卒業論文　2017 年度（平成 29 年度）

公的個人認証サービスを用いた スマートエスクローの実装

慶應義塾大学 総合政策学部

尾﨑 周也

shuya@sfc.wide.ad.jp

徳田・村井・楠本・中村・高汐・バンミーター・植原・三次・中澤・武田
合同研究プロジェクト

2018 年 1 月

卒業論文　2017 年度（平成 29 年度）

公的個人認証サービスを用いた スマートエスクローの実装

論文要旨

署名捺印を用いた本人確認の危殆化や，電子商取引の増加・多様化のため，取引の信頼性・本人性確認の担保が難しくなり，従来の契約方法では取引の安全性や信頼性の担保が難しい．本論文では，この商取引の問題に対し，契約の履行と本人性確認の観点からアプローチする．

本論文では，契約の履行の方法として，スマートコントラクトを用いた売買契約の不可分な履行を提案・実装した．本論文では，この契約方法をスマートエスクローと呼ぶ．スマートコントラクトは，プログラム化された契約を自動履行する仕組みで，これを用いてスマートエスクローを実現する．本人性確認には，公的個人認証サービスを利用する．スマートコントラクトに使用する取引のためのアドレスを，マイナンバーカードに搭載される署名用秘密鍵で署名し，署名検証が可能な形で公開する．本提案手法を用いることで，本人性確認を伴う，スマートエスクローを履行し，安全な電子商取引が可能になる．

評価として，機能要件の定性的評価と，既存の契約手法と実用性の比較を行った．提案システムによる本人性確認を行うスマートエスクローの実現の確認，また，本提案手法が実用性を有することを示した．

キーワード

マイナンバー，公的個人認証サービス，エスクロー，スマートコントラクト

慶應義塾大学 総合政策学部

尾﨑 周也

Abstract of Bachelor's Thesis Academic Year 2017

Implementation of Smart Escrow Using Japanese Public Key Infrastructure

Summary

With the personal identification by signing and sealing compromised and the diversification of electronic commerce increasing, it is becoming difficult to secure the reliability of transactions and confirmation of identity, making it impossible to guarantee the safety and reliability of trading under the traditional contract method. In this thesis, we take the approach to this commercial transaction from the viewpoint of execution of a contract and personal identification.

This thesis proposes indivisible execution of sales contract using smart contract as a method of execution of a contract. This contract method is hereinafter called smart escrow. Smart Contract is a mechanism that automatically executes programmed contracts by using this contract, which is used to realize smart escrows. To verify identity, Japanese Public Key Infrastructures are used. The Ethereum address specified by the Smart Contract is signed by the signature public key mounted on Individual Number card, and the signature can be verified in a publicly accessible form. By using the proposed method, it is possible to perform secure e-commerce by executing smart escrow after verifying identity.

For evaluation, qualitative evaluation of functional requirements and comparison between existing contract method with practicality were carried out. As the result of the evaluation, we confirm the realization of smart escrow and verify personal identity by proposed system, which showed that the proposed method has utility.

Keywords

Individual Number，Japanese Public Key Infrastructure，Escrow，Smart Contract

Bachelor of Arts in Policy Management

Keio University

Shuya Osaki

目 次

図 目 次

表 目 次

第1章　序論

1.1　研究の背景

商取引の複雑化・電子商取引の普及により，詐欺・トラブルといった電子商取引の安全性や信頼性を損なう問題が増加している．このトラブルを軽減させるアプローチとしてエスクローサービスの利用が期待されるが，一般に普及していないと指摘されている [1].

また，取引を行う際の契約締結には，取引相手・内容・契約内容の確認と否認防止が必要である．そして，契約内容の正当性の認証の手段として，署名捺印・記名押印[1]が用いられる [2]．しかし，筆跡や陰影をデジタル化して用いる場合，容易にコピーすることが可能で，単に照合する方式は有用でないと指摘されている [3].

実例として 2017 年 8 月に，積水ハウスが，他人の所有地を利用して詐欺を働く者である地面師による詐欺にあった事件は記憶に新しい [4]．この事件は，積水ハウスが土地の取得のために購入代金を所有者とされる人物に払ったにも関わらず，取得予定地の登記申請が拒否された．理由は，土地の所有者側の提出書類に真正でない書類が含まれていたためである．この案件で不動産購入の方法として，積水ハウスの契約相手先が所有者から土地購入後，積水ハウスに転売される形がとられた．そこでは，契約を仲介し履行を担保するエスクローは用いられなかった．また，本登記が登記官により却下されたが，仮登記は完了していた．つまり，仮登記までは偽造された書類が受領されていた [5].

これらは，一般的な商取引全般における課題である．1 点目は，紙による申請書類のために，確認が電磁的には行えず，人に依らざるを得なかった点．2 点目は，エスクロー取引のような，信頼される第三者による契約履行の代行によって防げた課題である．

1.2　研究の目的

本研究では，前節で挙げた二つの課題をブロックチェーン技術によって可能になるスマートコントラクトと，マイナンバーカードを用いた公的個人認証サービスの活用で，解決することを目指す．本研究では以下の 2 点からアプローチを行う．

- 定められた条件下での契約の自動履行
  ブロックチェーン技術によって可能となった，プログラムできる契約である，スマートコントラクトにより取引を自動化する．ブロックチェーンによるスマートコントラクトでは，取引が P2P ネットワーク上で実行・承認されるため，仲介者が不要になる．また，契約の条件の履行の確認も自動化して行われる．

[1]商法 32 条で，署名と記名押印の効力は以下の様に定められている．“この法律の規定により署名すべき場合には，記名押印をもって，署名に代えることができる．"

- 公的個人認証サービスを用いた本人性確認
  公的個人認証サービスの提供する，利用者証明用電子証明書を利用する．行政機関の発行した電子証明書を利用した，本人性確認が行える．

この 2 点によって，第三者の介在なしの預託取引であるスマートコントラクトと，公的個人認証サービスの活用による本人性確認の担保を実現する．

1.3 本論文の構成

本論文の構成を以下に示す．第 1 章では，本研究の背景と目的について述べた．第 2 章では，本研究の要素技術となる公的個人認証サービスとブロックチェーンについて整理する．第 3 章では，先行研究と事例をあげる．第 4 章では，本提案手法のシステムについて解説する．第 5 章では，本提案手法の実装を示す．第 6 章では，評価とその結果・考察について述べ，第 7 章で本研究のまとめと展望について言及する．

第2章　本研究の関連技術と制度

本章では，本研究の要素技術となる公的個人認証サービスとブロックチェーンについて，技術面と制度面から概説する．

2.1　現代の暗号技術

公的個人認証サービス・ブロックチェーンの要素技術となる電子署名と電子認証について，その技術と関連分野を整理する．

2.1.1　公開鍵暗号

電子署名・電子証明書の要素技術である公開鍵暗号について説明する．本論文においての公開鍵暗号とは，RSA 暗号を用いたものを指す．公開鍵暗号では**公開鍵・秘密鍵**のペアの鍵を使用する．公開鍵と秘密鍵は 2 本で 1 対のペアをなしており，この鍵の対を鍵ペアと呼ぶ．公開鍵・秘密鍵は両者とも，メッセージの暗号化・復号に用いることが可能である．また，公開鍵は誰に見られても良い一方で，秘密鍵からは公開鍵が作成できるため，鍵作成者だけが保持する．

公開鍵暗号では，同じ鍵ペアの鍵でないと，暗号化されたメッセージを復号することはできない．公開鍵と秘密鍵の関係は，錠前と鍵の関係で例えられる．図 2.1 では公開鍵が錠前，秘密鍵が鍵にあたる．図 2.1 に，公開鍵暗号方式の例を示す．

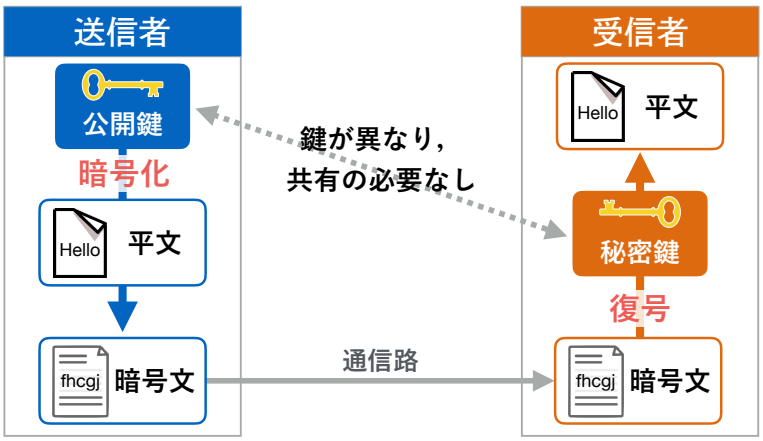

図 2.1: 公開鍵暗号のモデル．[6] を参考に作成．

2.1.2 電子署名

電子署名は，書類への署名を電子データ上で実現する技術である．電子署名は，メッセージの改ざんやなりすましの検出，否認防止を可能とする．また電子署名は，電子署名法に定められる電子的な署名行為[1]である．

電子署名では，公開鍵暗号と同様に，公開鍵・秘密鍵の鍵ペアを用いる．送信者は秘密鍵を用いて，メッセージに署名を付す．一方で公開鍵は，メッセージの受信者がメッセージと署名の検証を行うために用いられる．図 2.2 に，電子署名の例を示す．

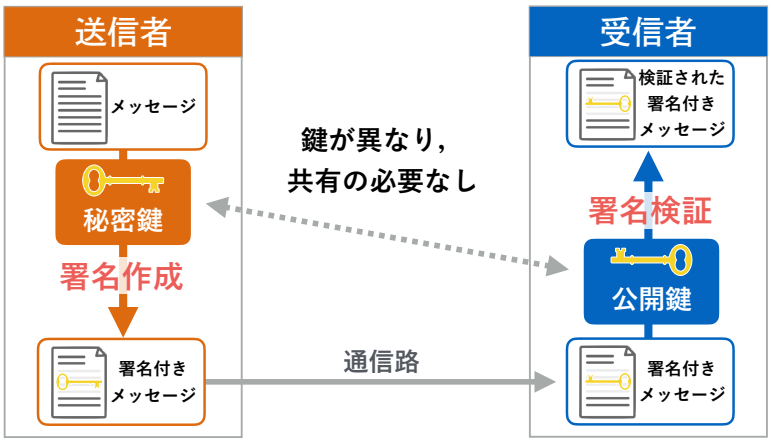

図 2.2: 電子署名のモデル．[6] を参考に作成．

2.1.3 電子証明書

電子署名では公開鍵を用いて署名の検証を行うが，その公開鍵が署名者の正しい公開鍵であるかは証明できない．この公開鍵の所有者の真正性は，電子証明書によって保証される．電子証明書には，公開鍵・所有者の名前・所属やメールアドレス等が記載され，認証局による電子署名が付されている．認証局とは電子証明書の内容を担保する第三者機関であり，後述する公的個人認証サービスでは地方公共団体情報システム機構 (J-LIS) が認証局を務める．

公開鍵基盤 -PKI-

公開鍵基盤 (Public Key Infrastructure) は，公開鍵暗号を用いた電子認証をを行う際の規格・仕様の総称である．PKI では，公開鍵の真正性を認証局と呼ばれる第三者機関を介することで証明する．主要な PKI の構成要素は，以下の 3 点である．

- 利用者
  PKI の利用者．認証局に公開鍵の登録や， 署名の検証を行う．
- 認証局 (CA)
  公開鍵の登録とそれに伴う本人認証や，電子証明書の作成・登録・破棄を行う．

