社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

IPFS における Sybil 攻撃のオンデマンド検知

姫野　貴一†　　上山　憲昭†

† 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，本稿は 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，効率的かつ有効な Sybil 攻撃の検知法を提案する．
キーワード　IPFS，Sybil 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† and Noriaki KAMIYAMA†

† 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

1. はじめに

現在の Web における情報取得は，サーバの所在地を指し示すロケーション指向型の仕組みに基づいている．利用者は URL を通じて特定のサーバへアクセスし，そこに保存された情報を取得する形態が一般的である．しかしこの方式では，情報の保存場所と管理主体が結び付いているため，管理権限がサーバ運営者に集中する．その結果，運営者の判断によって情報の削除や改変，公開範囲の制限が可能となり，検閲や恣意的な情報統制も実施できる．近年では，大規模プラットフォームが情報流通の中心を担い，情報公開の可否が一部主体に依存する状況も生じている．このような集中管理構造は，利便性の一方で情報の永続性や透明性を十分に保証できないという課題を持つ．こうした背景から，中央管理者に依存しない分散型情報基盤として IPFS が提案されている．IPFS は P2P ネットワーク上で各ノードがデータを分散保持するファイル共有システムである．データは内容に基づく識別子である Content ID により管理され，同一内容には同じ識別子が与えられるため，改ざん検出や重複排除が容易になる．この設計により， IPFS は物理的な保存場所に依存しない内容指向型取得を実現する．また複数ノードによる保持により，可用性や耐障害性の向上が期待できる．この特性から，IPFS は Web3 の基盤技術として注目されている．一方で，IPFS の探索は Kademlia に基づく DHT によって実現されるが，この仕組みには限界もある．特に自由参加型ネットワークでは悪意あるノードの混入を防ぎにくく，問題となるのが Sybil 攻撃である．Sybil 攻撃では，攻撃者が多数の偽ノードを生成し，見かけ上の存在数を増やして影響力を拡大する．攻撃ノードが ID 空間の特定領域を占有すると，探索経路を意図的に操作できる．その結果，正当ノードへ到達する前に攻撃ノードへ誘導され，応答を循環させることで探索が妨害される．利用者は本来取得可能なコンテンツに到達できず，事実上のアクセス遮断が生じる．これは分散型でありながら情報遮断を許すことを意味し，IPFS の理念と矛盾する．したがって Sybil 攻撃対策は不可欠である．これまでにも対策は提案されているが，多くは定期監視や全体統計に依存し，負荷が大きく大規模環境での適用が難しい．特に IPFS のような動的 P2P 環境では常時監視は現実的でない．そこで本稿では，必要時のみ検査するオンデマンド型検知に着目する．取得要求を契機に近傍ピア応答を収集し，Peer ID 分布を XOR 距離空間で解析する．通常は均等分布となるが，攻撃下では集中やエントロピー低下が生じるため，基準分布からの乖離で異常を検知する．さらにアクセス頻度の偏りを利用し，人気コンテンツを優先観測することで，少ない検査回数で高い検知効果を目指す．本稿の目的は，分散モデルを維持しつつ軽量で実用的な Sybil 検知機構を実現することである．提案方式により実質的な検閲を抑制し，IPFS の分散性と検閲耐性を維持した運用モデルの確立を目指す．

2. 関連研究

2.1 push 時の対策

Victor Henrique de Moura Netto らの研究では，コンテンツの push 時（PROVIDE 時）における ProviderRecord(PR) の保存先を制御することで，Sybil ノードへの記録集中を回避する手法が提案されている [1]．従来の IPFS では，CID に最も近い PID をもつピアから順に PR を保存するため，攻撃者が特定 CID 周辺の ID 空間を占有した場合，PR が攻撃ノードに集中しやすいという問題があった．この偏りを緩和するためにランダム性を導入した SR-DHT-STORE（SDS）方式を採用し，PR の保存先を確率的に分散させる．これにより，攻撃者が ID 空間の一部を囲い込んでいても，PR が単一領域に集中することを防ぎ，取得経路の多様性を確保できる．さらに，この方式は既存の DHT ルーティング機構を大きく変更せずに導入可能であり，実装上の互換性を保ちながら耐攻撃性を向上できる点に特徴がある．その結果，攻撃によってコンテンツ取得が阻害される確率を低減し，可用性の維持に寄与することが示されている．

