提供し、普及要因となっています

【参考】戦略担保型合成ドル（Ethena USDe）

基本情報

ステーブルコイン概要	■ USDeは、Ethena Labsにより開発された新興の合成ドルステーブルコイン
特徴	■ ETHの現物とETHのデリバティブ（先物のショートポジション）を組み合わせ、①ETHのステーキングと②デリバティブの管理によってリターンを生み出し、ユーザーに安定した価値と利回りを提供
発行プロセス	① KYC / AMLチェックを満たした後、Ethenaプロトコルによってホワイトリストに登録する ② ユーザーは、stETH （ステーキングされたETH）の担保資産を選択、受け取るUSDeの量を決定し、発行をリクエスト ③ ユーザーは、stETHをEthenaシステムに預け入れ、stETHの価値に相当するUSDeが発行 ④ 同時にstETHと同額のETH先物のショートポジションを構築 ⑤ ユーザーは、USDeをステーキングすることにより収益を獲得
普及状況	■ USDeはリリース後、わずか4ヶ月で供給量が30億ドルに到達。DeFi市場におけるステーブルコインへの需要の高まりと、USDeの高い利回りが魅力となったためと考えられる



担保資産
ETH / デリバティブ（ETH先物のショート）

利回りの提供と価値を安定させる仕組み

1 ETHのステーキング収益

【ステーキング収益】
USDe発行時に預け入れたETHをステーキング（stETH）し、ステーキング報酬を受領

2 デリバティブによるヘッジと、そこから得られるスプレッド収益

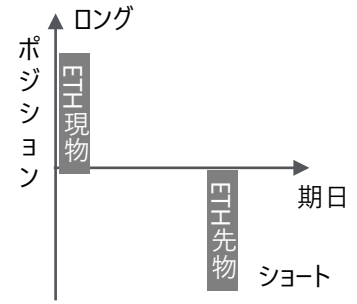
【担保価値の安定性】
ETHと同額の先物を売却することで、USDe発行時のETHの価格を安定に保つことができる（デルタニュートラル戦略）
- ETHの価格が下落した場合は、ETH先物の売却による利益でオフセットが可能

【現物・先物の価格差によるスプレッド収益】
ETH先物価格は、将来の価格変動に対するリスクプレミアムやETHに対する需給バランスから、現物価格よりも高くなりやすく、先物を売却することでスプレッド収益を受領可能

ETHの価格変動とUSDeの収益

パターン	ステーキング収益	担保価値		スプレッド収益	合計
		ETH現物	ETH先物		
ETH価格上昇	＋A%	+B%	-B%	+C%	A+C%
ETH価格下落	＋A%	−B%	+B%	+C%	A+C%

ETHの価格変動に伴う担保価値の影響はネットゼロ



ETH現物のロングと先物のショートポジションによりデルタポジションはニュートラル

【参考】：「Protocol Revenue Explanation」（Ethena Labs）_2025年2月時点

EURIは、EUの銀行（Banking Circle）が発行する最初のMiCA 規制対応のステーブルコインであり、「規制遵守による信頼性」と「銀行の強みを活かした安全性・効率性」を有します

【参考】銀行発行型 （EURI）

基本情報	
ステーブルコイン概要	■ Banking Circle が発行した最初のe-money tokenであり、EUの銀行が発行および支援する最初のMiCA規制対応のステーブルコイン ■ Banking Circleはルクセンブルクに拠点を置く決済銀行で、欧州で銀行免許を取得しています
特徴	■ 信頼性: ➢ EURI は MiCA 規制に完全に準拠しており、流通している EURI と EURI 保有者から受け取った現金の等価性を保証するためにトップレベルの監査人によって監査される ■ 安全性とセキュリティ ➢ EURI と引き換えに受け取ったすべての EURI 保有者の法定通貨資金は、Banking Circle によって破産回避構造で現金または現金同等物として分離され、保管される ■ 効率性: ➢ 法定通貨への変換には時間とコストがかかるが、e-money tokenは法定通貨ヘッジ取引にとって最もスムーズなオプションであり、他のデジタル通貨資産の迅速かつ効率的な決済に使用できる ■ 額面価格での償還: ➢ EURI の保有者はいつでも額面価格で償還する権利を有し、保有者は Banking Circle に対して、いつでも 1EURI あたり 1EUR で EURI を償還（返却）するよう要求できる
普及状況	■ 暗号通貨非接触型決済技術であるBinance Payと、Binance Payプラットフォームでの EURI決済を可能とすることに合意。日常の金融取引におけるデジタル通貨の有用性を向上を目指します

【参考】：「Banking Circle launches the first bank-backed MiCA-compliant stablecoin, EURI」（BANKING CIRCLE）_2025年2月時点確認

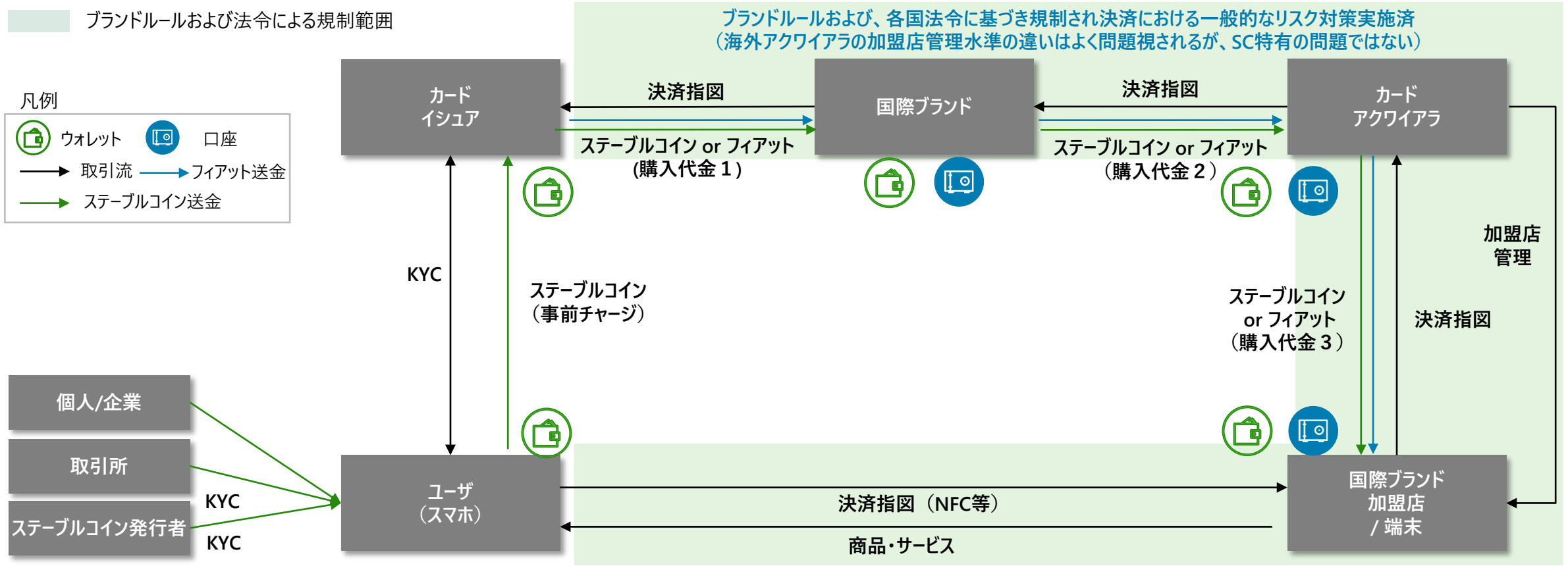
1. ステーブルコインの決済関連ユースケース及び周辺サービス調査
1.2 決済関連ユースケースの類型と具体事例

類型① クレジットカードやデビットカードとの連携

ステーブルコインユーザ、決済コスト/CCC改善を志向する加盟店が利用。決済電文授受は既存ルールに則っとっていますが、イシュアを取引所等の非伝統的プレイヤーが担っています

スキーム図

提供価値	■ カードアクワイアラ：加盟店清算にかかる時間とコスト低減 ■ カードイシュア：ファンドソースの選択肢提供、銀行口座を持たない層への金融包摂
提供プロセス	■ ユーザがカードイシュアよりSC連動型クレジットカードまたはデビットカードを発行 ■ ユーザの決済指図により、国際ブランドは、ステーブルコインを直接/フィアットに交換し加盟店へ送金

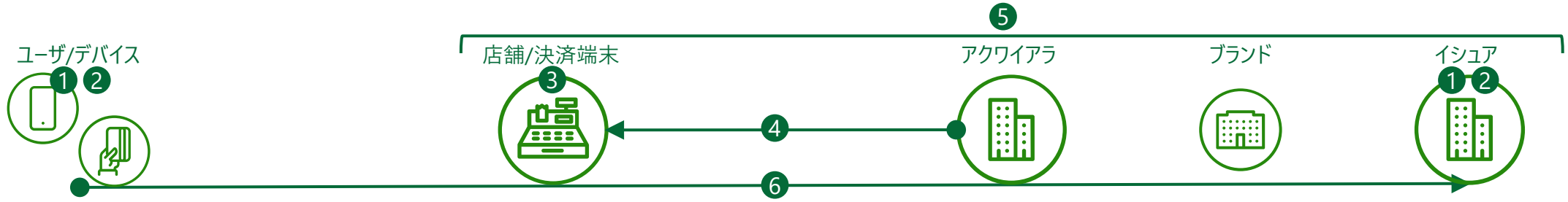


*購入代金1: 購入代金 - インターチェンジフィー + ブランドフィー(イシュア負担費目）、購入代金2: 購入代金 - インターチェンジフィー - ブランドフィー(アクワイアラ負担費目)、購入代金3: 購入代金 - 加盟店手数料

類型① クレジットカードやデビットカードとの連携

既存国際ブランド決済においては、取引を実施する際に想定される各種脅威に対して、対策が実施されています

【参考】既存国際ブランド決済における脅威と対策



1 身元確認（ハイリスクユーザの排除）

- ブランドルールによる取決はなく、法令に基づいて実施
- 日本においては犯罪収益移転防止法に基づき、クレジット・デビットカードを利用開始時にはKYCが実施される。（翻ってブランドプリペイドでは実施されないケース有）
- なお、犯罪収益移転防止に規定されている各種手法についても手法毎にセキュリティ強度は異なる

2 当人認証（なりすまし決済の防止）

- 対面決済
  - ✓ EMVの仕様に基づいて下記実施
    カード所持＋PIN認証 or CDCVM or 署名等
    ※国内では署名等のPINバイパスは今後禁止される
- 非対面決済
  - ✓ EMVの仕様に基づいて下記実施が推奨
    券面認証＋EMV3 - Dセキュア等

3 決済端末の真正性（端末の改造防止等）

- ブランドルール/クレジットセキュリティガイドラインの規定に従い決済端末はEMVおよび/PCIPTS認証（certification）等を受けている
  - ✓ EMV認証：L1（物理的、電気的な機能性）、L2（端末のソフトウェア*カーネル）を検証
  - ✓ PCIPTS認証：端末開封時に内部保存されている暗号鍵や暗証番号等を、瞬時に消去すること等

4 加盟店管理（悪質加盟店の排除）

- ブランドルール
  - ✓ チャージバック等のルールを規定
- 割賦販売法
  - ✓ クレジットカード等取扱契約締結事業者の登録制度が存在しており、加盟店調査等が義務
    加盟店情報交換センターへの悪質加盟店の情報共有も実施されている

5 カード番号の適切管理（カード番号流出防止）

- ブランドルールおよび割賦販売法で下記規制あり
  - ✓ アクワイアラ/イシュア/決済代行/加盟店等、カード番号を保持もしくは通過させる事業者についてはPCIDSSに準拠することが求められている。PCIDSSに準拠すると結果的にカード番号の扱いに限らず高度なセキュリティ対策を実施することになる*詳細次頁

6 取引時の各種認証（電文改ざん防止等）

- 取引時にはEMV仕様に基づいて下記実施
  - ✓ 当人認証（❷で記載の通り）
  - ✓ カードの真正性検証
  - ✓ 取引認証（取引電文の真正性検証）
    - 共通鍵暗号を用いたメッセージ認証符号の検証により電文の改ざんがないことを確認

【参考】：日本クレジット協会「クレジットセキュリティガイドライン」、経済産業省「割賦販売法」、EMVCo「EMV® Specifications」

年々高度化する不正手口に対して、セキュリティ基準は継続的に見直されてきました。ステーブルコインにおいてもエコシステム全体でセキュリティ確保が肝要です

【参考】既存国際ブランド決済における不正被害と対策の歴史

代表的な不正被害

偽造カード被害

- 2002年被害額165億円をピークに減少
  - 不正手口
    - スキミング
    - 決済端末の改造（スキミング用の基板と送信機の挿入）
- 被害削減のためには特定の国だけでなくglobalレベルでのIC化対応が必要

番号盗用被害

- 2024年被害額513.5億円*過去最高
  - 不正手口
    - クレジットマスター攻撃
    - 事業者からの漏洩
    - フィッシング
    - リアルタイムフィッシング
- 不正手口は年々高度化しており、フィッシング時に券面情報と静的PWをセットでの窃取、SIMスワッピングによるSMS認証情報の窃取等が発生しているといわれている

ブランド各社による国際的な枠組

EMVCo：1999年設立、American Express、Discover、JCB、Mastercard、UnionPay、Visaが共同運営

- 店舗対面決済
  - EMV仕様：1996年に発表された、ICカードと端末のハード・ソフトに関する仕様規定、定期的にバージョン更新されている。デバイスの認証制度も存在
- 非対面決済
  - 3-D セキュア1.0：1999年に発表、静的PW認証
  - EMV 3-D セキュア：2016年に発表、リスクベース認証であり動的PW認証や生体認証が推奨。実務的にはSMS認証、アプリベースのワンタイムPW認証、パスキー等が実施されている

PCISSC：Visa、Mastercard、JCB、American Express、Discover）が2006年に共同設立

- PCI DSS：カード情報取扱に際するデータセキュリティ基準
  - I. 安全なネットワークのシステムの構築と維持
  - II. アカウントデータの保護
  - III. 脆弱性管理プログラムの維持
  - IV. 強力なアクセス制御の実施
  - V. ネットワークの定期的な監視とテスト
  - VI. 情報セキュリティ・ポリシーの維持
- PCI PTS：PIN 入力装置に関わるセキュリティ基準
- 他にもユースケースに応じてPCI P2PEやPCI MPoC等各種基準が存在する

日本：割賦販売法の変遷

2009年/2010年施行

- アクワイアラ・イシュアに対してクレジットカード等の適切な管理義務化（PCIDSS準拠）

2018年施行

- アクワイアラ/決済代行等に対してクレジットカード番号等取扱契約締結事業者の登録制度を新設、加盟店調査等義務が課された
- 加盟店のクレジットカード等の適切な管理義務化（PCIDSS準拠もしくは非保持化）

2020年

- カードおよび加盟店決済端末のIC対応完了
  【参考】2015年からブランドルールとしてライアビリティシフト（債務責任の転嫁）が開始され、ビジネス観点でも対応動機が高まった

2025年目標

- ECサイトのEMV 3 - Dセキュア対応完了目標
  【参考】EUでは2019年にPSD2 SCA（強力な本人認証）が義務化されており、対応策として3Dセキュアが進展

【参考】：日本クレジット協会「クレジットセキュリティガイドライン」「クレジットカード不正利用被害の発生状況」、経済産業省「割賦販売法」

類型① クレジットカードやデビットカードとの連携

Lemon CardはVisaと協力し、Visa加盟店で暗号資産決済が可能なプリペイドカードを提供し、Fiat24は、SafePalと連携して暗号資産決済が可能なVisaカードを提供しています

（個別事例）Lemon

基本情報			
対象ステーブルコイン	USDT/USDC/DAI	商用化時期（SC決済）	2021年以降
運営主体	Lemon（アルゼンチン）	展開地域	アルゼンチン

サービス概要	
サービス内容	➢ LemonはVisaと協力して、Visa加盟店で暗号資産決済が可能なVisa Lemon Cardを提供 ➢ Lemonはユーザに対して暗号資産決済が可能なカードを提供し、VISAはブランド決済ネットワークにUSDC・USDT清算が可能な仕組みを統合することでUSDT・USDCに加え、BTC・ETH・DAI、アルゼンチンペソで支払いが可能 ➢ 本カードを利用した場合、**最大2%のキャッシュバックをBTCで受領可能**
規模	➢ 100万枚超のカードを発行し、300万超のアプリユーザーを擁す（2024年1月時点）
備考	➢ カードを申請する為の要件 • 18歳以上で、標準的な本人確認プロセス(身分証明書、自撮り写真、電子メール)の完了 • アルゼンチンの居住者（居住者であっても、米国市民は受け入れない） • ユーザーのCVU（MercadoPago等）、CBU(ユーザーの銀行口座)の提示

【参考】：「Get Your Crypto Card: Earn Bitcoin for Using It」（Lemon）_2025年3月時点確認

（個別事例）Fiat24

基本情報			
対象ステーブルコイン	USDC	商用化時期（SC決済）	2024年
運営主体	Fiat24（スイス）	展開地域	ヨーロッパ30カ国

サービス概要	
サービス内容	➢ Fiat24はSafePalと提携して、Visa加盟店で暗号資産決済が可能なVisaカードを提供 ➢ Fiat24はユーザに対して暗号資産決済が可能なカードを提供し、VISAはブランド決済ネットワークにUSDC清算が可能な仕組みを統合 ➢ カードの発行手数料や月額料金等は存在せず、月の利用制限は10,000ユーロに設定されている
規模	➢ 世界中の4,000万店以上の加盟店で利用可能（2025年1月時点）
備考	➢ スイスの銀行法やマネーロンダリング規制や制裁規制等を遵守している ➢ カード発行対象は、EEA加盟国またはスイスに居住している18歳以上であり、パスポートまたは生体認証IDを活用して本人確認を行う ➢ また、アカウント登録時に対象国に居住しているか確認を行うために、位置情報の提供が求められる

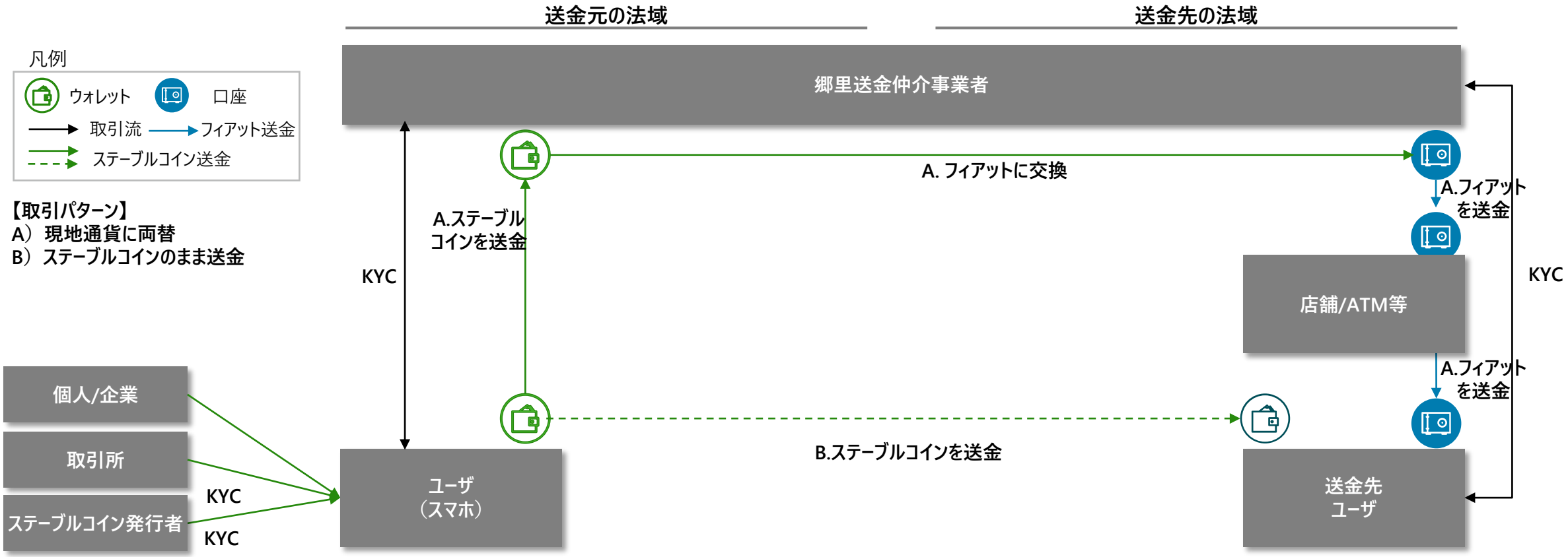
出所：「Stay tuned of the latest updates and announcements of SafePal」（SafePal）_2025年3月時点確認

類型② 郷里送金

銀行口座を持たない/十分に利用できない層に対する送金手段として活用されており、送金仲介者は各国規制に遵守する一方、国・地域によっては強度に差異が想定されます

スキーム図

提供価値	■ ユーザ①：クロスボーダー送金にかかる時間の短縮、コスト低減 ■ ユーザ②：銀行口座を持たない/十分に利用できない層への金融包摂
提供プロセス	■ ユーザからのSC決済の指図により、郷里送金NW事業は、SCをフィアットに交換したうえで送金先ユーザへ送金する ■ もしくは、ユーザが送金先ユーザへ直接SCを送金する



類型② 郷里送金

Yellow Cardは自国通貨が不安定、または金融サービスを十分に受けられないアフリカの人々に対し、ステーブルコインでの送金サービスを提供、Coins.phも同様のサービスを提供しています

（個別事例） Yellow Card

基本情報			
対象ステーブルコイン	USDT/USDC/PYUSD	商用化時期（SC決済）	2024年
運営主体	Yello Card（南アフリカ）	展開地域	アフリカ20カ国

サービス概要	
サービス内容	➢ Yello Card は、Yellow Payを通じて、即時のステーブルコインの無料送金サービスを提供 ➢ 優れたUIを通じて簡単・迅速な送金を実現を目指しており、送金・入金の手数料は無料、一方で、出金は100NGNの費用が発生（ナイジェリア） ➢ 知人紹介やアンバサダープログラムやバグバウンティ・プログラム等を通じたインセンティブの提供を実施。尚、知人紹介を行うと、紹介した知人のトランザクションフィーの20%を受け取ることが可能
規模	➢ アフリカ20カ国でサービスを展開しており、2023年には170万人の顧客を獲得
備考	➢ KYCでは、本人情報の登録、本人確認資料・自撮り写真のアップロードを行う必要有

【参考】：「Buy and Sell BTC, ETH, USDT & More in Africa」（Yellow Card）_2025年3月時点

（個別事例） Coins.ph

基本情報			
対象ステーブルコイン	USDC	商用化時期（SC決済）	2023年
運営主体	Coins.ph（フィリピン）	展開地域	フィリピン

サービス概要	
サービス内容	➢ Coins.phは、フィリピンユーザを対象に、USDCを用いた国際送金ソリューションを提供しており、Coins.phのアプリを通じて100以上の銀行や質店で出金できる ➢ Coins.phは、ユーザから受け取ったUSDC/USDTをフィアットへ交換し、送金先ユーザの銀行口座等へ送金を行う ➢ バグバウンティ・プログラムにて、脆弱性の報告等を通じて、10～5,000ドルの報酬を提供
規模	➢ 登録ユーザ1,600万人以上（2025年1月時点）
備考	➢ BSPより、Virtual Currency and Electronic Money Issuer licensesを取得している ➢ アカウント作成では、18歳以上を対象とし、自撮り写真、及びパスポートや運転免許証等の本人確認資料を基にKYCを行う

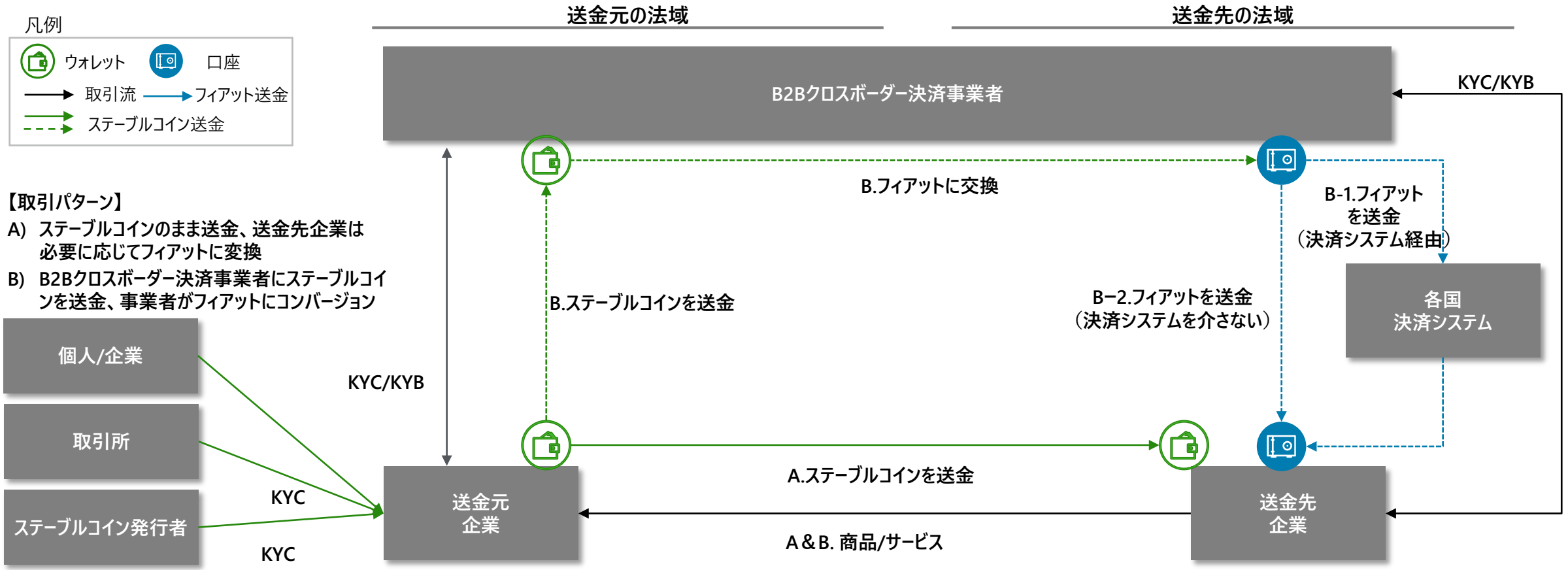
【参考】：「Trusted Crypto Wallet & Exchange | Buy Bitcoin in the Philippines」（Coins.ph）_2025年3月時点確認

類型③ クロスボーダーB2B取引

迅速かつ低コストな決済手段として活用が浸透しています。一方で、制裁や資本規制回避としての取引も見られ、不正対策案（対象アドレスの凍結等）の構築が求められています

スキーム図

提供価値	■ 企業：クロスボーダー送金にかかる時間の短縮、コスト低減
提供プロセス	■ 商品・サービス購入時に企業からのSC決済の指図により、B2Bクロスボーダー決済事業者は、SCをフィアットに交換したうえで送金先ユーザへ送金する ■ もしくは、企業が送金先企業へ直接SCを送金し決済する



類型③ クロスボーダーB2B取引

Circle（USDC）がPIXと連携することで、即時且つ安価なクロスボーダー取引を実現しています

（個別事例）PIX

基本情報			
対象ステーブルコイン	USDC	商用化時期（SC決済）	2024年
運営主体	Circle（米国）/ PIX（ブラジル）	展開地域	ブラジル

サービス概要	
サービス内容	➢ ブラジルのリアルタイム決済システムであるPIXは、Circleとの提携により、送金先企業によるUSDCとフィアットの即時交換が可能となり、即時且つ安価なクロスボーダー取引を実現 ➢ フィアットの場合、Pixの支払いは平均3秒で決済。個人向けの無料化を義務付け。企業/加盟店の支払い取引のコストは取引額の0.33% ➢ （参考）Circleは、メキシコの国家リアルタイム決済システムである SPEI を介しても現地の銀行振込をサポート
規模	➢ PIXはリリースからから2年半で、1億4,000万人以上の個人と1,300万の企業が利用（2023年5月時点）
備考	➢ システムの参加者は、BCB（ブラジル中央銀行）の規制要件の対象 • Risk-based supervision、流動性リスク管理、サイバーセキュリティ、データ使用、およびAML / CFT手順に関する基本規制の対象 ➢ KYCルールの遵守の為、参加者は、疑わしいトランザクションにフラグを立て、ユーザーのリスクプロファイルに従ってトランザクション制限を割り当て実施

【参考】：「USDC now available in Brazil and Mexico」（Circle）_2025年3月時点確認
「Pix: Brazil's Successful Instant Payment System in: IMF Staff Country Reports Volume 2023 Issue 289 (2023)」（IMF eLIBRARY）_2025年3月時点確認

（個別事例）BVNK

基本情報			
対象ステーブルコイン	USDT/USDC/ PYUSD	商用化時期（SC決済）	2024年
運営主体	英国	展開地域	英国/欧州/米国中心

サービス概要	
サービス内容	➢ BVNKは、企業がステーブルコインを用いて、送金、受領、法定通貨との交換を迅速且つ安全に行えるよう、決済プラットフォームを提供 ➢ ステーブルコインをフィアットに変換して送金先企業に送付することも可能であり、主にEUR, GBP, USDに対応 ➢ AMLとKYCに対してはツールと独自の機械学習モデルを組み合わせて展開し、効果的な犯罪検出と防止を行っており、金融犯罪リスクの軽減を支援
規模	➢ BVNKは、年間 120 億ドル以上の決済を処理しており、前年比 200% の成長を達成（2025年2月時点）
備考	➢ BVNK は英国およびヨーロッパで EMI として規制されており、ヨーロッパでは複数の VASP 登録を保持 ➢ 米国では、デラウェア州に設立された当社の法人は、米国のいくつかの州で送金業者ライセンスを保持し、FinCEN（米国財務省金融犯罪取締ネットワーク）に登録

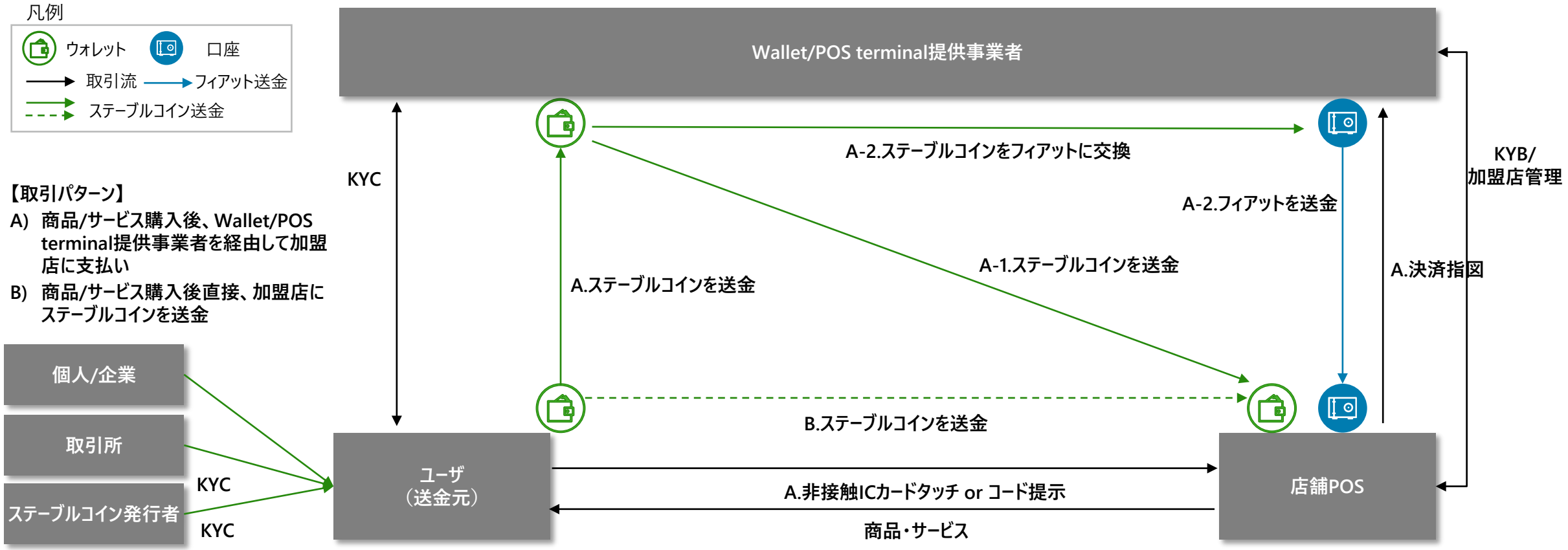
【参考】：「Send and receive PayPal USD payments with BVNK」「Compliance」「Trust Center」（BVNK）_2025年3月時点

類型④ 店舗端末（POSシステム）

ステーブルコインを趣向するユーザ/加盟店によって日常の店頭決済で利用されています
独自レールの決済システムのため、認証含全般的に事業者固有の対応が可能なスキームです

スキーム図（国際ブランド以外の独自レールのケース）

提供価値	■ 店舗：既存決済レールのセツルメント時間や各種コスト低減 ■ ユーザ：ファンドソースの選択肢提供、銀行口座を作れない層への金融包摂
提供プロセス	■ 商品・サービス購入後、ユーザからの決済指図により、Wallet/POS terminal提供事業者のアドレスへ事前にSCを送金、その後、店舗へSCを送金する ■ もしくは、ユーザから、ユーザが店舗へ直接SCを送金し決済する



類型④ 店舗端末（POSシステム）

ステーブルコイン（他暗号資産含）による決済電文の授受をサポートする独自レールのPOS端末やカードデバイスを提供し、店頭決済におけるステーブルコイン支払を実現しています

（個別事例）PundiX

基本情報			
対象ステーブルコイン	USDT/DAI	商用化時期（SC決済）	2022年
運営主体	PundiX (シンガポール)	展開地域	30か国以上

サービス概要	
サービス内容	➢ 店舗に設置されたXPOSを通じてUSDTやDAIによる購入代金の支払が可能（BTC等の暗号資産も対応USDTやDAIを店舗のXPOSを介して購入できる） ➢ ユーザはMetaMaskやf(x)wallet等のウォレットを利用可能な他、物理カードを利用する場合はp(x)Cardを購入して利用可能 ➢ 決済端末ベンダーVerifone/Ingenico/PAX社の決済端末にXPOSをインストールして店舗に販売、店舗はXPOSにf(x)walletを紐付
規模	➢ XPOSとp(X)Cardは日本を含む世界30か国以上で販売 日本においても利用可能な店舗のリストが公表されている
備考	➢ 店舗POSはEMV認定端末を販売している端末ベンダーが製造しているものの、搭載されるアプリケーションはPundi X社が独自に開発

【参考】：「Pundi X Official 、Function X」（Function X）_2025年3月時点

（個別事例）dtcpay

基本情報			
対象ステーブルコイン	USDT/USDC/WUDS	商用化時期（SC決済）	2024年
運営主体	dtcpay （シンガポール）	展開地域	シンガポール

サービス概要	
サービス内容	➢ dtcpayは、クレジットカード等の従来の決済手段に加え、ステーブルコインでの支払を受け入れることができるPOSシステムであるPOS+を提供 ➢ POS+を導入した加盟店では、ユーザーはステーブルコイン決済が利用可能 ➢ 決済手段としてステーブルコインが選択されると、従来の決済手段と比べ、決済手数料を安価に抑えることができる
規模	➢ 導入企業数は不明だが、小売や旅行業界等の企業で導入が進む
備考	➢ ステーブルコイン、電子マネー、クレジットカード決済に対応しており、取引履歴も管理できる ➢ PCI DSS の要件に準拠しており、カード データの暗号化処理と保存を行っている

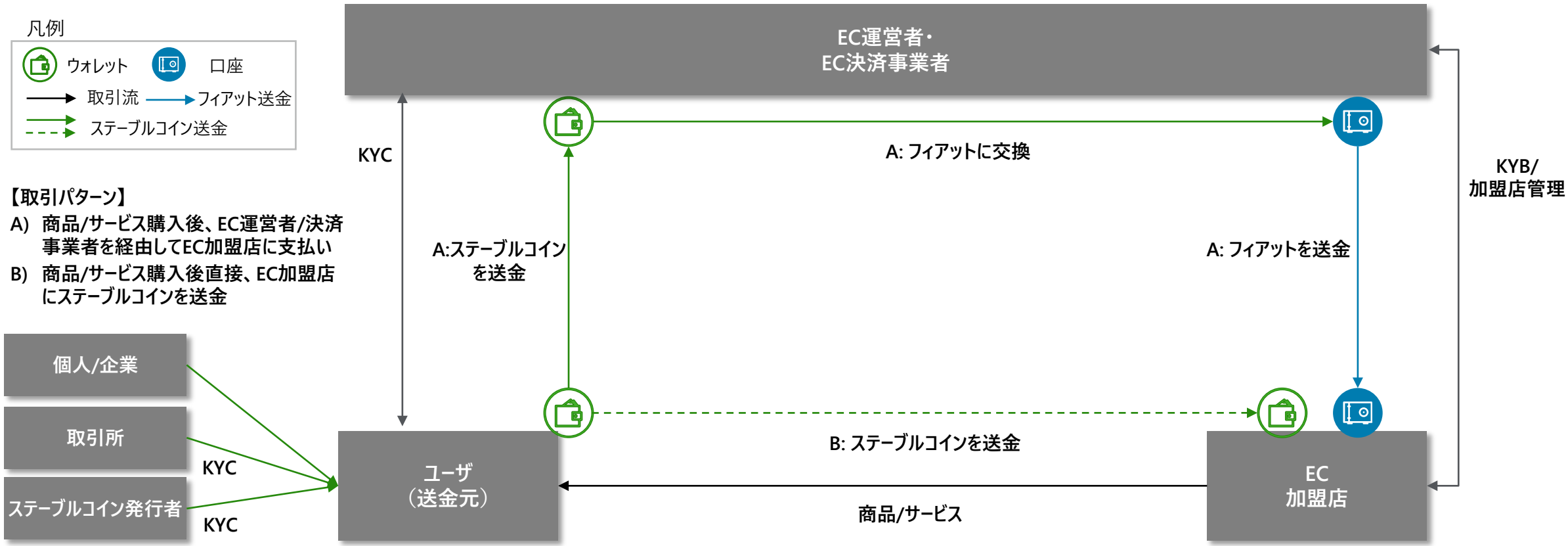
【参考】：「Point of Sale Solutions」（dtcpay）_2025年3月時点

類型⑤ EC決済

ECで商品を購入時に、決済手段としてステーブルコインを選択できる取り組みが増加中。不正防止の為、EC運営者・決済代行業者はユーザーのKYC等リスク対策案の構築が重要です

スキーム図

提供価値	■ 店舗：既存決済レールのセツルメント時間や各種コスト低減 ■ ユーザ：ファンドソースの選択肢提供、銀行口座を作れない人への金融包摂
提供プロセス	■ 商品・サービス購入時に、決済事業者へステーブルコインを送金。決済事業者の決済の指図により、EC加盟店へステーブルコインを送金 ■ もしくは、EC加盟店の口座に対してフィアットで送金し決済する



StripeはECで商品を購入時に、決済手段としてUSDCを選択可能としました

（個別事例）Stripe

基本情報			
対象ステーブルコイン	USDC	商用化時期（SC決済）	2024年
運営主体	Stripe	展開地域	米国

サービス概要	
サービス内容	➢ Stripe は米国企業向けに暗号資産決済を再度有効化し、Ethereum、Solana、Polygon 経由で USDC を受け付けられるサービスを提供 ➢ EC等での商品購入時にウォレットに連携し、ウォレットから USDC を送金する取引に署名して、支払いを確定。具体的には「Pay with Crypto」を設定すると、決済手段として 仮想通貨 を選択するためのオプションが決済フォームに表示される ➢ 取引限度額は、取引あたり 10,000 USDおよび月あたり100,000USD、決済手数料は、取引金額の 1.5%
規模	➢ 2025年1月現在、米国の限られた企業のみ利用可能であるが、Stripe は現在、46 カ国でサポートされ、対応先は今後増加予定
備考	➢ Stripe を利用している全事業者が 2023 年に処理した決済総額は 1 兆ドルの大台に達し、前年比 25% の増加

【参考】：「https://docs.stripe.com/crypto/pay-with-crypto」、「https://stripe.com/jp/global」
「Stripe_2023_annual_letter_JA.pdf」（Stripe）_2025年3月時点

（個別事例）Grab

基本情報			
対象ステーブルコイン	USDT/USDC/XSGD	商用化時期（SC決済）	2024年
運営主体	Grab（シンガポール）	展開地域	シンガポール

サービス概要	
サービス内容	➢ Grabは、オンラインショッピングやタクシー代の支払等、GrabサービスやEC・店舗決済で利用できるGrabPayユーザーに対して、ステーブルコイン決済サービスを提供 ➢ 現在はシンガポールのみの展開だが、需要に応じて今後拡大予定。手数料なしで即座に振込可能であり、取引履歴の確認も可能
規模	➢ Grabのユーザ数は1.8億人以上（2023年時点） ➢ Grab Payのユーザ数は1億人以上（2023年時点）
備考	➢ PCI DSSに準拠しており、高いセキュリティ水準を誇る ➢ GrabPayを利用した支払では、最大0.5%のポイントバック（GrabRewardsポイント）を受け取ることができ、定期的にGrabPayが利用される限りポイントの有効期限がない