[1]署名捺印と電子署名の効力は同等とされる．

- レポジトリ
  電子証明書を保管し，利用者が電子証明書を入手できるようにしたデータベース

PKI を利用する際の凡例を，図 2.3 に示す．

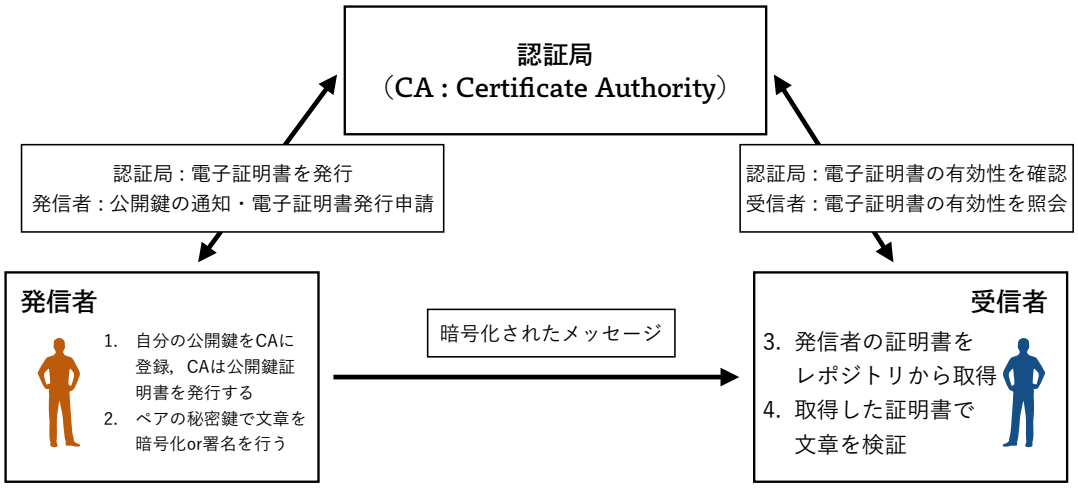

図 2.3: PKI の凡例

2.1.4 暗号技術利用のインタフェース

本項では，前項までに挙げた暗号技術を利用するための，各種規格群・ツールについて説明する．

PKCS

PKCS (Public-Key Cryptography Standards) は，公開鍵暗号に関連するデータ形式などの標準仕様を定めた規格群である．後述するマイナンバーカードで利用される公開鍵暗号技術も PKCS 規格に一部準拠する．

Open SC

Open SC はスマートカードを利用する際に必要な，一連のライブラリ群を提供するプロジェクトである．本研究では，マイナンバーカードとの通信に，Open SC の提供する API を利用する．

2.2 公的個人認証サービス

公的個人認証サービスは，インターネットを通じて行政手続きを行う際に用いられる，本人認証の手段である．本人認証は，電子証明書と呼ばれる電子的な身分証明書を用いて行わ

れる．都道府県知事の発行する電子証明書を耐タンパ性の高い IC カードに記録し，保持する．これを用いて，電子証明書によるユーザ認証や，申請書類等に電子署名を施すことで，本人が送付した情報だと示すことが可能になる [7]．本節では公的個人認証サービスについて制度面と技術面から解説する．

2.2.1 公的個人認証サービスの成り立ち

公的個人認証サービスは，国民等と行政間の申請・届出等手続きを 2003 年度末までにほとんど全てをオンライン化することを決定した “e-Japan 重点計画 2002” に基づき，導入された．同時に根拠法として，行政サービスの電子化に関わる行政手続オンライン化関係三法[2]が制定された [8]．この三法の趣旨を表 2.1 に示す．

表 2.1: 行政手続オンライン化関係三法の概要．[8] を基に作成．

法令名	略称	趣旨
行政手続等における情報通信の技術の利用に関する法律	行政手続オンライン化法	行政手続きを書面に加え，オンラインでも可能とするための法律
行政手続における情報通信技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律	整備法	行政手続オンライン化法で完全に規定できていない部分や例外を扱う
電子署名に係る地方公共団体の認証業務に関する法律	公的個人認証法	高度な個人認証サービスを提供する制度を整備するもの

行政手続きをオンライン化するにあたり，署名又は押印をオンライン上で実現するため，電子署名が必要になった．また，電子署名の活用にあたり確かな本人確認手段が求められ，公的個人認証サービスが設立された．公的個人認証は，オンラインで申請・届出を行った住民が，本当に住民基本台帳に記録されている本人か認証する仕組みであり，住民基本台帳の信頼性を根拠にオンライン上での本人認証を行う仕組みである．

マイナンバー制度以前に公的個人認証サービスを利用するためには，住民は自治体の窓口で住民基本台帳カード[3]を発行し，住基カードの IC チップ内に電子証明書と秘密鍵を格納する手続きをとる必要があった．

2.2.2 マイナンバー制度以後の公的個人認証サービス

従来の公的個人認証サービスにおける電子署名の利用は，前項で取り上げた行政手続オンライン化関係三法の通り，行政手続きをオンライン上で行うためと用途が限られていた．しかし，2013 年にマイナンバー法[4]の関係法律整備法が成立し，公的個人認証法が改正されたことで，サービスの利用範囲が変化した [9]．住基カードとマイナンバーカードの違いについて表 2.2 に示す．なお，表中の基本四情報とは，氏名・性別・住所・生年月日を指す．

まず，マイナンバーカードには電子証明書が標準搭載された．新しく加わった利用者証明用電子証明書は政府の提供するオンラインサイトであるマイナポータルへのログイン認証

[2]第 155 回国会 (平成 14 年 12 月 6 日) において成立，同年 12 月 13 日公布
[3]以下，住基カード
[4]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

表 2.2: 公的個人認証法改正に伴う変更．[10] を基に作成．

格納媒体	住基カード	マイナンバーカード	
電子証明書の種類	旧署名用電子証明書	署名用電子証明書	利用者証明電子証明書
電子証明書の発行者	都道府県知事	J-LIS	J-LIS
電子証明書の内容	基本四情報を含む	基本四情報を含む	基本四情報を含まない
基本四情報に変更がある異動の場合	電子証明書は失効する	電子証明書は失効する	電子証明書は失効しない
カードを紛失し届出した場合	住基カードの一時停止とは別に，電子証明書の失効申請を行う	マイナンバーカードの一時利用停止と連携して，電子証明書も一時保留となる	
カードを廃止した場合	住基カードを廃止しても電子証明書は失効しない	マイナンバーカードの廃止と連携して，電子証明書も失効する	

等に用いられる．用途は本人認証に限られるため，基本四情報は含まれない．公的個人認証サービスの電子証明書については，第 2.2.3 項で詳細を述べる．

次に，民間にも電子署名・電子認証サービスの利用が可能になった．公的個人認証法の改正によって，2017 年 1 月から総務大臣の認可を受け総務大臣認定事業者に認定されることで，マイナンバーカードの電子証明書の検証業務をが可能となった．2017 年 12 月時点での総務大臣認定事業者は 10 社である．

2.2.3 公的個人認証サービスと電子認証基盤

本項では，公的個人認証サービスの全体像と，関係する電子認証基盤について整理する．

公的個人認証サービスの全体像

公的個人認証サービスの全体像を図 2.4 に示した．公的個人認証サービスでは，電子証明書の発行・失効や認証局の役割を**都道府県単位認証局**で担っている．都道府県単位認証局を構成するのは都道府県知事と市区町村長であり，それぞれ以下の役割を担っている．

- **都道府県知事**
  電子証明の発行や失効情報の管理等の認証局の役割
- **市区町村長**
  電子証明書の発行時等における本人確認の役割

しかし，これらの認証業務を都道府県知事が行うのは必ずしも効率的とは言えない．そのため，公的個人認証サービスの電子計算機処理等の事務を委任を可能にする目的で，総務大臣による指定認証機関制度が設けられた．現在，指定認証機関は**地方公共団体情報システム機構**[5]のみで，全都道府県知事から認証事務[6]の委任を受けている [11].

公的個人認証サービスの電子証明書の発行

公的個人認証サービスを利用するには，電子証明書の発行を受ける必要がある．利用者は住民票のある市区町村役場で，マイナンバーカード[7]の IC カードに格納される形で電子証明

[5]J-LIS Japan Agency for Local Authority Information Systems
[6]電子署名に係る地方公共団体の認証業務に関する法律 34 条第 1 項に掲げる認証業務の実施に関する事務
[7]個人番号カード

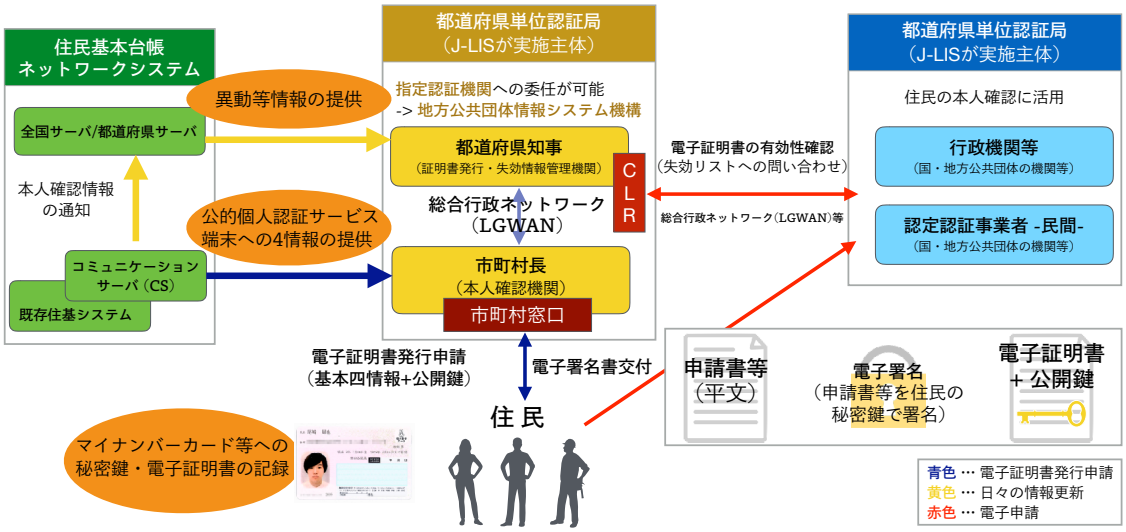

図 2.4: 公的個人認証サービスの概要．[12] を基に作成．

書が交付される．交付までの流れは以下の通りである．

1. 市区町村役場の受付窓口に申請書を記入し，マイナンバーカードと共に提出する．
2. 利用者の本人性の確認をし，窓口に設置された鍵ペア生成装置で公開鍵・秘密鍵を生成する．このとき利用者は，電子証明書に暗証番号の設定を行う．
3. 市区町村長は利用者の基本四情報と利用者の公開鍵を都道府県知事 (認証局サーバ) に通知する．
4. 都道府県知事は電子証明書を発行し，その電子証明書に電子署名を付し，市区町村長に通知する．
5. 都道府県知事の電子署名の付された基本四情報と公開鍵を含む電子証明書及び秘密鍵がマイナンバーカードに格納され，利用者に交付される．

公的個人認証サービスの電子証明書

公的個人認証サービスでは，2 種類の電子証明書が提供される．**署名用電子証明書**と**利用者証明用電子証明書**の 2 つである．図 2.5 に利用者クライアントソフト[8]を用いて表示した，公的個人認証サービスの電子証明書を示す．

署名用電子証明書と利用者証明用電子証明書の違いは，その利用用途と基本四情報を含むか否かである．両者の使用用途について，以下の通りである．

- **署名用電子証明書**
  基本四情報を含む．署名捺印が必要となる行政手続き等を行う際に，署名用電子証明

[8]電子証明書を利用した行政サービスを利用する際に必要となる，J-LIS が提供するソフトウェア https://www.jpki.go.jp/download/

(a) 署名用電子証明書　　(b) 利用者証明用電子証明書

図 2.5: 公的個人認証サービスの電子証明書

書を用いて電子申請を行う．電子文章の作成・送信者が利用者本人である，本人性確認に用いられる．

- **利用者証明用電子証明書**
  基本四情報を含まない．Web サービス等の利用者認証に用いられる．具体的には，マイナポータルへのログインやコンビニでの公的な文章の交付に用いられる．

公的個人認証サービスの電子証明書の検証

電子証明書の署名検証が必要となる場面は 2 通りある．行政機関が利用者の電子証明書の検証を行う場合と，利用者が行政機関等の官職証明書及び職責証明書を検証する場合である．

