デジタル・分散型金融への対応のあり方等に関する研究会（令和8事務年度第3回）

資料2

事務局説明資料

2026年11月26日

金融庁
Financial Services Agency, the Japanese Government

成長投資を促進するための金融戦略（2026年7月21日公表）
金融システムを支えるインフラへの投資

デジタル分散型金融への対応のあり方等に関する研究会（令和８事務年度）
第１回事務局説明資料（2026年10月）

課題

- AI時代を見据え、「24時間365日連続稼働」、「商流・物流と繋がるプログラマビリティ」、「決済基盤として信頼される安定性・安全性」の要素を備えた、ブロックチェーン技術を基盤とする「オンチェーン金融」の推進が重要。
- また、AI技術の進展に伴うサイバーリスクへの対処など、金融機関・金融システムへの信頼確保も不可欠。

対応

■ AI時代を見据えたオンチェーン金融イニシアティブ

金融庁が民間の資金決済全体の在り方について主導的役割を果たしつつ、 AI時代を見据えたオンチェーン金融実現に向け、以下の３つの切り口から、関係省庁等とともに議論、検討を行う「**AI時代を見据えたオンチェーン金融フォーラム**」を2026年夏に立ち上げ、**2027年初を目指して中間整理**

1. オンチェーン金融の社会実装の推進

官民連携でのロードマップ作成、決済高度化プロジェクト（PIP）を通じた**官民連携でのユースケース拡大支援**、アジアを含む**国際的な連携・発信**等

2. オンチェーン金融を発展させる環境整備

①**ステーブルコインの制度的枠組み**、②**様々な資産のトークン化に関する制度**、③分散型取引所（DEX）をはじめとする**分散型金融**（DeFi）**やウォレット提供業者に関するリスク低減策**の在り方の点検・検討

3. 新時代を支えるAI等の技術への適応

金融分野における**AIの浸透に応じた市場・金融機関の監督の在り方**の検討、**金融インフラにおけるブロックチェーンの量子耐性確保**に向けた検討

■ 金融機関・金融システムへの信頼の確保

- **フロンティアAIモデルによるサイバー脅威**の緊要性の増大を踏まえ、**官民連携して実効性ある対策を検討・推進**
- **プライベートクレジットのモニタリング実施**（金融機関のリスクテイク方針・管理態勢や、個人投資家向けの販売・管理態勢等を確認）
- 上場企業による会計不正事案を踏まえた、事案の究明・必要な処分の実施、再発防止の徹底

目次

I. 分散型金融（DeFi）に関するリスク低減策

A) DeFiの概要

B) DeFiに関する規制アプローチとリスク低減策

II. ウォレット提供業者（アンホステッド・ウォレット）に関するリスク低減策

A) アンホステッド・ウォレットの概要

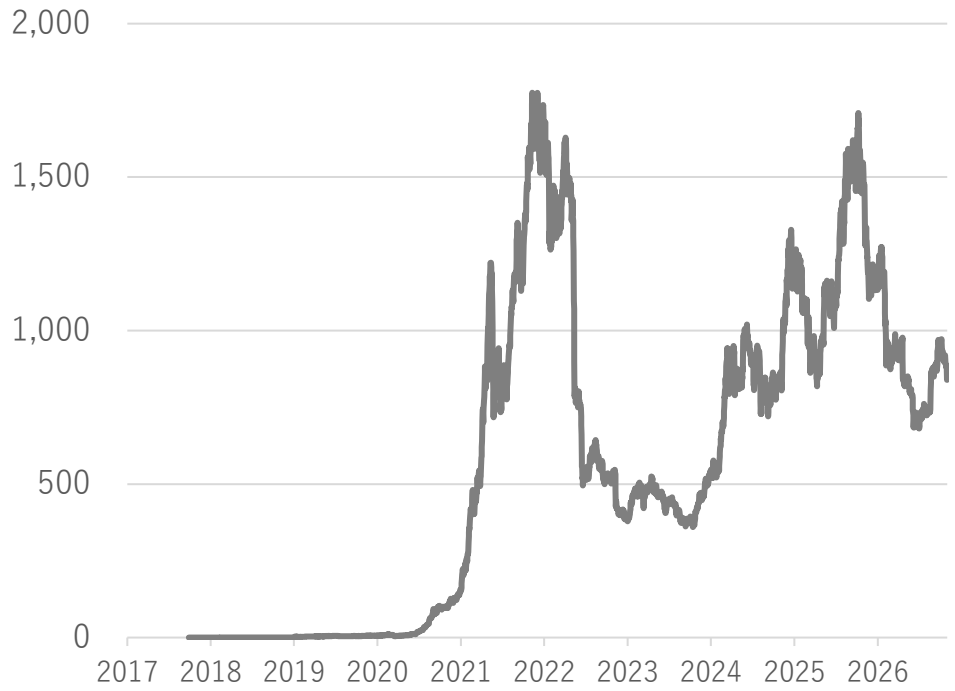
B) アンホステッド・ウォレットに関する規制アプローチとリスク低減策

III. ご議論いただきたい事項

DeFiの概要

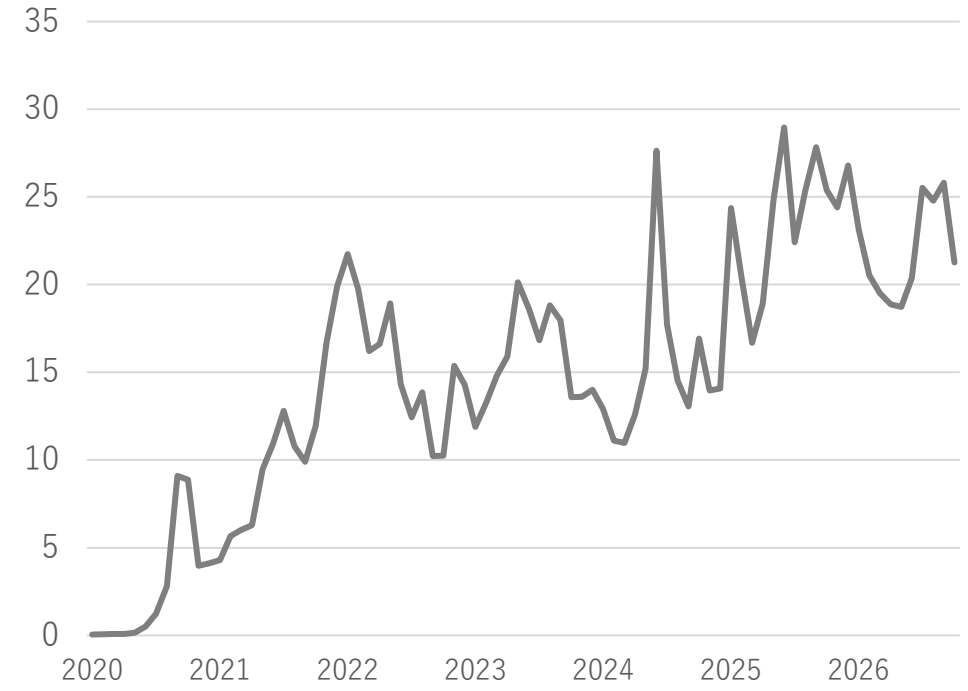
- いわゆるDeFi（Decentralized Finance：分散型金融）について明確な定義は存在しないが、FATFが2026年7月に公表したDeFi報告書（DeFiに係る規制上の課題に関する報告書）では、「一般に、売買、交換、貸付け、借入れ及び資産運用などの金融サービスを、従来の金融仲介業者ではなく、ブロックチェーン上の自律執行型スマートコントラクトを通じて提供する仕組み」と説明している。
- DeFi llamaのデータによると、DeFiのTVL（Total Value Locked ：DeFiサービスでロックされている資産の総額）は、2026年6月10日時点で約866.4億ドルとなっており、2023年5月10日時点の約468.6億ドルから約85%増加している。また、DEX（Decentralized Exchange：分散型取引所）の取引量は、CEX（Centralized Exchange：中央集権型取引所）の取引量と比べても一定の存在感を示しつつある。

DeFiのTVLの推移



（出所）DeFi llama（2017年9月27日～2026年10月31日のデータ）

DEX対CEX現物取引量比率



（出所）DeFi llama（2020年1月1日～2026年10月31日のデータ）

DeFiへの関心の高まり

- FATFのDeFi報告書は、金融セクターではパーミッション・パーミッションレスの双方の環境において**DeFiアレンジメントとの連携に対する関心が高まっていると**指摘している。金融機関、VASPとDeFiアレンジメントの相互接続が進むにつれ、DeFiエコシステム内で生じる事象がAML/CFTコンプライアンスにより広範な影響を及ぼす可能性があると指摘している。
- Coinbase及びEY-Parthenonが共同で実施した、**グローバルな機関投資家**351者を対象とする調査によると、**回答者の56%が2028年までにDeFiプロトコルを利用する意向**を示している。また、主な利用目的として、貸付け及びデリバティブ取引が挙げられている。

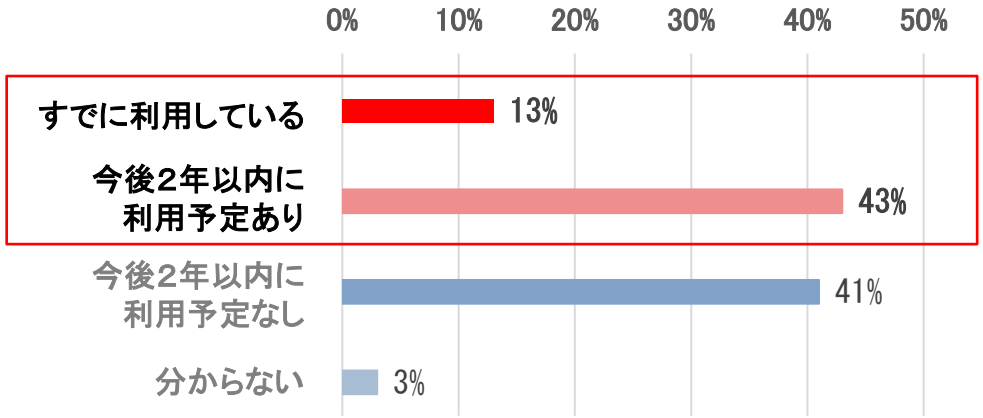
DeFiアレンジメントとの連携への関心の高まりの背景（FATF）

自動化された決済・清算	クロスボーダー取引機会の拡大	24時間365日稼働	相対的な高利回り

グローバルな機関投資家のDeFi利用の意向

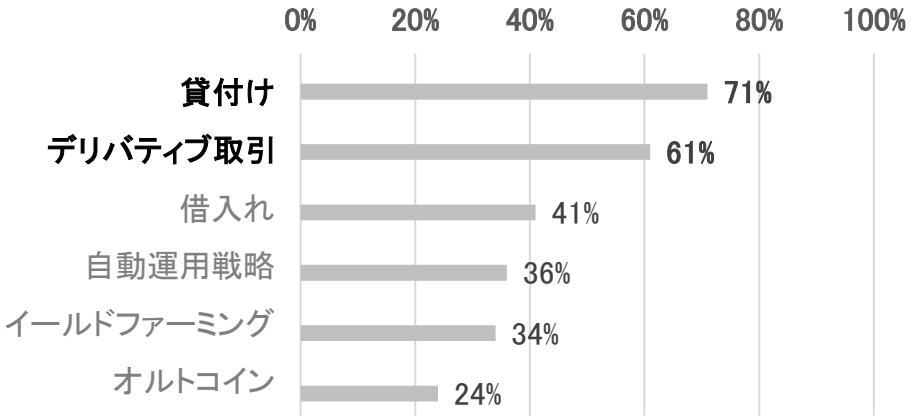
DeFiプロトコルを利用しているか。 [n=351]

例：仲介者を介さず、ブロックチェーン上のアプリケーションを利用して、貸付け、取引、イールドファーミング等を行うこと



特に関心のあるユースケース（上位3つ） [n=198]

（DeFiプロトコルをすでに利用している、利用予定ありの場合）



（出所）2026 Institutional Investor Digital Assets Survey (Coinbase & EY-Parthenon, 2026)

DeFiアレンジメントの特徴（FATF）

■ FATFのDeFi報告書では、DeFiアレンジメントを「DeFiのサービスを機能させるための人員、ガバナンス構造及び運営上の要素を含む、より広範なエコシステム」と定義し、以下の6つの特徴を挙げている。

DeFiアレンジメント固有の特徴

①スマートコントラクトによる自動化

特徴	公開されたスマートコントラクトが金融サービス・機能を完全に自動執行
リスク	支配を特定の者に帰属させることが困難

②オープンソース・組み合わせ可能

特徴	オープンソースで誰でもコードを検証・利用・複製可能、複数のDeFiサービスの相互接続も容易
リスク	複数のDeFiレイヤーや無登録オフショアVASP等を跨ぐ高速な資金移動に悪用

③アルゴリズムによる市場運営・リスク管理

特徴	AMM、流動性プール、レンディング機能等を通じた金利の自動調整や担保割れ時の自動清算
リスク	従来のコンプライアンスツールやブロックチェーン分析では監視困難な複層的取引

④利用者による流動性供給と手数料獲得

特徴	利用者が仮名性を保ちながらプールに流動性を供給し、手数料獲得
リスク	不正な収益を流動性プールに混入させ、手数料獲得

⑤開放性

特徴	ウォレットを保有していれば、CDDを経ずに誰でもサービスにアクセスできる
リスク	不正主体が仮名で参入し、複雑性を利用して資金洗浄

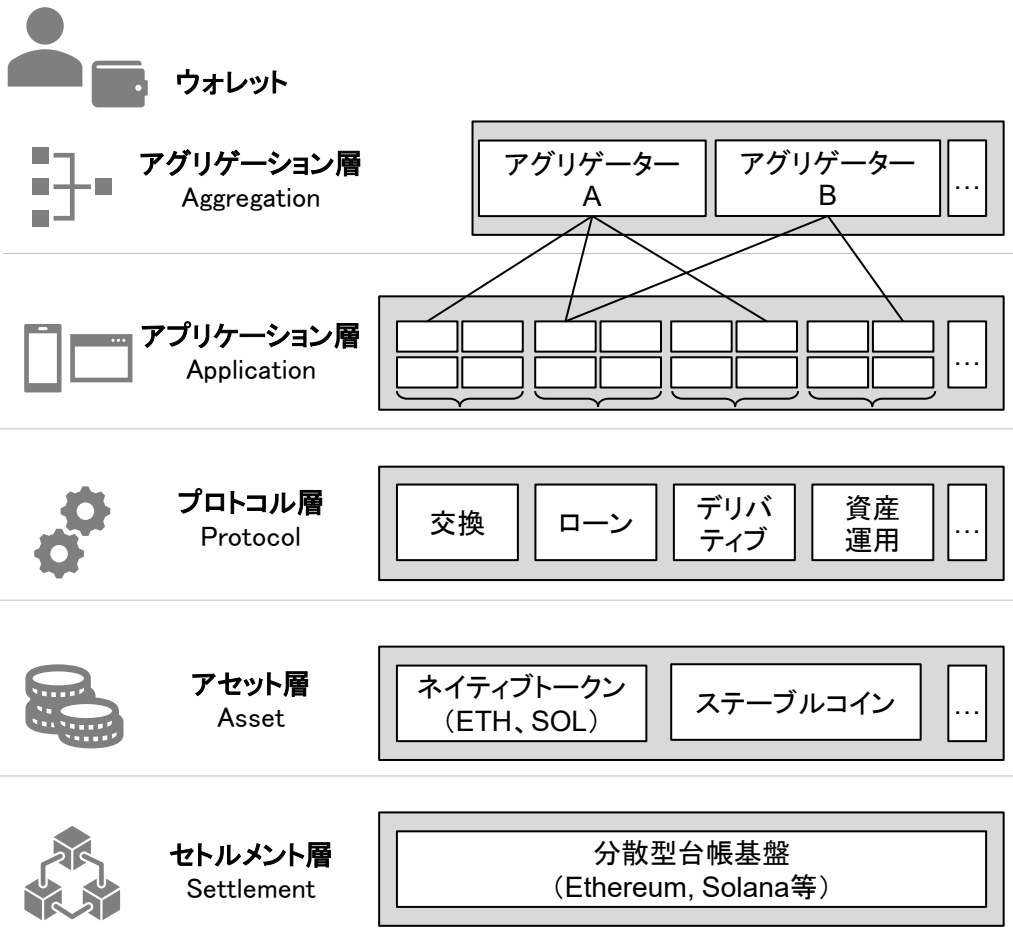
⑥オラクルへの依存

特徴	価格や金利などの外部データ（オラクル）が価格形成、担保評価、清算の基盤
リスク	オラクルの脆弱性を悪用した市場操作や不正清算、マネー・ローンダリング

DeFiのエコシステム

■ FATFのDeFi報告書は、DeFiエコシステムを①セトルメント、②アセット、③プロトコル、④アプリケーション、⑤アグリゲーションの5つのレイヤー（層）に分類している。

