特集
Special Feature

[Web3.0 時代のサイバーセキュリティ―インターネット経済のパラダイム転換に向けた課題と展望―]

5 金融分野の分散管理型システムのサイバーセキュリティ

― DeFi の活用事例とサイバーインシデントの紹介―

応用 一般

林　敬祐　金融庁 総合政策局 フィンテック参事官室

金融分野における分散管理型システム

金融分野における分散管理型システムについては，近年 DeFi（Decentralized Finance）の議論が盛んである．DeFi は，分散管理型金融と称され，従来の特定の金融機関がサービスを管理する中央集権的な金融サービスとは異なり，DAO（Decentralized Automated Organization, 分散型自律組織）により非中央集権的に自律的に運営されることを特徴とするが，確立した定義があるものではない．DeFi には分散型取引所（Decentralized Exchange, DEX），ステーブルコイン，レンディング，デリバティブなど暗号資産を用いたさまざまな金融サービスがある．

2023 年 2 月に FSB（Financial Stability Board, 金融安定理事会）が公表した「分散型金融の金融安定上のリスク」の報告書[1]（以下「FSB 報告書」という）によると，DeFi は暗号資産市場におけるさまざまなサービスを表すための総称であり，伝統的金融システムの一部の機能を再現する一方で，その機能を提供する仲介者が存在せずガバナンスを分散化させているように見せることを目的とするものとされている．DeFi は伝統的金融システムに見られる中央集権型（Centralized）のシステムと対比して，中央集権的な管理者がいない非中央集権型（Decentralized）のシステムの構築を目指しているとされ，そのような非中央集権的なガバナンスを持つ組織は DAO と呼ばれる．しかし，FSB 報告書は，DeFi のガバナンス体制はさまざまなものがあり，非中央集権的と謳いつつ実際には一部の者により支配されているものが多いと指摘している．DeFi は責任主体が曖昧であることから，既存の金融規制アプローチではサイバーセキュリティ対策を含め適切な規制を課すことができない懸念がある．本稿では DeFi の概要，活用事例を概説し，DeFi に対するサイバーインシデントやサイバーセキュリティリスクを紹介する．

DeFi の概要

DeFi の詳細はそれぞれのサービスにより異なるが，一般的には，運営コミュニティが管理する DeFi プロトコルが，ユーザインタフェースを通じて，個人や法人等のユーザへサービスを提供するものである．DeFi を構成する要素をどの範囲までにするかについて確立した定義があるものではないが，本稿では金融庁が外部委託先と合同研究を行った研究結果報告書[2]を参考に，運営コミュニティ，DeFi プロトコル，ユーザインタフェースの 3 点を主な構成要素とし，それぞれについて概説する（図 -1）．

運営コミュニティ

運営コミュニティは，通常，DeFi プロジェクトの創設者や DeFi プロトコルを開発・維持する運営者，ガバナンストークンという運営方針に関する投票権を持つ参加者等により構成される．この組織

はDAOと称され，特定の者に運営権限がゆだねられるのではなく，運営コミュニティを構成する者たち全員による多数決などで自律的に運営される．

会社などの法人であれば，法的に権利および義務の帰属主体が1つの法人に観念され，法人に所属する従業員等が行った行為やこれに関連して生じる権利および義務はすべて1つの法人に帰属する（たとえば，権限を持つ従業員が契約書に署名すれば契約の効力はその従業員が所属する法人に帰属する）．しかし，DAOは必ずしも法的な権利および義務の帰属主体が1つに定まっておらず，運営コミュニティ間の関係も不明確であり，誰がDeFiサービスに関し責任を負うのか，誰に対して規制をかけるべきなのかが明らかではないという点が既存の金融規制アプローチをとる際の課題となる．