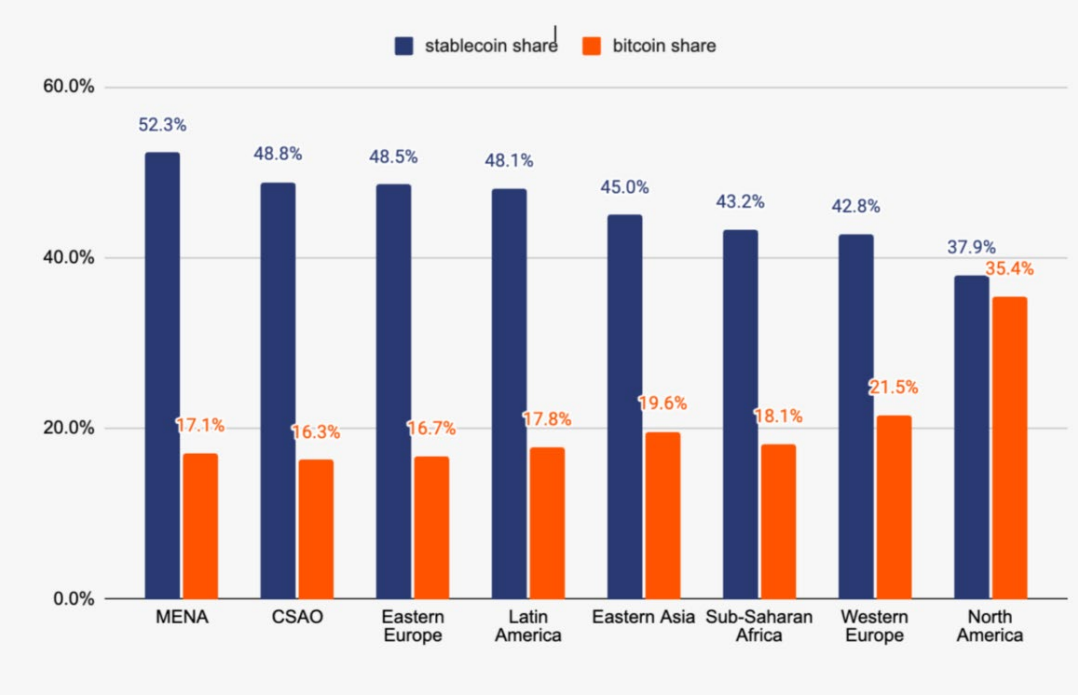
【参考】：「GrabPay - Mobile Wallet Payment Solution | Grab PH」（Grab）_2025年3月時点

1. ステーブルコインの決済関連ユースケース及び周辺サービス調査
1.3 普及を促進する要因となる技術やサービス

インフレ率が高く、フィアットの価格が不安定な国や銀行口座保有率が低い国ではステーブルコインの普及が進んでいるとされています

ステーブルコインの普及状況

暗号資産に占めるステーブルコインのシェア※1（地域別）



※1地域別の統計値は、トラフィックデータを活用して取引所にアクセスしている国に応じて案分して算出した数値

コイン別のシェアとインフレ/銀行口座保有率※1･4

		BTC	ETH	アルトコイン	ステーブルコイン	インフレ率※2	銀行口座保有率※3
North America	カナダ	23.7%	8.4%	26.8%	41.1%	3.35%	—
	米国	37.0%	6.8%	18.7%	37.5%	3.97%	95.0%
	バルミューダ	11.9%	4.1%	38.8%	45.2%	—	—
Latin America	アルゼンチン	14.7%	10.0%	13.4%	61.8%	69.98%	66.3%
	ブラジル	14.2%	12.1%	13.8%	59.8%	5.82%	83.6%
	コロンビア	13.7%	8.8%	11.5%	66.0%	6.29%	55.9%
	メキシコ	19.3%	16.6%	17.0%	47.2%	5.23%	49.1%
	ベネズエラ	12.2%	15.9%	15.4%	56.4%	4,874.00%	—
MENA	イスラエル	19.9%	7.3%	32.3%	40.6%	2.07%	—
	サウジアラビア	16.4%	7.8%	29.7%	46.1%	1.84%	—
	トルコ	15.6%	8.5%	20.7%	55.2%	34.65%	73.4%
	UAE	16.5%	7.8%	24.4%	51.3%	0.47%	—
世界全体		**22.3%**	**8.3%**	**24.6%**	**44.7%**	**5.34%**	**74.0%**

※2　消費者物価上昇率の過去５年平均（2019～23年）
※3　2021年時点の銀行口座保有率
※4　出所よりデータが取得可能な国のデータを整理

■ 自国のフィアットが不安定/ボラティリティの高い国が多いMENA・CSAO・東欧・ラテンアメリカ等の地域では、信頼性の高い決済・価値保存の手段としてステーブルコインが利用される割合が高い

■ ステーブルコインの保有割合とインフレ率には一定の順相関が見られ、インフレ率の高い（アルゼンチン、ベネズエラ）においては、ステーブルコインの保有割合は多い

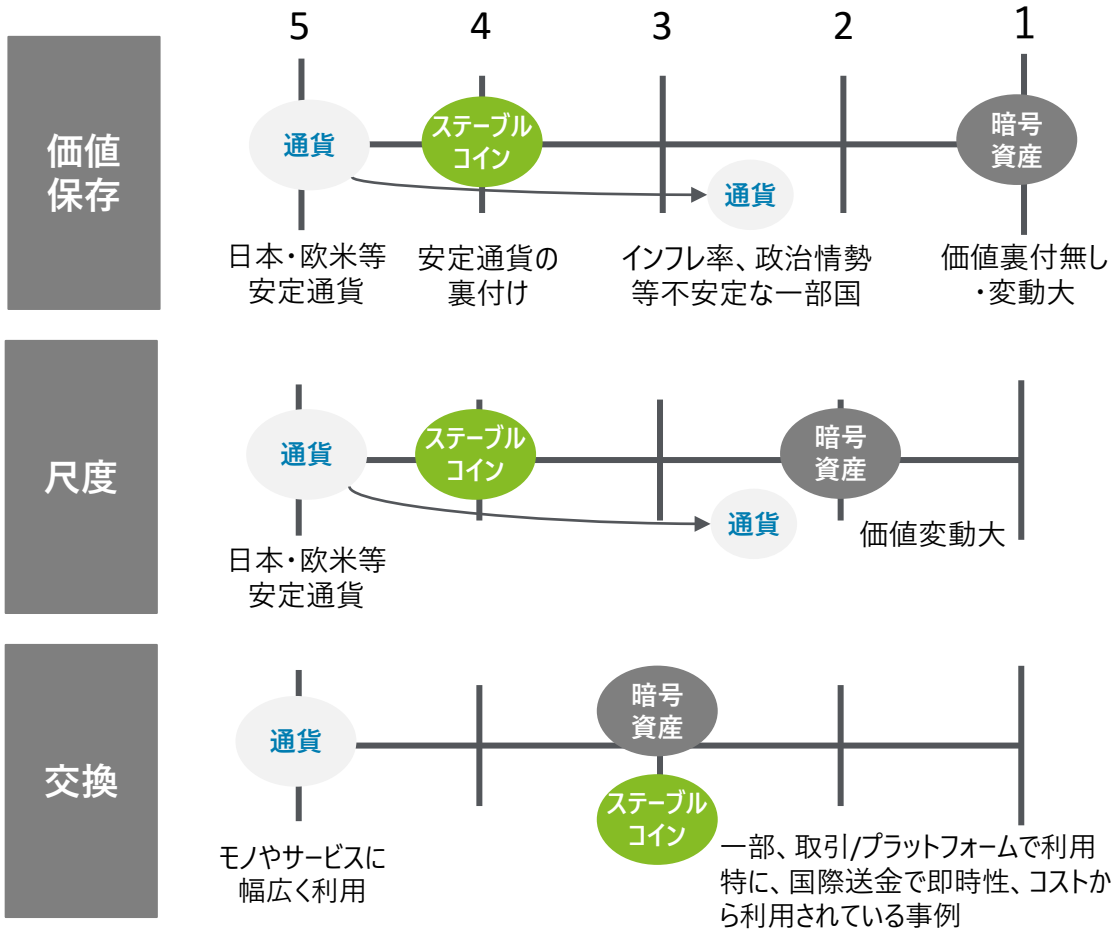
【参考】：「The 2024 Geography of Crypto Report」（chainalysis）_2025年3月時点

【参考】：「https://www.jetro.go.jp/biz/areareports/2022/82df5175afac50a6.html」（JETRO 銀行口座保有率）
「https://www.globalnote.jp/」（Globalnote, 消費者物価上昇率）_2025年3月時点

一部の国では、ステーブルコインが自国通貨よりも通貨の基本機能（「価値の保存」、「尺度」、「交換」）を充足しており、普及要因となっています。暗号資産は価値変動に課題があります

ステーブルコインの普及の要因

通貨の基本機能に対する、通貨・ステーブルコイン・暗号資産の充足度合い



ステーブルコインの普及要因

- 一部国における自国通貨の代替として価値保存
- 既存の決済ネットワークとの統合
- 通貨よりも優れた送金速度と手数料

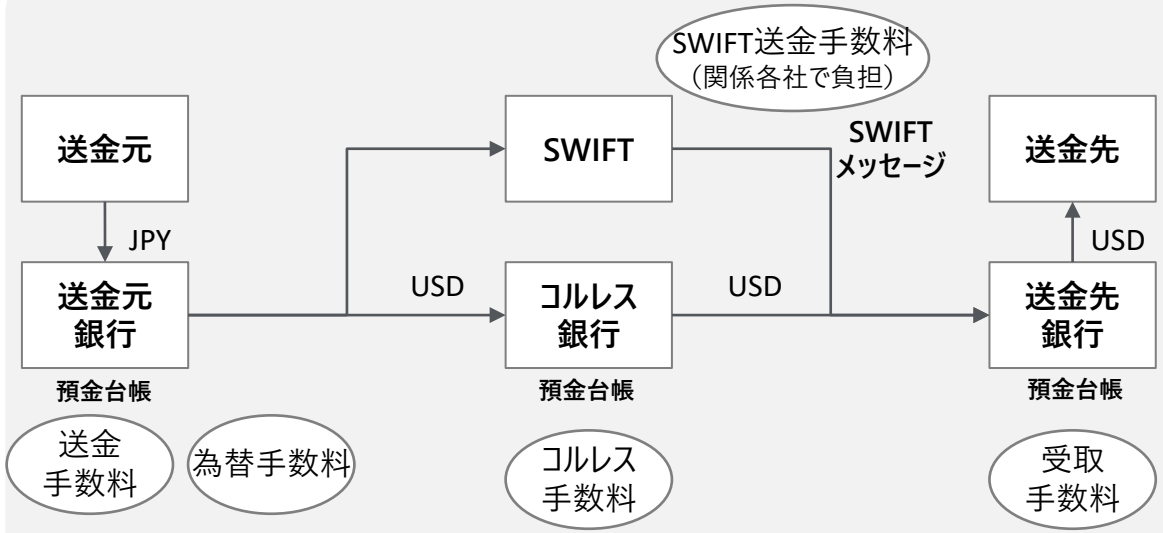
伝統的な決済では金融機関等の多くの仲介者が存在するが故にコストがかかるが、ブロックチェーンを活用したステーブルコイン決済ではP2P取引が行えるため、コストが削減できます

【参考】普及要因となる技術（クロスボーダー決済/送金）

伝統的な決済プロセス

■ 仲介する機関やシステムが多く存在するため、送金に時間やコストがかかる

国際送金

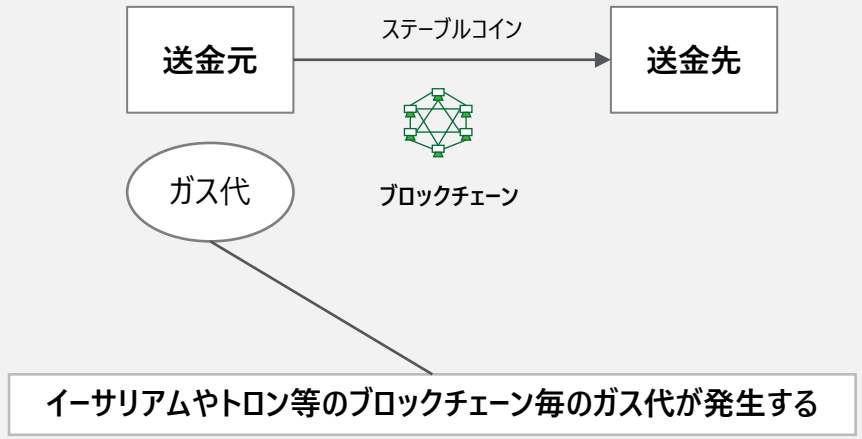


- 海外送金の場合、送金手数料とコルレス手数料と受取手数料の合計で約1万円、送金額と通貨別の手数料率に応じた為替手数料がコストとして発生する
- また、一般的には海外送金には数日～1週間ほどかかる

ステーブルコインの決済プロセス

■ ブロックチェーン上でP2P取引が実現するため、送金に要する時間が短く、コストが少ない

ステーブルコイン決済



- 海外送金であってもガス代しか主なコストは発生せず、且つ、ウォレットから直接送金されるため、送金が短時間で完了する

2. 主要なステーブルコインの利用状況・不正利用事例の調査

2.1 不正の定義、不正利用の類型および概況

「不正利用」とは正当な利用者の誰にとっても不当な結果をもたらす行為と、制裁対象主体がシステムを利用する行為と定義します

当報告書における不正利用の定義

- 「不正利用」とは、1.**システムが犯罪等に利用されることにより、社会通念上正当な利用者の誰にとっても不当な結果をもたらす行為**、および 2.**特定の国の立場から不当と判定され、制裁対象とされた国や個人、組織がシステムを利用**することをいう
- 2.における「特定の国」の概念は、その国にとっては不正利用といえるとしても、他の国からは不正利用とは言えない相対的なものとなる点に留意するべき

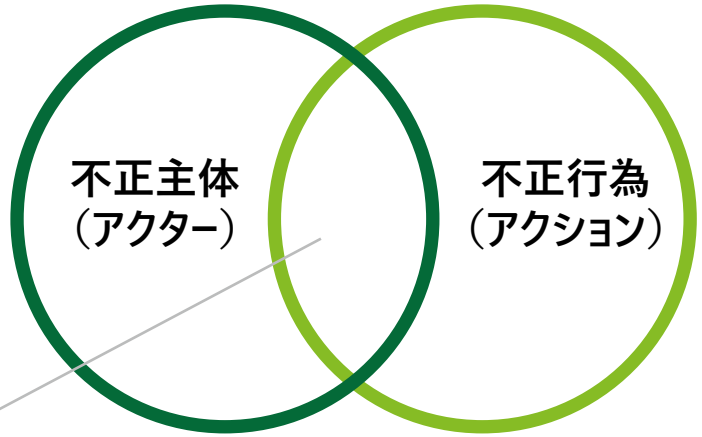
本報告書が注力する領域

- 上記で定義する不正利用には、①詐欺・攻撃の事件等があった結果としての資金流入と、②その後の洗浄・換金という捉え方ができるところ、本報告書では②に注力して分析を加えている
- すなわち、暗号資産交換業者へのハッキング攻撃に伴う大規模流出事件（①）そのものを扱うものではない点に留意されたい

不正利用の基本的な分類

- 不正利用は様々な類型化が試みられているが、**どのように不正を識別するのか**という観点から、以下の 2 つのグループに分類できると考えられる
  - ✓ **不正主体により識別するグループ**
  - ✓ **不正行為により識別するグループ**

  不正行為を行った主体が、その後不正主体として識別される等、**両グループは重なる部分はありうる**

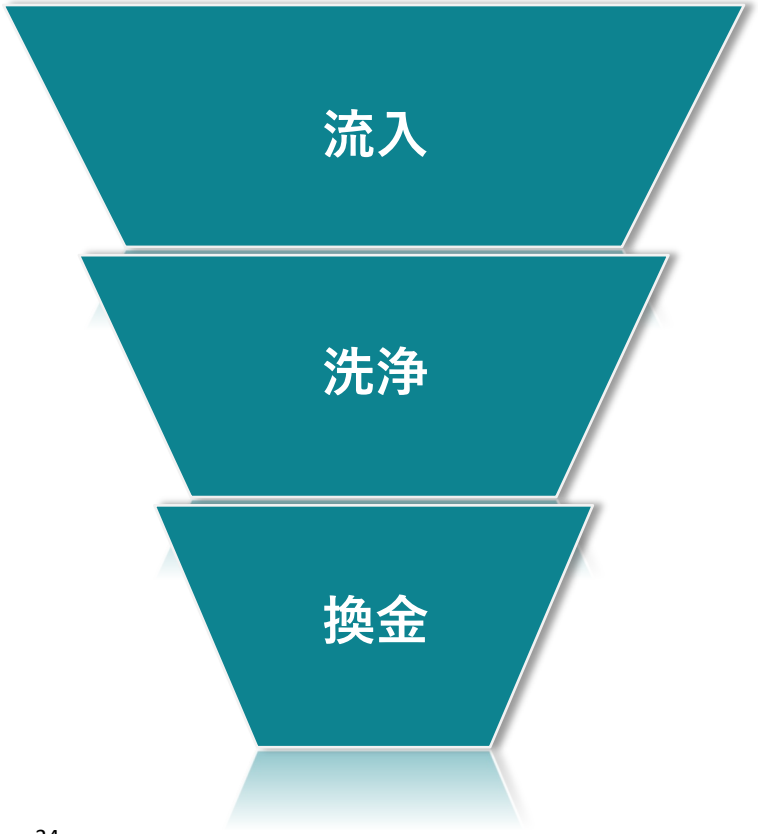


例）ハッキング攻撃という行為により識別されたアドレスが、特定の犯罪組織として識別されその後そのアドレスへの送付量が集計されるようなケース

ブロックチェーンを使った不正行為は、流入、洗浄、換金のステップごとに整理することができ、各段階における不正類型と対策を分析する必要があります

不正利用の段階別分類

前提事項	ステーブルコインは、様々な暗号資産との間で活発に交換されている。**暗号資産は互換性が高いという特徴を有しているため、**仮にステーブルコインの発行・流通において不正利用を抑止するための措置が整備されたとしても、暗号資産との交換を通じてこれらが潜脱される可能性がある



	概要
Step1	■ 盗難、詐欺等の犯罪が発生し、ブロックチェーン上の特定のアドレスにトークンを集める行為 • WebサイトやSNS等、オフチェーンツールを使った**トークンの盗取**や**ランサムウェア等による犯罪**、**ダークウェブにおける取引の決済**として使用や、**脱税の隠匿等**の行為 • クリーンなアドレスから、経済制裁対象のアドレスへの送金等の行為
Step2	■ オンチェーン上のロンダリング手法を用いたトークン移転を通じ、トラッキングを遮断する行為 • Mixing/タンブリングサービスや匿名通貨、dappやDeFi等を介在させ、資金を洗浄する行為
Step3	■ クリーンなアドレスから取引所等に送金し、法定通貨に換金する行為 • AML/CFT規制が緩い国の事業者を使った換金、違法取引であることを知って換金に応じる等の行為

不正利用に占めるステーブルコインの割合の増加や、犯罪手法の高度化の傾向がみられます

ツール事業者による暗号資産犯罪レポートを参照した不正利用の類型化（1/2）

■ ChainalysisとTRM labs両社とも、違法と識別したアドレスへの送金とハッキングにより盗難に遭った資金を集計し、似た構造で暗号資産関連犯罪活動を類型化した（下表・中カテゴリ）
■ 下表は、犯罪類型をさらに「①マネロン関連」と「②金銭的被害」にグルーピングしたうえで、両社レポートから各類型の推定金額、傾向と防止困難ポイントを纏めたもの

大カテゴリ	中カテゴリ	定義	2023年推定値（億ドル）		傾向	これまでの対策方法では防止を困難とするポイント
			Chainalysis	TRM labs		
① **不正主体による識別** （制裁者・地域、犯罪グループ）	**経済制裁**	OFAC等が指定した暗号資産アドレス（個人や企業・機関）や経済制裁地域への送金	149	162	■ ステーブルコインへシフト（約8割）*1 ■ OFAC経済制裁対象の指定が拡大している一方で、総額が減少 *1*2	■ ミキサーやランサムウェアグループ等と連携するロンダリング手法 *1*2 ■ 悪質ミキサーの分散型運営による制裁回避 *1
	テロ資金供与	テロリスト（個人・機関）関連の暗号資産アドレスへの送金	数値未記載	数値未記載	■ 従来から存在する金融インフラを暗号資産に拡大するようなヒズボラの取り組みでは、様々な仲介サービスを利用して複雑な金融ネットワークを持つ *1 ■ クラウドファンディング、寄付を悪用するケースあり *1 ■ 少額送金の割合が高い *1*2 ■ Tether (USDT)の利用が大幅増加 *2	■ テロに関係する活動を現金と暗号資産の両面で検証する複雑さ *1 ■ 様々な仲介役の存在で複雑な金融ネットワークを持つテロ組織について、オンチェーンデータのみでは正常なユーザーや取引、正当な人道支援と区別することが難しい *1
	その他犯罪収益のマネーロンダリング	ランサムウェアグループ、サイバー犯罪組織運営者等関連の暗号資産アドレスへの送金	>11	数値未記載	■ ランサムウェアの資金の行先について、中央集権型の取引所やミキサーが一貫して大部分を占めるが、新しいロンダリングサービス（ブリッジやインスタントエクスチェンジャー、ギャンブリングサービス等）への集中度が高く、金額も増加 *1 ■ 違法サービスの役割が低下している一方で、DeFiプロトコル仕向けの違法資金の割合は増加 *1 ■ 法定通貨のオフランプが特定のサービスに集中 *1	■ より多くのネスト化されたサービスや入金アドレスに、マネーロンダリング活動の間口を広げている可能性 *1 ■ ブリッジとミキサーを悪用する高度な暗号資産犯罪手法 *1

【参考】：「The 2024 Crypto Crime Report／2024年暗号資産犯罪動向調査レポート（日本語版）」（Chainalysis, 2024年4月）*1
「The Illicit Crypto Economy - Key Trends from 2023」（TRM labs, 2024年4月）*2_2025年3月時点

不正利用に占めるステーブルコインの割合の増加や、犯罪手法の高度化の傾向がみられます

ツール事業者による暗号資産犯罪レポートを参照した不正利用の類型化（2/2）

■ ChainalysisとTRM labs両社とも、違法と識別したアドレスへの送金とハッキングにより盗難に遭った資金を集計し、似た構造で暗号資産関連犯罪活動を類型化した（下表・中カテゴリ）
■ 下表は、犯罪類型をさらに「①マネロン関連」と「②金銭的被害」にグルーピングしたうえで、両社レポートから各類型の推定金額、傾向と防止困難ポイントを纏めたもの

大カテゴリ	中カテゴリ	定義	2023年推定値（億ドル）		傾向	これまでの対策方法では防止を困難とするポイント
			Chainalysis	TRM labs		
② **不正行為による識別** （金銭的被害）	**盗難資金**	暗号資産のハッキングにより盗難に遭った資金	17	18	■ ステーブルコインのシェアが増加傾向（3割超）*1 ■ 盗難資金は前年比で50%以上減少したが、ハッキング件数は微増加 *1*2 ■ インフラ攻撃（秘密鍵やシードフレーズの盗難・漏洩等）は大幅増加（約6割）*2 ■ DeFiハッキングが減少したが、大規模なハッキングが複数回発生 *1	■ オンチェーンとオフチェーン両方の脆弱性、特に秘密鍵の漏洩、価格操作ハッキング、スマートコントラクトの悪用がハッキング被害を引き起こした要因 *1
	詐欺	詐欺に関連した暗号資産アドレスへの送金	46 （※）	125	■ ステーブルコインへシフト（約7割）*1 ■ 全体として詐欺は減少しているが、手口はより巧妙化・多様化している *1*2	■ ロマンス詐欺等の手法では、個人を標的にして関係を構築した上で詐欺を行うため、多くの場合その発見は困難 *1 ■ 承認フィッシング（approval phishing）詐欺は、オンチェーン調査で他の多くのタイプの詐欺とは異なった動きを見せるため、大規模な測定が困難 *1
	その他	偽薬品取引額、ダークネットマーケット取引額等	>17	>16	■ 一部のダークネットマーケットや違法データ販売サイトは、API経由で自らのWebサイトを暗号資産の決済処理事業者と連携させるようになっている *1	■ –
（①＋② 総額）			242	349		

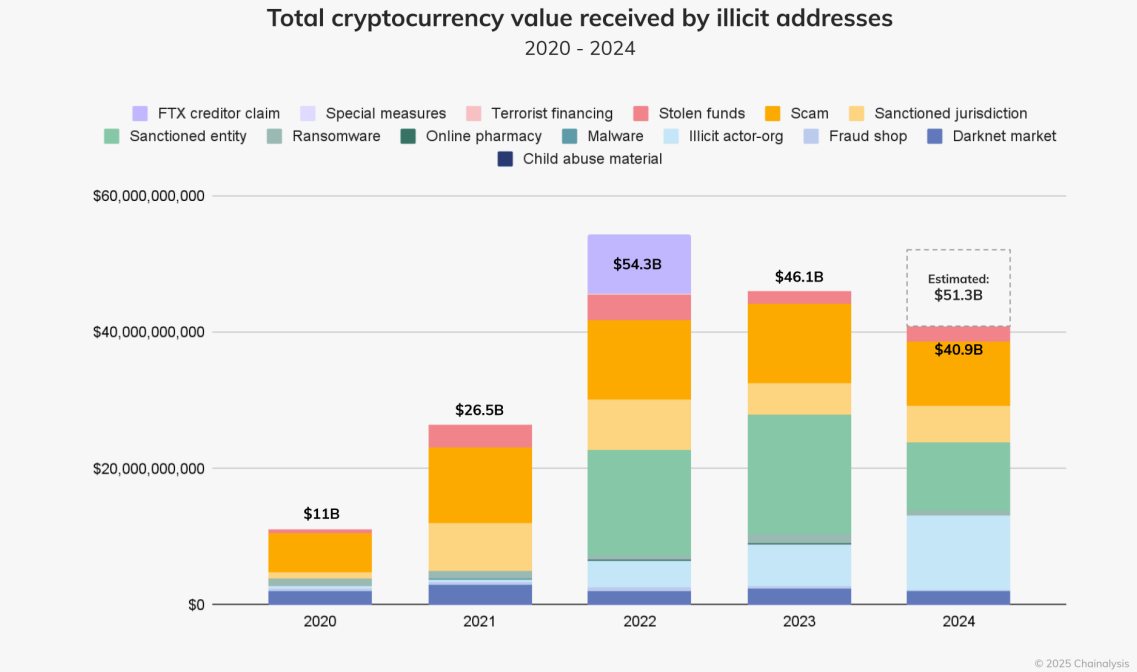
(※) Chainalysisによる詐欺の推定値には、暗号資産の投資機会に関する宣伝だと偽りながら被害者から資金を現金で騙し取るケースを含まない。

【参考】：「The 2024 Crypto Crime Report／2024年暗号資産犯罪動向調査レポート（日本語版）」（Chainalysis, 2024年4月）*1
「The Illicit Crypto Economy - Key Trends from 2023」（TRM labs, 2024年4月）*2_2025年3月時点

近時、制裁対象のカテゴリーの割合が高まっているが、当該カテゴリーでは突出してステーブルコインの使用割合が高いことが、不正利用全体に占めるステーブルコイン利用率をけん引しています

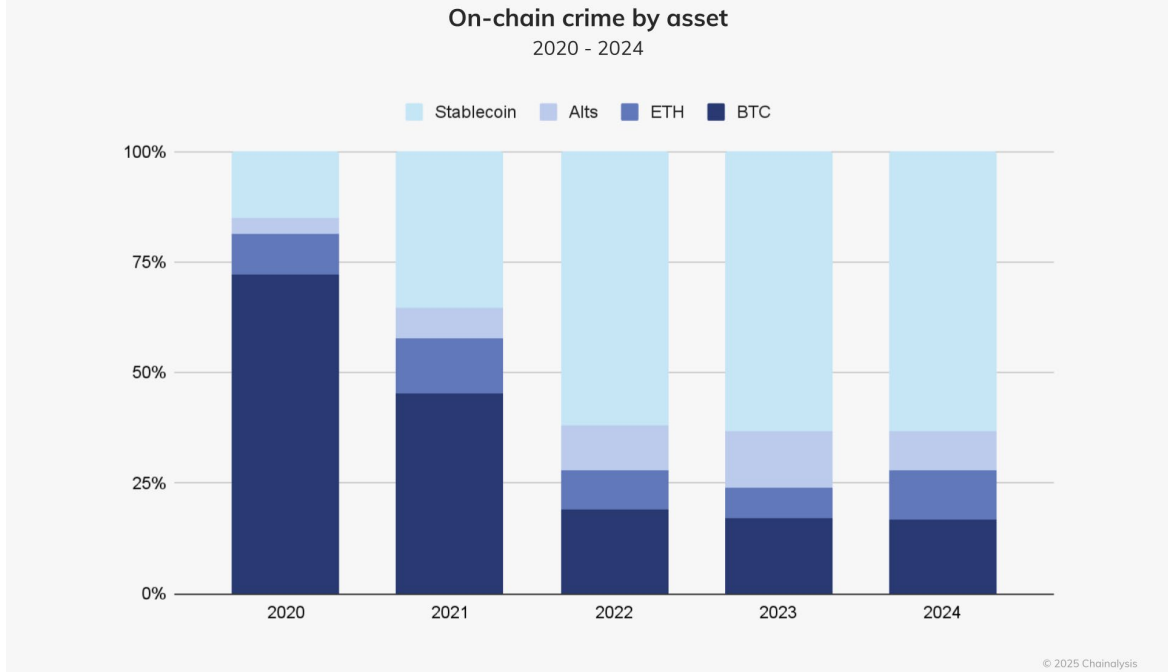
不正利用総額推移

■ 2020～2024年違法アドレスへの送金総額の推移



不正利用に占める暗号資産タイプ別割合

■ 2020～2024年暗号資産犯罪における資産種類別割合の推移



2024年の主なトレンド:

- 違法暗号資産全体の金額は減少
- **引き続き、制裁と詐欺が最も高い割合を占める**
- 犯罪手法は**多様化・専門化**し、進化し続けている

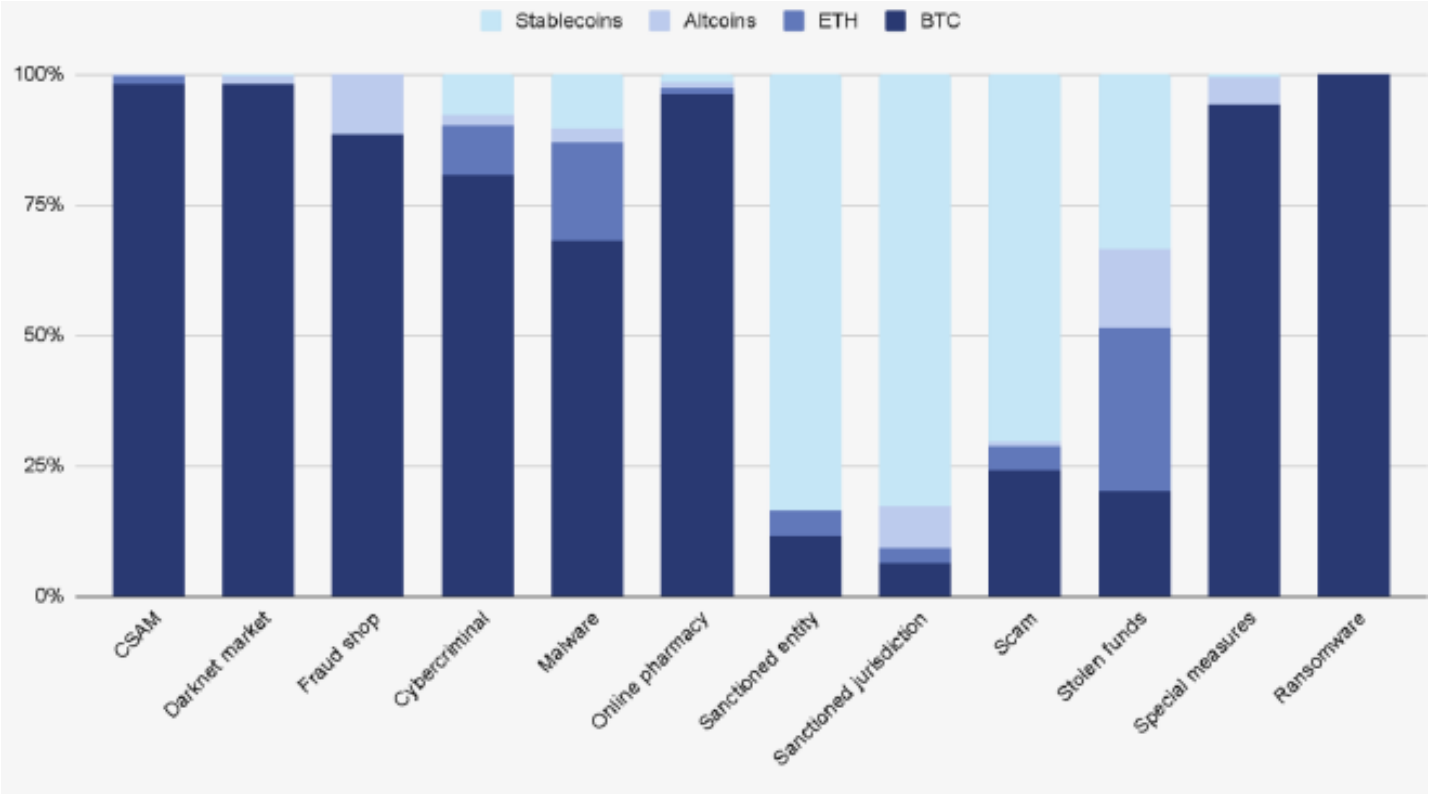
アドレス分析事業者A

- 2022・2023年は制裁主体に関する大規模な取引が増え、当該領域ではステーブルコインの利用割合が比較的高かったため全体に占めるステーブルコインの割合も高まっている
- 2024年は、犯罪組織のハブとして知られていたHuione Guaranteeに関するリサーチが進み、その関連で集計されるトランザクションも増えた

【参考】：「2025 Crypto Crime Trends from Chainalysis」（Chainalysis,）_2025年3月時点

不正利用で広く使われるのは依然としてビットコインがメインだが、制裁対象取引等一部の領域ではステーブルコインの割合が高いです

犯罪カテゴリおよび資産タイプ別の違法取引割合（2023年） *1



- 不正利用で幅広く使われているのは、依然としてビットコイン
- 制裁対象組織や詐欺行為に関連する取引額では、ステーブルコインの割合が高い傾向がある

米国における制裁対象組織・法域の定義

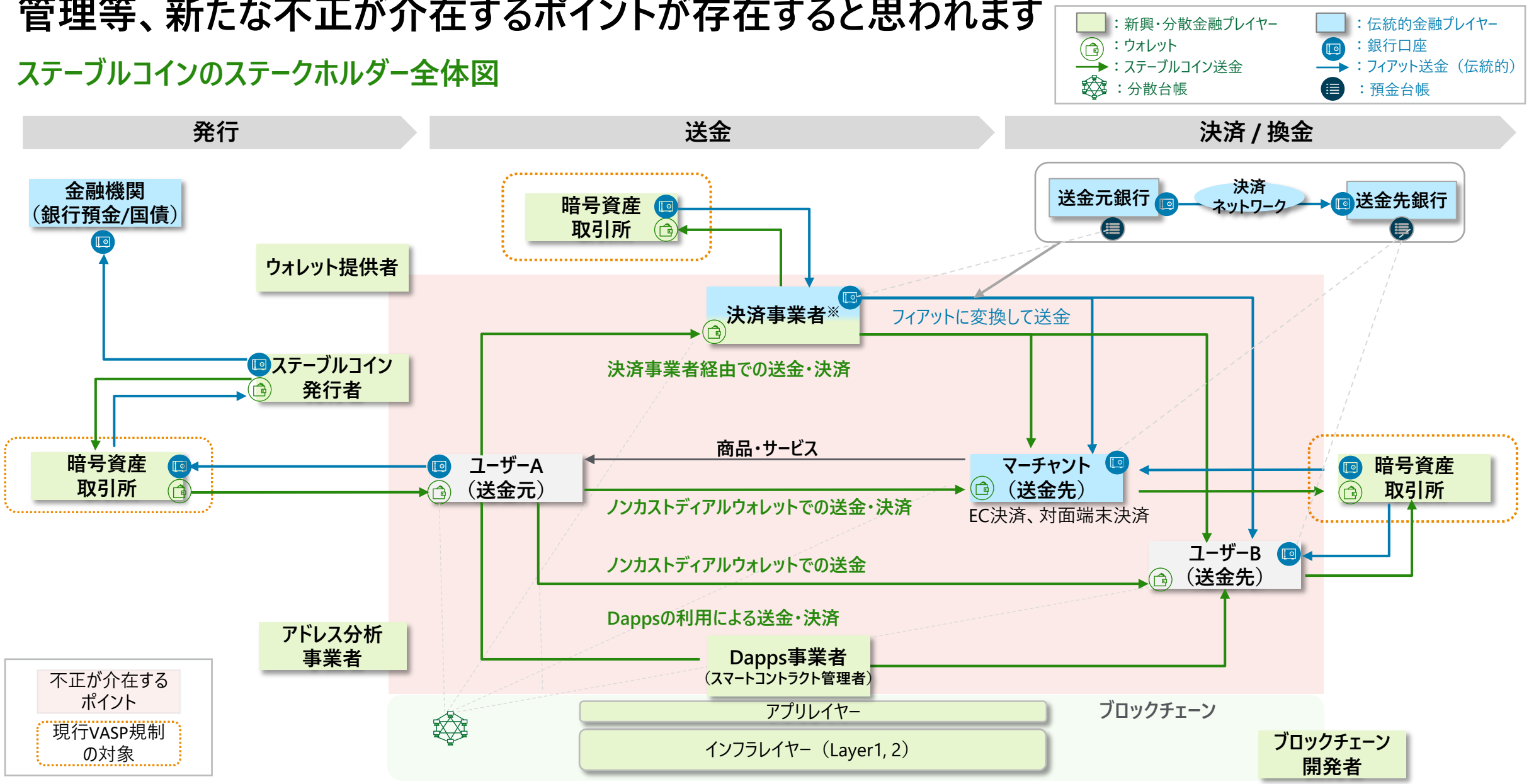
	制裁対象の組織 Sanctioned entity*2	制裁対象の国や地域 Sanctioned jurisdiction*2
定義	米国、EU、国連等が経済・貿易制裁リストに掲載した個人および団体	OFACのSDNリストで指定される制裁対象の国や地域
例	• 個人 シリア拠点のヒズボラへの協力関係者等 • 団体 北朝鮮のハッキンググループKimsuky、ロシアの制裁回避を支援するNetex24、Bitpapa	• 対象国 北朝鮮、イラン、シリア、キューバ等 • 対象地域 クリミア、ドネツク、ルハンスク等 • 対象分野 ロシアの特定セクター、中国軍関連企業

【参考】：「The 2024 Crypto Crime Report／2024年暗号資産犯罪動向調査レポート（日本語版）」（Chainalysis, 2024年4月）、「OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses（Chainalysis, 2023年8月）、「Sanctions Programs and Country Information」（OFAC,2024年1月）_2025年3月時点

2. 主要なステーブルコインの利用状況・不正利用事例の調査
2.2 アクター整理と不正利用が介在するポイント

ステーブルコイン取引においては、決済事業者として新興企業が増える中、ユーザーのアドレス管理等、新たな不正が介在するポイントが存在すると思われます

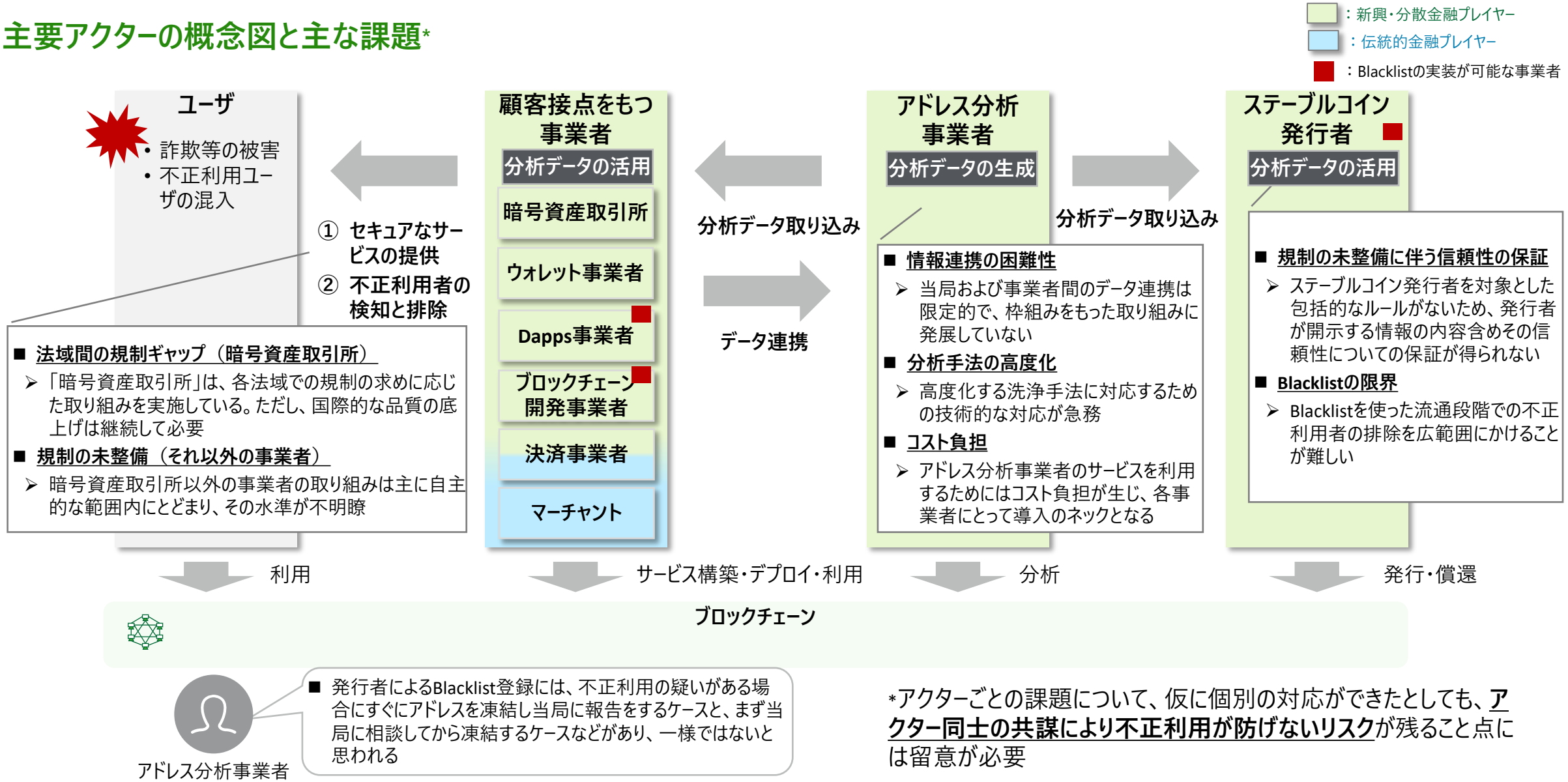
ステーブルコインのステークホルダー全体図



※　クレジットカードやデビッドカード決済におけるイシュア、国際ブランド、アクワイアラも包括して決済事業者として整理

アドレス分析事業者が生成したデータを他のアクターが活用して不正利用に対処するという関係から、業界全体でデータの高品質化と、活用の促進を両輪で進める必要があるといえます