DeFiのエコシステム（イメージ）



	概要	関連主体（例）	FATF基準の適用
アグリゲーション層 Aggregation	複数のプロトコルを束ね、利用者に最適な経路を提供	ソフトウェア提供者（アグリゲーター）	**適用あり** VASPサービスを提供・助長する限りで適用。価格表示・比較のみなら対象外となり得る。
アプリケーション層 Application	**フロントエンド**、Webサイト、アプリ、ダッシュボード、ウォレット等の接続口	ソフトウェア提供者（フロントエンド提供者）	**適用あり** VASPサービスを提供・助長する限りで適用。プロトコル層とは別の主体が支配する場合がある。
プロトコル層 Protocol	AMM、レンディング、流動性プール等の**スマートコントラクト（バックエンド）**	ソフトウェア提供者 分散型自律組織（DAO） オラクル提供者	**限定的に適用** スマートコントラクト自体は対象外。支配又は十分な影響力を有する者に適用。
アセット層 Asset	ネイティブトークン（ETH、SOL等）、ステーブルコインその他の**デジタル資産**	デジタル資産発行者	**適用あり** VASPの定義に該当するサービスを提供する者に適用。
セトルメント層 Settlement	Ethereum、Solana等の**分散型台帳基盤**（記録・合意形成・最終決済）	バリデータ	**原則なし** 決済インフラ自体は対象外。当該層の者がVASP該当サービスも行う場合は適用。

DeFiに係るリスク（IOSCO）

■ IOSCO「分散型金融（DeFi）についての報告書」（2022年3月）は、DeFiにおいては、投資家保護、市場の公正性（market integrity）、金融の安定性について、既存の金融と同様のリスクがあるとともに、DeFi特有のリスクや課題があると指摘。

DeFiが有し得るリスク例

1. 情報の非対称性や不正のリスク
- 不適切な広告や重要情報の不開示等によって投資家が損失を被る可能性
- 破綻コストを個人投資家に集中させるなど詐欺的なDeFiのスキームが存在

2. 市場の公正性（market integrity）に関するリスク
- 従来型の市場におけるリスクと同様の、開示情報における虚偽記載、相場操縦、利益相反等から生じるリスク

3. フロントランニング又は詐欺と同様のリスク
- 発掘者がブロックチェーン上の取引を再注文／検閲できる能力を利用して利益を得ることで、利用者が不利な取引を強いられ、ブロックチェーンによる取引処理・決済のファイナリティへの信頼が失われる可能性

4. フラッシュローン（DeFiプロトコルで見られる無担保融資の一種）
- 一つのトランザクション内で取引終了前に返済すれば担保は不要である仕組みだが、プロトコルのコーディングエラー等の脆弱性を招く可能性

5. 市場への依存
- バリデータ、裁定取引業者、流動性プロバイダー等が参加するにあたり手数料のインセンティブ構造が存在するが、その構造が破綻した際にプロトコルが破綻する可能性

6. レバレッジの利用
- レバレッジの利用は、清算リスクが顕在化した場合、そのリスクを悪化させる可能性

7. 不法行為リスク
- DeFiの多くの商品・サービスにはAML/CFT規制がなく、潜在的に重大なマネロン・テロ資金供与リスクが存在するとともに、不法行為者はミキサー等の匿名性強化技術を利用することで制裁回避等を行うことが可能
- DeFiで取引を行う者が制裁対象者や不正な活動によって調達された暗号資産と関わる重大なリスク

8. オペレーショナルリスク及びテクノロジーに基づくリスク
- オペレーショナルリスクとして、情報システムやプロセスの欠陥、ヒューマンエラー等が、商品やサービスの縮小、悪化、故障につながる可能性
- DeFiは、伝統的な仲介者からテクノロジーへ信頼を移行させることを目指しているため、テクノロジーに基づくリスクが内在

9. サイバーセキュリティ
- DeFiの発展途上かつパーミッションレスな性質のため、プロトコルやスマートコントラクトは、サイバーセキュリティ攻撃、特にハッキングの影響を受ける可能性

10. 発展途上であることに伴うリスク
- ブロックチェーン技術とDeFiは発展途上であることから、①インターフェイスの理解しやすさ、②取引処理のための拡張性（取引速度の迅速性・取引コストの問題を含む）、③サポート性、④信頼性（紛争メカニズム・救済の欠如等）に係る課題が存在

11. ガバナンスリスク
- 名目上は「分散型」でも、特定の投資家やベンチャーキャピタリスト等がプロトコルやスマートコントラクトのガバナンスに関して発言権や裁量権を有しうることによって他の投資家が被るリスク

12. 中央集権的／伝統的な市場へのリスクの波及
- 中央集権的な暗号資産取引プラットフォームは、暗号資産取引ひいてはDeFiの中核となっており、これらの暗号資産取引プラットフォームのリスク（利益相反リスク、カストディを通じた暗号資産の管理に関する集中リスク、レバレッジ、取引リスク等）がDeFiに直接影響を与える可能性
- 伝統的な金融機関がDeFiプロジェクトや取引、ステーブルコインビジネスの支援活動に関与する場合、伝統的なビジネスとその運営にリスクをもたらす可能性があり、（拡大した場合）運営に重大な影響を与える可能性

目次

I. 分散型金融（DeFi）に関するリスク低減策

A) DeFiの概要

B) DeFiに関する規制アプローチとリスク低減策

II. ウォレット提供業者（アンホステッド・ウォレット）に関するリスク低減策

A) アンホステッド・ウォレットの概要

B) アンホステッド・ウォレットに関する規制アプローチとリスク低減策

III. ご議論いただきたい事項

DeFiへの規制アプローチ

■ DeFiにおける金融サービスの多くは伝統的な金融サービスと「機能」において類似・重複すると指摘されており、**「同じ機能、同じリスクには、同じルールを適用／同じ規制効果を実現」という原則のもと、**DeFiの名称や技術ではなく実際に提供される**機能・リスクに応じた規制を適用するアプローチ**が国際的にも支持されている。

■ もっとも、**規制の名宛人をどのように特定するか**について、**どのような場合を規制の名宛人が特定されていると考えるかを含め、具体的な判断基準や監督実務は国際的にも十分に確立していない。**

金融の「機能」の分類と各「機能」において達成されるべき利益
（金融審議会 金融制度スタディ・グループ中間整理（2018年））

	決　済	資金供与	資産運用	リスク移転
現行法の例	資金決済法 銀　行　法	銀　行　法 貸金業法	金融商品取引法	保険業法
「機能」分類のイメージ	仲介者等を介して、 • 意図する額の資金を意図する先に移動すること • 債権債務関係を解消すること **預　金** 法定通貨とほぼ同等の決済手段	• サービス提供者が、資金需要者に対して信用供与を行うこと 資金供与の原資 資金供与と組み合わせることにより信用創造を構成	• 資金余剰主体が、自らの運用目的やリスク選好に従って運用を行うこと 国民に広く利用される価値の貯蔵、運用手段 • 市場メカニズム等を通じた資金配分が行われること	• 経済・生活上の様々なリスクの発生の可能性に応じて対価を支払い、保障を受けること
達成されるべき利益	① **「機能」の確実な履行** ② **利用者に対する情報提供等** ③ **利用者資産の保護** ④ **利用者情報の保護** ⑤ **マネー・ローンダリング及びテロ資金供与の防止** ⑥ **システミックリスクの顕在化の防止** （注）証券市場をはじめとした市場の公正性・透明性の確保も重要			

DeFiへの規制アプローチ（IOSCO）

■ IOSCOは、2023年12月にDeFi勧告（分散型金融（DeFi）に関する勧告）を公表。実質的に**同じ機能、同じリスクには、同じルールを適用する又は同じ規制効果を実現する**という原則（’ same activity, same risk, same regulation/regulatory outcome’）を強調。

DeFi勧告（IOSCO, 2023年12月）の概要

勧告１　DeFiの商品、サービス、活動及びアレンジメントの分析	規制当局は、自らの管轄内で行われ又は所在するDeFiの商品、サービス、活動及びアレンジメントについて、**「同じ機能、同じリスクには、同じルールを適用する又は同じ規制効果を実現する」の原則に従い、既存の規制枠組み又は新たな規制枠組みを適切に適用**することを目的として分析すべきである。
勧告２　責任主体の特定	規制当局は、DeFiアレンジメントに関与する者のうち、**規制対象者（責任主体）を特定するよう努めるべきである。**これらの責任主体には、当該DeFiアレンジメントによって提供される金融商品、金融サービス又は金融活動に対して支配又は十分な影響力を行使する者が含まれる。
勧告３　共通した規制効果の実現	規制当局は、IOSCO基準に整合的な形で、DeFiの商品、サービス、活動及びアレンジメントから生じるリスクを規制し、監督し、監視し、及び対処するため、既存の規制枠組み又は新たな規制枠組みを用いるべきである。**その規制アプローチは機能ベースであるべきであり、投資家保護及び市場の公正性について、伝統的金融市場で求められるものと同一又は整合的な規制効果を実現すべきである。**
勧告４　利益相反の特定と対応の要求	規制当局は、既存の規制枠組み又は新たな規制枠組みを適用するに当たり、適切な場合には、責任主体に対し、利益相反を特定し、それに対処することを求めるべきである。
勧告５　重要なリスクの特定及び対応の要求	規制当局は、既存の規制枠組み又は新たな規制枠組みを適用するに当たり、適切な場合には、責任主体に対し、オペレーショナル・リスク及び技術リスクを含む重要なリスクを特定し、それに対処することを求めるべきである。
勧告６　明確、正確かつ包括的な開示の要求	規制当局は、既存の規制枠組み又は新たな規制枠組みを適用するに当たり、適切な場合には、責任主体に対し、投資者保護及び市場の公正性を促進するため、利用者及び投資家に対して、提供される商品及びサービスにとって重要な情報を、包括的かつ明確に、正確に開示することを求めるべきである。
勧告７　適用可能な法令の執行	規制当局は、その権限の範囲内で、既存の規制枠組み又は新たな規制枠組みの対象となるDeFiの商品、サービス、活動及びアレンジメント並びにその責任主体に対して、認可、検査、調査、市場監視及び法執行に関する包括的な権限を行使すべきである。
勧告８　クロスボーダーの協力と情報共有	規制当局は、DeFiの商品、サービス、活動及びアレンジメントが国境を越える性質を有することを踏まえ、それらの商品、サービス、活動及びアレンジメントに関して、他の法域の規制当局及び関係当局と協力し、情報を共有する能力を有すべきである。
勧告９　DeFi、暗号資産及び伝統的金融市場の相互連関の理解と評価	規制当局は、DeFiアレンジメント、より広範な暗号資産市場及び伝統的金融市場の間の相互連関を理解するよう努めるべきである。

DeFiの責任主体の特定方法（IOSCO）

■ IOSCOのDeFi勧告は、**通常は規制対象となる「責任主体」が存在する**という認識に立ち、規制当局に対し責任主体の特定を求めている。

DeFi勧告2「責任主体の特定」のガイダンス（抜粋）（IOSCO, 2023年12月）

（略）

一部の業界関係者は、ある仕組みが分散化されているのであれば、それは規制対象ではない、あるいは規制できないと主張している。DeFiにおいて「分散化」という言葉は、通常、特定のガバナンス又は意思決定メカニズムの状態を指し、その多くはガバナンストークン、投票トークン又はDAOによって実現されている。もっとも、**ガバナンス構造や意思決定プロセスがどれほど「分散化」されているとしても、商品提供、サービス提供又は活動実施を支配し又はそれらに十分な影響力を及ぼす責任主体が存在するのが通常である。**したがって、規制当局は、あるアレンジメントについて「金融商品、金融サービス又は金融活動について責任を負う個人又は組織が存在しないほど分散化されている」との主張を慎重に検証し、自らの規制枠組みの下で責任主体を特定すべきである。

（略）

ある個人又は組織が責任主体に該当するかどうかは、その者が実際に金融商品の提供、金融サービスの提供又は金融活動の実施を支配し、又はそれらに十分な影響力を及ぼしているかどうかによって判断される。どのような組織形態を採用しているか、またその組織がどの程度「分散化」されているかは問われない。特定の事案において誰が責任主体であるかは、個別の事実関係及び事情に基づいて判断される。

（略）

支配又は影響力を示す事情としては、例えば、持分の保有、重要な経済的利害関係、重要な議決権、商品・サービス・活動の運営又は運営に影響を及ぼす能力、プロトコル利用者の権限又はアクセス権を設定する能力、他の利用者の権利に影響を与える能力、利用者資産を保有するスマートコントラクトに対する支配権、並びにプロトコル又は企業体のために法的契約を締結する能力などが含まれる。もっとも、何が「支配」に当たるかは、各法域の規制にも依存し得る。

（略）

一般に、以下のような者がDeFiアレンジメントに関与しており、事実関係に応じてそれぞれ責任主体に該当するか検討され得る。

- 創設者及び開発者ガバナンス・投票トークンの発行者
- ガバナンス・投票トークンの保有者又は投票参加者
- DAO又はDAO参加者
- スマートコントラクト又はプロトコルに対する管理権限を有する者（コード又は運用を変更できる者）
- プロトコル又はアクセス権等の維持・更新を担う者
- 他の参加者がアクセスできない重要情報にアクセスできる者
- ユーザーインターフェースの提供その他の方法によりプロトコル利用を促進する者、又はプロトコル更新を公表する者
- ユーザー資産を保管する者、又は管理者キーや投票構造等により実質的支配を有する者、あるいは取引を取り消す能力を持つ者
- ユーザー手数料などから利益を得ている者

（略）

DeFiへの規制アプローチ（FATF）

■ FATFのDeFi報告書は、**DeFiアレンジメントを①中央集権型（主体特定可能）、②中央集権型（主体特定困難）、③真に分散型に類型化し、その類型に応じて規制上の対応を取る**ことを提言。中央集権型（①・②）の場合はFATF基準の対象としている。

DeFiアレンジメントに「支配又は十分な影響力を有する者（規制対象主体）」が存在するか／その者を特定できるか

① 中央集権型（主体特定可能）
規制対象主体：あり／特定できる

特　徴
支配又は十分な影響力を有する者（例：管理者、ガバナンストークン保有者、開発者、出資者）が特定できる。分散型を標榜していても該当し得る。

FATF基準
対象

当局の対応
免許・登録等を義務付け、監督・執行の対象とする。

② 中央集権型（主体特定困難）
規制対象主体：あり／特定できない

特　徴
支配は存在するが、仮名性等により誰が支配しているかを特定することが困難。

FATF基準
対象

当局の対応
特定に向けた継続的な努力。実効的に規制できない場合は③と同様の低減措置を適用。

③ 真に分散型
規制対象主体：なし

特　徴
支配又は十分な影響力を有する者が存在しない。

FATF基準
対象外

当局の対応
ステーブルコイン発行者・VASP・フロントエンド等の接点で間接的にリスクを低減。

当局は、DeFi側の説明や「分散型」というマーケティング表現に依拠せず、独立して支配構造を分析すべき。
複数の者が異なる部分を支配していても、AML/CFT上の義務は消滅・希釈されない。②で規制を実効的に適用できない場合は、実務上は未規制として扱う。

