NFTの安全性について

A survey on the security of NFT

松坂惇平・システム分科会・情報セキュリティ大学院大学

In this paper, we introduces research on the security of NFTs. NFT (Non-Fungible-Token) is a non-fungible token. NFTs make digital content uniquely identifiable, giving it unique value. In 2021, digital art using NFTs was sold for approximately 7.5 billion yen, and NFTs received increased attention. In recent years, NFTs have been used in a variety of ways, not just for digital art. However, there have been reports of concerns about the safety of NFTs, such as the distribution of copies of digital art and fraud using NFTs. Therefore, this paper investigates and summarizes solutions to these problems and NFT security issues, as well as various ways to use NFTs, not just digital art.

1はじめに

●NFTはブロックチェーン技術を用いて，デジタルコンテンツを一意識別可能にした.デジタルコンテンツに唯一無二の価値を保証し，デジタルコンテンツに新たな価値を与えている.

●NFTは様々な利用方法が現れ，デジタルコンテンツの販売，学歴証明書などに活用されている.

●詐欺も増えている

●NFTは2014年にKevin McCoy(ケビン マッコイ)と Anil Dash (アニル ダーシ)がデジタルアートに対して所有権を主張する方法を模索したところから始まった※1

● NFTの安全性に対してどのような研究があるのかまとめていく.

2NFTの仕組み

デジタル画像をNFTと紐づけるには，ブロックチェーン上で，

トークンID，メタデータのURI，Owner Addressなどが保存され外部サーバーの中にメタデータとしてデジタル画像のタイトルや概要，デジタル画像の保存先のURLなどが保存されている.

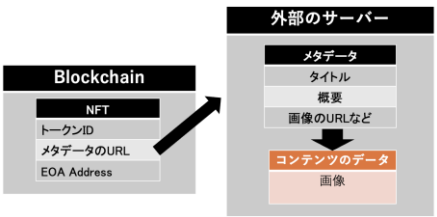

図2.1 デジタルコンテンツの保存先.
([3]をもとに作成)

3NFTの売上件数

●「OpenSea monthly NFTs sold」[4]によると，OpenSeaのNFTの月間売上件数は2022年1月に500万件を超え，それ以降は右肩下がりに売上件数は減少している.

●「CoinGecko仮想通貨レポート」[5]では，NFTを取り扱うマーケットプレイスのNFTの取引量は，2022年が263億ドルとなっており最高取引量を示している.

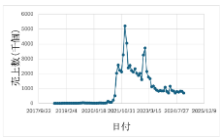

図3.1.1 OpenSeaの月間売上数
([4]をもとに作成)

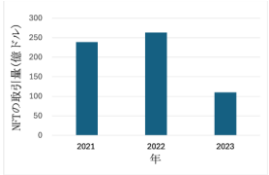

図3.1.2 NFTマーケットプレイスの上位10の取引量
(※2022は上位8)
([5]をもとに作成)

4 攻撃例

4.1イミテーション攻撃

DoS攻撃やプライバシーを侵害する攻撃，暗号資産を除くデジタルアート作品の贋作をマーケットにアップロードして不正に利益を得る攻撃を木村ら[21]は，イミテーション攻撃と呼んでいる.

NFTに対するイミテーション攻撃の課題や疑念点

木村らによると，

「NFTの取引によってアート作品を管理する際に生じる『アートそのものの真正性をNFTで証明出来ない』」[21]ことだと述べている.

木村らはイミテーション攻撃を2つに分類している

①悪意のある攻撃者がデジタルアート作品の贋作を用いて利益を得ようとする**フェイク攻撃**

②悪意のあるアート作者がデジタルアート作品を多重に流通して,1つのアート作品に対して多重に利益を得る**二重流通攻撃**

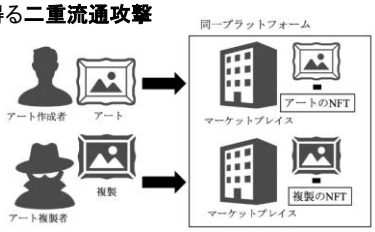

図5.2.1同一プラットフォーム上でのフェイク攻撃
([21]の図7をもとに作成)

4.2 Sleep mint

攻撃者がスマートコントラクトのバックドアを悪用し，有名人からNFTを購入したふりをし，その後，他の人に高値で販売する行為.

①攻撃者はあらかじめ所有者の承認なしに攻撃者に転送できるようするバックドアがあるスマートコントラクトでNFTと紐づいたコンテンツを有名人に発行する. 有名人は気づかず受け取る.

②バックドア経由でその有名人からNFTコンテンツを送り返す.

③有名人からNFTと紐づいたコンテンツを購入したと主張し高値で販売をする.

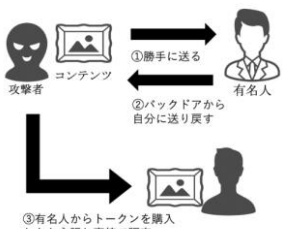

図5.8.3 Sleep mintの方法
([28]5.4 Copyright Theftをもとに作成)

5 考察とまとめ

今回は様々なNFTの安全性の研究について紹介してきた

●フェイク攻撃，二重流通攻撃，コンテンツのコピーや複製の問題ではマーケットプレイスとその周辺の機関による対策が必要となる.

●EditableMetadata脆弱性，Sleepmintは，スマートコントラクトのNFTをMINTするプログラム上での脆弱性であるため，スマートコントラクト側の対策やユーザーがNFTをMINTするときに信頼できるスマートコントラクトを利用するなど注意が必要である.

●フィッシング攻撃では，ユーザー側の対策が必要であり，信頼できるマーケットプレイスのみで取引をすることが望ましい.

●NFTの安全性を調査していくと，スマートコントラクトとNFTは強い関係がありスマートコントラクトが脆弱であるとNFTも危険にさらされる.

●本調査が終わるまではコンテンツそのものの偽造への対策が難しいと考えていたが，本調査を行っていくにつれ監査機関、鑑定機関などが設置されることでコンテンツ偽造問題が減っていくのではないかと考える.

●NFTは新しい技術であるからこそ，脆弱性も見つかってしまうが，少しずつ改善されNFTが様々なものに利用されることを期待している.

[4] Dune Analytics, “OpenSea monthly NFTs sold”, 最終閲覧 2024/12/22, https://dune.com/queries/47101/92814
[5] CoinGecko,” 仮想通貨レポート” 最終閲覧 2024/12/22, https://www.coingecko.com/ja/publications/reports

[3]ソーシャルレンディング，”NFT 取引の仕組みを 技術的に理解する”，更新日 2022/12/9，最終閲覧 2024/4/18 https://tech.nri-net.com/entry/how_NFT_work[20]大城侑也,池辺慶,櫻井幸一，”非代替性トークンが持つ一意識別性の問題点とそれに対する考察”，SCIS，2023を元に作成[21]木村圭吾,今村光良,面和成，”NFT の信頼性にあるセキュリティリスクの考察”，ISEC，2021-30をもとに作成[21]木村圭吾,今村光良,面和成，”NFT の信頼性にあるセキュリティリスクの考察”，ISEC，2021-30をもとに作成 [22]木村圭吾,今村光良,面和成，”NFT 流通における 深層学習を用いた分散型真正性検証プロトコルの提案”，SCIS，2022 をもとに作成 [28] Ma, K., Huang, J., He, N., Wang, Z., & Wang, H. (2023).” SoK: On the Security of Non-Fungible Tokens.” *arXiv preprint arXiv:2312.08000*をもとに作成