別記様式第４号

2019 年度 独創的研究助成費 実績報告書

２０２０年　３月１６日

報　告　者	学科名	情報通信工学科	職 名	准教授	氏 名	國島丈生
研 究 課 題	ブロックチェーンに基づく情報トレーサビリティの確保に関する研究					

研 究 組 織	氏　名		所 属 ・ 職	専 門 分 野	役　割　分　担
	代表	國島丈生	情報通信・准教授	情報工学	研究全般・統括
	分担者	石川遼太	情報系・修士	情報工学	システム応用
		佐々木友弥	情報系・修士	情報工学	システム応用
		山下直也	情報系・修士	情報工学	システム設計・実装
		久保麗	情報系・修士	情報工学	システム応用
		志村拓起	情報系・修士	情報工学	システム設計・実装
		向原峻平	情報系・修士	情報工学	システム設計・実装

研究実績の概要	
	仮想通貨の基盤技術の一つであるブロックチェーンは分散ネットワーク上に構成される台帳であり、暗号技術などによって書き換え不可能性を実現している点において、新たな応用につながる可能性がある一方、技術的にはまだ未成熟の段階にある。研究代表者は一昨年度よりブロックチェーンに関する学術的研究に取り組んでいる。本研究はブロックチェーンの書き換え不可能性を情報トレーサビリティ、すなわち、情報システムにおけるデータのトレーサビリティ（来歴・所在・変更履歴などを後から追跡できるようにすること）の確保に応用する場合の諸問題を検討し解決することを目的とした。

※ 次ページに続く

研究実績 の概要	研究実績を以下に示す。いずれも本学情報系工学研究科修士論文として公表したほか、国内学会にて口頭発表している（成果資料参照）。 1. ブロックチェーンを用いたインターネット投票プロトコル[2, 4]：インターネットを用いた投票（インターネット投票）は社会的に重要な情報システムであるが、その実現には技術的課題がいくつか残っている。そのうちの一つが投票運営者による投票結果への不正行為（改ざん等）である。ブロックチェーンは書き換え不能かつ分散的に管理されることから、投票結果の透明性（誰でも自身の投票が正しく集計されたことを検証することができる）を保証できる技術として注目されており、学術研究だけではなく実証実験も行われている。本研究では、従来のブロックチェーンを用いたインターネット投票では満たされていなかった秘匿性（開票時刻までは投票内容を秘匿し、他社の投票行動に影響を与えないようにする）を持たせる投票プロトコルを提案し、プロトタイプシステムの実装により実現可能性を示した。提案プロトコルは、公開鍵暗号の一種であるタイムリリース暗号を用いて投票内容を暗号化しブロックチェーンに記録する。タイムリリース暗号では、暗号化時に指定された時刻が来るまで復号を行うことができないため、秘匿性を実現できる。 2. マハラノビス・タグチメソッド（MT 法）とブロックチェーンを用いたトランプゲームのイカサマ検知[1, 3]：MT 法は製品の製造工程等における異常検知・要因解析を行う手法であり、異常原因がわかっていない場合に有用である。本研究ではこれを、トランプゲームにおけるイカサマの検知に応用し、ゲームのシミュレーション実験により有効性を検証した。本研究の主な提案は、トランプゲームにおける場札の履歴などを観測し、その情報をもとにリアルタイムで MT 法による異常検知・要因解析を行う点にあり、トランプゲームのモデル化、ブロックチェーンへのゲーム履歴の記録、ブロックチェーン上の自動実行プログラム（スマートコントラクト）による異常検知・要因解析、などから構成されている。本研究で提案する異常検知システムのアーキテクチャは必ずしもトランプゲームに限ったものではないため、より実用的な諸問題への適用が今後可能であると考えられる。
成果資料目録	1. 佐々木友弥, 國島丈生. MT 法を用いたトランプゲームのイカサマ行為防止のための異常検知システム, 情報科学技術フォーラム講演論文集, 18(2), pp. 269-270, 岡山大学, 2019年9月3日. 2. 石川遼太, 國島丈生. プライベートブロックチェーンを用いたインターネット投票, 情報科学技術フォーラム講演論文集, 18(4), pp. 341-342, 岡山大学, 2019年9月4日. 3. 佐々木友弥, 國島丈生. MTS を用いたトランプゲームのイカサマ行為防止のための異常検知システム. 第 21 回 IEEE 広島学生シンポジウム, A2-16, pp. 136-141, 岡山県立大学, 2019 年 11 月 30 日～12 月 1 日. （同シンポジウム優秀研究賞） 4. 石川遼太, 國島丈生. インターネット投票におけるブロックチェーンとサーバ間のデータ共有方法の提案. 第 21 回 IEEE 広島学生シンポジウム, A3-16, pp. 225-227, 岡山県立大学, 2019 年 11 月 30 日～12 月 1 日.