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　 ５ 月 ２５ 日現在

機関番号：１２６０１
研究種目：基盤研究(B)（特設分野研究）
研究期間：2017～2023
課題番号：１７ＫＴ００８１

研究課題名（和文）トラスト基盤におけるセキュリティ評価手法の工学的および経済学的研究

研究課題名（英文）Security Evaluation Methods in Trust Infrastructure Based on Engineering and Economics

研究代表者
松浦　幹太（Matsuura, Kanta）

東京大学・生産技術研究所・教授

研究者番号：００２９２７５６

交付決定額（研究期間全体）：（直接経費）　　14,300,000円

研究成果の概要（和文）：トラスト基盤におけるセキュリティ評価手法を工学的および経済学的に検討し、具体的に手法を開発して応用への知見を得るという目的を達成した。とくに、全ての項目にまたがる知見として、工学的なランダムネス発生源を、経済学的なトークンモデルにおける適合確率過程に利用できるだけでなく、ブロックチェーン上で稼働させる場合の検証証明（ブロックチェーンに記録された内容が正当であることを誰かが確かに検証した、という証拠）としても利用できる可能性を見出した。

研究成果の学術的意義や社会的意義
工学的研究では、高機能暗号技術に関して、とくに学術的意義の高い成果を得た。すなわち、ブロックチェーン上で実装した時にモデルが整合し、安全性の再評価をせず利用できる道を開いた。実際、主要な国内会議で学生論文賞を受賞し、主要な国際会議に２編採録され、うち１編は最優秀論文賞を受賞した。経済学的研究では、ブロックチェーンの消費電力を削減して社会受容性を高める研究へと発展する知見を得た。実際、社会的意義を第一に目指す後継プロジェクトがスタートしている。

研究成果の概要（英文）：In this project, we developed security evaluation methods in trust infrastructure from the viewpoints of both engineering and economics based on advanced but harmonized adversarial models. As planned, we obtained many implications for blockchain applications. In particular, as a generic implication related to all of the research items in this project, we found that the randomness source (e.g. a nonce in a DL-based digital signature) can be used for an adaptive stochastic process in the economic token models. In addition, it can be used as a Proof-of-Verification (PoV) which shows that someone certainly verified and validated the newly reported block. PoV is currently studied in a subsequent project on energy-efficient implementation of public blockchains towards better social acceptability.

研究分野：情報セキュリティ

キーワード：ブロックチェーン　トラスト基盤　暗号通貨　高機能暗号　プライバシー保護　セキュリティ経済学

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景
暗号通貨ビットコインの技術的基盤となるブロックチェーンは、金融機関間のネットワークに対して大きなイノベーションをもたらす可能性があると言われていた。また、ブロックチェーンの応用はフィンテックの範疇を超えると指摘されていると同時に、セキュリティを含む様々な性質の学術的な評価と検証はこれからの大きな課題とされていた。
ブロックチェーンの応用が広いとされる最大の理由は、費用対効果の高いトラスト基盤として機能するという期待があるからである。一方で、これが研究開始当初の時点で期待に過ぎなかったのはなぜかを考えると、前述の通り、学術的な評価と検証が不十分であることが大きな理由であった。

２．研究の目的
本研究は、トラスト基盤におけるセキュリティ評価手法を工学的および経済学的に検討し、具体的に手法を開発して応用への知見を得ることを目的とした。とくに、工学的研究においては、個々の技術に関しては汎用性を重視し、具体的なシステムに関しては公開性を重視することによって、それらに基づく評価の信頼性を最大化することを目指した。同じく、経済学的研究においては、理論モデルによる評価と実データによる検証を兼ね備えて、評価の信頼性を最大化することを目指した。

３．研究の方法
研究目的及び研究計画・方法の概要

研究目的
暗号通貨ビットコインの技術的基盤となるブロックチェーンは、金融機関間のネットワークに対して大きなイノベーションをもたらす可能性があると言われている。また、ブロックチェーンの応用はフィンテックの範疇を超えると指摘されていると同時に、セキュリティを含む様々な性質の学術的な評価と検証はこれからの大きな課題とされている。
ブロックチェーンの応用が広いとされる最大の理由は、費用対効果の高いトラスト基盤として機能するという期待があるからである。一方で、これが現時点で期待に過ぎないのはなぜかを考えると、前述の通り、学術的な評価と検証が不十分であることが大きな理由として挙げられる。本研究は、トラスト基盤におけるセキュリティ評価手法を工学的および経済学的に検討し、具体的に手法を開発して応用への知見を得ることを目的とする。

