

令和 5 年 6 月 9 日現在

機関番号：34315

研究種目：基盤研究(B)（一般）

研究期間：2019～2021

課題番号：19H04103

研究課題名（和文）高可用IoT/CPSのためのブロックチェーン連動型ネットワーク制御技術の研究開発

研究課題名（英文）Research and development of network control technology for blockchain-based highly-available IoT/CPS

研究代表者

山本 寛 (Yamamoto, Hiroshi)

立命館大学・情報理工学部・教授

研究者番号：80451201

交付決定額（研究期間全体）：（直接経費） 13,400,000円

研究成果の概要（和文）：本研究課題は高信頼なIoT/CPSを実現するための基盤技術を確立することを目的としており、ブロックチェーン基盤を活用して、現実空間に配備されているセンサノードが生成するデータの管理基盤を設計・試作した。また、ブロックチェーン上で管理されているデータを機械学習技術により解析することで、IoT/CPSに生じている異常を検知し、解析処理が正しく行われたことを検証する機能を実現した。さらに、IoT/CPSにおけるデータ管理/解析処理の局所性を実現するために、エッジコンピューティング技術や情報滞留技術を活用して、データを管理/解析するノードが特定のエリア内に存在することを保証できる技術を実現した。

研究成果の学術的意義や社会的意義

本研究課題の成果となるブロックチェーン基盤が実用化されることで、IoT/CPSにおけるデータの収集/解析/フィードバックの過程に攻撃者が介入して情報が不正に改竄される状況を防ぐことができ、高信頼なIoT/CPSが実現できる。これにより、IoT/CPSに関する技術が普及し、それらの技術を活用して人の社会活動や生活を支えるシステム/サービスの展開が加速する効果が期待できる。

研究成果の概要（英文）：The objective of this study is to realize a new platform technology for constructing a high-reliable IoT/CPS, and we have designed and prototyped a data management platform for storing the real-world sensor data utilizing an open-source blockchain platform, Hyperledger Fabric. In addition, we have proposed new analysis methods for detecting anomaly conditions in the IoT/CPS and verifying the correctness of the process of the data analysis. Furthermore, to realize the locality of the data management/analysis procedure, we have designed a new multi-layer blockchain architecture that has a function of guaranteeing that the mobile nodes exist within a limited range of the real-world.

研究分野：情報ネットワーク

キーワード：IoT/CPS Blockchain エッジコンピューティング 情報滞留技術

### 1. 研究開始当初の背景

近年、現実空間の様々な人・モノにセンサを装備し、網羅的に収集したデータを解析して災害や交通などに関する有益な情報を抽出して現実空間へフィードバックすることで、人々の生活や社会活動の品質を飛躍的に向上する IoT (Internet of Things)/CPS (Cyber Physical System) に注目が集まっている。しかし、IoT/CPS におけるデータの収集/解析/フィードバックの過程に攻撃者が介入し、不正に改竄された情報を基にフィードバックが行われることで、大きな被害が発生する可能性がある。特に、代表的な IoT/CPS であるスマートシティやコネクテッドカーが攻撃対象となることで、重大な事故につながる危険性も指摘されている。

一方、中央集権的な組織が管理する中央サーバを必要とせず、利用者間で発生する任意のデータの取引を、不正な改竄がなく完全性を持って分散管理できるブロックチェーンに注目が集まっている。また、Ethereum や Hyperledger のような新しいブロックチェーンには、スマートコントラクトと呼ばれる任意のコード(主に自動取引)を実行する仕組みが用意されている。スマートコントラクトはデータと機能がひと固まりとなった実体であり、内部で任意のデータを管理できるだけでなく、ブロックチェーン上のデータに基づき任意の処理を実行することも可能である。加えて、各スマートコントラクトでのデータ管理/解析の履歴も、改竄されることなく完全性を持ってブロックチェーン上で管理できる。つまり、ブロックチェーンを基盤として IoT/CPS におけるデータ収集/解析/フィードバックの機能を再設計することで、攻撃者によるデータ改竄の心配がない、高信頼 IoT/CPS を実現できる可能性がある。

