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　 ４ 月 １６ 日現在

機関番号：３７１１１
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２６１

研究課題名（和文）コンテンツ指向型センサネットワークにおけるセキュアキャッシング手法の研究開発

研究課題名（英文）A study on secure caching scheme for information-centric wireless sensor networks

研究代表者
森　慎太郎（Mori, Shintaro）

福岡大学・工学部・助教

研究者番号：９０７３４９１３

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：次世代インターネット技術として注目されている情報指向ネットワークを無線センサネットワークに導入する場合に必須であるセキュアデータ共有技術を実現するために、ブロックチェーンを用いた手法を開発した。提案手法は検証者の投票によるデータ検証方式を採用することにより、ハードウェアに制約のあるデバイスでも展開できる設計としている。また、テストベッドの開発および実機を用いた実証実験を通じた評価を行い有効性の検証を実施した。

研究成果の学術的意義や社会的意義
本研究開発が対象とする情報指向無線センサネットワークの研究領域は新規性が高い。本研究開発では、ブロックチェーンを用いたセキュアキャッシング手法だけでなく、提案手法を支える周辺技術（パケット分割・協力通信・グリーン化）の検証を、ハードウェア装置を用いた実証実験も併用して実施することにより、後続する新たな研究課題の創出・発展に貢献し有意な知見を与えられた。また、本研究開発の中核を担う論文に対し谷萩隆嗣記念特別賞（信号処理学会）に選出されるなど高い評価を受けた。

研究成果の概要（英文）：This study investigates a blockchain-based secure data caching scheme for information-centric wireless sensor networks, known as post-Internet technology. The proposed scheme is applicable to resource-limited node devices thanks to a novel voting-based verification method. The effectiveness of the scheme was demonstrated based on both computer simulations and hardware-based experiments.

研究分野：無線ネットワーク

キーワード：無線センサネットワーク　情報指向ネットワーク　ブロックチェーン　セキュアキャッシング

１．研究開始当初の背景

今日、無線センサネットワークは我々の身近な領域に幅広く普及し、そのセンシングデータの取り扱いに関して、莫大な量であるがゆえに効率化が求められているとともに、デリケートな個人情報をセキュアに取り扱う必要性にも迫られている。このような状況では、もはやデータをどこから取得するかは問題ではなく、何のデータを取得するかという点が問題の核心である。情報指向ネットワーク（ICN; Information-Centric Networking）は次世代のインターネットアーキテクチャとして研究開発が進められている。そこで、無線ネットワーク（WSN; Wireless Sensor Network）に対しても、本設計を拡大させ、一貫したネットワークアーキテクチャを実現させるべきである。情報指向無線センサネットワーク（ICWSN; Information-Centric Wireless Sensor Network）は、情報提供に際して場所に依存しない構成を実現できため、ノードが移動することが前提にある WSN においては大きな利点となるため本研究開発は有意義である。

２．研究の目的

先述した状況を鑑みて、本研究では、ICN と呼ばれている場所（アドレス）に依存しない新しいネットワークアーキテクチャを無線センサネットワークに導入することに焦点をあてる。このとき、とくに、それを実現するために必要不可欠なキャッシング手法に対して、ブロックチェーンに基づく分散台帳による相互認証の考え方を導入することを目的とする。

３．研究の方法

ICWSN におけるキャッシュデータをセキュアに取り扱えるようにするフレームワークを開発することを最大の目的としている。これを実現するために、ブロックチェーンにより実現できる機能を無線センサネットワークに応用する場合のシナリオとして問題設定を行い、それらの解決を図る。具体的には、プロトコル設計、計算機シミュレーション、および簡易なテストベッドを用いた基本的かつ初期的な評価を行う。それにより、ブロックチェーンを無線センサネットワークに導入するために浮上する問題点を洗い出し、それを解決する糸口を提供することを図る。