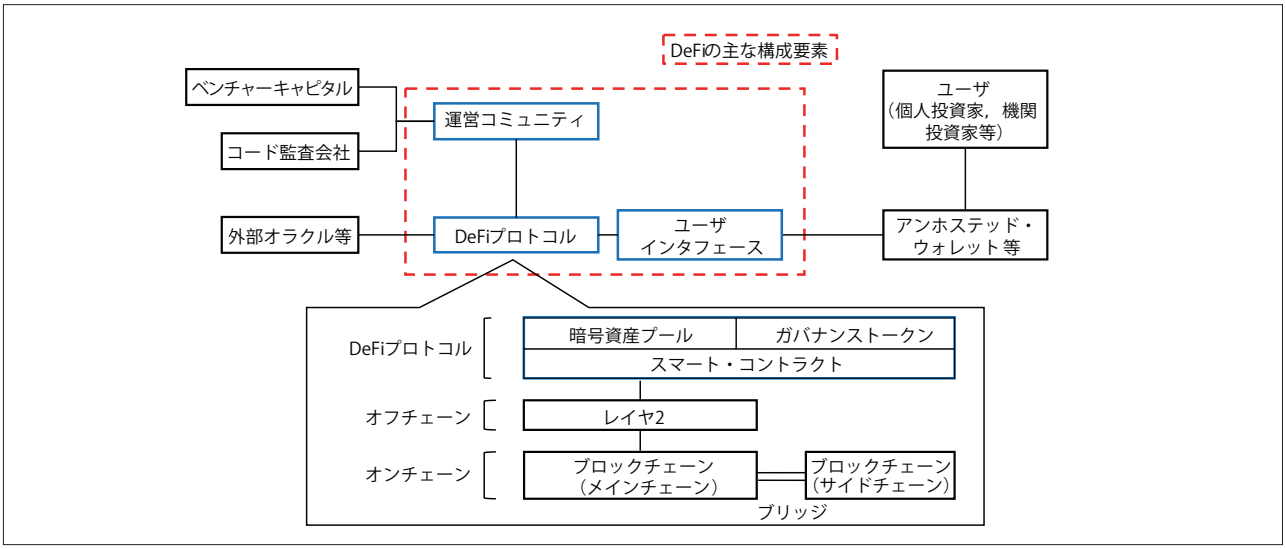
そのほか運営コミュニティに関連する者としては，DeFiプロジェクトが出資を受けているベンチャーキャピタル等の投資家や，DeFiプロトコルのコードにセキュリティ上の問題がないかなどにつき確認する外部のコード監査会社が挙げられる．

DeFiプロトコル

DeFiプロトコルには，DeFiサービスの内容を定めた取引条件が規定されており，これは複数のスマート・コントラクトとユーザインタフェースの組合せから構成される．スマート・コントラクトは，自動実行のコードで，ブロックチェーン上に設置され，自動的に取引条件を実行する．DeFiプロトコルが実行されることで，ブロックチェーン上に当該取引が記録される．また，DeFiサービスには，利用する暗号資産を保管するための暗号資産プールがあり，スマート・コントラクトを用いて暗号資産プールに保管された暗号資産が出し入れされる．

DeFiプロトコルで実行された取引はブロックチェーン上に記録されるが，処理速度の向上や費用を抑える目的で，あるブロックチェーン（メインチェーン）と別のブロックチェーン（サイドチェーン）とを接続し，当該サイドチェーンにおいて大量の取引処理をする場合が多い．2つのチェーンの取引記録を結びつけるものをブリッジという．ブリッジは，たとえば，メインチェーン上の暗号資産をロックし，そのロックした暗号資産に対応した別の暗号資産をサイドチェーン上で新たに記録（発行）し，サイドチェーン上の当該暗号資産を用いて大量の複数の取引処理を行い，これらの取引処理の最終結果のみをメインチェーン上に記録するといった処理を行う．

加えて，処理速度のさらなる向上等を目的として，オフチェーン上のレイヤ2（レイヤセカンド）で大量の複数の取引処理を行い，これらの取引処理の最



■図-1　DeFiの概要―文献1）および文献2）をもとに作成

終結果のみをメインチェーンに記録するといった処理も行われる場合がある．

DeFi プロトコルの取引対象となる暗号資産の市場価格等の情報はオフチェーン上の情報であるため，DeFi プロトコルの実行において，外部のオラクルに接続し価格情報等を取得する必要がある．

