論文の内容の要旨及び論文審査の結果の要旨の公表

学位規則第 8 条に基づき、論文の内容の要旨及び論文審査の結果の要旨を公表する。

<table>
<tr><td>フリガナ
氏名（姓、名）</td><td colspan="2">コサカタニ サトシ
小坂谷　聡</td><td>授与番号　甲 1494 号</td></tr>
<tr><td>学 位 の 種 類</td><td>博士(　工学　)</td><td>授与年月日</td><td>2021 年　3 月　31 日</td></tr>
<tr><td>学位授与の要件</td><td colspan="3">本学学位規程第 18 条第 1 項該当者　　[学位規則第 4 条第 1 項]</td></tr>
<tr><td>博士論文の題名</td><td colspan="3">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</td></tr>
<tr><td rowspan="2">審　査　委　員</td><td colspan="2">(主査) 上原 哲太郎
（立命館大学情報理工学部教授）</td><td>國枝 義敏
（立命館大学情報理工学部教授）</td></tr>
<tr><td colspan="2">野口 拓
（立命館大学情報理工学部教授）</td><td></td></tr>
<tr><td>論文内容の要旨</td><td colspan="3">本論文は、刑事事件における捜査や裁判において用いられる証拠のうち、デジタルデータとなっているものの改ざんを防止する手法を研究対象としている。本論文は 6 章からなる。1 章は刑事手続きにおいて、捜査手法に IT が用いられるようになってきていることや捜査対象がデジタルデータとなりつつあることにより、その改ざんの脅威が問題になっていることについて述べ、研究の目的としてこれらの改ざん防止手法の提案を挙げている。2 章は、刑事手続におけるデジタル証拠の収集手続について検討する前提として、刑事訴訟法によって規定されている証拠の収集手続に関して論じ、デジタル証拠の真正性・完全性等が刑事裁判において問題となる場合について例を挙げ、改ざん防止の必要性について論じている。3 章は通信傍受法において認められた暗号技術を用いた傍受手法について、暗号利用が法の求めを満たすための要件について整理し、現状の傍受装置が持つ問題点を挙げた上で、その問題を解決するためのシステムを提案している。 4 章は犯罪捜査において収集されたデジタル証拠の改ざんを防止するためにブロックチェーン技術を用いた証拠ハッシュ値の登録システムを提案し、さらにそのシステムを利用した上でデジタル証拠が改ざんされる場合があるかリスク分析を行っている。5 章は前章で提案したブロックチェーンを用いた証拠ハッシュ値の登録システムを 3 章で提案した通信傍受装置の証拠の改ざん防止に利用することを提案した上で、ブロックチェーンを円滑に運用するためにトークンエコノミーを構築することについて提案し、6 章で論文をまとめている。
本論文の要旨は以下のようにまとめられる。刑事手続におけるデジタル証拠について捜査機関においても証拠改ざんの可能性があることが裁判例より明らかになっている。通信傍受法においては証拠取得手続きの適正性を確保するために暗号技術を利用することが示されているが、単純に公開鍵暗号を利用するだけでは現行法の要求を全て満たすことは困難である。そこで、耐タンパ性を有する IC カードを用いることで法の規定に矛盾しない通信傍受装置が実現できることを示した。また、デジタル証拠の改ざん防止には一般にハッシュ値が用いられるが、ハッシュ値の記録場所が公開されていなければ証拠改ざんがないことを確認することは困難である。そこでブロックチェーン技術を用いれば広く公開された証拠ハッシュ値保全システムが実現可能であることを示した。またブロックチェーンシステムの維持のため、弁護士会がマイニングノードを運営し、トークンエコノミーを構築することでシステムを安定的に運用する手法を提案した。</td></tr>
</table>

