4U-02

# 発信者追跡可能かつ仮名型のP2P情報発信システム

辻尾尚樹 †　岡部寿男 ‡
京都大学大学院情報学研究科 †　京都大学学術情報メディアセンター ‡

## 1. はじめに

インターネットを通して我々は不特定多数の人に向けて自由に情報を発信したりアクセスしたりすることができるが，時にそれらが権力の介入により阻害される場合が存在する．そのようなインターネットの規制や検閲から表現の自由を守り，自由な情報発信や情報へのアクセスを実現しようという研究として代表的なものに Freenet [1] や Tor [2] がある．しかし規制や検閲を一概に悪いものだと決めつけて排除するのも問題がある．発信される情報には犯罪予告のような多くの人が発信者を特定して阻止したいと思うであろうものや，政府への批判記事のように国内外に多く共感する人が存在する可能性のあるものがある．これらのことから規制や検閲が悪だと見なされるのは情報発信の場にいる人たちの大多数の意見に背いてそれらが行われる場合であると考えられる．

そこで我々は政府権力による独裁的な検閲の影響を受けず，システム内のユーザーが協力することによって発信者の特定を可能にする情報発信のシステムを提案する．提案するシステムは不特定多数への記事発信システムとし，ユーザーは仮名で記事の発信を行うことができる．システムは P2P 型で，発信された記事はピア間で中継されて拡散されていく．その際ユーザー間の協力による発信者の特定の可能性を残すため，中継ごとにピアはローカルにその中継のログを残すことを考える．そして各ピアが協力してログを提示し合うことによって発信者の特定を試みる方式を検討する．このように仮名型でありながら発信者の特定の可能性を残すことにより，独裁的な検閲の排除と犯罪捜査の可能性とのバランスを考慮した点が Freenet を初めとする既存の匿名情報発信システムとの違いである．

## 2. システムの設計

今回は Netnews のような不特定多数への記事発信システムを設計する．ただし Netnews にある Newsgroup のような機能は付けず，記事を他ユーザーへ発信する，あるいは発信された記事を読む，という単純な機能だけを提供する．

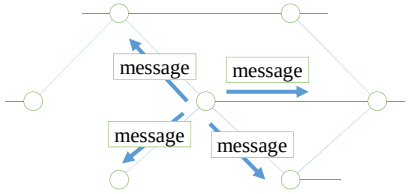


図 1: システムのイメージ図．図では中央のノードが隣接ノードに記事を発信しており，記事を受け取ったノードはその後さらに各自の隣接ノードにその記事を中継する．

### 2.1 可用性

システムに単一障害点がある場合そこを攻撃されると機能が停止してしまうため，単一障害点を持たせないようシステムを P2P 型のアーキテクチャーで設計する．システムのイメージ図を図 1 に示す．ユーザーは記事を発信し，発信された記事は隣接ノードに順次中継されていくことでネットワーク内に拡散されていく．

### 2.2 仮名性

本システムではユーザーは仮名で記事を発信する．記事には発信者を特定するような情報は付加しない．本システムにおける仮名とは，「原則として発信者の身元を特定するような情報は得られない」という意味である．この例外については 2.3 章で説明する．

記事を発信者から受け取ったノードはさらにその記事を隣のノードに中継する．このように多段中継によって記事が拡散される場合，たとえ発信者から記事を受け取る場合でも受け取ったノードは送信元が本当の発信者なのか，それとも誰かから記事を中継しただけなのか分からない．つまり発信者は身元を隠したまま記事を発信できたことになる．

### 2.3 発信者特定可能性

ここではそれぞれのユーザーは自身の証明書を持っていると仮定する．ユーザーが証明書を取得する方法として，今回は PGP (Pretty Good Privacy) で用いられている Web of Trust 方式を用いる．

---

A Traceable and Pseudonymous P2P Information Publication System

† Naoki Tsujio
Graduate School of Informatics, Kyoto University
‡ Yasuo Okabe
Academic Center for Computing and Media Studies, Kyoto University

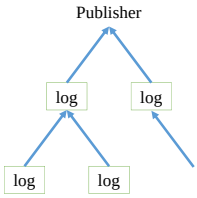


図 2: 記事の中継のログを繋ぎ合わせることによってできる木.