利用者の証明書を検証は，公的個人認証法第 17 条に定められた，署名検証者のみが可能である．行政機関，裁判所や総務大臣に認定を受けた民間事業者である総務大臣認定事業者がこれに当たる．電子証明書が失効するとして，利用者の IC カードの紛失や利用者の死亡がある．失効情報の確認方法は 2 方法ある．

- **OCSP レスポンダ方式**[9]
  指定された証明書の有効性の照会について，応答用のサーバから個別に状態を署名つきで応答する．
- **CRL**[10]
  失効情報の一覧を定期的にまとめて提供する．

次に利用者が公的機関等からの書類等を検証する場合では，官職証明書の検証が必要になる．公的個人認証サービスでは検証が行えないため，ブリッジ認証局を通して総合行政ネットワーク経由で政府認証基盤から証明書の検証を行う．この認証基盤の連携について図 2.6 に図示する．

[9]Online Certificate Status Protocol
[10]Certificate Revocation List

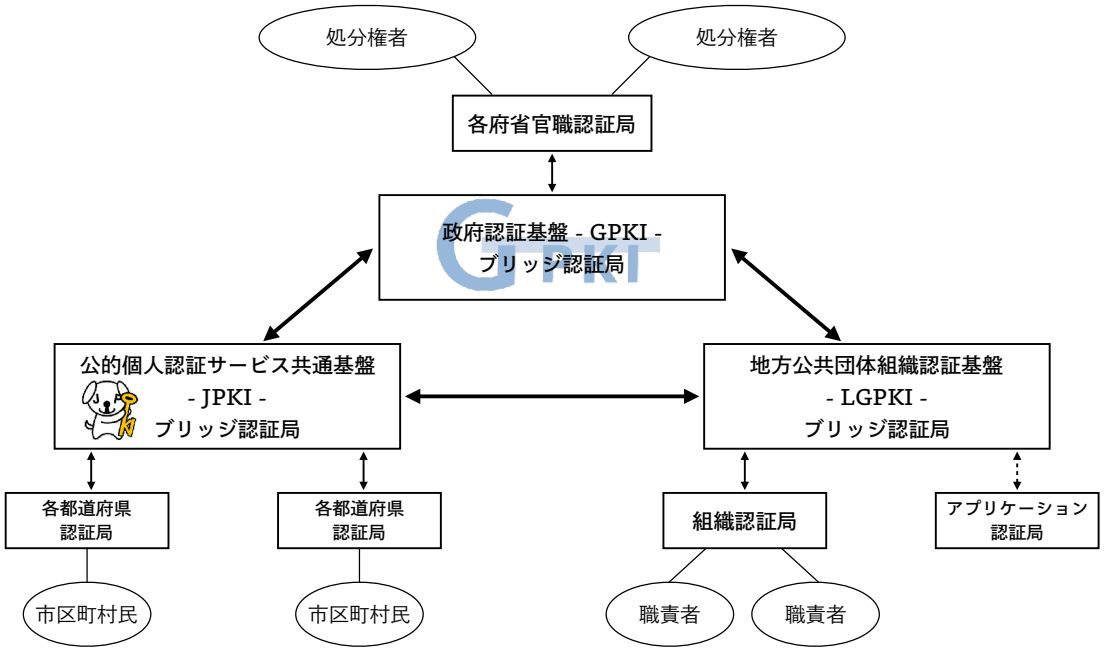

図 2.6: 電子認証基盤の構造．[9] を基に作成．

電子証明書の発行方針

表 2.3 に電子証明書の発行方針を示す．電子証明書の発行は，マイナンバーカードの所有者の年齢によって制限されており，既存の住基カードの方針を踏襲する．

表 2.3: 電子証明書の発行方針．[13] を参考に作成．

カードの発行年齢	署名用電子証明書	利用者証明用電子証明書	カードの有効期間
20 歳以上	発行する	発行する	10 回目の誕生日
20 歳以上 ~20 歳未満	発行する	発行する	5 回目の誕生日
15 歳未満	発行しない[a]	発行する[b]	5 回目の誕生日[c]

[a] 15 歳未満については，現行制度と同様に署名用電子証明書を原則発行しない (実印に相当するため)
[b] 15 歳未満については，法定代理人がパスワードを設定する
[c] 20 歳未満については，容姿の変動が大きいことから，顔写真を考慮して 5 回目の誕生日とする

2.3 マイナンバーとマイナンバーカード

マイナンバーとマイナンバーカードは報道機関においても，しばしば用語の混同が散見される [14]．本節では，マイナンバーとマイナンバーカードについて，制度とその技術面を整理する．

2.3.1 マイナンバー制度

マイナンバーは，社会保障・税・災害対策の分野で，住民の個人情報を効率的に管理するための社会基盤として導入された．日本国内に住民票を有する者[11]に悉皆に付番される，重複しない 12 桁の番号である [15] [16]．マイナンバー制度の特徴は，次の 3 点に象徴される．

- **付番**
  悉皆かつ，唯一無二で，基本四情報と結びついた個人番号である．
- **情報連携**
  複数の機関において，同一人情報を紐付けし，相互活用する．
- **本人確認**
  個人が自分であることの証明，個人番号の真正性を証明する．

マイナンバー制度の成り立ち

マイナンバー制度の嚆矢は，“平成 22 年度税制改正大綱” で言及された納税者番号としての番号制度の導入にある．番号制度は，2010 年 2 月からの社会保障・税に関わる番号制度に関する検討会から社会保障の分野での利用も検討され，2011 年 1 月に政府・与党社会保障改革検討本部で “社会保障・税に関わる番号制度についての基本方針” が策定された．2012 年 1 月には “社会保障・税一体改革素” が決定され閣議報告された．第 180 回国会に，マイナンバー関連三法案[12]が提出されるが衆議院解散により廃案．2013 年 3 月にマイナンバー関連四法案が閣議決定され，第 183 回国会に再提出され，同年 5 月 24 日に成立した [17] [18]．マイナンバー関連四法案について表 2.4 にまとめた．

表 2.4: マイナンバー関連四法案の概要．[19] を参考に作成．

法令名	略称	趣旨
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	マイナンバー法	マイナンバー・マイナンバーカードの定義，またその利用方法について
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の施行に伴う関係法律の整備等に関する法律	番号法整備法	マイナンバーを行政で利用できるよう，関連法案を整備
地方公共団体情報システム機構法	機構法	マイナンバーを用いた認証業務の実現
内閣法等の一部を改正する法律	政府 CIO 法	政府全体の IT 政策を統括する CIO の設置，情報提携ネットワークの整備

[11] マイナンバーは日本国内に住民票があれば，外国籍でも付番される．日本国籍でも住民票がない場合は，付番されない．

[12] 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案・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の施行に伴う関係法律の整備等に関する法律案・地方公共団体情報システム機構法案

情報提供ネットワークシステム

マイナンバーは個人を特定の番号を用いて名寄せすることで行政の効率化を狙うものであり，個人情報保護の観点から情報連携時に直接マイナンバーが利用されることはない．行政間で情報を連携する際には，情報ネットワークシステムを経由し，やりとりが記録される．

情報連携には，マイナンバーではない符号が用いられ，各情報機関ごとにマイナンバーに対応した符号が発行される．その符号を情報ネットワークシステムを経由して照会することで，情報連携を可能にする．図 2.7 に情報連携の仕組みを示す．

また，連携のすべての記録は**マイナポータル**[13]から本人が確認することができる．

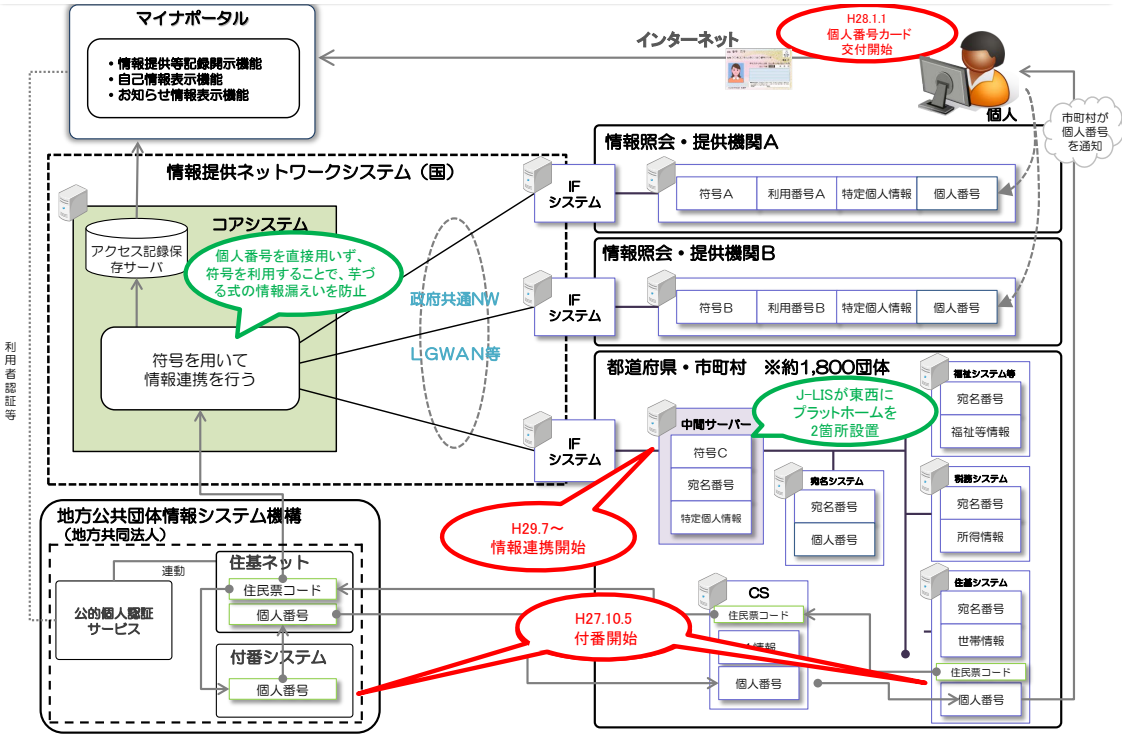

図 2.7: 情報連携の仕組み．[20] より引用．

2.3.2　マイナンバーカード

マイナンバーカードは，マイナンバーを持つ住民が申請すると無料で取得できるプラスチック製のカードである．カードの発行は J-LIS が一括して代行している．また，マイナンバーカードには IC チップと電子証明書が搭載されており，公的な身分証明書として利用できる IC カードでもある．マイナンバーカードの券面と，その技術仕様について述べる．

[13] https://myna.go.jp/

マイナンバーカードの券面

マイナンバーカードの表面には，基本四情報・顔写真・電子証明書の有効期限の記載欄・サインパネル領域[14]・セキュリティコード・臓器提供意思表示欄が記載される．裏面には，個人番号 (マイナンバー)・氏名・生年月日が記載されている．券面を図 2.8 に示す．いずれも八戸市 Web サイト [21] から引用した．

(a) マイナンバカードの表面　　(b) マイナンバカードの裏面

図 2.8: マイナンバーカードの券面

マイナンバーカードは，身分証明書として利用できるが，マイナンバーをコピー・保管できる事業者は法令により制限されており，みだりに個人番号が記載されている裏面をコピー・保管することはできない．

マイナンバーカードの技術仕様

マイナンバーカードは裏面に IC チップの端子を持つほか，非接触でも利用できるインタフェースを持つコンビネーション型の IC カードである．接触インタフェースは，ISO/IEC 7816 に準拠し，非接触インタフェースは ISO/IEC 14443 Type B に準拠している [22]．非接触インタフェースの分類を表 2.5 に示す．

表 2.5: 非接触インタフェースの分類．[22] を参考に作成．

分類	準拠規格	概要	利用例
Type A	ISO/IEC 14443 ISO/IEC 18092	低機能，小容量なカードが主流	taspo
Type B	ISO/IEC 14443	高機能，高セキュリティなカードが主流で PKI に対応したものも多い	住基カード・パスポート・運転免許証
Felica	ISO/IEC 18092	低機能，小容量なカードが主流．価格も安く高速処理ができる	Suica・楽 天　Edy・nanaco

