博士論文

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
(A Study on the Prevention of Tampering with e-Evidence in Criminal Procedure)

2021 年 3 月

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

小坂谷 聡

立命館大学審査博士論文

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

(A Study on the Prevention of Tampering with e-Evidence in Criminal Procedure)

２０２１年３月
March 2021

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

小坂谷　聡
KOSAKATANI Satoshi

研究指導教員：上原 哲太郎 教授
Supervisor : Professor UEHARA Tetsutaro

目 次

図 目 次

表 目 次

第１章　緒論

１.１　研究背景

今日，インターネットやコンピュータ，モバイル機器を始めとする情報通信あるいは情報処理技術の発展・普及に伴い，社会のあらゆる場面でIT化が進展し，あらゆる情報がデジタル化されている．ITは我々の生活を支える重要な社会基盤であり，ITの利用及び活用なくして社会の発展はありえないと同時に，我々が様々な場面で日々直面している社会的課題を解決するための必要な手段でもある．社会のIT化が発展・普及することによって，「人やモノの状態・活動・動作を巡る様々な情報が，デジタルデータとして記録可能」になり，その結果，「あらゆる情報がデジタルデータ」として「社会・経済活動に活用」することが可能となる[1]．当然，このようなIT化の潮流は，経済や産業の分野にとどまらず，行政や司法の分野においても及んでいる．例えば，行政機関における行政文書は，従来，紙媒体を正本・原本とするものが大半を占めていたことから，所在把握や管理業務に多大なコストがかかっていた．そのため，IT を導入し電子的に管理することにより，体系的・効率的な管理を進め，文書管理業務の効率性を向上させる取り組みが開始されている[2]．また，同じく，紙媒体の裁判書類が中心であった民事裁判手続きにおいても，適正かつ迅速な裁判の効果的・効率的な実現を図り，国民にとって一層利用しやすいものとすべく，民事裁判の IT 化への取り組みが本格化するに至っている．そして，この社会のIT化・デジタル化によって変化を求められているのは刑事手続の分野とて例外ではない．

ところで，刑事手続とは，刑事事件について，個人の基本的人権を全うしつつ，事案の真相を明らかにし，刑罰法令を適正かつ迅速に適用実現するための手続である（刑事訴訟法（以下，「刑訴法」と言う．）１条）．そして，刑罰法令を適用するための事案の解明（事実の認定）は，必ず「証拠」によらなければならない（刑訴法３１７条，証拠裁判主義の原則）．この証拠には，裁判所の職権によって収集・保全された証拠（刑訴法９９条以下参照）や被告人・弁護人によって収集・保全された証拠ももちろん含まれるが，実際の刑事裁判における影響力の大きさという点からは，捜査機関によって収集・保全された証拠が量的にも質的にも最も重要であると言える．従って，刑事手続の目的を適切に達成する上でも，捜査機関によって収集・保全される証拠の取り扱いにおける問題というものがこれまでも重要なテーマとなっていた．特に，証拠の収集・保全の過程において，捜査機関によって偽造・変造・すり替え・改ざん等が行われた場合，適正手続（憲法３１条）違反の観点から証拠として認めることを許すべきではないのは当然のこと（違法収集証拠排除），偽造等された証拠からは証明されるべき要証事実との間に何の関連性も見出すことはできず（自然的・法律的関連

性が認められない)，結局誤った事実認定の原因となることから，証拠として採用されるべきではないとされている（証拠能力が否定される)．

こうした刑事手続きにおける証拠の取り扱いに関する問題は，社会の IT 化及び情報のデジタル化の流れの中にあっても基本的な問題の構造自体には変わりはない．しかし，社会の IT 化に追随し，刑事手続きの分野においても IT 化・デジタル化への対応が余儀なくされるに伴って，これまでの延長では捉えられない課題に直面している．様々なデジタル技術が日々生み出され新たな捜査手法として採用されるようになるとともに，デジタルデータを対象とする捜査や証拠が大きな比重を占めるようになった．しかし，デジタルデータないしデジタル証拠（電磁的証拠）は，従来の書証や物証のような物理的な証拠とは異なり，それ自体，そもそも目に見えない性質を有するものである．ただでさえ，刑事手続きの実務においては，証拠の収集・保全そして保管の過程は十分に透明化，可視化されておらず，被疑者・被告人及び弁護人にとってはブラックボックスであり，捜査機関による証拠の改ざん等に対しては常に強い疑念が存在している．ましてや，それがデジタル証拠であれば，その収集・保全，保管の過程における不透明さは物理的な証拠の比ではない．加えて，デジタルデータないしデジタル証拠は，一般に改ざん・改変が極めて容易であるという性質を有しており，改ざんやすり替え等の容易さという点においても従来の物理的な証拠とは比べものにならない．詰まるところ，IT 社会を迎えた現在，捜査機関に対する証拠の改ざん疑念はこれまで以上に無視できるものではなくなり，現実問題として適正な刑事手続に対する大きな脅威となっていると見るべきである．

本来，刑事手続の分野にあっては，その目的である個人の人権保障と適切な事案の真相解明を達成する手段として IT 化が要請されなければならず，これは，社会的な課題を解決するために社会の IT 化が進められていることと同様のはずである．ところが，刑事手続きの分野では，IT 化という社会の変化に対して十分に追随できているとは言い難い状況にある．言い換えれば，社会の IT 化によってむしろより深刻な課題を抱えることになったと言える．従って，その解決に向けて，例えば立法的措置を講じることや，また，法律解釈を駆使することはもちろん重要である．しかし，それを前提としつつも，IT 化に伴う問題の場合であればなおのこと，制度を支える技術そのものの問題として捉え，そもそもそのような問題が惹起することを防止する技術的な措置を講ずることが結果的に法的安定性をもたらし，捜査の適正化・人権保障等にも資することになる．

本論文では，捜査機関による捜査のデジタル化及び証拠のデジタル化の現状を踏まえ，捜査機関におけるデジタルデータないしデジタル証拠に関する適正な取扱いという課題について，それらの性質に即し，技術的な観点からの解決策を検討する．

なお，本論文において，デジタルデータとは，デジタル（電磁的）方式によって電磁的記録媒体に記録されたデジタル（電磁的）情報一般のことを言い，デジタル証拠とは，デジタルデータが電磁的記録媒体に記録され電磁的状態で証拠化されたものを言う．また，デジタル証拠に関しては，刑法，刑訴法あるいは通信傍受法等において，「電磁的記録」と称され

ていることから，必要に応じて，法律上の呼称を使用する場合がある．

１.２　刑事手続におけるデジタル化の課題

刑事手続における捜査や証拠のデジタル化は，機械的に記録されたデジタルデータを対象とするものであり，デジタル化への流れは，自白偏重の捜査手法や人の記憶等主観的な証拠を過信する旧来の刑事手続の実態を，客観的・科学的な方向へ導くものとして期待されている．

従来の捜査員による尾行や張り込み捜査は，GPS 等の位置測位技術を利用することにより，より低コストで長時間，そして大規模に行えるようになった．また，コンピュータや携帯端末の Web ブラウザの閲覧履歴や SNS の利用履歴を取得することにより，必ずしも自白に頼らずとも，被疑者等の行動傾向や犯罪動機等の解明が容易になる．さらに，携帯電話の通信・通話履歴の取得，携帯電話等に内蔵された種々のデータの取得・解析，また，通信傍受の手法を利用することによって，犯罪の解明につながるより多くの証拠が，機械的・客観的に，そしてより容易に取得することができるようになった．

しかし，他方で，位置情報の取得捜査は，個人の私的領域に侵入しプライバシーを侵害しうる問題を孕んでいる．実際，装着型の GPS 端末を裁判所の令状もなく被疑者の車両に装着して当該車両の位置情報を取得していた捜査手法について，最判平成２９年３月１５日において，「合理的に推認される個人の意思に反してその私的領域に侵入する捜査手法である GPS 捜査は，個人の意思を制圧して憲法の保障する重要な法的利益を侵害するもの」であると判示されている[3]．また，コンピュータ，携帯端末ないし携帯電話から取得される様々なログ情報は，そのデータ量自体が膨大であるため，捜査の過程や訴訟の段階において手続の遅延をもたらしかねない状況に陥っている．加えて，捜査機関による無限定な収集活動は，被疑者・被告人のプライバシー権の重大な侵害をもたらすなど違法捜査や人権侵害を招きかねない。

また，デジタルデータを対象とした捜査手法によって大量に収集・保全されたデジタル証拠は，デジタルデータの性質上，改ざんが極めて容易であるというリスクを有しているにも関わらず，他方で，その客観的性質故に過度に信頼され過ぎるという大きな矛盾を抱えている．さらに，デジタルデータの不透明性・不可視性が捜査機関による収集・保全，保管等の過程のブラックボックス化を招いていることは前述の通りである．

このように，刑事手続におけるデジタル化の流れは，憲法上ないし刑訴法上，様々な解釈上の問題を生み，また，従来の法規制では対処できず，新たな立法化を要請する場面ももたらしており，法律上解決しなければならない課題を抱えている．その一方，デジタル技術によってもたらされた新たな捜査手法や捜査のデジタル化によって獲得されたデジタル証拠については，デジタル化された捜査や証拠の性質に即して，技術的に解決しなければならな

い問題ないし課題というものも存在する．言い換えれば，技術的な手法によって解決可能な問題というものを見極めなければならない．即ち，刑事手続のデジタル化の流れ，あるいはデジタル技術の採用・運用によって生じた新たな違法性や人権侵害のリスク，証拠の取り扱い上における問題等に対する適切な技術的課題を解決してこそ，IT 社会にとっての適正かつ迅速な刑事司法の実現が可能となる．

１.３　解決手段としてのデジタル技術

刑事手続のデジタル化の流れに伴う問題を検討する上で，新しいデジタル技術を採用した捜査手法に対する適正性の確保など，技術的に検討・解決しなければならない課題は少なくないが，その中でも特に重要な検討課題となるのが，改ざんが容易であるというデジタル証拠に特有の改ざん防止についての解決への道筋である．刑事手続とは，証拠に基づく事案の真相解明のための手続である以上，証拠に関わる課題・問題というのは、適正な刑事手続が確保されるための第一歩である．そして， IT 化された社会の中にあって，デジタル証拠の存在が大きな比重を占めるようになった今日の刑事手続においては，デジタル証拠の特性としての改ざんの容易性に起因する各種の改ざんリスクに対して如何にすればそれが防止されるのか，という問題についての解決を提示することが求められる．

本論文では，刑事手続におけるデジタル化に伴って解決すべき課題の１つとして，捜査機関によって収集・保全されたデジタル証拠の改ざん防止のための技術的な措置・枠組みについて取り上げることにする．

ところで，捜査機関が収集するデジタル証拠に関して，現行法上，一般的な規定としては，デジタル証拠の特性に基づいた改ざん防止のための規定（法制度）が特に設けられている訳ではなく，また，そのための技術的な措置が講じられている訳でもない．もっとも，特定の捜査手法において捜査機関が収集するデジタル証拠に関して，ある意味，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も評価することが可能な法律が平成２８年（２０１６年）新たに立法化された．暗号技術を利用した新たな通信傍受手法である．これは，従来，「立会人」よって担保されてきた捜査機関による傍受手続を，新たに「暗号技術」によって立会人に代替することを目的とした制度である．従って，直接的には，捜査機関による通信の傍受という特定の捜査手法の適法性を担保するために導入されたシステムであって，捜査機関が差押手続等によって収集するデジタル証拠一般についての改ざん防止のための措置ではない．しかし，捜査機関が傍受したデジタルデータを暗号化して裁判所で保管することによって，結果として，捜査機関が収集したデジタル証拠の改ざんを防止するという効果を及ぼしているという点も否定できない．

そこで，本論文では，この傍受データを裁判所で保管するというスキームが，デジタル証拠の改ざん防止のための一般的なシステムを検討する上でのヒントとなるのか，あるいは

そのための一定の示唆を与えるものとなるのかという観点から，まず，この暗号技術を利用した新たな傍受手法について，その課題や問題点などについて詳細に検討する．

そして，その上で，改ざんが極めて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策を構築する観点からより一般的なシステムとして，捜査機関によるデジタル証拠改ざん防止のための新たなシステムについて検討する．特に，捜査機関による捜索・押収、差押えによって収集・保全されたデジタル証拠が，収集後，捜査機関によって改ざんされていないことを客観的に確認するための具体的な技術システムの構築について提案する．収集作業時から電磁的に管理できるデジタル証拠の特性を利用して，押収したデジタル証拠をハッシュ化して保存するためのシステムの実現を目指すが，中立的なシステムとして捜査機関以外の第三者からでも容易に確認が可能であり，かつ改ざん耐性が認められる新しい技術として，ブロックチェーンを利用したシステムの可能性について検討し提案した．

１.４　本論文の構成

本論文は６章で構成され，各章の内容は以下の通りである．

第２章では，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，まず，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，証拠一般についての手続き及び電磁的証拠（デジタル証拠）について規定された手続きについて確認する．次いで，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った事例について概観した上で，デジタル証拠に対して裁判所がどのような姿勢で臨んでいるのかについて考察を加える．

第３章では，暗号技術を利用して新たに採用された通信傍受手法について，従来型の傍受方法との比較を通して，新設された３つの傍受方法及びそれぞれの要件等について確認する．この新たな傍受方法は，従来，捜査機関による不正に対処するための手段として立会人による立会いを適法性の担保として採用していたが，立会人に代わる新たな担保手段として暗号技術を採用した．しかし，暗号技術を利用するという手法が，果たして捜査機関の不正を抑止する機能を有しているのか，違法なプライバシー侵害の危険を払拭できるだけの技術的な裏付けが備わっているのか，ということに関しては十分に検討されているとは言い難い．また、通信文の暗号化によって捜査機関の不正が排除されるためには，通信文を暗号化するための傍受装置が適切に作動していることが前提であるが，それを客観的に担保する手段は存在するのかということも問題となる．そして，そもそも違法行為の起こりにくい傍受システムは実現可能であるのか，という問題についても検討が必要である．本章では，法が要求していると考えられる暗号化方式について検討した上で，導入にあたって想定される問題点について検討し，そこから発見される課題について解決策を探り，法の枠組みを逸脱せず違法を防止できるシステムとして，IC カードを利用した傍受システムの構築に

ついて提案し、簡易システムの実装と評価を行った.

第４章では，デジタル証拠の改ざんの容易性に関して実験を通じて検証した上で，デジタル証拠の改ざんの容易性を前提として，捜査機関による捜索・押収、差押えによって収集・保全されたデジタル証拠が，収集後，捜査機関によって改ざんされていないことを客観的に確認するための具体的な技術システムの構築について検討した．デジタル証拠の改ざん防止に関しては，押収したデジタル証拠のハッシュ値を利用する方法が最も適していることを指摘した上で，その保管システムについて既存技術と比較しながらブロックチェーンの有用性について検討する．そして，イーサリアムネットワークを利用したハッシュ値保管システムを提案し，改ざんに関するリスク評価を行った上で，その有効性を示し，最後に，システムの実装と評価を行った.

第５章では，暗号化技術を利用した通信傍受法における通信記録の記録システムに関して，一般的なデジタル証拠の保管システムへの応用（転用）の是非について評価し，ブロックチェーンを利用した証拠ハッシュ値保管システムとの関係について比較・評価を行った．そして，その評価を前提として，ブロックチェーンを利用した証拠ハッシュ値の保全システムの意義を再確認した上で，ブロックチェーンを円滑に運用するための独自のトークンエコノミーの構築について考察を加えた.

そして，最後に第６章では，結論として，第２章から第５章の各章で得られた結論を総括した．刑事手続のデジタル化の流れ、あるいは捜査及び証拠のデジタル化に伴い，解決されるべき新たな課題は少なくない．そのうち本論文では，捜査手法のデジタル化の観点からの問題として，暗号技術を利用した傍受方法についての提案を行い，また，証拠のデジタル化の観点から，デジタル証拠の改ざんの容易性に即したブロックチェーンを利用した証拠ハッシュ値保管システムの提案を通じた解決を提示し、その評価と今後の研究課題について述べる.

第２章　刑事手続におけるデジタル証拠とその課題

２.１　はじめに

刑事手続において，捜査機関による捜査活動とは，証拠の収集・保全のための活動を言う．従って，捜査機関による捜査方法の違法性，及び証拠の不適切な取り扱いにおける問題は，これまでも刑事法分野においては重要な検討課題となっていたが，今日のような社会の IT 化の流れに伴ってデジタルデータあるいはデジタル証拠の取扱量が激増するにつれ，捜査の適正性や証拠の適正な取り扱いに対する課題も，デジタル証拠に関する問題へとその比重が移りつつある．

そこで，本章では，捜査手法のデジタル化や証拠のデジタル化の問題を検討するための前提として，まず，捜査機関による証拠の収集等の手続一般，及びデジタル証拠についての手続等を概観する．そして，その上で，デジタル証拠の最大の問題点と言える改ざんの問題について，裁判実務での現状，及び課題等について検討する．

２.２　刑事手続におけるデジタル証拠の収集手続について

本節では，捜査機関によって収集される証拠（ここでは，特に，「物」としての証拠について説明する.）に関して，刑訴法上必要な手続や収集後の記録方法等に関して概観する．その上で，平成２３年（２０１１年）に新設されたデジタル証拠の３つの類型に関しても，同様に捜査機関による収集手続や記録方法について条文に即して説明する．

2.2.1　証拠の収集手続について

刑訴法上，捜査機関が証拠を収集する手段としては，犯罪現場に遺留された遺留物や被疑者・被告人、その他第三者からの任意提出物のように，捜査機関がその占有を取得する過程において強制力が行使されない「領置」（刑訴法２２１条）と，証拠物又は没収すべきと思慮する物につき強制的にその占有を取得し，または継続する処分である「差押え」（刑訴法２２１条，同２１８条１項前段，同２２０条１項２号，３項，同２２２条１項，同９９条１項，同３４６条，同９９条の２）の２つがある．また，領置及び差押えを含む概念として「押収」がある．

なお，差押えによる場合には，それが「逮捕の現場」において行われる場合を除き（刑訴法２２０条１項２号，３項)，裁判官の発する令状が必要とされる（刑訴法２１８条１項前段)．

2.2.1.1　差押手続について

捜査機関（検察官，検察事務官又は司法警察職員）は，犯罪の捜査のために強制処分が必要であると判断した時は，裁判官に対し，被疑者・被告人が罪を犯したと思慮されるべき資料を提供するとともに，差し押えるべき物，捜索等すべき場所，請求者の官公職の氏名，被疑者又は被告人の氏名，罪名及び犯罪事実の要旨等を記載した捜索・差押許可状請求書を提出し，令状の発布を求める（刑訴法２１８条，刑事訴訟法規則（以下,「規則」と言う.）１３９条，同１５５条，同１５６条，司法警察職員捜査書類基本書式例様式（以下，「様式」と言う．）２４号)．令状裁判官は，これに対して，捜索・差押えの必要性があると判断した時には，差し押えるべき物等を明示した令状（捜索・差押許可状）を発布する（刑訴法２１８条，同２１９条)．

捜査機関は，上記令状が発布されると，捜索すべき場所へ赴き令状を執行するが，その際，後述するように，処分を受ける者に令状を提示するとともに，一定の責任者（例えば，執行場所が人の住居等であれば，住居等を現実に支配管理している住居主やこれに代わるべき者）を立ち会わせなければならならない．なお，捜査段階における捜索・差押えについて規定された刑訴法２２２条１項が準用する同１１４条には，被疑者の弁護人の立会いは明記されていない（これに対し，裁判所が令状により捜索・差押えを実施する場合には弁護人も権利として立会権が明記されている（刑訴法１１３条１項)．）ことから，弁護人が住居主の代理人である場合を除いては，弁護人の立会いが認められるか否かは実状として捜査機関の裁量に委ねられている．

2.2.1.2　差押調書等の作成

捜査機関は，領置及び差押えを行った場合には，これら押収した物の「品名」や被押収人等の「住所，氏名」が記録された押収品目録が記載ないし添付された領置調書（刑訴法２２１条，同２２２条，様式２２号，同２３号参照）や（捜索）差押調書（刑訴法２１８条，同２２０条，同２２２条，同１２０条，規則９６条，様式２９号，同３０号，同３１号，同３２号，同３３号参照）を作成しなければならない．これらの調書には品名や被押収者等の住所，氏名が記録された押収品目録が記載添付される．そして，被押収者に対しては，品名，数量が記載された「押収品目録交付書」が交付される（刑訴法２２２条，同１２０条，規則

９６条，様式３５号参照)．

2.2.2　デジタル証拠について

従来，強制処分の場合には，デジタルデータが記録されたオリジナルの記録媒体からデータのみを差押えるという方法は認められていなかった．しかし，デジタルデータそのものだけが必要な場合やオリジナルの記録媒体を差押える必要がない，あるいは差押えることが不都合もしくは困難な状況も存在することから，平成２３年，情報処理の高度化等に対処するための刑法等の一部を改正する法律（平成２３年法律第７４号）により刑訴法の一部が改正され，次の通り，押収すべきデジタルデータに関し，他の記録媒体へ記録させ，その記録媒体を差押えることが可能となった．

2.2.2.1　電磁的記録についての３つの手続き

デジタル証拠（刑訴法上は、「電磁的記録」と規定されている．）については，そのデジタル情報が当初保管されてした媒体物に対する従来の差押えの他に，以下の３つ方法により差押えが可能となった．

⑴ 記録命令付差押え（刑訴法９９条の２，同２１８条１項）
裁判所が令状発布の際に，電磁的記録を保管する者等に命じて必要な電磁的記録のみを記録媒体に記録等させた上，当該記録媒体を差押える方法である．

⑵ 電磁的記録の複写等（刑訴法１１０条の２，同１２３条３項，同２２２条１項）
差し押えるべき物が電磁的記録に係る記録媒体であるときは，差押状の執行をする者が，その差押えの際にその差押えに代えて，差し押えるべき記録媒体に記録された電磁的記録を他の記録媒体に複写等した（あるいは差押えを受ける者に複写等させた）上，当該他の記録媒体を差し押える方法である．

⑶ 電気通信回線接続記録の複写（刑訴法９９条２項，同２１８条２項）
差し押えるべき物が電子計算機であるときは，当該電子計算機に電気通信回線で接続している記録媒体であって，当該電子計算機で作成・変更した電磁的記録又は当該電子計算機で変更・消去することができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから，その電磁的記録を当該電子計算機等に複写した上，当該電子計算機等を差押える方法である．

2.2.2.2　電磁的記録にかかる差押調書等

通常の差押えの場合と同様，電磁的記録についても捜索・差押えをする場合には管理者等の立会いが必要であり（刑訴法２２２条，同１１４条），差し押えた場合には，捜査機関は，（捜索）差押えの日時，場所，目的たる物，立会人，差し押えた物，差し押え経過について記録した（捜索）差押調書を作成し，また，押収品目録交付書を交付しなければならない．なお，電磁的記録の複写等の処分を行った場合及び電気通信回線接続記録の複写による差押えをした場合には，経過を記載する欄に，その旨及び経過を記載する（刑訴法２１８条，同２２２条，様式２９号，同３０号，同３１号，同３２号参照）．また，記録命令付差押えの場合には，記録命令付差押調書を作成し，記録命令差押えの日時，場所，立会人，記録させ又は印刷させた電磁的記録，記録等させた者，記録命令付差押えにより差し押えた物，記録命令付差押えの経過を記載しなければならない（刑訴法２１８条，同２２２条，同１２０条，規則９６条，様式２９の２，同３３号参照）．

２.３　刑事手続においてデジタル証拠の真正性・完全性が問題となった事例

任意処分による方法にせよ強制処分による方法にせよ，デジタル証拠を差し押える場合には，①目的となるデジタルデータが記録されているコンピュータ（電子的計算機），ハードディスクあるいはフラッシュメモリー等のオリジナルの記録媒体そのものを差押えるか（任意提出の場合であれば，領置する），若しくは②被差押者等に別途記録媒体を用意させ，その記録媒体にデジタルデータを記録させ，それを差し押える（あるいは任意提出してもらう）という方法によることになる．何れにしてもこれらのデジタルデータが犯罪立証の証拠たり得るのは，証拠化されて裁判所に提出される際に，警察や検察など捜査機関によって偽造や改ざんがなされていないということが保証されていることが前提である．しかし，以下に示す通り，刑事裁判においてデジタル証拠の真正性・完全性等が何らかの形であれ問題となった事例も実際に存在し，また，検察官でさえも自ら証拠の偽造に手を染めた不正も現実に存在している．このような事実を目の当たりにすると，もはや捜査機関であるからと言ってデジタル証拠の偽造・改ざんの危険性はないと全幅の信頼を与えることはできないと言う他ない．

そこで，本節では，実際の裁判実務において，デジタル証拠の改ざん等が問題となった事例について見ていくこととする．まず，2.3.1 節では，真正性・完全性以外の事例について概観し，次の 2.3.2 節では，真正性・完全性（改ざん）そのものが問題となった事例について見ていく．

2.3.1　真正性・完全性以外の事例

デジタルデータの解析結果についてその意義が問題となった事例として，改ざんそのものが争点となった訳ではないが，検察官によってデジタル証拠が改ざんされた，いわゆる厚労省フロッピーディスク改ざん事件として知られる一連の事例[5][6][7][8]がまずあげられる．この事件は，捜査を担当した主任検事によって差し押えられていた証拠資料であるフロッピーディスクのファイルシステム上のメタデータ（最終保存日時）が改ざんされたという事例である．主任検事は，当該フロッピーディスクを改ざんした後，これを作成者である被告人の弁護人に返還したが，返還を受けた弁護人が日時等の記録されたプロパティ情報に不審を抱いたことから，後日，専門業者によるデジタル・フォレンジック調査を依頼した．その結果，文書ファイルデータに記録されたメタデータとの齟齬が判明し改ざんの事実が発覚したというものである[9][10].

また，４人の人物が所持していたコンピュータからそれぞれウェブサイトへの書き込みを通じて実行された各殺人予告事件等が，後に，これら４人とは無関係な別の１人の人物によるコンピュータの遠隔操作等によって実行されていたことが発覚したコンピュータ遠隔操作事件[11]が有名である．この事件では，遠隔操作を実行した被告人も，当初は自分のコンピュータも遠隔操作されたと主張して無罪を争っており（最終的には公判中に自白するに至っている），被告人が職場で利用していたコンピュータのハードディスクに残った遠隔操作ウィルスの痕跡の解析結果が争点となっていた[12]．この事例もデジタルデータやデジタル証拠の改ざんの有無自体が争点となっていた訳ではないが，ハードディスク上に残されたデジタルデータの解析結果がその後の裁判の成り行きを直接左右する重要な要素とみなされた事例である．

この他にも，いわゆる電磁的記録不正作出罪や児童ポルノ関係などデジタルデータを直接対象とする犯罪以外の一般的な犯罪において，被告人の犯人性が争点となった事例で，デジタルデータの解析結果等のデジタル証拠が事実認定のための間接証拠の一つとしてその推認力が問題となった事案[13][14][15]についてもいくつか散見される[1]．もっとも，これらの事案についても，いずれもデジタルデータ自体の真正性や改ざんの可能性が争われたわけではない．

---

[1] 例えば，大阪地判平成２２年５月２５日判タ 1346 号 247 頁は，事件の凶器に関連する「ハンマー」という単語が検索されたという間接事実の推認力だけでは犯人性の立証には不十分であると判断された．また，金沢地判平成２４年３月２日（LEX/DB 25480441）や奈良地判平成２５年３月５日（LLI/DB 判例秘書 L06850138）などは，検索ログを間接事実の一つとして犯人性を推定している．

2.3.2　真正性・完全性（改ざん）が問題となった事例

デジタルデータやデジタル証拠の改ざんが直接問題となった事例である。

2.3.2.1　東京地判平成１７年３月２５日（ACCS 事件）

検察官が提出したサーバのアクセスログ（履歴）について，その改ざんが弁護人によって争われた事例である．この事例では，裁判所は，アクセスログの記録が第三者によって不正に作出された「可能性をうかがわせる具体的な事情は何ら存在しない上，第三者が被告人のアクセス記録をことさらに作出する必要性もないことから，アクセスログは正確に被告人のアクセスを記録していると認められる．」と判断した[16].

2.3.2.2　さいたま地判平成２１年７月２８日

被告人と共犯者間の PC ないし携帯メールの送受信に関して，共犯者が特殊なソフトウェアを使ってメールのヘッダ情報を書き換え，成り済ましメールを作成した事実があるとして被告人によって争われた事例である．しかし，裁判所は，「メールのヘッダー情報の書き換えが技術的に可能であるとしても」，共犯者において，「被告人との間のメールの送受信をわざわざ偽装する理由も必要性も見当たらない」として，被告人の主張を退けた[17].

2.3.2.3　高松高判平成２４年４月２６日

被告人が自らの主張を根拠付ける証拠として提出した IC レコーダに記録されたデジタル音声データについてその改ざんの有無が争われた事例である．これに対して，裁判所は，デジタルデータは痕跡を残さずに加除訂正することが容易であるとし，最終的に，やり取りの中には相当不自然な部分もあることを理由に，元の音声データに対し加除訂正が加えられたものであると認定した[18].

2.3.2.4　水戸地判平成２３年５月２０日

被告人から提出された写真データが保存されたハードディスクに関して，写真データの

EXIF 情報が改ざんされた痕跡は特に見当たらないとする捜査機関が実施した鑑定が存在するにもかかわらず，検察官がその改ざんの可能性の有無を争った事例である．しかし，裁判所は，当該写真に記録された撮影日時の情報について，人為的に改ざんが行われたことを推認させる具体的事情は特に認められないと判断し，検察官の主張を退けた．この事例では，裁判所は，一般論として EXIF 情報を編集することは編集ソフト等を使用すれば比較的容易であることを認めながらも，当該事案においては，実際にかかる編集ソフト等が使用された形跡が明らかにされた事実がないことを指摘している[19].

