資料3

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（第3回）

2026年11月26日

日本暗号資産ビジネス協会
Japan Cryptoasset Business Association

目次：DeFiの活用と、それを支えるセキュリティ

Japan Cryptoasset Business Association

DeFiが既存金融にもたらす価値と、その仕組みに即したセキュリティのあり方を整理（2026年10月31日時点）

P.3　DeFi概観（マネーレゴ）
- 積み重なる層と、全層を横断するリスク管理

P.4　伝統金融とDeFiがつながる構図
- 4つの橋と、接続による変化

P.5　伝統金融がDeFiを活用するメリット
- 7つのメリットと活用の前提

P.6　市場厚生の観点から見たDeFiの意義
- 摩擦の増減で見る差し引きの効果

P.7　AIの進化が伝統金融に突きつける課題
- AI活用・ステーブルコイン・AIによる攻防

P.8　DeFiセキュリティの実装
- レイヤーごとの論点と実装方法

P.9　各プロダクトのトラストポイント
- 信頼の所在と利用者との接点

P.10　DeFiセキュリティのフレームワーク
- 34の管理策と3つの層

P.11　取引の流れとセキュリティの介入点
- 署名から確定後までの介入点

P.12　まとめ
- 全体の論点整理（活用事例は別冊「参考資料」）

DeFi概観｜積み重なる層（マネーレゴ）

Japan Cryptoasset Business Association

下層の上に上層が組み上がる構造。金融サービス6類型は「コア金融」の層に該当。

アプリ・UX	**個人ウォレット** MetaMask・HashPort	**機関ウォレット** Fordefi等	**機関投資家の入口** トークン化ファンド Aave Horizon	**AIエージェント** 自動運用・LP管理	**全層を横断** リスク管理・セキュリティ・AML/CFT リスク設計 Gauntlet 脅威検知・遮断 Hypernative 署名前の検査 Blockaid 準備金証明 Chainlink 監査・形式検証 Certora 追跡・AML/CFT Chainalysis・TRM Labs
運用・集約	**キュレーター** Gauntlet・Steakhouse	**アグリゲーター** 1inch・Jupiter	**インテント執行** CoW・UniswapX	**利回り戦略** Pendle等	
コア金融	**① 交換** Uniswap・Curve **② 貸借** Aave・Compound **③ ステーキング** Lido・EigenLayer	**④ 先物** Hyperliquid	**⑤ 運用管理** Morpho・Euler	**⑥ 条件付き補償** Nexus Mutual	
データ・接続・鍵	**価格情報** Chainlink・Pyth	**チェーン間接続** CCIP・LayerZero	**カストディ** BitGo等	**鍵の管理** Safe・Dfns	
決済基盤	**L1** Ethereum・Solana	**L2** Base・Arbitrum	**金融特化L1** Hyperliquid	**取引の順序付け** ビルダー等	

上の層は下の層を部品として利用。利便性の一方で、価格情報・流動性・鍵への依存が層をまたいで連鎖し得る。

当局の用語：① 交換＝DEX（アグリゲーターも含み得る）／② 貸借＝レンディング／④ 先物＝デリバティブ／⑤ 運用管理＝イールドアグリゲーター

伝統金融とDeFiがつながる構図

Japan Cryptoasset Business Association

伝統金融の資産・信用とDeFiの流動性・即時性は補完関係にあり、接続により新たな価値が生じ得る

伝統金融 規制された仲介者

投資家・企業
△ 取引時間・地域が限定的

銀行・証券・運用会社
△ 照合・決済に時間とコストがかかる

法定通貨・証券
△ 担保が市場ごとに滞留しやすい

コンプライアンス
◇ 事前の本人確認・審査で信頼を担保

資産・事前審査の仕組み

お金の橋	ステーブルコイン・預金トークン	例：USDC、EURCV、JPMD、JPYC
資産の橋	トークン化	例：BUIDL、ACRED、トークン化国債
入口の橋	カストディ・ウォレット／許可型の接続	例：BitGo、Fireblocks、Aave Horizon
データの橋	オラクル	例：Chainlinkが価格・基準価額を届ける

利回り・流動性・24時間の即時決済

DeFi オープンな金融

DEX（取引）
◎ 24時間、グローバルな取引相手

レンディング（貸借）
◎ 担保を即座に資金化・運用できる

ステーキング・流動性供給
◎ 保有資産から利回りを得られる

コンプライアンス
◇ 取引をリアルタイムで監視し、不正を自動で遮断

伝統金融内で完結する場合 → DeFiと接続した場合

時間	流動性	資本効率	開発	透明性
平日の取引時間、決済はT+1～2	自社・国内の市場	担保・資金が市場ごとに滞留	商品ごとに自前でシステム構築	照合と事後の報告が中心
→ 24時間365日、取引と同時に決済	**→ 世界のオンチェーン流動性（ステーブルコイン送金は月約10兆ドル）**	**→ 同じ資産を担保・運用・決済に連続利用**	**→ 実績あるプロトコルを部品として利用**	**→ 台帳上でリアルタイムに検証**

主要金融機関の動向 BlackRock・JPMorgan・HSBC・Société Générale（子会社SG-FORGE）・Apolloが接続を進め、Swiftでは17行がトークン化預金を試行中

