様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月　 ４ 日現在

機関番号：１４６０３
研究種目：挑戦的研究（萌芽）
研究期間：2022～2023
課題番号：２２Ｋ１９７７６

研究課題名（和文）不正耐性をもつ投票型合意形成を実現するコンセンサス・コンピューティング

研究課題名（英文）Fraud-Resistant Voting Framework for Consensus Computing

研究代表者
笠原　正治（Kasahara, Shoji）

奈良先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：２０２６３１３９

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：不特定多数の参加者集団に対し，正直な参加者の貢献に加えて，悪意のある参加者さえもシステムに貢献する行動変容を誘発する投票型インセンティブ・メカニズムを創出するための基礎的検討を行った．具体的には，ブロック・チェーン・ネットワークにおける参加者間のインセンティブ相互作用の分析，電子投票システムにおける投票集計処理の正当性証明，SNSに参加するユーザの信頼度と情報拡散分析，の3点について研究を展開した．

研究成果の学術的意義や社会的意義
合意形成は多様な利害関係者間で意見の一致を図る重要なプロセスであり，近年ではブロック・チェーンにおけるコンセンサス・アルゴリズムを中心に信頼できる合意形成法が重要となってきている．本課題では，ブロック・チェーンに基づく情報サービスが持続的かつ健全に発展するための高信頼合意形成メカニズムについて，ユーザの信頼度，プライバシー保護，インセンティブ・メカニズムの観点から基礎的な研究を行ったものである．

研究成果の概要（英文）：We conducted foundational research to create a voting-based incentive mechanism that induces behavioral changes, encouraging both honest and malicious participants to contribute to the system in a crowd of unspecified participants. Specifically, we explored three aspects: analysis of incentive interactions among participants in blockchain networks, validity proof of vote counting processes in electronic voting systems, and analysis of trustworthiness and information dissemination among users participating in social networking services.

研究分野：情報ネットワーク

キーワード：ブロック・チェーン　インセンティブ・メカニズム　合意形成アルゴリズム　セキュリティ　トラスト

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

ビットコインやイーサリアムに代表されるパブリック型ブロック・チェーンでは，Proof-of-Work (PoW) と呼ばれるコンセンサス・アルゴリズムが新規ブロック承認にかかる合意形成処理を行なっている．PoW では難易度の高いハッシュ計算に基づくパズル的な問題を解くことでブロック承認を行うが，計算難易度の高さがブロック・チェーンの改ざんを困難にしている一方で，低スケーラビリティと莫大な電力消費量が欠点として知られている．PoW の欠点を克服するために提案された Proof-of-Stake では，トークンで代替されるステーク（拠出金）に応じて選出されたバリデータと呼ばれるノードが投票に基づくブロック承認を行う．Practical Byzantine Fault Tolerance に代表される投票型コンセンサス・アルゴリズムは処理負荷が小さく，少ない電力消費量で高速なブロック承認を行うことができる．しかしながら，投票を行うバリデータが善意のノードであることが必要不可欠なため，投票型コンセンサス・アルゴリズムはプライベート/コンソーシアム型のクローズドなブロック・チェーンで採用されているのみである．

ここで「投票」は合意を形成する基本的な手段であり，数理的な問題定式化や性質の分析は 18 世紀フランス革命期に研究されたコンドルセの陪審定理やボルダールールまで遡る．現在は社会科学の一分野である社会的選択理論やメカニズム・デザイン，オペレーションズ・リサーチにおける意思決定分野で，全投票者が投票結果にできるだけ満足できるような投票ルールに関する問題が活発に研究されている．近年では，投票者が正しく投票する確率を用いて一票の重みを決定する重み付き投票や，個人の選好の強さを一票に表せるように設計された Quadratic Voting など，新しい投票ルールが提案され，理論・実証の両面で研究が進んでいる．一方で情報科学における合意形成問題で投票を応用している研究は，一人一票に基づく単純な多数決原理を前提としたものが中心であり，投票者の投票行動や投票履歴，複数投票者が結託して行われる投票戦略などを考慮して投票者の行動変容を狙った投票型合意形成メカニズムの研究は皆無である．

