Vol.2017-DPS-170 No.19
Vol.2017-CSEC-76 No.19
2017/3/2

ブロックチェーンにおける本人性確認の方法に関する考察

永田 和之† 李 中淳† 福田 賢一† 岩丸 良明† 庭野 栄一†
谷内田 益義† 平良 奈緒子† 鈴木 裕之† 小尾 高史† 大山 永昭†

概要：ブロックチェーンは，分散型ネットワークにおいて，改ざんが困難なデータ構造を有するデータを検証及び保存することによって当該データの高可用性及び完全性を担保する技術であり，様々な分野での応用が期待されている．本稿は，ブロックチェーンを活用した新しいサービスの創出に資するよう，ブロックチェーンのユーザの本人性を確認する方法として，公的個人認証サービス（JPKI）を利用する場合の基本的な考え方及び処理手順について考察した．

キーワード：ブロックチェーン，公的個人認証サービス，本人性確認，分散型ネットワーク

A study on a method of identity verification in blockchains

Kazuyuki NAGATA† Joong Sun LEE† Kenichi FUKUDA† Yoshiaki IWAMARU†
Eikazu NIWANO† Masuyoshi YACHIDA† Naoko TAIRA†
Hiroyuki SUZUKI† Takashi OBI† Nagaaki OHYAMA†

Abstract: Blockchain is the technology that has data structure with anti-tampering and ensures high availability and integrity of the data which is verified and archived in a distributed network, and it is expected to be practically applied in a wide range of fields. Under such circumstances, aiming to contribute to the creation of new services using blockchain technology, we presented a basic method and procedure for identity verification of users in blockchains, utilizing the public certification service for individuals in Japan, called Japanese Public Key Infrastructure (JPKI).

Keywords: Blockchain, JPKI, Identity verification, Distributed network

1. はじめに

ブロックチェーン（blockchain）とは，一般社団法人日本ブロックチェーン協会の定義（広義）では，「電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち，且つ，当該データをネットワーク上に分散する多数のノードに保持させることで，高可用性及びデータ同一性等を実現する技術」とされる．

近年，ブロックチェーンの技術的な有用性が注目されるようになり，ブロックチェーンを利用した様々なサービスが現れているが，その利用の中心は仮想通貨の取引である．そして，一般的なブロックチェーンによる仮想通貨の取引システムでは，プライバシ保護の観点から，ユーザの匿名性を重視した運用がなされるのが一般である．

他方，ブロックチェーンは，分散型ネットワークにおいてデータを検証・保存する電子分散台帳としての特徴を有する．そこで，この電子分散台帳としての特徴を応用して，ブロックチェーンを様々なサービスに活用しようとする動きも活発である．

このような状況に鑑み，ブロックチェーンにおいて，トランザクション（2.1 (1) 参照）を実行する者の本人性を確実かつ簡易に確認する電子的手段があれば，ブロックチェーンの電子分散台帳的特徴を活用した新たなサービスの創出に資すると考えられる．

そこで，本稿では，電子的な本人性確認の手段として有効な「公的個人認証サービス」を利用して，ブロックチェーンにおける本人性確認の方法に関する基本的な考え方及び処理手順について考察した．

2. ブロックチェーンの概要

2.1 処理の概要

ブロックチェーンは，S. Nakamoto 氏の論文「Bitcoin: A Peer-to-Peer Electronic Cash System」[1]において，仮想通貨の一種である Bitcoin を実装する目的で考案された分散型ネットワーク技術の一つである．

今日，ブロックチェーンを応用した様々な技術及びサービスが開発されているが，本稿では，ブロックチェーンの中で最も基本的かつ一般的と考えられる Bitcoin のシステムを例に，本稿における考察に関連する処理等を中心にその概要を説明する．

(1) **トランザクション**[2]