研究計画・方法
(1) まず、連携先と立ち上げているトラスト基盤のテストネットワークについて、ノードの整備を進める。また、理論研究を主体として、セキュリティ評価手法に関する工学的研究とセキュリティ経済学的研究を進める。ノードの整備においては、ソフトウェアの観点でもハードウェアの観点でも、ブロックチェーンに基づくトラスト基盤を稼働させる上でのミニマム・セットから始め、必要に応じて拡大するという手順を踏む。また、ネットワークとしても活動としても、グローバルなスケールで進展させる。
セキュリティ評価手法を開発する研究のうち、工学的研究は、２つの研究を柱に据えて進める。一つ目の柱は、暗号理論分野で証明可能安全性と呼ばれているアプローチである。本研究では、まず、この証明パターンを適用あるいは自然に拡張してブロックチェーン技術に基づくトラスト基盤の評価に役立てる技術を考えるために、高機能暗号の理論研究を行う。その際、とくに、安全性の帰着先に留意する。二つ目の柱は、広く IT 分野で用いられるようになってきた強力なツールに関して、革新的な利用手法を確立するアプローチである。具体的には、人工知能（AI）とセキュリティ評価の関係をテーマとして、理論研究と基礎的な実験的研究を行う。
同じく、経済学的な研究は、トラスト基盤とその応用に関わる利害関係者の体系化から開始する。とくに、トラスト基盤への脅威を意図的なものと意図的でないものに分けて考える。
(2) 研究期間の前半に上記(1)の研究を進めた上で、後半には以下のようにして完成度を高める計画であった。まず、前半の工学的研究の成果のうちトラスト基盤上にプロトタイプ実装可能なものを厳選し、実装評価する。ブロックチェーンと同じ層の実装を選ぶか、あえて切り離して上の層の応用サービスプロトコルとして実装するか、あるいは両方かについては、研究進捗状況を踏まえて柔軟に判断する。
次に、セキュリティ経済学的研究から導出した知見は、無意味に遅滞させることなく、テストネットワークの運用や活動で活用すべく成果を随時発信する。とくに、ブロックチェーンとその応用システムを構成するプロトコルのうち、どこまでをプロトコル一式（プロトコル・スイート）として考えるべきか明らかにして、テストネットワークの次のフェーズ（部分的な標準化）に反映させるべく成果の発信を行う。

４．研究成果

(1) テストネットワーク

連携先と立ち上げたトラスト基盤（ブロックチェーン）のテストネットワークにおいて、ノードの整備が順調に進んだ。具体的には、発足当初 6 つであったものが、30 個となった。しかも、グローバルなスケールで進展させるという計画通り、南北アメリカに 7 個、アジアに 9 個、ヨーロッパに 13 個、アフリカに 1 個という広がりを確保できた。また、関連するコミュニティの活動として、2019 年 6 月に福岡市で開催された G20 財務大臣・中央銀行総裁会議において金融分野におけるブロックチェーンに関するパネルセッション企画に協力した。その成果である共同コミュニケに基づいて異種関与者対話の活動 BGIN（Blockchain Governance Initiative Network）が始まり、特定テーマを扱うワーキンググループの活動、1 年間に３～４回程度の定期的な国際会議の開催、成果としてのドキュメントの発行といった形で、発展的に継続している。

(2) 高機能暗号の研究において、まず秘密鍵が漏洩した場合でも漏洩前の処理結果に悪影響が出ない鍵漏洩耐性の研究で完成度の高い成果を得た。成果発表の論文は、主要な国内会議で学生論文賞を受賞し、主要な国際会議に２編採録され、うち１編は最優秀論文賞を受賞した。これは、従来よりも広いクラスの漏洩に耐えられること、すなわち CALM（Continual Auxiliary Leakage Model）というモデルで安全性証明できたことが高く評価された結果である。安全性証明の帰着先は、数学的な問題としては典型的な公開鍵暗号と同様のものであって、トラスト基盤特有のものではない。しかし、鍵漏洩の影響に関する安全性定義においては必然的に時間軸を考慮することとなり、タイムスタンプシステムに源流があるブロックチェーンの上で実装に起因する問題を抑制できる成果を得ることができた。