ユーザインタフェース

DeFi プロトコルとユーザが使用するアンホステッド・ウォレット等を結びつけるものがユーザインタフェースであり，画像のインタフェースやその他の構成要素を組み合わせてユーザにサービスを提供し，DApps（Decentralized applications）と呼ばれる．アンホステッド・ウォレットとは，暗号資産交換業者などが秘密鍵を管理するホステッド・ウォレットとは異なり，ユーザ自らが秘密鍵を管理するウォレットのことをいう．ユーザとしては個人投資家，機関投資家等がおり，アンホステッド・ウォレット等を用いて DeFi プロトコルに接続する．

DeFi の活用事例とサイバーセキュリティリスク

DeFi の活用事例として，分散型取引所（DEX）とステーブルコインを取り上げる．

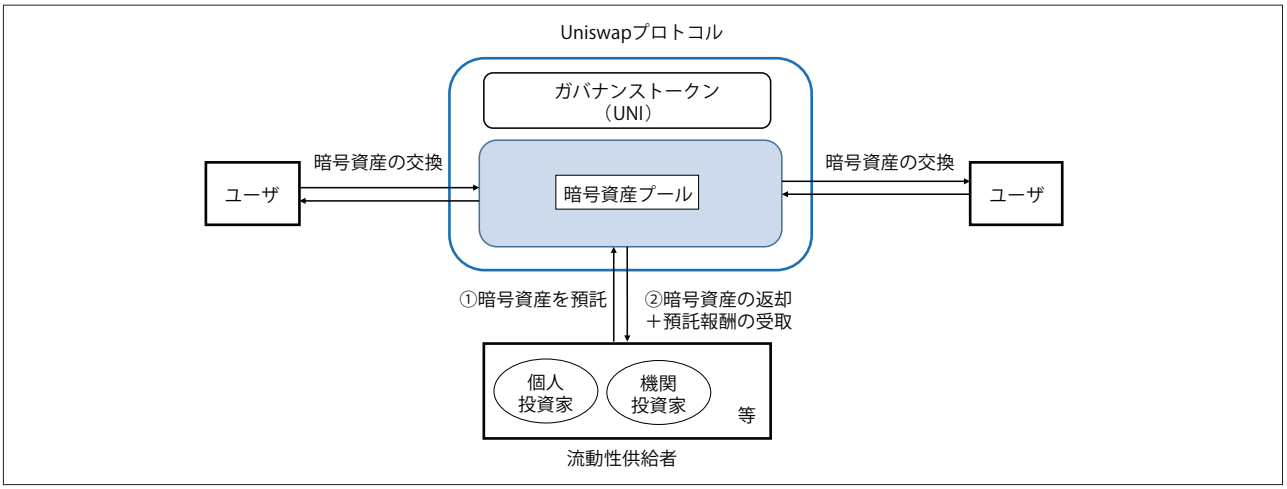
分散型取引所（DEX）

Uniswap の概要

分散型取引所は，スマート・コントラクトにより自動的に暗号資産の交換を行うプラットフォームである．暗号資産交換業者などの特定の運営主体が運営する中央集権型の取引所とは異なり，暗号資産の価格や流動性の管理の機能を有する DeFi プロトコルにより自律的に運営が行われる．代表的なものに Uniswap がある（図 -2）．

Uniswap の取引所の方式は，いわゆる自動マーケットメイカー（Automated Market Maker, AMM）方式といわれ，Uniswap プロトコルは自動化されたアルゴリズムによる取引所としての機能を担い，暗号資産プールに取引の対象となる暗号資産をたくわえる．取引は一方の暗号資産と他方の暗号資産を交換するものであるため，たくわえる暗号資産はペア（2 つで 1 組）となる（たとえば，イーサリアム（ETH）とステーブルコイン DAI（後述）のペアなど）．暗号資産プールへの暗号資産の供給は，個人投資家，機関投資家等（以下「流動性供給者」という）が暗号資産を預託することによって行われる．流動性供給者が暗号資産の返還を受ける際には，預託した数量分の暗号資産と報酬を受けとる．