ブロックチェーン上で実行される基本的な処理の一つはユーザ間での仮想通貨の取引（決済）であり，この処理

† 東京工業大学
Tokyo Institute of Technology

Vol.2017-DPS-170 No.19
Vol.2017-CSEC-76 No.19
2017/3/2

はトランザクション（transaction）と呼ばれる．

一般に，ブロックチェーンのトランザクションでは，楕円曲線暗号（ECDSA）が用いられ，トランザクションの実行毎に，①秘密鍵，②公開鍵及び公開鍵をハッシュ化（SHA-256 等）して得られる③アドレス（取引用 ID）が生成・使用される．これらの鍵等の生成・管理・利用等は，ウォレット（wallet）と呼ばれる機能により実現される．ウォレットには，インターネットのウェブサービスとして提供されるもの，ユーザの PC にソフトウェアをダウンロードして利用するもの，専用の端末で利用するもの等，様々な形態のものが存在する．

各トランザクションを構成するデータは，仮想通貨の使用権限の根拠（署名，公開鍵等）を含むインプット部，並びに仮想通貨の取引量及び宛先アドレスを含むアウトプット部からなる．例えば，仮想通貨をアドレス A からアドレス B に移転する場合，アドレス A，取引量，アドレス B 等のハッシュ値をアドレス A に対応する秘密鍵で暗号化したデータと当該秘密鍵に対応する公開鍵等をインプット部に記録し，仮想通貨の取引量とアドレス B 等をアウトプット部に記録してトランザクションのデータを生成する．

あるノードで生成されたトランザクションは，分散型ネットワークに接続された他のノードに送られ検証される．当該検証は，インプット部の暗号化されたデータを公開鍵で復号して得られるデータ（アドレス A，取引量とアドレス B 等のハッシュ値）と，関連するトランザクションに記録されているアドレス A，取引量とアドレス B 等の元データのハッシュ値を比較することにより行われる．

トランザクションは，各ノードの検証によって正当性が確認されれば更に他のノードに送られ，正当性が確認されなければ破棄される，という処理を経て，全ノードに伝搬する．その後，各ノードに伝搬したトランザクションは，承認待ちのトランザクションを一時保存するトランザクションプールで管理される．

(2) 採掘と承認[2]

採掘（mining）とは，特定の条件を満足した採掘者（miner）が，複数のトランザクションの検証を行った上で，正当性が確認されたトランザクション等をブロックと呼ばれるデータの塊の単位にまとめて記録するとともに，新規に発行された仮想通貨の所有者になる処理のことをいう．

現在，採掘の信頼性を担保する手段として様々な方法が考案されているが，Bitcoin では，Proof of Work (POW)と呼ばれる方法が採用されている．この POW とは，最新ブロックのデータの一部（一つ前のブロックのハッシュ値，マークルルートのハッシュ値とタイムスタンプ等）に Nonce（Number used once）と呼ばれる使い捨て値を付加し，それらのハッシュ値を目標値（difficulty target）より小さくする Nonce（解）を最初に発見したノードを採掘者と決定する方法である．以下では，Bitcoin の POW を例に，採掘の概要について説明する．

分散型ネットワーク上で採掘を行うノードは，トランザクションプールから抽出したトランザクションについて，仮想通貨の二重使用，データ不備の有無等の検証を行った結果，正当性が確認されたトランザクションをとりまとめ，ブロック生成の準備をする．

そして，採掘に参加するノードの中で，最初に解を発見したノードは，採掘者として新たなブロックを生成して全ノードに伝搬させる．その後，各ノードにおいて当該ブロックの正当性を確認してブロックチェーンに連結する．採掘者は，トランザクション毎に定められた処理手数料に加えて発掘報酬を仮想通貨で得る．これが各採掘者の POW 実施のインセンティブとなる．

以上のように，ブロックチェーンは，トランザクション等が記録された電子台帳を分散型ネットワーク上の各ノードで分散管理するとともに，採掘者になるノードが不特定となる仕組みが採用されていることから，単一障害点がなく，データのバックアップやシステムの冗長化が不要という特長がある．