[14]住所変更が生じた際等に使用される

マイナンバーカードの IC チップには，カード OS と呼ばれる IC チップ専用の OS が搭載されている．マイナンバーカードには 4 種類のカードアプリケーション (以下，カード AP) が搭載されており，カード OS はカード AP を制御する．図 2.9 にマイナンバーカードの内部構成を示す．表 2.6 にそれぞれのカード AP の機能をまとめた．

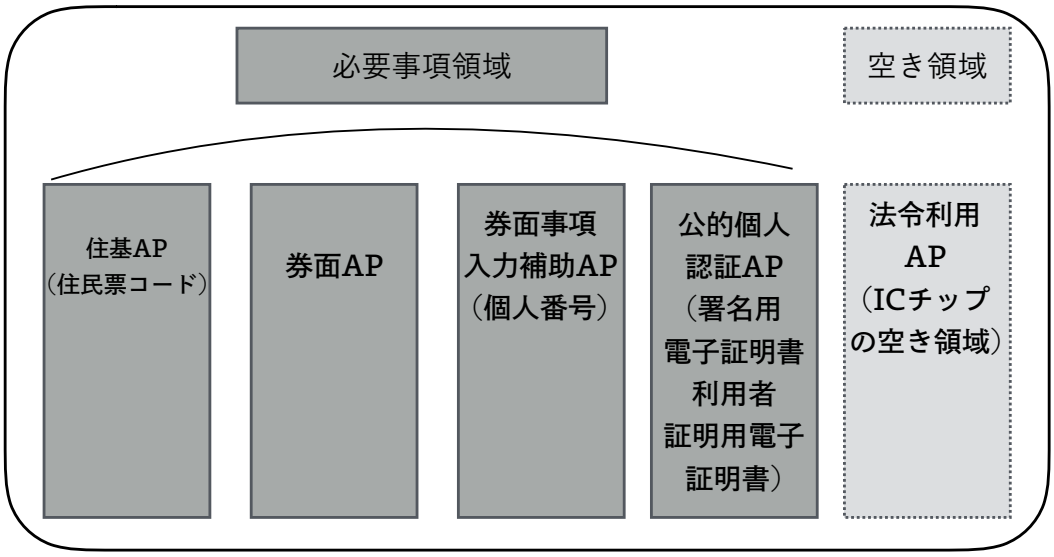

図 2.9: マイナンバーカードの内部構成．[23] を基に作成．

表 2.6: カード AP の機能

カード AP	利用目的	セキュリティ
公的個人認証 AP	署名用電子証明書 電子申請に利用	暗証番号：6~16 桁の英数字
	利用者証明用電子証明書 マイナポータルのログイン等に利用	暗証番号：4 桁の数字
券面 AP	券面の偽変造の有無の確認	基本四情報・顔写真・マイナンバーの画像を格納
券面事項入力補助 AP	マイナンバー・基本四情報の利用	4 桁の暗証番号や券面記載情報の入力
住基 AP	住民票コードを記録	4 桁の暗証番号

2.4 ブロックチェーン技術

ブロックチェーンは Bitcoin [24] の決済管理の基幹技術として開発された，分散型台帳技術の一種である．ブロックチェーンでは，取引記録はチェーン状に連なり管理される．記録の編集・削除も記録され，取引の整合性が確認可能な仕組みである．また全取引記録は，ブロックチェーンのネットワークに参加する全ての参加者により検証・保管されている．

本節では，Bitcoin ブロックチェーンを下敷きに，ブロックチェーンの要素技術について整理する．

2.4.1 ブロックチェーンの構造とトランザクション

ブロックチェーンの構造

ブロックチェーンは，分散型台帳技術の一つであり，データのブロックがチェーン状に連なるさまからブロックチェーンと呼ばれる．図 2.10 にブロックチェーンのデータ構造を示す．

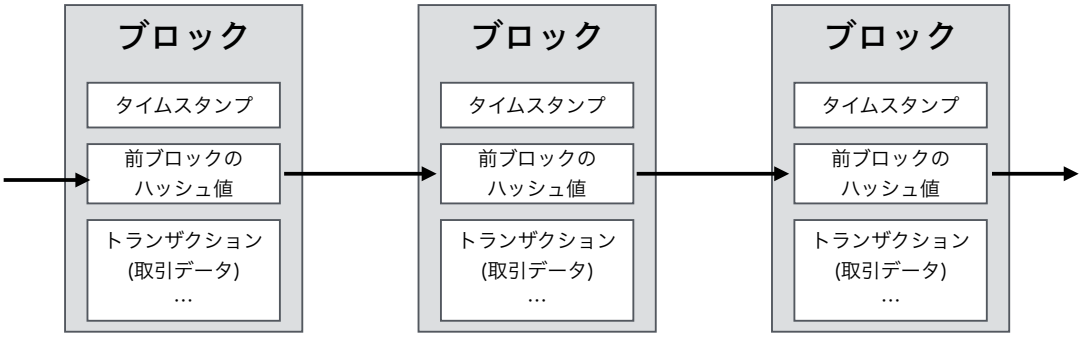

図 2.10: ブロックチェーンのデータ構造

ブロックには，一定の期間内に承認されたトランザクションと呼ばれる取引記録が格納され，時系列で繋がれる．全てのブロックはその生成時に．一つ前に連なるブロックの ID を保持する．どのブロックからブロックチェーンを辿っても，最初に生成されたブロックである Genesis ブロックに繋がる構造を持つ．

トランザクション

トランザクションとは，ブロックチェーンに記録されるデータの最小構造のことである．トランザクションのデータ構造は，インプット・アウトプットの 2 つによって構成される．インプットは資金源，アウトプットは送金先を意味する．

アウトプットには，未使用状態と使用済み状態の 2 つが存在する．未使用状態のアウトプットのことを，UTXO(Unspent Transaction Output) と呼ぶ．未使用状態のアウトプット，つまり UTXO はこれからインプットとして指定できるトランザクションである．

2.4.2 基盤となる暗号技術 –一方向ハッシュ関数と電子署名–

一方向ハッシュ関数

一方向ハッシュ関数とは，与えられた入力に対して固定長のハッシュ値を導出する関数のことである．一方向ハッシュ関数は以下のような性質を持つ．

- 任意長の入力 (メッセージ) から固定長のハッシュ値を導く．
- 入力 (メッセージ) の導出が不可能な固定長のハッシュ値を生成する．
- 入力 (メッセージ) が異なると，全く異なるハッシュ値を生成する．

ブロックチェーンにおける一方向ハッシュ関数は，データの真正性担保の目的で利用される．ブロックチェーンはブロックを生成する際に，一つ前のブロックのハッシュ値を計算し，ブロックに取り込む．ブロックの内容を偽造・改ざんしようとすると，改ざんしたブロック以降のブロックのハッシュ値が一方向ハッシュ関数の性質から全て変化する．そのため，改ざんを成功させるには，後に連なる全てのブロックのハッシュ値を再計算する必要がある．一方向ハッシュ関数の，入力が異なると異なるハッシュ値を生成する性質を利用し，ブロックの偽造・改ざんを困難にしている．

電子署名

電子署名の技術については，第 2.1.2 項で述べたとおりである．本項では，ブロックチェーンにおける電子署名の役割について説明する．

UTXO はそのままではロックされており，使用できない状態になっている．この UTXO をアンロックする方法として，電子署名が用いられる．UTXO をアウトプットに利用する際に利用者は，自分の秘密鍵を用いて電子署名を行い，UTXO をアンロックする．また同時に，自分の公開鍵をトランザクションに付すことで，第三者による署名の検証を可能にする．

2.4.3 P2P ネットワーク

P2P とは peer-to-peer の略記で，クライアント・サーバが対等な立場で通信を行う自立分散型のネットワークモデルである．クライアント・サーバ型モデルでは，各ノードの役割はデータを要求・アクセスするクライアント側，データを保持・提供するサーバ側に明確に別れる．一方 P2P では，各ノードはクライアント・サーバ双方の役割を果たし，ネットワークに参加するノード全体によってサービスが提供される．

ブロックチェーンでは，サービスの維持を P2P ネットワーク上で行なっている．トランザクションの変更があった際は，その変更はネットワークに参加するノード全てに共有される．これをブロードキャストと呼ぶ．

2.4.4 コンセンサスアルゴリズム

P2P ネットワークでは，各ノードの情報伝達のスピードにタイムラグがある．タイムラグにより，ノードによって異なったブロックが共有される可能性がある．各ノードにおける情報の揺れをただし，同一の結果に収束させるのがコンセンサスアルゴリズムの役割である．コンセンサスアルゴリズムは複数あり本項では，Bitcoin や Ethereum で採用されているコンセンサスアルゴリズムの PoW について説明する．

PoW(Proof of Work) は，計算量に応じてコンセンサスの決定権を与えるアルゴリズムである．膨大なコストがかかる計算問題を参加者に課し，はじめに問題をといた参加者に報酬 (ブロック) が与えられる．具体的には，特定の結果になるまでハッシュ計算を行わせ，はじめに特定の結果を得られた参加者に報酬を与えている[15]．

2.4.5 スマートコントラクト

スマートコントラクトは 1994 年に Nick Szabo が提唱した概念である [25]．スマートコントラクトとは，複数人が合意した契約を自動履行すること[16]を意味する．ブロックチェーンの文脈で述べると，ブロックチェーン上に契約履行の条件が改ざん不可能に定義され，条件が満たされると自動的に履行されるトランザクションと言える．

2.4.6 Ethereum

Ethereum は Ethereum Foundation が開発するブロックチェーンを利用した分散型アプリケーションの開発基盤である [26]．Ethereum ではコントラクトと呼ばれるコードをブロックチェーンに格納し，実行可能である．

Ethereum で実行されるスマートコントラクトは，EVM Code(Ethereum Virtual Machine Code) と呼ばれる低水準の機械言語で記述される．Ethereum プロジェクトは高水準言語でのスマートコントラクト記述のために，Solidity [27] に代表されるスマートコントラクト記述言語とそのコンパイラを提供する．

Ethereum Swarm

Ethereum Swarm[17]は，分散型ファイル共有サービスである．Ethereum Swarm は Ethereum ネットワークを用いて，改ざんが不可能な形で不特定多数のノードにファイルを分散配布する．個々のファイルの保管場所はエンドユーザーからは秘匿されるが，ファイルそのものには通常のアップローダと同様にアクセス可能である．

[15]Bitcoin ブロックチェーンでは，上位ビットに 0 が並ぶ数値を導出できるように計算をする．
[16]Szabo は契約を機械で自動履行する仕組みであるスマートコントラクトの例として，自動販売機を例示している．
[17]https://github.com/ethersphere/swarm

2.5 本章のまとめ

本章では，基礎的な暗号技術と，本研究の要素技術となる公的個人認証サービスとブロックチェーン技術について整理した．第 4 章より，本章で整理した技術を用いたシステムを提案する．

第3章　先行事例・研究

本章では，本研究に関係する公的個人認証サービスと，ブロックチェーン技術の先行研究について整理する．

3.1　先行研究

3.1.1　公的個人認証サービスを用いた電子署名

公的個人認証サービスの電子証明書を用いて電子署名を行う先行研究として，金子 [28] のものがある．この研究では，マイナンバーカードに搭載されている利用者証明用電子証明書を用いて電子署名を行なっている．システム構成図を図 3.1 に示す．