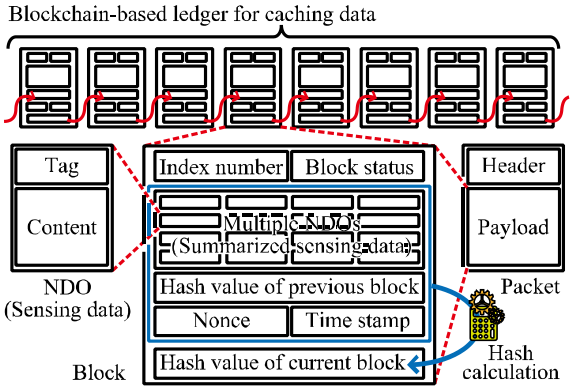

図１　セキュアキャッシングを実現するためのブロックチェーン構成と ICN パケット様式

４．研究成果

(1) セキュアキャッシング手法

積極的なオフパスキャッシングよるキャッシング対象ノード数の増大は、セキュアデータの不必要な拡散という点において課題が残る。そこで自律分散ネットワークとして設計された ICWSN への親和性を鑑み、ブロックチェーンに基づく分散台帳の導入を試みた。ブロックチェーンは集中制御によらない相互認証が可能なため、自律・分散・スケーラブルな構成を実現でき、合意形成アルゴリズムは構成ノード同士に信頼関係がなくても成立するので、ICWSN におけるアドホックネットワークとしての側面にも適している。そこで、セキュアキャッシング手法の中でも第三者によるキャッシュデータが書き換える（キャッシュ汚染）攻撃に対処可能な手法を提案した。本手法は計算機シミュレーションおよび試作機を用いて評価した（図 1-3）。

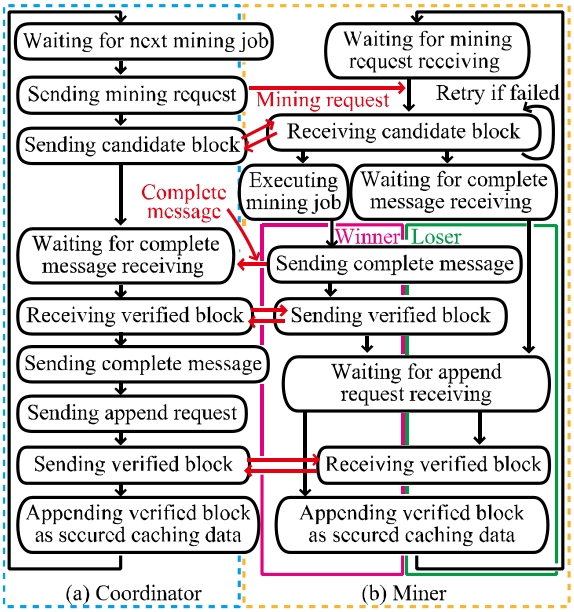

図２　実装したコーディネータとマイナーにおいて内部遷移フローと外部メッセージに対する処理手順

(2) ブロック認証手法の改良

前節で使用したブロックチェーンのコンセンサス手法は、ビットコインや代替

の典型的な暗号通貨で用いられている PoW（Proof-of-Work）方式を採用している。すわなち、新規ブロックに対しブロックチェーンを共有するメンバ間でマイニングに基づきコミットする。しかしブロック認証プロセスでは多量の演算（特定のハッシュ値を得るための総当たり計算）を行う必要があるため、ハードウェアに制約がある WSN を構成するデバイスには適しておらず、その実現性の面において課題がある。

そこで投票ベースの新たなブロック認証手法を提案した。提案手法は、Validator と呼ぶ検証ノードの大多数の承認によってブロックチェーンに追加するべきブロックを決定している点を新規性として主張し、UAV はデータ収集者としての役割だけではなく、Validator としても働く点に特徴がある。また UAV 間のアドホック無線伝送の過程でブロック認証が可能であり、ビットコインのリワードやイーサリアムのガスに相当するブロック認証に必要な取引手数料の交換機構も不要である利点も有する。またブロックに対してハッシュチェーンに基づくブロック署名手法、およびプロトコル設計についても検討した。また、本手法の画期的な理由として、本手法を採用することにより、本件研究開発において、当初計画で想定していた設計に頼らなくても、それだけですべてをまかなえる点にある。

