情報処理学会論文誌　デジタルプラクティス　Vol.5　No.1　23–32 (Jan. 2024)

オンライン手続き向け代理システムについての課題抽出と秘密分散法を用いた実現方法の提案

山本 穂奈美[1,a)]　鈴木 茜[1]　大島 訓[1]　古屋 聡一[1]

受付日 2023年4月21日, 採録日 2023年10月20日

概要：近年，公共，金融などの事務手続きでデジタル化が進み，オンライン処理による代替が浸透している．一方，事務手続きにおいては，本人が手続きを実施できない状況にある場合の「代理」という概念が社会システムを支えている．デジタル上でも代理人による手続きを可能にする仕組みは，オンライン処理の普及に欠かすことができない技術課題である．

本稿では，特に日本での代理人の活用が期待される高齢者や未成年者に関する事務において，オンライン処理における代理を支援するシステムの機能的要件と課題を多角的に調査・抽出した．それらをもとに電子的なやり取りにより実現する方式を提案する．提案方式では，複数人の代理人を立たせ，暗号技術の秘密分散法を用い秘密鍵の分割・復元し，署名の検証によって本人の意思に沿った代理行為を実現する．また，提案方式を実装し評価することで，代理が必要となる場面の特性（緊急度と被害の大きさ）とそれと適応する実現方式の関係を明らかにして電子化できる代理場面の拡張可能性を示す．

キーワード：秘密分散法，任意代理人，認知症患者，代理管理

Issue Analysis and Proposal of Implementation Method with Secret Sharing of Agent System for Online Processes

Honami Yamamoto[1,a)]　Akane Suzuki[1]　Satoshi Oshima[1]　Soichi Furuya[1]

Received: April 21, 2023, Accepted: October 20, 2023

Abstract: In recent years, digitalization has progressed in administrative procedures in the public sector, finance, etc., and online processing has been penetrating. On the other hand, these procedures have been supported by "agents" when the person himself/herself is unable to carry out the procedure. It is necessary to construct electronic application systems that support an agent. In this paper we extract the functional requirements and issues of online processing in administrative procedures for the elderly and minors who are expected to use agents in Japan. Then we propose implementation methods to solve them electronically. The proposed method carries out the procedure where the cryptographic secret sharing scheme is utilized, to set up multiple agents and to obtain their agreement. In addition, by implementing and evaluating the proposed method, we clarified the relationship between the characteristics of situations where agents are required and implementation methods. This shows the possibility of expanding the agent scenes that can be digitized.

Keywords: the secret sharing scheme, agents, dementia patients, agent management

1. はじめに

近年，公共，金融などの事務処理をはじめ，多くの手続きのオンライン処理による代替が社会的に浸透を進めている．公共分野ではマイナンバーカードの普及やデジタル庁の施策を梃として，旧来の多くの手続きの見直しが進んでいる．金融業界でも口座開設やキャッシュレス登録などのシーンでも，オンラインで完結する本人確認（eKYC）の採用や導入が拡大している．

これらのオンライン認証は，持ち物やパスワード，生体情報などにより精度や安全性の高い認証を実現しているが，社会的システムとしてはこれらは解決の一側面に過ぎない．こうしたすべての事務手続きにおいて，本人が手続

[1] 株式会社日立製作所 研究開発グループ サービスシステムイノベーションセンタ
Research & Development Group, Service Systems Innovation Center, Hitachi Ltd., Yokohama, Kanagawa 244–0817 Japan
[a)] honami.yamamoto.qm@hitachi.com

きを実施できない状況にある場合には，「代理」という概念が社会システムを支えている．たとえば社会的な責任を負うことができない幼児に対して，親権者が代理で手続きをするなどの仕組みはオンライン処理の普及に欠かすことができない技術課題である．

日本ではマイナンバーカードおよびマイナポータルを活用した代理人登録によって，デジタル上で代理人を証明する仕組みが存在する．しかし，そのようなケースでも，本人のデジタル技術への適合能力がない場合や，それがあったとしても事故や病気で急に代理事由が発生し本人と代理人で意思疎通が図れない場合がある．あるいは，本人と代理人との利害が相反する場合には，代理人に法的な権限を与えることが不適切な状況なども考えられる．これら様々な状況へシステムが個別に対応することは効率的でない．

本稿では，特に日本での代理人の活用が期待される高齢者や未成年者に関する事務におけるデジタル処理の課題を多角的に調査・抽出し 3 点にまとめ，それらを電子的なやり取りでもって解決するための実現方式を提案する．提案方式をさらに実装し，評価することで，代理が必要となる場面の特性（緊急度と被害の大きさ）とそれに適応する実現方式の関係を明らかにして電子化できる代理場面の拡張可能性を示す．

本稿の構成は次のとおりである．2 章で代理に関する定義と関連する概念の説明を行いながら，それを支援するシステムの本質的な機能を 3 点にまとめる．3 章では，多様な代理ケースの中から要件を示唆するものを 3 例選び，そこでの代理の実現に向けた課題をまとめる．4 章では，2 章で策定した要件 3 点の実現方式を，秘密分散の適用方法を中心に記述する．5 章では，これを前述の代理ケースへの適用可能性を評価し，最後にこれらを 6 章にまとめる．

2. 代理システムと代理ケースの定義

代理人制度は電子的か否かを問わず民法および関連法の中で規定されている．代理人には，法定代理人と任意代理人がある．法定代理人とは，民法の規定によって定められた代理人のことであり，親権者や未成年・成年後見人等が該当する．一方，任意代理人とは，法定代理人以外のことで，たとえば銀行のある特定の処理に対して事前に指定した代理人による代理を認める場合などで指定されるものである．これら代理人制度に関する法制度については，坂崎 [1] でまとめられている．

2.1 定義

本稿では，実際にサービスや支援を受ける人物である本人の代わりをすることを「代理」とし，その人物を「代理人」と呼ぶ．代理人が本人の代わりに実行する行為を「代理行為」と呼ぶ．代理行為の例として，住民票の写しの代理申請や，銀行口座の代理管理がある．

