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

令和４年６月

株式会社クニエ

当研究の背景、目的

ブロックチェーン技術に基づく分散型金融システムでは、仲介者や中央集権化されたプロセスの必要性を低減もしくは排除した P2P（Peer to Peer/Pool）の金融取引が可能となる。主にパブリック型のブロックチェーン上でスマートコントラクトを活用して構築される金融サービスは「DeFi (Decentralized Finance, 分散型金融)」と称され、DeFi で取り扱う TVL (Total Value Locked, 代表的な DeFi サービスに預けられた暗号資産の総額) が一時 1,000 億ドルを超える[1]など、現在、暗号資産市場は急速に成長している。一方で DeFi ではスマートコントラクトの脆弱性や秘密鍵の窃取などによる資金盗難が継続的に発生しており、2022 年 3 月時点の最高被害額が 6 億ドルを超える（本文 2-6-6 参照）など事件発生時の損害額が大きい。また、AML/CFT や利用者保護、金融システムの安定等の観点から懸念も指摘されている。

そこで、本研究調査においては、金融庁の「ブロックチェーン国際共同研究」の一環として、DeFi を含む分散型金融システムのトラストチェーン（本文 1-1-4 参照）における技術リスク等に関する研究を行うこととする。分散型金融システムは既存の金融システムと比べて分散かつ自律したシステムやガバナンスが強みとされるが、トラストポイント（本文 1-1-4 参照）が複数存在すると考えられる DeFi も多く、また DeFi を構成する構成要素のうち Weakest Link（本文 1-1-5 参照）を突かれたと考えらえるインシデント事例も存在する。また DeFi の運営は DAO（Decentralized Autonomous Organization, 分散型自律組織）と呼ばれる組織が運営するのが主流になっているが、DAO という名称にもかかわらず特定の権限者が運営している、ごく少数の大口ガバナンストークン保有者で意思決定が行われているなど、自律的な運営が行われていないと考えられるケースも見受けられる。そこで、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）の事例分析や過去のインシデント事例の分析、DeFi 関係者へのヒアリング等を通じて、分散型金融システムに関するリスクの特定を試みた。

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、規制対象ともなりうる（例：銀行）。他方で、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だと考えられる[2]。分散型金融システムがもたらしうるイノベーションの果実を社会全体が享受できるよう、分散型金融システムの健全な発展を見据え、当該システムのリスクを特定・評価した上でリスク低減策を検討することは重要であり、その方向性を検討するために本調査を実施するものである。

[1] DeFi pulse TVL(USD) 2021/11/9 9:00AM $110.26B https://www.defipulse.com/

[2] 尤も、ブロックチェーンの透明性や自律性、改ざん耐性といった特性を生かして、伝統的金融システムとは異なる形でリスク低減が実現される可能性もあり、従来の金融規制のアプローチが分散型金融においても最適解であるとは限らない。本調査は、客観的な分析に基づき、分散型金融の課題解決に向けて規制当局と開発者、ビジネス関係者等が協働するための視座を提供することに主眼を置いている。

謝辞

本報告書作成にあたっては、京都大学・岩下直行教授、早稲田大学・佐古和恵教授、慶応義塾大学・鈴木茂哉特任教授、米ジョージタウン大学・松尾真一郎研究教授から有益な助言やコメントを得た。また、デジタル庁・日本銀行のオブザーバー及び金融庁のご担当者からも有益な示唆・助言をいただいた。

もっとも、本報告書に関する内容の誤りは、すべて受託者である株式会社クニエに帰する。

免責事項

本報告書の内容は金融庁の公式見解を示すものではない。

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

目次

用語集

用語	定義
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism マネー・ローンダリング及びテロ資金供与対策
BIS	Bank for International Settlements 国際決済銀行
DAO	Decentralized Autonomous Organization 分散型自律組織
DeFi	Decentralized Finance 分散型金融
ERC	Ethereum Request for Comments イーサリアム技術提案
EVM	Ethereum Virtual Machine Ethereum 仮想マシン：Ethereum クライアント（ノード）を実行する仮想マシン[3]
FATF	Financial Action Task Force 金融活動作業部会
FSB	Financial Stability Board 金融安定理事会
FISC	The Center for Financial Industry Information Systems 金融情報システムセンター
IEC	International Electrotechnical Commission 国際電気標準会議
IPA	Information-technology Promotion Agency, Japan 独立行政法人 情報処理推進機構
IOSCO	International Organization of Securities Commissions 証券監督者国際機構
ISO	International Organization for Standardization 国際標準化機構
KYC	Know Your Customer 顧客確認のプログラム
TVL	Total Value Locked DeFi に預けられた暗号資産の総額

[3] Ethereum.org VIRTUAL MACHINE (EVM) https://ethereum.org/en/developers/docs/evm/

第 1 章 分散型金融システムのトラストチェーンについての全体像の把握

本章では、分散型金融システムの全体像を把握する目的で、分散型金融システムのトラストチェーン（1-1-4 参照）についての全体像を整理する。具体的には、分散型金融システムを構成する主要な構成要素を特定し、その構成要素をレイヤーに分けて全体のマッピングを行うことで、トラストチェーンの全体像がわかる形に整理する。

本章は次のように構成される。1-1 では、分散型金融システム、DeFi、DAO やトラストチェーンなど主な用語について定義し、1-2 では、それを構成する主要な構成要素について説明する。1-3 では、主要な構成要素をレイヤーに分けてマッピングし、トラストチェーンの全体像を明らかにする。1-4 では、レイヤー別に構成要素の技術特性を具体的な事例で説明する。1-5 ではレイヤー間やレイヤー内の構成要素に跨る Interoperability（相互運用性）の分析結果について説明する。

1-1　分散型金融システムに関する主な定義

1-1-1　分散型金融システム（Decentralized Financial System）

2019 年の FSB の報告[4]では、分散型金融システムを「分散型金融テクノロジーがもたらす可能性のあるシステム」と定義している。さらに、分散型金融テクノロジーを「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」と定義している。当報告書においても上記の定義を用いる。

なお、分散型金融システムは、既存の金融システムなどに見られる中央集権型（centralized)に対して非中央集権型(decentralized)のシステムの構築を目指しているとされる。一方、分散型システムの記述においては、分散型(distributed)とは計算機を分散配置することを意味しており、中央集権型のシステムも分散型システムの一形態と整理される。分散型金融システムに焦点を当てる本報告書においては、「分散」は非中央化の意味を含んでいるとして用いることとする。

1-1-2　DeFi（Decentralized Finance）

いわゆる DeFi については、様々な文献や記事などで論じられているが明確な定義はされていない。当報告書では参考文献[5]に従い「分散型金融システムの一部を構築する金融アプリケーション」と定義する。DeFi は、当初は資金調達のための独自トークン発行や、トークンの交換に従来型の取引所の仲介を必要としない DEX（Decentralized Exchange：分散型取引所）が主であったが、DeFi エコシステムの拡大に伴い、レンディングやデリバティブ、保険などの様々な取り組みが行われている。また、複数の DeFi の取引を 1 つの場所にまとめてサービスを提供するアグリゲーターなども存在する。

1-1-3　DAO（Decentralized Autonomous Organization）

DeFi を運営する分散型自律組織（DAO）について、定まった定義は存在していないが、2017 年の Chohan[6]や Ethereum.org[7]などで定義が試みられており、いずれの定義においても非中央集権的に組織の運営を行う点に主眼が置かれている。一般的に、DAO は伝統的な企業（例：株式会社）と比べて以下の特徴があるとされる。

---

[4] Financial Stability Board: Decentralised financial technologies: report on financial stability, regulatory and governance implications (2019). https://www.fsb.org/wpcontent/uploads/P060619.pdf

[5] Ryosuke Ushida and James Angel: Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs (2021). https://link.springer.com/chapter/10.1007/978-3-662-63958-0_2

[6] Chohan による DAO の定義：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）によって運営される組織　WChohan, U.W.: The decentralized autonomous organization and governance issues. J. Cyber Policy 1–7 (2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055

[7] Ethereum.org（Ethereum Foundation が運営するコミュニティ）による DAO の定義：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、インターネットの見知らぬ人と協力する安全な方法、特定の目的に資金を委ねるのに安全な場所 https://ethereum.org/ja/dao/

【主な DeFi プロジェクトにおける DAO の特徴】

・運営する会社や代表者・取締役会などが存在せず、参加者が自律的に運営を行う組織である
・組織の運営ルールがスマートコントラクトによってコード化されている
・ガバナンストークンなどと呼称されるトークンに紐づく形で一種の議決権（投票権）がトークン保有者に付与され、組織・コミュニティにおける一定の意思決定について、スマートコントラクトのルールに基づいて投票が行われる
・複数の国に所属する参加者がグローバルに活動する組織であり、また必ずしも管理法人が明確でないため、組織が所属する国や地域が特定されない

当報告書では、参考文献や MakerDAO の事例などを踏まえて、「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」と定義する。

DAO の初期の代表的事例として、2015 年 11 月にドイツ企業 Slock.it 社が立ち上げた投資ファンド組織「The DAO」が挙げられる。「The DAO」は営利目的で組成され、2016 年 6 月の資金流出事件により解散したが、それ以降に多数の DeFi プロジェクトでコミュニティの運営形態として導入されてきた。「The DAO」では、意思決定の権限が運営会社の Slock.it 社や指名されたキュレーターに集中していたが、現在では MakerDAO のように運営会社（Maker Foundation）を解散して分散度を高める動きも見られる。但し、DAO と称しているだけで実際には自律的な運営がなされていないケースも多い。

1-1-4　トラストポイント／トラストチェーン

トラストについて、金融庁の「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」中間論点整理においては、「相手の監視や制御が可能かどうかに関係なく、相手が自分にとって重要な行動をとってくれるという期待に基づいて、相手の行動に自身の「ヴァルネラビリティ」を託する意志」および「事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い」[8]と定義されている。

この定義に則った上で、当報告書では、トラストポイントを分散型金融システムにおける「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」と定義し、トラストチェーンは「依存関係の連なりの中にトラストポイントが含まれているもの」と定義する。

また、構成要素の関係を示すものに SPoF（Single Point of Failure）があり、その定義は「システムを構成する要素のうち、そこが停止するとシステム全体が停止してしまう部分」[9]である。トラストポイントと重なることも多い。

1-1-5　Weakest Link

Weakest Link とは、当報告書では、DeFi の構成要素及び構成要素間の接続部分のうち、セキュリティ上最も弱い部分を指す。攻撃者は Weakest link を狙うことで、攻撃が成功する可能性を最も高めようとする。

1-2　分散型金融システムの主要な構成要素

分散型金融システムは、ブロックチェーンやスマートコントラクトだけでなく、ユーザインターフェースやウォレット、開発者チーム、インフラプロバイダを含めて様々な構成要素から成り立ってい

[8] 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: 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 https://www.fsa.go.jp/news/r3/singi/20211117/seiri.pdf

[9] JPNIC SPOF とは https://www.nic.ad.jp/ja/mailmagazine/backnumber/2019/vol1667.html

る。分散型金融システムの主要な構成要素について、その技術特性を含めた各要素の概要と分散型金融システムにおける役割を説明する。

(1) 基盤ブロックチェーン

DeFi を構築する基盤として主に活用されているブロックチェーンとして以下のものがある。

a. メインチェーン（例：Ethereum）

DeFi プロトコルを実行するためのベースとなるブロックチェーンであり、サイドチェーンやレイヤー2 スケーリングソリューションの親チェーンになる。メインチェーンは一般的に以下の特徴がある（ここでは主に Ethereum を念頭に置いて記載する）。

- DeFi プロトコルをデプロイするための柔軟なスマートコントラクト機能を備える。
- ノード間で P2P（Peer to Peer）のネットワークを介してブロックなどのデータを共有する。クライアント（ノード）はスマートコントラクトを実行するために必要な仮想マシン（EVM）を搭載している。
- ブロックチェーンに保持される 2 種類のアカウントが存在する。
  - 外部所有アカウント（EOA：Externally Owned Account）は、秘密鍵で管理され、ネイティブトークンやトークンの送受信およびスマートコントラクトのデプロイ・実行ができる（いわゆるビットコインのアドレスに相当するもの）。
  - コントラクトアカウントは、デプロイされたスマートコントラクトのアカウントであり、外部所有アカウントや他のコントラクトアカウントからのメッセージの受信に応答して、スマートコントラクトが実行される。
- メインチェーンを構成するクライアント（Ethereum ノード）は、Ethereum Foundation 等から提供されている共通ソフトウェアである EThereum ノードソフトウェア、およびスマートコントラクトを実行するために必要な仮想マシン（EVM）を搭載している。
- メインチェーン上では多数の DeFi が稼働しており、利用者の増加によりトランザクション実行手数料（ガス代）の高騰やトランザクションが混雑してコードの実行（の前提となるブロックへの組み込み）に時間がかかるなどの問題が生じている。
- 最近は Avalanche や Solana などの新興チェーンも登場してきており、マーケット占有率にも一定の変化がみられる。
- メインチェーンのスケールアップを行う階層化チェーン[10]もあり、相互運用性およびスケーラビリティを有しているとされる。

b. サイドチェーン[11]（例：Polygon）

メインチェーンの処理速度向上等のスケールアップを行うため、メインチェーンと並列で動作するブロックチェーンであり、一般的に以下の特徴がある。

- メインチェーンのコンセンサスアルゴリズム（例：Ethereum は現時点において PoW：プルーフオブワークを採用）は電力消費が高く、また処理速度に限界があることが多い中、サイドチェーンは、メインチェーンと独立したコンセンサスアルゴリズム（PoA：プルーフオブオーソリティ、DPoS：委任されたプルーフオブステーク、BFT：ビザンチンフォールトトレランス等）を用いることで、電力消費を抑えて CO2 排出量を削減し、取引処理速度の向上やガス代を削減することを目指す。

---

10 階層化チェーン：Polkadot など、メインチェーンとそれに接続する個々のサブチェーンを含む独自のネットワーク構造のブロックチェーン。サブチェーンがスマートコントラクトを実行し、メインチェーンはメッセージ中継を行う。

11 Ethereum.org SIDECHAINS https://ethereum.org/en/developers/docs/scaling/sidechains/

・双方向ブリッジ[12]でメインチェーンに接続されている。メインチェーンとサイドチェーン間で資金をやりとりする場合、双方向ブリッジに資金をロックして二重支払いを防ぐ。
・サイドチェーンはメインチェーンと同様の仮想マシン（例：EVM）に基づいているものもあり、その場合はサイドチェーンでメインチェーン（Ethereum）と同じ開発言語やライブラリが機能する。
・サイドチェーンに保持されるアカウントは、一般には、メインチェーンと同じく外部所有アカウント、コントラクトアカウントの 2 種類である。

(2) レイヤー2 スケーリングソリューション

オフチェーンで Ethereum ブロックチェーンの処理速度向上等のスケールアップを行うソリューションとして、例えば以下の Rollup が存在。

※Rollup[13]：Ethereum メインチェーン(レイヤー1）の外部のオフチェーン（レイヤー2）でトランザクションを実行し、結果データのみをレイヤー1 に送信することで処理速度を向上する仕組み

a. Optimistic Rollup[14]

Optimistic Rollup は、トランザクションがデフォルトで有効であると想定し、書き込まれるデータの有効性の検証に必要な計算を行わないため、処理速度を向上させることができるとされる。また、Ethereum のセキュリティを継承している。
Ethereum メインチェーンへの書き込みが行われた時点では、書き込まれたデータの有効性の検証は行われない。その代わりに、Fraud-Proof（不正証明）により、チャレンジ期間（基本は 7 日間）に検証者が不正な状態遷移を検知すれば異議が申し立てられる。

b. zk-Rollup（ゼロ知識ロールアップ）[15]

zk-Rollup は、何百ものトランザクションを 1 つにまとめてオフチェーンで処理し、トランザクションデータの有効性の検証のために、暗号学的証明を生成する。すべてのトランザクションデータではなくゼロ知識の有効性の証明のみを Ethereum メインチェーンに送るため、含まれるデータが少なくなりブロックの検証がより迅速かつ安価になるとされる。
zk-Rollup はメインチェーンへ書き込みを行う時点でデータの有効性が検証されているため、Optimistic Rollup のようにレイヤー2 からレイヤー1 に資金を移動する際に不正証明のような遅延は発生しない。

(3) ネイティブトークン（ETH など）

基盤ブロックチェーン内で共通して利用される暗号資産などのトークンであり、トランザクションの実行手数料（ガス代）等として必要とされる。

(4) スマートコントラクト[16]

スマートコントラクトは、一般に、プログラムとして記述され、ブロックチェーン（分散台帳）上で自動的に実行処理されるルール（契約）を指す。Ethereum およびそれに準ずる「基盤ブロックチェーン」では、ブロックチェーンの特定のアドレスに存在するコード（機能）とデータ（状態）を指す。

---

[12] メインチェーンとサイドチェーン間でトークンを交換する機能 Ethereum.org Blockchain bridges https://ethereum.org/en/bridges/
[13] LAYER 2 ROLLUPS https://ethereum.org/ja/developers/docs/scaling/layer-2-rollups/
[14] Ethereum.org OPTIMISTIC ROLLUPS https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/
[15] Ethereum.org ZERO-KNOWLEDGE ROLLUPS https://ethereum.org/en/developers/docs/scaling/zk-rollups
[16] Ethereum.org INTRODUCTION TO SMART CONTRACTS https://ethereum.org/ja/developers/docs/smart-contracts/

Ethereum 等では、スマートコントラクトはコントラクトアカウントに保持され、メッセージを介して外部所有アカウントや他のスマートコントラクトから呼び出される。スマートコントラクトはブロックチェーンに書き込まれ、トランザクションの検証の過程でマイナーもしくはバリデータにより実行される。その実行ログと実行後の状態がブロックに記録されることで、誰もが真正なプログラムコードが実行されたことを確認でき、また状態を共有できる。

スマートコントラクトは通常は修正や削除ができず、実行結果は元に戻せないが、開発ツールによるサポート等を通して間接参照を用いれば、参照先を新たなコントラクトアドレスで置き換えることでスマートコントラクトをアップグレード可能とする余地も存在する。

また、スマートコントラクトはブロックチェーンにデプロイすることで実行可能になるが、DeFi におけるデプロイ作業は一般に管理者や権限者（スマートコントラクトのデプロイに必要な秘密鍵を保持している者）が保有する外部所有アカウントの秘密鍵が必要になる。

なお、本報告書では、DeFi の機能・サービスを実現するスマートコントラクトを「DeFi プロトコル」と呼称する。厳密にいうと、DeFi プロトコルは、ブロックチェーン上で稼働するスマートコントラクトと、そのスマートコントラクトを外部からユーザが操作するための DeFi プロトコルインターフェースがある。DeFi プロトコルインターフェースは、Web ブラウザに表示される DeFi プロトコルの操作画面や情報などを指す。

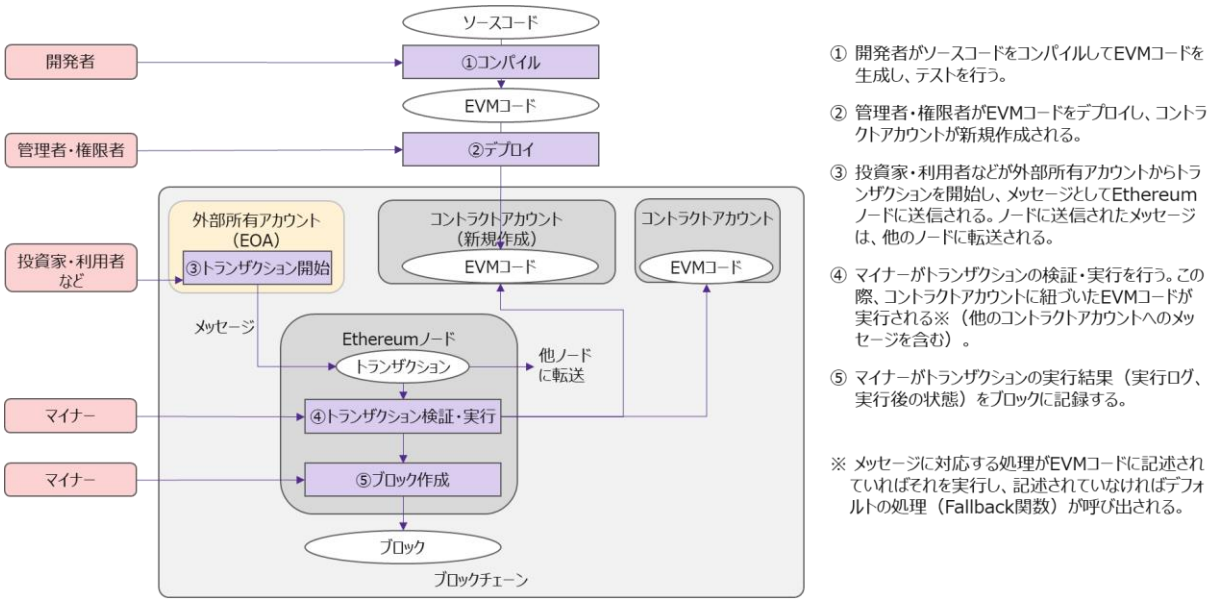

図 1-2　スマートコントラクトの実行の流れ（Ethereum の例）

(5) ウォレット

ウォレットは、ユーザの秘密鍵を管理し、かつユーザが秘密鍵を使ってトランザクションを実行するためのウォレットアドレスなどの情報の保持と、ユーザインターフェース（Web ブラウザやスマートフォンアプリの操作画面など）の提供を行う。DeFi の機能・サービスを利用する場合は通常、各 DeFi サービスに自身のウォレットを接続する。

【秘密鍵について】

ISO/IEC20008-1[17]では、公開鍵暗号による署名・検証にて署名に使う鍵は署名鍵（秘密鍵）、検証に使う鍵は検証鍵（公開鍵）と呼ぶ。当報告書ではそれぞれ秘密鍵、公開鍵と呼ぶ。IPA の説明[18]では、公開鍵暗号方式では対になっている 2 つの鍵（秘密鍵と公開鍵）を用

[17] ISO/IEC 20008-1:2013(en) Information technology — Security techniques — Anonymous digital signatures — Part 1: General https://www.iso.org/obp/ui#iso:std:iso-iec:20008:-1:ed-1:v1:en

[18] 2.2 公開鍵暗号方式　2.1 概要 https://www.ipa.go.jp/security/pki/022.html

いる。デジタル署名では、メッセージを秘密鍵を使って暗号処理を行い、それを対となる公開鍵を用いて検証することでメッセージの完全性と署名者の認証（1-2(6)参照）が可能になる。

a. コールド・ウォレット

コールド・ウォレットは、紙のペーパー・ウォレットや専用機器のハードウェア・ウォレットなどを用いてインターネットから完全に隔離された状態でユーザの秘密鍵を管理する。そのため、一般的には、ホット・ウォレットに比べ利便性は損なわれるが、ネットワーク経由の攻撃に耐性があるとされ、暗号資産交換所等において高額な暗号資産の保管などに利用されている。

b. ホット・ウォレット[19]

ホット・ウォレットは、ユーザの秘密鍵の保管場所により以下の２つに分類される。

- アンホステッド・ウォレット
  アンホステッド・ウォレットとは、一般にその保有者であるユーザが直接秘密鍵を管理するウォレットを指し、ユーザは暗号資産の移転取引等を直接実行できる。秘密鍵は通常、ユーザのローカル PC やスマートフォンなどに置かれて管理される。Ethereum ブロックチェーンと直接接続するため、web3.js 等の Ethereum ライブラリを利用する。
- ホステッド・ウォレット
  ホステッド・ウォレットでは、ユーザは秘密鍵の管理を暗号資産交換業者等のウォレット管理者（ホスト／カストディアン）に委託しており、ユーザは暗号資産の移転取引等を直接実行することが出来ない。

(6) ユーザインターフェース

IPA では、ユーザインターフェースは「ユーザが機器システムを利用するときに、ユーザと機器、システムが接する接面のこと」[20]と定義されている。DeFi では、DeFi サービスを利用する際の Web ブラウザやスマートフォンアプリのユーザ認証[21]画面やユーザ操作画面（GUI：Graphical User Interface）、運用オペレータが使用するコマンド（CLI：Command Line Interface）などを指す。

(7) インフラプロバイダ

インフラプロバイダはブロックチェーンノードのホスティングサービスで、DeFi 開発者やウォレットプロバイダなどが DeFi の機能・サービスを構築するにあたり、ブロックチェーンへのアクセスなど基盤となる部分の機能を API などで提供する主体である。代表的なものとして Infura（Consensys 社）や Quicknode（QuickNode 社）、alchemy（alchemy 社）など。

(8) DeFi システム開発ツール

DeFi システムの開発者が DeFi プロトコルのスマートコントラクトなどを開発/テストするための開発ツールであり、Ethereum では Truffle や Hardhat などがある。

---

[19] 金融庁 いわゆるステーブルコインに関する G20 財務大臣・中央銀行総裁への FATF 報告書要旨（仮訳）（2020/7）
https://www.fsa.go.jp/inter/etc/20200701.pdf

[20] IPA つながる世界の「利用時の品質」 https://www.ipa.go.jp/files/000057850.pdf

[21] ユーザ認証とは、システムまたはアプリケーションに対してユーザを識別するためのシステムである。このシステムを利用して、特定情報へのアクセス制御を行い、情報の保護を実現できる。以下のうち複数の要素を組み合わせてユーザを認証する「多要素認証」を用いるのが主流である。

- ユーザのみが知っているもの(パスワード)
- ユーザが所有するもの(鍵やカード、スマートフォン、電話など)
- ユーザの特徴を表すもの(指紋などのバイオメトリックス)

開発ツールの機能として、スマートコントラクトの開発／デバッグ、ソースコードのコンパイル、ローカルノードでのテスト、開発用ブロックチェーンへのデプロイなどがある。Infura などインフラプロバイダの機能を利用している開発ツールもある。

(9) コード監査会社

スマートコントラクトのコードについて、コード監査ツールによる静的検証（コード分析・形式検証など）、動的検証やコード監査者による机上検証などにより、設計上の問題、コードのエラー、セキュリティ上の脆弱性を検出するための分析サービスを提供する会社。

(10) クライアントソフトウェア[22]

DeFi の開発者や運営者が、スマートコントラクトのデプロイやメンテナンス、DeFi プロトコルの稼働監視などのオペレーションを行う場合に外部からクライアント（ノード）にアクセスするためのソフトウェアであり、ターミナルエミュレータや Web ブラウザ（インフラプロバイダを経由して利用する場合）などがある。

(11) オラクル[23]

スマートコントラクトがオフチェーンの外部データを取得するためのデータフィードであり、主に価格オラクルとして外部の市場価格や利率を取得するために使用されている。自己で複数の外部フィードを立てて外部の市場価格を取得する場合（Maker）や、Chainlink など外部の分散型オラクルサービスを利用する場合（Aave）などがある。

(12) ガバナンストークン・ガバナンス投票

ガバナンストークンの厳密な定義は存在しないが、一般には、コミュニティの意思決定に係る投票権（議決権）が付与されたトークンのことを指す。DeFi プロトコルの機能修正、追加や利率などのパラメータ変更、コミュニティ資金の使用などについて、ガバナンストークン保有者が保有量に応じて決められたルールに従って投票を行い、可決したものを実行する仕組みが「ガバナンス投票」と呼ばれることが多い。

(13) KYC 認証会社

Aave など機関投資家等に向けて DeFi サービスを提供している場合、外部の KYC 認証会社が機関投資家などの KYC 認証を行うことがある（一例として、KYC 認証会社が認証した機関投資家をホワイトリストに登録して DeFi に通知し、DeFi で KYC 済ユーザとして認識するなど）。

(14) アグリゲーター[24]

ブロックチェーン上に存在する様々な DeFi サービスを 1 つの場所（ウェブサイト等）に集約し、ユーザが取引に費やす時間を節約し、暗号資産取引の効率を高める目的で設置される。一般にアグリゲーターは、分散型取引所、レンディングサービス、流動性プールなどから最適なトークン交換条件や利回りを見出し、プラットフォーム上で提供する。

1-3　分散型金融システムを構成する主要な構成要素のマッピング

[22] Ethereum.org SPIN UP YOUR OWN ETHEREUM NODE https://ethereum.org/ja/developers/docs/nodes-and-clients/run-a-node/

[23] Ethereum.org ORACLES https://ethereum.org/ja/developers/docs/oracles/

[24] DeFi Aggregator https://coinmarketcap.com/alexandria/glossary/defi-aggregator

1-2 で概説した主要な構成要素を中心に、DeFi のトラストチェーンにおける依存関係を基に全体のマッピングを行った。

なお、当報告書では、基盤ブロックチェーンとして Ethereum を念頭に置いた分析を行い、その他のメインチェーンやサイドチェーンとの関係性はその都度明記することとする。また、トラストチェーンの依存関係を明確にするために各層に分けてマッピングを行うが、構成要素のトラストやセキュリティの関係は実際には層全体に跨る場合があり、各層に分けることで対象が特定の層に限定される訳ではないことを申し添える。

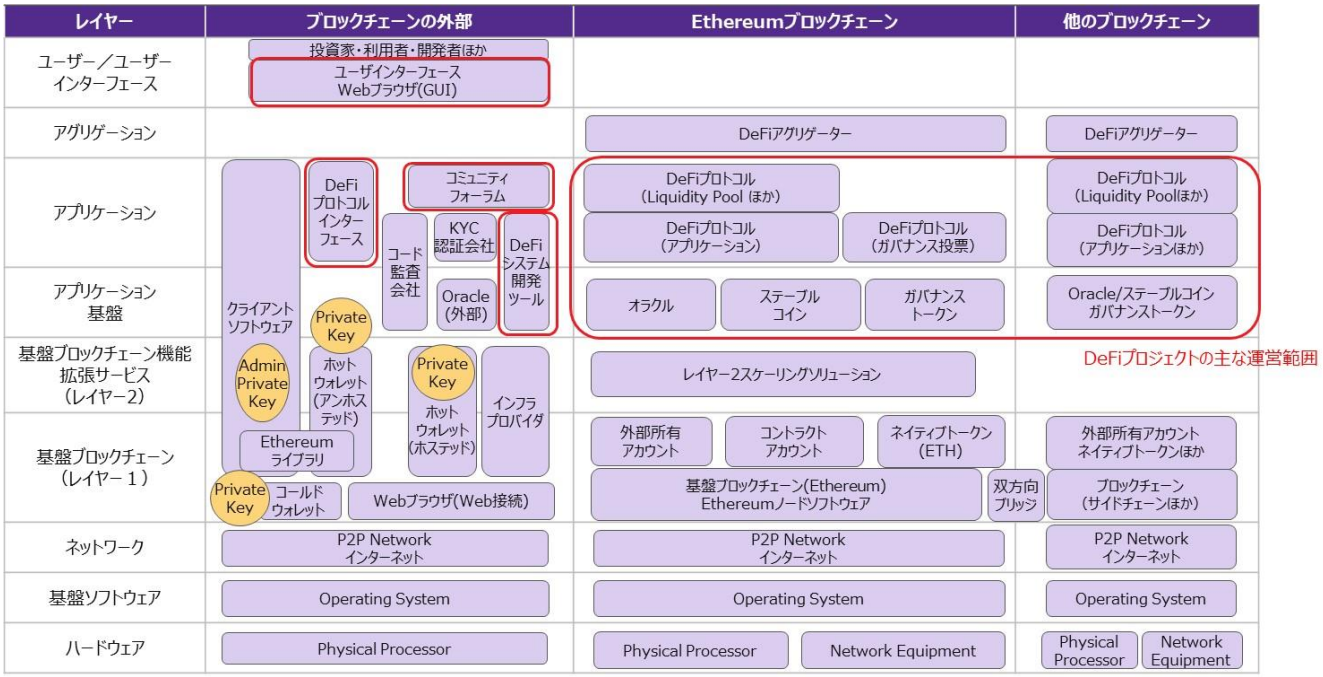

図 1-3　分散型金融システムの主な構成要素のマッピング

1-3-1　レイヤー分けの考え方

主要な構成要素を配置するレイヤー分けについて、構成要素間の依存関係をレイヤー間で上下に配置する目的で、以下の考え方で分類する。

(1) ハードウェア／基盤ソフトウェア層

ブロックチェーンの基盤となるハードウェア及びオペレーティングシステム、インターネット、P2P Network を配置する。

(2) 基盤ブロックチェーン（レイヤー1）層

基盤ブロックチェーンであるメインチェーン（Ethereum）およびサイドチェーン、階層化チェーンを配置する。外部所有（ユーザ）アカウントやコントラクトアカウント、ネイティブトークンもブロックチェーン機能の一部であるため、このレイヤーに配置する。

サイドチェーンは、メインチェーンの Ethereum と双方向ブリッジで接続して Ethereum と独立で稼働するため、Ethereum ブロックチェーンと並列で配置する。

ブロックチェーンの外部は、基盤ブロックチェーンと連携するインフラプロバイダや、外部所有アカウント・コントラクトアカウントと連携するコールド・ウォレットやホット・ウォレット、クライアントソフトウェアを配置する。

(3) 基盤ブロックチェーン機能拡張サービス（レイヤー2）層

基盤ブロックチェーン機能拡張サービス層には、基盤ブロックチェーンに依存して動くレイヤー2 スケーリングソリューションを配置する。

また、インフラプロバイダやアンホステッド・ウォレット、ウォレット管理者、クライアントソフトウェアはレイヤー１・２の双方に関係するため、両レイヤーに跨る形で配置する。

(4) アプリケーション基盤層

アプリケーション基盤層には、DeFi プロトコル（スマートコントラクト）などのアプリケーション層にとって通常必要とされるオラクル、ステーブルコイン、ガバナンストークンを配置する。

ブロックチェーンの外部では、オラクルと連携する外部オラクル、アプリケーション基盤を開発する DeFi システム開発ツール等を配置する。

(5) アプリケーション層

アプリケーション層には、DeFi プロトコル（スマートコントラクト）のアプリケーション（DeFi の各種機能・サービスなど）を配置する。

ブロックチェーンの外部は、DeFi プロトコルと連携する DeFi プロトコルインターフェースやコミュニティフォーラム、クライアントソフトウェア、DeFi システム開発ツール等を配置する。

(6) アグリゲーション層

アグリゲーション層には、複数の DeFi プロジェクトを集約する DeFi アグリゲーターを配置する。（マッピングは DeFi プロジェクトの依存関係を示すため、DeFi アグリゲーターのブロックチェーン外部の構成要素は記載を省略する）

(7) ユーザ／ユーザインターフェース層

ユーザ／ユーザインターフェース層には、ユーザと他の構成要素を繋ぐユーザインターフェースを配置する。

1-4　レイヤー毎の構成要素の技術特性の分析

1-4-1　基盤ブロックチェーン

以下の基盤ブロックチェーンについて、概要と主な技術特性を記述する。

(1) 基盤ブロックチェーンの概要・技術特性

表 1-4-1　基盤ブロックチェーンの技術特性

ブロックチェーン （ネイティブトークン）	Ethereum (ETH)	Polygon （MATIC）	Avalanche (AVAX)	BNB Smart Chain （BNB）	Polkadot （DOT）
分類	メインチェーン	サイドチェーン	メインチェーン	メインチェーン	メインチェーン （階層化チェーン）
概要	・多数の DeFi やスマートコントラクトが構築されている ・スケーラビリティなどの課題解決のため、Eth 2.0 への移行を段階実施中	・Ethereum のサイドチェーンで、EVM の互換性あり[25] ・スケーリング技術により処理速度が高速、かつ安価な送金手数料	・スケーリング技術で安価な送金手数料 ・Ethereum と EVM の互換性あり	・スケーリング技術で安価な送金手数料 ・Ethereum と EVM の互換性あり ・固定の 21 バリデータによるコンセンサスアルゴリズムで高速処理を実現	・メインチェーン（リレーチェーン）とパラチェーン（スケールアップを行う個々のブロックチェーン）を接続することで、相互運用性の高い基盤の構築を目指す
サービス開始	2015 年	2017 年	2020 年	2019 年	2017 年
創設者	Vitalik Buterin	Jaynti Kanani (CEO) Sandep Nailwal, Anurag Arjun	Emin Sirer (Professor at Cornwell)	Changpeng Zhao (CEO of Binance Exchange)	Dr. Gavin Wood (Ethereum の Co-founder)
開発チーム等	Ethereum Foundation	Polygon Technology	Ava Labs	Binance Holdings Ltd.	Web3 Foundation

[25] 本表において「互換性がある」とは、Ethereum のスマートコントラクトが他のブロックチェーンで稼働するということを意味する。

コンセンサスアルゴリズム	GHOST[26] (Proof of Work) ※Eth2.0: Proof of Stake に移行中	Proof of Stake	Proof of Stake	Proof of Staked Authority（PoSA)[27]	Nominated Proof of Stake（NPoS）
スマートコントラクト開発言語[28]	Solidity, Vyper	Solidity, Vyper	Solidity、Vyper	Solidity、Vyper	Solidity、Vyper
処理能力	15TPS	65,000TPS	400-1,500TPS/Chain	10,000TPS	1,000TPS
実行モデル（マシン）	Account-Based[29] (EVM)	Account-Based (EVM)	UTXO-Based[30] (AVM+EVM+more)	Account-Based (EVM)	Account-Based
平均ブロック生成時間[31]	14sec	2sec[32]	2sec	5sec	6sec
主なトークン規格	ERC-20, ERC-721, ERC-1155	ERC-20, ERC-721, ERC-1155	ERC-20, ERC-721, ERC-1155	BEP-20, BEP-721, BEP-1155	―
主なステーブルコイン	USDT, USDC, DAI, TerraUSD	USDT, USDC, DAI, TerraUSD	USDT, DAI, TUSD, TerraUSD	DAI, BUSD, TerraUSD	USDT, USDC, sUSD, TerraUSD
主な DeFi サービス	Uniswap, Maker, Aave	Uniswap, Maker, Aave	Maker, Aave, Pangolin	Maker, Aave, Pancake Swap	Reef, Curve
主な NFT サービス	Flow, Enjin, Mana, Opensea	Polygonpunks, Opensea	NFTrade, Kalao	Juggerworld, Treasureland	Bondly, Xen
主なウォレット	Metamask, Trust wallet	Metamask, Coinbase Wallet	Avalanche wallet, Metamask	Metamask, Trust Wallet	Polka Wallet, Trust Wallet

[26] GHOST (Greedy Heaviest Observed Subtree)：最も多くの計算が蓄積されているチェーンを正しいチェーンとする仕組み

[27] PoSA：PoS(Proof of Stake)と PoA(Proof of Authority)を組み合わせたもの。Binance Smart Chain What is Binance Smart Chain? https://docs.binance.org/faq/bsc/bsc.html

[28] https://chainstack.com/protocols/ethereum/

[29] Account-Based：通帳のようにアカウントの残高をそのままデータとして管理・記録する方法

[30] UTXO-Based (Unspent Transaction output)：取引データのみに基づいてアドレスの残高を計算して求める方法

[31] Solana comparison to other chains https://www.reddit.com/r/solana/comments/qpt2bb/solana_comparison_to_other_chains/

[32] Polygon PoS Chain Average Block Time Chart https://polygonscan.com/chart/blocktime

【コラム：Ethereum2.0 Sharding[33]】

シャーディングは Ethereum のスケーラビリティと容量を向上させるためのマルチフェーズのアップグレードである。このアップグレードは、2023 年にリリースされる予定。シャーディングの特徴は以下の通り。

- シャーディングは、データベースを水平に分割して負荷を分散するプロセスであり、ネットワークの混雑を減らし、「シャード」と呼ばれる新しいチェーンを作成することによって、1 秒あたりのトランザクションを増加させる。
- シャードチェーンは、ネットワーク負荷を 64 個の新しいチェーンに分散し、ハードウェア要件を低く抑えることで、ノードの実行が容易になる。
- シャードチェーンでは、バリデータは分割された小さなデータであるシャードを実行または保持するだけで良く、ネットワーク全体を検証する必要はない。これは処理を高速化し、必要なハードウェアの要件を減らす。
- シャーディングは、最終的には仲介サービスに頼らずに個人の PC やスマートフォンで Ethereum を実行することを可能にするとされる。より多くの人々がシャーディングされた Ethereum にクライアントとして参加したり、トランザクションを実行したりすることができると期待されている。

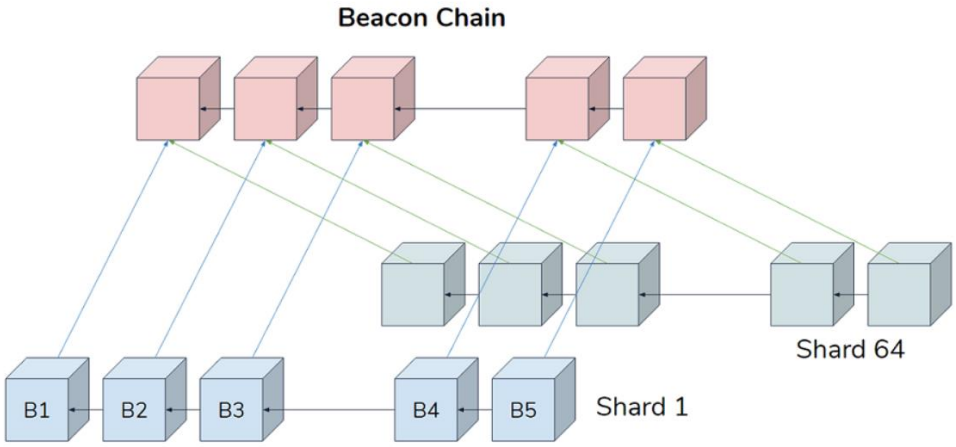

図 1-3-1　Ethereum 2.0 シャーディング[34]
※図の Beacon Chain が Ethereum2.0 のメインチェーンとなる

[33] Ethereum.org シャードチェーン https://ethereum.org/ja/upgrades/shard-chains/
[34] Ethereum 2.0 がガス代高騰問題に対処し、Dai および DeFi のスケールを拡大させる方法 https://blog.makerdao.com/eth2-0/

1-4-2　基盤ブロックチェーンの機能拡張サービス

処理能力の向上とガス代の削減を主目的とした以下のレイヤー２スケーリングソリューションについて、概要と主な技術特性を記述する

表 1-4-2　基盤ブロックチェーンの機能拡張サービスの技術特性

スケーリング ソリューション	**Optimism**	**Arbitrum**	**Loopring**	**zkSync**
概要	・Ethereum の Plasma Group から生まれたスタートアップが開発。 ・Ethereum の EVM と互換性がある。	・Princeton University の研究者が Offchain Labs を創業して開発。 ・独自の AVM（Arbitrum virtual Machine）を使用し、EVM と互換性がある。	・中国のスタートアップ Loopring が開発。 ・メインネットで最初の zk-Rollup であり、レイヤー2 に独自の製品と機能を構築することに重点を置いている。	・ベルリンのスタートアップ Matter Labs が開発。 ・Ethereum の EVM と互換性がある。
Rollup の種類	Optimistic Rollup	Optimistic Rollup	zk-Rollup	zk-Rollup
サービス開始	2021 年	2021 年	2019 年	2020 年
創設者	Jinglan Wang, Karl Floersch, Kevin Ho (Plasma Group)	Steven Goldfeder(CEO), Edward W. Felten(Chief Science Officer) , Harry Kalodner	Daniel Wang (Founder and CEO)	Alex Gluchowski (Co-Founder & CEO)
開発言語	Solidity	Solidity, Vyper, Yul	Solidity	Solidity, Zinc
処理能力	500TPS	500TPS	2,000TPS	2,000TPS
主なステーブルコイン	USDT, USDC, DAI	USDT, USDC, DAI	USDT, USDC, DAI	USDT, USDC, DAI
主な DeFi	Uniswap, Maker, Aave	Uniswap, Maker, Aave	Loopring Exchange	Maker, SynFutures
主な NFT サービス	Quixotic, Optipunks	STRATOS, tofuNFT	Gamestop	Tevaera, tofuNFT
主なウォレット	Metamask, Coinbase Wallet	Metamask, Coinbase Wallet	Loopring Wallet	Go Pocket, FoxWallet

1-4-3　アプリケーション基盤・アプリケーション

以下の DeFi プロジェクトについて、技術特性を含めた概要を説明する。

(1) 分散型取引所（DEX）

表 1-4-3-1　主な分散型取引所（DEX）の概要

DeFi プロジェクト	Uniswap	Curve Finance	SushiSwap
創設年・創設者・運営形態など	・2018 年 11 月創設 ・創設者：Hayden Adams ・Uniswap.org が運営	・2020 年 8 月創設 ・創設者：ロシアの科学者である Michael Egorov ・Egorov 氏が CRV（ガバナンストークン）の 71%を保有 ・Curve DAO が運営	・2020 年 9 月創設 ・創設者：Chef Nomi、共同設立者：0xMaki（共に仮名） ・2020 年 9 月、管理者権限を Alameda Research 社の CEO Sam Bankman-Fried に移譲 ・Sushiswap コアチームが運営
利用可能ブロックチェーン	Ethereum Polygon Optimism Arbitrum	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum　など	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum　など
概要・特徴など	・暗号資産・ステーブルコイン等のトークン交換のためプロトコル ・自動マーケットメーカー（AMM）によりトークン交換価格が自動的に決定 ・流動性提供者は、任意のトークンペアの流動性を流動性プールに提供することで手数料を得る	・ステーブルコインの交換に特化した分散型取引所 ・スリッページ率や取引手数料が低いステーブルコイン間の取引が可能とされる	・2020 年 9 月に Uniswap のフォークとして誕生 ・流動性を提供することで SUSHI トークン（ガバナンストークン）を報酬として得ることができる
TVL (2022/4/20 時点)	$7.04B	$10.32B	$1.49B

ガバナンス	・UNI による投票 ・投票 2 回で承認 ・スナップショット投票（提案対象選定） ・ガバナンス投票（実施可否決定）	・CRV による投票 ・投票 2 回で承認 ・スナップショット投票（提案対象選定） ・ガバナンス投票（実施可否決定）	・SUSHI による投票（投票は 1 回のみ） ・コミュニティは供給量の 40%で拒否権を発動できる ・一部（小さな変更とされるもの）は投票を行わず、運営者とコアチームが決定
インシデント発生事例	・2020/9/25 取引所 KuCoin の攻撃により 2 億 7,500 万ドルが流出した際に、Uniswap で ETH に交換され、資金洗浄が行われたとされる ・2020/4/18 ERC-777 リエントランシー脆弱性（2-2-4 参照）攻撃により 30 万ドルの損失	・2021/11/11 ガバナンス攻撃（ガバナンストークンの大量購入による投票の乗っ取り）により 3,000 万ドルの損失	・2021/9/17 MISO プラットフォーム（SushiSwap が提供する IDO（新規トークンを DEX 上でローンチして資金調達）を行うプラットフォーム）のサプライチェーン攻撃 (ソースに悪意あるコードを組込む）により 300 万ドルが流出

(2) ステーブルコイン発行プラットフォーム

本報告書では、ステーブルコインを以下の２種類に分類した上で議論を行う。

・デジタルマネー類似型ステーブルコイン　Tether、USD Coin など
法定通貨の価値と連動した価格（例：１コイン＝１ドル）で発行され、発行価格と同額で償還を約するもの（及びこれに準ずるもの）

・暗号資産型ステーブルコイン　DAI、TerraUSD など
DAI のように他の暗号資産及びステーブルコインを超過担保として保持することで価値の安定を試みるものや、TerraUSD のように無担保でアルゴリズムにより価値の安定を試みるものなどがある。

表 1-4-3-2　主なステーブルコイン発行プラットフォームの概要

DeFi プロジェクト	Maker (DAI)	Tether (USDT)	USD Coin (USDC)	TerraUSD（UST）
ステーブルコインの種別	暗号資産型	デジタルマネー類似型	デジタルマネー類似型	暗号資産型
創設年・創設者・運営形態など	・2017 年 12 月創設 ・創設者：デンマーク人 Rune Christensen ・分散型自律組織として分散度を向上させるため、2021 年 7 月に Maker Foundation が MakerDAO に運営を引き継いだ	・2014 年創設 ・Tether Limited 社（香港の有限会社）が発行・管理 ・iFinex 社（香港）が Tether 社と交換所 Bitfinex 社を管理	・2018 年 9 月創設 ・米 Circle 社や米 Coinbase 社が設立した米 Centre Consortium が発行・管理	・2018 年 1 月、Terraform Labs 社創設 ・創設者：Do Kwon（CEO：韓国 TMON 社創業者）、Daniel Shin ・Terraform Labs 社（Terra alliance 社の子会社）が運営（韓国ソウル）
利用可能ブロックチェーン	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum Loopring zkSync　など	Ethereum Polygon Avalanche BNB Smart Chain Polkadot Optimism Arbitrum Loopring zkSync　など	Ethereum Polygon Avalanche BNB Smart Chain Polkadot Optimism Arbitrum Loopring zkSync　など	Terra Ethereum Polygon Avalanche BNB Smart Chain Polkadot　など

概要・特徴など	・新しい DAI が発行される際に、DAI 発行額以上の暗号資産もしくはステーブルコインを担保化することで価格の安定化を図る。	・Tether 社が USDT の発行額と同等の裏付資産を保有・管理しているとされる。	・Circle 社が USDC の発行額と同等の裏付資産を保有・管理しているとされる。	・LUNA（Terra ブロックチェーンのネイティブトークン）の追加/削除により、UST が 1USD を維持するようにアルゴリズムで制御する。 ・Anchor Protocol に UST を預けて最大 19.5%の利回りを得ることができる
発行残高[35] (2022/5/18 時点)	$6.52B	$79.71B	$52.26B	$11.28B
ガバナンス	・MKR による投票 ・ガバナンス投票（ガバナンスに関する変更）またはエグゼクティブ投票（技術的変更）で承認	・Tether Limited 社が運営管理	・Centre Consortium が運営管理	・LUNA トークンによる投票 ・投票は 1 回のみ ガバナンス投票の 50%以上の賛成で決定
インシデント発生事例	・2020/3/12 市場価格の急落により強制清算が追いつかず、担保オークションへのゼロ入札により 832 万ドルの損失（2-3-4 参照）	・2021/3/1 偽造文書と脅迫メールによる 500BTC を要求する身代金攻撃（被害なし）	－	・2022/5/10 UST の大量売りにより市場価格が下落し、1USD の維持ができなくなり取り付け騒ぎが発生。価格が 87%下落。