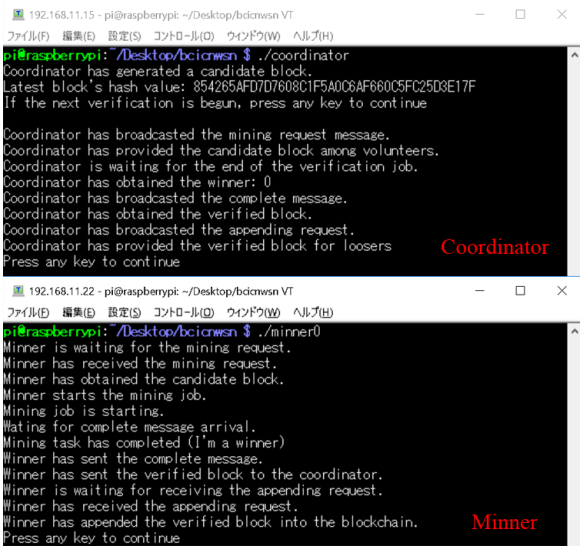

図 3　テストベッドを用いた動作検証中の表示画面

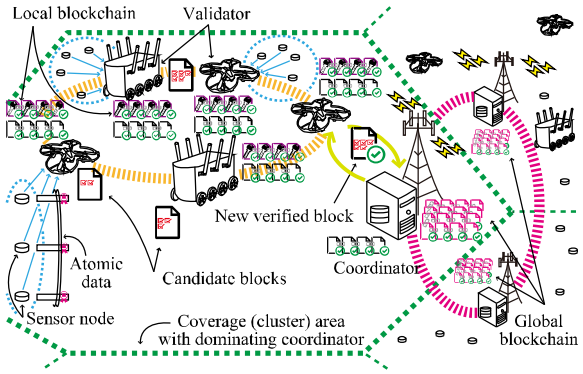

図 4　新たなブロック認証システムの概観

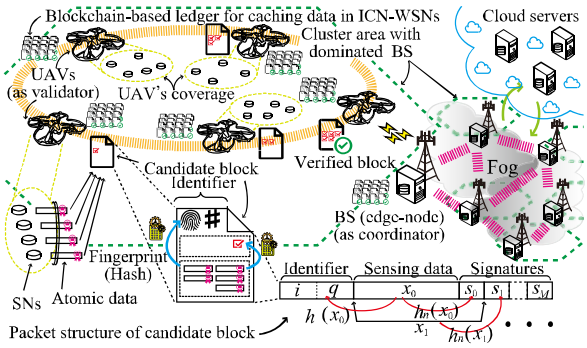

図 5　投票方式に基づくコンセンサス手法における データ処理手順・ハッシュチェーンによる署名の概観

(3) デバイス開発と評価

実フィールドでの実証実験・評価に先立ち、前節で実装した試作機と同じ構成（Raspberry Pi 4 [Quad-core CPU (ARMv8), 8GB RAM, Raspbian (buster) OS]）を用いてテストデバイスを実装した。試作機は Raspberry Pi 4 に LTE 接続のため 4GPi を組合わせ、ICN プラットフォームは ICN/CCN ベースのオープンソースソフトウェアである Cefore を使用した。Cefore では、cefnetd および csmgrd と呼ばれるデーモンプロセスにより、前者はパケット転送機能、後者はキャッシュ機能を提供する。センシングデータとして画像データを想定し、OpenCV から制御する USB3.0 で本体に接続したウェブカメラ(Logicool 社製 C270n)を用いて画像撮影のうえ、画像ファイルはローカルストレージに保存するとともに Cefore に対し cefputfile コマンドを用いてコミットする処理を Python 言語で実装した。一連の処理プログラムは cron を用いて毎分定期実行させ、cefputfile コマンドにより登録されたデータは csmgrd デーモンプロセスによりテストベッド上の RAM にキャッシュされ、300 秒を過ぎたキャッシュデータは FIFO アルゴリズムに従い削除されるように設定した。