### 2. 研究の目的

ブロックチェーンの基本的なデータ構造はリストであるが、近年登場した新しいブロックチェーンは、取引の履歴やスマートコントラクトを参照するための引用情報のみをリストに記録し、その実体はインターネット上の任意のノードに配置できるなどの自由度を持っている。本研究課題の目的は、情報滞留手法やエッジコンピューティングといった IoT/CPS 向けネットワーク技術を活用して、IoT/CPS を構成する機能の実体(スマートコントラクト)だけでなく、それらの利用履歴を管理する機能をフィールド上の特定のエリア内に局所化することで、高信頼性だけでなく、機密性とリアルタイム性を備えた高可用 IoT/CPS を構築できるブロックチェーンを利用した共通基盤を実現することにある。

本研究開発のポイントは、IoT/CPS 向けネットワーク技術を利用した IoT/CPS の提供範囲に合わせた局所的なブロックチェーンの構築であるが、そのためには各エリアで将来的に提供される IoT/CPS サービスとその性能要件(機密性、リアルタイム性など)を予測し、適切なネットワーク技術を適用する必要がある。一方、ブロックチェーンを利用して IoT/CPS 基盤を構築することで、過去から現在までに各エリアで提供された IoT/CPS の履歴が、改竄されることなくブロックチェーン上に記録される。この膨大な量の知識を AI (特に深層学習)により解析することで、将来的に各エリアで提供される IoT/CPS サービスを予測し、それを構成するデータ管理/解析と、その性能要件を事前に把握できる可能性がある。本研究開発の独自性と創造性は、AI を介してブロックチェーンと IoT/CPS 向けネットワーク技術が有機的に連携することで、様々な要件に対応できる高可用 IoT/CPS 基盤を構築することにある(図 1)。