一方，ユーザは，Uniswap を利用して自ら望む暗号資産（たとえば，ETH）を取得するために他方のペアの暗号資産（たとえば, DAI）を暗号資産プー



■図 -2　Uniswap プロトコルの概要―UniswapWeb サイト，文献 2）をもとに作成

ルに送付するのと引き換えに，Uniswap プロトコルから目的の暗号資産（ETH）を受けとることができる．暗号資産プール内の暗号資産の価格は，暗号資産プール内の暗号資産の数量に基づいて自動的に算出され，暗号資産がプールの中から出し入れされるたびに，プール内の暗号資産の価格が変動する．これにより外部の暗号資産取引所における暗号資産の価格との間で差異が生じ，その価格の差異を利用して利益を得る裁定取引の機会が生じる．こうした裁定取引が行われると，プールの中にある暗号資産の価格と外部の暗号資産取引所の暗号資産の価格の差異は縮小されることになる．

なお，Uniswap プロトコルの運営方針は，運営コミュニティや，ガバナンストークンである UNI トークンを保有する者等による投票により分散的・自律的に決定される．

Uniswap におけるサイバーセキュリティリスクやサイバーインシデント

Uniswap プロトコルは，中核となるスマート・コントラクト（以下「コアコントラクト」という）は修正できない仕様となっているため，一度ブロックチェーン上に設置してしまうと，外部からの攻撃に対応してプロトコルを柔軟に変更することができないという弱点がある．そのため，致命的な脆弱性が見つかった場合，脆弱性を修正したスマート・コントラクトを新たに作成し，それを用いて Uniswap プロトコルの機能改善を行う必要がある． Uniswap は機能改善等のため新しいプロトコルの実装を複数回行っており，2023 年 7 月現在，バージョン 1 から 3 までの 3 つのプロコトルが独立して稼働している．なお，Uniswap Lab によると現在バージョン 4 のプロトコルの作成に取りかかっている．

Uniswap におけるサイバーインシデントとしては，2020 年 4 月，Uniswap へリエントランシー脆弱性をついた攻撃が行われ約 30 万米ドルの損害が生じたものがある．この攻撃は，不正な再帰的な関数の実行によりもたらされた．プロトコルが正常に機能する場合，たとえば，ユーザと暗号資産プールとの間で暗号資産 A と暗号資産 B の交換が行われる際に，暗号資産プールからユーザに暗号資産 B が送付され，ユーザから暗号資産プールに暗号資産 A が送付される．しかし，サイバーインシデント事案では，暗号資産（ERC777 トークン）の脆弱性と Uniswap のリエントランシー脆弱性が悪用された．暗号資産プールからユーザに暗号資産 B が送付され，一方，ERC777 トークンの機能としてユーザから暗号資産プールに暗号資産 A（ERC777 トークン）を送信する前に，ユーザに承認依頼を送信するところ，この承認依頼の機能を悪用して，暗号資産の交換の処理の途中で，暗号資産 A と B の交換を再度呼び出すスマート・コントラクトを作成し，ユーザから暗号資産プールに暗号資産 A が送付される処理が実行されず，また，ほかの脆弱性により上記の処理全体がエラーとならず，繰り返し暗号資産プールからユーザに暗号資産 B が送付されることが行われた．これにより，大量に暗号資産 B が流出した．これは Uniswap バージョン 1 におけるインシデントであったが，コアコントラクトを修正できないため，Uniswap 運営チームは上記の問題を生じさせる特定のトークン（ERC777 トークン）を受け付けない措置を取った．その後新たに実装された Uniswap バージョン 2 ではこの問題に対応済みである．

Uniswap は 2018 年 12 月にソースコードの脆弱性をコード監査会社から指摘されていたが，コアコントラクトを修正することができないため，新しいバージョンを実装する際に対応することとし，即時の対応を行っていなかった．コアコントラクトを修正できないという仕様上の脆弱性とソースコードの脆弱性により生じたサイバーインシデントといえる．

ステーブルコイン

Maker DAO の概要

DeFi を活用したステーブルコインには，Maker DAO（2014 年 12 月に Maker Foundation が Maker プロトコルを創設したが，2021 年 7 月に解散し，運営を Maker DAO に移行）が提供する DAI がある（図 -3）．

