日本学術振興会に紙媒体で提出する必要はありません。

様　式　C－7－1

令和元年度科学研究費助成事業（科学研究費補助金）実績報告書（研究実績報告書）

機関番号	14603

所属研究機関名称		奈良先端科学技術大学院大学
研究代表者	部局	先端科学技術研究科
	職	教授
	氏名	笠原　正治

1．研究種目名　基盤研究(A)(一般)　　2．課題番号　19H01103

3．研究課題名　超スケーラブル汎用ブロック・チェーン技術に向けた情報学的研究

4．研究期間　令和元年度～令和４年度　　5．領域番号・区分　－

6．研究実績の概要

今年度は以下の3項目について研究成果を得た.
(1)ブロック・チェーンを応用したIoTアクセス制御技術：IoTシステムに対するセキュリティ保証技術として， Ethereumのスマートコントラクトを応用したアクセス制御方式を検討した．具体的には，CapBACとABACの二種類のアクセス制御についてスマートコントラクトを用いた方式を提案し，実証実験を通じて機能動作を確認するとともに，使用で発生するコストについて定量的な評価を行い，従来手法に対する優位性を検証した．また，次世代分散台帳技術であるIOTAを応用したIoTアクセス制御技術についても検討を行った．ここでは属性ベース暗号技術のCP-ABEを用いたアクセス制御方式を検討し，プロトタイプの実装を通じて提案方式の実証実験を行い，提案方式が有効に機能することを確認した.
(2)高速データ通信を実現するP2P技術の検討：P2Pファイル配信技術の高速化に向けた基礎的検討として，Tit-for-Tat（TFT）戦略と呼ばれるピア間データ交換促進手法に着目し，TFT型P2Pファイル配信における配信時間の最小化問題を線形計画問題として定式化してピア数やサーバ・ピア間のアップロード容量が最小配信時間に与える影響を定量的に分析した.
(3)ビットコインにおけるセキュリティ向上方策：ビットコインにおいて，特定のマイナーが複数の攻撃者と結託し，競合するマイナーの生成したブロックの拡散を妨害する，ブロック拡散妨害攻撃が知られている．ここでは推定ダウンロード速度に基づくブロック取得先ノード選択方式を検討し，計算機シミュレーションにより，提案手法の有効性を定量的に評価した．その結果，悪意あるノードの妨害攻撃下においてネットワーク帯域に変動が生じたとしても通常ノードが適切なノードを選択して迅速かつ正常にブロックを取得できることが確認された.

7．キーワード

ブロック・チェーン　DSSトリレンマ　低遅延P2Pネットワーク　高速ブロック同期　IoTアクセス制御

8．現在までの進捗状況

区分　(2) おおむね順調に進展している。

理由
本年度はブロック・チェーンにおけるセキュリティ脆弱性，簡潔データ構造の応用，IoTアクセス制御方式への応用について研究を進め，順調に進展している.
(1)セキュリティ脆弱性については，ビットコインを対象に，マイニング成功時に行われる承認ブロックのネットワーク伝搬を妨害するブロック拡散妨害攻撃，およびマイニングプールにおいて悪意ある参加者がマイニングに成功しても所属プールに通知しないBlock Withholding Attackの二種類について検討を行った．ブロック拡散妨害攻撃については，ビットコイン・ブロック・チェーンのブロック送受信プロトコルを模擬したシミュレータを開発し，妨害を行うノードの割合やネットワークにおける配置がブロック伝搬に与える悪影響を定量的に評価した．また，ブロック拡散妨害攻撃を防ぐための方策として，正常なブロック取得が期待される隣接ノードを選択する手法を検討し，計算機シミュレーションを通じて提案手法の有効性を明らかにした.
(2)簡潔データ構造を用いたブロック・チェーン技術では，情報を理論的下限まで圧縮しつつ，ブロックの探索や親子関係の計算等の必要な演算を高速に行えるデータ構造を用いて，DAG型ブロック・チェーンを表現する最適なデータ構造の設計を行った．また，その理論的な情報量の下限の解析を行った.
(3)ブロック・チェーンを応用したIoTアクセス制御方式では，Ethereumのスマート・コントラクトを応用し，CapBACおよびABACの二種類のアクセス制御方式を開発するとともに，実証実験を通じて有効性を確認した．また，近年IoT応用として注目されている分散台帳技術であるIOTAに着目し，IOTAの通信プロトコルMAMと属性ベールの暗号技術CP-ABEを組み合わせた高度なセキュリティ保証型通信技術を提案し，実機による実装と実証実験を通して手法の有用性を確認した.

