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　５ 年　 ６ 月　 ７ 日現在

機関番号：１２１０２
研究種目：基盤研究(B)（一般）
研究期間：2019～2021
課題番号：１９Ｈ０４１０７

研究課題名（和文）ブロックチェーンを基盤とする高信頼性を持った自律分散型監視技術

研究課題名（英文）Autonomous Decentralized Surveillance Technology with High Reliability Based on Blockchain

研究代表者

面　和成（Omote, Kazumasa）

筑波大学・システム情報系・教授

研究者番号：５０４１７５０７

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）：本研究では，暗号資産ネットワークを含む，より一般的なブロックチェーンを基盤とした自律分散型ネットワークにおいて，善良なユーザを保護するとともに，悪意あるユーザを監視できるセキュリティ技術について研究開発を行ってきた．具体的には，トークン利用型監視技術，サイバー攻撃対策技術，及び高機能暗号技術の3つのブロックチェーン関連の研究開発を行ってきた．　2019年度から2021年度までの3年間の研究成果には，国際ジャーナル4本，国際会議論文20本，国内シンポジウム論文多数ほか，国内シンポジウムにおける学生論文賞と奨励賞，及び国際会議における優秀プレゼンテーション賞の受賞がある．

研究成果の学術的意義や社会的意義
本研究では，トークンを悪意あるユーザに送信する「しるし」として使用するだけでなく，善良なユーザを保護するためのユーザ証明書のような拡張機能としても使用する．そのようなトークンを用いて実現される自律分散型監視技術は，ブロックチェーンやネットワークのデータから悪意あるユーザを検出し，その取引等を効率的に追跡するのみならず，善良なユーザの信頼性を証明するものである．我々は，自律分散型監視手法を支える技術として，ブロックチェーン，ネットワーク，暗号理論の異なる3つの分野を統合し，トークン利用型監視技術，サイバー攻撃対策技術，及び高機能暗号技術の3つについて包括的な研究を実施した．

研究成果の概要（英文）：In this study, we have conducted research and development on security technologies that can protect good users and monitor malicious users in more general blockchain-based autonomous decentralized networks, including crypto-asset networks. Specifically, we have conducted research and development on three blockchain-related technologies: token-based monitoring, cyber-attack countermeasures, and advanced cryptography. Research achievements during the three-year period from FY 2019 to FY 2021 include four international journals, 20 international conference papers, many domestic symposium papers, as well as student paper awards and encouragement awards at domestic symposiums, and an excellent presentation award at an international conference.

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　スマートコントラクト　トークン　サイバー攻撃対策技術　暗号技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

2018 年に入ってから暗号資産の盗難事件が頻発している．特に，2018 年 9 月に発生した事件では，暗号資産の盗難時における検出・追跡技術の未整備により，盗まれた暗号資産が善良なユーザを巻き込んで広く拡散し，その追跡が非常に困難となっている．このような背景から，暗号資産ネットワークでは，善良なユーザを保護する安全な基盤やマネーロンダリングなどの犯罪抑止が求められており，悪意あるユーザを検出・追跡するといったユーザの監視技術は喫緊の課題である．しかしながら，現在に至るまで，ブロックチェーンを基盤とした自律分散型ネットワーク環境において，そのような技術は確立されていない．

ブロックチェーンと相性の良い技術としてトークンがある．トークンは，取引情報として定義可能な権利や単位であり，ブロックチェーン上に記録可能な取引情報のフレームワークとして注目されている．またトークンは，ユニークな情報を定義できる性質から「しるし」として機能し，あるユーザ A から別のユーザ B に送信できる．2018 年 1 月に発生した暗号資産 NEM の盗難事件では，犯人を効率よく追跡するために，モザイクと呼ばれるトークンの利用が試みられ，トークンが犯人に送信された．さらに，自律分散型ネットワーク環境に適した，悪意あるユーザの追跡技術については，取引情報の分析が中心であり，トークンの仕組みを活用した学術的アプローチについては，研究がなされていない．