[35] Cryptocurrencies https://coinmarketcap.com/coins/

(3) レンディングプラットフォーム

表 1-4-3-3　主なレンディングプラットフォームの概要

DeFi プロジェクト	Aave	Compound
創設年・創設者・運営形態など	・2017 年 11 月創設 ・創設者：シリアルアントレプレナーの Stani Kulechov ・Aavenomics コミュニティが運営	・2017 年創設 ・創設者：Robert Leshner, Geoffrey Hayes（Compound プロトコルのソフトウェア開発会社 Compound Labs, Inc 社の CEO と CTO） ・Compound チームは運営に関与しないとされる。チームは十数人構成、半数はエンジニア。
利用可能 ブロックチェーン	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum zkSync　など	Ethereum Avalanche BNB Smart Chain
概要・特徴など	・貸付者は暗号資産やステーブルコイン等のトークンを流動性プールに提供することで利回りを得ることができる ・金利は需供に基づいて自動的に調整される ・Flash Loan（1 トランザクション内で借入から返済まで完結するトランザクション）の実行が可能	・貸付者は暗号資産やステーブルコイン等のトークンを流動性プールに提供することで利回りを得ることができる ・金利は需供に基づいて自動的に調整される
TVL (2022/4/20 時点)	$ 11.46B	$6.34B
ガバナンス	・AAVE による投票 ・投票 2 回で承認 ①スナップショット投票（提案対象選定） ②ガバナンス投票（実施可否決定）	・COMP による投票 ・投票は 1 回のみ ・投票作成から実行まで最短で 7 日間 ・予期しない脆弱性が発生した場合に備えて、一連のサービスを無効にする機能がある
インシデント発生事例	－	・2021/10/4 アップグレードの不具合により 1 億 6,200 万ドルの損失 ・2021/9/30 アップグレードの不具合により 9,000 万ドルを誤支払い

(4) デリバティブプラットフォーム

表 1-4-3-4　主なデリバティブプラットフォームの概要

DeFi プロジェクト	Synthetix	Opyn	Ribbon Finance
創設年・創設者・運営形態など	・2017 年 9 月創設 ・創設者：オーストラリア人 Kain Warwick ・5 つの DAO で運営 - Spartan Council - Protocol DAO - Synthetix DAO - Ambassadors DAO - GrantsDAO	・2019 年創設 ・創設者： Zubin Koticha, Alexis Gauba, Aparna Krishnan ・創設者 3 名のチームとパートナーが運営	・2021 年 2 月創設 ・創設者： Julian Koh （元 Coinbase エンジニア） ・Ribbon DAO が運営
利用可能 ブロックチェーン	Ethereum Polygon Avalanche BNB Smart Chain	Ethereum	Ethereum
概要・特徴など	・利用者が法定通貨や株式、金や石油などのコモディティの価格と連動するトークン（合成資産）を生成・取引することができる ・合成された資産 Synthetic Assets は Synthetix Exchange(Kwenta) という専用の取引所で取引される	・ユーザがオプションを購入、販売、作成できる DeFi プロトコル ・ユーザがオプションスプレッドとコンボを交換し、フラッシュミント[36](1 トランザクション内で返済まで行う無担保オプションの借入) を実行し、満期時に自動行使して新しいオプションを作成できる	・DeFi の様々なデリバティブを組み合わせて任意のストラクチャード商品を作ることができる ・価格変動への賭け、利回りの向上、元本確保など、特定のリスク・リターン目的を達成するために、デリバティブを組み合わせて使用するパッケージ型の金融商品
TVL (2022/4/20 時点)	$276.1M	$111.4M	$106.8M
ガバナンス	・2 つの改善提案を運営組織が承認する ① 改善提案（SIP） Spartan Council が SIP 作成者にインタビューして承認 ②構成変更提案 (SCCP) システム既存パラメータ変更を含む、他は SIP と同じ	・コアチームが運営管理 - ホワイトリスト/ブラックリスト登録 - モジュール更新 - Oracle 管理 - 緊急時システム停止 -トークン超過残高を引き出す	・RBN トークンによる投票 ・投票は 1 回のみ ・スナップショット投票 ・賛成または反対の 50%以上で判断
インシデント発生事例	・2019/6/25 FX 価格フィードのオラクル攻撃により 10 億ドルを喪失	―	・2021/10/8 エアドロップ(給付金)攻撃で 250 万ドルを流出後に変換

[36] What is a flash mint? https://github.com/opynfinance/v2-documentation

(5) 保険

表 1-4-3-5　主な保険プラットフォームの概要

DeFi プロジェクト	Armor	Nexus Mutual
創設年・創設者・運営形態など	・2020 年 11 月創設 ・創設者：Jose Macedo, Azeem Ahmed, Robert Forster ・ArmorDAO コミュニティが運営	・2019 年 5 月創設 ・創設者：Hugh Karp 英国の保険アクチュアリー ・Nexus Mutual Community が運営
利用可能ブロックチェーン	Ethereum	Ethereum Solana
概要・特徴など	・Uniswap, Maker, AAVE などの一般的なプロトコルにおけるスマートコントラクトのリスクから投資を保護する ・サポートされているプロトコル上の残高の変化を検知し、それに応じてプランを調整するよう促す。各プロトコルで保護されている正確な金額が秒単位で請求さるれる ・Nexus Mutual の保険をベースに複数プロトコルや補償範囲などを追加	・スマートコントラクトの脆弱性やその他の予測できない事象に対してリスクを共有することができる分散型保険のプラットフォーム ・ETH を利用したブロックチェーン上のユーザに分散型保険を提供する。英国で任意相互会社として運営されているデジタル協同組合であり 、Ethereum ユーザに「保険の代替手段」を提供する[37] ・Kenetic、Blockchain Capital、Version One、Semantic Ventures、Collider Ventures などの著名なアドバイザーやパートナーからの経験を引き出している
TVL (2022/4/20 時点)	$511.5M[38]	$481.7M
ガバナンス	・ARMOR トークンによる投票 ・投票は 1 回のみ ・２つのオーナーによりハイブリッドで制御 ①チームマルチシグ 運営チームによる管理 ②ガバナンス投票 ユーザによる投票	・NXM トークンによる投票 ・審査 1 回、投票 2 回 ①諮問委員会による報酬の設定（ホワイトリスト） ②諮問委員会の投票 ③メンバー投票
インシデント発生事例	・2021/2/28 チームメンバーの詐欺により 85 万ドルの損失	・2020/12/4 創業者の個人アドレスの標的型攻撃により 800 万ドルの損失

※ Nexus Mutual の KYC / AML 要件
メンバーになるには、KYC / AML プロセスを使用して本人確認を行う必要がある。これが失敗した場合、会費は返金される
【メンバー対象外の国】

[37] https://medium.com/multi-io/defi-explained-nexus-mutual-12d01f4471bb
[38] https://www.stelareum.io/en/defi-tvl/protocol/armor.html

中国、メキシコ、シリア、エチオピア、北朝鮮、トリニダード・トバゴ、インド、ロシア、チュニジア、イラン、セルビア、バヌアツ、イラク、韓国、イエメン、日本、スリランカ

(6) NFT（Non-Fungible Token　非代替性トークン）

NFT とは、一般に、ブロックチェーン上に記録される、スマートコントラクト内において一意で代替不可能なトークンのことを指し、画像・動画・音声、およびその他の種類のデジタルファイルなど、容易に複製可能なアイテムをメタデータとして関連づけるサービス等に活用されている。

表 1-4-3-6　主な NFT サービスの概要

DeFi プロジェクト	Opensea	CryptoPunks
創設年・創設者 運営組織	・2017 年 12 月創設 ・共同創設者： Devin Finzer（CEO）， Alex Atallah（CTO） ・Opensea 社が運営	・2017 年 6 月創設 ・共同創設者：Matt Hall, John Watkinson ・Larva Labs 社が運営
利用可能 ブロックチェーン	Ethereum Polygon　など	Ethereum Polygon
概要・特徴など	・NFT 最大手のプロジェクト ・世界最大規模の NFT マーケットプレイス ・アメリカのニューヨークを拠点	・NFT 最古のプロジェクトの一つ ・アート 1 つずつの所有権が Ethereum に記録された、初の NFT アート ・クレジットカード大手の Visa が購入し注目を集めている
累計取引総額[39] (2022/4/20 時点)	$23.5B	$2.66B
ガバナンス	Opensea 社が運営管理	Larva Labs 社が運営管理
インシデント発生事例	2021/10/14 セキュリティ脆弱性の指摘を受けて緊急修正（1時間で対応完了、被害なし）	－

1-4-4　アグリゲーション

表 1-4-4　DeFi アグリゲーターの概要

DeFi プロジェクト	Instadapp	DeFi Saver	1inch
創設年・創設者・運営形態など	・2018 年 12 月創設 ・創設者：Sowmay Jain（Co-founder & CEO） ・Instadapp Community が運営	・2019 年 4 月創設 ・創設者：Nenad Palinkasevic（Co-founder） ・Defi Saver が運営	・2020 年 12 月創設 ・共同創設者：Sergej Kunz, Anton Bukov ・1inch DAO が運営
ブロックチェーン	Ethereum	Ethereum	Ethereum Avalanche

[39] NFT Marketplaces https://dappradar.com/nft/marketplaces

			BNB Smart Chain など
概要・特徴など	・資産を管理するための MakerDAO, Compound, Uniswap などの DeFi プロトコルを集約するスマートウォレット。 ・ダッシュボードを使用すると、ユーザはすべての DeFi を 1 か所で確認できる。	・DeFi プロトコル用のワンストップ管理アプリ。 ・独自の自動資産管理および清算保護機能を備えている。 ・レバレッジ管理ツールとして知られている。	・流動性プロトコルは自動マーケットメーカー（AMM）として分散型トークンスワップを提供する ・プロトコルはアービトラージの差益をキャプチャするように設計されている。
TVL (2020/4/20 時点)	$5.19B	$509.7M	$14.5M
ガバナンス	・INST トークンによる投票 ・投票 2 回で承認スナップショット投票（提案対象選定）、ガバナンス投票（実施可否決定）	・Defi Saver が運営管理	・1INCH トークンによる投票 ・投票 2 回で承認スナップショット投票（提案対象選定） ガバナンスオンチェーン投票（実施可否決定）
インシデント発生事例	―	・2020/10/8 トークン交換コントラクトの脆弱性により 31 万 DAI の損失	―

1-4-5　ユーザおよびユーザインターフェース

(1) ユーザインターフェース

ユーザが暗号資産購入や交換、流動性プールへの暗号資産預入など DeFi の機能・サービスを利用する場合に、Web ブラウザやスマートフォンアプリのユーザ認証 画面やユーザ操作画面（GUI：Graphical User Interface）から取引を操作する。

(2) オペレータ（デプロイを行う管理者や権限者を含む）

スマートコントラクトのデプロイやメンテナンス、DeFi プロトコルの稼働監視などの DeFi システム運用作業を、クライアントソフトウェアのユーザ操作画面から操作する。

(3) DeFi システム開発者

DeFi プロトコル（スマートコントラクト）の開発・テストなどを Truffle などの開発ツールを使用して行う。

(4) コード監査者

スマートコントラクトの監査を監査ツールやテスト実行などにより行う。

(5) コミュニティ参加者

DeFi プロジェクトのコミュニティフォーラムへの投稿やガバナンストークンによるオンチェーン投票などを行う。

1-5　相互運用性（Interoperability）の分析

同一ブロックチェーン上にデプロイされた DeFi プロジェクト間の相互運用だけでなく、Ethereum ブロックチェーンとレイヤー2 スケーリングソリューションやメインチェーン・サイドチェーン間の相互運用も分析対象として、その技術特性と課題を考察する。

(1) ブロックチェーン（Ethereum）内の DeFi プロジェクト間のトークン間の相互運用

Ethereum では ERC-20 などのトークン規格が策定されており、多くの DeFi プロジェクトはこれらのトークン規格に準拠する形でガバナンストークンやステーブルコインの発行を行っている。規格に準拠するトークンはどの DeFi プロジェクトでも同じ型の操作対象として利用できるため、相互運用性が高い。

但し、どの DeFi プロジェクトからも連携される可能性があることも意味するため、アービトラージなどで予期しない攻撃を受けるリスクがある。

(2) Ethereum メインチェーンとレイヤー2 ソリューションとの相互運用

Ethereum のスケーリング対策としてレイヤー2 ソリューションの利用が高まっており、多くの DeFi プロジェクトがレイヤー2 ソリューションを採用している。レイヤー2 ソリューションは EVM 互換であり、Ethereum と同じ開発言語やライブラリが機能する。一方で、なお発展途上の技術であり、データの書き込み時点では有効性の検証が行われずトランザクションの確定は不正証明のチャレンジ期間を待つ必要があるなど（例：Optimistic Rollup）の課題も存在する。

(3) Ethereum メインチェーンとサイドチェーン間の相互運用

Ethereum メインチェーンとサイドチェーンは双方向ブリッジで接続できる機能が提供されており、多くのサイドチェーンが Ethereum と接続して運用している。サイドチェーンの多くが EVM 互換であり、Ethereum と同じ開発言語やライブラリが機能する。また、メインチェーンとサイ ドチェーン間で資金をやりとりする場合、双方向ブリッジに資金をロックして資金を交換することが可能になり、二重支払いを防止する。

近年は Ethereum のトランザクション混雑やガス高騰により、ゲームなどに必要な高速処理やガス代の低減を求めてサイドチェーンの利用が高まっている。その一方で、双方向ブリッジに数十億ドルの多額の資金がロックされて、攻撃者に狙われるリスクが高まっており、後述のようにインシデントも多発している。

第２章 主要な DeFi プロジェクトについての分析

本章では、主要な DeFi プロジェクトを選定し、その組織や関係者、技術特性、ガバナンス運用、金融機関との連携、インシデント事例などについて詳細に調査研究を行うことで、課題や問題点およびリスク事項の特定を行う。

本章は次のように構成される。2-1 では、調査対象とする DeFi プロジェクトを、分散型取引所、ステーブルコイン発行、レンディングの３つのサービスから選定する。2-2 から 2-4 では、選定した３つの DeFi プロジェクトについて詳細に調査した結果を報告する。2-5 では、３つの DeFi プロジェクトの分析結果を比較し、全体の傾向や各 DeFi プロジェクトの特徴を明確にする。2-6 では、他の DeFi プロジェクトで発生したインシデント事例を調査し、リスク事項について分析を行う。最後に、2-7 でトラストチェーンにおけるトラストポイントの分析結果を説明する。

2-1　調査対象とする DeFi プロジェクトの特定

TVL や調査目的などの指標を参考に、前述の主な DeFi プロジェクトの６つのサービスより、以下の３つを対象として選定した。

(1) 分散型取引所（DEX）

複数の暗号資産・ステーブルコインを自動的に交換する DeFi の基本的なユースケースであるため、調査対象とする。

(2) 暗号資産型ステーブルコイン発行プラットフォーム

暗号資産・DeFi 取引で使用されることが多いステーブルコインを発行するプロジェクトのうち、その発行自身も分散的に行われる暗号資産型ステーブルコインを調査対象とする。

(3) レンディングプラットフォーム

DeFi の基本的なユースケースであり TVL が最も大きいため、調査対象とする。

2-1-1　調査対象 DeFi プロジェクトの選定（分散型取引所）

分散型取引所について、以下の DeFi プロジェクトの比較結果より、調査対象として Uniswap を選定する。TVL が大きいこと、インシデント事例があること、スマートコントラクトをアップグレード不可にしているなど調査すべき技術特性があることなどから、調査対象として適切と判断した。

表 2-1-1　調査対象 DeFi プロジェクトの選定（分散型取引所）

DeFi プロジェクト	Uniswap	Curve Finance	SushiSwap
既存スマートコントラクトの修正（商品・サービス追加・パラメータ変更など）	パラメータの一部のみ修正可	ガバナンス投票で可決後、Curve チームが修正	ガバナンス投票で可決後、コミュニティメンバー9 名の投票で決定
既存スマートコントラクトの修正（コアコントラクトの変更）	コアコントラクトはアップグレード不可	ガバナンス投票で可決後、Curve チームが修正	ガバナンス投票で可決後、コミュニティメンバー9 名の投票で決定
新規スマートコントラクトの展開（バージョンアップ等の新たなスマートコン	開発会社（Uniswap Labs）が実施	Curve チームが実施	ガバナンス投票で可決後、コミュニティメンバー9 名の投票で決定

トラクトのデプロイなど）			
緊急時発動（サービス緊急停止など）	コアコントラクトは停止できない	コミュニティメンバー9名の投票で決定	コミュニティメンバー9名の投票で決定
ガバナンストークン	UNI	CRV	SUSHI
ガバナンストークン保有アドレス数・保有率	・27万6千アドレス ・1位保有率　17.34% ・上位 10 アドレス保有率　53.42%	・5万2千アドレス 1位保有率　36.07% ・上位 10 アドレス保有率　83.60%	・1万7千アドレス ・1位保有率　18.19% ・上位 10 アドレス保有率　65.18%
ガバナンス投票の提案対象	・流動性プールの追加や変更 ・手数料などの数値パラメータの変更 ・提案事項は特に限定されていないが、コアコントラクトが変更不可など、技術特性上ガバナンス投票の対象に制約が生じる。	・流動性プールの追加や変更 ・手数料などの数値パラメータの変更 ・コアコントラクトの変更	・コアコントラクトの変更や資金の利用
投票可決条件	①スナップショット投票：意見を幅広く募集して提案対象を選定 定足数5万UNI（全体の0.05%）、投票数の過半数の賛成 ②ガバナンス投票：提案の実施可否を決定4,000万UNI（全体の 4%）の定足数、投票数の過半数の賛成	①スナップショット投票：定足数 30%、賛成51% ②ガバナンス投票：定足数 15%、賛成60%	①スナップショット投票：500万SUSHIトークンの定足数、投票数の過半数の賛成 ②投票で可決された後、コミュニティメンバー9名のマルチシグで決定（6of9）
投票数（2021/12/12時点）	①32件中7件可決 可決率22% ②6件中5件可決 可決率83%	①68件中60件可決 可決率88% ②14件全て可決 可決率100%	15件中13件可決 可決率87%

2-1-2　調査対象DeFiプロジェクトの選定（暗号資産ステーブルコイン発行プラットフォーム）

暗号資産ステーブルコイン発行プラットフォームについて、以下のDeFiプロジェクトの比較結果より、調査対象としてMakerを選定する。TVLが高額であり、分散型自律組織（DAO）への移行がDeFiプロジェクトの中で最も先行している事例であること、また他のDeFiプロジェクトはいずれも会社が運営している中央集権型組織であり、Makerは多様な対象を調査する目的に合致することなどから、調査対象として適切と判断した。

表 2-1-2　調査対象 DeFi プロジェクトの選定（ステーブルコイン発行）

DeFi プロジェクト（ステーブルコイン）	Maker (DAI)	Tether (USDT)	USD Coin (USDC)
既存スマートコントラクトの修正（商品・サービス追加・パラメータ変更など）	ガバナンストークンによる投票で決定	Tether Limited 社が実施	Centre Consortium 社が実施
既存スマートコントラクトの修正（コアコントラクトの変更）	ガバナンストークンによる投票で決定	Tether Limited 社が実施	Tether Limited 社が実施
新規スマートコントラクトの展開（バージョンアップ等の新たなスマートコントラクトのデプロイなど）	ガバナンストークンによる投票で決定	Tether Limited 社が実施	Centre Consortium 社が実施）
緊急時発動（サービス緊急停止など）	オフチェーン投票による決定：5 万 MKR（全体の 5%）で実行）	Tether Limited 社が実施	Centre Consortium 社が実施
ガバナンストークン	MKR	－	－
ガバナンストークン保有アドレス・保有率	・7 万 6 千アドレス ・1 位保有率　17.39% ・上位 10 アドレス保有率　45.38%	－	－
ガバナンス投票の提案対象	提案内容により 2 種類に分けて行う ① ガバナンス投票 安定化手数料・担保比率変更など ②エグゼクティブ投票 Maker プロトコルの技術的変更	－	－
投票可決条件	①②とも同じ条件 1 万 MKR（1%）の定足数、過半数の賛成	－	－
投票数（2021/12/12 時点）	①302 件中 271 件可決 可決率 90% ②48 件中 47 件可決 可決率 98%	－	－

2-1-3　調査対象 DeFi プロジェクトの選定（レンディングプラットフォーム）

レンディングプラットフォームについて、以下の DeFi プロジェクトの比較結果より、調査対象として Aave を選定する。TVL が大きく機関投資家の KYC サービス開始など他にあまり見られないサービスを実施していることから、調査対象として適切と判断した。

表 2-1-3　調査対象 DeFi プロジェクトの選定（レンディング）

DeFi プロジェクト名	Aave	Compound

既存スマートコントラクトの修正 商品・サービス追加・パラメータ変更など	ガバナンストークンによる投票	
既存スマートコントラクトの修正（コアコントラクトの変更）	ガバナンストークンによる投票	ガバナンストークンによる投票
新規スマートコントラクトの展開 （バージョンアップ等の新たなスマートコントラクトのデプロイなど）	Aave Core Team が決定	Compound Labs が決定
緊急時発動（サービス緊急停止など）	Aave Core Team が決定	コミュニティメンバー6 名のマルチシグで決定（4-of-6）
ガバナンストークン	AAVE	COMP
ガバナンストークン保有アドレス・保有率	・10 万アドレス ・1 位保有率　18.54% ・上位 10 アドレス保有率 62.30%	・18 万 1 千アドレス ・1 位保有率　28.99% ・上位 10 アドレス保有率 54.32%
ガバナンス投票の提案対象	提案内容により 2 種類に分けて行う ①短時間ロック実行　迅速な介入を必要とする一部の変更など ②長時間ロック実行　ガバナンスに影響を及ぼす変更	・オンチェーン投票を行う（1 回のみ）
投票可決条件	①短時間ロック実行 定足数 2%と賛成/反対の差が 0.5%以上 ②長時間ロック実行 定足数 20%と賛成/反対の差が 15%以上	・提案：6.5 万 COMP（全体の 0.65%）の賛成 ・可決：40 万 COMP（全体の 4%）かつ投票数の過半数の賛成
投票数（2021/12/12 時点）	・50 件中 41 件可決　可決率 82%	・38 件中 32 件可決　可決率 84%

2-2　分散型取引所　Uniswap の分析

Uniswap を調査対象として、プロジェクト概要や運営組織、主な技術特性、ガバナンス運営、インシデント事例について詳細に調査研究を行う。Uniswap は開発会社の Uniswap Labs が Uniswap コミュニティの運営に一定程度関与していると考えられるほか、スマートコントラクトをアップグレード不可にしているなどの特徴がある。各項目の調査により実態を明らかにし、リスク事項を特定する。

2-2-1　プロジェクト全体概要

Uniswap の主な構成要素とそのマッピング、コミュニティ概要は下図・表の通り。

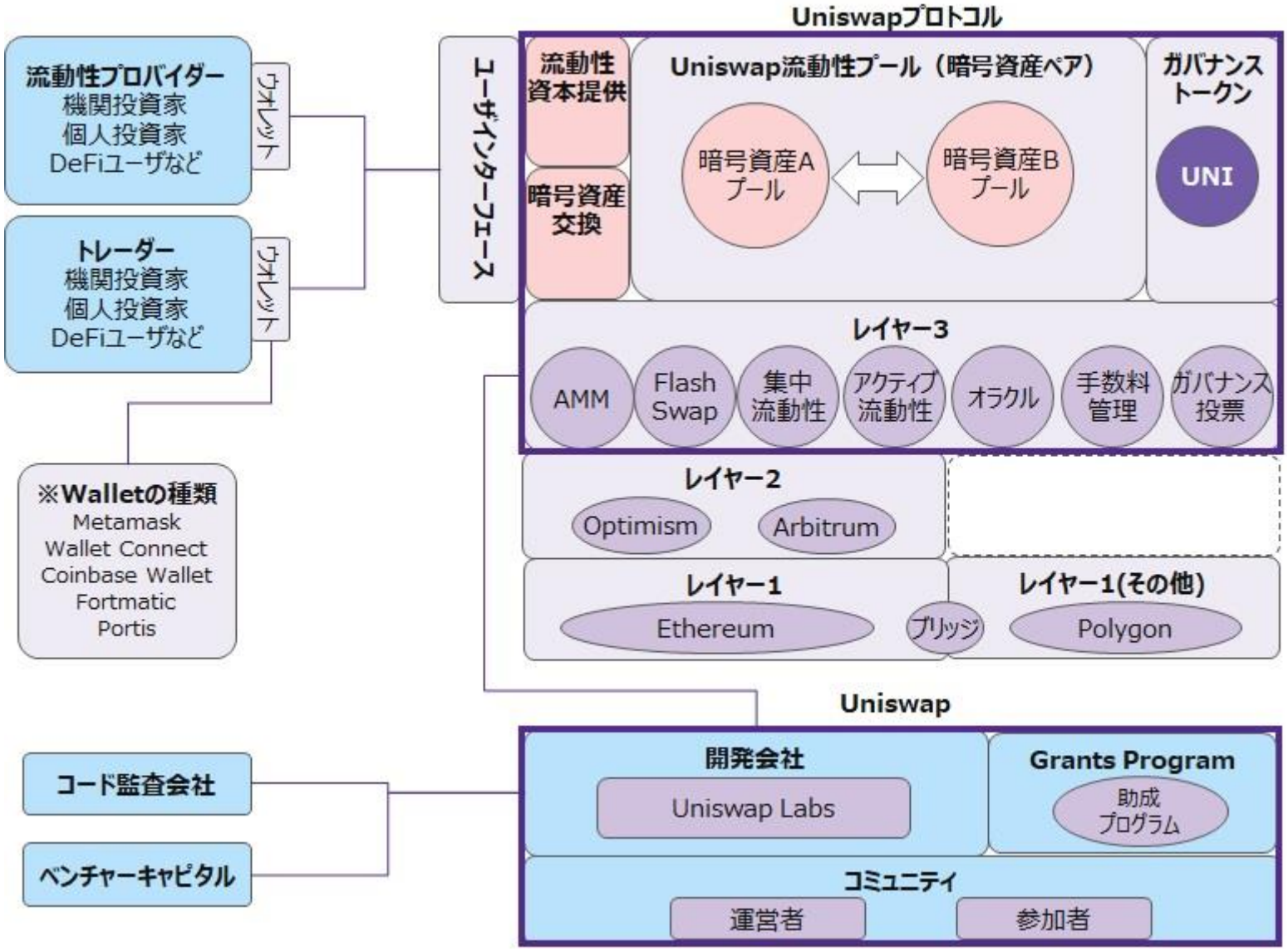

図 **2-2-1-1　Uniswap** の主な構成要素

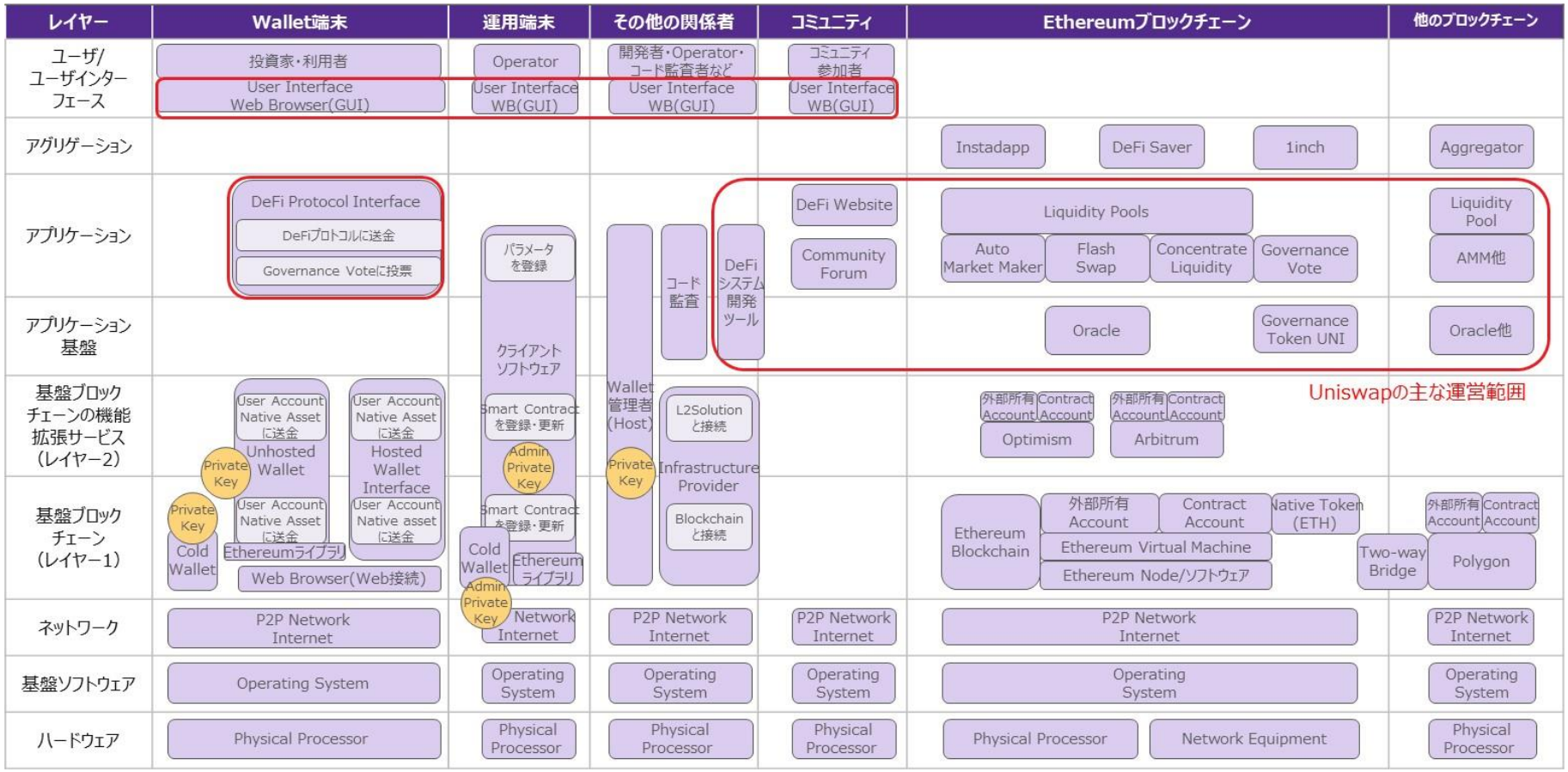

図 **2-2-1-2　Uniswap** の主な構成要素のマッピング

表 2-2-1　Uniswap：コミュニティ・開発会社・バージョン動向

区分	項目	概要	補足事項
組織	コミュニティ	Uniswap コミュニティ ガバナンストークン保有者による運営（保有アドレス：27 万 6 千）	DAO と称して活動中
	開発会社	Uniswap Labs 所在地：New York, United States 創設者, CEO：Hayden Adams 創設年月：2018/11	・Uniswap プロトコルや各種ツールの開発・管理 ・ウェブサイト（Uniswap.org）の運営 ・SEC（米国証券取引委員会）が Uniswap Labs に対する調査を行ったとの報道（2021/9）[40]
稼働バージョン	Uniswap バージョンと主な機能	(1) Uniswap v1 ・2018/11 ローンチ　Vyper 言語で開発 ・主な機能 AMM（自動マーケットメーカー） ETH を介した流動性プール（暗号資産ペアの交換）など	3 つのバージョンは別々に継続して稼働している Uniswap v1（2022/3 時点） 取扱暗号資産：約 200 取引ペア：385
		(2) Uniswap v2 ・2020/5 ローンチ Solidity 言語で開発 ・主な機能 暗号資産同士での流動性プール（ETH を介さない） Flash Swap TWAP（時間加重平均価格）オラクル　など	Uniswap v2（2022/3 時点） 取扱暗号資産：1,909 取引ペア：3,259
		(3) Uniswap v3 ・2021/5 ローンチ Solidity 言語で開発 ・主な機能 流動性集約機能（集中流動性など） 手数料の拡張、（NFT に仕様変更、手数料率を 3 段階など） オラクルの高度化　など	Uniswap v3（2022/3 時点） 取扱暗号資産：456 取引ペア：915

2-2-2　主な技術特性

Uniswap の主な技術特性について、その概要を説明する。

(1) AMM（Automated Market Maker）[41]

・スマートコントラクトが Uniswap の流動性プール（交換する暗号資産のペア）に預けられている暗号資産の量から取引価格（交換レート）を自動的に計算する仕組み

[40] SEC Investigating Uniswap Labs: Report https://www.coindesk.com/policy/2021/09/03/sec-investigating-uniswap-labs-report/

[41] What Is an Automated Market Maker? https://www.coindesk.com/learn/2021/08/20/what-is-an-automated-market-maker/

・初期の DEX で主に活用されていたオーダブック方式と比較して、オフチェーン処理が不要であり、かつ注文スピードが早いことが特徴とされる（Uniswap v1 から実装）

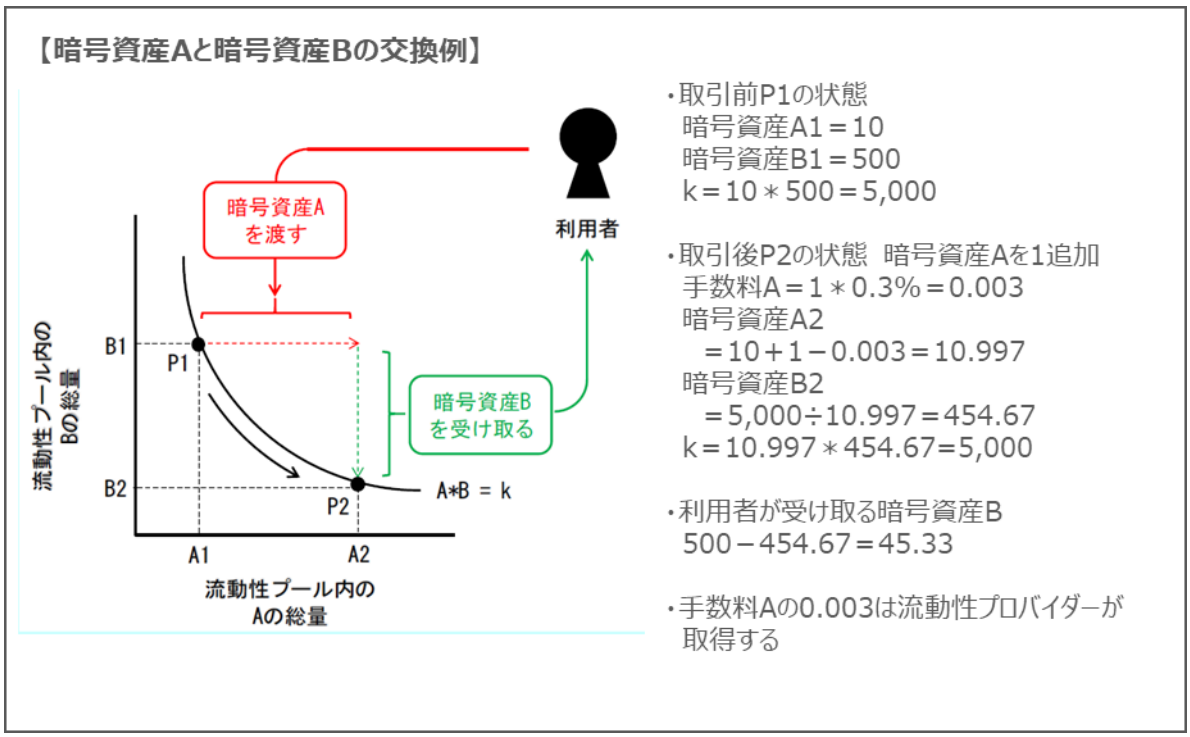

図 2-2-2-1　Uniswap AMM[42]（日本銀行ウェブサイトより図を引用）

(2) Flash Swap[43]

・暗号資産 A・B からなる流動性プールにおいて、1 回のトランザクション内で A と同額の B および手数料の合計を返却すれば、無担保で暗号資産 A を引き出して利用できる仕組みであり、主にアービトラージのために利用される。

・暗号資産 B が返却されなかった場合は、暗号資産 A を引き出すトランザクション自体が無かったことになり、無担保であることのリスクが軽減されているとされる

・Uniswap v2 にて実装

[42] 暗号資産における分散型金融　自律的な金融サービスの登場とガバナンスの模索
https://www.boj.or.jp/research/wps_rev/rev_2021/data/rev21j03.pdf

[43] Uniswap v2 Docs Flash Swap https://docs.uniswap.org/protocol/V2/concepts/core-concepts/flash-swaps

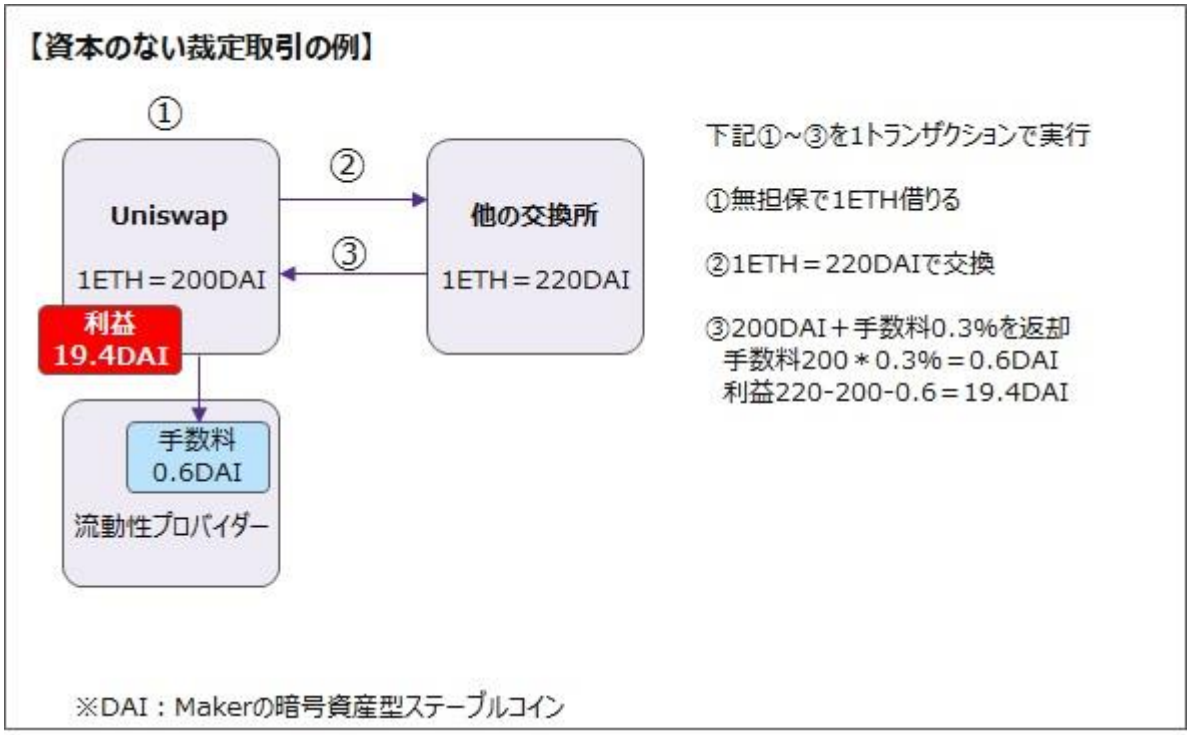

図 2-2-2-2　Uniswap：Flash Swap（Uniswap ウェブサイトをもとに弊社作成）

(3) 流動性集約機能[44]

・流動性プールに流動性を提供する際に、交換に応じる価格帯を指定できる機能。

・流動性プールの価格範囲を指定して、資本を集中させることにより流動性プロバイダの資本効率を上げるもの（上値・下値の価格範囲を指定して、市場価格が範囲に入るとプールの暗号資産に交換される指値注文に類似した形）。Uniswap v3 で導入され、v2 と比べて資本効率を 4,000 倍向上できるとされる。

・市場価格が指定した価格範囲の外に移動した場合には暗号資産ペアのうち一方の流動性が枯渇するため、それ以上の手数料が獲得できなくなる。

・流動性プロバイダ毎の流動性ポジションが異なる価格帯・異なる流動性で形成されるため、従来の代替性トークン（ERC20）ではなく非代替性トークン（NFT）で流動性ポジションを管理。スワップ手数料は v1, v2 では継続的に流動性プールに再投資されていたが、v3 より再投資されなくなった。

[44] Introducing Uniswap v3 https://uniswap.org/blog/uniswap-v3

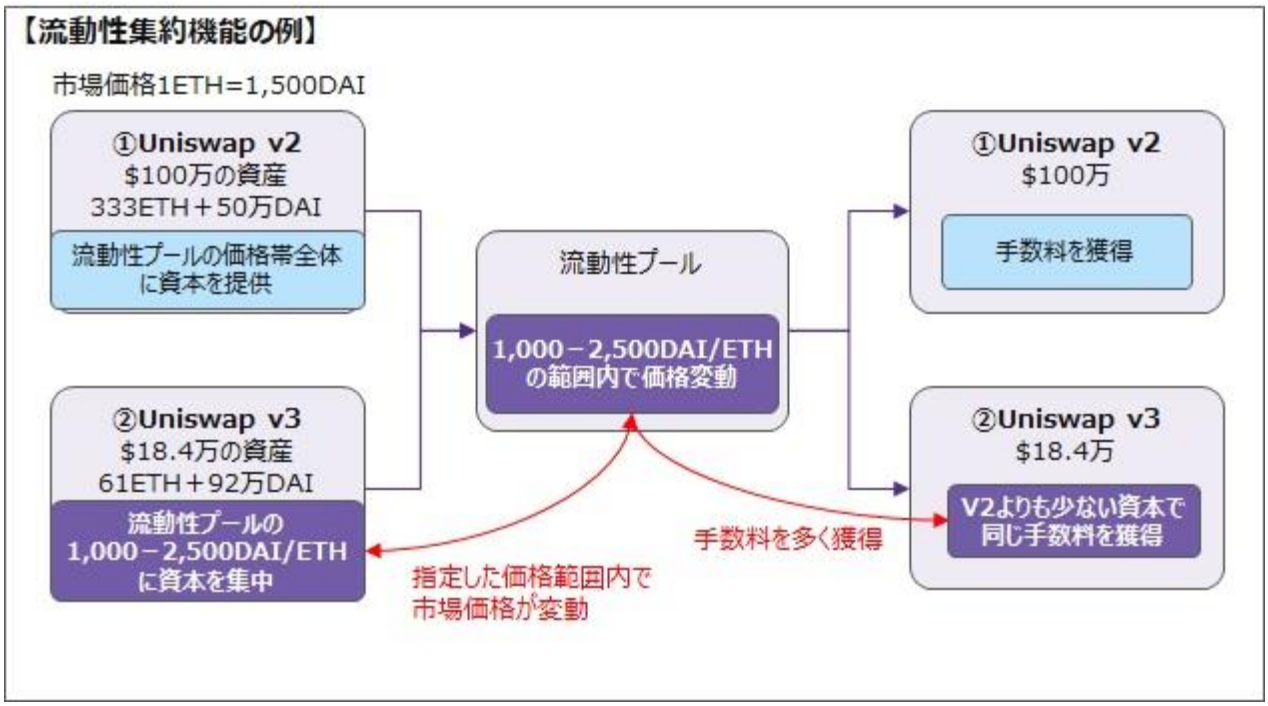

図 2-2-2-3　Uniswap：流動性集約機能（Uniswap ウェブサイトをもとに弊社作成）

【図の説明】

① Uniswap v2 は、資本を流動性プールの価格帯全体に提供する
ほとんどの流動性プールでは、この大部分が使用されることがなく資本効率が低かった。
例）DAI/USDC ペアは$0.99～$1.01 の間の取引のために、資本のわずか 0.50%しか使用しないが、最も多くの手数料を獲得する価格範囲になる。
※USDC（USD Coin）：Centre 社が発行するドル資産担保型のステーブルコイン

② Uniswap v3 は、資本を流動性プールの指定した範囲に集中して提供できる
市場価格が指定した範囲内で変動する場合は、資本が有効に使われるため、資本効率が向上する。少ない資本で多くの手数料獲得が可能になる。大幅な価格変動が生じた場合などにおいて、v3 は v2 に比べて提供する資本が小さいため、損失が小さくなるメリットがある。

(4) v3 における手数料の拡張[45]

・流動性プールおよび流動性プロバイダ毎に複数の手数料区分を提供

Uniswap v1, v2　0.3%に固定（ハードコーディングされている）
Uniswap v3　0.05%, 0.3%, 1%の 3 つから選択

・プロトコル料金スイッチを導入し、ガバナンス投票によりスイッチオンにするとガバナンストークン保有者が手数料を得ることができる（デフォルトはオフ。2022/5 現在オフの状態）

Uniswap v2　ガバナンス投票により手数料 0.3%のうち 0.05%を得る
Uniswap v3　ガバナンス投票により手数料の 10-25%の間に設定可能

[45] Uniswap v2 Overview https://uniswap.org/blog/uniswap-v2

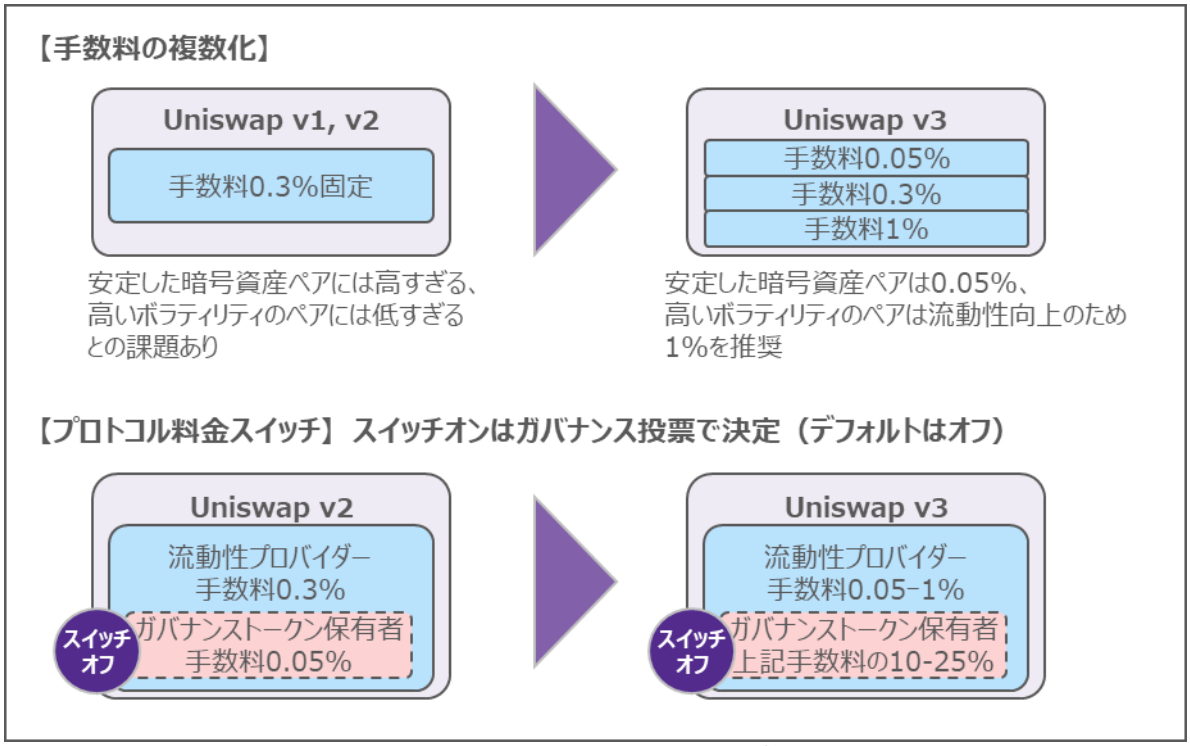

図 2-2-2-4　Uniswap 手数料の柔軟化

(5) オラクルの高度化

・Uniswap v2[46]：TWAP（時間加重平均価格）オラクル

各ブロックの開始時の市場価格を計測し、当該価格及びブロック間の生成に要した時間から、任意の暗号資産ペアの累積価格（Σ価格×ブロック生成時間間隔）を算出し、任意の２時点間の累積価格及び時間差から TWAP を計算

・Uniswap v3[47]：TWAP の効率化

過去 9 日以内の TWAP を効率的に取得できるようになり、ガス代の低減に寄与

[46] Price Oracles https://uniswap.org/blog/uniswap-v2#price-oracles

[47] Advanced Oracles https://uniswap.org/blog/uniswap-v3

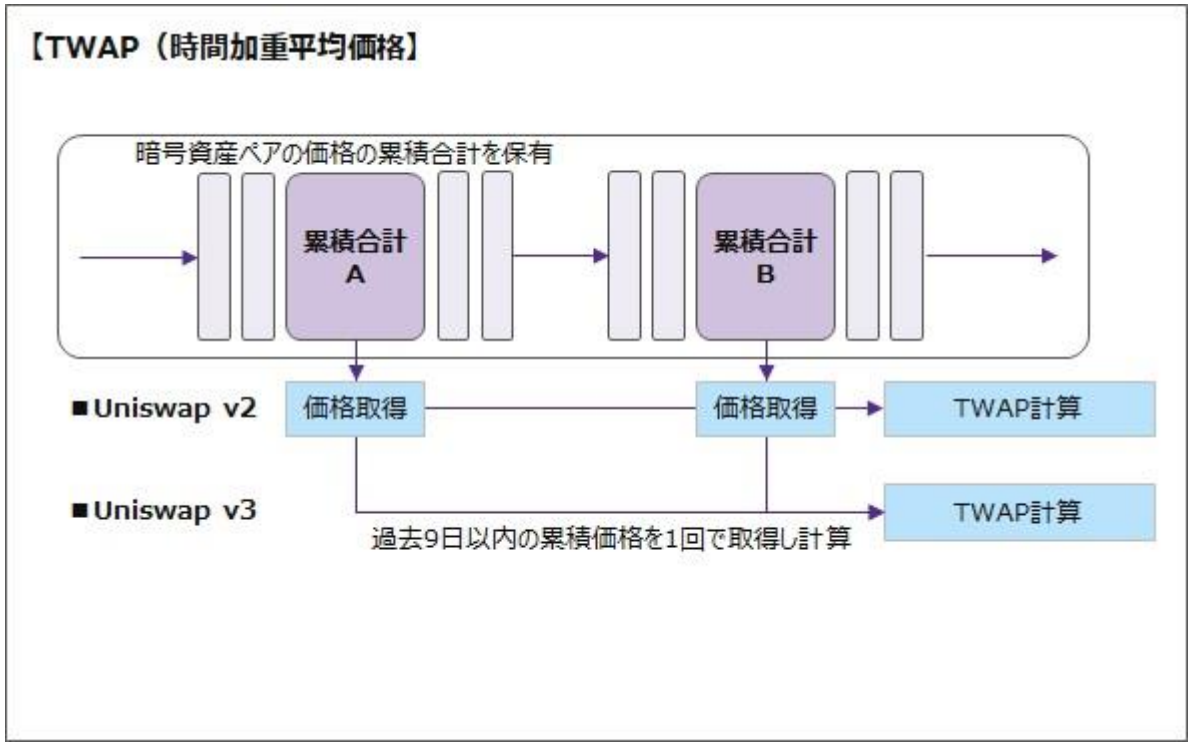

図 2-2-2-5　Uniswap オラクル

(6) スケーリング

・Ethereum のトランザクション数増加に伴うガス代高騰や処理速度低下の問題に対処するため、Uniswap v3 を Ethereum の Layer2 ソリューションおよび Ethereum 以外のブロックチェーンでもデプロイ。