また，「代理システム」とは，以下の一連の業務と手続きのことをいう．代理行為の際，代理人であることを提示し，それが検証され，正当な代理人であることが証明された後に代理行為を実行する．代理システムが扱う業務上の場面のことを「代理ケース」と呼ぶ．

本稿では代理人は，任意代理人のみを扱う．これは法定代理人と異なり，本人の意思によって選出し認定できる．そのため自由度が高く，権限の付与の自由度も含めて，これを電子化する場合のシステム側の要件が複雑である．

■慣習的代理システム

代理システムのうち，委任状などを用いた代理人証明を行うものを「慣習的代理システム」と呼ぶ．任意代理人のケースでは，この慣習的代理システムは慣習的に多く利用されている．以下で，住民票の写しの請求を例に，委任状を用いた代理人の証明と代理行為の実行の様子を説明する．

横浜市 [2] では，住民票の写しの請求に必要なものとして，住民票の写し等請求書（窓口用），窓口へ来た方の本人確認書類，代理権限を確認できる書類，手数料がある．そしてこれを代理で行うために，代理権限を確認できる書類として，本人が作成した委任状を用いる．代理人はこの委任状の中で指定できるため任意代理人のケースとなる．委任状には，代理人の住所，氏名，生年月日と，本人の住所，氏名，委任日，委任事項，権限を委任する旨の文章が記載される．代理行為を実行する際，代理人の本人確認に加えて委任状による代理権限を窓口で確認し，初めて代理行為を実行できる．

なお，横浜市では，住民票の写しをオンライン申請することも可能であるが，オンライン申請の場合，本人のみが対象となり，代理人は申請することができない．

2.2 先行研究・既存デジタルツールの紹介

本節では，先行研究として，現行の代理制度の課題や，代理人による代理行為の電子化に関する研究を挙げる．それから，すでに一般的に利用されている事例として，マイナンバーカードを用いたマイナポータルでの代理人登録アプリを既存デジタルツールとして紹介する．

■先行研究

まず，現行の代理制度として，後見制度や民事信託についてまとめ，それらの課題を指摘している研究として，八谷 [3] や伊室 [4] がある．八谷 [3] は，後見制度および民事信託は，自己決定権の尊重が基本理念であるとし，代理行為を通じて本人の意思を尊重する大切さを述べている．また，現実では，不十分な代理の契約が存在し，まだ社会的環境の整備が進んでいないと指摘している．伊室 [4] も後見制度での後見人による不正や代理行為できる対象が制限されていることを課題に挙げている．

代理人による代理行為の電子化に関する研究としては坂

崎 [1] がある．そこでは，手続きの電子化が進んだ場合に，機微情報も電子的に扱うようになり，データの暗号化によるプライバシー保護が必要になることを指摘しつつ，一方で暗号化すると本人以外の者が扱えないという課題を指摘している．それゆえ，たとえデータが本人宛に暗号化された状態でも，必要に応じて代理人がそのデータを「代理閲覧」をし，本人に代わって代理人が「代理申請」できる仕組みが必要と指摘し，その要件定義と方式提案をしている．

このように代理人に関して，電子的か否かを問わず現行制度に課題が存在していることや代理行為を電子化する仕組みが検討されている．本稿においては，正当な代理人でも不正をしうる点に着目したうえで慣習的代理システムの電子化の実現方式を扱う．

■既存デジタルツール

ここでは，既存デジタルツールの一例としてマイナンバーカードを用いたマイナポータルでの代理人登録を挙げる．このツールでは，事前に代理人登録をすることで，代理行為での「代理人の本人確認」と「代理権限の確認」とを電子的に証明することが可能となり，代理行為をすることができる．

デジタル庁の案内 [5] によれば，代理人の設定方法は，本人が代理人を設定する方法と，代理人が本人を設定する方法の 2 つがある．どちらの方法においても設定する際は，本人と代理人が同席のもと，本人または代理人のマイナンバーカードを用いてログインしたマイナポータルから，代理人に利用を許可するサービスや参照を許可する情報，代理できる期間等を設定し，本人または代理人のマイナンバーカードを読み込ませて登録する．登録後に代理行為が必要になったタイミングで，代理人がマイナポータルにログインし，代理行為の機能を実行できる．代理人は複数人登録でき，また解除もマイナポータルを通じて操作することができる．

このように電子的に代理人を登録，代理行為を実行する仕組みはすでに存在する．しかし，代理行為の対象は，「代理人が実行可能」として登録された機能のみとなっている．

2.3　代理システムの機能的範囲

次に本稿で扱う代理システムの機能的範囲をここで規定する．慣習的代理システムでの確認項目は，①代理人の本人確認と，②代理権限の確認がある．デジタル上の代理でもこの 2 点の確認は必要とすべきである．マイナポータルでは，マイナンバーカードを用いた本人確認と，事前の代理人登録によって，この 2 点を実現している．

②代理権限の確認については，民法第 643 条（委任契約）に次のように記載されている：「委任は，当事者の一方が法律行為をすることを相手方に委託し，相手方がこれを承諾することによって，その効力を生ずる」．本稿では，これを「本人と代理人とで，代理行為について合意をとること」と言い換えると，代理システムの要件として，合意の取得とその証明を電子的に達成することがあげられる．

この要件において重要な点は不正の防止である．代理行為は，自身のものではない他人の権限や資産，情報を管理することも含まれるものであり，代理人による不正につながりやすい．このことは先行研究においても課題として挙げられている [4]．この不正を抑止するシステム要件として，③代理行為の適正性の確認が考えられる．