事例・数値は各社の公表資料・報道に基づく（2026年10月時点）。

伝統金融がDeFiを活用するメリット

Japan Cryptoasset Business Association

DeFiは競合ではなく、24時間稼働する共通の金融インフラとして活用し得る

1 新たな運用・収益機会

保有資産を担保・貸付・流動性供給に回し、利回りや手数料収入を得る

事例 Apollo：トークン化ファンドACREDを担保にMorphoで借入・買い増し、利回りを上乗せ（参考資料 事例③）

2 資産・収益源の多様化

暗号資産に加え、トークン化されたプライベートクレジット・株式・コモディティなどに小口でアクセスできる

事例 BUIDL（米国債）やACRED（プライベートクレジット）など、従来は機関投資家向けの資産をトークンで保有（参考資料 事例②③）

3 24時間・即時の流動性

市場が休止せず、取引と決済が同時に完了。週末・夜間も資金移動が可能

事例 SG-FORGE（ソシエテ・ジェネラルの子会社）が発行するEURCV・USDCVを、24時間取引できるUniswap・Morphoに投入（参考資料 事例①）

4 資本効率の向上

同一資産を担保・決済・運用に連続して用い、遊休担保を削減する

事例 BlackRock：BUIDLを取引・決済に加え、担保やステーブルコインの裏付け資産としても再利用（参考資料 事例②）

5 開発・運用コストの削減

実績あるプロトコルを部品として組み込み、自社での一からの構築を省ける

事例 Coinbase：貸付基盤を自社で作らず、Morphoを裏側に組み込み暗号資産担保ローンを提供

6 世界の流動性への接続

国や取引所の壁を越え、グローバルな投資家と流動性に直接つながる

事例 SMBC日興：国内投資家向けの規制対応プールをBase上に置き、世界の流動性に接続する構想（参考資料 事例⑤）

7 透明性と自動化

取引・担保・準備をリアルタイムに検証でき、清算や決済もコードで自動実行

事例 Aave Horizon：トークン化ファンドの基準価額をオラクルで反映し、担保評価と清算を自動化

前提

コントラクト・オラクル・AML・流動性急変のリスクを、許可型の入口、キュレーター、保険、セキュリティ管理（P.8〜11）で抑えることが活用の条件

多様化の効果は資産間の相関に左右され、市場の急変時には相関が高まりやすい

例は各社の公表資料・報道に基づく（2026年10月時点）。

市場厚生の観点から見たDeFiの意義

Japan Cryptoasset Business Association

市場の摩擦の増減を整理することで、DeFiの差し引きの効果と必要な対策を明らかにする

考え方 取引費用や情報の非対称性といった「摩擦」は、本来成り立つはずの取引を失わせ、社会全体が得られる利益（市場厚生）を目減りさせる（死荷重）。DeFiがどの摩擦を減らし、どんな摩擦を新たに生むかを、仕組みに即して整理する

減る摩擦 コードによる自動執行、誰でも参加できる仕組み、取引と決済の同時完了、公開台帳から

摩擦	伝統金融での姿	DeFiでの変化	市場厚生への効果
取引費用	多層の仲介と照合、決済はT+1～2	コードが執行し、取引と同時に決済	**費用を理由に見送られていた取引が成立する（死荷重の縮小）**
情報の非対称性	担保・準備資産は事後に開示	台帳上で誰でも常時検証できる	**情報の不透明さによる取引回避が減り、取引が増える（逆選択の緩和）**
決済・相手方リスク	決済までの時間差に信用リスク	取引と決済が同時に完了する	**必要な担保が減り、その分の資金を生産的に活用できる**
参入障壁	免許・システム・顧客基盤が必要	誰でも接続・組み合わせできる	**競争が働き、手数料・金利が利用者に有利になる（競争可能性の向上）**
市場の分断	取引所・国ごとに流動性と担保が分断	共通の台帳で流動性・担保を共有	**価格形成が改善し、遊休資金が減る（価格発見の改善）**

新たに生じる摩擦とリスク と対策

MEV（取引順序の操作） 取引費用
先回り取引等により、利用者の利益が第三者に移転する
→ インテント、バッチオークション、MEV tax（P.8・9）

流動性提供者の不利（LVR） 逆選択
価格の乖離を突く取引の相手方となり、流動性提供者に損失が生じやすい
→ 動的手数料などのフック（P.8・9）

清算の連鎖 外部性
担保価格の急落で清算が連鎖し、下落を増幅
→ オラクル設計、キュレーターによる上限設定

相互依存による連鎖 外部性
組み合わせた先へ事故が波及（例：2026年4月 Kelp DAO→Aave）
→ 担保の受入審査・上限、緊急停止による凍結

コード・鍵・オラクルのリスク 運用リスク
不具合や署名の侵害が即座に損失になる
→ 監査、署名前の判定、監視（P.10・11）

差し引きの効果 ＝ 減る摩擦 − 新たに生じる摩擦
摩擦が減る分だけ、市場とコードに任せられる範囲が広がる。ただし、当事者以外に及ぶ害（外部性：清算・相互依存の連鎖、マネロン等への悪用）と、利益の行き渡り方（分配）には、的を絞った設計とルールが必要（P.8～11）

効果を測りやすい
取引・価格・担保がすべて公開台帳に残るため、減った摩擦と新たな摩擦の大きさを誰でも測定・検証できる（伝統金融では非公開データが必要）

参考：Coase（取引費用）、Akerlof（1970、逆選択）、Baumol ほか（1982、競争可能市場）、Daian ほか（MEV）、Milionis ほか（LVR）、Aave rsETH Incident Report（2026年4月）。情報処理能力の差は伝統金融にもあり、DeFiでは形を変えて残る（NY連銀）。

AIの進化が伝統金融に突きつける課題

Japan Cryptoasset Business Association

金融のAI化はブロックチェーンとの親和性を高める一方、攻撃もAIにより高度化している

① 金融でのAI活用

人が判断 AIは分析を補助

AIが提案 人が確認して実行

AIが実行 AIが自律的に取引

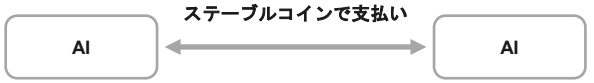
資産運用・融資の審査・顧客対応・不正の検知などで活用が進み、取引を行う主体が人からAI（AIエージェント）へ移り始めている