２．研究の目的

本研究課題では，不特定多数の参加者集団に対し，正直な参加者の貢献に加えて，悪意のある参加者さえもシステムに貢献する行動変容を誘発する投票型インセンティブ・メカニズムを創出するための基礎的検討を行う．具体的には，ブロック・チェーン・ネットワークにおける参加者間のインセンティブ相互作用の分析，電子投票システムにおける投票集計処理の正当性証明，SNS に参加するユーザの信頼度と情報拡散分析，の 3 点について研究を展開した．

３．研究の方法

(1) ブロック・チェーンにおけるユーザ・マイナー間インセンティブ相互作用分析

ビットコイン型ブロック・チェーンでは，高い手数料が付与されたトランザクションほど早くブロックに含められる優先処理がマイナーノードによって行われている．そのため，エンドユーザにとっては許容範囲の遅延でトランザクションが処理されるのに必要な手数料に興味がある．マイナーは収益を増やすために高い手数料を含むトランザクションをブロックに含めることに興味がある．ブロックサイズの増大はブロック承認処理やネットワーク伝搬遅延を増大させる傾向にあり，エンドユーザの効用を減少させるだけでなく，フォークの多発による脆弱なセキュリティ状況になる恐れがある．以前の研究[1]でトランザクション手数料，承認処理遅延，セキュリティの三要素の依存関係を表現する数理モデルを構築したが，ここではさらに新規発行コインとマイニングの全ハッシュレートを加えた拡張数理モデルを考え，その妥当性について検証を行った．具体的には，承認処理遅延については待ち行列理論を応用した確率モデルを構築し，手数料・報酬及びセキュリティについてはユーザ及びマイナーの効用に対するナッシュ均衡分析を行い，系のナッシュ均衡解がどのように推移するかを計算機シミュレーションにより評価を行った．

(2) ゼロ知識証明を活用した投票集計処理の正当性証明手法

民主主義的な組織運営において，投票による意思決定は重要な役割を担っている．近年の ICT 技術の発展により，遠隔地からも投票可能な電子投票システムの実用化が増大しつつあり，ネットワークを介した電子投票システムの安全性や信頼性が重要な問題になりつつある．一方で，既存の投票システム自体の信頼性はシステムを管理する主体に対する信頼性に依存しており，投票システム管理主体の信頼性を確認する手段については検討されてこなかった．本研究課題では，投票管理システム自体の信頼性を確認する手法として，スマートコントラクトを用いた加法的準同型暗号と非対話型ゼロ知識証明に基づく電子投票システムを検討した．具体的には，簡潔なゼロ知識証明アルゴリズムとインバウンドオラクルを組み合わせた投票メカニズムを設計し，有権者が管理者の投票集計行動の信頼性を検証できる枠組みを検討した．提案投票システムの有効性を検証するため，システムのプロトタイプを実装し，実機実験によるフィージビリティの確認，及び問い合わせの処理速度と処理コストについて定量的な評価を行った．

(3) 心理学の五因子モデルを応用した SNS ユーザ信頼度モデル

情報の信頼性（トラスト）を保証するアプローチが近年注目を集めている．代表的な情報サービスである SNS はユーザが情報を共有・交換する情報流通プラットフォームであるが，フェイクニュースによる誤った情報の拡散が大きな問題となっている[2]．そこで本研究課題では SNS ユーザの情報拡散過程に焦点を当て，心理学の五因子モデルを考慮したユーザ信頼度モデルとエージェントベースシミュレーションによる情報拡散分析を行った．ユーザ信頼度モデルでは，SNS ユーザが他ユーザからのニュースを信頼するメカニズムに着目し，文献[3]の信頼モデルを基にしつつ，情報自体の信頼度を考慮する形で拡張を行った．具体的には，アイデンティティ，ユーザ行動，関係性，フィードバック要因の 4 項目に加えて，新たに情報自体の信頼度を加えたトラストモデルを構築した．情報自体の信頼度は意味論的な特徴と表面的な特徴から構成され，前者は投稿の論理的観点から情報の正確さを定量化した指標で表され，後者は投稿の外観的な観点として写真の有無や投稿の人気度といった要素を定量化した指標で表現される．ここでは情報ベースの信頼度を投稿の論理的正確性，写真の有無，投稿人気度の 3 点から定量的に定義した．また五因子モデルについては文献[4]のアプローチを参考にエージェントシミュレーションにおいて SNS ユーザの人格特性を組み込んだモデルを作成した．