以上より，汎用的な代理システム構成における機能的な要件が次の 3 点に整理される．これらを代理システムの機能範囲として考える．

① 代理人の本人確認
② 代理権限の確認
③ 代理行為の適正性の確認

3.　課題抽出

3.1　通常対応が困難な代理ケース 3 例

2 章で機能要件を整理したが，それら機能を現実的に社会で機能させるための補助的な機能，あるいは非機能的な要件について次に考えてゆく．そこでまず本章では，多くの代理ケースの中から，機能の必要性を考えるのに好適な代理ケース 3 例について紹介する．

これら代理ケースの共通的な特徴として，デジタルデバイスの利用が困難な高齢者や判断力が未熟な子どもの代理行為が絡む場合である．これらには既存のデジタルツールをそのまま利用できない．

(1)　遠隔地に住む高齢者の代理ケース

遠隔地に住む高齢者の代わりに，たとえば行政手続きを実施する場合，まず慣習的代理システムの利用が考えられるが，本人による委任状等の作成が必要となる．そのため，高齢者自身での作業が必要になり，難しい場合は高齢者の住むところまで代理人が訪れ支援する必要がある．また，代理行為先が高齢者の住む自治体等であった場合も直接訪れる必要があり，時間がかかる恐れがある．次にデジタルツールを利用する場合を考えるが，高齢者によってはデジタル機器への慣れに個人差がある．慣れていない場合，支援なしで代理人等の登録をすることが難しく，格差が生じる．

このように，遠隔地に住む高齢者の代理ケースは，高齢社会において，充分に起こりえるケースであるにも関わらず，代理人側の負担が大きい，デジタルデバイドといった問題を抱えていると言える．

(2)　認知症患者の資産管理の代理ケース

近年，認知症患者は増加しており，それに伴い認知症患者の所有する資産も増加している．しかし，現時点では，認知症患者の銀行口座は，各金融機関の判断によって，口

座凍結されることが多い．つまり，家族であっても高齢者本人の口座を管理することができない．これを回避するため，認知症患者の口座においては，成年後見制度や後見制度支援信託等を利用した後見人等による代理管理が認められている．

しかし，制度の利用には，家庭裁判所の決定が必要であるため，制度を利用した人は2021年末時点で約24万人 [6] であり，認知症患者全体の約4%も満たず，一般に浸透しているとは言い難い．

認知症患者の資産の代理管理では，患者本人の意思の実現が基本的な理念である．しかし，認知症を発症すると本人の判断力が低下するため，本人による意思表示が困難になる．それゆえ代理管理ではトラブルも発生しやすく，実際にも前述の制度を利用して正式に認められた後見人ですら横領等の不正を働く事例も少なくない．今後，認知症患者の資産が増え続けていく中で，代理人による安全な代理管理の仕組みが期待されている．

(3)　虐待疑惑家庭の代理ケース

未成年者に代わって手続き等の代理行為を実行する場合，一般的には親および親権者が法定代理人となる．しかし，虐待の問題を抱えている家庭では，親および親権者が法定代理人の責務を果たすことは考えにくい．そのような被害を受けているかもしれないこども達への支援を実現させるためには，学校や病院，子ども食堂等の支援施設といった地域組織間の協力が効果的である．たとえば，学校の出校状況，病院での通院や診察の結果，子ども食堂でのこども個人に関する情報共有を行うことで対策の検討や実施，虐待の検知が容易になる．現時点においては，ソーシャルワーカーと呼ばれる社会福祉の専門家によって，こうした情報共有等支援がサポートされている．そして家庭状況により，虐待が疑われるような場合，は，児童相談所が介入し，児童相談所が法定代理人として親権を行う（児童福祉法第33条）．

その一方でソーシャルワーカーの人員不足や，個人情報保護により，迅速な情報連携が難しい場面がある．その場合，虐待疑惑家庭における代理行為として，ある組織が所有するこどもの個人情報を別組織へと情報連携するための代理で同意することが考えられる．たとえば，子ども食堂でのこどもの様子を学校へと連携するなどである．この同意は，本来，親および親権者からの同意があるべきであるが，虐待疑惑の家庭の場合，その同意の取得は困難である．このような場合でもこどもの支援を実施するために学校や支援施設関係者が代理で同意をとるような代理行為をケースとして本稿では設定する．個人情報への同意を本人以外が実施することは，個人情報保護法により認められているものではないが，虐待等の緊急時においてはこの限りではない（個人情報保護法第23条）．

3.2　3つの代理ケースからの課題抽出

前節で述べた各代理ケースから，代理システムの電子化における課題を抽出した結果，以下のようになった．

■デジタルに不慣れな者とのデジタル上での合意形成

慣習的代理システムでは，本人が委任状等を作成する動作がある．これを電子化するには，紙の委任状等に相当する，代理人に代理権を譲渡することへの合意をデジタル上で形成する必要がある．この合意形成においては，デジタルが不慣れな者でも実現可能にする必要がある．

■本人が意思表示できない場合の合意形成

本人が認知症を発症した場合は，本人の意思で操作をすることが叶わないことも考えられる．そのようなケースにも備え，事前に合意形成をし，認知症の発症というような決められた条件を満たした場合のみ効力を発生するという仕組みも必要となる．

■正当な代理人の不正

成年後見制度を利用し認められた後見人であっても不正を働く事例がある．実際，最高裁判所の調査では，後見人等による不正事例として，不正報告件数が169件，被害額約5.3億円（2021年）と報告されている [6]．正当な代理人による不正は常に存在している．電子的かを問わず多額の資産や重大な情報等を代理で管理する場合ほど不正事例が発生することが予想される．

■緊急時の対応

虐待等における本人の状態によっては，できるだけ早く代理人を決定し，代理人による代理行為を実現させ，本人へ支援する必要がある．そのような場合を緊急時とし，通常時とは異なる処理で代理行為を実行できるようにする仕組みが必要となる．