２.４　考察

刑事裁判においてデジタルデータやデジタル証拠の真正性・完全性（改ざん）が争点化された事例は，調査した限り現時点では件数自体は多くはなかった．しかし，個人の活動履歴としてデジタルデータがパーソナルコンピュータ，デジタルカメラ，IC レコーダ，携帯電話などの各種デジタルデバイスに記録される機会が量的にも割合的にも多くなるにつれ，そのデジタルデータが，犯罪立証あるいは犯人性立証のための重要な間接事実となることは当然の帰結である．インターネットの検索履歴やパーソナルコンピュータの操作履歴（ログ）等が裁判例に度々登場するようになってきていることはその証左である．従って，デジタルデータないしデジタル証拠の真正性や完全性が直接的な争点となる事例も今後は増加するものと考えられる．

では，何故これまでデジタルデータやデジタル証拠の改ざんが争点とされることが多くはなかったのであろうか．従来，デジタルデータが裁判で証拠として取調べ請求ないし採用される際には，紙等の媒体に再現（印刷）された形で，あるいは印刷物等と合わせて提出されることが多かったと思われる．その場合，原本データと照らし合わせ正確に再現（印刷）されているか否の確認が必要かつ重要であることは当然の前提となっていたものの，当該原本データの真正性自体にまで踏み込んで検証されることは少なかったと考えられる[2].

この点，これまでの裁判実務においては，デジタルデータに関する証拠を提出する法曹等に対する一定の信頼が暗黙の共通認識となっていたという指摘もなされているが[20]，その信頼には，デジタルデータ自体に対する信頼もあったと考えられる．つまり，デジタルデータは改変しやすい性質であるということを一般的な知識としては理解しつつも，それを現実的な問題としては必ずしも十分に捉え切れていなかったとは言えないだろうか．実際，

---

[2] この点，高橋郁夫他「デジタル証拠の法律実務Ｑ&A」272 頁では，特に供述証拠についてではあるが，伝聞法則が厳しい要件を課していることから，従来，真正性が問題になることは少なかったに過ぎないが，デジタルデータの改変可能性を考慮すると，今後は真正性についての議論がより必要になってくる旨指摘されている．

ACCS 事件においても，現に，改ざんの主張が認められるためにはその可能性を疑わせる具体的な事情が必要であるとされており，抽象的に改変・改ざんの疑念が主張されたに過ぎない場合では，たとえデジタルデータが改変可能だからといっても，証拠能力や証明力を否定するという判断がなされることは，少なくとも従前の考え方からすれば考え難い[21][22]．しかし，後述するように，デジタルデータの改ざんは，今や限られた専門家による高度な知識・技術がなければ不可能であるという状況ではない．専門的知識・技術のない素人であっても，デジタルデータの改ざん・改変を行うための情報やそれを可能にするツール等の環境はインターネット上に溢れている．このことは，捜査機関においても同じである．従って，証拠の収集保全段階において，仮に，必要な改ざん防止の措置が取られていないとすれば，それだけで，収集されたデジタル証拠は常に改ざんされた可能性が残ると見るべきである[3]．デジタル証拠に関する必要な改ざん防止の措置がとられていない場合，相手方に開示されるまでの間に改ざんする十分な時間があり，かつ，それが極めて容易であることは否定できない以上，かかる事実の存在さえ認められれば，既に改ざん行為の類型的な危険が認められる状況にあると考えられる[4]．

２.５　本章のまとめ

本章では，刑事手続においても今後ますます重要性を増すと考えられるデジタル証拠に関して，裁判実務での現状やその課題について検討した．その結果，現時点においては，裁判上，デジタル証拠の真正性・完全性が争点となった事案は，現在までのところ決して多くはないが，社会の IT 化がさらに進展・普及するにつれ，今後，デジタル証拠の重要性が増加することが見込まれることを指摘した．しかし，同時に，デジタルデータは一般に改ざんが容易でありながら，裁判所においては，捜査機関による偽造・改ざんのリスクが現実的な危険としては十分に意識されていないのではないかという課題が見える．同様に，刑訴法の改正によって新たに採用されたデジタル証拠（電磁的証拠）の差押手続に関する３つの手段

---

[3] 吉峯耕平他「デジタル・フォレンジックの原理・実際と証拠評価のあり方」122 頁では，改変防止の必要な措置が取られなかった場合，捜査機関によるデジタルデータ改変の機会は否定できず，少なくとも抽象的には改ざんの疑義が存在すると言えるが，その場合，検察官の証拠偽造事件（厚労省 FD 改ざん事件）が立証された事例が出現したことを考慮しても，なお抽象的な疑義だけでは足りないという判断が妥当するのか検討する必要がある旨指摘されている．

[4] なお，民事事件についてではあるが，大阪高判平成２１年５月１５日判タ 1313 号 271 頁は，電子メールの真正性が争われた事案に関して，「電子記録はその性質上改ざんしやすいものであるから，これを証拠として採用するためには，その記録が作成者本人によって作成され，かつ，作成後に改ざんされていないことを確認する必要がある．」と指摘している．

についても，捜査機関による改ざんなどの不正を防止するための措置は一切講じられていない．即ち，デジタル証拠の性質に即した特別な措置と言うものが一切考慮されていないのが現状である．これでは，社会の IT 化に即した新たな手続きを一見構築しているかに見えて，実際は，却って，より違法捜査を招きかねない事態に陥っているとさえ言い得る．そのため，捜査機関によってデジタル証拠が改ざんされることを技術的に防止するためのシステムが新たに必要とされることになる．

次章では，前章でも指摘した通り，捜査手法のデジタル化の観点から，改正通信傍受法によって新たに導入された暗号技術を利用した通信傍受手法について概観し，改正法が求めている要件に合致した傍受システム，あるいは違法行為の起こりにくい傍受システムについて検討及び提案を行う．そして，その次の第 4 章では，捜査機関によって押収されたデジタル証拠の改ざん防止システムについて検討及び提案を足がかりとして，最終的に，それらの検討を通じて，捜査手法のデジタル化に伴う違法捜査の抑止，及び，より一般的なシステムとして，捜査機関によるデジタル証拠改ざん防止のためのシステムに関するヒントを探っていく．

第３章　改正通信傍受法における暗号化技術を利用した新たな傍受手法

3.1　はじめに

平成２８年（２０１６年）５月，「犯罪捜査のための通信傍受に関する法律」（以下、「通信傍受法」と言う.）が施行後１６年を経て大幅に改正された（以下，「改正法」と言う.）．今回の改正法は，平成２７年（２０１５年）第１８９回国会に「刑事訴訟法等の一部を改正する法律案」として提出され，衆議院で可決（一部修正）されていた．参議院では審議未了のため継続審議となっていたが，第１９０回国会にて改めて参議院での審議等を経て可決，成立に至った．そして，令和元年（２０１９年）６月施行された．

今回の改正法では，対象犯罪の大幅な拡大と暗号化技術を使用した新たな傍受手続きの採用という２つの内容が盛り込まれている．対象犯罪は，これまでは，表 3.1 の通り，４種類の犯罪（通信傍受法・別表第１）に限定されていた．

表 3.1　通信傍受法：別表第 1 記載の犯罪

薬物関連犯罪	大麻取締法 24 条(栽培，輸入等)又は 24 条-2(所持，譲渡し等)の罪 覚せい剤取締法 41 条(輸入等)若しくは 41 条-2(所持，譲渡し等)の罪，41 条-3_Ⅰ③(覚せい剤原料の輸入等)若しくは④(覚せい剤原料の製造)の罪若しくはこれらの罪に係る 41 条-3_Ⅱ(営利目的の覚せい剤原料の輸入等)の罪若しくはこれらの罪の未遂罪又は 41 条-4_Ⅰ③(覚せい剤原料の所持)若しくは④(覚せい剤原料の譲渡し等)の罪若しくはこれらの罪に係る 41 条-4_Ⅱ(営利目的の覚せい剤原料の所持，譲渡し等)の罪若しくはこれらの罪の未遂罪 麻薬及び向精神薬取締法 64 条(ジアセチルモルヒネ等の輸入等)，64 条-2(ジアセチルモルヒネ等の譲渡し，所持等)，65 条(ジアセチルモルヒネ等以外の麻薬の輸入等)，66 条(ジアセチルモルヒネ等以外の麻薬の譲渡し，所持等)，66 条-3(向精神薬の輸入等)又は 66 条-4(向精神薬の譲渡し等)の罪 あへん法 51 条(けしの栽培，あへんの輸入等)又は 52 条(あへん等の譲渡し，所持等)の罪 国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等特例に関する法律 5 条(業として行う不法輸入等)の罪
銃器関連犯罪	武器等製造法 31 条(銃砲の無許可製造)，31 条-2(銃砲弾の無許可製造)又は 31 条-3①(銃砲及び銃砲弾以外の武器の無許可製造)の罪 銃砲刀剣類所持等取締法 31 条から 31 条-4 まで(けん銃等の発射，輸入，所持，譲渡し等)，31 条-7 から 31 条-9 まで(けん銃実包の輸入，所持，譲渡し等)，31 条-11_Ⅰ②(けん銃部品の輸入)若しくはⅡ(未遂罪)又は 31 条-16_Ⅰ②(けん銃部品の所持)若しくは③(けん銃部品の譲渡し等)若しくはⅡ(未遂罪)の罪
集団密航の罪	出入国管理及び難民認定法 74 条(集団密航者を不法入国させる行為等)，74 条-2(集団密航者の輸送)又は 74 条-4(集団密航者の収受等)の罪
組織的殺人	組織的な犯罪の処罰及び犯罪収益の規制等に関する法律 3 条_Ⅰ⑦に掲げる罪に係る同条(組織的な殺人)の罪又はその未遂罪

それが今回の改正法では，上記４類型に加え，さらに表 3.2 の通り，１１種類の犯罪（通信傍受法・別表第２）が追加された.

表 3.2　通信傍受法：別表第２記載の犯罪

爆発物の使用	爆発物取締罰則 1 条(爆発物の使用)又は２条(使用の未遂)の罪
現住建造物等放火	刑法 108 条(現住建造物等放火)の罪又はその未遂罪
殺人	刑法 199 条(殺人)の罪又はその未遂罪
傷害・傷害致死	刑法 204 条(傷害)又は 205 条(傷害致死)の罪
逮捕・監禁関係の罪	刑法 220 条(逮捕及び監禁)又は 221 条(逮捕等致死傷)の罪
略取・誘拐関係の罪	刑法 224 条から 228 条まで(未成年略取及び誘拐，営利目的等略取及び誘拐，身の代金目的略取等，所在国外移送目的略取及び誘拐，人身売買，被略取者等所在国外移送，被略取者引渡し等，未遂罪)の罪
窃盗	刑法 235 条(窃盗)の罪又はその未遂罪
強盗・強盗致傷	刑法 236 条_Ⅰ(強盗)若しくは 240 条(強盗致死傷)の罪又はこれらの罪の未遂罪
詐欺・電子計算機使用詐欺	刑法 246 条_Ⅰ(詐欺)若しくは 246 条-2(電子計算使用詐欺)の罪又はこれらの罪の未遂罪
恐喝	刑法 249 条_Ⅰ(恐喝)の罪又はその罪の未遂罪
児童ポルノ関係の罪	児童買春，児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律 7 条_Ⅵ(児童ポルノ等の不特定又は多数の者に対する提供等)又はⅦ(不特定又は多数の者に対する提供等の目的による児童ポルノの製造等)の罪

そのため，追加犯罪の中には必ずしも重大犯罪とは言いがたい犯罪が含まれていることも含め，対象犯罪がこれだけ増えれば，改正前には，年間約１０件程度しか実施されていなかったものが，今後は年間数百件にまで増加するのではないかと考えられ，市民生活にも重大な悪影響を及ぼすのではないかという批判も多く聞かれる．また，今回の改正を契機として，今後，通信傍受の対象犯罪が捜査機関にとって有用か必要かという基準によって，ことあるごとに拡大されることになるのではないかという批判もある[24].

対象犯罪の拡大とともに，今回の改正法で大きな変更となったのは後者の暗号化技術を利用した新たな傍受方法の採用である．従来は，通信傍受時には通信事業者等の立会いが必要とされ，傍受場所も事業者の施設内に限定されていたが，このことが捜査機関にとっては非常に大きな負担となっており，さらに，通信傍受の実施に対しても事実上の障害ともなってきたと指摘されている[25]．そこで，傍受手続きの合理化・効率化の観点から，新たに暗号化という技術的方法を用いることを担保として，立会人による立会いを不要とし，また，警察施設内での傍受の実施が可能となる方法を従来の傍受方法に加えて採用した．これにより，通信傍受は，捜査機関にとって格段に使い勝手の良い捜査手法となった．この新しい傍受手法は，捜査機関に傍受権限の濫用を招く懸念を抱かせるものであり，改正法が提案する技術的措置が立会人による立会いに代わり十分に捜査機関の不正を抑止する担保として機能すると言えるのか，厳しく吟味する必要がある．ところが，暗号化等の技術の採用が適切と言えるか，また，コンピュータ（特定電子計算機）による傍受が適切に運用されることが十分に担保されているか等，法改正の影響が最も大きく現れる部分については，必ずしも十分に議論されているとは言い難い状況にある．

本章では，このような問題意識から，特に，技術的側面から，今回の改正法における新たな傍受システムの概要について検討する．そして，現在想定されていると思われる傍受システムがそもそも改正法の要求する要件に技術的に合致するのか，あるいは，改正法を前提として，より違法行為の起こりにくい傍受システムとはどのようなものが考えられるか等，検討ないし一定の提案を行うものである．

３.２　暗号技術を利用した新たな傍受方法について

本節では，改正法で新たに追加採用された暗号技術を利用した傍受方法について説明するが，それとともに，新たな傍受方法のポイントを明確にするために，従来の傍受手法についても説明する．

3.2.1　従来の傍受方法について

今回，新しく暗号技術を利用した傍受方法が採用されたとしても，従来の傍受方法が廃止された訳ではなく，新たな選択肢として従来の方法に追加された形となっている．そこで，まず，従来型の傍受方法について簡単に整理する．なお，新たな傍受方法の追加に伴って，従来型の傍受方法に関する箇所についても，それに合わせて条文番号等も含め一部改正されている箇所もあるが，いずれも改正法に従って記載する．また，本章において，条文番号の記載のみで法律名の記載がない場合は，いずれも改正法のことを指している．

① 捜査機関（検察官又は司法警察員）が傍受の令状請求を行い（３条，４条１項），裁判官が原則として１０日以内の期間を定めて傍受令状を発布する（５条１項）．
② 捜査機関は，通信事業者に令状を提示する（１０条）．
③ 捜査機関は，通信事業者の施設内において，傍受すべき通信について，立会人の立会いのもと傍受を実施する（３条，１３条）．
④ 捜査機関は，傍受すべき通信に該当するかどうか明らかでないものについては，該当性判断のため必要最小限度に限り傍受する（１４条）．
⑤ 捜査機関は，傍受終了後傍受した通信について全て記録媒体に記録する（２４条）．
⑥ 立会人は，記録媒体を封印する（２５条）．
⑦ 捜査機関は，封印された記録媒体を遅滞なく裁判官に提出する（２５条４項）．

このように，従来方式による傍受方法は，実施手続自体はそれほど複雑ではない．従来方式による傍受方法の場合，不正の防止策については，立会人による傍受手続の常時立会いと記録媒体への封印の２つの措置が用意されていることが分かる．立会人制度には，常時監視の中で通信傍受を実施させることによって，捜査機関による違法な傍受手続きを防止する

役割が期待されている．但し，立会人には，当該傍受の実施に関して意見を述べることはできるが（１３条２項），通信の内容についてまでのチェック機能はなく，あくまでも外形的なチェックができることに留まることから，不正防止にとっては必ずしも万全なものとは言い難いものである．もっとも，全国で一箇所とされる通信事業者の施設に捜査官が出向き，立会人を予め全て準備しなければ実施できないという点で極めてハードルの高い捜査方法であり[26]，また，立会いには人の目があることにより，捜査機関が違法行為を行いにくくなるという事実上の抑止効果が認められていたと言える[27].

3.2.2　改正法で新設された３つの傍受方法

次に，今回の法改正に伴い新たに追加採用された以下の 3 つの傍受方法について検討する．いずれも，暗号化技術が採用され（２条４項ないし６項），従来方式の傍受手続で不正防止の要を担っていた立会人による立会いは不要とされている（２０条１項，２３条１項）．なお，これらの方法による傍受を行うには，いずれも裁判官の許可を受けることが必要であることにはこれまで通り変わりはない（４条３項，２０条１項，２３条１項）．

3.2.2.1　通信事業者での「一時的保存」の方法による通信傍受（２０条１項）

１つ目は，通信事業者の管理する施設において，傍受令状記載の傍受可能期間内のうち，検察官及び司法警察員が指定する期間（指定期間）に行われる全ての通信について，「暗号化」[5]させた上一旦「一時的保存」[6]の方法によりこれを「傍受」し，事後的に，同施設（この場合，通信事業者の管理する施設が傍受の実施の場所となる．）において，暗号化された通信を「復号」[7]して「再生」[8]する方法である．なお，この方法による傍受の場合に，立会が不要とされているのは（２０条１項），傍受の実施を直接担っているのが通信管理者であり（２０条１項），検察官及び司法警察員は，そもそも指定期間内に傍受の実施の場所に立

---

[5] 「暗号化」とは，通信の内容を伝達する信号，通信日時に関する情報を伝達する信号その他の信号であって，電子計算機による情報処理の用に供されるもの（以下「原信号」という．）について，電子計算機及び変換符号（信号の変換処理を行うために用いる符号をいう．以下同じ．）を用いて変換処理を行うことにより，当該変換処理に用いた変換符号と対応する変換符号（以下，「対応変換符号」という．）を用いなければ復元することができないようにすることという（２条４項）．

[6] 「一時的保存」とは，暗号化信号について，その復号がなされるまでの間に限り，一時的に記録媒体に記録して保存することをいう（２条５項）．

[7] 「復号」とは，暗号化により作成された信号（以下，「暗号化信号」という．）について，電子計算機及び対応変換符号を用いて変換処理を行うことにより，原信号を復元することをいう（２条４項）．

[8] 「再生」とは，一時的保存をされた暗号化信号（通信の内容を伝達する信号に係るものに限る．）の復号により復元された通信について，電子計算機を用いて，音の再生，文字の表示その他の方法により，人の聴覚又は視覚により認識することができる状態にするための処理をすることをいう（２条６項）．

ち入ることができないからである（２０条５項）．他方，再生の実施時については，従前通り立会いは必要とされている（２１条１項，１３条）．いずれにしても，この方法では，捜査機関が通信内容を聴取するのが傍受時ではなく，事後的な再生時であるという違いはあるものの，実質的には従前の傍受方法と同視できる（再生という方法によって傍受を事後的に再現している）と評価することも可能である．

3.2.2.2　通信事業者から通信を送信させ捜査機関の施設で特定電子計算機を用いて傍受する方法__その１（２３条１項１号）

２つ目は，通信事業者の管理する施設内で傍受するのではなく，通信事業者に，傍受の実施をしている間に行われる全ての通信について暗号化した上で捜査機関の施設（この場合，捜査機関の施設が傍受の実施の場所となる．）に設置された特定電子計算機[9]に伝送させ，その伝送された暗号化信号を受信するのと同時に，即時に（リアルタイムに）復号をし，傍受をする方法，即ち，リアルタイム方式（２３条１項１号）である．

3.2.2.3　通信事業者から通信を送信させ捜査機関の施設で特定電子計算機を用いて傍受する方法__その２（２３条１項２号）

３つ目は，同じく，傍受の実施をしている間に行われる全ての通信について暗号化した上で捜査機関の施設（この場合，捜査機関の施設が傍受の実施の場所となる．）に設置された特定電子計算機に伝送させ，その伝送された暗号化信号を受信するのと同時に，今度は，一時的保存をする方法により傍受をする方法，即ち，一時的保存方式（２３条１項２号）である．この方法によって傍受をした場合には，事後的に上記特定電子計算機において復号をし

---

[9] 「特定電子計算機」とは，次に掲げる８つの機能の全てを有する電子計算機をいう（２３条１項２号）．

ⅰ)伝送された暗号化信号について一時的保存の処理を行う．
ⅱ)電装された暗号化信号について復号の処理を行う．
ⅲ)リアルタイム方式において通信を傍受する同時に，又は一時的保存された通信を再生すると同時に，全て自動的に，暗号化の処理をして記録媒体に記録する．
ⅳ)傍受の実施をしている間における通話の開始及び終了の年月日時，リアルタイム方式で傍受した通信の開始及び終了の年月日時，一時的保存された通信の再生をした場合の通信の開始及び終了の年月日時その他政令で定める事項に関する情報を伝達する原信号を作成し，当該原信号について，自動的に暗号化の処理をして４号の記録媒体に記録する．
ⅴ)３号の記録媒体に記録される同号の通信及び４号の原信号について，３及び４号に掲げる機能により当該記録媒体に記録するのと同時に，暗号化処理をすることなく他の記録媒体に記録する．
ⅵ)入力された対応変換符号２号に規定する復号以外の処理に用いられることを防止する．
ⅶ)入力された変換符号が３及び４号に規定する暗号化以外の処理に用いられることを防止する．
ⅷ)１号に規定する一時的保存をされた暗号化信号について，２号に規定する復号をした時に，全て自動的に消去する．

た上で再生する．但し，この方法による再生の場合には，同じく再生を必要とする１つ目の方法（２０条１項）による場合とは異なり，立会人による立会いは必要とはされていない（２３条４項)．

３.３　特定電子計算機を使用した傍受方法について

これら３つの新しい方式のうち，今回の改正法の特徴を最もよく表していると言え，また，多くの問題点も指摘されているのが，２つ目と３つ目の方式，即ち，捜査機関に設置された特定電子計算機を用いた方式である．そこで，以下では，特にことわりのない限り，この特定電子計算機を用いた方式（２３条１項１号，２号）を念頭に議論を進めることにする．

3.3.1　特定電子計算機を使用した傍受実施手続きの概要

特定計算機を使用した傍受実施手続きの概要については以下の通りである．

① 捜査機関が傍受の令状請求を行い（４条１項，３項)，裁判官が令状を発布する（５条１項，３項，６条２項)．
② 裁判所は，変換符号を作成し通信事業者に提供するとともに，対応する対応変換符号を作成し指定された特定電子計算機以外で使用できない措置を講じた上で捜査機関に提供する（９条１項２号イ，ロ)．
③ 裁判所は，変換符号を作成し捜査機関に提供するとともに，それに対応する対応変換符号を作成し自ら保管する（９条１項２号ロ，ハ)．
④ 捜査機関は，通信事業者に令状を提示する（１０条)．
⑤ 捜査機関は，通信事業者に命じて，通信を暗号化させ，捜査機関の施設に設置された指定特定電子計算機に伝送させる（２３条１項)．
⑥ 捜査機関は，暗号化された信号を受信すると同時に，ｉ裁判所から提供を受けた対応変換符号を特定計算機に入力して即時に復号し傍受する（２３条１項１号)．あるいは，ii一時的保存の方法で傍受を行った後，事後的に対応変換符号を用いて復号した上で再生し聴取する（同２号，同条４項)．
⑦ 捜査機関は，傍受ないし再生した通信を裁判所より提供を受けた変換符号により自動的に暗号化させて記録媒体に記録する（２３条２項３号，２６条１項)．

3.3.2　３つの暗号化方式について

特定計算機を用いた方式においては，前述の通り，通信事業者の施設において，通信が暗号化され，それが捜査機関に設置された特定電子計算機において復号されるという規定となっているが（２３条１項１号，２号)，ここで行われる暗号化の処理は，裁判所で作成された「変換符号」を通信事業者に提供することによって行われる（９条１項２号イ，２条４項)．また，復号は，同じく裁判所で作成された上記変換符号の「対応変換符号」を，今度はそれを捜査機関に提供することによって行われる（９条１項２号ロ，２条４項)．

なお，ここで規定されている「変換符号」及び「対応変換符号」とは，暗号方式に用いられるいわゆる「暗号化鍵」ないし「復号鍵」のことを指している（２条４項)．

ところで，暗号方式には，大きく分けて，①共通鍵暗号方式と，②公開鍵暗号方式がある．①の共通鍵方式とは，文字通り，暗号化と復号において同じ鍵（共通鍵）を使用する方式である．この方式の場合，通信内容の盗聴防止のために，送受信者当事者以外の第三者に対してはこの共通鍵は秘密でなければならない．改正法に即して言えば，変換符号もその対応変換符号も同じ共通鍵ということになる．これに対して，②の公開鍵方式とは，暗号化と復号に異なる鍵を使用する方式である．暗号化の鍵と復号の鍵は対になっており，一方の鍵（公開鍵 Kp）で暗号化した場合，それに対応するもう一方の鍵（秘密鍵 Ks）でしか復号できない．改正法に即して言えば，変換符号が暗号化に用いる鍵（公開鍵）となり，対応変換符号が復号に用いる鍵（秘密鍵）となる．なお，この方式が公開鍵方式と呼ばれるのは，復号に用いる鍵は秘匿される（秘密鍵）一方，暗号化に用いる鍵は公開される（公開鍵）という性質に由来する．また，公開鍵方式は，通信内容の盗聴を防止するという本来の目的に加え，電子署名と呼ばれる機能を通じて送信者の認証にも使われる．即ち，通信文を公開鍵（鍵 Kp）で暗号化した場合，秘密鍵（鍵 Ks）を持つ者しか復号できないことにより盗聴防止という本来の機能を果たす一方，秘密鍵（鍵 Ks）で通信文が電子署名された場合には，公開鍵（鍵 Kp）でしかその署名を確認（検証）することができず，このことは，送信した者は秘密鍵（鍵 Ks）を持つ者に限定されるということを意味する．

そして，この共通鍵方式と公開鍵方式の２つの方式を組み合わせたものとして，③ハイブリッド方式がある．この方式は，通信内容の暗号化自体には共通鍵方式を用いる一方，それとは別に，一対の公開鍵と秘密鍵を用意し，通信に先立ち暗号化に用いる共通鍵を公開鍵方式で交換するというものである．これは，共通鍵方式と公開鍵方式を比較した場合，鍵交換時の漏洩のリスクを考慮すれば一般に公開鍵方式の方がより安全であると考えられているものの，他方，公開鍵方式は，共通鍵方式に比べ処理のための負荷が膨大であるというデメリットが存在することから，両者の利点を組み合わせた方式として考案されたところに基づく．

3.3.3　改正法が要求していると考えられる暗号化方式とは

では，改正法においてはいずれの暗号化方式が想定されていると言えるであろうか．

この点，どの暗号化方式を採用しなければならないという規定は，明文上は規定されていない．そうすると，変換符号と対応変換符号についても同じ一つの共通鍵として作成することも必ずしも否定されている訳ではないとも考えられる．実際，２０条１項による傍受の場合，暗号化と復号は，通信事業者によって行われることを考えれば，変換符号と対応変換符号について，敢えて一対の公開鍵と秘密鍵として作成する必要性は乏しいとも言える．また，法案の検討段階ではあるが，「法制審議会新時代の刑事司法制度特別部会」（以下，「特別部会」という．）においても，都道府県警察での傍受装に「装置の真正性を確認した上で共通鍵を入力」と共通鍵を前提とした記載も見られる[28]．

但し，改正法においては，暗号化及び復号に用いるための鍵として，「変換符号」及び「対応変換符号」という２種類の鍵（符号）が区別されて明記されていることに注意しなければいけない（２条４項，９条１項，２０条１項，２１条１項，２３条１項等）．そうすると，これらの鍵は，普通に考えれば，共通の１つの鍵としてではなく別個の２つの鍵として作成されるものと想定されていると考えるのが自然な解釈であると言えよう．即ち，法は，公開鍵方式の採用を予定していると考えられる．特に，特定電子計算機を用いる通信傍受の場合（２３条），裁判所から変換符号の提供を受けて暗号化する主体と，対応変換符号の提供を受けて復号する主体が，それぞれ，通信事業者と捜査機関と異なっていることもそれを裏付けている．

もっとも，公開鍵方式の場合，暗号化や複合に巨大な桁数の冪乗算や整数除算，剰余算などを利用することから，暗号化や復号の際には常に莫大な量の計算を行うことが要求される．そのため，暗号化ないし復号にかかる処理時間は，比較的単純な処理の組み合わせから構成されている共通鍵方式の場合と比べ実に数百倍も遅くなると言われている．しかし，これでは，通信の内容など長文の暗号化には時間がかかり過ぎて到底実用に耐えるものとはなり得ない．実際，高速な秘密通信が要求される分野においては，公開鍵方式が直接使用されることはないとされている．

そこで，公開鍵方式と共通鍵方式による暗号化及び復号処理にかかる処理時間の差異を確認するため，ここで，予備実験として次の比較実験を実施した．

３.４　音声ファイルの暗号化・復号実験

3.4.1　実験環境

実験環境は以下の通りである.