DeFiアレンジメントの支配の判断基準（FATF）

- DeFiアレンジメントの**支配者**（controller）には、実際に、**プロトコルの主要な運営や利用者へのサービス提供**の**実質的な決定権又は影響力を有する者**、及び／又は、その活動から一般のトークン保有者が享受する値上がり益や報酬とは異なる**重要な経済的利益**を得ている者が該当し得るとしている。
- もっとも、 DeFiアレンジメントの**支配**（control）**の有無を判断する画一的な基準は設けておらず、ガバナンス構造や運営実態を踏まえ、オン・オフチェーン双方の要素を総合的に考慮して判断**すべきとしている。また、DAOへの移行等により形式上は分権化されている場合でも、創設メンバーによる継続的な関与、ガバナンストークンの集中保有や議決権の委任等を通じて実質的な支配が維持されている可能性があることから、**実態に即して支配の有無を判断すべき**としている。

支配者（controller）の権限（例）

プロトコルレベルの運営統制	報酬、手数料又は新規発行トークンの配分その他の重要な運営事項を決定し、承認し、又は左右する権限
プロトコルの変更・停止	プロトコル又はプロトコルを構成するスマートコントラクトを変更、更新、一時停止又は終了させる権限
プロトコル資産の管理	プロトコル資産やトレジャリー資産（DeFiアレンジメントが保有・管理する資産）の運用、配分又は処分を決定する権限
参加者・バリデータの管理	利用者、バリデータその他金融サービスの提供を支える重要な参加者の追加、排除又は選定を行う権限
ガバナンス・運営体制の管理	開発者、マルチシグ署名者、オラクル運営者その他ガバナンス、運営又は管理に関する重要な役割を担う者を選任し、解任し、又はその活動を左右する権限

支配（control）の考慮要素

オンチェーン指標（一例）

- スマートコントラクトの更新・停止権限
- 手数料・担保条件・リスク上限等のパラメーター設定権限
- オラクルの選定・変更権限
- 中核スマートコントラクトの管理権限
- 手数料・収益の帰属先（MEV収益の還元、トークン新規発行による利益等）
- 参加者を限定するプールの管理、アクセス許可権限
- ガバナンストークンや委任された議決権の集中

オフチェーン指標（一例）

- 資産を管理するキーの保有者、マルチシグ署名者
- フロントエンド（Web・アプリ）の運営・配布
- 法人（会社・財団・ラボ）等による雇用、知的財産・資金の管理
- 開発方針・重要インフラの支配
- ブランディング・広報の実施、利用者向け情報の管理

DeFiへの規制アプローチ（米国CLARITY法案）

■ CLARITY法案では、DeFi取引プロトコルについて、**①プロトコルに対する支配権、②人的裁量の介在、又は③利用の制限・検閲権限の有無**に着目して、「中央集権型（non-decentralized）」に該当する場合を定義している。ただし、**DAO等の分散型ガバナンスシステムの運営や、サイバーセキュリティ上の緊急対応権限の保有は、それ自体では直ちにプロトコルの支配を意味しないことを明確化**している（Sec.10301, 20209）。

■ また、SEC・CFTCに対し、米財務省等と協議の上、**中央集権型のDeFi取引プロトコルの支配者について、証券・商品取引規制の適用関係を明確化するルール策定と、技術形式ではなく、**ブローカー業務、ディーラー業務、売買、執行、清算又はカストディ等の**機能・活動に応じた規制の適用**を指示している。また、**規制対象者には銀行秘密法に基づくAML/CFT規制を適用**することとしている（Sec.10301, 20209）。

DeFi取引プロトコルの支配の基準（CLARITY法案 Sec.10301, 20209）

DeFi取引プロトコル （decentralized finance trading protocol）	複数の参加者が以下の条件で金融取引を実行できる分散台帳システムをいう。 • あらかじめ定められた裁量性のない自動化されたルール又はアルゴリズムに従って行われること。 • 当該金融取引の対象となるデジタル資産について、利用者以外の者による保管又は支配に依存することなく行われること。
中央集権型DeFi取引プロトコル （non-decentralized finance trading protocol）	次のいずれかに該当するDeFi取引プロトコルをいう。 • 一の者又は共同支配下にある複数の者、若しくは協定、取決め、了解その他共同して行動する合意に基づいて行動する者の集団が、契約、取決め、了解、関係その他いかなる手段によるかを問わず、直接又は間接に、当該**DeFi取引プロトコルの機能、運営又はコンセンサス若しくは合意形成ルールを支配し、又は重要な変更を加える権限**を有する場合 • 当該DeFi取引プロトコルが、その運営、執行及び取引の実施を、分散台帳システムのソースコードに直接組み込まれた、**事前に確立された透明なルールのみに基づいて行っていない**場合 • 一の者又は共同支配下にある複数の者、若しくは協定、取決め、了解その他共同して行動する合意に基づいて行動する者の集団が、当該分散型金融取引プロトコルの運営を通じて、その**利用を制限し、検閲し、又は禁止する権限**を有する場合（システム上の利用者行動に関する制限を含む。）
特則・除外	• **分散型ガバナンスシステム**は、その運営のみを理由としては、「一の者」又は「共同支配下にある者の集団」若しくは「共同して行動する合意に基づく者の集団」とみなされない。 • **インシデント対応委員会又はセキュリティ委員会への参加**は、それのみをもって非分散型金融取引プロトコルに対する支配を構成するものとはみなされない。

※ 2026年9月14日ルミス上院議員公表のCLARITY法案の条文及び概要を基に作成。法案は未成立のため、今後内容が変更される可能性。

DeFiのトラストポイントに関する分析

分析の目的・背景

- **現在の主要なDeFiプロジェクトは一定のトラストポイント（利用者等が無条件にトラストせざるを得ない中央集権的要素）を有しているとの仮定に基づき、代表的なDeFiであるUniswap（分散型取引所：DEX）、Maker（暗号資産担保型ステーブルコイン）、Aave（レンディング）の事例分析を行ったもの**
  - ✓ DAO（Decentralized Autonomous Organization）の“Autonomous”である部分（スマートコントラクトにより自律的に運営が行われる部分）と、そうでない部分はどこか
    ※DAOの確立された定義は存在しないが、一般的には、中央集権的なリーダーシップが不在のメンバー所有のコミュニティで、コンピュータプログラムとしてエンコードされたルール（スマートコントラクト）によって運営が行われる組織のことを指す
  - ✓ ガバナンストークンを用いたオンチェーン・ガバナンスの実態把握
- **トラストポイントに関する金融規制上のインプリケーションの把握**
  - ✓ 一般的には、利用者などからトラストを受ける主体には責任が生じ、規制対象となりうる（例：銀行）
  - ✓ パラメータ変更やスマートコントラクトのアップグレード、資金使途の決定などがコミュニティに（一定程度）委ねられているDeFiでは、責任の分散化により規制対象の特定に困難が生じる可能性があり、各プロジェクトの詳細なトラストポイントの分析が必要

UNISWAP　MAKER　AAVE

DeFiのトラストポイントに関する分析

デジタル分散型金融への対応のあり方等に関する研究会（令和３事務年度）
第６回事務局説明資料（2022年６月）

特定された論点・リスク事項など

- **現状のDeFiプロジェクトには様々なトラストポイントが存在**
  - ✓ 開発チーム（法人）、管理権限保有者、関連法人、ユーザーインターフェース提供者、大口ガバナンストークンホルダー、ウォレット提供者、コード監査会社、インフラ提供者、ライブラリ提供者、双方向ブリッジ管理者など
  - ✓ トラストポイントが特定できた場合でも、なお規制の執行は困難である可能性（例：アドレスベースでの特定に留まり実在の主体の特定が難しい、個人ベースの活動が多く国境の移転が容易）
- **トラストポイントがWeakest Link（DeFiのセキュリティ上最も弱い部分）となりうる**
  - ✓ 多くのインシデントがトラストポイントにおいて発生（例：バリデータの秘密鍵の窃取、コード監査で発見されなかった脆弱性を突いた攻撃、インフラ提供者の不具合に伴う障害）
  - ✓ 他方、脆弱性が発覚した際に管理者権限で緊急対応を行うことが可能であるなど、トラストポイントが存在する利点も
- **“DAO”や“ガバナンストークン”と呼称されていても、プロジェクトによって大きな違いが存在**
  - ✓ Uniswapのガバナンストークン（UNI）で出来ることは限定的（例：コアコントラクトのアップデートは不可）だが、Makerのガバナンストークン（MKR）では比較的大きな権限を行使可能。ガバナンストークンに投票権以外の機能が付与されている場合も存在。
  - ✓ 少数の大口投資家や投票代理人が意思決定に強い影響力を持つと考えられるプロジェクトも存在。
- **イノベーション促進・技術革新支援の視点**
  - ✓ プロジェクトの初期段階では責任主体の特定が容易である可能性が高いが（例：解散前のMaker Foundation）、分散化の阻止はプロジェクトの成長（≒イノベーション）を阻害することにも繋がりうる
  - ✓ 技術中立性に関する論点：トークン交換などの金融機能は特定のエンティティではなくプログラム（スマートコントラクト）が提供しており、“技術”と“ビジネス”の境界が曖昧化している可能性

海外の無登録業者への対応

- 仮に規制の名宛人を特定できても、**海外に所在するため規制を執行することが困難な場合もあり得る。**
- 暗号資産WG報告では、外国の無登録業者が日本語のウェブサイト等により本邦居住者向けに暗号資産の勧誘をしている場合、行政において**警告・公表やアプリストアへの削除要請**といった対応を行うとともに、**外国当局との調査協力の強化等**を行っていくべきとしている。

暗号資産WG報告

Ⅲ　求められる対応
4. 業規制
(4)無登録業者への対応等
ア. 無登録業者への対応
　無登録業者による違法な勧誘等を抑止するため、暗号資産の売買等について金商業の対象とすることにより刑事罰を強化すべきである。
　また、金商法において金商業の無登録業者への対応として設けられている規定を暗号資産交換業にも適用することとし、無登録業者に対する暗号資産交換業を行う旨の表示等の禁止の規定や裁判所による緊急差止命令、証券監視委による緊急差止命令申立権限とそのための調査権限を整備すべきである。
　暗号資産については、本邦居住者が海外無登録業者等と取引するケースもある中、一律に無登録業者との売買契約等が暴利行為に該当するものと推定してよいか慎重に考える必要があるものの、他方で、無登録業者による詐欺的な勧誘等によって利用者被害が生じていることも踏まえながら、民事効規定を創設することが考えられる。

(5)海外の無登録業者・DEX等への対応
　ア. 海外の無登録業者への対応
　現状では、外国の無登録業者が日本語のウェブサイト等により本邦居住者向けに暗号資産の勧誘をしている場合、行政において警告・公表やアプリストアへの削除要請といった対応が行われている。引き続きそうした対応に注力するとともに、上記の無登録業者への対応や外国当局との調査協力の強化を行っていくべきである。

フロントエンド提供者への対応

- **フロントエンド提供者**について、暗号資産WG報告では、「DEXに接続するアプリ等のユーザー・インターフェース（UI）を国内居住者向けに提供する者に対しては、接続先に係るリスクについての説明義務や犯収法上の本人確認義務を含むAML/CFT対策等といった、**リスクに応じた過不足のない規制**を課すこと」を念頭に、各国の規制動向の注視や実態把握を提言している。
- 他方、FATFガイダンスにおいてDeFiアプリケーション（ソフトウェア）自体はFATF基準上のVASPに該当しないとされているなど、**価値中立的なソフトウェアの開発・公表等**の技術的活動を**直ちに規制すべきではない**との考え方が国際的にも支持されている。
- また、一部の法域では**フロントエンド提供者**について、**一定の場合は金融規制の対象外**であることを明確化する試みが行われている。

暗号資産WG報告

Ⅲ　求められる対応
4. 業規制
（5）海外の無登録業者・DEX等への対応
　イ. DEX等への対応
　（略）
　DEXに接続するアプリ等のユーザー・インターフェース（UI）を国内居住者向けに提供する者に対しては、接続先に係るリスクについての説明義務や犯収法上の本人確認義務を含むAML/CFT対策等といった、リスクに応じた過不足のない規制を課すことを念頭に、各国の規制動向を注視しながら、まずはそのようなUIを提供するサービスの実態把握を深めていく必要がある。
　なお、DEXプロトコルやDEXに接続するUIを通じた取引におけるAML/CFT対策のあり方は、必ずしも特定の国で完結するとは限らないことを踏まえ、国際的な議論を行っていくことが考えられる。

ソフトウェア開発・提供者の責任（Winny事件）

■ Winny事件（最決平成23年12月19日）は、ソフト自体が**適法な用途にも違法な用途にも利用できる価値中立的なソフト**であること（ソフト自体に適法利用の有用性もあり、違法用途に特化したソフトではないこと）を判断の前提とした上で「**…ソフトの開発行為に対する過度の萎縮効果を生じさせないためにも、単に他人の著作権侵害に利用される一般的可能性があり、それを提供者において認識、認容しつつ当該ソフトの公開、提供をし、それを用いて著作権侵害が行われたというだけで、直ちに著作権侵害の幇助行為に当たると解すべきでない**」と判示している。

最高裁平成23年12月19日第三小法廷決定（刑集65巻9号1380頁）（抜粋）

Winnyは、1、2審判決が価値中立ソフトと称するように、適法な用途にも、著作権侵害という違法な用途にも利用できるソフトであり、これを著作権侵害に利用するか、その他の用途に利用するかは、あくまで個々の利用者の判断に委ねられている。また、被告人がしたように、開発途上のソフトをインターネット上で不特定多数の者に対して無償で公開、提供し、利用者の意見を聴取しながら当該ソフトの開発を進めるという方法は、ソフトの開発方法として特異なものではなく、合理的なものと受け止められている。新たに開発されるソフトには社会的に幅広い評価があり得る一方で、その開発には迅速性が要求されることも考慮すれば、かかる**ソフトの開発行為に対する過度の萎縮効果を生じさせないためにも、単に他人の著作権侵害に利用される一般的可能性があり、それを提供者において認識、認容しつつ当該ソフトの公開、提供をし、それを用いて著作権侵害が行われたというだけで、直ちに著作権侵害の幇助行為に当たると解すべきではない。**

かかるソフトの提供行為について、幇助犯が成立するためには、一般的可能性を超える具体的な侵害利用状況が必要であり、また、そのことを提供者においても認識、認容していることを要するというべきである。すなわち、**ソフトの提供者において、当該ソフトを利用して現に行われようとしている具体的な著作権侵害を認識、認容しながら、その公開、提供を行い、実際に当該著作権侵害が行われた場合や、当該ソフトの性質、その客観的利用状況、提供方法などに照らし、同ソフトを入手する者のうち例外的とはいえない範囲の者が同ソフトを著作権侵害に利用する蓋然性が高いと認められる場合で、提供者もそのことを認識、認容しながら同ソフトの公開、提供を行い、実際にそれを用いて著作権侵害（正犯行為）が行われたときに限り、当該ソフトの公開、提供行為がそれらの著作権侵害の幇助行為に当たると解するのが相当である。**