本試作デバイスを実験室において長期運用テストを行ったところ、長時間の安定稼動に課題が残ることが明らかになった。具体的には、連続稼働中に突然ネットワークが切断される、定期実行が突然に動作しなくなる、外部ネットワークからのリモートアクセス中に本体がフリーズする症状が生じた。その問題を解決するために、産業用の組込みコンピュータとして実績のあるアドバンテック株式会社の MIC-710 AIX [Dual-core CPU (ARMv8.2), 8GB RAM, Ubuntu 18.04 with Jet Pack OS] に換装することにより抜本的な解決を図った（図 6）。MIC-710 AIX のプラットフォームは、NVIDIA Jetson Xavier NX を採用し設計されているため、これまでの試作機で実装した環境を容易に移植することができる利点がある。また、既存プロトコルとの互換性に関して、ユーザが ICWSN のプロトコルに対応していない場合に備えて、ゲートウェイがエンドユーザ

とブローカの間でセンシングデータの受渡しや制御メッセージの交換を行う仕組みを実装した。図 7 に HTTP-ICN 間の手続きに従い，本稿では Perl 言語を用いて、Gateway 上に CGI（Common Gateway Interface）として実装した。

開発したノードデバイスの実証評価のために、図 8(a)に示すネットワークを構築した。併せて、図 8(b)に示すように Broker および Gateway に FIB を設定し、BS および Broker にキャッシュ機能を具備した。表 1 に同一コンテンツを取得した場合におけるスループットおよび平均ジッタを示す。とくに Broker に対しキャッシュ機能を持たせることにより、2 回目以降のデータ取得に関して系においてボトルネック区間である無線区間のデータ伝送を削減できるため、キャッシュデータの提供による安定したコンテンツ取得が実現できる点が示されている。なお、レイテンシ（Ping 値）は、82.9 ms（BS-Broker）、0.399 ms（Broker-Gateway）、44 ms（Gateway-End-user）であった。図 9 は ICWSN に対応していない端末において、互換性を担保する仕組みを提供するプログラムを介してアクセスした結果である。結果より所望通りの動作が実現できていることが示されている。

(4) 提案手法を支える通信方式の検討

提案 ICWSN を耐災害スマートシティに導入することを想定し、それを支える下位レイヤプロトコルの検討を行った。具体的には、MAC（Media Access Control）レイヤにおいて、上位レイヤのパケットを複数のフレーム分割する場合、消去訂正符号化されたサブフレームを用いることにより、すべてのサブフレームが揃わなくても元のパケットを復元できることを目指し、基礎的な評価を行った。とくに欠損したサブフレームを近隣ノードから取得することにより、再送手続きを削減できる点が特徴である。また適用先アプリケーションにおいて、チャネル容量に関する問題を解決するために、送信側の協力通信とデュアルバンド対応ノードを利用することを検討した。両技術を導入することにより、計算機シミュレーションの結果、従来の WSN 向け無線通信システムでは対処できないと想定していた、多数ノードが散在する環境におけるシナリオに対し実現可能性を示した。また、実際の耐災害スマートシティのソリューションとして、河川モニタリングシステムの画像取得部分に対し、ICWSN の適用可能性を評価するために本テストベッドをベースに改良し動作検証を実施した。

図 6　開発したノードデバイス

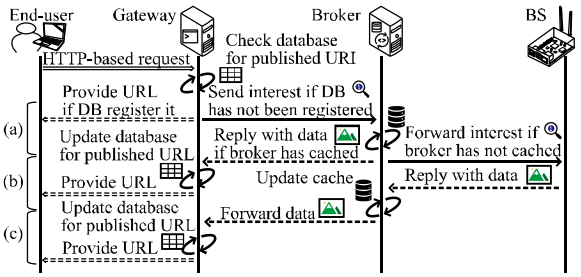

図 7　HTTP-ICN プロトコル変換手続き

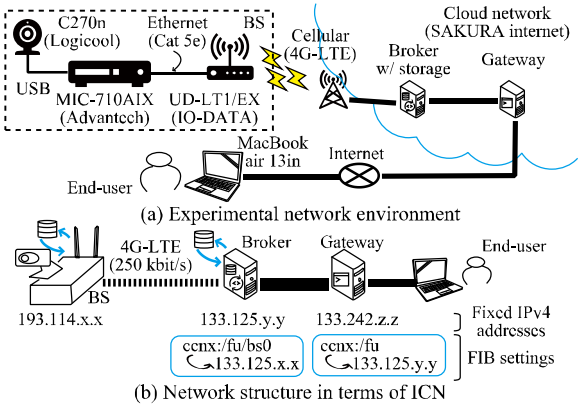

図 8　テストネットワークモデル

表 1　実験結果

Trial	Throughput (kbit/s)	Average jitter (μs)
1	331	25,400
2	89,200	90.6
3	89,600	90.2
4	87,500	95.4