② AIとブロックチェーンの相性

	伝統金融	ブロックチェーン
稼働時間	営業時間内	**24時間365日**
接続方法	個別に契約	**誰でも接続できる**
本人の確認	人が書類を審査	**電子署名で確認**
記録の確認	後から照合	**その場で台帳を確認**

AIは、機械が直接読めて、その場で確かめられ、止まらない仕組みの上で最も力を発揮する

③ AIの支払いはステーブルコインで



AIは銀行口座を開設できず、本人確認の手続きも行えない。少額の支払いを大量に即時で行うため、銀行振込やカードよりステーブルコインが向く

AI向けの支払いの仕組み（CoinbaseのX402、GoogleのAP2）が登場し、9か月で約1.4億件（1件平均約0.31ドル）。ほぼすべてがドル建てのUSDC。ただし規模はまだ小さい

一方で、攻撃もAIで高度化する → AIによる防御と、情報を一か所に集めない管理で対抗する

AIを使った攻撃

約1.3か月で倍増

AIによるスマートコントラクト攻撃の想定被害額（Anthropicの検証）

400億ドル

米国でAIを悪用した詐欺の損失、2027年の予測（Deloitte）

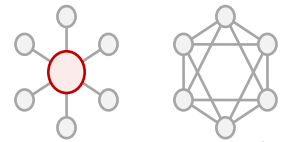
- ディープフェイク（偽の顔・声）による本人確認の回避
- プログラムの脆弱性をAIが発見し、短時間で悪用（Binanceでは約3分半で全額流出）
- 集中管理された鍵・データを標的とする（Binanceでは社内システムへの侵入を起点に約63億ドルが流出）

対

AIによる防御（P.11）

- 取引に署名する前に、AIが中身を確認して不審なものを止める（Blockaid、Hypernative）
- 攻撃の準備を見つけ、数秒でサービスを自動停止する
- 不正な資金の流れを追跡し、換金の出口で凍結する（Chainalysisなど）

情報を一か所に集めない管理（P.8・9）



- 資産を動かす鍵を分割し、複数で承認する
- 個人情報を渡さずに本人確認する（ゼロ知識証明）
- 資産を業者に預けず自己管理する

伝統金融にとっての課題 ① 決済の担い手がAI向けの新たな仕組みへ移行し得る ② 事前の本人確認と人の判断に依存する防御が機能しにくくなる ③ 集中管理された鍵とデータが主要な攻撃対象となる

出典：Anthropic（2025年12月、AIによるスマートコントラクト攻撃の検証）、Deloitte（AIを使った詐欺損失の予測）、Coinbase（x402）、Google（AP2）、BlockEden（エージェント決済の集計、2026年3月）、TRM Labs・Binance発表（2026年10月）

DeFiセキュリティの実装

Japan Cryptoasset Business Association

FATF報告書（2026年7月）は、透明性・自律性・改ざん耐性によるリスク低減の可能性を指摘

① ウォレット

MetaMask・Rabby等
関連特性：自律性

- 鍵を利用者が持つ非カストディ構造か
- 制裁対象アドレス等を警告するか、遮断するか
- **AML/CFT上の確認を、個人情報を渡さずに完結できるか**

実装：EIP-7702でEOAにスマートアカウントのコードを委任し、取引前チェックを追加。AML/CFTは属性の証明書からZK証明を生成し、プール／Vault側の検証コントラクトが証明のみ確認

インテント署名 → **取引 (Swap)**

預入 → **運用 (Lend)**

② インテント／ソルバー

UniswapX・CoW Protocol・1inch Fusion
関連特性：透明性

- ソルバーが利用者の資産を預からない設計か
- 執行結果を事後に検証できるか

実装：Permit2等でオフチェーン署名。UniswapXのReactor／CoWのSettlementコントラクトが決済し、条件不一致ならrevert。CoWはソルバーをallowlistで管理

③ キュレーター（Vault）

Morpho Vaults V2（Gauntlet等）
関連特性：透明性・改ざん耐性（市場とコード）

- 権限が配分・上限設定に限られるか
- 変更の前に利用者が退出できるか

実装：owner／curator／allocator／sentinelのロールを分離。リスクを高める変更はVaultごとのtimelock付き（低減は即時）、許可制は任意のGate

最良価格で約定 →

配分 →

④-a フック付きAMM

Uniswap v4（Permissioned Pools、Predicate等）
関連特性：改ざん耐性

- **AML/CFT要件をプール単位で適用できるか**
- フックの変更可否と監査

実装：PoolKeyでフックを指定（作成後は不変）。オフチェーン判定の署名をhookDataで渡し、beforeSwapで検証・不適合ならrevert

④-b レンディング

Morpho Blue・Aave
関連特性：改ざん耐性（Morpho Blue）・自律性

- 運営者の関与がどこまで残るか
- 隔離市場で損失を封じ込められるか

実装：Morpho Blueは貸出・担保資産、オラクル、LLTV、金利モデルを作成時に固定（非アップグレード）。Aaveは投票とタイムロックで更新可能

許可をかける層：参加者の限定はチェーンではなくアクセス層（プール・Vault・入口）で実装でき、AML/CFT上の統制と流動性・検証可能性は両立し得る

横断レイヤー：セキュリティ監視・自動防御（例：Hypernative、Blockaid） — **常時監視が事前の許認可をどこまで補完・代替できるかが論点**

署名前の判定：署名前に取引を検証し、方針違反を止める（両社）

運用ウォレットの保護：異常を検知したら、事前登録した退出取引を自動実行（両社）

プロトコルの自動停止：付与されたpause権限で、重大な異常時に自動停止（両社）

出典：Uniswap Foundation「Predicate Institutional Hook」、Morpho Docs、Uniswap Developers、Hypernative・Blockaid公式ブログ。FATF「DeFiに係る規制上の課題に関する報告書」（2026年7月、第43・52・53段落等の趣旨を要約）