表 2-2-2-6　Uniswap のデプロイ先

項目	概要	補足事項
Layer2 ソリューション	Optimism ・2021/7 の Optimism サービス開始から間もなく Uniswap v3 をデプロイ	・Optimistic Rollup のスケーリング技術により、処理速度の向上や手数料の削減が見込める ・但し、取引が完全に保証されるまで一定期間待たされる仕様のため、即時処理を行う場合はサードパーティの流動性プロバイダを利用する（手数料がかかる）などの対応が必要になる
	Arbitrum ・2021/9 の Arbitrum サービス開始から間もなく Uniswap v3 をデプロイ	・Optimistic Rollup と、独自開発したレイヤー2 ソリューションの「Arbitrum One」を利用した「Arbitrum Rollup」という手法を採用
ブロックチェーン	・Ethereum　Uniswap v1,v2,v3 ・Polygon　Uniswap v3 2019/4 に Polygon サービス開始、2021/12 に Uniswap v3 をデプロイ	・Ethereum 互換のブロックチェーンネットワークである「Polygon」を利用してスケーリングソリューションを提供する

(7) スマートコントラクトの変更（アップグレード）可能性

表 2-2-2-7　Uniswap：スマートコントラクトの変更可能性

項目	概要	補足事項
スマートコントラクトの変更可能性	(1) コアコントラクト ・Uniswap v1 設計上アップグレードが不可能（手数料を含む） ・Uniswap v2, v3 設計上アップグレードが不可能（手数料はコアコントラクトでは制御しない）	・コアコントラクト：重要なロジックが対象、最小限の設計 - 流動性プール、AMM、Flash Swap、流動性集約機能、手数料機能、オラクル機能 ・コアコントラクトのアップグレードはできないため、異なるセットを新しいバージョンとして実装し、それに併せて脆弱性の修正や機能改善を行う
	(2) コア以外の外部コントラクト 制約なく変更・追加・削除ができる（手数料の変更を含む）	・コア以外の外部コントラクト：手数料、周辺機能、インターフェース、ガバナンス投票など ・ガバナンス投票の可決を受けて Uniswap Labs が実施する

(8) ライセンス管理

表 2-2-2-8　Uniswap：ライセンス管理

項目	概要	補足事項
コアコントラクトのライセンス保護	Uniswap v3 プロトコルの商用ライセンス保護 ・Business Source License 1.1 により、ライセンスは商用または実稼働環境での v3 ソースコードの使用を最大 2 年間に制限 ・ガバナンス投票により、いつでもライセンス期間の変更や免除ができる ・ライセンス対象は、スマートコントラクト、数学ライブラリ、周辺機器コントラクト、インターフェイス、開発者 SDK を含む ・ソースコードの参照は可能 ・以前のバージョンで Sushiswap にソースコードを流用されたが、一定期間は他の流用を防止することが目的と言われている[48]	・開発した Uniswap Labs が、ソースコードのライセンス管理権限をガバナンストークン保有者に委託した形 ・再利用可とせずオープンソースでは無いことを明確化した事例

[48] https://www.coindesk.com/tech/2021/03/23/uniswap-v3-introduces-new-license-to-spoil-future-sushis/

2-2-3　金融機関との連携

表 2-2-3　Uniswap：金融機関との連携

項目	概要	補足事項
金融機関との連携	・Fintech 企業とタイアップしてコンシューマーファイナンス領域への市場参入を検討することを発表[49]	・PayPal, Robinhood（米株式運用アプリ運営） ・E*Trade（米オンライン証券会社） ・Stripe（米オンライン決済）等
	・UNI にパッシブ連動する ETP（上場投資商品）を上場[50] ⇒DeFi Technologies（カナダの Tech 企業）の子会社である Valour（スイス資産運用会社）を通して上場	・ドイツフランクフルト株式市場 ユーロ建 Valour Uniswap ETP（2021/10） ・スウェーデン株式市場 クローナ建 Valour Uniswap SEK（2021/12）
	・Sygnum Bank AG（スイスのデジタルバンク）が AAVE トークンを含む複数の DeFi トークン（ガバナンストークン）及びステーブルコイン（USDC）のカストディ、トレーディングサービスを開始することを発表 （2021/6）	・対象暗号資産：AAVE, UNI, ANT, CRV, MKR, SNX, 1INCH
	カストディおよびトレーディングサービスの開始（2021/11） ・Commonwealth Bank (オーストラリア)が Gemini Exchange、Chainalysis とパートナーシップを組んで、10 種類の暗号資産の交換（crypto exchange)とカストディサービスを開始	・Commonwealth Bank：1911 年創業 ・対象の暗号資産：BTC, ETH, BCH, UNI, LINK, MATIC, AAVE, COMP, LTC, FIL
	DeFi 関連銘柄の取引・カストディを提供（2022/1） ・Arab Bank Switzerland（スイス）が 10 種類の暗号資産のサービスを提供	・Arab Bank Switzerland：1962 年創業 ・対象の暗号資産：AAVE, FTM, COMP, SNX, LINK, MATIC, GRT, CRV, UNI, YFI

[49] https://www.coindesk.com/business/2021/07/28/uniswap-says-its-talking-with-paypal-robinhood-and-more-in-deleted-video/

[50] https://valour.com/press/valours-uniswap-exchange-traded-product-etp-goes-live-on-nordic-growth

2-2-4　ガバナンス運営

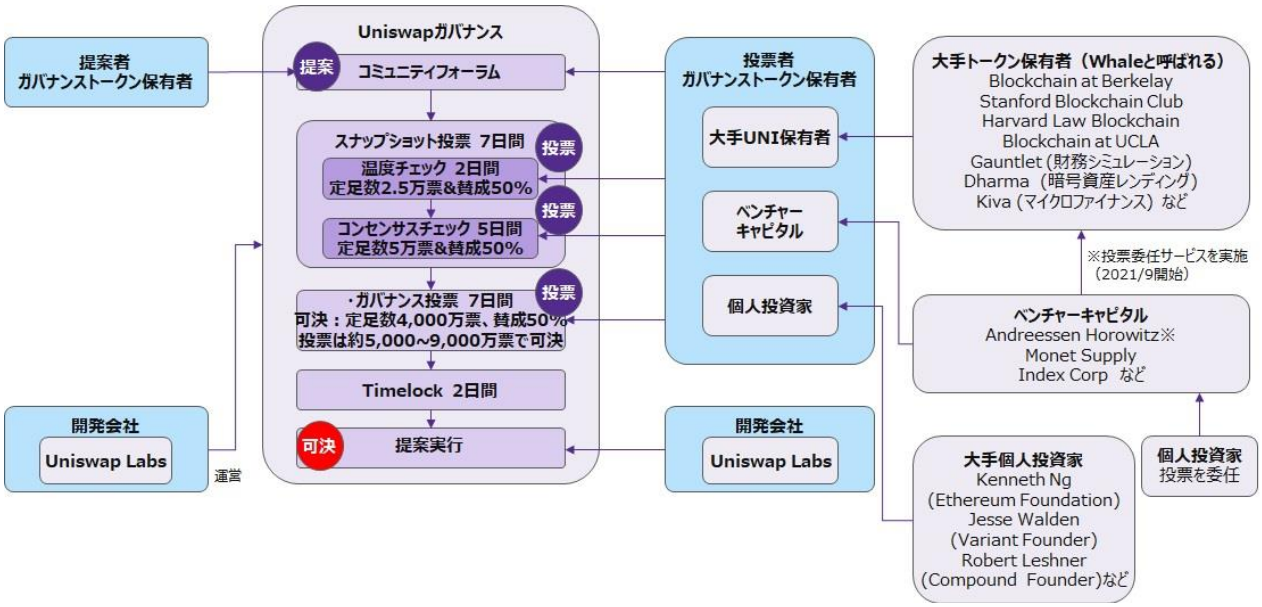

図 2-2-4　UNI を用いたガバナンス投票プロセス

(1)　コミュニティ

表 2-2-4-1　Uniswap：コミュニティ

項目	概要
コミュニティの目的（公式ドキュメントの記載を要約）[51]	・UNI（ガバナンストークン）はコミュニティ主導の成長、開発、および自己完結の目的のために導入され、コミュニティの所有権と活気に満ちた多様で専用のガバナンスシステムを可能にするもの。 ・トラストの最小化と中立性を受け入れてきており、ガバナンスが真に必要な場所に制限されることが重要 ・Uniswap ガバナンスはプロトコルの開発と使用の両方、およびより広範なエコシステムの開発に貢献することに限定される
コミュニティ形態	・ガバナンストークン UNI 保有者による分散型自律組織（DAO） 法定代表者、取締役会・理事会などの経営組織、監査役は不在

(2) ガバナンストークン（UNI）

表 2-2-4-2　Uniswap：ガバナンストークン

項目	概要	補足事項
UNI の配布	・2020 年 9 月より、4 年間で合計 10 億 UNI を配布予定 - コミュニティメンバー 60.00%　（6 億 UNI） - チームメンバー、従業員 21.266%（2 億 1,266 万 UNI） - 投資家	・既に約 5 億 UNI を配布済（2021/12 時点） ・未配布トークンはスマートコントラクトにロックされている。

[51] Introducing UNI https://uniswap.org/blog/uni

	18.044%（1 億 8,044 万 UNI） - アドバイザー 0.69%　（690 万 UNI）	
UNI 保有アドレス数[52]（2022/1 時点）	・UNI 保有アドレス数　27 万 6 千 ・1 位保有率　17.34% ・上位 10 アドレス保有率　53.42%	・投票を委任された UNI 大手保有者（Whale）の 5～7 アドレスが大きな決定権を握っているとの指摘　(Blog より)[53] ・投票方式・提案の閾値見直しが提案されたものの否決
UNI の機能	・オンチェーン投票における投票権（ガバナンストークン）	―

(3) 意思決定

表 2-2-4-3　Uniswap：意思決定

項目	概要	補足事項
意思決定方法[54]	・UNI によるガバナンス投票を以下の 2 段階で行う ①スナップショット投票 温度チェックとコンセンサスチェックの 2 回投票を行う ②ガバナンス投票 提案の実施可否を決定 投票は①②で各 7 日間、可決後に TimeLock2 日間で実行される	・スナップショット投票はオフチェーン、ガバナンス投票はオンチェーン上で実施される。 ・温度チェック：現状を変更するのに十分な意志があるかどうかを判断する ・コンセンサスチェック：提案に関する正式な議論を確立する
ガバナンス投票の可決条件	①5 万 UNI（配付予定総数の 0.005%）の賛成 ②提案：250 万 UNI（配付予定総数の 0.25%）の賛成 可決：4,000 万 UNI（配付予定総数の 4%)の定足数、投票数の過半数の賛成	・ガバナンスの運営を UNI 保有者に委ねるため、UNI の大口保有者や、UNI を市場で一時的に大量購入した匿名・仮名の者がコミュニティの意見を操作できる可能性
投票数実績（2021 年）	①35 件中 27 件を可決（可決率 77%） ②7 件中 6 件可決（可決率 86%）	・他プロジェクトに比べて提案された件数が少ない
ガバナンス投票で提案できる事項	(1)コア以外の外部コントラクトの追加・変更・削除 ・他のブロックチェーンとの連携（新規デプロイなど） ・Governor Bravo※（ガバナンス用コントラクト）の更新　など	・コアコントラクトは設計上アップグレード不可となっており、修正および停止ができない。万一脆弱性が発見された場合の対策が決められていない

[52] Etherscan Token Uniswap https://etherscan.io/token/0x1f9840a85d5af5bf1d1762f925bdaddc4201f984

[53] https://gov.uniswap.org/t/consensus-check-abolish-delegates-and-change-the-uni-governance-voting-system/13458

[54] https://docs.uniswap.org/protocol/concepts/governance/process

	(2)パラメータ値の追加・変更・削除 ・流動性プールの追加・削除 ・手数料などパラメータ値の変更 ・プロトコル料金スイッチのオン・手数料設定の変更 - 流動性プロバイダの手数料の一部を UN 保有者が徴収できる（ガバナンス投票で手数料徴収を可能とした） など	－
	(3)コミュニティ運営の変更 ・コミュニティ資金の使用（教育基金など） ・ガバナンス運営の変更（ガバナンス提案の閾値、投票方法見直し）	・大手 UNI 保有者が投票により手数料利益を誘導することが可能であり、防止策がない ・一部の UNI 保有者が結託して過半数をとると、利益が詐取される懸念がある。但し、不正が発覚すると参加者が離れて市場が縮小し、結果として自浄作用が働くとも考えられる
	(4)コアコントラクト商用利用禁止ライセンスの期間変更、免除 ・v3 はライセンスで 2 年間の商用利用禁止としたが、ライセンスの制御はガバナンス投票で変更できる	・他プロジェクトへの流用防止のため 2 年間のライセンスを導入したが、ガバナンス投票によりそれを覆すことが可能になっている

※ Governor Brabo：

・Compound で開発されたガバナンス用スマートコントラクトで、Uniswap においても導入

・ガバナンス投票により採用決定。

＜特徴＞

- Governor Brabo 自体のスマートコントラクトのアップグレードが可能
- 投票の「棄権」オプションの追加
- 投票時のコメント付加機能の追加
- 投票パラメータの設定変更が可能（投票期間、投票機関延長、定足数のしきい値）
- 提案者が自分の提案をキャンセルできる
- Guardian(ガバナンス管理者)の削除
- 提案 ID の連続番号採番が可能

(4) インシデント発生時の対応

表 2-2-4-4 Uniswap：インシデント発生時の対応

項目	概要	補足事項
インシデント発生時の緊急対応	・コアコントラクトは修正不可、かつ停止不可 ・コア以外の外部コントラクト、インターフェース、パラメータなどは、	・コアコントラクトの脆弱性が発見された場合、修正ができない ・外部から攻撃が止められない場合は、攻撃を防御できず致命的な状況になってしまう

	開発会社が緊急修正を行うことができる	
緊急対応の発動権限者	・定められたルールは特になく、明確な権限保有者は不明 - 開発会社の自己判断で緊急対応が行われる想定か	・緊急時は開発会社の判断で対応を行うことが前提になり、UNI 保有者の関与は限定的
インシデントによる損害賠償	・インシデント発生などによる損害はユーザ責任であり、賠償は行わない（Terms of Service[55]に明記されている）	・利用者に大きな損害が発生した場合、ガバナンス投票等でコミュニティ資金からの賠償が提案されることが考えられるが、大手 UNI 保有者の損害の状況により、適切な判断が行われない可能性

(5) その他

表 2-2-4-5　Uniswap：その他事項

項目	概要	補足事項
開発会社が実施できる事項	・新バージョンのスマートコントラクトのデプロイ - コアコントラクトのバージョンアップは開発会社が主導で実施	・新バージョンに搭載する新機能などは開発会社が決めるため、コミュニティの意見が反映されない懸念がある
	・コア以外の外部コントラクト、インターフェース、パラメータの修正 - ガバナンス投票で可決した事案の対応、および開発会社の判断で行うもの（ガス代削減など軽微な修正）がある	・開発会社の判断でコミュニティを通さずにコード修正ができてしまう
UNI 保有者の匿名性	・UNI 保有者は原則として匿名であり、実在する主体の特定が困難 - UNI の保有アドレスは特定できるが、KYC が行われていないため実名とはリンクできないケースが多い	・投票の決定に問題が発見されても、意思決定に関わった UNI 保有者を特定できず、決定の差し戻しや決定者の責任が問えない可能性

2-2-5　インシデント事例[56]

2020 年 4 月に発生したリエントランシー脆弱性[57]のインシデント事例について、その概要と発生理由、問題点を説明する。

(1) 発生日：2020 年 4 月 18 日

(2) 損害額：約 30 万ドル

[55] Uniswap Labs Terms of Service https://uniswap.org/terms-of-service

[56] https://peckshield.medium.com/uniswap-lendf-me-hacks-root-cause-and-loss-analysis-50f3263dcc09

[57] リエントランシー脆弱性とは、不正に再帰的な処理の実行（スマートコントラクトの処理が終了する前に同じ処理を再度呼び出すことで、例えば残高が引かれる前に何度も送金を実行させる）を引き起こす脆弱性

(3) 事件の概要

・4/18 に Uniswap が攻撃者にリエントランシー攻撃を受け、約 30 万ドルを窃取された。

・4/19 に同じ手口で別の DeFi プロトコルである Lendf.Me が攻撃され、約 2,500 万ドルが窃取された。

・Lendf.Me 攻撃後の資金移動において、攻撃者が暗号資産取引所のサービスを直接利用していたことにより、身元に関する重要なメタデータが検出された。この情報により Lendf.Me が攻撃者と交渉し、資金の 99%が返還された。

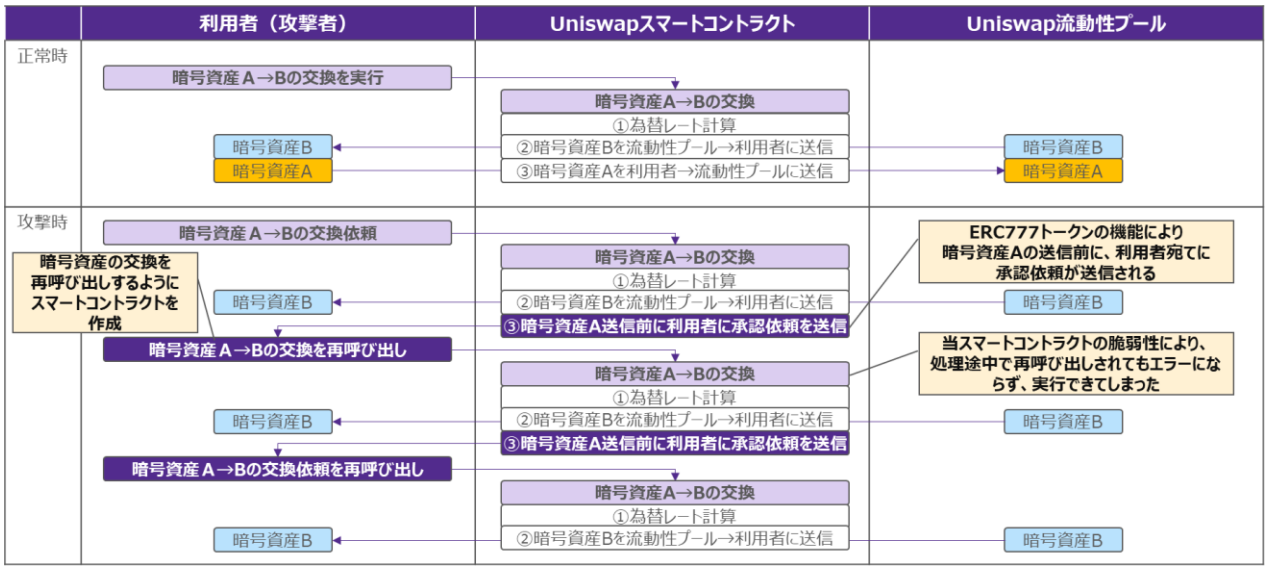

図 2-2-5-1　Uniswap リエントランシー脆弱性の仕組み

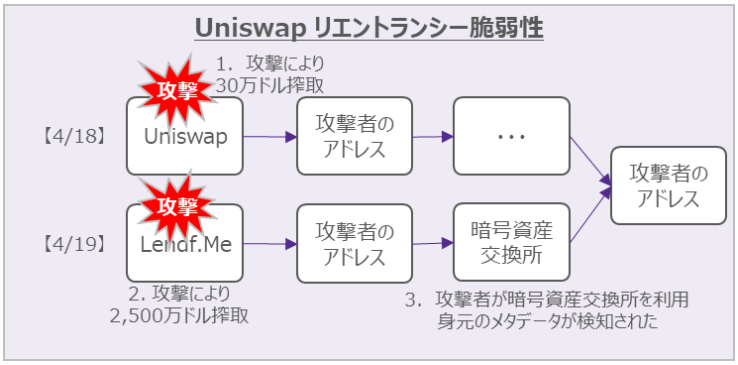

図 2-2-5-2　攻撃の概要

1. 4/18　Uniswap がリエントランシー攻撃を受け、約 30 万ドルが窃取された
2. 4/19　Lendf.Me が同じ手口で攻撃を受け約 2,500 万ドルが窃取された
3. 4/19　攻撃者が資金移動中に暗号資産交換所のサービスを直接利用し、身元のメタデータが検知された
4. 4/21　攻撃者の身元が判明し、Lendf.Me が交渉した結果、資金の 99%が返還された

(5) 窃取された資金と暗号資産

・Uniswap　約 30 万ドル　imBTC, ETH の 2 種類

・Lendf.ME 約 2,500 万ドル　WETH, USDT, HBTC, imBTC など計 12 種類

(6) 発生原因

・Uniswap および Lendf.Me のスマートコントラクトのリエントランシー脆弱性によるもの

- ERC-777 トークン対応が未整備だったことによるリエントランシー脆弱性があった。
- ERC777 トークンの承認依頼機能を悪用し、暗号資産交換の処理途中で再呼び出しを行うことで暗号資産が受け取られた。

(7) インシデントの問題点

表 2-2-5　Uniswap リエントランシー脆弱性の問題点

区分	種別	問題点の内容
現象的要因	デプロイメント	ERC777 トークンのリエントランシー脆弱性があった ・Uniswap v1 に ERC-777 トークン対応が未整備だったことによるリエントランシー脆弱性があり、攻撃者から攻撃を受けた
動機的要因	デプロイメント	ソースコードの脆弱性をコード監査で指摘されていたが、次のバージョンで修正することとし、即時に対応をしていなかった ・2018/12 の ConsenSys 社コード監査報告（即時公開）[58]で本件を指摘されていた - 重要度：メジャー（4 段階中クリティカルの次に重要度の高いランク。） 監査報告では計 7 件の指摘があり、本件指摘が重要度が一番高かった。 3.1 Liquidity pool can be stolen in some tokens (e.g. ERC-777) ・事件発生前に本件の脆弱性の指摘を受けていたが、コアコントラクトの修正ができないため、次バージョンで対応する計画であった。 - Uniswap v1 のコアコントラクトは修正できないため、ERC777 トークンを受け付けないよう対応した。（詳細は不明） - 脆弱性の修正は v2 で実施済。
	ガバナンス	コード監査で脆弱性の指摘を受けたが、コアコントラクトの仕様上コード修正ができなかった。 ・コード監査の結果報告は Uniswap Labs (CEO の Hayden Adams 宛て) に報告されており、脆弱性は開発会社経営陣も認識していたと考えられる。

2-2-6　Uniswap の主なトラストポイント

(1) Uniswap Labs（開発会社）

・米 NY 州に拠点を置き、Uniswap プロトコルや各種ツールの開発・管理に加え、ユーザインターフェース（ウェブサイト等）の運営を行っているものと考えられる

・当社で Community lead の採用を計画している こと等を踏まえると、Uniswap コミュニティの運営に一定程度の影響力を持つものと想定される

・ガバナンス投票で可決された提案を実行するためには、Uniswap Labs の承認が必要と考えられる。

(2) ベンチャーキャピタル

・初期投資家に UNI の約 18%が配布されており、ガバナンス投票において強い影響力を有する投資家が存在すると考えられる。

[58] ConsenSys Uniswap-audit-report-2018-12 https://github.com/ConsenSys/Uniswap-audit-report-2018-12#31-liquidity-pool-can-be-stolen-in-some-tokens-eg-erc-777-29

(3) コード監査会社

・ユーザはコード監査会社による監査結果を信頼してプロトコルを利用しているものと想定される。

(4) ウォレット提供者

・（Uniswap に限らず DeFi 全般について、）Metamask など少数のノンカストディアル・ウォレットを多くのユーザが使用しており、ウォレットに脆弱性が存在した場合の影響度は大きいと考えられる。

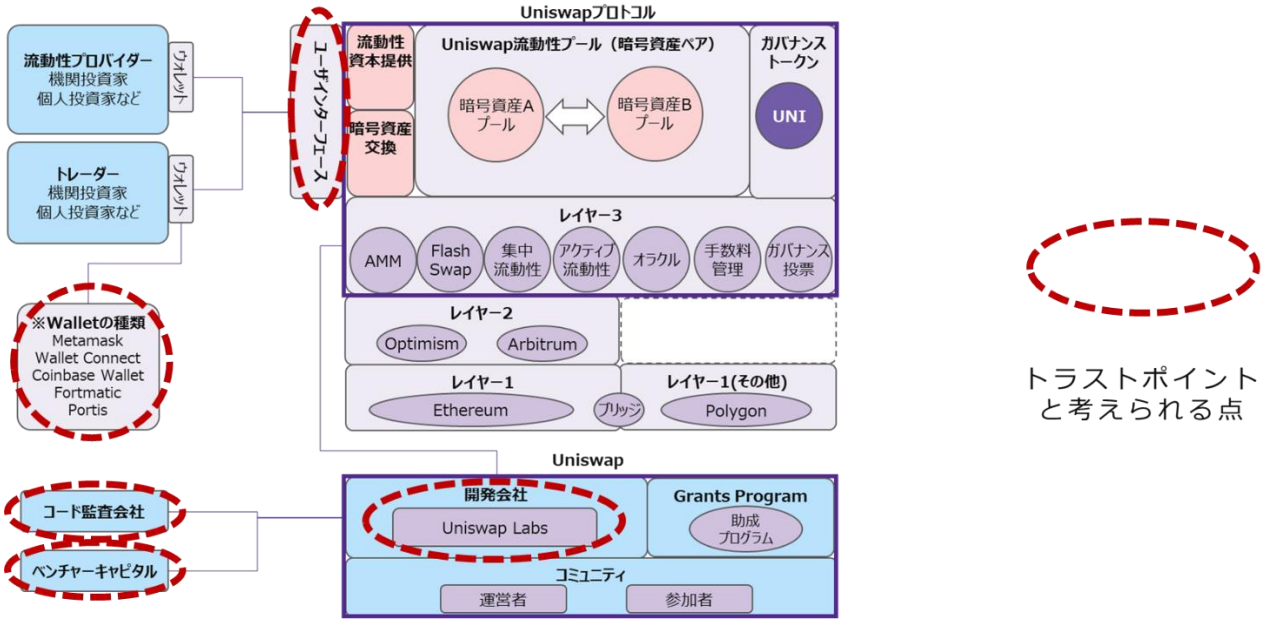

図 2-2-6-1　Uniswap の主なトラストポイント（構成要素）

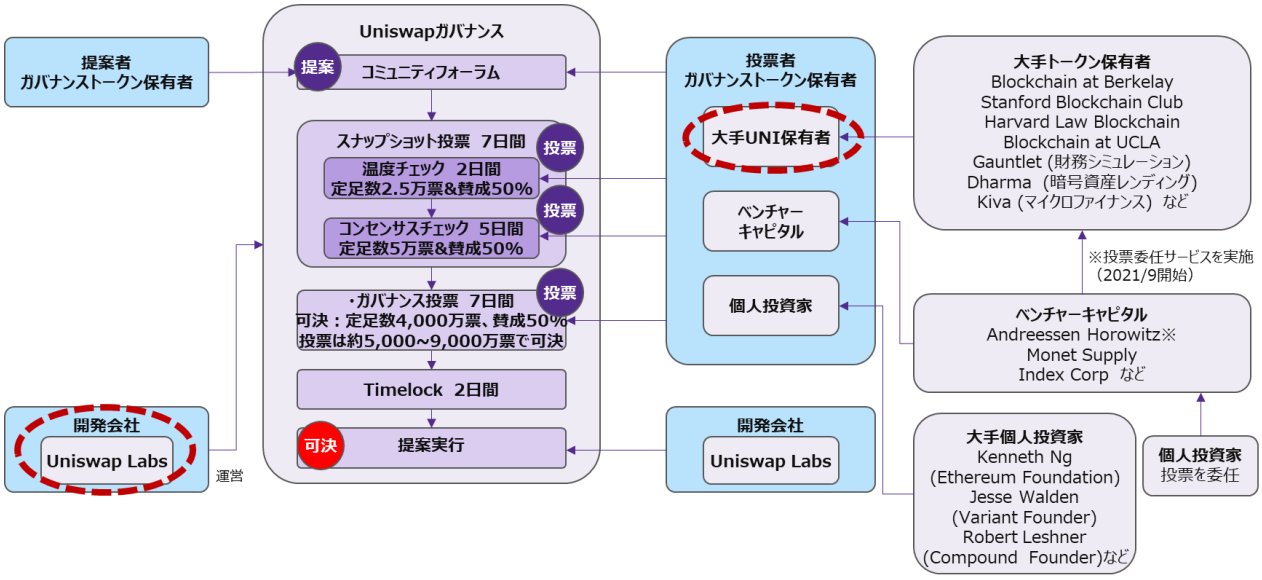

図 2-2-6-2　Uniswap の主なトラストポイント（ガバナンス投票）

2-3　ステーブルコイン　Maker（DAI）の分析

Maker を調査対象として、プロジェクト概要や運営組織、主な技術特性、ガバナンス運営、インシデント事例について調査研究を行った。Maker は創設会社の Maker Foundation が解散して MakerDAO に移行したこと、および DAO 運営に関して役割別にチームの組成やルールを制定していること、金融機関等と連携して実世界への展開を積極的に行っているなどの特徴がある。各項目の調査により実態を明らかにし、課題・問題点やリスク事項を分析する。

2-3-1　プロジェクト全体概要

Maker の主な構成要素とそのマッピング、コミュニティ概要は下図・表の通り。

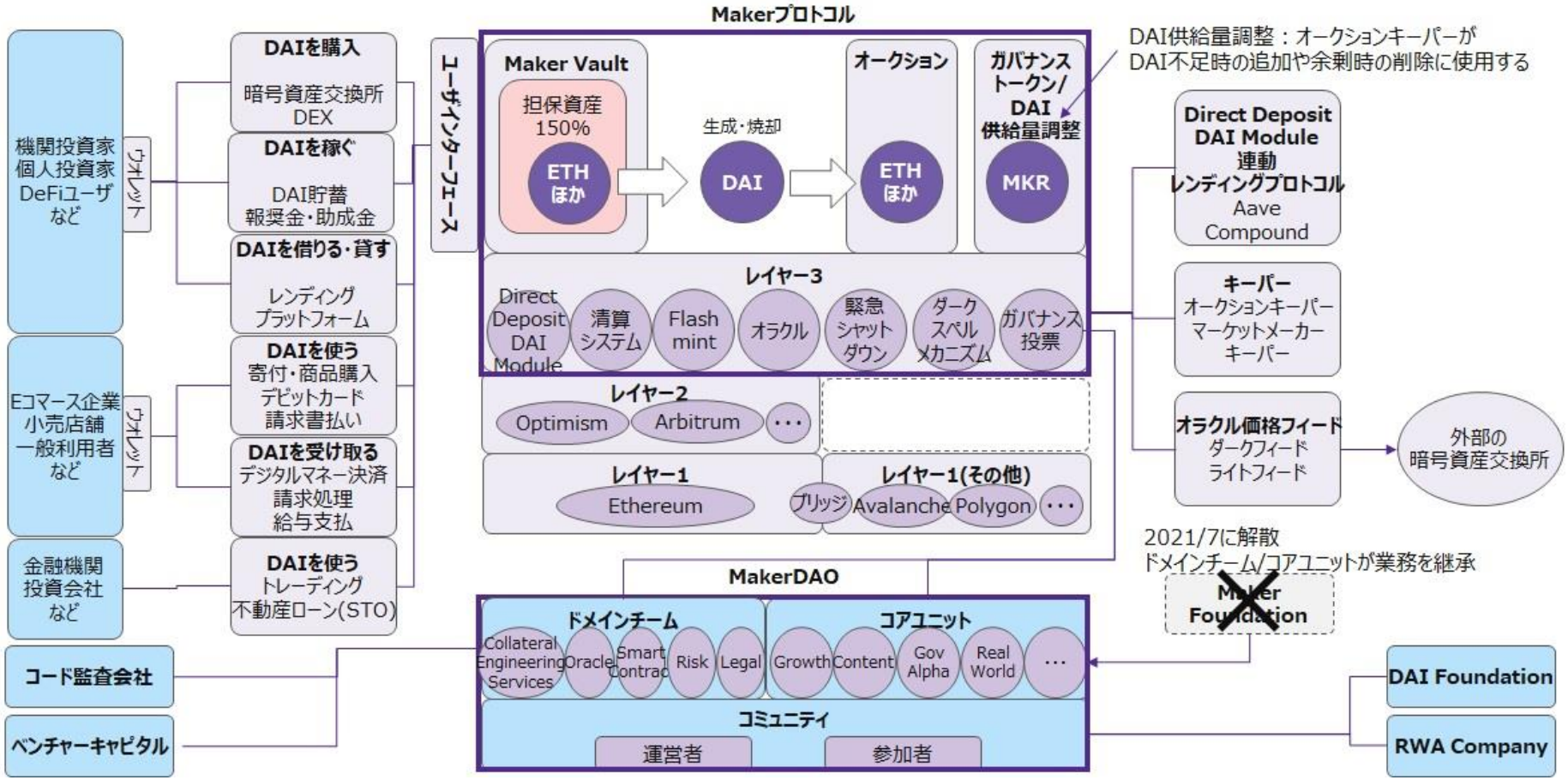

図 **2-3-1-1　Maker** の主な構成要素

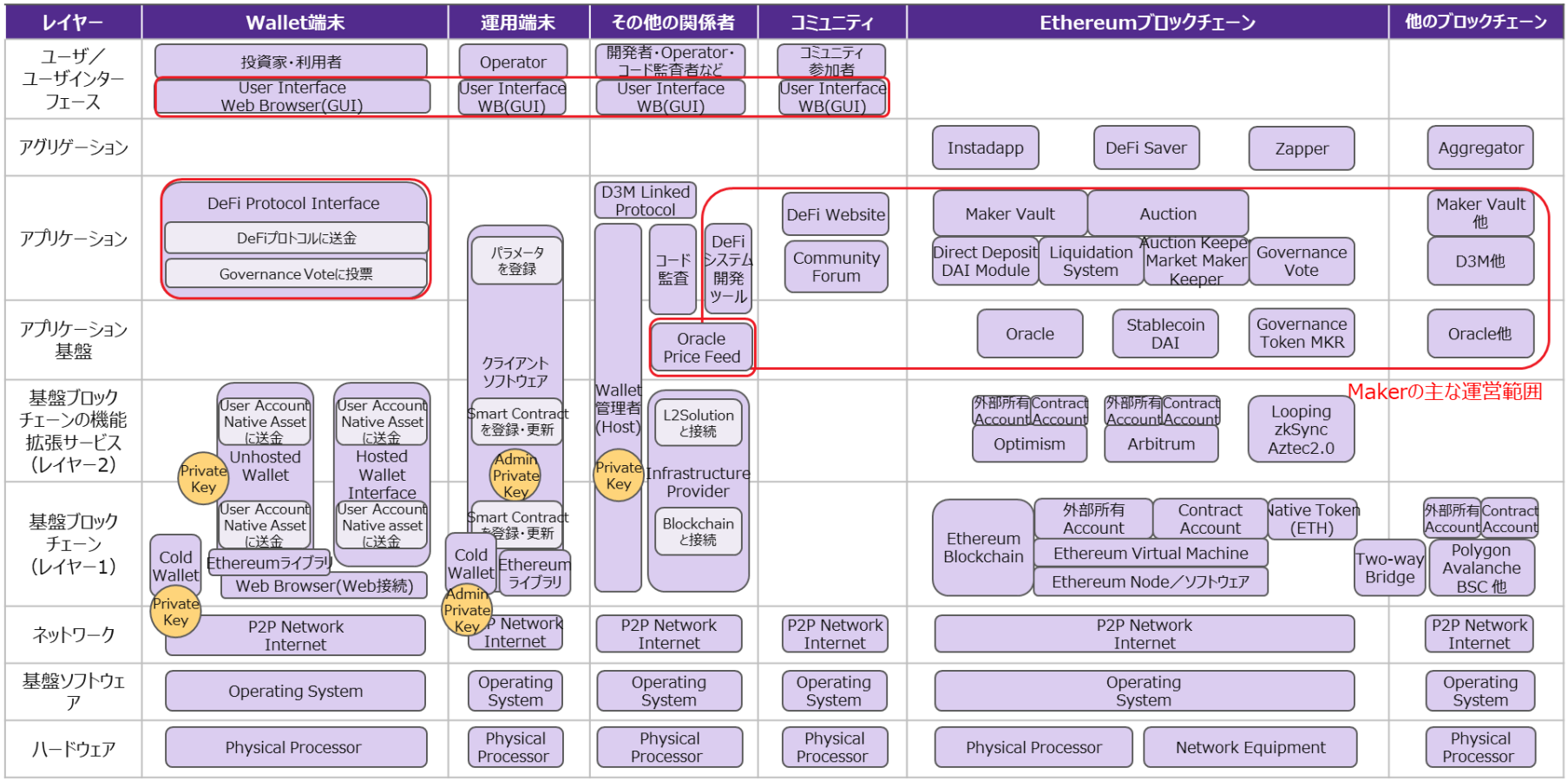

図 2-3-1-2　Maker の主な構成要素のマッピング

表 2-3-1　Maker：コミュニティ・関連法人

項目	概要	補足事項
コミュニティ（MakerDAO）	MakerDAO ・ガバナンストークン MKR 保有者によるオンチェーン投票：8 万 3 千アドレス ・MakerDAO の運営チームは以下の 2 つあり	・創設 2014/12 ・拠点：米カリフォルニア[59] ・創設者：Rune Christensen ・2021/7 に Maker Foundation（デンマーク）を解散し、同財団の資産を MakerDAO に移し、高度な分散型自律組織へ移行。
	(1)ドメインチーム（2022/5 時点）[60] ・担保資産の追加やオラクルメカニズムの設計などを行う ①担保エンジニアリングサービスチーム 新しい担保の導入およびメンテナンスプロセスの管理など ②オラクルチーム 新しい担保タイプのオラクルフィードメカニズムの設計など ③スマートコントラクトチーム 新しい担保のアダプター開発・デプロイなど ④リスクチーム 追加提案が行われた担保タイプに係るリスク分析など ⑤リーガルチーム 担保の合法的な作業成果物を作成など ・各チームのファシリテーター、コントリビューターが運営をリードする	・ドメインチームは、MakerDAO と契約した独立した個人などで構成される ・オンチェーン投票でドメインチームの組成や人選が承認される ・各チームの業務は Maker Foundation から継承されたもの ・ドメインチームの多くが Maker Foundation から継続してコード開発やオペレーションに携わっていると思われるため、現時点の品質リスクは低いと想定
	(2)コアユニット（2022/5 時点）[61] 計 22 チームで、各チームのファシリテーター 1 名が運営をリードする ・Real-World Finance ・Risk ・GovAlpha ・Protocol Engineering ・Growth ・Sustainable Ecosystem Scaling ・Oracles ・Governance Communications ・Dai Foundation ・StarkNet Engineering ・Collateral Engineering Services	・コアユニットは、MakerDAO と契約した独立した個人などで構成される ・オンチェーン投票でコアユニットの組成や人選が承認される ・各ユニットの業務は Maker Foundation から継承されたもの ・コアユニットの多くが Maker Foundation から継続してコード開発やオペレーションに携わっていると思われるため、現時点の品質リスクは低いと想定

[59] https://www.crunchbase.com/organization/makerdao

[60] MIP7: Onboarding and Offboarding Domain Teams (Collateral Onboarding) https://mips.makerdao.com/mips/details/MIP7#sentence-summary

[61] MIP38: DAO Primitives State https://mips.makerdao.com/mips/details/MIP38#makerdao-shop-mds-001-

	・Development and UX ・Strategic Happiness ・Data Insights ・Deco Fixed-Rate ・Immunefi Security ・Sidestream Auction Services ・Strategic Finance ・TechOps ・EVENTS ・Content Production ・MakerDAO Shop	
関連法人	RWA Company LLC[62] ・伝統的なクレジット市場と MakerDAO を接続することで、Maker プロトコル（Maker Vault）で Dai を生成する際の担保を暗号資産から実在の資産に拡張することを目指す。 - Maker コミュニティの代表組織として、クライアント（ローン組成者等）が、Maker Vault を通じて低い資本コストで資金（Dai）を借り入れられるように支援 - 契約主体となることが困難な DAO に代わって、クライアントとの各種契約の締結等を行う - MKR 保有者に対しては、レポートを提供するなどして透明性を確保	・2021/5 創設 ・拠点：ケイマン諸島（同国財団会社法に基づく） ・CEO：Gregory Di Prisco（元 Maker Foundation ビジネス開発リード）
	DAI Foundation[63] ・Maker コミュニティの知的財産（商標、ドメイン名、ソフトウェア、SNS アカウント等）を保護するための法人 ・2020 年初頭に Maker Foundation が Maker 及び Dai の商標権を移譲。	・2020/1 創設 ・拠点：デンマーク[64] ・会長：Solen PeterNielsen（Maker foundation の元プロダクト責任者） ・理事会は 6 名で運営

2-3-2　主な技術特性

(1) Maker Vault[65]

・Maker Vault コントラクトに担保資産（ETH 等の暗号資産や USDC 等のステーブルコイン）を預け入れることで、ステーブルコイン DAI が生成される

・DAI の返却時に安定化手数料（Stability Fee）が発生。同手数料は Maker プロトコル内のバランスシートに蓄積され、閾値を超過した場合は超過オークション（Surplus Auction）で DAI

62 RWA Company https://www.rwa.company/

63 The DAI Foundation https://daifoundation.org/

64 Announcing the Dai Foundation https://forum.makerdao.com/t/announcing-the-dai-foundation/1046

65 Makerdao Whitepaper Maker Vaults https://makerdao.com/en/whitepaper/#maker-vaults

と MKR の交換が行われ、入札に使われた MKR は焼却される

・Oasis[66]やコミュニティによって構築されたインターフェース（Instadapp, Zerion, MyEtherWallet など）により Maker Vault への簡易なアクセスが可能

・担保資産の価格下落等により担保資産が清算比率を下回った場合は、担保オークションにより自動（強制）清算される

・清算比率は担保資産毎にオンチェーン投票で選択される。ETH の場合は 150%前後、USDC は 101%など[67]。

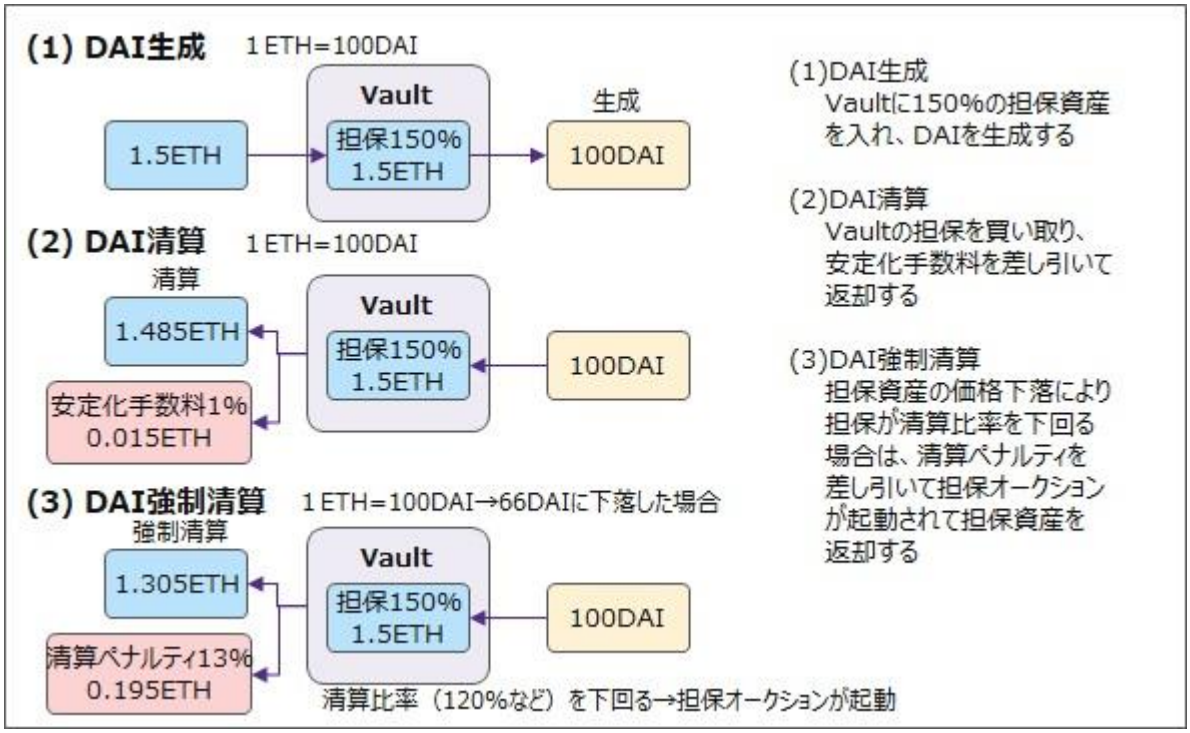

図 2-3-2-1　Maker Vault の概要

(2) ステーブルコイン DAI[68]

・ETH からステーブルコイン DAI、または DAI から ETH への変換を行う。

・ETH は ERC20 トークンではないため、Maker プロトコル内の ERC20 内部トークンに変換した後に他との取引を行う

・Vault 担保ルールへの資金預入、および Auction による清算は、外部市場価格に影響されないよう Maker プロトコル内部トークンを用いて資金の交換を行う

表 2-3-2-2　Maker：ステーブルコイン DAI の概要

項目	概要	補足事項
DAI の生成	・過剰担保を Maker Vault にロックすることで発行される Dai（暗号資産担保型ステーブルコイン）を生成 - MCD：Multi Collateral DAI　複数の担保資産をサポート	・Vault に預ける担保は担保資産により異なる。担保比率（清算比率）が 150%の場合は、100DAI 生成のために最低 150USD 相当の担保が必要

66 https://oasis.app/

67 https://daistats.com/#/collateral

68 https://makerdao.world/en/learn/Dai

	・USD にソフトペッグされている 1DAI＝1USD ・DAI 貯蓄率（DSR）はオンチェーン投票で決定する	・サポートする主な担保資産と、担保層総額に占める各資産のシェア[69] - USDC（51.5%） - ETH（22.3%） - WBTC（6.6%） - USDP（5.3%） （2022/4 時点）
DAI の購入	・暗号資産交換所で法定通貨と交換 ・暗号資産交換所で暗号通貨と交換 ・DEX で交換 - Uniswap, 1inch Exchange など ・P2P マーケットプレイスで交換 - Local Cryptos, Local Bitcoins, Bisq など	―
DAI を稼ぐ	・金利収入 - 保有する DAI を DSR（DAI 貯蓄率）コントラクトラクトにロックすることで金利を獲得 - Oasis ポータル、または Maker プロトコルへの様々な接続方法を介してアクセスする - DAI 貯蓄率に関するパラメータは、オンチェーンガバナンスで決定 - DAI が 1USD を超えると MKR 保有者は DSR を引き下げて需要を減らし、1USD 未満なら MKR 保有者は DAI を引き上げて需要を刺激するようにインセンティブが働く ・報奨金 - バグ・バウンティ（プロトコルのバグを見つけた者に対して報奨金を支給）など ・助成金 - Maker の開発助成プログラム（Gitcoin Grants など） ・レンディングプラットフォーム等での貸付 - Compound、AAVE、dYdX などのプラットフォームで DAI を貸し付け ・ハッカソン - MakerDAO ハッカソンイニシアチブなど ・ビデオゲームトーナメント	―

[69] https://daistats.com/#/overview

	- Axie Infinity（トーナメント報酬）	
DAI を借りる	・Maker もしくはサードバーティのレンディングプラットフォーム等での借入 - Oasis Borrow、Compound、AAVE、dYdX などのプラットフォームで所要の担保を差し入れた上で DAI を借入れ	―
DAI を使う	・チャリティへの寄付 - ユニセフ、NeedsList（災害支援）、PoolDai（慈善団体寄付基金）など ・オンラインでの商品購入（e コマース） - OpenSea（NFT）、Decentraland（仮想空間上の土地）、Gods Unchained（デジタル商品）など ・DAI デビットカード - Crypto.com、Fold App（ビットコイン購入）、 Monolith（VISA デビットカードとノンカストディアル・ウォレットを接続）、Wirex など ・ゲーム・ギャンブル - CelerX（e スポーツ）、Pool Together（宝くじ） ・ギフトカードの購入 - Bidalli ・請求書支払 - Gold Plus Energy（米テキサス・電気代支払い）、 living Room of Satoshi（豪）	暗号資産市場だけでなく、実社会での使用が徐々に増加している可能性
DAI を 受け取る	・Coinbase コマース（デジタルマネー決済） ・Ching-Store（モバイルストア） ・Request Network（請求処理） ・GILDED（オンチェーンの会計サービス）	―
DAI による 給与支払	・Whisp Money（KYC を使用しない給与ソリューション） ・Sablier	・一部のコミュニティ（Concource Open Community）では国外からのリモート勤務など身元の保証が困難な外部雇用者に DAI で給与支払を行っている

【参考：ステーブルコイン DAI の変換】[70]

① ETH→WETH
ETH は ERC20 トークンではないので、ERC20 トークンの WETH（Wrapped ETH）に変換して、他と取引できるようにする。1ETH＝1WETH

② WETH→PETH
WETH を PETH（Pooled ETH）に変換し、Vault に担保としてプールする。
PETH は MakerDAO 専用の暗号資産　Maker の内部レートにより変換
（1WETH＝1.04PETH など）。

③ PETH→DAI
PETH を元に DAI を生成する。レートにより変換する（DAI/ETH 市場価格より）。

④ DAI→SIN
DAI を清算する際は、SIN に変換してから清算される。1DAI＝1SIN

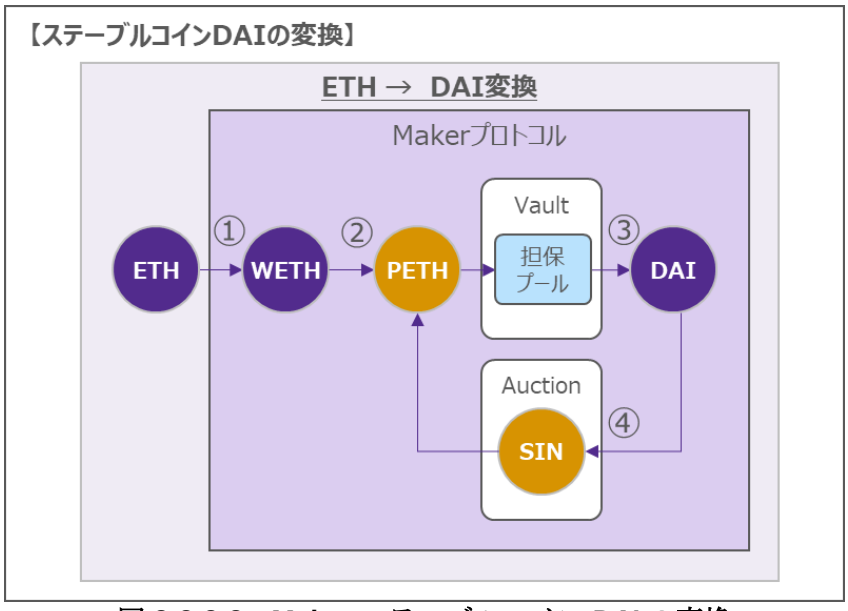

図 2-3-2-2　Maker ステーブルコイン DAI の変換

(3) Direct Deposit DAI Module（D3M)[71]

・サードパーティのレンディングプロトコルと連動して、当該プロトコルの流動性プールに DAI を効率的に移転することで、DAI の変動金利が Maker ガバナンス（ガバナンス投票）で決定された目標金利以下となるように調整するメカニズム