ソフトウェア開発者の保護（米国CLARITY法案）

■ CLARITY法案では、**ソフトウェア開発者の保護**というセクションを設け、**ブロックチェーンの開発等の技術的活動のみを理由として証券取引規制やデジタル商品取引規制の対象としない**こととしている。ただし、SEC・CFTCによる反詐欺・反相場操縦及び虚偽報告に関する権限執行については適用除外の対象としないこととしている（Sec.10601, 20209）。

Crypto Task Force Round Table on Decentralized FinanceにおけるアトキンスSEC委員長の発言（2025年6月9日）

前政権は、規制上の措置を通じて、そのようなソフトウェアの開発者がブローカー業務を行っている可能性があるとの見解を示すことで、自己保管型デジタルウォレットその他のオンチェーン技術に関するイノベーションを阻害した。**こうした種類のソフトウェアコードを公開したという理由だけで、エンジニアが連邦証券法の規制対象とされるべきではない。ある裁判所の表現を借りれば、自動運転車の開発者に対し、第三者がその車両を用いて交通違反を犯したり銀行強盗を行ったりしたことについて責任を負わせるのは不合理である。裁判所の判決文を引用すれば、「そのような場合、不正行為を容易にしたとして自動車会社を訴えるのではなく、不正行為を行った個人を訴えることになるだろう」**ということである。

ソフトウェア開発者の保護（CLARITY法案 Sec.10601, 20209）

本法（証券取引所法、商品取引所法）その他の規定にかかわらず、分散型台帳システム又はその構成要素の運営に関連して、ある者が以下の活動のいずれかを単独又は組み合わせて行うことのみを理由としては、当該者を本法及び本法に基づいて制定された規則の適用対象としてはならない。

- ネットワーク上のトランザクションを集約し（compiling）、又はトランザクションの中継（relaying）、探索（searching）、順序付け（sequencing）、バリデーション（validating）その他これらに類する機能を提供すること。
- 計算処理を提供すること、ノード又はオラクルサービスを運営すること、ネットワーク帯域を調達・提供・利用することその他これらに類する補助的サービスを提供すること。
- 分散型台帳システム又は、利用者が自己のデジタル資産若しくは署名鍵を保有・保護・管理することを可能にするソフトウェア若しくはシステム（ウォレットを含む。）を開発、公開又は提供すること。

※ 2026年9月14日ルミス上院議員公表のCLARITY法案の条文及び概要を基に作成。法案は未成立のため、今後内容が変更される可能性。

フロントエンド提供者への規制アプローチ（米国CLARITY法案）

- CLARITY法案では、**利用者がブロックチェーン・アプリケーションやDeFiプロトコルに対して取引に必要な指示を送信できるユーザー・インターフェース**（Distributed Ledger Messaging System）を米国人が所有又は運営する場合について、財務省に対し、**AML/CFT・経済制裁リスク管理のガイダンス**を財務省が策定することを求めている（Sec.10302）。
- 一方、 CLARITY法案では、利用者がDeFiプロトコルと通信するためのユーザー・インターフェースであっても、**利用者以外の者が利用者の資金を管理したり、利用者に代わって取引を執行する権限を有しないもの**（DeFi messaging system）については、**証券規制やデジタル商品の現物市場規制の対象外**とする方向性を示している。ただし、SEC・CFTCによる反詐欺・反相場操縦及び虚偽報告に関する権限執行については適用除外の対象としないこととしている。（Sec.10601, 20209）。

フロントエンド提供者規制のイメージ
（CLARITY法案 Sec.10302, 10601, 20209）



※ 2026年9月14日ルミス上院議員公表のCLARITY法案の条文及び概要を基に作成。法案は未成立のため、今後内容が変更される可能性。

フロントエンド提供者への規制アプローチ（米国SECスタッフ見解）

■ SECは、2026年4月、**利用者がアンホステッド・ウォレット**（self-custodial wallet）**を用いて自ら**トークン化証券（crypto asset securities）の**取引を実行することを支援するにとどまるUI**（ユーザー・インターフェース）については、**利用者の意思決定に干渉しない**こと等の条件を満たすことを前提に、**UI提供者がブローカー・ディーラーの登録を行わなくても異議を唱えない**との見解を公表した。なお、UIはウォレットに組み込まれている場合もあれば、独立してダウンロード可能な形で提供される場合もある。

ブローカー・ディーラーの登録を要しない条件

● UI提供者がUIの開発・提供・運営において以下の措置を講じていること

- ユーザーが取引条件を自由に設定できるようにしていること
- ユーザーに特定の暗号資産証券の取引を推奨・勧誘しないこと
- 接続・連携する取引所や取引システムを定めていること
- UI提供者が運営する取引所と接続・連携する場合は、その関係性を明確に開示し、他の取引の場と同等の条件で接続・連携すること
- 複数の注文執行ルートの中で単一の注文執行ルートのみ表示する場合は、ユーザーが他の注文執行ルートを確認できるようにすること
- 複数の注文執行ルートを表示する場合には、価格やスピードなどの客観的要素に基づく並び替えやフィルタリング機能を提供すること
- 特定の注文執行ルートを「最良」などと評価するコメントを行わないこと
- 取引指示作成や注文執行ルートの表示において、事前に開示された第三者により検証可能な客観的パラメータに基づいて動作するソフトウェアのみを使用すること
- UIが市場情報や証券取引について、裁量を行使したり、意思決定に関与しないこと
- 手数料は定額又は定率で客観的かつ一貫した基準に基づいて利用者に課すものとし、銘柄、執行ルート、執行市場又は取引相手によって変動させないこと
- UI提供者が、接続する取引所等の評価・選定・監査に係る方針、手順及び管理体制を整備するとともに、デフォルトの取引条件についても客観的基準に基づく選定・定期的な見直し及び利益相反への対応を行うこと
- UIの開発・提供・運営におけるUI提供者の役割、手数料、利益相反、特定の銘柄・市場データ・取引所等の利用制限、サイバーセキュリティー対策、相場操縦等からの利用者保護措置、接続・連携する取引所等、既定の注文執行条件などの重要事項について、ユーザーに対して明確に開示し、必要に応じて速やかに更新すること

● 以下のサービスを実際に行っている又は行っていると対外的に表示しているUI提供者はスタッフ見解の対象外

- 取引条件の交渉
- 特定の暗号資産証券の取引の勧誘
- 投資判断の推奨や投資助言
- 資金調達の手配
- 取引書類の処理
- 独立した立場での資産評価
- ユーザーの資金、証券・ステーブルコインの預託等
- 取引の執行や清算
- 注文の受付や他の事業者への注文の回送

（出典）Staff Statement Regarding Broker-Dealer Registration of Certain User Interfaces Utilized to Prepare Transactions in Crypto Asset Securities (Division of Trading and Markets, April 13, 2026)

フロントエンド提供者への規制アプローチ（英国FCA）

■ FCAは、2026年９月、ある事業や活動が認可を必要とするかどうかを判断するためのガイダンスであるPERG（Perimeter Guidance Manual：適用範囲マニュアル）に暗号資産に関するガイダンスを追加し、**適格暗号資産の交換を行う自動化プロトコルへの接続を可能にするインターフェースは、取引条件等に関する裁量や暗号資産の管理権がなくても「取引の媒介」に該当し得る**と整理。

■ しかし、同月に議会に提出された規則案を受け、10月にPERG改定案の市中協議を開始。**認可業者または分散型プロトコルへのアクセスを可能にするだけの技術サービス**について、**一定の要件の下で上記の規制から除外する（ただし、マネー・ローンダリング規制からは除外されない）**との解釈案を示している。

2026年9月最終化のPERG

規制対象性の判断

① 識別可能な人(an identifiable person)による実施
② 規制対象活動の実施
③ 業として実施
④ 英国内で実施
⑤ 除外・免除の適用有無

フロントエンド提供者への適用

- **適格暗号資産の交換を行う自動化プロトコルに接続するフロントエンド提供者**が認可を必要とするかは、上記①～⑤について個別の事実関係に基づいて判断。
- 暗号資産の適格暗号資産の売買やステーキングを手配するフロントエンド提供者は、（2026年の法改正により規制対象に追加された）売買又はステーキングの媒介業務に該当する可能性。
- **取引条件等に関する裁量や暗号資産の管理権がないことだけでは、媒介性は否定されない**。

2026年10月から市中協議中のPERG改定案

除外の要件

① 提供者(A)が認可業者・決済サービス提供者でない
② **単に技術サービス**を提供
③ その技術サービスにより利用者(C)が第三者のサービス又は分散型プロトコル(V)に**アクセス可能**になる
④ Vが当該規制活動について**認可等**を受けている、又は**分散型プロトコル**である

要件②「単に」「技術サービス」の詳細

✓ 判断基準は、**非裁量的で非実質的な技術機能**にとどまるかどうか。より使いやすくする機能などがあるだけでは除外は失われない。
✓ 「裁量」の基準となりうる要素：Aによる取引相手・経路・プロトコルの選択、Cの指示を送信する時期・順序や可否の判断、指示内容の変更、価格等に基づく経路の選択・調整、推奨・ランキング・絞り込み、ベストエグゼキューションの表示。
✓ アルゴリズムによる自動処理でもAが定めた基準を実装していれば「裁量」となりうる。

なお、技術サービス除外が適用されても、**マネー・ローンダリング規制や金融プロモーション規制の対象からは除外されない。**

（出典） PS26/18 Cryptoasset Perimeter Guidance (FCA, 2026年9月)、CP26/36 Cryptoasset Perimeter Guidance (FCA, 2026年10月)

金融サービスが適切に提供されるためのシステム管理責任

■ 本研究会の中間論点整理（令和3年11月17日）では、パーミッションレス型の分散型台帳やそれを利用したシステムに関して、システム全体に責任を負う者が不明確、社会的に不適切であることが明らかとなった取引について事後的な取消し等が困難といった課題を指摘している。

■ また、**パーミッションレス型の分散型台帳等を利用した金融サービスが幅広く利用されるためには、規制の名宛人として管理責任を果たせる立場にある者が役割を果たすべき**ことを指摘している。

「デジタル・分散型金融への対応のあり方等に関する研究会」中間論点整理（令和3年11月17日）

1．デジタル・分散型金融の動向と研究会における検討の概要

⑵ 分散台帳の分類とその特徴

（略）

パーミッションレス型の分散台帳や、それを利用したシステムに関して、本研究会では、以下のような指摘があった。

メリットとして、

・単一障害点（Single Point of Failure）を除去することが可能

・参加者がスマートコントラクトによって、複雑な条件を付す等オーダーメイド化された取引を、自律的に成立・執行させることが可能である

・誰もが自由にサービスの提供・利用が可能であり、イノベーションの源泉となる

ことが挙げられる一方で、

・システム全体に責任を負う者が不明確

・社会的に不適切であることが明らかとなった取引についても、自動的に執行され、事後的な取消し等が困難である可能性

・現金のような持ち運びの物理的制約が存在しない暗号資産等では（当局の監督下にある金融機関等による本人確認を経ない）P2P取引によるマネー・ローンダリング/テロ資金供与対策（AML/CFT）上の課題が存在

・アカデミア等による十分な検証が行われないまま、利用実態が先行

との点も指摘があった。

（略）

2．パーミッションレス型の分散台帳等を利用した金融サービスに関する基本的な課題

⑴ 総論

パーミッションレス型の分散台帳等を利用した金融サービスについては、複数のレイヤーに基づき、その一部のレイヤーについてのみ中央管理者を置く形態で提供されているものがある。一方、従来の金融規制の枠組みでは、金融機関が全レイヤーを管理する主体として存在し、規制の名宛人として管理責任を果たせる立場にあることを前提としている。

複数レイヤー全体を管理する主体が存在しない場合であっても、サービスが幅広く利用されるためには、システム全体が技術・契約・制度・インセンティブ・信頼等によって規律付けられる必要があり、規制の名宛人として管理責任を果たせる立場にある者がこうした状態を実現する必要があると考えられる。

（略）

Innovation Exemption（米国SEC）

- SECは、2026年９月、証券取引所法上の取引所登録なしでも、一定のオンチェーン市場でトークン化株式を売買できるようにする一時的免除命令（Innovation Exemption Order）を公表。
- **免除を利用できる主体**（TSV：Tokenized Securities Venue）は米国の法域に服する者（U.S. person）に限定されており、**SECへの事前届出を要する**とともに、**SECの監督下で運営**し、帳簿書類等に関する検査を受け入れる必要がある。

Innovation Exemptionの概要

AMMへの既存市場規制の不適用		• 一定のTSVを**取引所上の「取引所」から5年間、条件付きで免除**し、Regulation NMSの取引所やATS（代替取引システム）向け規定を適用しない。 • TSVでは、本人確認等を経た参加者が利用する許可されたAMM/流動性プールを使ってトークン化NMS（全国システム）株式を取引可能
条件	対象トークン	• 対象は、発行体自身または第三者がトークン化したNMS株式に限定（**合成型は除外**） • トークン保有者には、**原株と同等の経済的利益、配当、議決権等の権利**を付与
	勝手上場の制限	• 第三者が発行体と無関係にトークン化した株式をTSVに載せる場合、TSVは事前に原株の発行体へ通知 • 発行体には異議申立ての機会が与えられ、**異議が出されたトークン化株式はTSVで取引不可**
	ブロックチェーン	• **TSVで使用されるスマートコントラクトは、監査可能で公開されたパーミッションレス型の分散型台帳上に展開** • **AMMへの参加者やウォレットはTSVが審査し、許可・ホワイトリスト掲載された者だけが取引可能** • **TSVは本人確認、ウォレット確認、OFAC制裁やAML/CFT対応などの参加基準を設け、その内容を公開**
	銘柄数・出来高制限	• **銘柄数**はTier 1（大型・高流動性株）で最大75銘柄、Tier 2（その他）で最大250銘柄に**限定** • 各銘柄のTSV上の**出来高**も、前月の平均出来高に対して、Tier 1は0.25%、Tier 2は2.5%までに**抑制**
	取引停止	• **原株の主たる上場取引所で売買停止**となった場合、TSV上のトークン化株式も**同時に取引停止** • 対象となる停止には、市場全体のサーキットブレーカー、重要情報の公表待ち、SEC・自主規制機関による措置、上場廃止手続が含まれる
	情報公開と記録保存	• 価格、数量、取引時刻、プールアドレス、日次出来高、プールサイズ等のドル建て**取引データを公開** • 重大なシステム障害、サイバー侵害、AMM・スマートコントラクト障害等が発生した場合、参加者とSECに通知 • TSVは取引記録、参加者・ウォレット確認、手数料、障害情報等を記録・保存
流動性供給者のディーラー登録免除		• TSVのAMMに自己資金でトークン化NMS株式を供給する一定の**流動性供給者**（顧客への価格提示や、一定額の流動性を継続提供する契約を行う場合を含む）を、**取引所法上の「ディーラー」から一時的・条件付きで免除** • ただし、**反詐欺・相場操縦禁止規定等は適**用され、非登録であること等の開示・記録保存も必要

DeFiと接点を有する周辺主体

- FATFのDeFi報告書は、**真に分散型のDeFiアレンジメントでは、AML/CFT規制を直接適用してリスクを抑制することは困難であり、別途のリスク低減策を検討すべき**としている。具体的には、**DeFiアレンジメントに接続するリスクに関するガイダンスを規制対象事業者**（regulated entities）**に提供することや、DeFiアレンジメントへの接続が適切と考えられる条件**（追加的なAML/CFT管理措置の適用等）**を明確化**することが含まれるとしている。
- そして、**DeFiと接点を有する規制対象事業者**には、**ステーブルコイン発行者**、**オン・オフランプ提供VASP**、**フロントエンド提供者**および**金融機関**が含まれ得るとしている。