⑴　実験対象ファイル
MP3 音楽ファイル
容量：５.１MB
サンプルレート：４４,１００
再生時間：４分１４秒

⑵　使用 PC の仕様
Mac Book Pro (Early2015)
OS : Mac OS v.10.12
プロセッサ ：2.7GHz Intel Core i5
メモリ ： ８GB

⑶　プログラミング言語
Python3.5.2
暗号化用パッケージ：PyCrypto

3.4.2　暗号化および復号のためのプログラムの仕様

⑴　公開鍵方式
① RSA 方式による.
② 暗号化処理の手順
鍵長を 2048bit として，公開鍵，秘密鍵の鍵ペアを作成する.
対象ファイルをバイナリ形式で読込む.
RSA 方式の場合，鍵長に応じて暗号化できる平文の長さに上限がある．鍵長 2048bit の場合，パディング処理を考慮すれば 245 バイトまでしか暗号化できないので，上記バイナリデータを 1 ブロックとして 245 バイトずつ取り出し，公開鍵を用いて暗号化した上で，それを新規暗号ファイルに順次書き込んでいく.
なお，最後のブロックの長さは，対象ファイルの長さに応じて，1 バイトから 245 バイトとなる.

③ 復号処理の手順

RSA では鍵長 2048bit の場合，暗号化された平文の長さは 256 バイトになるので，上記暗号化ファイルから 256 バイトずつ取り出し，秘密鍵を用いて復号した上で，それを新規復号ファイルに順次書き込んでいく．

⑵ 秘密鍵方式

① AES 方式及び ECB モードによる．

② 暗号化処理の手順

AES 方式はブロック暗号であり，暗号鍵は 16 バイト，24 バイト，あるいは 32 バイトのいずれかでなければならない．今回は，32 バイトの暗号鍵を作成する．

また，暗号化の対象となる平文は 16 バイトの倍数でなければならない．

対象ファイルをバイナリ形式で読込み，16 バイトを 1 ブロックとして暗号化処理を行い，最後のブロック長（バイト長）が 16 の倍数でなければ，バイナリデータ（'_'）でパディング処理を行った上で同じく暗号化処理を行って，新規暗号ファイルに書込んでいく．

③ 復号処理

暗号鍵を使用し上記②で暗号化した対象ファイルに対して復号処理を行う．

そして，最後のブロック長（バイト長）が 16 の倍数でなければ，暗号化の際に追加したパディング文字（'_'）を削除して，最後のブロック長（バイト長）を１６の倍数にして新規復号ファイルを作成する．

3.4.3 処理時間の比較

⑴ 比較方法

対象ファイルに対して，上記公開鍵方式及び共通鍵方式プログラムをそれぞれ実行し実行時間を計測した．

計測方法は，Python の time モジュール内の time 関数を使用し，現在の時刻を調べ，各プログラムの処理を行い，最後にその時点の時刻を取得し，計測値の差を取る．この計測を各１０回ずつ行い各平均値を取る．

⑵ 計測結果

計測結果は以下の通りである．（単位：秒）

① 共通鍵方式

全行程にかかる時間　　：　0.1360

② 公開鍵方式

i　全行程にかかる時間　：　273.980
ii　鍵の生成時間　　：　　0.967
iii　暗号化時間　　：　16.805
iv　復号時間　　：　256.207

3.4.4　考察

5.1MB の MP3 音楽ファイルに対して，鍵の作成から暗号化及び復号に至る全行程にかかる時間について計測した．共通鍵方式の場合，約 0.14 秒程度であったところ，公開鍵方式の場合では，4〜5 分近くの時間を要し，公開鍵方式の場合，共通鍵方式の場合に比べ約 1950 倍もの時間を必要とすることが確認できる．また，公開鍵方式の場合，鍵ペアの生成時間だけでも約 1 秒を要しており，これだけで共通鍵方式の場合の全行程の 7 倍近くの時間を要している．以上の予備実験の結果からも明らかなように，公開鍵方式では処理に要する時間が共通鍵方式の場合に比して極めて大きいということが改めて確認された．特に，公開鍵方式の場合，復号にかかる時間が大半を占めているが，このことは，捜査機関が利用する傍受装置（特定電子計算機）での処理時間により影響を及ぼすことを意味する．通信量や装置の処理性能によっては再生の際に大幅な遅延や品質の悪化が生じることも考えられる．

この予備実験の結果から，共通鍵方式に比べ公開鍵方式の処理速度が大幅に遅いということが確認された．実際，通信データの暗号化の際に，公開鍵方式がそのまま用いられることは通常なく，一般的にも，両者の長所を生かしたハイブリッド方式が採用されている．

そこで，改正通信傍受法における暗号化システムにおいても通信データ等の暗号化の際に一般的に利用されているハイブリッド暗号化システムについて検討されるべきであるが，この場合，先に検討した通り，文理上，公開鍵方式を採用しているとも考えられる改正法に抵触するのではないかということが問題となる．

3.5　ハイブリッド方式の採用

ハイブリッド方式では，まず，送信者（X）が暗号化及び復号のための共通鍵（Kc）を受信者（Y）の公開鍵（Kp）を用いて暗号化し（Kp(Kc)）[10]，それを Y に送る．そして，Y は自身の秘密鍵（Ks）を用いて復号した共通鍵（Kc）を取得する．そして、X ないし Y は，共通鍵（Kc）を用いて通信データ（D）を暗号化し（Kc(D)），それを Y ないし X に送信する．そして，最後に X ないし Y は，これを共通鍵（Kc）で復号する．

[10] 鍵 A を用いてデータ B を暗号化（復号）した場合，A(B)と表現する．以下，同じ．

では，次に，これを改正法（２３条１項）に即して適用する場合，どうすればよいか．

まず，暗号化に用いる変換符号と復号に用いる対応変換符号と共通鍵（Kc），公開鍵（Kp），秘密鍵（Ks）の関係について検討する．捜査機関に提供される対応変換符号（9 条２号ロ）は，指定の特定電子計算機以外では使用できてはならず（9 条２号ロ），また，復号以外の処理に用いられることも許されていないことを考えれば（23 条２項６号），両者を同じ鍵としてそのまま利用すれば完全に法に抵触する可能性がある．従って，変換符号と対応変換符号はそれぞれ異なった鍵でなければならないと考える．そこで，前者を公開鍵（Kp），後者を秘密鍵（Ks）と考えてみる．しかし，ハイブリッド方式の場合，Kp も Ks も通信データの暗号化には直接関与しないことから，それでは９条２号イロに抵触する可能性がある．そこで，基本的な枠組みとして，次のように考える．まず，裁判所が，通信文を暗号化するための共通鍵（Kc）を作成し，通信事業者と捜査機関の双方に対し提供する．但し，捜査機関へ提供する鍵は，Kc そのものではなく，公開鍵（Kp）で暗号化された状態のものである（Kp(Kc)）．そして，通信事業者は，通信データ（D）を Kc で暗号化し（Kc(D)），捜査機関は，Kp(Kc)を，同じく裁判所から提供を受けた Ks で復号し Kc を入手した上で，通信業者から伝送された Kc(D)を，取得した Kc で復号する．

このように考えれば，捜査機関に提供される Kp(Kc)は，通信事業者に提供される Kc とは，符号的には別個のものであり，その限りで法の要求も満たし得ると評価できる．

３.６　改正法における傍受システムにおいて検討されたリスクないし問題点

ところで，こうした暗号化技術を利用した新しい通信傍受の仕組みの導入にあたっては，当然新しい仕組み故の様々なリスクや問題点が懸念されるところであり，十分な検討が必要となる．そこで，暗号技術を利用した通信傍受の導入にあたり，検討段階で想定された各種のリスクについて，ここでは，特別部会で検討されていた課題を中心に見ていく．

3.6.1　特別部会において想定していたリスク

まず，特別部会においても検討されたリスクについて検討する．

3.6.1.1　通信データの漏洩・改ざんのリスク

当該傍受システムでは，通信事業者から捜査機関へ通信データが伝送される仕組みとなっていることから，まず，当該データの伝送中の漏洩ないし改ざんのリスクが問題となる．

しかし，この点については，そのための暗号化であり，現代暗号の適切な採用を誤らなければ，特別部会が指摘するように問題はないであろう．なお，確実なセキュリティ対策として，専用回線を設けるなどの解決策も提示されているが[29]，全国の警察署等から専用回線を設けるとなるとその費用も膨大となるだろうし，現実的とは言えまい．もし，かかる措置を講じなければ十分なセキュリティを確保できないとするなら，そもそも本システム自体が信用できないことを意味する．

3.6.1.2　鍵管理におけるリスク

むしろ，それよりも重大なリスクとして想定されるのは，鍵自体が不適切な管理等に伴い漏洩するリスクであろう．即ち，通信事業者で暗号化された通信文を復号するための対応変換符号は，裁判所から捜査機関へ提供されることになっており（9 条 2 号ロ），そのため，適切に管理することが期待されている．しかし，その捜査機関が提供された鍵を特定電子計算機に一旦入力したとしても，その後，それを抜き取り不正に使用する危険性は否定できない．特に，捜査機関による不正な取り出しについては，通信データの改ざん等の問題に直結するためにその問題は重大である．

この点，対応変換符号がハードディスクに書き込まれる仕様であれば，容易に取り出すことが可能であるが，揮発性メモリに書き込まれる仕様を採用するなどすれば，取り出しは不可能であるいう指摘も見られる[30]．しかし，メモリ内部を直接読み取るなど物理的に解析する方法や，演算装置が秘密情報を処理する際の処理時間や消費電力等の情報伝達路を解析して情報を取り出す，いわゆるサイドチャンネル解析など，耐タンパ性に対する攻撃技術も日々進歩していることから，今後，具体的かつ十分な検証が必要とされるだろう．

3.6.1.3　原記録改ざんのリスク

捜査機関において傍受された通信データは，特定電子計算機によって記録媒体に記録され，遅滞なく裁判官に提出されることになっているが (26 条 1 項，4 項，9 条 2 項 3 号等)，その際，捜査機関によって原記録媒体の内容が改ざんされるのではないかということも問題となる．この点，特定電子計算機には，記録媒体に記録の過程で自動的に暗号化処理を施す仕組みが採用されている（23 条 2 項 3 号，4 号）．またその暗号化のための変換符号（9 条 2 項ロ）は暗号化以外の処理には利用できず，通信事業者から伝送された通信データを復号するための対応変換符号（9 条 2 項ロ）では復号できないとされていることから（23 条 2 項 6 号，7 号)，記録媒体に記録の過程で改ざんされることや，特定電子計算機において復号されることは不可能であると説明されている[31][32]．

しかし，それも，特定電子計算機に求められている上記の仕組み等が適切に機能して初めて担保され得ることである．また，記録媒体に記録された原記録自体が改ざんできなくても，後述するように，別の手段で記録媒体それ自体をすり替えるなどの方法も考えられる．

3.6.1.4　不正な傍受装置（特定電子計算機）を使用して通信データを傍受するリスク

また，捜査機関が，指定された特定電子計算機以外の不正な装置に対して，復号鍵を入力して通信内容を聴取する可能性も考えられる．この点については，特別部会での検討によれば，ハッシュ値を利用することによって傍受装置（特定電子計算機）が真正であるか否かを確認した上でなければ復号のための鍵を入力することができないとする説明がなされている[33].

但し，その具体的な方法や詳細等に関しては不明である．

3.6.1.5　所定の装置と同時に不正な装置にもデータを伝送させ傍受するリスク

さらに，指定された特定電子計算機を使用せずに，別の不正な特定電子計算機を使って，あるいは指定された特定電子計算機の使用と同時に，通話内容を別の不正な傍受装置にも送信させ，全通話を傍受する可能性についても考えられる．これに対しては，復号鍵がないために復号することはできず傍受は不可能であると指摘されている[34]．しかし，復号鍵については，捜査機関が保管しているものであって，それを複製することも技術的には不可能とは言えないだろう．

3.6.1.6　スポット傍受を利用して全会話を傍受するリスク

最後に，捜査機関が，所定の特定電子計算機を使用したとしても，スポット傍受[11]の時間を極めて長くすれば，実質的に全会話を傍受できるのではないかという問題も指摘されている．この問題に対しても，上記ハッシュ値を利用した傍受装置の真正性確認の手段や原記録には全ての記録が残っているため，そのようなことをしても不正は発覚するので心配な

---

[11] 捜査機関は，傍受すべき通信に該当するかどうか明らかでないものについては，傍受すべき通信に該当するかどうかを判断するために必要最小限度の範囲に限り，当該通信の傍受ないし再生ができる（２３条４項，２１条３項）．このように一定時間ごとにごく短時間の傍受等を繰り返す方法についてスポット傍受と呼ばれている．

い旨説明されている[35].

しかし，それが果たして有効な手段なのかについて疑問が残るということは前述の通りである.

3.6.2 それ以外に想定されるリスクないし問題

上記のように特別部会においても一定のリスク等については検討されている．しかし，想定されるリスクないし問題点についてはそれだけではない.

以下において，この点について検討する.

3.6.2.1 特定電子計算機についてのリスクないし問題

前述の通り，本傍受システムの適正性ないし安全性は，特定電子計算機等の傍受機器が，法律上の仕組みや改正法２３条１項２号が要求する要件等に合致し適正に作動して初めて担保されるものである．特定電子計算機が適正に作成されるのか，そして作動するのか，また，想定通りに機能するのか，等という点については根強い不信が払拭されないでいる[36]. この点については，未だ具体的な仕様書等も公開されていないので現時点では詳細な検討はできないが，既にシステムの運用も開始されており，今後，一定の時間が経過することによって，しっかりとした客観的な検証が必要となることは言うまでもない[37]．しかし，そもそも特定電子計算機に求められる機能を実現するためにソフトウェアでの作り込みが前提となっていると考えた場合には，例えば，特定電子計算機を改ざんし聴き放題のラインを引くことができるようなセキュリティホールやプログラム上のバグなどの機能面での脆弱性はないのか，あるいは，１つの機能を実現することによって他の機能のセキュリティが犠牲になることはないのか，全ての機能が相互に矛盾なく作用するのかなど，ソフトウェアでの作り込みに内在するリスクは列挙すれば切りがない.

3.6.2.2 鍵転送中の漏洩のリスク

また，復号鍵については，上記のような管理中におけるリスクだけではなく，例えば，裁判所から提供される過程で第三者等に盗まれたり，または，捜査機関自身が入力（使用）前に複製するなどして不正に利用することも十分に考えられる．これについては，必ずしも十分な議論がなされていたとは言えない.

3.6.2.3　立会人の担保機能として十分機能していない問題

従来，立会人に求められてきた役割は，捜査機関による通信傍受の実施手続きが公正に行われているか，捜査機関による違法な通信傍受を抑止することができるかという点にあった．この点，暗号化等の情報技術を使えばそれは可能であるという議論に対して，立法化の過程においてもあまり異論がなかったと報告されている[38]．また，通信事業者が，傍受実施期間内において行われた全ての通信を暗号化した上で特定電子計算機に伝送することから，通信事業者自身によって，①傍受のための機器を接続する通信手段が令状によって許可されたものに相違ないこと，②令状によって許可された傍受期間等が遵守されている点については既に担保されていることに加え，特定電子計算機は，傍受ないし再生した通信を同時に全て自動的に暗号化して記録する機能を備えていることから，③傍受した通信について全て録音されているかという点についても立会人に代替しうるという指摘もある[39]．

確かに，新しい傍受手法においても，前二者（①及び②）については，通信の暗号化の処理が通信事業者の施設で行われるため，改正前の傍受における立会人の担保機能と同程度に担保されていると期待することは可能である．しかし，その後の手続きについては，通信事業者という捜査機関にとっての第三者が関与することは一切予定されていない．つまり，ここで問題とされている捜査機関の管理施設内での復号及び傍受ないし再生の手続きにおいては，捜査機関の違法行為をチェックしうる第三者は存在しないため，③の手続きは従来と異なり立会人を十分に代替しうる担保があるとは言えない．

さらに③の点については，刑事手続きにおいて使用するための記録を作成するために，暗号化の処理をすることなく他の記録媒体に記録することが認められている（23 条２項５号，24 条１項後段，26 条２項）．従って，この記録媒体を改ざん等して原記録とすり替える可能性についても技術的には可能であり，それ故，かかる不正が不可能であるということを担保しておく必要がある．

そもそも，暗号化技術は，通信の過程において，通信内容が盗聴，改ざん等されないかという点に対して効果を発揮する技術であって，伝送され復号された後の手続きの適正さを担保する役割を期待することは適切とは言えないため，傍受手続の現場での外形的チェックに代わるものではない[40]．この点について端的に問題点が指摘されているのが，スポット傍受が適正な方法で行われているのかという問題である．この問題については，傍受内容の暗号化だけでは立会人の代替手段とはならない．これに対しては，事後的に不正が行われたかどうかの検証が可能であるとして，立会人がいる場合と本質的な部分で差異はないという反論がなされている[41]．しかし，傍受の経過が全て適切に記録されるのかということに対して十分な担保がない状態では，この部分はまさに立会人による担保と本質的に異なるのではないだろうか．

3.6.2.4　暗号化方式に関する問題

最後に，暗号化方式自体における問題があげられる．改正法において想定されている暗号化方式は，文理上，公開鍵方式と考えるのが最も素直な解釈であるというのは前述の通りである．しかし，公開鍵方式の場合，巨大な桁数の素因数分解など複雑な数学的計算の困難性を利用して安全性が構築されていることから，暗号化や復号の際には常に莫大な量の計算を行うことが要求される．そのため，公開鍵方式による暗号化ないし復号にかかる処理時間は，比較的単純な処理の組み合わせから構成されている共通鍵方式の場合と比べ，一般的に，実に数百倍も遅くなることは，前述の予備実験の通りである．しかし，これでは，電話通信の内容など長文の通信の暗号化には時間がかかり過ぎて到底実用に耐えるものとはなり得ない．実際，高速な秘密通信が要求される分野においては，直接公開鍵方式が使用されることはない．

このように，改正法の規定に従い，その求めるところを忠実に満たそうと考えた場合，前述の通り，解釈上別の考え方が可能であるとしても，果たして傍受システム自体を構築することが可能なのかということが，傍受システムを実際に稼働させる上で大きな問題となっている．

3.7　運用が開始された通信傍受システムにおける暗号化方式について

ところで，改正通信傍受法については 2019 年 6 月から施行され，暗号技術を利用した通信傍受システムについても運用が開始されている．現時点においては，施行後まだ日が浅く，実際にどのようなシステムが構築されたのか，また運用実態等についても十分な情報が乏しいことから，現在入手できた資料等を前提に検討を加えるものとする．ここでは，法律の立法段階において，警察庁の求めに応じて作成され，立法段階の資料として法務委員会の議員等に提供された民間専門機関よって作成された調査報告書[42]（以下，「調査報告書」と言う．），及びこの調査報告書等を参考に作成されたと考えられる技術仕様書[43]その他の資料をもとに採用されたと推測されるシステムに関して考察する．

3.7.1　推測される運用システムについて

まず，調査報告書では，装置の真正性を認証する方法として公開鍵方式を提案している．即ち，裁判所で作成した公開鍵と秘密鍵のペアのうち秘密鍵を装置のハードディスクに格納する一方，鍵媒体（トークン）には公開鍵で暗号化された通信暗号化鍵を格納し，それを

装置に挿入することにより，通信暗号化鍵の復号が完了した場合に，正規の装置に正規の鍵が挿入されていると判断する[44]．そして，通信データを暗号化し送信するプロセスについては，まず，データ暗号化鍵と送信装置の公開鍵で暗号化した通信暗号化鍵が格納された鍵媒体を使用して送信装置でデータを暗号化し，暗号化したデータを送信装置から受信装置へ暗号技術を用いて送信し，次に，データ復号鍵と受信装置の公開鍵で暗号化した通信復号鍵を格納した鍵媒体を使用して受信した暗号化データを復号するという方法が提案されている[45]．改正法の施行に伴い運用が開始されているシステムにおいても概ねこのような仕組みが採用されているものと推察される．なお，裁判所で作成される公開鍵と秘密鍵のペアについては，送信装置ないし受信装置の真正性を判断するという目的から考えて，各々の装置に対応した２組のペアが作成されることになると考えられる．しかし，データ暗号化鍵とデータ復号鍵の関係については詳細な説明はなく必ずしも明確ではでない．

3.7.2　問題点

確かに，推察されるシステムでは，各々の装置に対応した鍵媒体を利用することにより，装置の真正性を確認することが可能であり，その点は評価できる．しかし，まず，データ暗号化鍵とデータ復号鍵が共通鍵であるとすれば，変換符号と対応変換符号はそれぞれ異なった鍵でなければならないと考える本論文の立場からはそもそも疑問であると言わざるを得ない．また，公開鍵方式と考えた場合でも，公開鍵方式は通信内容の暗号化には適さないという問題は避けて通れない．さらに，データ暗号化鍵と通信暗号化鍵の関係についても不明である．

加えて，鍵媒体（USB トークン）に格納するとされている鍵は，公開鍵で暗号化した通信暗号化鍵ないし通信復号鍵であって秘密鍵ではない．秘密鍵は，送信装置ないし受信装置のハードディスクに格納するとされている．ここでは，秘密鍵の安全性は，傍受ソフトウェアの作り込みによって安全性を担保しようとしている．しかし，これでは，仮に，別途ハードディスクの暗号化の措置等がとられていたとしても，ハッキング等によって秘密鍵が抜き取られるリスクはなおも否定できない．そもそも，本調査報告書は，改正法成立前の警察が提案していた技術的措置の妥当性について，技術の選別や実現可能性等の視点から検討されたものであり，改正法の要件を子細に検討した上でそれを満たす範囲という観点から検討がなされたものとは言えない．したがって，改正法との関係では必ずしも整合的に検討されているは言えず，その限りにおいて，調査報告書を参考に構築されたと考えられる運用システムが改正法に抵触せず，技術的に合致していると言えるのかは不明である．また，セキュリティ面についても，前述の通り，秘密鍵の安全や捜査機関が行う可能性のある不正を防ぐという観点から，十分に検討されたものかも疑問である．

３.８　IC カードシステムの提案

3.8.1　鍵の提供方法についての問題点

特定電子計算機を使用する傍受システムにおいては，裁判所が作成した暗号化のための鍵（変換符号）及び復号のための鍵（対応変換符号）は，通信事業者ないし捜査機関へ提供されなければならないが（9 条２号イ，ロ），実際に傍受システムの構築を考えた場合，まず，この鍵の提供方法についての問題を解決しなければならない．一般的には，通信回線を利用して提供するか，USB メモリ等に格納して直接提供するか等の方法が考えられるだろう．この点，仮に，共通鍵方式を使用する場合（暗号化のための変換符号と復号のための対応変換符号を共通の秘密鍵とする場合）を考えると，まず，通信回線の利用は，漏洩のリスクが高く避けるべきであろう．そうすると，この場合には，変換符号が捜査機関に漏洩するというリスクを考慮する必要はないので，例えば，令状の発付を受ける際に，USB メモリ等に格納された共通鍵を２つ受け取り，その内の一つを変換符号として，令状提示の際に，裁判所に代って提供させるような方法が考えらえる．しかし，この方法では，捜査機関に提供される鍵（対応変換符号）は，通信事業者に提供される鍵（変換符号）と当然共通であるので，通信事業者での暗号化の処理にも利用することができてしまい，そのままでは 9 条２号ロ，23 条２項６号などに抵触する可能性が残る．

では，次に，公開鍵方式を採用する場合を考えてみることにする．公開鍵方式の場合，暗号化鍵（変換符号）と復号鍵（対応変換符号）は，非対称鍵の性質を有することから，上記の抵触の問題は解決できる．また，この場合，捜査機関に提供される対応変換符号の秘密性が保持されれば十分であって，通信事業者に提供される変換符号はたとえ公開されていても問題がないので，捜査機関に一旦預けるような方法をとらなくても，別途通信を利用するなどの方法も含めて比較的自由に提供できる．そうすると，改正法における新システムにおいては，仮に公開鍵方式の採用を前提として実装を考えれば，鍵提供の問題は解決できると考えられる．

具体的には，３.５節で検討した通り，通信データの暗号化に関しては公開鍵方式が直接利用されることはなく，ハイブリッド方式が採用されることにより，公開鍵方式が間接的に利用されることになる．３.５節の例によれば，通信事業者に提供される鍵を共通鍵 Kc としつつ，捜査機関に提供される鍵を，共通鍵を公開鍵で暗号化した Kp(Kc)とすることで，符号的には別個の鍵がそれぞれに提供される．

もっとも，この場合，捜査機関は，裁判所から提供される秘密鍵 Ks を用いれば，当然，Kp(Kc)を復号することが可能であることから簡単に共通鍵 Kc を入手することができてしまい，これでは，変換符号と対応変換符号を分離した趣旨に合致するとは言えないではないかという疑問もある．

そこで，これらの問題を解決する手段として，ここでは，IC カードを利用する方法を提案したい．IC カードを利用すれば，共通鍵 Kc は，IC カードが挿入された特定電子計算機内部でしか復号処理を行わない仕組みを作ることができ，捜査機関が容易に共通鍵 Kc を入手することを防ぐことも可能である．また，前述した秘密鍵の提供に伴う漏洩のリスクも防げる．

3.8.2　IC カードを利用する利点

IC カードは，1 チップ（IC チップ）からなるコンピュータであり，サービスに応じたソフトウェアによって制御され，専用のリーダ／ライタを介して端末と通信する[46]．IC カードに搭載される IC チップの一般的な構成要素としては，①IC カード内で演算処理を行う CPU，②公開鍵暗号の演算を高速に実行するための暗号コプロセッサ，③一時的なデータを読み書きするための高速メモリである RAM，④プログラムを格納するために使用する読み出し専用メモリである ROM，⑤主にデータを格納するために使用する書き換え可能なメモリである EEPROM，及び⑥IC カード外部との通信制御を実施する通信インターフェースなどがある．

このように，IC カードは，文字通り小さなコンピュータであるが，この IC カードを利用する最大のメリットは IC カードに要求されている高いセキュリティ要件である．具体的には，①IC カード内部に書き込まれた情報が不正に取り出されたり，改ざんされないこと，②IC カードと読み取り端末，IC カードとサービスの間の通信が第三者に傍受されたり，偽造 IC カードを通信対象として認証しないこと，③ IC カード自体が本来の所有者以外の人物に不正に使用されないこと，があげられる[47]．IC カードでは IC チップの耐タンパ性と OS のデータ管理機能から IC カードの内のデータが守られており，秘密情報の外部からの参照を完全に防ぐことができる．IC カードに格納された秘密情報は，IC カードの外部には一切流出せず，IC カードとの間でやり取りされる情報は，演算処理の結果だけである[48]．

このように，IC カードは非常に高い安全性が認められており，傍受システムのセキュリティあるいは不正防止を確保する上で十分期待できると考える．

3.9　IC カードを利用したシステムの試案

では，実際に IC カードを利用した傍受システムについてどのように実装できるのか．以下の手順によることが，前述の課題も含め改正法に抵触しない形で具体化するもっとも妥当な方法でないかと考える．

3.9.1　手順１（裁判所が行う準備）

⑴　以下の鍵を作成
ICカード１（秘密鍵 Ks1 を格納）
ICカード２（秘密鍵 Ks2 を格納）
ICカード１に対応する公開鍵（Kp1）
ICカード２に対応する公開鍵（Kp2）
通信文の暗号化に用いるための共通鍵 Kc1（9条２号イ：変換符号）
記録用の暗号化に用いるための共通鍵 Kc2（9条２号ロ：変換符号）

⑵　通信事業者に提供
共通鍵Kc1

⑶　捜査機関に提供
ICカード１（Ks1）
ICカード２（Ks2）

⑷　捜査機関に提供（通信もしくはUSB等の媒体による）
公開鍵Kp1を使って共通鍵Kc1を暗号化したもの（Kp1(Kc1)）
（ICカード１がないと捜査機関はKc1を利用することができなくなる）

⑸　捜査機関に提供
公開鍵 Kp2 を使って共通鍵 Kc2 を暗号化したもの（Kp2(Kc2)）

3.9.2　手順２（通信事業者が行うこと）

⑴　通信文（D）を共通鍵 Kc1（9条２号イ：変換符号に相当）で暗号化

⑵　特定電子計算機（捜査機関）に伝送

3.9.3　手順３（捜査機関での通信傍受）

⑴　ICカード１（Ks1）を指定の特定電子計算機に挿入

⑵　公開鍵Kp1で暗号化された共通鍵Kc１（Kp1(Kc1)）を傍受装置に入力する

⑶　特定電子計算機は公開鍵Kp1で暗号化された共通鍵Kc1（Kp1(Kc1)）に対してICカード1（Ks1）を使ってその内部で復号する

⑷　特定電子計算機は共通鍵Ks1で復号されたKc1（=(Ks1(Kp1(Kc1))）を用いて，内部で通信文（D）を復号する
同時に，傍受ないし再生された通信文（D）のハッシュ値（Hm）を計算する
傍受ないし再生された通信文（D）はICカード2（Ks2）を挿入した特定電子計算機内部で公開鍵Kp2を利用し復号された共通鍵Kc2で暗号化を行う
そのまま記録媒体に記録する

⑸　傍受が終了後
特定電子計算機はICカード1（Ks1）を用いてハッシュ値（Hm）に電子署名を付す
記録媒体に記録する
記憶媒体をICカード1，2と共に裁判所に返還する
傍受に使った特定電子計算機には最終的に以下のものが書込まれた状態で残ることから，捜査機関は，これを速やかに消去する