各プロダクトのトラストポイントと利用者との接点

Japan Cryptoasset Business Association

例：MetaMaskから1inch・Uniswapで交換し、Gauntletがキュレートするmorpho Vaultに預け入れ

レイヤー｜プロダクト例	トラストポイント（何を信頼するか）	利用者との接点・個人情報	主な統制
ウォレット・画面 **MetaMask**	拡張機能の配信元（Consensys）、署名画面の表示内容	署名と取引内容の確認。既定のRPC（Infura）がIPアドレス等を取得し得る	Blockaidによる署名前の警告・取引シミュレーション（既定で有効、最終判断は利用者）
アグリゲーター **1inch（Fusion）**	見積・注文中継（オフチェーン）、リゾルバー（執行者）、Limit Order Protocol・Fusion決済拡張	注文への署名とトークンの承認。スクリーニング等のためアドレス・IPアドレス等を処理し得る	署名した条件（最低受取額等）をコントラクトで強制、リゾルバーの参加要件（事業者の本人確認等）、監査
インテント **UniswapX**	フィラー（執行者）の執行、決済コントラクト（Reactor）	注文への署名のみ。個人情報は不要	Dutchオークションで価格を競争、条件不一致ならrevert
DEXのコア **Uniswap v4**	PoolManager（変更不可）、プールごとのフック	直接の接点なし（画面経由）	コアは変更不可。フックはプールごとに固定（フック自体の変更可否は設計次第）
キュレーター **Gauntlet USDC Prime（Morpho）**	ownerが任命したキュレーターが市場と上限を選定、allocatorが上限内で配分（Gauntletは両方）	預入・引出（画面経由または直接）。個人情報は不要。制裁チェックは画面の運営者が実施	リスクを高める変更は7日のタイムロック（低減は即時）、配分は常時公開。流動性不足時も現物での退出が可能
レンディングのコア **Morpho Blue**	市場作成時に固定された条件と、選ばれたオラクルの設計・データ源	誰でも直接利用可能。多くは統合先・Vault経由（各自のアクセス制御）	停止・変更機能のない隔離市場、誰でも清算可能、不良債権は当該市場に限定、監査・形式検証
レンディングのコア **Aave v3**	ガバナンス（AAVE保有者）の判断、リスクパラメータの設定	直接の接点なし	ガバナンスのタイムロック、停止権限の範囲設計、監査
オラクル・ブリッジ **Chainlink／CCTP（USDCの移転）**	価格フィードのノード運営者、Circleによる移転の証明	接点なし（間接的に影響）	複数ノードによる集約、担保の上限設定

付随的な情報が生じ得る接点

1つの取引に、別々の主体のトラストポイントが連なる

取引所1社に資産・鍵・個人情報が集まる構造と異なり、信頼の対象が画面・執行・運用・データの各主体に分かれる。一者の侵害で全体が失われにくい一方、1つの弱点が全体に影響し得るため、各点の統制が必要

入出金（法定通貨との交換）とチェーンの層は含まない。出典：MetaMask・1inch・Uniswap・Morpho・Gauntlet・Aave・Chainlink・Circle（CCTP）の公式ドキュメント。構成は説明用の一例で、各プロダクトの設定・時点により異なる

DeFiセキュリティのフレームワーク

Japan Cryptoasset Business Association

34の管理策を3層で整理。単一業者の内部管理に依らず、構築・運用・常時監視の各段階で対策

構築フェーズ（作る）

インフラ層

チェーン／プロトコル自体は安全で信頼できるか？

プロトコルの安全性

- 24 コア実装の安全性・監査
- 25 アップグレード／ロールバックの安全性

鍵・ガバナンス

- 26 **権限キーの保管・管理**
- 27 ガバナンス操作の正当性・改ざん耐性
- 28 ガバナンス攻撃面・インセンティブ分析
- 29 ゲーム理論的な前提の検証

レジリエンス・運用

- 30 運用レジリエンス・災害復旧
- 31 オンチェーン可視化・SIEM連携
- 32 変更管理（レビュー・追跡・巻き戻し）

保証・SOC

- 33 継続的レッドチーム（CBEST/TIBER）
- 34 Web3 SOCの成熟度・IR連携

運用フェーズ（使う・守り続ける） 取引のライフサイクルに沿って3段階

赤：近年の大規模流出事案で特に問われた管理策

STEP 1 取引前

この取引を行うべきか？

- 4 取引相手アドレスの評判チェック
- 5 トークン／資産の正当性分析
- 6 送金先アドレスの詐欺分析
- 7 コントラクトの脆弱性・監査状況
- 8 流動性プールの健全性監視
- 9 ドレイナー・フィッシング検知

＋インフラ層から適用： 24 25 28

STEP 2 取引中

この取引は安全に実行できるか？

- 10 **事前シミュレーション**
- 11 取引の異常検知
- 12 社内ポリシーの自動適用
- 13 **マルチシグ承認の確認**
- 14 オラクル・外部データの安全性

＋インフラ層から適用： 26 27

STEP 3 取引後・継続監視

環境は今も安全か？

- 15 リアルタイム監視（異常・MEV）
- 16 財務リスク・エクスポージャー監視
- 17 ブリッジ／クロスチェーンの安全性
- 18 フロントエンド・供給網の侵害検知
- 19 **インシデントの自動封じ込め**
- 20 外部委託先（ベンダー）の監視
- 21 DeFiポジション・利回り戦略の監視
- 22 ステーキング・バリデータ監視
- 23 コンプライアンス・規制報告