さらに、高機能暗号の研究においては、プライバシーに配慮した技術開発を進めた。トラスト基盤としてのブロックチェーンに実装するアプリケーションには、複雑なプライバシー要件が課されるものが少なくない。中でも、サーバにクエリや入力の意味を開示せず所望の品質で情報検索や決定性有限オートマトンのタスクなどを実行させる仕組みは、応用範囲が広く、トラスト基盤との親和性が高い。そこで、本研究では、公開鍵型検索可能暗号やクエリの出し方にも匿名性を高める工夫をしたレンジクエリ型 PIR（Private Information Retrieval）方式に関して技術的な完成度の高い成果を出し、安全性定義に関する新たな知見とともに、複数のジャーナル論文を著した。

以上要するに、いくつかの高機能暗号技術に関して、ブロックチェーン上で実装した時にモデルが整合し、安全性の再評価をせず利用できる道を開く成果を得た。

(3) 工学的研究のもう一つの柱である人工知能のセキュリティに関しては、深層学習で使われる畳み込みニューラルネットワーク（Convolutional Neural Network, CNN）に対する攻撃と対策に関して、完成度の高い成果を得た。

CNN は、画像認識や音声認識、自然言語処理などへ応用した際に高い精度を出すことがわかってきたため注目を集めている。しかし一方で、CNN への入力データに微小な改変を加えることで出力を大きく誤らせることが可能な敵対的入力の存在が報告されており、CNN を実社会で用いる際に大きな脅威となることが予想される。この問題に対して頑健な識別器を構成するテクニックとして、敵対的入力も学習用データに加えて学習する「敵対的訓練（Adversarial Training）」と呼ばれる手法が提案されており、敵対的入力に対する耐性を向上させることが確認されている。本研究では、この敵対的訓練における問題点として副作用を指摘し、その対策法を提案した。具体的には、CNN に対して敵対的訓練を行うと（本来高い精度で識別できるはずの）ランダムノイズが乗ったデータに対する識別率が大きく減少してしまうことを指摘した。その問題を解決するためにランダムノイズを付加した画像も教師データに加えて学習する手法を提案し、計算機実験により提案手法の有用性を実証した。さらに、画像以外の対象を同様に論じる際の着眼点についても考察した。また、これらの議論がブロックチェーンを利用した分散環境でも成り立つことを考察し、適用可能性を確保した。

(4) 経済学的な研究では、暗号通貨よりもさらに広義のブロックチェーン応用プロトコルにおいて、リスク管理に有効な経済学的モデルの一般化を進めた。その結果、システムで扱われるトークンを 4 つの属性に着目してモデル化できることが明らかとなった。その詳しい内容を国際誌の招待論文や著書で発表した。とくに、適合確率過程という概念で一般化した属性が、暗号通貨を金融工学的に安定させるだけでなく、電子証拠物として本質的に新しい機能を実現することを示した。すなわち、その証拠が、過去のある時刻になって初めて生成された（つまり、十分新しい証拠である）ことをサポートできるようになった。

さらに、経済学的な研究では、「ブロックチェーンに追加する最新の記録（暗号通貨の場合には、取引情報）が正しいことを信頼できるか（正しいことを誰かが確かに検証した証拠があるか）定かでない」という問題を行動経済学的に分析して抽出した。さらに、工学的アプローチ（暗号技術）によって、問題解決方法を考案した。具体的には、ブロックチェーンのコンセンサスプロトコルに電子署名を実装する際に登場するランダムネス発生源を経済学的なモデルにおける適合確率過程と組み合わせ、従来のトラスト基盤に欠けていた検証証明（PoV: Proof-of-Verification）の機能を実現した。ただし、新型コロナウィルスの影響でネットワーク環境の管