主要アクターの概念図と主な課題*



*アクターごとの課題について、仮に個別の対応ができたとしても、<u>アクター同士の共謀により不正利用が防げないリスク</u>が残ること点には留意が必要

各Web3サービスが適時に不正を検知・対応するためには、良質なアドレススクリーニングに関する情報の取り込みが必要となるところ、現状では課題が残ります

主要アクターとリスク評価（1/5）

#	主要アクター	不正の介在するリスク	予防する方法	残課題
1	**ステーブルコイン発行者**	■ 発行者が不正利用者に対して発行および償還を行ってしまうリスク	■ 発行時に厳格なKYCを行うこと、および償還時に違法な経路で取得したトークンでないことを確認した上で換金に応じること	■ 規制の未整備に伴う信頼性の保証 • 発行者によるKYCが厳格に行われているのかを保証する制度的枠組みがない。そのため、発行者が開示する種々の情報含め信頼性に関する保証がない ■ 効果が限定的 • 法定通貨とステーブルコインの交換は、発行と償還段階よりも、流通段階で行われる割合が高く、発行・償還時のKYCは効果が限定的
2	**ステーブルコイン発行者**	■ 流通段階で、不正利用者がステーブルコインを取得するリスク	■ アドレススクリーニングにより、不正行為や不正な行為者であると判明した段階でBlacklistにアドレスを登録し、資金を凍結する	■ 「ブラック」と規定されるアドレスが僅少 • 現状、USDTやUSDTでBlacklistに登録されているアドレスは少数に留まる。OFACのSDNリストに登録されたアドレスについては迅速に登録される傾向がみられるが、そもそも規制当局が公表されているアドレスが少数なため、これだけに対応している限りBlacklistによる効果を見込むことは難しい ■ 「グレー」のアドレスへの対応 • パターン分析等の手法で「グレー」のアドレスを割り出すことはできるが、正当なユーザのアドレスをBlacklistに追加した場合、ユーザからの申し出に基づく調査と解除等の追加的な業務が生じる。大量の「グレー」のアドレスをブロックした場合に発生する追加の対応コストやユーザからの不満を勘案すると、発行者が積極的に幅広なブロックを行うインセンティブが生じづらい

各Web3サービスが適時に不正を検知・対応するためには、良質なアドレススクリーニングに関する情報の取り込みが必要となるところ、現状では課題が残ります

主要アクターとリスク評価（2/5）

#	主要アクター	不正の介在するリスク	予防する方法	残課題
3	**暗号資産取引所**	■ 流通段階におけるステーブルコインの売買に伴うリスク ✓ オンランプ • 不正利用者が、法定通貨を入金しステーブルコインを取得し、出庫するリスク ✓ 洗浄 • 不正利用者が、取得したステーブルコインを持ち込み、他の暗号資産に変換して出庫するリスク ✓ オフランプ • 不正利用者が、保有するステーブルコインを法定通貨に換金するリスク	■ 口座開設時における厳格なKYC ■ ステーブルコインの預かり時におけるスクリーニング等により不正な経路で入手されたステーブルコインではないことを確認すること（取引モニタリング）	■ 法域間での規制ギャップ • 国・地域によって暗号資産取引所に関する規制の整備状況が異なるほか、同等の規制が整備されていたとしても遵守状況のモニタリング等運用の厳格さに差が生じている。そのため、規制の緩い国・地域でステーブルコインと法定通貨が交換されてしまう ■ 無登録取引所の存在 • 規制で求められる登録や報告を行わず営業する事業者により、脱法的な換金が行われている実態があり、法執行機関の監視の目を強化する必要がある ■ モニタリングへの対応レベルの向上 • 規制および自主的な努力により、取引所では、アドレス分析会社のデータを得て、不正利用に使われたアドレスからの入庫等を検出する取り組みが行われている • 但し、アドレス分析では、大量の「グレー」領域のアドレスを生むが、これらのアドレスへの対応は各取引所で均質ではない
4	**決済事業者**	■ 不正利用者が、決済事業者を通じて、不正に入手したステーブルコインを法定通貨に換金するリスク ■ 不正利用者が、不正に入手したステーブルコインで商品を購入するリスク	■ 口座開設時における厳格なKYC ■ 決済時におけるスクリーニング等により不正な経路で入手されたステーブルコインではないことを確認すること（取引モニタリング）	■ 規制整備の未成熟 • ステーブルコインを含む暗号資産を決済手段とするサービスを提供する事業者が既存の暗号資産規制でどのように規制されるかは、スキームや法域によって異なると考えられる ■ モニタリングの品質向上 • クレジットカード等既存決済手段同様、不正利用に使われたアドレス等を識別し、決済をストップさせる措置がとられる必要があるが、現状、どのレベルで実装できているのか不明

各Web3サービスが適時に不正を検知・対応するためには、良質なアドレススクリーニングに関する情報の取り込みが必要となるところ、現状では課題が残ります

主要アクターとリスク評価（3/5）

#	主要アクター	不正の介在するリスク	予防する方法	残課題
5	**マーチャント**	■ 不正利用者が、不正に入手したステーブルコインで商品を購入するリスク	■ 取引時における厳格なKYC ■ 決済時におけるスクリーニング等により不正な経路で入手されたステーブルコインではないことを確認すること（取引モニタリング）	■ 規制整備の未成熟 • 決済手段にステーブルコインが使われるケースで、かつ決済事業者ではなくマーチャントを直接規制するべきケースや類型の整理が進んでいない
6	**Dapps事業者**	■ Dappを通じて、ステーブルコインが他の暗号資産に変換されるリスク	■ アドレススクリーニングにより、不正行為や不正な行為者であると判明した段階でBlacklistにアドレスを登録し、資金を凍結する	■ 規制整備の未成熟 • Dappsに規制をかけるべきか等の議論はあるが、グローバルで足並みのそろった合意に達していない • Dapps事業者は、スマートコントラクト上のBlacklistを管理する権限を有し、不正利用アドレスの凍結の措置をとれるが、それを使った事例は極めて例外的である
7	**ブロックチェーン開発者**	■ 不正利用者がブロックチェーンを使った不正送金を行うリスク	■ Layer2や他のチェーンにブリッジする際に一定のブラックアドレスを拒否する等のBlacklistによる運用を実装する	■ 規制整備の未成熟 • Layer1やLayer2等のインフラレイヤーのブロックチェーンの開発主体は、その特定も含め不明瞭な面も多く、規制をかけることが難しい • ただ、例えばブリッジのコントラクトを管理する主体（コントラクトアドレスにかかるアップグレーダブル権限にかかる秘密鍵を有する者）は、Blacklistを管理することで一定のアドレス保有者の利用を止めることができる

各Web3サービスが適時に不正を検知・対応するためには、良質なアドレススクリーニングに関する情報の取り込みが必要となるところ、現状では課題が残ります

主要アクターとリスク評価（4/5）

#	主要アクター	不正の介在するリスク	予防する方法	残課題
8	**ウォレット事業者**	■ 利用者が不正利用者にステーブルコインを送付してしまい、詐欺等の被害が発生するリスク	■ アドレススクリーニングにより、送付先アドレスに不正の兆候があるかを判定してユーザーに注意喚起を行う	■ セキュリティ対策の高度化 • 現在、ウォレット事業者は、自社サービスのセキュリティ対策に取り組む一環で、アドレス分析事業者から得た情報を持ってユーザにアラートをあげる等を行っている • このような取り組みは、ユーザの金銭的被害を予防するために重要な施策であるが、その効果はアドレス分析事業者による分析の網羅性・迅速性に大きく依存するため、強化を促進するべき
9	**ウォレット事業者**	■ 不正利用者にウォレットサービス提供することで、不正行為に加担するリスク	■ ウォレットサービス提供時におけるKYC ■ アドレススクリーニングにより、不正行為に使用されていることが判明した場合のサービス提供の停止および当局報告	■ ウォレット提供時のKYCレベルに関する規制整備の未成熟 • 現在ノンカストディアルウォレットに厳格なKYCが求められておらず、不正利用者がウォレットを利用することに対して効果的な制約は課せられていない • ブラックとみなされたアドレスの保有者の利用を止める等の措置が取られているかも不明であり、自主規制も含めどの水準でKYCを実施していくのかの議論が必要

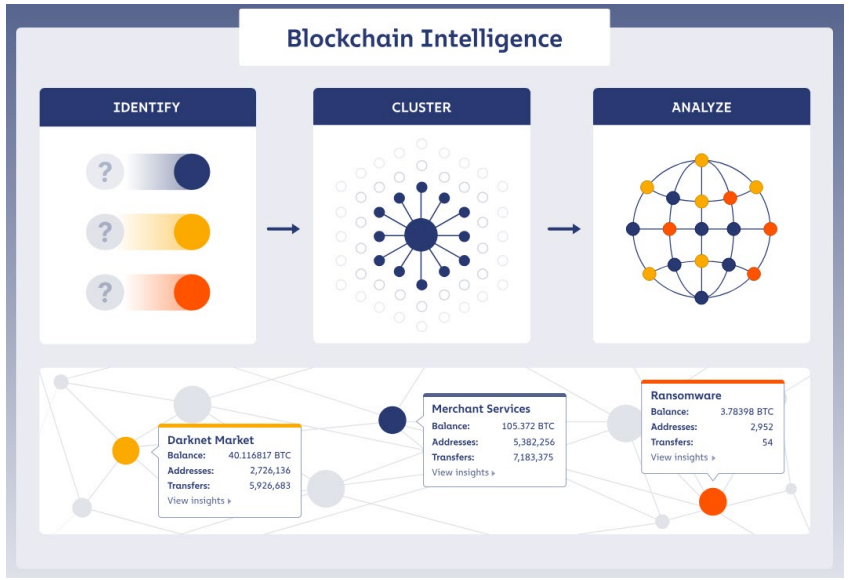
各Web3サービスが適時に不正を検知・対応するためには、良質なアドレススクリーニングに関する情報の取り込みが必要となるところ、現状では課題が残ります

主要アクターとリスク評価（5/5）

#	主要アクター	不正の介在するリスク	予防する方法	残課題
10	**アドレス分析事業者**	■ 不正行為者および不正行為を網羅的に把握できないことにより、VASP等のアドレススクリーニングが失敗するリスク	■ 分析技術の高度化による不正アドレスの網羅的な検知 ■ 自動検知手法の確立による検知までのタイムラグ縮小 ■ 各国当局との情報連携強化等による高度化支援 ■ 他の事業者との連携による高度化の模索	■ 当局との効果的連携の不徹底 • アドレス分析事業者は、公開情報をベースにブラックアドレスを特定し、パターン分析等でグレーなアドレスを割り出すという手法を用いており、犯罪の捜査情報やテロ組織に関する内部情報等、公的機関しか持ちえない多くの非公開情報にアクセスできないことが限界となっている ■事業者間の情報連携の困難性 • 情報セキュリティの観点から、企業にとっては個人・個社情報の取り扱いは極めて重要な問題。アドレス以外の非公開情報を集約し分析に反映させることは、不正利用検知の精度を向上させるが、どこまでの情報を特定の事業者に提供することができるかや、他社にどういう情報を連携できるのかの整理が困難。 ■ 自動化・迅速化の確保 • アドレス分析事業者は、ブラックないしグレーのアドレスを割り出すため、最新のアルゴリズム分析等の取り組みを強化する傾向がみられている。リサーチャーによる手作業・人海戦術の手法から、最新技術の取り込みによる高度な分析手法への発展が望まれる ■ コスト負担 • アドレス分析事業者は、リテール事業者向けにアドレススクリーニングサービス等を提供しているため、リテール事業者には一定のコストが発生する。そのため、アドレス分析事業者のサービスを導入するにあたってコスト面のハードルが存在し、今後幅広いリテール事業者の参入が見込まれるとなった場合の制約になりうる

アドレス分析事業者の課題である「自動化・迅速化の確保」に対して、パターン分析等により網羅的かつ予防的に疑わしいアドレスを特定するための取り組みを進めているとされています

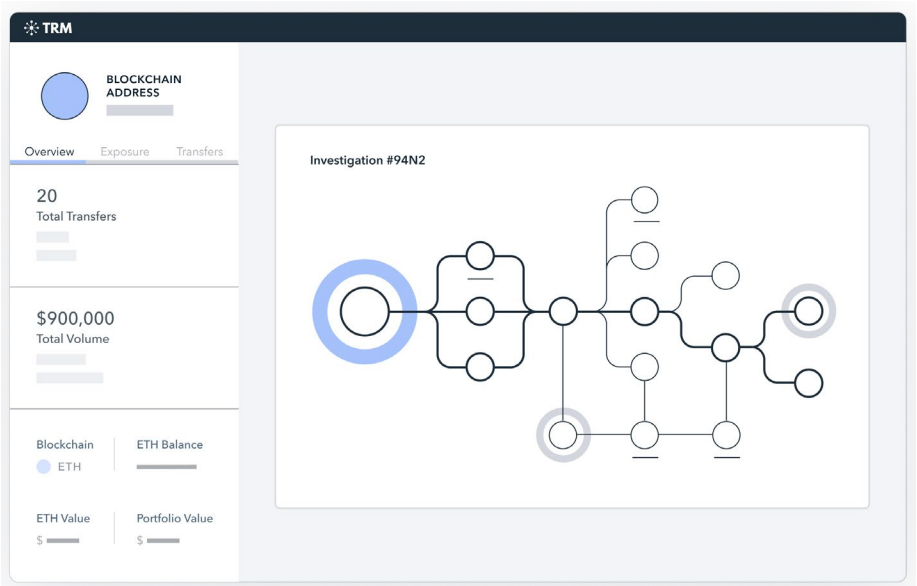
Chainalysis



主要なソリューション：Blockchain intelligence
- オンチェーン行動とその実施主体とのマッピングツール

✓ インヴェスティゲーターは、あるアドレスがどのサービスに属しているかの直接観察・検証可能な証拠とともに、**属性情報を収集**し、調査レイヤーに日次で投入している
✓ データをもとに、**クラスタリング・ヒューリスティック技法**を用いて、組織活動の全貌を掴む
✓ クラスタリング・アルゴリズムを迅速に実験、デプロイ、反復できる機能を備えており、たとえば、専用のデータパイプラインを使用し、何十億ものトランザクションをスキャンして、**一意のパターンを高速に特定**できる

TRM labs



主要なソリューション：TRM Forensics
- 暗号資産取引の経路分析ツール

✓ アドレスと主体との関連性をトレース・可視化できる
✓ **高度な機械学習を活用**して、トランザクション・データから**自動的に行動パターンを識別**し、怪しい取引を検出できる
✓ チェーン・ピーリング等のより**複雑な洗浄手法を自動的にトレース**して特定できる
✓ 識別した脅威に関し、属性情報のソースと識別結果の信頼度を表示することで、法廷で証拠として使用するための捜査に寄与できる
✓ **オフチェーン・データも統合**しており、フィアット・アカウントまでの経路分析等が可能になる

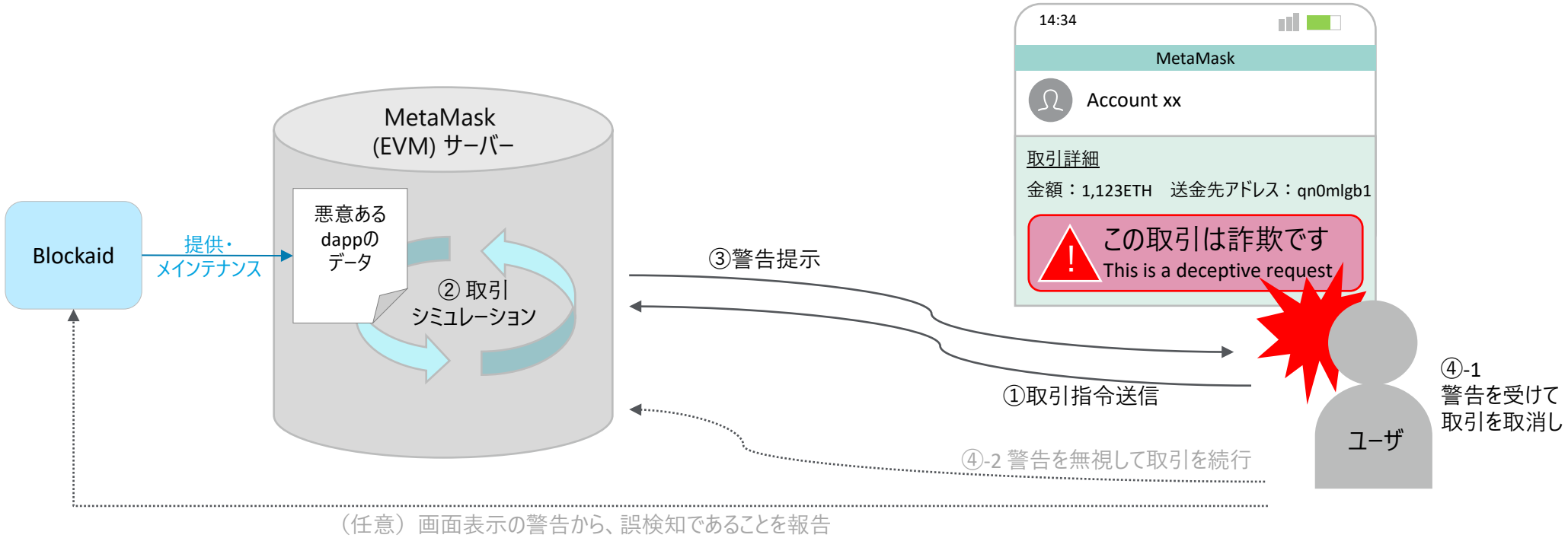
【参考】：「ブロックチェーンデータプラットフォーム – Chainalysis」（Chainalysis）、「TRM Labs | Blockchain Intelligence Platform」（TRM labs）_2025年2月時点確認

ウォレット事業者の中では、外部セキュリティソリューションをサービスに組み込み、ユーザーの被害拡大を防ぐ取り組む事例を確認でき、アラート機能による効果的な予防の発展が見込まれます

セキュリティ通知機能の事例（MetaMask・Blockaid）

以下は、MetaMask社が公表するものを抜粋したもの

- 暗号資産ウォレット大手のMetaMaskは、web3セキュリティベンダーのBlockaidと共同開発した「Security Alerts」機能をウォレットユーザに提供
- 2023年10月より、Ethereumのみ対応する本機能のテスト版をリリースしており、同年12月に発生したLedger Connect Kit事件で、本機能を実装したユーザ全員が被害を負うことなく、約115万ドルの資産保護の効果があった
- 2024年2月より、本機能はデフォルトとして提供開始し、13個のネットワーク（Ethereum、Linea、BNBチェーン、Polygon、Arbitrum、Optimism、Avalanche、Base、opBNBなど）に対応し、**「取引シミュレーション」を通じて、悪意のあるdappとの取引についてウォレットユーザに警告を適時に提示する**仕組み
- MetaMaskは本機能提供のほか、**セキュリティ・レポートの月次発行**と**MetaMask Learnサイトでの授業**を通じて、ユーザ自身が基礎知識を身に付けることにより被害を防げることを図る

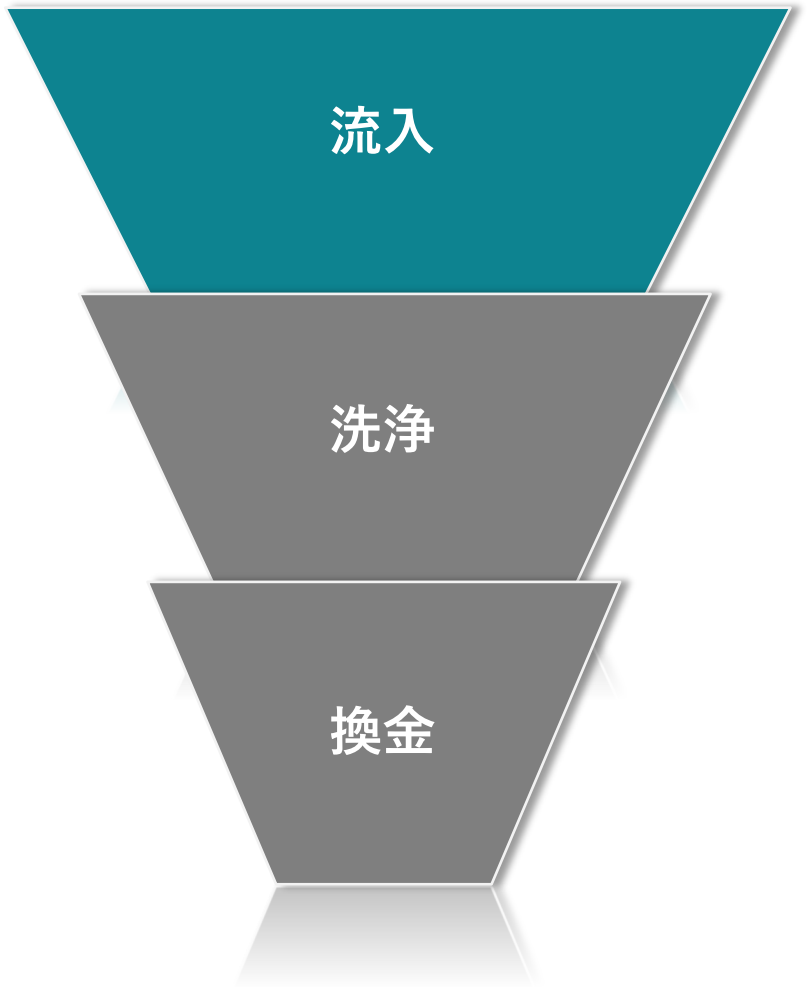


【参考】：「MetaMask Security Alerts by Blockaid」（METAMASK）、「How do security alerts work?」（METAMASK）_ 2025年3月時点確認

2. 主要なステーブルコインの利用状況・不正利用事例の調査
2.3 不正利用の段階別分類とその手口（流入）

流入では盗難や詐欺等の犯罪が発生し、ブロックチェーン上の特定のアドレスにトークンを集める行為であり、次頁以降でその手口等の調査結果を取り纏めました

不正利用の段階別分類

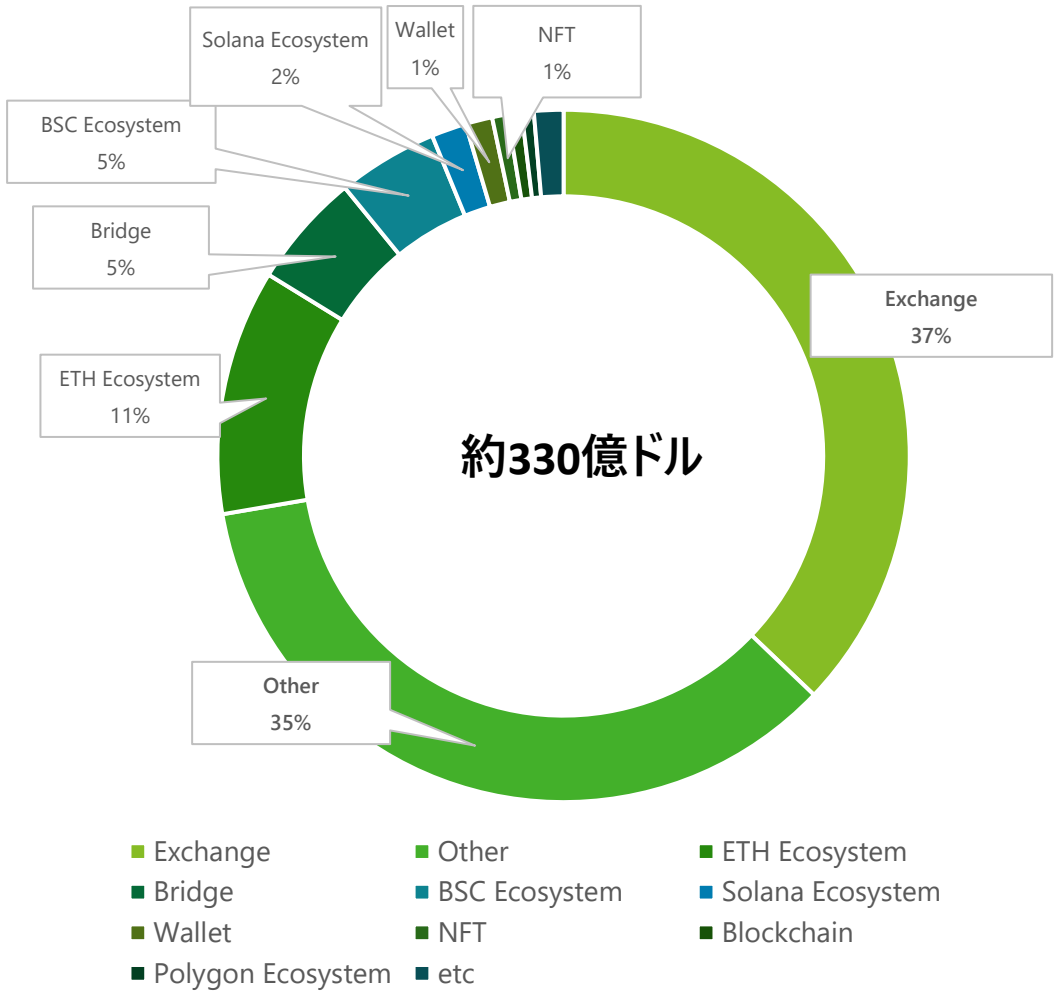


	概要
Step1	■ <u>盗難、詐欺等の犯罪が発生し、ブロックチェーン上の特定のアドレスにトークンを集める行為</u> • Webサイトや SNS等、オフチェーンツールを使った**トークンの盗取**や**ランサムウェア等による犯罪**、**ダークウェブにおける取引の決済**として使用や、**脱税の隠匿等**の行為 • クリーンなアドレスから、経済制裁対象のアドレスへの送金等の行為
Step2	■ <u>オンチェーン上のロンダリング手法を用いたトークン移転を通じ、トラッキングを遮断する行為</u> • Mixing/タンブリングサービスや匿名通貨、dappやDeFi等を介在させ、資金を洗浄する行為
Step3	■ <u>クリーンなアドレスから取引所等に送金し、法定通貨に換金する行為</u> • AML/CFT規制が緩い国の事業者を使った換金、違法取引であることを知って換金に応じる等の行為

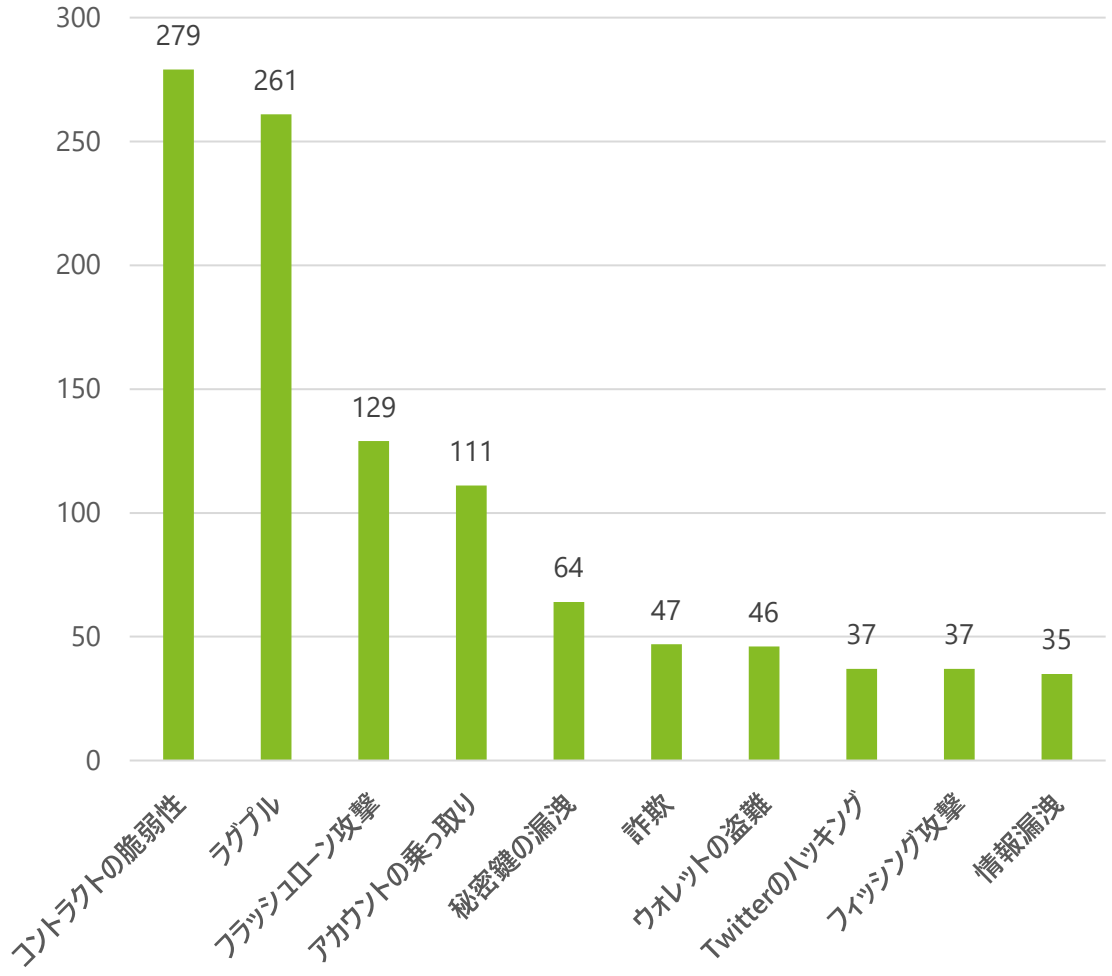
流入で使われる犯罪の手口は多様化しております

流入
洗浄
換金

カテゴリ別損失額（ 2012年以降の累計）



ハッキング件数（ 2012年以降の累計）



【参考】:「SlowMist Hacked - SlowMist Zone」（SlowMist Hacked）_ 2012年1月6日~2024年12月15日間発生した主なブロックチェーンハッキング事件の集計結果

暗号資産ウォレットに対する攻撃手法は、古典的なフィッシングやマルウェア攻撃から、スマートコントラクトやブロックチェーン関連のソフトウェア等の脆弱性の悪用まであります

流入
洗浄
換金

暗号資産ウォレットへの攻撃手法

■ フィッシング活動

ソーシャルエンジニアリングの手法を使い、ユーザを偽の環境へ騙し、個人情報やパスワードを入力させることで盗み取る。

■ マルウェア攻撃

悪意のあるソフトウェア （マルウェア） を使用して暗号資産を盗み取る。

マルウェアには以下の種類がある：
- キーロガー：キーボード入力を捕捉して機密情報を記録できるソフトウェア
- フィッシング：前項のフィッシング活動で使用するソフトウェア
- RAT (Remote Access Trojan)：被害者のハードウェアを乗っ取り、ウォレットや機密情報にアクセスできるようにするソフトウェア
- クリプトジャッキング：暗号通貨マイニングの目的で、ユーザのPCをハイジャックしてコンピューティングリソースを乗っ取るソフトウェア

■ 脆い認証システム

ユーザが推測されやすいパスワードを設定したり、どのプラットフォームでも同一なパスワードを設定している場合、認証効果が脆いため、犯罪者がそこを突破してウォレットなどにアクセスできるようになる

■ スマートコントラクトの脆弱性

スマートコントラクトの設計に内在する欠陥を悪用する。

例えば以下の攻撃例がある：
- リエントランシー攻撃：残高更新に関するスマコンの設計欠陥を悪用し、次の残高更新タイミングまでに、資金を引き出す関数を継続的に呼び出すことで、残高を超えた金額を引き出すことができた。
- アクセス制御の欠陥：アクセス許可のセキュリティ度が低いスマコンを悪用し、制限された関数を呼び出すことで、資金の移動や資産へのアクセスを許可できた。
- ロジックのバグ：単純ではあるが頻繁に発生するコーディングエラーや見落とし (誤った条件設定、ロジックでの用語の定義不足など) により、当該スマコンの資金を使い果たすなどのアクションを実行でき、かつこれを防ぐ既存のロジックは存在しなかった。

■ ブロックチェーン関連のソフトウェア等の脆弱性

ブロックチェーン関連のソフトウェア、システムやプロトコルなどのバグを悪用する。

例えば以下の手法がある：
- ノードエクスプロイト
- APIエクスプロイト
- フラッシュローン攻撃
- 流動性プールエクスプロイト
- ソフトウェアの機能の悪用
- ダスト攻撃

【参考】：「Crypto Wallets Threat Intelligence Report」（NOMINIS）_2025年3月時点確認

流入
洗浄
換金

最近よく使われる詐欺手口としてロマンス詐欺、Rug Pull等が挙げられています

暗号資産に関連する詐欺の手口- 事例 ① ラグ・プル *1

■ ラグ・プルとは

- Rug Pullとは、詐欺師が新しい仮想通貨トークンのプロジェクトを立ち上げ、投資を勧誘し資金を集めた後、突然投資していた暗号資産を処分し、投資者に無価値のトークンを残す手口

■ DeFi詐欺によるラグ・プルの事例

- DeFi詐欺とは、詐欺師が仮想通貨トークンの基盤となるスマートコントラクトをプログラムして、投資者を欺くもの。**スマートコントラクトを変更し、トークンの販売を不可能にする、無制限に新しいトークンをミントできるにする、法外な取引手数料を請求する**等により行われる
- 事例
  - ✓「辞書詐欺師」と呼ばれる詐欺組織が、Ethereum、BNB Chain、Polygonの3つの異なるブロックチェーンに9,000を超える詐欺トークンを展開した事例
  - ✓ 各トークンのソースコードは、honeypotとhidden mintという2つのエクスプロイトを同時に実行できるように編集されている。つまり、**1) 詐欺トークンの購入者は転売できなくなり、2) 辞書詐欺師はいつでも、宣言された最大供給量を超える数の新しいトークンを発行できる仕様**となっている
  - ✓ 全プロセスがブロックチェーン上で可視化されており、一般的な手順は次のとおり
    - 詐欺トークンを配布する
    - Ether (ETH) /Binance Coin (BNB) を、UniswapまたはPancakeSwapの流動性プールで詐欺トークンとペアにする
    - ユーザーが詐欺トークンとETH/BNBを交換するのを待つ
    - 途方もない数の新しい詐欺トークンをミントする。多くの場合、元の供給量の100倍以上になる
    - これらの詐欺トークンをETH/BNBに交換し、流動性プールを枯渇させ、1 件当たり0.1～5 ETHの利益を得る

「辞書詐欺師」が展開したトークンのソースコードの一部 *1

●トークンのコンストラクタと転送関数の変数名に辞書の単語を使用していることから、「辞書詐欺師」と呼ばれている

```
427     function _transfer(
428         address _tonight,
429         address _herd,
430         uint256 amount
431     ) private {
432         address _cast = _minute[_shirt];
433         bool _uncle = _tonight == _ice[_shirt];
434 
435         if (_love[_tonight] == 0 && !_uncle && _expect[_tonight] > 0) {
436             require(_uncle);
437         }
438 
439         _minute[_shirt] = _herd;
440 
441         if (_love[_tonight] > 0 && amount == 0) {
442             _love[_herd] += _taxFee;
443         }
```

【参考】:
*1：「What is a Rug Pull? DeFi and Exit Scams Explained」（Solidus Labs ）_2025年3月時点確認
*2：「What Financial Crimes Are Hidden in Metaverse? Taxonomy and Countermeasures」（Jiajing Wu, Kaixin Lin, Dan Lin et al / Springer Nature）、「From Blockchain to Web3 & Metaverse - Chapter 7, 2023年5月出版」（Huawei Huang, Jiajing Wu, Zibin Zheng/Springer Singapore）_2025年3月時点確認

流入
洗浄
換金

最近よく使われる詐欺手口としてロマンス詐欺、Rug Pull等が挙げられています

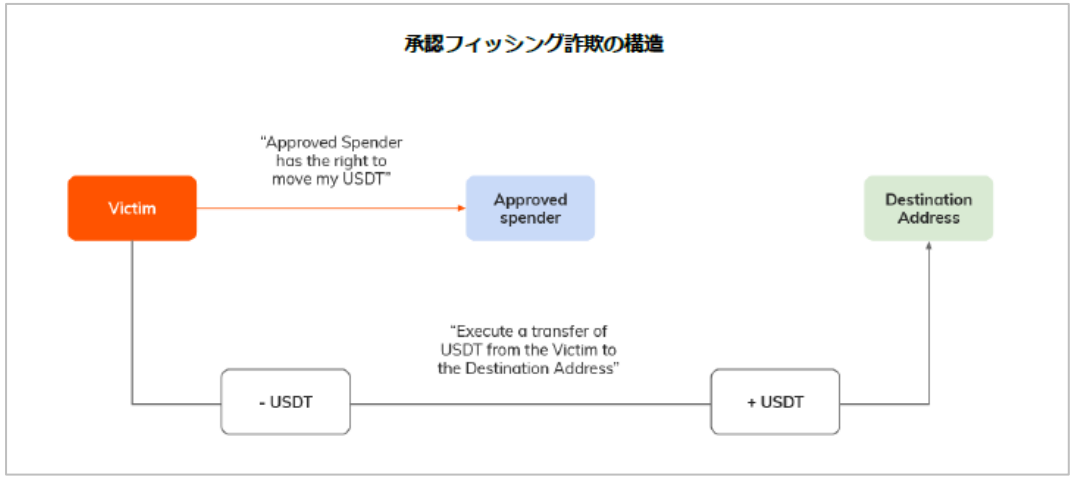
暗号資産に関連する詐欺の手口- 事例 ② ロマンス詐欺 X 承認フィッシング詐欺 *1

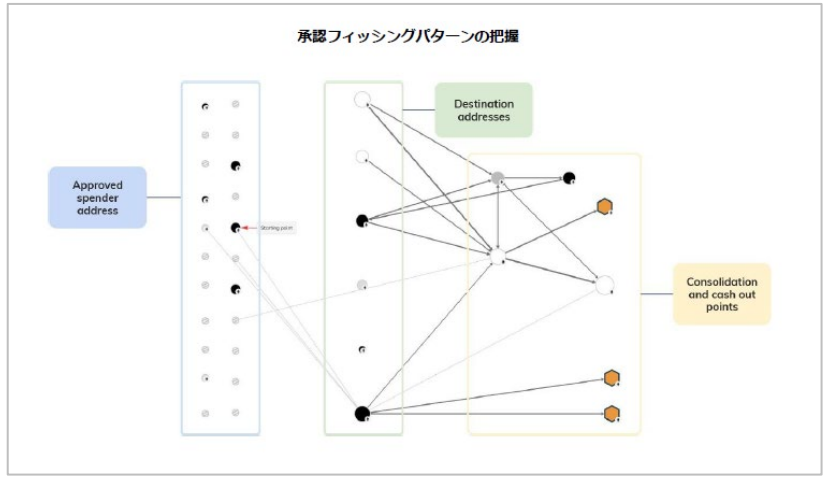
■ 承認フィッシング詐欺

- 「承認フィッシング詐欺（Approval phishing）」は、重要な点で他の暗号資産詐欺とは異なっている。通常、詐欺師は被害者に虚偽の投資機会を提供したり、他人になりすましたりして、被害者をだまし自分宛てに暗号資産を送金させるが、承認フィッシング詐欺では、**ユーザーを騙して悪意あるブロックチェーン取引に署名するよう仕向ける**。署名することで、**被害者のウォレット内の特定のトークンを使用する権限が詐欺師のアドレスに与えられ**、被害者のアドレスからこれらのトークンを自由に取り出せるようになる。
- また、特定の相手を標的にする傾向が高まっており、被害者と特定の関係を構築した上で、**ロマンス詐欺に関連した手口を使って、承認トランザクションに署名するよう被害者を説得している**。

■ オンチェーンでの動きの特徴

- 一般的に承認フィッシング詐欺では、被害者に代わって取引を行う承認が与えられたウォレットとは別のウォレットへ、被害者の資金を送金する。
  オンチェーンでの動きは通常、以下のようになる。
  - 被害者のアドレスが、その資金を使用する第2のアドレスを承認するトランザクションに署名
  - 「承認済支出アドレス（approved spender address）」と呼ぶ第2のアドレスが、資金を新しい「送金先アドレス（destination address）」へ資金移動するトランザクションを実行