2.2 定期検知型の Sybil 攻撃対策

Ethereum の P2P ネットワークを対象とした研究として，Eisenbarth らは，監視ノードによる周期的なネットワーククロールを通じて，ノード ID 分布や接続関係の偏りを測定する手法を提案している [2]．この手法では，ネットワーク状態を継続的に観測し，通常時と異なる構造的特徴を検出することで Sybil 攻撃の存在を推定する．特に，特定領域にノードが集中する傾向や，接続トポロジの異常な密度変化を指標とすることで，ルーティングを妨害するタイプの Sybil 攻撃に対して有効であるとされる．ただし，広域クロールを継続する必要があるため，観測コストや監視ノードへの負荷が増大するという課題も指摘されている．さらに，Ioannidis らや Grover らは，一定期間ごとの観測ウィンドウにおいてノード ID 分布を収集し，Gini 指数を用いて分布の不均衡度を評価する方式を提案している [3]．Gini 指数は不平等度を測る統計指標であり，ID 分布の偏りが大きい場合に Sybil 攻撃の可能性が高いと判断する．この定期検知型アプローチは，分布変化を時系列的に追跡できる点で有効であるが，攻撃発生から検知までに時間遅れが生じる可能性があり，リアルタイム性の面で制約がある．

2.3 計算パズルによる Sybil 攻撃対策

Li らは，DHT における Sybil 攻撃耐性を高めるため，各ノードに対して定期的に計算パズルの解答を要求する SybilControl を提案している [4]．この方式では，ノードが継続的に計算問題を解くことで，計算資源を有する正当ノードであることを証明する．攻撃者が多数の偽ノードを維持しようとすると，それぞれに対して計算資源を割く必要があるため，攻撃コストが大幅に増加する．これにより，大規模な Sybil ノード生成を経済的・計算的に困難にする効果がある．さらに，ノード間で解答の検証を行うことで，相互に正当性を確認し合う仕組みが構築され，ネットワーク全体の整合性維持に寄与する．一方で，計算負荷が増加するため，低性能ノードが参加しにくくなるという側面もあり，適用範囲の検討が必要とされている．

3. 提案手法

3.1 提案方式の概要

従来研究では，IPFS における Sybil 攻撃は，CID 周辺に Sybil ノードを大量に配置することで，正常ノードに PR の配布を妨害する攻撃や、攻撃者が任意で破棄を行う攻撃が想定されていた．これに対して本稿では，CID 周辺に Sybil ノードを配置することで，要求が Sybil ノードに到達した際に，Sybil ノード同士が要求を相互に転送し続け，正当なノードへ到達できなくするタイプの攻撃に着目する．このような攻撃に対して，Peer ID の分布の偏りに着目し，KL ダイバージェンスなどの統計的手法を用いた異常検知を提案する．また，すべてのコンテンツを常に監視するのではなく，ユーザからの要求をトリガとして検知を行うオンデマンド型の攻撃検知方式とすることで，アクセス頻度の低いコンテンツに対しても，無駄な検知コストを抑えつつ有効な対策を実現する．提案方式および比較対象方式では，要求対象 CID 周辺に存在する Peer ID の分布を観測し，その分布の偏りを用いて Sybil 攻撃の有無を判定する．こ

の分布の差異を定量的に評価する指標として KL ダイバージェンスを用いる．KL ダイバージェンスは，観測分布と基準分布の乖離度を表す指標であり，観測分布 P と基準分布 Q の間の乖離度を $D_{\mathrm{KL}}(P \parallel Q)$ として定義する．この $D_{\mathrm{KL}}(P \parallel Q)$ を以下の式 (3.1) で与える．

$$D_{\mathrm{KL}}(P \parallel Q) = \sum_{i=1}^{n} p_i \log_2 \frac{p_i}{q_i} \tag{3.1}$$

ここで，$P = \{p_i\}$ は観測された Peer ID 分布を表し，$Q = \{q_i\}$ は基準分布を表す．基準分布 Q は，シミュレーション開始時における正当なピアのみが存在する状態での PID 分布とする．n は XOR 距離空間を一定幅で分割した区間の総数を表し，各区間に対応する Peer ID の出現頻度を用いて分布を構成する．KL ダイバージェンスの値が大きいほど，観測分布が基準分布から大きく乖離していることを意味し，CID 周辺における Peer ID の集中が強い，すなわち Sybil 攻撃が発生している可能性が高いと判断される．