２．研究の目的

ユーザの検出・追跡技術が真に高信頼なシステムとなるためには，ブロックチェーンの解析研究だけではなく，サイバー攻撃対策や暗号理論的安全性の観点の研究との分野横断的な連携が極めて重要である．そこで本研究は，ブロックチェーン解析，サイバー攻撃対策，暗号理論の三つの観点から，悪意あるユーザの検出・追跡に関する基礎的研究をさらに発展・深化させ，自律分散型ネットワーク上で悪意あるユーザを監視できるセキュリティ技術について，研究開発を行うものである．このために本研究では，トークンを用いた高信頼な自律分散型監視システムの構成法を提案する．なお，本研究におけるブロックチェーンを基盤とした自律分散型ネットワークは，暗号資産ネットワークのみならず，スマートコントラクト（ブロックチェーン上で自動実行されるプログラム）が動作する自律分散型ネットワークも対象とする．さらに，本研究では，自律分散型ネットワーク環境において誰が監視するのか，サイバー攻撃耐性やトークンの不正利用など安全性をどこまで保証するのか，という検証と評価を実施する．

３．研究の方法

本研究では，トークンを悪意あるユーザを識別する「しるし」として使用するだけでなく，善良なユーザを保護するためのユーザ証明書のような拡張機能としても使用する．そのようなトークンを用いて実現される自律分散型監視技術は，ブロックチェーンシステムにおける透明性や匿名性を損なうことなく共存可能であり，悪意あるユーザの検出を容易にし，その取引等を効率的に追跡するのみならず，善良なユーザの信頼性を証明するものである．自律分散型監視手法を支える技術として，ブロックチェーン，ネットワーク，暗号理論の異なる 3 つの分野を統合して包括的な解決策を提案すべく，主に以下の内容の研究を推し進めた．

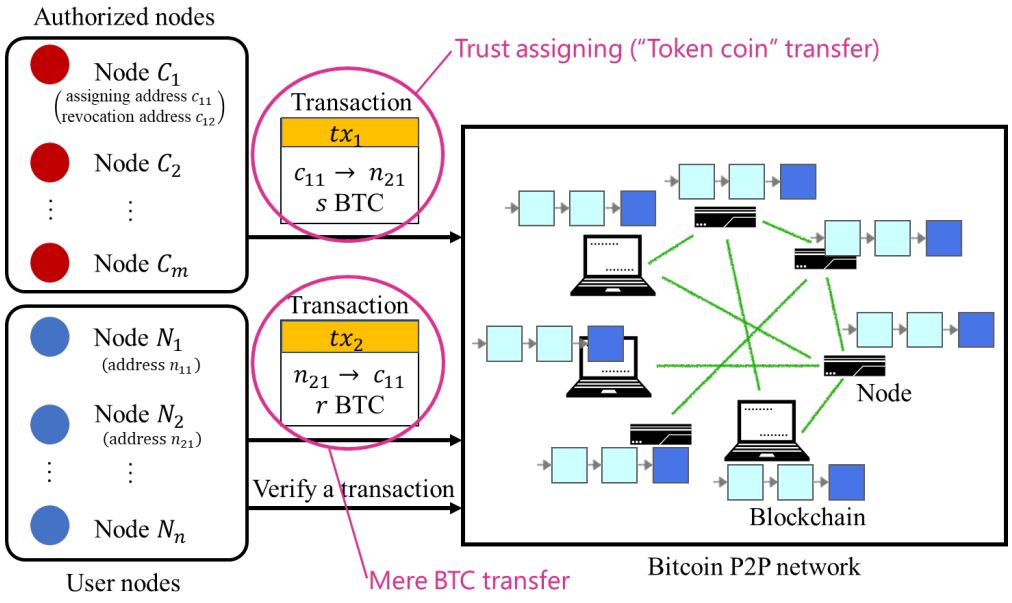

図 1　ブロックチェーンアドレスにトークンを付与する方式の具体例

(1) ブロックチェーンアドレスにトークンを付与する方式：
ブロックチェーンには，ユーザアドレスに信頼を与える方法がない．非金融情報などの格納領域に証明書を挿入することで，ユーザアドレスに信頼を与えることは可能であるが，効率性の観点で課題があった．本研究は，トークン利用型監視技術の基礎的研究として，暗号資産自体をトークンと見立てて信頼できるアドレスや不審なアドレスにトークンを付与する基本方式を検討し，暗号資産の送金のみで効率的にユーザアドレスに信頼を付与する手法を提案したものである．図 1 は Bitcoin のケースで説明した図であり，スマートコントラクトを利用することなく信頼を与えることが可能となっている．本方式の主なアイデアは，「トークン・コイン」（暗号資産の送金そのもの）を信頼提供メカニズムとして利用できる点にある．さらに，このトークンの付与機能を発展させることによって，グローバル ID に柔軟かつ動的に属性を付与，あるいは失効する方式を提案した．

