情報処理学会論文誌 Vol.61 No.9 1444–1457 (Sep. 2020)

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

小坂谷 聡[1,a)] 上原 哲太郎[2,b)]

受付日 2019年12月9日, 採録日 2020年6月1日

概要：刑事手続きにおいてデジタル証拠が扱われる際に，しばしば提出されたデジタル証拠が警察や検察の手によって改ざんされたものではないのか問題となることから，我々は，ブロックチェーンを用いた証拠の改ざん防止システムについて提案する．提案システムでは，利用者・参加者に対してトークンを付与することにより一定のインセンティブとして有効かつ効果的に活用されることを想定しているが，そのためには，トークンを活用して価値ある一定の経済圏，すなわち，トークンエコノミーが構築されることが必要であると考えらえる．本論文では，提案システムに対するリスクについても検討し，実装によりその有効性を検証したうえで，提案システムによって構築すべきトークンエコノミーについて考察する．

キーワード：ブロックチェーン，刑事手続き，デジタル証拠，改ざん防止，トークンエコノミー

Token Economy on Anti-tampering System Using Blockchain Technology for e-evidence

Satoshi Kosakatani[1,a)] Tetsutaro Uehara[2,b)]

Received: December 9, 2019, Accepted: June 1, 2020

Abstract: When dealing with e-evidence in criminal proceedings, it is often questioned whether the submitted e-evidence has been tampered with by police or public prosecutors. We propose an anti-tampering system using blockchain technology for e-evidence. The proposed system assumes that granting tokens is necessary for users as they can be used effectively as an incentive to establish an economic sphere of value, i.e., a token economy. In this paper, we discuss the risks to the proposed system, verify its effectiveness by implementation, and validate the token economy to be built by the proposed system.

Keywords: blockchain, criminal procedure, e-evidence, anti-tampering system, token economy

1. はじめに

個人や企業等の活動の痕跡として機械的に記録されるデジタルデータを解析することによって得られるデジタル証拠は，客観的・科学的証拠の１つとしてそれ自体高い信頼性が認められており，裁判実務においても重要な証拠として扱われる機会も必然的に多くなっている．

しかし，デジタル証拠は一般に改ざんが容易であるという特性が認められる．その一方，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，いったん改ざん等がされた場合には，かえって誤判の危険性は増大し，その場合の弊害はきわめて深刻になる．特に，人権問題に直結する刑事裁判において捜査機関が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．

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

[1] 立命館大学大学院情報理工学研究科，弁護士
Graduate School of Information Science & Engineering, Ritsumeikan University, Kusatsu, Shiga 525–0058, Japan, Attorney at Law
[2] 立命館大学情報理工学部
College of Information Science & Engineering, Ritsumeikan University, Kusatsu, Shiga 525–0058, Japan
a) kosakatani@cysec.cs.ritsmei.ac.jp
b) t-uehara@fc.ritsumei.ac.jp

保され，かつ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．我々はすでに，押収したデジタル証拠のハッシュ値を特定の第三者機関が管理する中央管理型登録用サーバにアップロードするシステムの構築を提案し [1]，このシステムをより信頼性の高い永続的なシステムとするために，新たにブロックチェーン技術について着目し，Ethereum（イーサリアム）ネットワークを利用したハッシュ値保全システムについて考察してきた [2]．

本論文では，このシステムについてさらに議論を進め，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の保管方法について，既存のシステムを採用することの問題点を指摘したうえで，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を提案する．そして，実際のシステムのプロトタイプを作成し，Ethereum の testnet を利用した実験を通じてその有効性について評価する．透明性が強く求められるデジタル証拠について，ブロックチェーンを利用することによってその同一性が確保されていることを，随時どのステークホルダからも確認できる手法を示す．提案システムはブロックチェーンを利用したシステムであるため，特定のステークホルダによってデータが改ざんされる可能性をきわめて低くすることができ，証拠の真正性・完全性が容易に推認できるようになる．