・目標金利が確実に達成されるように、DAI を自動的に預入/引出

・Aave、Compound に適用済。Maple に適用検討中（投票中）（2022/3 時点）

[70] MakerDAO Tokens Explained: DAI, WETH, PETH, SIN, MKR. Part 1 https://medium.com/coinmonks/makerdao-tokens-explained-dai-weth-peth-sin-mkr-part-1-a46a0f687d5e

[71] Maker Direct Deposit Dai Module（D3M） https://governance.aave.com/t/the-maker-direct-deposit-dai-module-d3m/3514

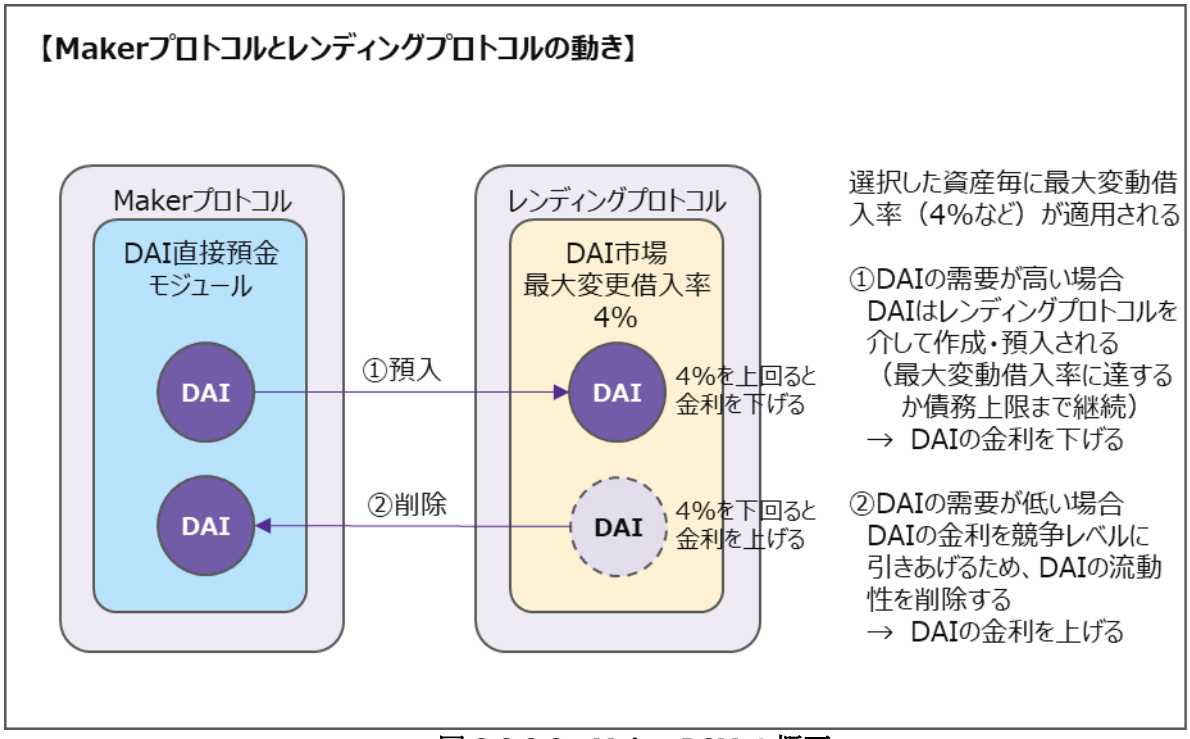

図 2-3-2-3　Maker D3M の概要

(4) 清算システム 2.0[72]

・所定の担保比率を下回り強制清算に移行した際に、担保不足となった Vault に預けられていた担保資産をオークションにかけて負債（DAI）の清算を行う仕組み。オークション参加者は DAI を入札することで担保資産を取得する

・2021/4 にローンチしたダッチオークション方式の新たな清算メカニズム
担保が購入されるまでオークションの入札額が引き下げられる

・部分入札を可能とし、オークション額を 1 人または複数の入札者が提示価格を分割して担保を購入できる

・Flash Loan をサポートし、元手がなくても借入と返済を同時に行うことでオークションに参加が可能となる

・オークション入札時間や入札額引下率はオンチェーン投票で選択される

[72] Maker Protocol Technical Docs Liquidation 2.0 Module https://docs.makerdao.com/smart-contract-modules/dog-and-clipper-detailed-documentation

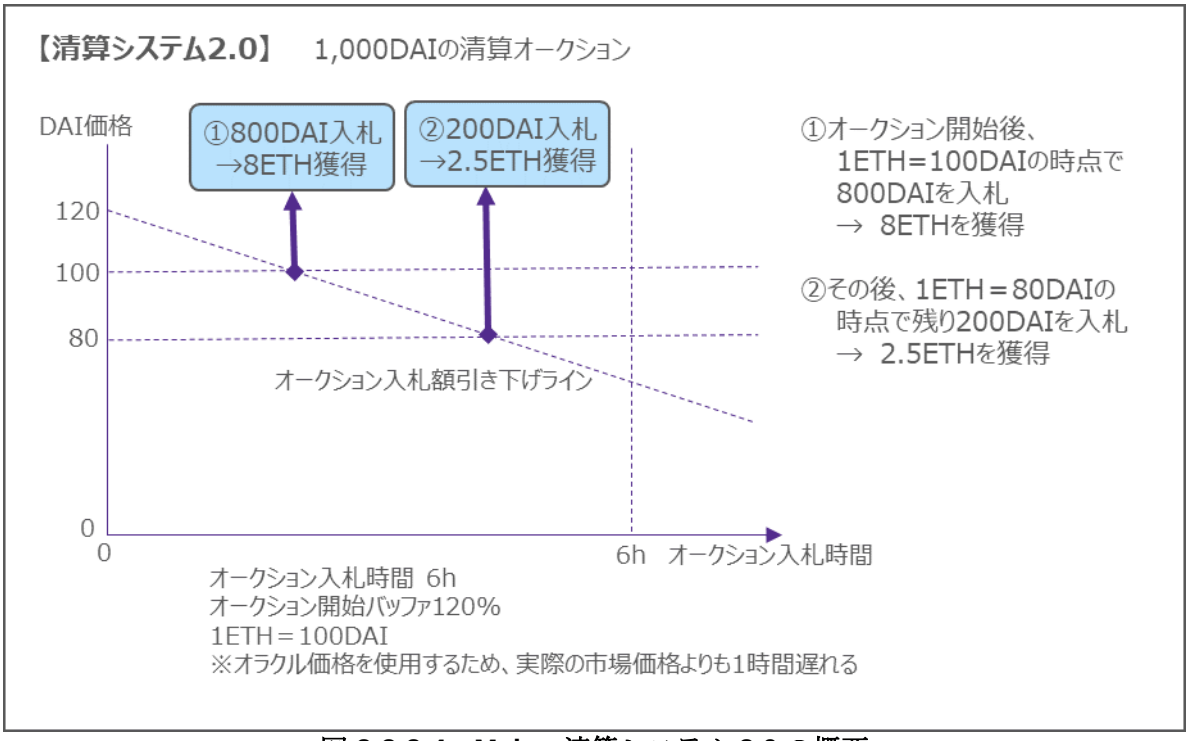

図 2-3-2-4　Maker 清算システム 2.0 の概要

(5) オラクル管理[73]

- Maker プロトコルは、ETH/USD 等の必要な市場価格について、オラクル価格フィードから受け取る価格群（Aave, Compound, Uniswap など外部の 24 の市場価格を参照[74]（2022/4 時点））から中央値を算出し、担保清算に必要な参照価格を決定する
- オラクルセキュリティモジュール（OSM）により、価格反映を意図的に 1 時間遅らせることで、相場の急激な変動やオラクル攻撃への対応を行っている（例えば、担保資産価格が大幅に下落した際に、清算回避のために追加担保の差し入れ等の措置を取ることが可能）。
- 参照する価格フィード先などはオンチェーン投票で選択される。

[73] Makerdao Community oracle https://github.com/makerdao/community/blob/master/faqs/oracles.md

[74] MIP10c17: Subproposal for List of Feeds https://github.com/makerdao/mips/blob/master/MIP10/MIP10c17-List-of-Feeds.md

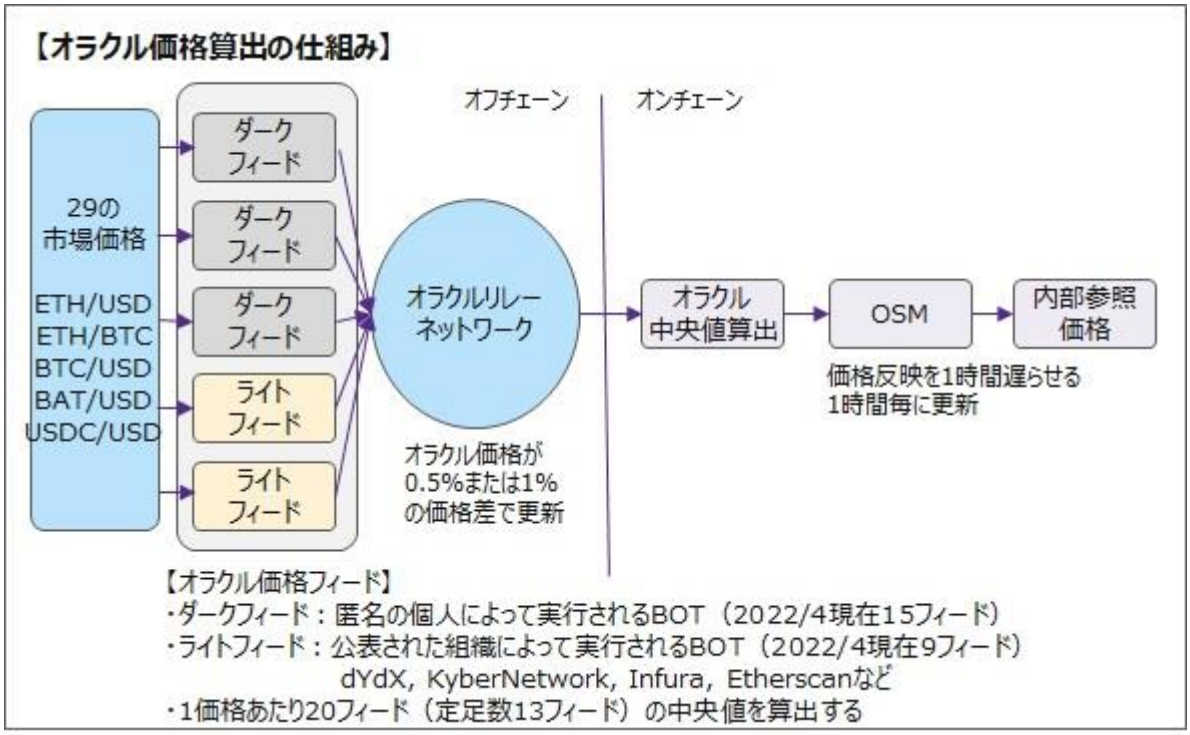

図 2-3-2-5　Maker オラクル管理の概要

(6) Maker プロトコルオークション

・強制清算時、Maker プロトコルは清算された Vault 担保を取得し、オークションメカニズムを使用してそれを販売する

表 2-3-2-6　Maker：プロトコルオークションの概要

項目	概要	補足事項
Maker プロトコルオークション[75]	①余剰オークション DAI が Maker バッファーの上限額を超える場合、超過分の DAI を余剰として MKR トークンを買い取り、MKR トークンの量を減らす ②債務オークション 未払いの債務がある場合に DAI が不足すると、MKR トークンを発行して入札者に売却し、DAI を確保する ③担保オークション トークン価格の下落などで担保不足の場合に、清算ペナルティを徴収して担保を強制清算する	―

[75] Maker Protocol Technical Docs The Auctions of the Maker Protocol Auctions https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol

(7) キーパー

表 2-3-2-7　Maker：キーパーの概要

項目	概要	補足事項
キーパー[76]	キーパーはアルゴリズムに従いアービトラージのために自動的に動く外部エージェント（主に BOT） ・マーケットメーカーキーパー - DAI が目標価格（1USD）を上回った時に DAI を販売し、下回った時に DAI を購入する。指定された 24 取引所（Binance, Coinbase など）がキーパーを構築できる[77] ・オークションキーパー - 余剰・債務・担保オークションに参加し、入札を行う	・マーケットメーカーキーパーは、指定された取引所の市場価格を参照して自動的に取引を行う ・マーケットメーカーキーパーは、指定された取引所の市場価格を参照して自動的に取引を行う

(8) Flashmint

表 2-3-2-8　Maker：Flashmint の概要

項目	概要	補足事項
Flashmint[78]	・1 トランザクションで借入と返却（手数料を含む）を行う条件で DAI を作成できる ・担保不要でアービトラージの機会が利用できる	・債務上限額の設定がある（DAI/ETH：150 億 ETH など）

(9) DAI 貯蓄率（DSR）

表 2-3-2-9　Maker：DAI 貯蓄率の概要

項目	概要	補足事項
DAI 貯蓄率（DSR）[79]	・任意の DAI 保有者が貯蓄により利子を獲得できる ・Oasis Save ポータル、または Maker プロトコル各 GW を介してアクセスする ・DAI 保有者が得る金額を決定するパラメータは、オンチェーンガバナンスで決定する	―

[76] Maker Protocol Technical Docs The Auctions of the Maker Protocol Keepers https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol

[77] MakerDAO market-maker-keeper https://github.com/makerdao/market-maker-keeper

[78] Maker Protocol Technical Docs Flash Mint Module https://docs.makerdao.com/smart-contract-modules/flash-mint-module

[79] Makerdao whitepaper The DAI Saving rate https://makerdao.com/en/whitepaper/#the-dai-savings-rate

	・DAI が 1USD を超えると MKR 保有者は DSR を引き下げ、1USD 未満なら MKR 保有者は DAI を引き上げる	

(10) GSM（Governance Security Module）

表 2-3-2-9　Maker：GSM の概要

項目	概要	補足事項
GSM[80]	・GSM により、ガバナンス投票による提案可決後のコード修正などの執行が一定時間待たされる ・システムに加えられる変更を確認し、それらの変更が悪意があると見なされた場合は、GSM 遅延時間の間に提案キャンセル（コアチームが実施すると考えられる）や Emergency Shutdown（MKR 保有者が投票）による対応を行う	・GSM 遅延時間は 48 時間（2022/1 時点）

(11) Dark Spell Mechanism

表 2-3-2-10　Maker：Dark Spell Mechanism の概要

項目	概要	補足事項
Dark Spell Mechanism[81]	・重大な脆弱性の修正を行うためにスマートコントラクトを修正する仕組み ・ダウンタイムなしでプロトコルの修正を適用する ・作業のプロセス ①ダークスペル（修正コード）を MakerDAO のスマートコントラクトドメインチームが開発 - 修正コード適用前のオンチェーン投票や GSM 遅延期間中に、リバースエンジニアリングで内容を読み取られないよう、修正反映までコードを秘匿） ②コミュニティの特定者と信頼できるサードパーティにダークスペルを伝達 ③信頼できるサードパーティが迅速に議論を調整し、投票を認識	・利害関係者 - スマートコントラクトドメインチーム - ガバナンスファシリテーター - 信頼できるサードパーティ（オンチェーン投票で選定。現在は登録なし） - Maker コミュニティの特定の者（非公表） ・通常のガバナンス投票やエグゼクティブ投票とは異なるプロセスで行われる - 投票時間は 24 時間に設定（固定） - 投票の定足数や可決の閾値は定義されていない

[80] Makerdao whitepaper Governance of the Maker Protocol https://makerdao.com/en/whitepaper/#use-of-the-mkr-token-in-maker-governance

[81] Makerdao MIP15: Dark Spell Mechanism https://mips.makerdao.com/mips/details/MIP15#sentence-summary

	④信頼できるサードパーティがガバナンスファシリテーターに投票を指示 ⑤投票がスケジュールされ、通過した後に GSM 遅延期間を待つ ⑥GSM 遅延期間経過後、コード修正を適用する ⑦信頼できるサードパーティとスマートコントラクトドメインチームが、ダークスペルの事後分析を作成し、コミュニティ全体に公表する	

(12) 緊急シャットダウン

表 2-3-2-12　Maker：Emergency Shutdown の概要

項目	概要	補足事項
緊急シャットダウン[82]	・悪意のある攻撃から Maker プロトコルを保護する、または Maker プロトコルのアップグレードを容易にするためにプロトコルをシャットダウンする機能。 ・MKR 保有者が MKR を緊急シャットダウンモジュール（ESM）に預け、閾値を超えると即座に実行される ・実行は 3 フェーズで行われ、その後、発生要因に応じて再展開が行われる ①Maker プロトコルがシャットダウン ・オラクル価格フィードが凍結され、Vault 所有者が資産を引き出す ②緊急停止後のオークション処理 ・シャットダウン開始後、担保オークションによる強制清算が開始され、全てのオークションが終了した後にプロトコルが停止する ③DAI 保有者が残りの担保を請求する ・DAI 保有者は固定レートで直接担保を請求する ・Vault 保有者が DAI 保有者よりも優先される ④攻撃の内容に応じてプロトコルを再デプロイする ・ガバナンス攻撃 攻撃者を無効にして、他はそのままで再デプロイする ・オラクル攻撃	・緊急シャットダウン開始の閾値は 75,000MKR（2022/1 時点） ・ブラックスワンイベント：重大な奇襲攻撃 オラクル攻撃など高度に調整された外部からの価格操作など対策が難しく、直接の回避策がない

[82] Makerdao Whitepaper Emergency Shutdown https://makerdao.com/en/whitepaper/#emergency-shutdown

	オラクルモジュールを修正し、他はそのままで再デプロイする ・ブラックスワンイベント 新しい改善を加えて再デプロイする ・不当な緊急シャットダウン 攻撃者を無効にして、他はそのままで再デプロイする	

(13) 利用可能プラットフォーム

表 2-3-2-12　Maker：DAI が利用可能なプラットフォーム

項目	概要	補足事項
Layer2 Solution	複数の Ethereum の LAYER2 ソリューションで DAI が利用できる ・Optimism ・Arbitrum ・Loopring ・zkSync ・Aztec 2.0	―
ブロックチェーン	複数のブロックチェーンで DAI が利用できる（ブリッジによる利用）[83] ・Ethereum ・Avalanche ・Polygon ・Binance Smart Chain ・Fantom ・klaytn ・xDAI ・Harmony ・Solana ・Celo ・Moonriver	―

2-3-3　金融機関との連携

表 2-3-3　Maker：金融機関との連携

項目	概要	補足事項
金融機関との連携	カストディおよびトレーディングサービスの開始（2021/6） ・Sygnum Bank AG（スイスのデジタルバンク） - Maker ほか複数の暗号資産トークンのカストディ、トレーディングサービスを開始することを発表。 - Usd Coin（USDC）のバンキングサービスは既に実施済	対象の暗号資産 - Aave（AAVE）、Uniswap（UNI）、Aragon（ANT）、Curve（CRV）、Maker（MKR）、Synthetix（SNX）、1inch network（1INCH）

[83] Avalanche Token Dai Stablecoin https://snowtrace.io/token/0xd586E7F844cEa2F87f50152665BCbc2C279D8d70

	不動産ローン市場への参入（2021/10） ・Forge（仏 Société Générale のデジタル資産子会社） - STO（セキュリティトークンオファリング）による不動産ローンで提携。 - 「Security Token Refinancing（セキュリティトークンによる借り換え）」のローンとして、不動産ローンを裏付けとする「OFH セキュリティトークン（住宅金融債）」での借り換えを提案。 - トークンはフランスの法律に基づいて行われ、2000 万ドル（約 22.2 億円）のローンを DAI で借り入れる際の担保とする。	・老舗銀行が MakerDAO と連携する債券担保の初の事例。 ・DAI 発行計画について、Forge は 6 つの事業体を挙げている ①Société Générale ②Forge ③MakerDAO プロトコル ④MakerDAO のリーガル代表者 ⑤DIIS グループ（仏債券投資家）証券エージェントの役割 ⑥取引所 ・フランスの関連法律は、ローンの清算などを確保するための証券エージェントを必要とするため、現実世界の法律要件をクリアする対策と見られている

2-3-4　ガバナンス運営

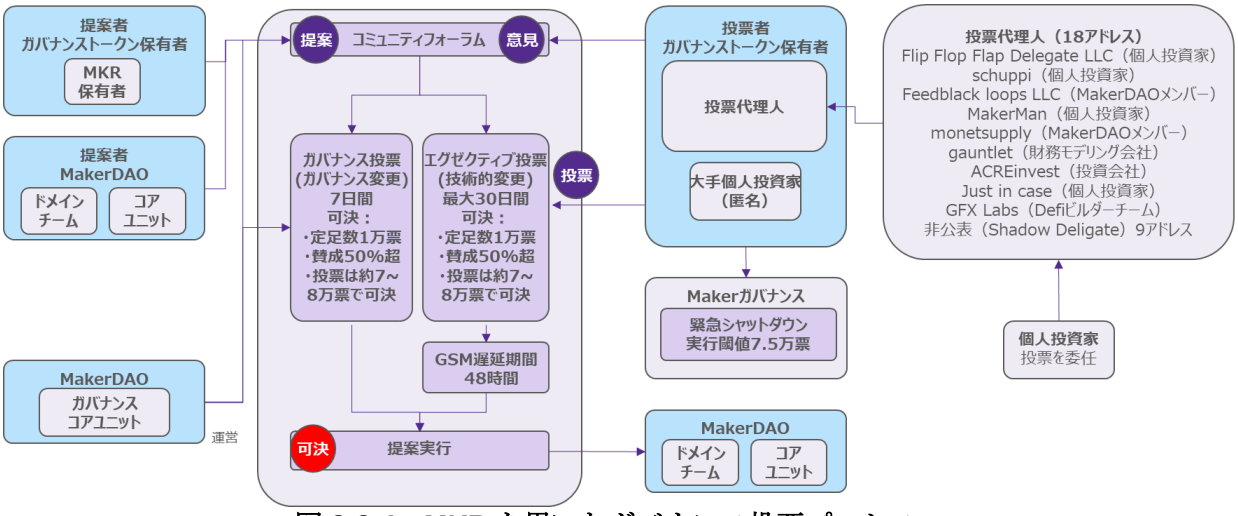

図 2-3-4　MKR を用いたガバナンス投票プロセス

(1)　コミュニティ

表 2-3-4-1　Maker：コミュニティの基礎知識

項目	概要
コミュニティの目的（公式ドキュメントの記載を要約）[84]	・MakerDAO は、世界をリードする分散型ステーブルコインである DAI の生成を可能にする分散型ガバナンスコミュニティ ・MakerDAO の分散型ガバナンスコミュニティは、Maker プロトコル内に組み込まれたガバナンスメカニズムを通じて DAI の生成を管理する ・MKR 保有者は、投票を通じてシステムに変更を加える唯一の権限を持っている

[84] MakerDAO https://makerdao.world/en/learn/MakerDAO

コミュニティ組織形態	・ガバナンストークン MKR 保有者による分散型自律組織（MakerDAO） MakerDAO の運営は、ドメインチーム、コアユニットが行う。 ドメインチームやコアユニットのファシリテーターが運営をリードする。

(2) ガバナンストークン（MKR）

表 2-3-4-2　Maker ガバナンストークン

項目	概要	補足事項
MKR の配付[85]	MKR：100 万トークンを配布済（2022/1 時点） ・一部をアーリーアダプターに配布 ・一部を VC に販売 （Andreessen Horowitz, Polychain Capital ほか）	―
MKR 保有アドレス数[86]（2022/1 時点）	・MKR 保有アドレス数　7 万 6 千 ・1 位保有率　17.39% ・上位 10 アドレス保有率　45.38%	・UNI のように、スマートコントラクトにロックされた未配布分は存在しない
MKR の機能[87]	①オンチェーン投票における投票権（ガバナンストークン） ②再資本化のための原資 - Maker プロトコルが債務超過に陥った際に、MKR を追加供給（MKR に価格上昇圧力） - Maker プロトコルのバランスシートに DAI が過剰に蓄積された場合には、MKR と DAI を交換し MKR を償却（MKR に価格上昇圧力）	・②の機能により、MKR の価格上昇を期待する保有者に対してプロトコルを健全に維持するインセンティブを与えている

(3) 意思決定

表 2-3-4-3　Maker：意思決定

項目	概要	補足事項
意思決定方法	・MKR によるオンチェーン投票を提案内容により 2 つに分けて行う ①ガバナンス投票 - Maker プロトコルの技術的変更以外のガバナンスと DAO プロセスを決定 ②エグゼクティブ投票 - Maker プロトコルの技術的変更を決定。①で可決した提案や予算に従った DAI 配布などのプロトコル変更を行う	・②は①で決定したガバナンス投票のうち、プロトコル変更を伴う重要性の大きい提案が投票にかけられているケースが大半

[85] Maker Profile https://messari.io/asset/maker/profile/launch-and-initial-token-distribution

[86] Etherscan Token Maker https://etherscan.io/token/0x9f8f72aa9304c8b593d555f12ef6589cc3a579a2

[87] MKR Token https://makerdao.world/en/faqs/mkr-token/

	・投票期間：①7 日間、②最大 30 日間 - ②は継続的承認投票モデルとなり、最新の成功した提案の投票数を超えれば可決。超えなければ否決となる	
ガバナンス投票の可決条件（2022/1 時点）	・定足数 1 万 MKR（全体の 1%） 可決：投票数の過半数	―
投票数実績（2021 年）	①307 件中 275 件可決（可決率 90%） ②47 件中 47 件可決（可決率 100%）	―
ガバナンス投票で提案できる事項	・MKR 保有者は、例えば以下のようなフォーラムでの提案及びガバナンス投票への参画が可能 - 新しい担保資産タイプの追加 - リスクパラメータの変更・追加 - DAI 貯蓄率の変更 - オラクル価格フィードの選択 - 緊急シャットダウンを実行 - システムのアップグレードを決定 - インフラなどのサービスへの支払い - 投票は公表された代理人に委託可能	・提案は以下の 9 カテゴリーのフォーラムで議論される ①アップデート（最新情報の通知） ②ガバナンス（ガバナンス全般） ③Maker プロトコル改善提案（MIP）（パラメータ変更など） ④コアユニット（コアユニットの各種活動について） ⑤担保のオンボーディング（担保資産の追加） ⑥開発者（ツールとドキュメント） ⑦コミュニティ開発 ⑧従業員募集 ⑨サイトフィードバック（サイト利用の Q&A） ・合意の意見形成と過半数の賛成を得た提案がオンチェーン投票に送られる（コアユニットチームが判断）
Maker ガバナンスが制御する Maker Vault のリスクパラメータ	・Maker Vault の主なリスクパラメータの例 ①債務上限 単一の担保タイプで作成できる債務の上限額 ②安定化手数料 DAI 精算時に発生（Vault の担保資産と生成した DAI から計算された清算手数料） ③清算比率 ある担保タイプについて最低限要求される担保率。担保率が清算比率を下回ると清算プロセスに入る。 ④清算ペナルティ 清算時に追加的に徴収される手数料 ⑤Maker プロトコルオークションの期間	―

	- 債務・余剰オークションの期間を変更（最大期間は変更不可）	
Maker ガバナンスの投票者（2022/1 時点）	・オンチェーン投票は投票代理人と個人で行われるが、ほぼ全ての投票が投票代理人によって行われている。 ・投票代理人の内訳 - 計 18 アドレス：公表 9、非公表 9（Shadow Delegate） - 保有票数：98,500 票（全体の 10.0%　2022/1） ・主な公表されている投票代理人は以下の通り ①Flip Flop Flap Delegate LLC（個人投資家）3.2 万 ②schuppi（個人投資家）　2.0 万 ③Feedblack loops LLC　1.0 万 Tim Black, MakerDAO Community Contributor ④MakerMan（個人投資家）0.52 万 ⑤Monetsupply　0.50 万 MakerDAO Risk Core Unit Core Contributor ⑥gauntlet（財務モデリング会社）3,000 ⑦ACREinvest（投資会社）1,000 ⑧Just in case（個人投資家）54 ⑨GFX Labs（DeFi ビルダーチーム）28 ・上記の他に、ベンチャーキャピタルも関与していると言われている。以下の VC は 2019 年まで直接投票していたが、現在は投票を行っていない模様[88] - Andreessen Horowitz（米カリフォルニア） - Field Technologies Inc.（米ミネソタ）	・投票代理人のうち 2 名は MakerDAO メンバーであり、2 名で 1.5 万票を保有。この 2 名で提案の定足数（1 万票）を超えており、ガバナンス投票による意思決定に大きな影響力を有していると考えられる。

(4) インシデント発生時の対応

表 2-3-4-4　Maker インシデント発生時の対応

項目	概要	補足事項
インシデント発生時の緊急対応	・MKR 保有者が MKR を緊急シャットダウンモジュール（ESM）に預け、閾値を超えると即座にシャットダウンが実行される	・緊急シャットダウンの実行は現在 75,000MKR（提案で 10 万に引上げ中）であり、投票代理人だけでは 10 万票に届かない。他に多数の MKR 保有者（個人投票者）の協力が必要と

[88] Centralized Governance in Decentralized Finance (DeFi): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3971791

	・ダークスペルメカニズムにより、重大な脆弱性の修正を行う	なる。投票代理人の対応が遅れたり、他に協力者がいない場合は、攻撃を即時に防御することが難しいと想定される ・ダークスペルメカニズムはコード修正に最短 3 日かかるため、公知の不具合の場合は対応が間に合わない懸念がある
緊急対応の発動権限者	・緊急シャットダウンは MKR 保有者が発動する ・ダークスペルメカニズムはガバナンスファシリテーターが発動する	・ダークスペルメカニズムは信頼できるサードパーティやコミュニティの特定者など利害関係者が公表されておらず、権限者を信頼する必要がある
インシデントによる損害賠償	・インシデント発生などによる損害はユーザ責任であり、原則として賠償は行わない（Terms of Use[89]に明記されている） ・2020 年 3 月のインシデントによる損害賠償がガバナンス投票に提案され、投票の結果、補償しないことで決定した（補償は MKR の増刷で行われるため、MKR の値下げを懸念する大手保有者が反対した）	・大手 MKR 保有者の損害の状況により、ガバナンス提案に賛成するか反対するかが決まってしまい、平等な判断が行われない可能性

(5) その他

表 2-3-4-5　Maker ガバナンス運営その他事項

項目	概要	補足事項
MKR 保有者の匿名性	・MKR 保有者は原則として匿名であり、実在する主体の特定が困難 MKR の保有アドレスは特定できるが、KYC が行われていないため実名とはリンクできないケースが多い ・但し、投票代理人は属性を公表しているため、個人・法人の特定が可能	・意思決定に関わった MKR 保有者を特定できず、決定の差し戻しや決定者の責任が困難である可能性

2-3-5　インシデント事例[90]

2020 年 3 月に発生したゼロ入札攻撃のインシデント事例について、その概要と発生理由、問題点を説明する。

[89] MakerDAO Terms of Use https://vote.makerdao.com/terms

[90] https://blog.makerdao.com/the-market-collapse-of-march-12-2020-how-it-impacted-makerdao/
https://insights.glassnode.com/what-really-happened-to-makerdao/
https://www.blocknative.com/blog/mempool-forensics
https://makerdao.com/en/whitepaper/
https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol#to-summarize-we-have-three-types-of-auctions
https://docs.makerdao.com/keepers/auction-keepers
https://www.coindesk.com/tech/2020/09/23/makerdao-users-hosed-by-march-flash-crash-wont-get-mkr-payouts-say-mkr-whales/

(1) 発生日：2020 年 3 月 12 日

(2) 損害額：約 832 万ドル

(3) 事件の概要

ETH 価格暴落によるネットワーク輻輳やガス高騰により、Maker の担保強制清算が発生した際　に入札が正しく行われない弱点を攻撃され、ゼロ入札により約 832 万ドル相当の ETH を損失し　た。

(4) 事件の流れ

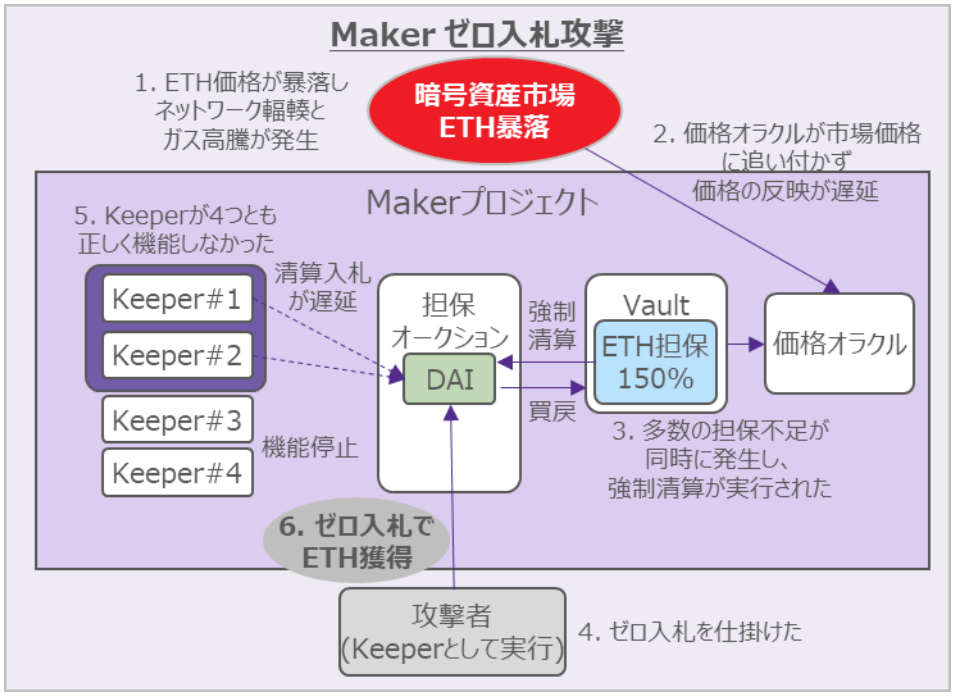

図 2-3-4-1　Maker ゼロ入札攻撃

1. Black Thursday（COVID-19 や米国の渡航禁止例などによる株式市場の暴落）により ETH 等の暗号資産が暴落（ETH：$194→$111 に 43%下落）。Ethereum 上のトランザクションが急増し、ネットワークの輻輳とガス価格の急騰が発生。
2. 上記により、Maker の価格オラクルが価格を更新できず遅延。ETH の市場価格に追いつかず、参照価格の反映が遅延した。
3. その後、価格オラクルが一気に更新された結果、Maker 内の ETH 価格が約 20%下落。多数の Vault で ETH の担保不足が発生し、約 1,200Vault の強制清算（担保オークション）が実行。
4. 担保オークションにおいて、攻撃者が「ゼロ入札」（DAI=0 で ETH に交換）を仕掛けた。
5. 強制清算により、4 つの Keeper が清算のための DAI 買取り入札を行うが、4 つとも正しく機能　せず入札ができなかった。
   - Keeper#1,#2　ガスの高騰に起因して、入札のトランザクションが制限時間（10 分）以内に処理されなかった。
   - Keeper#3　Maker Foundation が運営していたが、ネットワーク輻輳により技術的な問題が　　発生し、機能しなかった。
   - Keeper#4　清算するための DAI が枯渇し、処理が数時間停止した。

6. 攻撃者がゼロ入札（ETH をゼロ DAI で購入する入札）を行い、4 つの Keeper が全て機能しなかったため攻撃者が入札を勝ち取り、合計 832 万ドル相当の ETH を窃取した。（Keeper や攻撃者が行ったオークション入札 4,447 件のうち、1,462 件がゼロ入札であった）
7. 3/19 に Maker プロトコルによる債務オークションを実施し、MKR を追加発行することでゼロ入札により生じた 540 万ドルの担保不足を解消（3/29 時点で 20,980MKR を生成して 530 万 DAI が供給された）

(5) 発生原因

・ETH 価格暴落による Ethereum のガス高騰により、Keeper が正しく動かないことを悪用してゼロ入札を仕掛けたことによるもの

・事件後の調査で、Ethereum のネットワーク輻輳は意味のない大量のトランザクションにより意図的に行われた可能性があり、攻撃者がガス高騰を引き起こして Keeper が正しく動かない状態を作り上げ、ゼロ入札攻撃を行った可能性も指摘されている。[91]

(6) インシデントの問題点

表 2-3-5　Maker ゼロ入札攻撃の問題点

区分	種別	問題点の内容	存在するリスク
現象的要因	デプロイメント	Keeper のオークション入札がガス価格の問題により処理できなかった ・Keeper のガス価格は Ethereum 上の平均価格を基に算出しているが、ガス価格が急激に上昇した場合はそれに追いつかず、低いガス価格で入札のトラクザクションが出されたため、オークションの制限時間内に処理されなかった。	・正当なオークション入札ができず、悪意のある入札が通過し、ゼロ入札などの攻撃を受けてしまう
		オラクルの価格反映が遅延した ・ネットワーク輻輳とガス高騰により、複数あるオラクル価格フィードの市場価格の取得が遅延し、ETH 価格の内部反映が遅延した ・オラクル価格フィードは複数の匿名の個人による BOT（ダークフィード）で運営していたため、ネットワークが輻輳の影響を受けて市場価格の取得が遅延してしまった	・オラクルが正常な価格を反映できず、市場価格との差が発生することでオラクル攻撃を受けてしまう
	プラットフォーム	大量のトランザクションにより Ethereum のネットワークが輻輳し、ガス価格が高騰した ・ETH 価格暴落による取引増加や、意味のない大量のトランザクション（意図的に行われた可能性あり）により、ネットワークが輻輳しガス高騰を引き起こした	・トランザクションの増加により処理遅延やガス高騰が発生し、正常なトランザクションが通らなくなり様々な悪影響が発生してしまう
	オペレーション	Vault の強制清算による担保オークションの処理中に、攻撃者がゼロ入札を行った	・状況によってはゼロ入札を受け入れてしまう

[91] Evidence of Mempool Manipulation on Black Thursday: Hammerbots, Mempool Compression, and Spontaneous Stuck Transactionshttps://www.blocknative.com/blog/mempool-forensics

		・担保オークションは、本来は Keeper により内部市場価格に応じて DAI の買取りが行われるが、攻撃者のゼロ入札が受け入れられてオークションを通過してしまった。	
		攻撃発生時に Keeper の 1 つが機能していなかった ・Keeper#3 は Maker Foundation が運営していたが、ネットワーク輻輳により技術的な問題が発生し、機能しなかった	・オークション入札の処理能力が低下し、処理の遅延や入札が失敗してしまう
		同時に多数の強制清算が行われた際に、清算で使用する DAI 資産が不足した ・Keeper#4 は正しく稼働していたが、多数の強制清算が同時に行われたため、DAI が枯渇して入札ができず、機能しなかった。この時点では ETH が暴落しており、清算に必要な DAI を調達することが困難であった。	・担保資産の枯渇により強制清算ができなくなり、正当な入札ができなくなってしまう
動機的要因	オペレーション	ETH 価格の暴落などによる担保資産の攻撃に対して、事前に対策ができていなかった ・今回は ETH が単一の担保資産であったことから、ETH 価格の暴落により DAI が強制清算されて大きな影響を受けた。 ・MakerDAO はこの攻撃を「ブラックスワンイベント（重大な奇襲攻撃）」と呼び、攻撃に対するフェイルセーフなソリューションはなく、適切なガバナンスと Maker プロトコルの組合せで対応すると述べている	・担保資産の価格操作により、大量の強制清算が引き起こされて正当な入札ができなくなる
		Keeper が全て停止した場合の対策ができていなかった ・攻撃時は Keeper が 4 つしか稼働しておらず、結果として全て機能しなかった。Keeper が全て停止した場合の影響と対応が事前に検討できておらず、被害を発生させた。	・Keeper が停止すると正当なオークション入札や価格を 1USD を保つためのアービトラージが行われず。入札の悪用や大幅な価格変動が発生する
	ガバナンス	オンチェーン投票が大手 MKR 保有者に支配され、損失が補償されなかった ・オンチェーン投票の結果、投資家の損失を補償しないことが決定（2020/9） - 投票は大手 MKR 保有者によって支配され、MKR 保有者の 9%（38 ユーザ）の投票で否決された。補償内容に MKR トークンの増刷が含まれており、追加発行で価格が下がることに対する反対が補償提案を上回った。	・オンチェーン投票が大手 MKR 保有者に支配され、少数の MKR 保有者が損害を受ける可能性がある
		事件で損失を受けた投資家に訴訟された（2020/4）	・市場価格暴落の外部要因であっても、投資家に起

		・資金を失った投資家 20 名が Maker の組織に対して訴訟を起こした。訴訟理由は、Vault の強制清算に起因して担保の全額を失うリスクを説明していなかったとの主張 ・訴訟の対象となる組織、関連当事者 -Maker Foundation -Maker Ecosystem Growth Foundation -Dai Foundation -Maker Foundation を含む関連当事者 ・オレゴン州ポートランドのハリス・ベルン・クリステンセン LLP が代表する原告ピーター・ジョンソンによって、カリフォルニア北部地方裁判所に提起された ・2020/9/25　被告（Maker）の申し立てが認められ、訴訟は保留されて米国仲裁協会に委任された。被告の申し立ては、原告が Maker プラットフォームのサインアップ時に「DAI 利用規約」を見る契約になっていると主張した	因しない理由で損失が発生した場合は、訴訟される可能性がある
	法規制	・Ethereum のネットワーク輻輳は攻撃者が意図的に発生させたという記事があるが、犯罪捜査は特に行われていない様子であり、832 万ドルの窃取が罪に問われていない	・DeFi プロジェクトに対する攻撃が罪に問われにくく、犯罪を増長する可能性がある

2-3-6　Maker の主なトラストポイント

(1)　RWA Company 、DAI Foundation（関連法人）

・Maker Foundation は解散したものの、クライアントとの各種契約の締結等を行う RWA Company や、Maker コミュニティの知的財産の管理法人である DAI Foundation は引き続き存在。

(2)　ドメインチーム・コアユニット（MakerDAO）

・MakerDAO 内に組織されたドメインチーム及びコアユニットが Maker Foundation の主要業務（コード開発、リスク管理、営業活動など）を継承している。

(3)　ベンチャーキャピタル／投票代理人

・ICO により MKR の一部をベンチャーキャピタル等に販売しており、初期投資家がガバナンス投票に一定の影響力を有している可能性が高い。
・18 アドレスの投票代理人が個人投資家から投票を委任されており、ガバナンス投票において大きな影響力を有している。なお、９アドレスは保有主体が公表されていない。

(4)　ダークスペルメカニズム

・修正コードをドメインチームが開発し、コミュニティの特定の者や信頼できるサードパーティが特別の権限の下で重大な脆弱性の修正を行うための仕組み。サードパーティ等の詳細は非公表。

(5)　キーパー

・担保資産価格下落に伴う強制清算が適切に処理されるためには、担保オークションへの応札等を行うキーパーが機能することが前提となっており、機能不全に陥ると上述のようなインシデ

ントに繋がる。

(6) コード監査会社

・ユーザはコード監査会社による監査結果を信頼してプロトコルを利用しているものと想定される。

(7) ウォレット提供者

・（Maker に限らず DeFi 全般について、）Metamask など少数のノンカストディアル・ウォレットを多くのユーザが使用しており、ウォレットに脆弱性が存在した場合の影響度は大きいと考えられる。

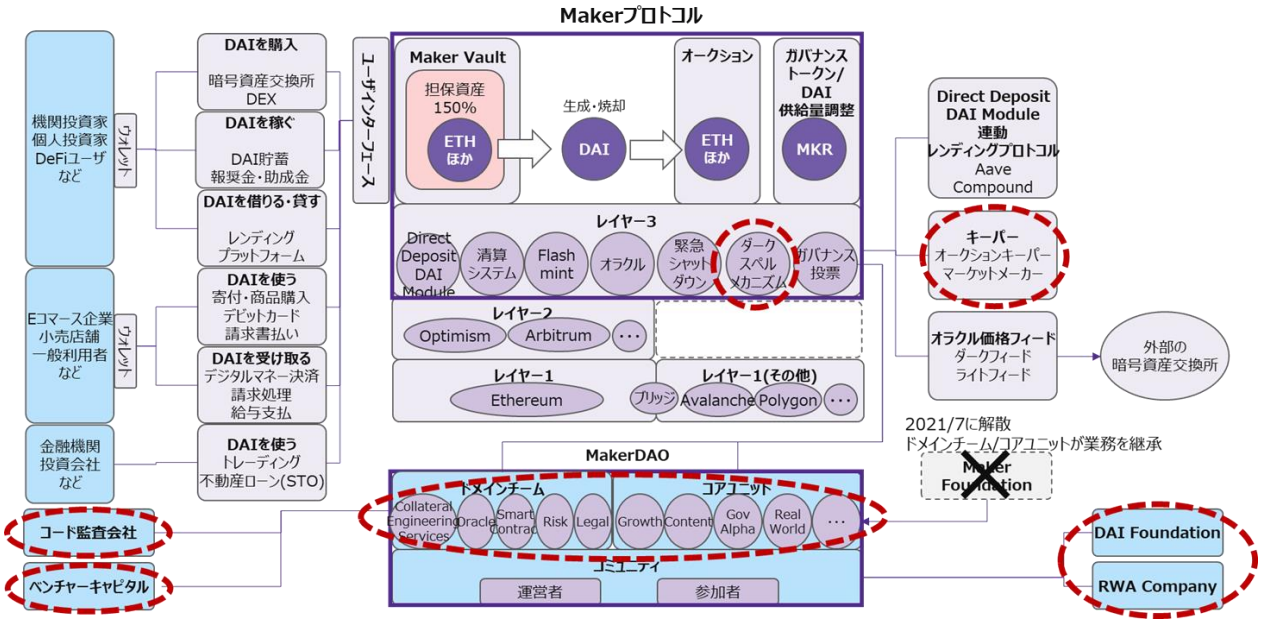

図 2-3-6-1　Maker の主なトラストポイント（構成要素）

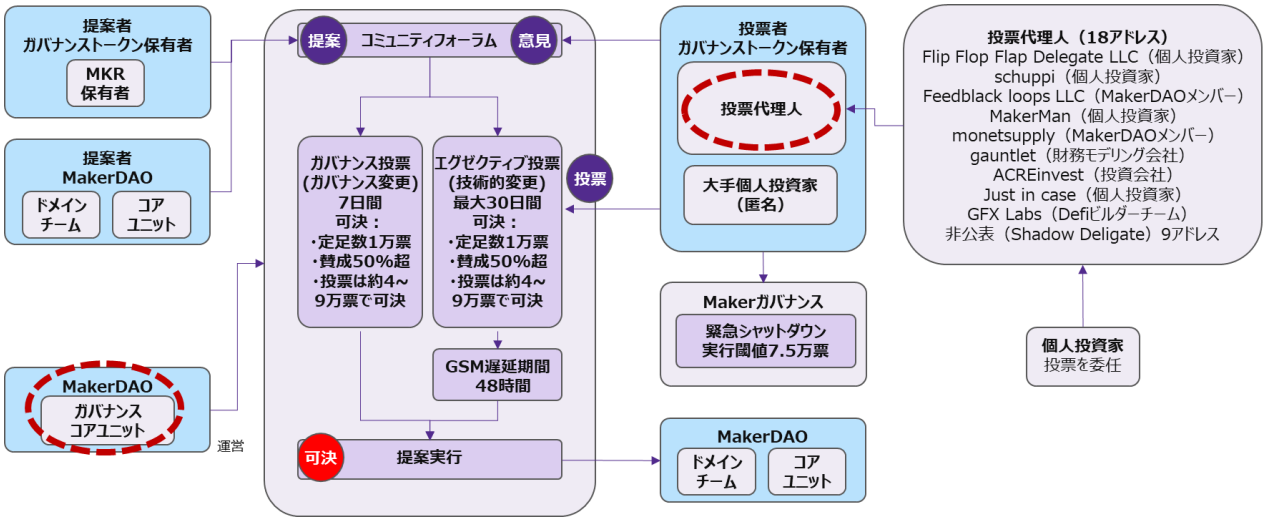

図 2-3-6-2　Maker の主なトラストポイント（ガバナンス投票）

2-4　レンディング　Aave の分析

Aave を調査対象として、プロジェクト概要や運営組織、主な技術特性、ガバナンス運営について詳細に調査研究を行う。レンディングプロトコルである Aave は KYC プロバイダーと連携した機関投資家向け DeFi サービスや信用委任など先進的なサービスなどを行っており、また金融機関等と連携して金融市場への展開を積極的に行っているなどの特徴がある。各項目の調査により実態を明らかにし、課題・問題点やリスク事項を分析する。