Kp1で暗号化されたKc1（(Kp1(Kc1)）
Kp2で暗号化されたKc2（(Kp2(Kc2)）
通信文のハッシュ値Hm
HmをKs1で電子署名したもの

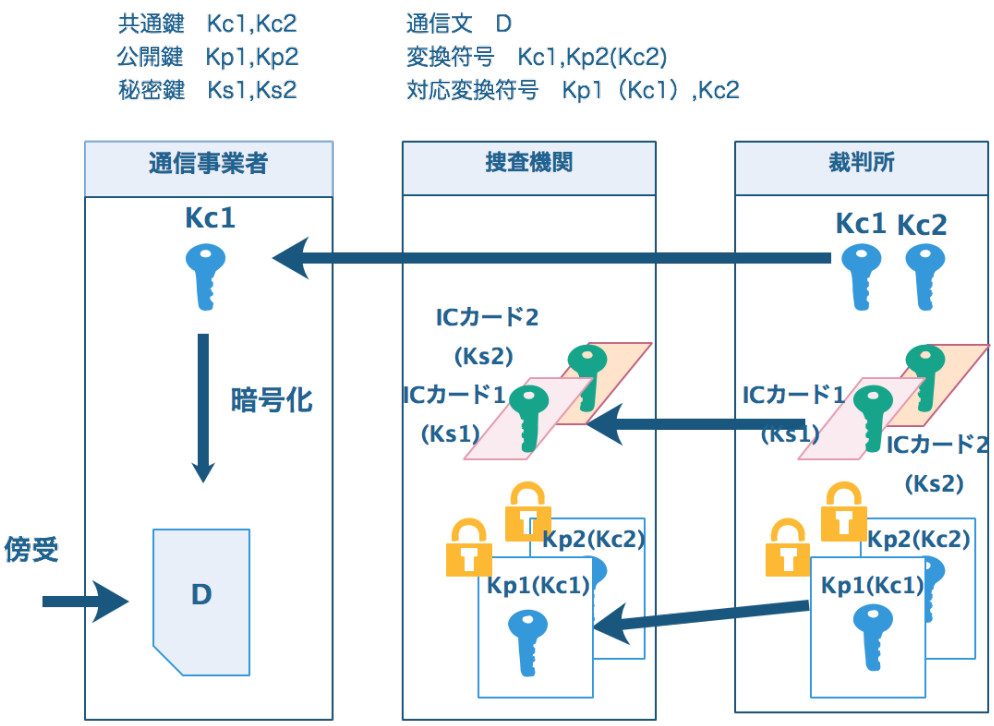


図 3.1　手順 1 および 2

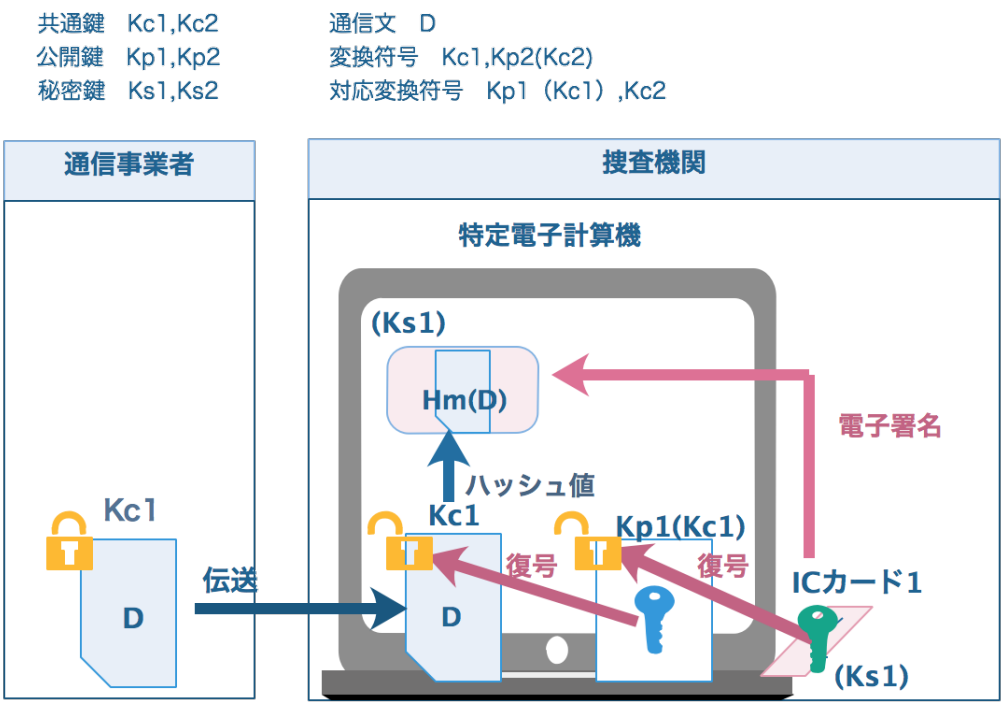


図 3.2　手順 2 および 3

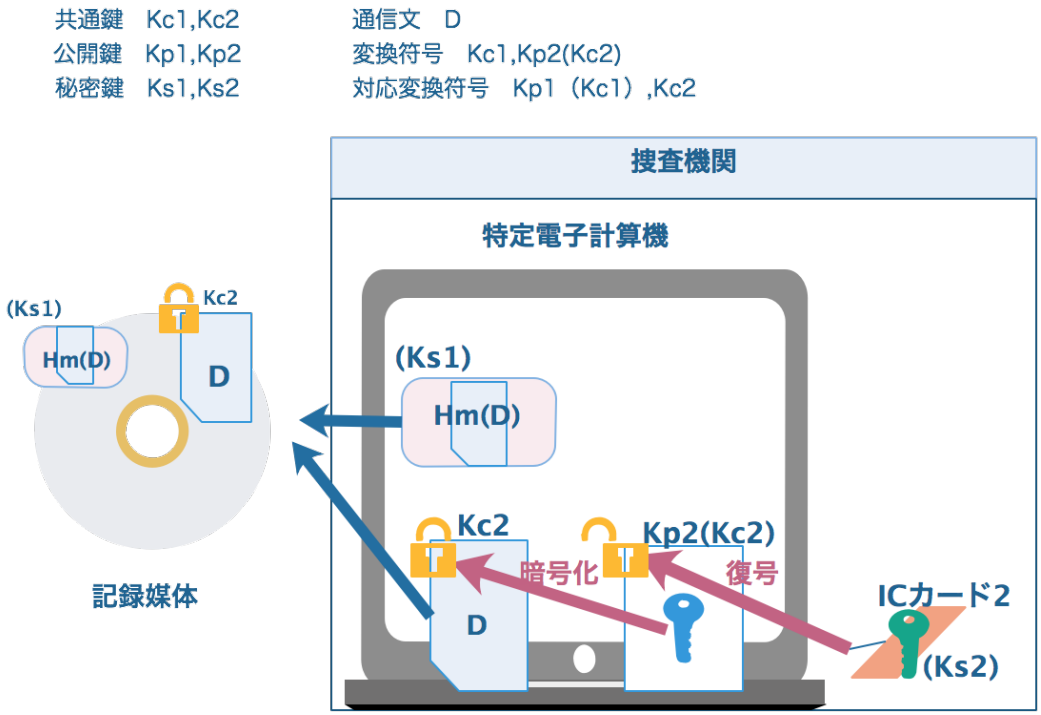


図 3.3　手順 3

なお，ここでは，IC カードの授受の際になりすましなどにより裁判所から当該捜査機関外に提供されることは想定していない．また，提案システムでは，共通鍵 Kc1 を裁判所から直接通信事業者に提供しているが，他の保護手法によって確実に通信事業者に提供されれること，および通信事業者が共通鍵 Kc1 を漏洩させないことを前提としている．

3.10　簡易傍受装置の構築

最後に，上記提案システムを活用ないし運用する上での新たな問題点について検討すべく，簡易的な傍受装置を構築して評価した．

3.10.1　IC カードシステムを利用した簡易傍受装置の構築

本提案システムの実用性を検証するために，実際に IC カードを使って簡易傍受装置を構築した．システムの構築にあたっては以下の機器を用いた．

⑴　IC カード
　　Advanced Card System 社　ACOS5-64

⑵　ソフトウェア
　　ACOS5-64 Client Kit

⑶　開発用 Windows 機および接触型 IC カードリーダ（OS：Windows10 Home 64bit）

ACOS5 は，ISO7816 準拠の接触型 IC カードであり，RSA による電子署名・暗号化と AES の CBC モードでの暗号化などをサポートしている．また，64K バイトの EEPROM を持ち，ISO7816–4 準拠のファイルシステムによってユーザデータを格納できる．Windows 向けの開発キットが提供され，Windows Cryptographic API（以下，「CryptoAPI」と言う．）を用いた開発が容易に行えるため，本開発で用いた．

開発にあたっては，3.3.4 節の手順 1 と手順 3 について行った．手順 2 は通信データの暗号化であるが，これは単に生成した暗号鍵（Kc1）を用いてサンプルの音声データを暗号化することで代替した．

裁判所の手順を模した手順 1 の実装は以下のように行った．２枚の IC カードを用意し，IC カード 1，２とした．これらそれぞれに鍵を生成した．ACOS5 の鍵生成機能を用いて生成したため，秘密鍵 Ks1，Ks2 を安全に生成し格納することができた．IC カードから公開鍵を取り出し，それぞれ Kp1，Kp2 とした．これに加えて，Kc1，Kc2 は CryptoAPI の機能を用いて Windows 機上で生成し，Kp1，Kp2 を用いて暗号化し，Kp1(Kc1)，Kp2(Kc2) とした．この上で，ACOS5 の機能を用いて IC カード 1 のユーザ領域に Kp1(Kc1)を，IC カード２のユーザ領域に Kp2(Kc2)を格納することができた．

次に，捜査機関の手順を模した手順 3 を以下のように実装した．受け取った音声データは Kc1 を用いて暗号化されていることから，まず，IC カード 1 から Kp1(Kc1)，Kp2(Kc2)を取り出す．そして，この Kp1(Kc1)と暗号化された音声データを直接 IC カード 1 に入力し，音声データを取り出す．最後に，取り出した音声データにハッシュ値を計算し，音声データとハッシュ値，Kp2(Kc2)を IC カード２に入力して暗号化するようにプログラムを作成した．

3.10.2　評価と考察

本節で試作したシステムによって，本提案の要件を満たすように開発できることは確認できた．しかし，執筆時点において本システムは完全に要件通り動作するに至っていない．現時点で問題となっているのは，IC カード内における音声データの暗号化・復号が動作しないため，手順３における動作が終了しないことである．そのため，現時点では，手順３における音声データの暗号化と復号を IC カード内でなく特定電子計算機に見立てた PC 上で行うことで対処している．改正された通信傍受法が求める要件においては，特定電子計算機は十分に耐タンパ性を有しており，捜査機関における不正が起きないと仮定されているため，このような実装でも問題にはならないが，本研究での提案である，より高いセキュリティレベルを達成するためには，IC カード内での処理が必要である．

この原因については，現時点では突き止められていないが，問題になりうると考えられる原因としては，IC カードのインターフェースの能力不足である．本件では，音声データを直接 IC カード内で処理することを目指しているが，本研究で用いた ACOS5 のインターフェースは仕様上，200kbps までの入出力ができることになっているものの，内部の処理負荷によってこの能力が発揮できておらず，通信が途絶するなどの原因が考えられる．

通信傍受法は，傍受の対象を音声に限ってはいないため，仮に将来的に動画像データの処理行うのであれば，より高い性能の IC カードか同等の耐タンパ性を有するデバイスの利用が必要であることが明らかになった．

3.11　本章のまとめ

本章では，改正された通信傍受法における暗号化技術に関して，技術的観点も踏まえて，解釈上も条文の規定に抵触しない方法としてハイブリッド方式による暗号化方式が採用されるべきであることを示すことができた．そして，裁判所から通信事業者及び捜査機関への鍵提供に際して求められるべきセキュリティ確保の観点を踏まえて，IC カードを利用した通信傍受のシステムについて提案した．加えて，簡易傍受装置の構築によって一定の課題はあるものの十分実装が可能であることも示すことができた．

確かに，令和元年（２０１９年）６月に改正法が施行されて１年余りしか経過していないことから，具体的な技術仕様書等については十分な検討には至っておらず，前記技術仕様等に基づいた議論という観点からは必ずしも十分なものとはなっていない可能性は否めない．

しかし，本章の提案システムによって，捜査機関が改正法で許容された通信傍受の範囲を超えた違法・不正な傍受行為に及ぶ危険を防止することが技術的に十分可能であることを示すことができたと考える．

もっとも，改正法の規定を前提としてシステムの構築を考えた場合，改正法の趣旨に合致

したものとしては，提案システムがもっとも合理的な仕組みであると考えるが，それでもハイブリッド方式における鍵を法条文上どのように解釈するべきか，などの点においてなおも不自然さを感じさせる部分があることは否定できない．これは，改正法の構造自体が，善解すれば，変換符号ないし対応変換符号の規定の仕方など，不正を防止するための規定として厳正さを追求しようとしている一方，それがために却って技術的な実現可能性を十分に考慮していないためと考えられる．

そもそも暗号化技術は，あくまでも通信上の秘密を守るためのものであって，立会いの要不要を図る指標とはなりえないという問題も依然残る．既に述べた通り，例えば，通信傍受の結果については，原記録媒体に自動的に保存されることになっている点に鑑みれば，確かに原記録媒体に保存された情報を改ざんすることは困難であるかもしれない（23 条２項３号，４号，６号，７号等）．しかし，原記録に記録すると同時に，証拠用の資料を作成するために暗号化の処理をすることなく他の記録媒体に記録することも求められており（23 条 2 項３号，４号），これを改ざんして原記録等とすり替えることも不可能ではなく，記録の過程で改ざんされる余地は十分に残されている．

加えて，傍受された（復号された）データの漏洩・窃用の可能性はないのか，消去されたはずのデータの復元の危険はないのか等，本論文では検討できなかったが，今回想定されている暗号化の技術だけでは解決できない問題も依然多く残っている．

傍受システムの構築にあたり今後の課題としては，提案システムが安定的に稼働してその実効性を示すことと，通信事業者，捜査機関，裁判所を模したロールプレイングで実際に通信傍受の手順を追うことにより，その実務上の問題点，特にリスクポイントを洗い出すことである．

第４章　ブロックチェーンを利用した証拠の改ざん防止システムについて

４.１　はじめに

個人や企業・法人等の活動の痕跡として，パーソナルコンピュータ（本章では，以下，「PC」と言う.），デジタルカメラ，IC レコーダ，携帯電話などの各種デジタルデバイスに記録されるデジタルデータが，裁判実務においても，民事事件・刑事事件を問わず，デジタル証拠として扱われる場面が増えている．図 4.1 は，判例検索[12]を用いて，刑事裁判（児童ポルノ，公然わいせつ，リベンジポルノを除く.）に限定した上，４つのデジタル機器（①「デジタルカメラ」(「デジカメ」を含む.)，②「IC レコーダー」，③「パソコン」(「パーソナルコンピュータ」，「PC」を含む.)，④「デジタルビデオ」）の用語を含む条件で検索した結果を３年単位でグラフ化したものであるが，このグラフからもデジタル証拠が扱われる裁判例が全体として増加傾向にあることが窺える[13].

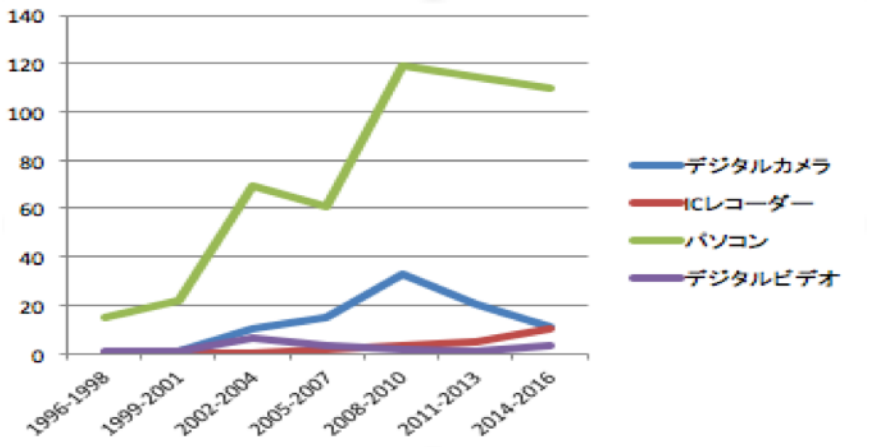


図 4.1　デジタル機器が判決文中に含まれる刑事裁判の年代別動向

[12] 判例秘書 INTERNET によって，2017 年 2 月 27 日に検索した.
[13] なお，デジタルカメラの件数が減少傾向にあるが，近年，スマートフォンの台頭によって，使用頻度自体が減少していることを反映していると考えられる.

デジタル証拠は，機械的に記録されたデジタルデータを解析することによって得られる客観的・科学的証拠の一つとして，曖昧あるいは主観的な人の記憶に基づいた供述証拠に比べ，それ自体高い信頼性が認められている．特に，自白偏重の弊害が指摘されて久しい刑事裁判においては，今後もますます重要な役割を果たしていくと期待されている．

しかしながら，デジタル証拠は一般に改ざんが可能であり，かつ容易であるという特性が認められる．その一方で，デジタル証拠はその客観的性質ゆえ信頼性が高いと評価される反面，一旦改ざん等された場合には，却って誤判の危険性は増大し，その場合の弊害は極めて甚大である．特に，人権問題に直結する刑事裁判では，デジタル証拠の収集保全に関して圧倒的な権限を有する捜査機関が仮にデジタル証拠を改ざんする不正に関与するようなことがあれば，その弊害は計り知れない．手続きの担い手が警察や検察であるということにのみ信頼の基礎を置いていては，国民の信頼に資する裁判の実現には到底及ばない．

以上の理由から，捜査機関によって収集保全されたデジタル証拠に関して，改ざんされていないことが客観的に担保され，かつ被疑者・被告人や弁護人等からも容易に改ざんの有無を確認できるシステムの構築が求められる．そこで本章では，まず，観察実験を通じてデジタルデータの改ざんが如何に容易であり，改ざんのリスクがもはや無視できない現実的なリスクであるということについて確認した上で，改ざん防止の観点から，一般的なシステムとして，デジタル証拠が改ざんされていないことを客観的に確認できる具体的なシステムの構築について考察した．

４.２　デジタル証拠の改ざんの容易さ

4.2.1　改ざんの容易性を確認するための予備調査

まず予備調査として，デジタル証拠となりうるようなデータの改ざんが一般的な PC の利用者にとってどの程度容易であるかを確かめるため，観察実験を実施した．

4.2.1.1　実験の被験者

被験者には，業務上，書類作成等の事務作業のために日常的にＰＣを使用しているが，画像加工や情報分野の専門的知識を有していない IT 分野の非専門家として，表 4.1 の記載の通り，弁護士４名，司法書士１名を選んだ．被験者はいずれもデジタル証拠の改ざんについての予備知識は有さない．

表 4.1　被験者

	年齢(代)	性別	職業	PC 使用歴	主な使用目的	主な使用ソフト
A	30 代後半	女	弁護士	15 年	仕事	ワープロ，表計算，メーラー，ブラウザ
B	30 代前半	女	弁護士	24 年	仕事	ワープロ，表計算，メーラー，ブラウザ
C	30 代後半	女	弁護士	20 年	仕事	ワープロ，表計算，メーラー，ブラウザ
D	30 代後半	男	弁護士	20 年	仕事	ワープロ，表計算，メーラー，ブラウザ
E	30 代前半	男	司法書士	15 年	仕事	ワープロ，表計算，メーラー，ブラウザ

4.2.1.2　実験環境

実験環境は以下の通りである.

⑴　PC：
Windows10 がプリインストールされたノート型 PC

⑵　インストール済みソフトウェア：
Adobe Photoshop CC2015
Adobe Acrobat Pro DC
Adobe Acrobat Reader DC
Microsoft Word 2016
F6 Exif

全てのソフトウェアはショートカットをデスクトップに置いており，インストールされていることにはすぐ気づくようにしてある．

4.2.1.3　実験課題

実験にあたっては，以下の３つの課題を用意し被験者にその場で作業を行わせるものである．

⑴　実験１　被験者に写真 1（jpg ファイル），及びその中央に写っている人物を消去した写真２（図 4.2）を示し，そのように編集することを依頼する．

⑵　実験２　被験者に写真 1 の Exif 情報（撮影日，撮影場所）を変更することを依頼する．

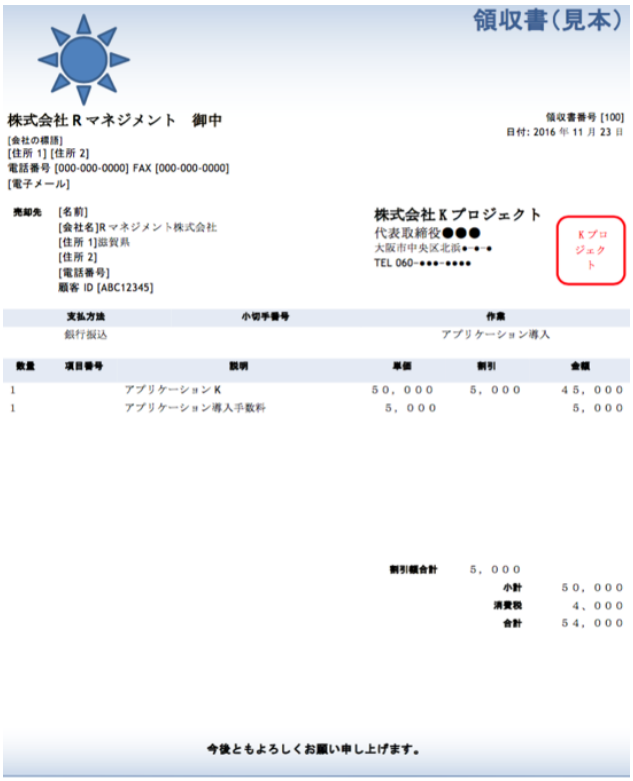
⑶　実験３　被験者に領収書を模した PDF ファイル（図 4.4）の金額欄など記載内容の変更を依頼する．

実際の改ざんは，実験 1 については Photoshop の持つ「コンテンツに応じた塗り」機能，実験２については F6 Exif の持つ機能，実験３については Word による PDF の読み込みと編集，書き出し，または Acrobat Pro による編集で行うことができるが，その手法自体は被験者には伝えず，インターネット検索などを通じて手法を自ら発見し，実際に作業が行えるかどうかを観察した．

図 4.2　写真 1

図 4.3　写真 2

図 4.4　領収書（見本）



領収書（見本）

株式会社 R マネジメント　御中
[会社の標語]
[住所 1] [住所 2]
電話番号 [000-000-0000] FAX [000-000-0000]
[電子メール]

領収書番号 [100]
日付: 2016 年 11 月 23 日

売却先　[名前]
[会社名]R マネジメント株式会社
[住所 1]滋賀県
[住所 2]
[電話番号]
顧客 ID [ABC12345]

株式会社 K プロジェクト
代表取締役●●●
大阪市中央区北浜●-●-●
TEL 060-●●●-●●●●

K プロジェクト

支払方法	小切手番号	作業
銀行振込		アプリケーション導入

数量	項目番号	説明	単価	割引	金額
1		アプリケーション K	50，000	5，000	45，000
1		アプリケーション導入手数料	5，000		5，000

割引額合計	5，000
小計	50，000
消費税	4，000
合計	54，000

今後ともよろしくお願い申し上げます。

4.2.1.4　実験手順

実験の手順は以下の通りである．

⑴　実験開始とともに，実験１ないし３の課題を与える．

⑵　制限時間は，実験１ないし３併せて３０分以内とする．

⑶　インターネット検索は自由に行える．

⑷　使用するソフトウェアや使用方法については各自が自由に選択する．

⑸　インストール済みのソフトウェア以外を使用することも自由である．但し，インストール済みのソフトウェアだけで可能であることは告知済み．

4.2.2　実験結果

実験１ないし３の結果は以下の表 4.2 ないし 4.5 の通りである．
なお，各実験については６つの評価ポイント（step1~step6）を設け，各 step ごとに達成度に応じて３段階で評価した．
また，実験終了後の被験者に対するアンケートの結果を表７に示す．

【Step】
step1　課題の意味を理解する．
step2　インターネットで検索する際に，適切なキーワードを利用できる．
step3　想定していた対応可能なソフトウェアに辿り着く．
step4　上記ソフトウェアが PC 内にあることを発見する．
step5　対応可能なソフトウェアの適切な機能を見つけることができる．
step6　適切な機能を用いて，実際に課題を解決できる．

【評価】
Y：達成
N：未達成
＃：未評価（想定と異なる方法をとるなどしたため）

表 4.2　実験 1 の結果

	1	2	3	4	5	6	時間(分)	不成功の原因に繋がった行動
A	Y	Y	Y	Y	N	N		ファイルの開き方が分からなかった
B	Y	Y	Y	Y	Y	Y	16	
C	Y	Y	#	N	#	#	(15)	標準ソフトのコピペ機能で対応
D	Y	Y	Y	Y	N	N		適切な機能を発見できなかった
E	Y	Y	Y	Y	Y	Y	7．5	

達成者の平均所要時間：　約１１分半

表 4.3　実験 2 の結果

	1	2	3	4	5	6	時間(分)	不成功の原因に繋がった行動
A	Y	Y	N	N	N	N		プロパティに気を取られた
B	Y	Y	Y	Y	N	N		適切な操作方法が分からなかった
C	Y	Y	Y	N	N	N		時間切れ
D	Y	Y	Y	Y	Y	Y	6	
E	Y	Y	Y	#	#	#	(9)	プロパティでの対応にこだわった

達成者の平均所要時間：　約６分

表 4.4　実験 3 の結果

	1	2	3	4	5	6	時間(分)	不成功の原因に繋がった行動
A	Y	Y	Y	Y	N	#		アクロバットの使用方法が分からなかった
B	Y	Y	Y	Y	Y	Y	3．5	
C	Y	Y	Y	Y	Y	Y	12．5	
D	Y	Y	Y	Y	Y	Y	3	
E	Y	Y	Y	Y	Y	Y	7	

達成者の平均所要時間：　約６分半

表 4.5　実験終了後のアンケート内容（自由記載）

A	方法については全然知らなかった 思っていたよりは少し正解に近づきそうになった気がした もう少し時間があれば何とかなったかもしれない 躍起になりすぎた もう少し柔軟に色々試せばよかった
B	画像消去と PDF ファイル編集はやったことはあったが，別のアプリなどでしたことがあった記憶がぼんやりあるだけ いざ方法を問われると明確に思い出せず，すべて Web で調べながらやった Exif 情報の改変は初めてやった 時間制限ありで難しかった できると面白くてはまりそうになった
C	写真ファイルの人物消去は時間をかけてもっと綺麗に消去したかった 時間があれば，インターネットで検索して調べれば大抵のことはできそうだと思った
D	方法については知らなかった デジタルデータの改ざんが思いの外簡単にできることを実際にやってみて理解できた
E	写真の人物を簡単に消せたことについてはビックリした やり方についてはほぼ知らなかった ネットで検索すれば意外と簡単にすぐに方法が出てくることにも驚いた

4.2.3　考察

今回の実験では，PDF の編集を経験したことがある者が 1 名（B）いた．他は，実験 1 ないし 3 の全てについて事前に経験していた被験者はおらず，最終的にすべての実験課題を完成（step6）させた者はいなかった．もっとも，もう少し時間があればある程度はできそうだと思ったという趣旨の感想を述べた被験者が 3 名（A，B，C）いた．いずれの被験者も日常的に業務で PC を使用し，PC の扱いについては十分慣れていたため，課題の意味を理解し（step1），検索エンジンを利用し方法等を検索すること（step2）については全く問題なかった．しかしながら，日常的な PC の使用方法については，全員が業務における事務作業に使用しており，趣味等で画像編集等を行っている者がいなかったことから

も分かるように，各自不慣れな作業であったということに加え，制限時間の短さが影響したため，このような結果となったと考えられる．

実験別にみると，実験３（PDF ファイルの編集）の成功率が最も高く，４名（B，C，D，E）が成功した．これは，被験者の間でも PDF ファイルは馴染みがあり，Adobe Acrobat の編集機能についても認知されていたことによると考えられる．唯一１名のみ成功しなかった A については，一旦は Adobe Acrobat の存在に気付いて立ち上げるまでに至ったものの当該ファイルを同ソフトで開くという使用方法が分からず，結局，当該ファイルをダブルクリックで開いてしまい（当該環境では PDF ファイルをダブルクリックすると AcrobatReader が起動し開くようになっていた），そのまま同ソフトでの編集にこだわってしまったためと思われる．なお，A については，実験１及び２においても達成できなかったが，ファイルを開く際，ダブルクリックで開いては閉じるという行動を繰り返しており，アプリケーションから開く方法について不知あるいは不慣れであることが窺えた．

これに対して，成功率が最も低かったのが実験２（Exif の編集）で，最終的に成功した者は１名（D）だけであった．F6 Exif のウェブサイトを発見しながら，既に PC にインストールされていたことに気付かなかった者が２名（C，E），インストールされていたことに気付きながら操作の方法が分からず完成できなかった者が１名（B）いた．実験２は編集作業にはいわゆるフリーウェアを利用することが求められていたが，主に仕事上の事務作業でしか PC を使用しない層にとっては，フリーウェアの使用に馴染みがなく障害になったと推察される．なお，実験２については，全員がプロパティによって Exif 情報が読み取れることには比較的早い段階で確認することができ，うち１名（E）がプロパティの操作によってファイルのタイムスタンプの編集まではできた．しかし，それが却ってプロパティを操作すれば全て達成できるという誤解を助長して結果的に無駄に時間を掛けすぎてしまい時間不足を招いたと推測される．

最後に，実験１（写真上の人物の消去）については，Adobe Photoshop の標準機能を使用し完成させた者が２名（B，E），Windows 標準のペイントソフトのコピー&ペーストの機能を利用して類似の編集を行った者が１名（B）という結果であった．残り２名（A，D）については，Adobe Photoshop の存在には気付いたものの，A はそもそも Adobe Photoshop で当該ファイルを開くことができず，そして，D は Adobe Photoshop で当該ファイルを開くことはできたものの，その機能の使用方法が分からなかった．制限時間の制約内でソフトの機能に気付き，実際に色々と試行したか否かが結果を分けたと考えられる．