＋インフラ層から適用： 30 31 32 34

基盤層（常時稼働）

▲ 全フェーズを下支えする組織能力

1. **資産インベントリ** — 何を・どこに保有しているか？
2. **脅威インテリジェンス** — どのような脅威が顕在化しているか？
3. **インシデント対応** — 問題発生時にどう動くか？

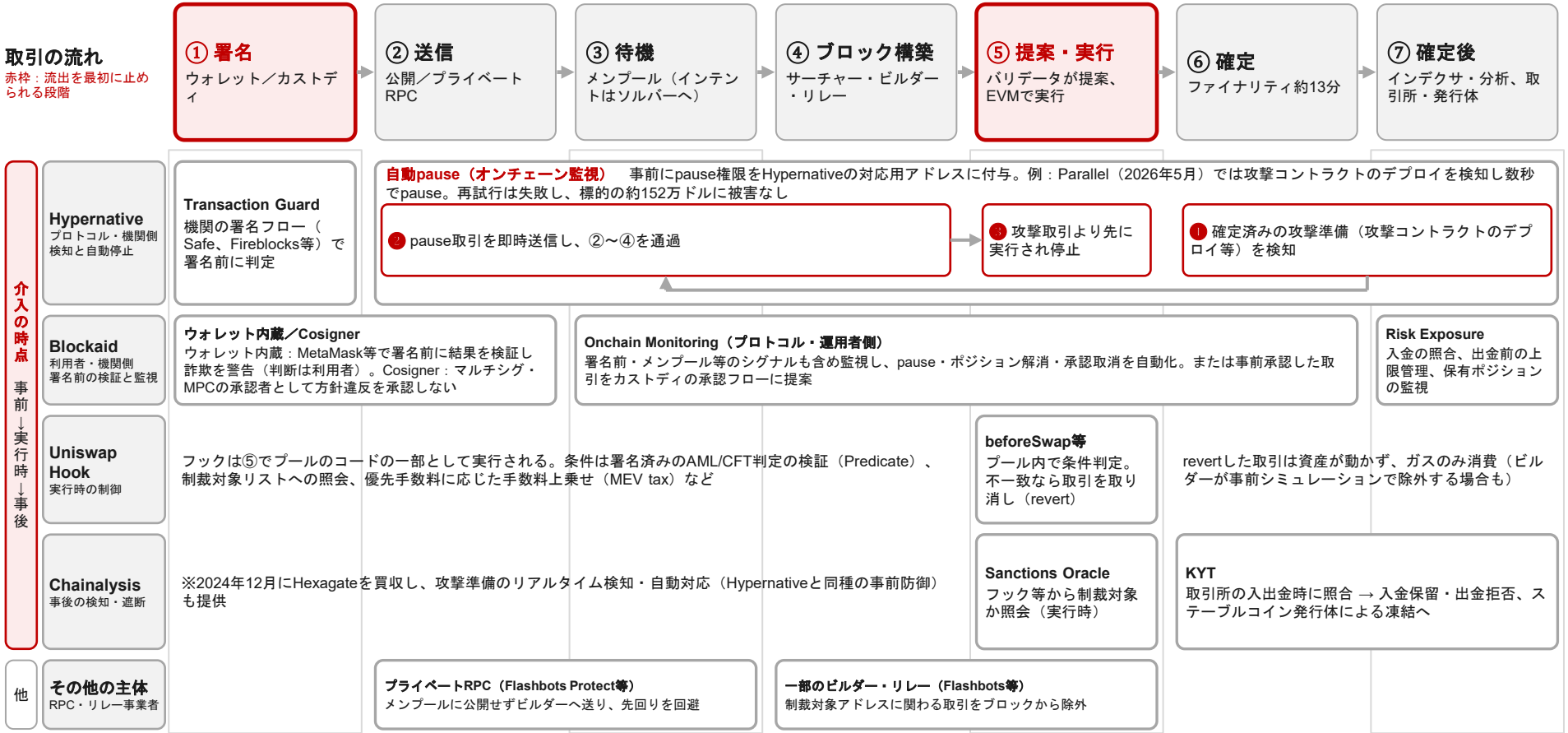
既存基準との対応： 基盤層・変更管理・SOC等はSOC 2・ISO 27001・NIST CSF、鍵の管理はCCSSと重なる。プロトコル・ガバナンス・オンチェーン監視はDeFi固有

出典：Hypernative「Web3 Security Controls Framework」を基に日本語で再構成。丸数字は原典の管理策番号（全34項目）。既存基準との対応は本資料の整理。

取引の流れとセキュリティの介入点

Japan Cryptoasset Business Association

単一の管理者に依らず、署名から確定後までの各段階で独立した主体が重層的に確認（Ethereumの場合）



事前（署名前・実行前） Hypernative、Blockaid、Hexagate
被害を防止・抑制し得る。 Hypernativeは主にプロトコル・機関側、Blockaidは利用者の警告から機関の署名・監視まで。署名経路外の取引には常時監視を併用

実行時（ブロック内） Uniswap Hook、Sanctions Oracle
コードにより確実に執行される。 条件はプール単位。フックの変更可否は設計次第で、不変なら変更には流動性の移行が必要

事後（確定後） Chainalysis KYT、発行体の凍結
オンチェーン上の移転自体は取り消せない。 資金の出口で停止し、追跡・回収・抑止につなげる

出典：Hypernative公式ブログ（Parallel事例）・製品ページ、Decrypt（Chainalysis 2022年3月・2024年12月）、Blockaid製品ページ（Cosigner・Onchain Monitoring・Risk Exposure）・事例（Scallop、Midas 2026年8月）、MetaMaskヘルプセンター（セキュリティアラート）、The Block（MetaMask×Blockaid、2024年2月）、Uniswap Foundation（Predicate）

