# 博士論文要旨

# 論文題名：刑事手続におけるデジタル証拠の改ざん防止に関する研究

立命館大学大学院情報理工学研究科
情報理工学専攻博士課程後期課程

コサカタニ サトシ
小坂谷　聡

情報処理技術の発展・普及，社会基盤化に伴い，社会のあらゆる場面で IT 化・デジタル化が進展しているが，この変化の波は刑事手続の分野とて例外とは言えない．ところが，刑事手続の分野においては IT 化の変化に十分に追随できず，本来，社会的な課題解決の手段となるべき IT 化 がかえって人権侵害を招く深刻な課題をもたらしている状況が見受けられる．そこで，本論文では，刑事手続の分野における IT 化がもたらした課題として，今後，一層比重が増してくると考えられるデジタル証拠に対する捜査機関による改ざんリスクの問題に焦点を絞り，このような不正を防止するための技術的なシステムの提案を行った．

まず初めに，通信傍受という特定の分野ではあるが，傍受されたデジタルデータに関して，改ざんを防止するための技術的な措置が規定されていると評価できる 2016 年改正通信傍受法に着目した．傍受データを裁判所で保管するという同法が規定するスキームがデジタル証拠の改ざん防止のための一般的なシステムとして参考とすることができるのかという観点から，まず，同改正法によって新設された暗号技術を利用した通信傍受手法について検討し，耐タンパ性に優れた IC カードを利用した傍受システムを提案した．もっとも，提案した傍受システムは，捜査機関による違法行為を技術的に防止するための枠組みとしては十分に意義があるが，この仕組みをデジタル証拠一般に応用することに対しては刑事手続の当事者主義的訴訟構造の観点等から必ずしも妥当とは言えない．そこで，改ざんが容易であるというデジタル証拠の特性に即した改ざん防止のための新たなシステムとして，ブロックチェーンを利用した証拠のハッシュ値保管システムを提案した．提案したブロックチェーンシステムでは，デジタル証拠が捜査機関によって押収された際，そのハッシュ値が直ちにブロックチェーンに登録されることから，弁護人は，検察官から開示されたデジタル証拠のハッシュ値とブロックチェーン上に保管された証拠ハッシュ値を比較することによって容易に改ざんの有無を確認することが可能となる．そして，本論文では，提案したブロックチェーンシステムが効果的に運用されるための仕組みとして，トークンを活用した一般市民ないし弁護士等から構成されるトークンエコノミーについてのモデル構築を提案した．

本論文では，これらの提案システムを通じて，法律的観点からだけでは解決しきれない刑事手続の分野における IT 化・デジタル化の課題について技術的な観点から解決するための指針を示すことができた.

# Abstract of Doctoral Dissertation

# Title：A Study on the Prevention of Tampering with e-Evidence in Criminal Procedure

Doctoral Program in Advanced Information Science and Engineering
Graduate School of Information Science and Engineering
Ritsumeikan University

コサカタニ サトシ
KOSAKATANI Satoshi

With the development and dissemination of information processing technology and the development of social infrastructure, IT and digitalization are progressing in all aspects of society, and this wave of change is no exception in the field of criminal procedure. In the field of criminal procedure, however, it has not been able to keep pace with the changes in the use of information technology, and the use of information technology, which is supposed to be a means of solving social problems, has led to serious problems that may lead to human rights violations. In this paper, we focus on the problem of the risk of tampering with digital evidence by investigative agencies, which is expected to increase in importance in the future, as an issue brought about by IT in the field of criminal procedure, and propose a technical system to prevent such fraud.

To begin with, we focus on the 2016 Amended Communications Interception Act, which, although in the specific field of communications interception, can be evaluated as providing technical measures to prevent tampering with respect to intercepted digital data. From the viewpoint of whether the scheme of storing intercepted data in a court of law can be used as a general system to prevent tampering of digital evidence, a communication interception method using cryptographic technology newly introduced by the law is investigated and a tamper-resistant IC card interception system is proposed. Although the proposed interception system is significant enough as a framework to technically prevent illegal acts by investigative agencies, it is not necessarily appropriate to apply this system to digital evidence in general from the perspective of the party-oriented litigation structure of criminal proceedings. Therefore, we proposed a new system to prevent tampering of digital evidence, which is easy to tamper with, by using a blockchain to store hash values of evidence. In the proposed blockchain system, when digital evidence is seized by an investigative agency, its hash value is immediately registered in the blockchain, so that the defense attorney can easily check for tampering by comparing the hash value of the digital evidence disclosed by the prosecutor with the hash value of the evidence stored on the blockchain. In this paper, we propose a model of a token economy, which consists of ordinary citizens and lawyers using tokens, as a mechanism to operate the proposed blockchain system effectively.

In this paper, through these proposed systems, we were able to show a guideline to solve the problems of IT and digitalization in the field of criminal procedures from a technical point of view, which cannot be solved only from a legal point of view.