特集

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―

編集にあたって

石黒正揮 | （株）三菱総合研究所　山崎重一郎 | 近畿大学
佐々木貴之 | 横浜国立大学

暗号資産，デジタル所有権 NFT（非代替性トークン），分散型自立組織（DAO）などブロックチェーン技術をベースとした一群の応用・サービスは Web3.0（または Web3）と呼ばれ，従来のインターネット経済に大きなパラダイム転換をもたらすものとして注目されている．Web3.0 では，ブロックチェーン技術を用いることで，中央集権的な管理組織に依存せずに信頼を構築することが可能となる．また，個人やクリエータに帰属するデータやコンテンツに唯一無二性や所有権を保証することができる．これにより，プラットフォーマの枠を超えてインターネット上で価値の創出と交換が可能となり，新しい時代のデジタル経済社会への転換が期待される．

Web3.0 の特徴として以下のものが挙げられる．

- **非中央集権的トラスト**
  特定の中央管理者なしに信頼を構築可能（**トラストレストラスト**）
- **単一障害点の解消**
  構造のない P2P ネットワークにより特定の個所の障害に対するリスクの解消（**可用性の向上**）
- **取引プロセスの自動化**
  取引・プロセスをプログラムとして自動実行可能にする（**スマートコントラクト**）
- **検証可能性・透明性の確保**
  匿名性を確保しつつ，取引情報に対する検証可能性により高い非改竄性の確保（**完全性の確保**）

このような特徴を活かしたサービスが多数生み出されている．特に，金融，ゲーム，コンテンツ文化などの分野を中心に Web3.0 経済は成長しており，Web3.0 によるイノベーションを通じて，日本の価値をいかに高めていくかが重要となっている．

政府においても，内閣府，経産省，総務省などにより Web3.0 経済の推進に向けて検討が進められている．2022 年 6 月，内閣府の「骨太の方針」においては「Web3.0 の推進に向けた環境整備の検討を

進める」ことが盛り込まれ，自民党 Web3 プロジェクトチームの検討においては「誰もがデジタル資産を利活用する時代へ」として Web3.0 推進に向けた提言を掲げられている．

一方で，国内外において Web3.0 に対する大規模なハッキングや事件が繰り返し発生し，Web3.0 経済の発展の障害となっている．Web3.0 にかかわる脆弱性やリスクとしては以下のようなものが挙げられる．

- **ブロックチェーンにかかわる脆弱性**
  ブロックチェーン技術の構成やアルゴリズムの脆弱性を狙った攻撃である．たとえば，ブロックチェーンの共有台帳の一貫性を担保するコンセンサス・アルゴリズムにおいて，合意形成における計算資源の過半数や，検証者の担保資金の過半数を支配することで，過去の合意済の台帳記録を無効にする 51%攻撃が存在する．
- **システムの実装や運用にかかわる脆弱性**
  Web3.0 システムの実装や運用にかかわる脆弱性リスクが存在する．たとえば，2022 年，分散型金融（DeFi）の多重署名の秘密鍵の窃取により 2,500 万ドルを北朝鮮のハッカーに盗まれる事件や，取引を自動実行させるスマートコントラクトの記述に関する脆弱性などの事故がある．

このような脆弱性やリスクにより，大規模な損害事故や暗号資産の市場価値の下落などが繰り返されてきた．

Web3.0 システムが社会から受容され，市場が拡大していくためには，リスクの構造を明らかにすることで透明性を高め，技術的な課題を克服することが求められる．そのためには，Web3.0 システム固有のリスクと従来の情報システムと共通するリスクに分解し，実用性を確保しつつ，リスクを許容範囲に抑えることの保証や課題の解決が求められる．

Web3.0 経済は，技術，制度，ビジネスなどさまざまな分野の影響を受けるため，本特集では，アカデミア，ガバメント，インダストリに渡る専門家が集まり最新の動向，課題，今後の展望についてまとめることとした．

Web3.0 システムの進化は過渡期にあり，課題も多く，将来の可能性は未知数である．Web3.0 システムによりできること，できないことの境界が明確ではなく，誤って認識されることもあり，Web3.0 システムの発展の障害となっている．本特集を通じて，Web3.0 システムのリスクや課題を明らかにするとともに，Web3.0 システムでできること，できないことを少しでも明確にして，漠然とした懸念を解消するとともに，技術的な課題の解決の方向性や将来展望を示すことができれば幸いである．

（2023 年 7 月 31 日）

概要

1 ブロックチェーン技術がサイバー空間に与える信頼のメカニズムとその再考

基 般

松尾真一郎 | Virginia Polytechnic Institute and State University / Georgetown University

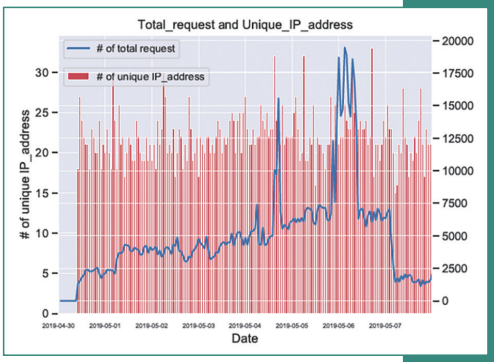
ブロックチェーンに関する研究開発は，Satoshi Nakamoto の未査読の論文から想起される形で，基礎的な研究から幅広い応用の実現までさまざまな形で行われている．一方でその多くは，Satoshi Nakamoto の発明につながる技術史を考えた場合，Satoshi Nakamoto の発明がサイバー空間におけるトラストの実現方法に与えたインパクトを台無しにしているか，それゆえにブロックチェーンそのもののセキュリティを犠牲にする結果になっており，結果として「Why Blockchain（なぜブロックチェーンを使うのか）」という疑問を生じさせている．本稿では，改めて Satoshi Nakamoto の発明が与えたインパクトを振り返り，ブロックチェーンがもたらしているもの，もたらしていないものを振り返った上で，今後のブロックチェーンの研究開発の方向性を述べる．