4.　電子的代理システムの実現方式の実装

ここでは，2.3節で定義した3つの機能範囲を実現し，かつ，3.2節で示した課題を解決するような，電子的代理システムの実現方式を検討する．

以下，各機能の実現方式を検討する．機能によっては，実現方式が複数あるが，これは，代理ケースの分類に合わせて適切な形式を選択することを想定している．

4.1　代理人の本人確認機能

代理人の本人確認をする方法としては，すでに民間サービスの登録時に導入されているオンライン本人確認（eKYC）を用いることができる．現在，オンライン本人確認は，銀行の口座開設や，キャッシュレス決済の登録，携帯電話の契約等において活用されている．これらは犯罪収益移転防止法（以下，犯収法）および関連法（携帯電話不正利用防止法等）に則った本人確認方法となっている．

具体的なやり方は，犯収法第6条（本人特定事項の確認方法）に記載されており，本人確認時に写真付き書類の写

しと本人の容貌を順番に送信する形式が採用されていることが多い．

4.2　代理権限の確認機能

代理権限の確認機能では，本人および代理人の間で，代理行為の内容について合意をとり，合意したことを証明できるようにする必要がある．また，3.2 節で抽出した課題のうち，デジタルに不慣れな者とのデジタル上での合意形成と，本人が意思表示できない場合の合意形成を解決できる方式を検討した．その結果，(i) リモート会議方式と (ii) 複数代理方式を提案する．

(i)　リモート会議方式

リモート会議方式は，デジタルに不慣れな者とのデジタル上での合意形成を実施するための方式である（**図 1**）．これは，代理行為への合意をする場所として，リモート会議（ここでは，オンライン上でお互いの顔を見ながら会話をすることを指す）を用意する．ここに，本人と代理人，代理行為先の担当者が参加する．これにより，リモート会議の中での対話で，代理行為の内容等を決めることができる．これは，デジタルに不慣れな者でも利用することができる．このリモート会議の IT 環境設備に関しては，山口県 [7] の取り組み例であげられるような，身近な公民館等を活用して提供されるオンライン窓口サービスの利用を想定する．

対面による合意がとれた後は，それを証明するため，電子的な合意書を作成し，そこにリアルタイムで秘密鍵を作成し電子署名を実施する．

このようにして，リモート会議を活用して合意形成し，電子署名を検証することで合意の証拠となり，合意書に記載の代理行為へとつなげることができる．

(ii)　複数代理方式

複数代理方式は，本人が意思表示できない場合の合意形成を解決するための方式である（**図 2**）．将来，認知症等を発症し，判断能力が低下する場合に備えて，発症前に代理人と合意形成をすることが前提となる．そして，発症後にその合意が有効になるようにし，それを証拠として，代理行為へとつなげていくものである．

具体的には，暗号技術である秘密分散法を活用する．秘密分散法とは，ある秘密情報を n 個に分割し，そのうちの k 個以上が集められたときのみ，秘密情報の復元が可能になる手法である [8]．

また，この方式のポイントは，複数人の代理人を設定するところである．これは慣習的代理システムでは代理人は一人である点とは異なる部分である．

本方式では，まず，本人が事前準備として，合意形成用の秘密鍵を作成し，対応する公開鍵の認証を公開鍵暗号基盤を用いて実現する．この秘密鍵を秘密分散法により，代理人の人数分に分割し（以降，分割した情報を分散情報と呼ぶ），分散情報を代理人に分配する．その際，本人意思として代理行為の内容や効力の発生条件（例：本人の認知症発症後，3 人以上の代理人分散情報が収集できたときに効力を持つ）を記載した合意書を作成し，本人を含めて代理人全員で電子署名を実施しておく．

本人の判断力が低下したとみなされたときには，代理人で分散情報を集めて秘密鍵を復元し，それを使って合意書に対して電子署名を実施する．これにより効力が発生したとみなされる．電子署名を検証することで，合意の証拠となり，合意書に記載の代理行為へとつなげることができる．

このように，事前準備で本人の意思を表明した後，代理人からの合意を集め，条件を満たしたときのみ代理行為を実行できるようにすることで，本人の意思に沿うことができる．

一方，秘密分散法の性質上，悪意を持った代理人ら k 人以上が結託すれば不正に合意をとることが可能である．誰が代理人であるかを代理人に知らせなければ結託は難しくなるが，本稿における代理ケースでは，代理人は親族など閉じられた関係の中で設定されることが多いため，現実

図 1　(i) リモート会議方式
Fig. 1　(i)Remote-conference type method.

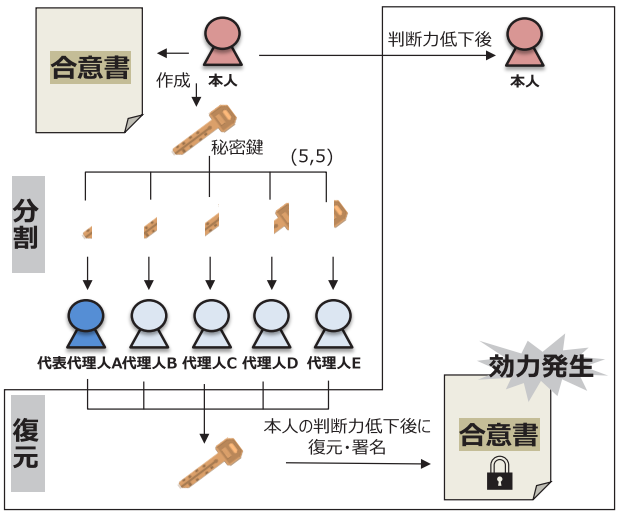

図 2　(ii) 複数代理方式
Fig. 2　(ii)Multi-agent type method.