3.2 提案方式の動作

本稿で提案する方式では，コンテンツ取得要求が PR を保持するピアに到達した時点で，当該要求を受信した PR 保持ピアが検知および対処処理を実行する．本方式は，ネットワーク全体を対象とした周期的な監視を行わず，実際に要求が発生した場面に限定して処理を行う点に特徴がある．PR を保持するピアは，要求されたコンテンツの CID を基準として，その周辺に位置する Peer ID（PID）を収集する．収集された PID を用いて分布を構成し，あらかじめ設定された基準分布との乖離度を評価することで，当該要求に関連する領域における異常の有無を判定する．乖離度の評価には KL ダイバージェンスを用い，その値が所定の閾値を超えた場合に，当該コンテンツに対して異常が発生していると判断する．この判定は，要求を受信した PR を保持しているピア単独で行われ，他のピアとの協調や全体的な同期処理を必要としない．異常が検知された場合には，要求を受信した PR 保持ピアが PR の再配布処理を実行する．再配布先の選択において，正当な PID を事前に識別することは行わず，SR-DHT-STORE(SDS) に基づく方式を用いる．SDS は，PR を CID に最も近い単一のピアに集中して保存するのではなく，CID との XOR 距離に基づいて段階的に異なる距離帯に位置する複数のピアへ分散して保存することで，可用性と耐攻撃性を向上させることを目的とした手法である．本稿では，この SDS の考え方を PR の再配布に適用する．再配布にあたっては，再配布先の正当性を事前に識別することは行わず，距離に基づく分散配置を用いることで，攻撃下においてもコンテンツ取得が継続可能な状態を回復する．また，再配布数には上限を設けることで，過剰な PR 配布によるネットワーク負荷の増大を防止する．一方で，異常が検知されなかった場合には，追加の処理は行わず，通常の IPFS におけるコンテンツ取得処理を継続する．このように，要求が到達した PR 保持ピアのみが検知および再配布を担う構成とすることで，不要な検知処理や過剰な PR 再配布を抑制しつつ，攻撃発生時には迅速な対処が可能である．本方式における具体的な処理手順を，Algorithm 1 に示す．

Algorithm 1: オンデマンド検知および SDS を考慮した Provider Record 探索とコンテンツ取得処理

Input: CID（取得したいコンテンツの識別子）
Output: コンテンツデータ

1: 自身のルーティングテーブルを確認し，対象 CID の Provider Record（PR）を保持していれば，PR に記載された Provider へ GET を送り，コンテンツを取得して終了
2: PR が存在しない場合，CID と XOR 距離が近い上位 k 個のピアを候補リストとする
3: **while 候補リストが空でない do**
    4: 候補リスト内のピアに対して並列に「対象 CID の PR を保持しているか」を問い合わせる
    5: 問い合わせを受けた各ピアは次のいずれかで応答する
        - PR を保持している場合：PR を返す．併せて，当該 CID 周辺の Peer ID 分布を観測し，分布に偏りが認められる場合は SDS に基づき PR を追加配布する
        - PR を保持していない場合：ルーティングテーブル内に CID により近いピアがあれば，そのピア情報を返す
        - それ以外の場合：何も返さない
    6: すべての応答を収集する
    7: **if** *PR* **を返したピアが存在する then**
        8: PR に記載された Provider へ GET を送り，コンテンツを取得して終了
    9: PR が得られなかった場合，応答に含まれる「CID により近いピア集合（closer peers）」のみを集め，候補リストを更新する
    10: **if** *closer peers* **に基づく探索を繰り返しても** *PR* **が得られない then**
        11: 探索範囲を CID 近傍に限定せず，SDS で PR が配置される可能性のある広い ID 領域（遠方を含む領域）から新たに候補リストを構成する
12: コンテンツが取得できなかった場合は失敗として終了