(2) Ethereum ブロックチェーンの汚染に対する分析：
トークン利用型監視技術がセキュアなものになるためには，Bitcoin や Ethereum などの実稼働しているパブリックブロックチェーンの信頼性が確保されていることが極めて重要である．先行研究[1]では，Bitcoin ブロックチェーンのデータ解析を行い，ブロックチェーンのデータ領域が汚染されていることを明らかにし，Bitcoin のリスク分析について報告がなされた．これに対して本研究は，より多くのデータがブロックに格納可能な Ethereum ブロックチェーンを対象として，そのポイズニング攻撃の実態について分析したものである．さらに，ブロックチェーンベースの C&C（Control and Command）攻撃[2]の可能性が指摘されているなか，ブロックチェーンエクスプローラの利用による C&C 攻撃の実行容易性について指摘した．

(3) ブロックチェーン技術の応用：
ブロックチェーンにおけるトークン及び監視手法の安全性・可能性を探るために，並行してブロックチェーン技術を IoT ネットワークなどに応用したセキュアなシステムを提案する研究を進めてきた．例えば，決済に暗号資産を導入する研究が進んでいるなか，ユーザの秘密鍵が盗まれると，それに紐づく暗号資産も盗まれる可能性がある．本研究は，この問題を解決するため，コントラクトウォレットを用いた安全な自動決済システムを提案したものである．提案方式は，IoT 機器を用いたサービスにコントラクトウォレットを導入することで，秘密鍵が盗まれた場合でも暗号資産の窃取を限定的なものにすることができる．

(4) ブロックチェーンネットワークに対するサイバー攻撃対策：
Ethereum のクライアントの設定不備を狙うサイバー攻撃を観測するためのハニーポットを構築し，運用を行うことで，これらを狙う様々な攻撃を観測し，不正に利用される Ethereum アカウントの情報を収集する仕組みを構築する．さらに，同様の設定不備をもつ Ethereum クライアントを広域スキャンシステムにより探索し，当該クライアントに紐づく Ethereum アカウントを調査することで不正に利用される Ethereum アカウントの情報を収集する．このように収集した悪性アカウントに関するトランザクションをブロックチェーンエクスプローラにより調査し，不正アカウントの活動実態を分析する．

(5) 暗号技術のブロックチェーンへの適用：
匿名性と追跡性とを兼ね備えたアカウンタブルリング署名が様々な暗号資産へのプライバシー保護型トークン付与，すなわち匿名信頼性付与方式に適用可能なことを検証するため，Bitcoin，Ethereum，NEM について検討および実装評価を行った．また匿名性によりプライバシーを向上させる一方で一度発行したトークンの失効が難しいという問題が発生するため，暗号的コミットメント方式を利用したトークンの失効についても検討を行った．また中核技術であるアカウンタブルリング署名とスマートコントラクトを用いたプライバシー保護集金システムの検討を行った．さらに秘密情報を直接扱うことが難しいスマートコントラクトにて秘密情報を安全に扱うためにゼロ知識証明を用いたプロトコルの検討を行った．

４．研究成果
本章では，前章で説明した研究方法のそれぞれについて研究成果を記載する．

(1) ブロックチェーンアドレスにトークンを付与する方式：
本研究では，暗号資産の送金のみで効率的にユーザアドレスやグローバル ID に信頼を付与する手法を新たに提案し，その主な研究成果は 2 本の査読付き国際会議論文に採録された．本方式の実現可能性を検討するために，Bitcoin 及び Ethereum のテストネットにおいて，信頼付与の実証実験を行い（図 2 参照），Bitcoin と Ethereum においてトークンの付与が実現可能であることを示しただけでなく，暗号資産の基本機能しか用いていないことから，送金機能を持つほぼすべての暗号資産にも容易に適用できることを明らかにした．