4．研究成果

(1) ユーザ・マイナー間インセンティブ相互作用分析

数値実験を通して，提案した数理モデルにより，トランザクションの承認遅延，手数料，セキュリティの 3 要素がどのように依存して系が推移するかを定量的に評価できることが確認された．一例として，トランザクション承認遅延と攻撃成功確率の均衡点推移の結果を紹介する．数値実験のパラメータは，ビットコイン・ネットワークの状況を参考に設定した．図 1 は新規発行コインが 0 のときの承認遅延に対する攻撃成功確率の推移を表している．この図より，新規発行コインが 0 のときは承認遅延を増大させても攻撃成功確率が上昇を繰り返し，セキュリティが脆弱になる状況に推移する傾向が観察される．一方，新規発行コインが 12.5 の場合，図 2 より，承認遅延と攻撃成功確率が均衡点に収束する状況が観察される．これらの結果より，ビットコイン・ブロック・チェーンでは新規発行コインの総量がセキュリティを保証した安定状況の維持に重要な役割を担っていることが確認された．また，一方でマイニングにかかるコストが低下する状況で数値実験を行った結果，セキュリティが多少脆弱な環境でも承認遅延が小さいところで均衡点が存在することが確認された．

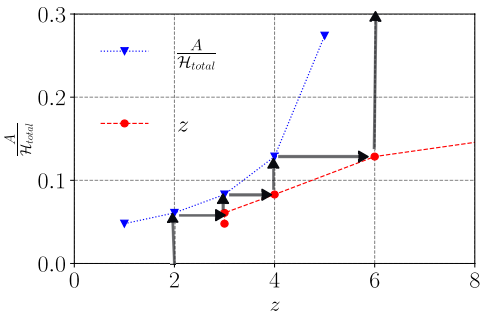

図 1 攻撃成功確率と承認遅延
（新規発行コイン 0 の場合）

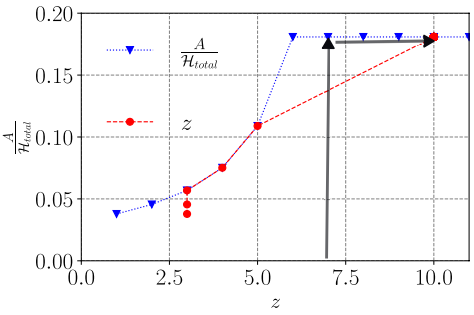

図 2 攻撃成功確率と承認遅延
（新規発行コイン 12.5 の場合）

(2) ゼロ知識証明を活用した投票集計処理

提案システムの概要を図 3 に示す．提案システムの実現可能性を検証するため，提案システムのプロトタイプを Ethereum のスマートコントラクトとして実装した．具体的にはローカルな Ethereum ブロック・チェーンである Ganache を用い，投票メカニズムは Solidity，包括ゼロ知識生成，サーバ・コマンド，投票検証のアルゴリズムについては Python で実装を行った．また，オンチェーン環境とオフチェーン環境を接続してゼロ知識証明を ZKP コントラクトにアップロードするオラクル実現のために Provable を選択した．