2 ブロックチェーン・暗号資産に関するサイバーセキュリティの動向と課題―NFT のリスクからコントラクトハニーポットまで―

基 専

面　和成 | 筑波大学

Web3.0 というキーワードが話題になっている中，ブロックチェーンへのサイバー攻撃が年々増加しており，莫大な暗号資産が盗まれるという実被害も発生している．本稿では，ブロックチェーン・暗号資産におけるセキュリティ面を中心に，ブロックチェーンへの攻撃，およびブロックチェーンを悪用した攻撃に関するサイバーセキュリティ・リスクの最新の話題を取り上げ，本分野の最新動向および課題について解説する．

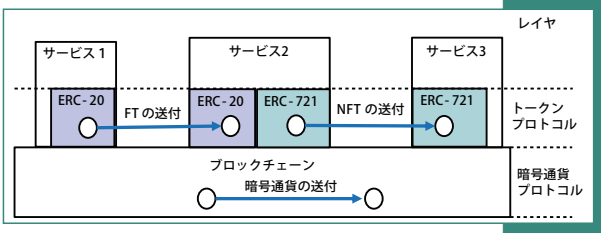


3 分散管理型システムの課題とDAO におけるサイバーセキュリティの取り組み

基 専

山崎重一郎 | 近畿大学

分散管理型システムに対する主な攻撃対象は，暗号技術ではなくコンセンサスである．そしてその攻撃に対する安全性は暗号通貨で計量されるゲーム理論的コストとして評価される．これは DAO への攻撃でも同様である．DAO の運営には，出資金を原資とする金融機機能が必須だが，参加者による DAO のガバナンスに失敗すると保有資産や収益を失う危険性がある．そしてこれも本質はコンセンサスへの攻撃であり，その防御には信頼できるアイデンティティ管理が必要である．



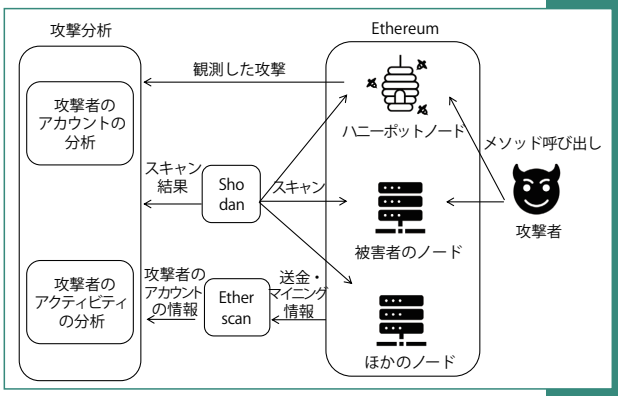
概要

4 Ethereum ノードに対する脅威と攻撃観測

応 専

佐々木貴之　吉岡克成　横浜国立大学

Ethereum のノードに対する脅威と攻撃の観測手法，観測結果を紹介する．Ethereum のノードの API がインターネットに公開されており，かつ，脆弱なパスワードが利用されている場合，さまざまな攻撃を受けることが明らかになった．具体的には，仮想通貨の不正な送金や，マイニングが行われる危険性がある．今後，これらの脅威に対して対策技術を研究，開発していく予定である．

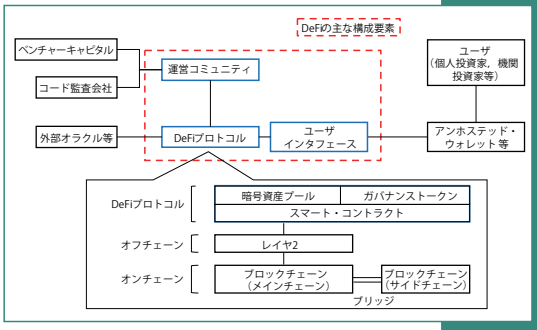


5 金融分野の分散管理型システムのサイバーセキュリティ— DeFi の活用事例とサイバーインシデントの紹介—

応 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として，近年 DeFi（Decentralized Finance）の議論が盛んで，分散型取引所（Decentralized Exchange, DEX），ステーブルコインなど暗号資産等を用いたさまざまな金融サービスを提供するが，確立した定義はない． DeFi は責任主体が曖昧で，既存の金融規制アプローチでは適切な規制を課すことができない可能性がある．本稿では DeFi の概要，活用事例を概説し，サイバーインシデントやセキュリティリスクを紹介する．



6 分散型 ID とサイバーセキュリティ
—進化するデジタルアイデンティティとそのセキュリティ—

応 専

仙頭洋一　小川博久　（株）三菱総合研究所

分散型 ID の検討動向として，自己主権型アイデンティティおよび分散型アイデンティティの概念を示し，近年のデジタルアイデンティティウォレットに至る動向を示す．また，検討が進んでいる欧州におけるデジタルアイデンティティウォレットのセキュリティ検討の概要を示した上で，国内検討に求められる検討内容や整備を報告する．