理体制を十分組めなかったため、テストネットワークを活用した本格的な実装評価ではなくノードレベルでの評価にとどまった。他に、同じく工学的研究との橋渡しになる課題としてスマートコントラクトの不正分類に取り組んだ。こちらも、ノードレベルの評価で良好なパフォーマンスを確認した。
検証証明は、その後、ブロックチェーンにおける検証作業の冗長性を下げるために利用できることが分かった。その結果、本研究の後継であるプロジェクトにおいて、ブロックチェーンの消費電力を削減して社会受容性を高める研究へと発展している。

以上 4 つの研究項目における主な成果とそれらの関係は、図 1 のようにまとめることができる。すなわち、トラスト基盤におけるセキュリティ評価手法を工学的および経済学的に検討し、具体的に手法を開発して応用への知見を得るという目的を達成した。とくに、全ての項目にまたがる知見として、工学的なランダムネス発生源を、経済学的なトークンモデルにおける適合確率過程に利用できるだけでなく、ブロックチェーン上で稼働させる場合の検証証明（ブロックチェーンに記録された内容が正当であることを誰かが確かに検証した、という証拠）としても利用できる可能性を見出した。

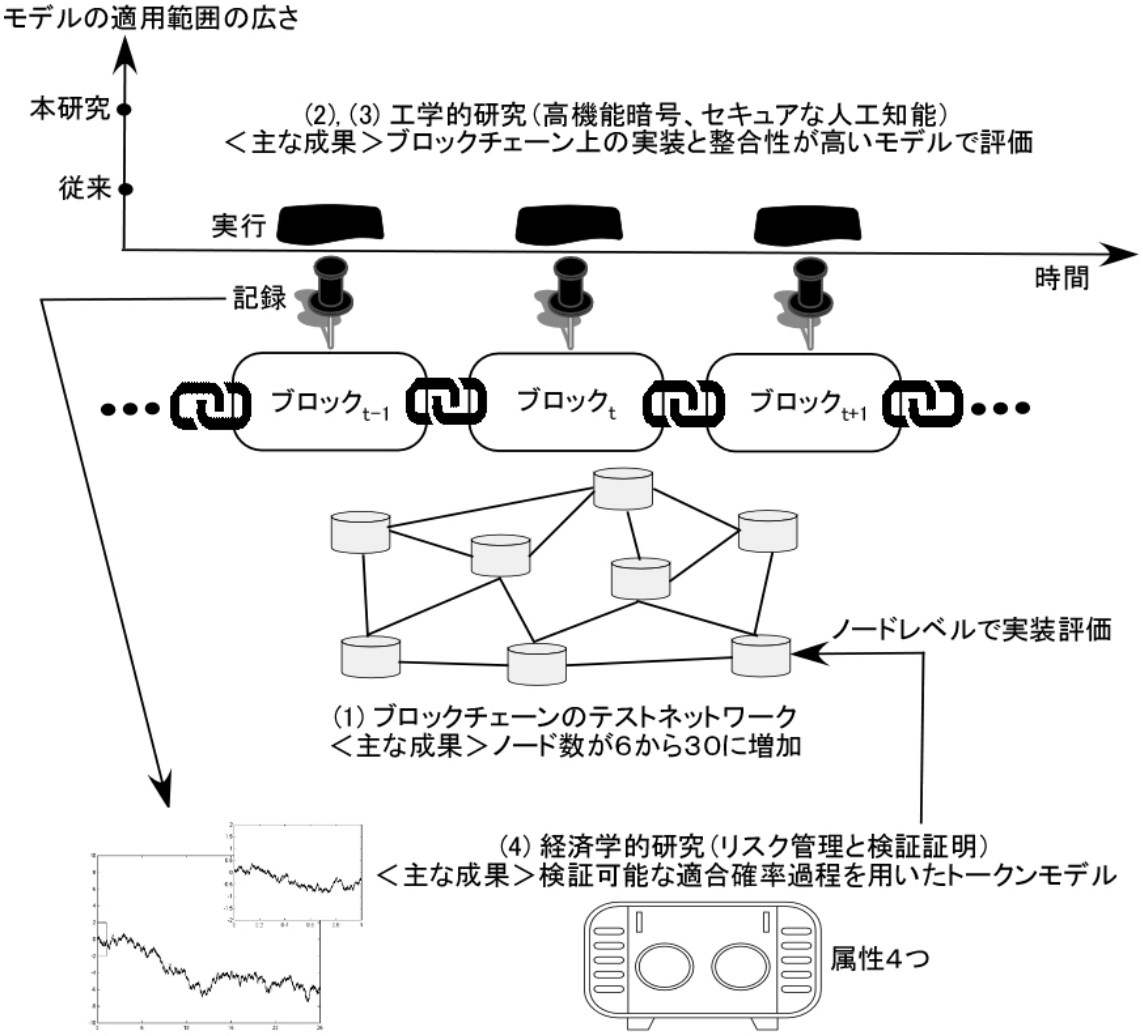

図 1．4 つの研究項目における主な成果とそれらの関係

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　12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 Kittiphop Phalakarn, Nuttapong Attrapadung, Kanta Matsuura	４．巻 13269
２．論文標題 Efficient Oblivious Evaluation Protocol and Conditional Disclosure of Secrets for DFA	５．発行年 2022年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 605-625
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-09234-3_30	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 Takeshi Miyamae, Kanta Matsuura	４．巻 7
２．論文標題 Coin Transfer Unlinkability Under the Counterparty Adversary Model	５．発行年 2022年
３．雑誌名 Ledger	６．最初と最後の頁 17-34
掲載論文のDOI（デジタルオブジェクト識別子） 10.5195/ledger.2022.260	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 Kittiphop Phalakarn, Vorapong Suppakitpaisarn, Nuttapong Attrapadung, Kanta Matsuura	４．巻 12835
２．論文標題 Evolving Homomorphic Secret Sharing for Hierarchical Access Structures	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 77-96
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85987-9_5	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 Ryu Ishii, Kyosuke Yamashita, Yusuke Sakai, Takahiro Matsuda, Tadanori Teruya, Goichiro Hanaoka, Kanta Matsuura, Tsutomu Matsumoto	４．巻 12809
２．論文標題 Aggregate Signature with Traceability of Devices Dynamically Generating Invalid Signatures	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 378-396
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-81645-2_22	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 Hayata Junichiro、Schuldt Jacob C. N.、Hanaoka Goichiro、Matsuura Kanta	4．巻 12309
2．論文標題 On Private Information Retrieval Supporting Range Queries	5．発行年 2020年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 674～694
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-59013-0_33	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 HAYATA Junichiro、KITAGAWA Fuyuki、SAKAI Yusuke、HANAOKA Goichiro、MATSUURA Kanta	4．巻 E104.A
2．論文標題 Equivalence between Non-Malleability against Replayable CCA and Other RCCA-Security Notions	5．発行年 2021年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 89～103
