

2025 年 2 月 4 日
さくら情報システム株式会社

国際会議にて暗号通貨のプライバシー保護と犯罪抑止を両立する
新たな理論提案「Fair-Anonymity」を発表
～匿名性と法令順守を両立させる新たなアプローチ～

さくら情報システム株式会社(本社：東京都港区、代表取締役社長：伊延 充正)は、当社の樋口大志(情報セキュリティ大学院大学〔IISEC〕博士後期課程在籍)が執筆した研究論文「Fair-Anonymity: A Novel Fairness Notion for Cryptocurrency」(公正な匿名性：暗号通貨のための新しい公正性の概念)を、第 18 回 ネットワークセキュリティとアプリケーションに関する国際会議(18th International Conference on Network Security & Applications〔CNSA 2025〕)で発表したことをお知らせします。

■注目ポイント

今回の論文ではブロックチェーンを用いた暗号通貨における「匿名性と法令順守」を両立させる新たなアプローチとして「Fair-Anonymity」を提案しました。この研究は、暗号通貨の利用が増加する中で、犯罪抑止とユーザープライバシー保護の両方を実現することを目指しています。

■発表の概要

- ・発表者：樋口 大志

さくら情報システム株式会社／情報セキュリティ大学院大学 大塚研究室 博士後期課程在籍

- ・会議名：第 18 回ネットワークセキュリティとアプリケーションに関する国際会議

(18th International Conference on Network Security & Applications〔CNSA 2025〕)

- ・開催地：デンマーク・コペンハーゲン

- ・日程：2025 年 1 月 25 日～26 日

本国際会議は、ネットワークセキュリティ分野の学界および産業界の研究者・実務家が一堂に会し、現代のセキュリティ脅威への対策や新たな協力関係の構築について議論を行う場です。

- ・発表内容のポイント：

1. 「Fair-Anonymity」という新しい概念・スキームの提案

ブロックチェーン上の取引額に応じて、信頼機関のみが取引の送金者を追跡可能とする仕組み

2. 技術的な工夫(「Exponential Saturation Function」を応用)

分割送金による追跡回避を防ぎ、より安全なシステムを実現

3. 改良された情報交換技術(改良型 k-out-of-n コミットメント忘却伝送(Committed Oblivious Transfer))の採用

取引の透明性を保ちながら、必要に応じて追跡できる技術を導入し、システムの信頼性を高める

上記により、善意の利用者は、必要に応じて自分の身分を信頼機関に開示することに前向きである可能性が高くなります。一方で、犯罪者は少しでも追跡される可能性があるため、それを避けようとする心理が働きます。この理論に基づき、暗号通貨の送金において、「Fair-Anonymity」を利用するクリーンな経済圏と、これを利用しない不正な取引が行われる可能性のある経済圏を明確に区別する方法を提供します。

■研究の背景と意義

近年、暗号通貨の利活用が進む一方で、資金洗浄や違法取引といった犯罪利用防止のため、規制当局によるトレーサビリティの確保が重要視されています。

しかし、過度な規制や情報開示、検閲は、ユーザープライバシー保護や暗号通貨のイノベーションを損なうおそれがあります。そこで、樋口大志は「匿名性と法令順守」の両立というテーマで研究を進めています。

2023 年にはブラインド署名技術を用いたデジタル通貨「Open-cash」の理論研究を完成させ、Financial Cryptography and Data Security(DeFi ワークショップ)にて論文を発表しました [1]。

今回の「Fair-Anonymity」は、異なる切り口で、既存のブロックチェーン基盤による暗号通貨に適用可能な新たなスキームとして、匿名性と規制要請を両立することを目指した研究の成果となります。

■当社の取り組みについて

当社は、社会インフラを支える IT サービス企業として、金融・公共・産業分野におけるシステム開発とセキュリティ技術の研究開発に注力しています。

今回の発表は、情報セキュリティ分野における先進的な研究成果の一端であり、これまでの技術・知見をさらに発展させるものです。

■今後の展望

今回の研究発表では、違法取引防止やマネーロンダリング対策が求められる一方で、正当なプライバシー保護が重視される暗号通貨市場に対し、新たに柔軟な規制対応やシステム設計の可能性を示します。

当社は、今後も引き続き学術機関や国際コミュニティとの連携を図りながら、「Fair-Anonymity」の高度化とブロックチェーン等への実装・実証を推進していきます。

さらに、犯罪利用を抑止する安心・安全なデジタル通貨基盤の確立に向け、既存の「Open-cash」研究やセキュリティ関連技術とのシナジーを追求し、イノベティブで持続可能な社会の発展に貢献していきます。

[1] Higuchi Taishi and Akira Otsuka. "Electronic Cash with Open-Source Observers." International Conference on Financial Cryptography and Data Security. Cham: Springer Nature Switzerland, 2023.
https://link.springer.com/chapter/10.1007/978-3-031-48806-1_19

■さくら情報システムについて

<会社概要>

商号 : さくら情報システム株式会社(オーグス総研・三井住友銀行のグループ企業)
本社 : 東京都港区白金 1-17-3 NBF プラチナタワー
設立 : 1972 年 11 月 29 日
URL : <https://www.sakura-is.co.jp>
業務内容 : 三井住友銀行およびグループ会社の基幹システムを支え、幅広いお客様にハイレベルなサービスを提供してまいりました。豊かな経験から培ったノウハウ、技術、信頼を基に、会計・人事給与・金融・BPO・セキュリティ・システム運用の強みを軸に、今後もお客様の課題解決をトータルにサポートしていきます。

※ 本リリースに記載されている製品名、会社名は各社の商標または登録商標です。

<報道機関からのお問い合わせ先>

さくら情報システム株式会社 マーケティング戦略部 マーケティング推進グループ
担当：天野・小川
電話：03-6757-7211
E-mail：solution1@sakura-is.co.jp