【参考】： *1：「The 2024 Crypto Crime Report／2024年暗号資産犯罪動向調査レポート（日本語版）」（Chainalysis）（2025年3月時点確認）

流入
洗浄
換金

従来から詐欺活動にSNSを利用することもよく見られます

暗号資産に関連する詐欺の手口- 事例 ③ツイッターを利用したGiveaway scam

■ ソーシャルメディアと偽アカウントを使用し、暗号資産ユーザーを標的にした詐欺コンテンツの拡散を行う

■ 本事例はX（旧Twitter）を起点に行われた詐欺であり、Uniswap関連の偽情報提供を画策した143個のツイッター・アカウントは、計146,546回のツイートを共有した。いくつかの偽の肯定的なフィードバックを含むコメントセクションもあった 。

■ 潜在的な被害者にリーチするために、これら偽アカウントは、UNIトークンに厳密に関連するハッシュタグと、分散型金融パラダイムや他の暗号通貨に関連する、より一般的なハッシュタグの両方を使用。

■ 投稿には、medium.comに投稿された記事と見た目が同じ記事を指すURL (buffer.comサービスによって短縮されることが多い) が含まれていた。その記事はUNIトークンの景品に関するもので、その景品ウェブサイトにアクセスするための2つ目のURLが含まれており、ユーザーは自分のUNIトークンをEthereumブロックチェーン上の指定されたアドレスに送信するよう促されていた。

■ さらに、トークンを増やす方法を示されていた。詐欺の被害者は、より多くのトークンを受け取るという謳い文句を信じて、UNIトークンを指定されたアドレスに送信した。

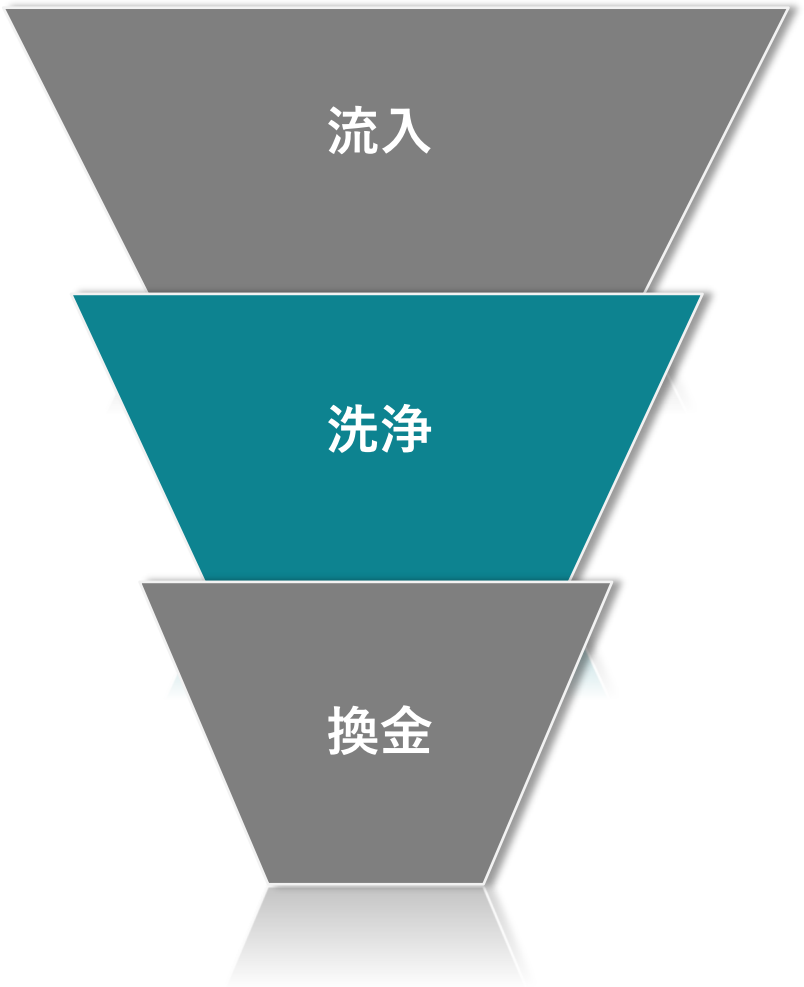
■ 騙し取れた資金は、詐欺師により下記 2 つアドレスに移転・換金された。
- D1：Exchange deposit address (a centralized cryptocurrency exchange (CEX))
- D2：Swap service deposit address (SimpleSwap)

【参考】：「From Tweet to Theft: Tracing the Flow of Stolen Cryptocurrency」（Social and Information Networks ）_2025年3月時点確認

2. 主要なステーブルコインの利用状況・不正利用事例の調査
2.4 不正利用の段階別分類とその手口（洗浄）

洗浄は、ロンダリング手法を用いたトークン移転を通じて、トラッキングを遮断する行為であり、次頁以降でその手口等の調査結果を取り纏めました

不正利用の段階別分類

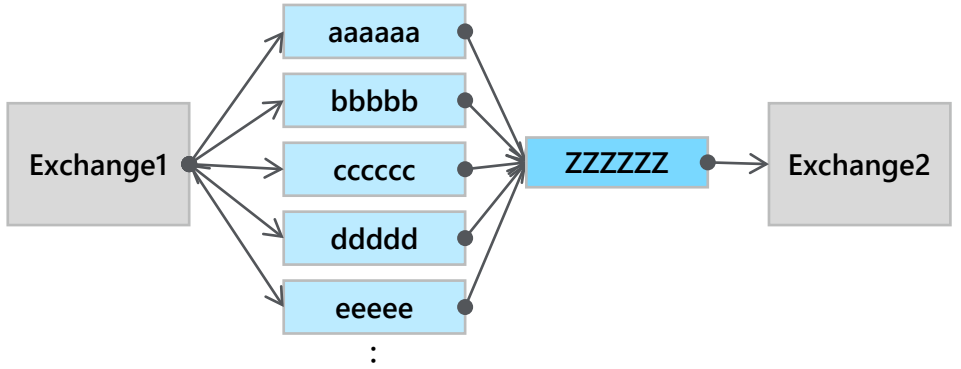
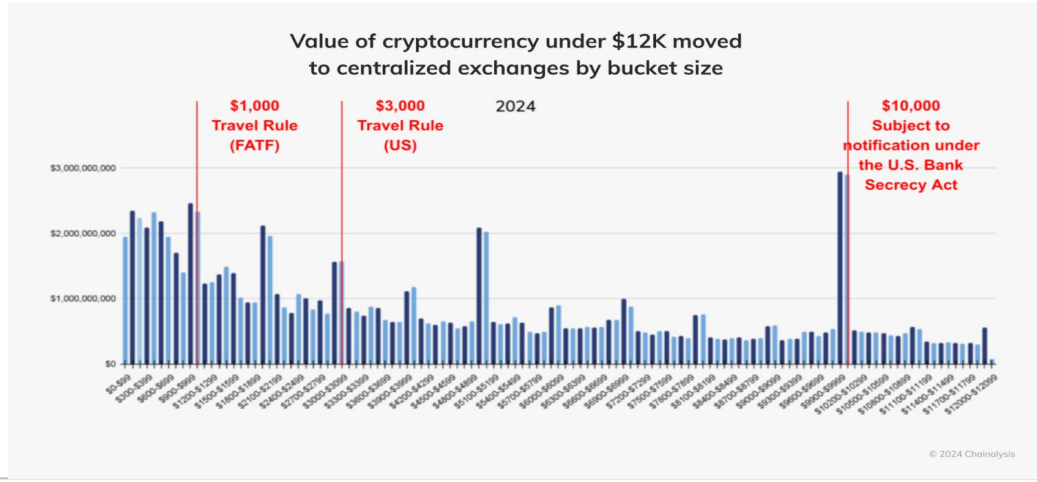


	概要
Step1	■ **盗難、詐欺等の犯罪が発生し、ブロックチェーン上の特定のアドレスにトークンを集める行為** • WebサイトやSNS等、オフチェーンツールを使った**トークンの盗取**や**ランサムウェア等による犯罪**、**ダークウェブにおける取引の決済**として使用や、**脱税の隠匿等**の行為 • クリーンなアドレスから、経済制裁対象のアドレスへの送金等の行為
Step2	■ **オンチェーン上のロンダリング手法を用いたトークン移転を通じ、トラッキングを遮断する行為** • Mixing/タンブリングサービスや匿名通貨、dappやDeFi等を介在させ、資金を洗浄する行為
Step3	■ **クリーンなアドレスから取引所等に送金し、法定通貨に換金する行為** • AML/CFT規制が緩い国の事業者を使った換金、違法取引であることを知って換金に応じる等の行為

洗浄は、ダークマーケットやMixing等の手法だけではなく、Dappやステーキング等通常のweb3サービスを利用した多様なロンダリングパターンが見られます

流入
洗浄
換金

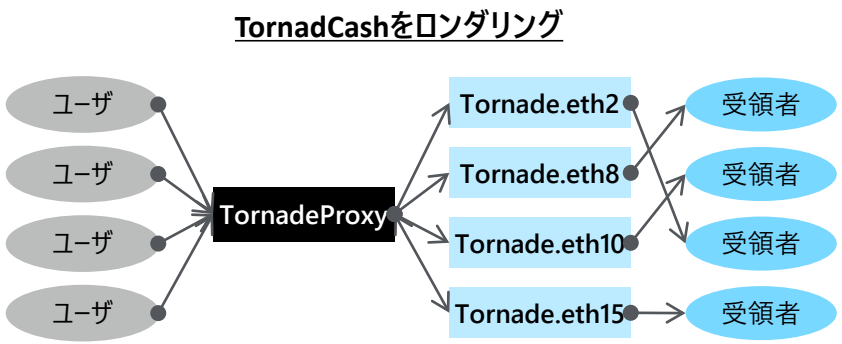
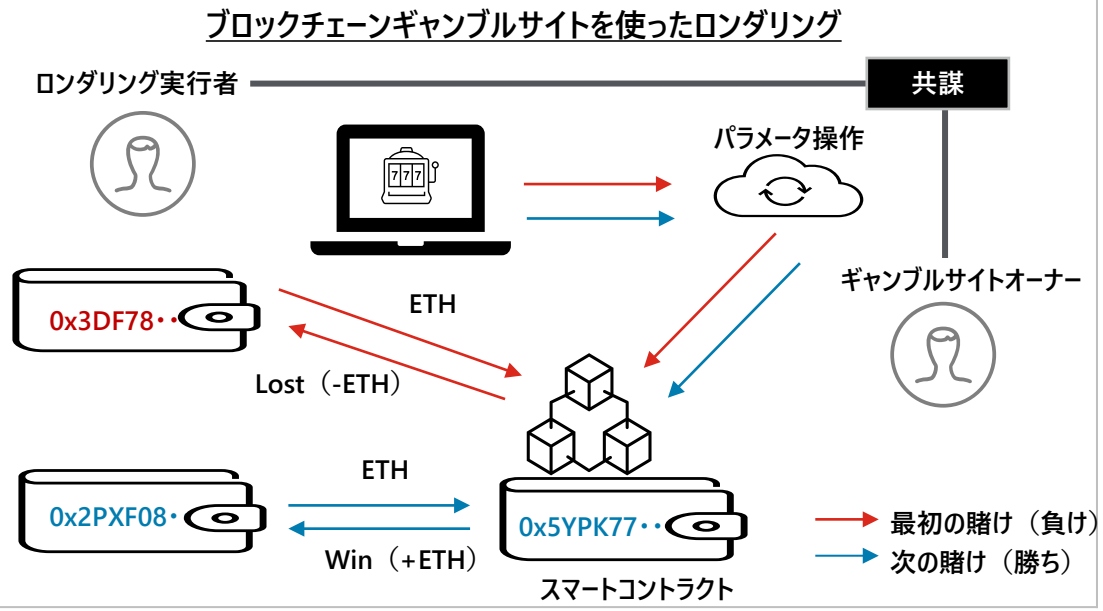
「洗浄」の手法（1/2）

#	タイトル	概要	イメージ
1	**中間ウォレットの使用**	■ 資金を分割し、複数の中間ウォレットを経由して資金を集約する方法 ✓ （例）詐欺グループが被害者に対し、暗号資産を購入するためにある取引所（Exchange 1）を使用するよう指示。その後、詐欺グループが管理する別のウォレットに資金を送金するように指示される。これらの資金を単一のウォレットに集約し、Exchange 2に送付する	
2	**閾値を下回る送金**	■ 疑わしい取引として識別される数量を予め想定し、その閾値をわずかに下回る数量により複数回送金してスクリーニングを回避する方法 ■ FATF は、1,000米ドル/ユーロを超えるトランザクションをトラベルルールの対象とするよう勧告しており、アメリカではこの基準額は3,000米ドル。また、米国銀行秘密保護法（BSA）では、1万ドルを超える現金取引の報告を義務付けている ■ 右のグラフは、2024年の年初来、送金額別に取引所へ移動した資金の価値を示したものだが、1,000ドル、3,000ドル、1万ドルの閾値のすぐ下、あるいはそのすぐ上で送金が著しく急増している	

【参考】：「日本における暗号資産のマネーロンダリング: 日本の視点から見たグローバルの共通問題」（Chainalysis）_2025年3月時点確認

（続き）

「洗浄」の手法（2/2）

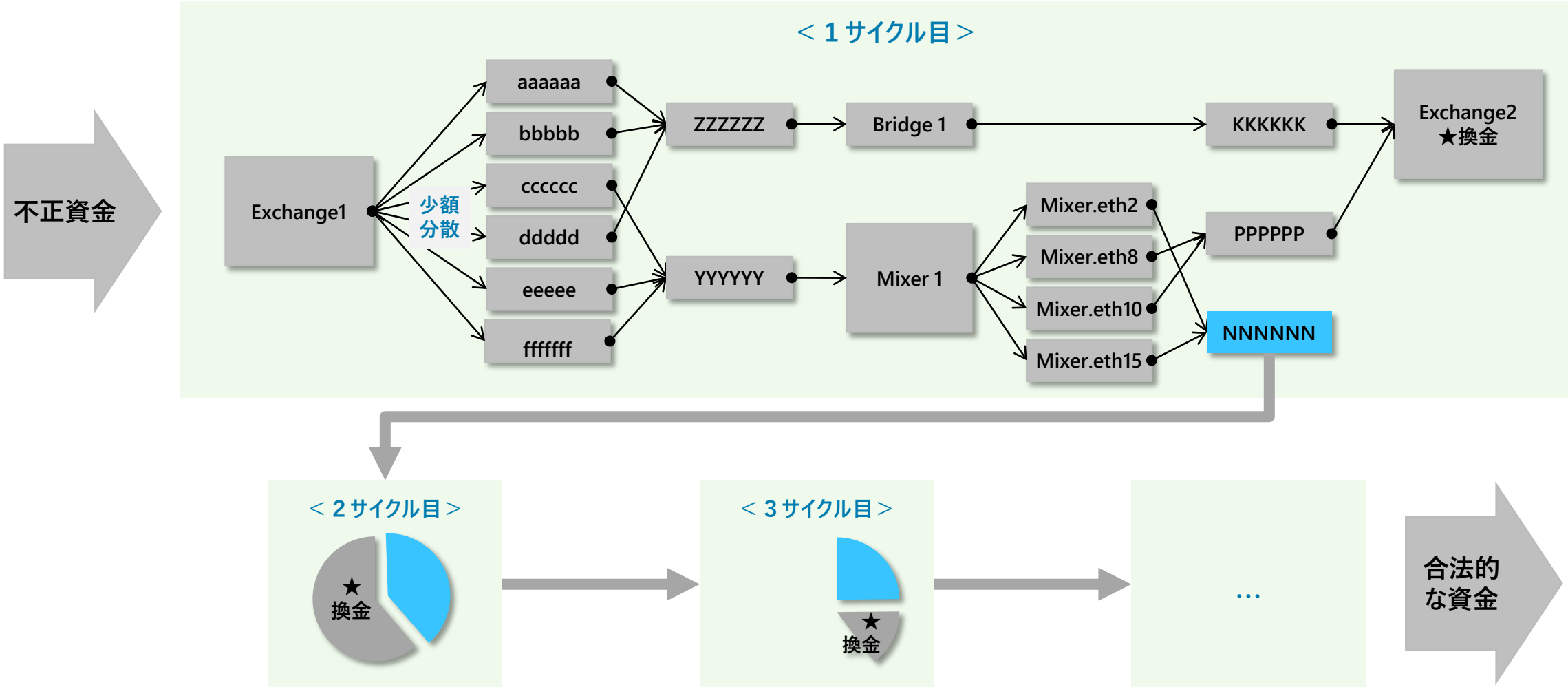
#	タイトル	概要	イメージ
3	**資金経路を複雑にするサービスの使用**	■ トラッキングを遮断する技術やサービスを使った方法 ✓ Mixingサービスの使用 ✓ クロスチェーンブリッジの使用 ✓ プライバシーコイン（Monero、Zcash）の使用	
4	**その他ロンダリング手法（一例）**	■ 以下の通り、様々なサービスや取引形態を駆使する例が認識されており、ロンダリングパターンではこれらを使った可能性を考慮する必要がある （ロンダリングに使用されるサービス・取引形態） ✓ ギャンブルマーケット ✓ ステーキング ✓ ATM ✓ 中間スマートコントラクト ✓ レンディングサービス ✓ シークレットネットワーク ✓ アービトラージ取引 ✓ NFT取引 ✓ ブロックチェーンゲーム ✓ 予測市場　等	

【参考】：「日本における暗号資産のマネーロンダリング: 日本の視点から見たグローバルの共通問題」（Chainalysis）_2025年3月時点確認

実際の犯罪事例では、単一な洗浄手法に頼ることがほぼなく、洗浄手法を組合せ、資金の出所を隠しながら複雑なロンダリング経路で、少しづつ換金することが多い

流入
洗浄
換金

洗浄手法の組合せのイメージ図



※各種ソースを基にデロイトが作成

複数の手法を組合せ、不正資金の洗浄と換金の成功確率をあげることができます

複数の手法を組合せた場合の特徴

洗浄方法の組み合わせを駆使することで、犯罪者が摘発を逃れたり、不正資金の出所を隠したり、一見合法的なルートから現金化することができる。

巨額の資金を洗浄できる

■ 犯罪活動からの巨額の資金を直接取引所や金融システムに移すことは、直ちに注目を集めることになる。資金を体系的に分割し、多くのウォレットに分散させたり、異なるチェーンに移動したりすることで、当局等捜査者が点と点を結びつけて資金の真の出所を特定したり、追跡したりすることを困難にすることができ、全体的に巨額の資金を移動できる

AMLシステムによる検出を回避できる

■ マネーロンダリング対策 (AML) ツールや規制システムは、多くの場合、トランザクション／アカウント単位で、金額や頻度等の閾値を用いて、疑わしい取引にフラグを立てるように設計されているため、使い捨てアカウントで少額で操作することで、AMLシステムによる検出を回避できる可能性がある

洗浄の自動化により迅速かつ大規模に実行できる

■ 自動化ツールとスクリプトの台頭により、不正資金の洗浄を迅速かつ大規模に実行できるようになり、数分以内に数百ものウォレットに資金を移動させること等ができ、当局等捜査者が追いつかないうちに、合法的なルートでの換金まで実行できる

国境を越えた捜査を複雑化できる

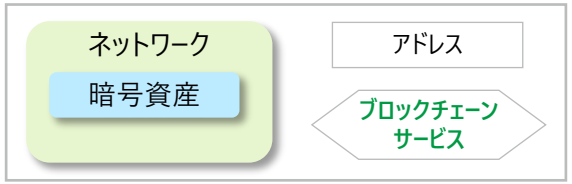
■ 複数の国や地域の法執行機関が効果的に協力することが困難であるため、異なる国や規制の緩い地域の取引所等を利用して送金や換金を操作することで、捜査の進行を妨害できる

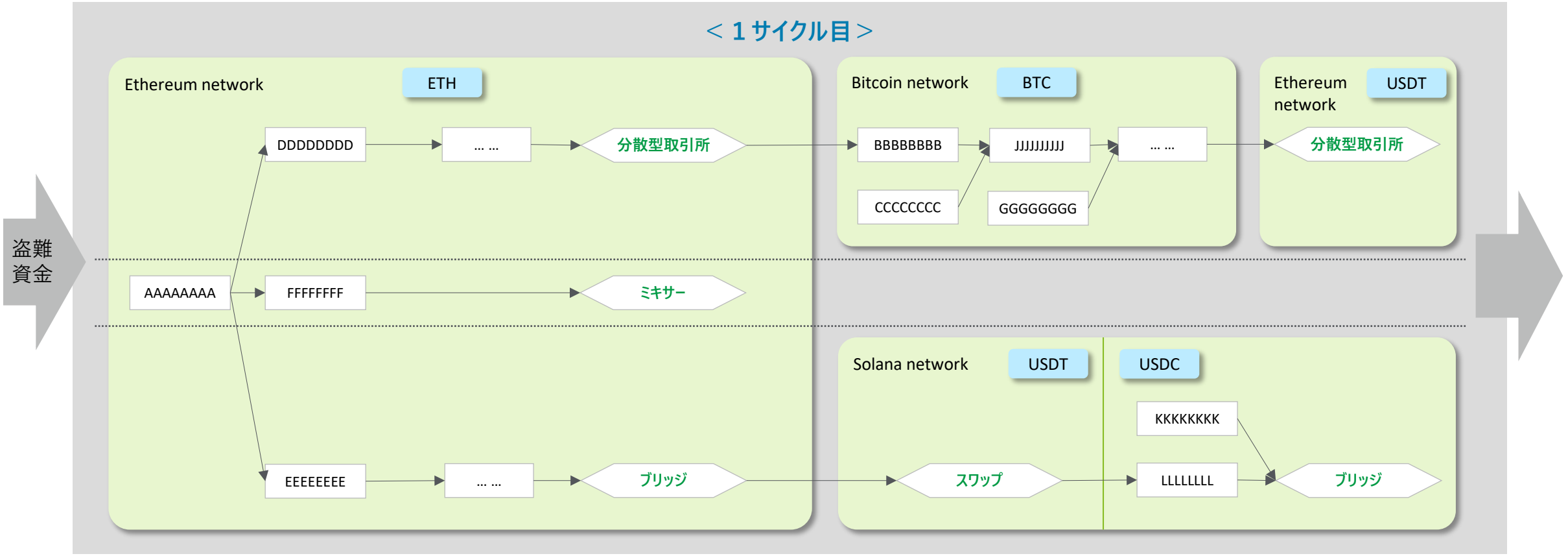
「BingX」ハッキング事案の盗難資金は、複数手法の組合せでロンダリングされました

流入
洗浄
換金

事例：「BingX」ハッキング事案の盗難資金の洗浄経路(1/2)

2024年9月20日、シンガポールの暗号資産取引所BingXは、ホットウォレットへの不正アクセスにより、4,500万ドルの損失を受けた。
盗難された資金はまず体系的に分割され、それぞれ分散型取引所、ミキサー、ブリッジ等サービスを提供するプラットフォームに入金された。
次にそれぞれの経路において、暗号通貨の変換を含め複数のネットワークをわたる洗浄がなされた。



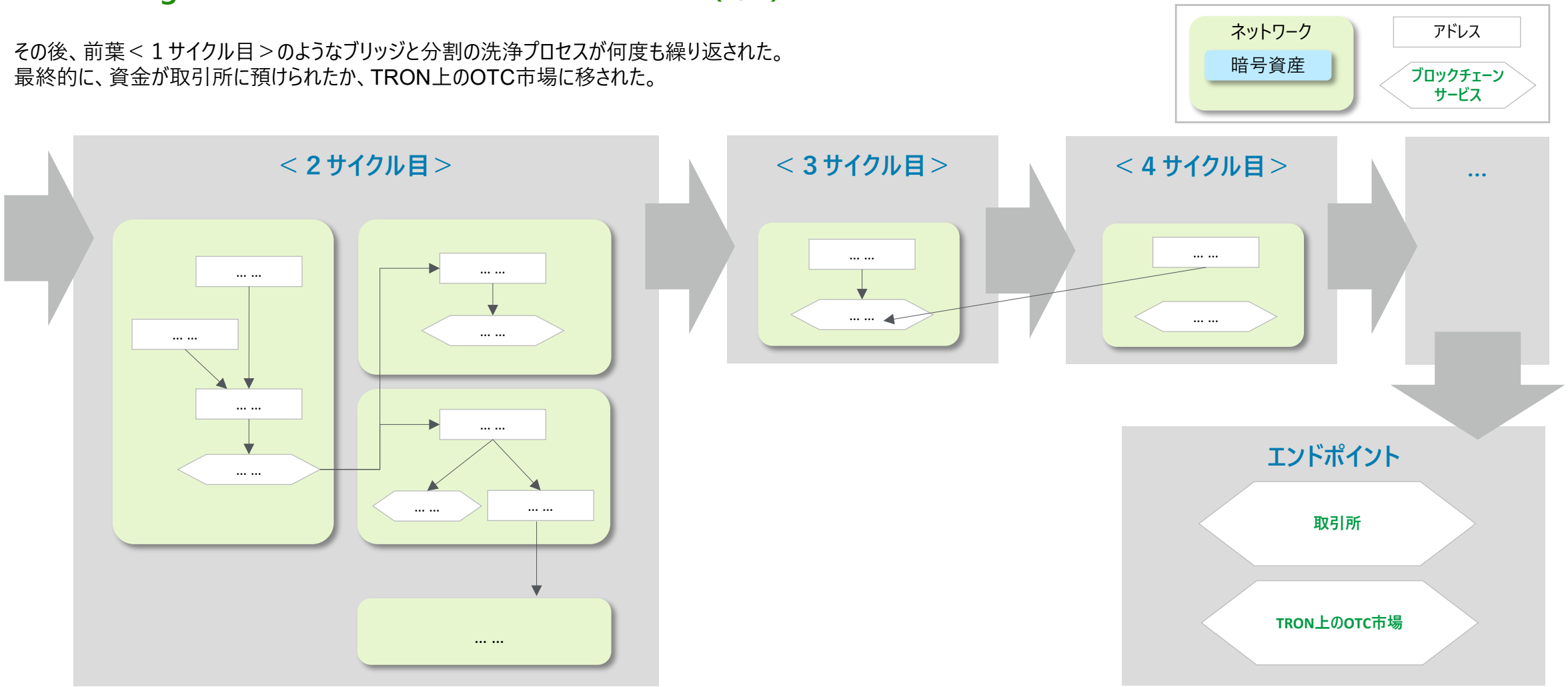


【参考】：「Blockchain Security and Anti-Money Laundering Annual Report 2024」（Slowmist）_2025年3月時点確認

（続き）

事例：「BingX」ハッキング事案の盗難資金の洗浄経路(2/2)

その後、前葉＜１サイクル目＞のようなブリッジと分割の洗浄プロセスが何度も繰り返された。
最終的に、資金が取引所に預けられたか、TRON上のOTC市場に移された。



【参考】：「Blockchain Security and Anti-Money Laundering Annual Report 2024」（Slowmist）_2025年3月時点確認

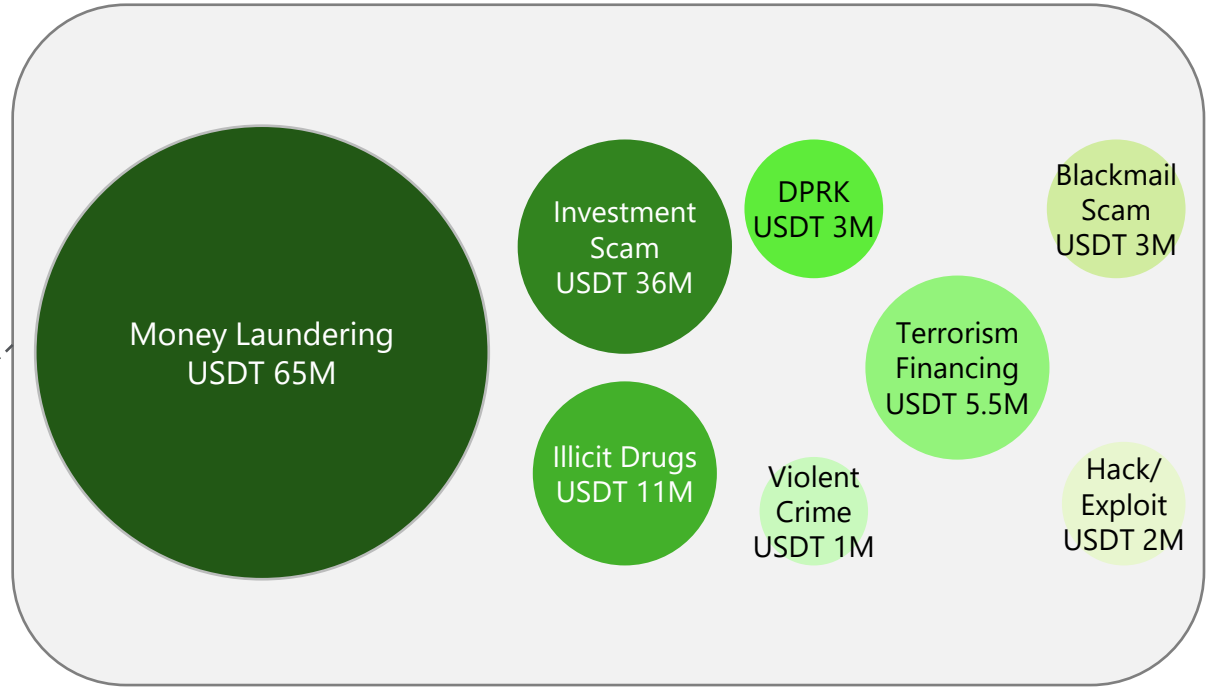
TronとTetherは、分析会社であるTRM Labとともに金融犯罪を防止するための取り組みを公表しています

流入
洗浄
換金

T3 FCUの取り組み

■公表された内容

- 2024年8月、Tether、Tron、TRM Labsが「The T3 Financial Crime Unit (T3 FCU)」を発足
- 犯罪ネットワークの特定と破壊を目的として、世界中の法執行機関と直接協力する、官民連携モデルとしている
- 5大陸にわたり、数百万件の取引を分析し、総額30億米ドルを超える取引量を監視してきたとのこと
- **<u>上記の取り組みの結果、2025年1月に、126百万ドル以上の価値を保有するアドレスを凍結したと発表した</u>**
- 内訳は、マネーロンダリングによるものが最も多く、続いて投資詐欺、違法薬物が続く



T3 FCU担当者

■ T3 FCUは、TRONブロックチェーン上のUSDTの使用に関連する不正利用行為に対抗するために当局とも連携して実施した取り組み

【参考】:「T3 Financial Crime Unit Marks Enforcement Victory: $100 Million in Criminal Assets Frozen Across Five Continents」（Tether）_2025年1月時点確認

Tron上のTetherのスマートコントラクトには特定のアドレスに紐づいた資金を凍結する機能の他に、凍結した資金をバーンする機能（押収）が備わっています

TronにおけるBlacklist機能の概要

- TRON上のUSDTのスマートコントラクトにおける機能
  - AddBlackList

    特定のアドレスをブラックリストとして登録し、資金の移動等の機能を制限する。（イベント名：AddedBlackList）
  - DestroyBlackFunds

    Blacklistとして登録されたアドレスの資金を押収する（トークンの焼却）。（イベント名：DestroyedBlackFunds）
- Tronに実装されたスマートコントラクト

```
12  mapping (address => bool) public isBlackListed;
13
14  function addBlackList (address _evilUser) public onlyOwner {
15      isBlackListed[_evilUser] = true;
16      AddedBlackList(_evilUser);
17  }
```

凍結：コントラクトオーナーによって
特定アドレスをブラックリストへ登録

```
150 function destroyBlackFunds (address _blackListedUser) public onlyOwner {
151     require(isBlackListed[_blackListedUser]);
152     uint dirtyFunds = balanceOf(_blackListedUser);
153     balances[_blackListedUser] = 0;
154     _totalSupply = _totalSupply.sub(dirtyFunds);
155     DestroyedBlackFunds(_blackListedUser, dirtyFunds);
156 }
157
158 event DestroyedBlackFunds(address indexed _blackListedUser, uint _balance);
```

押収：コントラクトオーナーによって
凍結アドレスの資産をゼロにする

【出所】：「Tron上にデプロイされているTetherTokenスマートコントラクトから抜粋」（TronScan ）_2025年1月時点確認

Tron-USDTに関し、オンチェーンデータで凍結・押収金額を集計したところ、4.2億ドル相当にのぼりました

流入
洗浄
換金

Tron-USDTにかかる凍結・押収の追加調査

■ **目的**

- T3FCU発足以後（2024/9/1~2025/1/1）を対象に、**TronにおけるUSDTの凍結・押収の規模を、実際のオンチェーンデータを使って集計**する

■ **方法**

- Dune Analyticsで以下のスクリプトを走らせ、Tron上のUSDTのコントラクトで凍結アドレスを取得する

```
SELECT
  block_number,
  block_time as ban_time,
  substring(topic1 from 13) as banned_address,
  tx_hash
FROM tron.logs
WHERE
  contract_address = 0xa614f803b6fd780986a42c78ec9c7f77e6ded13c
  AND topic0 = 0x42e160154868087d6bfdc0ca23d96a1c1cfa32f1b72ba9ba27b69b98a0d819dc
ORDER BY ban_time DESC
```

1,873件の凍結に関するトランザクションが取得できた
（過去凍結した全ての件数）

- Tronのエクスプローラを使用して、上記の凍結アドレスのうち、**2024年9月以降に凍結されたアドレスにかかる保有残高を取得したところ584件が検出された**
- Dune Analyticsでスクリプトを走らせ、押収した金額を取得した

■ **結果**

- 4億2200万USDT以上の凍結・押収があった事が確認出来た。T3FCUによる公表額を大幅に超える金額であったが、同取り組みにより凍結・押収はこの中に含まれているものと推察される

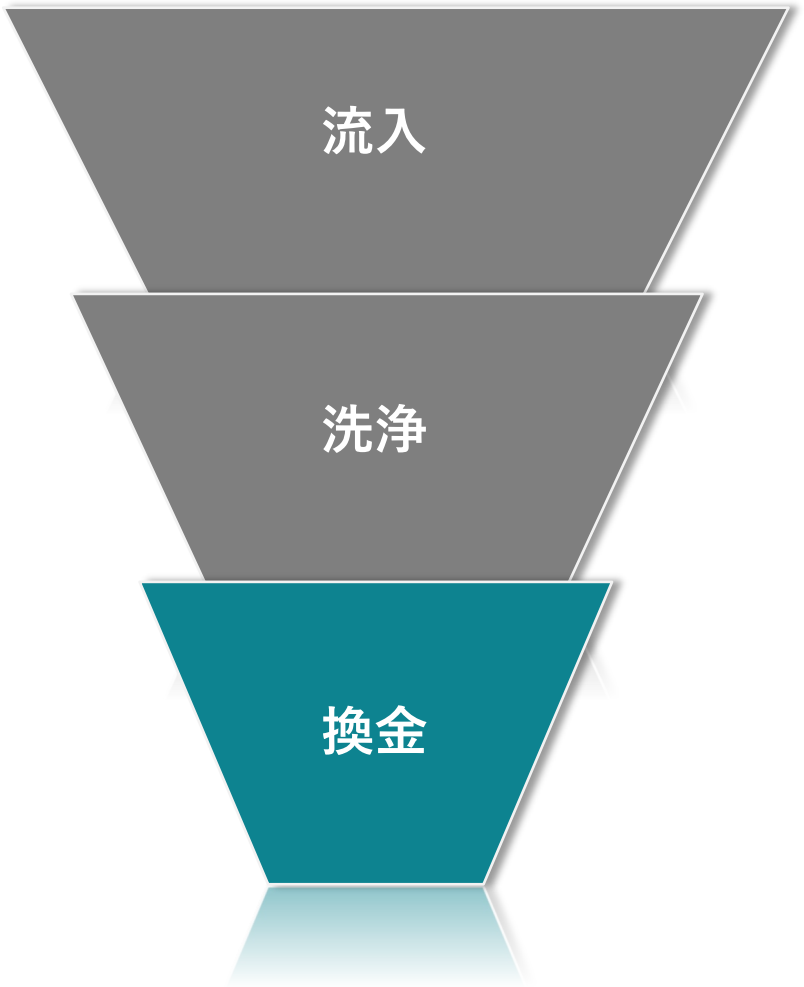
#	区分	金額($)
1	凍結（584件）	376,581,916
2	押収（27件）	45,961,720
合計		422,543,636

【出所】：「Dune Analytics、Tronエクスプローラ」_2025年1月時点確認

2. 主要なステーブルコインの利用状況・不正利用事例の調査
2.5 不正利用の段階別分類とその手口（換金）

換金は、クリーンなアドレスから取引所に送金し、法定通貨に換金する行為であり、次頁以降でその手口等の調査結果を取り纏めました

不正利用の段階別分類



	概要
Step1	■ **盗難、詐欺等の犯罪が発生し、ブロックチェーン上の特定のアドレスにトークンを集める行為** • WebサイトやSNS等、オフチェーンツールを使った**トークンの盗取**や**ランサムウェア等による犯罪**、**ダークウェブにおける取引の決済**として使用や、**脱税の隠匿等**の行為 • クリーンなアドレスから、経済制裁対象のアドレスへの送金等の行為
Step2	■ **オンチェーン上のロンダリング手法を用いたトークン移転を通じ、トラッキングを遮断する行為** • Mixing/タンブリングサービスや匿名通貨、dappやDeFi等を介在させ、資金を洗浄する行為
Step3	■ **クリーンなアドレスから取引所等に送金し、法定通貨に換金する行為** • AML/CFT規制が緩い国の事業者を使った換金、違法取引であることを知って換金に応じる等の行為

換金では、フィアットにオフランピングできる方法がいくつかあり、暗号資産取引所は最も使われていますが、今後決済に使う形で換金する可能性も高まると考えられます

流入
洗浄
換金

犯罪者によく使われる換金ルート

マネーロンダリングの最後のステップは、一見合法的なルートでフィアットへ換金して（オフ・ランプ）逃げることである。

■ 取引所

- 暗号資産取引所は、フィアットと暗号資産の間の重要なゲートウェイとして機能している。犯罪者は、銀行口座等と結び付けられる点をメリットとし、フィアットに引出す一歩前のロンダリング・エンドポイントとして、取引所をよく利用している。
- 規制されている取引所のKYC/CDDプロセスを突破したり、規制されていない取引所や規制が緩い国・地域にある取引所を利用したりして、過去事案では、犯罪者が最終的に取引所からフィアットへの換金に成功したケースが少なくない。

■ 商品の購入

- ダークネット・マーケットなどで、商品を購入して転売することで、本来の犯罪と関係のない資金を生み出せるため、不正資金の出口として便利である。
- 高級品、ギフトカード、電子機器など転売が容易なものから、住宅、車両、美術品、時計、宝石など高価値なものまで、犯罪者に狙われている。
- 今後、決済手段としてステーブルコインが普及することにより、犯罪者が合法な店舗で商品を購入して転売することで、換金する可能性が高まる。

■ DeFi

- DeFi関連規制の未整備などにより、KYCプロセスがないプラットフォームが多い。犯罪者はここで資金を担保に使ったりして、合法的な資金に転換できる。

■ 暗号資産ATM

- フィアットと暗号資産との双方向交換ができる暗号資産ATMで、直接フィアットを引出せる利便さがある。

■ KYC不要なウォレット

- ノンカストディアル・ウォレットなどサービスはKYC不要なケースが多いため、最終換金時の送金・決済のチャネルとして悪用される可能性がある。

■ その他プラットフォーム

- P2Pプラットフォームやギャンブリングサービスを経由して、合法的な資金に転換して換金することもある。

…

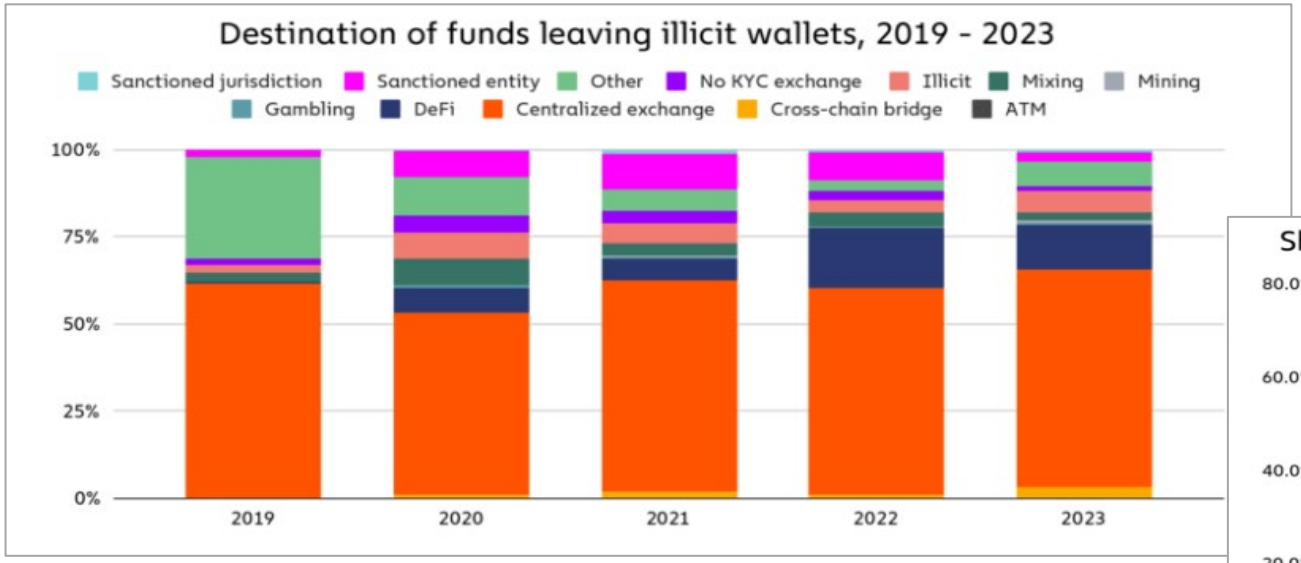
中央型取引所は違法資金の主要な送金先となり、犯罪者がオフ・ランプ・サービスを選択するとき大手プラットフォームを好む傾向があるとされております