まとめ：DeFiの活用と、それを支えるセキュリティ

Japan Cryptoasset Business Association

DeFiは既存金融の機能と市場厚生を高め得る。その仕組みに即したセキュリティは、AIの脅威への備えにもなる

① DeFiは既存金融にとって有用	② 仕組みに即したセキュリティが必要	③ 結果としてAI対策にもなる
金融機能の向上 24時間の即時決済、同一資産の担保・決済・運用への連続利用、実績あるプロトコルの部品化（P.3〜5）	**信頼の所在は層ごとに残る** ウォレット・ソルバー・キュレーター・フック・オラクル等、層ごとのトラストポイントを特定し統制する（P.8・9）	**AIで攻撃は高速・低コストに** ディープフェイクによる本人確認の回避、脆弱性の自動探索。流出は数分で完了する（P.7）
市場厚生の向上 取引費用と情報の非対称性を減らし、死荷重の縮小・逆選択の緩和につながり得る（P.6）	**取引の各段階で介入できる** 署名前の判定、実行時のフック、確定後の追跡・凍結。34の管理策を構築・運用・監視で整理（P.10・11）	**分散と透明性で被害を抑える** 鍵・データを一か所に集めず、台帳で常時検証できるため、一か所の侵害が全体に波及しにくい（P.7〜9）
活用は既に始まっている SG-FORGE・BlackRock・Apollo等がパブリックなDeFiに接続（別冊「参考資料」）	**事案で有効性と課題を確認** Bybit・Binanceとも署名前の検証が鍵。確定後の凍結ではBinanceで約30億ドルの実績	**AIでAIを迎え撃つ** 攻撃準備をAIで検知し、人の判断を待たずに自動停止。既存金融の防御にも応用できる（P.7・11）

結論 DeFiは既存金融を置き換えるものではなく、その機能と市場厚生を高め得る基盤。活用には、集中管理を前提とせず、DeFiの仕組みに即したセキュリティ対策が欠かせない。その対策は、AIの進化が既存金融に突きつける脅威への備えにもなる

各章の出典を参照。

用語集

Japan Cryptoasset Business Association

本資料に出てくる主な用語を、テーマ別に簡単に説明

基本

DeFi（分散型金融）
取引・貸借などをスマートコントラクト（ブロックチェーン上のプログラム）で自動実行する金融サービス

ステーブルコイン
法定通貨と価値が連動するよう設計されたトークン。額面償還を約するものは日本では「電子決済手段」として暗号資産と区別（USDC、JPYCなど）

トークン化
国債・ファンド・株式などの権利をブロックチェーン上のトークンとして発行すること

オラクル
価格など外部のデータをブロックチェーンに届ける仕組み。Chainlinkなど

カストディ
顧客の資産（署名鍵）を預かって管理する業務

AML/CFT
マネー・ローンダリング及びテロ資金供与対策

VASP
FATF基準上の暗号資産サービス提供者。顧客のために交換・移転・保管等を業として行う者で、AML/CFT規制の対象

ウォレット・署名

署名鍵・署名
資産を動かす権限そのもの。鍵で署名した取引だけが有効になる

EOA
署名鍵1つで動く通常のアドレス。鍵＝全権限で、独自の制御を組み込めない

スマートアカウント
コントラクトで作るウォレット。複数承認・上限・停止などのルールを組み込める（Safeなど）

EIP-7702
EOAの操作をコントラクトに委任し、スマートアカウント化するEthereumの仕様

MPC・マルチシグ
鍵を分割して共同で署名する方式／複数の鍵の承認を必要とする方式

パーミッションレス／許可型
誰でも検証に参加できるチェーン／参加者が限定されたチェーン。前者の上でも許可型プール等を設定可能

delegatecall
外部のコードを自分の権限で実行させる命令。ウォレットの中身を差し替えられる

取引の仕組み

インテント
「何をしたいか」だけを署名で示す注文。実際の執行方法はソルバーが決める

ソルバー（フィラー）
インテントを最良の条件で約定させるため競争する執行事業者

AMM
数式で価格を決め、プールの資金と自動で交換する取引所の方式（Uniswapなど）

フック（Hook）
Uniswap v4のプールに付け足す追加プログラム。取引の前後に条件判定などを行う

キュレーター／Vault
預かった資金の配分先と上限を決める運用役／その資金を入れる器（Morphoなど）

Perp
期限のない先物（無期限先物）

revert
条件を満たさない取引を取り消し、何も起きなかった状態に戻すこと

リスク・監視

メンプール
ブロックに取り込まれる前の取引が待機する場所

ビルダー・リレー
取引を並べてブロックを組み立てる事業者と、それをバリデータに渡す仲介

ファイナリティ
取引が覆らない状態として確定すること（Ethereumでは2エポック＝64スロット×12秒で最短約12.8分）

MEV
取引の順序を操作して得る利益。先回り取引等により利用者の利益が移転する

LVR
価格の乖離を突く取引の相手方となることで、流動性提供者が被る損失

pause・Guardian
異常時にプロトコルを一時停止する機能／その権限を持つ役割

KYT
取引（資金の流れ）を監視して不正な資金を見つける仕組み。Chainalysisなど

用語の説明は本資料の文脈に合わせた簡略なもの。

参考資料
伝統金融によるDeFi活用事例

本編「DeFiの活用と、それを支えるセキュリティ」の別冊（2026年10月31日時点）

活用事例（金融機関・上場企業5社）

① Société Générale-FORGE
② BlackRock
③ Apollo
④ SharpLink
⑤ SMBC日興証券 DeFi Gateway

各事例の「本資料のメッセージとの対応」に記載のページ番号は、本編のページを指す

事例①：Société Générale-FORGE｜銀行がDeFiへ直接供給

Japan Cryptoasset Business Association

自社発行のステーブルコインをパブリックなUniswap・Morphoに投入し、流通と融資を拡大

仕組み

伝統金融

Société Générale-FORGE 発行体（銀行グループ）
MiCA準拠のEURCV・USDCVを1対1の裏付けで発行。流通拡大・24時間利用・融資事業の拡大を狙う