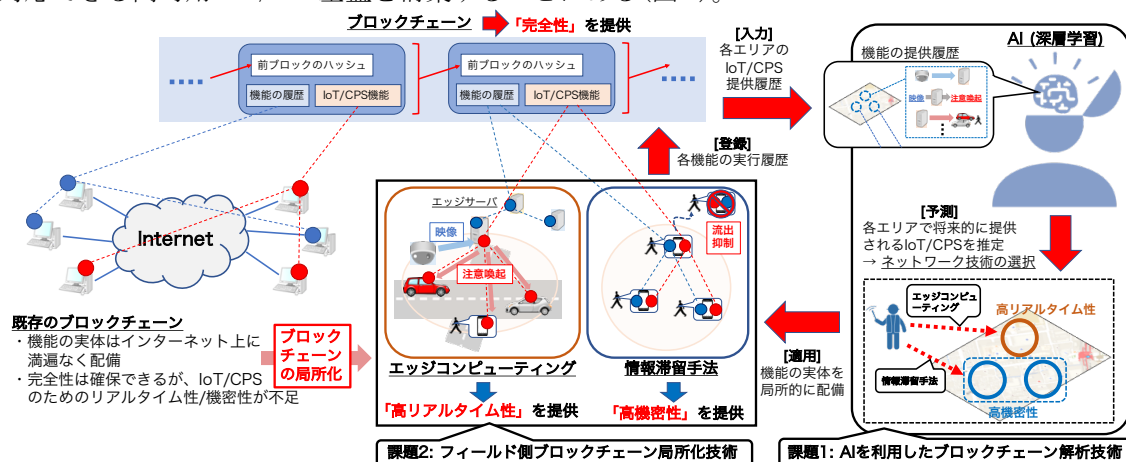


図 1 高可用 IoT/CPS 基盤の全体像

### 3. 研究の方法

本研究課題では、目的を達成するために以下の 3 つの課題に取り組んだ。

#### (1) AI を利用したブロックチェーン解析技術の研究

AI を利用したブロックチェーン解析技術を確立するために、まずはブロックチェーンを用いた IoT/CPS の応用事例を想定した試作を行う。特に、IoT/CPS 基盤に必要な不可欠であるスマートコントラクトに対応しているオープンソースのブロックチェーン(例: Ethereum, Hyperledger) を利用し、物流や人流観測などの応用事例について、現実空間に設置したセンサから収集したデータを管理・解析する機能を、ブロックチェーンおよびスマートコントラクトにより構築できることを検証する。また、ブロックチェーン上で管理されている多様なデータに対して、汎用的なライブラリ (TensorFlow, PyTorch など) により構築した AI 機能から参照できることを確認する。

また、研究開発したインタフェースを通して、AI 等の技術によりブロックチェーンに記録されているデータを解析し、そのデータの信頼性を検証する手法を確立する。加えて、その解析した履歴もブロックチェーン上に記録して第三者による参照を可能とすることで、IoT/CPS におけるデータ管理・解析の過程が正しく行われたことを検証できる手法を確立する。

#### (2) フィールド側ブロックチェーン局所化技術の研究

高い計算能力を備えたエッジサーバを配備し、IoT/CPS を構成するデータ管理/解析の機能とその利用履歴を管理する機能を、エッジサーバを中心とした限られたエリア内のネットワークに配備し、局所的なブロックチェーンを構築する手法を考案する。特に、データ解析やマイニングといった計算量の多い処理を、近隣エリアに配備されたエッジサーバ群が連携して担当し、ブロックチェーンで管理されているデータが改竄されていないことを確認する仕組みを検討する。また、フィールドのネットワーク状態に応じて各エッジサーバが担当する処理をスケジューリングすることで、高いリアルタイム性を実現する手法を検討する。

次に、フィールド上に存在するモバイルノードがアドホックネットワークを構築して情報を特定のエリア内に滞留させる情報滞留手法を活用し、データ管理/解析がフィールド上の特定のエリア内で確実に完結する局所的なブロックチェーンを構築する手法を考案する。特に、プライバシー情報を含む映像や位置情報のようなデータがエリア外に流出することを避けるために、モバイルノード/データの位置をブロックチェーンへ定期的に記録し、データを保有しているモバイルノードが確実にエリア内のみ存在することを相互に監視して高い機密性を実現する仕組みを検討する。また、ブロックチェーンに記録されているモバイルノード間での通信履歴を解析することで、エリア内からデータが流出する原因となる、モバイルノードに生じている異常な状態 (GPS による位置情報に大きな誤差が生じる状態など) を特定する手法を検討する。

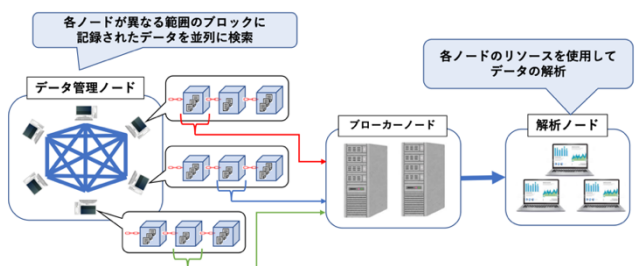
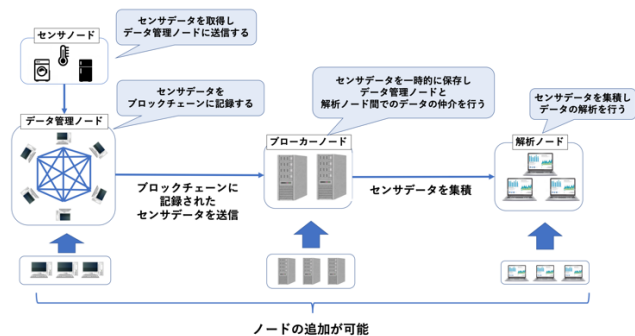
#### (3) AI とブロックチェーンが連動する IoT/CPS 基盤の設計・試作