今回の実験は，被験者にとって過去に一度でも同様の作業経験があれば容易に完成できる作業について，知識・経験がない場合にどの程度行えるかということを確認する目的で実施したものである．実験の結果からは，課題がいずれも被験者にとって未経験であるため試行錯誤が行われたが，その過程において情報科学的な知識の欠如により作業が困難に

なる様子が窺えた．特に，Exif 情報の改ざん作業は，写真や PDF の加工といった外見的な作業とは異なり，ファイルの内部情報に関する作業であって，情報科学の基礎知識を有しない被験者にとってはその意味を理解することが困難であったようである．また，制限時間という一定の制約や自身の作業内容が観察されるという実験環境内での緊張から作業が困難になったと思われる行動や言動も見られた．全ての被験者が，実験後，デジタルデータの改ざんが簡単にできるということを実感したとアンケートなどで述べている．そうすると，被験者にとって，デジタルデータの改ざんが実は簡単であるということの知識さえ備われば，今後同様の作業を要求しても，今回の実験のように時間的制約がなく観察による緊張もない状況であったなら，文字通り簡単にデジタルデータの改ざん作業が行えるようになったのではないかと考えられる．デジタルデータの改ざんや編集については，容易に実行できる多くの定番ソフトウェアが有償無償を問わず存在し，それらの使用方法等や改ざんの方法を解説・説明するウェブサイトも多く存在する．少なくとも，今回の実験を通じて，動機付けさえあれば，容易にそれらの情報にアクセス可能であることも明らかになった．

これらのことから，デジタル証拠の改ざんが一般的な PC 利用者にとっても，事例さえ示されれば事前の知識がなくとも行える場面が少なからずあることが明らかになったことが確認できたと考えられる．

４.３　刑事手続におけるデジタル証拠の改ざん防止措置の必要性

既に，2.3 節で指摘した通り，デジタル証拠が証拠として裁判上適法たり得るのは，捜査機関によって押収等の過程で偽造や改ざんなど不正に晒されていないということが保証されていることが前提である．しかし，実際の刑事裁判においても検出されている通り，現実の刑事手続の現場においては捜査機関の不正を疑わざるを得ない事案ないし事由も少なからず存在する．そうすると，もはや捜査機関であるからと言って全幅の信頼を前提とすることはできない．

4.3.1　デジタル証拠の改ざんのリスク

捜査機関は，刑事手続におけるデジタル証拠を含めた証拠の押収・保全機関として最前線に位置しているがゆえに，捜査機関による偽造・改ざんのリスクは無視できない．デジタル証拠の収集過程において，捜査機関による偽造・改ざんなど不正が存在するリスクについて，我々は，その現実を直視し，十分に警戒しなければならない．ここに，捜査機関がデジタル証拠を押収等した際に，客観的に真正性・完全性を担保することができ，かつ弁護人や

被疑者・被告人からも容易に，そして安全に改ざんの有無を確認できるシステムの構築が求められる理由がある．

4.3.2　ハッシュ値の活用

この点，捜査機関によって収集保全されたデジタルデータの改ざん防止策としては，オリジナル媒体に記録されているデジタルデータと同一であることをハッシュ値によって確認することが最も効果的である．捜査機関等がハッシュ値を確実な手段で証拠化しておくことで，同一性あるいは改ざんの有無を確認することができる．弁護人としては，捜査機関が押収したデジタル証拠に対して，ハッシュ値が記録されているかどうかを確認し，仮にこれが同一でなかった場合には，提出されたデジタル証拠の証拠能力や証明力を争うことになる．しかし，問題はそのハッシュ値の確認手段ないし方法である．

ところで，押収すべき電磁的記録が捜査機関によって偽造ないし改ざん等される可能性を考えた場合，（ⅰ）押収される段階と（ⅱ）保管・管理を行う段階での２つの場面が想定できる．そこで，この２つの場面に分けて，ハッシュ値確認の手段について検討する．

4.3.3　押収段階での改ざんの危険性

4.3.3.1　立会人について

捜索・差押えの際には，一定の立会人による立会いが必要とされているが，これは，捜査機関が，令状記載の差押えるべき物（電磁的記録に係る記録媒体）以外の物を差押えていないか，その場に存在しない物を存在したと称して証拠を捏造していないか等，違法な差押えを抑止するための適法性の担保としての機能を有しているからである．そこで，この立会人の役割について検討する．

立会人とは，捜索・差押えの執行場所が「公務所」である場合には，「その長又はこれに代わるべき者」（刑訴法２２２条，１１４条１項）とされており，また，公務所以外の「人の住居又は人の看守する邸宅，建造物若くは船舶」である場合には，原則として，「住居主若くは看守者又はこれらの者に代わるべき者」（刑訴法１１４条２項前段）とされている．もっとも，これらの者の立会いができないときには，「隣人又は地方公共団体の職員」を立ち会わせればよく（刑訴法２２２条１項，１１４条２項後段），住居主が不在等や立会いを拒否した場合であっても捜索・差押手続きができなくなる事態に陥ることはない．なお，令状を執行する際には，立会人とは別に，処分を受ける者に対して令状を提示しなければならないが，処分を受ける者とは，差押えの目的物又は捜索の対象たる場所の直接の支配者を言

う．電磁的記録に関して言えば，電磁的記録が記録された記録媒体を所持している者など電磁的記録を自己の実力支配内に置いている者や当該電磁的記録を排他的に管理できる者に限らず，単にアクセスして当該電磁的記録を利用することができる者も含まれる．「立会人」と「処分を受ける者」とは一致することが多いが，必ずしも一致するとは限らない．従って，処分を受ける者が不在等のために令状を提示することが不可能である場合もあり得るが，そのような場合には令状を示さないで執行しても違法ではないとした事例がある[49][50]．

しかし，被疑者の弁護人の立会いが制度的に保障されていない現状においては，立会人に対して捜索・差押え等の手続きについて法的に精通していることは望めない．その上，特に被疑者が身体拘束を受けている場合などでは，立会人は隣人等，当該事件とは無関係の全くの第三者に過ぎない場合もあり，捜査機関による執行の違法性をどれだけチェックできるのかということに関しては自ずと限界がある．特に，電磁的記録に関しては，法的知識以外にもコンピュータ等の機器の操作やデジタルデータの処理など情報処理についての高度な専門的知識や技能が要求され，かかる専門的知識がなければ，電磁的記録に係る記録媒体の差押え等に際して，捜査機関が何を行っているのかということについても簡単に理解できるとは思われない．従って，立会人の担保機能に限界があることは認めざるを得ない．

4.3.3.2　押収品目録交付書について

捜索の適法性を担保するための手段としては，他に，捜索・差押調書及び押収品目録交付書の作成等が挙げられる．これは，令状記載の物以外の物は差押えていないか，あるいは被処分者等が知らない間に差押えられた物はないか等違法な捜索・差押えを抑止するために押収物の記録等が義務付けられていることに基づく．

しかし，差押調書に添付の押収品目録や被処分者に交付される押収品目録交付書に記載されるのは，「物」としての押収品である．電磁的記録の場合であれば，押収物そのものは電磁的記録が記録された記録媒体であることから，その記録媒体が記載され，そこに記録されている電磁的記録自体は特に特定され記載が求められている訳ではない．確かに，電磁的記録に関する差押等については，令状の請求に当たって，対象となる電磁的記録ついては一定の特定が必要であり，差押段階においても記録媒体の中身を確認した上で差押えることが必要であることは当然である．しかし，実際に差押えられた記録媒体については，それに格納された電磁的記録まで記載することまでは求められていないことは前述の通りである．また，警察官がフロッピーディスク１０８枚等を内容を確認することなく差押えた事案について，一定の場合には内容を確認せずに差押えることが許されるとした事例もある[51]．

いずれにしても，これでは，差押えの対象とされたオリジナルのデジタルデータがそのままの状態で複製等されているか否かについては事後的に確認できない．デジタルデータに

関してはその性質に沿った記録方法が考慮されるべきであり，その方法としては前述のハッシュ値の記録が考えられるが，現状においては目録等への記載は義務付けられていない．

4.3.4　保管・管理段階での改ざんの危険性について

通常の押収物の場合には，保管・管理中に捜査機関により中身がすり替えられたり，改ざんされたりするリスクについては，そのプロセスから検証しなければならない．この点は，電磁的記録が記録されている記録媒体であっても同様である．しかし，電磁的記録の場合には，仮に，押収段階において適切にハッシュ値が算出・記録されてさえいれば，改ざんの検出は容易であり，別途，改ざん防止の措置をとる必要性は乏しい．

従って，ここでは，差押段階において，差押えられた記録媒体に記録された電磁的記録のハッシュ値が計算・記録されていなかった場合について検討することが必要となる．

この点，捜査機関の中にも，記録媒体の解析に際し，解析対象の記録媒体を物理的にコピー（デュプリケート）ないしイメージファイル化し，解析対象の記録媒体とコピー双方のハッシュ値を計算して記録・保管しておくことを推奨する見解が見られる．確かに，この手続きが適切に実施されるのであれば，少なくとも，差押後に差押えられた記録媒体のハッシュ値は記録される．しかし，そもそも，差押時ないし実際にハッシュ値が計算されるまでの間に改ざんがなされなかったことについては何の担保もないが，この点は差し置くとしても，この手続きでは，捜査官による関与しかなく，その運用に委ねられている以上，客観性の担保が弱いと言わざるを得ない．

4.3.5　押収段階での客観的ハッシュ値記録システムの必要性

以上の検討結果から，いずれにしても，捜査機関が押収した電磁的記録が押収時の状態のまま適切に保管・管理され，改ざんされていないことを証明するためのシステムとして，押収段階においてハッシュ値を記録・確認するための客観的かつ統一的な制度ないしシステムの確立が求められることとなる．

4.4　デジタル証拠のハッシュ値の記録先としてのブロックチェーンの有用性

捜査機関が押収したデジタル証拠が押収時の状態のまま適切に保管・管理され，改ざんされていないことを証明するためには，押収段階において当該デジタル証拠のハッシュ値を

そのまま記録することが効果的である．問題はそのハッシュ値の記録・確認のための客観的かつ統一的な制度ないしシステムとしてどのようなシステムが適しているのかということである．

デジタル証拠の存在・非改ざん証明のために，デジタルデータのハッシュ値の客観的・公的保存手段に関して，電子公証制度やタイムスタンプを活用する提案[52]や，電子データの証拠性を確保する前提としてタイムスタンプ等による完全性保証データの必要性が指摘されている[53]．また，刑事手続きにおいても，押収したデジタル証拠のハッシュ値を証拠化しておく手段として，同じく電子公証制度や民間事業者が提供するタイムスタンプサービスを利用する方法が指摘されている[54]．そこで，本節では，まず，これら既存の制度を利用することの可否について考察する．

4.4.1　既存技術の活用の可否

4.4.1.1　公証制度に基礎を置く電子公証制度

公証人による公証制度は，文書等を公的に証明する手段である．そこで，捜査機関が作成した電磁的記録のハッシュ値についてもこの公証制度を利用することができないか検討する．

電子公証制度とは，従来，紙の文書に限定されていた公証制度について，一部の電子的なデータ（電磁的記録）に関しても公証人による公的な証明を施すべく，公証人のうち新たに電子公証事務を行う公証人を指定公証人として創設された公証制度の１つである[55]．技術的には，法務大臣が発行した指定公証人電子証明書を信頼の基点としており，公証人が電磁的記録の作成者を確認し，自らの秘密鍵を用いて電子署名を付すプロセスに瑕疵がないことを前提としている．現在，電子公証制度には大きく分けて，①電磁的記録の認証（作成者の確認）と②日付情報の付与（電子確定日付の付与）の制度がある．このうち②は，指定公証人が電磁的記録に記録された情報に日付を内容とする情報を付し，これに電子署名をすると，当該情報を確定日付のある証書とみなすことができる制度であり（民法施行法５条２項），文書の存在を証明する制度として利用されることから，この制度を公的なハッシュ値の存在証明および非改ざん証明として利用することが考えられる．

しかし，公証制度は，民間における法律関係の明確化等を図ることを目的とした制度であり，そもそも公務員が作成した文書についての利用を前提としていない．法文上も公務員が職務上作成した電磁的記録以外のものに限定されている（公証人法１条１項４号但書，民法施行法５条２項但書）．

もっとも，公務員が作成ないし管理・保管している書面や電磁的記録であるからと言って，それらが，改ざんのリスクと無関係であるという訳ではない．従って，現行制度の枠組

みに必ずしも限定される必要はなく，広く電子公証制度を捉え直す視点を持つことも必要であるが，それには新たな立法を必要とする．つまり，電子公証制度をデジタル証拠の改ざん防止に利用することは，公証人の社会的位置づけも含めた現行制度の大きな変更を必要とする．

4.4.1.2　民間のタイムスタンプサービス

次に，民間事業者による電子署名を用いたタイムスタンプサービスの利用について検討する．

タイムスタンプサービスとは，タイムスタンプ局とよばれる第三者機関が，利用者の管理するデジタルデータに対して，ある時刻以前に存在したことを証明するタイムスタンプ技術を利用したサービスである[56]．この制度は，電子署名法に基づいて特定認証業務を行う事業者として認定された認証業者など信頼性の高い民間事業者による電子署名を用いた制度であり，電子公証制度と同じく技術的には公開鍵暗号を用いた，第三者機関の電子証明書の信頼に基づいた制度である[57]．

このサービスを利用すれば，電磁的記録のハッシュ値を生成した際に，そのハッシュ値をタイムスタンプ局に送信し，タイムスタンプ要求を行えば，タイムスタンプ局において時刻証明となる情報を添付したタイムスタンプ・トークンを生成し，それにタイムスタンプ局のデジタル署名を施して返送されることから，これを元のデータとともに保管しておけば，時刻証明された時刻以前にその内容のデータが存在したということが保証される．よって，デジタル証拠に対してタイムスタンプを付与することで，ある時刻での存在証明と非改ざん証明が可能となる．

4.4.1.3　立会人による電子署名

捜査機関が裁判所から令状の発布を受けて証拠の差押え等を行う場合には，前述した通り，捜索すべき場所において居住主等を立会人として立会わせることが必要とされている．これは，捜索場所に対する管理者として立会人が監視の目を光らせることを通じて，捜査機関による違法行為を抑止するための担保としての機能が期待されているからである．

そこで，捜査機関が押収したデジタル証拠のハッシュ値が改ざんされることを防止する手段として，この立会人を利用し，ハッシュ値に対して直接立会人の電子署名を求めた上でデータベースへ登録するなどの方法が考えられる．この場合，立会人が電子署名に用いる電子証明書の信頼性が PKI 等で確保されていることも前提となる．

4.4.1.4　既存技術をデジタル証拠の存在証明に用いる際の問題点

電子公証制度をベースとした電子公証システムにせよ民間事業者を利用したタイムスタンプ制度にせよ，さらに立会人による電子署名にせよ，技術的には公開鍵暗号に基盤を置いた制度であり，特に前二者については公的に認められた第三者に依存した制度である．デジタル証拠の改ざん防止という観点では，電子署名が正しく付与されていることを前提とすると，電子署名を付与する主体となる第三者，即ち，公証人，タイムスタンプ局及び立会人の果たす役割のみが異なる．

まず，特に前二者の制度については，公的に認められた第三者により，当該のデジタル証拠の存在と作成者の認証を行うことになる．電子署名を付与する主体となる第三者は高い信頼があることは利点である．その一方でこれらの第三者はデジタル証拠の存在については認証するが，その真正性については確認の手段を持たないため，その担保がない．逆に立会人による電子署名は，捜査機関が証拠の捜索や取得の過程で何らかの不正を行っていないか立会人によって監視することが期待されているという意味で，当該デジタル証拠に対する真正性は確保できているが，一方で立会人の信頼性には担保がない．

また，例えば，タイムスタンプは，タイムスタンプ局の電子署名が施されていることによってその時刻証明が保証されるが，その保証は，電子認証局がタイムスタンプ局に発行した公開鍵証明書の有効期限（通常は１０年）に限られる．有効期限を越えたデータは検証手段がなく，その有効期限を越えて保証されるためにはタイムスタンプを付し直さなければならない．電子公証では２０年の有効期限であり，立会人においてはその電子証明書の期限までとなる．従って，これらの制度では情報を長期的・永続的に保存することに限界がある．

さらに，電子公証制度においても，タイムスタンプ制度においても，情報の同一性を証明した電磁的記録やタイムスタンプが付された情報を公開する場所や手段がなく透明性が確保されていないという問題がある．タイムスタンプが付されたデジタルデータ（電磁的記録のハッシュ値）は，利用者の手元に保管されているだけであり，タイムスタンプ局が，時刻証明となる情報を一元的かつ集中的に管理・公開する訳ではない．この点は，立会人による電子署名の場合においても，データベースの管理者が捜査機関である場合には同じである．また，仮に，中立の第三者機関を想定した場合でも，当該第三者機関に過度な負荷や責任を負担させることになる点で問題が残る．

なお，電子公証制度において利用者が日付情報の付与を受けた電磁的記録と情報の同一性に関する証明を請求するためには（また，タイムスタンプ制度においても，申請の際，利用者による電子署名を要求するなら），電子署名（電子証明書の取得）が必要とされている（なお，現行法上，日付情報の付与の請求自体に関しては，当該電磁的記録に電子署名を付与する必要はない．）．しかし，押収された電磁的記録のハッシュ値を保全するシステムを考えた場合，直接的な利用が想定される警察官や検察官においては，例えば官職証明書を利用

するなどの方法が考えられるが，それに代わる制度のない弁護人にとっては利用しづらい制度となる．司法書士など多くの士業においては，司法書士会等各業界団体が主導して民間業者等を利用した職業上の電子証明書が付与されるシステムが既に構築されている．しかし，弁護士が「弁護人」ないし「代理人」として業務を行う上での同様のシステムは存在せず，弁護士が電子証明書を利用するには，新たに，PKI に基盤を置いた弁護士認証システムのような仕組みを構築する以外には，現状では，各弁護士が個人として電子証明書を作成するか，あるいは，同じく個人として公的個人認証サービスを利用するなどしか方法がない．

4.4.2　ブロックチェーンを利用する意義

そこで，特定の機関に過度に負荷が集中せず可用性が保証され，さらに，誰でも，そしていつでも情報を確認することができる透明性が確保され，しかも半永久的に保存可能なシステムとして，本論文では，ブロックチェーンを利用するシステムについて提案する．

ブロックチェーンとは，データベース全てをネットワーク参加者（ノード）全員が分散して共有し，そのデータの正当性を相互に保証する分散型台帳システムである．ブロックチェーンでは，ネットワークに送信された各データ（電磁的記録のハッシュ値）が複数纏められその全体のハッシュ値と一つ前のブロック全体のハッシュ値等から次のブロックが形成されるようにして，ブロックのチェーンが形成される仕組みとなっている．そのため，一旦格納されたデータに関して，1 つのノードで改ざんがあれば，ネットワークの全ノード間での整合性が保てなくなることから，データの改ざんは極めて困難となる．また，従来の技術は，特定の事業者や機関など中央集権的にデータを管理する機関の存在が前提とされていたが，ブロックチェーンでは，ネットワークに参加する全ノード間の相互の監視機能を以てデータの真正性を担保している．従って，その特定の機関が十分に信頼に足りる場合には敢えてブロックチェーンを利用しなければならない必要性は乏しいかもしれない．しかし，この場合でも，特定の機関に負荷が集中するリスクは避けられない．また，そもそもその特定の機関に対する信頼関係を前提に置けない場合，例えば，デジタル証拠を収集保管する捜査機関に対して根強い不信感から信用性を客観的に担保する制度が必要であると考える立場を前提とすれば，第三者機関であったとしても捜査機関の影響が強く及ぶ機関であれば意味がない．このような疑念を払拭して弁護人からも信頼できるシステムを構築する上でも，非中央集権的な管理の仕組みを持つブロックチェーンを利用する意義は十分見出せる．

現在，ブロックチェーンについては様々な用途への応用が模索されており，情報の真正性を保証するための公証システムとしてもその役割が期待されている[58]．本論文では，刑事手続におけるデジタル証拠の非改ざん証明としても，ブロックチェーンの有するこの公証システムが活用できるものと着目した．

４.５　ブロックチェーンを利用したハッシュ値保全システムの検討

押収された電磁的証拠のハッシュ値を保存・検証するためのシステムとして，既存システムを利用したシステムの問題点を指摘した上で，新たにブロックチェーンを利用したシステムの可能性について指摘した．そこで，次に，具体的にどのようなシステムが適しているか検討する．

4.5.1　ブロックチェーンの種類

ブロックチェーンには，大きく分けて(ⅰ)アンパーミッションド型（パーミッションレス型）と(ⅱ)パーミッションド型が存在する．前者(ⅰ)は，ビットコインやイーサリアム等に代表される中央の管理者を必要とせず，ネットワークへの参加について制限を設けない自由で開かれたシステムである．このシステムにおいては，利用者の身元確認は必須ではなく，台帳に書き込まれたデータは誰でも閲覧・参照が可能であるとされる．これに対して，システムに接続し台帳のデータを書き込んだり，閲覧・参照ができる利用者を一定の資格を有する者に制限したいという要請から，システムへの参加要請等に対して，単独ないし複数の管理者によるシステム許可ないし承認を必要とするものが後者(ⅱ)である[59].

4.5.2　ハッシュ値保全システムにとってのブロックチェーンとは

では，ハッシュ値保全システムを構築するにあたってはどのタイプのブロックチェーンの利用が適しているか.

分散型台帳に保全されるデータは，捜査機関が押収した電磁的証拠のハッシュ値であることや台帳に書き込まれたデータを参照・確認するニーズを有している者は弁護人や被疑者・被告人，被押収者等の当事者，あるいは捜査機関や検察等に限られる．また，台帳に書き込むことが想定されている主体も捜索押収の実施主体である捜査機関に限られている．これらのことを考えると，広くシステムの利用を一般に開放する必要性は乏しく，パーミッションド型のブロックチェーンの方が適していると考えることもできる.

もっとも，台帳に記録されるデータは，電磁的証拠それ自体ではなく，あくまでもそのハッシュ値であり，その値自体には特別な意味はない．また，押収された電磁的記録のハッシュ値の保全を目的としたシステムの構築を検討しているが，翻って考えてみれば，民事・刑事を問わず，訴訟において利用されるデジタル証拠一般に広く応用可能であると言える．そうすると，必ずしも，システムの利用者を捜査機関や法曹関係者に限定しなければならない

理由も薄い．実際，改ざんの有無を検証するためのハッシュ値情報の開示は，広く一般に公開されている方がより客観的であり，かつ信頼性も高い．また，逆に，ブロックチェーンのネットワークへのデータの送信（書き込み）に関しても，利用者を限定しない場合の弊害はさほど大きくないと考える．確かに，ブロックチェーンの利用者を限定せず広く一般に開放した場合，無関係な情報が溜まっていく可能性は否定できず，また，制度に便乗し私的な利用が横行したり，ひたすらブロックを生成したりする攻撃にさらされるリスクも高まるかもしれない．しかし，ブロックチェーンにおける信頼の源泉は，ブロックチェーンのネットワークにより多くのノードが参加し，ブロックが長く続いていくことによる耐改ざん性にある．とすれば，できるだけ多くの参加者に利用されることによってもたらされるメリットも無視できない．

以上の点を勘案して，パブリックなシステムとして検討した場合のメリットを重視して，基本としてアンパーミッションドなブロックチェーンの枠組みを利用することによって，システム利用者に対する参加制限等は特に設けないものの，他方，ネットワークを確実に稼働させる上で必要となるマイナーとなりうる特定のノード（フルノード）を複数設置してブロックチェーンネットワークで結ぶシステムの構築を提案する．

4.5.3　電子署名

ブロックチェーンを利用する際にはユーザはアカウントを作成しなければならないが，利用者に限定がなく自由に参加できるアンパーミッションドなブロックチェーンの場合，このアカウントは任意に作成できることが一般的である．アカウントの作成には，秘密鍵と公開鍵の鍵ペアを生成し，この公開鍵をハッシュ化する等の方法による．また，ここで生成された秘密鍵は，ユーザがトランザクションを発行する際に，トランザクションの内容が不当に改ざんされないように署名を行う際にも使用される．

ところで，アンパーミッションドなブロックチェーンにおいて使用される秘密鍵と公開鍵のペアは，PKI とは基本的に異なるものである．PKI においては，秘密鍵と公開鍵を所有する者を信頼される第三者機関（認証局）が証明する仕組みとなっているが，特定の機関によって管理されていないアンパーミッションドなブロックチェーンにおいては，単に公開鍵やアドレスによってのみユーザが識別され，それが実際は誰なのかはブロックチェーン内部の仕組みからは確認できない．従って，ユーザが電子署名を行ったとしても，そのユーザが誰なのかは分からない．しかし，利用者を制限せずに誰でも利用できるシステムの構築を検討するにしても，ブロックチェーンへの情報の登録者が全く誰かも分からないのではシステムの利用に支障が生じ得る．従って，ユーザ確認のための手段についての検討が必要となる．

4.5.4　利用者確認手段の検討

そこで，まず，利用者（ユーザ）を確認（KYC）するための手段に限定して PKI ないし類似の仕組みを利用することはできないか検討する．この点，捜査機関に関しては官職証明書の利用が可能であるが，特に，弁護士に関しては，弁護士 PKI のようなシステムが存在していないことは前述した通りである．従って，利用者確認の手段として PKI ないし類似の仕組みを適用し，かつ，利用者として，捜査機関関係者だけではなく，広く弁護士に対しても開こうとするなら，弁護士PKIのようなシステムを新たに構築することが必要となる．具体的には，例えば，登録弁護士に関して，登録身分証として IC カードを新たに発行し，そこに秘密鍵と公開鍵の鍵ペアを登録し，日弁連あるいは各単位会において，誰にどの鍵ペアを配布したのかという情報として，各登録弁護士の公開鍵を登録番号等から検索できるように開示する方法が考えられる．しかし，新たな弁護士 PKI システムの構築をブロックチェーンによるデジタル証拠保全システムの前提とすることについては，実現に向けての不確定な要素が大きく，必ずしも適切とは言えない．

そこで，詳しくは，4.6.3.3 節で詳述するが，弁護人や立会人など利用者の KYC として，システム利用者がブロックチェーン上で初めに鍵ペアを生成した際に，生成されたアカウント（アドレス）を所属機関等に届け出て，アカウント保管用サーバにおいて記録・管理する制度が考えられる．但し，この方法では，登録する際に，なりすましや名義貸し等の一定のリスクは避けられないかもしれない．しかしながら，例えば，立会人については，捜査機関において身元の確認がなされていると言えるし，弁護士について言えば，所属の弁護士会が利用者である弁護士の身分を確認することは容易であることから，上記リスクは最低限に抑えられると考える．

4.6　Ethereum ブロックチェーンを利用したハッシュ値保全システムの提案

4.6.1　Ethereum（イーサリアム）ネットワークの利用

以上の検討を踏まえて，ブロックチェーンを利用したハッシュ値保全システムをアンパーミッションドなブロックチェーンのネットワーク上で実行させるプラットフォームとして，実装の容易性を考慮して Ethereum（イーサリアム）ネットワークを利用する．イーサリアムは，暗号資産（仮想通貨）の分野では Ether と呼ばれる暗号資産として，ビットコインに次ぐ市場規模を有しているが，本来的には，単なる暗号資産のための基盤としてだけではなく，スマートコントラクトと呼ばれるブロックチェーン上で実行する任意の自動プロ

グラムのプラットフォームとして開発されたものである．現在も開発が継続しており，実績のあるプラットフォームの１つである[60][61][62][63].