的ではない．この方式での代理人の結託による不正については 5 章でも触れる．

また，分割した分散情報の配送にも注意しなくてはならない．秘密情報を安全に配送するためには，公開鍵を使った暗号化をするため公開鍵のインフラが必要となる．日本においては，マイナンバーカードのような社会インフラの活用がポイントとなり，マイナンバーカードの秘密鍵の対になる公開鍵で暗号化すれば，カードを保持している本人しか復号できず，安全に秘密情報を配送できる（現在は機能制限のため暗号化はできない仕様になっている）．

4.3　代理行為の適正性の確認機能

代理行為の適正性の確認では，(ii) 複数代理方式と同様に，代理人を複数人設定する．複数の代理人で相互監視し代理行為が適正か確認する．確認の方法としては，(iii) しきい値型監視方式と (iv) 階層型監視方式を提案する．この 2 方式は，代理人を対等に扱うか，代理人の内で権限の優先順位をつけるかで異なる．

(iii)　しきい値型監視方式

しきい値型監視方式では，ある代理人が代理行為を実行する前にその他の代理人にそれについて合意するか意思表示させる．合意した代理人の数がしきい値以上であった場合，その代理行為は適正であるとみなされ，代理行為の実行へと移ることができる．しきい値は，代理行為の内容に応じて決定する（例：認知症になった高齢者の口座から 100 万円送金する場合，代理人 5 人の内 3 人の合意が必要）．

この意思表示の仕方においては，(ii) 複数代理方式における秘密分散法によって代理人個々に与えられた分散情報を用いたやり方が考えられる．代理人は自身が合意するか判断し，合意する場合は，分散情報を送信する．分散情報がしきい値以上集まれば秘密鍵を復元でき，その秘密鍵による電子署名でもって，代理行為の適正性を確認できる．

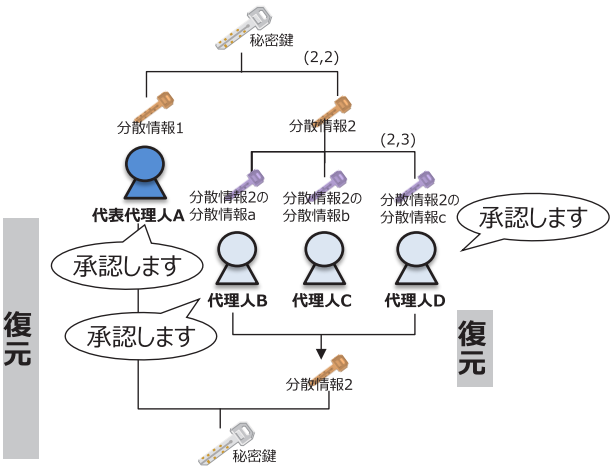

図 3　(iv) 階層型監視方式

Fig. 3　(iv)Layered-monitoring type method.

(iv)　階層型監視方式

(iii) と同様に，ある代理人が代理行為を実行する前にその他の代理人からの合意を集める．階層型監視方式では，代理人の中でも優先順位をつけ，誰からの合意かを取り入れて代理行為の適正性を判断することができる．

具体的には，**図 3** のように，秘密鍵の秘密分散法による分割を 2 度繰り返して，各代理人に分配する．この分割であると，代理人 A の合意がないと秘密鍵を復元することができない．一方で，代理人 B〜D は，この 3 人の内 2 人の合意があれば最終的に秘密鍵を復元することができる．このように，代理人 A の権限を大きくし，代理人 B〜D との差をつけることができる．

4.4　デモの開発

本稿では，前述した各機能のうち，代理権限の確認機能と代理行為の適正性の確認機能を実現する代理システムのデモを開発した（**表 1** 赤枠）．なお，代理人の本人確認機能は，eKYC アプリ等といったサービスとして一般的にも普及しているため，省略する．

実装では (ii) 複数代理方式と (iv) 階層型監視方式を採用した．慣習的代理システムと既存デジタルツール，開発したデモにおける方式比較は次の**表 2** のようになる．

表 1　各機能における実現方式

Table 1　Implementation types by functions.

要件	代理人の本人確認	代理権限の確認	代理行為の適正性の確認
実現方式	オンライン本人確認	(i)リモート会議方式	(iii)しきい値型監視方式
	(eKYC)	(ii)複数代理方式	(iv)階層型監視方式
		デモ実装範囲	

表 2　方式比較

Table 2　Method comparison table.

機能		現在の代理システム		電子的代理システムのデモ
		慣習的代理システム	既存デジタルツール	
代理人の本人確認機能	本人確認方法	本人確認書類の提示	マイナンバーカードによる電子署名	オンライン本人確認
代理権限の確認機能	合意の取り方	委任状への記名・捺印	マイナポータルへの代理人登録の実行	代理人らから分割情報を収集し，秘密鍵が復元できるか判定
	代理権限の証明方法	委任状	マイナンバーカードによる電子署名	秘密鍵による電子署名
代理行為の適正性の確認機能	監視方法	なし	なし	秘密鍵による電子署名
実操作内容	本人の操作	委任状の作成	代理人登録作業	委任条件の設計
	代理人の操作	委任状の保管	代理人登録作業	分散情報の保管

5.　電子的代理システムの評価

5.1　留意すべき要件における評価

本節では，開発したデモを留意すべき要件で評価した（**表 3**）．要件の観点には次の 5 点，1. 長期的な観点でユーザに変化があってもシステム利用への障害が増えないという性質，2. 処理性能，3. 代理業務の運用的側面，4. 業務・法律の変化・改訂への対応，5. 安全性を考えた．これにより，電子的代理システムとして，秘密分散法を活用した方式 (ii)，(iv) のメリットとデメリットを評価できる．

処理速度の観点では，秘密鍵の分割処理に約 0.04 秒，復元処理に約 0.02 秒程度を要するのみであり（**表 7**，**表 8**），秘密分散法の活用は一連の操作を妨げるものではないと言える．

一方で，安全性においては，代理人が結託することによる不正を防ぐことはできないことが分かった．これを解決するにはたとえば，秘密鍵が復元され代理行為が実行される際に，代理人全員へ通知させ，おかしな動きがないか確認できるようにするなど運用上の仕組みが必要となる．

5.2　代理ケースへの適用性の評価

本節では，開発したデモを 3.1 節の通常対応が困難な代理ケース 3 例に適用した場合のメリット，デメリットを評価する．デモの操作内容および各代理ケースでの適用例は**図 4** のようになる．