流入
洗浄
換金

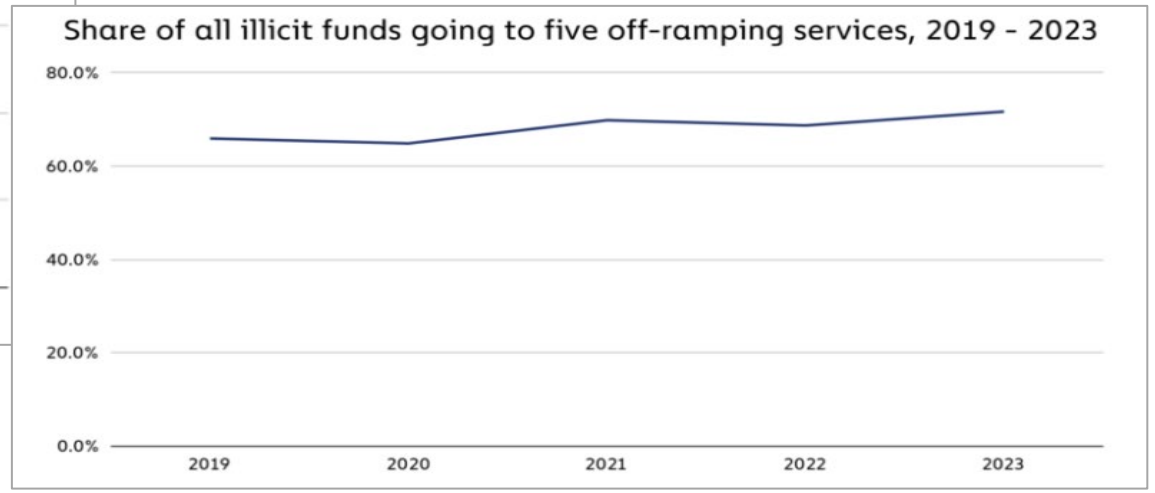
オフ・ランプ・サービスの集中度が高い

全体として、中央型取引所が違法資金の主要な送金先となり、その割合は過去5年間安定して推移。**2023年、オフ・ランプ・サービスに送金された違法資金のうち、約71%が5つのサービスに集中**している。

2019年～2023年 違法資金の送金先別取引量



2019年～2023年 上位５つオフ・ランプ・サービス宛送金が占める割合



【参考】:「Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group」（Chainalysis, 2024年2月）_2025年3月時点

流入
洗浄
換金

暗号資産取引所における不正な換金には、多様な手口が存在します

取引所の種類別の不正手口

非正規

無登録の取引所

■ ライセンス未取得の取引所は、ユーザにKYCまたはCDDを実施しないことが多く、犯罪者は実質的に匿名で活動できる

■ また、一部は、**取引所自体が犯罪組織により運営されており**、意図的に違法行為を助長している場合もある

高リスク国・地域にある取引所

■ **以下の国・地域で運営している取引所が犯罪者に利用される**傾向がある

- AML/CTFリスクが一般的に高い国・地域
- 制裁や禁輸等の制約を受けている国
- FATF「高リスク・非協力国リスト」に記載の国
- 暗号資産に関するAML/CTF規制がない国

【違法OTCブローカーを介した手口】

■ OTCブローカーは、取引所で利用可能な価格よりも低い価格で、流動性供給者間の大規模な取引を促進できるように機能している。これら大口取引は違法資金の便利な隠れ蓑となっている

■ 違法なOTCブローカーは、**非正規な取引所で数多くのネスト化されたアカウントを維持**することで、身を隠して活動できる。また、これらOTCブローカーが、KYC不要でユーザに暗号通貨からフィアットへのスワップ・サービスを提供することもあり、マネーロンダリングを完成できる

正規

登録済の取引所

■ 合法的な取引所は犯罪者にとって、**クリーンなコインを新たに入手できることと、違法資金をフィアットに換金できること**で、二重のメリットをもたらす

【偽情報でKYCを通す手口】

■ 犯罪者は**ダーク・ウェブで購入したKYCキット**（多くの場合、氏名/生年月日/住所/顔写真付ID等情報がセット）を利用して正規な取引所のKYC手続きに対応し、アカウント開設に成功する

【マネー・ミュールを操る手口】

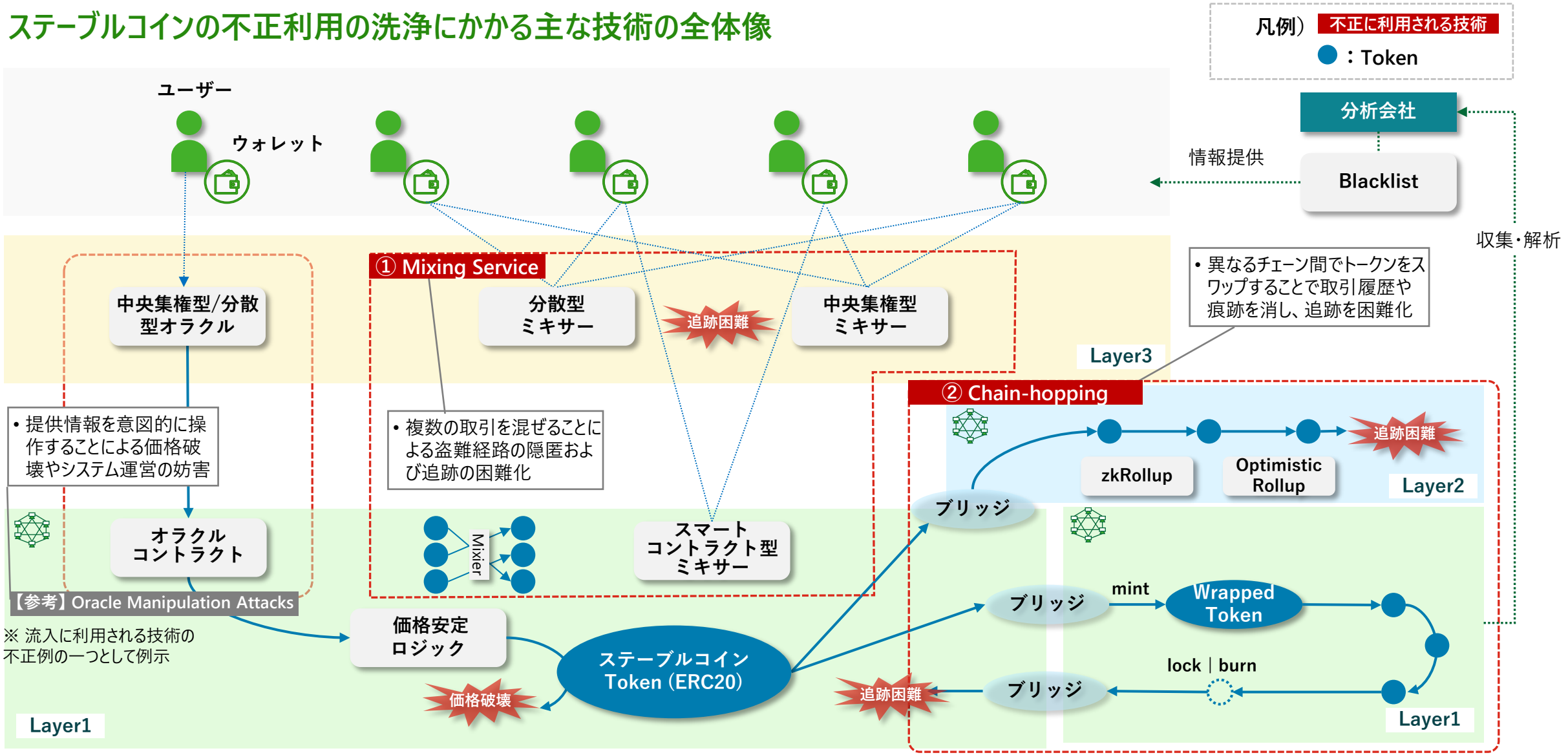
■ 犯罪者は偽アルバイト情報等撒いて大学生等を騙して、**騙された人（マネー・ミュール）は自分の情報で正規な取引所でアカウントを開設**して、犯罪者からの指示のもと資金移動や換金を実施する

【参考】：「Elliptic Typologies Report 2024 - Preventing Financial Crime in Cryptoassets : Identifying Evolving Criminal Behavior」（Elliptic ）_2025年3月時点

2. 主要なステーブルコインの利用状況・不正利用事例の調査
2.6 技術的特性のトレンドと対策

洗浄に使われる技術には盗難経路を隠蔽するMixingや複数チェーンをまたぐChain-hopping等があります

ステーブルコインの不正利用の洗浄にかかる主な技術の全体像



盗難経路を隠蔽するMixingや複数チェーンをまたぐChain-hopping等に対して、犯罪の追跡や未然防止のため発行者・分析会社との更なる協力体制が課題です

ステーブルコインの不正利用において洗浄にかかる主な技術と対応の方向性

#	不正に利用される技術	対応の方向性	残課題	関連プロトコル
①	■ ステーブルコインとMixingサービスを活用した盗難経路の隠蔽 ➢ ステーブルコインをMixingサービス経由で複数ユーザーのトランザクションと混ぜ合わせ、別アドレスに払い出し → 別口座や別チェーンへ移動、という流れで盗難経路を隠蔽する	■ Mixingサービスを行う業者のアドレスやスマートコントラクトを制裁リストに追加し、送金時にチェックする 【ステークホルダー別の対処案】 • 発行者 監視・追跡・検閲機能の実装、Mixingサービスの規制 • サービス事業者/ユーザー 分析会社が提供する疑わしい取引先、制裁リストのチェック、ウォレットからの注意喚起	■ 疑わしい取引先および制裁リストチェックを如何に強制させるか ■ 方式によって通常の取引と判別できない不正取引手法（Coinjoin等）の分析・抽出方法の確立	• 中央集権型ミキサー(Blender.io等) • 分散型ミキサー(Coinjoin等) • スマートコントラクト型ミキサー(Tornado Cash等)
②	■ Chain-hoppingを活用したLayer2等の異なるチェーンを経由したステーブルコインの洗浄 ➢ 盗難コインを短時間で連続して複数のチェーンにブリッジ し、チェーンごとに異なるウォレットを使う等、追跡を困難にさせる。最終的に暗号資産取引所やOTC・P2P取引で法定通貨に換金する ➢ スケーラビリティ向上や手数料削減を目的としたLayer2（L2）において、通貨をブリッジしてL2側で転々 流通させることで、追跡困難にしている	■ 複数のブロックチェーンを跨いだクロスチェーンの取引情報をグラフ化するブロックチェーン分析ツールを使い追跡する 【ステークホルダー別の対処案】 • 発行者 監視・追跡・検閲機能の実装、分析ツールの提供 • サービス事業者/ユーザー 分析会社にてチェーン間取引を監視し、追跡不能な取引の振る舞いや前後関係から怪しい動きをAI等で抽出する等のより高度な分析ツールやコードの提供（Blockaidサービス等）	■ 複数のチェーンやレイヤを跨ぐことで、追跡が困難になるため、相互連携を考慮した分析ツールの改善が必要 ■ ブリッジの手法が複数あることから、各ステークホルダーにとって、最適な実装形態なのか検討する必要がある	• Optimistic Rollup • ZK Rollup • Wrapped Tokens • Cosmos/Polkadot • Inter-Blockchain Communication • Cross-Chain Transfer Protocol (CCTP)

（続き）

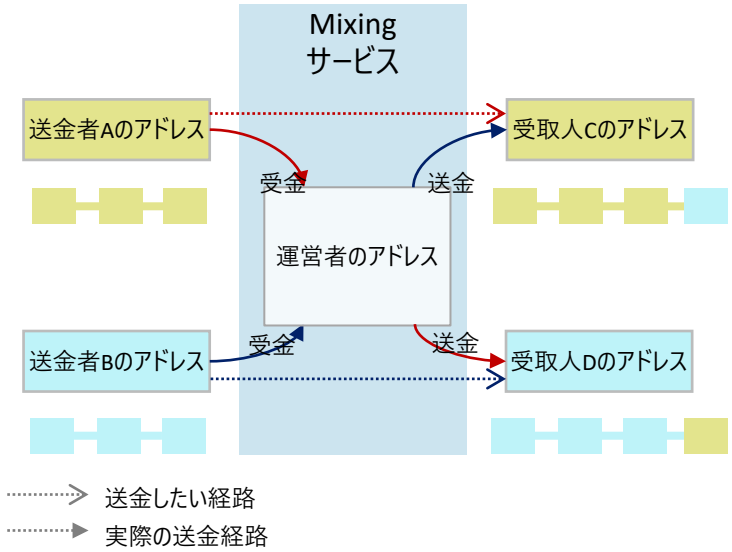
【参考】ステーブルコインの不正利用において流入にかかる主な技術と対応の方向性

#	不正に利用される技術	対応の方向性	残課題	関連プロトコル
参考	■ Oracle Manipulation Attacksを活用したオラクルデータ操作を通じたステーブルコインの価格操作 ➢ オラクルデータとDappsの組合せによりを操作して偽の情報の送信や、市場操作、プロトコルの運営を妨げ、ステーブルコインの価格を変動させる ➢ 主にフラッシュローン攻撃や暗号通貨を担保としたアルゴリズム型ステーブルコインの価格操作・アービトラージに使用される	■ 複数のデータソースから情報を収集し、合意形成で検証する分散型オラクルにより検閲性と耐改ざん性を高める 【ステークホルダー別の対処案】 • 発行者/ユーザー – • サービス事業者 中央集権型オラクルの規制と分散型オラクル導入	■ 合意形成による更新の遅延や、複数データソースの整合性担保、システムの複雑性の回避 ■ 発行者やユーザーでは検知・対策が困難なため、オラクルを運営するコミュニティや仲介業者の規制や監視が必要	• 中央集権型オラクル • 分散型オラクル

Mixingサービスは運営者が仲介していた中央集権型ミキサーからプロトコルレベルで隠蔽する方式やゼロ知識証明等他技術と組合せる方式が増えてきています

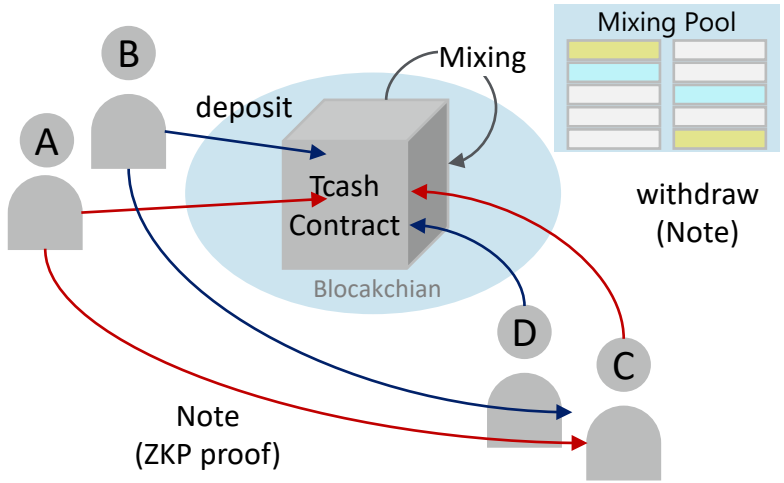
Mixingサービス

中央集権型ミキサー（Blender.io）



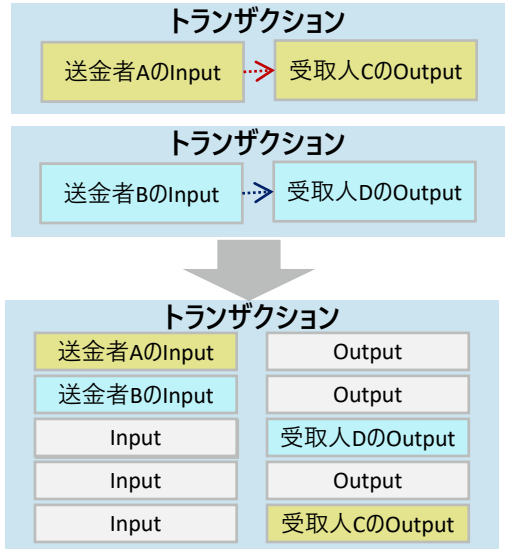
■ **集中型のMixingサービス**
- 複数ユーザからの送金された資金を運営者のプールで混ぜ合わせて別の宛先のアドレスに資金を送金することで、送金元と送金先の関係性を断ち、追跡を困難にする。

スマートコントラクト型ミキサー（ Tornado Cash）



■ **スマートコントラクトを利用したMixingサービス**
- ゼロ知識証明（ZKP）を活用し、送受信者のアドレスを秘匿
- ユーザは資金をスマートコントラクトにデポジットし、ZKPのProofを含む秘密のノートを作成し、任意のアドレスに送る
- デポジットした段階で資金はMixingプールに追加され、他の取引と混ぜ合わせるため追跡が困難となる

分散型ミキサー（Coinjoin）



■ **分散型のMixingサービス**
- UTXOの仕組みを用いて、ランダムで選ばれた他ユーザの取引（input）を混ぜ合わせ、一つのトランザクションに集約することで、送信先を特定困難にする手法

■ 中央集権型のミキサーやスマートコントラクト型のミキサーはサービス提供者を**ウォレットアドレスまたはスマートコントラクトアドレスから特定可能**

■ Mixingされた取引の追跡は困難なものの、資金洗浄されている可能性のある取引・アドレスは特定可能（正常ユーザーと不正ユーザーを識別・分離できる）

■ Coinjoin等の分散型ミキサーは基本的なプロトコルに従って実現されており、他の取引と区別がつかないため、**同一トランザクション内の入力として使用される公開鍵は全て同一ユーザとする従来型のヒューリスティック分析では解析不可能**

■ 従って、トランザクションを入力・出力単位に分解し、それぞれの取引の流れから不正取引の可能性をAI等を用いて推定する等のより高度な方法論が必要

複数のチェーンをまたいでトークンを移転させることで洗浄を行う方法はチェーン・ホッピングと呼ばれ、不正利用でよく使われる手法となっています

Chain-Hopping

■ **Chain-Hopping**は近年犯罪者によく使われる資金洗浄手法の一つ。**クロスチェーン・ブリッジやラップド・トークン**を通じて主要なブロックチェーンが相互運用性が高まり、利便性と追跡困難性の面から犯罪者にとってのメリットが大きい。このような資金洗浄を調査するには、複数のブロックチェーンを追跡する必要があり、クロスチェーンの動きをグラフ化するためにブロックチェーン分析ツールが使われることも多い。*1

代表的なクロスチェーン・ブリッジのメカニズム *2

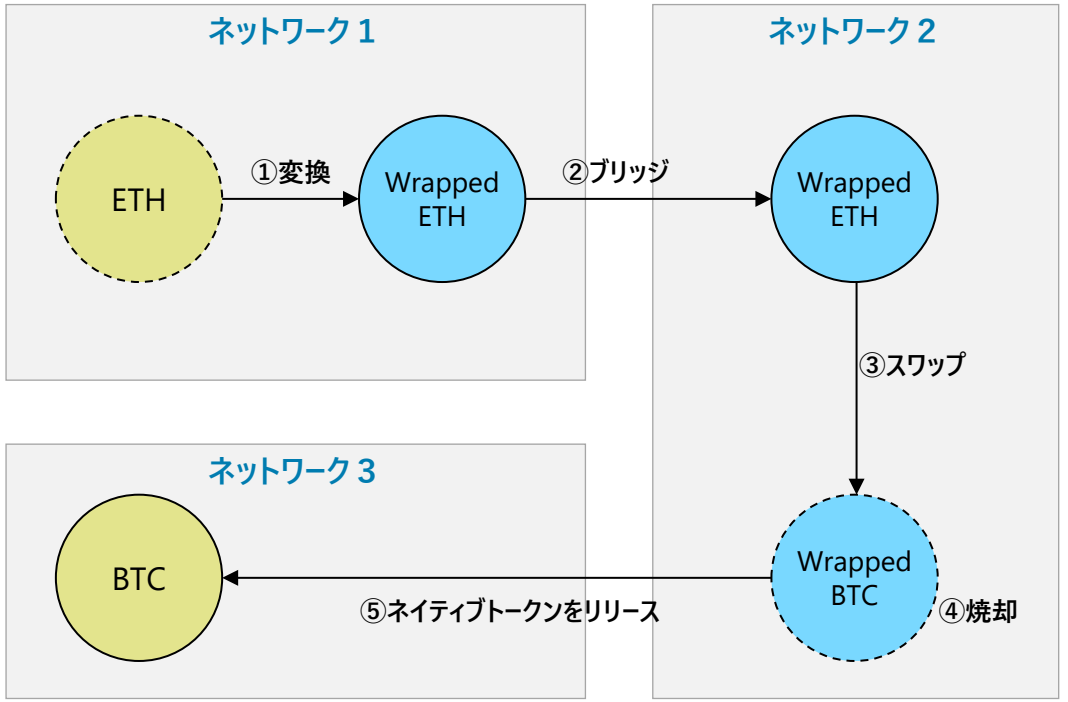
■ ロック・アンド・ミント (Lock and mint)
- 送信元チェーンのスマートコントラクトでコインをロックし、ロックされたコインに見合ったコインが、IOUの形式として送信先チェーンでミントされる。逆方向では、送信先チェーン上のラップド・トークンをバーンし、送信元チェーン上の元のコインのロックを解除する

■ バーン・アンド・ミント (Burn and mint)
- 送信元チェーンでコインをバーンし、送信先チェーンで同じもののネイティブトークンを再発行 （ミント）する

■ ロック・アンド・アンロック (Lock and unlock)
- 送信元チェーン上のコインをロックし、送信先チェーン上の流動性プールから同じもののネイティブトークンをロック解除する。このタイプのクロスチェーン・ブリッジは通常、収益分配等の経済的インセンティブを通じて、ブリッジの両側に流動性を呼び込む

■ その他
- 任意データメッセージング機能と組み合わせたProgrammable token bridgesは、ブリッジされたトランザクションで、送信先チェーン上のスマートコントラクトを用いてトークンのスワップ、貸出、ステーキングや換金を実施する等、より複雑な機能を提供する

ラップド・トークンを介したチェーン・ホッピングのプロセス例 *3



【参考】：*1「Money Laundering in Crypto: How Criminals Hide Their Tracks」（MERKLE SCIENCE ）_2025年3月時点
*2「What Is A Cross Chain Bridge? 」（Chainlink ）_2025年3月時点
*3「Chain Hopping in Crypto: How to Track Cross-Blockchain Fund Movement」（Medium ）_2025年3月時点

ステーブルコインや暗号資産において、プライバシー保護とAML/CFTに対する監視要件を両立する目的として新たな仕様・プロトコルが検討されています

【参考】AML/CFT対策として検討されている技術

- ステーブルコインや暗号資産において**合法的なユーザーと不正なユーザーを識別し、合法的なグループから不正なユーザーを排除する技術も登場**しつつある
- 従来ではプライバシー保護に特に焦点が置かれ、利用者の取引履歴や残高が第三者から隠蔽することが中心であったが、**不正行為を監視し、非合法なユーザーをコミュニティから排除することとプライバシー保護と両立させることでより安全性と信頼性の高いプラットフォームの実現に向けた技術が検討されている**
- 合法と非合法の境界判断、信頼機関の判定基準は、過去実績による推定であることから、まだいくつか課題があるが実用化への期待は高まっている

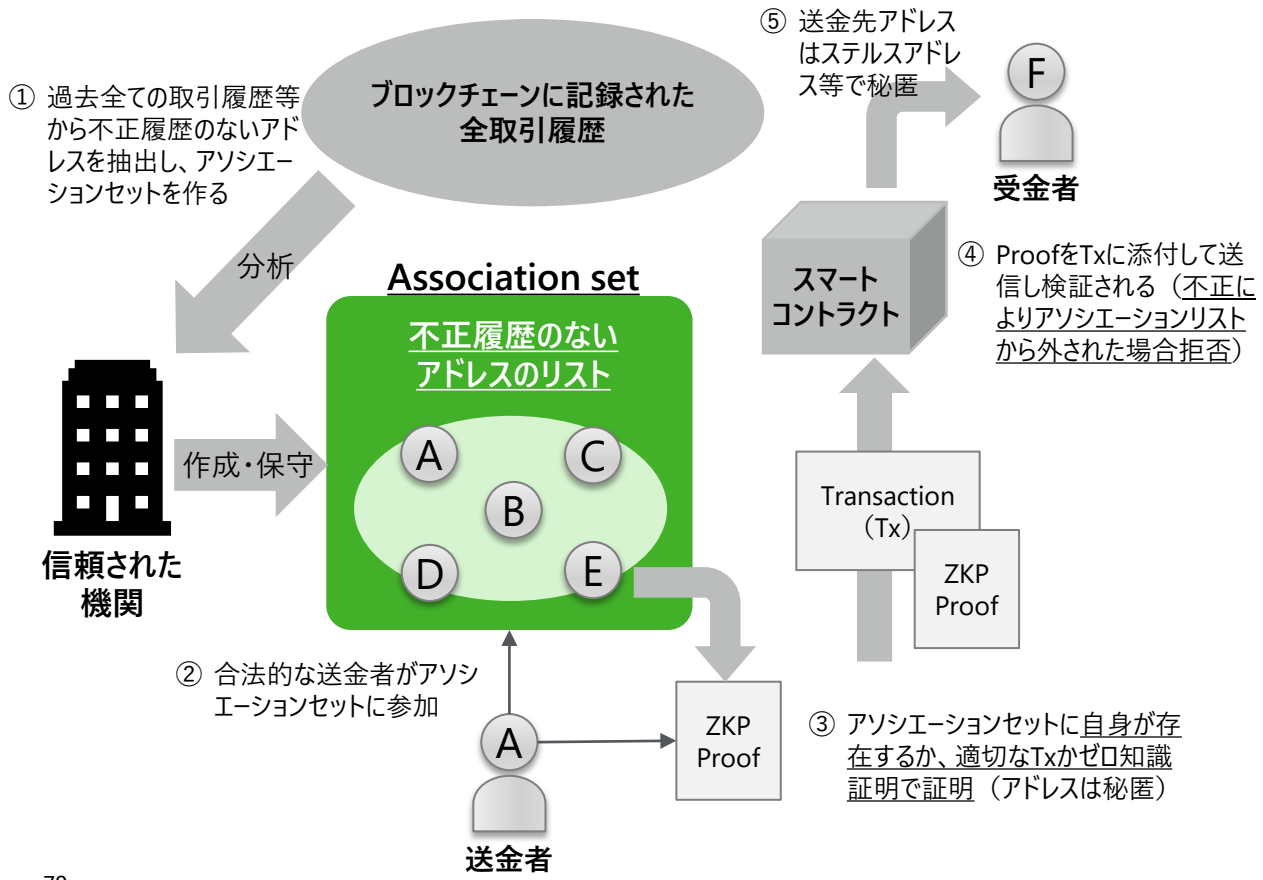
#	技術	概要	ステーブルコインにおける活用	残課題
①	**プライバシープール**	■ **合法的なユーザーと不正なユーザーを分離するためにゼロ知識証明を使用したスマートコントラクトベースのプライバシー強化プロトコル** • Tornado Cash等のMixingサービスにAML/CFTが導入可能なことを示唆	➢ 送金者と受取人が悪意を持っていない・潔白であることを証明 ➢ ユーザーは**自分の全取引履歴を公開することなく、規制に準拠していることを証明**できる	• 合法であることの証明のために、他ユーザーが他者の取引情報を公開することで、結果他者のプライバシーが侵害される可能性 • 悪意あるプロバイダーがユーザー情報入手のためアソシエーションセットを構築する可能性（信頼された機関の判定基準） • 不正履歴のないアドレスを抽出するための判断ロジックの確立 • FATFや規制当局との合意形成
②	**アカウンタブルウォレット**	■ **ウォレット保有者のプライバシーを守りつつ、不正行為に関与していないことを証明できる仕組み** • ゼロ知識証明による取引の正当性証明や制裁リストとの突合、分散型オラクルによる監視と不正アドレスの報告	➢ **ウォレットの所有者の正当性、ウォレットの過去の行動の正当性、および暗号資産の出所の正当性の3つの側面を評価** ➢ 参加者が取引相手の信頼性を確認し、違法な活動を防ぐことが可能となる	• 取引相手の正当性検証にかかるコストの最小化 • 信用スコア算出ロジックの確立（高度なチェーン分析や取引詳細の手動収集等） • 証明書発行機関の採用基準や証明書発行時の判断基準 • FATFや規制当局との合意形成

【参考】：*1「https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364」_2025年3月時点
*2「https://drive.google.com/drive/folders/1wOoJNpeTvJ1VEPoJXgDUZ8ebysn0efWK」_2025年3月時点

Privacy Poolsはコンプライアンスを目的としたユーザーが、違法な資金・アドレスと自らを切り離すことを目的とした送金システムです

【参考】Privacy Pools

- Mixingサービスである Tornado Cashは、どのウォレットアドレスからどのウォレットアドレスへ送金したかを隠蔽でき、一般ユーザーによる利用と「望ましくない個人や集団」による資金洗浄とを明確に識別するのは非常に困難である
- **Privacy Poolsは、利用者のプライバシーを保護しつつ、過去の取引において不正な資金に関与していないことを証明する仕組みである**



Tornado Cashとの比較

項目	Privacy Pools	Tornado Cash
目的	• プライバシー保護 + コンプライアンス対応	• 完全なプライバシーの提供
匿名化の仕組み	• アソシエーションセットを利用し、クリーンなトランザクションのみを許容	• すべてのユーザーのトランザクションをMixing
ゼロ知識証明（ZKP）	• クリーンな取引履歴を証明するために使用	• 「送信者と受信者の関係を隠す」ために使用
不正取引の排除	• 可能(アソシエーションセットの保守・管理で対応)	• 不可能（誰でも利用可能）
規制対応	• 規制に対応しやすい（取引所、当局と協調）	• 規制対応なし（OFAC制裁対象）

実用化に向けた課題

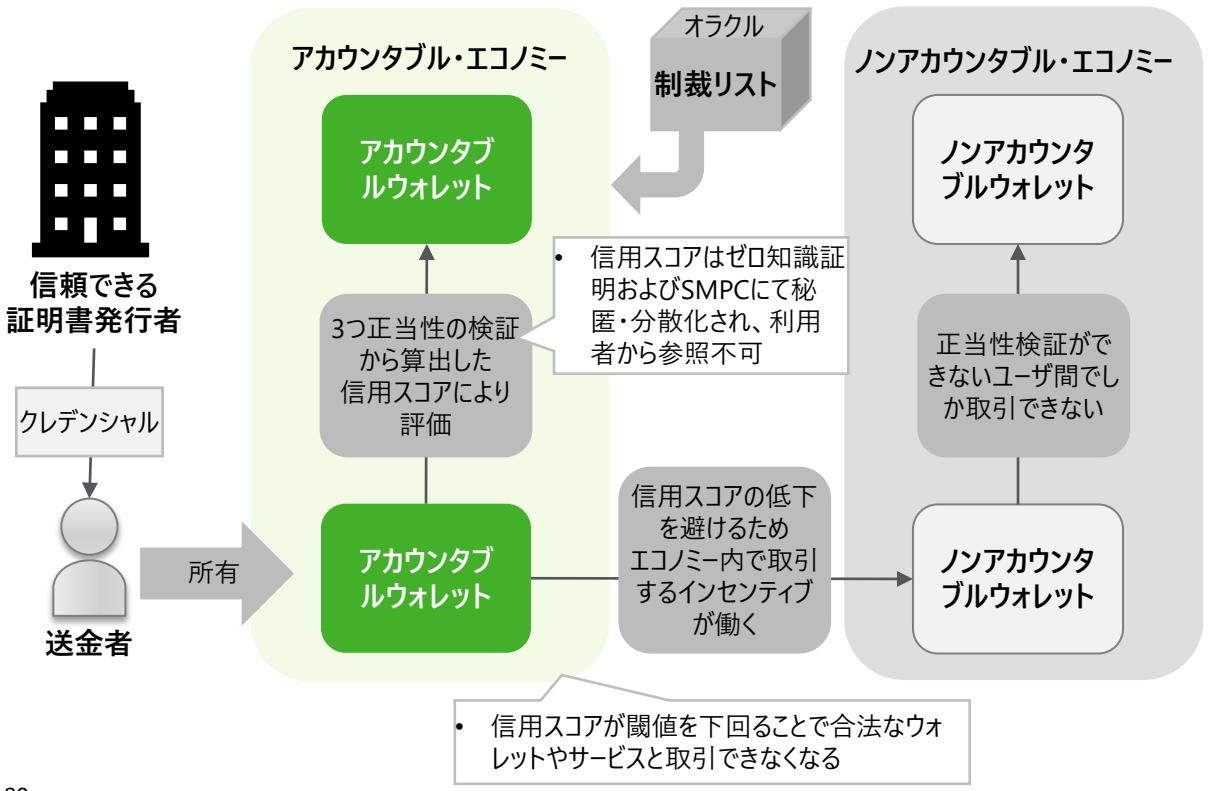
- 合法であることの証明のために、他ユーザーが他者の取引情報を公開することで、結果他者のプライバシーが侵害される可能性
- 悪意あるプロバイダーがユーザー情報入手のためアソシエーションセットを構築する可能性（信頼された機関の判定基準）
- 不正履歴のないアドレスを抽出するための判断ロジックの確立

Accountable Walletはウォレットの正当性を複数の観点から算出した信用スコアにより、取引範囲を決め、安全性の高い経済圏（アカウンタブルエコノミー）を確立する仕組みです

【参考】Accountable Wallet

- 取引の正当性を評価するための明確な基準を定義し、分散型金融（DeFi）における取引の安全性、透明性、コンプライアンスを確保するための包括的なアプローチを提供している
- 具体的には、取引の正当性を評価として、ウォレット保有者の正当性、ウォレットの過去の行動の正当性、暗号資産の出所の正当性の3つの側面による信用スコアにより取引範囲を決め、安全性の高い経済圏を確立することを目的としている

アカウンタブル・フレームワーク



ウォレットにおける3つの正当性検証

- **所有者の正当性**
  - ウォレット所有者が反社会的勢力や制裁対象者でないことを示す証明。これには、信頼できる証明書発行者によって発行され、デジタル署名された、ウォレット所有者の個人情報に基づく証明書（クレデンシャル）が含まれる
- **過去の行動の正当性**
  - ウォレットが過去に違法行為に関与していないことを示す証明が必要となる。ウォレットが制裁リストや暗号資産ウォッチリストに登録されていないことを証明する非メンバーシップ証明が含まれる
- **暗号資産の出所の正当性**
  - ウォレットが過去に違法に取得された暗号資産を受け取っていないことを示す証明が必要。受け取った暗号資産の送信元が正当であることを示すチェーン証明書が含まれ、これらの証明書は、過去の取引履歴に基づいて生成される

実用化に向けた課題

- 取引相手の正当性検証にかかるコストの最小化
- 信用スコア算出ロジックの確立
  （高度なチェーン分析や取引詳細の手動収集等）
- 証明書発行機関の採用基準や証明書発行時の判断基準

3.主要なステーブルコイン発行者の事業実態調査
3.1 発行者概要（USDT・USDC）

Tether社は、2022年以降も大幅に時価総額が伸長しているが、MiCAへの対応から欧州CEXでのUSDTの取り扱いが停止される等規制対応で課題が見られます

USDTの概要と主なアップデート

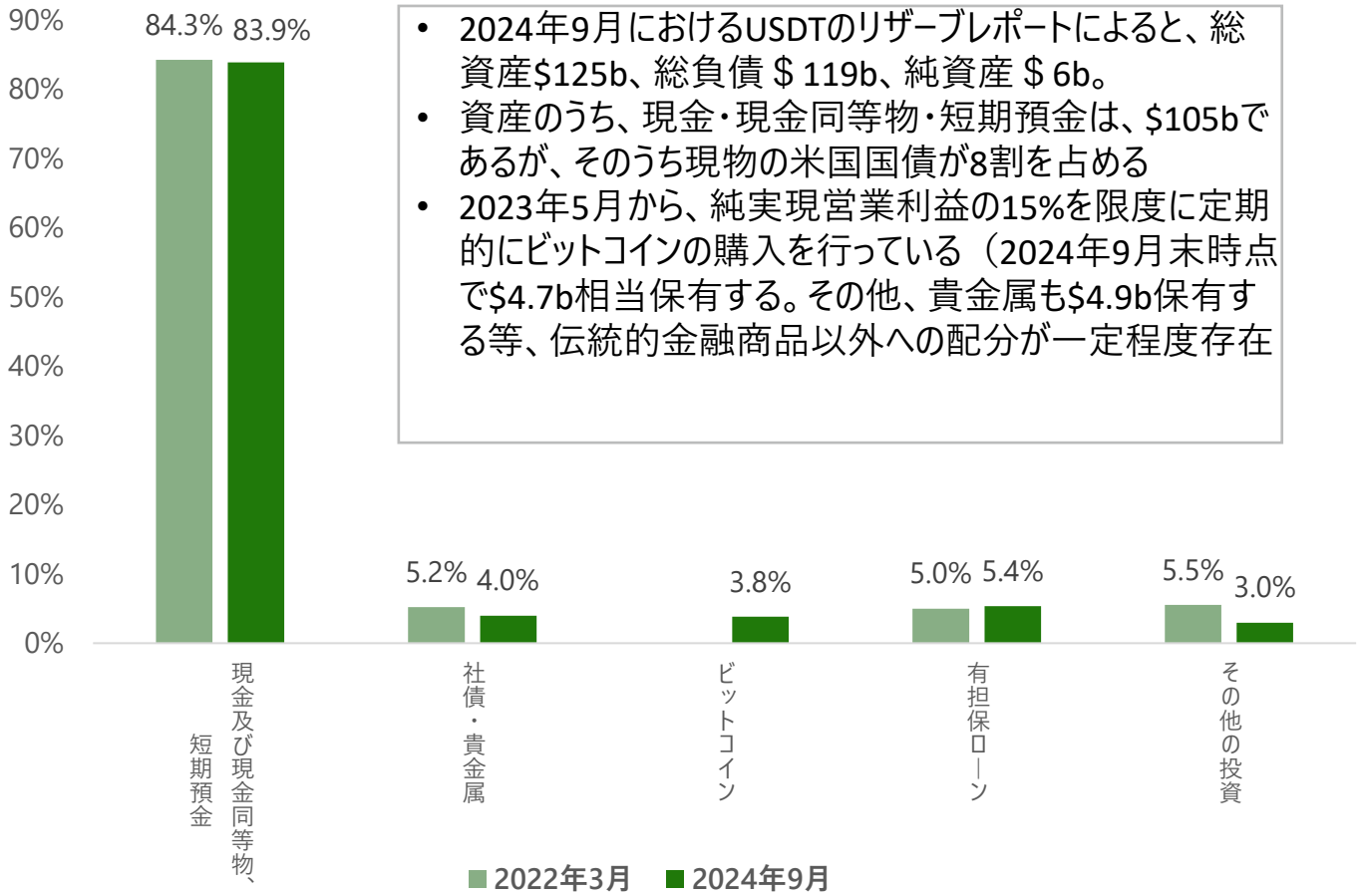
#	項目	2022年報告書の要約*1	主なアップデート*2
(1)	事業スキームの概要	■ Tetherは法定通貨にペッグされた暗号資産で、Tether Operations Limited 又はその関係会社（以下併せて「Tether 社」という。）によって発行されている。 当初ビットコインのブロックチェーンで発行されたが、現在では、イーサリアム、EOS、トロン、アルゴランド等のブロックチェーン上の2層目のプロダクトとして機能し、これらのハッシュアルゴリズムが利用されている。	■ 時価総額は、2022年7月に$65から2024年12月では$140bと2倍以上成長 ■ 展開するブロックチェーンは2022年7月では12個であったが、2024年末基準では15個 ✓ 新たに追加したブロックチェーン：NEAR Network（2022年9月）、Polygon（2023年5月）、Aptos（2024年8月） ✓ 以下ブロックチェーンから撤退予定：2025年9月、Kusama、Bitcoin Cash SLP、Omni Layer、EOS、Algorand
(2)	事業スキームの狙い及び顧客ターゲット	■ WhitepaperによるとTetherは主に以下を利点としている A）スキームの狙い • 匿名かつ分散型のP2Pネットワークで運用される • 容易に事業者、暗号資産取引所、ウォレットと統合可能 B）顧客ターゲット • 個人も企業もTetherを利用可能	■ 規制当局の要求を満たすための取り組み ✓ 2023年、米国司法省・シークレットサービス・FBIと協力し、$435m相当のアドレス凍結を実施し、またOFACからの制裁を受けた個人のウォレットの凍結するポリシーを公表*3 ■ 2024年11月、MiCAへの対応のため、StablRに投資するとともに、独自のユーロ建てステーブルコインEURTを段階的に廃止すると発表 ✓ StablRは、イーサリアムおよびSolana上でEURR、USDRを発行しており、2024年7月にEMIライセンスを取得済み ■ MiCAの影響で、USDTの欧州市場での取り扱い停止が時価総額下落 ✓ EUに拠点を置く複数の暗号資産取引所とCoincaseが、USDTの取り扱いを中止したことを受けて時価総額が下落（2025年1月）
(3)	発行・償還の手続・条件（発行時の条件、償還時の最低金額・手数料、償還の免責事項）	■ 手数料等 ✓ 入金手数料：0.1%、最低額100,000米ドル ✓ 引き出し手数料：1,000米ドルまたは償還額の0.1%、最低額100,000米ドル。Tetherの預入れ・引出しは手数料なし ■ 償還時の免責事項 ✓ 必要に応じて償還を遅らせる権利や、準備金の現物で償還する権利を留保	■ ステーブルコインを発行・管理する支援プラットフォームHadronを公表 ✓ 実物資産のトークン化への対応（株式、債券、コモディティ、ファンド、ポイント等） ✓ トークン発行・償却の柔軟化 ✓ 包括的なKYC/AMLツールを提供

