2021 年 10 月 8 日

# 2021 年 9 月 3 日に発生した NFT 流出に関するご報告書

SBINFT 株式会社
代表取締役　高　長徳

平素より NFT マーケットプレイス『nanakusa』をご利用いただき、ありがとうございます。

先般、『nanakusa』にて 9 月 3 日(金)に、ご利用者のウォレットアドレスにて所有する一部 NFT が、外部に流出する事案が発生したことにより、サイト全体の見直しを行うことを目的に、メンテナンスモードとさせていただいておりました。

その後、『nanakusa』は、2021 年 9 月 19 日（日）18 時にサービスを再開しております。ご利用の皆様、ご関係者の皆様、ご理解いただき誠にありがとうございました。

グローバルでの NFT ビジネスに与える影響を鑑み、情報の透明性を図ることが弊社の社会的使命と認識し、今回の事案について可能な限り情報公開いたします。

1) 流出の経緯
2) 当社の対応の経緯
3) NFT 流出原因
4) 不正アクセス対策について
5) 今後の対応
につきまして、改めてご説明致します。

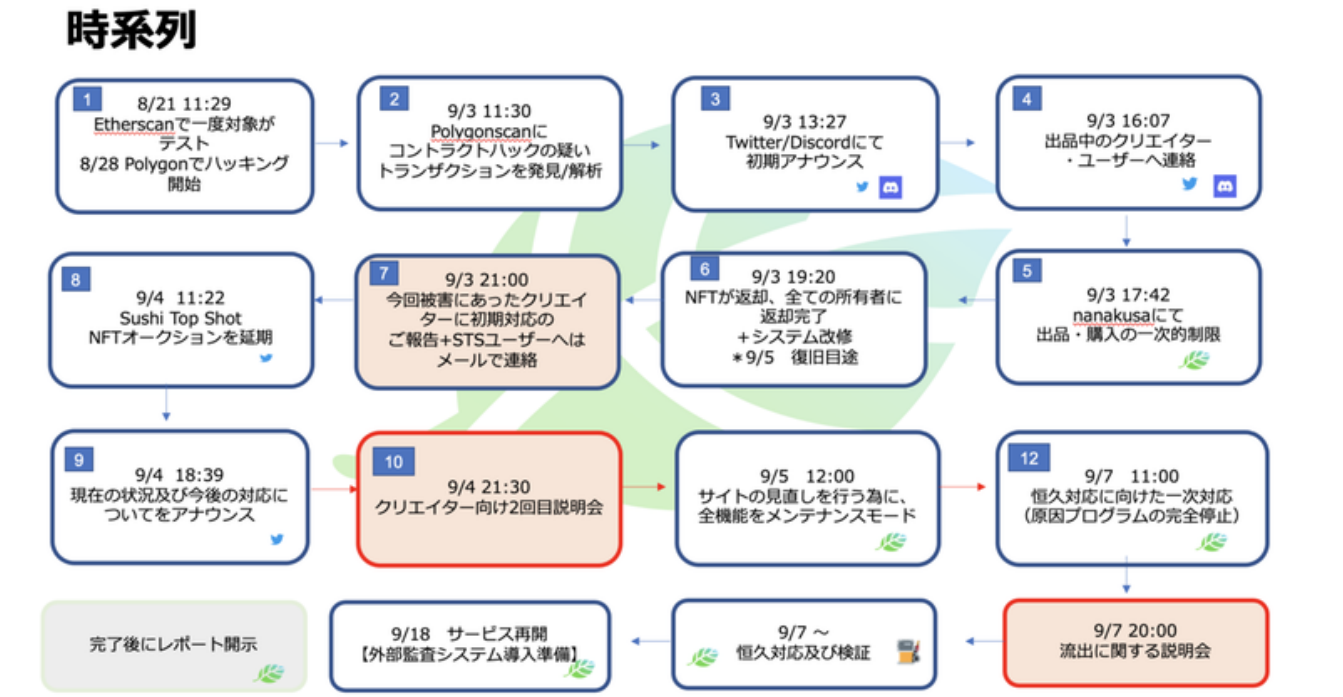
## 1) 流出の経緯

※全て UTC(協定世界時)時間になります。
●8 月 21 日（土）11 時 29 分：ETH ネットワークで不正な NFT 流出の試み及び、2 件不正に NFT 流出
●8 月 28 日（土）4 時 56 分より：Polygon ネットワークにて 6 件不正に NFT 流出
●8 月 29 日（日）12 時 26 分より：Polygon ネットワークにて 5 件不正に NFT 流出
●8 月 30 日（月）12 時 14 分より：Polygon ネットワークにて 6 件不正に NFT 流出
●8 月 31 日（火）11 時 44 分より：Polygon ネットワークにて 1 件不正に NFT 流出
●9 月 1 日（水）11 時 56 分より：Polygon ネットワークにて 8 件不正に NFT 流出