提案システムでは，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する．その際，立会人の協力を得るためのインセンティブとしてトークンを付与する仕組みを提案する．提案システムが効果的に運用されるためには，そのトークンを活用して構築される独自の経済圏，すなわち，トークンエコノミーをいかに構築していくかという視点が必要不可欠となる．そこで，ブロックチェーンの最大の課題であるシステム運用のインセンティブを保つ方法として，提案システムによって生成されるトークンに弁護士会および相談者の間で利用可能な価値を付与することにより，効果的なトークンエコノミーを確立する手法を示す．

2. 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や [3]，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 [4]．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 [5]．そこで，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．

2.1 既存技術の活用の可否

(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 [6]．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る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見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いって，それらが，改ざんのリスクと無関係であるわけではないので，現行制度の枠組みに必ずしも限定されず広く電子公証制度をとらえ直すこともできるが，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．

(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，利用者が持つデジタルデータが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 [7]．この制度は，電子署名法に基づいた特定認証業務を行う事業者として認定された認証業者等，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 [8]．

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．

(3) 立会人による電子署名

捜査機関が強制処分として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，捜索すべき場所において居住主等を立会人として立ち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うえでデータベースへ登録する等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) 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，すなわち公証人，タイムスタンプ局およ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．デジタル証拠の改ざん防止の観点からは，信頼性および真正性の双方の要件が担保されていなければならないが，いずれの制度も一部要件が欠けている．

また，たとえば，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．したがって，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・公開するわけではない．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，たとえば官職証明書を利用する等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にくい制度となる．司法書士等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すでに構築されている．しかし，弁護士が「弁護人」ないし「代理人」として業務を

行ううえ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等しか方法がない．

以上の点から，公開鍵暗号に基盤を置いたこれら既存の制度を利用する方法では，デジタルデータのハッシュ値を保存するシステムとしての役割は十分には果たしえないと考えられる．

2.2 ブロックチェーンを利用する意義

そこで，信用性かつ信頼性が担保され，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であり，また特定の機関に過度に負荷が集中せず可用性が保証されるシステムとして，本論文では，改ざん耐性にも優れている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，データベースすべ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）が複数まとめられその全体のハッシュ値と 1 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，いったん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，データの改ざんはきわめて困難となる．また，従来の技術は，特定の事業者や機関等，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もってデータの真正性を担保している．したがって，その特定の機関が十分に信頼に足りる場合には，あ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，たとえば，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関与が強くうかがわれる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うえでも，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 [9]．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．

2.3 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

ハッシュ値保全システムとして，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が，具体的にどのようなシステムが適しているか検討する [10], [11]．

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方が適していると考えることもできる [12]．

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いえる．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，我々は，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うえ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．

3. 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概要

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，我々は，実装の容易性を考慮してイーサリアムネットワークを利用する．

3.1 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・保管するためのハッシュ値保全システムの大まかな概要は以下の図 1 のとおりである．

① 主なシステム利用者

i 捜査機関：証拠ハッシュ値を登録する．

ii 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．

iii 弁護人：証拠ハッシュ値を閲覧．

② 捜査機関の活動

i デジタル証拠を押収する．

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

iii 証拠ハッシュ値および暗号化された付加情報はツール（PC）上で QR コードに変換され画面に表示される．

iv QR コードをスマートフォンで読み取る．

v ②iv で読み取った情報をブロックチェーン上に登録する．

③ 立会人の役割

i ②iii で表示された QR コードをスマートフォンで読み取る．

ii ②v 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 弁護人の役割

i 起訴後，捜査機関からデジタル証拠の開示を受ける．

ii ブロックチェーン上の証拠ハッシュ値を閲覧する．

iii 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，③ii の署名時から改ざんされているか否か確認する．

3.2 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および手順は以下の図 2 のとおりである．

(1) システム利用者

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

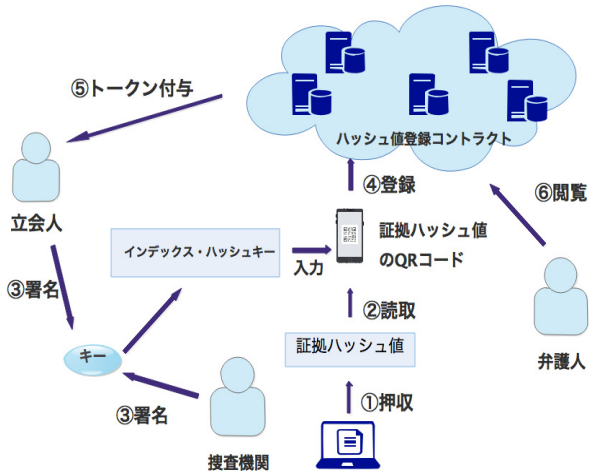

図 1 証拠ハッシュ値保全システムの概要

Fig. 1 Overview of hash value storage system.