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0015	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 Junichiro Hayata, Masahito Ishizaka, Yusuke Sakai, Goichiro Hanaoka, Kanta Matsuura	4．巻 E103-A
2．論文標題 Generic Construction of Adaptively Secure Anonymous Key-Policy Attribute-Based Encryption from Public-Key Searchable Encryption	5．発行年 2020年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 107-113
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019CIP0014	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 Yuya Senzaki, Satsuya Ohata, Kanta Matsuura	4．巻 E103-D
2．論文標題 Simple Black-box Adversarial Examples Generation with Very Few Queries	5．発行年 2020年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 212-221
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019INP0002	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 Kanta Matsuura	４．巻 2019
２．論文標題 Security Evaluation Methods in Trust Infrastructure Based on Engineering and Economics	５．発行年 2019年
３．雑誌名 Impact	６．最初と最後の頁 24-26
掲載論文のDOI（デジタルオブジェクト識別子） 10.21820/23987073.2019.10.24	査読の有無 無
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 Masahito Ishizaka, Kanta Matssura	４．巻 11060
２．論文標題 Strongly Unforgeable Signature Resilient to Polynomially Hard-to-Invert Leakage under Standard Assumptions	５．発行年 2018年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 422-441
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-99136-8_23	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 Masahito Ishizaka, Kanta Matssura	４．巻 11124
２．論文標題 Identity-Based Encryption Resilient to the Auxiliary Leakage under the Decisional Linear Assumption	５．発行年 2018年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 417-439
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-00434-7_21	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 Kanta Matsuura	４．巻 E102-A
２．論文標題 Token Model and Interpretation Function for Blockchain-Based FinTech Applications	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 3-10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.3	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 Jun'ichiro Hayata, Masahito Ishizaka, Yusuke Sakai, Goichiro Hanaoka, Kanta Matsuura	４．巻 -
２．論文標題 Generic Construction of Adaptively Secure Anonymous Key-Policy Attribute-Based Encryption from Public-Key Searchable Encryption	５．発行年 2018年
３．雑誌名 Proceedings of the 2018 International Symposium on Information Theory and its Applications	６．最初と最後の頁 739-743
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40件（うち招待講演　8件／うち国際学会　6件）