(1)　遠隔地に住む高齢者の代理ケース

この代理ケースにおける適用では，図 4 中の (1) のように代理人を設定し，秘密鍵の分割と分配を行う．②代理権限の確認および③代理行為の適正性の確認では，高齢者と家族・親族らで事前に合意した合意書と，代理人から収集した分散情報によって秘密鍵を復元・署名し検証できるかによって確認する．この場合，代表代理人 A である高齢者の息子による合意（分散情報の送信）がないと秘密鍵が復元できないこととなる．

デモの活用によるメリットは，代理人の間で相互監視が可能となる点である．これにより，これまでの慣習的代理システムでは，ある一人の代理人のみの責任となり，その代理人の独断は防ぐことができなかったことに対し，複数人の代理人で責任を分散して高齢者の代理行為を進めることができる．これは，親族間の揉め事を防止することにつながる．また，本方式では，正しい分散情報でないと最終的に秘密鍵を復元することができないため，代理人のなりすましを防ぐこともできる．

しかし，デメリットは，高齢者がデジタル操作に不慣れな場合，事前準備としての秘密鍵の作成，条件設定が困難となり利用できない点である．また，代理行為内容として行政手続きが主である場合，手続きの頻度や緊急度が大き

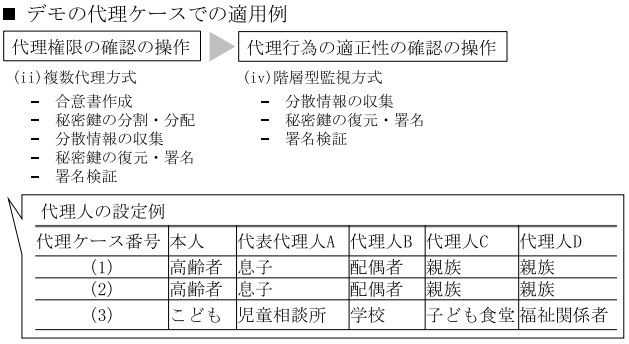

図 4　デモの操作内容と代理ケースへの適用例
Fig. 4　Application example of demo operations and cases.

表 3　留意すべき要件における評価
Table 3　Evaluation of each requirement.

No.	留意すべき要件の観点	留意すべき要件	提案方式への評価結果	評価方法
1	長期的な観点でユーザに変化があっても，システム利用への障害が増えないという性質	(1a)認知症等による判断力の喪失	可: 代理行為の実現によって対応可能.	システム仕様を評価．プロト実装済.
		(1b)家族構成や代理事業者の変更	可: 秘密分散法の性質から n を増加させることは容易.	システム仕様を評価．プロト実装済.
		(1c)物理的な移動能力の低下	可: 通信によるリモート処理として実装したため対応可能.	システム仕様を評価．プロト実装済.
		(1d)異なる代理行為への拡張	事前設定していれば可	システム仕様を評価.
		(1e)しきい値などの設定の複雑さ	社会情勢や慣習を反映して決定するための別の取り組みが必要.	システム仕様を評価.
		(1f)長期間にわたる秘密情報の管理	別の手段にて対策が求められる.	システム仕様を評価.
2	処理性能	(2a)条件設定時の処理時間	秘密鍵の分割時間（約 0.04 秒）	プロトにて計測.
		(2b)合意取得時の処理時間	秘密鍵の復元時間（約 0.02 秒）	プロトにて計測.
3	代理業務の運用的側面	(3a)執行済案件への争議時の正当性トレース	可: 秘密鍵での署名による担保.	システム仕様を評価．プロト実装済.
		(3b)代理権限の重みづけ	可: 秘密分散法を階層的に繰り返すことで対応可能.	システム仕様で充足．プロト実装済.
4	業務・法律の変化・改訂への対応	(4a)暗号技術の危殆化などによる暗号方式の変更	可: デジタル署名，暗号化処理，乱数生成などは原理的に可能．秘密分散はそれ自身情報理論的安全であり，これの変更は考慮していない.	システム仕様を評価.
		(4b)代理やその権限に関する法的扱いの変化	不可: ある時点での仕様が将来の法に対応するわけではないが，法が変化しうるものの多くは，機能変更での対応が可能と考える.	システム仕様を評価.
5	安全性	(5a)権限を超越する処理の実施・業務的な不正への耐性	充足: 不正防止の手段として機能を設計．これには前提条件がある．暗号技術と運用の健全性，システム脆弱性がないことなどが含まれる.	システム仕様を評価.
		(5b)なりすましへの耐性	充足: ただしプロトでは一部のみ実装．またこのユーザ管理の健全性を維持する運用も別途必要.	システム仕様を評価.

くないこと，不正時の被害を考慮すると，秘密鍵を用いた代理人による相互監視はオーバースペックであるとも捉えられる．

つまりデジタルが不慣れな者を対象とし，緊急度が小さく，被害も少ない代理ケースにおいては，適用性が低いと評価できる．

(2)　認知症患者の資産管理の代理ケース

この代理ケースにおける適用では，図 4 中の (2) のように代理人を設定し，秘密鍵の分割と分配を行う．これは高齢者が意思表示できるときに合意書の作成とともに行う．その後，高齢者の判断力が低下した際に代理人から分散情報を収集し秘密鍵を復元して署名をする．これにより合意書の効力が発生する．実際に代理人が代理行為を実行するときも，他の代理人からの合意を集め秘密鍵の復元条件を満たす必要がある．

これにより本人が意思表示できない場合でも事前の本人意思に沿った代理行為としての資産管理を続けていくことができる．金融資産を他人が代理で管理する場合には横領なども起こりえるが，複数の代理人によって代理行為の適正性が確認されてから代理行為が実行されるため，防ぐことができる．このように不正による被害が大きい代理ケースにおいては，適用性が高いと評価できる．