論文審査の結果の要旨	本論文は、過去に刑事手続におけるデジタル証拠の改ざんが発生しており、その再発の可能性が否めないという問題意識のもと、刑事手続の透明性を確保し、デジタル証拠に改ざんがないことを事後的に確認可能なシステムを提案している点が特徴である。通信傍受法では暗号化に利用する鍵について変換符号、対応変換符号という用語が定義されているが、これらをそれぞれ公開鍵、秘密鍵に当てはめると、公開鍵暗号は一般に共通鍵の暗号化に利用されている現状と矛盾が生じる。そこで変換符号を暗号化に使う共通鍵とし、対応変換符号を公開鍵で暗号化された共通鍵とすることで、法の要求を満たしたシステムが実現できる。しかしこの実装では捜査機関は保有する秘密鍵を用いて通信事業者に提供された共通鍵（変換符号）を入手可能であり、証拠の復号と改ざんが可能になる。これを防止するために耐タンパ性のある IC カード内で通信データの復号処理を行うことで法の要求と実装の整合を取る手法を提案している。さらに、刑事手続において押収・収集されたデジタル証拠が捜査の過程で改ざんされることを防止するため、ブロックチェーンを用いる手法を提案している。家宅捜索等において証拠が押収される際には立会人が求められているが、立会人にとってデジタル証拠が押収時と裁判時に同一であるか確認することは容易ではない。そこで立会時に証拠のハッシュ値を取得した上で、その値に立会人および捜査機関がそれぞれ電子署名し、ブロックチェーンに登録することで、押収時の証拠が事後に改ざんされても容易に検出できるシステムを提案している。さらに、そのシステムを弁護士会をマイニングノードとするブロックチェーンとして運営することで、弁護士会が実質発行するトークンを立会人に付与し、そのトークンを弁護士会の主催する法律相談の利用料などに使えるトークンエコノミーを構築することで、立会人にインセンティブを与えるとともにシステムを安定的に運用し続ける手法を提案した。 本論文では、提案しているシステムがいずれもプロトタイプにとどまっており、その有効性を実証実験を通して証明するまでには至っていない。しかし、未だ研究や提案が十分とは言えないにもかかわらず現実の脅威が高まっているデジタル証拠の改ざんに対して、技術的な解決策を法との整合性を保ちながら提案している点が大きな特徴である。暗号技術を活用した通信傍受手法については、現行法に単純に暗号技術を当てはめると矛盾が生じかねないことを指摘し、実現可能なシステムを提案した。これにより、通信傍受法の改正が元々目指していた立会人が不要かつ傍受手順の適正性が事後に確認可能となった。ブロックチェーンを用いた証拠ハッシュ値保全システムについては、証拠の改ざんがないことが誰にでも確認可能な透明性のあるシステムを提案している。さらにブロックチェーンの永続性について問題になるノード維持の負担について、トークンエコノミーの構築により解決することを、具体的なトークンの利用法とともに提案していることも大きな特徴である。 公聴会での口頭試問結果を踏まえ、本論文は本研究科の博士学位論文審査基準を満たしており、博士学位を授与するに相応しいものと審査委員会は一致して判断した。
試験または学力確認の結果の要旨	本論文の審査に関して、2021 年 2 月 10 日（水曜日）13 時 00 分から 14 時 30 分にオンライン（Zoom）にて公聴会を開催し、学位申請者による論文要旨の説明後、審査委員は学位申請者に対する口頭試問を行った。審査委員および公聴会参加者より、公開鍵暗号を直接利用の際の処理速度の問題は計算機能力により解決可能ではないか、IC カードの利用が提案システム上で重要なのか、ブロックチェーンのシステムが何故アンパーミッション型であってそれで安全性が保てるのかについて質問があったが、いずれの質問に対しても学位申請者の回答は適切なものであった。主査および副査は、公聴会の質疑応答を通して、学位申請者が十分な学識を有し、博士学位に相応しい能力を有することを確認した。 以上の諸点を総合し、審査委員会は、本学学位規程第 18 条第 1 項に基づいて、学位申請者に対し「博士（工学　立命館大学)」の学位を授与することが適当であると判断する。