AI によるブロックチェーン解析の結果に基づき各フィールドにとって適切な局所化の技術を選択し、関連するエッジサーバやモバイルノードに対して、IoT/CPS のための局所的なブロックチェーンを構築するための機能を適切に配備できる基盤を設計・試作する。また、試作した IoT/CPS 基盤を用いて具体的な応用事例を想定した実証実験を繰り返すことで、IoT/CPS 基盤が備えるべき機能を高度化して完成させる。

### 4. 研究成果

#### (1) AI を利用したブロックチェーン解析技術の研究

様々なデータの登録・蓄積に対応しているブロックチェーン基盤である Hyperledger Fabric を活用して、現実空間に配備されているセンサノードから収集したデータを管理する基盤を設計・試作した。この基盤は、図 2 のようにデータを取得してブロックチェーンに登録するセンサノード、ブロックチェーンを構成するデータ管理ノード、ブロックチェーン上のデータを解析用のノードへ転送するブローカーノード、およびブロックチェーン上のデータを解析する解析ノードで構成されている。センサノードは、計測したデータの追加要求をデータ管理ノードに送信することで、生成したデータをブロックチェーンに登録する。また、データ管理ノードはブロックチェーンに登録されたデータを読み出し、ブローカーノードを介して解析ノードに送信する。さらに、解析ノードでデータを解析することで、ブロックチ





チェーンに記録されているデータの真正性を検証する。また、この基盤では、ブロックチェーンに記録されたデータの参照/解析を、複数ノードにより分散して行う。具体的には図3に示すように、各データ管理ノードが異なる範囲のブロックに記録されたデータを検索し、ブローカーノードを介して解析ノードにデータを送信する。また、複数の解析ノードがクラスタを構成しており、クラスタの全リソースを使用して解析処理を行う。以上のように、提案する基盤はデータ検索/解析の高速化を図る設計となっており、データ管理ノード/解析ノードの数を増やすことで、ブロックチェーン上のデータに生じている異常の特定に要する時間を、線形に短縮できることを実証実験により明らかにしている。

また、現実空間に配備されたセンサノードから収集できる現実空間の環境・状態に関する情報に加えて、IoT/CPSに関連する通信の履歴から抽出できる通信状態に関連する特徴量を蓄積することのできるデータ管理基盤を設計・試作した。図4に示すように、新型コロナウイルス対策のために入退室管理の自動化や室内の人群密度の推定を行うシステムを想定しており、カメラや環境センサからデータを収集するIoT/ネットワーク機器と、ブロックチェーンを活用して複数レイヤーの情報を収集/解析するデータ管理基盤で構成される。またこの基盤は、IoT/CPSに対する多様な攻撃を検知するために、ネットワーク層の情報を解析する機能を備えている。解析処理の流れは図5の通りであり、IoT/CPSを構成するネットワーク機器から通信履歴を取得してグラフ構造で表現し、正常な状態のネットワークから導出できるグラフ構造との類似性を機械学習の技術(ランダムカットフォレスト)を用いて検証することで、異常検知を実現している。

さらに、センサノードにより計測・収集されたセンサデータが計測・収集・管理の過程で改ざんされていないことを保証し、ブロックチェーンに登録されたデータが正しく解析されたことを検証する機能を備えた基盤を設計・試作した。この基盤は図6のように、ブロックチェーンを活用したセンサデータ管理機能、ブロックチェーンを構成する各ブロックに登録されているデータの索引を保持することで高速なデータの参照を実現するブロックメタデータベース、スマートコントラクトにより実装されているデータの登録・解析機能、および最新のセンサデータやセンサデータの解析結果を保持する状態共有データベースにより構成されている。この基盤では、図7のようにブロックチェーンに登録されたセンサデータを参照して解析する機能をスマートコントラクトとして実装することによって、解析に使用するデータおよび解析処理の信頼性を向上させている。また、解析結果を利用するエンティティが解析対象のデータに直接アクセスすることなく、同一のデータ・同一の解析処理内容を基に解析結果の検算を行うことができ、データのプライバシー/所有権を確保しながら解析処理の信頼性を検証することが可能となる。