●9 月 2 日(木)11 時 06 分より:Polygon ネットワークにて 8 件不正に NFT 流出
●9 月 3 日(金)19 時 20 分頃:流出した NFT 全ての返却を確認

上記が流出の経緯となります。
結果的に、流出件数は以下の通りです。
流出した NFT 総数:36 件(ETH 2 件 / Polygon 34 件)
流出した NFT のウォレットアドレス数:17 件

## 2) 当社の対応の経緯




今回の対応の時系列をお伝え致します。

●9 月 3 日(金) 11 時 30 分:Polygonscan にコントラクトハックの疑い/トランザクションを発見/解析
●9 月 3 日(金)13 時 27 分:Twitter/Discord にて初期アナウンス
●9 月 3 日(金)16 時 7 分:出品中のクリエイター・ユーザーへ連絡
●9 月 3 日(金) 17 時 42 分:『nanakusa』にて出品・購入の一次的制限
――一時的に、コントラクトの hash に必要なパラメータを変更
●9 月 3 日(金)19 時 20 分:NFT が返却、全ての所有者に返却完了及びシステム改修 ＊この時点では 9 月 5 日(日)復旧目途としておりました

●9 月 3 日（金） 21 時 00 分：今回被害に遭われたクリエイターに初期対応のご報告及び Sushi Top Shot ユーザーへはメールで連絡
●9 月 4 日（土）11 時 22 分：Sushi Top Shot NFT オークションを延期
●9 月 4 日（土）18 時 39 分：現在の状況及び今後の対応についてアナウンス
●9 月 4 日（土） 21 時 30 分：クリエイター向け 2 回目説明会
●9 月 5 日（日）12 時 00 分：サイト見直しのため全機能をメンテナンスモード
●9 月 7 日（火）11 時 00 分：恒久対応(コントラクトの改修)に向け一次対応（原因プログラムの完全停止）
―Dapps の遮断(timestamp の実効許容時間を 0 に)
ーコントラクトオーナー権限の変更
―コントラクトの改修により、ユーザーにお願いする予定だった setApproveforAll のキャンセル対応が不要に
●9 月 7 日（火） 20 時 00 分：流出に関する説明会（ウェビナー）
●9 月 7 日（火）～ 9 月 18 日（土）：恒久対応及び検証
●9 月 19 日（日） 18 時 00 分：サービス再開
●9 月 20 日（月）：NFT 流出対象者へ再出品用の GAS 代及び、お詫び NFT を送付

上記の経緯にて対応を行いました。

## 3) NFT 流出の原因

NFT の購入処理を実行する権限を生成するプログラムに不正アクセスがなされたため、実行権限が不正に奪取されたことが直接的な原因となります。

結果として、販売価格を無視した価格で購入を実行したことで、無償同然で NFT の所有権が移動されました。

根本的な原因としては、実行権限取得の暗号化アルゴリズムの複雑性が不足していたため暗号化アルゴリズムに不正アクセスがなされ、一部の実行権限が奪われたことが判明しています。

暗号化の複雑性不足によって、これまで NFT マーケットプレイス上でユーザーが取引を行うにあたって著しく問題となる事態は発生しておりませんでしたが、当社としては、『nanakusa』における NFT の取引流通量の増加やユーザー数の増加などを考慮して、システムを見直し、暗号化の複雑性を向上させるなどセキュリティレベルをより高い水準にすることを検討していたところ、今回のような不正アクセスの攻撃を受ける事態になりました。

当社においてご利用者の皆様が安全に NFT の取引を行うにあたって、当社のセキュリティリスクに対する認識が十分であったとまでは言い切れず、セキュリティ評価が十分になされていなかったことに対して、深く反省しております。

今後は、セキュリティリスクに対して、常に評価可能な体制を構築し、リスクに対する組織としての意識を高めるよう、努めて参ります。

## 4）不正アクセス対策について

現状の不具合を解消するため、以下の対応を行いました。
●秘密鍵の暗号化アルゴリズム強化
●ACL 強化による、実行権限の制限
●暗号強度そのものの複雑化

以上の対応により、想定しうるリスクは回避されたことと考え、9 月 19 日にサービスを再開いたしました。

## 5）今後の対応

●トランザクション監視システムの導入
トランザクション監視につきましては、『nanakusa』にて監視体制を構築しております。
そして、トランザクション監視につきましては、過不足の評価を社内で行い、順次必要なソリューションを実装いたします。

今後、このような事態が二度と起こらないよう対策を施して参ります。
引き続き、『nanakusa』をご愛顧頂けますよう、よろしくお願い申し上げます。

敬具