また，ブロックチェーンは，採掘を通じて，一つ前のブロックのデータから得られるハッシュ値を次のブロックに引き継ぐデータ構造を採用しているので，ブロック高が高くなるにつれて，過去に連結されたブロックに含まれるデータの改ざんが困難になるという特長を持つ．なお，各ブロックは，約 1,500 以上のトランザクションを有し，各ブロックのデータの大半をトランザクションが占めている．

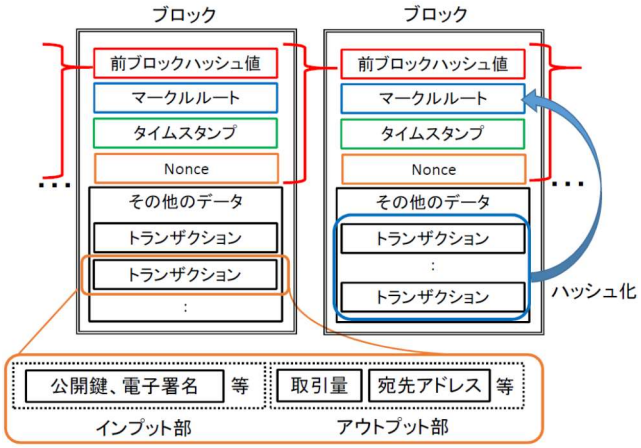

図 1　ブロックチェーンのデータ構造概要

一般に，ブロックチェーンには採掘を行うノードが多数存在するので，複数の異なるノードが偶々同時に採掘に成功した場合，新たなブロックが複数生成され，ブロックチェーンが分岐する可能性がある．この場合，各ノードは，その後のブロックの連結状況を比較し，ブロックの連結が最も長い分岐を正規のものとして選択する．そして，各ノ

ードが選択するブロックチェーンに更に複数個のブロックが連結されれば，最新のブロックから数ブロック遡ったブロックに含まれるトランザクション群については，改ざんが非常に困難となるので，承認されたものとして扱われる．

2.2 ブロックチェーンの現状と課題

ブロックチェーンは，仮想通貨を発行して分散型ネットワーク上に流通させることを前提として設計・運用されるものが多い．そして，現在，一般に流通する仮想通貨のうち，総取引量が最も多く，大規模かつ広範囲に流通しているのが Bitcoin である．

Bitcoin はオープンソースのプロジェクトである．このため，そのコードは他の多くのブロックチェーン関連のソフトウェアの基盤となっており，これを応用した様々な技術及びサービスが開発されている．

例えば，ブロックチェーンの電子分散台帳的性質に着目して，メタデータをブロックチェーン上に記録して利用するものなど，多種多様なブロックチェーンのサービスが存在している．しかし，現時点において，このような性質を持つブロックチェーンのサービスは，Bitcoin と比べ普及が進んでいるとは言い難い．

他方，ブロックチェーンの決済手段的性質に重きを置くサービスでは，匿名性の確保が重視される傾向にある．例えば，Bitcoin は，仮想通貨の流通を目的として考案されたという経緯から，トランザクション毎に異なるアドレスを用いる運用が一般的であり，ユーザ特定の可能性をできる限り排除しようとする設計思想が垣間見られる．

このような状況に加え，電子空間上で本人性確認を行う基盤の普及が世界的に遅れている状況もあり，ブロックチェーンのユーザの本人性情報と他の有価値な情報を紐づけて，オープンなブロックチェーン上で管理・利用するサービスが普及しにくい環境になっているものと考えられる．

この点，我が国は，3. で述べるように，電子空間上で本人性を確認する基盤が整っているので，当該基盤を利用することにより，ユーザの本人性情報と有価値な情報を紐付けてブロックチェーン上で管理・利用することが可能と考えられ，ブロックチェーンの電子分散台帳的性質に注目した新たなサービスの創出が期待できると考える．

3. 公的個人認証サービス（JPKI）の概要[3]

「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び関連法が施行され，2016 年 1 月から申請者に対しマイナンバーカード（IC カード）の交付が開始された．