一方，デメリットは，本人による事前準備から実際に代理行為が実行されるまで数年〜数十年以上経過する場合があり分散情報の長期保存や暗号移行への対応が必要になる点である．しかし，これらはシステムの運用方法を検討することで解決できる可能性がある．

(3)　虐待疑惑家庭の代理ケース

この代理ケースにおける適用では，図 4 中の (3) のように代理人を設定し，秘密鍵の分割と分配を行う．また，代理行為を，とあるこどもの個人情報をしかるべき機関へと連携するために代理で同意をすることと想定する．合意書作成時は，本人（こども）による操作となるが，未成年者のためその法定代理人である親および親権者が行う．しかしこの時点で合意が取れない場合は児童相談所の判断で合意書の作成を行うこととする．②代理権限の確認および③代理行為の適正性の確認では，この合意書と，学校や子ども食堂などの代理人から収集した分散情報によって秘密鍵を復元・署名し検証できるかによって確認する．代表代理人 A を児童相談所とすることで，児童相談所による合意（分散情報の送信）がないと秘密鍵は復元されない．

デモの活用によるメリットは，本来あるべき親の合意が取れない場合でも，関係者からの代理での合意を集め，こどものための情報連携を実施することができる点である．他人の個人情報に対して連携を合意することには流出のリスクも伴うが，複数の代理人によって代理行為の適正性が確認されてから情報連携するため，こども本人の個人情報を守ることができる．

しかし，この代理ケースの想定上，実行する際は緊急性が求められるものであることが多い．そのため，もし，適正性の確認で代理人らで分散情報を収集する時間がかかった場合や代表代理人による送信が遅れた場合，システムとして次に進めることができず，こどもへの支援も遅れることとなる．

よって，開発したデモは，緊急性が求められる代理ケースにおいては，適用性が低いと評価できる．

5.3　代理ケースの特性と実現方式の関係

前節でデモの代理ケースへの適用性を評価した結果，(2) 認知症ケースでは適用可能性が確認できた．一方で，(1) 遠隔地ケースや，(3) 虐待疑惑家庭のケースでは適用可能性が低いことが分かった．これは 3.2 節で抽出した課題のうち「デジタルに不慣れな者とのデジタル上での合意形成」と「緊急時の対応」の課題，解決できていないことが大きい．しかし，これらの課題は 4.2 節と 4.3 節で述べた (i) リモート会議方式もしくは (iii) しきい値型監視方式を採用すると解決できる可能性がある．

たとえば，(1) 遠隔地ケースの場合，②代理権限の確認では (i) リモート会議方式，③代理権限の適正性の確認では (iii) しきい値型監視方式とする．すると，デジタル操作に不慣れな場合でもリモート会議で参加しながらの合意形成ができる．開発デモでメリットとなった代理人を複数人に設定できるということはできなくなるが，その分簡便化できる．(iii) しきい値型監視方式においてしきい値 1 人以上と設定すれば，代理人を一人としたときに利用できる．

また，(3) 虐待疑惑家庭のケースにおいては，緊急性が高いため，できるだけ早く合意をとれる方法が適している．しかし，他人の個人情報を代理管理することに対して，慎重に行わなければならない側面もある．そこで，②代理権限の確認では (ii) 複数代理方式，③代理権限の適正性の確認では (iii) しきい値型監視方式とする．すると，代理人を複数人に設定できるというメリットを残しつつ，状況に合わせてしきい値を小さく設定すれば，早く適正性も確認できる．

このように，通常対応が困難な代理ケース例をもとに残りの実現方式の適用可能性も評価できた．次に，これらの代理ケース例を，緊急度，被害の大きさを軸にして分類する．これにより，代理ケースの特性として表現でき，特性に合わせた実現方式を検討できる．

この緊急度（大・中・小）とは，代理が必要になったときから代理行為が実行できるまでの時間の指標である．たとえば，(3) 虐待疑惑家庭のケースの場合，対象となる子どもへの迅速な支援へとつなげるために代理行為も早く実行するべきであり，緊急度が高いと定義する．

また，被害の大きさ（大・中・小）とは，代理行為が不

正に実施されたことによって，本人が被る損害を指標とする．前述のとおり，正当な代理人であっても不正をする事例はいくつもある．たとえば，(2) 認知症ケースの場合，悪意のある代理人によって不正に代理行為が実行されると，本人が所有する金融資産などが奪われることとなるため被害の大きさは大きいと定義する．

このように代理ケース例を緊急度と被害の大きさで分類すると**表 4** のようになる．

以上を踏まえ，代理ケースの特性における各実現方式の適用性を整理すると**表 5** のようになった．提案する 4 方式，すなわち代理権限の確認方法としての (i) リモート会議方式，(ii) 複数代理方式，そして代理行為の適正性確認方法 (iii) しきい値型監視方式，(iv) 階層型監視方式，それぞれについて，対応可能な緊急度と被害の大きさの大小を示している．これにより，状況・条件によって様々存在する代理ケースについて，緊急度と被害の大きさで特性分類しながら適した実現方式を組み合わせ・選択し，電子的代理システムの構築に役立てることができる．

6. まとめ

6.1 得られた知見

本稿では，高齢者や未成年者の代理行為を対象とした代理の場面における課題を抽出し，それらを電子的なやり取りでもって解決するための実現方式を検討し，デモを開発した．

また，本稿では，開発したデモの評価を通じて，代理が必要となる場面の特性（緊急度と被害の大きさ）とそれと適用する実現方式の関係を明らかにした．これにより，電子化できる代理場面の拡張可能性を示すことができた．

表 4　代理ケースの特性
Table 4　The characteristics of agent cases.

代理ケース		(1)遠隔地ケース	(2)認知症ケース	(3)虐待疑惑家庭のケース
特性	緊急度	小	小	大 但し代理行為後に迅速性が必要
	規模 被害	中 行政手続きができない	大 資産を損失	小 個人情報が流出

表 5　代理ケースの特性と各実現方式の対応関係の整理
Table 5　Summary of compatibility of each proposed method against the characteristics of agent cases.