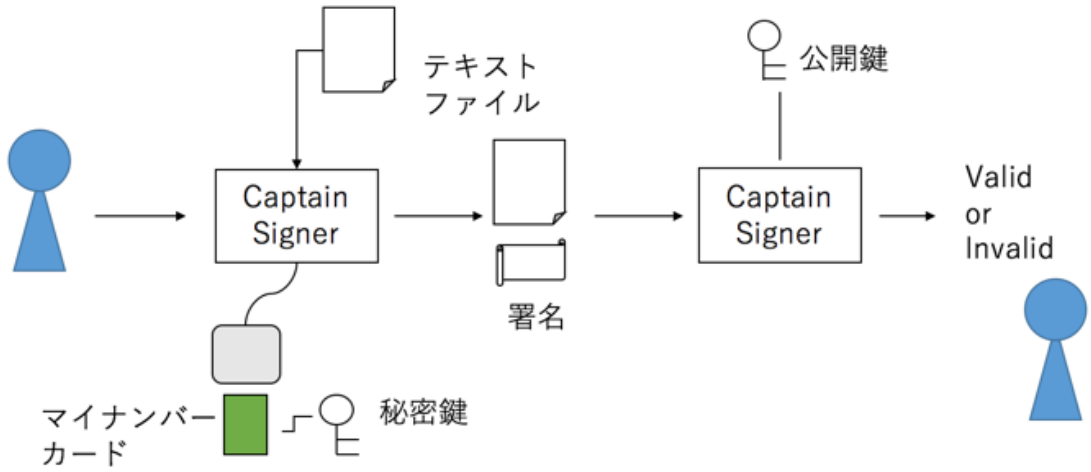

図 3.1: システム構成図．[28] より引用．

3.1.2　公的個人認証サービスとブロックチェーンを用いた本人性確認

公的個人認証サービスとブロックチェーンを用いて本人性確認を行なっている先行研究として，2017 年に永田らが行なったものがある [29]．この研究では，Bitcoin のトランザクションを利用し，実行者の本人性の確認を検討している．

具体的には，署名検証者として総務省認定事業者が存在すると仮定し，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を発行し，ブロックチェーン上に記録するものである．図 3.2 にシステムの概要図を示す．

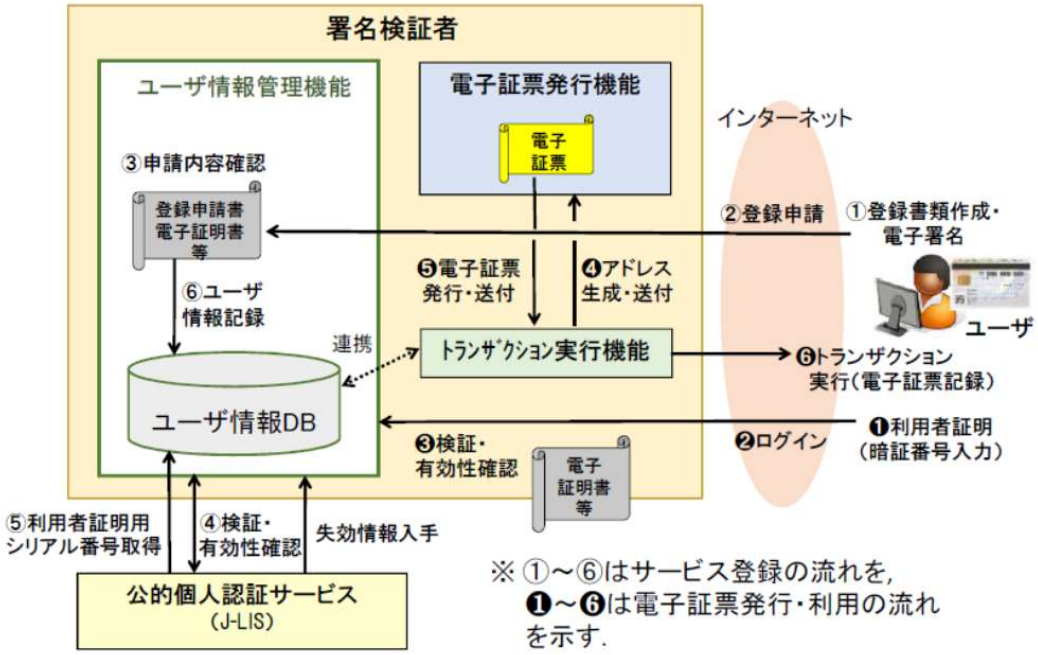

図 3.2: 電子帳票発行サービスの概要．[29] より引用．

3.1.3 スマートコントラクトを用いた権利移譲

カーシェアリングシステム

Ethereum のスマートコントラクトを用いた権利移譲の研究に，大上らの研究 [30] がある．この研究では，第 3 者機関を置くことなくカーシェアを実現するために，Ethereum によるスマートコントラクトを利用している．貸与者の車所有権・借用者の個人情報は，保証機関を通じて Ethereum アカウントに紐づいた形でブロックチェーン上に公開される．貸与権・借用権をそれぞれ相手に預け，コントラクトをデプロイする形である．

売買契約

スマートコントラクトによる土地の売買の研究として斉藤の研究 [31] がある．斉藤の示すモデルでは，売主が土地の権利を，買主が土地の代金を，それぞれ自動化された売買契約のスマートコントラクトに預託し，双方が揃った状態でのみ売買を実行する．図 3.3 にスマートコントラクトによる土地売買の概要を示す．

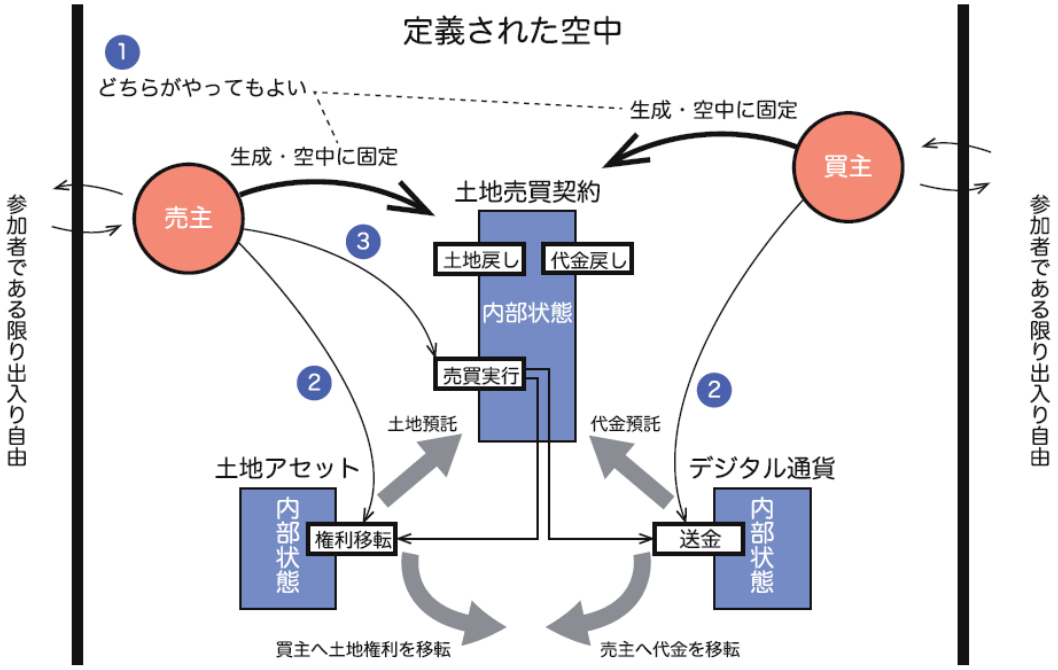

図 3.3: 自動エスクローによる土地売買．[31] より引用．

3.2 本章のまとめ

本章では，公的個人認証サービス・スマートコントラクトを利用した先行研究を整理した．

第4章　公的個人認証サービスを用いたスマートエスクロー

本章では，本研究で提案する公的個人認証サービスを用いたスマートエスクローについて述べる．

4.1　商取引における信用の問題

第 1 章でも述べたように，商取引の方法の変化と印刷技術の発達により，取引の信頼性が問題になっている．本研究では，取り上げる取引の問題として 2 点取り上げる．契約の不履行と本人性確認の問題である．

まず，契約の不履行の問題だが，次のような問題が考えられる．土地の取引を行う際に，

- 売主が土地の代金を受け取ったが土地を権利を以上しない
- 売主が土地の権利を以上したが購入者が代金を支払わない

といった場合がある．また，電子商取引であるネットオークションを例にすると，契約と所有権の移転が異なる場所・時間で行われるため，契約遵守の点にリスクが存在する．そこで理想的な取引の形としては，売り・買いの契約は不可分な履行が求められる．

次に本人性確認については，署名捺印を用いた本人確認の危殆化が指摘されている [2]．紙による取引では，本人確認に署名捺印が用いられる．しかし印刷技術の発達により，筆跡や陰影の偽造は容易になっている．また電子商取引では，Web サイト上のプロフィールなど相手に関する情報は限られたもので本人性確認は難しく，取引のリスクは高まる．

4.2　問題解決へのアプローチ

契約の不履行・本人性確認の問題に対し，本研究では公的個人認証サービスを用いたスマートエスクローを提案する．本手法は，契約の履行をスマートコントラクトによるエスクロー，そのアドレス交換に公的個人認証サービスを用いることで，前述の問題の解決を目指す．次項から，本提案手法の機能要件を示す．

4.2.1　定められた契約の自動履行 -スマートコントラクト-

契約の不履行の問題は，売り・買いの契約の不可分な履行によって解決される．本論文では，この売買が不可分に実行される契約のことを，スマートエスクローと呼称する．契約の

不履行を防ぐ仕組みとして，信頼できる第三者に契約を預託するエスクローがある．エスクローを用いると，契約を仲介する第三者が売り手・買い手以外にも必要になり，人的コスト・契約を確認する時間的コスト等が要される．

そのため本提案手法では，スマートエスクローを実現する方法としてエスクローではなく，スマートコントラクトを採用する．スマートコントラクトとは，プログラム化された契約を自動履行する仕組みであり，スマートコントラクトを用いればスマートエスクローを実現できる．スマートコントラクトを用いたスマートエスクローにより，エスクローを用いた際に必要とされた人的・時間的コストを軽減できる．

4.2.2 本人性確認 -公的個人認証サービス-

スマートエスクローをスマートコントラクトを用いて，プログラムとして実現するためには，オンライン上での本人性確認が必要となる．スマートコントラクトを用いる際に，取引相手とコントラクトアドレスの交換を行うが，そのアドレスが意図している契約相手のものである保証はない．ブロックチェーン上の秘密鍵・公開鍵ペアの真正性では，本人性確認ができない．

そこで，本提案手法では公的個人認証サービスを用いたアドレス交換を提案する．コントラクトアドレスに公的個人認証サービスを用いて署名を付し[1]，その署名を検証できる形で公開する．公的個人認証サービスを用いて署名を行うことは，J-LIS によって認証された鍵ペアを利用することであり，本人性確認が J-LIS によって担保される．