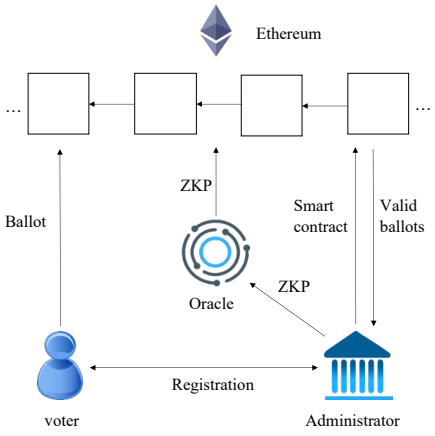

図 3 提案電子投票システム

実機実験より，提案アルゴリズムが正常に動作することを確認するとともに，処理遅延と処理コストについて計測を行った．処理遅延については，1 票を投じる際の全体の実行時間は約 1.438 秒から 2.243 秒であり，既存文献で報告されている実行時間よりも優れていることが確認された．一方で，投票処理時間のほとんどがスマートコントラクトによる処理時間であることが判明した．また，ゼロ知識証明の生成にかかる処理時間については投票者数に比例して線形的に増加することが確認された．最大 500 人の有権者が参加するケースにおいては，ゼロ知識証明の生成時間は 1.5 秒程度であり，提案手法は比較的大規模な投票者集団における投票でも十分に機能することが判明した．一方，投票

処理のコストについては，投票の検証処理のコストが相対的に高いことが確認された．投票処理コストについては実装に依存するところが大きく，処理コスト削減のための実装方法については今後の課題である．

(3) 心理学の五因子モデルを応用した SNS ユーザ信頼度モデル

計算機シミュレーション実験では，NetLogo 6.0.4 を用いて SNS 用のエージェントベースモデルを開発した．シミュレーションでは，最初に SNS ユーザの論理的ネットワークが Barabási Albert モデルに従って生成され，つづいて五因子モデルによってユーザの人格特性が決定される．次に正常ニュースとフェイクニュースが確率的に生成され，五因子モデルの特性に従ってニュースが SNS ネットワーク上を伝搬する．1 時間ステップ毎に SNS ユーザの信頼度が更新され，シミュレーション終了時間までこのプロセスを繰り返す．図 4 は SNS ユーザ間のニュース拡散の状況をスナップショット的に図示したものである．図 4 左側は開始後のニュース拡散の状況を表し，右側はシミュレーション終了時点での最終的なニュース拡散状況を示している．

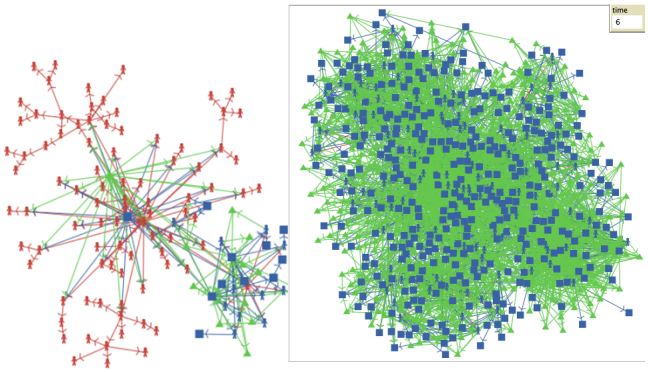

図 4 SNS ユーザ間のニュース拡散

提案したユーザ信頼度の妥当性を検証するため，ユーザに送信された全ニュース数に対する受け取ったニュース数の割合で定義されたユーザ信頼性指標[5]と提案ユーザ信頼度の比較を行った．図 5 は横軸にユーザ信頼性指標，縦軸にユーザ信頼度を取った点をプロットしたものである．この図より，信頼性指標の増加とともに信頼度もほぼ線形に増加していることがわかる．この傾向は文献[5]においても報告がなされており，提案したユーザ信頼度が概ね妥当であると考えられる．