１．発表者名 宮前剛，松浦幹太
２．発表標題 ゼロ知識性の概念を利用したブロックチェーン匿名通貨のプライバシー解析
３．学会等名 日本セキュリティ・マネジメント学会 第35回全国大会
４．発表年 2022年

１．発表者名 松浦幹太
２．発表標題 サプライチェーン応用におけるブロックチェーン研究の特徴と示唆
３．学会等名 JBAサステナビリティワークショップ（招待講演）
４．発表年 2022年

１．発表者名 五十嵐太一，松浦幹太
２．発表標題 スマートコントラクトにおけるセキュリティに関する調査
３．学会等名 2023年暗号と情報セキュリティ・シンポジウム(SCIS2023)
４．発表年 2023年

１．発表者名
Kanta Matsuura

２．発表標題
Energy-efficient Implementation of Consensus Algorithms by Minimizing the Redundancy of Signature Verification

３．学会等名
2022 IEEE 1st Global Emerging Technology Blockchain Forum（国際学会）

４．発表年
2022年

１．発表者名
松浦幹太

２．発表標題
ブロックチェーンの消費電力を抑えるProof-of-Verification

３．学会等名
4th Workshop Basing Blockchain

４．発表年
2021年

１．発表者名
石井龍，山下恭佑，宋子豪，照屋唯紀，坂井祐介，花岡悟一郎，松浦幹太，松本勉

２．発表標題
対話的追跡機能付き集約署名における署名送信間隔に関する制約と評価

３．学会等名
2022年暗号と情報セキュリティ・シンポジウム(SCIS2022)

４．発表年
2022年

１．発表者名
林リウヤ，浅野泰輝，林田淳一郎，松田隆宏，山田翔太，勝又秀一，坂井祐介，照屋唯紀，シュルツ・ヤコブ，アッタラパドゥン・ナッタポン，花岡悟一郎，松浦幹太，松本勉

２．発表標題
モノの電子署名: 物体に署名するための一検討

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム2021

４．発表年
2021年

１．発表者名
林リウヤ，浅野泰輝，林田淳一郎，松田隆宏，山田翔太，勝又秀一，坂井祐介，照屋唯紀，シュルツ・ヤコブ，アッタラパドゥン・ナッタポン，花岡悟一郎，松浦幹太，松本勉

２．発表標題
モノの秘匿性を考慮した「モノの電子署名」

３．学会等名
2022年暗号と情報セキュリティ・シンポジウム

４．発表年
2022年

１．発表者名
浅野泰輝，林リウヤ，林田淳一郎，松田隆宏，山田翔太，勝又秀一，坂井祐介，照屋唯紀，シュルツ・ヤコブ，アッタラパドゥン・ナッタポン，花岡悟一郎，松浦幹太，松本勉

２．発表標題
「モノの電子署名」の複数物体への拡張

３．学会等名
2022年暗号と情報セキュリティ・シンポジウム

４．発表年
2022年

１．発表者名
松浦幹太

２．発表標題
DXに希望をもたらす情報セキュリティとトラスト基盤

３．学会等名
JAPAN Security Summit 2021（招待講演）

４．発表年
2021年

１．発表者名
宮里俊太郎，松浦幹太

２．発表標題
内部のバイトコード実行を悪用したスマートコントラクトへの攻撃の早期検知

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム2020(CSS2020)