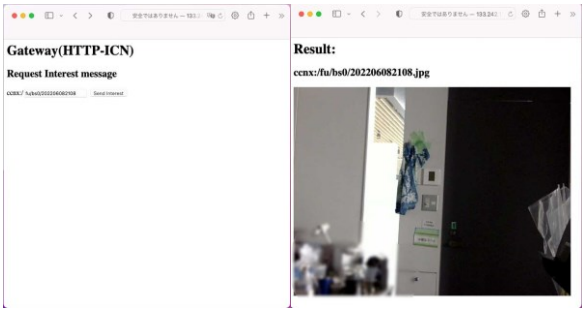

図 9　ユーザ端末の表示例

(5) ネットワーク符号・肯定的干渉による ICWSN を支える無線ネットワークプロトコルの検討

ICWSN の下位レイヤにおいては、フラッディング（ブロードキャスト）に基づき無線データ伝送がなされる。そのため、ICN ベースのネットワークプロトコルと親和性の高い下位レイヤプロトコルとして、新たな無線通信技術の開発が不可欠である。そこで、協力通信に基づく ICWSN を支える MAC レイヤ・PHY レイヤ技術を検討した。提案手法は中継ノードによる重複伝送によるパ

スダイバーシチの効果を狙い、ネットワークコーディング（NC; Network Coding）手法による伝送効率の改善を図った。本貢献としては、中継ノードの他にアシストノードが介在するリレー伝送において、それらのノード周辺に生じるパケット衝突に対し、肯定的干渉（Constructive Interference）現象に基づく干渉の低減を図る点にある。一般的な WSN においては、デバイス簡素化のため、積極的な端末間同期・衝突回避の機構を簡略化されうる。このとき、ある特定エリアにおける NC データ干渉は、複数の送信側ノードからのベースバンド信号の重ね合わせを受信側ノードが検出できれば、その干渉の影響を無視できる。すなわち、許容範囲内の位相のずれた複数の搬送波信号を重ね合わせることにより、受信側において高い確率で正しい検出が可能となる。とくに、ICWSN のフラッディング通信に対して本技術は特に有効であると考え、深刻な衝突がないパケット伝送の実現に向けて組入れた。

(6) ICWSN によるグリーン化の効果

本研究開発の導入によって得られる副次的な利点としてシステムのグリーン化が挙げられる ICWSN においては、個々のデータに対し、アドレスではなく名前付きデータとして取扱う点、キャッシング技術によるデータ転送量削減・伝送遅延低減に特徴がある。そのため、ICWSN におけるデータの授受によって、データ伝送距離の低減（キャッシング設計）や不必要なデータ伝送の削減（プル型ネットワーク設計）により、システム全体の消費電力の削減に寄与できる余地があることが明らかとなった。また付随的に、無線データ伝送量の削減による電波の有効利用も達成可能である。しかし ICWSN を構成するノードデバイス（末端）では、バッテリー制約、計算機資源などのハードウェア資源の制約、有線ネットワークと比較して貧弱な無線通信環境という状況の中、有線ネットワークを対象として設計されてきた技術を、そのまま ICWSN に適用させることは困難であり解決するべき技術課題が残っている。本研究課題を通じて、本節で述べる新たな研究テーマを生み出す成果を得た。

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　3件）

１．著者名 S. Mori	４．巻 15
２．論文標題 A Cooperative and Coded Communication Scheme using Network Coding and Constructive Interference for Information-Centric Wireless Sensor Networks	５．発行年 2022年
３．雑誌名 International Journal on Advances in Networks and Services	６．最初と最後の頁 54-61
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 S. Mori	４．巻 26
２．論文標題 Secure Caching Scheme using Blockchain for Unmanned Aerial Vehicle-assisted Information-Centric Wireless Sensor Networks	５．発行年 2022年
３．雑誌名 Journal on Signal Processing	６．最初と最後の頁 21-31
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 S. Mori	４．巻 14
２．論文標題 Data Collection Scheme using Erasure Code and Cooperative Communication for Deployment of Smart Cities in Information-centric Wireless Sensor Networks	５．発行年 2021年
３．雑誌名 International Journal on Advances in Networks and Services	６．最初と最後の頁 54-64
掲載論文のDOI（デジタルオブジェクト識別子） なし	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14件（うち招待講演　6件／うち国際学会　7件）