DeFiと接点を有する事業者

ステーブルコイン発行者

凍結・ブロック・バーン・再発行が可能。DeFi内の暗号資産の約9割をステーブルコインが占める。

VASP（オン・オフランプ）

KYC/CDDと疑わしい取引の届出。最終的な出口として資産回収の要所となる。

フロントエンド提供者

支配者を特定でき、AML/CFT義務を負い得る。不正な主体の接続を自動で遮断できる場合も。

金融機関

DeFiと取引する際、自らの態勢の実効性を維持する責任を負う。

デジタル資産仲介業者への規制アプローチ（米国CLARITY法案）

■ CLARITY法案では、SEC又はCFTCの監督対象となるデジタル資産仲介業者（暗号資産取引所など）がDeFiプロトコルを利用する場合に、AML/CFT、詐欺・相場操縦、サイバーセキュリティリスクを含めた包括的なリスク管理体制の構築を求めている（Sec.10308）。

デジタル資産仲介業者に求められるリスク管理基準（CLARITY法案 Sec.10308）

DeFiプロトコルのリスク分析	DeFiプロトコルについて、以下のリスクを分析するとともに、特定されたリスクを軽減するための方針・手続を整備 ① マネー・ローンダリング及び制裁回避リスク、 ② 詐欺・相場操縦リスク、 ③ オペレーショナルリスク及びサイバーセキュリティリスク（決済リスクを含む）
顧客へのリスク開示	リスク分析を通じて特定したDeFiプロトコルのリスクについて、顧客に対し平易で分かりやすい言葉で説明
不正取引の監視	ブロックチェーン分析ツール等も活用しながら、DeFiプロトコル上で発生する詐欺・相場操縦、サイバー攻撃、マネー・ローンダリング及び制裁回避を検知するための強固かつリスクベースの能力を維持
高リスク取引の遮断	マネー・ローンダリング、制裁回避、詐欺又は相場操縦の疑いを踏まえ、DeFiプロトコルに関連する入出庫取引について、執行、拒否又は停止のいずれとするかを判断するための実効的かつリスクベースの手続を整備

※ 2026年9月14日ルミス上院議員公表のCLARITY法案の条文及び概要を基に作成。法案は未成立のため、今後内容が変更される可能性。

DeFiガイダンス：オペレーショナル・レジリエンス（英国FCA）

■ FCAは、2026年10月、**事業者がDeFiを利用して金融サービスを提供する場合**であっても、**従来の金融サービスと同様に求められる規制上の成果を引き続き実現**することが求められるとし、**オペレーショナル・レジリエンスや金融犯罪に関連する既存のルールの遵守を支援するためのガイダンス案**について、市中協議を開始した。

DeFiガイダンス（オペレーショナル・レジリエンス）

重要業務の特定	□ 障害が起きると顧客に許容し難い被害を与え、または英国市場の健全性・金融安定を脅かすサービスを重要業務として特定する。 ● DeFi利用企業は技術やプロトコルではなく、顧客に提供するサービスを重要業務とする（例：暗号資産の取引・移転・貸付け・借入れ・ステーキング） ✓ （例） Firm A（顧客の暗号資産をDeFiプロトコルを通じてステーキングするサービスを提供）は、プロトコルの選定・利用を含むステーキングサービスを重要業務とした。許容し難い被害を生む障害として、選定先・接続先プロトコルの脆弱性、基盤ネットワークの障害、バリデータの停止（スラッシング損失、顧客資産の返還不能）を想定
影響許容度	□ 重要業務ごとに許容できる最大の障害水準を設定する。 ● DeFi利用企業は①顧客が資産にアクセス・移転・取引できない、②取引の失敗・遅延・巻戻し、③価格の不正確さ・データ障害、④資産がアクセス不能になる、または更なる障害やハッキングに晒される点を考慮 ✓ （例） Firm Aは、影響を受ける顧客数、顧客の損失額、サービスを利用できない期間で許容度を設定
マッピング	□ 重要業務を支える主体・プロセス・技術・施設・情報を、脆弱性を特定・是正できる程度にマッピングする。 ● DeFi利用企業はサービス提供を支える第三者・外部依存を十分に理解する ● DeFi利用企業はブロックチェーン基盤・決済基盤、クラウド・技術提供者、外部プロトコル・スマートコントラクト・ミドルウェア（オラクル、ブリッジ）、顧客向けインターフェース／社内機能（インシデント対応、鍵管理、ガバナンス、監督、顧客コミュニケーション）をマッピングに含めることが考えられる。 ● DeFi利用企業は重要業務に影響しうるガバナンス（プロトコルのアップグレード、緊急時の統制）と変更管理（管理者鍵）の仕組みも特定すべきである ✓ （例）Firm B（DeFiへのアクセスを可能にするノンカストディアル・ウォレットを提供）は、ネットワーク手数料推定のオラクル、最良執行を可能にするDEXアグリゲーター、残高・取引を独立に検証する仕組みをマッピング
シナリオテスト	□ テスト計画を策定し、生じ得る深刻な障害の下で影響許容度内に収まるかをシナリオテストで検証する。 □ 重要業務の提供が第三者に依存する場合は、その第三者と協力してテストの妥当性を確保する。第三者がテストする場合は手法・シナリオの適切性を確認する。品質・正確性の最終責任は自社にある。 □ テスト後・障害後に教訓を洗い出し、弱点の特定と改善につなげる。 ● DeFi利用企業はブロックチェーン基盤、クラウド・技術提供者、スマートコントラクト、第三者サービス、データフィード、ブリッジ、顧客向けインターフェースに生じ得る影響をテストすることが考えられる。 ✓ （例）Firm Bは、ウォレット基盤の停止、署名・送信の失敗、手数料情報の誤り・欠落、RPCプロバイダーとの切断を生じ得る深刻な障害と想定し、サービス継続や顧客への連絡、取引失敗・遅延への対応を検証。RPCの1社依存を発見して是正。
顧客への連絡	□ 障害時に迅速かつ効果的に対応できるコミュニケーション戦略を維持する。 ● DeFi利用企業はデジタルチャネルや顧客向けインターフェースを含め、障害時に顧客・関係者へどう連絡するかを検討し、関連情報を集めて影響を評価するプロセスを持つ □ 顧客に明確・適時・関連性のある情報を提供する。必要に応じ、障害の内容、想定される影響、救済の限界、顧客が被害を減らすために取れる行動を説明する
第三者依存	● DeFi利用企業は自社が管理しないDeFiプロトコル・インフラ・サービス提供者に依存している可能性。 □ 重要業務へのリスクを理解・管理する責任は自社にある □ ①主要な依存先とその役割のマッピング、②第三者の障害を制御・回復できる範囲の限界の理解　③重要な依存先の性能・レジリエンスの監視　④生じ得る深刻な障害の影響のテスト、⑤集中リスクと代替手段の評価、⑥障害時の顧客・規制当局との明確な連絡

DeFiガイダンス：金融犯罪リスク対策（英国FCA）

■ FCAは、2026年10月、**事業者がDeFiを利用して金融サービスを提供する場合**であっても、**従来の金融サービスと同様に求められる規制上の成果を引き続き実現**することが求められるとし、**オペレーショナル・レジリエンスや金融犯罪に関連する既存のルールの遵守を支援するためのガイダンス案**について、市中協議を開始した。

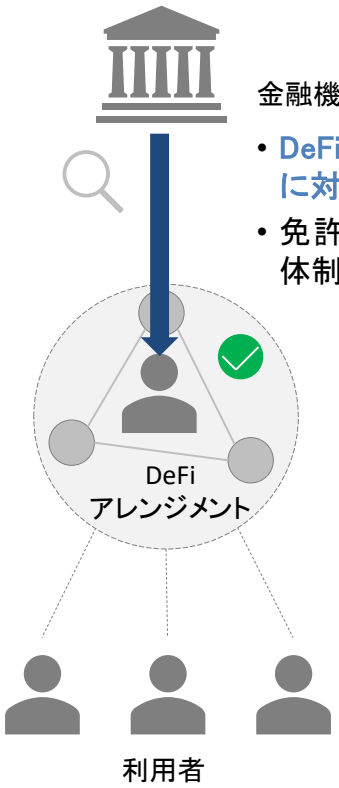
DeFiガイダンス（金融犯罪リスク）

リスクの特定・評価	□ 事業全体のML/TF/PFリスクへのエクスポージャーを評価 ● 1つの取引で複数のプロトコル・スマートコントラクト・サービスを使うことで取引の流れが複雑になり、参加者の特定や資金の出所・行き先の追跡が難しくならないかを考慮し、統制の評価に反映 □ 業務に関連する資金源のリスクを検討 ● DeFiが絡む取引では、ダークネット市場、ミキシングサービス、制裁対象者・サービスなど、不正に関係する主体との接点を高リスクの兆候として確認
リスクの低減（方針・手続）	□ 金融犯罪に利用されるリスクを低減するための方針・手続を整備・維持 ● ①利用するDeFi商品・サービス・プロトコルがマネロン等や制裁回避の新たな機会を生まないか　②顧客のサービスアクセス経路がリスクの特定・管理を難しくしないか　③複数のプロトコル・チェーンにまたがる取引で監視・調査が難しくならないか、④ウォレットアドレス・スマコン・プロトコルを通じた不正への関与を特定できるか、⑤第三者インフラや高リスク法域への依存が追加リスクを生まないか、といったDeFi特有のリスクを考慮
顧客管理	□ 継続的顧客管理（CDD）を実施する。高リスクの場合は厳格な顧客管理（EDD）を実施する ● 高リスク判断の要素として、①不正・制裁に関係するウォレット・プロトコル・サービスとの接点、②プライバシー強化技術の利用、③複数のプロトコル・サービス・チェーンにまたがり資金の流れがわかりにくい構造、④出所・所有者・行き先を隠そうとする兆候、といったDeFi特有の要素を考慮 ● 必要に応じて資金源を把握し、DeFiを利用する金融サービスのリスクを特定・評価・管理できるようにする ● リスクを特定した場合は、追加の情報やモニタリングが必要か、活動が顧客のリスクプロファイルと整合しているかを検討する
取引モニタリング	□ リスクに応じて継続的にモニタリングする。 ● 利用するプロトコル、取引の流れ、ブロックチェーン上の活動の性質から、追加のモニタリングが必要かを検討する。①新たに展開された暗号資産・トークン化資産・スマートコントラクトとの取引、②詐欺の兆候（ラグプル、アカウントの乗っ取り）、③レイヤリングなど出所・行き先を隠すパターン、④制裁対象の人物・ウォレット・プロトコル・サービスとの直接・間接のエクスポージャーが関連する要素となる
疑わしい取引の届出	□ ML/TF/PFを把握し、または疑われる場合の法的な報告義務を理解し遵守 □ 疑わしい取引の届出方法と、NCAに報告すべき内容を把握する。 □ 特定した疑わしい取引を踏まえ、取引モニタリングの手法を強化する
トラベルルール	□ 暗号資産の移転についてトラベルルールの要件を遵守する ● DeFiの利用が、必要な情報の取得・検証・送信・保存に影響しないかを評価する。ノンカストディアル・ウォレット、複数の仲介者、本人確認・記録保存の水準が異なる環境では難しくなりうる ● ノンカストディアル・ウォレットは特有の不正リスクがあり、統制の回避に使われうるため、関連リスクを低減する。64G条により、送付人・受取人のいずれの顧客にも情報を求められる ● 送付人・受取人情報が欠落・不完全な場合の手続（リスク評価、移転の扱いの決定）を整備する

金融機関・VASPがDeFiと取引する際に求められる措置（FATF）

- FATFのDeFi報告書は、**金融機関・VASPがDeFiアレンジメントに関与する場合、** DeFiアレンジメントの**支配者の特定可否に応じたリスク評価、リスク管理・低減措置**を講じることを求めている。
- 真に分散型の**DeFiアレンジメントに実効的なリスク低減措置**が講じられている場合、**利用者に適用するAML/CFT措置は残余リスクに応じて調整可能と**し、リスク低減措置を講じるDeFiアレンジメントが選ばれやすくなる枠組みを提示している。
- また、規制・監督当局に、民間部門と連携し、真に分散型のDeFiプロトコルにおいても適用可能な**革新的なAML/CFT対策（暗号技術やデジタルID技術の活用、ブロックチェーン分析の利用）**について検討することを推奨している。

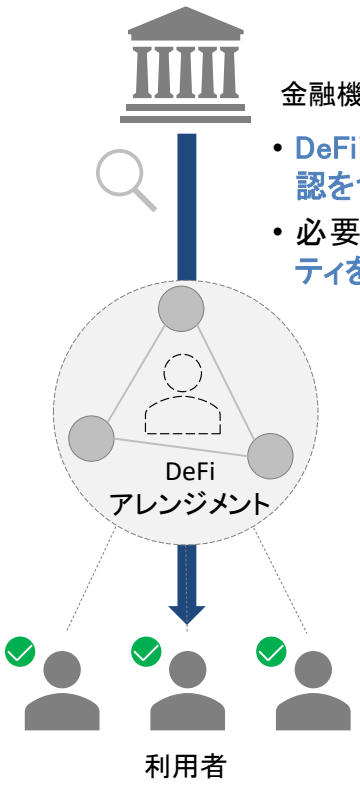
支配者が特定可能



- **DeFiアレンジメントにおけるFATF基準該当者に対し、**コルレス先管理に準じた**CDDを実施**
- 免許・登録・監督の有無及びAML/CFT管理体制を確認

- AML/CFT措置なしで**誰でもアクセスできるDeFiアレンジメントは高リスク**であり、利用可否を慎重に精査する必要

支配者が特定困難・真に分散型



- **DeFiアレンジメントの利用者に対し、本人確認を含めた適切なAML/CFT措置を実施**
- 必要に応じ、**プロトコルの健全性・セキュリティを継続的に監視**

- CDD等のAML/CFT措置が実施できない**DeFiアレンジメントへの関与は控えるべき**
- 真に分散型の**DeFiアレンジメントが実効的なリスク低減措置**（第三者KYC/CDD、組込みKYC/CDD、許可・拒否リスト）を講じている場合、**利用者に対して適用するAML/CFT措置は残余リスクに応じて調整可能**

ステーブルコイン発行者のリスク低減措置

■ 資金移動業者は、犯罪行為が行われた疑いがあると認められる場合に為替取引の停止等を行う措置を講じることが求められており、**電子決済手段を発行する場合にあっては、自らが管理しないウォレットに係る電子決済手段の移転及び償還を停止するための態勢を整備**することが求められている。

■ なお、信託銀行・信託会社が電子決済手段を発行する場合においても、資金移動業ガイドラインの一部規定に準じて取り扱うものとされている。

○ 資金移動業者に関する内閣府令（平成二十二年内閣府令第四号）

（その他利用者保護を図るための措置等）

第三十一条　資金移動業者等は、資金移動業の利用者の保護を図り、及び資金移動業の適正かつ確実な遂行を確保するため、次に掲げる措置を講じなければならない。

一　その行う為替取引について、捜査機関等から当該為替取引が詐欺等の犯罪行為に利用された旨の情報の提供があることその他の事情を勘案して犯罪行為が行われた疑いがあると認める場合には、当該為替取引の停止等を行う措置

二～六　（略）

○ 事務ガイドライン（第三分冊：金融会社関係 14 資金移動業者関係）

Ⅱ－２－１－２－１ 主な着眼点

⑸ 資金移動サービスの不正利用等を防止するため、現金の支払や内閣府令第29条第１項第２号に規定する為替取引を継続的に又は反復して行うことを内容とする契約（以下「口座開設契約等」という。）の締結に当たって、必要に応じ、取引時確認の実施や口座の利用目的等の確認を行うなど、資金移動サービスの不正利用による被害防止のあり方について検討を行い、必要な措置を講じているか。