イーサリアムのネットワーク上では，ブロックチェーン上に実現したい各種のスマートコントラクトを格納し，ノード間で実行・共有することが可能であるが，そのスマートコントラクトを実行するためのコストとして，Gas と呼ばれる手数料が Ether を利用して支払われる．また，スマートコントラクトは，１６０ビットのアドレスで表示されるアカウントと呼ばれる概念で管理される．アカウントには，イーサリアムを利用するユーザが保持する外部所有アカウント（EOA : Externally Owned Account）とスマートコントラクトを表すコントラクトアカウント（CA）の２種類がある．外部所有アカウントは，秘密鍵によって管理されたアカウントであり，Ether を送金するトランザクションやスマートコントラクトを実行するトランザクションを発行する際にそのトランザクションに秘密鍵で電子署名を付すことでトランザクションの発行が認証される．そして，コントラクトアカウントは，スマートコントラクトをブロックチェーンにデプロイした際に外部所有アカウントからトランザクションを介して生成されるアカウントとしてブロックチェーン上に存在し，外部所有アカウントが発行するトランザクションをトリガーにスマートコントラクトに記述されたコードを実行する．但し，外部所有アカウントとは異なり，秘密鍵は持たない．

4.6.2　システムの概要

捜査機関が押収したデジタル証拠の同一性確保のためのハッシュ値（以下，「証拠ハッシュ値」という．）をブロックチェーンネットワーク上に登録・保全するための証拠ハッシュ値保全システムの大まかな概要は以下の図 4.5 の通りである．

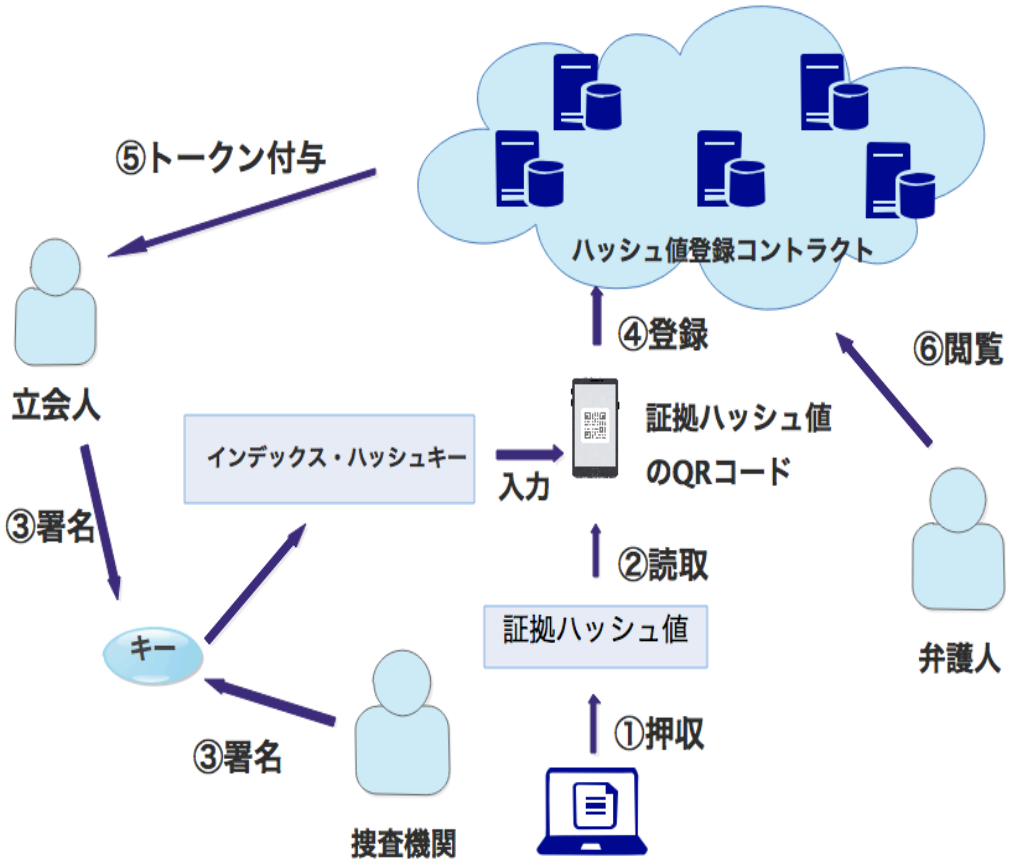


図 4.5　証拠ハッシュ値保全システムの概要

4.6.2.1　主なシステムの利用者

(1)　捜査機関
証拠ハッシュ値を生成しそれをシステムに登録する.

(2)　立会人
捜査機関による登録に対して電子署名（マルチシグ）を行う.

(3)　弁護人
捜査機関が登録し立会人が電子署名した証拠ハッシュ値を閲覧することができる.

4.6.2.2　捜査機関の活動

⑴　デジタル証拠を押収する．

⑵　ツールを用いてデジタル証拠の証拠ハッシュ値及び暗号化された日時情報等の付加情報を生成する．

⑶　証拠ハッシュ値及び暗号化された付加情報は捜査機関のツール（PC）上で QR コードに変換され画面に表示される．

⑷　QR コードをスマートフォンで読取る．

⑸　4.6.2.2 節⑷で読み取った情報をブロックチェーン上に登録する．

4.6.2.3　立会人の役割

⑴　4.6.2.2 節⑶で表示された QR コードをスマートフォンで読取る．

⑵　4.6.2.2 節⑸の登録に対して押収現場での立会いの証明として電子署名（マルチシグ）を付加する．

4.6.2.4　弁護人の役割

⑴　起訴後，捜査機関からデジタル証拠の開示を受ける．

⑵　ブロックチェーン上の証拠ハッシュ値を閲覧する．

⑶　開示されたデジタル証拠のハッシュ値と比較することによって，4.6.2.3 節⑵の立会人の署名時から改ざんされているか否か確認する．

4.6.3　証拠ハッシュ値保全システムの具体的内容について

証拠ハッシュ値保全システムの具体的な内容及び手順は以下の図 4.6 の通りである．

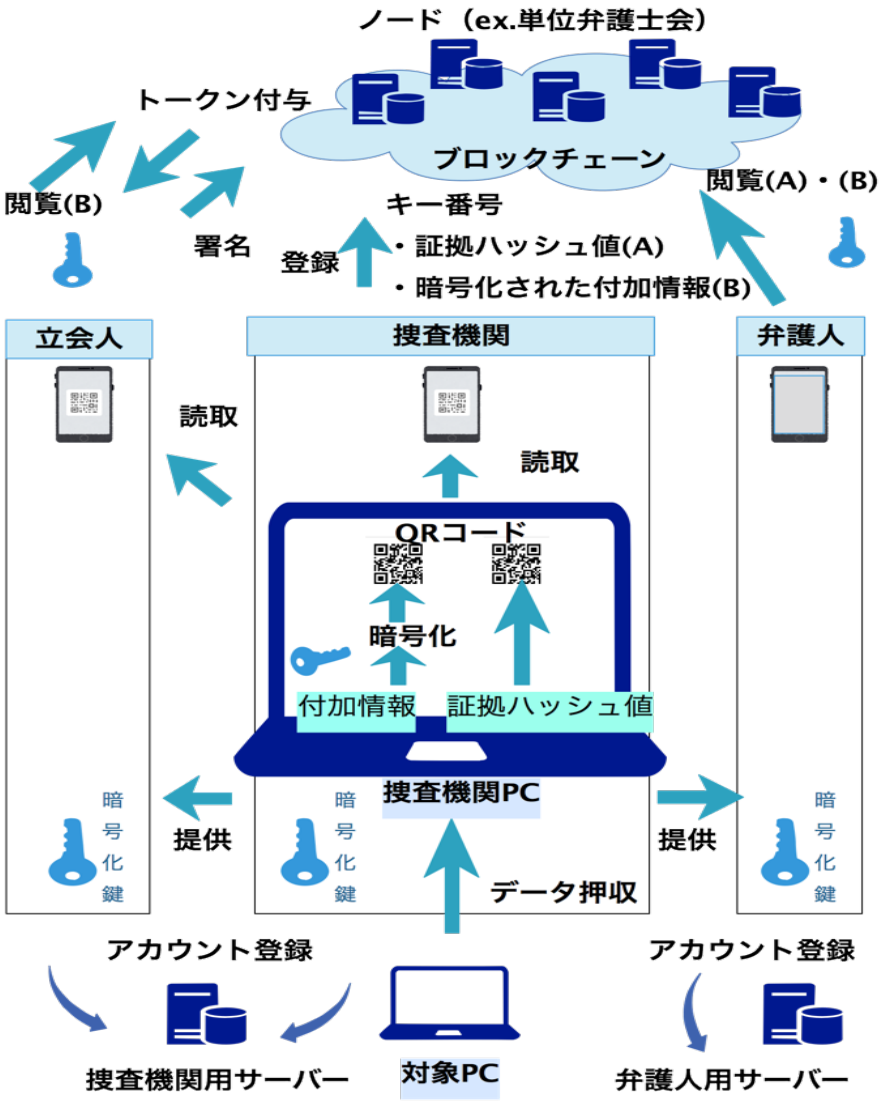


図 4.6　証拠ハッシュ値保全システムの具体的内容・手順

4.6.3.1　システムの利用者

このシステムの主な利用者としては，証拠ハッシュ値を登録する警察官や検察官等の捜査機関，押収手続きの適法性の担保として捜査機関による登録に対して電子署名（マルチシグ）を行う立会人，そして証拠ハッシュ値を閲覧し，立会人が署名した時からデータの内容

が改ざんされていないかを確認する弁護人を想定している．主たるユースケースとしては，このように刑事事件において捜査機関が証拠ハッシュ値を登録し弁護人が閲覧・確認するケースを想定するが，弁護人が登録し，捜査機関に閲覧させるケースもある．また，後述するが，民事事件において，弁護士等当事者同士が利用することもできる．なお，証拠ハッシュ値の閲覧・確認については利用者を限定せず，検索キーを知る限りシステム上は誰でも利用可能とすることで信用性を担保する．

4.6.3.2　特定ノードの設置

ネットワークを確実に稼働させるためにブロックチェーンを構成する特定のノードを複数設置する．この点，ノードを局地的に偏在させることなく，また，全国的に一定のノード数を確保するという観点から，例えば，全国の地方検察庁（または警視庁及び道府県警察本部）ごとに設置する案や地方裁判所ごとに設置する案，あるいは単位弁護士会ごとに設置する案，若しくはそれらを組み合わせた案などが考えられる．しかし，まず，現行刑事訴訟制度が採用する当事者主義的訴訟構造を前提とすれば，敢えて裁判所を関与させる必要はない．重要なことは，このシステムが捜査機関側にとっても弁護人側にとっても安心して利用できるシステムであるということである．そうすると，捜査機関と弁護士会が協同してシステムを運用する方法が望ましいと言えるかもしれない．しかし，そもそも本システム構築の目的が捜査機関の不正を防止し，弁護人からも信頼できるシステムを構築するという点にあること，各弁護士会が結託していわゆる５１パーセント攻撃を仕掛けるような不正な事態が想定しにくいことを考えれば，弁護士会設置のノードが過半数となるようノードを設置する．最低でも，各単位弁護士会によるノード設置とする．

4.6.3.3　システムの利用方法

システムの利用者は，利用時にシステムを利用するためのスマートフォンアプリ（ウォレットアプリ）をダウンロードする．この点，ウェブサイト上で稼働するウェブアプリを利用した方が利用者の利便性を考えた場合便宜であるとも考えられるが，サイト管理者による秘密鍵の管理・責任の問題を回避するために，ここではスマートフォンアプリを採用する．

アプリインストール後，アプリ内で電子署名用の鍵ペアを作成する．但し，特定の公開鍵の利用者が推測されるリスクを防止するために 1 人につき１つの鍵ペアに限定（固定化）することはせずに，手続きごとに作成する．また，固定化しないことで，秘密鍵を紛失した場合のリスクも最小限に抑えることが可能となる．そして，システム利用者（捜査機関，弁護人及び立会人）に対しては，公開鍵（利用者アカウント）を捜査機関及び弁護士会が別途

設置したアカウント登録用サーバにその場で登録させ，秘密鍵は各スマートフォンで各自が管理する．そして，ユーザ確認のために，アカウントとともに氏名，所属も合わせて登録させる（後日の報告でも可）．但し，立会人（捜査機関以外）に対しては，プライバシーに配慮してアカウントと氏名のみの登録を求め，住所等の個人情報の登録までは求めない．なお，捜査機関及び立会人については，捜査機関が設置した登録用サーバに登録させ，弁護士については，弁護士会が設置した登録用サーバに登録させ，それぞれ本人確認の義務を負担，相互に確認できる仕様とする．

なお，立会人が，自分は捜査機関の押収手続に立会っていない，ブロックチェーンへの証拠ハッシュ値の登録に対して署名などしていない，あるいはこのアドレスは自分のものではない等と立会人であることを否定する場合もあるかもしれない．しかし，提案システムにおいては，立会人の公開鍵（利用者アカウント）及び氏名については捜査機関が別途設置したアカウント登録用サーバに登録させる仕組みとなっており，一定の本人確認は担保されている．また，そもそも捜査機関は，押収手続に際して，立会人の住居，職業，氏名，年齢について記録している．従って，たとえ立会人本人が自分は立会人ではない等と否認した場合であっても，署名自体の検証は可能である．もっとも，立会人の情報については捜査機関において管理されているとは言っても，捜査機関が虚偽の情報を開示することはないのか，どこまで信用しても良いのかという問題は残る．しかし，後述する通り、立会人の電子署名を検証できなければ，捜査機関にとっては自らの不正が疑われるだけであって，捜査機関が虚偽の申告をする実益は事実上考えられない．

4.6.3.4　登録情報

捜査機関は，デジタル証拠を押収し，ツール（特定のアプリケーションがインストールされた PC 等）を使用して証拠ハッシュ値を作成する．証拠ハッシュ値を算出するためのハッシュアルゴリズムは，現在安全性が認められ一般的に使用されている SHA-256 を採用する．また，データ自体ではなく記録媒体自体に対してハッシュ値を取る場合，ハッシュ値を取る対象となるデータについて，媒体のデータのみを対象とするのか，媒体のメタデータを含むのかについては，予め合意を形成しておくか，前述の証拠開示の際に別途通知する等して弁護人らに開示する．

また，捜査機関は，証拠ハッシュ値の生成時に，その生成時の日時情報，生成場所の位置情報，同一性確保のためのデータサイズ（Byte 単位）の情報，及び目録情報（以下，「付加情報」という．）についてもツールを用いて自動的に生成する．付加情報は，捜査情報として第三者に公開されるべきでないことから，生成と同時に暗号化する．

4.6.3.5　具体的な登録手順

証拠ハッシュ値及び暗号化された付加情報は，それぞれ PC の画面上に QR コードとして表示される．

捜査機関は，この QR コードをウォレットアプリがインストールされたスマートフォンで読取りブロックチェーンに登録する．登録に際しては，弁護人等システムの利用者が，事件ごとに登録情報を検索するための検索キーとして，当該事件ごと（事件単位）に付された一意の番号（以下，「キー番号」という．）を付す．これは一括して検索できるようにした方が利便性に優れているからであるが，他方で，無関係の第三者がむやみに検索することを防ぐために，このキー番号にランダムな数値（ソルト）を加えハッシュ化したものを検索キーとして利用する．

立会人においても，ウォレットアプリをダウンロードしたスマートフォンを利用してこの QR コードを読み取り，捜査機関による登録に対して，電子署名（マルチシグ）を施すことを要するものとする．こうすることで，立会人が，押収手続きの現場にいたことの証明となり，押収手続きの適法性の担保の一つとなる．

また，詳細については後述するが，立会人が電子署名を行うことなどのインセンティブを得るために，立会人の署名に応じて一定数のトークンが当該立会人に付与される仕組みとする．このトークンは，弁護士会が発行し，弁護士会が提供する各種リーガルサービス等に利用できることとする．立会人は，捜査機関から付加情報を暗号化する際に使用された暗号化鍵（復号鍵）の提供を受けることにより，付加情報の内容を確認することができる．

なお，立会人は，自らが立ち会った押収現場で押収されたデジタル証拠だけではなく，自らは立ち会っていない，同一事件であるが別の機会に別の現場で押収されたデジタル証拠に関する付加情報についても，同一の検索キー（キー番号）で検索・閲覧できる可能性が懸念される．この点，これを直接防ぐためには，立会人ごとにソルト値を変更する方法が考えられる．しかし，そうすると，弁護人における前述の一括検索の便宜が損なわれ，あるいは，捜査機関と立会人が共謀して証拠の存在を隠蔽するリスクを生む危険をもたらす．もっとも，付加情報については自動的に暗号化されていることから，立会人ごとに一意の暗号化鍵（復号鍵）を用意すれば，立会人にとっては，自らが立ち会った現場で押収されたデジタル証拠以外の証拠の付加情報は全て暗号化されており内容を確認することは不可能であるから，この問題は回避できる．

4.6.3.6　証拠ハッシュ値の記録・開示

最後に，捜査機関は，証拠ハッシュ値等及びキー番号を，捜索手続終了時に作成される押収品目録ないし弁護人に証拠開示される際に作成される開示証拠目録等に記載する．弁護

人は，キー番号をもとに当該事件に関連してブロックチェーン上に格納された証拠ハッシュ値等の情報について一括して閲覧・確認することが可能となる．弁護人は，公判段階において，検察官から提出されたデジタル証拠についての報告書等の書証に関して，データの内容が改ざん等されていないか真正性・完全性を確認する必要が生じた場合，検察官から当該デジタル証拠の物理コピーないしイメージファイル等の提供を受け，これから算出したハッシュ値とブロックチェーン上のハッシュ値を比較し，改ざん等の可能性を判断し，弁護活動に活用する．

４.７　システムの信頼性評価

刑事裁判においては，捜査機関が押収した証拠のうち，検察官が公判で取調べを請求する予定の証拠は公訴提起後必ず弁護人に開示される．また請求証拠以外の証拠でも，一部の証拠は任意ないし法定の開示制度に従い弁護人に開示される．弁護人は，検察官から開示された証拠を吟味し，その真正性・完全性等に疑念があると考えれば，裁判所に対して，それが公判において証拠として取り調べられることに対して不同意ないし異議の意見を述べて争う．そして異議等の意見が採用されず取り調べられることになった場合は，公判において証拠の信用性等について争う．デジタル証拠の場合，弁護人が真正性・完全性，あるいは信用性等を争うための方法として，デジタル証拠の原本の物理コピー等から算出されたハッシュ値を検討することが必要となる．その際，提案システムを利用し証拠ハッシュ値が押収時に登録されていれば，弁護人は，証拠ハッシュ値との齟齬を確認して改ざんの有無を検知することができ，公判において，その齟齬の存在を根拠に証拠能力や信用性等について争うことが可能となる．

従って，提案システムに期待される最も重要な機能は，弁護人にとって，証拠が改ざんされているかもしれないと疑うに足りる根拠が示されること，即ち，開示された証拠と登録されている証拠ハッシュ値の間に齟齬が存在する場合である．

他方，証拠ハッシュ値をブロックチェーンに登録する過程で不正な手段が介在し，正しくないハッシュ値が登録される場合は，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に登録されているハッシュ値との間に齟齬が存在しない場合が生じる可能性も否定できず，その場合，弁護人は，改ざんを検知することができない．従って，提案システムを活用しても，弁護人が不正の端緒を発見できないリスクが高いのであれば，提案システムに対する信頼は得られない．そこで，本節では，提案システムの信頼性に対する評価に関して，弁護人にとって捜査機関の不正の端緒を発見困難とするリスクとしてはどのようなリスクが考えられるかという観点から検討する．なお，提案システムへの登録の過程で不正や過誤が生じるケースとしては，立会人による場合，当事者以外の第三者による場合も考え得るが，提案システムは，捜索押収現場での捜査機関による不正防止を主な目的としていること

から，ここでは前提として，不正行為の主体は捜査機関であるという場合に限定して検討する．

4.7.1　想定されるリスク

捜査機関がデジタル証拠を押収し，提案システムに登録する過程で生じる可能性のある不正として以下の図 4.7 の通りのケースを想定した．Ⅰ 最終的に押収証拠から算出された正しい証拠ハッシュ値が登録されない場合，Ⅱ 正しい証拠ハッシュ値が登録されているものの，同一事件でありながら異なる現場で押収された証拠に同一のキー番号が付されていない場合，そして，Ⅲ 立会人ないし立会人のアドレスが差し替えられる場合が考えられる．そして，Ⅰの場合には，さらに，Ⅰ_1 正しくない証拠ハッシュ値が登録される場合と，Ⅰ_2 証拠ハッシュ値がそもそも登録されない場合が考えられる．また，Ⅰ_1 の場合は，Ⅰ_1_①登録前に証拠自体を改ざん，あるいは捏造，すり替えて，その改ざん等した証拠から証拠ハッシュ値を計算して登録する場合と，Ⅰ_1_②もとの証拠自体は改ざん等していないものの、正しくない証拠ハッシュ値を算出・捏造して，その正しくない証拠ハッシュ値を登録する場合，そして，Ⅰ_1_③正しい証拠ハッシュ値が一旦適切に登録されたにも関わらず，同一証拠につきオリジナルデータを改ざん等した上で改めて証拠ハッシュ値を算出してそれを登録する場合が考えられる．

なお，それぞれの場合ごとに，捜査機関の故意による場合，過失等ヒューマンエラーが発生した場合，そして捜査機関のツールやスマートフォンアプリの不具合・エラー・バグ等システムや機械関係のエラーによる場合が考えられる．もっとも，証拠ハッシュ値及び付加情報の生成，これら情報の QR コードへの変換・表示は，捜査機関のツール上で自動化されている．また，QR コードをスマートフォンで読取り，その情報をブロックチェーン上に登録するプロセスについてもほぼ自動化されていることに鑑みると，ヒューマンエラーが生じるリスク自体は低いと評価できる．また，ツールの不具合やシステム自体のエラー等についても，リリースまでに通常想定できる程度の適切なテスト等を経ていれば発生確率はさほど高くはないと評価できる．しかも，ヒューマンエラーにせよツールの不具合にせよ，弁護人に開示されたデジタル証拠から算出されたハッシュ値との間で齟齬が生じることになり，結果として，捜査機関によるデジタル証拠の改ざんが強く疑われる事態を招く．かかる事態は，捜査機関にとっては不利益となるだけである．従って，捜査機関による不正防止の観点からは，この場合のリスクは考慮する必要に乏しいことから，本論文では，ヒューマンエラーやツールの不具合等については検討の対象から外し，捜査機関の故意による場合を前提とする．

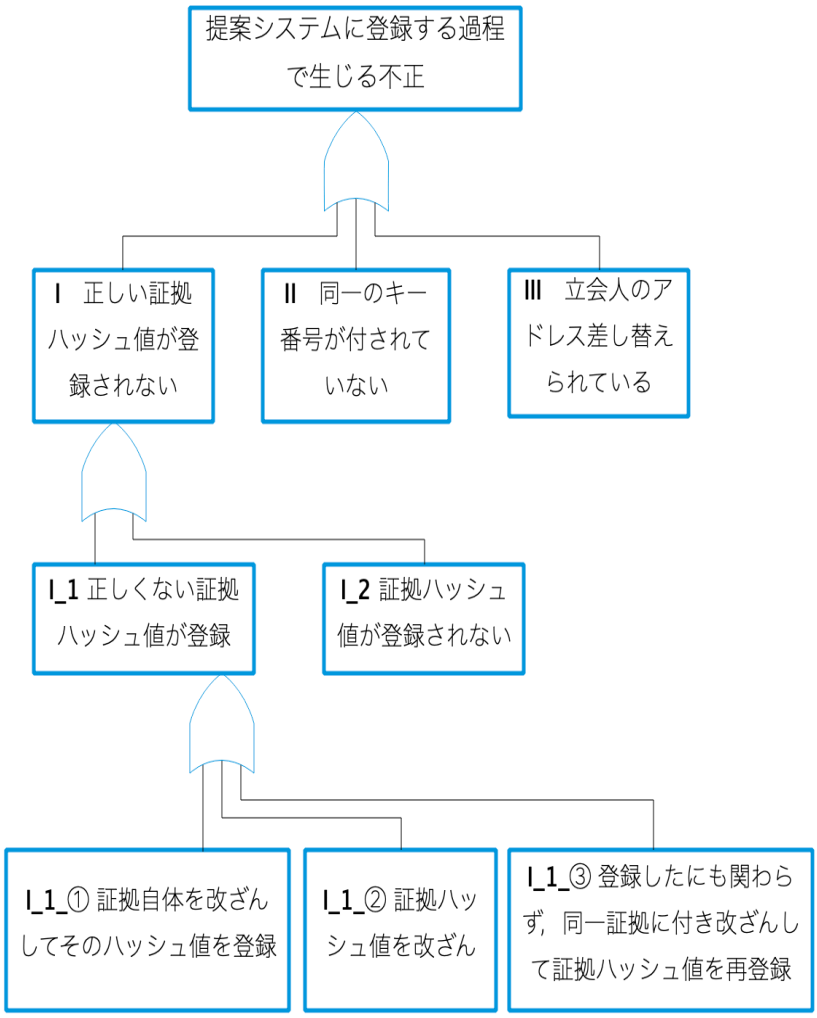


図 4.7　提案システムに登録する過程で発生する不正

4.7.2　想定する必要性の乏しいリスク

提案システムを活用してデジタル証拠の改ざんが検知できるケースは，開示された証拠と登録されている証拠ハッシュ値の間に齟齬が存在する場合であるが，図 4.7 のうちその条件に該当しないケースは以下の３つである．

4.7.2.1　同一のキー番号を付さないリスク（Ⅱ）

前述の通り，本論文では，事件単位での検索を可能とするキー番号を提案するが，捜査機

関が，同一事件内の手続きでありながら手続きごとないし証拠ごとに別のキー番号を付す，あるいは，キー番号に変更を加えずとも別々のソルト値を付加することで，弁護人の一括検索を困難にし，隠したい証拠の存在を隠蔽するリスクである．この場合，捜査機関は，ブロックチェーン上に登録してはいるが，一部の証拠について，結果的にその存在を隠蔽していることになり，その点では，Ⅰ_2 の場合と同様である．押収したデジタル証拠に関して，別々のキー番号，ソルト値が一旦付されてしまえば，証拠改ざんのリスクは低いにせよ，隠蔽のリスクを完全に防ぐことは難しい．従って，同一事件内での押収手続きにおいて，異なるキー番号，異なるソルト値が付される可能性を排除するための技術的工夫は必須である．もっとも，捜査機関が証拠の存在を隠蔽する意図を有しながら，それでもなおブロックチェーン上に登録するような事態は，捜査機関にとっても隠蔽が発覚するリスクなどを考えれば，現実的にはその可能性は低いと評価できる．

4.7.2.2　正しく計算されていないハッシュ値が登録されるリスク（Ⅰ_1_②）

捜査機関が押収した対象証拠自体は改ざん・捏造されていなくとも，ハッシュ計算を行う際に正しく計算せず，正しくない証拠ハッシュ値がブロックチェーンに登録されるリスクである．このような不正が行われるケースも，可能性としては想定できる．しかし，ヒューマンエラーやツールの不具合等による場合と同様，このような不正が存在したとしても，弁護人に開示されたデジタル証拠から算出されたハッシュ値との間で齟齬が生じることになってしまい，結果として，捜査機関によるデジタル証拠の改ざんが強く疑われる事態を招く．従って，捜査機関にとって，正しくない証拠ハッシュ値を作成し，ブロックチェーンに登録する実益はなく，捜査機関による不正防止の観点からは，この場合のリスクは考慮する必要に乏しい．

4.7.2.3　捜査機関が立会人あるいは立会人のアドレスを差替えるリスク（Ⅲ）

捜査機関が実際の押収手続に立会った立会人を隠蔽するなどし，虚偽の立会人の情報を開示，あるいは立会人のアドレスを差替える等のリスクである．しかし、捜査機関がこのような不正を行った場合，真の立会人による電子署名（マルチシグ）の検証ができなくなるだけである．これは，捜査機関にとっては，証拠ハッシュ値の登録に対して何らかの不正が行われたという疑いを向けられる以外のことはなく，捜査機関がかかる不正を働く実益は事実上考えられない．

4.7.3　提案システムでは検知が困難な不正

以上のケースでは，リスクとして想定可能ではあるが，現実的には考慮する必要性に乏しいリスクであると評価できる．これに対して，以下の３つのケースの場合は，提案システムでは検知が困難であり，大きなリスクをはらんでいると評価できる．

4.7.3.1　デジタル証拠を改ざん（すり替え）してハッシュ値を算出するリスク（Ⅰ_1_①）

(ⅰ)捜査機関が，押収現場でデジタル証拠を発見しても，それをブロックチェーンに登録する前に改ざんしその改ざんしたデジタル証拠の証拠ハッシュ値を登録する場合，また，(ⅱ)押収現場に存在していなかったデジタル証拠を捜査機関自ら押収現場に持ち込み，その場で押収したかのように偽装して（押収証拠をすり替えて），ブロックチェーン上に登録するリスクである．提案システムでは，捜査機関による改ざんの不正は検知できない．登録前に既に改ざんされている以上，登録された証拠ハッシュ値と開示を受けたデジタル証拠のハッシュ値との間には当然齟齬が生じていないことから，弁護人は，公判段階で，デジタル証拠の証拠開示を受けても，改ざんを発見することが困難となる．

もっとも，捜査機関が，デジタル証拠をブロックチェーンに登録するためには，押収現場での立会人によるマルチシグが必要であることから，捜査機関がデジタル証拠を押収後，警察署等に持ち帰った後に登録することは立会人と結託する以外事実上不可能である．従って，捜査機関が証拠を発見後ブロックチェーンに登録する前にデジタル証拠を改ざんする(ⅰ)の場合であれば，捜査機関は，押収後直ちに，あるいは極めて短時間のうちに改ざんを実行しなければならないという限りで一定のハードルは存在する．そこで，捜査機関によるこのような不正行為を防止するためには，押収したデジタル証拠をコピーするツールと証拠ハッシュ値を生成するツールを同じツール上で行い，捜査機関が押収したデジタル証拠の改ざんを実行できるプロセスを介在させないような仕組みが必要となる．

これに対して，捜査機関が，初めからデジタル証拠をすり替えて登録する(ⅱ)の場合は，デジタル証拠は押収の段階で既に偽造されていることになって，この場合は提案システムの守備範囲を超えている．立会人が捜査機関と結託している場合はもとより，そうでない場合であっても，立会人がその場で即座に不正を見抜く可能性は現実的には期待できず，提案システムではこのような不正に対処することはできない．従って，このような不正を見逃さないためには，例えば，デジタル証拠を捜査機関のツール上にコピーするプロセスからログを保存させておき事後的に検証できるような仕組みなど提案システムを補完するための仕組みが別途必要となる．

4.7.3.2　一旦登録した後に当該証拠を改ざんした上で正しくない証拠ハッシュ値を再び登録するリスク（Ⅰ_1_③）

捜査機関がデジタル証拠を発見した後，一旦は適切な手続きに従い，証拠ハッシュ値を算出し登録したものの，その後，対象証拠を改ざんして新たに不正な証拠ハッシュ値を算出してこれを再びシステムに登録するリスクである．捜査機関が証拠を改ざんしても，証拠ハッシュ値が既にシスムテに登録されていれば，証拠ハッシュ値との間に齟齬が生じることになる．しかし，改ざんされた証拠から再び証拠ハッシュ値を算出し，それを改めて登録し，新たなキー番号とともに弁護人に開示されれば，デジタル証拠の改ざん前に登録された証拠ハッシュ値は事実上発見することは困難であり，表面的にはハッシュ値の齟齬は認識されず，改ざんの検知は困難となる．但し，提案システムにおいて証拠ハッシュ値を登録するためには立会人による電子署名（マルチシグ）が必要である．従って，この不正が成り立つためには立会人の協力が不可欠である．立会人が被処分者である場合はともかく，住居の管理者等第三者であった場合，捜査機関による不正に関心を示さず，捜査機関による不正がなされてもなされるがまま放置する可能性も十分ありうる．ことに立会人が，捜査機関と結託・共謀して，捜査機関による改ざん等の不正を知りながら敢えて署名（マルチシグ）を行う場合を想定すれば事態はより深刻なものとなる．本来，立会人の制度は，捜査機関の不正・違法に対する担保のための制度であり，提案システムもその担保機能を利用している．従って，捜査機関と立会人が共謀して不正に関与した場合に関しては，提案システムでは十分な改ざん検知の効果は期待しえないと言える．

しかし，もともと立会人の存在だけで捜査機関による不正・違法が完全に防げる訳はない．だからこそ，立会人の担保機能を活用しつつ，それだけに依存するのではなく，上記 4.7.3.1 節(ⅰ)及び(ⅱ)で検討したような提案システムを補完し捜査機関による不正に対処するための仕組みが求められる．

4.7.3.3　証拠ハッシュ値を登録しないリスク（Ⅰ_2）

捜査機関が，ある現場において押収したデジタル証拠に関して，その一部ないし全部の証拠ハッシュ値をブロックチェーン上に登録しないリスクである．このような不正が行われた場合についても，提案システムを利用した改ざん検知は困難となる．押収した証拠が捜査機関によって都合の悪い証拠であったので敢えて登録しなかった場合や現場での登録を失念した場合（この場合，例えば，警察署に戻った後で登録しようとしても，立会人の署名が得られない以上，事後的に登録することもできない．）等が考えられる．この点，確かに，捜査機関にとっては，意図的であろうが過失であろうが通常の手続きを経なければ立会人

の不信を招きかねず，このような不正を防止するためにこそ立会人の存在意義があるとも言える．しかし，立会人は，必ずしも法律や情報科学の専門家ではなく，捜査機関の不正を看破できるとは限らない．また，そもそも捜査機関の不正に対して無関心である場合もないとは言えない．立会人の存在が捜査機関の不正防止に対する一定の担保として重要な役割を果たしていることは否定できないが，その機能には自ずと限界がある．提案システムでは，捜査機関が押収したデジタル証拠の存在を意図的に隠蔽しようとした場合には，その効果は期待できない．但し，一旦隠蔽したはずのデジタル証拠を，検察が公判段階で証拠請求した場合や，弁護人が公判前整理手続き等を経て証拠開示を受けた場合には，ブロックチェーン上に登録されていないことが明らかにされ，隠蔽の事実や改ざんの可能性が却って強く疑われることになるという反射的な効果は期待できる．そうすると，かかる不正は，検察にとっても信頼を揺るがす大きなリスクを伴う．

4.7.4　課題

提案システムは，捜査機関によって押収されたデジタル証拠に対して押収と同時にハッシュ値が算出され，そのハッシュ値が押収後直ちにブロックチェーンに登録されることを前提にしていることから，開示されたデジタル証拠から算出されたハッシュ値とシステムに登録されているハッシュ値の間に齟齬が生じていない上記 4.7.3 節で着目したリスクに対しては提案システムの範囲を超えており一定の限界が存在しているのは確かである。従って，このようなリスクに対しても対処するためにも，提案システムを補完する総合的な仕組みを構築することが重要な検討課題となる．

4.8　イーサリアムプライベートネットワークを利用した簡易ハッシュ値保全システムの構築

4.8.1　プロトタイプの概要

提案システムの有効性を検証するため，実際のシステムのプロトタイプを作成した．まず，証拠ハッシュ値を得るシステムとして， Python embeddable を用いて，パソコン内の Windows システムディスク（C ドライブ）のハッシュ値を計算し QR コードで画面上に表示するソフトウェアを構築した．このシステムを USB 上に構築した Windows PE for Windows 10 環境上に実装することで，USB 上からシステムをブートし，起動前状態の C ドライブのハッシュ値を計算して表示するシステムとした．ハッシュ値は C ドライブのデータを最初からセクタ単位で読み出して全体に対して SHA-2 で計算する．提案システムで

はこのハッシュ値を証拠ハッシュ値と考えることにした.