１．発表者名 森慎太郎
２．発表標題 情報指向無線センサネットワークのテストベッド試作と基礎評価
３．学会等名 電子情報通信学会技術報告SeMI研究会
４．発表年 2022年

１．発表者名
Shintaro Mori

２．発表標題
(Keynote) Information-Centric Wireless Sensor Network: A Study and a Survey

３．学会等名
IARIA Congress 2022（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
森慎太郎

２．発表標題
(チュートリアル) グリーン情報指向無線センサネットワーク実現のための高効率・省電力化に関する一検討

３．学会等名
信学総大 2023（招待講演）

４．発表年
2023年

１．発表者名
Shintaro Mori

２．発表標題
Prototype Development of River Velocimetry using Visual Particle Image Velocimetry for Smart Cities and Disaster Area Networks

３．学会等名
Proc. 20th International Symposium Communication and Information Technology（国際学会）

４．発表年
2021年

１．発表者名
Shintaro Mori

２．発表標題
A Fundamental Analysis of an Erase Code-enabled Data Caching Scheme for Future UAV-IC-WSNs

３．学会等名
Proc. IARIA the 20 th International Conference on Networks（国際学会）

４．発表年
2021年

１．発表者名
Shintaro Mori

２．発表標題
Survey on unmanned aerial vehicle-assisted information-centric wireless sensor networks for smart city applications

３．学会等名
Proc. IARIA the 20 th International Conference on Networks（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
森 慎太郎

２．発表標題
情報指向無線センサネットワークにおいてブロックチェーンを用いてセキュアキャッシングを実現するための一検討

３．学会等名
電子情報通信学会 技術報告 SeMI研究会

４．発表年
2021年

１．発表者名
森 慎太郎

２．発表標題
情報指向無線センサネットワークに関する一研究

３．学会等名
電子情報通信学会 総合大会（チュートリアルセッション）（招待講演）

４．発表年
2022年

１．発表者名
Shintaro Mori

２．発表標題
A Fundamental Analysis of Caching Data Protection Scheme using Light-weight Blockchain and Hashchain for Information-centric WSNs

３．学会等名
Proc. 2nd Conf. Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020)（国際学会）

４．発表年
2020年

１．発表者名
森慎太郎

２．発表標題
コンテンツ指向型無線センサネットワークにおけるセキュアキャッシング手法に対するテストベッドの試作と基礎評価

３．学会等名
子情報通信学会 技術報告 センサネットワークとモバイルインテリジェンス（SeMI）研究会

４．発表年
2019年

１．発表者名
Shintaro Mori

２．発表標題
(Invited) Secure and Effective Caching Scheme using Blockchain for Information-centric Wireless Sensor Networks

３．学会等名
Asia Pacific Society for Computing and Information Technology (APSCIT) 2019 Annual Meeting（招待講演）

４．発表年
2019年

１．発表者名
森慎太郎

２．発表標題
(依頼講演)コンテンツ指向型センサネットワークにおける高効率・セキュアキャッシング手法の研究

３．学会等名
電子情報通信学会 技術報告 センサネットワークとモバイルインテリジェンス（SeMI）研究会（招待講演）

４．発表年
2019年

１．発表者名
Shintaro Mori

２．発表標題
Caching Data Protection Scheme for Information-Centric Wireless Sensor Networks

３．学会等名
IARIA the 19-th Int. Conf. Networks (ICN 2020)（国際学会）

４．発表年
2020年

１．発表者名
Shintaro Mori

２．発表標題
A Study on Zero-touch-design Information-centric Wireless Sensor Networks

３．学会等名
IARIA the 22th Int. Conf. Networks (ICN 2023)（国際学会）

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
科研費プロジェクト　コンテンツ指向型センサネットワークにおける セキュアキャッシング手法の研究開発
https://cross-layer.com/kaken19K20261.html

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

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