特に、内閣府令第31条第１号に基づき、自らが提供している資金移動サービスについて、捜査機関等から当該為替取引が詐欺等の犯罪行為に利用された旨の情報の提供があることその他の事情を勘案して、犯罪行為が行われた疑いがある場合について、以下の態勢を整備する必要がある。

① 犯罪行為に利用された疑いのある当該為替取引を速やかに停止するための態勢

② 口座開設契約等を締結している者が当該契約を犯罪行為に利用していると疑われる場合には、当該者に対する資金の払出しを停止するための態勢

（注１）①又は②に基づき、為替取引や資金の払出しを停止した場合であって、かつ、当該為替取引が犯罪行為に利用されたと認めるに足りる相当な理由がある場合又は口座開設契約等を締結している者が当該契約を犯罪行為に利用していると認めるに足りる相当な理由がある場合には、資金移動業者の管理下にある当該為替取引及び資金の払出しに係る資金を被害者に返金する等の被害回復のための措置を講じることが望ましい。

（注２）**例えば、資金移動業者が、電子決済手段を発行する場合にあっては、自らが管理しないウォレットに係る電子決済手段の移転及び償還を停止するための態勢を整備する必要がある。**

ステーブルコイン発行者に期待されるリスク低減措置（FATF）

- FATFが2026年３月に公表したステーブルコイン及びアンホステッド・ウォレット（P2P）に関する報告書では、発行市場ではステーブルコイン発行者が顧客にCDDを実施する一方、流通市場では、アンホステッド・ウォレットを介してステーブルコイン発行者が利用者の本人情報を把握できないまま取引が行われ得ると指摘。
- その上で、各国に対し、**ステーブルコイン発行者がスマートコントラクトの機能を活用して、流通市場のML/TFリスクを低減するための措置**を講じるよう求めることを検討すべきとしている。



許可済み（アローリスト）

- **事前承認された主体・アドレスに限り、ステーブルコインの保有・受領・移転を認め**、それ以外のアドレスが送付元又は送付先となる取引を自動的に拒否。
- 事前承認に際しては、発行者又は承認された第三者によるCDDを組み込むことが可能。



拒否（デナイリスト）

- **拒否リストに掲載された主体・アドレスによるステーブルコインの保有・受領・移転を制限**し、当該アドレスが送付元又は送付先となる取引を自動的に拒否。
- リストへの追加基準には、ブロックチェーン分析や法執行機関の情報等を活用可能。



凍結・回収

- **非許可アドレス又は拒否リスト掲載アドレスとの取引について、取引のブロック、ステーブルコインの凍結、バーン・再発行等による回収を行える技術的機能を実装**し、法令に基づく当局の命令にも対応。
- ウォレットアドレスごとに、1件当たり又は1日当たりの取引上限等を設定し、セカンダリー市場のリスクや拒否リストの潜脱リスクを低減。



監視

- 各国は、発行者に対し、**ブロックチェーン分析ツールを活用して、セカンダリー市場におけるステーブルコインの所在・利用状況を能動的に監視**することを義務付けるべきか検討。
- リスクに応じた追加措置として、流通状況の定期報告を求めることも検討。

目次

I. 分散型金融（DeFi）に関するリスク低減策

A) DeFiの概要

B) DeFiに関する規制アプローチとリスク低減策

II. ウォレット提供業者（アンホステッド・ウォレット）に関するリスク低減策

A) アンホステッド・ウォレットの概要

B) アンホステッド・ウォレットに関する規制アプローチとリスク低減策

III. ご議論いただきたい事項

アンホステッド・ウォレットの概要

- 現在一般的に利用されている**ウォレット**は、PCやスマートフォン上のアプリケーションとして提供され、署名鍵の保管に加え、利用者の操作に基づく署名鍵での署名実行、ブロックチェーンへのトランザクション送信、残高の読み込みなどを行う、**デジタル資産の管理及び取引のためのインターフェースとして機能**している。
- ウォレットは、暗号資産交換業者などの事業者が利用者の署名鍵を管理する**ホステッド・ウォレット**と、利用者自身が署名鍵を管理する**アンホステッド・ウォレット**に大別される。アンホステッド・ウォレットの開発主体は特定の企業が担う場合も多い一方、DAOやオープンソースコミュニティといった不特定多数の集団がウォレットの開発・維持を行っているケースも存在するとされる。

	ホステッド・ウォレット	アンホステッド・ウォレット
利用者	• 仮に利用者がパスワード等を紛失しても、鍵は安全に管理されているため、復旧は容易	• 利用者自身で署名鍵を管理 • 基本的には鍵の紛失・盗難が起こると資産の復旧は難しい • ハッキング等による資産流出リスクが存在
ウォレット提供業者	• 事業者がコールドウォレット等で利用者の鍵の安全管理を行う • 事業者の破綻やハッキングによって一度に大量の資産流出が発生するリスクが存在	• 提供業者は鍵管理を行わない
外部サービス	• 事業者が許可していないDeFi等のいわゆるDappsには基本的にはアクセスできない	• DeFi等のいわゆるDappsに対してアクセス可能

（出典）「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）を基に事務局で一部記載を調整

アンホステッド・ウォレットの利用背景

■ 利用者がホステッド・ウォレットではなく、あえて**アンホステッド・ウォレットを利用する背景**には、署名鍵を自身で管理するという目的のほか、**DeFiの利用**、**CEXで扱われないトークンの保有**といった目的があると考えられる。

アンホステッド・ウォレットの利用背景

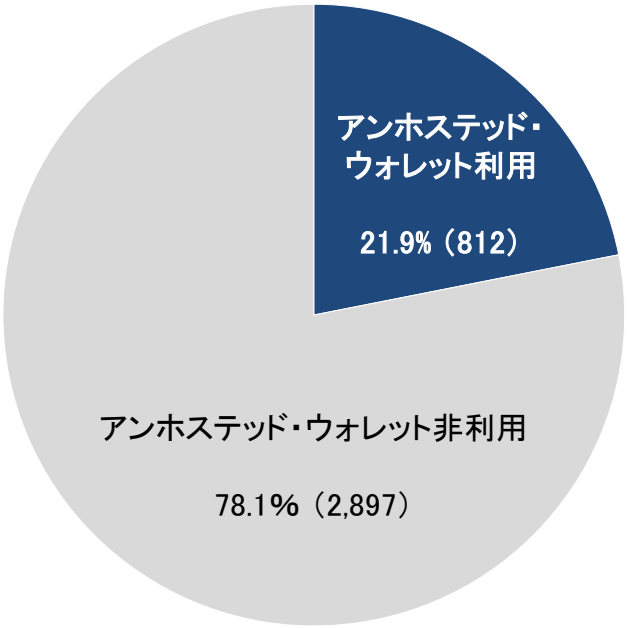
本質的な用途	署名鍵の自主管理	• 自分の資産を管理するための署名鍵を自身で管理できるため、CEX等の破綻の第三者リスクを排除できる • CEX等による送金時確認を通さず、いつでも即時に資産移転ができる
機能的な用途	DeFiの利用	• CEXではアクセスできない各種DeFiプロトコルに接続し、スワップ・レンディングをはじめとした多様な金融サービスを利用できる
	CEXで扱われないトークンの保有	• CEX未上場のトークン（各種ステーブルコインやガバナンストークンを含む）が保有できる

（出典）「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）を基に事務局で一部記載を調整

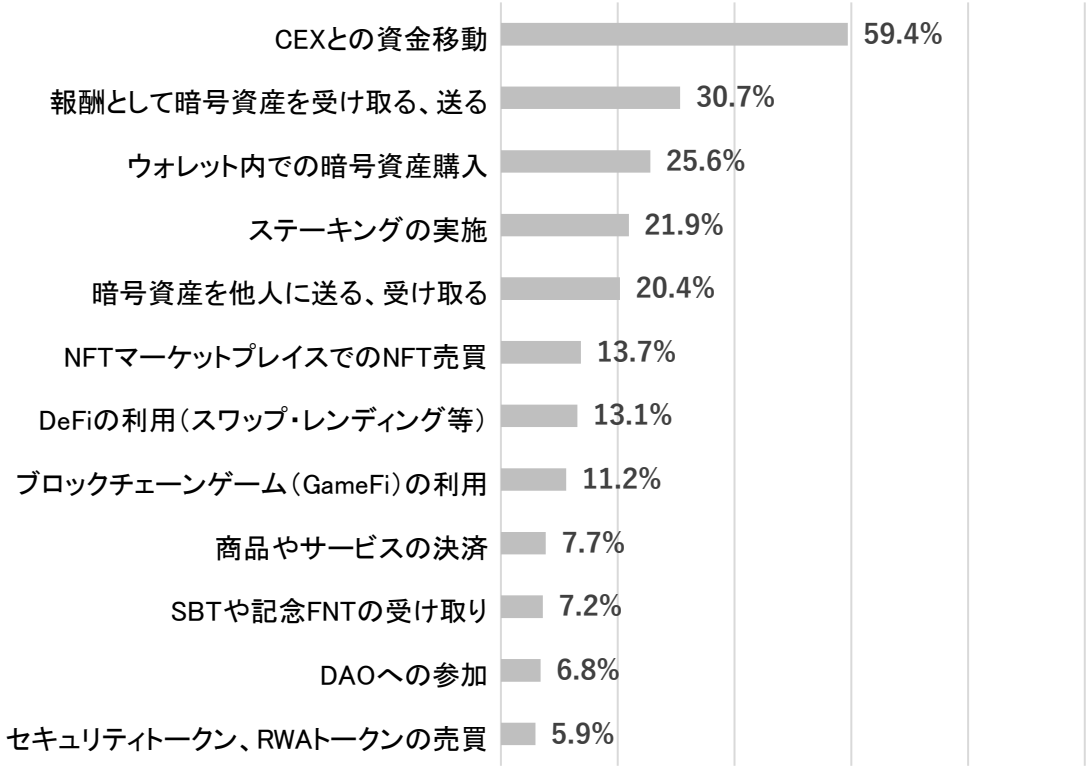
アンホステッド・ウォレットの利用実態

■ 「令和７年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和8年3月）によれば、**暗号資産・NFT保有者に占めるアンホステッド・ウォレット利用者の割合は約2割**であり、その利用用途としては、「CEXとの資金移動」が約6割と最も多くなっている。

暗号資産・NFT保有者に占めるアンホステッド・ウォレット利用者の割合



アンホステッド・ウォレット利用者の主要ユースケース



（出典）「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）

アンホステッド・ウォレット利用に係るリスク

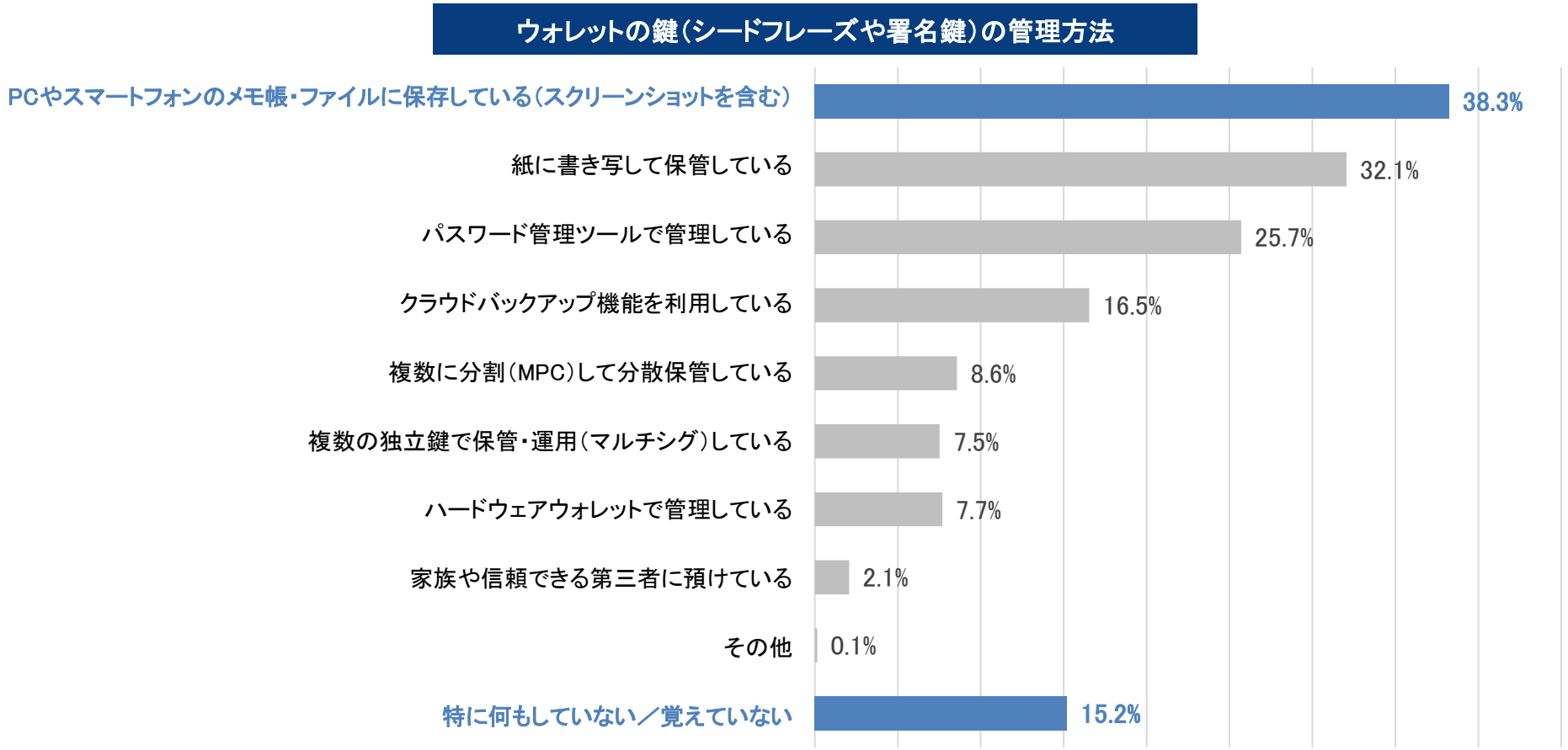
■ アンホステッド・ウォレット利用に係るリスクとして、利用者の誤操作、ウォレットの不備・破綻、詐欺・サイバー犯罪、マネー・ローンダリング・テロ資金供与のリスクが挙げられる。

	アンホステッド・ウォレット利用に係るリスク
利用者の誤操作	• **署名鍵の失念**（署名鍵やシードフレーズを利用者自身が紛失・忘却） • **送付・取引のオペレーションミス**（宛先アドレスやネットワーク選択を誤って誤送金した結果、回復が困難となる）
ウォレットの不備・破綻	• **ウォレットの機能不全**（ウォレットソフトウェアが欠陥や負荷上昇等でダウンし、正常利用できなくなる） • **ウォレット提供業者の不正・倒産**（ウォレット提供業者が利用者資産を窃取する、又は倒産により一部利用者が資産にアクセスできなくなる等）
詐欺・サイバー犯罪	• **署名鍵の盗難**（被害者が「操作代行」を名乗る攻撃者に署名鍵を送付し、攻撃者がアンホステッド・ウォレットを復元して即時送金する等） • **フィッシングによる不正署名**（検索広告等から偽サイトへ誘導し署名させ、攻撃者のコントラクトがトークンを移転する等） • 投資・交換業者関連詐欺（マッチングアプリ等を通じて偽投資サイトや無登録交換業者へ誘導し、入金後に出金不能となる等） • 本人確認情報の窃取・悪用（資産残高が多いアドレス所有者の本人確認情報を把握した攻撃者が強盗を起こす等）
マネー・ローンダリング・テロ資金供与	• **マネー・ローンダリング・テロ資金供与**（サイバー犯罪の犯人がミキシングサービスを経由してマネー・ローンダリングを行う、テロ組織や経済制裁下の主体に匿名で送金を行う等）