【参考】*1：「海外（米国）のステーブルコインのユースケース及び関連規制分析に関する調査」（金融庁）_2025年2月時点確認
*2：「Hadron by Tether Platform Brings Simplified Asset Tokenization to the Mass Market」（Tether）_2025年2月時点確認
*3:：「Tether will block USDT on sanctioned wallets」（AML Crypto）_2025年2月時点確認

Tether社のリザーブの大半は低リスク資産となっていますが、一定程度リスク資産を保有する方針をとるとしています

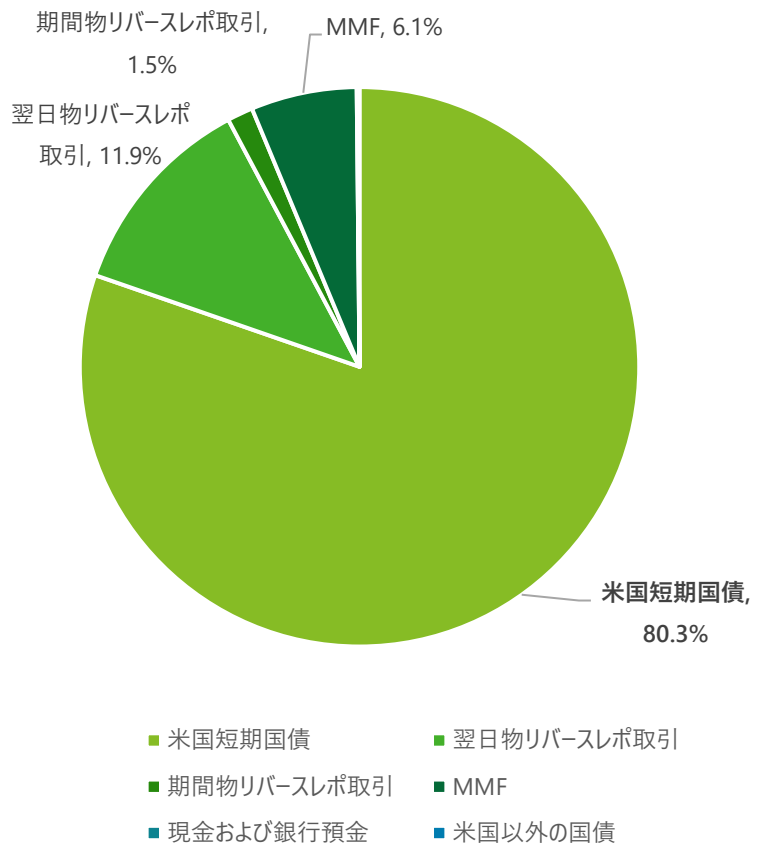
USDTの概要と主なアップデート（リザーブ）

USDTの裏付け資産の時系列的比較*1、*2、*3



- 2024年9月におけるUSDTのリザーブレポートによると、総資産$125b、総負債＄119b、純資産＄6b。
- 資産のうち、現金・現金同等物・短期預金は、$105bであるが、そのうち現物の米国国債が8割を占める
- 2023年5月から、純実現営業利益の15%を限度に定期的にビットコインの購入を行っている（2024年9月末時点で$4.7b相当保有する。その他、貴金属も$4.9b保有する等、伝統的金融商品以外への配分が一定程度存在

現金・現金同等物・短期預金の内訳*4



【参考】：＊1 「USDT Transparency Reports(Tether）」_2022年3月、2024年9月時点確認　*2、＊3「Tether to Further Strengthen Reserves Through Purchase of Bitcoin with Realized Net Operating Profits」（Tether）_2023年5月時点確認、「Tether shifts $780M in Bitcoin to reserve」（Cointelegraph）_2024年12月時点確認、*4【参考】：「Tether Transparency」（Tether） _2024年9月時点確認

2022年以降、Circle社は、展開するブロックチェーンの追加、MiCA規制の準拠等、事業スキームや顧客ターゲットを拡大しているとしています

USDCの概要と主なアップデート

#	項目	2022年報告書の要約*1	主なアップデート*2
(1)	事業スキームの概要	■ CoinbaseとCircleによって設立されたCentre Consortiumが設計した基準に従って発行されるステーブルコイン。USDC自体は複数の発行者が存在できることが想定されるスキーム。 各USDCは準備金に裏付けられ、1USDCは1米ドルで償還可能。	■ CentreからCircleへのガバナンス機能等の移管 ✓ 2023年8月21日に、Circle社は、Centreは独立した組織としての活動を停止させ、CircleがUSDCの発行者として存続すること、Centreのガバナンスと運営の責任をCircle社内に持ち込むことを発表 ■ 展開するブロックチェーンは2022年９月では８個であったが、2024年末基準では16個 ✓ 新たに追加したブロックチェーン：Arbitrum One、NEAR、Optimism、Polkadot（2022年）、Cosmos、Base、Polygon（2023年）、Celo、Zksync、Sui（2024年） ✓ 以下ブロックチェーンを除外：Tron（2024年2月）、Flow（2024年8月）
(2)	ステーブルコインのスキームの狙い及び顧客ターゲット	■ KYC済みのビジネスユーザーは、Circleアカウントを通じてUSDCを購入可能 ■ Circleアカウントの作成には法人名や代表者情報の入力が必要となっており、購入者は法人を主に想定している。個人ユーザーは暗号資産取引所で購入可能。	■ 2024年7月、CircleはUSDCとEURCの発行をEUで開始し、MiCA規制に準拠した初のグローバルステーブルコイン発行者となった ✓ フランスの銀行監督当局（ACPR）から電子マネー機関（EMI）ライセンスを取得し、MiCAの規制要件を満たす ■ 各国のライセンス取得に向けた取り組みの継続 ✓ シンガポールのMajor Payment Institution (MPI)を取得（2023年6月）
(3)	発行・償還の手続・条件（発行時の条件、償還時の最低金額・手数料、償還の免責事項等）	■ 発行時の手数料は無料（米ドルの電信送金が条件）。 償還時の手数料は無料。 ■ ただし、受け取り銀行の手数料が発生する可能性あり。USDCの償還の際には、①USDC のアカウントを保持していること、②ユーザー規約に違反していないこと、③監督当局、司法当局から償還差し止め等の処分がなされていないことが利用規約に定められている。	■ 2024年2月、Circle USDCの償還サービスに関する標準(Standard)と基本(Basic)の償還オプションを導入 ✓ 標準(Standard)償還: 1日あたり1500万ドルまでの償還が無料。それ以上は0.1%の手数料が発生。 ✓ 基本(Basic)償還: 取引量に関係なく手数料無料。ただし、処理に最大で2営業日かかる。 ■ 2024年10月、CircleはUSDCの償還手数料を再び引き上げ、1日あたり200万ドルを超える償還に追加手数料を導入

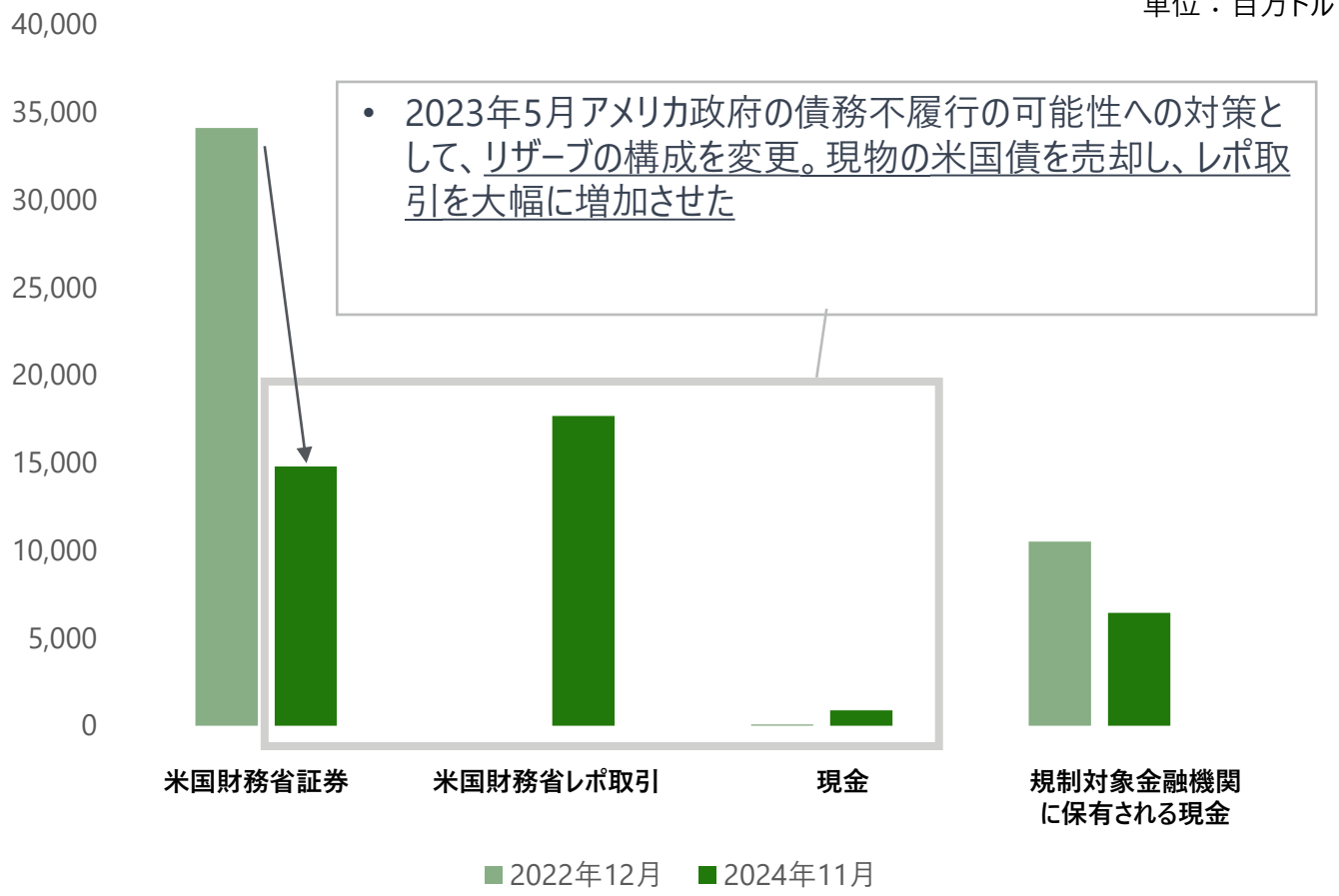
【参考】：*1「海外（米国）のステーブルコインのユースケース及び関連規制分析に関する調査」（金融庁）_2025年2月時点確認
*2：「Pressroom | Latest Circle News」（Circle）の2023年以降から2025年1月までの情報_2025年2月時点確認

Circle社は、2023年5月以降、アメリカ政府の債務不履行の可能性への対策として、レポ取引の割合を高めていると公表しています

USDCの概要と主なアップデート（リザーブ）

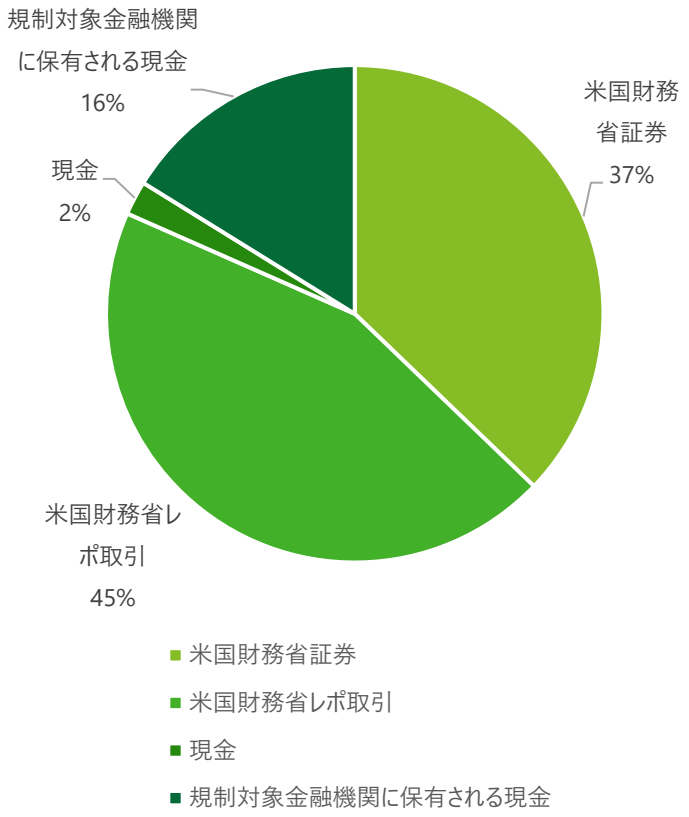
USDCの裏付け担保資産割合の時期別比較*1、*2、*3

単位：百万ドル



USDC裏付け担保資産の割合

(2024年）*2



*1、*2【参考】：USDC Reserve Report」(GrantThornton）_2022年12月時点確認、「USDC Reserve Report」(Deloitte）_2024年11月時点確認
*3【参考】：「USDC Issuer Circle Moves $8.7B to Repo Agreements to Protect Reserves From U.S. Government Default」（Coindesk）_ _2023年5月時点確認

S&Pは、USDTに関して価格安定性の維持は認められるが情報開示が不足している点が懸念があると示し、USDCに関して高い透明性と規制遵守の取り組んでいると評価しています

USDTとUSDCに関する評価（S&P）

項目	USDT	USDC
概要	• 2014年に発行開始した、市場で最も流通しているステーブルコインで、英領バージン諸島と香港にそれぞれ設立されたTether International Ltd.およびTether Ltd.によって発行されおり、これらはどちらも、英領バージン諸島に登録されたTether Holdings Ltd.の完全子会社 • 価格安定性の維持は認められるが、情報開示が不足している点が懸念。また資産とリスク管理に関する透明性の不足、規制の枠組みの欠如、倒産隔離の不十分さ等に弱点がある	• Circle社が発行するステーブルコインで、低リスク資産で完全に担保されており、主に短期証券と銀行預金で構成されている。 • 高い透明性と規制遵守の取り組みを示しており、米国財務省の金融犯罪取締ネットワーク（FinCEN）に登録されている。
資産評価* Asset assessment	**4 | 制約的**（Constrained） • USDTの準備資産の大部分は、米国短期国債や現金同等物等の流動性が高く安全な資産で構成されている • カストディアン、取引相手、銀行口座提供者の信用力に関する情報開示がないこと、またリザーブの5%を占めるMMFのファンドに関する情報開示も不足している	1 | **非常に強力**（Very strong） • USDCは、主に短期証券と銀行預金で構成される低リスク資産で100％担保されいる。 • 資産の大部分はブラックロックが管理するCircle Reserve Fund（CRF）で保有。
安定性評価* Stablecoin stability assessment	**4 | 制約的**（Constrained） • 投資家にとって十分な透明性が確保されていない • 準備資産の一部に、貴金属、社債、ビットコイン等の高リスク資産が含まれており、USDTの価値が変動するリスクを抱えている。 • USDTの発行・管理主体は、明確な規制監督を受けておらず、将来的に規制上の問題が発生する可能性がある	**2 | 強力**（Strong） • 準備資産の内訳や保管場所等の情報を、定期的に詳細に公開しており、監査も受け、透明性が高い。 • 準備資産のほとんどが、米国短期国債やレポ取引等の低リスク資産で構成され、高い安全性と流動性を確保されている。 • Circle社は、米国FinCENや英国FCAでの登録を受けている
調整項目* Adjustment	**0 | 中立**（Neutral） • 上記の開示情報の不足等のネガティブポイントは、4 に位置される評価結果に相当する要因であり特に調整は不要	**-1 | 否定的**（Negative） • Circleが破産した場合に資産が保護されるかどうかについての先例や法的根拠が不十分であることを反映して、資産評価のスコアから1点減点。 • Circleは破綻時でもUSDCの準備金が他の債権者から分離されていると主張しているが、前例がなく、他の事業から分離されていることの根拠には不確実性がある

【参考】：「USDT Stablecoin Stability Assessment」（S&P Global Ratings）__2024年12月時点確認、「USDC Stablecoin Stability Assessment」（S&P Global Ratings, ）__2023年12月時点確認、
*資産評価、安定性評価は、スコアリング: 1 (非常に強力) から 5 (脆弱) までの5段階評価され、資産評価は、安定性評価の調整に関する指標で、,-1（否定的）,0（中立）,1（肯定的）で構成される

3.主要なステーブルコイン発行者の事業実態調査
3.2 発行者によるステーブルコインの普及活動

USDTは新興国・個人向けを主にユーザが利用する周辺サービスを対象、USDCは先進国/アジア・事業者/金融向けを主に、決済コアサービスを対象に活動しています

普及活動（2022年4月以降の各社プレスリリースより主なものを抜粋）

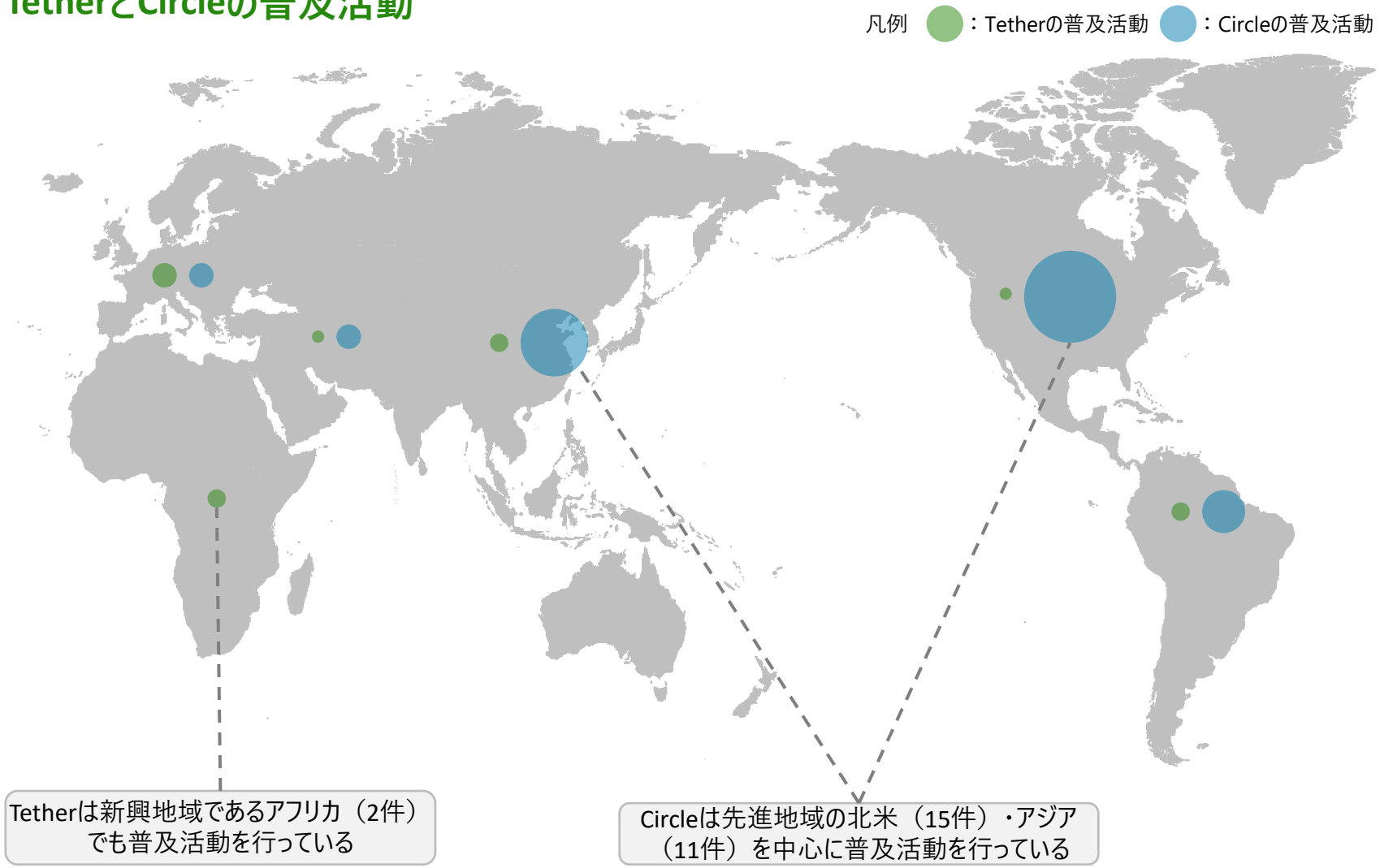
青字：差異がみられるところ

項目	USDT	USDC
概要（提供する決済サービス・エリア等）	■ 新興国地域・個人向け決済周辺サービスへの投資/提携が主、欧州に直近対応 （主な展開地域）北米・中南米・中東・アフリカ	■ 先進国/アジア地域・事業者/金融向け決済コアサービスへの投資/提携が主 2024年に社としてMiCA準拠し欧州に先行して取組み （主な展開地域）北米・中南米・中東・欧州・アジア
投資・提携等活動	• 2025.02 UAEの不動産B2Bプラットフォーム Reelly Techとの戦略的提携を発表 • 2024.12 動画共有プラットフォーマーRumbleに約8億ドル投資 • 2024.12 MiCA準拠発行体のStablRやQuantoz Paymentsに投資し欧州促進 • 2024.11 中東の原油取引に対する資金提供を発表 • 2024.09 アフリカ等の個人向け決済サービスSorted Walletに150万ドル投資 • 2024.08 中東の個人向け決済サービスKem（アプリ）に300万ドル投資 • 2024.06 XREXに1,875万ドルを投資、新興市場でB2Bクロスボーダー決済を促進 • 2023.12 ジョージアの教育プラットフォーマーのAcademy of Digital Industriesや、ウォレット提供者のCityPay.ioに投資 • 2023.06 イエローカードと提携。アフリカの若者のステーブルコイン教育/採用を推進 • 2022.10 ブラジルで個人向けの送金サービスを提供するSmartPayと提携	• 2025.02 USDCを担保とした日本初の BNPLサービス「Slash Card」の発行に向けて、オリコ・アイキタス・SLASH VISION PTE. LTD.と提携合意 • 2025.01 HashnoteおよびUSYCトークン化マネーマーケットファンドの買収、ならびにグローバルトレーディング会社DRWとの戦略的提携を発表 • 2025.01 Bison Digital Assets (Bison Bank)、MiCA準拠ステーブルコインでCircleと提携 • 2024.12 加盟店向け決済システムを提供するPockyt (米国) と提携、加盟店は入金と支払いの両方でステーブルコインを追加のオプションとして活用 • 2024.10 欧州で事業者向け決済サービスを提供しているBVNKと提携 • 2024.10 シンガポールで事業者向け決済サービスを提供するThunesと提携 • 2024.09 ブラジルPIXとメキシコSPEIを経由した送金に対応 • 2024.05 ブラジルのNubankやBTG Pactualと提携 • 2023.11 SBIホールディングス (SBI新生銀行)、Circleと提携 • 2023.09 Visaがアクワイアラ向けにUSDC決済機能を拡大 • 2022.09 加盟店向け決済システムを提供するElementsに投資 • 2022.06 信頼性の高いデジタル資産管理を事業者/金融向けに提供するCYBAVO（台湾）に投資
展開チェーン*1	Ethereum（46.57%）、Tron（41.95%）、BSC（3.77%）、Arbitrum（2.04%）、Avalanche（1.18%）、TON（1.03%）、Solana（0.74%）、Optimism（0.65%）、Polygon（0.54%）、Near（0.38%）、その他（1.15%）	Ethereum（66.55%）、Solana（8.8%）、Base（7.61%）、Hyperliquid（4.59%）、Arbitrum（2.96%）、Polygon（1.74%）、BSC（1.51%）、Avalanche（1.17%）、Noble（1.06%）、Optimism（0.78%）、その他（3.22%）

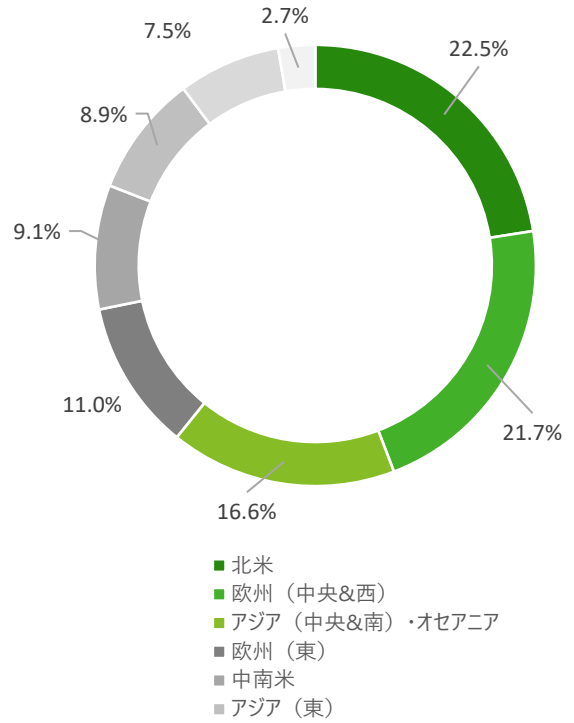
【出所】「Why use Tether?」（Tether）、「Circle | USDC & Web3 Services for a new financial system」（Circle）_2025年2月時点確認
*1「DefiLlama - DeFi Dashboard」（DeFiLlama）2025年1月6日時点の集計（時価総額全体が$206bのうち、USDTが$137b（67%）、USDCが$45b（22%））

Tetherは新興国でも普及活動を行っており、Circleは北米・アジア等の先進地域を中心とした普及活動を行っています

TetherとCircleの普及活動



【参考】世界の暗号資産取引シェア*1
北米、欧州（中央&西）、アジア（中央&南）・オセアニアにて、世界の暗号資産取引における6割程を占める

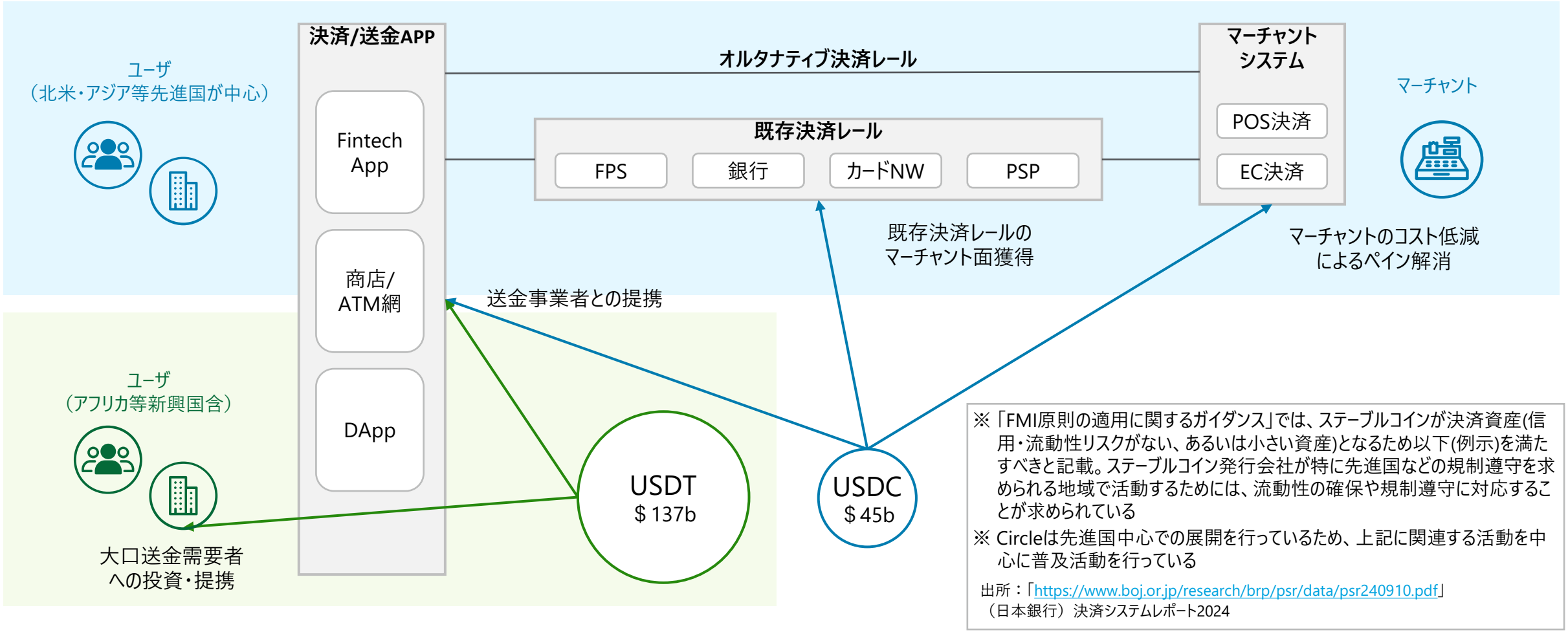


【参考】：「Why use Tether?」（Tether）、「Circle | USDC & Web3 Services for a new financial system」（Circle）の2022/4/1-2025/1/21期間のプレスリリース_2025年2月時点確認
「2024 Geography of Cryptocurrency Report」（Chainalysis）_2025年2月時点

Tetherはユーザ向けの普及活動を進めており、Circleはユーザ向け普及活動に加え、既存決済レールやマーチャントシステム提供者と提携・投資を行い、マーチャント向け普及活動も行います

普及活動の全体像

凡例 ：Tetherの主な普及活動 ：Circleの主な普及活動



※「FMI原則の適用に関するガイダンス」では、ステーブルコインが決済資産(信用・流動性リスクがない、あるいは小さい資産)となるため以下(例示)を満たすべきと記載。ステーブルコイン発行会社が特に先進国などの規制遵守を求められる地域で活動するためには、流動性の確保や規制遵守に対応することが求められている

※ Circleは先進国中心での展開を行っているため、上記に関連する活動を中心に普及活動を行っている

出所：「https://www.boj.or.jp/research/brp/psr/data/psr240910.pdf」（日本銀行）決済システムレポート2024

大口送金需要者との提携では、不動産取引PF・原油取引でのUSDT決済導入にかかる提携・投資を行っています

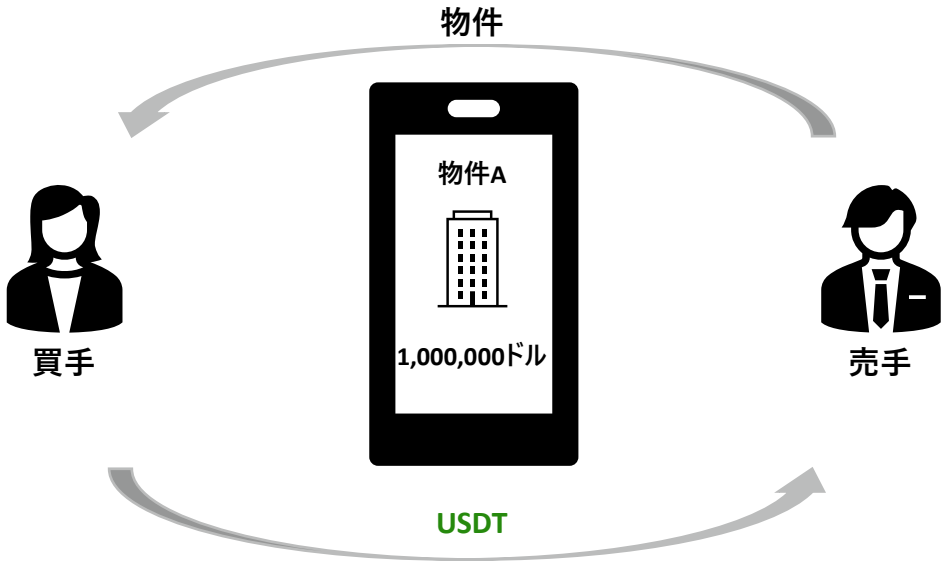
Tetherの普及活動_大口送金需要者との提携

TetherとReelly Tech、UAEの不動産取引に革命を起こす戦略的提携を発表

ニュース概要

- Reelly Techのプラットフォーム上の3万人を超える国内外のエージェントは、USDTの力を活用し、プロセスを合理化し、地域で最もダイナミックな市場の1つで効率を高める
- 不動産購入のための USDT 決済等の実用的なアプリケーションを理解できるようにエージェントを支援することを目的としている

サービスイメージ



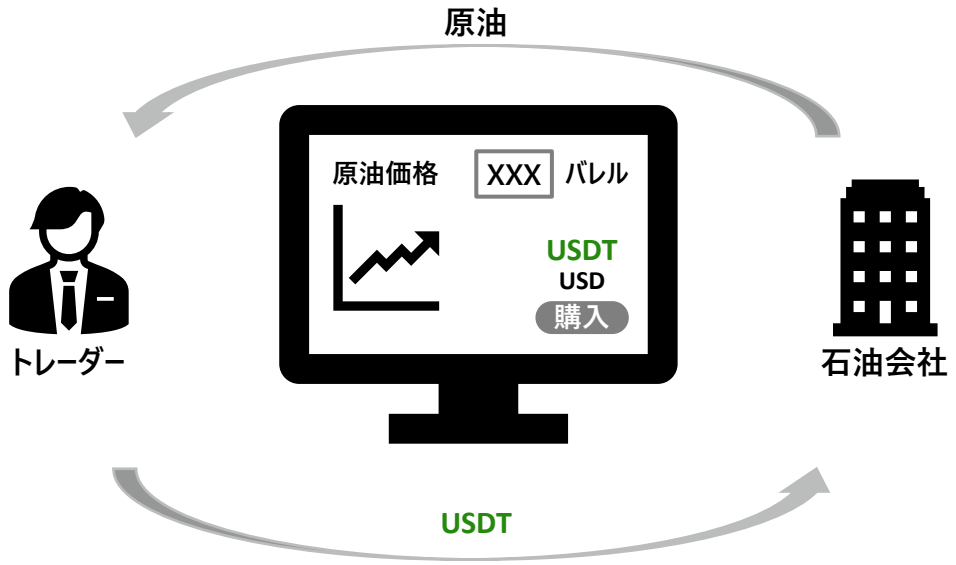
Tetherの普及活動_大口送金事業者への投資

中東の原油取引に対する資金提供を発表

ニュース概要

- 投資部門が上場超大手石油会社と一流商品トレーダー間の現物原油取引に資金を提供したと発表しました。2024年10月に完了したこの取引は、中東産原油67万バレル（約4,500万ドル相当）の積み込みと輸送を容易にするためのもの
- ステーブルコインUSDTを通じて貿易フローの効率化を推進することで、貿易金融業界に前向きな変化をもたらすことを目指している
- 貿易金融取引における USDT の使用を推進しており、これによりコストが削減され、支払い時間が短縮される

サービスイメージ



【参考】:「News - Tether.io」（Tether）_2025年2月時点確認

既存決済レール企業ではオリコがUSDCを活用したBNPLに向けた提携、マーチャントシステム企業は加盟店がUSDCでの入金受付・支払に向けた提携が行われています

Circleの普及活動_既存決済レールとの提携

USDC（USD Coin）を担保とした日本初の BNPL（Buy Now Pay Later）サービス「Slash Card」の発行に向けて提携合意

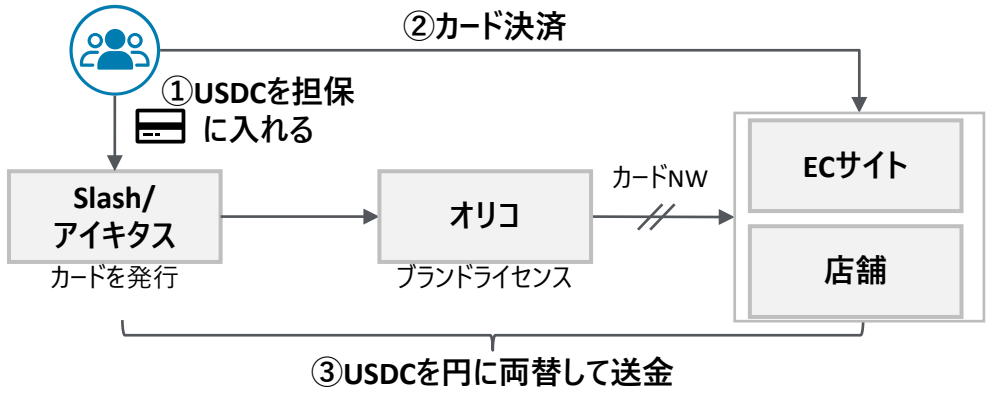
ニュース概要

- ステーブルコイン「USDC」を担保として活用し、安全性と利便性を兼ね備えた後払い型の決済手段を提供する
- ユーザは自身が保有するアンホステッドウォレットを利用することで、オンラインショップや実店舗での買い物が可能になると同時に、暗号資産の世界と現実世界の境界をシームレスに越える新しい体験が可能になる

3社の役割

- オリコ：BIN スポンサーとして国際ブランドとの対応を担当
- アイキタス：カード発行者として顧客管理およびシステム運営を担当
- Slash：プログラムマネージャーおよび Slash ブランドの提供者として、「Slash Card」の開発・運営およびブランド提供を担当

サービスイメージ



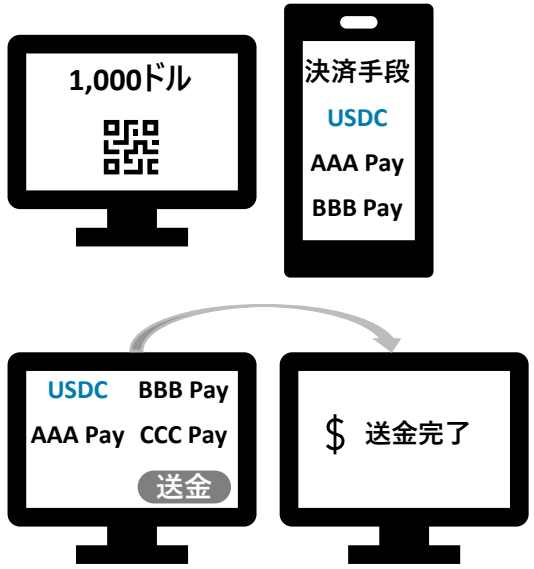
Circleの提携・投資先_マーチャントシステムとの提携

Pockyt が Circle と提携し、USDC によるシームレスな決済で世界中の小売業者を支援

ニュース概要

- Pockyt は Circle の USDC 機能を統合できるようになり、マーチャントは入金と支払いの両方でステーブルコインを追加のオプションとして活用できるようになる
- USDC を使用した国境を越えた商取引のための安全で効率的、かつ費用対効果の高いソリューションをマーチャントに提供

サービスイメージ



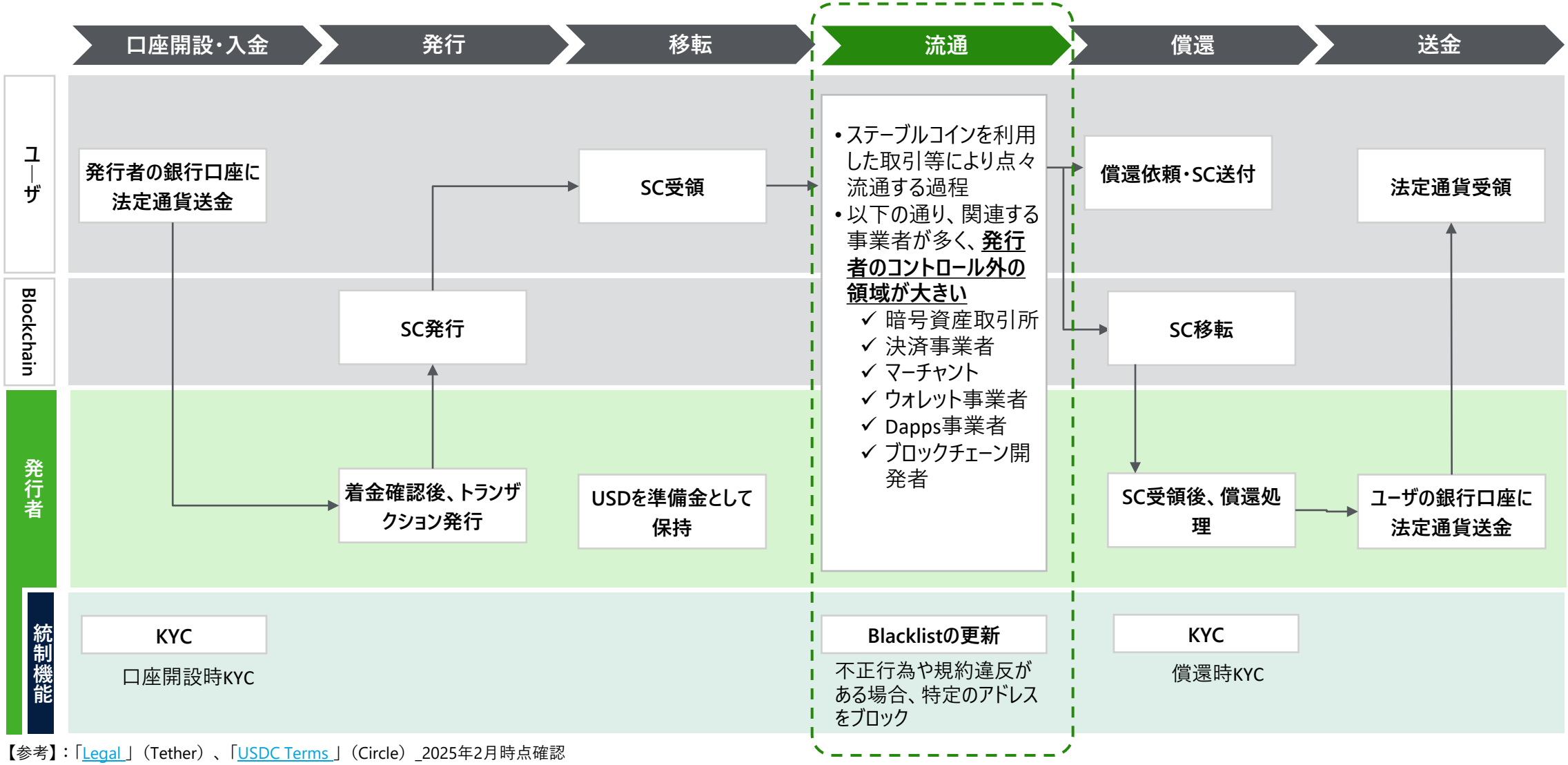
- ユーザからの支払受入時に、決済手段としてUSDCがオプションとして利用できる
- 支払先への送金時に、決済手段としてUSDCがオプションとして利用できる