このマイナンバーカードの IC チップには，JPKI の署名用電子証明書，利用者証明用電子証明書等が格納される．JPKI は，電子的な手続等を安全かつ確実に行えるよう，公開鍵暗号（RSA-2048）を用い，他人による電子的なりすまし及び改ざんがないことを確認し，電子的な意思表示等に対する否認行為を防止するとともに，電子的な認証を行う公的基盤である．

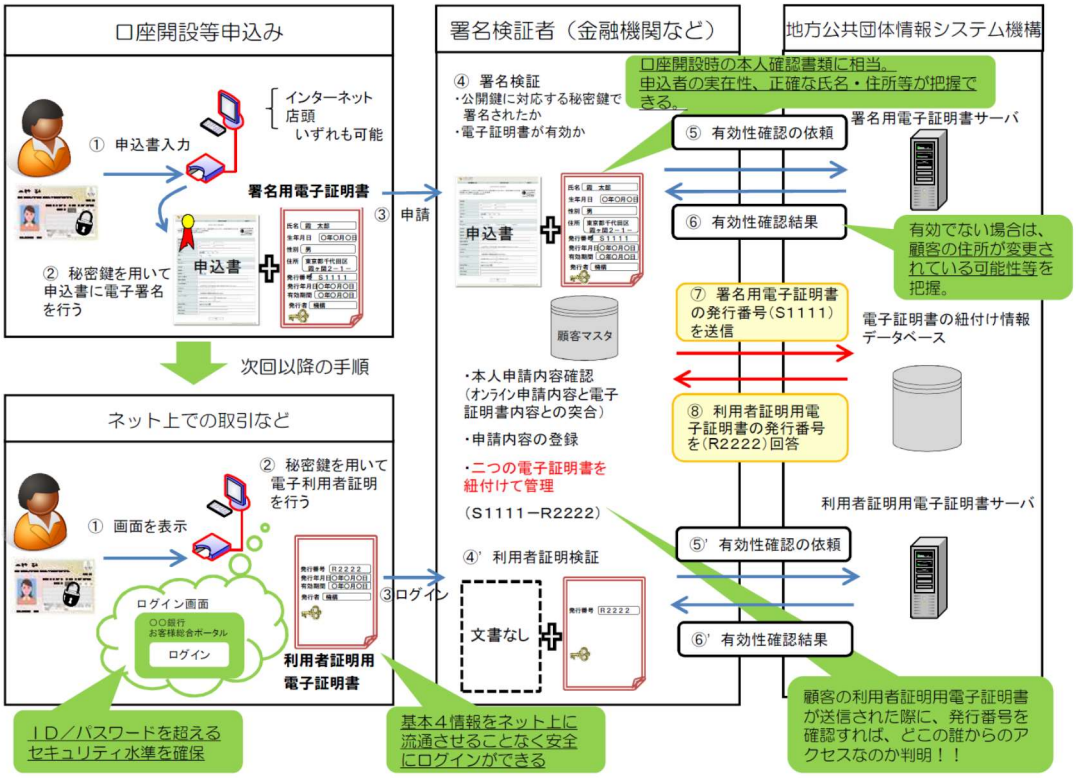

図 2　民間事業者の JPKI の利用イメージ（出典：総務省資料[3]）

ここで，署名用電子証明書とは，市区町村長が発行する署名用秘密鍵に対応し，地方公共団体情報システム機構（以下，「J-LIS」という.）が電子署名を付与した公開鍵の電子証明書であり，マイナンバーカードの所有者の個人情報（住所・氏名・生年月日・性別）を含み，電子的な手続等において，他人による電子的ななりすまし及び改ざん並びに利用者本人の電子的な意思表示の否認行為を防止する目的で利用されるものである．また，利用者証明用電子証明書とは，市区町村長が発行する利用者証明用秘密鍵に対応し，J-LIS が電子署名を付与した公開鍵の電子証明書であり，上記の個人情報を含まず，電子的な手続等において他人による電子的ななりすましを防止し，利用者本人による電子的なアクセスを認証する目的で利用されるものである．