９．今後の研究の推進方策

(1)フォークメカニズムの数理的解明：フォークの発生は，合意形成アルゴリズムの処理速度とP2Pネットワークの伝搬遅延に起因するが，合意形成にかかる時間やP2Pの物理網・論理網のトポロジー構成，物理リンク特性，通信プロトコルがフォーク発生パターンやセキュリティ強度に与える影響については詳しいことはわかっていない．ここでは合意形成アルゴリズムとP2Pネットワークの特性がフォーク発生に与える影響を，数理的分析と大規模シミュレーション実験により定量的かつ多角的に分析を行う．
(2)超低遅延P2Pネットワーキング：参加ノード間での高速なブロック同期のためには，承認ブロックデータを全ての参加ノードに高速ブロードキャストする必要がある．ブロック転送遅延を抑制するため，ここでは任意の2ノード間で短いブロック転送遅延を実現するP2Pネットワーキング技術を検討する．具体的には，物理リンクの伝搬遅延を考慮しつつ任意の2ノード間でのブロック転送遅延を最小化するP2Pトポロジー構成法を検討する．
(3)先進的データ構造を用いたブロック・チェーン技術：ここでは簡潔データ構造と呼ばれる，情報理論的に最小までデータ量を圧縮しつつ，トランザクション情報の参照や真正性検証に必要な検索を，データの展開無しに高速に行える圧縮データ構造を設計し，簡潔データ構造を用いたブロック・チェーン・データの表現法や高速な更新方法について検討を行う．
(4)IoTアクセス制御技術：IOTAフレームワークによるIoTアクセス制御方式では，不正にトークンを入手したユーザによる不正アクセスを検出・防止できないという問題点があるため，その対策について検討を行う．また，CapBACのようなトークン更新による権限の削除機能を可能にすること，及び既存手法との性能比較を通して実用性の検証についても行う．

１０．研究発表（令和元年度の研究成果）

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著論文　0件／うちオープンアクセス　1件）

１．著者名 Nakamura Yuta、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji	４．巻 20
２．論文標題 Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things	５．発行年 2020年
３．雑誌名 Sensors	６．最初と最後の頁 1793～1793
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s20061793	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 Nakamura Yuta、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji	４．巻 -
２．論文標題 Capability-Based Access Control for the Internet of Things: An Ethereum Blockchain-Based Scheme	５．発行年 2019年
３．雑誌名 IEEE GLOBECOM 2019	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/GLOBECOM38437.2019.9013321	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 Yutaka Mirei、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji	４．巻 -
２．論文標題 Using Ethereum Blockchain for Distributed Attribute-Based Access Control in the Internet of Things	５．発行年 2019年
３．雑誌名 IEEE GLOBECOM 2019	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/GLOBECOM38437.2019.9014155	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 Nishi Yohei、Sasabe Masahiro、Kasahara Shoii	4．巻 -
2．論文標題 Impact of Locality-awareness on Tit-for-Tat-based P2P File Distribution	5．発行年 2020年
3．雑誌名 IEEE Consumer Communications & Networking Conference 2020 (IEEE CCNC 2020)	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/CCNC46108.2020.9045338	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7件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 藤田 健太郎，張 元玉，笹部 昌弘，笠原 正治
2．発表標題 Block Withholding Attackが存在する場合のマイニングプール選択問題
3．学会等名 電子情報通信学会技術研究報告 (NS2019-189)，pp. 71-76，2020.3.5.
4．発表年 2020年

1．発表者名 豊 美玲，張 元玉，笹部 昌弘，笠原 正治
2．発表標題 Ethereumブロックチェーンを用いたIoT向け分散型属性ベース・アクセス 制御方式のコスト評価
3．学会等名 電子情報通信学会技術研究報告 (NS2019-189)，pp. 77-82，2020.3.5.
4．発表年 2020年

1．発表者名 山本 将成，笹部 昌弘，張 元玉，笠原 正治
2．発表標題 ビットコインネットワークにおけるブロック拡散妨害攻撃への対抗策 ～推定ダウンロード速度に基づくブロック取得先選択～
3．学会等名 電子情報通信学会技術研究報告 (NS2019-191)，pp. 83-81，2020.3.5.
4．発表年 2020年

日本学術振興会に紙媒体で提出する必要はありません。

3版

1．発表者名 中西 瑠海，張 元玉，笹部 昌弘，笠原 正治
2．発表標題 IOTAに基づいたIoTアクセス制御方式の設計と実装
3．学会等名 電子情報通信学会技術研究報告（NS2019-230），pp. 295-300，2020.3.6.
4．発表年 2020年

1．発表者名 山本 将成，笹部 昌弘，笠原 正治，
2．発表標題 ビットコインネットワークにおけるブロック拡散妨害攻撃のリスク評価
3．学会等名 電子情報通信学会技術研究報告（CQ2019-88），pp. 1-6，2019.11.21.
4．発表年 2019年

1．発表者名 山本 将成，笹部 昌弘，笠原正治
2．発表標題 Bitcoin ネットワーク上でのブロック拡散遅延攻撃における攻撃者数の影響
3．学会等名 電子情報通信学会2019年ソサイエティ大会，講演論文集，B-11-10，2019.9.10.
4．発表年 2019年

1．発表者名 森 順平，川原 純，湊 真一
2．発表標題 次数制限付きハッセ図表現の情報理論的下限
3．学会等名 電子情報つ信学会技術研究報告（COMP2019-53），pp. 51-56，2020.3.
4．発表年 2020年

日本学術振興会に紙媒体で提出する必要はありません。

〔図書〕　計0件

１１．研究成果による産業財産権の出願・取得状況

計0件（うち出願0件／うち取得0件）

１２．科研費を使用して開催した国際研究集会

計0件

１３．本研究に関連して実施した国際共同研究の実施状況

―

１４．備考

超スケーラブル汎用ブロック・チェーン技術に向けた情報学的研究
http://www-lsm.naist.jp/blockchain-study