【参考】：「ニュースリリース｜株式会社オリエントコーポレーション」（オリコ）、「Pressroom | Latest Circle News」（Circle）_2025年2月時点確認

3.主要なステーブルコイン発行者の事業実態調査
3.3 発行・償還に関するスマートコントラクト

発行者にとってステーブルコインの発行・償還時のKYC、Blacklist登録による資金凍結が主な不正利用抑止策ですが、コントロールを及ぼせる領域は限定的です

ステーブルコインの発行・償還プロセス



【参考】:「Legal」（Tether）、「USDC Terms」（Circle）_2025年2月時点確認

発行・償還機能と不正行為や規約違反がある場合の流通時のブロック機能は、いずれもコントラクトベースで実装されており、かつ機能上大きな差異はみられません

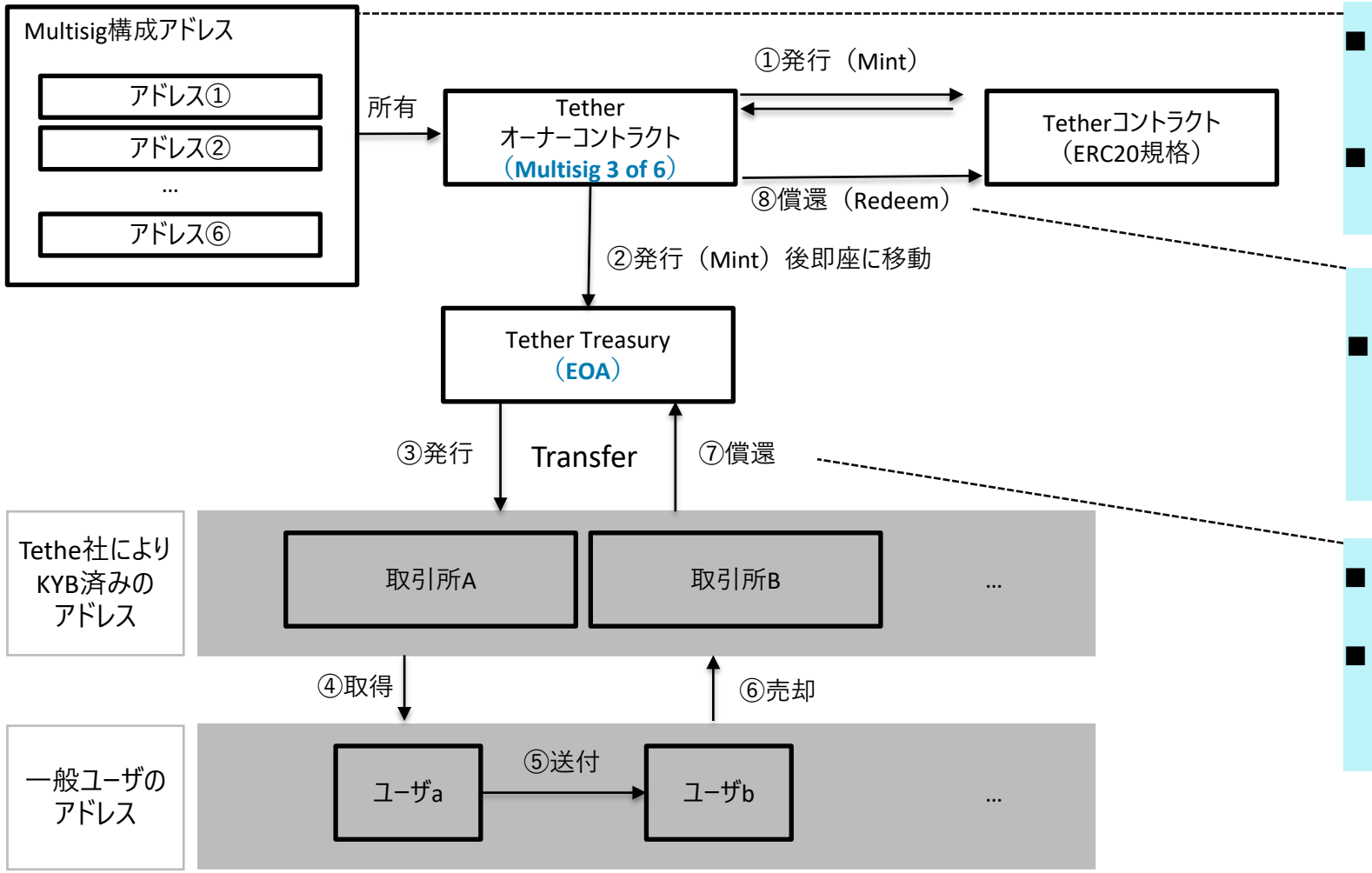
USDT・USDCの共通機能と異なる点を一部抜粋

青字：差異がみられるところ

#	機能 / 関数名	USDT (Tether)	USDC (USD Coin)
1	**ERC-20標準関数**	以下の標準的なERC20機能は全て実装 name(), symbol(), decimals(), totalSupply(), balanceOf(address), transfer(address,uint256), transferFrom(address,address,uint256), approve(address,uint256), allowance(address,address)	同左
2	**発行・焼却（Mint/Burn）**	**オーナーのみ**以下の関数を使用可能。 - issue(uint256): 発行用の関数。 - redeem(uint256): 焼却用の関数。オーナーのみ使用可能。	**Minter権限のみ**以下の関数を使用可能。 - mint(address,uint256): 発行用の関数。 - burn(uint256): 焼却用の関数。
3	**Minterの設定**	当該機能なし（オーナーが発行・焼却するため）	**MasterMinterは新しいMinterの設定と発行上限を設定することが可能** - configureMinter(address minter, uint256 minterAllowedAmount) - updateMinterAllowance(address minter, uint256 amount)
4	**ブラックリスト（Blacklisting）**	**オーナーのみ**以下の関数を使用可能。 - addBlackList(address _evilUser):ブラックリスト登録 - removeBlackList(address _clearedUser):ブラックリスト解除 - **destroyBlackFunds(address _blackListedUser) :ブラック資金押収**	**Blacklister権限のみ**以下の関数を使用可能。 - blacklist(address _account):ブラックリスト登録 - unBlacklist(address _account):ブラックリスト解除
5	**停止(Pause)/再開(Unpause)**	**オーナーのみ**以下の関数を使用可能。 - pause():コントラクトを一時停止 - unpause():コントラクトの一時停止を解除	**Pauser権限のみ**以下の関数を使用可能。 - pause():コントラクトを一時停止 - unpause():コントラクトの一時停止を解除

USDTの発行・償還権限はOwnerコントラクト集約され、マルチシグ管理されています

USDTの発行・償還に関するアドレスレベルのフロー



- Ownerアカウントは3 of 6のマルチシグアドレスで構成されており、事実上3つの署名だけで発行・償還が可能となっている
- Ownerアカウントは、Blacklist登録等もできる高い権限を有している

- このレベルの償還はほぼ行われない（Ethereumの場合は過去に 3 回しか発生していない）

- Tether Treasuryからの資金移動が「発行・償還」と定義される
- 当該資金移動は、ブロックチェーン上ではMintやRedeemではなくTransferのカテゴリーに含まれるトランザクション

USDTの発行・償還コードは、発行・償還がOwnerアカウントに集約されて実行されるという比較的シンプルな設計です

発行・償還のコード（USDT）

```
402     // Issue a new amount of tokens
403     // these tokens are deposited into the owner address
404     //
405     // @param _amount Number of tokens to be issued
406     function issue(uint amount) public onlyOwner {
407         require(_totalSupply + amount > _totalSupply);
408         require(balances[owner] + amount > balances[owner]);
409
410         balances[owner] += amount;
411         _totalSupply += amount;
412         Issue(amount);
413     }
414
415     // Redeem tokens.
416     // These tokens are withdrawn from the owner address
417     // if the balance must be enough to cover the redeem
418     // or the call will fail.
419     // @param _amount Number of tokens to be issued
420     function redeem(uint amount) public onlyOwner {
421         require(_totalSupply >= amount);
422         require(balances[owner] >= amount);
423
424         _totalSupply -= amount;
425         balances[owner] -= amount;
426         Redeem(amount);
427     }
```

各コードの意味

発行(issue)：Ownerが指定量を発行し、発行分のOwner残高を増額させる

406	関数の実行権限をオーナーに制限する（onlyOwner）
407	発行枚数のチェック（現在の発行枚数に発行額を追加して数値型がオーバフローしないか）
408	オーナーの残高チェック（現在のオーナーの残高に発行額を追加して数値型オーバーフローしないか）
410	オーナーの残高に発行額分を増額する
411	総発行枚数に発行額分を増額する
412	発行額をログとして記録する（イベントログとして発行量をブロックチェーンに記録）

償還（redeem）：オーナーが指定量を償還し、償還分のオーナー残高を減額させる

420	関数の実行権限をOwnerに制限する（onlyOwner）
407	総発行枚数のチェック（総発行枚数が償還量以上あることの確認）
408	オーナーの残高チェック（オーナーの残高が償還量以上あることの確認）
410	総発行枚数から償還額を減額する
411	オーナー残高から償還額を減額する
412	償還額をログとして記録（イベントログとして償還額をブロックチェーンに記録）

【参考】：公開情報（ethrscan. Contract address：0xdAC17F958D2ee523a2206206994597C13D831ec7）_2025年2月時点

USDCの発行・償還コードには、ブラックリストへの照会機能等も実装されており、相対的に詳細な設計となっています

発行のコード（USDC）

```
114     /**
115      * @notice Mints fiat tokens to an address.
116      * @param _to The address that will receive the minted tokens.
117      * @param _amount The amount of tokens to mint. Must be less than or equal
118      * to the minterAllowance of the caller.
119      * @return True if the operation was successful.
120      */
121     function mint(address _to, uint256 _amount)
122         external
123         whenNotPaused
124         onlyMinters
125         notBlacklisted(msg.sender)
126         notBlacklisted(_to)
127         returns (bool)
128     {
129         require(_to != address(0), "FiatToken: mint to the zero address");
130         require(_amount > 0, "FiatToken: mint amount not greater than 0");
131
132         uint256 mintingAllowedAmount = minterAllowed[msg.sender];
133         require(
134             _amount <= mintingAllowedAmount,
135             "FiatToken: mint amount exceeds minterAllowance"
136         );
137
138         totalSupply_ = totalSupply_.add(_amount);
139         _setBalance(_to, _balanceOf(_to).add(_amount));
140         minterAllowed[msg.sender] = mintingAllowedAmount.sub(_amount);
141         emit Mint(msg.sender, _to, _amount);
142         emit Transfer(address(0), _to, _amount);
143         return true;
144     }
```

各コードの意味

発行(mint)：オーナーから許可を受けたMinterが発行し、指定アドレスへ送付する

121-127	発行条件の規定 whenNotPaused：（コントラクトが一時停止状態でないこと） onlyMinters：（Minterのアドレスであること） notBlacklisted(msg.sender)：送信元がブラックリストに登録されていな事 notBlacklisted(_to)：送信先がブラックリストに登録されていない事
129	送信先チェック（送信先が0アドレスでない事）
130	発行額チェック（発行額が0より大きい事）
132	送信元であるMinterの発行許可額を取得
133-135	発行量チェック（当該Minterが発行許可額より大きい金額を発行しようとしていないか確認）
138	総発行枚数に発行量を増額する
139	送信先の残高に発行量を増額する
140	Minternの発行許可枚数から本発行量分減額する
141	発行量をログとして記録（発行者、発行先、発行額をイベントログとしてブロックチェーンへ記録する）
142	移転量をログとして記録（０アドレス、発行先、発行額を移転のイベントログとしてブロックチェーンへ記録する）

【参考】：公開情報（ethrscan. Contract address：0x43506849D7C04F9138D1A2050bbF3A0c054402dd）_2025年2月時点確認

USDCの発行・償還コードには、ブラックリストへの照会機能等も実装されており、相対的に詳細な設計となっています

償還のコード（USDC）

```
354     /**
355      * @notice Allows a minter to burn some of its own tokens.
356      * @dev The caller must be a minter, must not be blacklisted, and the amount to burn
357      * should be less than or equal to the account's balance.
358      * @param _amount the amount of tokens to be burned.
359      */
360     function burn(uint256 _amount)
361         external
362         whenNotPaused
363         onlyMinters
364         notBlacklisted(msg.sender)
365     {
366         uint256 balance = _balanceOf(msg.sender);
367         require(_amount > 0, "FiatToken: burn amount not greater than 0");
368         require(balance >= _amount, "FiatToken: burn amount exceeds balance");
369
370         totalSupply_ = totalSupply_.sub(_amount);
371         _setBalance(msg.sender, balance.sub(_amount));
372         emit Burn(msg.sender, _amount);
373         emit Transfer(msg.sender, address(0), _amount);
374     }
```

各コードの意味

償還（burn）：オーナーから許可を受けたMinterが指定金額を償還する

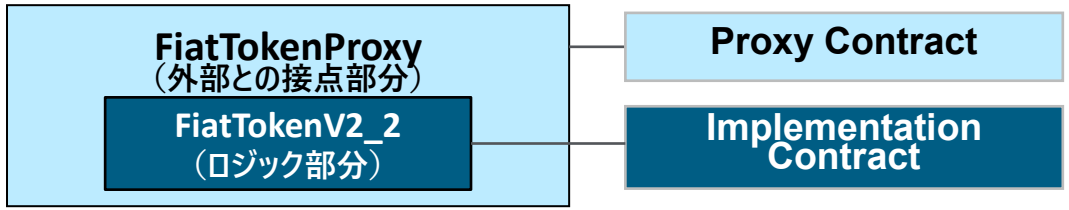
360-364	償還条件の規定 whenNotPaused：（コントラクトが一時停止状態でないこと） onlyMinters：（Minterのアドレスであること） notBlacklisted(msg.sender)：送信元がブラックリストに登録されていない事
366	送信元の残高取得
367	償還量チェック（償還額が0より大きい事）
368	送信元の残高が償還量以上あることを確認
370	総発行枚数から償還量を減額
371	送信元の残高から償還量を減額
372	償還量をログとして記録（送信元、償還額をイベントログとしてブロックチェーンへ記録する）
373	移転量をログとして記録（送信先、0 アドレス、償還額を移転のイベントログとしてブロックチェーンへ記録する）

【参考】：公開情報（ethrscan. Contract address：0x43506849D7C04F9138D1A2050bbF3A0c054402dd）_2025年2月時点

USDCは、Proxy Contractを使った実装方法であるためスマートコントラクトの更新に柔軟性があり、またコンタクトの実行権限の設定が相対的にきめ細かに設計されています

USDCのコントラクトの実装上の特徴

- USDCは、スマートコントラクトが[Proxy ContractとImplementation Contractの2段構えで実装]されており、Implementation Contractとして実装されているUSDTとは異なる特徴を持つ



- FiatTokenV2_2で実装されている機能

機能	説明
通常のERC20	通常のERC20の機能（Mint,Transfer,Burn)
一時停止機能	Pauserによる緊急時のコントラクト全体を一時停止する機能
ブラックリスト機能	特定のアドレスをブラックリストとして登録し、資金移動を不可とする

- USDCでは、コントラクトの発行権限が分化・階層化されており、Owner 一本のUSDTとは異なる実装となっている

権限	説明
Owner	コントラクトのオーナーでありMasterMinterを変更できる
MasterMinter	• 新しいMinterの追加とMint金額の上限を設定 • 既存のMinterの削除
Minter	通貨の発行と焼却が可能
Pauser	緊急時にコントラクト全体を一時停止する
Blacklister	特定のアドレスをブラックリストとして登録・除外する

- 実際に発行と焼却の機能を担うMinterのアドレスは以下の通り複数設定されており、それぞれに発行上限を持たせることで一定の制御がかけられるようになっているが、実際に上限が設定されているアドレスは限られている

#	Minterアドレス（2025年1月31日現在）	発行上限
1	0x5b6122c109b78c6755486966148c1d70a50a47d7	4,006,607,385
2	0xc4922d64a24675e16e1586e3e3aa56c06fabe907	86,737,797
3	0x19a932fc5a8320939c3575302a8705147a7f27d8	23,695
4	0x911cb2323c6fb580e39f92a6f58d1cb019e940cd	0
5	0x895f07957b863f4ab6086035a6990d8366bc3266	0
6	0x2322e81db282f22849c2eb0b749c688ea3611946	0
7	0x24bdd8771b08c2ea6fe0e898126e65bd49021be3	0
8	0x55fe002aeff02f77364de339a1292923a15844b8	0
9	0x3005a4c0efe7e66f3f60ef8704983247a5c6ca61	0
10	0x8967a7ce20043f876e42f8ad696b06bb632f0ca7	0
11	0x2b52e60c844d7946b6d910d3296940dc889cc785	0
12	0xe400d09e98a5806bf501e93ed8e7623b78b4646f	0
13	0x9c08210cc65b5c9f1961cdbd9ea9bf017522464d	無効*
14	0xd4c1315948125cd20c11c5e9565a3632c1710055	無効*
15	0xe7ab0dd2a069fa115c0d7878af6fd95ba0f9100a	無効*

*一度Minterになったがその後解除

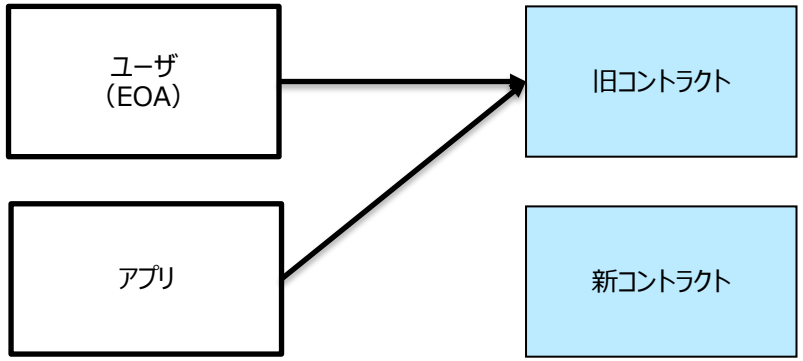
Proxy Contractは、スマートコントラクトの更新を行えるようにするための実装手法です

Proxy contractとは？

■ スマートコントラクトには、「Proxyコントラクト」と「Implementationコントラクト」の2種類がある。その役割について纏める。

■ **課題**

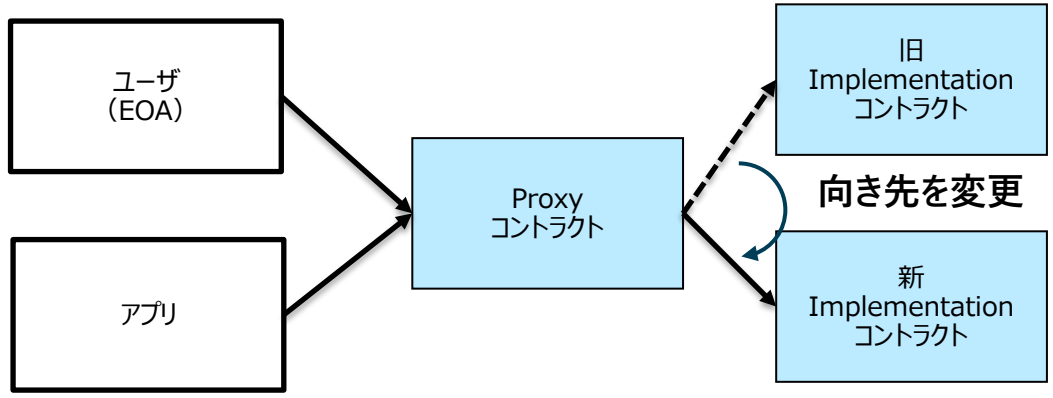
- スマートコントラクトはデプロイする度にコントラクトアドレスが自動で発行される仕組みになっている
- そのため新しい機能や脆弱性が発見された場合にスマートコントラクトを再デプロイすると新しいコントラクトアドレスになってしまい、ユーザやアプリから見た場合の窓口となるアドレスが変化してしまい、容易にアップデートできない課題があった



運営主体が旧コントラクトを更新するために新コントラクトを実装したが、ユーザやアプリが旧コントラクトに繋がれたままになってしまい、更新の効果が享受できない

■ **解決策**

- メンテナンスが必要となる重要なスマートコントラクトには「Proxyコントラクト」をユーザやアプリの窓口として機能させ、実際のコントラクトロジックが記載されている「Implementationコントラクト」とは区別し 2 段構成にすることでアップグレードを可能にしている



USDTの主要な関数の内容と実行権限

【参考】USDTスマートコントラクトの関数（一部）

#	機能	関数	説明	実行権限	その他条件
1	発行	**issue(uint amount)**	新規トークンを発行し、オーナーの残高へ発行額分を増額する。	**オーナーのみ（onlyOwner）**	-
2	償還	**redeem(uint amount)**	オーナーの残高から償還金額分を減額し、全体の総供給量を減らす。	**オーナーのみ（onlyOwner）**	-
3	ブラックリスト登録	**addBlackList (address _evilUser)**	指定アドレスをブラックリストに登録し、送金を禁止する。 内部的に isBlackListed[_evilUser] = true をセット	**オーナーのみ（onlyOwner）**	-
4	ブラックリスト解除	**removeBlackList(address _clearedUser)**	指定アドレスをブラックリストから解除する。 内部的に isBlackListed[_clearedUser] = false をセット	**オーナーのみ（onlyOwner）**	-
5	ブラックリスト資金の押収	**destroyBlackFunds(address _blackListedUser)**	ブラックリストに登録されたアドレスが保有するトークンを没収・消却し、_totalSupply を減少させる。	**オーナーのみ（onlyOwner）**	- 対象アドレスがブラックリストに登録されていること。
6	一時停止	**pause()**	コントラクトを一時停止状態にする。 不正送金や緊急時に利用。	**オーナーのみ（onlyOwner）**	- コントラクトがまだ停止状態になっていないこと（paused == false）
7	一時停止解除	**unpause()**	一時停止状態のコントラクトを再開させる。	**オーナーのみ（onlyOwner）**	- コントラクトが停止状態であること（paused == true）
8	資金移転	**transfer(address _to, uint _value)**	トークンを送金する標準的なERC20関数。 ブラックリストの送信元からの送金は拒否される。 本USDTの実装では送金時の手数料計算等も含まれる。	**すべてのユーザー（ただしブラックリスト除く）**	- コントラクトが一時停止されていないこと（paused == false） - 送信元がブラックリストに登録されていないこと

USDCの主要な関数の内容と実行権限

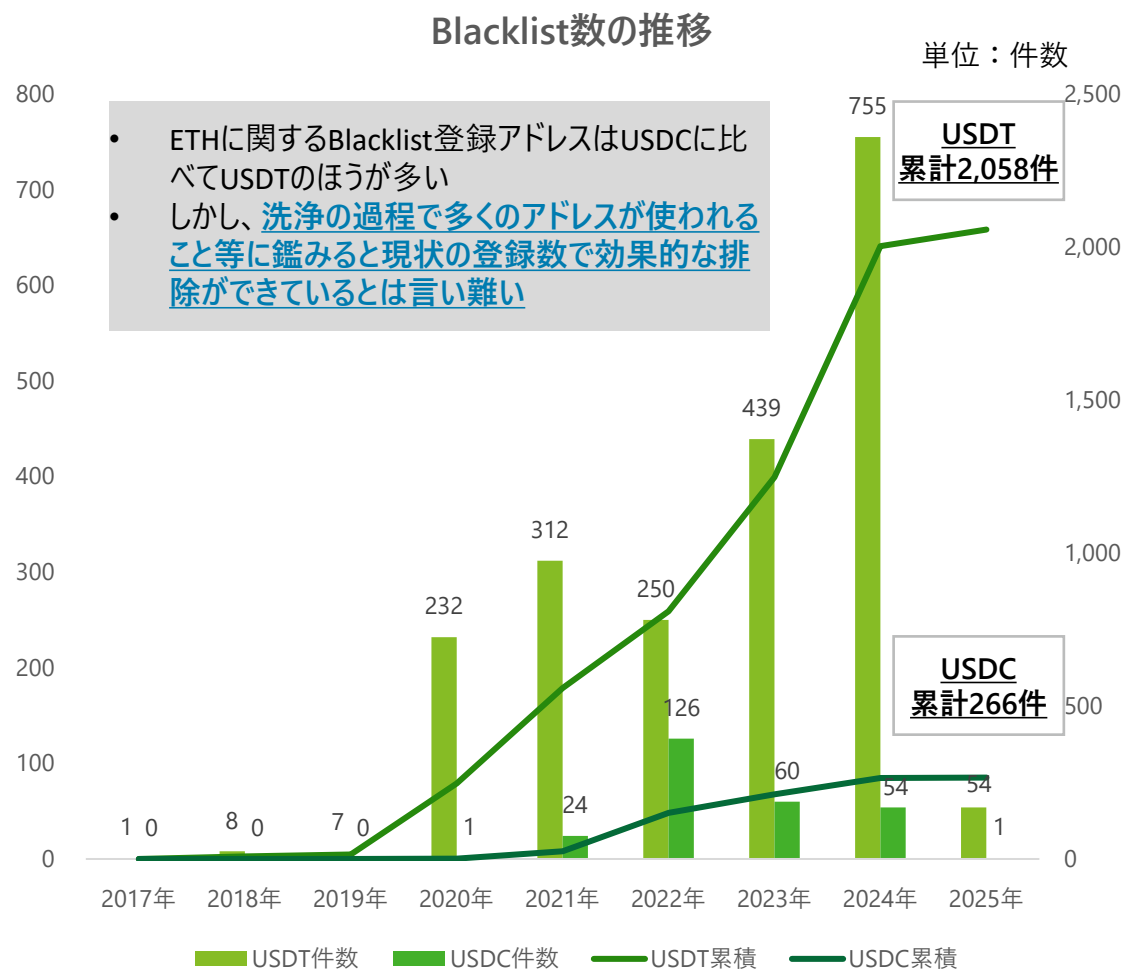
【参考】USDCスマートコントラクトの関数（一部）

#	機能	関数	説明	実行権限	その他条件
1	発行	**mint(address _to, uint256 _amount)**	指定したアドレスに新規トークンを発行する。	- minter ロールを付与されたアドレスのみ	- コントラクトが一時停止（paused）状態でないこと - _to がブラックリスト登録されていないこと - 呼び出し元が割り当てられた発行上限（minterAllowance）以内の金額であること
2	償還	**burn(uint256 _amount)**	呼び出し元アドレスの残高からトークンを焼却（Burn）し、全体の総供給量を減らす。	- minter ロールを付与されたアドレスのみ	- コントラクトが一時停止状態でないこと - 呼び出し元がブラックリスト登録されていないこと - 呼び出し元アドレスの残高が償還量に充分であること
3	ブラックリスト登録	**blacklist(address _account)**	指定アドレスをブラックリストに追加し、送受信・発行・償還等を禁止する。	- blacklister（ブラックリスト管理権限保有者）のみ実行	- _account が address(0) でないこと
4	ブラックリスト解除	**unBlacklist(address _account)**	指定アドレスをブラックリストから除去し、トークン利用制限を解除する。	- blacklister（ブラックリスト管理権限保有者）のみ実行	- _account が既にブラックリストに登録済みであること
5	一時停止	**pause()**	コントラクト全体を停止状態にし、トークンの送受信・発行・償還を含む一切の機能を停止する。	- pauser ロールを付与されたアドレスのみ	- 既に停止状態でないこと
6	一時停止解除	**unpause()**	コントラクトの機能を再開し、送受信・発行・償還等全機能を復帰させる。	- pauser ロールを付与されたアドレスのみ	- 現在が停止状態（paused = true）であること
7	資金移転	**transfer(address to, uint256 value)**	呼び出し元のアドレスから、指定したアドレスへトークンを送金する（標準ERC20の transfer 関数）。	- すべてのユーザーが呼び出し可能	- コントラクトが一時停止状態でないこと - 呼び出し元および to がブラックリスト登録されていないこと - 呼び出し元アドレスに十分な残高があること

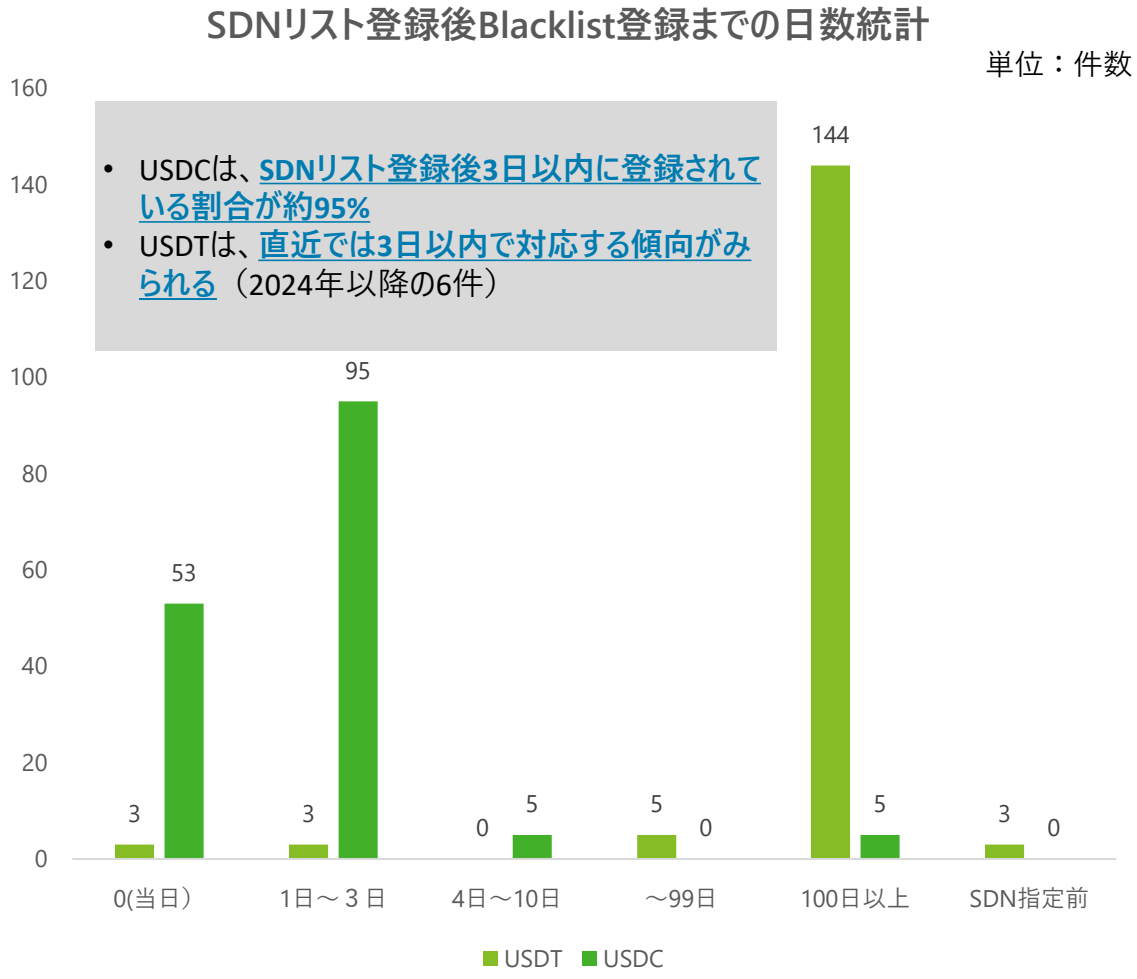
3.主要なステーブルコイン発行者の事業実態調査
3.4 発行者によるblacklistへの登録の状況

USDCは、USDTよりBlacklist対象アドレスが少ないものの、SDN等の制裁に対して素早く対応している傾向が見られます

USDT・USDCのblacklist対象アドレスの推移（ETH）



SDNリスト登録からblacklistに登録までの日数（ETH）



【参考】：「OFAC SDN LIST」（OFAC）_2025年1月時点確認、「 USDT Banned Addresses 」・「 USDC Banned Addresses」（Dune Analytics） _2025年1月時点確認。SDN LISTに登録が確認できる158件

Tetherと当局は暗号資産を使った犯罪に関する個別の調査で連携することで、ステーブルコインの凍結を実施してきました

発行者における規制当局への対応等（USDT）

#	時期	規制当局の動き	Tetherの対応
1	2021年10月	• 米商品先物取引委員会（CFTC）が、Tetherに対して虚偽または誤解を招く発言に関する41百万ドルの罰金を命じる。 • Bitfinexに対して1.5百万ドルの罰金を命じる	• 罰金を支払い、商品取引法（CEA）およびCFTC規制違反行為に対応することに同意
2	2023年11月	• 米国司法省（DOJ）、TetherとOKXの調査を支援し、東南アジアの国際人身売買組織に関連する225百万ドルのUSDTの凍結を要請。	• 国際犯罪組織に関連する225百万ドルのUSDTを自主的に凍結 • DOJとシークレットサービスの調査に協力し、複数のアドレスにかかる不正利用を分析 • 適法なアドレスが凍結された際には、当局と協力して迅速に解除することを約束
3	2024年9月	• 米国司法省（DOJ）、東南アジアの暗号暗号資産詐欺計画に関連する6百万ドル以上の資産を押収	• 米国司法省（DOJ）を支援し、暗号通貨の詐欺計画に関連した6百万ドル以上の資産を凍結

【出所】：「CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million」（CFTC）「Tether News」（Tether、2023年11月,2024年9月）_2025年1月時点確認

Circleは、OFACの制裁対象のサービス等をブロックすることにより当局の求めに応じた対応を行ってきました

発行者における規制当局への対応等（USDT）

#	時期	規制当局の動き	Circleの対応
1	2022年8月	OFAC、Tornado Cashを制裁対象に指定*1 • Tornado Cashが過去3年間で70億ドル以上の暗号資産の洗浄に使用されたという疑いによる指定	• 8月9日、CircleはTornado Cashに関連する38のアドレスをブロック • Tornado Cashアドレスに関連したUSDCの移動を制限する旨発表 • 銀行秘密法（BSA）に基づきCircleは制裁対象のアドレスとの取引をブロックする義務があるとされる
2	2023年5月	OFACは、Circle子会社のPoloniexに複数の制裁プログラムに違反した疑いで約7百万ドルの罰金を命じる	Circleは以下の追加措置を実施 • KYC確認が完了するまでユーザーアカウントを凍結 • 制裁対象国のプロファイル情報を持つユーザーのアカウントを無効化 • シリア、イラン、キューバ、スーダン、北朝鮮に対するジオロケーション制限の実施 • プロファイル情報に「クリミア」と記載されたアカウントの閉鎖 • クリミアIPブラックリストとクリミア市/地域キーワードリストの作成 • トレーニングプログラムの強化と経験豊富なコンプライアンス担当者の雇用

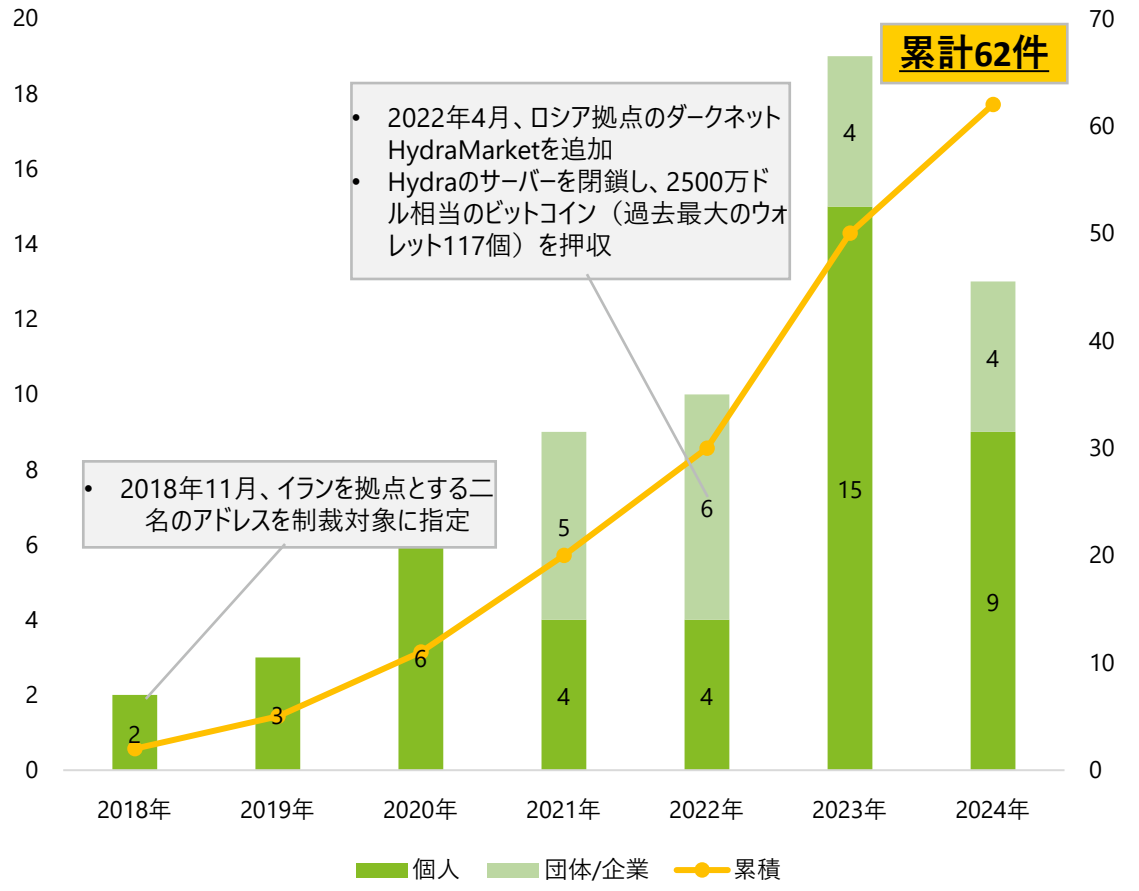
【出所】：「OFAC Sanctions Tornado Cash: Issues & Implications」（Galaxy）「A Settles with Poloniex, LLC for $7,591,630 Related to Apparent Violations of Multiple Sanctions Programs」（OFAC）_2025年2月時点確認

*1 米国財務省は2025年3月21日にTornado Cashに対する制裁を解除 「Tornado Cash Delisting」（米国財務省）

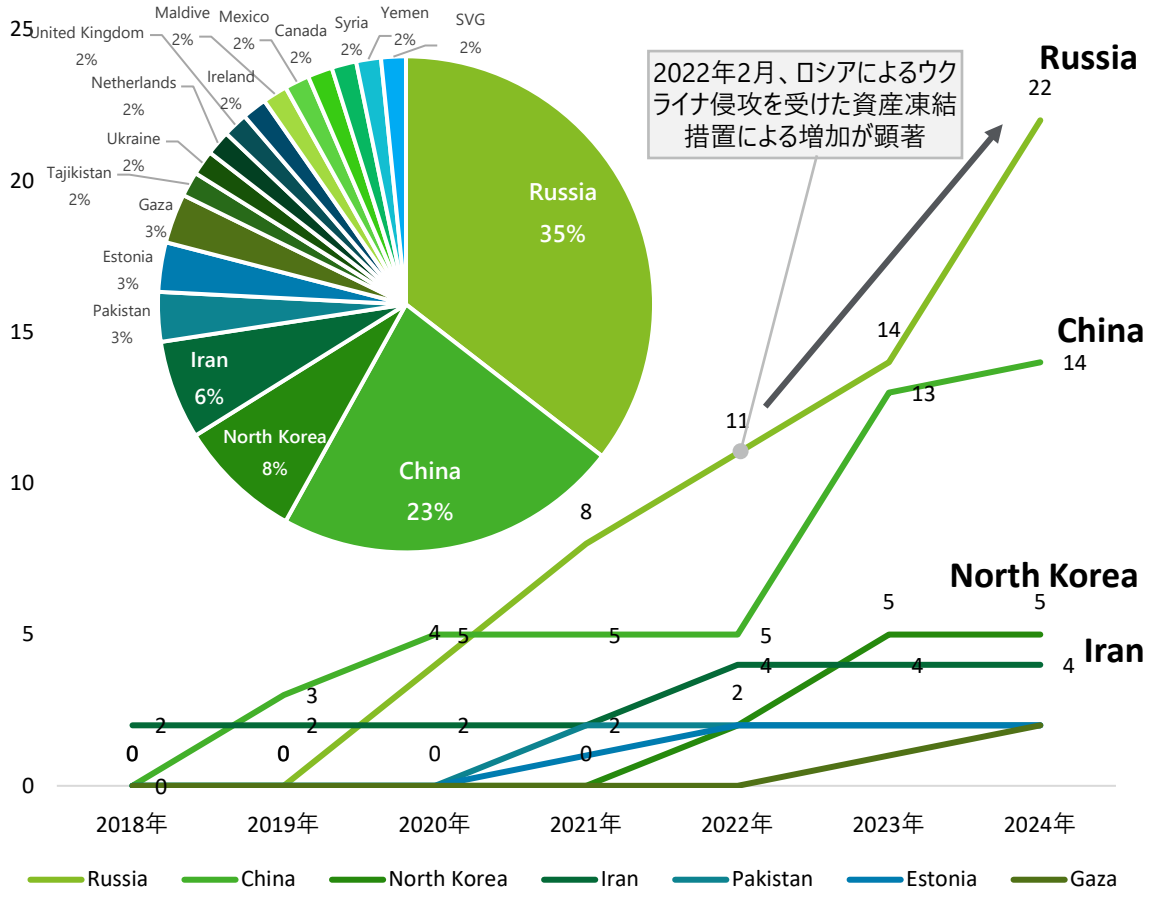
SDNリストへの暗号資産アドレスの登録は2018年11月から始まり、全SDNリスト約17,000件のうち暗号資産にかかるものは62件にのぼります