2-4-1　プロジェクト全体概要

Aave の主な構成要素とそのマッピング、コミュニティ概要は下図・表の通り。

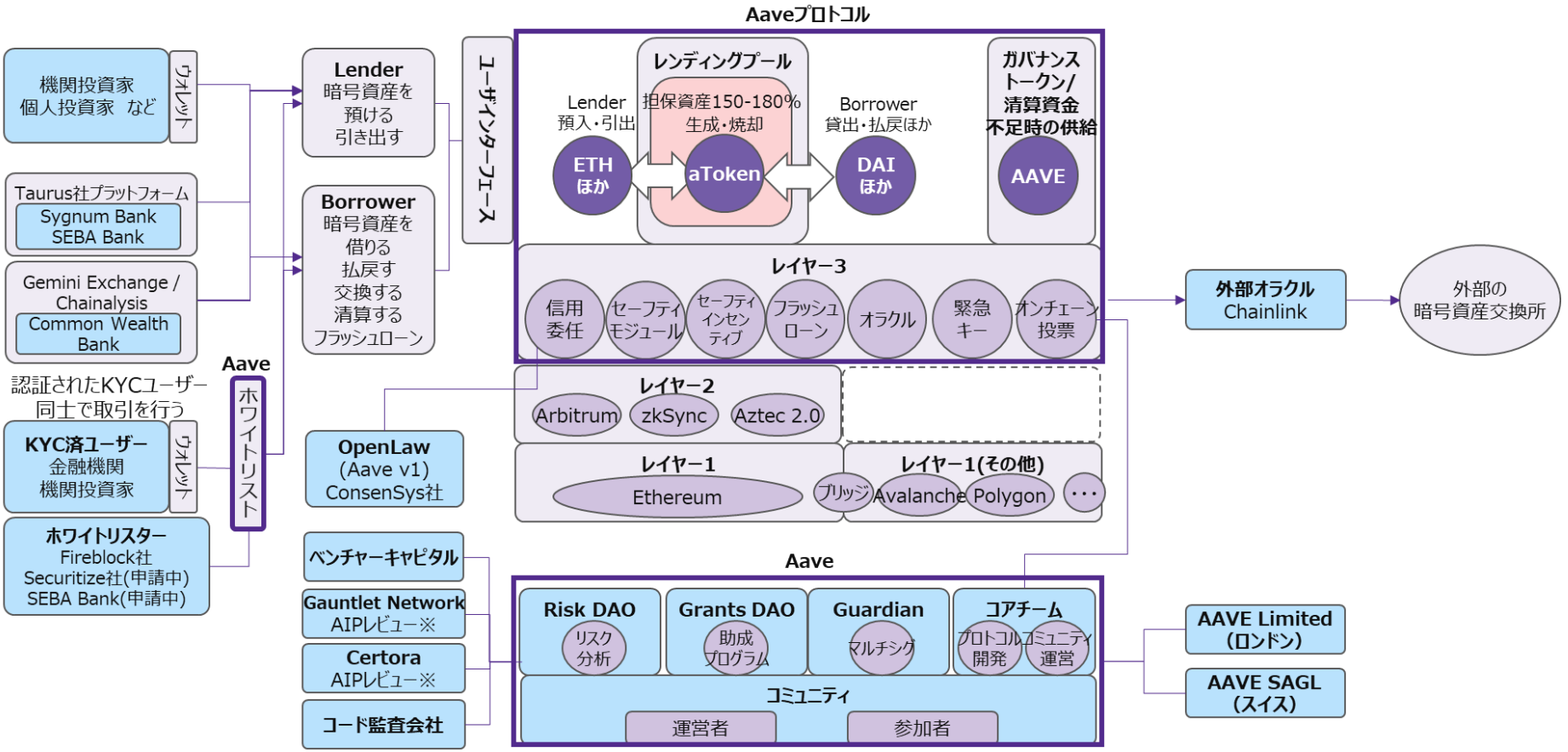

図 2-4-1-1　Aave の主な構成要素

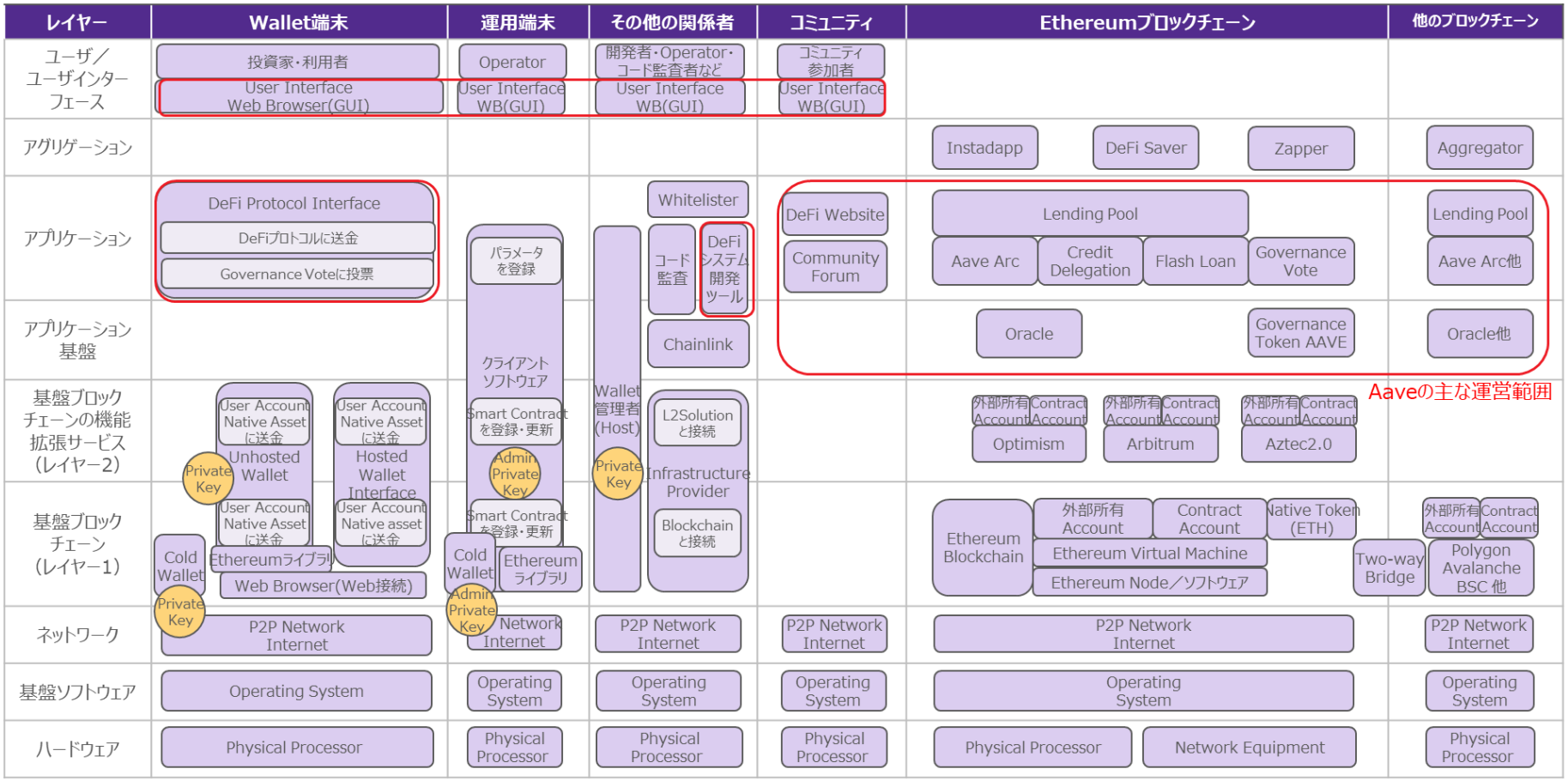

図 2-4-1-2　Aave の主な構成要素のマッピング

表 2-4-1-3　Aave：コミュニティ・開発会社・バージョン動向

項目	概要	補足事項
バージョンと主な機能	2017 年　ETHLend として発足 2018 年　名称を Aave に変更 2020 年　v1 ローンチ（ETHLend プロトコルは機能停止） 2021 年　v2 ローンチ 2022 年 3 月　v3 ローンチ	－
コミュニティ	・Aave コミュニティ（DAO） - ガバナンストークン保有者による運営（保有アドレス数：10 万） - Aavenomics と称する方針に基づき、更なる分散性・自立性の向上を目指す[92] - Aave コミュニティの運営は Aave Core Team が実施	－
関連法人	Aave Limited[93] ・Aave の英国法人 ・イギリスの金融行動監視機構（FCA）から「電子マネー機関」の営業ライセンス認可を取得（2020 年 7 月認可） ・法人としての活動の詳細は不明	・創設：2017/5　拠点：ロンドン ・創設者：Stani Kulechov（Founder&CEO） ・運営メンバー：53 名　イギリス、アメリカなど各国に所在（2022/1）[94] ・調査時点では、イギリスでの具体的な活動はされていない模様[95]
	Aave SAGL ・スイス法人 ・活動の詳細は不明	・創設：2018 年 拠点：スイス（キアッソ） ・創設者：Stani Kulechov（Founder&CEO）
Aave Core Team	・Aave のプロトコル開発・運用（コード修正やそれに伴うオペレーション）、コミュニティ運営を行う	・リード：Stani Kulechov ・Aave 運営メンバーが役割を分担している
Aave Risk DAO（2022/2 時点）	・Aave プロトコルと Safety モジュールのリスク分析・評価を行う ・活動予算　年間 75 万ドル ・運営資金　計 6 名のマルチシグ（4-of-6）で決定 - RiskDAO3 名、Gauntlet2 名、Aave コンミュニティ 1 名を指名	・7 名＋大学生で運営 ・プロジェクトマネジメント&ガバナンス monet-supply ・マーケットリスク分析 Thomas, Jack, Roberto, Jeremy ・技術リスク　Mateusz ・実世界アセットリスク　Will ・学生コントリビューター Blockchain at Berkeley
Aave Grants DAO	・コミュニティ開発者のより幅広いネットワークに力を与えることに焦点を当て、コミュニティによって提出された	Lead: Shreyas Hariharan （Llama Founder, Uniswap grants） Reviewers:

[92] Decentralizing Aave https://docs.aave.com/aavenomics/

[93] Aave Limited https://aave.co.uk/

[94] RocketReach Aave Information https://rocketreach.co/aave-profile_b443387efa0db443

[95] The Financial Services Register https://register.fca.org.uk/s/firm?id=0010X00004U9vVAQAZ

（2022/2 時点）	アイデアに資金を提供する助成プログラム ・補助金の予算：年間 400 万ドル ・運営予算：年間 50 万ドル ・委員会：計 8 名　リード 1 名、レビューワー7 名	・Aleks Larsen（Blockchain Capital） ・Jose Maria Macedo（Delphi Digital） ・Imran Khan（DeFi Alliance） ・Maggie Love （W3BCLOUD and SheFi） ・Corbin Page（ConsenSys Codefi） ・Nick Cannon（Gauntlet） ・Calvin Chu（Independent）
Guardian（2022/2 時点）	・集中化されたアクターによる潜在的なガバナンスの乗っ取りから保護するためのコミュニティマルチシグとして設立された ・マルチシグは 5-of-10 で実行 ・スマートコントラクトのアップデート、緊急キー（プロトコルの一時停止）が発動できる ・メンバーは 10 名で運営しており、2021 年 9 月に全員改選された - 提案者は Grants DAO のリード（Shreyas Hariharan）	対象者 10 名 ・Arthur0x (DeFiance Capital) ・coderdan (Aavegotchi) ・Gavi Galloway (Standard Crypto) ・Isa Kivlighan (Aave community, previously head of marketing on Aave Genesis team) ・0xMaki (Sushi) ・Hilmar Maximilian Orth (Gelato) ・Meltem Demirors (Coinshares) ・Corbin Page (ConsenSys Codefi, Aave Grants DAO) ・Imran Khan (DeFi Alliance, Aave Grants DAO) ・Dennison Bertram (Tally)
協力会社[96]	・Gauntlet Network[97] - Aave の資本効率とリスクのバランスをとるパラメータの推奨値をダッシュボードで提供する - Aave ガバナンス提案の AIP（Aave 改善提案）のレビューに、リスク貢献者として参加	・2018 年創業　本社：US, ニューヨーク ・社員 32 人 2022/3 時点）
	・Certora[98] - Aave プロトコルのコード監査を行う - Aave ガバナンス提案の AIP（Aave 改善提案）のレビューに、セキュリティ貢献者として参加	・2019 年創業　本社：イスラエル, テルアビブ ・社員 37 人（2022/3 時点） ・アドバイザリーボードに、Aave 創設者の Stani Kulechov が参加

2-4-2　主な技術特性

(1) プロトコルの全体像[99]

[96] Aave Developers Governance Guide https://docs.aave.com/developers/guides/governance-guide

[97] Gauntlet Networks, Inc. https://www.crunchbase.com/organization/gauntlet

[98] Certora Inc. https://www.crunchbase.com/organization/certora

[99] aave-v2-whitepaper https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf

・ユーザ（個人／機関投資家など）は、Aave プロトコルのレンディングプール（スマートコントラクト）に暗号資産（一部のステーブルコイン含む）を預け入れることで金利を獲得でき、また所定の担保資産を預け入れることを前提に同プールから借り入れを行うことができる（2022/1 時点で ETH、LINK、USDT、AAVE を含む 30 以上の暗号資産・ステーブルコインに対応）

・レンディングプールに暗号資産を預け入れると、1:1 で当該暗号資産の頭文字に a を付与した aToken[100]（例：aETH）を受け取り、同プールが獲得した収益は aToken 保有者に配分される。当　該暗号資産を引き出す際には aToken を焼却する。

・暗号資産価格は外部オラクル（Chainlink）を参照する[101] 。

・貸出・借入金利は Oracle を参照することで、システム的に算出される。

・借入時、担保資産価格が下落した場合には清算が発生する

・暗号資産を預け入れたユーザは、当該暗号資産を担保とする与信枠を他者に譲渡することができ、譲渡を受けた者は無担保で借り入れを行うことができる（信用委任）。信用リスクの対価として譲渡人（Delegator）は追加的な収益を得る。

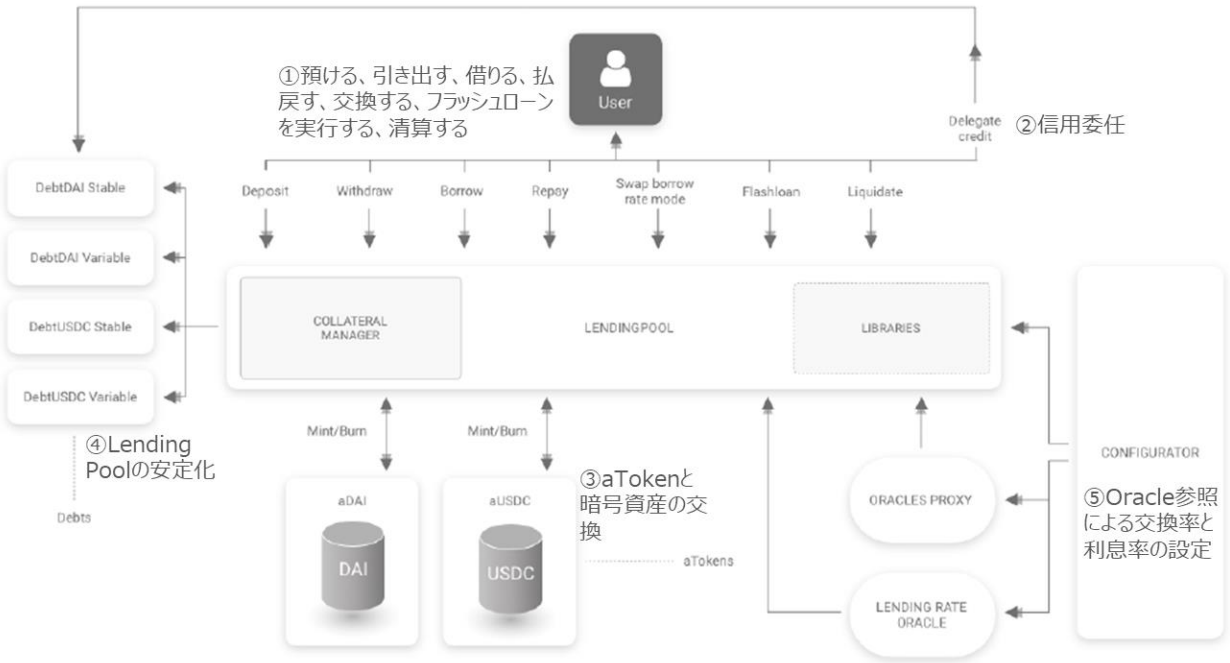

図 2-4-2-1　Aave：プロトコルの全体像

(2) Aave interest bearing tokens (aToken)[102]

[100] Aave AToken https://docs.aave.com/developers/tokens/atoken

[101] Price Oracle https://docs.aave.com/developers/v/2.0/the-core-protocol/price-oracle

[102] Aave Developers aTokens https://docs.aave.com/developers/v/1.0/developing-on-aave/the-protocol/atokens#:~:text=The%20aTokens%20are%20interest%2Dbearing,safely%20stored%2C%20transferred%20or%20traded .

・aTokens は、暗号資産を預け入れると、その暗号資産の頭文字に a がついたトークンが１：１で生成され、暗号資産を引き出す時に焼却される。

・例えば、1ETH を入金すると 1aETH トークンが得られ、1aETH を焼却すると、1ETH が返却される。

・aToken は、Aave プロトコル内でガス代をかけずに利息をリアルタイムで直接付与することが　可能というメリットがある。

(3) 清算[103]

・ユーザがレンディングプールに預けた暗号資産の価値低下や借り入れた暗号資産の価値上昇などにより、決められた担保比率を下回った場合に清算が行われる。

・清算では担保の最大 50%が払戻しされ、担保から清算手数料が差し引かれる。

(4) Safety Module/ Safety Incentive[104]

・Safety Module（SM）：大量の清算発生時において、プロトコルの債務超過解消を目的としてユーザが任意でステーキングを行った AAVE トークンから補填を行う仕組み

・Safety Insentive（SI）：SM へのステーキングを行う対価として手数料が得られる仕組み

【Safety Module/ Safety Incentive の詳細】

① AAVE トークン保有者は、SM に AAVE トークンをステーキング（ロック）する。

② ステーキングを行った者に対して、AAVE の手数料収入の一部が対価として支払われる。

③ 大規模清算の発生等により資金不足が生じた際には、SM に預けられた AAVE トークンがオークション（Auction Module）によって売却される（ステークされた AAVE トークンの最大 30％から補填される。

④ オークションにより獲得した資金を資金不足解消に充当する。

⑤ オークション実施後もなお資金が不足した場合は、運用準備金（Ecosystem Reserve）から補填される。これらの補填は Auction Module というプロトコルで AAVE トークンが売却される。

※AAVE トークンの総発行数 1600 万トークンのうち、運用準備金に 300 万トークンが配布されている。

103 Aave FAQ Liquidations https://docs.aave.com/faq/liquidations

104 Aavenomics Safety Module https://docs.aave.com/aavenomics/safety-module

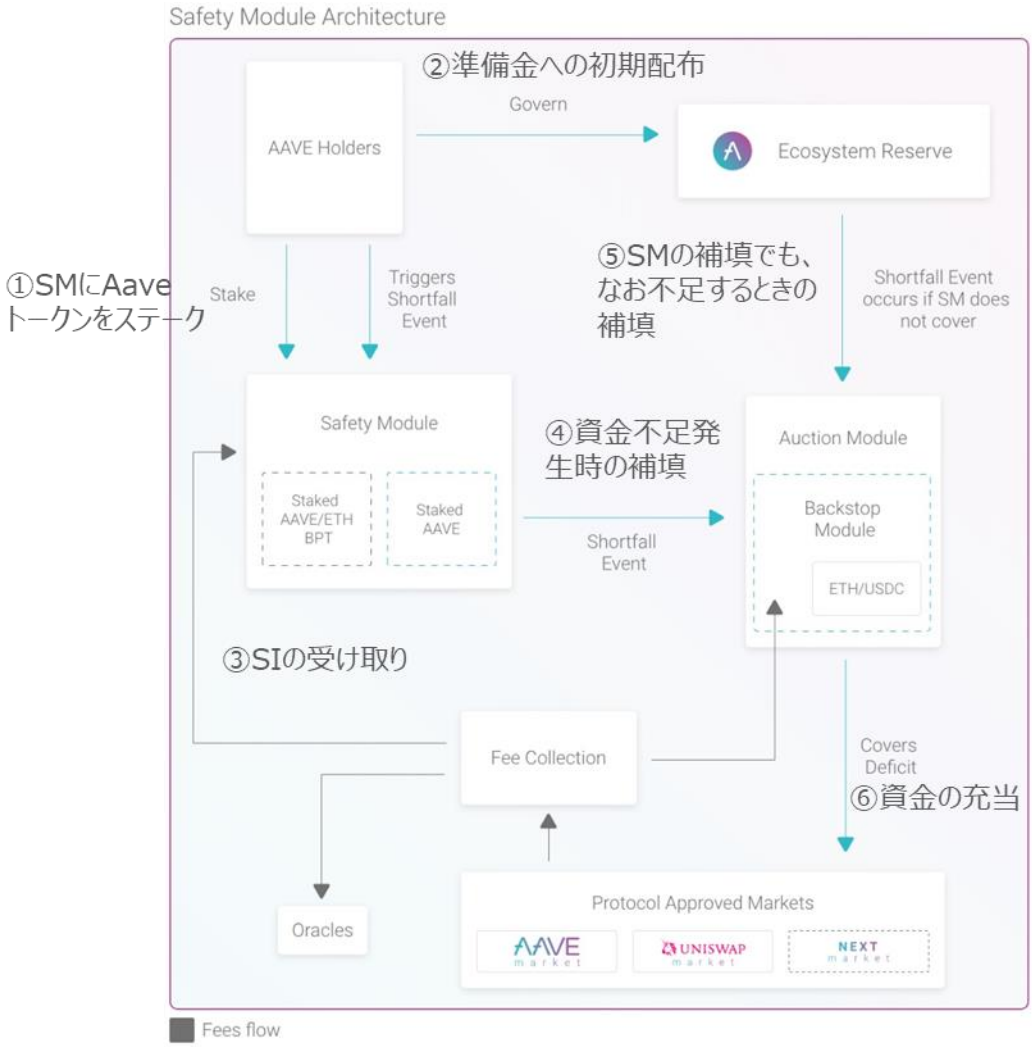

図 2-4-2-2　Aave：Safety Module / Safety Incentive

(5) Flash Loan[105]

・1 トランザクション内で借入から返済まで完結させることで、事前に担保を預け入れることな借入等を可能とする仕組み（期限内に返却されなかった場合、その処理はすべて実行されない）
・主な用途として、アービトラージや、担保交換などが想定されている
・手数料は借りたトークン建て債務の 0.09%。そのほかに、デプロイとスマートコントラクトの実行にガス代が発生する。
・流動性プールを介することで、暗号資産の需要よりも供給を潤沢に用意することで、フラッシュローンを利用した攻撃を防ぐ設計となっている。

【Flash Loan の具体例（AAVE マーケットと他の取引所の間でアービトラージの機会が生じている場合を想定）】

下記①～⑤を 1 トランザクションで実行する

① 無担保で流動性プールから 1ETH を借りる。
このとき、Aave Market では 1ETH を 200DAI で交換できる状態とする。

② 交換レートに差がある他の交換所で、①で借りた 1ETH を 220DAI で交換取引予約する。

[105] Aave Developers Flash Loans https://docs.aave.com/developers/guides/flash-loans

③　Aave Market で 200DAI と 1ETH の交換予約を行う。

④　1ETH と手数料 0.09%の 0.0009ETH を返却する。

⑤　交換取引予約を実行する。結果として、19.82DAI※相当の利益を獲得する（実際にはこれにガス代が引かれる）。※20DAI- 0.0009ETH（0.18DAI）

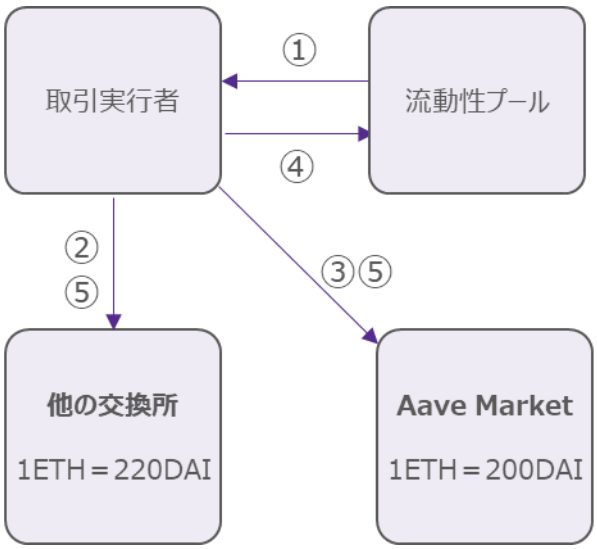

図 2-4-2-3　Aave：Flash Loan

(6) 信用委任（Credit Delegation）[106]

・信用委託とは、Aave に暗号資産を預けた人が、その暗号資産を担保とする与信枠を他者に譲渡することで、さらに追加利回りを享受できる仕組みをいう。

・貸手・借手の間で利率や期限について合意し、契約を締結する。現在は担保資産毎に譲渡先を 1 人指定できるが、今後は複数人への譲渡機能を検討予定。

【信用委任の具体例】

図 2-4-2-4 の例では、カレンがチャドの代わりに担保を差し入れることで、チャドが暗号資産を借りることを可能にしている。

・カレン・チャド間の契約締結時において、V1 では両者のオフチェーンでの合意に基づき OpenLaw※というスマートコントラクトを内包する電子契約サービスを活用して契約の強制力を持たせる仕組みを取り入れていた。V2 では、電子契約機能を Aave に取り入れている。

※OpenLaw[107] ：ConsenSys 社が提供するブロックチェーンを用いた電子契約サービス

[106] Aave Developers Credit Delegation https://docs.aave.com/developers/guides/credit-delegation

[107] OpenLaw REAL WORLD CONTRACTS FOR ETHEREUM https://www.openlaw.io/

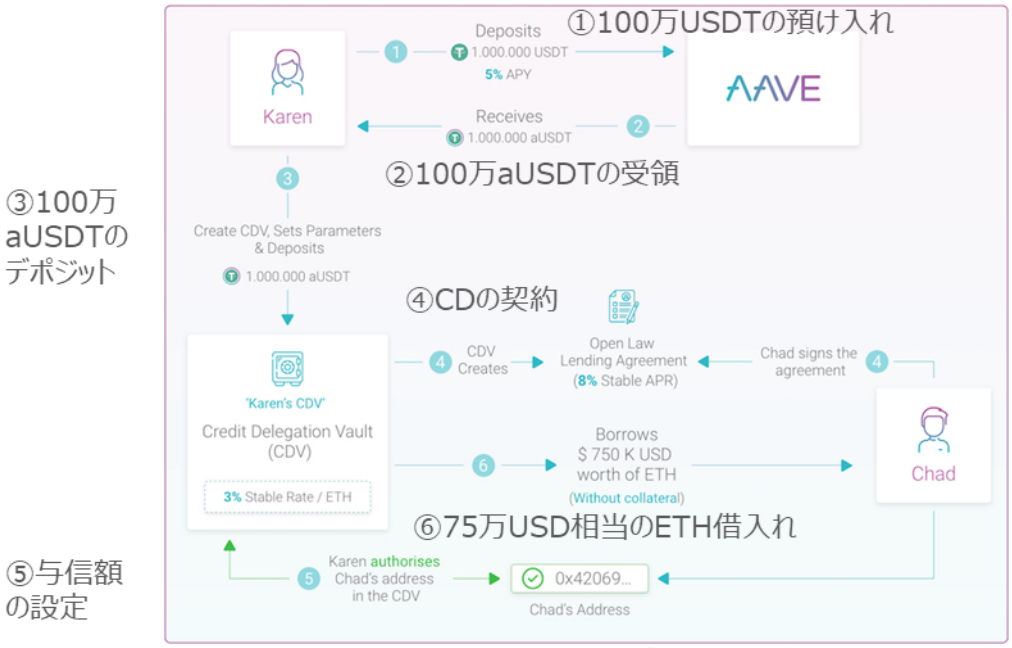

図 2-4-2-4　Aave：信用委任の概要

①② カレンは Aave のレンディングプールに 100 万 USDT を預け入れ、100 万 aUSDT を取得する。

③ Karen は CDV（Credit Delegation Vault）に 100 万 aUSDT を預け入れることで、3%の固定金利で ETH を獲得する。

④ 無担保での借入を希望するチャドとカレンの間で、与信額・金利（図では年利 8%）等の借入条件について合意し、契約を締結する（AaveV1 では OpenLaw により信用委任契約に署名）

⑤ 契約締結後、カレンは契約に従ってチャドの与信額を設定する。

⑥ チャドは当該与信額の範囲で借入れを行う（図では 75 万 USD 相当の ETH を借入れ）。信用委任によって、カレンはより高い利回りを獲得でき、チャドは担保なしで資金を調達できている。

(7) AaveArc/ Whitelister[108]

a. AaveARC

・機関投資家等がコンプライアンスに準拠した形で DeFi エコシステムに参加することを目的とした、Permissioned 型の機関投資家向け DeFi プロトコル。

・KYC 及び財務デューデリジェンスを機関投資家が、同様の承認を受けた他の機関投資家との間のみで AAVE プロトコルの主要機能を活用して、運用を行うことができる。現時点での対象の暗号資産は、ETH、WBTC、USDC、AAVE の 4 つ。

・2022 年 1 月に Ethereum の L2 ソリューションである Arbitrum と Optimism 上でデプロイ[109]

b. Whitelister

・AaveArc を介して AAVE プロトコルにアクセスする機関投資家に対してデューデリジェンスを 実行し、すべての参加機関が KYC および AML 規制に準拠できるように承認し、「ホワイトリスト」に登録する。

---

[108] Aave launches permissioned DeFi platform Aave Arc, Fireblocks becomes first whitelister https://www.theblockcrypto.com/post/129277/aave-arc-permissioned-defi-platform-fireblocks-first-whitelister

[109] Wall Street's Jane Street Borrows $25M Via DeFi Lending Platform https://thedefiant.io/jane-street-25/

・米 Fireblocks 社が 1 社目としてローンチ済、米 Securitize 社、スイス SEBA Bank はガバナンス提案実施中（2022/2 現在）

【Whitelister の具体例①：FireBlock 社　DeFi ゲートウェイ[110]】

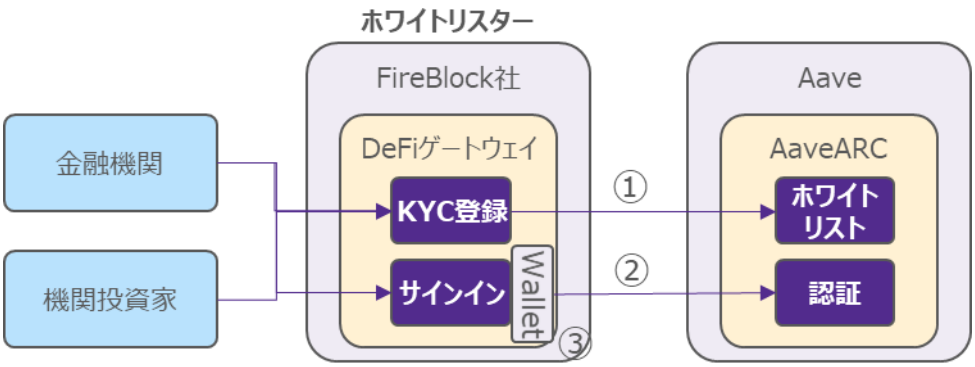

図 2-4-2-5-1　Aave Whitelister：FireBlock

【認証の流れ】

① Fireblocks 社のフレームワークで KYC を実行し、金融機関・機関投資家をホワイトリストに登録する

② ホワイトリスト登録を受けた者は、Fireblocks の DeFi ゲートウェイを介して AaveArc にアクセスする

③ Fireblocks 社のセキュアな MPC（Multi Party Computing) ウォレットを使用する

・30 の金融機関・機関投資家を登録済
Bluefire Capital、Celsius、CoinShares、Seba Bank、GSR、Ribbit Capital、
QCP Capital、Wintermute など

【Whitelister の具体例②：Securitize 社　SecuritizeID[111]】

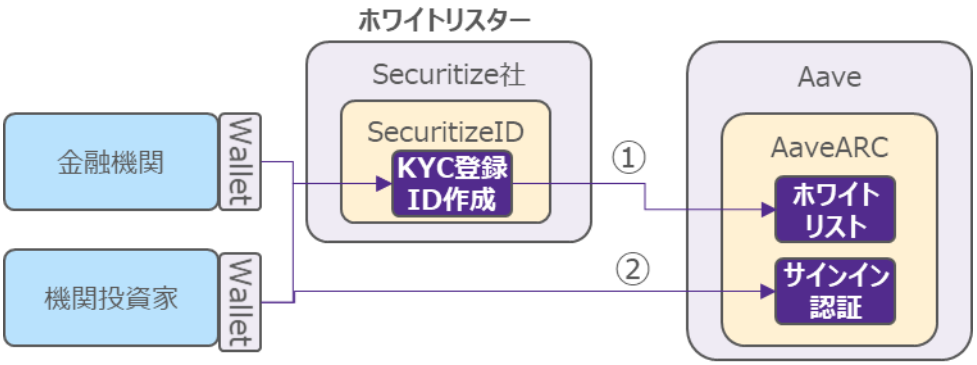

図 2-4-2-5-2　Aave Whitelister：Securitize

① 金融機関・機関投資家が自身のウォレットで SecuritizeiD を作成すると、当該ウォレットが AaveARC のホワイトリストにリンクされる

---

[110] Aave Governance Add Fireblocks as a whitelister on Aave Arc https://governance.aave.com/t/add-fireblocks-as-a-whitelister-on-aave-arc/5753

[111] Aave Governance ARC: Appoint Securitize as a Whitelister to Aave Arc https://governance.aave.com/t/arc-appoint-securitize-as-a-whitelister-to-aave-arc/6434

② 当該ウォレットから AaveArc にサインインして認証を取得すると、ウォレットアドレスに AaveArc で貸出・借入・清算等の取引を行うための権限が付与される

(8) オラクル[112]

・外部オラクルとして Chainlink と提携し、暗号資産の市場価格の情報を取得している。Chainlink は、分散型オラクルとして複数の市場価格から適正な価格を算出するサービスを提供している。

(8) スケーリング

表 2-4-2-8　Aave スケーリング

項目	概要	補足事項
Layer2 Solution	複数の LAYER2 ソリューションで Aave が利用できる ・Arbitrum ・zkSync ・Aztec 2.0	・プラットフォームにより、実行できる機能に制約が存在 ・プラットフォームにより、デプロイされているバージョンが異なる（例えば Ethereum では V2、Avalanche では V3）
ブロックチェーン	複数のブロックチェーンで Aave が利用できる ・Ethereum ・Avalanche ・Polygon ・Binance Smart Chain ・Fantom ・xDAI ・Heco ・Solana	

2-4-3　金融機関との連携

表 2-4-3　Aave：金融機関との連携

項目	概要	補足事項
金融機関との連携	・Taurus 社（スイスフィンテック企業）が AAVE と戦略的提携を結び、同社のデジタル資産インフラに AAVE V1・V2 を統合することで、顧客である金融機関や機関投資家向けに AAVE プロトコルへのアクセスを提供[113]（2021/3）	・主な顧客 - Sygnum Bank（スイス） - SEBA Bank（スイス） - Arab Bank Switzerkland（スイス） - Vontobel（スイス投資企業）
	・Sygnum Bank AG（スイスのデジタルバンク）が AAVE トークンを含む複数の DeFi トークン（ガバナントークン）及びステーブルコイン（USDC）のカストディ、トレーデ	・対象暗号資産：AAVE, UNI, ANT, CRV, MKR, SNX, 1INCH

[112] Aave Developers Price Oracle https://docs.aave.com/developers/v/2.0/the-core-protocol/price-oracle

[113] Taurus and Aave announce strategic collaboration https://blog.taurushq.com/taurus-strategic-collaboration-aave/

	ィングサービスを開始することを発表[114]（2021/6）	
	カストディおよびトレーディングサービスの開始（2021/11） ・Commonwealth Bank (オーストラリア)が Gemini Exchange、Chainalysis とパートナーシップを組んで、10 種類の暗号資産の交換（crypto exchange)とカストディサービスを開始	・Commonwealth Bank：1911 年創業 ・対象の暗号資産：BTC, ETH, BCH, UNI, LINK, MATIC, AAVE, COMP, LTC, FIL
	DeFi 関連銘柄の取引・カストディを提供（2022/1） ・Arab Bank Switzerland（スイス）が 10 種類の暗号資産のサービスを提供	・Arab Bank Switzerland：1962 年創業 ・対象の暗号資産：AAVE, FTM, COMP, SNX, LINK, MATIC, GRT, CRV, UNI, YFI

2-4-4　ガバナンス運営

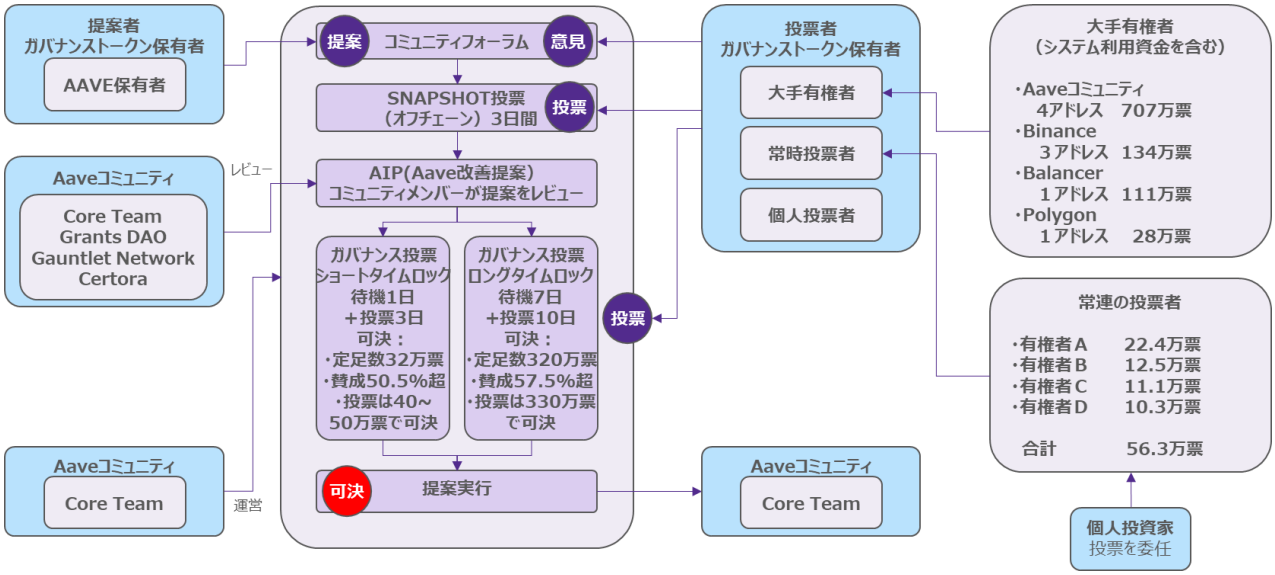

図 2-4-4　AAVE を用いたガバナンス投票プロセス

(1) コミュニティ

表 2-4-4-1　Aave：コミュニティの基礎情報

項目	概要
コミュニティの目的（公式ドキュメント	・Aavenomics に基づき、Aave プロトコルの分散化と自律性を向上させる

[114] Sygnum launches first phase of institutional-grade access to decentralised finance
https://www.insights.sygnum.com/post/sygnum-launches-first-phase-of-institutional-grade-access-to-decentralised-finance

の記載を要約）[115]	
コミュニティ組織形態	・ガバナンストークン AAVE 保有者による分散型自律組織（DAO） ・Aave コミュニティの運営は Core Team がリードする

(2) ガバナンストークン（AAVE）

表 2-4-4-2　Aave：ガバナンストークン

項目	概要	補足事項
AAVE の配布	・AAVE 総供給量の 1,600 万トークンのうち - LEND（旧ガバナンストークン）保有者への配布：1,300 万トークン - Ecosystem Reserve 資金（スマートコントラクトにロック）：300 万トークン	・2017 年 11 月に ETHLend として LEND トークンの ICO を実施、1,620 万ドルを調達[116] ・Aave v1 ローンチに伴い 100:1 の割合で LEND トークンを AAVE トークンへ転換[117]
AAVE 保有アドレス数[118]（2022/2 時点）	・AAVE 保有アドレス数　10 万 ・1 位保有率　18.54% ・上位 10 アドレス保有率　62.30%	・大手 AAVE トークン保有者（システム利用資金を含む） ①Aave プロトコル/ Ecosystem Reserve　4 アドレス　707 万票 ②Binance　3 アドレス　134 万票 ③Balancer　1 アドレス　111 万票 ④Polygon　1 アドレス　28 万票 ・AAVE 上位保有者うち、1 位-9 位はプロトコルや暗号資産交換所だが、この中から投票が行われる場合がある - 2021/5　ロングタイムロック提案の賛成 330 万票のうち、1 アドレスで 270 万票の投票があった。票数からみて 1 位保有者が投票したと思われる（提案内容：Aave Safety モジュールのインセンティブの終了日を 100 年延長する）
AAVE の機能	①オンチェーン投票における投票権（ガバナンストークン） ②AAVE プロトコルの安定化ツール - 債務超過に陥った際に SM に預けられた AAVE をオークションで売却して損失補填 - 一定額の AAVE 準備金として留保し、資金不足時の補填に活用	―

[115] Decentralizing Aave https://docs.aave.com/aavenomics/

[116] ETHLend Token Sale event successfully Closes With $16.2 million usd raised　https://medium.com/aave/ethlend-token-sale-event-successfully-closes-with-16-2-million-usd-raised-d0e0a1206141

[117] Aave Migration and Staking https://docs.aave.com/faq/migration-and-staking

[118] Etherscan Token Aave https://etherscan.io/token/0x7fc66500c84a76ad7e9c93437bfc5ac33e2ddae9#balances

(3) 意思決定

表 2-4-4-3　Aave：意思決定

項目	概要	補足事項
意思決定方法	提案を 3 段階に分けて意思決定を行う ①スナップショット投票　提案について賛成の動向を見る（温度チェック） ②AIP（Aave 改善提案）　コミュニティによる提案内容のレビュー ③ガバナンス投票　AAVE 保有者の投票により可決/否決を決定する	投票・提案は委任可能
ガバナンス投票の可決条件	①スナップショット投票（オフチェーン） - 投票期間：3 日 - 可決条件：提案の定足数 50 票超、かつ過半数の賛成で可決 ②AIP（オフチェーン） - 予め指定されたコミュニティメンバー（Core Team、Grants DAO、Gauntlet Network、Certora）が可否を判断 ③ガバナンス投票（オンチェーン） A.　ショートタイムロック ・提案内容 - 資産リスト、パラメータ更新、エコシステム支出などガバナンスに関連しない提案 - Aave プロトコル・料金徴収コントラクト・AAVE リザーブエコシステム・ - ショートタイムロックパラメータの変更など ・投票期間：待機期間 1 日、猶予期間 5 日、投票期間 3 日 ・可決条件：定足数 32 万票（全体の 2%）、投票数の 50.5%の賛成 B.　ロングタイムロック ・提案内容 - ガバナンスのコンセンサスに影響を与える Aave プロトコルの変更 - AAVE トークン・Aave プロトコルのアップグレード、ガバナンスパラメータの変更、ロングタイムロックのパラメータ変更など ・投票期間：待機期間 7 日、猶予期間 5 日、投票期間 10 日	・②AIP は投票ではなく、決められたコミュニティメンバーにより判断される ・③において、悪意のある提案が行われた場合の対策として、ガバナンス投票の待機時間内に Guardian が 5-of-10 のマルチシグ承認により提案をキャンセルできる仕組みが設けられている

	・可決条件：定足数 320 万票（全体の 20%）、投票数の 57.5%の賛成	
投票数実績（2021 年）	ガバナンス投票：53 件中 46 件可決（可決率 87%）	・ガバナンス投票 53 件のうち、ロングタイムロック提案は 2 件あり（1 件可決、1 件は定足数不足により否決）
ガバナンス投票で提案できる事項	①Aave プロトコル・料金徴収コントラクト・AAVE リザーブエコシステム・　ガバナンスパラメータ・投票パラメータの変更 ②AAVE トークン・Aave プロトコルのアップグレード ③コミュニティ資金の配布（助成金、報酬など） ④Guardian の推薦	―
Aave ガバナンスの投票者（2022/2 時点）	・常連の投票者（ほとんどの提案に同じメンバーが投票） ①有権者A　22.4 万票 ②有権者B　12.5 万票 ③有権者C　11.1 万票 ④有権者D　10.3 万票 合計　56.3 万票	・常連の投票者 4 名の票数合計が、ガバナンス提案（ショートタイムロック）の定足数 32 万票を超えている ・各投票者の個人情報は不明

(4) インシデント発生時の対応

表 2-4-4-4　Aave：インシデント発生時の対応

項目	概要	補足事項
インシデント発生時の緊急対応	・ガバナンス投票で悪意のある提案が行われた場合の対策として、待機時間内に、Guardian がマルチシグ承認により提案をキャンセルできる[119] ・外部攻撃などの緊急時に、Guardian がマルチシグにより、緊急キー（プロトコルの一時停止）を発動できる[120]	・マルチシグの承認はいずれも 5-of-10（Ethereum ブロックチェーン）
緊急対応の発動権限者	・Guardian10 名のマルチシグにより発動	・Guardian はガバナンス投票により決定（直近は 2021/9 に全員改選されている）
インシデントによる損害賠償	・インシデント発生などによる損害はユーザ責任であり、賠償は行わない	―

[119] AIP 4: Activation of Aave Protocol Governance V2 https://aave.github.io/aip/AIP-4/

[120] Authorize the Guardian to hold the emergency keys for V2 https://staging.aave.com/governance/proposal/49/

	（Terms of Use[121]に明記されている）	

(5) その他

表 2-4-4-5　Aave：ガバナンス運営その他事項

項目	概要	補足事項
AAVE 保有者の匿名性	・AAVE 保有者は原則として匿名であり、実在する主体の特定が困難 - AAVE の保有アドレスは特定できるが、大半のアドレスでは KYC が行われていないため実名とはリンクできないケースが多い ・ホワイトリストに登録された機関投資家は、KYC 済であり特定ができる	・意思決定に関わった AAVE 保有者を特定できず、責任の追及が困難である可能性

2-4-5　Aave の主なトラストポイント

(1)　AAVE Limited 、AAVE SAGL（関連法人）

・英 FCA から電子マネー業者ライセンスを取得している AAVE Limited（ライセンスの適用範囲等の詳細は不明）など関連法人が存在。

(2)　Gurdian（DAO）

・ガバナンス投票によって選出された 10 名で構成される Gurdian がマルチシグを管理し、ガバナンス提案のキャンセルやインシデント発生時等における緊急対応のための強い権限を有する。

(3)　ベンチャーキャピタル／大口ガバナンストークン保有者

・少数のガバナンストークン保有者が大半のガバナンス投票をコントロールしている実態が存在。

(4)　外部オラクル

・暗号資産価格等のデータを外部オラクル（Chainlink）から取得しているため、外部オラクルに機能不全等が生じた場合には担保清算等に影響が及ぶ可能性。

(5)　ホワイトリスター

・AaveARC ホワイトリストへ機関投資家等を登録するため、AAVE から認定された特定の企業が KYC 等を行う。

(6)　AIP（Aave 改善提案）レビュアー

・協力会社 2 社が、AIP（Aave 改善提案）のレビューに参加しており、AIP の信頼性を担保する役割を果たしていると考えられる。

(7)　コード監査会社

・ユーザはコード監査会社による監査結果を信頼してプロトコルを利用しているものと想定される。

[121] Aave.com Terms of Use https://aave.com/term-of-use/

(8)　ウォレット提供者

・（Maker に限らず DeFi 全般について、）Metamask など少数のノンカストディアル・ウォレットを多くのユーザが使用しており、ウォレットに脆弱性が存在した場合の影響度は大きいと考えられる。

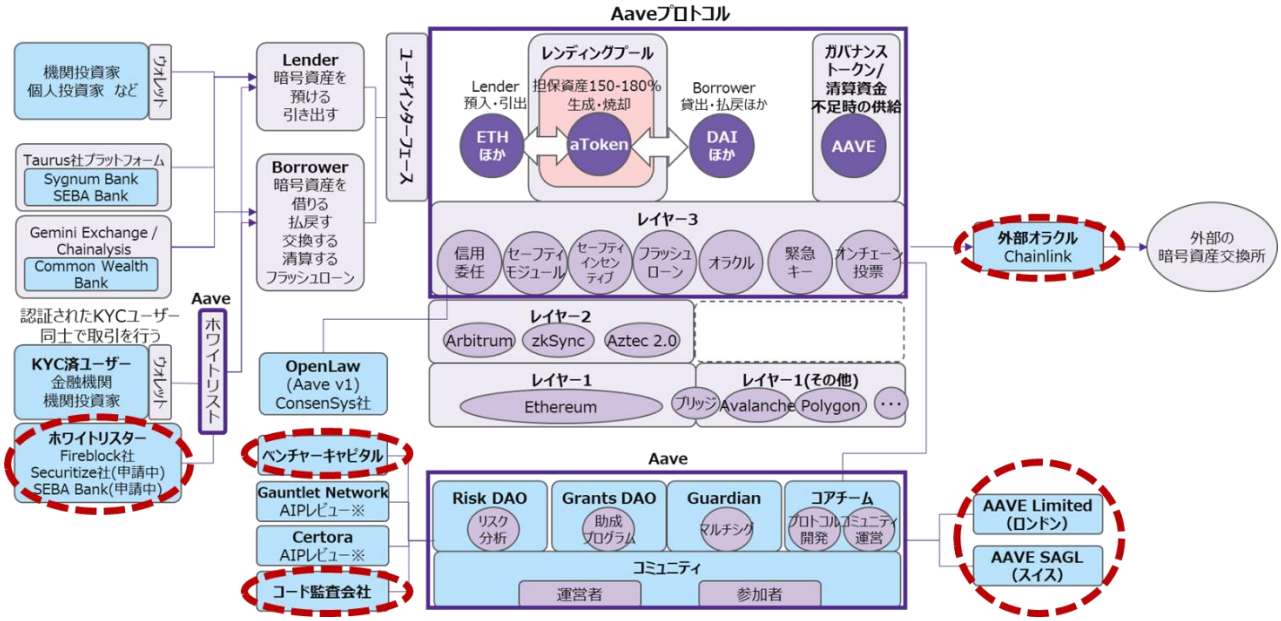

図 2-4-5-1　Aave の主なトラストポイント（構成要素）

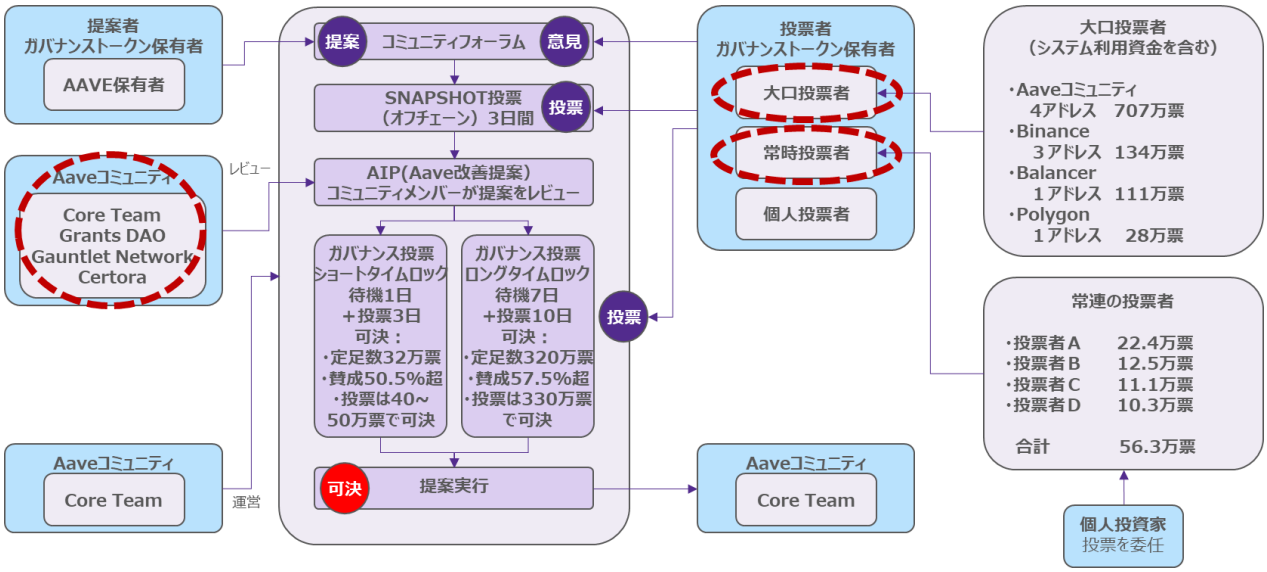

図 2-4-5-2　Aave の主なトラストポイント（ガバナンス投票）

2-5　調査対象プロジェクトの分析結果

調査対象の３プロジェクトについて、調査した組織、金融機関との連携、技術特性、ガバナンス運営について比較し、DeFi プロジェクト全体の傾向および個々の DeFi プロジェクトの特徴を分析する。

