SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

NFT 流通市場に対する Editable Metadata 脆弱性の一考察
A Study on Editable Metadata Vulnerabilities on NFT Marketplaces

清水 嶺 * 矢内 直人 * 今村 光良 † クルーズ ジェイソン ポール *
Rei Shimizu Naoto Yanai Mitsuyoshi Imamura Jason Paul Cruz
岡村 真吾 *
Shingo Okamura

キーワード 非代替性トークン, メタデータ, Ethereum, メタデータ差し替え攻撃

あらまし

ブロックチェーンを通じた分散アプリケーションとしてゲームやアートを売買するサービスが台頭する昨今, それらサービスの中核技術として注目を集めている技術が非代替性トークン (Non Fungible Token, NFT と呼称) である. NFT はトークンにメタデータと呼ばれる付加情報を与えることにより, トークンの唯一性とメタデータの真贋性を保証できる点で, 従来のブロックチェーンにおけるトークン技術と比較して画期的な技術といえる. 一方, NFT におけるメタデータの存在は, 攻撃者にとっては新たな攻撃の切り口ともなりうる. メタデータのような容量の大きいデータは, ブロックチェーンの情報量の制限から一般にはオフチェーンと呼ばれるブロックチェーン外のファイルサーバなどに保存されている. このトークンとメタデータの結びつきは, ブロックチェーン上で管理されているデータと比較すると非常に弱い. NFT は暗号技術やセキュリティ技術に明るくないユーザの利用も予想されることから, NFT とメタデータの関係性において新たな攻撃を考察することは, 脅威を事前に防ぐという観点で非常に重要といえる.

NFT の脅威として, 現在はメタデータ差し替え攻撃が注目されている. ここでいうメタデータ差し替え攻撃とは, 現状の対策には IPFS (InterPlanetary FIle System) [1] がある. 本稿の主たる問いは, IPFS が利用されている状況においても, 悪性なコントラクトの生成を通じてメタデータ差し替え攻撃ができるか明らかにすることである. 現状の社会の認識では, NFT とメタデータのリンクは弱いものの, IPFS などの分散ファイルサーバを用いることによって, メタデータの差し替え攻撃は防げるというものが一般的である. しかしながら, IPFS によるメタデータとトークンへの紐づけを保証するような結果は, 著者が知る限り, これまでに示されてこなかった.

上述した問いに対し, 本稿は IPFS が利用されている状況においても, 悪性なコントラクトの生成を通じてメタデータ差し替え攻撃ができることを示す. 大まかには, NFT とメタデータの関係性の脆弱性をついた攻撃 [2] に着目し, 悪性なコントラクトを生成する攻撃者を仮定することで, メタデータへの URL を差し替えることができる. また, その攻撃に対して実際にマーケットが対策できているかについても, Das らの研究結果 [2] を通じて確認した. その結果, 既存のマーケットプレイスでは, コントラクトサイドからのメタデータの差し替え攻撃に対する防御手法が不完全であることを確認した.

参考文献

[1] https://ipfs.io

[2] DAS, Dipanjan, et al. Understanding Security Issues in the NFT Ecosystem. arXiv preprint arXiv:2111.08893, 2021.

* 大阪大学大学院情報科学研究科, 大阪府吹田市山田丘 1-5, Graduate School of Information Science and Technology Osaka University, 1-5 Yamadaoka, Suita, Osaka, Japan
† 野村アセットマネジメント, 住所, Nomura Asset Management, Address,