（出典）「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）を基に事務局で一部記載を調整

アンホステッド・ウォレットの署名鍵の管理方法

- 「令和７年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）は、利用者の約４割が、シードフレーズや署名鍵をオンライン端末内に平文又は画像として保存するなど、**署名鍵をセキュリティ上のリスクが高い方法で管理**しており、**セキュリティに関する意識が低い層も一定数存在**すると指摘。
- 署名鍵の紛失・漏えいに伴う資産喪失リスクを低減する上では、例えばMPCやマルチシグ等の技術を用いた署名鍵の分散管理・保護やスマートコントラクトウォレットを用いた署名鍵のバックアップと回復が考えられる。



（出典）「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）を基に事務局で一部記載を調整

目次

I. 分散型金融（DeFi）に関するリスク低減策

A) DeFiの概要

B) DeFiに関する規制アプローチとリスク低減策

II. ウォレット提供業者（アンホステッド・ウォレット）に関するリスク低減策

A) アンホステッド・ウォレットの概要

B) アンホステッド・ウォレットに関する規制アプローチとリスク低減策

III. ご議論いただきたい事項

ウォレット提供業者（アンホステッド・ウォレット）への対応

■ **ウォレット提供業者**（アンホステッド・ウォレット）について、暗号資産WG報告では、**署名鍵の紛失等が生じた場合に利用者が暗号資産を移転できなくなるリスク**を指摘しつつも、**現状では、個人の利用者は、国内の交換業者が提供するウォレットを利用することが中心であるため、直ちに規制を設ける必要性は低い**と考えられるが、どのように規制していくべきか、**将来的な課題として検討**していくことが適当としている。

暗号資産WG報告

Ⅲ　求められる対応
4. 業規制
（2）個別論点
ウ. 利用者財産の管理
72　なお、事業者が、利用者の暗号資産を移転するために必要な署名鍵の一部を預かるにとどまる場合には、暗号資産の管理を行っているものではないため、暗号資産交換業の登録は不要とされているが、署名鍵の紛失等が生じた場合、利用者が暗号資産を移転できなくなるリスクがある。現状では、個人の利用者は、国内の交換業者が提供するウォレットを利用することが中心であるため、そうしたサービスについて直ちに規制を設ける必要性は低いと考えられるが、当該事業について暗号資産交換業の対象とすることは規制が過重なものとなり得るとの指摘があることも踏まえ、どのように規制していくべきか、将来的な課題として検討していくことが適当と考えられる。

○　事務ガイドライン（第三分冊：金融会社関係 16 暗号資産交換業者関係）
Ⅰ－1－2－2暗号資産交換業の該当性の判断基準
③　法第2条第15項第4号に規定する「他人のために暗号資産の管理をすること」に該当するか否かについては、個別事例ごとに実態に即して実質的に判断するべきであるが、利用者の関与なく、単独又は関係事業者と共同して、利用者の暗号資産を移転でき得るだけの秘密鍵を保有する場合など、**事業者が主体的に利用者の暗号資産の移転を行い得る状態にある場合には、**同号に規定する**暗号資産の管理に該当する。**
（注2）上記③の「主体的に利用者の暗号資産の移転を行い得る状態」に該当するか否かについては、個別事例ごとに実態に即して実質的に判断するべきであるが、**例えば、以下のような場合は、「主体的に利用者の暗号資産の移転を行い得る状態」には該当しないものと考えられる。**
・**事業者が、単独又は関係事業者と共同しても、利用者の暗号資産を移転するために必要な秘密鍵の一部を保有するにとどまり、事業者が単独又は関係事業者と共同して保有する秘密鍵のみでは利用者の暗号資産を移転することができない場合。**
・事業者が利用者の暗号資産を移転することができ得る数の秘密鍵を保有する場合であっても、その保有する秘密鍵が暗号化されており、事業者が当該暗号化された秘密鍵を復号するために必要な情報を保有していない場合。

アンホステッド・ウォレットのリスクへの対応策

- 「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和8年3月）では、**アンホステッド・ウォレット利用に係るリスクのうち利用者の誤操作、ウォレットの不備・破綻、詐欺・サイバー犯罪、マネー・ローンダリング・テロ資金供与への対応策**を整理している。
- もっとも、**アンホステッド・ウォレットに係る直接的な規制**・規範を実装するような事例は**諸外国を含め、確認されなかった**としている。

アンホステッドウォレットのリスクへの対応策

a	鍵管理・回復	秘密鍵の分散管理やバックアップ・回復手段の提供により、鍵の紛失・漏えいに伴う資産喪失リスクを低減する取組	アンホステッド・ウォレット提供者による対応策
b	本人確認・認証	段階的KYCやプライバシーに配慮した本人確認、パスキー等の認証強化により、不正利用の抑止や本人確認を行う取組	
c	取引の安全性・監視	署名前のトランザクションシミュレーションや悪性アドレスへの接続警告、送金上限の設定、リアルタイム監視等により、取引時のリスクを検知・制限する取組	
d	ガバナンス・エコシステム上の対策	ウォレット提供者自身のセキュリティ監査や情報開示等のガバナンス確保と、エコシステム全体でのリスク情報共有や認証制度の構築を通じて利用者保護を担保する取組	
e	CEXにおける対策	オンランプ・オフランプを担うCEXにおいて、ウォレットの所有権証明や高リスクアドレスとの取引遮断、本人確認情報とウォレットアドレスの紐づけ管理等を行う取組	アンホステッド・ウォレット外部における対応策
f	接続先における対策	DeFiやNFTマーケットプレイス等のWeb3サービスにおいて、接続・取引の制限、詐欺疑いのあるトークン等への警告表示、接続先の真正性検証等を行う取組	
g	規制・規範	法規制やガイドライン、業界団体による自主規制、規格化・標準化等を通じて、上記の各対応策が一定の実効性をもって実装・運用されることを制度面から担保する取組	

（出典）「令和7年度Web3分野におけるアンホステッド・ウォレットに係る整理・検討に関する調査報告書」（デジタル庁委託、株式会社野村総合研究所、令和８年３月）

アンホステッド・ウォレットへの規制アプローチ（FATF）

■ FATFが2021年10月に公表した「暗号資産及び暗号資産サービス提供者に対するリスクベース・アプローチに関するガイダンス」改訂版では、**FATF基準は技術中立的であり、ソフトウェア又はハードウェアの開発・販売のみにとどまるアンホステッド・ウォレット提供業者は、通常、VASPとして規制されない**としている。

■ 一方で、**アンホステッド・ウォレットとの取引**について、その**匿名性や管理者による移転制限の欠如**により、VASP間の取引よりも**相対的にマネー・ローンダリング等のリスクが高く、**かかるリスクへの対応の必要性を指摘。

「暗号資産及び暗号資産サービス提供者に対するリスクベース・アプローチに関するガイダンス」改訂版（FATF）

安全保管・管理

75. VASPの定義の類型（iv）（暗号資産の安全保管・管理）との関係では、各国は、本人の暗号資産を安全に保管する機能、又は当該暗号資産を管理若しくは移転する権限を提供するサービス又はビジネスモデルを考慮すべきである。（略）安全保管・管理サービスには、他人に帰属する暗号資産に関連付けられた署名鍵を支配する者、又は、自らは当事者ではないものの、他人に帰属する暗号資産が関係するスマートコントラクトを支配する者が含まれ得る。

76. （略）**ソフトウェア／ハードウェアの開発・販売のみにとどまるソフトウェア開発者又はアンホステッド・ウォレット提供者も通常VASPの定義を満たさない。**もっとも、各国は、具体的な事案にこの定義を適用するに当たって、個別の事実及び状況を検討しなければならない。

定義の適用範囲

81. 前述のとおり、**FATF基準は技術中立的である。**したがって、**FATFは、暗号資産又はVASPの活動の基礎となる技術を規制しようとするものではない。**むしろ、FATFが規制しようとしているのは、そのような技術の背後に存在し、他の自然人又は法人のために、前述したVASPの活動を事業として行う自然人又は法人である。

83. **FATFは、暗号資産ネットワークに付随的なサービス又は製品を提供する自然人又は法人をVASPとして規制することも意図していない。これには、ハードウェア・ウォレット製造業者又はアンホステッド・ウォレット提供者などによる付随的サービスの提供が含まれる。**ただし、それらの者が、他人のために、又は他人に代わって、前述した対象となる暗号資産活動又は業務のいずれかを、事業として併せて行い、又は積極的に促進していない限りにおいてである。（略）

アンホステッド・ウォレットへの／からの暗号資産の移転

295. **VASP及びその他の義務主体は、非義務主体（例：アンホステッド・ウォレット）との間で暗号資産（VA）の移転を行うことがある。そのような場合、VASPは送付人及び受取人に関する必要な情報を自らの顧客から取得すべきである。**なぜなら、別のVASPから当該情報を取得することができないからである。こうした移転は、取引モニタリング及びターゲット型金融制裁の遵守を含む、VASPのより広範なAML/CFT義務の対象となる。

296. **VASPは、アンホステッド・ウォレットとの間の暗号資産移転及び関連するP2P取引がもたらすリスクを認識すべきである。このような取引は、匿名性、持ち運び可能性に対する制限の欠如、高い移動性、取引速度及び利用容易性により、違法行為者にとって魅力的となり得る。**したがって、VASPはアンホステッド・ウォレットとの取引に関するデータを収集し、その情報を必要に応じてモニタリング及び評価すべきである。これは、当該取引が自らのリスク許容度の範囲内にあるかを判断し、当該取引又は個々の顧客に適用すべき適切なリスクベースの管理措置を決定し、さらに疑わしい取引の届出（STR）義務を履行するためである。（略）

アンホステッド・ウォレットへの規制アプローチ（米国CLARITY法案）

- CLARITY法案では、**アンホステッド・ウォレット**（self-custodial wallet）**の開発等の技術的活動のみを理由として証券取引規制やデジタル商品取引規制の対象としない**こととしている。ただし、SEC・CFTCによる反詐欺・反相場操縦及び虚偽報告に関する権限執行については適用除外の対象としないこととしている（Sec.10601, 20209）。
- また、同法案では連邦政府機関は、**個人がアンホステッド・ウォレットを利用して自身のデジタル資産を保管する能力を禁止、制限、又は阻害してはならない**ことを規定している。一方で、**米財務省、SEC、CFTC、銀行監督当局その他の連邦政府機関が、違法金融、マネー・ローンダリング、テロ資金供与および制裁に関する既存法令を執行する権限は維持される**としている（Sec.10605）。

Crypto Task Force Round Table on Decentralized FinanceにおけるアトキンスSEC委員長の発言（2025年6月9日）

ブロックチェーン技術のもう一つの中核的な特徴は、個人が暗号資産を自身のデジタルウォレットで自己保管（セルフカストディ）できる点にある。**自らの私有財産を自己保管する権利は、米国の基本的価値観の一つであり、その権利はインターネットに接続した途端に失われるべきものではない。**私は、市場参加者が暗号資産を自己保管することについて、より大きな柔軟性を認めるべきだと考えている。特に、仲介者の介在が不必要な取引コストを生じさせたり、ステーキングその他のオンチェーン活動を行う能力を制限したりする場合にはなおさらである。

ソフトウェア開発者の保護（CLARITY法案 Sec.10601, 20209）

本法（証券取引所法、商品取引所法）その他の規定にかかわらず、分散型台帳システム又はその構成要素の運営に関連して、ある者が以下の活動のいずれかを単独又は組み合わせて行うことのみを理由としては、当該者を本法及び本法に基づいて制定された規則の適用対象としてはならない。

- 分散型台帳システム又は、**利用者が自己のデジタル資産若しくは署名鍵を保有・保護・管理することを可能にするソフトウェア若しくはシステム（ウォレットを含む。）を開発、公開又は提供すること。**

※ 2026年9月14日ルミス上院議員公表のCLARITY法案の条文及び概要を基に作成。法案は未成立のため、今後内容が変更される可能性。

（再掲）フロントエンド提供者への規制アプローチ（米国SECスタッフ見解）

■ SECは、2026年4月、**利用者がアンホステッド・ウォレット**（self-custodial wallet）**を用いて自ら**トークン化証券（crypto asset securities）の**取引を実行することを支援するにとどまるUI**（ユーザー・インターフェース）については、**利用者の意思決定に干渉しない**こと等の条件を満たすことを前提に、**UI提供者がブローカー・ディーラーの登録を行わなくても異議を唱えない**との見解を公表した。なお、UIはウォレットに組み込まれている場合もあれば、独立してダウンロード可能な形で提供される場合もある。

ブローカー・ディーラーの登録を要しない条件

● UI提供者がUIの開発・提供・運営において以下の措置を講じていること

- ユーザーが取引条件を自由に設定できるようにしていること
- ユーザーに特定の暗号資産証券の取引を推奨・勧誘しないこと
- 接続・連携する取引所や取引システムを定めていること
- UI提供者が運営する取引所と接続・連携する場合は、その関係性を明確に開示し、他の取引の場と同等の条件で接続・連携すること
- 複数の注文執行ルートの中で単一の注文執行ルートのみ表示する場合は、ユーザーが他の注文執行ルートを確認できるようにすること
- 複数の注文執行ルートを表示する場合には、価格やスピードなどの客観的要素に基づく並び替えやフィルタリング機能を提供すること
- 特定の注文執行ルートを「最良」などと評価するコメントを行わないこと
- 取引指示作成や注文執行ルートの表示において、事前に開示された第三者により検証可能な客観的パラメータに基づいて動作するソフトウェアのみを使用すること
- UIが市場情報や証券取引について、裁量を行使したり、意思決定に関与しないこと
- 手数料は定額又は定率で客観的かつ一貫した基準に基づいて利用者に課すものとし、銘柄、執行ルート、執行市場又は取引相手によって変動させないこと
- UI提供者が、接続する取引所等の評価・選定・監査に係る方針、手順及び管理体制を整備するとともに、デフォルトの取引条件についても客観的基準に基づく選定・定期的な見直し及び利益相反への対応を行うこと
- UIの開発・提供・運営におけるUI提供者の役割、手数料、利益相反、特定の銘柄・市場データ・取引所等の利用制限、サイバーセキュリティー対策、相場操縦等からの利用者保護措置、接続・連携する取引所等、既定の注文執行条件などの重要事項について、ユーザーに対して明確に開示し、必要に応じて速やかに更新すること

● 以下のサービスを実際に行っている又は行っていると対外的に表示しているUI提供者はスタッフ見解の対象外

- 取引条件の交渉
- 特定の暗号資産証券の取引の勧誘
- 投資判断の推奨や投資助言
- 資金調達の手配
- 取引書類の処理
- 独立した立場での資産評価
- ユーザーの資金、証券・ステーブルコインの預託等
- 取引の執行や清算
- 注文の受付や他の事業者への注文の回送

（出典）Staff Statement Regarding Broker-Dealer Registration of Certain User Interfaces Utilized to Prepare Transactions in Crypto Asset Securities (Division of Trading and Markets, April 13, 2026)