4. 性能評価

4.1 評価条件

提案方式の有効性を検証するために，本稿では IPFS を模擬した計算機シミュレーションによる数値評価を実施する．評価では，Sybil 攻撃が発生する環境下において，攻撃検知の性能およびコンテンツ取得への影響を定量的に比較する．ネットワークは一定数のピアから構成され，各ピアは一意な Peer ID(PID) を持つものとする．ピアは起動および停止を繰り返すものとし，ノードの離脱および再参加が発生する動的なネットワーク環境を想定する．コンテンツは CID によって識別され，各 CID に対して PR が存在する．PR は CID に XOR 距離が近い複数のピアに分散して保存されるものとし，IPFS の仕様に従った配置を行う．コンテンツ取得要求は一定の時間間隔で発生し，各要求は 1 つの CID を対象とする．要求が発生すると IPFS のルーティング処理が開始され，IPFS のルーティング処理は短時間で完了するため，本稿では，コンテンツ探索は要求発生時点で起動しているピアおよびそれらが保持するルーティングテーブルの情報に基づいて行われるものとする．また，本来 IPFS ではルーティングテーブルや PR の管理はノードの参加状況を反映して更新されるが，本評価ではその詳細な更新挙動は考慮せず，簡略化したモデルとして扱う．Sybil 攻撃は，攻撃者が複数の攻撃ノードを生成し，特定の CID に対して XOR 距離が近い ID 空間に集中配置することで発生させる．この結果，コンテンツ取得要求が攻撃ノードへ優先的に到達し，正当な Provider ノードへ到達できなくなる状況を再現する．数値評価では，P2P ネットワークにおける Sybil 攻撃対策として広く知られている KL ダイバージェンスに基づく定期検知方式 (periodic) と，本稿で提案するオンデマンド検知方式 (on-demand) の 2 つを比較対象とする．定期検知方式は，一

定の時間間隔ごとにネットワーク状態を観測し，Sybil 攻撃の有無を判定する方式である．一方，オンデマンド検知方式は，ユーザによるコンテンツ取得要求を契機として検知処理を実行する方式である．両方式について，検知性能，検知コスト，および攻撃下におけるコンテンツ取得性能の観点から評価を実施する．数値評価で用いたシミュレーションのパラメタ設定値を表 1 に示す．

表 1　評価に用いたパラメタ設定値

記号	定義	値
N_{node}	ノード数（正当ノード）	10,000
N_{Sybil}	Sybil ノード数（1 コンテンツにつき最大）	1,000
$N_{request}$	要求発生数	100,000
θ	Zipf 分布のパラメタ	0.9
r_{active}	ピアの稼働率	0.5
T_{up}	ピア平均連続起動時間	40 minutes
C_{rt}	ルーティングテーブル容量	64
T_{rt}	ルーティングテーブル更新間隔	30 minutes

4.2　検知性能評価

本節では，Sybil 攻撃に対する検知性能を定量的に評価する．シミュレーションは 4,320 minutes（3 日間）実行し，コンテンツ数は 40,000 とした．提案方式であるオンデマンド検知方式と，比較対象である KL ダイバージェンスに基づく定期検知方式について，攻撃検知の正確性および誤検知の傾向を比較する．Sybil 攻撃検知の性能評価には，二値分類問題として一般的に用いられる真陽性（TP），偽陰性（FN），偽陽性（FP），真陰性（TN）を用いる．まず，定期検知方式およびオンデマンド検知方式における検知結果を表 2 に示す．なお，定期検知方式は 10 分間隔で検知処理を実行する設定とした．

表 2　検知結果の集計

	定期検知方式	オンデマンド検知方式
真陽性（TP）	1,830	6,285
偽陰性（FN）	16,380	11,925
偽陽性（FP）	21	60
真陰性（TN）	176	137

表 2 より，定期検知方式は偽陽性（FP）が非常に少なく，正常なクラスタを誤って攻撃と判定する頻度が低いことが分かる．一方で真陽性（TP）が低く，偽陰性（FN）が高いという特徴が確認できる．これは，定期検知方式が一定間隔でのみ検査を行うため，検査と検査の間に発生した Sybil 攻撃を見逃す可能性が高いためであると考えられる．これに対して，提案方式であるオンデマンド検知方式では，真陽性（TP）が大きく増加し，偽陰性（FN）が減少している．これは，ユーザのコンテンツ取得要求を契機として検知処理を実行するため，攻撃が発生した直後であっても速やかに検知が行われたことが原因だと考えられる．一方で，オンデマンド検知方式では偽陽性（FP）が定期検知方式よりも増加している．これは，要求発生時の一時的な分布の偏りを攻撃として誤検知する可能性があるためと考えられる．しかしながら，FP の絶対数は依然として小さく，実運用において過剰な誤検知が頻発する状況ではないと判断できる．以上の結果を踏まえ，検知性能をより定量的に評価するため，検知率（Recall），精度（Precision），偽陽性率（False Positive Rate）を指標として用いる．これらの指標を用いて算出した検知性能指標を表 3 に示す．