マイナンバーカードの交付に際しては，地方公共団体の職員による厳格な本人確認が行われ，JPKI の利用を希望する者に対して，窓口の専用端末を用いて，マイナンバーカードの IC チップの耐タンパー領域に電子署名及び利用者証明に用いる秘密鍵等が記録される．当該秘密鍵は，利用者本人のみが知りうるパスワード等でアクセスコントロールされているので，JPKI の電子署名等を利用する者はマイナンバーカードの名義人本人であると推定できる．

このように，JPKI は，電子的な本人性確認の手段として，我が国において最も信頼性の高い基盤の一つであると考えられる．

この JPKI は，以前は民間事業者等による利用が認められていなかったが，2016 年 1 月から，総務大臣の認定する民間事業者等が，JPKI の署名検証者として JPKI を利用したサービスを実施できるようになった．また，2017 年 1 月から，利用者証明用電子証明書の更新に対応できるよう，当該電子証明書の新旧発行番号（シリアル番号）の紐付けサービスが開始され，民間事業者の利便性が向上した．

このような状況から，JPKI は，セキュリティが十分に確保された環境の下で電子的に本人性確認を行うニーズを有する，民間の金融機関，医療機関等における本人性確認及び認証手段として期待されている．このような状況を踏まえ，我々は，JPKI の社会実装に向けた検討を行ってきたところである[4][5][6].

そこで，本稿は，ブロックチェーンを活用した新しいサービスの創出に資するよう，ブロックチェーンのユーザの本人性を確認する方法として，JPKI を利用する場合の基本的な考え方及び処理手順について考察した．

4. ブロックチェーンにおける本人性確認

これまで述べてきた内容を踏まえ，ブロックチェーンのユーザの本人性確認を行う方法として，JPKI を利用する場合の基本的な考え方及び処理手順について考察する．

本考察では，各種ブロックチェーンのサービスの中で最も普及が進んでおり，オープンソースで開発・改良が容易な Bitcoin について，トランザクションの実行者の本人性確認を行う方法を検討対象とした．

Bitcoin は，ユーザの匿名性確保の観点から，一般にトランザクション毎に異なるアドレスが用いられ，仮名（アドレス）によりトランザクションが行われるので，当該トランザクションの実行者の本人性を第三者に対して主張する根拠となる電子的情報をブロックチェーン上に記録することは，別途の仕組みを利用しなければ困難である．そこで，電子空間における本人性の確認手段として有効な JPKI を利用して，トランザクションの本人性確認を行う方法等を検討することとした．

また，Bitcoin が既に多くのユーザに利用されていることに鑑み，Bitcoin の仕様及び運用の根本的な部分への変更を極力避けるとともに，できる限り簡易な処理によって実現することを基本として検討を行った．

【本考察の前提】
- Bitcoin のトランザクションの実行者の本人性を確認する方法を検討対象とする．
- 本人性を確認する方法として JPKI を利用する．
- Bitcoin の仕様及び運用の根本的な部分の変更を必要としない簡易な方法を検討する．

4.1 他者を介在させない方法

まず，ユーザが，他者を介在させず，本人性の根拠となる電子的情報をブロックチェーン上に記録する方法を検討する．

そもそも，この場合は，トランザクション毎に生成されるアドレスに対し，それらが確実に本人によって生成された旨証明する手段を担保することは難しいと考えられる．

また，仮に，ユーザのマイナンバーカードの JPKI で当該ユーザが利用するアドレスを暗号化（電子署名）して得られる電子的情報を利用する場合を考えても，当該情報の正当性を確認する者は JPKI の署名検証者となる必要がある上，当該データのサイズが 2,048 ビット（256 バイト）程度となるので，Bitcoin の運用上推奨される方法によれば，データをトランザクションに記録する「OP_RETURN」スクリプトの仕様（最大 80 バイト）に抵触する．なお，この仕様の制限は，ブロックチェーンのデータの肥大化をできる限り避け，各ノードにおけるサーバ及びストレージのコスト増を防ぐ目的から設けられているものである．