提案する方式(これらは排他的ではなく一部組合せも可能)		代理ケースの特性	
		緊急度	被害の大きさ
代理権限の確認	(i)リモート会議方式	小	小
	(ii)複数代理方式	中	中
代理権限の適正性の確認	(iii)しきい値型監視方式	大	小
	(iv)階層型監視方式	小	大

6.2 今後の課題

留意すべき要件の評価でも挙げたとおり，悪意を持った代理人らの結託による不正行為や，秘密鍵を分割した分散情報の管理といった運用面での課題がある．また，本人による事前準備から実際に代理行為が実行されるまで数年〜数十年以上経過する場合も考えうるため，長期保存や暗号移行への対応が不可欠である．このようにシステムの運用方法を検討が必要である．

さらに実現方式を現行法および将来を見据えた法制度と照らし合わせ，合意書の効力性や秘密分散法を活用した電子署名の証拠性が保証されるか検討が必要である．

謝辞　本稿の審査過程では，匿名にて査読いただいた査読者の皆様より，論文向上のための大変有益なコメントを数多くいただきました．謹んで感謝の意を表させていただきます．

参考文献

[1] 坂崎尚生：代理人制度に向けたプロキシ再暗号化方式の要件定義とその方法，情報処理学会論文誌，Vol.60, No.9, p.1489–1499 (2019)
[2] 住民票の写し・住民票記載事項証明書について：〈https://www.city.yokohama.lg.jp/kurashi/koseki-zeihoken/todokede/koseki-juminhyo/shoumei/jyuminhyou.html〉,（参照 2023-03-01）.
[3] 八谷博喜：高齢社会における信託の有用性と家族を受託者とする信託（民事信託）の課題，中央大学大学院法学研究科博士論文 (2021)
[4] 伊室亜希子：後見制度支援信託の概要と考察，明治学院大学法律科学研究所年報，Vol.29, pp.85–92 (2013)
[5] 代理人/全体概要：〈https://img.myna.go.jp/manual/03-07/0115.html〉,（参照 2023-03-09）.
[6] 成年後見関係事件の概況，後見人等による不正事例：〈https://www.courts.go.jp/toukei_siryou/siryo/index.html〉,（参照 2022-06-10）.
[7] シビックテックチャレンジ YAMAGUCHI:〈https://cc-yamaguchi.jp/〉,（参照 2023-03-10）.
[8] Shamir, A.: How to Share a Secret, *Communications of ACM*, Vol.22, No.11, pp.612–613 (1979)

付録

付録 A.1　電子代理システムの評価における計算機環境

5.1 節において評価するにあたり利用した計算機環境は**表 6** である．

付録 A.2　秘密分散法における秘密鍵の分割処理時間および復元処理時間

表 6 の計算機環境下にて，秘密分散法により秘密鍵を分割および復元した際の処理時間は表 7，表 8 である．各処理時間は，分割数と復元に必要となる分散情報の数を変化させ，それぞれ 1000 回実施し，その最小値と最大値，平均値を計算した．たとえば，5 人の内 3 人の合意があれば

表 6　計算機環境
Table 6　Computational environment.

ライブラリ		Secrets.js-grempe
方式		楕円曲線暗号方式 (ECDSA)
鍵長		521 ビット (Secp521r1 曲線を利用)
計算環境 (AWS 仮想マシン)	OS	Ubuntu 18.04.5 LTS
	仮想 CPU 数	2
	メモリ	8GB
	ストレージ	EBS のみ

表 7　秘密鍵の分割処理時間
Table 7　Processing time to divide the private key.

分割数	復元	処理時間 (秒)		
		最小値	最大値	平均値
100	65	0.156	0.219	0.168
10	6	0.011	0.041	0.012
5	3	0.004	0.028	0.005
3	2	0.002	0.029	0.003

表 8　秘密鍵の復元処理時間
Table 8　Processing time to restore the private key.

分割数	復元	復元使用数	処理時間 (秒)		
			最小値	最大値	平均値
100	65	100	0.056607	0.097173	0.063664
		65	0.030473	0.069836	0.037976
10	6	10	0.002640	0.017809	0.003708
		6	0.001345	0.015996	0.002390
5	3	5	0.001355	0.012697	0.001911
		3	0.000591	0.012997	0.000989
3	2	3	0.000830	0.013266	0.001185
		2	0.000346	0.007789	0.000559

復元可能であると設定するときには，分割数：5，復元：3 となる．復元処理においては，復元使用数として，秘密鍵を復元する際に使用する分散情報の数として復元使用数を用意し，復元と同じ数（＝復元するのに使用する分散情報の最小の数）と，分割数と同じ数（＝復元するのに使用する分散情報の最大の数）を各設定で計算した．

山本 穂奈美（非会員）

2019 年慶應義塾大学大学院理工学研究科修了．同年，株式会社日立製作所入社．情報セキュリティ，金融システム，児童福祉システムの研究に従事．

鈴木 茜（非会員）

2006 年東京工業大学大学院総合理工学研究科修士課程修了．同年株式会社日立製作所入社．セキュリティシステム，特に電子認証の研究開発に従事．

大島 訓（正会員）

1998 年東京理科大学大学院理工学研究科修士課程修了．同年株式会社日立製作所入社．オペレーティングシステム，計算機仮想化，ブロックチェーンの研究に従事．2016 年 Hitachi America Ltd. Research&Development Division 出向．

古屋 聡一（正会員）

1997 年九州大学大学院システム情報科学研究科修了．同年日立製作所入社．2004 年九州大学大学院システム情報科学研究科博士後期課程修了，博士（工学）．情報セキュリティ，システム工学，スマートシティの研究に従事．1998 年ケンブリッジ大 Industrial Research Fellow，2018 年世界経済フォーラム第四次産業革命センターフェロー．電子情報通信学会会員．