4.3 本章のまとめ

本章では，商取引における信用の問題を，スマートコントラクトによるスマートエスクローと公的個人認証サービスを用いた本人性確認を用いることでの解決を提案した．

[1]以後，署名付きアドレスと呼ぶ．

第5章　実装

5.1　システムの設計

本節では，第 4 章で提案した公的個人認証サービスを用いたスマートコントラクトの設計について述べる．図 5.1 に提案システムの図を示す．

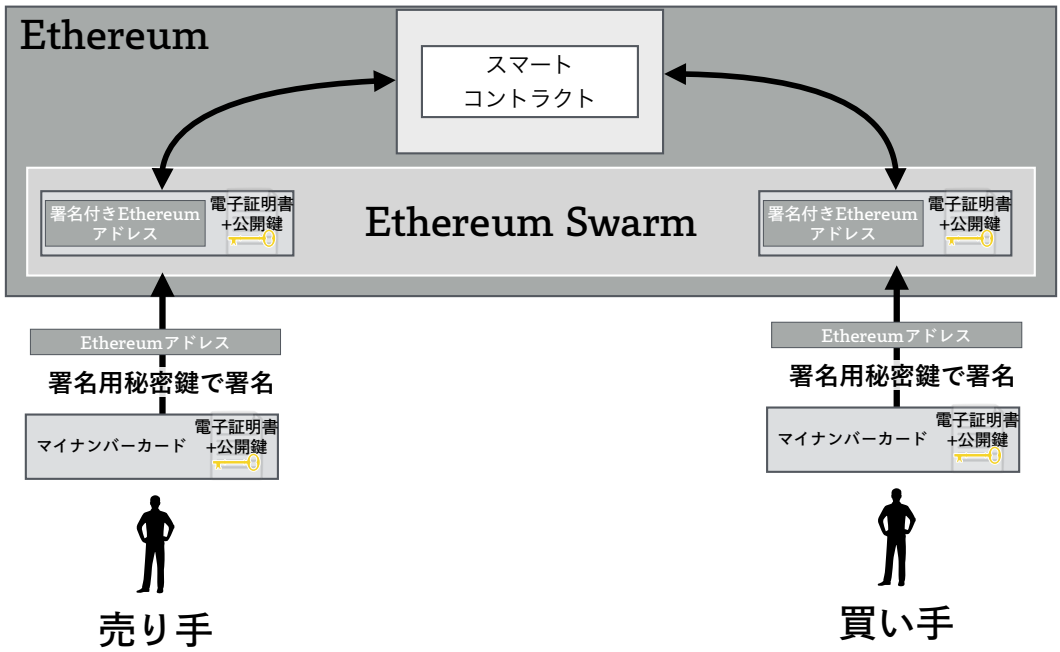

図 5.1: 提案システムの概要図

本システムはその機能から，アドレス登録部とスマートコントラクト部に分類される．アドレス登録部では，マイナンバーカードを用いて Ethereum アドレスを暗号化し，Ethereum Swarm 上で暗号化されたアドレスを共有可能にする．スマートコントラクト部では，商品に見立てたトークンに対し設定金額以上の送金があった際に，契約の履行を行う．

5.2　アドレス登録部

アドレス登録部では，マイナンバカードの署名用秘密鍵による取引に用いる Ethereum アドレスへの署名，鍵ペアの公開鍵・署名用電子証明書による署名の検証により，利用者同士のセキュアな Ethereum アドレスの交換を可能にする．まず，図 5.2 にアドレス登録部の構成図を示す．

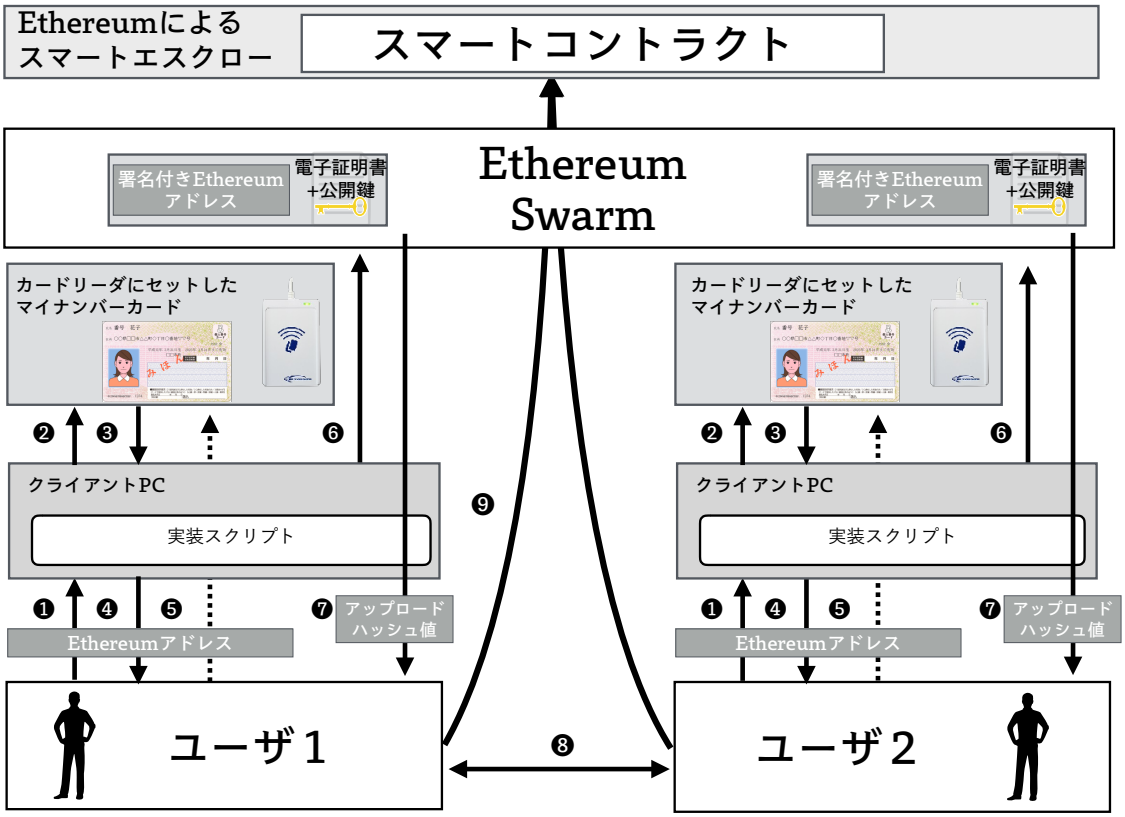

図 5.2: アドレス登録部の構成図

アドレス登録部の動作の手順は，次の通りである．

❶ Ethereum アドレスの暗号化を，実装スクリプトに要求する．
❷ 実装スクリプトは，マイナンバーカードに，アドレスへの署名・公開鍵・署名用電子証明書を要求する．
❸ マイナンバーカードは，公開鍵・署名用電子証明書を渡し，PIN コードの入力を求める．
❹ 実装スクリプトは，マイナンバーからの，PIN コードの入力をユーザに通知する．
❺ ユーザは実装スクリプトを通し，PIN コードを入力する．
❻ 実装スクリプトは，署名付きアドレス・公開鍵・署名用電子証明書を Ethereum Swarm にアップロードする．
❼ 実装スクリプトは，Ethereum Swarm へのアップロードにより得られたハッシュ値を，ユーザに通知する．
❽ ユーザは安全な経路を用いて，ハッシュ値を取引相手と交換する．
❾ 交換したアドレスをもとに，スマートエスクローを実行する．

次に，図 5.3 にアドレス登録部のシーケンス図を示す．

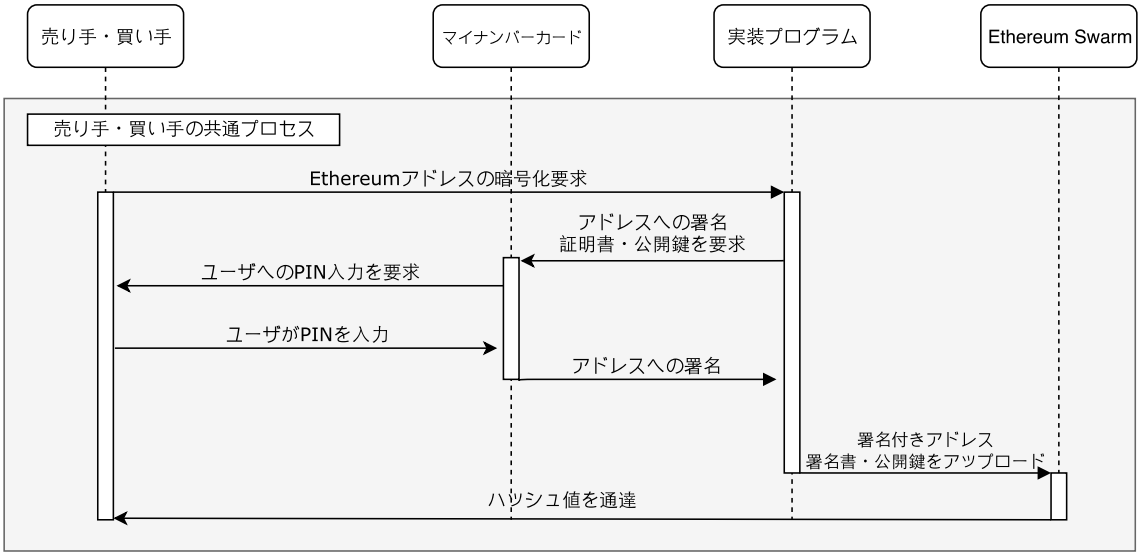

図 5.3: アドレス登録部のシーケンス図

取引に用いる Ethereum アドレスの暗号化は，売り手・書い手ともに必要となるため，両者とも同様の流れで Ethereum アドレスの暗号化を行う．本システムでは，暗号化としてマイナンバーカードの署名用秘密鍵で，Ethereum アドレスに署名を行う．また，署名の検証には署名用公開鍵と，その公開鍵を証明する署名用電子証明書が必要になる．本システムでアップロードするファイルは，以下の 3 点である．

- **Ethereum アドレス**
  署名用電子証明書の秘密鍵で署名される．
- **署名用公開鍵**
  署名検証に使用される．
- **署名用電子証明書**
  本人性確認のために使用される．

また本提案手法では，アップロードファイルの完全性を担保するため，分散ファイルストレージサービスの Ethereum Swarm にファイルをアップロードする．Ethereum ネットワークの P2P の特性から，可用性も向上する．表 5.1 に，一般的なインターネットを用いたファイルのアップロードと，Ethereum Swarm を利用した際の可用性の比較を示す．なお本研究では，得られた Ethereum Swarm のハッシュ値は，安全な経路で交換するものとする．

表 5.1: ファイルアップロードの可用性の比較

	中央集権のファイル共有サービス	Ethereum Swarm
DDoS 耐性	DDoS 攻撃が容易	DDoS 攻撃耐性がある
稼働率	メンテナンスや障害による動作不能時間がある	P2P によるゼロダウンタイム
信頼性	システムエラーの可能性	フォールトトレランスがある

5.3 スマートコントラクト部

スマートコントラクト部では，アドレス登録部で登録した署名付きアドレスを用いてスマートエスクローを実行する．図 5.4 にスマートコントラクト部のシーケンス図を示す．

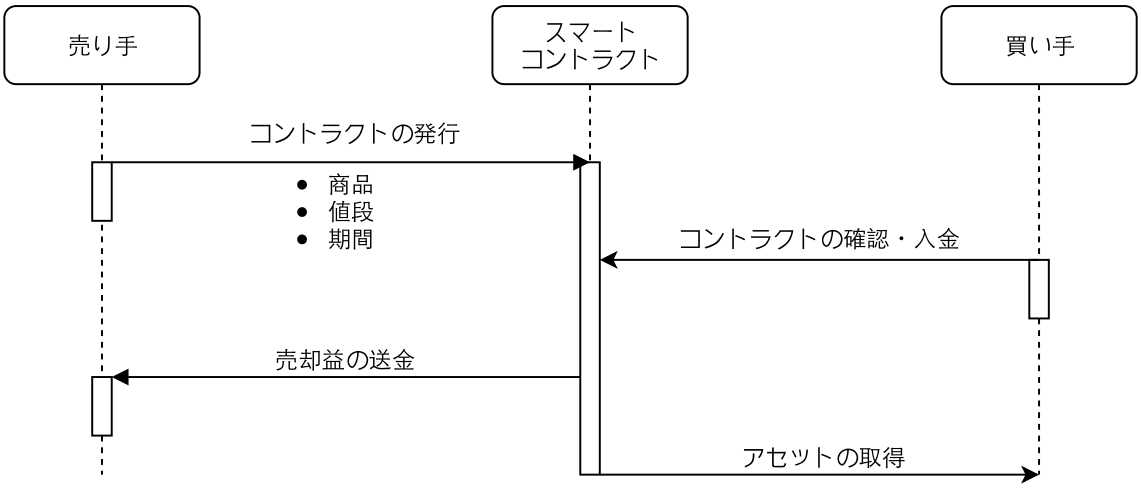

図 5.4: スマートコントラクト部のシーケンス図

本システムでは，スマートエスクローとしてのスマートコントラクトを，トークンを模擬商品と見立て，Ether と交換を行うコントラクトを設計した．コントラクトの処理の流れは，以下の通りである．