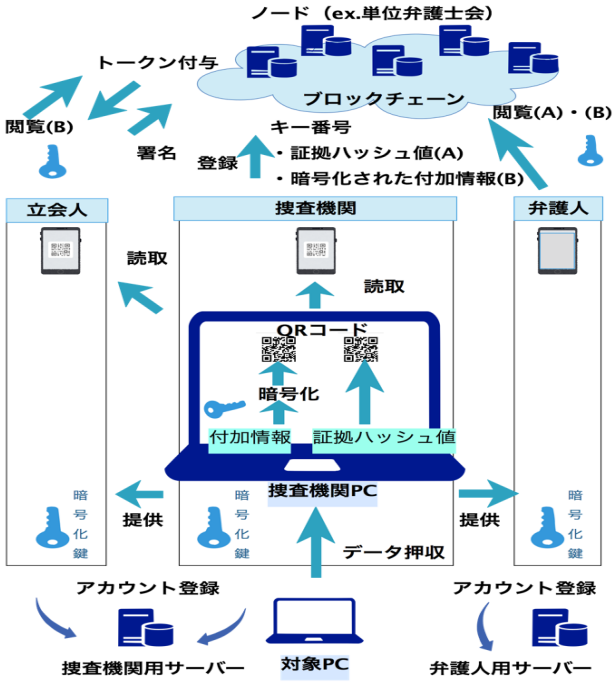

図 2 証拠ハッシュ値保全システムの具体的内容・手順

Fig. 2 Contents and procedure of the proposed system.

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，立会人が署名したとき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．

(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，および現行刑事訴訟制度が採用する当事者主義的訴訟構造に鑑みれば，たとえば，全国の各地方検察庁（または警視庁および各道府県警察本部）ごとに設置する案，あるいは各単位弁護士会ごとに設置する案もしくはそれらを組み合わせた案等が考えられる．いずれにしても，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中立な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最も適しているとも考えられる．しかし，そもそも提案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ことが望ましい．最低でも，各単位弁護士会によるノード設置とする．

(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，Web サイト上で稼働する Web アプリを利用した方が利用者の利便性を考えた場合便利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や責任の問題を回避するために，ここではアプリ形式を採用する．

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．ただし，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，弁護人および立会人）に対しては，公開鍵（利用者アカウント）を捜査機関およ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，所属もあわせて登録させる（後日の報告でも可）．ただし，立会人（捜査機関以外）に対しては，プライバシ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．そして，捜査機関およ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，弁護人については，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ち会っていない，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等していない，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）およ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．したがって，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いっても，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いのかという問題は残る．しかし，後述のとおり，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) 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とる場合，ハッシュ値をと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，あらかじ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，および目録情報（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．

(5) 具体的な登録手順

証拠ハッシュ値およ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み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）を付する．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．また，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1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等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（番号キー）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，前述したとおり，弁護人における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すべ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．

(6) 証拠ハッシュ値の記録・開示

最後に，捜査機関は，証拠ハッシュ値等およびキー番号を，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. 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．

したがって，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，すなわち，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や過誤が介入し正しくないハッシュ値がアップされる場合等のケースでは，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，弁護人は，改ざんを検知することができない．したがって，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，本章では，提案システムの信頼性の評価について，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うるが，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．

4.1 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 3** のとお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