↓ 発行・償還は許可された取引相手に限定

許可型の入口（アクセス層）

発行・償還の入口／Flowdesk アクセス層・マーケットメイク
保有・償還は「許可された譲受人」に限定。Flowdeskが初日からUniswapで流動性を提供

↓ 誰でも使えるDeFiの市場へ

パブリックチェーン上のDeFi

Uniswap 交換市場
EURCV・USDCVのスポット市場をEthereum上のAMMで提供（2025年9月～）

↓ 貸借市場で運用・調達

Morpho Vault（キュレーター：MEV Capital） 貸借市場
wBTC・wstETH・トークン化MMF（Spiko）を担保にEURCV・USDCVを貸借。担保の選定・配分・デフォルト対応はキュレーターが担う

本資料のメッセージとの対応

P.4・5　動機：使われなければ広がらない
EURCV約5,600万ユーロに対しCircleのEURCは2.2億ユーロ超。同社は「流動性・流通の拡大」を優先事項に掲げる

P.8　許可をかける層
発行・償還の入口のみ限定し、交換・貸借は誰でも使えるUniswap・Morphoを利用

P.9　トラストポイントの移転
銀行が担っていた与信判断の一部を、キュレーター（MEV Capital）とコード上のパラメータが担う

規制　規制上の整理
社内コンプライアンスは保有者を把握できない点に慎重だったが、MiCAが常時の保有者特定を求めない整理が後押しに

論点・留意点

- 二次流通で保有者を特定しない運用と、AML/CFT上の確認（発行・償還時のみで足りるか）のバランス
- 流動性と与信の質が特定のマーケットメイカー・キュレーターに依存する点／規模はまだ小さく、普及は途上

出典：SG-FORGEプレスリリース（2025年9月30日）、Morpho事例紹介、DL News（2025年9月30日）、Blockstories（Stenger CEO発言・流通量）、CoinDesk（2025年10月14日）

事例②：BlackRock｜トークン化ファンド「BUIDL」のDeFi接続

Japan Cryptoasset Business Association

伝統的なファンドをトークン化し、許可型の入口を通じてDeFiの流動性・決済に接続

仕組み

伝統金融

BlackRock 運用者
米国債等で運用するトークン化ファンドBUIDLを組成（運用資産 約24億ドル、2026年2月時点）。BNB Chain・Solana等にも展開

↓ ファンド持分をトークンとして発行

許可型の入口（アクセス層）

Securitize トークン化・コンプライアンス
発行・名義管理と、適格投資家の審査・ホワイトリスト管理。米国の登録ブローカー・ディーラー／ATSを運営

↓ 審査済みの投資家のみ取引可能

パブリックチェーン上のDeFi

UniswapX（RFQ方式） 取引・決済
Securitize Markets経由で見積もりを取得し、スマートコントラクトでオンチェーン決済（2026年2月～）。BlackRockはUNIも取得

↓ 保有したBUIDLを他の用途に再利用

担保・裏付け資産としての利用 資本効率
ラップ版BUIDLをEuler等のDeFiで利用。取引所での担保、ステーブルコイン（Ethena USDtb）の裏付け資産にも

本資料のメッセージとの対応

P.8 **許可をかける層**
参加者の限定はSecuritizeのホワイトリスト（アクセス層）で行い、決済・流動性はパブリックチェーン上のUniswapを利用

P.4・5 **24時間の流動性と資本効率**
週末・夜間も取引・決済でき、同じ資産を担保や裏付け資産として連続して活用

P.6 **市場の分断の解消**
自社専用の基盤を作らず、既存のDEXの流動性・決済に接続

P.9 **役割の分担**
運用（BlackRock）・審査と名義管理（Securitize）・執行（Uniswap）の役割が分かれ、一者に集中しない

論点・留意点

- RFQ方式で取引相手は審査済みの投資家に限られ、誰でも参加できるAMMプールではない（許可型と許可不要型の組み合わせ方）
- 移転制限のあるトークンを、組み合わせ可能なDeFiでどこまで再利用できるか／大手運用会社がガバナンストークンを保有することの意味

出典：The Block、CoinDesk（2026年2月11日）、Securitize。運用資産額はThe Blockのデータ。取引所担保・USDtbの裏付けは各社の公表に基づく

事例③：Apollo｜プライベートクレジットをDeFiで運用

Japan Cryptoasset Business Association

トークン化ファンドとキュレーターによる自動運用を組み合わせ、利回り戦略をオンチェーンで提供

仕組み

伝統金融

Apollo 運用者
分散型クレジットファンド（ACRED、約10億ドル）を提供

↓ ファンド持分をトークンとして発行

許可型の入口（アクセス層）

Securitize トークン化・コンプライアンス
ACREDをトークン化し、DeFiで使うためのsACREDを発行。適格投資家の要件を維持したままDeFiに接続

↓ Vaultに預け入れ

パブリックチェーン上のDeFi

Morpho（Compound Blue） 貸借市場・Vault
sACREDを担保にUSDCを借り入れ、ACREDを買い増すループで利回りを上乗せ（Polygon、2025年4月～）

↓ リスクを常時監視

Gauntlet リスク管理
レバレッジ比率を監視し、市場急変時にはポジションを自動で縮小

本資料のメッセージとの対応

P.4・5 **新たな運用・収益機会**
伝統的なファンドに、DeFiの貸借市場を使った利回り戦略を上乗せ

P.8 **キュレーターと権限分離**
運用判断・リスク管理を外部の専門主体が担い、権限はコントラクト上で分離・開示

P.11 **自動化による防御**
急変時のポジション縮小を人の判断を待たず自動で実行

動向 **プロトコルへの関与**
2026年2月、ApolloはMorpho協会と協力合意。4年間で最大9,000万MORPHOを取得でき、Morpho上の貸借市場を支援