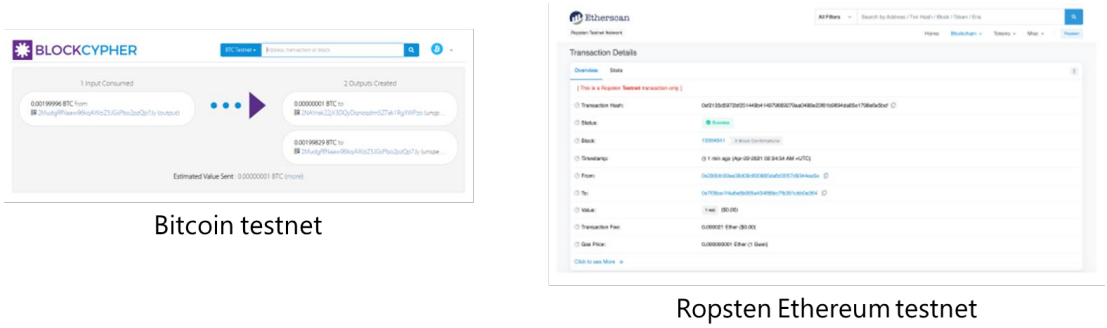

図 2　Bitcoin 及び Ethereum のテストネットによる実証実験の結果

(2) Ethereum ブロックチェーンの汚染攻撃に対する分析：
本研究では，Ethereum ブロックチェーンのデータ領域に不正なデータが多数埋め込まれていることを初めて明らかにし，その主な研究成果は査読付き国際会議論文に採録され，さらにその中で Best Paper Award を受賞した．本分析においては，図 3 のとおり，本来格納されるはずのスマートコントラクト以外で 153 個のファイルが埋め込まれていることを確認し，特に 3 つの exe ファイルが「W32.Duqu」というマルウェア（Virus Total による判定結果）であることを明らかにした．さらに，プライベートなブロックチェーンネットワーク環境を構築し，ブロックチェーンエクスプローラを用いた C&C 攻撃の実行容易性について検証・考察を行うとともに，新たな対策案を提示した．今後は，NFT を対象としたブロックチェーンの汚染攻撃に対する分析を行う．

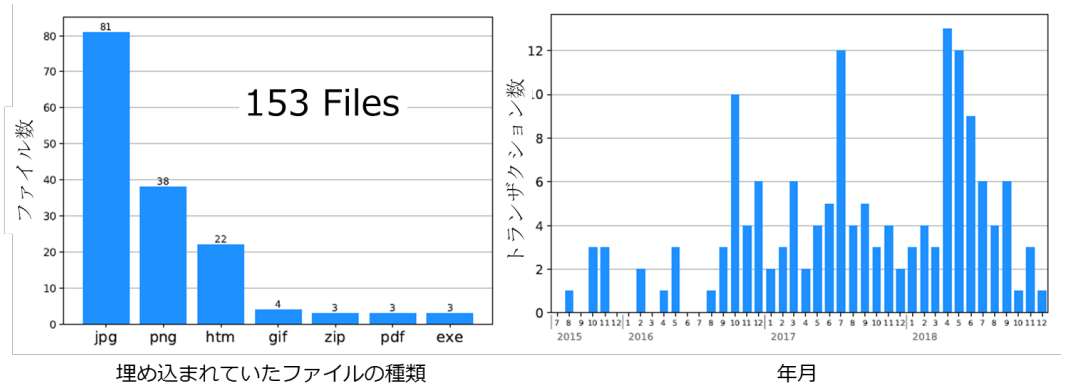

図 3　Ethereum ブロックチェーンに埋め込まれたファイル内訳と埋め込まれた時期
（2015 年 7 月 30 日 ~ 2018 年 11 月 30 日）

(3) ブロックチェーンの応用：
本研究では，主に Ethereum のスマートコントラクトを用いて，暗号資産の自動決済やインセンティブを利用した新たなシステムを提案し，その主な研究成果は 1 本の査読付き国際ジャーナル，2 本の国際会議論文に採録され，さらに国内シンポジウムにおいて学生論文賞（上位約 7%）を受賞した．本方式の実現可能性を検討するために，Ethereum のテストネットにおいて実装したスマートコントラクトを動作させることで提案手法が効率的に動作することを検証し，必要な手数料等の評価を行った．ブロックチェーンにおけるトークン及び監視手法の安全性・可能性を探るために，今後もブロックチェーンを用いた新たなセキュアシステムの構築に関する研究を行う．