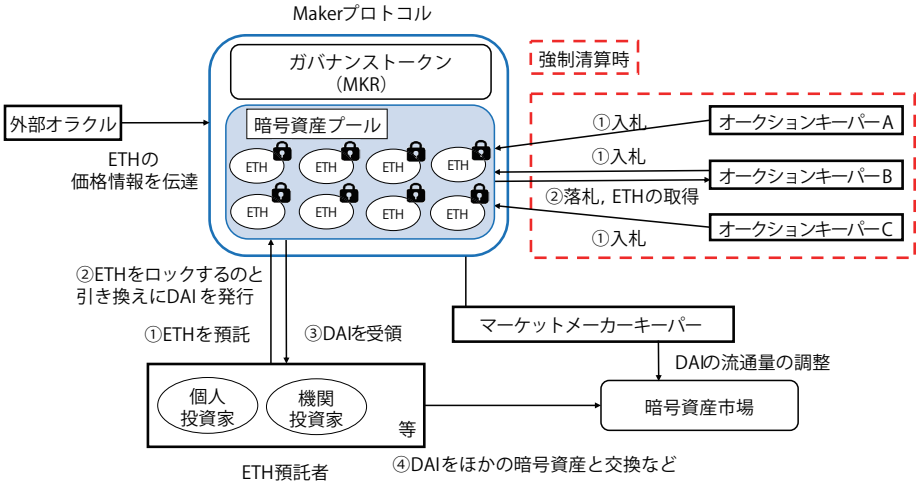
DAI は暗号資産を担保に発行されるステーブルコインであり，1DAI ＝ 1 米ドルを目標価格とする Maker プロトコルにより発行される．具体的には，ユーザが ETH を暗号資産プールに預託するのと引き換えに DAI が発行され，預託された ETH は DAI の価値を担保するための資産となる．ETH を預託した者（以下「ETH 預託者」という）は DAI の発行を受け，暗号資産市場でほかの暗号資産に交換するなどして利用することができる．また，外部のマーケットメーカーキーパーが，暗号資産市場の需給を調整して，1DAI ＝ 1 米ドルとなるよう調整する．具体的には，マーケットメーカーキーパーは，アルゴリズムに従い自動的に，DAI が目標価格（1 米ドル）を上回ったときに DAI を販売して DAI の価格を下げ，目標価格を下回ったときに DAI を購入して DAI の価格を上げることで暗号資産市場における DAI の価格を 1DAI ＝ 1 米ドルになるように調整する．

DAI のように暗号資産を担保とするステーブルコインは，発行するステーブルコインの価値以上の暗号資産を担保（過剰担保）として受け入れることによりその価値が裏付けられている．暗号資産プールに預託された ETH はスマート・コントラクトによりロックされ ETH 預託者が自由に取り出すことができなくなり，取り出すには DAI と手数料を支払う必要がある．ここで手数料の支払いも求めることで，ETH 預託者に，DAI を返還してロックされている ETH を取得するインセンティブが働きづらくなるようにしている．また，最低担保率として約 150％が設定され，ロックされている ETH の価値が下がり発行した DAI の価格の約 150％を下回った場合（たとえば，100DAI（＝ 100 米ドル）を発行しているときは，その発行と引き換えにロックされている ETH の価値が約 150 米ドルを下回った場合）は，強制清算される．この強制清算は，Maker プロトコルのスマート・コントラクトで自動的に開始され，担保としてロックされている ETH は，オークション形式により販売される．オークションキーパーはアルゴリズムに従い自動的に入札を行う外部エージェントとしてこのオークションに入札を行い，落札したオークションキーパーが落札価格に相当する DAI を支払うのと引換えに ETH を取得する．

Maker プロトコルではロックされている ETH の価格は外部オラクルの価格情報を基準に算出される．また，Maker プロコトルの手数料や外部オラクルの選定等はガバナンストークンである Maker（MKR）の保有者による投票等を通じて行われる．