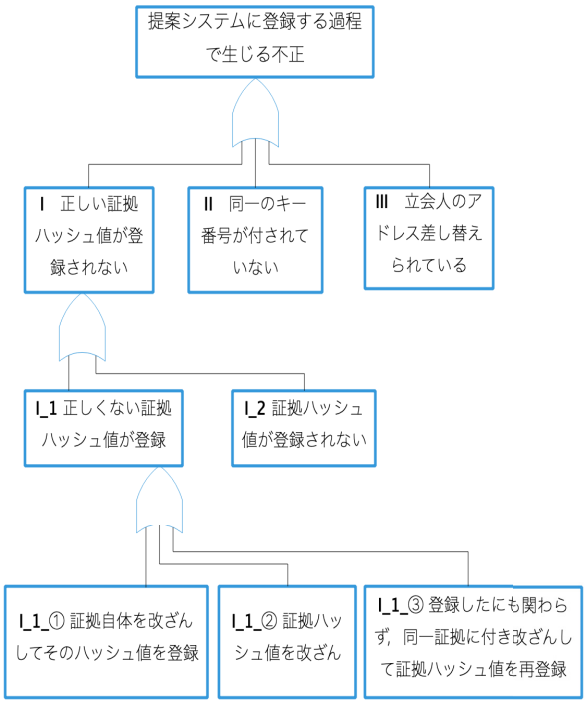

図 3 提案システムに登録する過程で発生する不正
Fig. 3 Fraud that occurs during registration in the proposed system.

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いったん適切に登録されたにもかかわらず，同一証拠につき改ざん等したうえ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，証拠ハッシュ値および付加情報の生成，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み取り，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を考えると，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．したがって，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．

4.2 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 3 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．

(1) 同一のキー番号を付さないリスク（II）

前述のとおり，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る，あるいは，キー番号に変更を加えなくて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，ソルト値がいったん付されてしまえば，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．したがって，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等を考えれば，現実的にはその可能性は低いと評価できる．

(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，捏造されていなくても，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．このような不正もケース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．したがって，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．

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

捜査機関が実際の押収手続に立会った立会人を隠蔽等し，

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し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．これでは，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不利益以外の何ものでもなく，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．

4.3 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．

(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．登録前にすで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．したがって，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，押収後ただちに，あるいはきわ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すでに偽造されており，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．したがって，このような不正を見逃さないためには，たとえば，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等，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．

(2) いったん登録して後に当該証拠を改ざんしたうえ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，いったん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，証拠ハッシュ値がすで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，新たな登録キー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．ただし，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．したがって，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あえて署名（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．したがって，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いえる．

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わけはない．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 4.3 節 (1)，(2) 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．

(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，提案システムでの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

証拠であったのであ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，たとえば，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いえる．しかし，後述するとおり，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いえない．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．ただし，いったん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かえ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ともなう．

4.4 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ただ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 4.3 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．したがって，このようなリスクに対して対処するためにも，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．

5. 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

5.1 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 [13] 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うえ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 [14], [15], [16].

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 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を調べ，されていなければ証拠ハッシュ値とアドレスを登録し，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 は，指定された証拠ハッシュ値がすで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 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等，安全な環境に持つのが望ましい．

5.2 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 66000 gas，execution cost に約 41000 gas の合計約 107000 gas を要した．また，checkHash 関数の実行には transmission cost に約 24000 gas，execution cost には約 590 gas の合計約 24600 gas を要した．いずれも ETH 換算

ではきわ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わけではないが，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．

6. トークンを活用したトークンエコノミーの構築について

6.1 トークンエコノミーの構築の重要性

提案システムでは，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，提案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ほかならない．しかし，そのトークン自体に何の利用価値も認められず，トークンの発行およ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提案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，提案システムの円滑な運用のためのインセティブとなりうる独自の経済圏（トークンエコノミー）の構築が求められる [17]．

6.2 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，そもそも一般市民である押収手続に立会う立会人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．

(1) 一般市民による利用

i 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．したがって，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契機，依頼者の獲得につな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．

ii 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，一定の法律研修等を受けることは価値のあるサービスを受けることであり，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．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．

iii 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）もありうる．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，たとえば，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とらえる方法が考えられる．

iv 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．

(2) 弁護士による利用

i 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．

ii 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もっ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．

iii 電子公証システムとしての利用

提案システムは，証拠ハッシュ値の保管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，たとえば，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提案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が，前述のとおり，弁護士がこれらの制度等を利用することに対しては多くの負担が存在する．しかし，ブロックチェーンを利用した提案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，システムの利用料（gas を含む）として，電子公証制度やタイムスタンプと比較して安価な負担となるようにトークンの支払いを設計すれば費用負担の面で弁護士等の利用者にとって大きなメリットとなりうる．また，利用者は，それぞれの居場所から提案システムを利用することができ，その利便性も高い．また，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提案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．