(4) ブロックチェーンネットワークに対するサイバー攻撃対策：
構築したハニーポットによる観測により，Ethereum ハニーポットへ 41 種類のメソッドからなる 538 アドレスからの攻撃を観測した．特に，これまでに報告されていない Eclipse Attack などの新規の攻撃の観測に成功した．また，16 件の不正アカウントを発見した．広域スキャンシステム Shodan による探索では，多数のノードと紐づき，攻撃に悪用されている可能性が高いアカウントを 64 発見した．このように収集した不正アカウントに関するトランザクションをブロックチェーンエクスプローラにより調査し，その活動実態を分析した結果，実際にこれらの不正アカウントが少なくとも 21.5[ETH]，観測当時のレートで 1,000 万円以上のトランザクシ

ョン記録が存在することが判明した．これらの成果は，国際会議 International Conference on Cryptography, Security and Privacy (CSP 2022)において発表され，当該発表は Best Presentation Award を受賞した．

(5) 暗号技術のブロックチェーンへの適用：
ブロックチェーンシステムにおける匿名信頼性付与手法，特に匿名性の担保について，暗号理論的側面から検討を行った．その主な成果として 1 本の国内会議，1 本の査読付き国際ジャーナル，1 本の査読付き国際会議に採録された．またスマートコントラクトを用いたプライバシー保護集金システムの提案を行い，1 本の査読付き国際会議に採録された．またコミットメント，ゼロ知識証明，スマートコントラクトを利用することで入札額の上限漏洩を防止した資金拘束型の封印入札オークションを提案し，国内会議にて奨励賞を受賞した．

「参考文献」
[1] R. Matzutt et al. ″A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin“, FC2018.
[2] S.T. Ali, “Zombiecoin 2.0: Managing Next-generation Botnets Using Bitcoin,” International Journal of Information Security, 2018.

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4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 Haga Shinya、Omote Kazumasa	４．巻 2021
２．論文標題 IoT-Based Autonomous Pay-As-You-Go Payment System with the Contract Wallet	５．発行年 2021年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1～10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2021/8937448	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 Sato Teppei、Emura Keita、Fujitani Tomoki、Omote Kazumasa	４．巻 9
２．論文標題 An Anonymous Trust-Marking Scheme on Blockchain Systems	５．発行年 2021年
３．雑誌名 IEEE Access	６．最初と最後の頁 108772～108781
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2021.3097710	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 Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, Kazuma Ohara, Kazumasa Omote, Yusuke Sakai	４．巻 2019
２．論文標題 Group Signatures with Message-Dependent Opening: Formal Definitions and Constructions	５．発行年 2019年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1-36
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2019/4872403	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 Keita Emura, Takuya Hayashi	４．巻 103-A(1)
２．論文標題 A Revocable Group Signature Scheme with Scalability from Simple Assumptions	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 125-140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019CIP0004	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51件（うち招待講演　1件／うち国際学会　20件）

1．発表者名
Jia Wang, Takayuki Sasaki, Kazumasa Omote, Katsunari Yoshioka, and Tsutomu Matsumoto

2．発表標題
Multifaceted Analysis of Malicious Ethereum Accounts and Corresponding Activities

3．学会等名
The 6th International Conference on Cryptography, Security and Privacy（国際学会）

4．発表年
2022年

1．発表者名
Kazuki Hara, Takeshi Takahashi, Motoya Ishimaki, and Kazumasa Omote

2．発表標題
Machine-learning Approach using Solidity Bytecode for Smart-contract Honeypot Detection in the Ethereum

3．学会等名
The 21st International Conference on Software Quality, Reliability and Security Companion（国際学会）