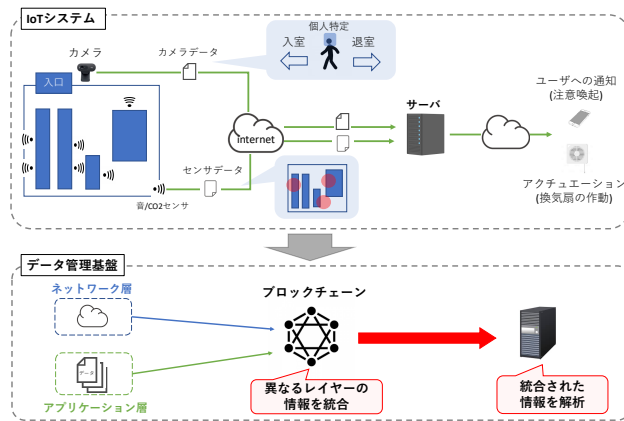


図4 複数レイヤーに跨るデータ管理/解析基盤の全体像

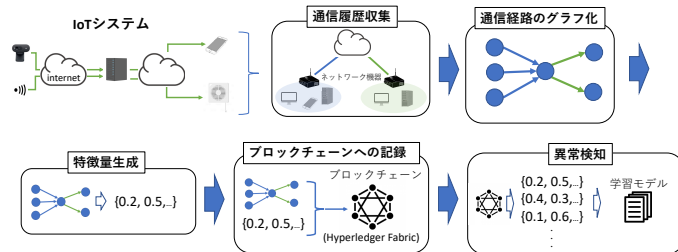


図5 ネットワーク層を対象とした解析の流れ

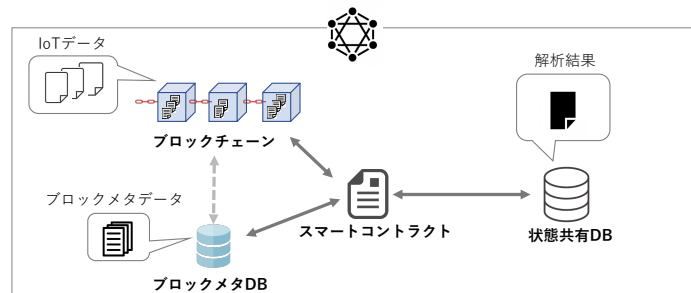


図6 解析処理の信頼性検証機能を備えた基盤の全体像

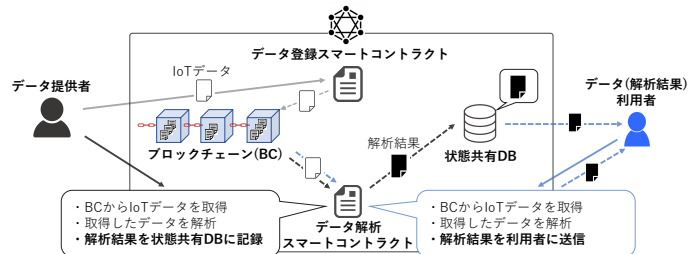


図7 解析処理の信頼性を検証する流れ

## (2) フィールド側ブロックチェーン局所化技術の研究

エッジコンピューティングによる高リアルタイム性ブロックチェーンの構築に関して、まずは低遅延エッジコンピューティングの現実的なモデルの性能をシミュレーションにより評価した。当該モデルでは、ネットワーク内にオーケストレータと呼ばれる制御ノードを設置し、モバイルノードからの計算要求を複数の計算ノードにどのように分散するか、などについて明らかにした。また、このモデルを実装し、実ネットワークに展開する際の課題を抽出し、実環境での性能評価を実施した。さらに、実際に東京と札幌にエッジコンピューティングのサーバを配置し、タスクの受け入れポリシーを検討した。加えて、今後の IoT 環境で重要となる不正な DoH 通信の検知技術について検討し、その基本設計を明らかにした。