2-5-1　主要な DeFi プロジェクトの構成要素マッピング

調査対象とした３プロジェクトの主要な構成要素のマッピング結果より、構成要素を汎用的にした主要な DeFi プロジェクトの構成要素のマッピング例は以下となる。なお、マッピング例は調査対象の主な DeFI プロジェクトを基にした基本的な構成を示しており、特定のアプリケーションで構成されるサイドチェーンなど個別の要件は考慮していない。

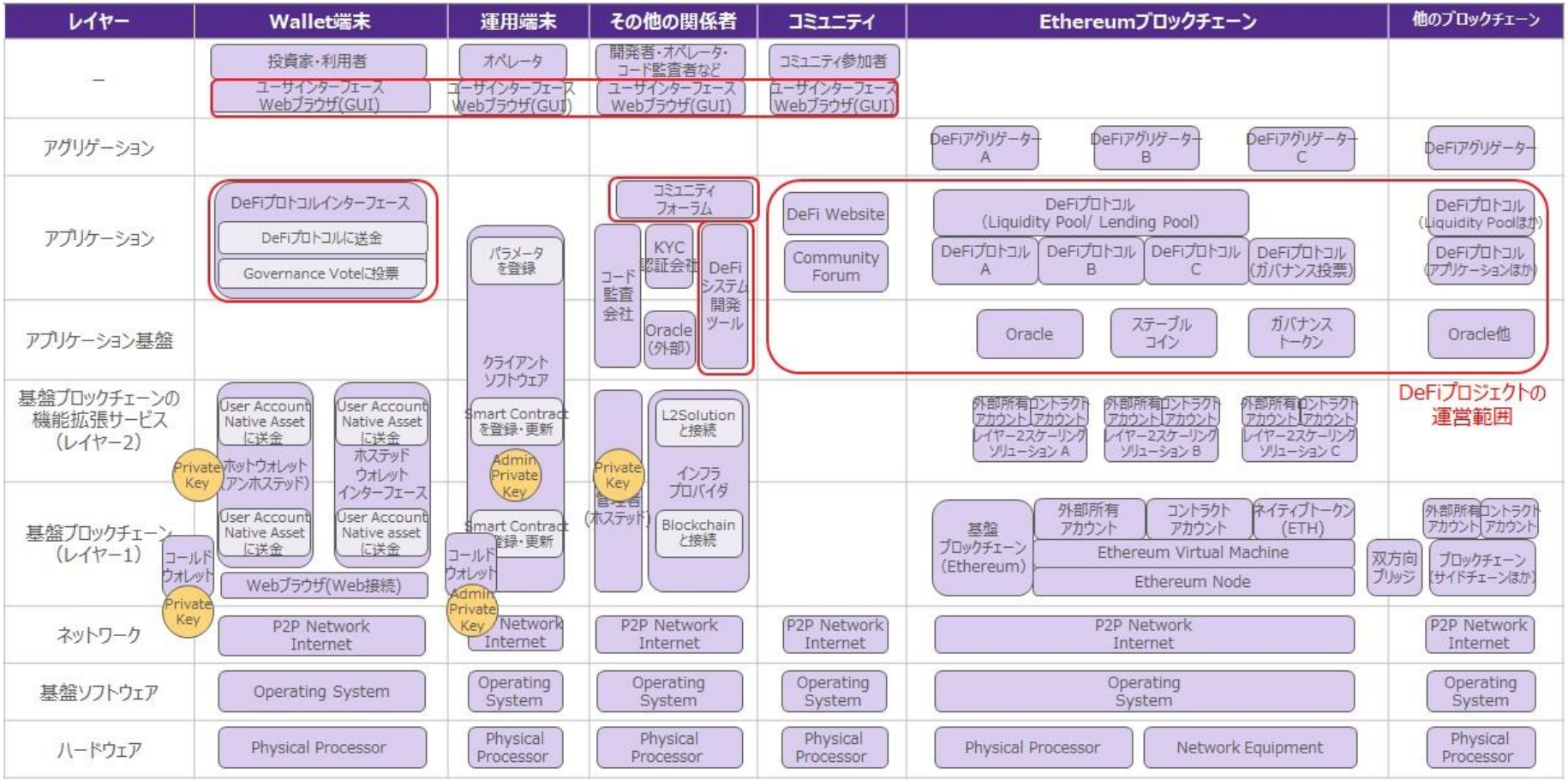

図 **2-5-1**　主要な **DeFi** プロジェクトの主な構成要素のマッピング

2-5-2　調査対象プロジェクトの分析結果の比較

調査対象の 3 プロジェクトの比較結果は表の通り。

表 2-5-2　調査対象プロジェクトの分析結果の比較

項目	内容	Uniswap	Maker	Aave
概要	提供サービス	分散型取引所（DEX）	ステーブルコイン（DAI）発行	暗号資産担保レンディング
	サービス開始時期	2018/11	2014/12	2017/5
	TVL（2022/2/13）	TVL 82.9 億ドル	発行残高 169.5 億ドル	TVL 074.4 億ドル
	手数料総額（2021 年）[122]	16.5 億ドル ・流動性プール手数料による収入 - UniswapV2 8.27 億ド UniswapV3 8.17 億ドル ほか	0.69 億ドル ・安定化手数料、清算ペナルティなどによる収入	3.10 億ドル ・貸出手数料による収入 - Aavev2 2.56 億ドル Aavev1 0.27 億ドル ほか
	ガバナンストークン	UNI（保有アドレス：27.6 万）	MKR（保有アドレス：8.3 万）	AAVE（保有アドレス：10.6 万）
コミュニティ・関連組織	創設者	Hayden Adams	Rune Christensen	Stani Kulechov
	コミュニティ	Uniswap コミュニティ（DAO）	MakerDAO	Aavenomics コミュニティ（DAO）
	コミュニティ運営	・ガバナンストークン保有者を中心とした運営 ・関連組織や DAO 内チームの一定のコミュニティ運営への関与あり		
		・Uniswap Labs が中心となってプロトコル開発・管理やインターフェースの運営・管理を行う	・コミュニティ内の組織がプロトコル開発・管理やコミュニティ運営を中心的に行う - ドメインチーム 5 チーム - コアユニット 22 チーム	・コミュニティ内の組織（コアチーム）がプロトコル開発・管理やコミュニティ運営を行う ・Guardian によるコミュニティマルチシグ（外部の有識者をガバナンス投票で承認。計 10 名）
	コミュニティの目的	・「UNI はコミュニティ主導の成長、開発、および自己完結の目的のために導入され、コミュニティの所有権と活気に満ちた多様で専	・「MakerDAO は世界をリードする分散型ステーブルコインである DAI の生成を可能にする分散型ガバナンスコミュニティ」	・「Aavenomics は Aave プロトコルの分散化と自律性への正式なパスを導入する」

[122] https://cryptofees.info/2021

	（公式ドキュメントの記載を要約）	用のガバナンスシステムを可能にするもの」 ・「トラストの最小化と中立性を受け入れ、ガバナンスが真に必要な場所に制限されることが重要」	・「分散型ガバナンスコミュニティは、Maker プロトコルに組み込まれたガバナンスメカニズムを通じて DAI の生成を管理する」	・「ガバナンスメカニズムと金銭的インセンティブをカバーし、Aave エコシステム内のさまざまな利害関係者、プロトコル機能、および Aave プロトコルのコアセキュリティ要素としての AAVE トークン間の調整のビジョンを共有することを目的とする」
	コミュニティ資金の管理	・Grants Program の資金を保有するウォレットの管理 - Grant Allocation Committee において、6 人の委員のうち 4-of-5 のマルチシグで承認される[123]	・コミュニティ資金を保有するウォレットの管理 - コアユニットのファシリテーターのうち 4 名が指名され、2-of-3 のマルチシグで承認される[124]	・コミュニティ資金を保有するウォレットの管理 - ドキュメント等に明示されていないが、コミュニティメンバー（Core Team や Grants DAO など）が管理者の秘密鍵を保有していると思われる ・Aave の Polygon マーケットのマルチシグ（3-of-5）の署名者が不明であり、1 人の Aave メンバーが 5 つの秘密鍵を保持している可能性があるとの指摘がされた。Aave コミュニティからの回答なし。（2021/5 DefiWatch より）[125]
	主な関連組織	・Uniswap Labs（米） - プロトコル開発・管理やコミュニティ運営への関与など	・DAI Foundation（デンマーク） - 知財管理等 ・RWA Company LLC（ケイマン諸島） - 実世界の資産への投資管理、クライアントとの契約締結等	・Aave Limited（英） - FCA から電子マネー業者ライセンスを取得済 ・Aave SAGL（スイス） - ソフトウェアメーカーとして登録

[123] Uniswap Grants Program v0.1 https://gov.uniswap.org/t/rfc-uniswap-grants-program-v0-1/9081

[124] MIP47: MakerDAO Multisignature Wallet Management https://mips.makerdao.com/mips/details/MIP47#sentence-summary

[125] Defi Watch Aave on Polygon has an admin key https://defiwatch.net/tag/aave/

			・Maker Ecosystem Growth Foundation（MEGF）（ケイマン諸島） - エコシステム、Oasis システム（ウォレット等）開発 - コミュニティとの情報連携	
	解散済組織	―	・Maker Foundation（デンマーク） - 2021/7 の解散に伴い Maker Foundation の資産は MakerDAO に移管され、業務は MakerDAO 内のドメインチーム／コアユニットが継承	―
	協力会社	―	―	・Gauntlet Network（米） - AIP（Aave 改善提案）のレビューに、リスクパラメータ評価貢献者として参加 ・Certora（イスラエル） - Aave ガバナンス提案の AIP（Aave 改善提案）のレビューに、セキュリティ貢献者として参加
技術特性	主な技術特性	・AMM（自動マーケットメーカー） ・Flash Swap ・流動性集約機能 ・手数料の拡張	・Maker Vault（DAI 生成） ・清算システム 2.0 ・Dai Direct Deposit Module（D3M） ・キーパー（マーケットメーカー・オークション） ・Flash Mint	・Aave interest bearing tokens (aToken) ・Flash Loan ・信用委任 ・Aave Arc／ホワイトリスター ・担保スワップ・担保返済
	オラクル機能	・オラクルを用いず、自己プロジェクト内で価格算出 - 暗号資産ペアの価格累積合計を取得して TWAP（時間加重平均価格）を計算	・自己プロジェクト内でオラクルの仕組みを構築 - 複数の外部市場の価格を「オラクル価格フィード」が取得 - 全体の中央値を算出し、1 時間後に内部価格に反映	・外部オラクルサービスに依存 - 分散型オラクルサービスの Chainlink を利用して市場価格および貸付レートを取得し、内部に反映

		- 全ての暗号資産ペアについて、取引が行われる前に市場価格を測定		
	アップグレード可否	・コアコントラクトは設計上アップグレード不可 - AMM、流動性集約機能、オラクル機能など） ・一部パラメータ（手数料）は変更可能 ・コア以外のコントラクト（手数料、周辺機能、インターフェース、ガバナンス投票など）は変更可能 - 開発会社がコード修正できる管理者権限（管理者の秘密鍵）を保有していると考えられる	・スマートコントラクトはアップグレード可能 - スマートコントラクトに事前にアップグレードが可能になる機能を組み込んでおくことにより対応 ・ドメインチームおよびコアユニットのファシリテーターが、コードのデプロイにおいて管理者権限を保有していると考えられる	・Guardian10 名のマルチシグによりコードのデプロイを承認 - Core Team の 3-of-5 マルチシグ管理であったが、2020/11 に Aave ガバナンスの管理に委譲
	対応ブロックチェーン（Scalability） ※プロトコルのデプロイ先及びトークンが利用可能なチェーン	・Ethereum ・Ethereum 2nd Layer ソリューション（Optimism、Arbitrum） ・サイドチェーン（Polygon）	・Ethereum ・Ethereum 2nd Layer ソリューション（Optimism、Arbitrum、Loopring、zkSync、Aztec2.0） ・サイドチェーン（avalanche、Polygon、BSC、Fantom、Klaytn、xDAI、Harmony、solana、Celo、Moonriver）	・Ethereum ・Ethereum 2nd Layer ソリューション（Arbitrum、zkSync、Aztec2.0） ・サイドチェーン（avalanche、Polygon、BSC、Fantom、xDAI、Heco、Sora）
	緊急時の対応(1)悪意のある提案のキャンセル	・詳細不明 - スマートコントラクト上は管理者による提案キャンセルが可能になっているが、提案キャンセル機能および実行できる管理者は定義されていない（緊急時は開発会社やコアユニットが実施することを想定か）		・ガバナンス提案をキャンセル可能 - 悪意のある提案が行われた場合の対策として、ガバナンス投票の待機時間内に、選ばれた権限者（Guardian）がマル

				チシグ承認により提案をキャンセルすることができる
	緊急時の対応(2) 緊急のスマートコントラクト修正	・コアコントラクトがアップグレード不可のため、原則対応不可	・ダークスペルメカニズムによる緊急修正が可能 - 重大な脆弱性の修正を行うためにスマートコントラクトを修正する仕組み。 - 特定の関係者のみで対応し、修正完了後一定期間が経過するまで内容を公表しない	・対応有無は不明 - ドキュメントに定義されていないため内容不明（緊急時はコアチームが実施することを想定）
	緊急時の対応(3) 攻撃を受けた時の対応		・緊急シャットダウンによるプロトコル停止が可能 - 一定数のガバナンス投票により、悪意のある攻撃からMakerプロトコルを保護する - 提案にかかわらず、いつでも投票できる	・緊急キーによるプロトコルの一時停止が可能 - 外部攻撃などの緊急時に、Guardianのマルチシグ承認により緊急キーを発動できる
コミュニティの意思決定	ガバナンストークン配布数	UNI：10億トークンを順次配布中（2020/9より4年間で配布中）	MKR：100万トークンを配布済（2022/1時点）	AAVE：1,600万トークンを配布済（2022/1時点）
	ガバナンストークンの初期配布 (1)無償配布	以下の割合で初期配布中 ・コミュニティメンバー　60% ・チームメンバー、従業員　21.266% ・投資家　18.044% ・アドバイザー　0.69%	100万トークンを配布および販売 ・一部をアーリーアダプターに配布	・旧LENDトークン保有者　1,300万トークン 内訳：Founder&Project　23% 投資家　77% ・リザーブ資金：300万トークン[126]
	ガバナンストークンの初期配布	なし	・ベンチャーキャピタルにICOで販売（Andreessen Horowitz, Polychain Capitalほか）	なし

[126] https://messari.io/asset/aave/profile/launch-and-initial-token-distribution

	(2)有償配付			
	ガバナントークン保有アドレス数	27.6 万アドレス	8.3 万アドレス	10.6 万アドレス
	ガバナントークンの役割	①オンチェーン投票	①オンチェーン投票 ②ステーブルコイン DAI の再資本化（DAI の追加・削除）に使用 ③清算資金不足時の資金（MKR を発行）として使用	①オンチェーン投票 ②清算資金不足時の予備資金（セーフティモジュール）として使用
	ガバナンス投票で提案できる事項 (1)アプリケーション	①スマートコントラクトの変更 ・コア以外のアプリケーション処理（流動性プールの追加変更、インターフェース、ガバナンス投票など） ・パラメータ値（手数料など）の変更	①スマートコントラクトの変更 ・アプリケーション処理（D3M、Vaults、清算システム、オラクルなど） ・パラメータ値の変更 - 新しい担保資産タイプの追加変更 - 既存のリスクパラメータの追加変　更 - DAI 貯蓄率の変更 ・システムのアップグレードの決定 ②オラクル価格フィードの選択	①スマートコントラクトの変更 ・アプリケーション処理（Lending、SM/SI、Flash Loan、信用委任など） ・パラメータ値（手数料など）の変更 ・システムのアップグレードの決定
	ガバナンス投票で提案できる事項 (2)ガバナンス	①コミュニティ運営の変更 ・コミュニティ資金の配布、ガバナンス投票の変更 ②コアコントラクト商用ライセンスの期間変更、免除	①コミュニティ運営の変更 ・コミュニティ資金の配布、ガバナンス投票の変更 ②緊急シャットダウンの実行（常時投票可）	①コミュニティ運営の変更 ・コミュニティ資金の配布、ガバナンス投票の変更 ②Guardian の推薦
	ガバナンス投票で提案できない事項	①スマートコントラクトの変更 ・システムのアップグレード（開発会社が実行）	－（特に制約なし）	－（特に制約なし）
	ガバナンス投票の流れ	・スナップショット投票とガバナンス投票の 2 段階投票 ①スナップショット投票 - 投票 2 日間、定足数 0.05%、50%以上賛成	・提案内容によりガバナンス投票とエグゼクティブ投票のどちらかを選択 ①ガバナンス投票	・スナップショット投票とガバナンス投票の 2 段階投票 ①スナップショット投票 - 投票 3 日間、定足数 50 票、50%以上賛成

		②ガバナンス投票 - 投票 5 日間、定足数 4%、50%以上の賛成	- 金額・利率や人選などスマートコントラクトの変更以外の方針等を決定） - 投票 7 日間、定足数 1%、50%以上の賛成 ②エグゼクティブ投票 - スマートコントラクトの変更部分のみを決定 - 投票 30 日間、定足数 1%、50%以上の賛成	②ガバナンス投票 - ショートタイムロック（ガバナンスに関連しない）：投票 3 日間、定足数 2%、50.5%以上の賛成 - ロングタイムロック（ガバナンスに影響する提案：投票 10 日間、定足数 20%、57.5%以上の賛成
		・提案可決後の待機期間 2 日間 ・待機期間中に管理者が提案をキャンセルできる ・待機期間終了後、管理者によりデプロイされる	・提案可決後の待機期間（B のみ 2 日間） ・待機期間中に権限者が提案をキャンセルできる ・待機期間終了後、誰でもデプロイできる	・提案可決後の待機期間 ①1 日間、②7 日間 ・待機期間中に選ばれた権限者（Guardian）が提案をキャンセルできる ・待機期間終了後、管理者によりデプロイされる
	ガバナンス投票率（2021 年実績）	・ガバナンス投票率　約 5-9%	・ガバナンス投票率　約 4-9%	・ガバナンス投票率　約 2-3%
	ガバナンス提案可決率（2021 年実績）	・スナップショット投票　77%（27/35 件） ・ガバナンス投票　86%（6/7 件）	・ガバナンス投票　90%（275/307 件） ・エグゼクティブ投票　100%（47/47 件）	・ショートタイムロック　88%（45/51 件） ・ロングタイムロック　50%（1/2 件）
	主な投票者	・大手トークン保有者　主に 10 団体 - ４大学（Berkelay, Stanford, Harvard, UCLA） - フィンテック（Gauntlet、Dharma、Kiva） - VC（Andreessen Horowitz, Monet Supply, Index Corp） → 個人投資家が投票権を委任できる	・投票代理人　18 アドレス - 公開代理人 9 アドレス - 非公開代理人 9 アドレス →個人投資家が投票権を委任できる ・大手個人投資家（匿名）	・大手トークン保有者　4 アドレス（システム利用資金を含む） - Aave - Binance - Balancer - Polygon ・常連の投票者　4 アドレス（匿名） - 当該 4 アドレスの投票により、①スナップショット投票

		・他の投票者　主に 3 名 - DeFi プロジェクト関係者（Ethrerum Foundation, Variant, Compound など）		の殆どの提案が意思決定されている - 個人投資家が投票権を委任できる
金融機関との連携	決済関連	デビットカードの決済資金に利用する ・Crypto.com - UNI・MKR・AAVE 等で商品購入（Shopping.io）や旅行（Travala.com）など約 30 店舗への支払いが可能		
		-	Monolith ・DAI を法定通貨に交換し、VISA デビットカードにロードして使用	-
	金融商品	・DeFi Technologies（カナダの Tech 企業）の子会社 Valour（スイス資産運用会社）を通して、UNI にパッシブ連動する ETP（上場投資商品）を上場 - ドイツフランクフルト株式市場：ユーロ建 Valour Uniswap ETP（2021/10） - スウェーデン株式市場：クローナ建 Valour Uniswap SEK（2021/12）	-	-
	カストディ・トレーディングサービス	・Sygnum Bank AG（スイスのデジタルバンク）が AAVE トークンを含む複数の DeFi トークン（ガバナンストークン）及びステーブルコイン（USDC）のカストディ、トレーディングサービスを開始することを発表（2021/6）		

		・Commonwealth Bank (オーストラリア)が Gemini Exchange、Chainalysis とパートナーシップを組んで、10 種類の暗号資産の交換（crypto exchange)とカストディサービスを開始（2021/11）	―	・Commonwealth Bank (オーストラリア)が Gemini Exchange、Chainalysis とパートナーシップを組んで、10 種類の暗号資産の交換（crypto exchange)とカストディサービスを開始（2021/11）
		・Arab Bank Switzerland（スイス）が 10 種類の暗号資産関連サービスを提供（2022/1）	―	・Arab Bank Switzerland（スイス）が 10 種類の暗号資産関連サービスを提供（2022/1）
	STO 不動産ローン ※STO：Security Token Offering		・Forge（仏 Société Générale のデジタル資産子会社）と STO による不動産ローンで提携（2021/10） ※DAI 発行計画における 6 つの事業体 ①Société Générale ②Forge ③MakerDAO プロトコル ④MakerDAO のリーガル代表者 ⑤DIIS グループ（仏債券投資家） 証券エージェントの役割 ⑥取引所	
	その他の取組み	・Fintech 企業とタイアップして市場参入を検討中との報道（2021/7） - PayPal - Robinhood（米株式運用アプリ運営） - E*Trade（米オンライン証券会社） - Stripe（米オンライン決済）等	・チャリティに寄付する（USD として支払う） - ユニセフ（慈善団体） - NeedsList（災害支援） - PoolDai（慈善団体寄付基金） ・給与ソリューション - Whisp Money（一部のコミュニティでは KYC が不安定な外	・AaveARC - 財務デューデリジェンスを受けた機関投資家が、他に承認を受けた機関投資家と暗号資産を貸借できるようにする機能 ・ホワイトリスター - AaveARC ホワイトリストに登録する機関投資家を登録する

			部雇用者に DAI で給与支払を行っている）	ために Aave から承認された会社 登録済：米 Fireblocks 社（2022/1） 登録手続中：米 Securitize 社、スイス SEBA Bank

2-6　他の DeFi プロジェクトの主なインシデント事例分析結果

調査対象の３プロジェクト以外で発生した主なインシデントについて、その概要と発生理由、問題点と対応内容を説明する。

2-6-1　The DAO Attack

The DAO とは 2016 年 4 月に Slock.it 社（ドイツ）がデプロイした Ethreum 上の分散型投資ファンドであり、最初期の DAO とされる。参加者は ETH を The DAO に送金することと引き換えに DAO トークンを受領し、当該トークン保有者により投資対象が投票で決定され、投資リターンが報酬として配分される仕組みであった。この The DAO において 2016 年 6 月に発生したリエントランシー脆弱性を狙った攻撃、及びその対応策として実施された Ethereum のハードフォークについて、その概要と発生理由、問題点を説明する。

(1) 発生日：2016 年 6 月 17 日
(2) 事件の概要
　攻撃者は、The DAO の報酬送金機能の脆弱性を利用して、親 DAO に紐づく自身の子 DAO（自分専用の資金の払出用アドレス）に大量の報酬を送金して 360 万 ETH を獲得した。但し、子 DAO の資金は 27 日間移動できない仕様であったため、その前に Ethereum のハードフォーク（取引の無効化）を行うことで被害を回避した。
(3) 損害額：ハードフォークにより被害なし。一時的に窃取された被害額は約 7,000 万ドル (360 万 ETH)
(4) 事件の流れ[127]

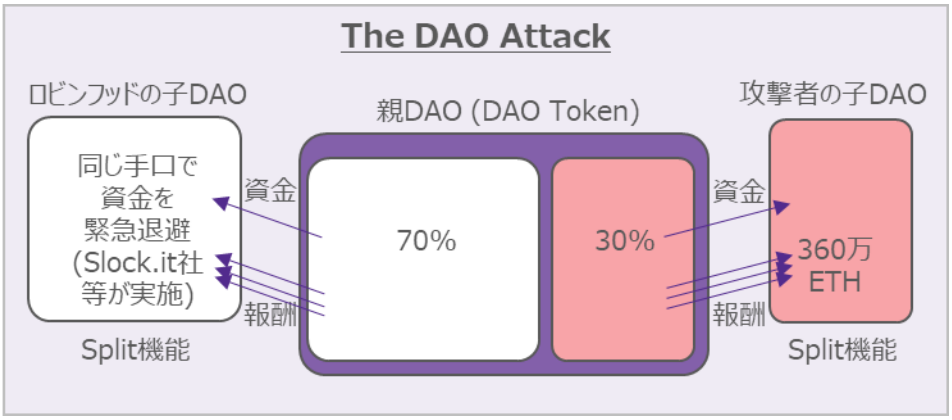

図 2-6-1　The DAO Attack

1. The DAO[128]の Split 機能[129]を利用し、親 DAO から独立した自身の子 DAO を作成。
2. Split 機能の脆弱性を悪用し、親 DAO から子 DAO への資金移動に伴う親 DAO の残高が更新される前に、報酬の送金を自動的に繰り返すスマートコントラクトを埋め込み、自身の保有分以上の資金を子 DAO に何度も送金して合計 360 万 ETH を獲得した。
3. 緊急対策として防御者が「RobinHoodGroup」を立ち上げ、攻撃者と同じ手法により、全体の 70%の資金を退避した。（攻撃者よりも多い報酬を得るように工夫して資金を素早く対比した）

---

[127] SEC Report；https://www.sec.gov/litigation/investreport/34-81207.pdf
Harvard Law School Report：https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3014782

[128] The DAO：Slock.it 社（ドイツ）が設立した自律分散投資ファンド

[129] Split 機能：ある投資提案に反対するユーザが、投資資金プールである親 DAO から自身の資金を切り離し、子 DAO に分割できる機能。Split 機能による子 DAO 作成には、キュレーターの承認および DAO 投票（1 週間）による承認が必要。

4. Split 機能を使った子 DAO にある資金は、27 日間は移動ができないという制約があったため、攻撃者は 360 万 ETH の資金を子 DAO から移転させることはできなかった。
5. 事件の解決策として以下３案が検討され、③ハードフォーク[130]が実行された。
   ①フォークを行わず、資金を攻撃者に明け渡す
   ②ソフトフォークを行い攻撃者のアカウントを凍結
   ③ハードフォークを行い取引自体をなかったことにする
6. ハードフォークの反対派が Ethereum の内部で分裂し、元の取引記録を維持した Ethereum Classic が誕生した。

表 2-6-1-1　The DAO 設立からインシデント発生までの経緯

日付	イベント	内容	補足
2015/11	DAO の提案	ドイツ企業 Slock.it UG が立ち上げた投資ファンド組織 The DAO が、「クラウドファンディング」と称して仮想通貨 ETH との交換によって DAO トークンを発行することを表明した	ロンドンで開催された Ethereum Developer Conference で、Slock.it 社 CEO の Christoph Jentzsch は、DAO の提案を「営利目的の DAO」として説明した
2016/4/29	The DAO コードのデプロイ	Slock.it 社は、Ethereum ブロックチェーンに DAO コードをデプロイした	－
2016/4/30 ～2016/5/28	DAO トークンの提供・販売	DAO トークンの提供および販売を開始した 提供期間中、DAO は合計約 1,200 万 ETH と引き換えに約 11.5 億 DAO トークンを販売した（当時の評価額は約 1 億 5,000 万ドルと評価）	トークンの価格は、提供期間中にトークンを購入した時期に応じて、100DAO トークンあたり約 1～1.5ETH の範囲で変動した （注）DAO トークンは有価証券であるため、本来は DAO トークンの提供と販売を登録する必要があったと米 SEC が 2017 年 7 月の報告書において指摘
2016/5/26	The DAO コード脆弱性の表面化とセキュリティ提案	スマートコントラクトのコードに欠陥があることを GitHub のユーザが発見 このユーザは、Ethereum 開発者と Bitcoin Foundation 創設者の Peter Vessenes に通知した これらの懸念に応えて、Slock.it 社は The DAO のコードの特定の更新の開発とセキュリティ専門家の任命を求める「DAO セキュリティ提案」を公表した	Slock.it 社は当初、「DAO セキュリティ」グループの結成、「バグ報奨金プログラム」の設立、DAO のコードに対する定期的な外部監査などを含む、より広範なセキュリティ提案を行っていたが、この提案にかかる費用（125,000ETH：The DAO の資金から支払われる）が即座に高すぎると批判され、Slock.it は提案を修正して提出することにした
2016/6/3	DAO 提案の一時停止提案	Slock.it 社 CEO の Christoph Jentzsch が、Slock.it 社を代表して、DAO のコードの脆弱性を修	－

[130] ハードフォーク：フォーク以降の後方互換性を保証しないアップデート。ルールを書き換えるため、永続的な分岐となる。

		正するための変更が実装されるまで、すべての投資提案を一時停止することを提言した	
2016/6/12	DAO 脆弱性の公表	The DAO のスマートコントラクトに脆弱性があることを Slock.it 社が発表した 同日に GitHub にコードのアップデートがあった	Slock.it 社は The DAO の脆弱性の回避策が作成され、もはや脆弱性のリスクにさらされている DAO ファンドはないと述べた 但し、回避策のコードは開発されたがデプロイされなかった
2016/6/17	DAO 事件発生	攻撃者が約 360 万 ETH（DAO オファリングによって調達された ETH の 30%）を窃取	窃取された ETH は攻撃者が制御するアドレスに保持されたが、攻撃者は DAO のコードによって、27 日間は ETH をそのアドレスから移動できなかった
―	DAO 資金の流出防止	スマートコントラクトを更新する迅速な解決策がなかったため、The DAO の利害関係者は「RobinHoodGroup」を構成。コミュニティや投資家から 6 万ドルの DAO トークンを寄付で集め、攻撃者と同じ手口を使って資金の 70%を回収した	「RobinHoodGroup」の主要メンバー Slock.it 社コミュニティマネージャー　Griff Green Ethereum 開発者　Alex Van de Sander Slock.it 社 CEO　Christoph Jentzch　など
2016/6/28 ～2016/7/15	解決策の検討	窃取された 360 万 ETH について、解決策として以下の 3 案が議論された 1. 何もしない 　攻撃者は 360 万 ETH を獲得する 2. ソフトフォーク 　攻撃者の子 DAO を凍結し、移転できないようにする。但し、360 万 ETH は投資家に戻らず、投資家の損失となる 3. ハードフォーク 　窃取された 360 万 ETH を含む全ての投資家の資金を The DAO から回復用アドレスに移すことで、投資家の損失を回避する	・ハードフォークは、Ethereum Foundation が提案した緊急計画であり、取引の巻き戻しは不可能であるべきというブロックチェーンの理念に反する提案であるとして、コミュニティ内で大きな議論となった ・ハードフォーク賛成派の意見 - 人間が社会的なコンセンサスを通じて最終的な判断を下すべき。 - 攻撃者が利益を得ることは倫理的に間違っておりコミュニティの介入が必要。 - ETH を攻撃者の手に残しておくと将来的にその価値が下がる可能性がある。 ・ハードフォーク反対派の意見 - 取引の巻き戻しが「Code is Law」「信頼性」「不変性」というブロックチェーンの理念に反している。 - Ethereum ブロックチェーンの本来の目的を損な
2016/6/24	ソフトフォークの検討～断念	Ethereum Foundation とコミュニティは、当初はソフトフォークによる解決を目指したが、ソフトフォークのコードに DoS 攻撃を可能にする欠陥が見つかり、ソフトフォークを実施しないことを決定した	
2016/7/15	ハードフォークの決定	投票プラットフォームに少額の ETH を送る形式でハードフォーク案の投票が行われ、可決された	

2016/7/20	ハードフォークの実施	Ethereum ブロックチェーンのノードの大部分が必要なソフトウェアアップデートを採用した後、新しいフォークされた新たな Ethereum ブロックチェーンがアクティブになった	い、コードベースのルールが人間の利益に左右されてしまう。
2016/7/20	Ethereum Classic の誕生	ハードフォークの数時間後に、ハードフォーク反対派が元のブロックチェーンの採掘を再開し、Ethereum Classic が誕生した	－

(5) 発生原因

・現象的要因

①リエントランシー脆弱性
　The DAO のスマートコントラクトがリエントランシーの可能性を考慮しておらず、資金と報　酬を送金した後に内部トークン残高を更新していた。

②動いているスマートコントラクトをアップデートする仕組みが欠けていた。

・動機的要因
Slock.it 社が上記②の認識に欠けており、攻撃される前に修正コードのデプロイに至らなかった。

(6) インシデントの問題点

表 2-6-1-2　The DAO Attack インシデントの問題点

区分	種別	問題点の内容	インプリケーション
現象的要因	デプロイメント	DAO 報酬送金機能にリエントランシーの脆弱性があった ・DAO スマートコントラクトが資金送金後に内部トークン残高を更新する設計だったため、トークン残高を更新する前に別の関数を呼び出すことで、トークン残高を更新することなく再度送金が行えてしまう脆弱性が存在した	・脆弱性攻撃により参加者が金銭的な損害を受ける
		DAO ソースコードの脆弱性をコード監査で事前に発見できなかった ・セキュリティ監査会社にソースコードのレビューを受けていたが、脆弱性を発見できなかった （参考）SEC 報告：「DAO のソースコードが「世界をリードするセキュリティ監査会社の 1 つ」によってレビューされ、5 日間のセキュリティ分析の間に何の問題も残されなかった」	
		デプロイ済のスマートコントラクトを緊急でアップデートする仕組みが欠けていた	・緊急時にスマートコントラクトをアップデートで

		・事件前にコードの修正がデプロイされていたが、アップデートにはソフトフォーク／ハードフォークが必要であり、事件発生時に緊急のアップデートができなかった	きず、攻撃が防御できない
	ガバナンス	組織として脆弱性を認識していたが、対策を積極的に行っていなかった ・Slock.it 社はコードの脆弱性を事前に認識して発表し、脆弱性の回避策が作成され脆弱性のリスクにさらされている DAO ファンドはないと述べたが、回避策のコードはデプロイされなかった ・Slock.it 社は当初は広範なセキュリティ提案を行っていたが、この提案にかかる費用が高すぎると批判され、対策を限定していた	・脆弱性を公表したが対策を行わず攻撃を受けてしまう結果に
動機的要因	オペレーション	キュレーター（フェイルセーフ機能となる管理者）に権限が集中していた ・キュレーターは Slock.it 社が指名した個人であった ・キュレーターが主観的な基準で判断することができた - 投資提案の採否・時期・順序・頻度・投票定足数の半減の決定（キュレーター解任提案を含む）など	・創業会社やキュレーターの意思通りに投資案件を決めてしまい、参加者の意思が反映されない ・参加者がキュレーターを事実上解任できない
		DAO トークンの議決権が制限されていた ・キュレーターが参加者（DAO トークン保有者）に対して提案に関する情報を十分に提供していなかった ・参加者が匿名であり、団結してキュレーターに対抗することが困難であった	・参加者の不利益による改善活動が発動できず、創業会社・キュレーターに頼らざるを得ない
	ガバナンス	事件の解決策としてソフトフォーク／ハードフォークが検討され、ブロックチェーンの理念（Code is Law, 信頼性、不変性）に反した根幹を揺るがす事態となった	・ブロックチェーンの理念と人間の利益（人為的介入による被害回復）とのトレードオフ
		DeFi プロジェクトの事件が Ethereum プラットフォーム全体に影響を及ぼした ・攻撃を受けたのは The DAO であるが、解決策として Ethereum プラットフォームがハードフォークを行うことになった ・Ethereum のハードフォークにより、The DAO と関係しない Ethereum 上のアプリケーションも影響を受けた	・DeFi プロジェクトの不具合がプラットフォーム全体に影響を及ぼす ・プラットフォームの対応により、他のアプリケーションにも影響を及ぼす
	コンプライアンス	グローバルなプラットフォーム上の事件に対する国際的なルールが未制定 ・Ethereum はグローバルなプラットフォーム（Ethereum Foundation はスイスの非営利団体）であり、それ自体が登録し	・登録国以外の参加者が法的に保護されない ・事件発生時のグローバルな捜査・対応が円滑にできない

		ている国しか規制がかけられない（各国の法規制が及ばない） ・Ethereum で事件が発生した場合に、どう捜査・対応するか等の国際的な合意がない	
		The DAO が証券取引所として登録されていなかった ・DAO トークンの売買プラットフォームを提供しているという点で、The DAO は米国の証券取引所の定義を満たすため、登録が必要であった可能性	・投資家保護上の懸念
		DAO トークンの販売登録がされていなかった ・DAO トークンは米国証券取引委員会（SEC）に有価証券と判断され、DAO トークンの販売を登録する必要があった	・投資家保護上の懸念

2-6-2　Flash Loan Attack #1

2020 年 2 月に証拠金取引及びレンディングプラットフォームである bZx[131]で発生した Flash Loan Attack のインシデント事例について、その概要と発生理由、問題点を説明する。

(1) 発生日：2020 年 2 月 15 日
(2) 損害額：約 35 万ドル
(3) 事件の概要
　bZx の証拠金取引スマートコントラクトの脆弱性を攻撃して、ETH の大量交換により故意に WBTC 価格を高騰させ、アービトラージにより 1,271ETH を窃取した。
(4) 事件の流れ[132]

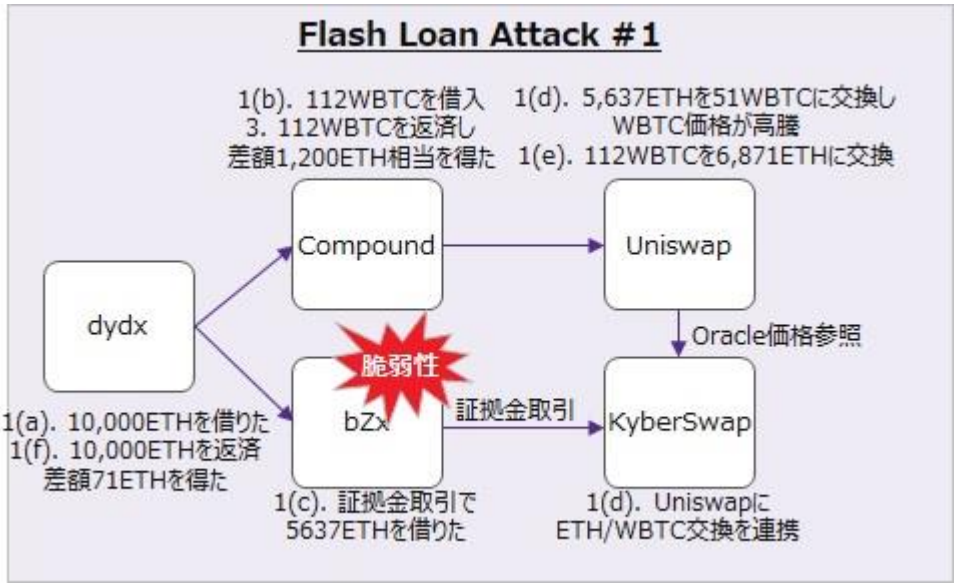

図 2-6-2　Flash Loan Attack #1

131 https://bzx.network/

132 https://peckshield.medium.com/bzx-hack-full-disclosure-with-detailed-profit-analysis-e6b1fa9b18fc
https://bzx.network/pdfs/CertiK_Review_Report_for_bZx_v2.pdf

1. Flash Loan により以下(a)-(f)を 1 トランザクションで連続実行した。
   a) dYdX[133]から、Flash Loan で 10,000ETH を借りた。
      （Flash Loan 機能を提供している主な DeFi：Aave、dYdX、Equalizer など）
   b) Compound[134]から、5,500ETH を担保として 112WBTC[135]を借りた。
   c) bZx から、1,300ETH を担保として証拠金取引で 5,637ETH を借りた。
      （約 4.3 倍のレバレッジ）
   d) Zx で借りた 5,637ETH を、KyberSwap[136]で 51WBTC に交換した。
      KyberSwap は、提携する複数の分散型交換所のうち Uniswap で ETH を WBTC に交換した。ETH を大量に交換したことにより Uniswap の WBTC 価格が通常時の約 3 倍に高騰した。
      （Uniswap の交換レート：通常時の 38ETH/WBTC　→　約 3 倍の 109ETH/WBTC に高騰）
   e) Uniswap の WBTC 価格が高騰したところを狙って、Uniswap で Compound から借りていた 112WBTC を ETH に交換し、6,871ETH を得た。
   f) dYdX で、Flash Loan で借りていた 10,000ETH を返済し、差額として利益 71ETH を得た。
      （利益 71ETH＝交換した 6871ETH＋未使用の 4,200ETH－返済した 10,000ETH）

2. その後、WBTC 価格が通常時に戻り、38ETH/WBTC になった。

3. Compound で借りていた 112WBTC を返済し、4,300ETH で清算。担保との差額として利益 1,200ETH 相当の WBTC を得た。

(5) 発生原因

・bZx の証拠金取引スマートコントラクトの脆弱性を突かれた攻撃のため。
bZx 証拠金取引機能を利用して大量の ETH を WBTC に交換し、WBTC 価格が高騰（ETH 価格が下落）していたにも関わらず ETH の担保不足でポジション清算がされない脆弱性により、故意に WBTC 価格を高騰させてアービトラージで差額を窃取された。

表 2-6-2　Flash Loan Attack #1 インシデントの問題点

区分	種別	問題点の内容	存在するリスク
現象的要因	デプロイメント	bZx の証拠金取引スマートコントラクトに脆弱性があった ・bZx 証拠金取引が ETH の担保不足でポジション清算がされない脆弱性により、故意に WBTC 価格を高騰させた - 2/15 にインシデント発生後、一旦システムを停止し、2/16 にスマートコントラクトのアップグレードを発表した（2/17 に修正を反映した）	・脆弱性攻撃により参加者が金銭的な損害を受ける ・攻撃により被害が広がることで該当の暗号資産の信頼度や投資が低下する ・攻撃が多発すると、DeFi 市場全体の信頼度が低下してしまう
		bZx ソースコードの脆弱性を事前に発見できなかった ・コード監査会社にソースコードのレビューを受けていたが、脆弱性を発見できなかった	

[133] dYdX：証拠金・デリバティブ取引のための DeFi プラットフォーム：https://dydx.exchange/
[134] Compound：AAVE に次ぐ TVL を有するレンディングプラットフォーム：https://compound.finance/
[135] WBTC：Wrapped BTC Ethereum 上で Bitcoin と連動するステーブルコイン
[136] Kyberswap：分散型取引所の DeFi プラットフォーム：https://kyberswap.com/about/kyberswap

		- 2020/2 に CertiK 社が監査しており、重大な脆弱性はないが改善情報 6 点を指摘している。但し、今回の原因となった脆弱性は検出していない	
動機的要因	デプロイメント	デプロイの方法が投票と緊急時の 2 つあり、運営に課題がある ・通常時はガバナンストークンの投票により承認されるが、緊急ではない脆弱性の修正は定期アップデートに含まれ、対応に時間がかかる（脆弱性の修正は投票で決めるべきではない） ・緊急時は投票なしにデプロイが可能であり、開発者の故意など抜け道ができてしまう	・定期アップデートの脆弱性対応を修正前に攻撃されることによる参加者の損害 ・該当する暗号資産の信頼度低下
	ガバナンス	ガバナンストークン（BZRX）の投票による運営を行っていたが、実態は創設会社「bZeroX, LLC」のコア Founder とチームメンバーが管理しており、意思決定権限が一元化されていた （当インシデントとガバナンス問題との関係は特になし）	・創業会社やコア Founder 等による意図的な提案により、参加者が損害を受ける

※ガバナンス問題の対策として、bZx ガバナンスルールを改訂した（2021/8 運営開始）[137]
- ガバナンストークン（BZRX）の投票により提案を承認するプロセス
  ステージ 1：フォーラムディスカッション　　提案を出してレビューを受ける
  全体の 0.5%（515 万 BZRX）の同意が必要（2 日間）
  ステージ 2：スナップショット投票
  賛成 50%以上＋全体の 4%（4,120 万 BZRX）の同意が必要（3 日間）
  ステージ 3：オンチェーンガバナンスの決定
  TimeLock の後に提案内容が実装される（2 日間）最短で計 7 日間
- 提案する項目
  資金提供、手数料、トークン関連、エコシステム関連、マーケティング、開発ロードマップ／機能の優先付け、給与と人事移動

2-6-3　Flash Loan Attack #2

2020 年 2 月に 2-6-2 のインシデント直後に再度 bZx で発生した Flash Loan Attack のインシデント事例について、その概要と発生理由、問題点を説明する。

(1) 発生日：2020 年 2 月 18 日

(2) 損害額：63.3 万ドル（2,378ETH）

(3) 事件の概要
bZx の Oracle 脆弱性を攻撃して、ETH の大量交換により故意に sUSD[138]価格を高騰させ、アービトラージにより 2,378ETH を窃取した。

[137] https://bzx.network/blog/bzx-dao
https://bzx.network/pdfs/CertiK%20Verification%20Report%20for%20bZx.pdf
[138] sUSD：Synthetix の暗号資産名

(4) 事件の流れ[139]

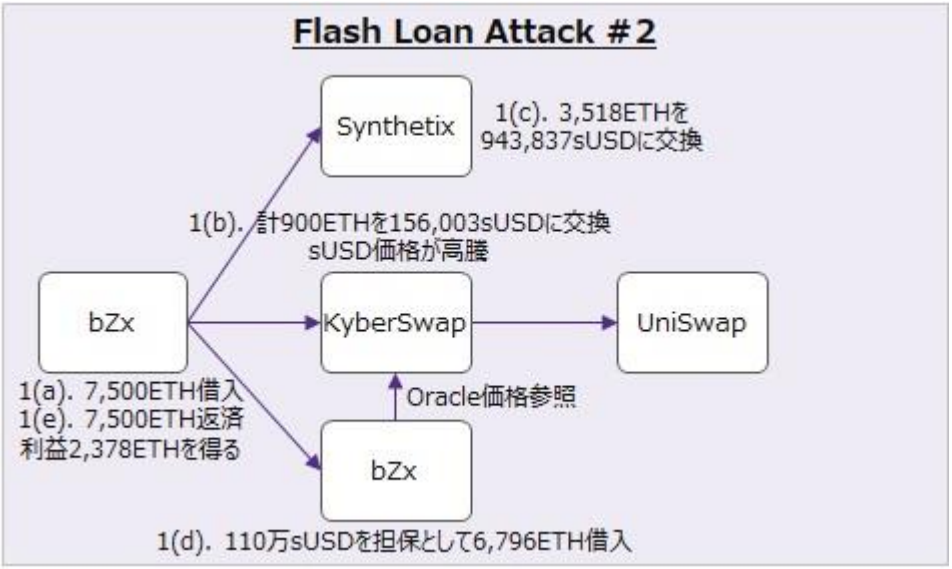

図 2-6-3　Flash Loan Attack #2

1. Flash Loan により以下(a)-(e)を 1 トランザクションで連続実行した。

a) bZx から、7,500ETH を Flash Loan で借りた。

b) KyberSwap で、540ETH を 92,419sUSD に交換。続けて 360ETH を 63,584sUSD に交換。（合計 900ETH を 156,003sUSD に交換）。KyberSwap は、提携する複数の分散型交換所のうち
Uniswap で ETH を sUSD に交換した。これにより、KyberSwap の sUSD 価格が約 3 倍に高騰した。
（KyberSwap の交換レート：通常時の 0.00372ETH/sUSD　→　約 3 倍の 0.00899ETH/sUSD に高騰）

c) Synthetix[140]で、6,000ETH を sUSD に交換。sUSD 不足のため、3,518ETH を 943,837sUSD を交換し、2,482ETH が払戻しとなった。（交換レート：通常時の 0.00372ETH/sUSD）

d) bZx から、110 万 sUSD を担保に 6,796ETH を借りた。通常時の sUSD 価格では約 4,000ETH が借入限度となるところ、bZx が KyberSwap を Oracle 参照しているため、sUSD の高騰により 6,796ETH を借りることができた。（攻撃者は借りた状態のまま返済せずに放置）

e) bZx に借りた 7,500ETH を返済し、利益 2,378ETH を得た。
（利益 2,378ETH＝借りた 6,796ETH＋未使用の 3,082ETH－返済した 7,500ETH）

(5) 発生原因

・bZx が Oracle 価格参照を KyberSwap に依存していたことにより、kyberSwap で sUSD 価格を故意に高騰させ、通常価格との相違が大きくなったところをアービトラージにより差額を窃取された。

表 2-6-3　Flash Loan Attack #2 インシデントの問題点

139 https://peckshield.medium.com/bzx-hack-ii-full-disclosure-with-detailed-profit-analysis-8126eecc1360

140 Synthetix：分散型取引所の DeFi プロジェクト

区分	種別	問題点の内容	存在するリスク
現象的要因	デプロイメント	bZx の Oracle 参照に脆弱性があった ・bZx が KyberSwap に Oracle 価格参照を依存していたことにより、KyberSwap で sUSD の価格を故意に高騰させ、通常価格との相違が大きくなったところを狙われた	・脆弱性攻撃により参加者が金銭的な損害を受ける ・攻撃により被害が広がることで該当の暗号資産の信頼度や投資が低下する ・攻撃が多発すると、DeFi 市場全体の信頼度が低下してしまう
		bZx の Oracle 参照の脆弱性を事前に発見できなかった ・コード監査会社にソースコードのレビューを受けていたが、脆弱性を発見できなかった - 2020/2 の CertiK 社の監査では、今回の原因となった脆弱性は検出していない	
動機的要因	―	2-6-2 Flash Loan Attack #1 と同じ	―

2-6-4　マネー・ローンダリング

2020 年 9 月に発生したマネー・ローンダリングのインシデント事例についで、その概要と発生理由、問題点を説明する。

(1) 発生日：2020 年 9 月 26 日

(2) 損害額：約 2 億 7,500 万ドル

(3) 事件の概要

・シンガポールの暗号資産取引所 KuCoin[141]から、取引所の管理者のホット・ウォレット秘密鍵が盗まれて約 2 億 7,500 万ドル相当の暗号資産が窃取された。

・その資金は 200 以上の Bitcoin や Ethereum,その他ブロックチェーンの交換所などに分散して送金された。

・Chainalysis 社（ブロックチェーン分析会社）の調査では、攻撃は Lazarus Group という北朝鮮のサイバー犯罪集団によるものと発表されている。

・同年 11 月には、各交換所などによる資産凍結、警察の協力などにより 2 億 400 万ドルは回収され、保険による補償を含めて被害のほぼ全額を補填した。

(4) 事件の流れ[142]

[141] KuCoin：香港の暗号資産取引所

[142] https://www.kucoin.com/news/en-kucoin-ceo-livestream-recap-latest-updates-about-security-incident
https://www.kucoin.com/news/en-kucoin-ceo-livestream-recap-latest-updates-about-security-incident-0930
https://www.kucoin.com/news/en-the-latest-updates-about-the-kucoin-security-incident
https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap-japanese
https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack-japan