4．発表年
2021年

1．発表者名
Kota Chin and Kazumasa Omote

2．発表標題
Analysis of Attack Activities for Honeypots Installation in Ethereum Network

3．学会等名
The 4th IEEE International Conference on Blockchain（国際学会）

4．発表年
2021年

1．発表者名
Mitsuyoshi Imamura and Kazumasa Omote

2．発表標題
Toward Achieving Unanimity for Implicit Closings in a Trustless System

3．学会等名
The 17th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness（国際学会）

4．発表年
2021年

１．発表者名
Keigo Kimura and Kazumasa Omote

２．発表標題
Risk Analysis for Abusing Blockchain Poisoning

３．学会等名
The 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services（国際学会）

４．発表年
2021年

１．発表者名
Tomoki Fujitani, Keita Emura, and Kazumasa Omote

２．発表標題
A Privacy-Preserving Enforced Bill Collection System using Smart Contracts

３．学会等名
The 16th Asia Joint Conference on Information Security（国際学会）

４．発表年
2021年

１．発表者名
Mitsuyoshi Imamura and Kazumasa Omote

２．発表標題
Investigation and Analysis of Features in Decentralized Network Management of Minor Cryptocurrencies

３．学会等名
The 35th International Conference on Advanced Information Networking and Applications（国際学会）

４．発表年
2021年

１．発表者名
Wataru Taguchi and Kazumasa Omote

２．発表標題
Risk Analysis for Worthless Crypto Asset Networks

３．学会等名
The 35th International Conference on Advanced Information Networking and Applications（国際学会）

４．発表年
2021年

１．発表者名
Mitsuyoshi Imamura and Kazumasa Omote

２．発表標題
Empirical Study of Software Adoption Process in the Bitcoin Network

３．学会等名
The 35th International Conference on Advanced Information Networking and Applications（国際学会）

４．発表年
2021年

１．発表者名
Teppei Sato, Keita Emura, Tomoki Fujitani, and Kazumasa Omote

２．発表標題
An Anonymous Trust-Marking Scheme on Blockchain Systems

３．学会等名
The IEEE International Conference on Blockchain and Cryptocurrency（国際学会）

４．発表年
2021年

１．発表者名
Shinya Haga and Kazumasa Omote

２．発表標題
Autonomous Pay-As-You-Go Payment System with IoT Device Using Contract Wallet