表 3　検知性能指標の比較

	定期検知方式	オンデマンド検知方式
検知率（Recall）	0.1005	0.3451
精度（Precision）	0.9887	0.9905
偽陽性率（FPR）	0.1066	0.3046

オンデマンド検知方式は定期検知方式と比較して検知率が大きく向上していることが分かる．これは，攻撃の発生に対して迅速に検知処理を行えるため，攻撃状態を早期に捉えやすい特性を有しているためであると考えられる．一方で，精度はいずれの方式においても高い値を維持しており，オンデマンド検知方式においても誤検知が過度に増加していないことが確認できる．この傾向をより詳細に分析するため，コンテンツごとの要求数（人気度）に着目し，人気度別に検知率を比較した結果を図 1 に示す．

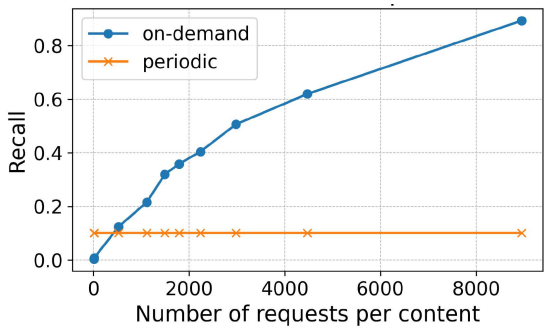

図 1　コンテンツ人気度別の検知率比較

図 1 より，オンデマンド検知方式はコンテンツの人気度が高くなるにつれて検知率が大きく向上することが分かる．これは，本稿で提案するオンデマンド検知方式が，ユーザからのコンテンツ取得要求を契機として検知処理を実行するという特性を持つためである．人気コンテンツは要求回数が多く，その分だけ検知処理が繰り返し実行されるため，PID 分布の偏りを十分に観測でき，Sybil 攻撃の兆候を捉えやすくなると考えられる．一方で，要求回数が少ない不人気コンテンツに対しては，検知処理が発生する機会自体が限られるため，検知率は低い値にとどまっている．しかしながら，不人気コンテンツはアクセス頻度が低く，攻撃による実質的な影響も相対的に小さいと考えられる．そのため，すべてのコンテンツを一律に監視するのではなく，影響の大きい人気コンテンツに対して重点的に検知を行うというオンデマンド検知方式の設計は，実運用を想定した場合に合理的であるといえる．以上の結果から，定期検知方式は誤検知を抑制できる一方で検知漏れが多く，オンデマンド検知方式は検知漏れを大幅に削減できる代わりに，一定の誤検知を許容する方式であることが分かる．本稿の目的である実際に影響の大きい Sybil 攻撃を早期に検知するという観点においては，オンデマンド検知方式がより適した特性を有しているといえる．

4.3　コンテンツ取得性能および検知コスト評価

本節では，Sybil 攻撃下におけるコンテンツ取得性能および検知コストについて評価を実施する．シミュレーションは 1440 minutes（1 日間）実行し，コンテンツ数は 10000 とした．提案手法であるオンデマンド検知方式と，比較対象である KL ダイバージェンスに基づく定期検知方式について，コンテンツ取得成功率，平均ホップ数，および検知に要する調査回数の観点から比較評価を実施する．なお，定期検知方式は 30 分間隔で検知処理を実行する設定とした．はじめに，攻撃なし環境，定期検知方式，および提案手法における全体的な性能比較結果を表 4 に示す．

表 4　全体性能の比較結果

方式	取得成功率 [%]	平均ホップ数	調査回数
攻撃なし環境	88.24	2.17	–
定期検知方式（30 minutes）	74.08	2.53	480,000
オンデマンド検知方式	74.18	2.52	100,000