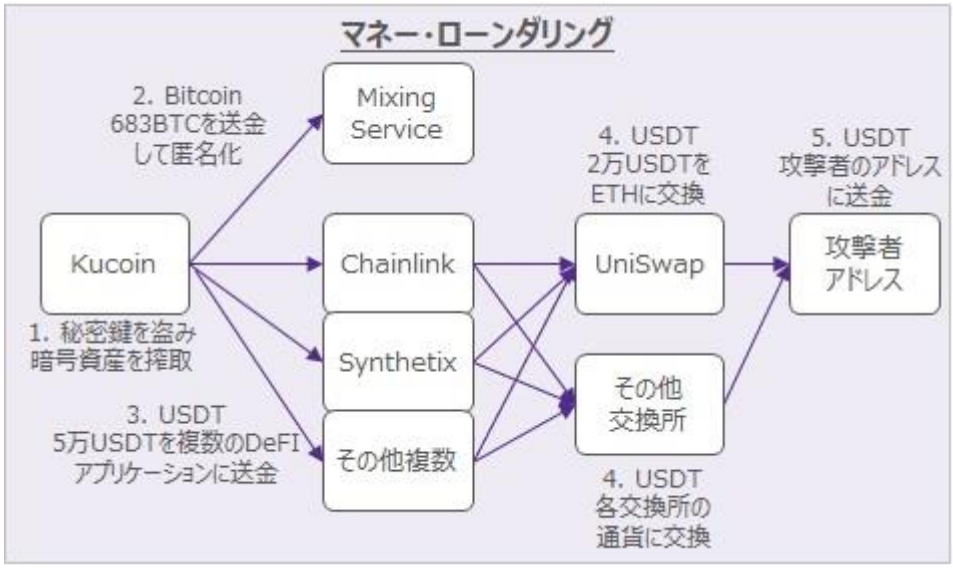

図 2-6-4　マネー・ローンダリング

1. 攻撃者が KuCoin の管理者のホット・ウォレット秘密鍵を盗み、多額の暗号資産が窃取された。
2. Bitcoin：盗んだ 1,008BTC のうち、683BTC をミキシングサービス[143]に送金して匿名化した。
3. USDT：盗んだ 1,983 万 USDT のうち、5 万 USDT を Chainlink[144]、 Synthetix ほか複数の DeFi に送金した。
4. USDT：送金した USDT を Uniswap ほかの交換所に送金し、他の通貨に換金した。
5. USDT：換金後に攻撃者のアドレスに送金した。

【Kucoin から流出した主な暗号資産】
- 1,983 万 USDT (1,983 万ドル)
- 1,008 BTC (1,076 万ドル)
- 1 億 4,700 万ドル相当の各種 ERC-20※6 トークン（USDT 除く）
- 8,700 万ドル相当の Stellar※7 トークン　など

(5) 発生原因
- KuCoin の管理者のホット・ウォレット秘密鍵が盗難されたため。但し、管理者の秘密鍵の盗難の経緯を含む事件の詳細情報は、現時点では未発表。（警察・治安当局による調査が完了次第公開すると発表されている）
- コールド・ウォレットの資産は流出していない

表 2-6-4　Flash Loan Attack #2 インシデントの問題点

区分	種別	問題点の内容	存在するリスク
DeFi 現象的要因	オペレーション	・盗まれた暗号資産が何の問題もなく交換された - 盗まれた USDT のうち、2 万 USDT は Uniswap で即時に ETH に交換された	・盗まれた暗号資産が簡単に資金洗浄されてしまう

143 ミキシングサービス：ビットコインの複数の送金データを混ぜ合わせて利用者のプライバシーや匿名性を守る手法。どこからどこに資産が送られたのか追跡を困難にする。

144 Chainlink：オンチェーンとオフチェーンを繋ぐ分散型オラクルネットワーク

		・盗まれた暗号資産の凍結（資金移動ができない状態）に時間がかかった - 暗号資産の凍結は、送金された多くの交換所などの協力により実施された（資産凍結の対応は各交換所で個別に行われた）	・盗まれた暗号資産の被害が止められず拡大してしまう
		・攻撃者が特定できない - 盗まれた暗号資産が多数の DeFi に送金され、攻撃者の送金先とアドレスはブロックチェーン上に記録されるが、KYC が不要な交換所を利用しているため、誰が行ったかは特定できない	・攻撃者を特定できないまま、資金移動が繰り返されてしまう
		・盗まれた資産の追跡が難しい - Bitcoin ではミキシングサービスにより匿名化を行っており、それ以降の資金の動きの特定が難しくなっている	・資金移動により、盗まれた暗号資産の行方が特定できなくなる
	オペレーション	・KuCoin の管理者のホット・ウォレット秘密鍵が盗難された - 但し、管理者の秘密鍵の盗難の経緯を含む事件の詳細情報は、現時点では未発表	・管理者の秘密鍵の盗難による暗号資産の流出と参加者の損害 ・該当する暗号資産の信頼度低下
KuCoin 動機的要因	テクノロジー	・管理者の秘密鍵を管理する技術が不足していた - 管理者の秘密鍵を管理するために必要な技術が使用されていなかった可能性がある（詳細は未公表のため不明）	・脆弱な技術による管理者の秘密鍵の盗難
	オペレーション	・管理者が秘密鍵の厳密な管理を行っていなかった - 管理者が秘密鍵を管理することの重要性に対する意識が弱かったと想定	・管理者の杜撰な管理による秘密鍵の盗難
	ガバナンス	・管理者の秘密鍵の盗難に対する防御策が不十分であった - 管理者の秘密鍵盗難の原因が未発表であり詳細は不明だが、秘密鍵管理のオペレーションに問題がある場合は、有効な盗難防止策が必要であったと考えられる	・該当する暗号資産の信頼度低下
	法規制	・管理者の秘密鍵盗難対策について、指導が必要であった可能性がある - 管理者の秘密鍵盗難の詳細原因は不明だが、秘密鍵管理のオペレーションに問題がある場合は、盗難防止策として一定の基準を設ける必要があると考えられる	・同様な管理者の秘密鍵盗難事件の多発による DeFi 市場全体の信頼度低下

2-6-5　ビットコインの脆弱性（CVE-2018-17144）[145]

2018 年 9 月に発生したビットコイン脆弱性のインシデント事例について、その概要と発生理由、問題点を説明する。

(1) 発生日：2018 年 9 月 18 日

(2) 損害額：なし

(3) 事件の概要

・Bitcoin Core[146]バージョン 0.15.x, 0.16.0, 0.16.1, 0.16.2 について、
- Dos 攻撃[147]と二重支払いに関する脆弱性が発見され、バージョン 0.16.3 および 0.17.0rc4 にて修正された。

・この脆弱性を突くことでビットコインネットワークのノード[148]を意図的にクラッシュさせることが可能であり、ハッシュレートの過半数のノードに修正したプログラムが適用されないと 51%攻撃等の攻撃を受ける危険があった。よって、過半数のノードがアップグレードする時間を確保するため、脆弱性の公表を遅らせた。

(4) 事件の流れ[149]

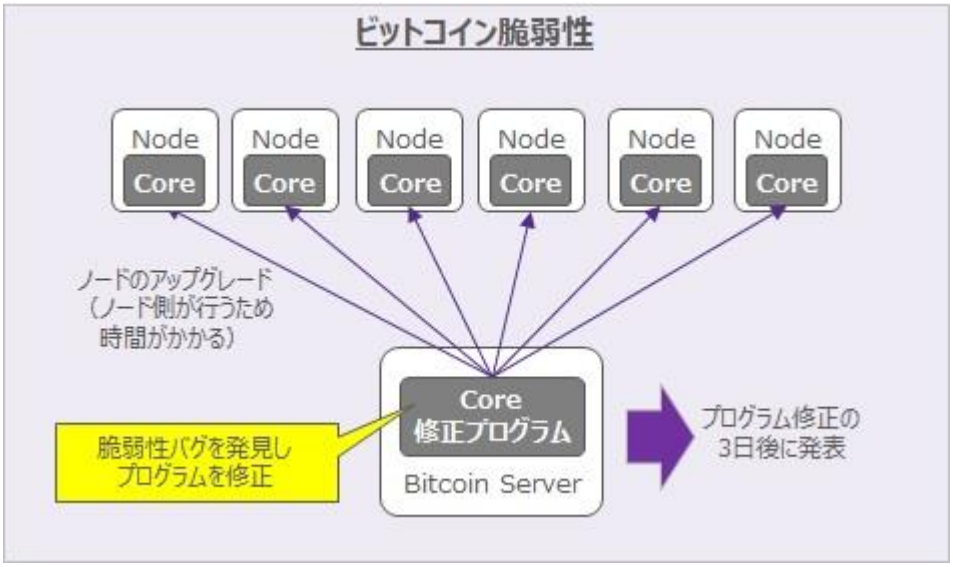

図 2-6-5　ビットコイン脆弱性

1. 9/17 14:57 匿名の報告者が脆弱性を発見し、Bitcoin Core の複数の関係者に報告。
2. 9/17 17:47 Bitcoin Core 開発者が脆弱性を確認。
3. 9/18 20:44 Bitcoin Core 開発者が修正プログラムをリリース。
4. 9/18 21:47 ノードのアップグレードを促す公開バナーを reddit などで展開。

---

145 CVE-2018-17144：Common Vulnerabilities and Exposures (共通脆弱性識別子)　米国非営利団体の MITRE 社が採番している識別子

146 Bitcoin Core：Bitcoin のマイニングや取引などを行うための参照ソフトウェアとなるオープンソースプログラム

147 Dos 攻撃：Denial of Service Attack 悪意を持ってサーバに大量のデータを送りつけてサービスの実行を事実上不可能にするサイバー攻撃

148 ノード：ブロックチェーンの処理を行う機器。ノードの持つ機能は、ルーティング・ブロックチェーンデータベース・マイニング・ウォレットがある

149 https://bitcoincore.org/notice/
https://hackernoon.com/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362

5. 9/19 14:06 ノードのアップグレードを促す追加メッセージをメーリングリストで配信。

6. 9/20 本件の脆弱性を完全に開示。

(5) 発生原因

表 2-6-5　ビットコイン脆弱性インシデントの問題点

区分	種別	問題点の内容	リスク／インプリケーション
現象的要因	デプロイメント	・UTXO（トランザクションの未使用アウトプット）を二重に入力しているケースで、トランザクションの正当性のチェックをすり抜ける場合があった	・システム停止や資金の窃取が行われるリスク
動機的要因	デプロイメント	・トランザクションの正当性のチェックと UTXO の管理については最適化が続けられてきた中で、バージョン 0.15 の修正で更なる最適化のためにチェックが緩められた結果、脆弱性が生じた	（同上）
		・脆弱性へ対処するためにハッシュレートで過半数のノードに修正プログラムを適用する必要があり、対応に時間を要した	・ノードに修正プログラムの反映が間に合わず攻撃されるリスク ・仮に DAO において同様の脆弱性が発見された際には、プログラム修正を投票で承認する必要がある場合に、「責任ある開示（Responsible Disclosure）」により脆弱性の発表を遅らせることができず、緊急の脆弱性があることが周知されてしまう可能性
		・ノードのアップグレードはノード側の判断で行われるため、修正プログラムの反映を要請しても対応してもらえる保証がない ・悪意のあるノードは、古いプログラムのまま更新しない可能性がある	・ノードが古いプログラムのままアップグレードせず、脆弱性が修正されない
		・Bitcoin Core バージョン 0.15.x から脆弱性が内在していたが、長期間発見できなかった ・今回の事例では匿名の報告者からの指摘で脆弱性を発見した	・今回の事例では匿名の報告者が脆弱性を公表せずに Bitcoin Core 開発チームに報告を行ったが、脆弱性を公表するかどうかは報告者の意思次第

2-6-6　サイドチェーンの双方向ブリッジにロックされた資金の窃取（Ronin Network）

2022 年 3 月に発生したサイドチェーンの双方向ブリッジにロックされた資金窃取のインシデント事例について、その概要と発生理由、問題点を説明する。当インシデントの発生原因はバリデータの

秘密鍵の窃取であるが、9 個のバリデータを 2 社で管理しており、1 社のシステム攻撃で同時に 5 個のバリデータの秘密鍵が窃取されており、秘密鍵管理の好ましくない例である。

(1) 発生日：2022 年 3 月 23 日

(2) 損害額：約 6 億 2,010 万ドル　※発生時点での最高額

(3) 事件の概要

・3/23　Axie Infinity[150]が稼働する Ronin Network[151] の一部のバリデータの秘密鍵が盗難され、Ethereum ネットワークと Ronin ネットワークを繋ぐ双方向ブリッジ（Ronin Bridge[152]）の資金が窃取された。
・3/29　ユーザが Ronin Bridge から資金が引き出しできず、事件が発覚した。Ronin Bridge 運営元の Sky Mavis 社が Roni Bridge を停止し、原因を調査。
・4/6　損失補填のため、Sky Mavis 社（ベトナム）が複数の VC から 1 億 5,000 万ドルの資金調達。
・4/14　米連邦捜査局（FBI）が北朝鮮のハッカー集団「ラザルス・グループ」と「APT38」の犯行であること発表。
・4/20 時点で、Ronin Bridge は停止中。

(4) 事件の流れ[153]

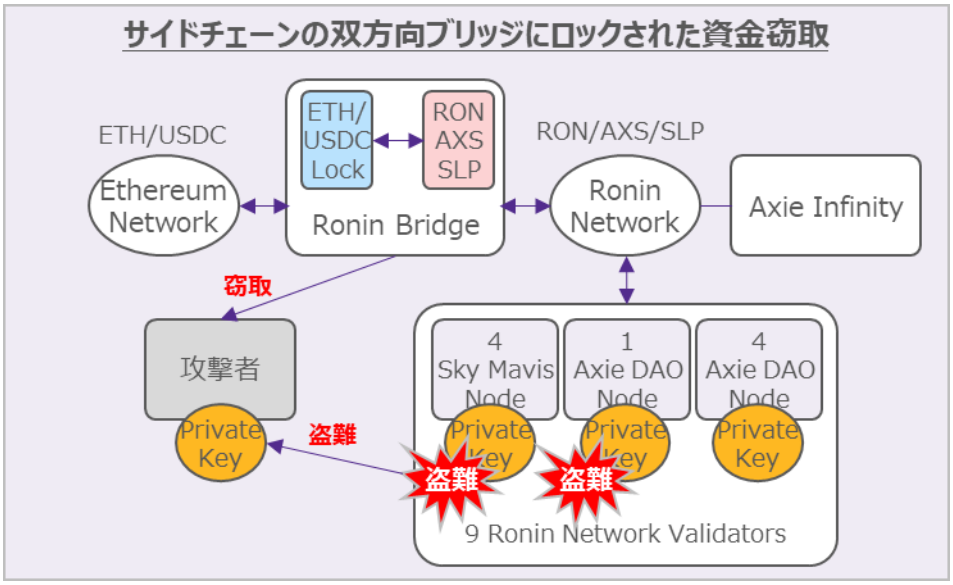

図 2-6-6　事件の概要

1. 3/23　Ronin Network Validator の 9 ノードのうち 5 ノードの秘密鍵が盗難され、Ronin Bridge にロックされていた ETH や USDC が窃取された。（9 ノードのうち 5 ノードの承認が必要な仕組みだった）

[150] Axie Infinity：NFT ペットを収集・育成して対戦させるオンラインゲーム　プレイヤー830 万人（2021 年 12 月時点）

[151] Ronin Network：Ethereum のサイドチェーン（親となるメインチェーンとは異なるブロックチェーンを作り、双方向ブリッジで資金を転送する）。2021 年 2 月に運営元の Sky Mavis 社が Axie Infinity 専用にローンチした。

[152] Ronin Bridge：Ethereum Network と Ronin Network の間で資金を転送するブリッジ。親チェーンの Ethereum のコインをブリッジにロックすることで二重使用を防ぐ。

[153] https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=r
https://medium.com/uno-re/biggest-crypto-hack-of-all-time-a-breakdown-of-the-ronin-network-hack-ef8d9e25ba6b
https://www.nansen.ai/research/ronin-the-engine-powering-axie-infinitys-growth

2. 3/29　ユーザが Ronin Bridge から ETH を引き出すことができず、事件が発覚。即時にバリデータの閾値を 5→8 に修正。窃取された資金の殆どは攻撃者のウォレットに保有されていることを確認。政府機関と協力して攻撃者の捜査とウォレット監視を実施中。

3. 3/31　窃取された Sky Mavis 社管理の 4 ノードと Axie DAO（Sky Mavis 社が DAO への移行を計画しており、移行先候補の DAO）の 1 ノードを置き換えた。新しいバリデータの追加を検討中。

【窃取された資金と暗号資産】　合計 6 億 2,010 万ドル
・ETH　173,600ETH（5 億 9,460 万ドル）
・USDC　2,550 万ドル

(5) 発生原因
・Ronin Network Validator の 9 個のノードのうち、5 個のノードの秘密鍵が盗難されたため。

① Sky Mavis 4 ノード

Sky Mavis システムへの攻撃により、集中サーバに保管されていたバリデータの秘密鍵が 4 ノードとも盗難された。（攻撃手段は未発表）

② Axie DAO 1 ノード

2021 年 11 月、Ronin Network の急激なトランザクション増加に伴う手数料高騰への対策として、ユーザに無料のトランザクションを提供するため、Axie DAO を 1 ノード追加し、Sky Mavis ノードの代理署名を許可した。
その対応は 2021 年 12 月に終了したが、Sky Mavis 社が代理署名許可リストの削除を行っていな　かった。その結果、Sky Mavis 社の 4 ノードの盗難に伴い自動的に盗難された。

表 2-6-6　サイドチェーンの双方向ブリッジにロックされた資金窃取の問題点

区分	種別	問題点の内容	リスク・インプリケーション
現象的要因	オペレーション	・Sky Mavis 社システムが攻撃を受けて、バリデータノード 4 個のバリデータの秘密鍵が盗難された。（攻撃の内容は未発表）	・バリデータの秘密鍵の盗難により資金が窃取される ・バリデータの乗っ取りにより、悪意のあるコントラクトの実行など他の攻撃に利用される可能性がある
		・Sky Mavis 社のバリデータノード 4 個の秘密鍵が集中サーバに保管されていたため、上記攻撃により 4 個のバリデータの秘密鍵が同時に盗難された	・Axie DAO バリデータの秘密鍵も含めると、事実上、1 回の攻撃により秘密鍵の過半が盗難される状況となっていた
		・Sky Mavis 社の 4 つとは別途管理されていた Axie DAO バリデータの秘密鍵も同時に盗難された。	・Sky Mavis 社への攻撃により自動的に Axie DAO の秘密鍵も盗難される蓋然性が高い状況にあり、秘密鍵の分散管理が実質的には行われていなかった
動機的要因	オペレーション	・秘密鍵 9 個が、Sky Mavis 社と Axie DAO（Sky Mavis 社の 2 つの組織で管理	・バリデータノードを少数の組織で運営している

		されており、ノードの管理が集中している。 ・Ronin Network のバリデータは、運営元の Sky Mavis 社が指定していた可能性。	と、バリデータの秘密鍵を同時に盗まれるなど、ブロック決定に必要なノード数のバリデータの秘密鍵が盗難されるリスクが高まる
		・Ronin Network の PoA コンセンサスのバリデータ閾値が「5」（9 個中 5 個でブロック決定）であった - Ronin Network は Axie Infinity ゲーム専用のブロックチェーンであり、ブロック作成時間が約 3 秒と短いため、PoA にかかる時間を最小とするために最低限の閾値としていた。	・閾値が小さいと、ブロック決定に必要なノード数のバリデータの秘密鍵が盗難されるリスクが高まる
	デプロイメント	・Ronin Network などのサイドチェーンは、Ethereum の資金をブリッジにロックしてサイドチェーンの暗号資産に変換する仕組みのため、ブリッジに多額の資金がロックされ、このブリッジを攻撃者に狙われやすい。	・取引額が多いサイドチェーンは、ブリッジに多額の資金がロックされており、攻撃者に狙われやすい 【参考】 ・2022/2/22 に発生した Solana ブロックチェーンでは Wormhole ブリッジが攻撃され、3 億 2,500 万ドルの被害が出ている（原因は署名コントラクトの脆弱性を攻撃された） ・他のサイドチェーンもブリッジに多額の資金をロックしている。[154] - Polygon　約 55.1 億ドル - Avalanche　約 49.7 億ドル　など （2022/4/12 時点）
	ガバナンス	・今回の攻撃により、Axie Infinity のプレイヤーで、Ethereum の ETH や USDC を Ronin の RON や AXS、SLP に交換していた場合は、ETH や USDC の払出しができななくなった。	・資金の払戻しができない ・今回の場合は、Sky Mavis 社が 4/6 に複数の VC から 1 億 5,000 万ドルの資金調達を行い、影響を受けた全てのユーザが払戻しを受けられるよう対応すると発表

[154] https://dune.xyz/eliasimos/Bridge-Away-(from-Ethereum)

2-6-7　2020 年以降の主なインシデント事例[155]

ソフトウェアの脆弱性や秘密鍵の管理不備に起因するインシデントが多く発生している。

表 2-6-7　2020 年以降の主なインシデント事例

発生日	原因	関連 DeFi	被害額	事件の概要
2020/4/19	ソフトウェアの脆弱性（リエントランシー）	Lendf.Me（レンディング）	2,500 万ドル [うち 2,100 万ドルを回収]	・イーサリアムの脆弱性を突いた ERC777 トークンのリエントランシー攻撃を受けた ・攻撃者が窃取した暗号資産（ETH 等）の現金化に手間取り、大半は返却された
2020/8/25	ソフトウェアの脆弱性（ステーキングプール処理の不具合）	YFValue (現 Value DeFi)（イールドファーミング）	最大 1 億 7,000 万ドル [全額回収]	・YFValue（YFV）のステーキングプールの脆弱性により、YFValue のタイマーがリセットされ、プールに一部の資金がロックされて引き出せなくなった ・ステーキングプールにある合計 1 億 7,000 万ドルがロックされて引き出せなくなる危険性があり、攻撃者から恐喝を受けた ・その後、運営チームがステーキングプールにロックされている資金を救済した[156]
2020/9/14	ソフトウェアの脆弱性（トークン不正増刷）	bZx（デリバティブ）	800 万ドル [全額回収]	・bZx の iToken（利息を蓄積できるトークン）が不正に増幅できる脆弱性を悪用されて、約 800 万ドルが盗まれた ・後日、攻撃者を発見し、全額を取り戻した
2020/10/26	オラクル価格の不正操作（担保資産の枯渇）	Harvest Finance（イールドファーミング）	3,400 万ドル [うち 250 万ドルを回収]	・攻撃者が 20WETH を Harvest Finance のコントラクトに送金し、Curve の価格を操作して、暗号資産（fUSDT, fUSDC）の資金を枯渇させた。その後、攻撃者は資金を renBTC に変換し、総額約 3,400 万ドルを窃取した。攻撃者は応答時間を与えず、7 分間にわたってエンドツーエンドで攻撃した ・攻撃者は Ethereum のミキシングプラットフォーム「Tornado.cash」を使用して資金移動を隠した。 ・攻撃者は 250 万ドルを USDT と USDC で開発者に返した
2020/11/30	ソフトウェアの脆弱性（償還処理の不具合）	Saffron Finance（レンディング）	5､000 万ドル [全額回収]	・スマートコントラクトの償還エラー（特定の入力を書き込むと資金を引き出すことができなくなる脆弱性）を攻撃され、5,000 万 DAI の預金が 8 週間ロックされた
2021/5/18	オラクル価格の不正操作	Venus（レンディング）	7,700 万ドル	・Venus のトークン（XVS）の価格が、大口取引によって価格操縦され 2 倍に上昇。上昇した XVS を借入の担保に使用

[155] https://hacked.slowmist.io/en/

[156] https://valuedefi.medium.com/yfv-update-staking-pool-exploit-713cb353ff7d

	（担保資産の枯渇）			し、数億ドル相当の BTC と ETH が借入された。 ・XVS 価格が下がり、XVS を担保にして借入れた暗号通貨の返済をする時、XVS の流動性が低かったために期日内の返済にシステムが対応出来ず、Venus プロトコルで 7､700 万ドルの損失が発生した ・流動性を供給する際は 10%の手数料が掛かるため、本件で攻撃者は 5,500 万ドル、流動性供給者は 2,000 万ドル、転売者は 200 万ドルの利益を得た
2021/8/10	ソフトウェアの脆弱性（ブロックチェーン間取引の不具合）	Poly Network（クロスチェーンブリッジ）	6 億 1,000 万ドル [全額返還]	・Poly Network が、ブロックチェーン間取引の脆弱性を突かれたハッキング攻撃を受け、6 億 1,000 万ドルを超える暗号資産が窃取され、Binance Smart Chain, Ethereum, Polygon 等の複数口座に送金された ・脆弱性を知らしめるために攻撃をしたという声明が出され、数日後には全額が返還された
2021/10/27	ソフトウェアの脆弱性（フラッシュローン攻撃）	Cream Finance（レンディング）	1 億 3,000 万ドル	・フラッシュローン攻撃により Cream LP トークンや ERC-20 トークンの合計約 1 億 3,000 万ドルを窃取された ・コードの脆弱性を狙われたとし、該当部分の究明と対応は完了と発表。Cream Finance にとって 2 月、8 月に続く 3 度目のフラッシュローン被害となった
2021/10/30	秘密鍵の管理不備	BoyX High Speed（BXH）（DEX）	1 億 3,900 万ドル	・管理者キーの漏洩により 1 億 3,900 万ドルの資金が流出 ・攻撃者は管理者キーホルダーのコンピューターに侵入したか、BXH の技術スタッフの 1 人だった可能性
2021/11/5	秘密鍵の管理不備	bZx（デリバティブ）	5,500 万ドル [全額返還]	・Polygon と BSC の間でプロジェクトの展開を制御するために使用された開発者の秘密鍵が漏洩し、55 百万ドルが窃取された ・bZx DAO の投票により、損害全額の補償計画が承認された
2021/11/30	ソフトウェアの脆弱性（トークン価格設定の不備）	Monox（DEX）	3,100 万ドル	・スマートコントラクトの脆弱性（トークンの売却と購入の参照価格に同じトークン価格が使用されていた脆弱性）を攻撃され、Mono トークンの価格を操作し上昇させた上で、別のトークンに交換・引出しされた
2021/12/2	ソフトウェアの脆弱性（フィッシング UI の	Badger DAO（イールドファーミング）	1 億 2,000 万ドル	・外部ネットワークの Cloudflare の欠陥を攻撃されて、攻撃者が悪意のある API key を作成し、フィッシング用の UI（User Interface）を挿入した

	不正挿入）			・ユーザがその UI をクリックすることでユーザのアドレスが犯人に盗まれて、資金が窃取された
2021/12/3	ソフトウェアの脆弱性（トークン不正増殖）	Polygon（サイドチェーン）	200 万ドル	・12/3 にホワイトハッカーにより重大な脆弱性（攻撃者が Polygon のコントラクトを使ってトークンを任意に生成できる）が Polygon に通知され、12/5 に修正パッチがリリースされたが、パッチ適用までの間に、悪意あるハッカーにより 200 万ドル相当の MATIC コインが盗まれた ・責任ある開示により脆弱性の発表を遅らせ、12/29 に修正情報を開示した
2022/2/2	ソフトウェアの脆弱性（署名検証処理のの不具合）	Wormhole（双方向ブリッジ）	3 億 2,000 万ドル	・スマートコントラクトの脆弱性（署名を検証するコントラクトの不具合）を攻撃され、ブリッジにロックしていた資金が窃取された ・Wormhole の親会社である JumpCrypto 社は Solana エコシステムをサポートするために損害を独自の資金でカバーした
2022/4/17	ソフトウェアの脆弱性（緊急コミット条件の不備）	Beanstalk（ステーブルコイン）	1 億 8,200 万ドル	・ガバナンス投票スマートコントラクトの脆弱性を悪用され、Flash Loan により資金を窃取された。[157] ・事件の流れ ①事件の前日に悪意のあるガバナンス提案（悪意のあるスマートコントラクトアドレスを指定）と通常の提案（ダミーのウクライナ寄付提案）の 2 件を提案し、1 件目がアドレス指定間違いの提案のように見せて、悪意のある提案をごまかした ②事件当日に Aave で Flash Loan により以下を実行 - Aave から ETH・USDC・USDT で計 10 億ドルを借用 - 借りた資金で Beanstalk のガバナンストークンの 2/3 を購入 - 購入したガバナンストークンで悪意のある提案に投票 - Beanstalk の Emergency Commit を起動して悪意のあるスマートコントラクトの実行に成功し、Beanstalk の資金を窃取した ・原因 ①悪意のある提案にコミュニティの誰も気づかなかった

[157] Beanstalk Farms loses $182M in DeFi governance exploit
https://cointelegraph.com/news/beanstalk-farms-loses-182m-in-defi-governance-exploit

				- 提案の検証はコミュニティメンバーの協力に依存されており、誰も悪意のある提案を発見できなかっ ②Emergency Commit に悪意のある提案をキャンセルする仕組みがなかった - 提案をキャンセルする仕組み、およびキャンセル期間を設ける必要があった ③Beanstalk の Emergency Commit の起動条件の不備 - （起動条件）提案後 1 日経過＆2/3 以上の賛成票で実行される - 提案可決後に一定期間（2 日間など）を待つ仕様にすれば Flash Loan による攻撃は受けない ④Aave の Flash Loan が悪用された - Aave の Flash Loan が無担保無制限に借りられるため、他の DeFi プロジェクトの攻撃に悪用された
2022/5/10	ステーブルコインの大量売りによる市場価格の大幅下落	Terra ブロックチェーン TerraUSD（UST） Anchor Protocol	市場価格の下落 UST 83% LUNA 99%	ステーブルコイン UST の大量売りにより市場価格が 1USD を維持できず、大幅に下落した[158]。これまで 1USD を一時維持できない事態が 2 度発生していたが、今回は価格が戻せなくなった。 ・事件の流れ ①5/5　Bitcoin や ETH など暗号資産全体の価格が下落。（Bitcoin は 5/12 に最大 32%下落） ②5/7　Anchor Protocol から大口出金（14 億ドル）があり預金量が減少し、ステーブルコイン UST の価格が下がり始める。（大口出金者は不明。資産運用会社のブラックロック、シタデルは関与を否定） ③5/8　UST が 2 億 5,800 万ドル売られ、更に価格が下がる。 ④5/9-10　UST が 2%下落し、1USD を維持できなくなった。LFG（Luna Foundation Guard）が価格維持のために保有していた Bitcoin 約 40 億ドルの全額を放出したが、売りに対して資金不足のため 1USD に戻らなかった。（5/8 時点の UST 時価総額 186.4 億ドル） - UST が取り付け騒ぎで大量に売られて価格が暴落し、アルゴリズムによりネイティブトークン LUNA が大量鋳造され、LUNA の価格が下落した。

158 テラ USD（UST）のディペッグ騒動　https://coinpost.jp/?p=350288

				- LUNA 総供給量：5/5 時点約 7.3 億トークン→5/13 時点 6.5 兆トークンに増加（約 8,900 倍） ⑤5/13　Terra ブロックチェーンの運用を一時停止。 - 市場価格　UST：$1.0→$0.17（83%下落）、LUNA：$80→$0.02（99%下落） ※Anchor Protocol：Terra ブロックチェーンの貯蓄プロトコル。UST トークンを預けると最大 19.5%の利回りを提供する。 - LUNA：Terra ブロックチェーンのネイティブトークン。UST の価格維持のために使用される。（UST が 1USD を超えると焼却、1USD を下回ると鋳造して UST＝1USD を維持する）

2-7　トラストチェーンにおけるトラストポイント・Weakest Link の分析

トラストチェーンにおける主要な構成要素のマッピング結果および主要な DeFi プロジェクトの分析結果、主なインシデント事例より、トラストポイントおよび Weakest Link と思われる部分として以下が挙げられる。

2-7-1　トラストポイントの分析

(1) Ethereum ライブラリ[159]

・Ethereum ブロックチェーンにアクセスするウォレットなどブロックチェーン外部の各種サービスは、Ethereum Foundation 等から提供されている共通ライブラリを利用しており、利用者はこのライブラリが正しく振る舞うことを前提としている。
・図 2-7-1 のアンホステッド・ウォレットとクライアントソフトウェアが Ethereum Library に依存しており、Ethereum Library がトラストポイントになると考えられる

(2) Ethereum ノードソフトウェア[160]

・Ethereum ブロックチェーンで稼働するノードは、Ethereum Foundation が提供する共通ソフトウェアの利用が推奨されており、ノード運用者はこのソフトウェアが正しく振る舞うことを前提としている（ノード運用者はそれぞれのソフトウェアの開発者やサプライヤーなどが脆弱性などの問題がないコードを提供していることを前提としている）。
・図 2-7-1 の Ethereum ノード利用者やマイナーが Ethereum ノード、Ethereum Virtual Machine のソフトウェアに依存しており、これらのソフトウェアがトラストポイントになると考えられる。

(3) インフラプロバイダ提供サービス

・Ethereum ブロックチェーンを利用するためには Ethereum ノードからトランザクションを実行するが、このノードを自分で構築するには負荷が高く、安価なインフラプロバイダのサービスを利用する場合がある。このサービス利用者は、インフラプロバイダのサービスが正しく振る舞うことを前提としている。

159 Ethereum.org JAVASCRIPT API LIBRARIES https://ethereum.org/ja/developers/docs/apis/javascript/

160 Ethereum.org NODES AND CLIENTS https://ethereum.org/ja/developers/docs/nodes-and-clients/

・図 2-7-1 の Wallet 端末や運用サーバがインフラプロバイダに依存しており、インフラプロバイダがトラストポイントになると考えられる。

⑷ Web ブラウザに組み込まれたコード

・DeFi やウォレットの利用時に Web ブラウザで動くコードは、DeFi やインフラブロバイダ等が提供するものが稼働しており、DeFi やインフラプロバイダ等が組み込んだコードが正しく振る舞うことを前提としている

(5) DeFi で使用する汎用コード

・DeFi プロトコルや周辺機能などを開発する際に、特定機能の実現などのためにサプライチェーンなどの外部から汎用的なオープンソースのコードを取り込んで利用することがあり、その場合はサプライヤーが提供したコードが正しく振る舞うことを前提としている

(6) インターネット

・投資家や利用者のウォレットとインフラプロバイダの接続やマイナーが運営する Ethereum ノード間の P2P ネットワークなど、分散型金融システムのネットワーク接続はインターネットを経由しており、インターネットサービスプロバイダやデータセンタ事業者など複数の異なるインターネットが相互接続されたサービスを利用している。投資家や利用者、マイナーなどは、インターネット接続サービスが正しく振る舞うことを前提としている。
・図 2-7-1 の Wallet 端末や運用サーバ、インフラプロバイダ、Ethereum ノードはインターネットに依存しており、インターネットがトラストポイントになると考えられる。

(7) 外部オラクルサービス

・一部の DeFi プロジェクトはオラクル攻撃防御などの目的で、自己プロジェクト内ではオラクル価格を算出せず、Chainlink などの外部オラクル価格提供サービスを利用してトークンの市場価格や手数料利率を入手している。この DeFi プロジェクトは、外部オラクル価格提供サービスが正しく振る舞うことを前提としている。
・図 2-5 の Oracle が外部 Oracle に依存しており、外部 Oracle がトラストポイントになると考えられる。

(8) DeFi プロトコルの処理実行（清算などを実行する BOT 処理）

・DeFi プロトコルで提供されているサービスでは、トークン価格維持や清算処理などを実行するために外部の複数の BOT（一定のタスクや処理を自動実行するアプリケーション）を使用して処理を実行しているが、その詳細内容は公開されておらず、利用者はその BOT が正しく振る舞うことを前提としている。
・図 2-3-1-1 の Maker プロトコルが外部の BOT であるオークションキーパー／マーケットメーカーキーパーに依存しており、オークションキーパー／マーケットメーカーキーパーがトラストポイントになると考えられる。

(9) DeFi プロトコル開発（スマートコントラクトの修正など）

・ガバナンス投票の提案などによりスマートコントラクトの修正を行う場合、大半のガバナンス投票参加者はスマートコントラクトのコード内容を理解しておらず、提案の内容通りに正しく振る舞うことを前提としている。
・図 2-7-2 の投票者が提案者のスマートコントラクトのコード内容に依存しており、提案者がトラストポイントになると考えられる。

(10) ガバナンス投票の委任

・ガバナンス投票は実際には少数者の投票で運営されており、多くの個人投票者は大手トークンホルダーに投票を委任している場合がある。この個人投票者は、委任した大手トークンホルダーが自分の期待した通りの投票を行ってくれることを前提としている。
・図 2-3-3 の Maker の個人投資家が投票代理人に依存しており、投票代理人がトラストポイントになると考えられる。

(11) ガバナンス投票で可決したスマートコントラクトやパラメータ修正などのデプロイ
・機能追加や利率変更などスマートコントラクトやパラメータを修正する提案がガバナンス投票で可決した後、自動ではデプロイされず、管理者や権限者がデプロイ作業を行う必要がある。提案者は、この管理者や権限者が可決した内容を正しく速やかにデプロイすることを前提としている。
・図 2-7-2 の提案者が管理者や権限者のデプロイ作業に依存しており、この管理者や権限者がトラストポイントになると考えられる。

(12) 緊急時のスマートコントラクト修正
・脆弱性の発見など緊急のスマートコントラクト修正が必要になった場合、Ethereum の開発ガイド等に従い、脆弱性を外部に公表せず関係者のみで対応を行う場合がある。利用者は、DeFi プロジェクトのコアチームなどの管理者や開発者がスマートコントラクトを正しく修正し、損害を出さずに対応してくれることを前提としている。
・図 2-5 の投資家・利用者が、DeFi Protocol Interface を経由して DeFi システム開発ツールに依存しており、DeFi システム開発ツールがトラストポイントになると考えられる。

(13) 権限者による緊急時のシステム停止・悪意のある提案のキャンセル
・一部の DeFi プロジェクトでは、緊急時のシステム停止や悪意のある提案キャンセルをガバナンス投票で選任された権限者のマルチシグ投票で可決するルールとしている。利用者は権限者によるシステム停止や提案キャンセルが正当な理由で実行されることを前提としている。
・図 2-7-2 の投票者（利用者を含む）が提案キャンセル権限者の正当な行動に依存しており、提案キャンセル権限者がトラストポイントになると考えられる。

(14) サイドチェーンに接続する双方向ブリッジの資金ロック
・メインチェーンとサイドチェーンを接続する双方向ブリッジに、チェーン間で移動する資金がロックされる仕様になっており、多額の資金が双方向ブリッジに集中して保管される。チェーン間で移動する資金は双方向ブリッジにロックされた資金が担保となっており、ロックされた資金が攻撃などで流出するとチェーン間の資金移動ができなくなった。（Ronin Network インシデント事例）
・図 2-5 の Ethereum ブロックチェーンと Sidechain が双方向ブリッジの資金ロックに依存しており、双方向ブリッジがトラストポイントになると考えられる。

2-7-2　Weakest Link の分析

(1) サイドチェーンのバリデータ秘密鍵管理
・サイドチェーンを構成する基盤ブロックチェーンや DeFi など複数のレイヤーの構成要素のうち、バリデータの秘密鍵管理に弱点があり、この弱点を攻撃されて双方向ブリッジにロックされている資金が窃取された。（Ronin Network インシデント事例）
・図 2-5 の他のブロックチェーンの複数のレイヤーのうち、基盤ブロックチェーン層の Sidechain の中にあるバリデータの秘密鍵管理が Weakest Link になると考えられる。

(2) 悪意のある提案に対する検証
・悪意のある提案が行われた場合、その検証はコミュニティメンバーの協力に依存されているため、検証を実施する役割が明確でなく、誰も悪意のある提案を発見できなかった。分散型の組

織において、コミュニティは自由参加であり役割が明示されていないため、悪意のある提案に対して検証が確実に行われるかどうかは不明である（Beanstalk インシデント事例）
・ガバナンス投票を構成する DeFi プロトコルや投票ルール、提案者、投票者などの構成要素のうち、提案を検証する役割を誰にも明示していなかったガバナンス投票のルール不備が Weakest Link になると考えられる。

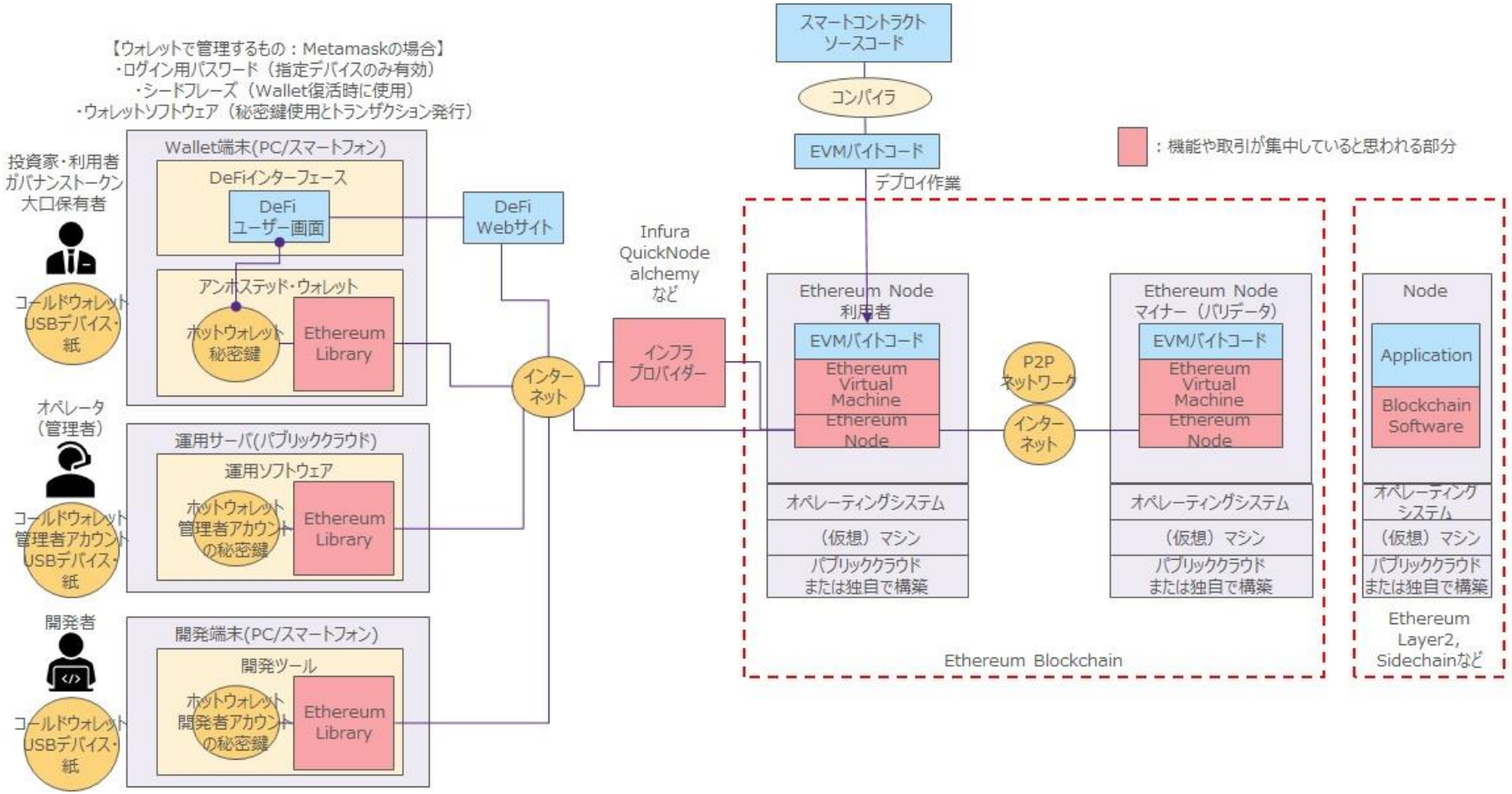

図 2-7-1　トラストチェーンにおけるトラストポイントの分析（ウォレット端末・運用サーバ・Ethereum ノード）[161]

[161] Ethereum.org NODES AND CLIENTS https://ethereum.org/en/developers/docs/nodes-and-clients/

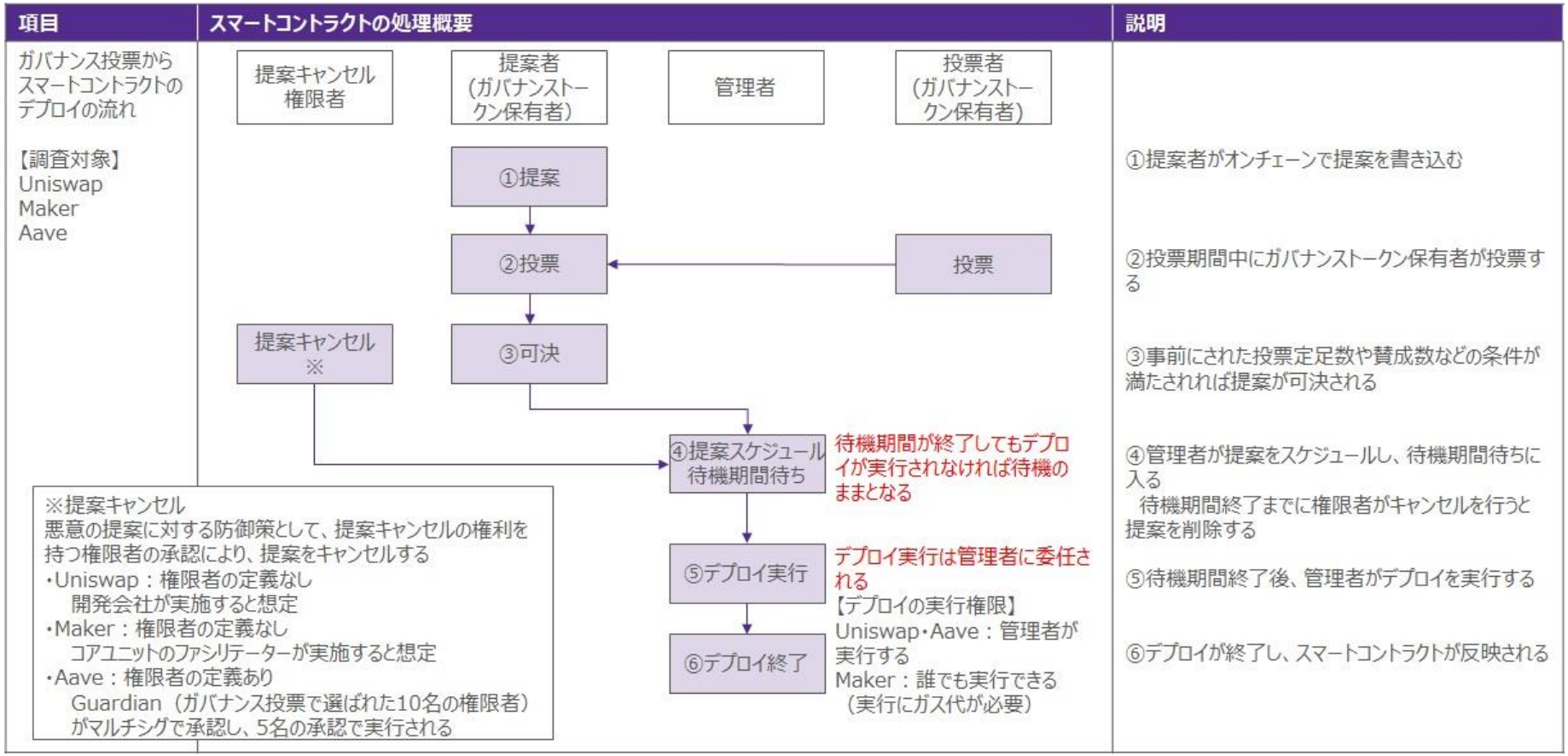

図 2-7-2　トラストチェーンにおけるトラストポイントの分析（ガバナンス投票・デプロイ）[162]

[162] Uniswap Governance Smartcontract https://github.com/Uniswap/governance/tree/master/contracts
Maker Governance Smartcontract https://github.com/makerdao/governance-portal-v2
Aave Governance Smartcontract https://github.com/aave/governance-v2

第３章 分散型金融システムにおけるリスクの特定

本章では、第１章で特定した分散型金融システムを構成する主要な構成要素を元に、第２章の主要 DeFi プロジェクト及びインシデント事例の分析結果を踏まえ、分散型金融における主要なリスク要因の特定を試みた。3-1 ではシステム運用、3-2 ではシステム開発、3-3 ではガバナンス、3-4 では金融市場との関わりにおける観点から、各々のリスク事象を整理し、考えられるリスク要因について考察を行った。

なお、以下で列挙した項目の中には、DeFi に特に密接に関わる問題（DeFi の機能・サービスや運用を行うために専ら必要となるもの）と、DeFi に限らず暗号資産・ブロックチェーン全般への影響を及ぼす問題が存在する。この区別はセキュリティの確保等における重要性の軽重とは無関係ではあることと、両者の境界線は必ずしも明確ではないことを強調しつつ、第４章では DeFi に特に密接にかかわる問題を中心にリスク低減策の検討を行う。

3-1　システム運用におけるリスク要因の特定

a. ハードウェア

表 3-1-1　システム運用のリスク要因（ハードウェア）

大項目	中項目	リスク事象	考えられるリスク要因	DeFi に密接に関わる問題
PC/スマートフォン	－	・PC/スマートフォンが故障し、一時的にウォレットが利用できなくなる	・予備の PC/スマートフォンを準備していない（予備機があれば代替が可能）	× 一般的な機器故障
サーバ機器	－	・Ethereum ノードの機器故障により、トランザクションが実行できない	・予備のノードを準備していない	× 一般的な機器故障
パブリッククラウド	拠点障害・サーバの多数同時停止	・パブリッククラウドの拠点単位の電源故障などの不具合により、多数のノードが同時に停止してしまい、多数のトランザクションが実行できなくなる ・パブリッククラウドのサーバに対する OS パッチ一括適用作業の不具合などにより、多数のサーバが同時に使用できなくなり、トランザクションが実行できない	・パブリッククラウドを単一拠点で契約している	× パブリッククラウド利用方法の問題
コールド・ウォレット	コールド・ウォレット秘密鍵の紛失・使用不能	・コールド・ウォレット機器（USB メモリなど）が故障して、ユーザの秘密鍵が使	・コールド・ウォレット機器のバックアップを準備していない（Metamask では紙を推奨）	× 一般的な機器故障