次に，Python Kivy[64]を用いて，カメラで撮影した QR コードを読み取り，スマートコントラクトを用いてその値をブロックチェーン上に登録した上で電子署名を付加する Android アプリケーションを作成した. ブロックチェーンとしては Ethereum の testnet である Ropsten を対象としている. PC 上に geth v1.11.5 を用いてフルノードとして Ropsten に参加し，その PC に対して Android アプリケーションから HTTP により接続してブロックチェーンに対する登録操作を行う構成とした．スマートコントラクトは Solidity で記述し，あらかじめブロックチェーン上に登録（デプロイ）しておく. 用いた Solidity のバージョンは v0.4.23 である[65][66][67][68].

スマートコントラクトには 3 つの関数を実装した. 1 つめは，捜査機関と立会人が証拠ハッシュ値をブロックチェーン上に登録するための関数（receiveHash 関数）である. 本関数は，捜査機関，立会人それぞれが異なるアドレスのウォレットから同一のハッシュ値を登録しようとするのを前提に，そのハッシュ値をキーとして動作するようにしている. つまり，当該の証拠ハッシュ値がブロックチェーン上に登録されているかどうか否かを調べ，登録されていなければ証拠ハッシュ値とアドレスを登録し，登録されていればそれに対して後から登録を試みたウォレットのアドレスをさらに紐付けることにより 2 名による電子署名（マルチシグ）を実現する．2 つめの関数（checkHash 関数）は，指定された証拠ハッシュ値が既にブロックチェーン上にあり，2 名により電子署名（マルチシグ）されているかどうかを確認するものである. 3 つめとして，何らかの理由で誤った証拠ハッシュ値が登録されていたときのために，その証拠ハッシュ値に対して無効フラグを加える関数（deleteHash 関数）も実装した.

なお，今回の実装では Android スマートフォン側にはウォレットを持たせず， PC 内においておき，Android アプリケーション側から PC 上のどのアドレスのウォレットを用いるかを指定している. だが，本来は捜査機関，立会人それぞれがウォレットをスマートフォン内など安全な環境にもつのが望ましい.

4.8.2 システムの評価

実際にこのプロトタイプを用いて証拠ハッシュ値を登録したところ，receiveHash 関数の実行には transmission cost に約 66000gas，execution cost に約 41000gas の合計約 107000gas を要した. また, checkHash 関数の実行には transmission cost に約 24000gas, execution cost には約 590gas の合計約 24600gas を要した．いずれも ETH 換算では極めて小さな値になる.

このプロトタイプにおけるシステムは実際の Ethereum の testnet 上に実装しているが，本来は，testnet ではなく，Ethereum のライブネットワーク上にブロックチェーンを構築

するべきものである．よって，この gas が直接システムの運用コストに反映される訳ではないが，ブロックチェーンへの証拠ハッシュ値登録がシステム運用に対して大きなコスト負担にはならないということはできる．

４.９　本章のまとめ

本章では，捜査機関によって収集されたデジタル証拠が収集・保全段階で捜査機関によって改ざんされることを防止するための証拠ハッシュ値保管システムを提案した．デジタル証拠の改ざんが，もはや特別な技術を必要としなくとも誰でも容易に行うことが可能であることが観察実験を通じて確認され，そのデジタル証拠が，捜査機関による押収段階及び保管・管理段階を問わず捜査機関による改ざんの危険性に常に晒されていることを示した．捜査機関によるデジタル証拠の改ざんを防止するためには，ハッシュ値の利用が効果的であるが，そのハッシュ値を保管するためのシステムとして，高い改ざん耐性を持つことが認められているブロックチェーンに着目し，実装のしやすやを考慮してイーサリアムネットワークを利用した証拠ハッシュ値補完システムを提案した．

弁護人は，本章での提案システムを使うことによって，検察から開示を受けたデジタル証拠から算出された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れば，仮に，捜査機関が押収したデジタル証拠を押収後に改ざんしたとしても、両者の間に齟齬が生じ，改ざんの有無を容易に検知することができる．提案システムのこの改ざん検知機能によって，捜査機関がデジタル証拠に対して改ざんなどの違法な行為を働くことを防止することに役立つ．そして，捜査機関が押収したデジタル証拠を改ざんしているのではないかという疑念を払拭することにもなり，ひいては国民に信頼される裁判に資することにも貢献できる．

もっとも，ブロックチェーン技術については，未だ発展途上の技術であり，提案システムが不具合なく，かつ効果的に動き続けるかどうかということについての検証は不可欠である．

また，提案システムは，押収されたデジタル証拠自体の改ざんを不可能にするようなシステムでも，また，証拠自体から改ざんの痕跡等を発見するためのシステムでもない．あくまでも，デジタル証拠の押収後に，仮に改ざんした事実があれば，その事実を検出するためのシステムである．従って，捜査機関がデジタル証拠（電磁的証拠）の押収手続きを実施した後できるだけ速やかにこのシステムが利用されなければ捜査機関による押収証拠の改ざんの疑念は減少しない．押収手続きと同時に押収した全てのデジタル証拠（電磁的記録）のハッシュ値を計算し，登録することができて初めて，その有効性・信頼性は確保されると言える．しかし，デジタル証拠の重要性が増すに比例して押収されるデジタル証拠の情報量等も膨大になっていけばいくほど，デジタル証拠の取扱いに対する捜査機関の実際の運用とし

ては，押収手続きから解析・ハッシュ値登録段階に至るまでの時間はむしろ長くなっていくことが容易に予想される．そうすると，捜査機関が提案システムを利用したとしても，デジタル証拠の改ざん防止に対する効果は限定的とならざるを得ない．もっとも，このような場合については，訴訟の場において，押収手続きの日時から実際にハッシュ値を登録した日時までの時間，あるいはそれだけの時間を要した理由の有無ないし理由の合理性等を検証して，改ざんの可能性の有無を判断する合理的な根拠を抽出する実務を積み重ねていくほかない．そして，最終的には，運用ないし立法，及び技術的な進展によって，押収と同時にハッシュ値を計算して登録可能なシステムの実現が目標となろう．

第５章　評価と考察

５.１　はじめに

刑事手続のデジタル化の流れに伴い技術的に検討・解決しなければならない課題として，２つの問題について検討した。第３章では，捜査手法のデジタル化に関する問題として，立会人の代わりに暗号技術を利用して適法性の担保とした改正通信傍受法に関して，法の枠組みを逸脱せず違法な通信傍受を防止できるシステムについて検討し，IC カードを利用した傍受システムの構築について提案した．そして，第４章では，捜査機関が押収したデジタル証拠に関して，捜査機関による改ざん防止のためのシステムとして，ブロックチェーンを利用した証拠のハッシュ値保全システムについて提案した．本論文で検討してきたこの２つの課題に対する提案は，前者においては捜査上の違法手段という問題点から見た課題に対して，そして後者においては押収されたデジタル証拠の改ざん可能性という問題点から見た課題に対して，それぞれ IT 化・デジタル化社会にとっての適正な刑事手続の実現のために解決しなければならない重要な課題に対して技術的な解決策を提案したものである．ところで，改正通信傍受法における暗号技術の利用については，1.3 節でも指摘した通り，主として，違法な捜査（盗聴）を防止するための担保としての性質が認められる一方，通信傍受によって得られた証拠（傍受記録）としての側面から見れば，裁判所における証拠の保全制度という性質も見て取れる．そこで，本章では，まず，改正通信傍受法における暗号技術の利用について，証拠の保全・管理の観点からの評価の是非について検討する．そして，その検討を踏まえた上で，ブロックチェーンを利用した証拠の保全システムとの関係についても言及し，最後に，ブロックチェーンシステムが円滑に運用できるための手段について考察する．

５.２　証拠保全の観点からみた通信傍受法の応用の是非

5.2.1　刑事手続における裁判所による証拠保管

改正通信傍受法によって採用された暗号技術は，主として，従前の立会人に代わって捜査の適法性を担保するための手段として採用された技術である．他方，改正通信傍受法では，捜査機関が傍受した通信記録は，裁判所によって発行された公開鍵で暗号化され，同じく裁判所によって発行され，裁判所のみが保管する秘密鍵によってしか復号できない傍受の原

記録として裁判所によって保管される仕組みになっている．従って，かかる側面から通信傍受法を評価すれば，一種の証拠の保全システムとしての機能ないし役割を有していると言える．刑事手続の一般原則として，捜査機関が行う証拠の収集・保全手続である捜索・押収は，裁判官によって発布された令状によって捜査機関が実施するものであるが，押収された証拠の管理・保全は，当事者主義の観点から，捜査機関が責任を持って行うものであり，裁判所が関与することはない．その限りでは，捜査機関による捜査活動の結果である傍受記録が裁判所によって保管される仕組みが採用された通信傍受法の建て付けは，当事者主義的訴訟構造を採用する現行の法体系のもとでは，ある意味で特異であると言えるかもしれない．これは，通信傍受という捜査手法がそもそも違憲の問題も含め人権侵害の可能性の高い捜査手法として批判も多いことから，例外的に裁判所の関与を認めようとした趣旨によるところが大きいと言えよう．

5.2.2　通信傍受法の仕組みの応用（転用）

しかしながら，他方で，捜査機関によって収集された証拠（傍受記録）に対して，裁判所による保管のための一定の仕組みがいずれにしても制度化されているという事実に目を向ければ，この仕組みを捜査機関が押収したデジタル証拠一般にも応用することが可能ではないのかということが考えられる．例えば，捜査機関が裁判所から捜索・押収令状の発布を受ける際に，裁判所が発行した公開鍵を合わせて受領し，捜索現場で押収した全デジタル証拠について暗号化した上で，裁判所に対して，「押収の原記録」のようなものとして提出するという仕組みが考えられる．この場合，捜査機関，被押収者及び弁護人等は，通信傍受法における開示手続に類する手続に基づき，必要に応じて，裁判所に対して，「押収の原記録」の開示を求めることができるということになろう．

このように，通信傍受法には，証拠の改ざん防止につながる裁判所における証拠保管のための制度が存在し，この制度を応用（転用）することによって，捜査機関によって押収されたデジタル証拠全般に対する一般的な改ざん防止のための保管システムを構築することに対しては，既存制度の応用に伴う一定のハードルの低さのようなものがあるのかもしれない．

5.2.3　問題点

しかし，通信傍受法における裁判所による「傍受の全記録」の保管の仕組みは，当事者主義的訴訟構造を前提とする現行刑事訴訟法制度のもとでは，あくまでも例外的な制度であると考えるべきである．そして，通信傍受という人権侵害の可能性について批判の多い捜査

手法に対して特別に定められた制度であると考えるなら，それをデジタル証拠の保全のための仕組み全般にまで広げることにはやはり疑問が残る．また，実質的な観点から見ても，捜査機関が押収したデジタル証拠の保管を全て裁判所の責任とすることについては，裁判所に対して過度な負担を負わせることにもなりかねず現実的とは言えない．通信傍受法における暗号化技術を利用したシステムの導入は，立会人に代わる担保の手段として，捜査機関による不正行為の防止としてこそ意味のあるシステムであって，傍受記録を裁判所が保管するという制度は，捜査機関の不正の有無を事後的に検証するための手段の１つとして設けられた制度に過ぎない．

5.2.4　通信傍受法における傍受記憶の保管とブロックチェーンを利用したデジタル証拠の改ざん防止システムの関係

捜査機関が押収したデジタル証拠に対してその改ざんを防止するために構築されるべきシステムとしては，確かに，通信傍受法における証拠の保管・管理のための仕組みを応用することも１つの方法としては可能である．しかし，通信傍受法において暗号技術を中心に構築されている仕組みは，あくまでも違法な捜査（盗聴）手続に対する抑止としての効果を期待するものである．裁判所による傍受の全記録の保管についても，人権侵害を招く違法捜査の懸念が特に強い通信傍受の分野において，捜査手続の違法性の抑止にとって有用であると考えられているからこそ採用されている制度である．また，当事者主義的訴訟構造を前提とする以上，裁判所による証拠の保管責任はあくまでも補完的・例外的な制度であると言うべきである．従って，捜査機関によって押収されたデジタル証拠について，その改ざんを防止するためのシステムとして，現行法上認められた類似の仕組みを応用（転用）できるという魅力もさることながら，当事者主義的訴訟構造の性質にも即した独自のシステムを構築しなければならないという理由があり，ここに，第４章で検討してきたブロックチェーンを利用した証拠の改ざん防止のためのハッシュ値保全システムを新たに提案する意義が認められる．

従って，本論文では，捜査機関が押収するデジタル証拠全般に対する改ざん防止のためのシステムとしては，中立的な中央集権的機関である裁判所による一括管理の方式を転用するのではなく、ブロックチェーンを利用した証拠ハッシュ値保全システムを提案する．

そこで，最後の検討課題として，次節では，このブロックチェーンを利用した証拠の改ざん防止システムについて，それが本当に円滑に運用されるのか，円滑に運用されるためにはどのような仕組み作りが欠かせないのかという観点から，さらにトークンエコノミーの構築について考察を加える．

５.３　ブロックチェーンを利用したデジタル証拠の改ざん防止システムの円滑な運用について

ブロックチェーンシステムは，捜査機関が押収したデジタル証拠の同一性確保のためのハッシュ値をブロックチェーンネットワーク上に登録・保管するためのハッシュ値保全システムであるが，捜査機関がハッシュ値を登録するための条件として，押収手続の際に立会いが求められている立会人による電子署名（マルチシグ）を必要とすることで信頼性担保の手段とした．本論文では，立会人の協力を得るためのインセンティブとして立会人に対してトークンを付与する仕組みを提案した．しかし，立会人に対してトークンを付与することが，立会人のインセンティブとなり本システムが有効に利用されるためには，そのトークンを活用して構築される独自の経済圏，即ち，トークンエコノミーを如何に構築していくかという視点が必要不可欠となる．

5.3.1　トークンエコノミーの構築の重要性

前章の提案システム（以下，本章で「提案システム」という場合は，前章での提案システムをいう．）では，立会人が電子署名（マルチシグ）を行うことに対して協力を得るためのインセンティブとなるために，立会人の電子署名に応じて一定数量のトークンが付与される仕組みを採用している．また，このトークンは，弁護士会が発行し，弁護士会が提供する各種リーガルサービス等に利用できることを想定している．このようにトークンの活用を想定しているのは，本システムが利用者ないし参加者にとって有効かつスムーズに運用ないし利用されるための仕組みの１つとして期待できるからに他ならない．しかし，そのトークン自体に何の利用価値も認められず，トークンの発行及び取得がシステムの参加者にとって何のインセンティブにもならなければそもそもトークンの活用による本システムの円滑な運用は叶わない．

そこで，ブロックチェーンのノードとしてトークンを発行・付与する弁護士会にとっても，また，付与されたトークンの利用者ないしシステムの参加者にとっても，本システムの円滑な運用のためのインセティブとなり得る独自の経済圏（トークンエコノミー）の構築が求められる[69]．

5.3.2　トークンの使用ケース

提案システムにおけるトークンは，そもそも立会人として押収手続に立会う一般市民に対して付与されることを想定して設計されているが，トークンエコノミーの構築を考える

場合，それに限らずにシステム参加者の立場や役割等に応じて広く利用場面について検討する必要がある．

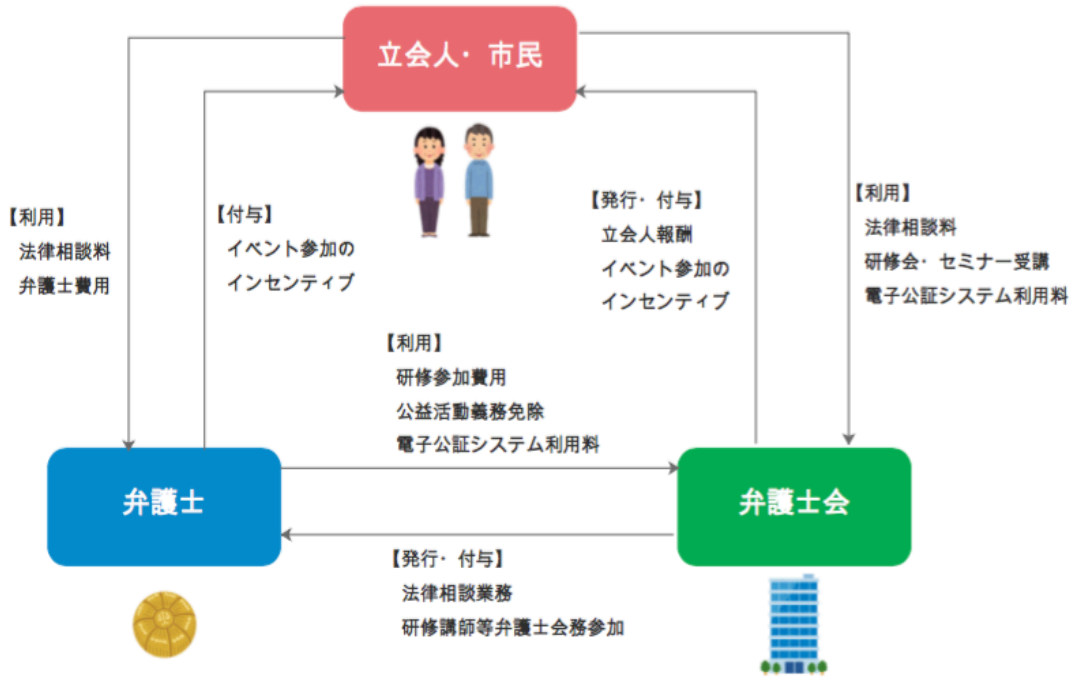


図 5.1　トークンエコノミーの概念図

5.3.2.1　一般市民による利用

⑴　法律相談

立会人を含め一般市民によるトークンの利用場面を考えた場合，本件トークンが弁護士会の発行によるものであることを前提とすれば，各弁護士会ないし弁護士会に所属する個々の弁護士が提供する各種リーガルサービスでの使用が考えられる．具体的には，まず，弁護士会や各弁護士が実施する法律相談業務に対する相談料としての使用が想定できる．もっとも，個々の弁護士にとって法律相談を受けることは通常の業務の一環である以上，一定の相談料の支払いを受けることが一般的である．従って，法律相談料をトークンで受領す

ることに対しては一定の抵抗も予想できる．しかし，近時，営業上の理由等から一定の場合無料相談を実施する場合も少なくないことや相談業務の機会が増えることは新たな業務への契機，依頼者の獲得に繋がる可能性もあることを考えれば，個々の弁護士にとっても十分にメリットが認められると考える．

⑵　研修会の受講

次に，弁護士会等が主催する各種法律研修会や法律セミナーの受講も考えられる．後述するシンポジウム等への参加とは異なり，一定の法律研修会などを受講することに対しては一定の価値があると認められ，通常であれば利用者にとってはコストの負担が求められることも少なくない．そのサービスに対してトークンの利用が可能であることは利用者にとっても価値があると考える．

⑶　弁護士費用

さらに，民事事件や私選の刑事事件に関して個々の弁護士に依頼する際の弁護士費用への一部充当（弁護士費用に対する実質的な値引き）も有り得る．なお，個々の弁護士にとって依頼者からの法律事務の委任は本業である以上，その全額の支払いをトークンで可能とすることに対しては，法律相談以上の抵抗が考えられることから，この場合，例えば，１割ないし２割引となるような一種のクーポンのようなものとしてトークンを捉える方法が考えられる．

⑷　電子公証システム

加えて，詳細については後述するが，民事事件等における電子公証システムとして利用する際の利用料としても考えられる．

5.3.2.2　弁護士による利用

⑴　研修参加

まず，弁護士会が実施する各種研修を受講するためのコストとしてのトークンの利用が考えられる．弁護士が受講する弁護士会実施の研修については，一般に，一部を除いて無料である場合が多く，受講コストとしてトークンの支払いを義務付けることは，現状においては合理的ではないとも考えられる．しかし，他方で，各単位会の運用にもよるが，弁護士においては一定数（一定単位）の研修の受講が義務付けられているケースも多く，後述するように，弁護士会によるトークンの付与も含めたトークンエコノミーの構築という視点から考えた場合，受講のためにトークンを必要とする仕組みについても十分に検討に値すると考える．

⑵　公益活動義務の免除

また，各弁護士会の運営にもよるが，弁護士は，その所属する弁護士会に対して，委員会への出席や市民法律相談の担当の割り当て等一定の公益活動への参加が義務付けられている場合が多い．しかし，その場合であっても，何らかの事情により参加が叶わない場合等に一定の出捐を以て免除となる制度が採用されている．そのような場合の出捐の手段としてトークンの利用も考えられる．

⑶　電子公証システムとしての利用

本システムは，証拠ハッシュ値の保全を想定したシステムであるが，その本質は，ある特定の日時にある電子（デジタル）文書が存在したことを証明するための電子（デジタル）文書の存在証明システムである．そこで，例えば，利用者ないしその代理人弁護士が，保存したいデジタル文書のハッシュ値を表示させ，それを専用アプリで読み取りブロックチェーンにアップロードすることによって本システムを電子文書の保存システムとして利用する方法が考えられる．

ところで，デジタル文書の客観的・公的存在証明の手段としては，公証制度に基礎を置く電子公証制度や民間業者による電子署名を用いたタイムスタンプサービスの制度が存在することは第４章でも指摘した通りである．しかし，電子公証システムにせよタイムスタンプ制度にせよ，特定の第三者機関に依存した制度であり，特定の認証機関ないし限定された指定公証人に負荷が集中するリスクを伴うことから，サービスを受けたい時に受けられないリスクは否定できない．また，電子署名による時刻証明は，公開鍵証明書の有効期限に当然縛られ情報を長期的・永続的に保存することに限界がある．さらに，情報の同一性を証明した電磁的記録やタイムスタンプが付された情報を公開する場所や手段もない．

なお，電子公証制度において利用者が日付情報の付与を受けた電磁的記録と情報の同一性に関する証明を請求するためには（また，タイムスタンプ制度においても，申請の際，利用者による電子署名を要求するなら），電子署名（電子証明書の取得）が必要とされている（但し，現行法上，日付情報の付与の請求自体に関しては，当該電磁的記録に電子署名を付与する必要はない．）が，現在，弁護士が「弁護人」ないし「代理人」として業務を行う上での電子証明書のシステムは存在していない．

このように，弁護士が電子公証制度やタイムスタンプを利用することに対しては多くの負担が存在するが，ブロックチェーンを利用した本システムを電子文書の存在証明として利用することを考えた場合，電子公証制度やタイムスタンプと比較してより安価な負担でシステムが利用できるように，システムの利用料（gas を含む．）として，トークンの支払いを設計すれば費用負担の面でも弁護士等の利用者にとっては大きなメリットとなり得る．また，利用者は，それぞれの居場所から本システムを利用することができ，その利便性も高い．トークンを有していない一般市民の立場から見た場合でも，トークンを有している弁護士に依頼することで本システムを利用することも可能である．ブロックチェーンの利用は、

暗号技術に対する信頼を基礎に置くものであるが，その信用性は，公証人に対する信頼に基礎を置く公証制度と比べても劣るものではい．

5.3.3　トークンの付与

次に，ブロックチェーンを運営する各ノードとしての役割を果たす各単位弁護士会によるトークンの付与について検討する．

5.3.3.1　一般市民に対する付与

⑴　証拠ハッシュ値の登録に対する立会人として

まず，本システムに本来想定された捜査機関による証拠ハッシュ値の登録手続きに対する立会人として，トークンが付与される．

⑵　シンポジウム・イベント参加

次に，弁護士会が主催する各種シンポジウムやイベント等への参加に対するインセンティブとしてトークンを付与することも考えられる．一般市民に対して弁護士会主催の各種イベント等への積極的な参加を働きかけることは，司法への市民参加を活動目的の１つとしている弁護士会としても当然のことであり，そのためのインセンティブとしてトークンを付与することは，弁護士会が市民に対して求める行為に対する活動として合理的と言える．

⑶　電子公証システムとして利用された際の立会人

最後に，本システムを電子文書の存在証明の電子公証システムとして利用する際に，利用者から依頼された立会人に対するトークンの付与が考えられる．本システムの利用においては，利用者が電子データのハッシュ値をブロックチェーンにアップロード（登録）することが必要であるが，そのアップロードに際しては，本システムの通常の利用と同様に立会人によるマルチシグを求めることにより，デジタルデータ（ハッシュ値）の登録時におけるセキュリティ及び適法性の担保とするが，この立会人に対して，立会いのインセンティブとしてトークンを付与する．トークンを付与された者は，別途本システムの利用を希望する際には，このトークンを利用することが可能となる．

なお，システムの利用に際して登録利用者の他に立会人を求めることに対しては，利用者にとっては一定の負担となり得る．しかし，例えば，企業の場合であればその従業員，弁護士の場合であれば法律事務所の事務員等が立会人になることも考えられ，トークンの付与

及び利用を含めてトークンエコノミー全体としてみれば，必ずしも大きな負担とはならないと考える．

5.3.3.2　弁護士に対する付与

⑴　法律相談

弁護士会等が実施する各種法律相談等に参加する弁護士に対してトークンが付与されるケースが考えられる．もっとも，現状においては，弁護士会等が実施する法律相談への参加に対しては，一定の報酬が支払われていることを鑑みれば，弁護士からの抵抗も予想される．しかし，後述する会務への参加と同様，市民サービスを実施する会務への参加という観点や新たな依頼者の発掘や拡大という観点を考えればメリットとなり得る．

⑵　弁護士会会務への参加

弁護士会が実施する研修会の講師として，あるいは委員会活動等の会務や各種公益活動への参加に対してもトークンが付与される．各弁護士は，受講が義務付けられた研修に参加するため，あるいは本システムを利用した電子公証システムを利用するためにも多くのトークンを得る必要に迫られることから，弁護士会が求める会務活動への積極的参加を促すことにつながる．

5.3.4　トークンに対するインセンティブとしての価値

本システムにおけるトークンを活用したトークンエコノミーの構築に関して，利用者の立場に応じたトークンの利用場面やトークンが付与される活動について検討してきた．トークンを活用することによって，弁護士会ないし個々の弁護士にとっても，また一般市民にとっても十分なインセンティブとなり得ることが分かる．

弁護士会や個々の弁護士にとっては，トークンの活用は，弁護士会が期待する弁護士会実施の様々なイベントへの一般市民の参加を促すことにつながっており，その結果として，弁護士会及び弁護士の市民へのアクセスの機会が増えることが期待できる．市民との接点の拡大は，個々の弁護士にとっても，引いてはその業務の機会を拡大することにも通じる可能性がある．

また，一般市民にとっても，トークンを媒介として，一般的に敷居が高いと言われている弁護士へのアクセスの機会を増やす効果が期待できる．また，より安価なコストでかつ利便性にも優れた本システムを利用した電子公証サービスを有効に活用できるという新たなリーガルサービス創設という観点も考えれば，弁護士・一般市民双方にとって，価値のあるト

ークンエコノミーの建設は十分に実行可能である.