1. 売り手は，トークン・販売価格・期間を設定しコントラクトを発行．
2. 買い手は，コントラクトを確認し，送金を行う．
3. 送金量が販売価格に達していたら，コントラクトが実行される．
4. トークンが買い手に，Ether が売り手に送金され，コントラクトが破棄される．

5.4 開発環境

本システムは，表 5.2 に示す開発環境で開発された．署名・証明書の検証等の暗号化関数の利用は，OpenSSL [32] を利用した．マイナンバーカードと通信には，スマートカード利用のミドルウェアである OpenSC [33] を用いた．スマートコントラクト実行環境としては，Go 言語による Ethereum インタフェースである Geth [34]，コントラクト記述には Solidity [27] を使用した．

5.5 本章のまとめ

本章では，提案システムの実装方法を示した．実装における設計，各モジュールの処理の流れ，公的個人認証サービスの利用方法，スマートコントラクトの実装に用いた開発環境について説明した．

表 5.2: 開発環境

ソフトウェア	実装環境	バージョン
カードリーダー	ACR1251-NTTCom	–
暗号ライブラリ	OpenSSL	1.1.0g
暗号ライブラリ	OpenSC	0.16.0-314-g6430f089
ブロックチェーンクライアント	Geth	1.7.3-stable
コントラクト記述言語	Solidity	0.4.19+commit.c4cbbb05.Emscripten.clang

第6章　評価

6.1　機能要件における定性的評価

6.1.1　本人性確認

本提案システムでは，公的個人認証サービスと Ethereum Swarm を利用して，Ethereum アドレスの交換を行う．そのため，マイナンバーカードを用いて，スマートコントラクを利用者の Ethereum アドレスに署名をし，署名付きアドレス・公開鍵・署名用電子証明書を Ethereum Swarm にアップロードした．Ethereum Swarm 得られたハッシュ値をもとに，再度ファイルをダウンロードし，署名付きアドレスを公開鍵で復号した結果，正しい Ethereum アドレスが取得できることを確認した．

公的個人認証サービスと Ethereum Swarm を用いることで，本人性確認が可能な状態で Ethereum アドレスの交換を実現した．

6.1.2　契約の自動履行

本論文で定義するスマートエスクローの実行のため，第 5.3 節でスマートコントラクトを設計した．定義したコントラクトに，契約が実行されるよう送金を行うと，コントラクトが実行されることを確認した．

提案手法のスマートコントラクトを用いることで，スマートエスクローの実行を実現した．

6.2　既存の取引手法との比較

本節では，既存の取引手法と提案手法を比較し，提案手法が実用性を有するか検討する．契約手法の比較表を，表 6.1 に示す．

表 6.1: 契約手法の比較

	対面式取引	ネットオークション・フリーマケット	エスクロー	提案手法
本人性確認	場合による	×	○	○
契約履行リスク	×	エスクローを一部サービスが提供	○	○
取引時間	場合による	×	×	○
取引コスト (煩雑さ)	場合による	×	×	○
第三者取引コスト	–	–	×	○

本人性確認

本人性確認については，確実に行えるのは第三者が取引相手の精査を行うエスクローと，公的個人認証サービスによって本人認証が行われる提案手法の 2 つである．対面式取引は，相手との関係に本人確認の信頼性を依存する．また，ネットオークションでは相手の提示する情報を無条件に信頼せざるをえない．

契約履行のリスク

契約履行のリスクも，第三者により取引を仲介するエスクローと，スマートエスクローを実現する本提案手法の 2 つの方式がリスクを逓減可能である．ネットオークション・フリーマーケットの一部には，エスクローサービスが導入されている．また対面式取引では，契約履行リスクは取引相手に依る．

取引時間

取引時間は，スマートエスクローを実行する本提案手法が最も迅速に取引を完了できる．その他の取引方法は，取引相手・場合に取引時間が左右される．

取引コスト

取引のコストだが，提案手法が最も少ない．スマートコントラクトによるスマートエスクローの実行により，設定されたコントラクト以外の取引を考慮する必要がないためである．その他の取引方法は，時と場合に，取引コストが左右される．

第三者取引コスト

第三者取引コストが関係するのは，提案手法とエスクローである．エスクローでは，取引に預託を行う第三者が必要なため，預託者という取引コストが発生する．提案手法では，スマートコントラクトという仕組みに預託するため，コストを増やさず第三者取引を実現可能である．

6.3 本章のまとめ

本章では，機能要件における評価によって，提案システムが，第 4 章で提案した機能要件を満たしていることかを示した．そして提案システムの実装が，第 4 章で述べた機能要件を満たしていることを示した．また，既存の取引手法と提案手法を比較し，提案手法が実用性を有することを確認した．

第7章　結論

7.1　本研究のまとめ

本研究では，商取引の複雑化によるトラブルに着目し，その問題として契約の不履行・本人性確認を設定した．問題解決のアプローチとして，公的個人認証サービスを用いたスマートエスクローシステムを提案・実装した．

提案システムでは，契約の履行へのアプローチとしてスマートコントラクトを用いたスマートエスクローを設計し，売買契約が不可分に実行されることを確認した．また，本人真正性を担保するため，取引に用いるEthereumアドレスをマイナンバーに搭載される署名用秘密鍵で署名し，検証できる形で公開した．これにより，Ethereumアドレスを本人性確認が可能な形で，交換することに成功した．

本システムを用いることで，電子商取引において，取引相手の本人性確認がともなった，契約の不可分な実行が可能である．

7.2　本研究の課題・展望

7.2.1　本研究の課題

提案手法では，Ethereumアドレスの暗号化に，マイナンバーカードの署名用秘密鍵を用いた．また署名付きアドレスを，署名検証が可能な形で配布した．しかし，電子証明書の有効性確認が可能なのは第2.2.3項であげたように，総務大臣認定事業者のみである．そのため，本システムでは電子証明書の失効情報の確認ができない．電子証明書の有効性確認の方法について，検討する必要がある．

7.2.2　本研究の展望

本システムでは，それ単体では本人性確認が不可能なEthereumアドレスを，本人性確認が可能な形での交換を実現した．ブロックチェーン技術で利用される公開鍵ペアは，所有者と結びつかない形で利用される．しかし，著作権管理のような鍵所有者の現実世界でのトレーサビリティ必要となるブロックチェーンアプリケーションも存在する．本研究で提案したアドレス交換方法を用いることで，容易に鍵所有者の本人性確認を提供することができる．

7.3 公的個人認証サービスの民間活用に向けて

本研究を通して得られた知見から，今後の公的個人認証サービス・マイナンバーへの提言を，電子政府先進国であるエストニアとの比較を通じて行う．

7.3.1 エストニア ID カード

本項では，エストニアの国民番号制度について解説を行う．

エストニアでは，2002 年から電子的な身分証明書である eID カードを発行している．2018 年 1 月現在，eID(e-identity) として以下の 4 形態の eID が配布されている．本項では主要な形態である，ID カードについて概説する．

- **ID カード**
  エストニア国民や在留者が所有するカード．本人確認に券面の記載事項が利用可能である．
- **Mobile-ID**
  SIM カードを利用．電子認証・電子署名に利用可能．提携プロバイダとの契約が必須である．
- **e-Residency**
  エストニア非居住者用の eID．一部制限があるが，ID カードと同等の機能が利用可能である．
- **Smart ID**
  Android・iOS アプリケーション[1]として提供される本人認証サービスである．

エストニア国民番号

エストニア国民は誕生と同時に，11 桁の国民 ID 番号が付番される．国民 ID 番号はマイナンバーと違い秘匿するものでなく，周知の番号として取り扱われることが個人情報保護法 (Personal Data Protection Act) によって定められている．国民 ID 番号は，性別・生年月日・シリアル番号・チェックデジットによって構成される．表 7.1 に 11 桁の個人番号を `GYYMMDDSSSC` とした際の番号構成の内訳を示す．

表 7.1: 国民 ID 番号の構成

値	内容
G	性別 (男-奇数，女-偶数) と誕生した世紀．1-2(19)， 3-4(20)， 5-6(21 世紀)
YY/MM/DD	下二桁の誕生年/月/日
SSS	シリアル番号
C	チェックデジット

[1] `https://www.smart-id.com`

ID カードの電子データ

eID カードの電子チップには，認証用の公開鍵証明書・署名用の公開鍵証明書が含まれる．認証用には 4 桁の PIN，署名用には 5 桁の PIN があらかじめ付与される．公開鍵証明書にはカード保有者の氏名と国民 ID 番号が記録される．また，認証用証明書にはカード保持者に発行される `FIRSTNAME.LASTNAME@eesti.ee` のメールアドレスが記録される．なお，このメールアドレスは転送用のエイリアスで，メール環境 (IMAP・SMTP サーバ等) は提供されない．このアドレスからメールを送信したいときは，`eesti.ee`[2]のマイページからメールを送信することができる．また，ID カードに関する開発はオープンな環境で行われており，github[3] 上でプロジェクトが確認可能である．

7.3.2 e-Residency

e-Residency とは，非エストニア居住者にエストニアの電子在留権を認める政策である．その政策の一環として，e-Residency カードは電子在留者用の ID カードとして，2014 年からエストニア政府が発行を開始した．e-Residency カードは，非エストニア居住者にも電子認証を提供するため，エストニア政府が所有者に ID 番号を付番するカードである．エストニアでの居住権を示す，または身分証明書として使うことはできない．e-Residency カードを，図 7.1 に示す．

図 7.1: e-Residency カード

e-Residency カードの取得には，エストニア政府の提供するポータルサイト[4]から申請が必要である．エストニア国境警察による審査が通ると，各国のエストニア大使館でカードを受領できる．e-Residency カードの受領者である e-Resindet は，エストニア在留者の ID カードと比較して利用できるサービスは限られるが，エストニア電子政府サービスが利用可能である．以下に，e-Residency カードで利用可能な主なサービスを列記する．

- 電子証明書の利用
- 電子データへの電子署名
- エストニアでの会社の設立

[2] `https://www.eesti.ee`
[3] `https://github.com/open-eid`
[4] `https://apply.gov.ee`

- エストニアでの銀行口座の解説
- エストニアでの税の申告

7.3.3 電子行政基盤

X-Road

X-Road はエストニアの電子行政基盤である．エストニアの行政システムでは，データは集中管理されず，個々の省庁が分散管理する．その分散されたデータの交換プラットフォームが X-Road である．X-Road の個人認証には，eID が用いられ安全性を担保している．X-Road の接続機関は官公庁だけでなく，民間にも解放されている．官民組織からのデータ利用を，共通のインタフェースで提供することで，行政の効率化をはかるのが目的である．エストニアの電子行政基盤の概要を図 7.2 に示す．

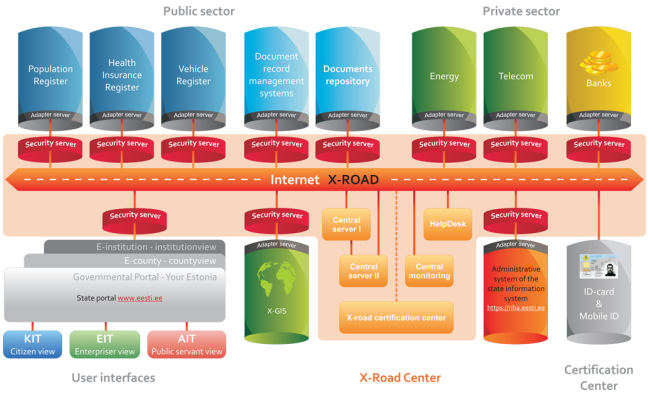

図 7.2: エストニアの電子行政基盤の概要．e-estonia[5]より引用．

電子行政基盤でのブロックチェーンの利用

エストニアでは 2012 年から電子行政基盤の一部に，ブロックチェーンを導入している．エストニアでは，医療記録が電子化されており，医療従事者からのデータを患者が利用できるよう提供している．この医療記録の完全性を保証するため，ブロックチェーンが利用されている．患者はこの医療記録に，ポータルサイト[6]から eID で本人認証を行い，アクセスが可能である．