以上により，ユーザが，他者を介在させず，本人性の根拠となる電子的情報をブロックチェーン上に記録する方法は，実現上の困難性を孕むうえ，Bitcoin の基本的な仕様等の変更が必要になる可能性が高いことから，本稿では扱わないこととした．

4.2 他者を介在させる方法

次に，ユーザが，JPKI の署名検証者として総務大臣に認

定された民間事業者等を介在させて，本人性確認を行う方法を検討する．

この場合，署名検証者が，トランザクションの実行者の本人性の根拠となる電子的情報（以下，「電子証票」という．）を発行し，ブロックチェーン上に記録するという方法が考えられる．ここで，電子証票は，①電子証票の発行者を区別する識別符号及び②ユーザの利用するアドレスを署名検証者が暗号化・ハッシュ化したデータ等から構成されるものとし，そのデータサイズが数十バイト以下となるようにする．

また，トランザクション毎に生成されるアドレスについて，それらが本人の意思表示により生成されたことを担保できるよう，署名検証者は，Bitcoin の利用上普及しつつあるウェブウォレット又はオンラインウォレットと呼ばれる仮想通貨の取引代行のインターネットウェブサービス提供者として，ユーザの秘密鍵とそれに由来するアドレス等の生成・管理を代行しているものとする．

以上を踏まえ，この方法における基本的な処理の考え方を示す．

(1) サービスへの登録申請

まず，ユーザは，あらかじめ，署名検証者に対し，JPKI の電子署名を付して当該サービスに登録申請を行う．

(2) ユーザ情報の紐付け・管理

署名検証者は，JPKI の運営主体である J-LIS に対し，当該電子申請を通じてユーザから受領した署名用電子証明書の発行番号（署名用シリアル番号）に基づき，当該ユーザの利用者証明用電子証明書の発行番号（利用者証明用シリアル番号）を問い合わせ，両シリアル番号と当該ユーザの情報との紐付けを行い，データベースで管理する．

(3) ログイン及び電子証票の発行依頼

ユーザは，当該サービスへの登録後，JPKI の利用者証明機能による認証により暗証番号を入力して，当該サービスの当該ユーザ用アカウントにログインし，電子証票の発行を依頼する．

(4) 電子証票の生成

署名検証者は，ユーザのログイン中にのみ当該ユーザが依頼した処理のみを実行できるように管理されたトランザクション実行機能により，当該トランザクションに使用する秘密鍵及び公開鍵を生成するとともに，当該公開鍵から生成される取引用のアドレスを生成する．

そして，電子証票発行機能により，当該アドレスを署名検証者が定める暗号方式により暗号化した後，そのハッシュ値（例えば，SHA-256 等）等を得た上で，それに署名検証者の識別符号をヘッダ情報として付加して電子証票を生成する．

(5) 電子証票の記録・管理

署名検証者は，トランザクション実行機能により，依頼されたトランザクションを実行するとともに，「OP_RETURN」スクリプトを用いて電子証票をトランザクションに記録する処理を実行する．当該電子証票は，ユーザ情報（アドレス，利用者証明用シリアル番号等）と紐づけられ，ユーザ情報管理機能において管理される．

なお，本方式では，アドレス毎に異なるデータの電子証票が発行されることから，ブロックチェーン上におけるユーザの匿名性は，現システムと同程度に担保できるものと考えられる．