３．学会等名
The IEEE International Conference on Blockchain and Cryptocurrency（国際学会）

４．発表年
2021年

１．発表者名
内田大暉，面和成

２．発表標題
Ethereum RPC ハニーポットの最小要件の調査と軽量化手法の提案

３．学会等名
コンピュータセキュリティ研究会（CSEC）

４．発表年
2022年

１．発表者名
福田竜央，面和成

２．発表標題
プライバシーを考慮したブロックチェーンを用いた柔軟なコンタクトトレーシング手法

３．学会等名
Symposium on Cryptography and Information Security

４．発表年
2022年

１．発表者名
木村圭吾，今村光良，面和成

２．発表標題
NFT流通における深層学習を用いた分散型真正性検証プロトコルの提案

３．学会等名
Symposium on Cryptography and Information Security

４．発表年
2022年

１．発表者名
藤本真吾，面和成

２．発表標題
スマートコントラクトによるデジタル資産取引におけるプライバシに配慮した取引仲介の実現に向けて

３．学会等名
コンピュータセキュリティ研究会

４．発表年
2021年

１．発表者名
岩田琴乃，面和成

２．発表標題
IoT機器とスマートコントラクトを用いた警備用自動監視システム

３．学会等名
Computer Security Symposium

４．発表年
2021年

１．発表者名
陳浩太，江村恵太，佐藤慎悟，面和成

２．発表標題
入札額の上限漏洩を防止した資金拘束型の封印入札オークション

３．学会等名
Computer Security Symposium

４．発表年
2021年

１．発表者名
芳賀慎也，面和成

２．発表標題
マイナンバーカードを用いたブロックチェーンによる自動確定日付システム

３．学会等名
Computer Security Symposium

４．発表年
2021年

１．発表者名
木村圭吾，今村光良，面和成

２．発表標題
NFTの信頼性にみるセキュリティリスクの考察

３．学会等名
情報セキュリティ研究会

４．発表年
2021年

１．発表者名
今村光良，面和成

２．発表標題
Dogecoinネットワークの特徴とセキュリティリスクの考察

３．学会等名
情報セキュリティ研究会

４．発表年
2021年

１．発表者名
上野隆治，面和成

２．発表標題
ブロックチェーンを用いた医療情報共有システムの提案に向けて

３．学会等名
情報セキュリティ研究会

４．発表年
2021年

１．発表者名
Natsuo Shintani, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto,

２．発表標題
Measurement and Factor Analysis of the Impact of Amplification DDoS Attacks Observed by Amppot

３．学会等名
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
2021年

１．発表者名
Jia Wang, Takayuki Sasaki, Kazumasa Omote, Katsunari Yoshioka, Tsutomu Matsumoto

２．発表標題
Etherpot: A Honeypot for Observing Cyberattacks on Ethereum Client

３．学会等名
電子情報通信学会情報システムセキュリティ研究会

４．発表年
2021年

１．発表者名
毛 清昕，牧田 大佑，吉岡 克成，松本 勉

２．発表標題
ハニーポットで観測される絨毯爆撃型DRDoS攻撃の分析

３．学会等名
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
Tatsuhiro Fukuda and Kazumasa Omote

２．発表標題
Efficient blockchain-based IoT firmware update considering distribution incentives

３．学会等名
DSC 2021（国際学会）

４．発表年
2021年

１．発表者名
Kazuki Hara, Teppei Sato, Mitsuyoshi Imamura and Kazumasa Omote

２．発表標題
Profiling of Malicious Users Targeting Ethereum’s RPC Port Using Simple Honeypots

３．学会等名
IEEE Blockchain 2020（国際学会）

４．発表年
2020年

１．発表者名
Kazumasa Omote, Asuka Suzuki and Teppei Sato

２．発表標題
A New Method of Assigning Trust to User Addresses in Bitcoin

３．学会等名
BCCA 2020（国際学会）

４．発表年
2020年

１．発表者名
陳浩太，面和成

２．発表標題
Ethereumネットワークにおけるハニーポット設置に向けた攻撃活動の分析

３．学会等名
情報セキュリティ研究会（ISEC）

４．発表年
2021年

１．発表者名
原和希，高橋健志，面和成

２．発表標題
Ethereumにおけるスマートコントラクトハニーポット検出のためのSolidityバイトコードを活用した機械学習モデルの検討

３．学会等名
SCIS 2021

４．発表年
2021年

１．発表者名
藤谷知季，江村恵太，面和成

２．発表標題
スマートコントラクトを用いたプライバシー保護集金システム

３．学会等名
SCIS 2021

４．発表年
2021年

１．発表者名
木村圭吾，面和成

２．発表標題
ブロックチェーンの汚染による悪用リスクの考察

３．学会等名
CSS 2020

４．発表年
2020年

１．発表者名
芳賀慎也，面和成

２．発表標題
コントラクトウォレットを用いたIoT機器による暗号資産従量課金制の自動決済システム

３．学会等名
CSS 2020

４．発表年
2020年

１．発表者名
田口渉，面和成

２．発表標題
ブロックチェーン技術の分散性による無停止メカニズムのリスク分析(2)

３．学会等名
情報セキュリティ研究会（ISEC）

４．発表年
2020年

１．発表者名
藤谷知季，江村恵太，面和成

２．発表標題
NEMのブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価

３．学会等名
情報セキュリティ研究会（ISEC）

４．発表年
2020年

１．発表者名
今村光良，面和成

２．発表標題
ブロックチェーンネットワークの不均衡と収束による再中央集権化の評価

３．学会等名
情報セキュリティ研究会（ISEC）

４．発表年
2020年

１．発表者名
Natsuo Shintani, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto

２．発表標題
Measurement and Factor Analysis of the Impact of Amplification DDoS Attacks Observed by Amppot