		用できずウォレットが利用できなくなる		
		・コールド・ウォレットとしてユーザの秘密鍵ないしニーモニック列を印刷保管した紙を紛失し、ユーザの秘密鍵が不明になりウォレットが利用できなくなる	・ユーザの秘密鍵ないしニーモニック列を印刷した紙を適切に保管していない（保管場所忘れ、誤って破棄など）	× 秘密鍵管理の問題
	コールド・ウォレット秘密鍵の盗難	・コールド・ウォレットとしてユーザの秘密鍵ないしニーモニック列を印刷保管した紙を盗撮され、攻撃者がユーザの秘密鍵を使用して資金が盗まれる	・ユーザの秘密鍵ないしニーモニック列を印刷した紙を重要なものとして保管していない（施錠保管をしていないなど）	× 秘密鍵管理の問題
		・マルウェア等が仕込まれたコールド・ウォレットを知らずに使用してしまい、秘密鍵が盗まれる	・安全なコールド・ウォレットであることを外見から判断することが難しい	× 安全なコールド・ウォレットの判別方法の問題

b. 基盤ソフトウェア・ネットワーク

表 3-1-2　システム運用のリスク要因（基盤ソフトウェア・ネットワーク）

大項目	中項目	リスク事象	考えられるリスク要因	DeFi に密接に関わる問題
オペレーティングシステム	マルウェア	・ウォレット端末や運用サーバが標的型攻撃などによりマルウェアに感染し、ユーザの秘密鍵の盗難やデータ不正ロック（ランサムウェア攻撃）などが発生する	・マルウェアを防御する対策を行っていない（最新の修正パッチ適用、バックアップの取得、最新マルウェアの対策教育など）	× 一般的なマルウェア対策の問題
	オペレーティングシステムの脆弱性	・ノードの OS(Linux や Windows など）の脆弱性発見により、修正前に脆弱性を突かれてシステムを悪用される（内部データ漏洩や不正操作など）	・OS 修正パッチを速やかに適用する仕組みを実行していない	× 一般的なオペレーティングシステムの問題
インターネット	通信の不具合、データの漏洩	・ウォレット端末、運用サーバ、Ethereum Node などのインターネットの	・同質の P2P ネットワークノードの間が相互に互いを信用せず動作するような形で	× インターネットを経由する P2P ネットワークやイン

		通信不具合（プロバイダやキャリア等の通信インフラの問題）により、資金利用などの操作ができない、通信データが漏洩するなどのリスクがある	構成されている場合、質の異なる P2P ネットワーク同士の結合点においては、何らかの外部参照に頼るか、同一のノード上でそれら P2P ネットワークに参加させる等の方法を取らないと結合点が脆弱になり得る ・インフラプロバイダに対する接続方法により、データ漏洩などのリスクが考えられる	フラプロバイダの接続方法に関する問題

c. 基盤ブロックチェーン

表 3-1-3　システム運用のリスク要因（基盤ブロックチェーン）

大項目	中項目	リスク事象	考えられるリスク要因	DeFi に密接に関わる問題
ブロックチェーン	トランザクションの慢性的な増加による処理遅延	・Ethereum で稼働する DeFi の取引量増加により、Ethereum が慢性的に混雑し、処理の遅延やトランザクションが失敗する懸念がある ・Ethereum の混雑は、スケーリングソリューションである 2nd Layer や他のブロックチェーンの利用では本質的には解決されない	・Ethereum メインチェーンのスケーリン対策がまだ実施されていない ・但し、Ethereum2.0 シャーディングは現在移行中であり、2023 年に完了予定	× ブロックチェーン一般に関する問題
	Ethereum ガス高騰	・Ethereum のトランザクション増加によりガス代が高騰する ・ガス代の高騰が大きくなると、小規模ユーザの Ethereum 利用者離れや、DeFi プロジェクトの流動性資金不足などが発生する懸念がある	・ガス代高騰の要因は Ethereum スケーリング対策がまだ実施されていないため ・但し、レイヤー2 ソリューションやサイドチェーン・階層化チェーンなどガス代の安い環境が既に提供されている	× ブロックチェーン一般に関する問題
	市場影響によるトランザク	・市場価格暴落などの外部要因などにより	・予期しない外部要因により、暗号資産の	×

	ションの急激な増加	大量のトランザクションが実行され、ネットワークが輻輳してガス価格の高騰やトランザクションの遅延が発生する	市場価格が暴落すると、売買が連鎖して暗号資産全体の価格が変動する ・市場に反応して更にトランザクションが増加する	ブロックチェーンネットワークの問題であり
	P2PNetWorkへの依存	・利用者はP2PNetworkが停止しないことを信頼して利用しており、不具合による利用停止を想定していない	・利用者がP2PNetworkが停止することを想定した対応を考えていない	× ブロックチェーンネットワークの問題
	フロントランニング攻撃、サンドイッチ攻撃	・マイナーやバリデータが取引の前後に故意に自分の取引を挿入し、市場価格を先取りして利ざやを稼ぐ ・マイナーやバリデータが故意に取引の処理順序を入れ替えてガス代を増額させる	・戦略的なマイナーやバリデータが存在する（自分に有利になるように行動する） ・ブロックチェーンの仕組み上、戦略的なマイナーやバリデータを排除できない	× ブロックチェーンのマイニングやバリデートの問題
	マイニングの独占	・51%攻撃（ネットワーク全体の採掘速度の50%を超えて独占する）により悪意のあるマイナーがマイニングを支配し、改ざんした取引を有効にするなど正当な動作を保証できなくなる	・悪意のあるマイナーが存在する ・ブロックチェーンの仕組み上、悪意のあるマイナーを排除できない	× ブロックチェーンのマイニングの問題
	マイナーのインセンティブ低下	・Proof of Work市場環境においてマイナーのインセンティブが低下する場合（マイナー報酬＜マイニング費用）、マイナーがマイニング実行に消極的になり、正当な動作を保証できなくなる	・マイナーは報酬のインセンティブがないとマイニングを行わない	× ブロックチェーンのマイニングの問題
	バリデータの共謀	・Proof of Stakeのバリデータが共謀する（バリデータが固定されて自由市場競争が排除される）と、悪意のあるバリデータがバリデートを支	・悪意のあるバリデータが存在する ・ブロックチェーンの仕組み上、悪意のあるバリデータを排除できない	× ブロックチェーンのバリデートの問題

		配し、正当な動作を保証できなくなる		
	プラットフォームのハードフォーク	・1 つのアプリケーションの攻撃によって発生した損害の回復のため、プラットフォーム全体のハードフォークを行う事態となり得る（The DAO の事例）	・プラットフォームのハードフォークにより、プラットフォーム仕様が変更される（DeFi プロトコルで対応が必要になる場合がある。但し、利用者の対応要否は状況により異なる） ・プラットフォームのハードフォークは、最終的にはプラットフォームの管理者（Ethereum Foundation 等）が意思決定する	○ ブロックチェーンのアップデートにより DeFi プロトコルが大きな影響を受ける可能性
	ブロックチェーンへの依存	・利用者はブロックチェーンがフォーク（仕様変更などのアップデートによるブロックチェーンの分岐）しないことを信頼して利用している。 ・例えばハードフォークによりトークンの価格下落や一部取引の停止などが発生することを想定していない	・利用者がブロックチェーンがフォークすることを想定した対応を考えていない	○ ブロックチェーンのアップデートにより DeFi 利用者が大きな影響を受ける可能性
	利用者のプライバシー保護	・ブロックチェーンの取引は全て公開されるため、利用者のアドレスの取引や残高が公表されてしまう（取引履歴が他人から見られる、保有トークンの多いアドレスが攻撃に狙われやすいなど） ・但し、利用者個人とアドレスの紐づけはされない	・取引の公開による透明性や安全性を重視することで、プライバシー保護が重視されていない懸念がある	× ブロックチェーンの仕様の問題
ソフトウェア・ウォレット（ホッ	ホット・ウォレットへの攻撃	・大口ガバナンストークン保有者やコミュニティ資金管理者など大量のトークンを	・トークンの大口保有者が存在する（特定のアドレスにトーク	○ DeFi の特定アドレスへの資金集中

ト・ウォレット）		保有するウォレットは、攻撃者から狙われやすい	ンを大量に保有している） ・ウォレットアドレスとトークン数が公開されている	
	ウォレット業者のサービス停止	・ウォレット業者の倒産などによりホステッド・ウォレットサービスが停止し、ウォレットの資金が利用できなくなる	・ウォレット業者が保管しているホステッド・ウォレットが利用できなくなる（ユーザの秘密鍵があれば他のウォレット業者が利用できる場合がある）	× ウォレット業者の運営の問題
	好ましくないウォレットの利用	・セキュリティや品質などに問題があるなど好ましくないウォレットがあっても、利用者が認知できずに使用してしまう	・利用者が自分で安全なウォレットを調べようとしない（リテラシーが低い利用者など） ・ウォレットアプリケーションの安全性などの情報が開示されていない、情報を開示する仕組みがない	× 安全なウォレットの判別方法の問題
ソフトウェア（OS除く）	ソフトウェアの脆弱性（ウォレット、クライアントソフトウェアなど）	・ソフトウェアの脆弱性により、ウォレットやシステムクライアントソフトウェアが中断し、ウォレット利用やシステム運用が一時的に実施できなくなる	・ソフトウェアの脆弱性によるサービス中断を想定した準備をしていない（複数のウォレットやクライアントソフトウェアの利用など）	○ ウォレット等の利用ができなくなることにより、DeFi 利用者が影響を受ける可能性
	Ethereum ライブラリ（Web3.js, ethers.js 等）の脆弱性	・Web3.js ライブラリ等で致命的な脆弱性などが発見され、当ライブラリが使用不可になると、ウォレットやシステム運用など外部から Ethereum の接続ができず、多くのサービスが影響を受ける ※Web3.js ライブラリ等は Ethereum ブロックチェーンアクセス共通ソフトウェアであり、脆弱性が発生すると外部からの接続に大きな影響がある	・ライブラリの脆弱性によるサービス中断を想定した準備をしていない（複数のウォレットやクライアントソフトウェアの利用など） ・特定のライブラリに利用者が集中する ・ライブラリの開発体制が属人的な場合がある（ethers.js は開発保守者が 1 名など）	○ ライブラリの脆弱性により DeFi サービスが影響を受ける可能性

	Ethereum Node ソフトウェアの脆弱性	・Ethereum Node のソフトウェア脆弱性によりノード間の通信ができず Ethereum 全体が稼働できなくなる ・Ethereum Node, Ethereum Virtual Machine はノード共通ソフトウェア（開発言語や実装毎に異なる）であり、不具合が発生すると該当するノードが稼働できなくなる。 ・当ソフトウェアに脆弱性が含まれていると、それを利用する全てのノードが脆弱性の影響を受けてしまう	・ソフトウェアの脆弱性によるノード稼働停止を想定した準備をしていない（複数の言語や実装を考慮したノードを準備する） ・当ソフトウェアのうち特定の実装のものに利用者が集中する	○ Ethereum Node ソフトウェアの脆弱性により DeFi サービスが影響を受ける可能性
	Ethereum ライブラリ、Ethereum Node ソフトウェアへの依存	・DeFi 開発者は Web3.js ライブラリや Ethereum Node ソフトウェアに不具合がないことを信頼して利用している	・当ライブラリに不具合が発生した場合を想定した対策を考えていない（代替ソフトウェアの変更、複数ソフトウェアの利用など）	○ DeFi は該当ソフトウェアの使用が必要なシステム構造になっている
	開発元（Ethereum Foundation など）の Ethereum ライブラリ提供中止	・開発元の活動中断などで Web3.js ライブラリ等の提供を中止すると、ウォレットが Ethereum に安全に接続できなくなる懸念がある	・開発元が運営しなくても、他の有志がライブラリの運営を継続できる仕組みになっているか不明である（継続利用できないと利用者への影響が大きい）	× DeFi が利用するライブラリ開発元の運営一般の問題であるが、DeFi に一定影響は及ぼす
	Ethereum ライブラリ、Ethereum Node ソフトウェアの多様性の欠如	・共通ソフトウェアは、当初は様々な仕様や実装により多様化しているが、使っていくうちに単一のものに収斂してしまい、集中度が高まる懸念がある	・共通ソフトウェアの開発元（Ethereum Foundation など）が開発した共通ソフトウェアについて、複数の仕様や実装による多様性を維持管理する仕組みがない	○ DeFi が利用するライブラリやソフトウェアの複数の実装は、DeFi 特有の問題である
インフラプロバイダ	インフラプロバイダ提供サービスの利用集中	・利用者のスマートコントラクト駆動処理が、利便性の高い一部のインフラプロバイダに集中している	・利用者が独自に Ethereum ノードなどのブロックチェーン接続機能を構築することが技術やコストの問題で難しいた	○ 主として DeFi 利用者がインフラプロバイダを利用する

			め、基盤部分は利便性の高いインフラプロバイダが利用される	
	インフラプロバイダ提供サービスの中断	・インフラプロバイダのソフトウェア脆弱性等によりサービスが中断すると、それを利用するスマートコントラクト駆動ソフトウェアが実行できなくなる（Infuraのインシデント事例）	・利用者がインフラプロバイダのサービス停止を想定した対応を検討していない（複数のプロバイダの利用など）	○ 主としてDeFi利用者がインフラプロバイダを利用する
	インフラプロバイダ提供サービスへの依存	・利用者はインフラプロバイダのサービスに不具合がないことを信頼して利用しており、不具合を想定した対策を行っていない	・利用者がインフラプロバイダのサービス停止を想定した対応を検討していない	○ 主としてDeFi利用者がインフラプロバイダを利用する

d. アプリケーション基盤・アプリケーション

表 3-1-4　システム運用のリスク要因（アプリケーション基盤・アプリケーション）

大項目	中項目	リスク事象	考えられるリスク要因	DeFiに密接に関わる問題
DeFi プロトコル	緊急時のDeFiサービス停止	・外部からの攻撃による資金流出やトークン不正増刷などが発生した場合、DeFiサービスの緊急停止ができず、被害が止められない	・緊急時の手段としてDeFi プロトコルを緊急停止する対応を検討していない ・ブロックチェーンの仕様では通常スマートコントラクトは止められないため、DeFi プロトコルで対応する必要がある	○
	緊急時の対応手順	・不測の事態（市場価格暴落や外部からの攻撃など）が発生した場合に、迅速な対応ができずサービスに影響を出す懸念がある ・不測の事態における対応策が明確になっていない可能性がある	・不測の事態に対する対応方針や手順を準備していない ・不測の事態を想定した仕組みや機能を実装していない	○

	DeFi プロトコル利用者の特定	・利用者が仮名の場合、事件発生時に攻撃者・被害者が特定できない	・DeFi プロジェクトでは通常利用者に KYC を求めない	○
	資金流出の防止	・DeFi プロトコルには、外部攻撃などにより資金が流出した場合の資金凍結機能がないものが多く、被害が増大する	・トークンの凍結機能など、不測の事態を想定した対策が取り入れられていない	○
	DeFi プロトコル停止時の資金引き出し	・DeFi プロトコルに脆弱性などの不具合が発生してサービスが停止すると、復旧まで資金を引き出しできない	・DeFi プロトコル停止時に、流動性プールや担保プールなどから資金を引き出す手段を設けていない	○
	Flash Loan による無制限の資金借用	・Flash Loan で巨額の取引を行うと流動性プールの資金が枯渇し、トークン価格が暴落する	・Flash Loan を無担保無制限で借りることができる（但し、高額借用すると手数料が高くなるデメリットもあり、利益を得るためには高度な知識が必要）	○
オラクル	オラクル攻撃	・オラクル価格決定における脆弱性を狙われて外部攻撃を受ける （市場価格と内部オラクル価格の差額を故意に発生させることによるアービトラージなど）	・オラクル価格決定方法は DeFi プロジェクトにより異なり、安全な実装方法が確立していない ・DeFi プロジェクトのうち、オラクル価格が特定プロジェクトの市場価格に連動している場合がある	○ オラクルの脆弱性は DeFi 特有の問題
	外部オラクル価格の反映遅延	・ネットワーク混雑などによる外部オラクルの価格参照が遅延した場合、外部市場と内部オラクル価格の差額が発生する	・オラクル価格の反映を故意に遅らせている場合、市場価格が急変するとオラクル価格が追い付かず差額が大きくなってしまう	○ オラクル価格の反映は DeFi 特有の問題である

3-2　システム開発におけるリスク要因の特定

表 3-2　システム開発のリスク要因

大項目	中項目	リスク事象	考えられるリスク要因	DeFi に密接に関わる問題

ソフトウェア（OS 除く）	Web ブラウザで動くコードのリスク	・Web ブラウザで実行される Defi プロトコルインターフェースなどのコードに脆弱性が発見されると、ウォレットの秘密鍵を窃取されるなどのリスクがある	・DeFi の利用者は Web ブラウザで提供されるウォレットの画面から秘密鍵などの情報を入力することがあり、脆弱性が発見されると被害を受ける懸念がある。	× Web ブラウザで動くコードは他のソフトウェアなどで使用されており、DeFi に密接に関わる問題ではない
スマートコントラクト	スマートコントラクトがアップグレード不可	・アップグレード不可のスマートコントラクトで脆弱性バグが発見されると、修正ができず攻撃による被害が増大する懸念がある ・Upgradability に関する不具合バグがあると、想定した修正ができない	・スマートコントラクトの脆弱性バグを全て解消することは極めて難しく、アップグレード不可はリスクが高いと考える	○ スマートコントラクトの設計は DeFi 特有の問題
	スマートコントラクトがアップグレード可能	・アップグレードの執行は脆弱性バグがないことが前提になっている（一般的にソフトウェアは脆弱性バグがあることを前提としているが、スマートコントラクトは脆弱性バグが損失や攻撃に直結するため、バグの発生が許されない）	・ブロックチェーンで実行した取引は取消しできない（基本的には実行済取引の巻き戻しや過去の金額補正などができない） ・これにより、スマートコントラクトがアップグレード可能であっても、脆弱性バグが許されない状態になっている	○ スマートコントラクトの設計は DeFi 特有の問題
	コードの脆弱性	・既知のコード脆弱性が再発している事例があり、脆弱性が防止できない ⅰ)リエントランシー脆弱性（The DAO, Uniswap など） ⅱ)Flash Loan 攻撃（bZx, Harvest Finance など）	・スマートコントラクトは複雑な機能があり、脆弱性を全て検出することが技術的に難しい	○ スマートコントラクトの脆弱性は DeFi 特有の問題
	不正コードの侵入	・サプライチェーン等から取り込んだ汎用コードに埋め込まれた不正コードにより、スマートコント	・汎用コードを利用する場合に、プログラム仕様を検証していない（または検証するスキルがない）	× 不正コードはソフトウェアの一般的な問題

		ラクトに外部から脆弱性が侵入する		
	テスト検証の制約	・テストネットでは一部のテスト検証ができないが、メインネットでもテストに制約があり、完全なテスト検証ができない	・テストネットではインセンティブに関わる取引確認ができないため、十分なテストをせずにメインネットにデプロイする場合がある（機能はメインネットと同じだが、トランザクションフィーが無料、取引の混雑度が異なるなど）	○ テストネットの環境は DeFi 特有の問題
	スマートコントラクトの誤動作	・自己作成したスマートコントラクトの誤動作（送金アドレス相違など）により資金を損失しても、訂正ができず資金が回収できない	・テストやコード監査ではスマートコントラクトの動作を全て検証できない	× スマートコントラクトの誤動作は DeFi 特有の技術の問題だが、利用者の自己問題であり影響が限定的である
	高度な開発エンジニアの確保	・リエントランシーなど複雑な処理で脆弱性の無いコードを開発できる高度な技術者の確保が難しい（リエントランシー脆弱性は The DAO で発生後、4 年後に Uniswap で再発している）	・スマートコントラクトの開発に必要なセキュリティ技術が確立されていない ・スマートコントラクトの開発エンジニアの技術力を図る指標がない	× 開発エンジニアの確保の問題
	開発エンジニアのスキル問題	・経験の浅いエンジニアがプログラムを開発することで、品質低下やデグレードの発生が懸念される	・エンジニアが既存の開発ルールや品質管理方法などを知らずに開発すると、一定の品質が確保できない	× システム開発の一般的な問題
	コード監査の懸念	・複雑な処理はコード監査で脆弱性を発見できない懸念がある（複数のスマートコントラクトを跨る場合など）	・スマートコントラクトに対する攻撃は高度化しており、コード監査者の専門スキルや監査ツールの検証技術が新しいまたは複雑な攻撃パターンに追い付かない	○ コード監査は DeFi 特有の問題
ブロックチェーン	双方向ブリッジにロックされた資金の攻撃	・Ethereum とサイドチェーン間の双方向ブリッジにロックされた資金を狙われ	・Ethereum の仕様により、サイドチェーンとの資金のやりとりで双方向ブリッジ	○ ブロックチェーン間の資金のやりと

		て、バリデータの秘密鍵を窃取された攻撃により多額の損失が発生する（2022/3 Ronin Network の事例） ・Polygon や Avalanche では数十億ドルの資金がロックされており、万一攻撃を受けて資金を窃取されると甚大な被害となる懸念がある	に多額の資金がロックされるため、攻撃者から狙われやすい	りは DeFi 特有の問題
	ブロックチェーン間の接続	・ブロックチェーンを跨る処理の脆弱性を狙った外部攻撃を受ける ・クロスチェーンのスマートコントラクト呼び出し脆弱性の事例（PolyNetwork） ・トークンブリッジプロトコルの署名検証脆弱性の事例（Wormhole）	・ブロックチェーンを跨る取引が複雑であり、テストでの検証が難しい（テストケースが網羅的でない、異常系テスト・境界条件テスト等が不足）	○ ブロックチェーン間のスマートコントラクトの連動は DeFi 特有の問題
	他のブロックチェーンやレイヤー2 ソリューションの品質問題によるメインチェーンの影響	・Ethereum のスケーリング対策として、サイドチェーン・階層化チェーンやレイヤー2 ソリューションの利用が増加している ・品質に懸念がある他のブロックチェーンやレイヤー2 ソリューションと接続すると、メインチェーンが脆弱性攻撃などの影響を受けるリスクが高まる（Polygon は複数の脆弱性が報告されているなど）	・ブロックチェーンやレイヤー2 ソリューションが多数存在しており、そのうち脆弱性などに懸念があるものが存在する ・プラットフォームの脆弱性などを比較・情報開示する仕組みがない	○ ブロックチェーン間のスマートコントラクトの連動は DeFi 特有の問題
DeFi プロトコル	DeFi プロトコル一部機能の不具合（ガス高騰時の考慮もれ）	・市場価格暴落などの外部要因などにより大量のトランザクションが実行され、ガスの急激な高騰により DeFi プロジェクトの清算処理等が正	・DeFi プロジェクトの業務処理について、急激なガス高騰が発生した場合に自分のトランザクションのガス価格を追い	○

		常に稼働せず、業務処理が中断する（Keeper のトランザクションがガス高騰に追いつかない）	付かせる考慮がされていない	
	DeFi プロトコル一部機能の不具合（ゼロ入札の防止もれ）	・ガス高騰により本来の処理が動かない状態で、ゼロ入札処理により資金が流出する	・ゼロ入札など本来発生しない取引の防止処理が組み込まれていない	○
	DeFi プロトコル間の連動	・DeFi プロトコル間の連動を悪用されて、外部からの要因で前提としていたものを破られる（オラクル価格など） ・Flash Loan（無担保無制限）で借りた巨額の資金を他の DeFi プロトコルの流動性プールに投入され、オラクル価格が急変する ・外部の特定の DeFi プロトコルの市場価格をオラクルで参照している場合、その特定プロトコルの価格を操作することにより、オラクル価格が変動してしまう	・取引額の上限を設定していない（流動性プールの預入額など） ・様々な DeFi プロトコルから連携されることを考慮した設計としていない	○

3-3　ガバナンスにおけるリスク要因の特定

表 3-3　ガバナンスのリスク要因

大項目	中項目	リスク事象	考えられるリスク要因	DeFi に密接に関わる問題
ガバナンス投票	ガバナンス投票の支配	・少数の大手ガバナンストークン保有者が可決の定足数を満たす票数を持つことで、投票が支配される ・コミュニティや開発会社がシステム利用分などを含めてガバ	・ガバナンストークンは暗号資産市場で売買されており、資金を持つ者が多くの投票権を得る仕組みになっている（DAO の意思決定が分散化されていない）	○

		ナンストークンを大量保有しているため、投票が支配される	・ガバナンストークンの保有数に制限がない	
	ガバナンス投票者が仮名	・ガバナンス投票が仮名で行われることで、投票結果の責任を問う相手が特定できない場合がある	・ユーザアカウントのアドレスと個人を紐づける仕組みがない	× ブロックチェーンの仕組みの問題であり DeFi 特有ではない
	投票の定足数が少ない	・ガバナンス投票の定足数が少なく、少数意見で意思決定がされてしまう（主な DeFi プロジェクトの定足数が 1-4%と極めて低い）	・ガバナンス投票の投票率が低いため、提案を可決するために定足数を少なくしていると考えられる	○
	投票率が低い	・ガバナンス投票の投票率が低く、一部の投票者で意思決定がされてしまう（主な DeFi プロジェクトの投票率が約 2-9%と極めて低い）	・暗号資産市場ではガバナンストークンに価値があり投機対象であるため、投機目的のトークン保有者は投票を行う意思が弱い ・ガバナンストークン保有者が投票に動機付けられていない（動機付ける仕組みがない）	○
	悪意のある提案の検証	・悪意のある提案が行われた場合、その検証はコミュニティメンバーの協力に依存されているため、検証を実施する役割が明確でなく、誰も悪意のある提案を発見できない懸念がある。	・分散型の組織において、コミュニティは自由参加であり役割が明示されていない ・悪意のある提案に対して検証が確実に行われるかどうかは不明である	○
	スマートコントラクト修正の依存	・ガバナンス投票の提案によりスマートコントラクトの修正を行う場合、大半のガバナンス投票参加者はスマートコントラクトのコード内容を理解しておらず、提案の内容通りに正しく振る舞うことを前提としている	・ガバナンス投票参加者のうち、スマートコントラクトを技術的に解釈できる人は一部であり、大半は営利目的である ・スマートコントラクトの修正に関する情報開示が不十分であり、コミュニティフォーラム等で提示さ	○

			れたコメントの正当性は保証されない	
	DAO の組織	・DAO は代表者や取締役会が不明確であり、問題が発生しても責任追及が難しい ・DAO は追及先となる組織が存在しない	・DAO は信頼しない参加メンバーによる組織であり代表者がいない ・DAO に適用される法規制がなく、組織の形が定まっていない	○
	DAO の所在地、構成員	・DAO の所在地が不明確である ・DAO の構成員が世界各国に分散しており、国境を越えた規制・追及ができない	・DAO は公的機関に登録されておらず、所在地が不明確である ・どの国の法規制にあたるかも不明確である	○
DeFi プロトコル	DeFi プロトコル利用規約の未周知	・利用者が、DeFi プロトコル利用規約の内容を知らずにサービスを利用して損失を受ける懸念がある	・DeFi プロトコル利用規約（利用者の自己責任）を、サービス利用前に利用者に確認させる仕組みになっていない	○

3-4　金融市場との関わりにおけるリスクの特定

表 3-4　金融市場との関わりのリスク

大項目	中項目	リスク事象	考えられるリスク要因	DeFi に密接に関わる問題
暗号資産市場	暗号資産市場のバックストップ機能がない	・金融市場で法定通貨の価格暴落などのシステミックリスクが発生した場合、バックストップとして各国の中央銀行が機能するが、暗号資産市場ではバックストップ機能がない ・暗号資産市場でシステミックリスクが顕在化すると、市場全体が大きな影響を受ける ・2020 年 3 月のブラックサーズデイなど実際に大暴落を経験しており、対策が難しい	・暗号資産市場でトークンの価格が下落する場合に、その価格を安定させるメカニズムがない	× 暗号資産市場一般に関する問題

	損失リスクの説明不足	・専門知識の低い一般投資家が、ボラティリティの高い暗号資産のリスクを知らずに取引を行い、損失を受ける懸念がある	・取引における損失リスクを利用者に認識させる仕組みになっていない	× 暗号資産市場一般に関する問題
DeFi プロトコル	金融機関の損失リスク	・DeFi アプリケーションと接続して暗号資産取引を行った金融機関が、市場価格の下落やインシデント時に損失を計上する可能性	・脆弱性が潜んでいる可能性がある DeFi プロトコルの利用やボラティリティの高い暗号資産の保有に伴う損失リスク	○ DeFi アプリケーションと接続した金融機関の問題
	企業の損失リスク	・ガバナンストークン等も含めた暗号資産に投資した企業が、価格下落に伴い損失を被る可能性	・脆弱性が潜んでいる可能性がある DeFi プロトコルの利用やボラティリティの高い暗号資産の保有に伴う損失リスク	○ DeFi プロトコルで使用する暗号資産のボラティリティの問題
	ユーザへの説明不足	・利用者が、DeFi プロトコルの利用規約や免責事項が一般的な金融サービスと異なる点や、損害時の対応（損害補償なし）を知らずに取引を行い、損失を受ける懸念がある	・法定通貨と異なる点や損害時の対応を、取引前に利用者に注意を促す仕組みになっていない	○ DeFi ユーザへの説明責任に関する問題
スマートコントラクト	市場安定性	・特定の暗号資産の価格下落などがスマートコントラクトを通じて他に自動的に連鎖していき、市場全体の不安定化に繋がる	・スマートコントラクトはコードに従い決められた取引を自動実行するが、金融市場を安定させるための仕掛け（影響を伝播させない機能など）が組み込まれていない	○ スマートコントラクトの機能は DeFi 特有の問題

第４章 分散型金融システムにおけるリスク低減策についての分析

本章では、前章で整理したリスク要因のうち DeFi 特有の問題について、具体的なリスク低減策と当局監督における対応案の考察を試みる。

4-1 ではシステム運用、4-2 ではシステム開発、4-3 では金融市場との関わりにおける観点からリスク低減策と実現に向けた案を分析する。

分析したリスク低減策について、前述のとおり分散型金融システムのトラストポイントが集中している部分が複数存在しているため、既存の金融機関と同じリスクを有していることになり、リスク低減策も既存の金融機関と同じく中央集権的な対策になると考えられる。

但し、分散型金融システムの分散化が進むと、今回分析したリスク低減策が使えるとは限らないため、対策内容の見直しが必要と考える。

また、DeFi プロジェクト運営組織や利用者にトラストポイントを正しく認識させる必要がある。本調査研究の分析で検出した複数のトラストポイントについて、DeFi プロジェクトのコミュニティなどではトラストポイントに関する議論は特に行われておらず、DeFi プロジェクトの運営組織や利用者がトラストポイントを正しく認識していない懸念がある。よって、トラストポイントを DeFi プロジェクト運営組織や利用者に正しく認識させることが重要である。

なお、リスク低減策の実現については、DeFi プロジェクトやブロックチェーンの管理団体などがリスク低減策の実施に対して協力的であることが議論の前提になっているため、対策の実施においては協力を得る仕組みを検討することが必要である。

4-1　システム運用におけるリスク低減策の分析

表 4-1-1　システム運用のリスク低減策

大項目	中項目	考えられるリスク要因	リスク低減策（案）	留意事項等
ソフトウェア（OS 除く）	Ethereum ライブラリ、Ethereum Node ソフトウェアの多様性が損なわれる	・共通ソフトウェアは、複数の仕様や実装を装備していても、時間が経過すると単一のものに収斂してしまい、多様性を維持管理する仕組みがない	・開発元の団体（Ethereum Foundation など）が、本件のリスクを認識し、利用者を複数のソフトウェアに分散する仕組みを実装する ・当局の監督が及ぶ組織については、ソフトウェアの調達において設計多様性が満たされることを条件にする（仕様や実装が異なる複数のソフトウェアの準備を条件にする） ・ソフトウェア間の利便性に相違がないように利用条件を工夫し、利用集中が起きないように工夫する ・ソフトウェアの分散が難しい場合は、ソフトウェア開発の品質向上策により解決を図る	・規制当局から開発元の団体への働きかけを行う方法の検討が必要（ブロックチェーン管理団体はグローバルな組織であることが多く、日本からの連携が難しい懸念あり） ・複数のソフトウェアに分散しても、利便性などにより単一のものに収斂しないよう、利用状況を含めて継続的に監視する必要がある

	Ethereum ライブラリ、Ethereum Node ソフトウェアへの依存	・利用者がソフトウェアの品質や継続利用できることに依存し、使用できない場合の対策を考えていない	・開発元の団体が、利用者に本件のリスクを周知する	・開発元の団体への働きかけを行う方法の検討が必要
	ホット・ウォレットの攻撃	・トークン大口保有者は、アカウントアドレスとトークン保有量が公開されており、攻撃されやすい（特定のユーザーアカウントアドレスにトークンを大量に保有している場合）	・ブロックチェーンの仕様上、トークン大口保有者のアカウントアドレスとトークン保有量を非公開にすることは難しい ・対策として、トークン大口保有者にユーザの秘密鍵の安全な保管方法などの技術情報を周知する	・規制当局またはそれに準ずる機関が、安全性の高いユーザの秘密鍵保管技術を検証・認定し、利用者に周知するルールを検討する必要がある ・秘密鍵の保管技術の例 ⅰ)秘密分散： 秘密鍵を複数に分割し、複数人で分けて保管する（有識者ヒアリングにて利用を確認） ⅱ)ソーシャルウォレット： 信頼できる知人・友人に公開鍵変更権を渡して保管を委ねる ・ウォレット技術は複数存在するため、利用者にオプションを提供することが重要である（有識者ヒアリングより）
インフラプロバイダ	インフラプロバイダ提供サービスの利用集中	・利用者が独自に Ethereum ノードなどのブロックチェーン接続機能を構築することが技術やコストの問題で難しいため、基盤部分は利便性の高いインフラプロバイダが利用される	・インフラプロバイダが、利用者に対してサービス利用集中によるリスクを周知する（サービス利用時にリスクを確認できる仕組みの提供など） • DeFi のサービスが停止する事態の重要度に応じて、複数のインフラプロバイダを冗長に使用することを推奨する	・リテラシーの低い利用者に、リスクを認識させたうえで利用させることが必要である。
	インフラプロバイダ提供サービスへの依存	・利用者は、インフラプロバイダのサービスが停止しないことに依存している		

	インフラプロバイダ提供サービスの中断	・利用者がインフラプロバイダのサービス停止を想定した対応を検討していない（複数のプロバイダの利用など）	・インフラプロバイダが、不慮のサービス停止を防止するため、カオスエンジニアリングなどの不具合による耐性強化策を実施する ・インフラプロバイダが、品質に関する認証（SOC2）を取得し、サービス停止のリスクを低減する	対策として考えられる施策は以下の通り ・カオスエンジニアリング： 本番環境に障害を注入し、回復する機能を常に動かしておく手法。Netflix や AWS で実施している ・SOC2：System and Organization Controls 2 アウトソーシング事業者（受託会社）における内部統制・保証報告の枠組みを利用する
DeFi プロトコル	Flash Loan による無制限の資金借用	・利用者が Flash Loan を無担保無制限で借りることができる（但し、高額借用すると手数料が高くなるデメリットもあり、利益を得るためには高度な知識が必要）	・DeFi プロトコル開発者が本件のリスクを認識し、取引上限額などの設定を検討する ⅰ)Flash Loan 利用時の担保額設定（借入資金の n%） ⅱ)Flash Loan 利用額の上限設定	・無担保借入を担保必要に変更することで、巨額の借入には巨額の担保が必要になり、悪用が防止できる
	緊急時の DeFi サービス停止	・緊急時の手段として DeFi プロトコルを緊急停止する対応を検討していない ・ブロックチェーンの仕様ではスマートコントラクトは止められないため、DeFi プロトコルで対応する必要がある	・DeFi プロジェクトに対して、緊急時に DeFi プロトコルを緊急停止できる機能を設けるよう指導する	・攻撃を受けても影響しない完全なスマートコントラクトの開発は極めて難しいと考える ・よって、緊急時に被害を最小限に抑える手段として緊急停止機能を備えておくことが重要である
	不測時の対応	・不測の事態に対する対応方針や手順を準備していない ・不測の事態を想定した仕組みや機能を実装していない	・DeFi プロジェクトが不測の事態に対するコンティンジェンシープランを策定し、必要なシステム対応を明確にする ・その方針に従い、外部オラクル停止や DeFi プロトコ	・コンティンジェンシープランや定期的な訓練実施は、ブロックチェーン管理団体が DeFi プロジェクト向けにガイダンスを出す方法が考えられる ・Maker では主な不測の事態を 5 つ設

			ル緊急停止などの対応を実装する ・また、DeFi プロジェクトがコンティンジェンシープランの定期的な訓練を計画・実施することで、万一の発生時に円滑な対応ができるようにしておく	定し、そのコンティンジェンシープランを策定している ・定期的な訓練として、ハードニングなどの手法が考えられる ※ハードニング：運営者と攻撃者の 2 チームに分かれて攻撃と防御を実際に行い、運営者が実地で経験を積むこと
	資金流出の防止	・DeFi プロトコルは、攻撃による資金流出など、不測の事態を想定した対策を検討していない場合がある	・DeFi プロトコルは攻撃を受けるリスクが高いことから、ブロックチェーン管理団体が、攻撃時の資金流出を防止する対策のルール化や実装のガイドを行う	
	DeFi プロトコル停止時の資金引き出し	・DeFi プロトコル停止時に、流動性プールや担保プールなどから資金を引き出す手段を設けていない	・DeFi プロジェクトに対して、緊急時に一定額の資金引き出し機能を設けるよう指導する（但し攻撃を受けるリスクの懸念あり）	・資金引き出し不可は利用者保護として重大なリスクであり、対策は必須と考える ・発生時の影響を低減させるため、利用者にリスクを認識させることで利用額を制限するなどの対策も考えられる
オラクル	オラクル攻撃	・オラクル価格決定方法は DeFi プロジェクトにより異なり、安全な実装方法が確立していない ・DeFi プロジェクトのうち、オラクル価格が特定プロジェクトの市場価格に連動している場合がある	・ブロックチェーン管理団体が、DeFi プロジェクト横断でオラクル価格決定方法の標準化や推奨方式の検討・周知を行う	・安全なオラクル利用方法を周知することで、一定の安全度を確保する
	外部オラクル価格の反映遅延	・オラクル価格の反映を故意に遅らせている場合、市場		

		価格が急変するとオラクル価格が追い付かず差額が大きくなってしまう		

システム運用のリスク低減策を分析した結果、特に重要と考えられるリスク低減策として以下を指摘する。

a. ブロックチェーン管理団体（Ethereum Foundation など）への働きかけ

Ethereum ライブラリや共通ソフトウェアの利用集中は、分散型金融システムのメリットである SPoF の解消ができなくなる懸念があり、既存の金融機関と同じ中央集権的なリスクを有する問題となる。この問題は意図的に複数の実装などを準備して単一のものに収斂しないよう継続的に監視することが重要であり、実現性について検討する必要があると考える。

b. 利用者へのウォレット・DeFi の安全な利用方法の周知徹底

利用者がウォレットや DeFi を利用するにあたり、リテラシーの低い利用者であっても安全に利用できる方法を特定して周知する仕組み（認証機関による認証やガイドの発出、リスクの周知など）を検討することで、利用者が不利益を受けないように保護することが必要と考える。

4-2　システム開発におけるリスク低減策の分析

表 4-2　システム開発のリスク低減策

大項目	中項目	考えられるリスク要因	リスク低減策（案）	留意事項等
スマートコントラクト	スマートコントラクトがアップグレード不可	・開発者やコード監査会社がスマートコントラクトの脆弱性を全て解消することは極めて難しく、アップグレード不可はリスクが高い	・スマートコントラクトをアップグレード可能にすることで、リスクが低減されると考える	・スマートコントラクトのアップグレードには、一般的にインフラプロバイダの提供サービス（OpenZeppelin Upgrades Plugins など）を利用することになり、どのサービスを導入するか検討が必要になる
	スマートコントラクトがアップグレード可能	・ブロックチェーンの仕様により、実行した取引を後から取消しできないため、スマートコントラクトの脆弱性が許されない状態になっている（基本的には実行済取引の巻き戻しや過去の金額補正などができない）	・DeFi プロトコルが、過去取引を取消す逆取引（送金取引を逆に実行して資金を戻すなど）によりリスクが低減できると考えられる ・逆取引の実現性や有効性について今後の検討が必要と考える	・ブロックチェーンの仕様上は過去取引の取消しはできないが、逆取引を自動的に行う仕組みにより過去取引が取消しできる可能性がある

	コードの脆弱性	・開発者やコード監査会社は、スマートコントラクトの複雑な機能から脆弱性を全て検出することが技術的に難しい	・DeFi プロトコルの開発において、ソフトウェア開発の品質を確保するための最新技術を駆使し、脆弱性をできる限り排除する ⅰ)形式検証 ⅱ)機械学習による自動テスト　など ・開発技術の事例周知や推奨は、ブロックチェーン管理団体が行うことが望ましい	・ブロックチェーン管理団体への働きかけを行う方法の検討が必要
	テスト検証の制約	・開発者は、テストネットでインセンティブに関わる取引確認ができていない状態で、メインネットにデプロイする懸念がある（機能はメインネットと同じだが、トランザクションフィーが無料、取引の混雑度が異なるなど）	・テストネットにインセンティブに関わる取引確認の手段を提供する ・内容により、メインネットにおけるテスト手法を検討する	・対策はテストネットの機能強化が好ましいが、コスト面など実現性が難しい問題があると考えるため、実現性の検討が必要
	コード監査の懸念	・スマートコントラクトに対する攻撃が高度化しているため、コード監査者が専門スキルや監査ツールの検証技術が新しい、または複雑な攻撃パターンに追い付かない	・コード監査会社が、スマートコントラクト脆弱性検知技術やツールの検知精度を向上させる ・コード監査会社が協業して技術向上の仕組みを行う（定期的にコンペを行いランク付けするなど）	・コード監査ツールの分析技術例 ⅰ)静的検証 スマートコントラクトのコードを検証 ⅱ)動的検証 スマートコントラクトを実行しながら検証 ⅲ)形式検証 形式手法や数学的手法を利用し、 形式仕様記述やプロパティに照らして コードが正しいことを証明する
ブロックチェーン	双方向ブリッジにロックされた資金の攻撃	Ethereum とサイドチェーンの資金のやりとりのため、双方向ブリッジに資金をロックする仕様であ	・資金を狙う攻撃の防止策の実施（秘密鍵管理技術の高度化、安全な秘密	・秘密鍵の保管技術の例 ⅰ)秘密分散： ⅱ)ソーシャルウォレット：

		り、この資金を狙われる	鍵管理方法の周知など） ・双方向ブリッジに資金をロックする仕様の見直し（巨額の資金が１ヶ所に集中しないように考慮）	・双方向ブリッジの仕様見直しは実現性の検討が必要
	ブロックチェーン間の接続	・ブロックチェーンを跨る取引は、処理が複雑でありテストでの検証が難しい（テストケースが網羅的でない、異常系テスト・境界条件テスト等が不足）	（4-2 コードの脆弱性と同じ）	（4-2 コードの脆弱性と同じ）
	他のブロックチェーンやレイヤー2 ソリューションの品質問題によるメインチェーンの影響	・ブロックチェーンやレイヤー2 ソリューションが多数存在しており、そのうち脆弱性などに懸念があるものが存在する ・プラットフォームの脆弱性などを比較・情報開示する仕組みがない	・レイヤー2 ソリューションや他のブロックチェーンとの連携検討時に、品質確保について DeFi プロジェクト関係者間で検討を行う	・インフラプロバイダでは、連携する DeFi プロジェクトの開発者同士でプロトコル間の影響などを直接確認し、品質確保に努めているとされる
DeFi プロトコル	DeFi プロトコル一部機能の不具合（ガス高騰時の考慮もれ）	・開発者は、一部の DeFi プロトコルで急激なガス高騰が発生した場合に自分のトランザクションのガス価格を追い付かせる考慮がされていない	・Ethereum および 2nd Layer のスケーリング技術の採用により、急激なガス高騰を発生させない仕組みを構築する	スケーリング対策として以下が計画、実施されている ・Ethereum2.0（シャーディング）の利用（計画中） ・2nd Layer ソリューションの利用 ・サイドチェーンの利用
	DeFi プロトコル一部機能の不具合（ゼロ入札の防止もれ）	・開発者は、一部の DeFi プロトコルでゼロ入札など本来発生しない取引の防止処理を組み込んでいない	・DeFi プロトコルにゼロ入札の防止策として最低金額を設定する ・本来の入札機能が稼働しなかった問題は、ガス高騰時の考慮もれ対策により解決される	・Maker では入札の最低金額を元値の 3%に設定した
	DeFi プロトコル間の連動	・DeFi プロトコルは、取引額の上限を設定していない	・DeFI プロトコルトが、外部の様々な DeFi プロトコルか	（4-2 コードの脆弱性と同じ）

		（流動性プールの預入額など） ・DeFi プロトコルは、様々な DeFi プロジェクトから連携されることを考慮した設計としていない	ら連携されることを考慮し、自己防衛のためのテスト検証を行う必要があると考えられる ・テスト検証の手法については、コードの脆弱性対策に含む	

システム開発のリスク低減策を分析した結果、主なリスク低減策として以下が考えられる。

a. 過去の取引を取消しできる仕組みの検討が必要

ブロックチェーンの仕様により一度実行した取引は後から取消しできないため、スマートコントラクトの脆弱性が許されない状態になっている（基本的には実行済取引の巻き戻しや過去の金額補正などができない）

対策として、脆弱性発見時の安全な巻き戻しができる仕組み（送金取引を逆に実行して資金を戻すなど）について、実現性や有効性を含めて今後の検討が必要である。

b. スマートコントラクトの脆弱性対策の高度化

インシデント事例より、スマートコントラクトの脆弱性は現在も解消せず、過去に発生したリエントランシー脆弱性などのインシデントがその後再発するなど、脆弱性を完全になくすことは極めて難しい。有識者ヒアリングの情報より、最先端の技術では機械学習による自動テストなど高度な開発ツールが準備されており脆弱性の検出能力が高まってきているが、。スマートコントラクトの脆弱性の完全な解消にはまだ程遠い状況である。

直近の対策としては経験のある開発者を揃えて脆弱性を低減することが必要であるが、今後のスマートコントラクト脆弱性の解消に向けて検出技術の高度化を継続的に進めることが重要と考える。

c. 双方向ブリッジにロックされた資金の窃取の防止

サイドチェーンの双方向ブリッジには最大で数十億ドルの資金がロックされており、攻撃者に狙われている。このリスク低減策として、秘密鍵管理技術の高度化や安全な秘密鍵管理方法の周知などが重要である。また、双方向ブリッジに資金をロックする仕様について、巨額の資金が１ヶ所に集中しないように考慮する必要がある。

4-3　ガバナンスにおけるリスク低減策の分析

表 4-3　ガバナンスにおけるリスク低減策

大項目	中項目	考えられるリスク要因	リスク低減策（案）	留意事項等
ガバナンス投票	投票の定足数が少ない	・ガバナンス投票の投票率が低いため、提案を可決するために定足数を少なくしていると考えられる	・ガバナンス投票の投票率の向上に合わせて、本来望ましい定足数に増やしていく	・ガバナンス投票が少数の意見に偏らないように、適切な投票率や定足数を維持するための運営組織のルールを設けるよう指導する
	投票率が低い	・暗号資産市場ではガバナンストーク	・投票委任の仕組みや、投票によるト	

		ンに価値があり投機対象であるため、投機目的のトークン保有者は投票を行う意思が弱い	ークン付与など、ガバナンストークン保有者の投票のインセンティブを向上する	・運営組織への指導はブロックチェーン管理団体が行うことが望ましい
	悪意のある提案の検証	・分散型の組織において、コミュニティは自由参加であり役割が明示されていない ・悪意のある提案に対して検証が確実に行われるかどうかは不明である	・運営組織の役割として、提案の検証者を明示的に設ける（有償が望ましい）。または形式検証による提案検証の検討など。 ・悪意のある提案を検証するための作業期間（提案のタイムロック）を適切に設定する	・提案の検証者の設置や内容開示などの役割について、運営組織のルールを設けるよう指導する ・運営組織への指導はブロックチェーン管理団体が行うことが望ましい
	スマートコントラクト修正の依存	・ガバナンス投票参加者のうち、スマートコントラクトを技術的に解釈できる人は一部である ・提案内容の情報開示が不十分であり、提案の正当性が保証されない懸念がある	・運営組織の役割として、提案の検証者がスマートコントラクトの内容を投票者に開示する（提案内容と齟齬がないことをチェックする）	

4-4　金融市場との関わりにおけるリスク低減策の分析

表 4-4　金融市場との関わりのリスク低減策

大項目	中項目	考えられるリスク要因	リスク低減策（案）	留意事項等
金融機関との関わり	金融機関の損失リスク	・脆弱性が潜んでいる可能性がある DeFi プロトコルの利用やボラティリティの高い暗号資産の保有に伴う損失リスク	・DeFi プロトコルの信頼性に関する検証を行う。 ・暗号資産のボラティリティを考慮して資産配分や上限額を設定する	・暗号資産はボラティリティが高く、また攻撃などによる資金盗難リスクも考慮する必要があり、リスクを十分に考慮した資産運用が重要
企業との関わり	企業の損失リスク			
スマートコントラクト	市場安定性	・スマートコントラクトはコードに従い決められた取引を自動実行するが、金融市場を安	・不測の事態による金融市場への影響を防ぐ目的で、価格変動連鎖防止な	暗号資産の市場安定化機能として、以下が考えられる ・急激な価格変動でオラクル価格を緩

		定させるための仕掛け（影響を伝播させない機能など）が組み込まれていない	ど市場安定化機能を検討する	やかに反映する機能 ・基準額を超えた価格変動ではオラクル価格の反映を抑止する機能　など

おわりに

当報告書は、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等に関する調査研究を行った結果を述べているが、分散型金融システムや DeFi は未だ発展途上であり、今回の調査対象外である NFT サービスやアグリゲーターが数多く出現しているなど、成長を続けている。また、今回の調査研究では主にブロックチェーン内部の DeFi プロジェクトについて技術リスクの調査研究を行ったため、ブロックチェーンの外部の構成要素については詳細なリスクの特定ができていない認識である。ついては、以下の項目については今後の主な課題として整理し、将来の活動において深堀り調査が必要と考えられる。

【今後の課題として深堀りが必要と思われる事項】

・ブロックチェーン外部のウォレット端末や運用サーバなどを構成する構成要素の技術リスク特定
　オペレーティングシステム、Web ブラウザ、ウォレット、クライアントソフトウェア、ユーザインターフェースなどを対象とした技術リスクの特定を行う。

・スマートコントラクトの脆弱性検出技術の状況アップデート
　スマートコントラクトの脆弱性を検出する技術はまだ成熟まで程遠い状況であり、機械学習を利用した開発ツールやインシデント事例を踏まえた監査ツールなどが開発されているが、継続してアップデート状況を注視する必要がある。

また、当報告書で指摘したリスク低減策はあくまで一例に留まり、最適なリスク低減策を見出すためには、DeFi 開発者やビジネス関係者、アカデミア、当局などのステークホルダーに課題解決に向けた議論を行うことが欠かせない。例えば、DeFi プロジェクト側において、ソフトウェア開発の品質を確保するための脆弱性の低減に向けた取り組みを行い、開発技術の事例周知や推奨は、ブロックチェーンを管理団体（Ethereum Foundation など）が行う。金融監督当局側は、DeFi の仕様や情報セキュリティ（コード開発・テスト検証技術等）に関する知見を有する技術者等を確保するなど、イノベーションと必要なリスク低減の両立に向けた態勢整備を行うといったことが考えられる。当報告書が、ステークホルダー間の今後の建設的な対話に向けた一助となれば幸いである。