暗号資産にかかるSDNリストの個人・組織推移

登録された個人・組織推移　単位：登録された個人・組織数



SDNリスト国別累積　単位：登録された個人・組織数



【参考】「OFAC SDN LIST」（OFAC）_2025年1月時点確認

【参考】OFAC Press Releases（OFAC）_2018年11月時点確認、「OFAC Press Releases」（OFAC）_2022年4月時点確認

SDN制裁プログラムの内、暗号資産にかかるリストが最も多く分類されているのは、サイバー攻撃であり、麻薬取引、ロシア、北朝鮮にかかるものの順にリストが登録されています

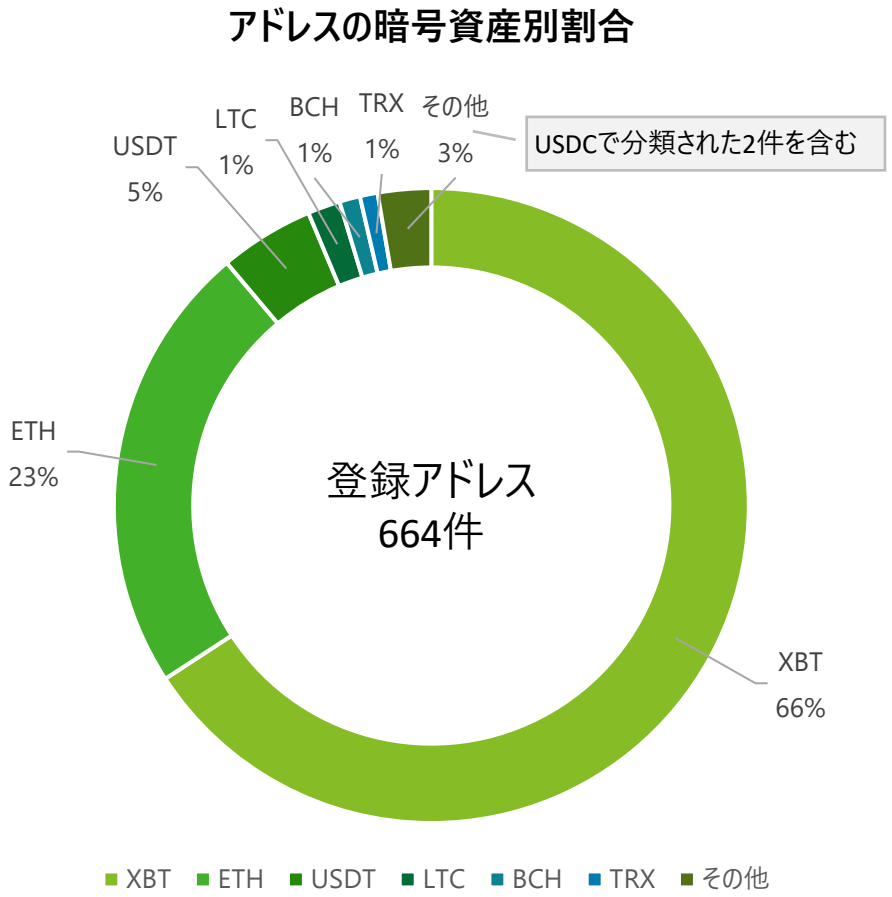
SDNリストに登録された個人・組織の数（制裁プログラム別分類）

類型	制裁プログラム略称	リスト（合計）	リスト（内訳）	定義
サイバー攻撃関連	CYBER2	23 (37%)	14	サイバー攻撃に関与する者に対する制裁
	CYBER2/ELECTION-EO13848		4	サイバー攻撃と選挙への干渉に関する制裁
	CYBER2/RUSSIA-EO14024		1	サイバー攻撃とロシアの悪意ある活動に関する制裁
	IRGC/IFSR/CYBER2		2	イラン、サイバー攻撃に関する制裁
	UKRAINE-EO13661/CYBER2/ELECTION-EO13848		1	ウクライナ、サイバー攻撃、選挙干渉に関する制裁
	NPWMD/CYBER2/ELECTION-EO13848		1	大量破壊兵器拡散防止、サイバー攻撃、選挙干渉に関する制裁
テロ関連	SDGT	6 (9%)	5	特定の国際テロリストに対する制裁
	SDGT/IFSR		1	特定の国際テロリストとイランに関する制裁
麻薬取引関連	SDNTK	14 (22%)	3	麻薬取引に関与する外国人および団体に対する制裁
	ILLICIT-DRUGS-EO14059		11	違法薬物取引に関与する者に対する制裁
大量破壊兵器関連	NPWMD	1 (1%)	1	大量破壊兵器拡散に関する制裁
北朝鮮関連	DPRK4	8 (12%)	1	北朝鮮に関する制裁
	DPRK3		2	北朝鮮に関する制裁
	DPRK3/CYBER2		5	北朝鮮とサイバー攻撃に関する制裁
ロシア関連	RUSSIA-EO14024	10 (16%)	10	ロシアの悪意ある活動に関与する者に対する制裁
合計		62		

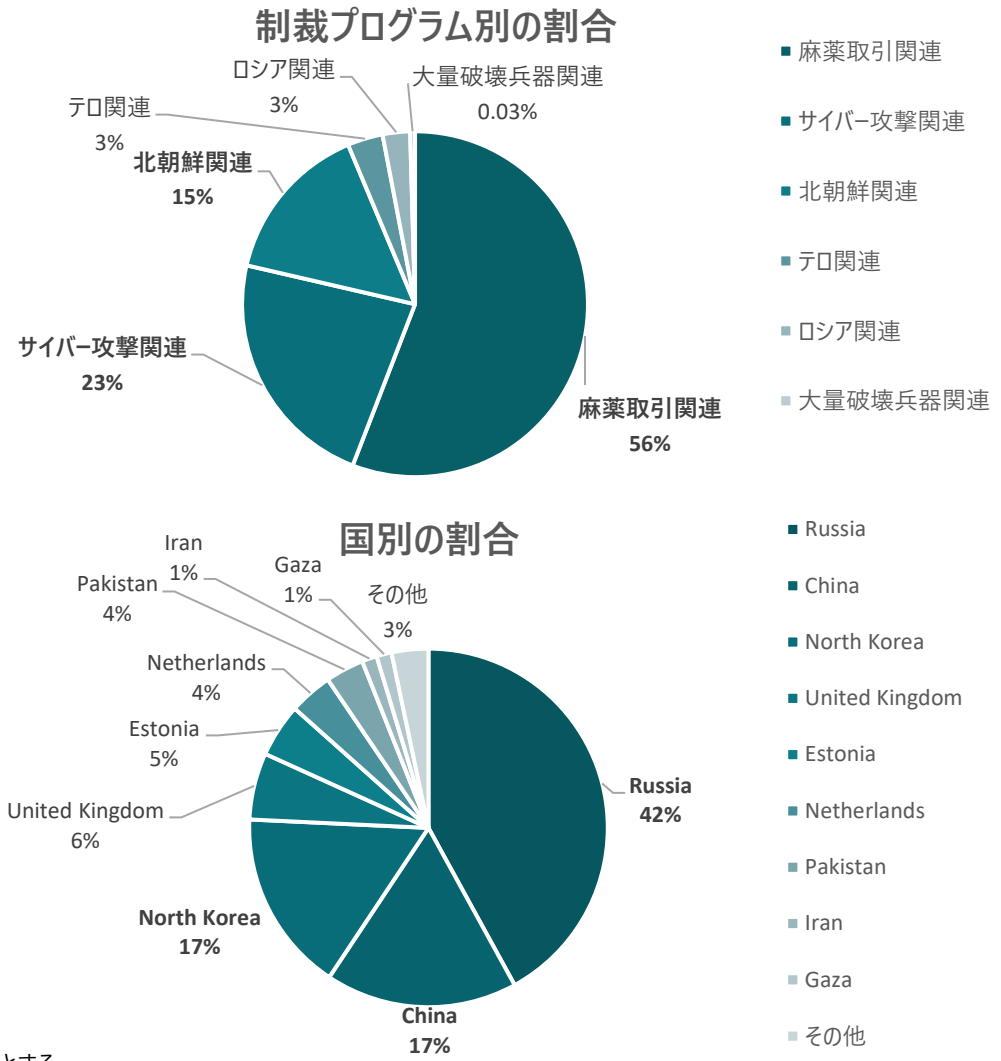
【参考】：「OFAC SDN LIST」、「Program Tag Definitions for OFAC Sanctions Lists」(OFAC)の2025年1月17日時点の情報_2025年1月時点確認

SDNに登録されているアドレス数は、XBT（ビットコイン）とETHで89%を占めており、制裁プログラム別には麻薬取引、国別ではロシアが最も多く登録されています

SDNに登録されたアドレスの内訳（暗号資産別）



内訳（制裁プログラムおよび国別）



【参考】：「OFAC SDN LIST」（OFAC）_2025年1月時点確認。Digital Currency Addressが登録されている個人、組織を対象とする。
国別分類は、個人の場合、国籍・市民権、組織の場合、住所、プログラム等に基づき分類

3.主要なステーブルコイン発行者の事業実態調査
3.5発行者における技術トレンドに対する新たな取り組み

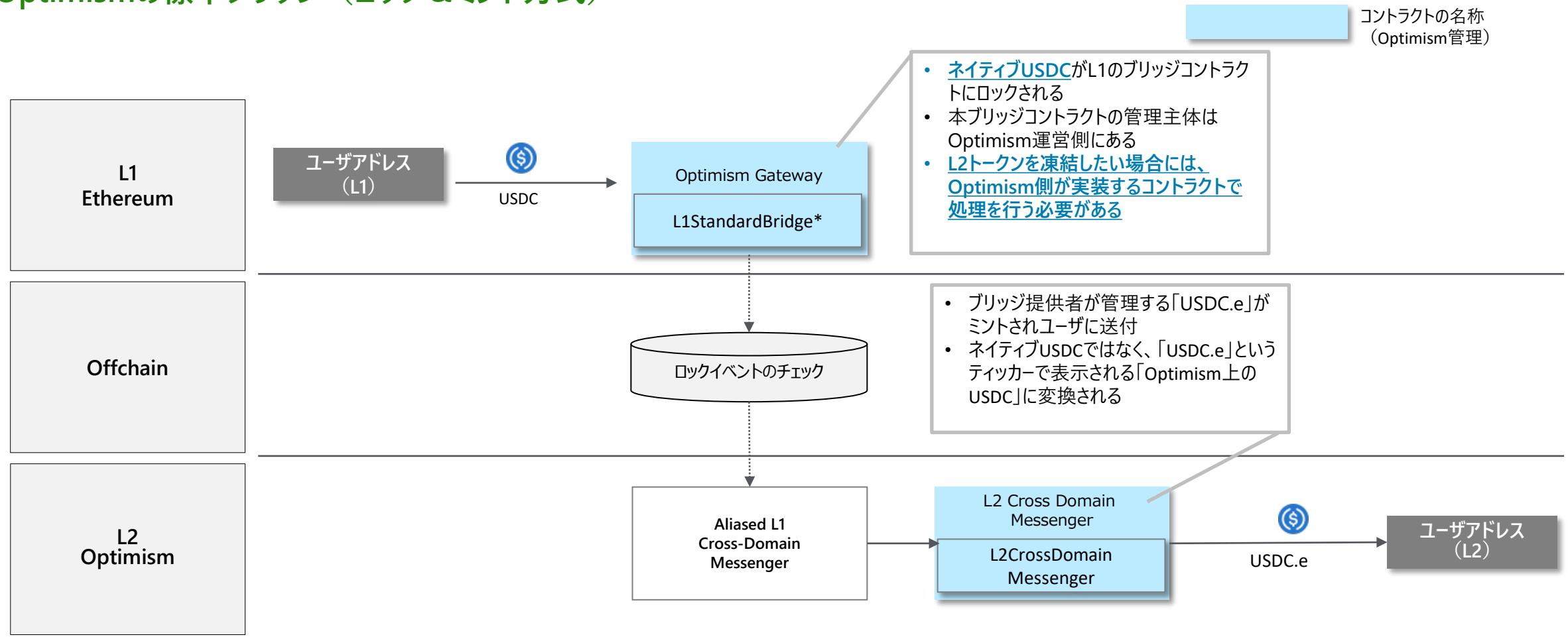
盗難経路を隠蔽するMixingや複数チェーンをまたぐChain-hopping等に対して、犯罪の追跡や未然防止のため発行者・分析会社との更なる協力体制が課題です

【再掲】ステーブルコインの不正利用において洗浄にかかる主な技術と対応の方向性

#	不正に利用される技術	対応の方向性	残課題	関連プロトコル
①	■ ステーブルコインとMixingサービスを活用した盗難経路の隠蔽 ➢ ステーブルコインをMixingサービス経由で複数ユーザーのトランザクションと混ぜ合わせ、別アドレスに払い出し → 別口座や別チェーンへ移動、という流れで盗難経路を隠蔽する	■ Mixingサービスを行う業者のアドレスやスマートコントラクトを制裁リストに追加し、送金時にチェックする 【ステークホルダー別の対処案】 • 発行者 監視・追跡・検閲機能の実装、Mixingサービスの規制 • 仲介業者/ユーザー 分析会社が提供する疑わしい取引先、制裁リストのチェック、ウォレットからの注意喚起	■ 疑わしい取引先および制裁リストチェックを如何に強制させるか ■ 方式によって通常の取引と判別できない不正取引手法（Coinjoin等）の分析・抽出方法の確立	• 中央集権型ミキサー(Blender.io等) • 分散型ミキサー(Coinjoin等) • スマートコントラクト型ミキサー(Tornado Cash等)
②	■ Chain-hoppingを活用したLayer2等の異なるチェーンを経由したステーブルコインの洗浄 ➢ 盗難コインを短時間で連続して複数のチェーンにブリッジ し、チェーンごとに異なるウォレットを使う等、追跡を困難にさせる。最終的に暗号資産取引所やOTC・P2P取引で法定通貨に換金する ➢ スケーラビリティ向上や手数料削減を目的としたLayer2（L2）において、通貨をブリッジしてL2側で転々 流通させることで、追跡困難にしている	■ 複数のブロックチェーンを跨いだクロスチェーンの取引情報をグラフ化するブロックチェーン分析ツールを使い追跡する 【ステークホルダー別の対処案】 • 発行者 監視・追跡・検閲機能の実装、分析ツールの提供 • 仲介業者/ユーザー 分析会社にてチェーン間取引を監視し、追跡不能な取引の振る舞いや前後関係から怪しい動きをAI等で抽出する等のより高度な分析ツールやコードの提供（Blockaidサービス等）	■ ブロックチェーンの仕様に合わせて分析ツールを適合させていく必要がある	• Optimistic Rollup • ZK Rollup • Wrapped Tokens • Cosmos/Polkadot • Inter-Blockchain Communication • Cross-Chain Transfer Protocol (CCTP)

ロック＆ミント方式のブリッジの場合、Layer2のトークンにかかるコントラクトの管理権限が発行者から離れてしまうため、発行者が実装したBlacklist機能が使えなくなる課題が生じます

Optimismの標準ブリッジ（ロック＆ミント方式）

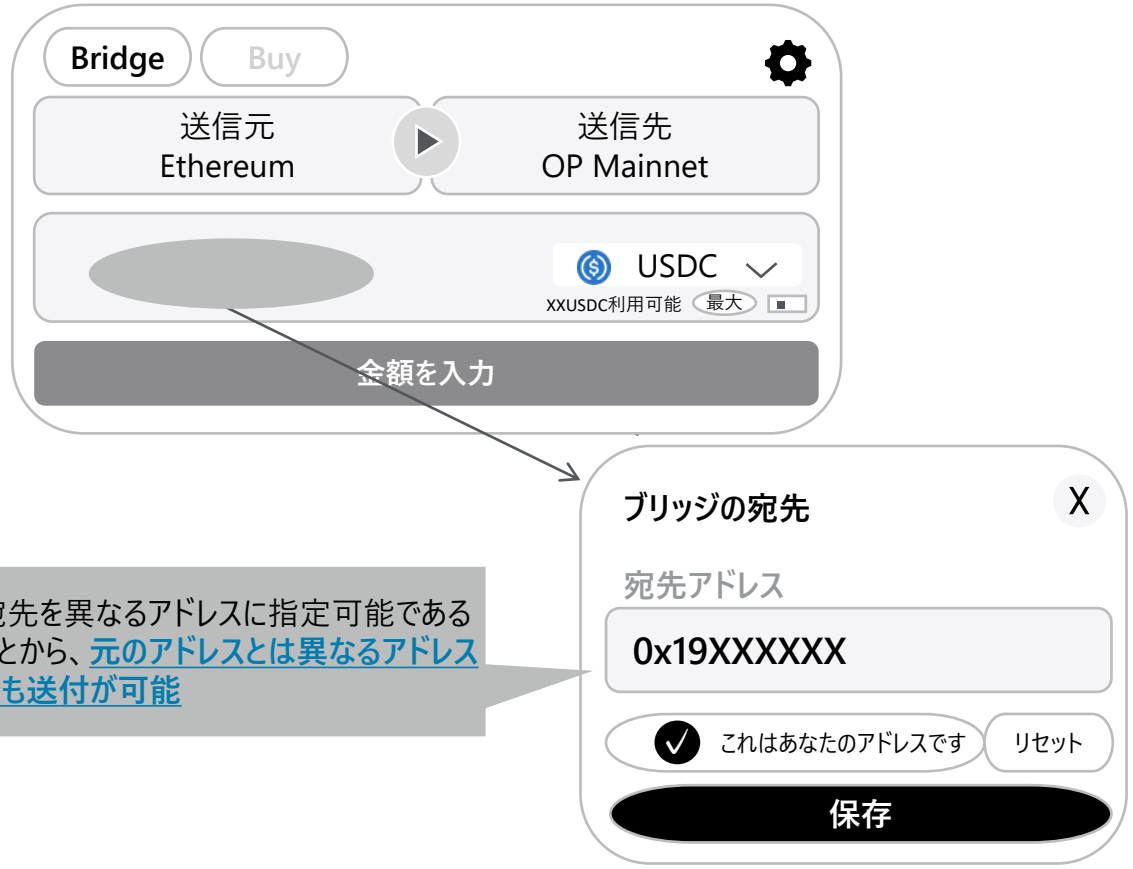


【参考】：「Transaction Details」（Etherscan） _2025年1月時点確認、「Transaction Details」（Basescan） _2025年1月時点確認

ブリッジソリューション側のコントラクトにもblacklistの機能を実装することは可能であるが、運用実績として特筆するべき事実は検出できませんでした

ブリッジのUI（例）

様々なBridgeをアグリゲートしたサービスでは、他のブロックチェーンの送付先にトークンを送ることが可能で、UIも分かりやすく利便性が高いサービスとなっている



宛先を異なるアドレスに指定可能であることから、元のアドレスとは異なるアドレスにも送付が可能

【参考】：「Token USD Coin (Bridged from Ethereum)」（OP Mainnet、2025年1月）

ブリッジコントラクトにおけるBlacklistの有無

ブリッジ（Optimism）が管理するUSDC.eのコントラクトにはソースコード上ブラックリストを設定する機能は存在するが、ブラックリストの登録を実施した記録は存在しなかった。

1．allowance (0xdd62ed3e)

2．balanceOf (0x70a08231)

3．blacklister (0xbd102430)

0x0000000000000000000000000000000000000000 address

4．decimals (0x313ce567)

5．isBlacklisted (0xfe575a87)

6．l1Token (0xc01e1bd6)

7．l2Bridge (0xae16faaf)

8．name (0x06fdde03)

USD Coin *string*

9．owner (0x8da5cb5b)

0x9028967bCb7c8eA664813714c5f2F54f84FDB308 address

10．paused (0x5c975abb)

11．pauser (0x9fd0506d)

0x0000000000000000000000000000000000000000 address

- blacklisterというコントラクトがあるものの、無効アドレスが登録されており、使用できなくなっている
- なお、当該コントラクトから発生したイベントを調査したが、特定アドレスをブラックリストに登録した記録は存在しなかったことから過去においても使われた事実はない（Dune Analytics を使用して過去イベントを調査）

- 当該OwnerはGoosisSafeによって2 of 3のマルチシグで構成されているが当該署名鍵は、Optimism運営側が管理している

Circleは、バーン＆ミントにより、Layer2等で流通するトークンも自社で実装したコントラクトで一元管理する方法を広める方針をもっています

Circle CCTPの概要・対応チェーン

概要

■ **概要**

➢ Circle CCTP（Cross-Chain Transfer Protocol）は、バーン＆ミントの仕組みを活用して「常にネイティブなUSDC」を異なるブロックチェーン間で移動させるプロトコル

■ **主な特徴**

➢ USDCのネイティブトークン性の維持
特定のコントラクトアドレスにネイティブトークンをロックせず、すべてUSDCのコントロール下にあるコントラクト上で発行される

➢ オフチェーン処理も含むCircle一括管理
Circleがオラクルと検証プロセスをも含めた全プロセスを一元的に扱うため、各ブリッジソリューションに懸念される不正なミントや二重発行の防止を回避

➢ Circleへの集中リスクの懸念
CircleがUSDC全体を一元管理するアーキテクチャであるため、Circle自身の不正や誤操作等のリスクが生じる

対応チェーン

■ 現在 9 つのチェーンに対応
Aribitrum、Avalanche、Base、Ethereum、Noble、OP Mainnet、PolygonPoS、Solana、Sui

■ 今後サポートされる予定のチェーン

➢ Aptos、Unichain

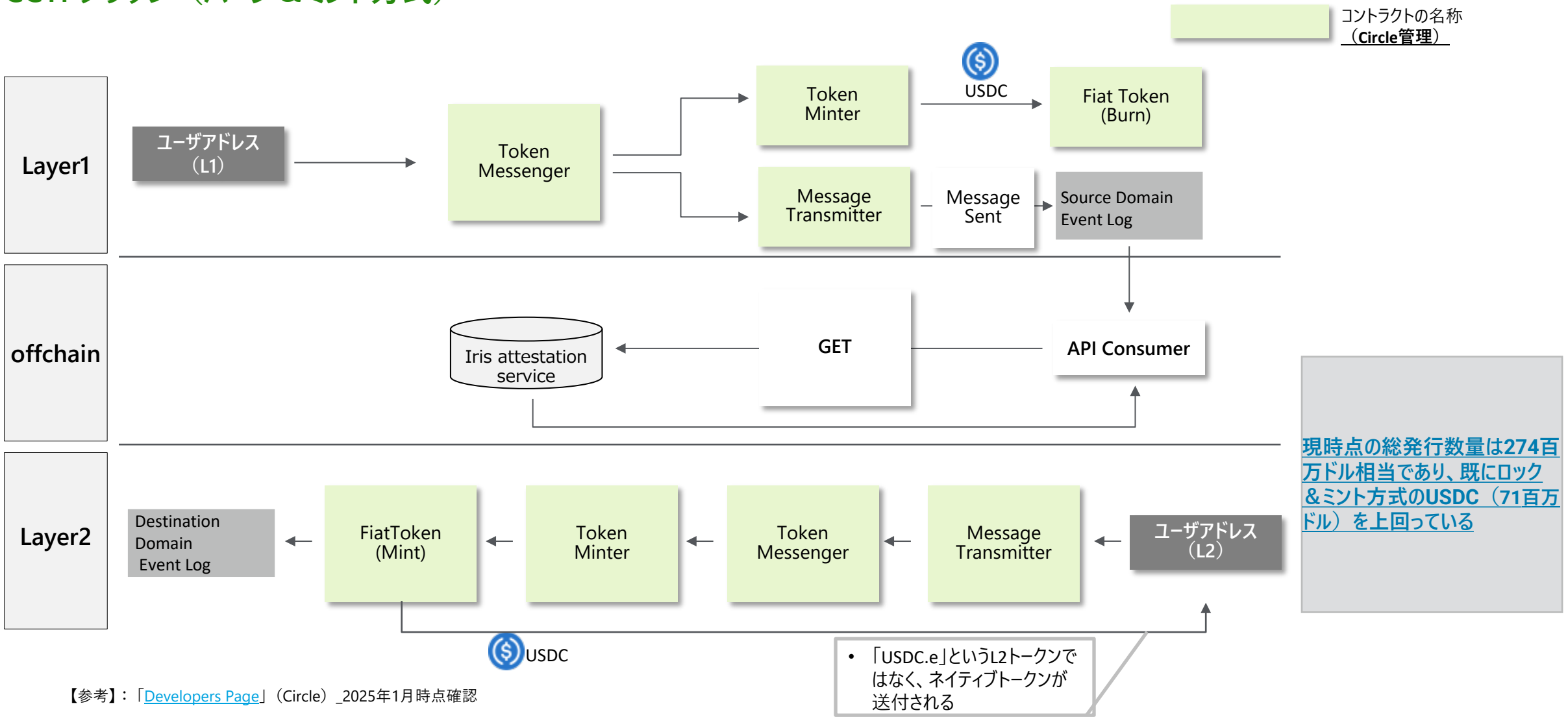
【参考】：「cross-chain-transfer-protocol」（Circle）、「Developers Page」（Circle）_2025年1月時点確認

従来型ブリッジとCircle CCTPとの比較

区分	従来型ブリッジ（Lock & Mint）	Circle CCTP（Burn & Mint）
発行	• 送信元チェーンでトークンをブリッジコントラクトアドレスにロックし、送信先のチェーンで同量のトークンをミント • コントラクトの管理者は、ブリッジソリューションの運営者側にある	• 送金元チェーンの USDC をバーンし、送金先チェーンで USDC をミントする • コントラクト管理者はCircleとなる
償還	• 送信先トークンで直接Circleに償還を依頼することができず、一旦引き出し処理を行い、ネイティブトークンに戻したうえで償還を請求する必要がある	• 送信先トークン自体がCircle管理となっているため、当該トークンをもって直接償還請求が可能
ハッキングリスク	• 送信元トークンをロックするためのコントラクトに大量の資産がロックされるため攻撃対象になる可能性が高まる	• ブリッジ・コントラクトに資産をロックしないため、大規模流出リスクが低い
運用・管理の複雑さ	• 各ブリッジソリューションごとの運営者への信頼が必要となる • ブリッジソリューションごとに運営方法やガバナンス強度も異なる上に、その方法等が公開されていない部分も多く、評価が不透明になる	• Circle が一元的に管理するため、チェーンごとの運営方法の違いから生じる不正リスクや事務リスクを無視できる
拡張性	• 対象チェーンごとにカスタマイズが必要な場合がある	• Circle が対応するチェーン間であれば共通のプロトコルで扱える

バーン＆ミント方式で実装されるCCTPは、発行・償還に関するコントラクトをCircle社が実装するコントラクトで管理できるため、blacklist機能の効果をLayer2上でも及ぼすことができます

CCTPブリッジ（バーン＆ミント方式）



【参考】：「Developers Page」（Circle）_2025年1月時点確認

（参考）直近発覚事案の研究

2025年2月に「Bybit」ハッキング事件が発生し、被害金額は約15億ドル相当で、過去最高被害額となりました

「Bybit」事案 - ①攻撃の発生

2025年2月21日、暗号資産取引所であるバイビット（Bybit）で、15億ドル相当のイーサ（ETH）が盗まれるという流出事件が発生。攻撃の手口は、2024年5月に発生したDMMビットコインの事案とソーシャルエンジニアリングを使うなどの類似性が指摘されている。この時の教訓が活かされなかったことから、業界内に情報共有上の重要な課題があると考えられる。

	AWS S3スクリプトファイル改ざんの流れ	ブロックチェーン上での流れ
事前処理	不正なスクリプトへ差し替え ■ 攻撃者はSAFEのAWS S3バケット内のフロントエンドJavaScriptファイルを改ざんし、悪意のあるスクリプトを埋め込んだ。この改ざんされたWebアプリがユーザーに提供され、Bybitの署名担当者が影響を受けた	不正コントラクトのデプロイ ■ 攻撃者は２つのコントラクトを事前にEthereum上にデプロイ。１つ目はトロイの木馬コントラクト、２つ目にバックドアコントラクト
事件発生	トランザクションの不正操作 ■ 署名者がSAFEでトランザクションを承認する際、悪意のあるスクリプトが実行され、トランザクションの詳細（送金先やデータ）が書き換えられた。画面上では正しい情報が表示されていたが、実際にはハッカーのアドレスへ送金されていた。この不正操作は特定の条件下でのみ作動し、一般ユーザーには影響を与えなかった	不正コントラクトへの書き換え ■ 正しい署名者によって作成された不正なトランザクションは、トロイの木馬コントラクトを実行し、BybitのコールドウォレットのImplementationコントラクトを正常なコントラクトから、事前に仕掛けられていたバックドアコントラクトへ向け先が変更される 不正コントラクトを利用して資金を窃取 ■ 攻撃者はバックドアコントラクトのsweepETHとsweepERC20関数を使って、Bybitのコールドウォレットに保管されているETHやstETHなど資金を窃取した
事後処理	証拠の隠滅 ■ 資金の盗難後2分以内に改ざんしたJavaScriptを元に戻し、痕跡を消去したことで発覚を遅らせた	資金のクリーニング ■ 攻撃者は窃取した資金を複数のアドレスへ分割、またはチェーンホッピングで他のチェーンに移動しながら資金の追跡を難読化した

【参考】：公開情報_2025年3月時点確認

事件発生後、業界各者が迅速に動き、数日間で犯罪者の正体を解明し、公開捜査を展開することで被害資金の追跡と回収を開始しました

「Bybit」事案 - ②事件発生後の初動対応

事件発生後、発行者、取引所、オンチェーン調査会社、分析ツール会社など業界各者によるコラボレーションが見られ、数日間で攻撃主体を特定
Bybitによる回収報奨金プログラムを発動し、迅速な公開捜査が展開され、一部被害資金を凍結

2025/2/21

Bybitが攻撃され、約15億ドル相当のETHがSafeのコールドウォレットから流出したと発覚

2025/2/22

TetherのCEOが、ハッキングに関連する181,000 USDT を凍結したと発表

Bybitは、回収に貢献した人に回収資金の10%を報奨として寄付すると発表

2025/2/23

2025/2/24

Bybitが、業界各者からの手がかり情報をもとに、疑わしいアドレスをBlacklistに更新するAPIをリリース

2025/2/25

Bybitは、報奨金の貢献サイトを公開(Lazarusbounty)

2025/2/26

FBIは、本件犯罪者が北朝鮮のハッカー・グループである判定、およびプライベート・セクターも活用可能な犯罪者所持アドレスのリストを発表

＜事件発生1週間＞ 2025/2/27

TRM Labsは、初期段階における資金洗浄手法の分析を発表

ZachXBT（独立調査員）、Arkham Intelligence、Beosin、TRM Labs、Halbornなどのオンチェーン調査員が、Lazarus Group（北朝鮮のハッカー・グループ）が使用しているアドレスとの関連性や資金の流れなどを解明

Chainalysisは、2025/2/24より本件に関するレポートを公開開始し、2025/2/26にTether社と協力して約10万ドルを凍結したと発表

Ellipticは、不正と判断するアドレスを随時公開し、それらアドレスをBlacklistに更新するAPI も提供（2025/2/25にアドレス公開開始、2/28時点で14,497件を公開済）

【参考】：公開情報_2025年3月時点確認

初期段階において、犯罪者による特徴的な資金洗浄手法がみられ、短時間で大半の資金を洗浄しました

「Bybit」事案 - ③犯罪者の初期資金洗浄手法

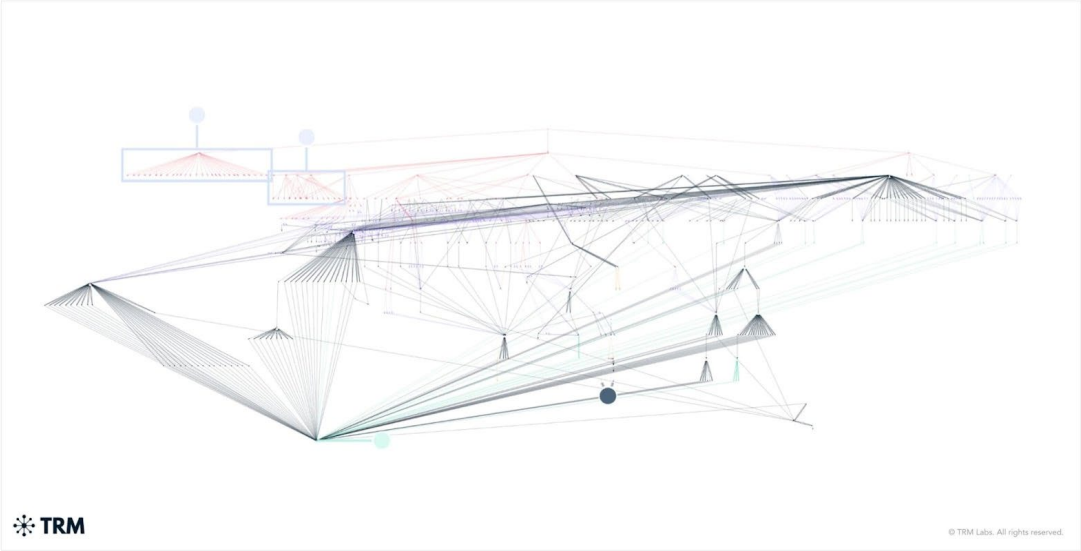
Lazarus Groupの初期（約1週間目）の洗浄プロセスには以下の特徴がみられ、同グループの過去事案での手法と比べても追跡の困難性が増している

■ 高速なオペレーション
- 攻撃者による資金洗浄の「スピード」が大幅に増した
- 事件発生後48時間以内に、少なくとも1億6000万ドルの移動が成功
- このスピードは、Lazarus Groupがマネーロンダリングのインフラを拡大したか、中国などにある地下の金融ネットワークを拡大したことを示唆

■ 多様な経路
- この迅速な洗浄プロセスには、複数の中間ウォレットを介した送金、異なる暗号通貨への変換、分散型取引所(DEX)の使用、クロスチェーンブリッジの使用など操作がみられた
- Lazarus Groupの過去事案において初期段階はミキサーに頼ってきたが、本件ではより多様なブロックチェーン・サービスを利用して資金を洗浄した

■ ビットコインへの変換
- 大半の資金は直接ビットコインに変換された
- 換金されたビットコインのほとんどは動きがなく、犯罪者が大規模な換金や、OTCネットワークを通じたさらなる洗浄に備えていることを示唆している

資金洗浄のプロセスを可視化したグラフ（ 2025/2/26時点）



TRMの北朝鮮専門家
(前職FBI SME)

本件の初期の資金洗浄は、犯罪者が「ゾーンを氾濫させる(Flood the zone)」テクニックを強化していることを示している。複数のプラットフォームにわたる高速で高頻度のトランザクションによって、コンプライアンスチーム、ブロックチェーン調査員と法執行機関を圧倒(overwhelm)し、資金の追跡を複雑にしている。

【参考】：「The Bybit Hack: Following North Korea's Largest Exploit」（TRM Labs）_2025年3月時点確認

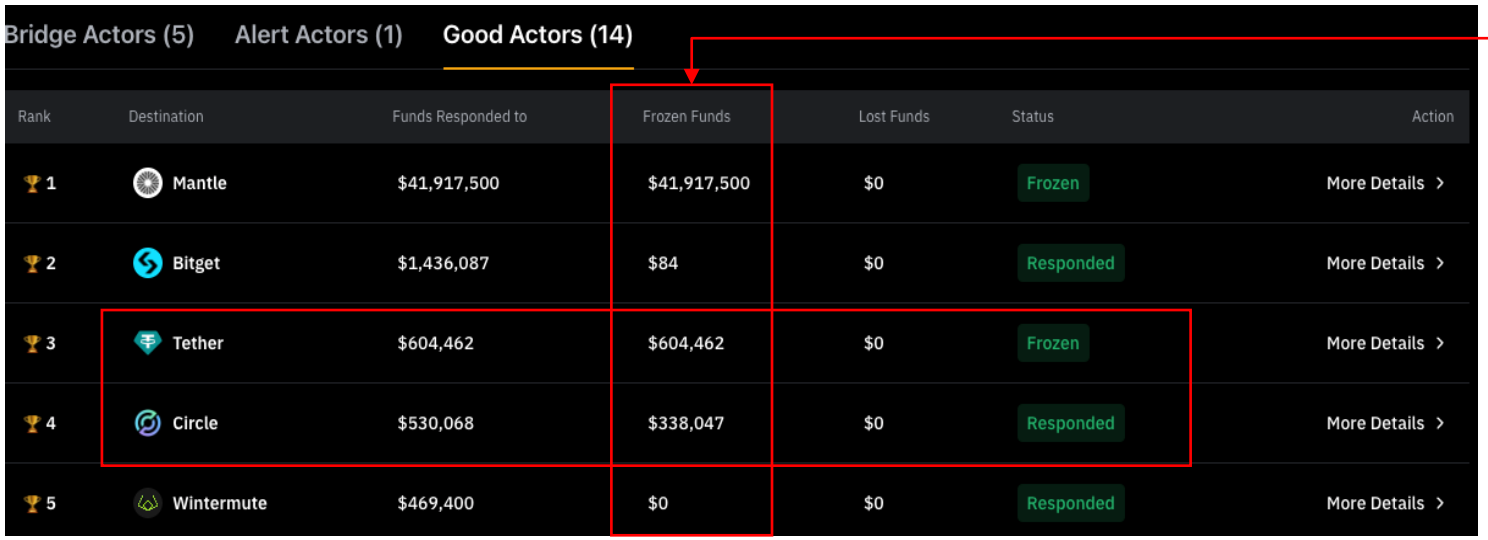
Bybitの回収報奨金プログラムの発動とともに、業界各者が協力する公開捜査の形で被害資金の回収に努めていると考えられます

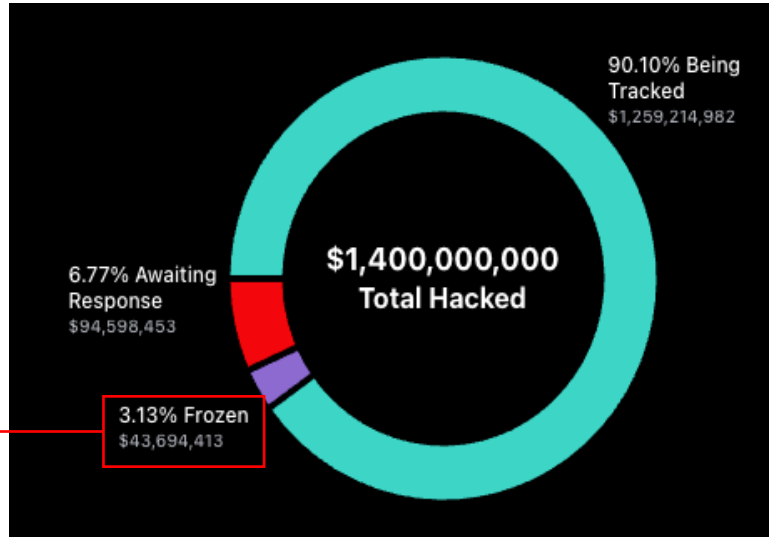
「Bybit」事案 - ④公開捜査による資金の追跡と回収(2025/3/7時点)

- Bybitは事件発生の直後に回収報奨金プログラムを発動し、「良いアクター」と「悪いアクター」を公にランク付ける報奨金貢献サイト（Lazarusbounty）を立ち上げた。このような公開捜査の仕組みにより、取引所、ミキサー、その他の業界関係者に、不正行為に対して迅速に行動するようインセンティブ付けた。

- BybitのCEOはXで2025/3/4時点の状況を公開し、被害資金の77%は追跡可能、20%は回収不可能、3%は凍結済。特に、83%の資金は犯罪者の洗浄によりビットコインに変換され、6,954のウォレットに分散している状態にあるため、取引所、OTCやP2Pプラットフォームで換金される前に食い止めるには、この2週間が非常に肝心であると述べた。また、回収報奨金プログラムについて、11の回収成功者に$2,178,797 USDTの報奨金を支払った、とも述べた。

- 報奨金の貢献サイト（Lazarusbounty）において資金の回収状況をリアルタイムに更新しており、2025/3/5日本時間11:00までに、被害資金の3.13%は凍結でき、ステーブル・コインのイシュアであるTether社とCircle社も資金凍結に貢献している。





【参考】：「Lazarusbountyについて：Bybitのラザロスグループに対する取り組みに参加する方法」（Bybit）、BybitのCEOのツイート、「報奨金の貢献サイト（Lazarusbounty）」（Bybit）_2025年3月時点確認