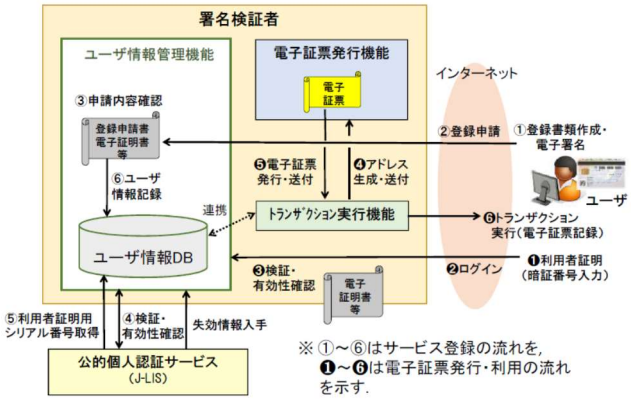

図 3　電子証票発行サービスの概要

(6) 本人性の確認方法

あるトランザクションの本人性確認を実施しようとするユーザ又は第三者は，ブロックチェーン上の電子証票に含まれる識別符号に基づき，電子証票の発行者（署名検証者）を特定する．

そして，当該電子証票に対応するアドレスを当該署名検証者に問い合わせ，当該トランザクションで使用されたアドレスと一致するアドレスが回答されるか否かを確認することによって，当該トランザクションの本人性を確認する．

4.3 業務フロー例

以上の考察を踏まえ，以下に電子証票の発行に係る業務フロー例を示す．ただし，本稿の業務フロー例は，基本的な仕組みを簡略に可視化する観点から粗めの粒度で記述した．したがって，具体的なシステムの実装においては，更に詳細な検討を要する点に留意が必要である．

なお，業務フローの記述には，国際標準として記法が確立している BPMN（Business Process Modeling and Notation）[7]を使用した．