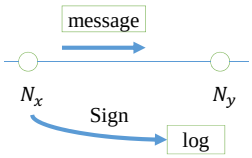


図 3: 記事の中継のログに対して中継元が署名をする様子.

記事の発信者を特定するための仕組みとして，本システムではユーザーは記事を中継する際にログをローカルに残すことを考える．ログの内容は「いつ」「誰から」「どのような記事を受け取った」というものである．それぞれのログの「誰から」の情報を繋ぎ合わせることによって図 2 のような木を作ることができ，ルートに位置する発信者を追跡することができる．

ただしログは各ユーザーの手元に保存されているので容易に改ざんやねつ造が可能である．そこでそれぞれのログに中継元の署名を付けることを考える．つまり記事を受け取ったユーザーは「その中継元から記事を受け取った」というログを残し，その中継元はそのログに対して署名を行うのである (図 3)．

オリジナルの発信者であるかどうかは署名が付与されたログを提示できるかどうかで判断する．その記事が自分が発信したものでなく誰かから中継したものであるならばその中継元ユーザーの署名が付いたログを保持しているはずだからである．

このように，ユーザーが各自のログを持ち寄ることによって記事の発信者を特定することができる．ユーザーがログを提示するかどうかはそのユーザーが記事の発信者を特定したいと思うかどうかが問題となる．例え全てでなくとも一定以上のログが集まれば発信者を特定できる可能性があるので，発信者を特定したいと思うユーザーが多くいればそれだけ特定できる可能性は高まる．逆にごく少数のユーザーのみが発信者を特定したいと思ってもその他のユーザーの協力が得られなければそれは困難となる．

## 3. 評価

提案するシステムは政府権力による独裁的な検閲からユーザーの自由な情報発信を守ろうというものである．そのため政府機関によるユーザーの仮名性を破ろうとする攻撃がいくつか想定される．

### 3.1 多数のノードの潜入

今回の発信者追跡の仕組みでは発信者を特定したいユーザーから発信者までのパス上にいるユーザーがログを提示するかしないかが問題となる．そのため予めシステム内に多数のスパイノードを潜入させておき，都合の悪い記事が発信された場合にその発信者との距離を小さくなるようにしておくという攻撃が考えられる．今回のシステムでは参加するユーザーは自身の証明書を持っており，ピアリングするノードをユーザーが選択できるようになっている．そのため政府が侵入させたスパイノードと疑われるノードとはピアリングしないことがとれる対策のひとつとして考えられる．

### 3.2 法的措置

発信者を特定するために，政府が法的措置等によってユーザーにログの提示を強制することが考えられる．しかし一般に，政府の権力は自国内でしか有効でなく，国境を越えた先では通用しない場合が多いはずである．この場合，国境を越えた発信者特定の捜査を行うためには国家間の合意が必要となる．つまり本研究の目的である単一の主体による独裁的な検閲の排除という点は果たされる．そのためユーザーが取れる対策としては，ピアリングするノードはなるべく国外のノードにするというものが考えられる．

## 4. おわりに

本稿では政府権力による独裁的な検閲の排除と犯罪捜査の可能性のバランスを考慮した，仮名型の情報発信システムを提案した．システムには記事の中継のログを残すことによる発信者特定の仕組みを導入した．今後はシステムの実装，また具体的なシステムへの攻撃についてのさらなる考察が課題である．

## 参考文献

[1] I. Clarke, O. Sandberg, B. Wiley, and T.W. Hong: Freenet: A Distributed Anonymous Information Storage and Retrieval System, *International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*, pp. 46 – 66, 2001.

[2] R. Dingledine, N. Mathewson, and P. Syverson: Tor: The Second-generation Onion Router, *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, pp. 21 – 21, 2004.