３．学会等名
研究報告マルチメディア通信と分散処理（DPS）

４．発表年
2021年

１．発表者名
Teppei Sato, Keita Emura, Tomoki Fujitani, and Kazumasa Omote

２．発表標題
An Anonymous Trust-Marking Scheme on Blockchain Systems

３．学会等名
IEEE ICBC 2021（国際学会）

４．発表年
2021年

１．発表者名
Shinya Haga and Kazumasa Omote

２．発表標題
Autonomous Pay-As-You-Go Payment System with IoT Device Using Contract Wallet

３．学会等名
IEEE ICBC 2021（国際学会）

４．発表年
2021年

１．発表者名
Keigo Kimura and Kazumasa Omote

２．発表標題
Risk Analysis for Abusing Blockchain Poisoning

３．学会等名
BRAINS 2021（国際学会）

４．発表年
2021年

１．発表者名
Kazumasa Omote, Mitsuyoshi Imamura and Teppei Sato

２．発表標題
Blockchain and its Security Risk

３．学会等名
2020 IEEE International Conference on Big Data and Smart Computing (BigComp 2020)（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
Mitsuyoshi Imamura and Kazumasa Omote

２．発表標題
Difficulty of decentralized structure due to rational user behavior on blockchain

３．学会等名
13th International Conference on Network and System Security (NSS 2019)（国際学会）

４．発表年
2019年

１．発表者名
Teppei Sato, Mitsuyoshi Imamura and Kazumasa Omote

２．発表標題
Threat Analysis of Poisoning Attack against Ethereum Blockchain

３．学会等名
13th WISTP International Conference on Information Security Theory and Practice (WISTP 2019)（国際学会）

４．発表年
2019年

１．発表者名
今村光良，面和成

２．発表標題
ブロックチェーン技術はSDGsに貢献するか？

３．学会等名
情報セキュリティ研究会

４．発表年
2019年

１．発表者名
佐藤哲平，江村恵太，面和成

２．発表標題
ブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
市野樹也，面和成

２．発表標題
スマートコントラクトを用いたIoT機器の効率的な認証手法

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
福田竜央，面和成

２．発表標題
ブロックチェーンを用いたインセンティブ付与を考慮した効率的なIoT機器ファームウェア配布手法

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
佐藤哲平，江村恵太，面和成

２．発表標題
ブロックチェーンシステムにおける匿名トークン付与に関する一考察

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2019年

１．発表者名
鈴木明日香，佐藤哲平，面和成

２．発表標題
ビットコインにおけるユーザへの信頼性付与の手法

３．学会等名
情報セキュリティ研究会

４．発表年
2019年

１．発表者名
田口渉，今村光良，面和成

２．発表標題
ブロックチェーン技術の分散性による無停止メカニズムのリスク分析

３．学会等名
情報セキュリティ研究会

４．発表年
2019年

１．発表者名
原和希，佐藤哲平，今村光良，面和成

２．発表標題
ブロックチェーンネットワークにおけるハニーポット設置に向けた悪意あるユーザのプロファイリング

３．学会等名
情報セキュリティ研究会

４．発表年
2019年

１．発表者名
今村光良，面和成

２．発表標題
ブロックチェーン上におけるソフトウェア更新から考察するユーザーの振る舞い

３．学会等名
第82回全国大会

４．発表年
2020年

〔図書〕　計3件

１．著者名 面 和成	４．発行年 2021年
２．出版社 コロナ社	５．総ページ数 232
３．書名 入門　サイバーセキュリティ　理論と実験	

1．著者名 Bikramaditya Singhal、Gautam Dhameja、Priyansu Sekhar Panda、面　和成	4．発行年 2020年
2．出版社 オーム社	5．総ページ数 384
3．書名 ブロックチェーン実践入門	

1．著者名 Kazumasa Omote and Makoto Yano	4．発行年 2020年
2．出版社 Springer	5．総ページ数 8
3．書名 Bitcoin and Blockchain Technology	

〔産業財産権〕

〔その他〕

面研究室　研究業績
https://www.risk.tsukuba.ac.jp/omote-lab/achievement/

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	吉岡　克成 (Yoshioka Katsunari) (60415841)	横浜国立大学・大学院環境情報研究院・准教授 (12701)	

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	江村　恵太 (Emura Keita) (30597018)	国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所・研究マネージャー (82636)	

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