アンホステッド・ウォレット等との取引に係る義務

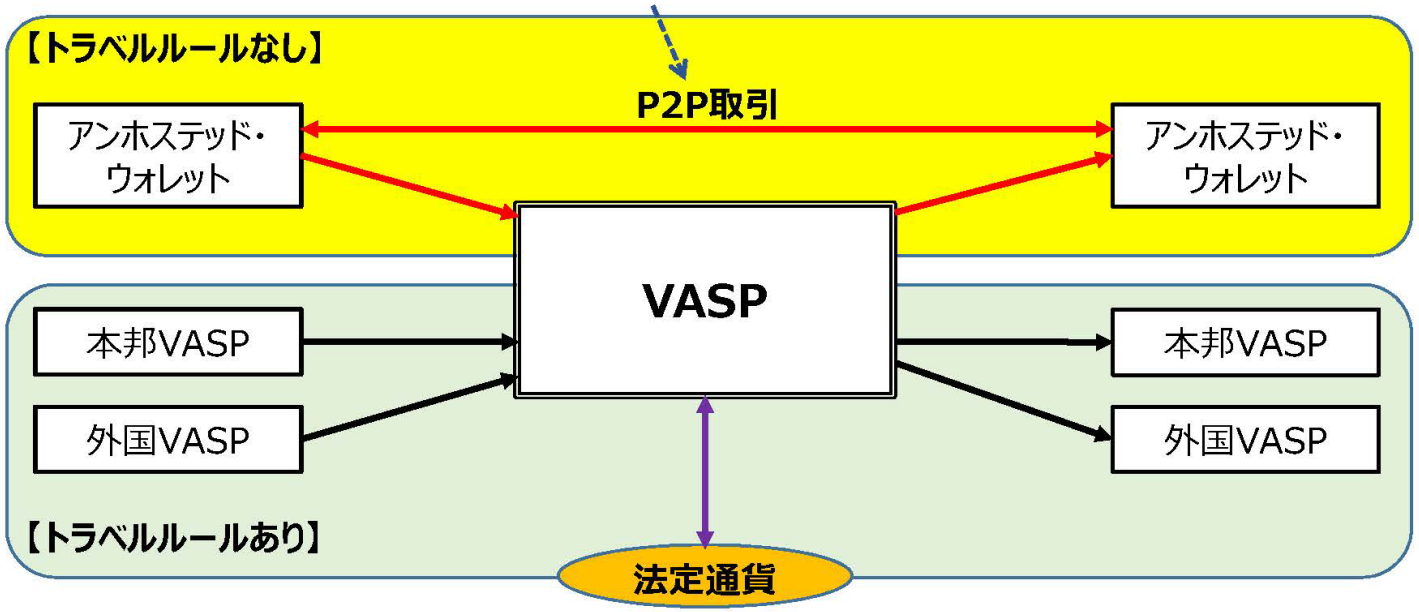
■ 犯収法においては、アンホステッド・ウォレットとの取引を行う国内VASPに対し一定の義務（当該取引に係る記録保存、情報収集義務等）を課している。

■ 暗号資産・電子決済手段は、利用者が自ら管理するウォレットである「**アンホステッド・ウォレット**※」に対して移転することが可能であり、当該ウォレットを用いた**P2P取引**が可能。

■ アンホステッド・ウォレットとの取引は、その匿名性や管理者による移転制限の欠如によるリスクが存在するところ、**FATF等においても対応の必要性が指摘されており、我が国においても対応を検討**。

※ アンホステッド・ウォレットとは、事業者がホスト（管理）していないウォレット（口座）を意味する。

為替取引における個人間の現金取引に相当し、VASPは取引に関与していないため、VASPによる把握は困難



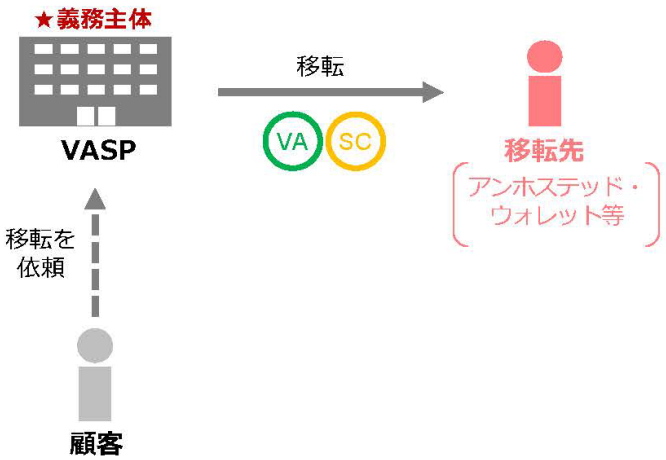
アンホステッド・ウォレット等との取引に係る義務

■ 犯収法においては、アンホステッド・ウォレットとの取引を行う国内VASPに対し一定の義務（当該取引に係る記録保存、情報収集義務等）を課している。

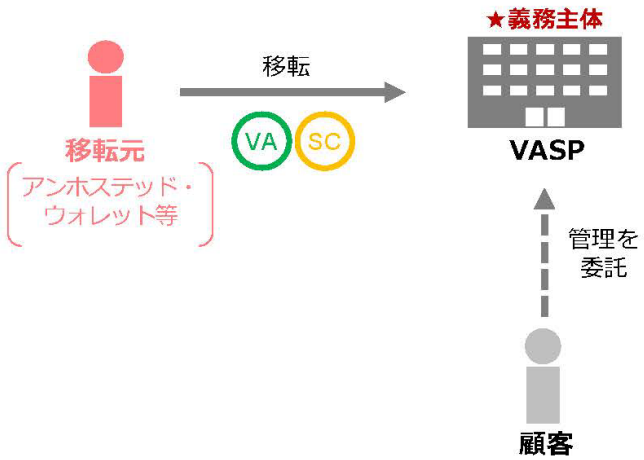
■ VASPに対し、**アンホステッド・ウォレット等＊との取引についても所有者情報を収集・保存することを求め**、トラベルルールと合わせて、**取引経路の可視化を進める**。

＊個人が管理するウォレットのみならず、無登録業者や通知義務が課されていない国等に所在する事業者が管理するウォレットなど、通知義務の対象外のウォレットを指す。

【取引ケース①（移転を行う場合）】



【取引ケース②（移転を受ける場合）】



記録・保存義務 ［規則第24条］

➢ 取引相手のアンホステッド・ウォレット等の所有者情報（氏名・アドレス等）を取得し、記録することを求める（注）。

（注）移転を受ける場合には、自らの顧客が送付元の所有者情報を全て把握しているとは限らないことから、知り得た事項に限る。

情報収集義務等 ［規則第32条］

➢ 体制整備の内容として、以下の措置を講ずることを求める。

✓ 取引相手のアンホステッド・ウォレット等の属性について調査・分析し、マネロンリスクの評価を行うこと

✓ 取引相手の所有者情報（氏名・アドレス等）を収集すること

暗号資産に係る規制の見直し

- **令和8年金商法・資金決済法改正**では、暗号資産取引業者に対して暗号資産の管理を行うための重要なシステムの提供等を行う事業者に係る規制（事前届出、システムの安全性確保義務等）を導入している。
- また、**暗号資産が詐欺的な投資勧誘の支払手段として利用されることを未然に防ぐ措置**（内閣府令事項）として、例えば、**新規口座開設直後にはアンホステッド・ウォレットへ移転できない等の熟慮期間を設ける等の措置**を講じることを求めることとしている。

暗号資産WG報告

Ⅲ　求められる対応
4. 業規制
（2）個別論点
ウ. 利用者財産の管理
（略）**最近の不正流出事案では、交換業者向けのウォレットソフトウェアを提供する事業者がサイバー攻撃を受けたことが不正流出の一因となったものが見られる。**こうした事案の再発防止の観点から、交換業者が委託先に対する指導等を適切に行う責任を負うことを前提としつつも、**交換業者に対して暗号資産の管理を行うための重要なシステムの提供等を行う事業者[73]について、その業務の適切な運営を確保するための規制を設けるべきである。**具体的には行政への事前届出を義務付けた上で、過去における交換業者の登録取消等の一定の欠格事由や交換業者に提供するシステムの安全性の確保義務等の行為規制を設けることとし、必要な場合に行政において直接に実態把握及び是正措置を命ずることができるよう監督権限を設けることが適当である。その上で、交換業者が、外部の者から暗号資産の管理を行うための重要なシステムの提供等を受ける場合には、例えば、届出を行った事業者のみから提供を受けることができることとすることが考えられる 。
なお、その場合の規制内容の詳細については、規制負担が重過ぎるために有用なサービスを提供する事業者が撤退し、かえって利用者の利便性やシステムの安全性が低下することのないよう、適切な水準とすることが重要であり、また、必要な経過措置も検討すべきである。
73　利用者の暗号資産の管理を行っておらず、現行法上、暗号資産交換業の登録は不要。

（4）無登録業者への対応等
ウ. 支払手段としての利用者被害の未然防止
暗号資産が詐欺的な投資勧誘の支払手段として利用されることを未然に防止するため、**交換業者に対し、法令上の義務として、利用者がアンホステッド・ウォレットや無登録業者のウォレットに暗号資産を移転する場合に、詐欺的事案の可能性に関する警告や移転目的の確認、取引モニタリングの適切な実施、新規口座開設直後及び新規ウォレット先への移転について一定の熟慮期間を設けるなどの対応を求めることが適当である。**
（略）

目次

I.　分散型金融（DeFi）に関するリスク低減策

A)　DeFiの概要

B)　DeFiに関する規制アプローチとリスク低減策

II.　ウォレット提供業者（アンホステッド・ウォレット）に関するリスク低減策

A)　アンホステッド・ウォレットの概要

B)　アンホステッド・ウォレットに関する規制アプローチとリスク低減策

III.　ご議論いただきたい事項

ご議論いただきたい事項

Ⅰ．DeFiに関する規制アプローチとリスク低減策

- いわゆるDeFi（Decentralized Finance：分散型金融）については、明確な定義は存在しないが、スマートコントラクトを利用することで様々な金融サービスを中央集権的な管理者が存在しない形で構築する試みであり、その一例としてDEX（Decentralized Exchange：分散型取引所）が挙げられる。もっとも、分散型と称するDeFiの商品・サービスの中には、実際には中央集権的な性質を有している場合があるとの指摘もある。
- 「同じ機能・リスクには同じルールを適用／同じ規制効果を実現する」との考え方に基づく、機能・リスクに応じた規制適用アプローチが国際的にも支持されている。もっとも、規制の名宛人をどのように特定するかについて、どのような場合を規制の名宛人が特定されていると考えるかを含め、具体的な判断基準や監督実務は国際的にも十分に確立していない。

【ご議論いただきたい事項】

- **DEXをはじめとするDeFiについて、そのメリットやユースケース、リスクや金融規制・監督上の課題についてどのように考えるか。**
- 分散型と称するDeFiについて、実際には中央集権的な性質を有している場合があるとの指摘もあるところ、**どのような場合を規制の名宛人を特定できると考えるかを含め、**規制の名宛人を特定する**判断基準や規制アプローチをどう考えるか。**
- **金融サービスが幅広く利用される前提として、**システム全体が技術・契約・制度・インセンティブ・信頼等によって規律付けられる必要があり、**規制の名宛人として管理責任を果たせる立場にある者**がこうした状態を実現するべきではないか。
- **既存の金融事業者がDeFiを活用して金融サービスを提供する場合**、金融規制上達成されるべき利益(注)の確保に向け、**金融事業者はどのような役割を果たすべきか。**
- **規制の名宛人として管理責任を果たせる立場にある者が明らかではない場合、**金融規制上達成されるべき利益(注)を確保できず、**幅広く利用される金融サービスとしての前提を欠くのではないか。**また、このような場合、日本法の下で与えられている利用者保護が及ばない、トラブルが生じた際の対応が困難である等、**利用者に不利益が生じる可能性もあるところ、リスク周知や規制の在り方を含め、利用者保護を図る観点からどのような方策が考えられるか。**

（注）①「機能」の確実な履行、②利用者に対する情報提供等、③利用者資産の保護、④利用者情報の保護、⑤AML/CFT、⑥システミックリスクの顕在化の防止

- DeFiの**フロントエンド提供者**について、FATFの報告書においてはFATF基準の適用対象となり得る旨が指摘されている一方で、一部の法域においては適法な用途にも違法な用途にも利用できる価値中立的なソフトウェアの開発・公表等の技術的活動を直ちに規制すべきではないとの考え方に基づき、一定の場合は金融規制の対象外であることを明確化しようとする試みもみられるところ、**規制を及ぼすことの是非や規制の在り方についてどう考えるか。**

ご議論いただきたい事項

Ⅰ．DeFiに関する規制アプローチとリスク低減策（続き）

- **既存の金融事業者が金融サービスの提供に当たりDeFiを活用する場合**においても、「同じ機能・リスクには同じルールを適用／同じ規制効果を実現する」という考え方に基づき、**同じ規制効果を実現する必要がある**と考えられる。
- **規制の名宛人として管理責任を果たせる立場にある者が明らかではない場合**について、利用者がリスクを理解した上で利用することは基本的に自己責任であるとの考えもありうるが、その場合でも**マネー・ローンダリング及びテロ資金供与の防止等**は、**利用者保護とは別個の公益的要請として確保される必要**があると考えられる。
- 一方、**マネー・ローンダリング及びテロ資金供与の防止等**について、DeFiにおいて**リスクを低減する技術的措置**を講じる動きも見られる。

【ご議論いただきたい事項】

- 規制の名宛人として管理責任を果たせる立場にある者が明らかではない場合であっても、**まずはDeFiと接点を有する規制対象事業者（ステーブルコイン発行者、オン・オフランプ提供事業者、金融機関）を通じて、マネー・ローンダリング及びテロ資金供与の防止等を図ることが適当ではないか。**また、**どのようなリスク低減策が考えられるか。**
- AML/CFTが確保されていないDeFiへの**利用者のアクセスを抑止する必要性についてどのように考えるか。**

ご議論いただきたい事項

Ⅱ．アンホステッド・ウォレットに関する規制アプローチとリスク低減策

- ウォレットは、暗号資産交換業者などの事業者が利用者の署名鍵を管理するホステッド・ウォレットと、利用者自身が署名鍵を管理するアンホステッド・ウォレットに大別される。
- **現状では、個人の利用者は国内の交換業者が提供するホステッド・ウォレットを利用することが中心**である。一方、今後、様々な金融資産のトークン化が進むと、ワンストップで各種資産の管理を行えるアンホステッド・ウォレットサービスの利用が進む可能性もある。
- **国際的に、**アンホステッド・ウォレットの利用や、ソフトウェア又はハードウェアの開発・販売のみにとどまる**アンホステッド・ウォレット提供業者を直接規制する動きは広くは見られない。**また、例えば米国では、アンホステッド・ウォレットにフロントエンド機能が組み込まれている場合についても、一定の要件を満たす場合にはブローカーに該当しないことを明確化する動きもある。
- アンホステッド・ウォレットについては、**署名鍵の紛失等が生じた場合に利用者が暗号資産を移転できなくなるリスク**などが指摘されている。
- 利用者がリスクを理解した上でアンホステッド・ウォレットを利用することは基本的に自己責任であるとの考えもありうるが、その場合でも**マネー・ローンダリング及びテロ資金供与の防止等は、利用者保護とは別個の公益的要請として確保される必要**がある。
- 我が国では、アンホステッド・ウォレットとの取引を行う国内VASPに対し当該取引に係る記録保存、情報収集義務等を課しているほか、暗号資産が詐欺的な投資勧誘の支払手段として利用されることを未然に防ぐ措置（内閣府令事項）として、例えば、新規口座開設直後にはアンホステッド・ウォレットへ移転できない等の熟慮期間を設ける等の措置を講じることを求めることとしている。

【ご議論いただきたい事項】

- **（アンホステッド・）ウォレットについて、そのメリットや考えられるユースケース、リスクや金融規制・監督上の課題についてどのように考えるか。**
- 国内のアンホステッド・ウォレットの利用者の中には、署名鍵をセキュリティ上のリスクが高い方法で管理しており、セキュリティに関する意識が低い層も一定数存在するとの指摘がある。**アンホステッド・ウォレットについても、**日本法の下で与えられている利用者保護が及ばない、トラブルが生じた際の対応が困難である等、**利用者に不利益が生じる可能性もあるところ、リスク周知や規制の在り方を含め、利用者保護を図る観点からどのような方策が考えられるか。**
- マネー・ローンダリング及びテロ資金供与の防止等に係る**更なるリスク低減策の必要性についてどのように考えるか。**