４．発表年
2020年

１．発表者名
Junichiro Hayata, Jacob C. N. Schuldt, Goichiro Hanaoka, Kanta Matsuura

２．発表標題
On Private Information Retrieval Supporting Multi-dimensional Range Queries

３．学会等名
2021年暗号と情報セキュリティ・シンポジウム(SCIS2021)

４．発表年
2021年

１．発表者名
石井龍，照屋唯紀，坂井祐介，松田隆宏，花岡悟一郎，松浦幹太，松本勉

２．発表標題
動的に不正署名を生成するデバイスを追跡可能な集約署名

３．学会等名
2021年暗号と情報セキュリティ・シンポジウム(SCIS2021)

４．発表年
2021年

１．発表者名
Kanta Matsuura

２．発表標題
Proof-of-Verification for Proof-of-Work: Miners Must Verify the Signatures on Bitcoin Transactions

３．学会等名
Scaling Bitcoin Workshop 2019（国際学会）

４．発表年
2019年

１．発表者名
Toshinori Usui, Yuto Otsuki, Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, Kanta Matsuura

２．発表標題
My Script Engines Know What You Did In The Dark: Converting Engines into Script API Tracers

３．学会等名
The 35th Annual Computer Security Applications Conference (ACSAC 2019)（国際学会）

４．発表年
2019年

１．発表者名
Takahiro Nagamine, Kanta Matsuura

２．発表標題
A New Protocol for Fair Addition of a Transaction Fee When Closing a Payment Channel Uncooperatively

３．学会等名
The 24th International Conference on Financial Cryptography and Data Security (FC2020)（国際学会）

４．発表年
2020年

１．発表者名
長嶺隆寛，松浦幹太

２．発表標題
ビットコインにおける手数料を考慮したオフチェーントランザクションの管理

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム2019(CSS2019)

４．発表年
2019年

１．発表者名
Ke Huang, Satsuya Ohata, Kanta Matsuura

２．発表標題
Privacy-Preserving Approximate Nearest Neighbor Search: A Construction and Experimental Results

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム2019(CSS2019)

４．発表年
2019年

１．発表者名
長嶺隆寛，松浦幹太

２．発表標題
非協力的なペイメントチャネル終了時の公平な手数料追加プロトコル

３．学会等名
2020年暗号と情報セキュリティ・シンポジウム(SCIS2020)

４．発表年
2020年

１．発表者名
Ke Huang, Satsuya Ohata, Kanta Matsuura

２．発表標題
Approximate Privacy Preserving Top-k Algorithm with Reduced Communication Rounds

３．学会等名
2020年暗号と情報セキュリティ・シンポジウム(SCIS2020)

４．発表年
2020年

１．発表者名
林田淳一郎, Jacob C. N. Schuldt, 花岡悟一郎, 松浦幹太

２．発表標題
A Private Information Retrieval Scheme Supporting Range Queries

３．学会等名
2020年暗号と情報セキュリティ・シンポジウム(SCIS2020)

４．発表年
2020年

１．発表者名
Miodrag Mihaljevic and Kanta Matsuura

２．発表標題
On the Consensus Protocols for Public Blockchains

３．学会等名
Interop Tokyo 2019（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Takurou Hosoi, Kanta Matsuura

２．発表標題
Security Proof of POW-Based Blockchain Revisited: Explicit Formulation and Implications

３．学会等名
The 23rd International Conference on Financial Cryptography and Data Security

４．発表年
2019年

１．発表者名
Masahito Ishizaka, Kanta Matsuura

２．発表標題
Identity/Attribute-Based Signature Resilient to Hard-to-Invert Leakage under Standard Assumptions

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム2018(CSS2018)

４．発表年
2018年

１．発表者名
林田淳一郎，北川冬航，坂井祐介，花岡悟一郎，松浦幹太

２．発表標題
公開鍵暗号のReplayable CCA環境下での安全性概念間の等価性について

３．学会等名
電子情報通信学会2019年暗号と情報セキュリティ・シンポジウム(SCIS2019)