表 4 より，提案手法は定期検知方式とほぼ同等のコンテンツ取得成功率および平均ホップ数を維持しつつ，検知に要する調査回数を約 5 分の 1 に削減できていることが分かる．この結果は，ユーザ要求を契機として検知処理を実行するオンデマンド検知方式により，不要な検査を抑制できていることを示している．次に，コンテンツの人気度ごとに取得成功率を比較した結果を図 2 に示す．ここで，図 2 の横軸は各コンテンツに対する取得要求数を表しており，Zipf 分布に従って生成された要求の中から，代表的な人気度階層として 100，695，1101，5525 回の要求を受けたコンテンツを抽出して評価を行っている．定期検知方式については、検知頻度によって性能が大きく変わるため、検知間隔として 20，30，50，70，110minutes の 5 通りを設定した．

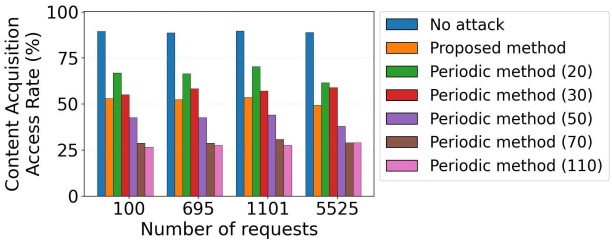

図 2　人気度別コンテンツ取得成功率

高人気コンテンツから低人気コンテンツに至るまで，取得成功率に大きな差が生じていないことが確認できる．これは，提案手法において PR の再配布数に上限を設けているため，検知後はコンテンツの人気度に依存せず，ほぼ同数の PR が再配布される設計となっていることが要因である．また，攻撃期間中にはすべての人気度帯のコンテンツに対して取得要求が発生しており，検知および再配布処理が適切に行われていたことも，人気度間で取得成功率の差が小さくなった一因であると考えられる．一方で，取得要求がほとんど発生しない極端に低人気なコンテンツについては，検知や再配布が行われず，取得成功率が低下する可能性がある．さらに，定期検知方式では検知間隔が長くなるにつれて，コンテンツ取得成功率が低下していることが確認できる．これに対し，提案方式であるオンデマンド検知方式は，定期検知方式を 30 minutes 間隔で実行した場合とほぼ同等の取得成功率を達成している．次に，オンデマンド検知方式と定期検知方式における攻撃対象コンテンツの取得成功率と調査回数の関係を表 5 に示す．

表 5　各検知方式における攻撃対象コンテンツ取得成功率と調査回数

方式	攻撃対象取得成功率 [%]	調査回数
オンデマンド検知方式	52.15	100000
定期検知方式（20 minutes）	66.21	500000
定期検知方式（30 minutes）	57.33	330000
定期検知方式（50 minutes）	41.93	200000
定期検知方式（70 minutes）	29.33	140000
定期検知方式（110 minutes）	27.71	90000

このとき，表 45 に示すように，オンデマンド検知方式の調査回数は約 100000 回であり，定期検知方式（30 minutes）と比較して約 3 分の 1 に抑えられている．この結果から，提案方式は検知コストを大幅に削減しつつ，定期検知方式と同程度の性能を維持できていることが分かる．また，オンデマンド検知方式と調査回数を揃えた場合，定期検知方式では検知間隔が 110 minutes 相当となる．この条件における攻撃対象コンテンツの取得成功率と比較しても，提案方式はより高い取得成功率を示しており，限られた検知回数の下でも効率的な検知および再配布が行われていることが確認できる．本稿の評価では，攻撃対象のコンテンツ ID 単体で見ると，提案方式は既存方式より取得成功率が低く見える場合がある．しかし，Sybil 攻撃は 1 つのコンテンツ ID のみに影響するのではなく，XOR 距離的に近い周辺 ID にも影響が広がる．提案するオンデマンド検知方式では，最初の取得失敗をきっかけとして攻撃を検知し，攻撃対象 CID に限定せず，XOR 距離的に近い周辺コンテンツに対しても PR の再配布を迅速に行う．一方，定期検知方式では検知タイミングが固定されているため，周辺コンテンツに対する再配布が遅延しやすい．その結果，攻撃対象 ID 単体では性能が低下して見える一方で，周辺コンテンツの回復が早まり，表 5 に示した結果からも分かるように，全体平均としては取得成功率が向上する．以上の結果から，提案手法は検知コストを大幅に削減しつつ，定期検知方式と同程度のコンテンツ取得性能を維持できていることが確認できる．特に，攻撃発生後に迅速に検知および再配布を行うことで，安定したコンテンツ取得を実現できている点は，オンデマンド検知方式の有効性を示す重要な結果である．