7.3.4 ROCA Vulnerability への対応

RSA 鍵生成アルゴリズムの脆弱性が報告された ROCA: Vulnerable RSA generation (CVE-2017-15361) が，エストニアの ID カードも影響することが判明し，ID カードの電子証明書の更新が行われた．脆弱性が判明したのちの，エストニア政府の対応は以下である．

[5]https://e-estonia.com/estonian-cyber-security-innovation/
[6]https://www.digilugu.ee/login?locale=en

- 脆弱性の報告から 1 ヶ月ほどで電子証明書の更新ソフトウェアを作成
- eID 利用者に更新手続きを通知
- 該当 ID カードの電子証明書の利用停止

電子証明書の更新は，ID カード利用の管理ツールである ID Card Utility[7]を用いて行われた．ID Card Utility の動作画面を，図 7.3 に示す．

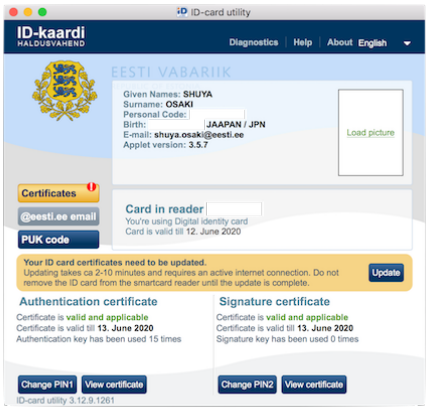

図 7.3: ID Card Utility の動作画面

脆弱な電子証明書の所有者には，上図のように電子証明書の更新を行うようアラートが表示される．電子証明書の更新には，PIN コードの入力が複数回求められ，更新の終了後に新しい電子証明書の PIN コードが表示された．

7.3.5 公的個人認証サービス・マイナンバーのあるべき姿

上述したエストニアの番号制度から，公的個人認証サービス・マイナンバーに取り入れるべき施作を，ここに列記する．

- 個人番号の秘匿を不要とする．
  エストニアでは，個人番号は周知のものとして扱われている．一方で，マイナンバーは秘匿すべきものとされている．しかし，マイナンバーは住民票コードから生成されるものであり，それ単体で個人を識別することはできない．マイナンバーは隠すものという印象からの不安感により，マイナンバーの利活用が妨げられていると推測する．
- サービスを利用可能な形態を増やす．
  エストニアでは eID は 4 形態で提供されている．一方で，公的個人認証サービスはマイナンバーカードでのみ利用可能だ．エストニアのように，スマートフォンで利用可能な形態を整備することが，公的個人認証サービスの普及につながるだろう．
- 開発をオープンに行う．
  マイナンバーカードや搭載される電子証明書の仕様は公開されていない．そのため，マイナンバーカードを用いたサービスの開発は難しい．他方，エストニアでは開発環境がオープンであり，開発コミュニティが醸成されている．日本でも開発環境をオープンにすることで，魅力的なサービスの創出する基盤を整える必要がある．

[7] https://github.com/open-eid/qesteidutil

- ユーザインタフェースの充実させる．
  エストニアでは，カード利用のユーザインタフェースが整備されている．ROCA Vulnerability への対応はカード付随のアプリケーションから行われた．利用者とのコミュニケーションのため，メールアドレスを発行している．また，各種行政サービスも，第 7.3.3 項で示したように，ポータルサイトから閲覧できる．日本では，電子証明書の更新は役所の窓口でしかできず，ユーザとのコミュニケーションの窓口もマイナポータルのみである．また，マイナポータルで提供される情報も一部に限られる．ユーザーインタフェースを充実させ，カードの快適な利用環境の整備が利用率の向上につながるだろう．

日本のマイナンバー制度はまだ施行されてから日が浅く，本論文で示したように課題も多い．一方で，エストニアの例に示したように，番号制度の導入には行政サービスの効率化・IT 先進国としてのプレゼンス向上・新しいビジネスの創出といった大きな可能性が秘められている．公的個人認証サービス・マイナンバー制度の今後の普及と発展を祈り，本論文の結びとする．

謝辞

本論文の執筆にあたりご指導頂いた，慶應義塾大学環境情報学部教授 村井純博士，同学部客員教授 徳田英幸博士，同学部教授 中村修博士，同学部教授 楠本博之博士，同学部准教授 高汐一紀博士，同学部准教授 Rodney D.Van Meter III 博士，同学部准教授 植原啓介博士，同学部教授 三次仁博士，同学部准教授 中澤仁博士，同学部教授 武田圭史博士，同学部講師 斉藤賢爾博士，同大学政策・メディア研究科特任准教授 鈴木茂哉博士，同研究科 特任准教授 佐藤雅明博士，同研究科 特任講師 Achmad Husni Thamrin 博士，同研究科特任助教 空閑洋平博士，同研究科 中島博敬氏，永山翔太博士に感謝いたします．

鈴木茂哉博士に重ねて感謝いたします．ご多忙な中，研究やプレゼンテーションの指導はもとより，研究者・技術者としての姿勢を学ばさせていただきました．博士の指導なしには，卒業論文を執筆することはできませんでした．中島博敬氏に重ねて感謝いたします．慶應義塾大学 CNS コンサルタントの上司として，研究アドバイザーとして，研究室の先輩としてと，多面的に指導をしていただきました．DICOMO シンポジウムでの研究発表は，氏の尽力なしには行えませんでした．また，本研究の核となるアイディアも氏から示唆していただきました．

慶應義塾大学政策メディア・研究科 阿部涼介氏に感謝いたします．氏には，研究室に所属した当初から指導していただきました．私の研究テーマがブロックチェーン技術に関係するようになってからは，多くの効果的なアドバイスをいただきました．

慶應義塾大学村井純研究室 KUMO 研究グループの皆様に感謝いたします．澤井優作氏には計算機科学全般やスマートコントラクトについてご教授いただきました．小林茉莉子氏に感謝いたします．氏が情報基礎の SA を担当していなければ，KUMO 研究グループに所属することはありませんでした．同期の，桑原誠尚氏，瀬下明紗子氏，増田雄一氏，ローランド リチャード氏に感謝いたします．皆様にはグループのリーダとして至らない私を，なんども助けていただきました．

慶應義塾大学村井純研究室の皆様に感謝いたします．永山翔太博士に重ねて感謝いたします．博士には研究者としての姿勢を教えていただきました．研究室で多くの時間を共に過ごした皆様に，重ねて感謝いたします．研究室での交友関係があってこそ，計算機科学に興味をもち，見識を深めることができました．

最後に，私の学生生活を支えてくださった母 仁美に感謝いたします．

参考文献

[1] 総務省．エスクローサービス利用促進に関する調査研究．http://www.meti.go.jp/policy/it_policy/statistics/outlook/060605houkokusyo.pdf, March 2006.

[2] 信森毅博．認証と電子署名に関する法的問題．Technical report, 日本銀行金融研究所 Discussion Paper, 1998.

[3] 小山謙二ほか．情報セキュリティ: ディジタル署名と暗号鍵管理．情報処理, Vol. 25, No. 6, 1984.

[4] 積水ハウス．　分譲マンション用地の購入に関する取引事故につきまして．https://www.sekisuihouse.co.jp/company/topics/datail/__icsFiles/afieldfile/2017/08/02/20170802.pdf, 2017.10.06 参照.

[5] 産経 WEST. 積水ハウス、登記できず…「偽造書類に６３億円」. http://www.sankei.com/west/news/170802/wst1708020087-n1.html, 2017.12.20 参照.

[6] 現代暗号のしくみ: 共通鍵暗号、公開鍵暗号から高機能暗号まで. 共立スマートセレクション. 共立出版, 2017.

[7] 総務省．公的個人認証サービス利用のための民間事業者向けガイドライン．http://www.soumu.go.jp/main_content/000400619.pdf, 2017.12.16 参照.

[8] 猿渡知之．公的個人認証サービス–その制度とシステムの概要．地方自治, No. 663, pp. 39–82, feb 2003.

[9] 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.

[10] JPKI : 公的個人認証サービス (no.019) 特集マイナンバーカードと電子証明書の連携について. J-LIS = ジェイリス : 地方自治情報誌, Vol. 3, No. 7, pp. 79–82, oct 2016.

[11] JPKI : 公的個人認証サービス (no.001) 特集 公的個人認証サービス. J-LIS = ジェイリス : 地方自治情報誌, Vol. 2, No. 1, pp. 54–59, apr 2015.

[12] 総務省．公的個人認証サービスの利活用について．http://www.soumu.go.jp/main_content/000324414.pdf, 2017.12.04 参照.

[13] JPKI : 公的個人認証サービス (no.005) 特集個人番号制度における公的個人認証サービス電子証明書. J-LIS = ジェイリス : 地方自治情報誌, Vol. 2, No. 5, pp. 62–64, aug 2015.

[14] 大豆生田崇志. もう笑えないマイナンバーとマイナンバーカードの混同. http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/041200821/, 2017.12.04 参照.

[15] 内閣官房番号制度推進室内閣府大臣官房番号制度担当室. マイナンバー pr キャラクター概要資料. http://www.cao.go.jp/bangouseido/pdf/seidogaiyou_2912.pdf, 2017.12.17 参照.

[16] 尾崎周也, 中島博敬, 鈴木茂哉, 中村修. 公的個人認証とブロックチェーンを用いたスマートコントラクトシステムの提案. Open Research Forum 2017 第 15 回研究発表大会, pp. 55–58, November 2017.

[17] 内閣府. マイナンバー法成立までの経緯. http://www.cao.go.jp/bangouseido/pdf/seiritsukeii.pdf, 2017.12.17 参照.

[18] 近藤佳大. 日本の番号制度（マイナンバー制度）の概要と国際比較:個人識別子と行政統制の視点から. 情報管理, Vol. 56, No. 6, pp. 344–354, 2013.

[19] Fujitsu. マイナンバー制度について マイナンバー制度の関連法案. http://www.fujitsu.com/jp/solutions/industry/public-sector/local-government/mynumber/overview/law.html, 2017.12.17 参照.

[20] 総務省個人番号企画室. マイナンバー制度における情報連携について. http://www.soumu.go.jp/main_content/000429540.pdf, 2018.1.19 参照.

[21] 八戸市. 個人番号カード（マイナンバーカード）の申請・交付についてマイナンバーカードのイメージ. http://www.city.hachinohe.aomori.jp/index.cfm/13,81102,45,70,html, 2017.12.04 参照.

[22] 西村幸浩, 小野津崇之, 志賀正裕. マイナンバーカードの技術仕様と利活用方式 (特集 マイナンバー) – (マイナンバー制度の利用拡大). *Fujitsu*, Vol. 68, No. 4, pp. 59–65, jul 2017.

[23] 総務省. マイナンバーカード マイナンバーカードのアプリの概要. http://www.soumu.go.jp/kojinbango_card/03.html, 2017.12.18 参照.

[24] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[25] Nick Szabo. Smart contracts. *Unpublished manuscript*, 1994.

[26] Ethereum. https://www.ethereum.org/.

[27] Solidity. https://github.com/ethereum/solidity.

[28] 金子曜大. マイナンバーカード利用者証明用電子証明書を用いた電子署名アプリケーションの開発. Bachelor thesis, 明治大学, April 2016.

[29] 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. 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. 研究報告マルチメディア通信と分散処理（DPS）, No. 19, feb 2017.

[30] 大上智也, 稲葉宏幸. Ethereum のスマートコントラクトを用いた信頼性の高いカーシェアリングシステムの提案. 電子情報通信学会技術研究報告= IEICE technical report: 信学技報, Vol. 117, No. 69, pp. 37–40, 2017.

[31] 斉藤賢爾. スマートコントラクトによる土地売買を考える (特集 不動産テックの動向). 土地総合研究, Vol. 25, No. 3, pp. 18–24, 2017.

[32] OpenSSL. https://www.openssl.org/.

[33] OpenSC. https://github.com/OpenSC.

[34] Geth. https://github.com/ethereum/go-ethereum/.