次に、情報滞留手法による高機密性ブロックチェーンの構築に関して、まずは情報滞留手法のためのブロックチェーン技術を用いたデータトレース手法を提案し、データを利用するユーザが受信した情報をエリア内で滞留しているか検証できる事を示した。また、所望の地理空間範囲内で確実にデータ滞留が行われていることを検証できるように、ブロックチェーンを利用して各滞留範囲におけるデータ流通の状態を共有・比較するデータ監査技術を提案した。加えて、ブロックチェーン上で情報が拡散・共有される過程を模擬できるシミュレータを用いて、監査の正確性及びリアルタイム性に関して有効性を評価した。さらに、情報滞留を構成する車両が滞留エリア外での配信を検知するための監査機構として、多層化ブロックチェーンシステムを提案した。このシステムでは、下位層のブロックチェーンでは特定の地域での情報共有を実現し、上位層のブロックチェーンでは地域を跨いだ情報共有手段を提供する。また、本システムにおける効率的なデータ探索を実現するために上位層ブロックチェーンの探索手法を提案し、シミュレーションによってその有効性を評価した。

## (3) AI とブロックチェーンが連動する IoT/CPS 基盤の設計・試作

IoT/CPS 基盤における AI とブロックチェーンの連携制御のための機能をエッジサーバやモバイルノードへ配備できる IoT/CPS 基盤と、その基盤を活用した具体的なアプリケーションについて検討を行った。その結果、小型ボードコンピュータを活用してエッジ/モバイルノードを試作し、ブロックチェーン上に配備された機械学習技術と連携する IoT/CPS 基盤を構築し、その基盤を活用して現実空間の状態を観測するシステムを設計・試作した。

5. 主な発表論文等

〔雑誌論文〕 計3件（うち査読付論文 3件 / うち国際共著 0件 / うちオープンアクセス 2件）

1. 著者名 Hasegawa Yuki, Yamamoto Hiroshi	4. 巻 10
2. 論文標題 Reliable IoT Data Management Platform Based on Real-World Cooperation Through Blockchain	5. 発行年 2021年
3. 雑誌名 IEEE Consumer Electronics Magazine	6. 最初と最後の頁 82 ~ 92
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/MCE.2020.3011646	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 INTHARAWIJITR Krittin, IIDA Katsuyoshi, KOGA Hiroyuki, YAMAOKA Katsunori	4. 巻 E104.B
2. 論文標題 Empirical Study of Low-Latency Network Model with Orchestrator in MEC	5. 発行年 2021年
3. 雑誌名 IEICE Transactions on Communications	6. 最初と最後の頁 229 ~ 239
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2020NVP0005	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 INTHARAWIJITR Krittin, IIDA Katsuyoshi, KOGA Hiroyuki, YAMAOKA Katsunori	4. 巻 E102.B
2. 論文標題 Simulation Study of Low-Latency Network Model with Orchestrator in MEC	5. 発行年 2019年
3. 雑誌名 IEICE Transactions on Communications	6. 最初と最後の頁 2139 ~ 2150
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2018EBP3368	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 -

〔学会発表〕 計13件（うち招待講演 0件 / うち国際学会 3件）

1. 発表者名 三橋力麻, 金勇, 品川高廣, 飯田勝吉, 高井昌彰
2. 発表標題 機械学習による不審なDoH 通信検出システムに関する一検討
3. 学会等名 2021年電子情報通信学会総合大会
4. 発表年 2021年

1. 発表者名 小宮 迅人, 山本 寛
2. 発表標題 ブロックチェーンを活用したIoTネットワーク異常検知システムの検討
3. 学会等名 電子情報通信学会コミュニケーションクオリティ研究会
4. 発表年 2021年

