

# IPFS におけるシビル攻撃のオンデマンド検知

姫野 貴一<sup>†</sup> 上山 憲昭<sup>†</sup>

<sup>†</sup> 立命館大学情報理工学部

〒567-8570 大阪府茨木市岩倉町 2- 150

E-mail: †is0687hh@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし 現在の Web は、情報へのアクセスにロケーション指向型の仕組みを用いている。この方式は情報を提供するサーバの管理者に大きな責任と権限が集中し、管理者の判断で情報を削除・改ざん・検閲が可能である。結果としてインターネット上の情報が一部の巨大プラットフォームに支配される状況を招いている。こうした集中管理の課題を根本から見直すために登場したのが、IPFS (InterPlanetary File System) である。IPFS は P2P ネットワーク上で動作し、各ノードが自律的に情報を保持・共有する分散型の仕組みを採用している。これにより、中央集権運営に依存せずに情報を管理できるため、検閲や改ざんに強く、障害への耐性も高いという特徴がある。しかしながら、現行の IPFS プロトコルは Sybil 攻撃に対して脆弱である。Sybil 攻撃とは、偽のノードを大量に生成してネットワークを攪乱する攻撃である。このような攻撃が発生すると、攻撃ノードによって正当なノードへのルーティングが妨げられ、実質的な検閲が可能になる。そのため、本研究は IPFS における Sybil 攻撃を要求に応じてオンデマンドに検知する手法の確立を目指し、攻撃の特定手法を検討する。提案方式は、ユーザのコンテンツ取得要求をトリガとして周辺ピアの計測を起動し、応答したノードの Peer ID 分布を XOR 距離空間で解析する。正常時には CID 近傍の PID はおおむね均等に散らばる一方、Sybil 攻撃下では偏りや分布のエントロピー低下が生じる。この差異に基づき、基準分布からの乖離度を指標として異常を判定する。さらに、オンデマンド検知の性質上、コンテンツ人気度により検知率・検知コストが変動するため、その影響を評価し、効率のかつ有効な Sybil 攻撃の検知法を提案する。謝辞 本研究は JSPS 科研費 (JP25K03113, JP23K28078) の助成を受けたものである。ここに記して謝意を表す。

キーワード IPFS, シビル攻撃, KL ダイバージェンス, オンデマンド検知

## On-Demand Sybil Attack Detection in IPFS

Takakazu HIMENO<sup>†</sup> and Noriaki KAMIYAMA<sup>†</sup>

<sup>†</sup> College of Information Science and Engineering, Ritsumeikan University

2- 150, Iwakura-cho, Ibaraki, Osaka 567-8570, japan

E-mail: †is0687hh@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

**Abstract** The current Web uses a location-based mechanism for accessing information. This method concentrates a great deal of responsibility and authority in the hands of the administrators of the servers that provide the information, allowing them to delete, alter, or censor information at their discretion. As a result, information on the Internet is dominated by a few large platforms. The InterPlanetary File System (IPFS) was developed to fundamentally address these issues of centralized management. IPFS operates on a P2P network and employs a decentralized mechanism in which each node autonomously stores and shares information. This allows information to be managed without relying on centralized operation, making it resistant to censorship and tampering and highly tolerant to failures. However, the current IPFS protocol is vulnerable to Sybil attacks. A Sybil attack disrupts the network by generating a large number of fake nodes. When such an attack occurs, the attacking nodes prevent routing to legitimate nodes, effectively enabling censorship. Therefore, this research aims to establish an on-demand method for detecting Sybil attacks in IPFS and to examine techniques for identifying attacker hosts. The proposed method initiates measurements of nearby peers when a user requests content, and analyzes the Peer ID distribution of the responding nodes in an XOR metric space. Under normal conditions, PIDs near a CID are roughly evenly distributed, whereas under a Sybil attack, bias and a decrease in distributional entropy appear. Based on this difference, deviation from the reference distribution is used as an indicator to detect anomalies. Furthermore, due to the nature of on-demand detection, the detection rate and cost vary depending on the popularity of the content. We evaluate these effects and propose an efficient and effective method for detecting Sybil attacks.

**Key words** IPFS, Sybil attack, KL divergence, on-demand detection