6.3 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．

(1) 一般市民対する付与

i 証拠ハッシュ値の登録の際の立会人として

まず，提案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．

ii 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いえる．

iii 電子公証システムとして利用された際の立会人

最後に，提案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．提案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，提案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およ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，別途提案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うる．しかし，たとえば，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，トークンの付与およ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．

(2) 弁護士に対する付与

i 法律相談

弁護士会等が実施する各種法律相談における参加弁護士に対してトークンが付与される．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考えれば，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うる．

ii 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，あるいは提案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．

6.4 トークンに対するインセンティブとしての価値

提案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うることが分かる．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，弁護士会お

よ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業務機会の拡大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い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も優れた提案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．

したがって，提案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．

6.5 課題

他方，トークンエコノミーを効果的に構築・運営していくうえで，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うえで，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等決定しなければならないことは多い．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（2020 年 5 月施行の法改正により仮想通貨から置き換えられた．以下同じ）ないし前払式支払手段に該当するかという問題は，それによって発行主体である弁護士会が暗号資産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する問題として重要である．

たとえば，提案システムにおける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等との相互交換は欠かせない条件であるといわれている [9]．しかし，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．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 号暗号資産に該当する可能性は低いといえる（法 2 条 5 項 1 号参照））．したがって，その場合，弁護士会が「暗号資産交換業者」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，有償での本トークンの販売は認められない．また，仮に，本トークンが暗号資産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．したがって，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．

7. まとめ

本論文では，改ざんが可能かつ容易なデジタル証拠（電磁的証拠）について，特に捜査機関による押収後の改ざんの疑念を払拭させ，国民に信頼される裁判に資するための客観的なデジタル証拠の改ざん防止システムとして，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を利用するシステムの有効性を示した．また，提案システムが有効に利用されるうえで必要不可欠となるトークンを活用したトークンエコノミーの構築について検討した．

今後の課題としては，より実運用に近い環境を実現するため，Android アプリケーション内にウォレットを実装する等，現在欠けている機能を実装したうえで，今回実装できていないトークン付与機能を加えたシステムの上での評価を行うことがあげられる．

参考文献

[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（DICOMO2017）シンポジウム研究報告 (2017).

[2] 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・社会基盤研究会研究報告（2018-EIP-82, pp.1–8）(2018).

[3] 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，NBL，No.1098, pp.15–22 (2017).

[4] 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）(2012).

[5] 吉峯耕平，倉持孝一郎，藤本隆三，新井幸宏：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，No.77, pp.134–154 (2014).

[6] 法務省：公証制度に基礎を置く電子公証制度について，入手先〈http://www.moj.go.jp/MINJI/DENSHIKOSHO/index.html〉.

[7] 宮内　宏ほか：電子契約の教科書—基礎から導入事例まで，日本法令 (2017).

[8] 手塚　悟，向　賢一ほか：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).

[9] 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).

[10] 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).

[11] 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).

[12] 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).

[13] 久保幹雄監修，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).

[14] Modi, R.：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).
[15] 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).
[16] 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).
[17] 高 榮郁：トークンエコノミービジネスの教科書，KADOKAWA (2019).

小坂谷 聡 （学生会員）

1994 年一橋大学大学院法学研究科修士課程修了．2001 年司法修習生を経て，2002 年弁護士登録（大阪弁護士会）．2016 年立命館大学大学院情報理工学研究科博士課程後期課程入学．

上原 哲太郎 （正会員）

1995 年京都大学大学院工学研究科博士後期課程研究指導認定退学．同大学院工学研究科助手，和歌山大学システム情報学センター講師，京都大学大学院工学研究科附属情報センター助教授，同大学学術情報メディアセンター准教授，総務省情報通信国際戦略局通信規格課標準化推進官を経て，2013 年より立命館大学情報理工学部教授．京都大学博士（工学）．デジタル・フォレンジック，システムセキュリティ等の研究に従事．共著に『基礎から学ぶデジタル・フォレンジック』（日科技連出版）等．