1. 発表者名 小宮 迅人, 山本 寛
2. 発表標題 ブロックチェーンに記録されていた大規模データを対象とした高速処理技術の検討
3. 学会等名 2020年電子情報通信学会総合大会 ISS特別企画「学生ポスターセッション」
4. 発表年 2020年

1. 発表者名 Yuki Hasegawa, Hiroshi Yamamoto
2. 発表標題 Highly Reliable IoT Data Management Platform Using Blockchain and Transaction Data Analysis
3. 学会等名 2020 IEEE International Conference on Consumer Electronics (ICCE) (国際学会)
4. 発表年 2020年

1. 発表者名 長谷川 悠貴, 山本 寛
2. 発表標題 ブロックチェーンを活用した高信頼IoTデータ管理基盤の開発と評価
3. 学会等名 電子情報通信学会 インターネットアーキテクチャ研究会
4. 発表年 2019年

1. 発表者名 加藤 耕平, 野林 大起, 塚本和也, 池永 全志
2. 発表標題 時空間データ滞留方式におけるブロックチェーン技術を用いたデータトレース方式の提案
3. 学会等名 2020年電子情報通信学会総合大会
4. 発表年 2020年

1. 発表者名 Takuro Kamada, Hiroshi Yamamoto
2. 発表標題 Location Information Verification for Reliable Resource Collaboration in Sharing Economy
3. 学会等名 2023 IEEE International Conference on Consumer Electronics (ICCE) (国際学会)
4. 発表年 2023年

1. 発表者名 鎌田拓朗, 山本 寛
2. 発表標題 位置情報検証機能を備えた高信頼資源連携プラットフォームの開発と評価
3. 学会等名 電子情報通信学会 インターネットアーキテクチャ研究会
4. 発表年 2022年

1. 発表者名 Hayato Komiya, Hiroshi Yamamoto
2. 発表標題 Design of High-Reliability IoT System Delivery Platform Based on Blockchain and System Prototyping
3. 学会等名 2022 IEEE International Conference on Consumer Electronics (ICCE) (国際学会)
4. 発表年 2022年



1. 発表者名 小宮 迅人, 山本 寛
2. 発表標題 ブロックチェーンを活用した高信頼IoTシステム提供基盤の開発と評価
3. 学会等名 電子情報通信学会コミュニケーションクオリティ研究会
4. 発表年 2021年

1. 発表者名 鎌田 拓朗, 山本 寛
2. 発表標題 ブロックチェーンを活用した高信頼IoTデータ管理基盤の設計と車両管理を対象としたシステム試作
3. 学会等名 電子情報通信学会 ネットワークシステム研究会
4. 発表年 2021年

1. 発表者名 上田 純輝, 塚本 和也, 山本 寛, 野林 大起, 池永 全志
2. 発表標題 時空間データ滞留システム監査を目的とする多層化ブロックチェーンの提案
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 2021)
4. 発表年 2021年

1. 発表者名 上田 純輝, 塚本 和也, 山本 寛, 野林 大起, 池永 全志
2. 発表標題 多層化ブロックチェーンを用いた時空間データ滞留システム監査機構に関する研究
3. 学会等名 電子情報通信学会 ネットワークシステム研究会
4. 発表年 2021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	飯田 勝吉 (Iida Katsuyoshi) (00332768)	北海道大学・情報基盤センター・教授  (10101)	
研究分担者	塚本 和也 (Tsukamoto Kazuya) (20452823)	九州工業大学・大学院情報工学研究院・教授  (17104)	
研究分担者	野林 大起 (Nobayashi Daiki) (40632906)	九州工業大学・大学院工学研究院・准教授  (17104)	
研究分担者	池永 全志 (Ikenaga Takeshi) (50284716)	九州工業大学・大学院工学研究院・教授  (17104)	

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
---------	---------