5. ま と め

IPFS は分散型 Web を支える基盤技術として注目されている一方で，Kademlia DHT に基づくルーティングは Sybil 攻撃に対して脆弱であり，特定コンテンツへのアクセスが妨害されるという課題を抱えている．特に，攻撃者が CID に近い Peer ID を持つノードを大量に配置することで，コンテンツ取得要求を循環させ，正当な Provider に到達できなくする攻撃は，IPFS の検閲耐性を根本から損なうものである．本稿では，ユーザのコンテンツ取得要求を契機として攻撃検知を行うオンデマンド検知方式を提案し，Peer ID 分布の偏りを KL ダイバージェンスにより評価することで，軽量かつ即時性の高い Sybil 攻撃検知を実現した．計算機シミュレーションによる評価の結果，提案方式は定期検知方式と比較して検知率を向上させ，攻撃を早期に捉えやすい特性を有することが確認された．一方で，精度は高い水準を維持しており，誤検知が過度に増加しないことも示された．また，Sybil 攻撃下におけるコンテンツ取得性能の評価では，提案方式は定期検知方式と同程度の取得成功率および平均ホップ数を維持しつつ，検知に要する調査回数を大幅に削減できることが分かった．これにより，検知コストを抑えながら，実用上十分なコンテンツ取得性能を確保できることが確認された．以上より，本稿で提案したオンデマンド検知方式は，IPFS の分散性や自律性を損なうことなく，Sybil 攻撃に対する実用的な検知・対処手法を提供するものであると結論づけられる今後の課題として，本稿では PR を保持する複数のピアがそれぞれ独立に攻撃検知を行い，再配布を実施する方式を想定していたが，この方式では検知回数が依然として多く，Provider Record を過剰に再配布する可能性が残されている．そこで今後は，選任アルゴリズムを導入し，コーディネータとなるピアを選出することで，攻撃検知および PR の再配布を集約的に実施する方式への拡張を検討する予定である．これにより，無駄な検知処理や再配布を抑制し，より効率的な Sybil 攻撃の検知・対処が可能になると考えられる．

謝辞　本稿は JSPS 科研費（25K03113, 23K28078）の助成を受けたものである．ここに記して謝意を表す．

文　　献

[1] Victor Henrique de Moura Netto, Thibault Cholez, and Claudia-Lavinia Ignat, Active Sybil Attack and Efficient Defense Strategy in IPFS DHT, arXiv preprint arXiv:2505.01139, 2025.

[2] Thomas Eisenbarth, Laura M. Roberts, and Federico Lombardi, Ethereum' s Peer-to-Peer Network Monitoring and Sybil Attack Prevention, Journal of Network and Systems Management, 2022.

[3] Ben Groves and Cong Pu, A Gini Index-Based Countermeasure Against Sybil Attack in the Internet of Things, IEEE MILCOM 2019, Nov. 2019.

[4] Frank Li, Prateek Mittal, Matthew Caesar, and Nikita Borisov, SybilControl: Practical Sybil Defense with Computational Puzzles, 7th ACM Workshop on Scalable Trusted Computing (STC 2012), Oct. 2012.

[5] Thibault Cholez and Claudia-Lavinia Ignat, Sybil Attack Strikes Again: Denying Content Access in IPFS with a Single Computer, Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024), 2024. DOI: 10.1145/3664476.3664482

[6] Juan Benet, IPFS – Content Addressed, Versioned, P2P File System, arXiv:1407.3561, 2014.

[7] Petar Maymounkov and David Mazières, Kademlia: A Peer-to-Peer Information System Based on the XOR Metric, Proceedings of IPTPS 2002, pp.53–65, 2002.

[8] John R. Douceur, The Sybil Attack, Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002), 2002.

[9] Thibault Cholez, Isabelle Chrisment, and Olivier Festor, Detection and Mitigation of Localized Attacks in a Widely Deployed P2P Network, Peer-to-Peer Networking and Applications, Vol.6, No.2, pp.155–174, 2012.

[10] Christian Baumgart and Stefan Mies, S/Kademlia: A Practicable Approach Towards Secure Key-Based Routing, Proceedings of ICPADS 2007, 2007.