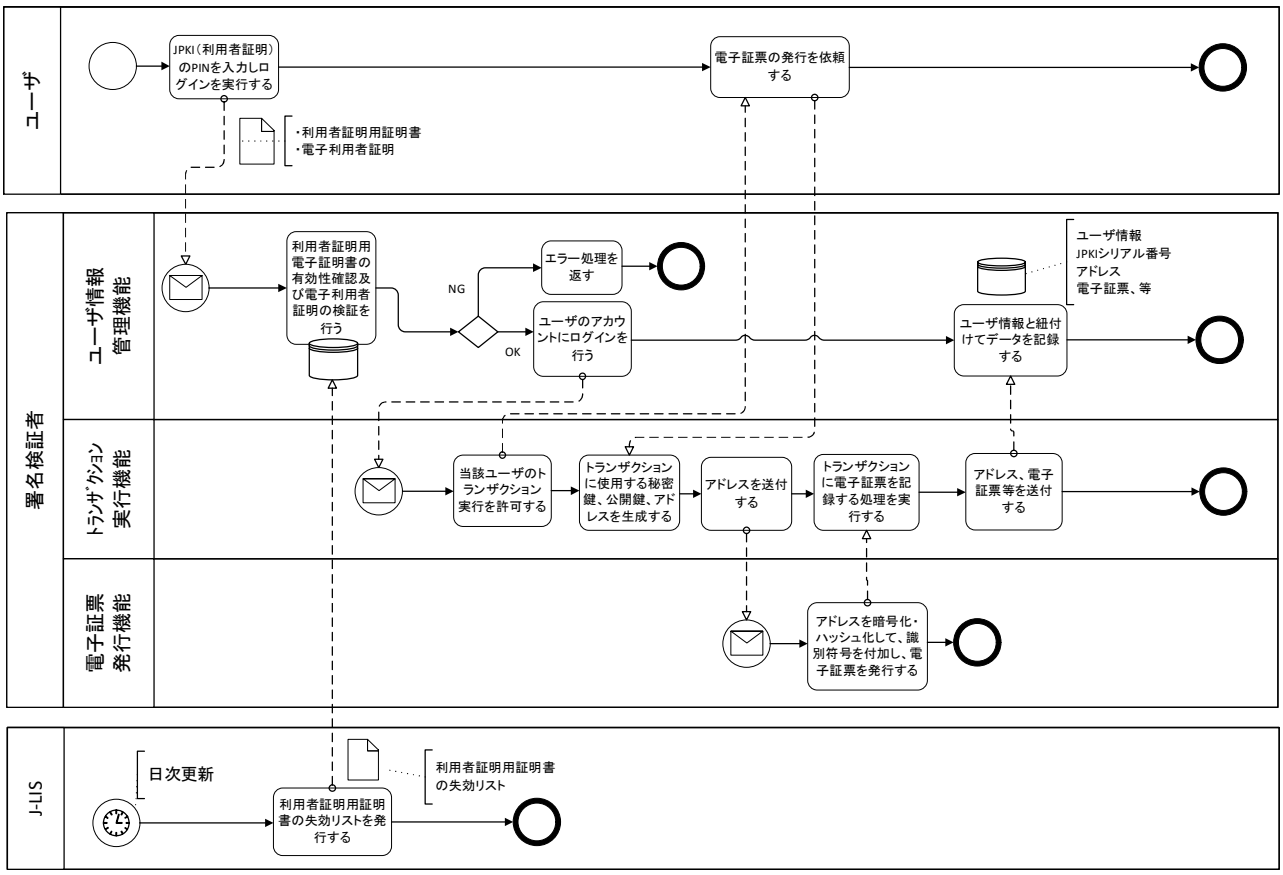

図 4　電子証票の発行に係る業務フロー例

5. おわりに

本稿では，ブロックチェーンのユーザの本人性確認の方法として，JPKI を利用する場合の基本的な考え方及び処理手順を示した．

これにより，電子証票とユーザ本人に係る有価値な情報を紐付けてブロックチェーン上で管理・利用することが可能となり，様々なサービスへの応用が可能と考えられる．ただし，具体的なサービスを実施するに際しては，実環境での実証実験等を通じて，処理手順等の精緻化，セキュリティの検証等を行う必要がある．

また，本内容の導入に当たっては，署名検証者の業務に対する信頼性確保が不可欠になるので，これを制度的に担保する必要がある．したがって，セキュリティ確保等を含めた署名検証者の業務に対する規制に加え，当該業務を実施する署名検証者の許可・認証制度等が必要になるものと考えられる．

今後，具体的なサービスシーンを踏まえ，当該システムの実装に向けた詳細検討が行われることに期待したい．

本内容が，ブロックチェーンを活用した新しいサービスの創出に資するとともに，政府が推進する JPKI の利活用拡大の一助となれば幸いである．

謝辞　本考察にご協力頂いた皆様に，謹んで感謝の意を表する．

参考文献

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2008
[2] Andreas M. Antonopoulos, “Mastering Bitcoin”, O’ Reilly Media, Dec. 2014, 今井崇也・鳩貝淳一郎 訳, NTT 出版, July 2016
[3] 総務省自治行政局住民制度課, “マイナンバーカードの概要及び公的個人認証サービスを活用したオンライン取引等の可能性について”, http://www.soumu.go.jp/main_content/000418560.pdf, 2016 年 11 月
[4] 藤田和重, 小尾高史, 谷内田益義, 李中淳, 平良奈緒子, 奥信人, 庭野栄一, 則武智, 岩丸良明, 大山永昭, “金融・決済分野における公的個人認証サービスの活用に関する考察”, 信学技報, vol.114, no.500, LOIS 2014-84, pp.135-140, Mar.2015
[5] 藤田和重, 小尾高史, 御代川知加大, 谷内田益義, 李中淳, 夏目哲也, 平良奈緒子, 庭野栄一, 熊倉誠, 岩丸良明, 大山永昭, “公的個人認証サービスを用いた官民連携の可能性について”, 信学技報, vol.113, no. 381, pp.29-34, Jan. 2014
[6] 小尾高史, 藤田和重, 大山永昭, “新たな公的個人認証サービスとその医療分野での利用に関する検討”, 2014 年暗号と情報セキュリティシンポジウム(SCIS2014), SCIS2014 論文集, 4B1-3, Jan. 2014.
[7] Information technology — Object Management Group Business Process Model and Notation, ISO/IEC 19510, Jul.2013