論点・留意点

- ループによるレバレッジと清算リスク／流動性の低いプライベートクレジットを担保とする際の評価・清算の方法
- 運用会社がプロトコルのガバナンストークンを保有することによる利益相反と、その開示

出典：CoinDesk・Securitize（2025年4月30日）、Morpho Association（2026年2月13日）、Gauntlet

事例④：SharpLink｜上場企業（DAT）が財務資産をDeFiで運用

Japan Cryptoasset Business Association

適格カストディアンに資産を置いたまま、保有ETHをパブリックなDeFiで運用

仕組み

上場企業

SharpLink（Nasdaq上場） DAT（暗号資産を財務資産として保有）
約88万ETH超を保有。株主・監査人・開示義務を負ったまま、保有ETHの一部をオンチェーンで運用

↓ 資産は適格カストディアンが保管

許可型の入口（アクセス層）

Anchorage Digital Bank 適格カストディアン
運用の全過程で資産を保管。Lidoでステーキングし受け取ったwstETHも同行で保管

↓ 2億ドル分のETHをリステーキング（2026年10月）

パブリックチェーン上のDeFi

ether.fi／EigenLayer リステーキング
ETHをリステーキングし、流動性トークンweETHを発行

↓ LayerZeroでL2へ移転

Linea（Consensys） L2上での運用
weETHをLinea上のDeFiで運用し、追加の利回りを得る。別途、Galaxyと1.25億ドルのオンチェーン運用ファンドで覚書（2026年5月）

本資料のメッセージとの対応

P.4・5 新たな運用・収益機会
ステーキングだけで約1.88万ETHの報酬（2025年6月以降）。財務資産を「持つだけ」から「運用する」へ

P.9 保管と運用の分離
保管は適格カストディアン、運用はオンチェーン。上場企業の受託者責任・監査とDeFiの利用を両立させる構成

P.9 トラストポイントの連鎖
ether.fi・EigenLayer・LayerZero・Lineaと、信頼の対象が複数の主体に分かれて連なる

P.6 相互依存による外部性
リステーキングとブリッジを経由するため、2026年4月のKelp DAO事案（ブリッジ侵害→Aave）と同種のリスクを負う

論点・留意点

- 株主への開示：どのプロトコル・チェーンに、どれだけ・どのリスクで運用しているか／会計・監査上の評価
- ブリッジ・スラッシング・流動性のリスク管理。参考：XRPのDAT「Evernorth」（2026年10月上場）もXRP Ledger上のDeFi活用を計画（現時点は計画段階）

出典：Crypto Economy・The Crypto Times（2026年10月22～23日）、CoinDesk（2026年5月12日）、Cointelegraph、Evernorthプレスリリース（2026年1月21日）、Coinpaper（2026年10月15日）。保有量は報道ベース

事例⑤：SMBC日興証券｜規制対応型DeFi基盤「DeFi Gateway」

Japan Cryptoasset Business Association

パーミッションレスな基盤上に、フックで規制対応の仕組みを組み込む国内の取り組み

仕組み

伝統金融

SMBC日興証券 共同リード
規制当局との対話を主導し、コンプライアンス・リスクモデル・運用の知見を提供。2026年2月にDeFiテクノロジー部を新設

↓ 規制要件を技術で実装

技術開発

Nethermind 共同リード
技術設計・開発、AI統合、スマートコントラクトのセキュリティ。Nyx Foundationがフックとマーケットメイク設計を助言

↓ フックとしてプールに組み込み

許可型の入口（アクセス層）

規制対応型流動性プール Uniswap v4フック
フックでAML/CFT（取引相手アドレスの事前確認、随時更新のブラックリスト）と投資家保護を実装。相場急変時の手数料調整も

↓ Base上で世界の取引相手と接続

パブリックチェーン上のDeFi

Base上のUniswap・AIエージェント型Vault 基盤・利用者接点
プールは同社のシステム外のBase上に置く。AIが投資判断を支援・代行し、判断過程を検証・再現可能に。開発完了は2027年半ばが目途

本資料のメッセージとの対応

P.8 **許可をかける層**
「パーミッションレスな環境に信頼できるレイヤーを挿入」。基盤は開いたまま、統制はプール単位のフックで

規制 **集中管理に依らない守り方**
従来型の本人確認と集中的なデータ管理をそのまま適用しない方針。当局とルールを定め、技術で実装

P.6 **市場の分断の回避**
国内の遊休資金をグローバルな流動性に接続。LP損失（LVR）を抑えるフック設計も

P.7 **AIとの接続**
AIエージェント型Vaultと、Baseの少額決済プロトコルx402の統合を検討

論点・留意点

- 法的な位置づけ：既存規制で対応できる部分・届かない部分・規制不要な部分の切り分け（金融庁研究会でDeFi・DEXが検討候補に、2026年10月）
- フックによるAML/CFTの実効性と、利用者にとっての説明責任・投資家保護の担い手をどう定めるか

出典：CoinPost（2026年10月2日）、NADA NEWS（2026年10月29日、SMBC日興 磯野氏・Nyx Foundation 太田氏インタビュー）

本資料に関するご留意事項

本資料は、「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」における議論の参考に供することのみを目的として当団体が作成したものであり、投資勧誘や特定のプロジェクト・プロトコル・サービスの推奨を行うものではありません。
記載されている情報・事例の正確性や完全性について保証するものではなく、本資料の情報に基づいて行われた判断や行為により生じた損害について、当団体は一切の責任を負いかねます。