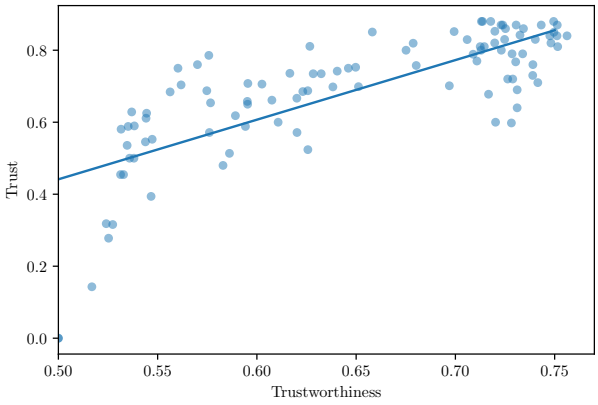

図 5 ユーザ信頼度と信頼性指標の比較

五因子モデルとユーザ信頼度の関係については，ユーザのフェイクニュースを共有する確率が低い場合，誠実性と外向性がユーザ信頼度の値を増加させる傾向にある一方で，開放性と神経症的傾向についてはユーザ信頼度の値を減少させる傾向にあることが判明した．

参考文献

[1] Hiraide, T., and Kasahara, S., “A Mathematical Model of Blockchains Considering Dependencies of Fees, Confirmation Latency, and Security,” 2022 International Conference on Emerging Technologies for Communications (ICETC2022), S3-3, November 29, 2022.

[2] Cigi-Ipsos global survey internet security and trust 2019 part 3: social media, fake news and algorithms. Cigi-Ipsos, 2019.

[3] Gao Y, Li X, Li J, Gao Y, Philip SY (2019) Info-trust: a multi-criteria and adaptive trustworthiness calculation mechanism for information sources. IEEE Access 7:13999-14012.

[4] Burbach L, Halbach P, Ziefle M, Calero Valdez A (2019) Who shares fake news in online social networks? In: Proceedings of the 27th ACM conference on user modeling, pp. 234-242.

[5] Antoci A, Bonelli L, Paglieri F, Reggiani T, Sabatini F (2019) Civility and trust in social media. J Econ Behav Organ 160:83-99.

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　1件／うちオープンアクセス　2件）

１．著者名 Hiraide Takumi、Kasahara Shoji	４．巻 6
２．論文標題 Analysis of interaction between miner decision making and user action for incentive mechanism of bitcoin blockchain	５．発行年 2023年
３．雑誌名 Frontiers in Blockchain	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.3389/fbloc.2023.1067628	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Muhammad Radifan Fitrach、Kasahara Shoji	４．巻 14
２．論文標題 Agent-based simulation of fake news dissemination: the role of trust assessment and big five personality traits on news spreading	５．発行年 2024年
３．雑誌名 Social Network Analysis and Mining	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13278-024-01235-8	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Qu Qianyue、Zhang Yuanyu、Kasahara Shoji	４．巻 2023
２．論文標題 Analysis of Eavesdropping Region in Hybrid mmWave-Microwave Wireless Systems	５．発行年 2023年
３．雑誌名 Wireless Communications and Mobile Computing	６．最初と最後の頁 1～14
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2023/3178335	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Wiraatmaja Christopher、Kasahara Shoji	４．巻 -
２．論文標題 Cost-Efficient Anonymous Authentication Scheme Based on Set-Membership Zero-Knowledge Proof	５．発行年 2023年
３．雑誌名 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/BRAINS59668.2023.10316788	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Wu Yuxiao、Kasahara Shoji	４．巻 -
２．論文標題 Smart Contract-Based E-Voting System Using Homomorphic Encryption and Zero-Knowledge Proof	５．発行年 2023年
３．雑誌名 Applied Cryptography and Network Security Workshops (The 5th International Workshop on Application Intelligence and Blockchain Security (AIBlock 2023))	６．最初と最後の頁 67～83
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-41181-6_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計14件（うち招待講演　2件／うち国際学会　5件）

１．発表者名 Radifan Fitrach Muhammad, Kasahara Shoji
２．発表標題 Agent-based Simulation Approach to Information Dissemination in Social Networking Service: The Impact of Big Five Personality Traits on User Trust
３．学会等名 2022 International Conference on Emerging Technologies for Communications (ICETC2022), S3-2（国際学会）
４．発表年 2022年