従って，本システムを有効に運営していくための手段としてトークンを活用していくことに対しては十分な効果が期待できると考えられる.

5.3.5 課題

他方，トークンエコノミーを効果的に構築・運営していく上で，解決しなければならない課題も残っている.

トークンエコノミーの構築を設計する上で，トークンの総発行量はどの程度を見込むのか，流通量をコントロールする必要はあるのか，1トークンの価値を法定通貨に換算していくらに設定するのか，法定通貨との交換を認めるのか，認めるとしても投機の対象にしないために交換レートは固定するのか否か等決定しなければならないことは多岐に渡っている.特に，本トークンに関して，それが資金決済法において定義される暗号資産（仮想通貨）ないし前払式支払手段に該当するか否かという問題は，それによって発行主体となる弁護士会が，暗号資産（仮想通貨）交換業者ないし前払式支払手段発行者として，同法の規制を受けるか否かという問題にも直結して重要である.

例えば，提案システムに限らず，トークンエコノミーがトークンの利用者にとって価値ある経済圏であり続けるためには，法定通貨や他の暗号資産（仮想通貨）等との相互交換は欠かせない条件であると言われている[70]. しかし，提案システムにおいて発行される本トークンに関して，発行者による制限なく，前記のような相互交換を認めると，少なくとも，いわゆる２号暗号資産（仮想通貨）に該当する可能性が生じることになる（資金決済法２条５項２号参照）. 従って，この場合，弁護士会が「暗号資産（仮想通貨）交換業者」として資金決済法による規制が及ぼされないようにするためには，有償での本トークの販売は認められない.

なお，本トークンは，弁護士会ないし弁護士が提供する前述のようなリーガルサービスの利用に限定した使用法を想定しており，「不特定の者に対して使用することができ」る価値としては想定しないことから，いわゆる１号暗号資産（仮想通貨）に該当する可能性は低いと言える（法２条５項１号参照）.

また，仮に，本トークンが暗号資産（仮想通貨）に該当しないとしても，利用者から対価を得て発行される（有償での販売）ものである場合，前払式支払手段に該当する可能性がある. 従って，その場合であっても，資金決済法上の規制を受ける可能性を考慮しなければならない. これらの法規制を避けるためには，発行者である弁護士会での有償での販売は行わないとすることが必要となる.

５.４　本章のまとめ

本章では，第３章と前章での検討を踏まえて，第３章で検討した暗号化技術を利用した通信傍受法における傍受記録の保管のためのシステムが，改正通信傍受法で許容された範囲での傍受システムとして合理的であるとしても，そのシスムテをデジタル証拠全般のための保全システムとして応用（転用）することは妥当ではないことを示した．通信傍受法における裁判所によるデジタルデータ（通信データ）の保管の制度は，あくまでも通信傍受法という限定された枠内で許容された例外的な制度として捉えられるべきであって，捜査機関によって押収されたデジタル証拠一般にまで拡大させる必要はない．デジタル証拠に対する一般的なシステムとしては，当事者主義的訴訟構造にも即した独自のシステムを構築することが必要である．

本章での検討を通じて，第４章で検討したブロックチェーンを利用した証拠ハッシュ値の保全システムの存在意義及び必要性が改めて確認できた．

他方，デジタル証拠の改ざん防止システムとしてブロックチェーンを利用することに対しては，ブロックチェーンの円滑な運用が必要不可欠となる．提案システムでは，そのための仕組みとして立会人の電子署名（マルチシグ）に対してトークンを付与する仕組みを提案した．そこで，ブロックチェーンが効果的に運用されるためにはこのトークンが活用される必要があるが，本章では，そのためのトークンエコノミーの必要性について検討した．トークンエコノミーに関しては，トークンによる独自の経済圏をいかに設計するか，利用者にとって得られるトークンがどれだけ魅力あるものとなり得るかなど，その仕組み作りが重要な要素となるが，本章では，利用者に応じたトークンの利用ケースやトークンが付与されるための仕組みについて弁護士会によるトークンエコノミーのモデルケースを提示した．これによって，第４章で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モチベーションとして，利用者にとっての利用価値（魅力）を示すことができた．

今後は，提案した証拠ハッシュ値保管システムのより具体的な実装実験を通じて，運用のための費用面や時間的なコストの観点も考慮して，より実用的なシステムが構築できるよう一層検討を重ねていく必要がある．

第６章　結論

６.１　本論文のまとめ

本論文では，社会のIT化・情報のデジタル化に伴って生じた社会的な課題の１つとして，刑事手続，とりわけ捜査機関におけるデジタル証拠に対する適正な取扱いという課題に着目した．デジタル証拠は，客観的な科学的証拠として信頼されている一方で，その性質上改ざんが極めて容易であることから，捜査機関による不正（改ざん）がひとたび行われればそれによって引き起こされる誤判ないし人権侵害の危険は計り知れない．そのため，捜査機関によってこのような不正が行われるリスクに対して，これを技術的に防止するための解決策が求められている．デジタル証拠は，目に見えないデジタルデータから構成され，物理的証拠に比べてそもそも改ざんのリスクが大きく，さらに，改ざんされた場合に伴って生じる誤判など影響力の大きさを重視し，最終的に，捜査機関がデジタル証拠を収集・保全する際に改ざんなどの違法・不正を行うことを防止するための技術的な解決策を構築することを目指した．

第２章では，刑事手続におけるデジタル証拠の収集・保全の手続について検討する前提として，刑訴法によって規定されている通常の証拠及びデジタル証拠（電磁的証拠）に関する規定について確認した上で，デジタル証拠の真正性・完全性等が実際の刑事裁判においてどのように扱われてきたのかについて若干の事例を通じて確認した．本章の検討を通じて，デジタル証拠ないしデジタルデータは一般に改ざんが容易でありながら，裁判実務においては，捜査機関による改ざんなどのリスクが必ずしも現実的なリスクとして捉えられていないという課題を浮き彫りにすることができた．そして，それに伴い，捜査機関によってデジタル証拠が改ざんされることを技術的に防止するためのシステムの構築がいかに重要であるかということを改めて示すことができた．

第３章では，現行法上の中で，ある意味，デジタルデータの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も評価できる改正通信傍受法について着目した．そして，その上で，改正通信傍受法における暗号技術を利用した証拠（傍受記録）の保管システムの応用（転用）の是非を検討する前提として，改正通信傍受法によって採用された暗号技術に基づいた適法性担保のシステムが，そもそも立会人に代わり得る違法捜査抑止の担保となり得るのかという問題について検証した．即ち，改正通信傍受法の規定する要件を遵守することによって違法な通信傍受を抑止することが不可能ないし困難であるとすれば，そもそも改

正通信傍受法の枠組みを応用する前提に欠ける．本章では，このような問題意識に基づき，まず，改正通信傍受法で新設された３つの傍受方法について要件等を確認し，加えて，改正通信傍受法における暗号化システムにおいても，通信データの暗号化において一般的に利用されているハイブリッド方式の採用が解釈上許容されることを示すことができた．そして，その上で，法の要件を充足し，捜査機関による不正・違法な通信傍受が行われないための傍受システムとして，耐タンパ性に優れた IC カードを利用した通信傍受システムを提案した．これによってデータの暗号化と復号を捜査機関の手の及ばない IC カード内で行うことが可能となるセキュアなシステムが実現できた．そして，捜査機関が改正法で許容された以外の違法・不正な傍受行為に及ぶ危険を防止することが技術的に十分可能であることを示すことができた．この提案システムによって，捜査機関による不正・違法な通信傍受を防止することが可能となり，違法な通信傍受による人権侵害のリスクが低減されることが期待できる．

第４章では，デジタル証拠の改ざんの容易性という問題に焦点を当て，第３章で検討したシステムの転用とは別に，捜査機関がデジタたる証拠を押収する際の改ざん防止のための新たな独自シスムテとしてブロックチェーンを利用した証拠ハッシュ値の保全システムについて検討した．まず，デジタル証拠が改ざんされやすい性質を有することを実証実験などを通じて確認した．そして，デジタル証拠の改ざんを防止するための有効な手段の１つとしてハッシュ値の活用があることを確認した上で，ハッシュ値の保管先としてブロックチェーンが有効であることを既存の技術との比較を通じて示した．そして，捜査機関が押収したデジタル証拠に対して，弁護人からも容易に不正の痕跡を確認する手段として，ブロックチェーンの１つであるイーサリアムネットワークを利用した証拠ハッシュ値保全システムを提案した．提案システムでは，捜査機関に押収されたデジタル証拠は，押収と同時にハッシュ値が算出され，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が求められている．弁護人は，このシステムを使うことによって，検察官から開示を受け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ができ，仮に，捜査機関が押収したデジタル証拠を押収後に改ざんした事実があるとすれば、両者のハッシュ値の間に齟齬が生じていることから，容易に改ざんの有無を確認することが可能となる．これにより，捜査機関がデジタル証拠に対して改ざんなどの違法行為に及ぶリスクは減少し，捜査機関が押収したデジタル証拠を改ざんしているのではないかという疑念を払拭することにもつながる．

そして，第５章では，前章までの総括として，まず，第３章で提案した IC カードを利用した傍受システムと第４章で提案したブロックチェーンを利用した証拠ハッシュ値保全システムとの関係について、そして次に、ブロックチェーンを利用した証拠保全システムが円滑に運用できるためのトークンエコノミーについて検討した．

第３章で提案したICカードを利用した傍受システムが，たとえ法の趣旨に即した捜査機関の不正を防止するための通信傍受システムとして十分に機能することが前提となるとしても，裁判所が傍受記録を管理・保管するという制度を捜査機関が押収したデジタル証拠一般に応用することは困難であるという結論を提示した．そもそも通信傍受という捜査手法は，科学的・客観的な捜査手法として導入されたものであるが，それは，個人のプライバシー権に直接関わり，人権侵害のリスクの極めて高い捜査手法として，憲法解釈上も今なお批判が少なくない．そのため，捜査機関の不正（違法な盗聴）に対しては，（違憲等の批判を回避するに足りる措置であるか否かはともかく）それを防止するための一定の立法措置として，立会人による立会制度，あるいは新たに暗号技術による不正防止の措置が講じられた．このように，改正通信傍受法は，本質的な性質としては，情報技術（IT）を採用した新しい捜査手法に対して，捜査機関による不正（違法な盗聴，プライバシー権の侵害）の発生を抑止するための枠組みが基本であって，裁判所における傍受記録の管理という側面は，あくまでも副次的・補完的な役割にすぎないというべきある．なぜなら，現行の憲法ないし刑訴法においては，そもそも裁判所は中立な判断権者であるべきあって，訴訟を含めた手続きの追行については当事者が責任を有するべきであるという当事者主義的訴訟構造を採用していることを前提と考えれば，裁判所の関与を認める制度はそれ自体が例外的な措置であるというべきだからである．通信傍受という捜査手法は，前述の通り，プライバシー権を侵害し，人権侵害に及ぶ危険が極めて大きいことから，敢えて当事者主義の例外として，裁判所による関与を認めたに過ぎない．そうすると，今なお違憲の見解も少なくないという現状に鑑みても，他に，捜査機関がデジタル証拠を収集・保全する際に改ざんなどの違法・不正を行うことを防止することができる技術的措置について追求・検討するべきであるということが分かる．そのような手段が存在しないならともかく，そうではない以上，例外的な制度を拡張することは控えるべきである．

以上の考察を踏まえ，改正通信傍受法における暗号技術を利用した裁判所によるデジタル証拠の保全システムは，通信傍受という個人のプライバシーに対する侵害の程度が大きい捜査手法に対して法が例外的に裁判所による関与を認めた制度であって，デジタル証拠一般の保全システムとして転用（応用）することは妥当ではないということが理解できる。ここに，第４章で提案したブロックチェーンを利用した証拠ハッシュ値の保管システムをデジタル証拠の保全システムとして提案する意義が認められる．

そして，第４章での提案システムでは，協力者としての立会人の電子署名に対してインセンティブとして一定数量のトークンが付与される仕組みを採用していることを踏まえ，提案システムが効果的に運用されるために，そのトークンを活用して構築されるトークンエコノミーの重要性について確認した．トークンの使用ケースとして一般市民による利用と弁護士による利用などトークンの利用者の立場に応じてトークンの利用場面を想定した．また，トークンが付与される活動についても，利用者の利用場面に応じて具体的・総合的に想定することによって，インセンティブとしての一定の価値について示すことができた．本

章での検討を通じて，ブロックチェーンを利用した証拠ハッシュ値保全システムを円滑に運用するための仕組みとして，利用者にとって価値のあるトークンエコノミーを構築することが実用化のためには何よりも不可欠であるという結論が導かれた．そして，そのようなトークンエコノミーの構築のためには，利用ケースや利用者ごとに如何にすればモチベーション（魅力）を感じることができるのかという視点がなければならいないが，本章での検討を通じて，その 1 つのモデルを示することができたと考える．

社会のあらゆる情報がデジタル化された IT 社会の中で，刑事手続の分野においても捜査の IT 化，あるいはデジタル証拠の占める割合がこれからますます大きくなることはむしろ当然とも言える．しかし，捜査の IT 化やデジタル証拠の重要性が増すにつれ，デジタル証拠の特性等に応じたリスクや問題に対しても適切に備えておかなければ，誤判や人権侵害など深刻な弊害を招きかねない．そこで，刑事手続分野における IT 化に対するリスクやデジタル証拠の特性としての改ざんの容易性に起因するリスクに対して，それを防止するための技術的な解決策の提示が求められている．本論文では，このような技術的な解決策が求められている課題として，捜査機関がデジタル証拠を収集・保全する際に改ざんなどの違法・不正を行うことに対する社会的なリスクを取り上げ，その解決策を探った．そして，まず，通信傍受という特定の捜査手法の分野に焦点を当て，IC カードを利用した通信傍受システムを提案することによって，捜査機関による違法な傍受捜査が行われるリスクを技術的に防止するための手段を提示することができた．そして，その上で，捜査機関が押収したデジタル証拠一般に関して，ブロックチェーンを利用した証拠ハッシュ値保全システム及びトークンエコノミーの構築について提案することによって，捜査機関がデジタル証拠を押収した後にそのデジタル証拠を改ざんするリスクを防止するための技術的な解決策を提示することができた．

本論文で提案したこれらのシステムが実用化され，刑事手続が適切に運用されることの一助となれば幸いである．

６.２　今後の研究課題

本論文では，改正通信傍受法で採用された暗号技術を利用した通信傍受システムについて，技術的な観点から，捜査機関による違法な傍受を防止するためにはどのようなシステムを構築するべきかという課題に対して IC カードを利用した傍受システムについて提案を行った．また，改ざんが容易であるデジタル証拠に関して，捜査機関がその収集過程で改ざんなどの違法行為を行うことを技術的に防止するためシステムとして，ブロックチェーンを利用した証拠ハッシュ値の保全システムの提案を行い，あわせてブロックチェーンシステムが円滑に運用されるためのトークンエコノミーの構築の必要性について研究を進め，そ

れぞれ，立法や法律解釈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に解決する指針を示すことができた．

他方，第 1 章において指摘した通り，刑事手続とは，要するに，刑事事件において，適正手続を全うしつつ事案を解明すための手続きであり，証拠裁判主義の観点から，証拠を中心として，捜査機関による捜査（証拠の収集・保全手続）と裁判所における事実認定・法令適用の場面に分けることができる．従って，刑事手続の IT 化について論じる場合においても，捜査手続きの場面と裁判（公判）手続の場面が存在し，それぞれに関して解決しなければならない課題がある．本論文では，その中でも，捜査機関による個人のプライバシー権の侵害や証拠の改ざんのリスクの大きさや問題の重要性に鑑みて，刑事手続の場面の中でも捜査機関における IT 化の影響，課題について取上げた．そして，捜査機関における IT 化の課題に焦点を当てた場合でも，証拠を軸に大きく次の２つの場面に重点を置いて課題を捉えることができる．1 つは，証拠の収集・保全手続である捜査手法自体の IT 化（IT（デジタル）技術を利用した捜査手法）に伴う課題であり，もう 1 つは，被疑者・被告人のもとに存在するデジタル情報化された証拠（デジタル証拠）そのものに対して行われる収集・保全（捜索・押収）に伴う課題である．IC カードを利用した通信傍受システムの提案は，裁判所による通信データの保管システム関する一般的なデジタル証拠の保管システムへの応用（転用）の可否という問題，及びその課題の解決への前提として，暗号技術を利用した通信傍受という IT 化・デジタル化された新しい捜査手法において生じた課題に対する解決である．また，ブロックチェーンを利用した証拠ハッシュ値に保管システムの提案及びトークンエコノミーの構築は，捜査機関が押収したデジタル証拠が押収後捜査機関によって改ざんされることを防ぐための解決策である．

以上のことからも分かる通り，刑事手続ないし捜査の IT 化に伴って技術的に解決しなければならない問題は多方面に渡って存在しており，本論文で解決を得た課題はその一部に過ぎない．例えば，GPS 等を利用した位置情報の捜査ないしそれを利用した追跡捜査，AI 技術等を活用した防犯ビデオによる監視ないし映像解析，デジタル写真・ビデオを利用した現場状況の記録，取調べの録音・録画など捜査手法自体の IT 化に伴って生じる個人のプライバシー権の侵害等に対する人権侵害・違法捜査に対して技術的に防止・担保するためのシステム等の構築が課題としてあげられる．また，それらの捜査手法によって捜査機関が獲得した各種のデジタル証拠に対しても，捜索・押収によって獲得したデジタル証拠と同様，改ざんを防止するためのシステムを構築することが求められる．

本論文で指摘しつつも検討することができなかったこれらの残された課題については，引き続き研究を進めていかなければならない．

また，ブロックチェーンを利用したデジタル証拠の改ざん防止システムについても，より実運用に近い環境を実現し，トークンの付与を伴うエコシステムの構築に向けての実証実験を行うことや，さらに，令和元年（２０１９年）６月に施行され捜査の現場で実用化されるに至った通信傍受システムについても，その運用上の課題など本格的に検証していくこ

とも必要であるが，いずれも今後の研究課題としたい．

謝辞

本研究を進めるにあたり，指導教員として，長期にわたり丁寧かつ熱心なご指導及びご助言を賜りました立命館大学情報理工学部の上原哲太郎教授に心より深く感謝致します．上原教授には，弁護士である私が立命館大学大学院情報理工学研究科博士課程後期課程へ進学する機会を与えて頂きました．そして，在学中も，毎週お忙しい中貴重なお時間を割いて頂き，情報セキュリティ及びデジタルフォレンジックの分野で研究活動に従事するための数え切れないほど多くのご助言を下さりました．本当にありがとうございました．また，本論文の副査としてご助言及びご指導を賜りました立命館大学情報理工学部の國枝義敏教授，野口拓教授に心より深く感謝致します．

本論文をまとめるにあたり，貴重なご助言を賜りました大阪大学情報科学研究科の猪俣敦夫教授（立命館大学客員教授）に心より深く感謝致します．

さらに，本論文の執筆に至るまで，多くのご支援とご協力を頂いた上原研究室の皆様に心より深く感謝致します．

最後に，研究の遂行や論文の執筆を見守り，長きにわたる学生生活を仕事の面や家事の面でも支えてくれた妻麻子に心より深く感謝致します．

参考文献等一覧

[1] 総務省：令和元年版情報通信白書（2019)128 頁

[2] 平成３１年３月２５日内閣総理大臣決定：行政文書の電子的管理についての基本的な方針 1 頁（2019）

[3] 最高裁大法廷判決平成２９年３月１５日：判例タイムス第 1437 号 78 頁

[4] 松本裕，倉持俊宏、山口貴亮：捜索・差押えハンドブック（３刷）（立花書房，2017）43 頁以下

[5] 大阪地裁判決平成２２年９月１０日：判例タイムス第 1397 号 309 頁

[6] 大阪地方裁判所判決平成２４年 1 月 23 日：判例タイムス第 1404 号 373 頁

[7] 大阪地方裁判所判決平成２３年４月 12 日：判例タイムス第 1398 号 347 頁

[8] 大阪高等裁判所判決平成２５年９月２５日：判例タイムス第 1408 号 293 頁

[9] 鈴木一朗：デジタルデータ（フロッピーディスク）分析　厚労省事件，季刊刑事弁護 71 号，pp.60-62（2012）60 頁

[10] 高橋郁夫他：デジタル証拠の法律実務 Q&A（日本加除出版，2015）284 頁

[11] 東京地方裁判所判決平成２７年２月４日（判例集未搭載）

[12] 前掲・高橋他・298 頁

[13] 大阪地方裁判所判決平成２２年５月２５日：判例タイムス第 1346 号 247 頁

[14] 金沢地方裁判所判決平成２４年３月２日：LEX/DB 25480441

[15] 奈良地方裁判所判決平成２５年３月５日：LLI/DB 判例秘書 L06850138

[16] 東京地方裁判所判決平成１７年３月２５日：判例タイムス第 1213 号 314 頁

[17] さいたま地方裁判所判決平成２１年７月２８日：LLI/DB 判例秘書 L06450468

[18] 高松高等裁判所判決平成２４年４月２６日（判例集未搭載）

[19] 水戸地方裁判所土浦支部判決平成２３年５月２０日：LLI/DB 判例秘書 L06650285

[20] 吉峯耕平他：デジタル・フォレンジックの原理・実際と証拠評価のあり方，季刊刑事弁護 77 号，pp.109-129（2014）122 頁

[21] 前掲・高橋他・272 頁

[22] 前掲・吉峯他・122 頁

[23] 大阪高等裁判所判決平成２１年５月１５日：判例タイムス第 1313 号 271 頁

[24] 第 189 回国会法務委員会第 33 号山下幸夫参考人意見（平成 27 年 7 月 29 日）http://www.shugiin.go.jp/internet/itdb_kaigirokua.nsf/html/kaigirokua/00041892

0150729033.htm
[25] 川出敏裕：通信傍受法の改正について，東京大学大学院ローレビュー10 巻 11 号，pp.103-110（2015）106 頁
[26] 前掲・山下参考人意見
[27] 前掲・川出・109 頁
[28] 法制審議会新時代の刑事司法制度特別部会第 23 回会議配布資料：「通信傍受の合理化・効率化，会話傍受」資料 6
[29] 前掲・川出・108 頁
[30] 前掲・特別部会第２３回会議配布資料・資料５
[31] 同・資料３
[32] 同・資料８
[33] 同・資料７
[34] 同上
[35] 同・資料８
[36] 安村勉：通信傍受法改正と捜査，法律時報 88 巻 1 号，pp.26-32（2016）31 頁
[37] 前掲・川出・110 頁
[38] 前掲・安村・31 頁
[39] 前掲・川出・109 頁
[40] 前掲・山下参考人意見
[41] 前掲・川出・109 頁
[42] デロイト トーマツ コンサルティング株式会社：通信傍受法改正検討に伴う技術的措置に関する調査研究に係る報告書（平成２７年３月２５日）公刊物未搭載
[43] 警察庁情報通信局 警通仕施第６２号：通信傍受法用構成機器仕様書（平成３１年１月３０日制定）
[44] 前掲・デロイト トーマツ コンサルティング・20 頁ないし 23 頁
[45] 同・25 頁
[46] 菅沼知久：第3回 IC カードとセキュリティ，ビジネスコミュニケーション 39 巻 10 号，pp.101-104（2002）101 頁
[47] 長谷川春彦：IC カードをめぐる３つのセキュリティ要素，（2005）https://www.atmarkit.co.jp/ait/articles/0509/13/news117.html
[48] 前掲・菅沼・102 頁
[49] 東京高判昭和４０年１０月２９日判時 430 号 33 頁
[50] 最判昭和４２年６月８日判時 487 号 38 頁
[51] 最決平成１０年５月１日刑集 52 巻 4 号 275 頁
[52] 足立昌總：タイムスタンプを活用した電子データの存在・非改ざん証明–営業秘密侵害に係る民事訴訟を例に，NBL1098 号，pp.15-22（2017）

[53] 宮崎一哉，木村道弘，前田陽二，辻秀一：証拠性確保を重視した電子記録マネジメントのためのパッケージ構造, 情報処理学会, 情報システムと社会環境研究会研究報告,（2012-IS-119-01）
[54] 前掲・吉峯他・122 頁
[55] 法務省：公証制度に基礎を置く電子公証制度について，http://www.moj.go.jp/MINJI/DENSHIKOSHO/index.html
[56] 宮内宏他：電子契約の教科書 基礎から導入事例まで（日本法令，2017）39 頁以下
[57] 手塚悟, 向賢一：マイナンバーで広がる電子署名・認証サービス,（日経 BP 社, 2015）34 頁以下
[58] 岸上順一，藤村滋，渡邊大喜，大橋盛徳，中平篤：ブロックチェーン技術入門,（森北出版，2017）104 頁
[59] セコム株式会社 IS 研究所，NEC 編：ブロックチェーン技術の教科書,（C&R 研究所, 2018）39 頁
[60] 加嵜長門, 篠原航:ブロックチェーンアプリケーション開発の教科書, (マイナビ出版, 2018)
[61] 田篭照博：堅牢なスマートコントラクト開発のためのブロックチェーン[技術]入門,（技術評論社，2017）
[62] Andreas M.Antonopolulos,Gavin Wood：マスタリング・イーサリアム,（オライリー・ジャパン，2019）
[63] 赤羽喜治，愛敬真生：ブロックチェーン 仕組みと理論（増補改訂版),（リックテレコム，2019）
[64] 久保幹雄，原口和也：実践 Python ライブラリー Kivy プログラミング　Python でつくるマルチタッチアプリ,（朝倉書店，2018）
[65] Ritesh Modi：Solidity プログラミング　ブロックチェーン・スマートコントラクト開発入門,（講談社，2019）
[66] 加嵜長門，篠原航，金志京，河西紀明，田中克典，佐々木亮彰，平野浩司，前川彰，DMM.com ブロックチェーン研究室：試して学ぶ スマートコントラクト開発,（マイナビ出版，2019）
[67] 中村誠吾，中越恭平：ブロックチェーン システム設計,（リックテレコム，2018）
[68] 渡辺篤，松本裕太，西村祥一，清水俊也：はじめてのブロックチェーンアプリケーション　Ethereum によるスマートコントラクト開発入門,（翔泳社，2017）
[69] 高榮郁：トークンエコノミービジネスの教科書,（KADOKAWA，2019）17 頁他
[70] 同・70 頁他

著者発表論文

本研究に関する主要論文

[1] 小坂谷聡，上原哲太郎：ブロックチェーンを利用したデジタル証拠の改ざん防止システムとトークンエコノミーの構築, 情報処理学会論文誌, Vol.61, No.9, pp.1444-1457（2020）.

[2] 小坂谷聡，上原哲太郎：改正通信傍受法における通信傍受の暗号技術に関する研究，情報ネットワーク・ローレビュー，第 15 巻，pp.119-137（2017）.

本研究に関する口頭発表等

[1] 小坂谷聡，上原哲太郎：刑事手続におけるデジタル証拠の改ざん防止措置について，情報処理学会マルチメディア，分散，協調とモバイルシンポジウム 2017 論文集（DICOMO2017），pp.680-688（2017）.

[2] 小坂谷聡，上原哲太郎：改正通信傍受法が定める傍受装置の暗号利用の不整合および改善されたシステムの提案，情報処理学会第 40 回インターネットと運用技術研究会研究報告，pp.1-4（2018）.

[3] 小坂谷聡，上原哲太郎：ブロックチェーンを利用した刑事手続におけるデジタル証拠の改ざん防止システムについての考察, 情報処理学会第 82 回電子化知的財産・社会基盤研究会（EIP）研究報告，pp.1-8（2018）.

[4] Satoshi Kosakatani, Tetsutaro Uehara, Songpon Teerakanok : Japan’s Act on Wiretapping for Criminal Investigation: How the system is implemented and how it should be, The International Conference for Internet Technology and Secured Transactions(ICITST-2020)(2020)

その他

[1] 小坂谷聡，上原哲太郎，西口三千：無線 LAN アクセスポイントへの無断接続に関する考察，情報法制研究，第 7 号，pp.11-23（2020）