４．発表年
2019年

１．発表者名
石坂理人，松浦幹太

２．発表標題
DLIN仮定下で強偽造困難性及び多項式的逆変換困難漏洩耐性を持つ電子署名

３．学会等名
電子情報通信学会2019年暗号と情報セキュリティ・シンポジウム(SCIS2019)

４．発表年
2019年

１．発表者名
Kanta Matsuura

２．発表標題
Machine Learning from the Viewpoints of Security Evaluation: Hopes and Open Problems

３．学会等名
LINE and Intertrust Security Summit 2018 Spring（招待講演）

４．発表年
2018年

１．発表者名
松浦幹太

２．発表標題
AIセキュリティの長い歴史と最新動向

３．学会等名
第53回ISSスクエア水平ワークショップ（招待講演）

４．発表年
2018年

１．発表者名
松浦幹太

２．発表標題
基盤としてのブロックチェーンとセキュリティ

３．学会等名
第４回金融機関におけるブロックチェーンに関するワーキンググループ（招待講演）

４．発表年
2018年

１．発表者名
松浦幹太

２．発表標題
AI技術と情報セキュリティ技術の相互依存性について

３．学会等名
第8回バイオメトリクスと認識・認証シンポジウム（招待講演）

４．発表年
2018年

１．発表者名
Kanta Matsuura

２．発表標題
Defender Movement: Significant Productivity Improvement of Mutually-unknown Defenders by Open Internet-based Collaboration

３．学会等名
2017 USENIX Summit on Hot Topics in Security（国際学会）

４．発表年
2017年

１．発表者名
先崎佑弥，大畑幸矢，松浦幹太

２．発表標題
深層学習におけるAdversarial Trainingによる副作用とその緩和策

３．学会等名
コンピュータセキュリティシンポジウム2017(CSS2017)

４．発表年
2017年

１．発表者名
石坂理人，松浦幹太

２．発表標題
Continual Auxiliary Leakageに耐性を持つ適応的安全な述語署名

３．学会等名
コンピュータセキュリティシンポジウム2017(CSS2017)

４．発表年
2017年

１．発表者名
今田丈雅，松浦幹太

２．発表標題
ブロックチェーンと秘密分散法を用いた情報ライフサイクル制御

３．学会等名
コンピュータセキュリティシンポジウム2017(CSS2017)

４．発表年
2017年

１．発表者名
先崎佑弥，大畑幸矢，松浦幹太

２．発表標題
深層学習に対する効率的なAdversarial Examples生成によるブラックボックス攻撃とその対策

３．学会等名
2018年暗号と情報セキュリティ・シンポジウム(SCIS2018)

４．発表年
2018年

１．発表者名
今田丈雅，松浦幹太

２．発表標題
暗号通貨を用いたワンショット型の公平なストレージサービス

３．学会等名
2018年暗号と情報セキュリティ・シンポジウム(SCIS2018)

４．発表年
2018年

１．発表者名
林田淳一郎，石坂理人，坂井祐介，花岡悟一郎，松浦幹太

２．発表標題
公開鍵型検索可能暗号を用いた適応的安全な匿名鍵ポリシー型属性ベース暗号の一般的構成

３．学会等名
2018年暗号と情報セキュリティ・シンポジウム(SCIS2018)

４．発表年
2018年

１．発表者名
細井琢朗，松浦幹太

２．発表標題
POW型ブロックチェーン安全性証明の明示的定式化

３．学会等名
第80回情報処理学会コンピュータセキュリティ研究会

４．発表年
2018年

１．発表者名
松浦幹太

２．発表標題
ブロックチェーンと信頼関係のもたらす防御者革命

３．学会等名
「ブロックチェーンの未来」ワークショップ

４．発表年
2017年

１．発表者名 松浦幹太
２．発表標題 ブロックチェーン応用のモデルと金融工学
３．学会等名 Blockchain EXE #4「ブロックチェーン技術の活用ポイント～既存技術との融合」（招待講演）
４．発表年 2017年

〔図書〕　計1件

１．著者名 松浦幹太	４．発行年 2019年
２．出版社 コロナ社	５．総ページ数 224
３．書名 情報セキュリティ基礎講義	

〔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

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