１．発表者名 平出託海, 笠原正治
２．発表標題 A mathematical model of user-miner interaction through confirmation latency and fees in Bitcoin-type blockchains
３．学会等名 第39回（2022年度）待ち行列シンポジウム「確率モデルとその応用」, 早稲田大学本キャンパス小野記念講堂, pp. 112-121
４．発表年 2023年

１．発表者名 玉井駿哉, 笠原正治
２．発表標題 貨幣数量説に基づくユーティリティートークンの流通方式に関する考察
３．学会等名 日本オペレーションズ・リサーチ学会2023年春季研究発表会, アブストラクト集, pp. 102-103
４．発表年 2023年

１．発表者名
Yamada, K., Hara, T., and Kasahara, S.

２．発表標題
A Repeated Stochastic Game Approach for Offload Mining in Distributed Applications in a Permissionless Blockchain Network

３．学会等名
2023 International Conference on Emerging Technologies for Communications (ICETC2023)（国際学会）

４．発表年
2023年

１．発表者名
Muhammad, R.F., and Kasahara, S.

２．発表標題
An Agent-Based Model for Social Networking Service Users in Exchanging Information

３．学会等名
2023 International Conference on Emerging Technologies for Communications (ICETC2023)（国際学会）

４．発表年
2023年

１．発表者名
Shoji Kasahara

２．発表標題
Modeling and Analysis of Bitcoin Mining Mechanism -A Queueing Theoretical Approach-

３．学会等名
Blockchain Kaigi 2023 (BCK23)（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
Shoji Kasahara

２．発表標題
A Matrix-Analytic Approach to Mining Process of Bitcoin Blockchain: How is the transaction-confirmation time affected by transaction arrival process?

３．学会等名
The International Teletraffic Congress ITC 34（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
笠原正治

２．発表標題
Proof-of-Stake ブロック・チェーンにおける投票型コンセンサスアルゴリズムと信頼度を用いた報酬罰則型インセンティブ・メカニズム

３．学会等名
日本ＯＲ学会 待ち行列研究部会

４．発表年
2022年

１．発表者名
山田浩太，原崇徳，笠原正治

２．発表標題
分散アプリケーションにおけるゲーム理論に基づくマイニングタスクのオフロード手法に関する一検討

３．学会等名
電子情報通信学会技術研究報告（NS2023-198），pp.154-159

４．発表年
2024年

１．発表者名
玉井駿哉，笠原正治

２．発表標題
クジラ問題と談合問題を考慮した DAO の投票メカニズム

３．学会等名
第40回（2023年度）待ち行列シンポジウム「確率モデルとその応用」，高知城ホール，pp. 156-165

４．発表年
2024年

１．発表者名
玉井駿哉，笠原正治

２．発表標題
Quadratic Voting 採用型 DAO における不正結託耐性に関する検討

３．学会等名
日本OR学会 2023年度関西支部若手研究発表会

４．発表年
2023年

１．発表者名
Qianyue Qu, Yuanyu Zhang, and Shoji Kasahara

２．発表標題
Auction Game in RIS-aided Secure Wireless Communication from the Physical Layer Security Perspective

３．学会等名
日本OR学会 待ち行列研究部会

４．発表年
2023年

１．発表者名
山田浩太，原崇徳，笠原正治

２．発表標題
ゲーム理論を用いた分散アプリのオフロードマイニングにおけるLyapunov 最適化

３．学会等名
電子情報通信学会 超知性ネットワーキングに関する分野横断型研究会（RISING）

４．発表年
2023年

１．発表者名
山田浩太，原崇徳，笠原正治

２．発表標題
分散アプリにおけるオフロードマイニングのための繰返確率ゲーム

３．学会等名
電子情報通信学会2023年ソサイエティ大会，講演論文集，B-6-19

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	笹部　昌弘 (Sasabe Masahiro) (10379109)	関西大学・総合情報学部・教授 (34416)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	原　崇徳 (Hara Takanori) (70907881)	奈良先端科学技術大学院大学・先端科学技術研究科・助教 (14603)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
中国	Xidian University			