Maker DAO におけるサイバーセキュリティリスクやサイバーインシデント

前項で述べた通り，DeFi プロトコルは外部オラクルから暗号資産の価格情報を取得する必要がある



■図 -3　Maker プロトコルの概要―― Maker DAOWeb サイト，文献 2）をもとに作成

が，このような外部の第三者との関係がサイバーセキュリティリスクを生じさせ得る．

2020 年 3 月，Maker プロトコルの強制清算手続にゼロ入札攻撃が行われ，約 832 万米ドルの損害が生じた．その背景として，COVID-19 により米国の株式市場が下落する局面において，同月 12 日に ETH の価格が約 43% 下落したことで，イーサリアムネットワークでアクセス集中や取引処理手数料（ブロックチェーン上で取引の処理が行われるために必要な手数料．ユーザ等が取引に際し ETH で支払う．取引が集中した場合，一般に手数料の高い取引から順に処理される）の高騰が生じた．その結果，Maker プロトコルに価格情報を提供する外部オラクルが暗号資産市場の ETH の価格をタイムリーに提供することが一時的にできなくなり，その後外部オラクルが ETH の下落後の価格を提供した結果，Maker プロトコルにロックされた ETH の価格が一気に下落して最低担保率を下回り，約 1,200 個のロックされた ETH の強制清算が生じた．ここで，各オークションキーパーは，イーサリアムネットワークのアクセス集中による技術的影響で入札に参加できない，取引処理手数料の高騰によりオークションキーパーの入札取引が制限時間内に処理されずオークションが終了する，オークションキーパーが保有する DAI がなくなり入札するために必要な DAI を暗号資産市場から調達することができず入札に参加できない，といった事情によりオークションキーパーによる入札が正しく行われず，悪意のある攻撃者による入札が行われ，強制清算の対象となる大量の ETH が落札価格ゼロで攻撃者に渡ることとなった（ゼロ入札攻撃という）．なお，ETH のネットワークのアクセス集中は価値のない大量取引により意図的に行われた可能性があることから，攻撃者が意図的に取引処理手数料の高騰を引き起こし，オークションキーパーが正常に作動しない状態を作り上げ，ゼロ入札攻撃を行った可能性が指摘されている．

このインシデントを踏まえると，暗号資産市場は相場の価格変動が大きく，急激な価格変動が生じる可能性があるため，DeFi プロトコルの実行が外部オラクルの提供する価格情報に依拠する場合，攻撃者が暗号資産の急激な価格変動等に乗じて，意図的に取引処理手数料を高騰させて DeFi プロトコルの機能を停止させ，サイバー攻撃をしかけるリスクがあることが分かる．

DeFi の健全な発展に向けた課題

DeFi におけるサイバーセキュリティリスクは，各 DeFi の仕組みにより異なり得るが，本稿で解説した通り，DeFi プロトコルのスマート・コントラクトの仕様上の脆弱性やソースコードの脆弱性，異なるブロックチェーンをつなぐブリッジの脆弱性，DeFi プロトコルが依拠している外部の第三者の脆弱性などが考えられる．

DeFi は新しい可能性を秘めた金融システムではあるが，たとえば DAO により運営されており責任主体が不明確な点や正確な情報が十分に得られないというデータギャップの問題があり，DeFi にかかわるサイバーセキュリティリスクは十分に特定されていない状況である．しかし，今後 DeFi が健全に発展し世に受け入れられるためには，サイバーセキュリティを含めたあらゆるリスクを特定し，規制の対象となる責任主体の明確化を含め，DeFi による便益を享受しつつリスクを軽減するための適切な措置や規制について議論を深めていくことが求められよう．

参考文献
1）FSB : The Financial Stability Risks of Decentralised Finance (2023)
2）（株）クニエ：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（2022 年 6 月）．

（2023 年 7 月 2 日受付）

本稿で示された内容や意見は，筆者個人のものであり，金融庁の公式見解を表すものではない．

■林　敬祐　keisuke.hayashi@fsa.go.jp

金融庁総合政策局フィンテック参事官室課長補佐，東京大学法学部卒業，東京大学法学政治学研究科法曹養成専攻修了．弁護士（日本／ニューヨーク州）．2018 年からアンダーソン・毛利・友常法律事務所勤務，2022 年から現職．特にフィンテック分野に従事し，暗号資産交換業者の監督業務，金融安定理事会による DeFi の金融安定脆弱性の調査業務等に従事．