氏　　名	島岡 政基
学位(専攻分野)	博士(情報学)
学 位 記 番 号	総研大甲第 1724 号
学位授与の日付	平成26年9月29日
学位授与の要件	複合科学研究科 情報学専攻 学位規則第6条第1項該当
学 位 論 文 題 目	保証レベルに応じた身元確認スキームの設計手法に関する研究
論 文 審 査 委 員	主　査　教授　曽根原 登 教授　越前 功 教授　合田 憲人 教授　山田 茂樹 准教授 佐藤 周行 東京大学

(別紙様式 2)
(Separate Form 2)

論文内容の要旨
Summary of thesis contents

保証レベルに応じた身元確認スキームの設計手法に関する研究

情報空間(Cyber space) と実世界(Physical world) が連携または融合するサイバー・フィジカル融合社会が到来する．サイバー空間における情報財の価値はますます高まる一方で，様々なプライバシー情報もまた蓄積されるようになり，サイバー空間における情報財にまつわる事件や自己が実社会に与える影響は無視できなくなってきている．このように利便性だけでなくリスクの面でもサイバー・フィジカル融合が進むと，サイバー空間において情報財にアクセスする人やコンピュータなどのエンティティが，実社会における誰であるのかを紐付ける身元確認が非常に重要になってくる．

身元確認は，その方法によって確からしさに差が生じる．例えば金融機関における身元確認は身元確認書類を二種類提出する必要があり，他人が不正に二種類揃えることは難しい．メールアドレスの到達性確認は，登録したメールアドレスに送信された URL にアクセスする方法で，メールの本文さえ傍受できればなりすまし可能であること，そもそも確認対象がメールアドレスだけでは，実社会におけるエンティティとの紐付けが困難であることなど，その確からしさには明らかに違いがある．この身元確認は，1) 架空の人物でないこと(実在性) および 2) 他人への成りすましでないこと(同一性) を担保する行為として整理されており，その確からしさの違いは，国際標準化機構(ISO) 等で保証レベルとして標準化され，4 段階の尺度でレベル分けされる．

一方，近年では情報検索サービスやソーシャル・ネットワーキング・サービスのようなサービスと，認証機能の分離を前提とした認証プロトコル(SAML や OpenID など) の発展・普及が進み，サービス提供者(SP, Service Provider) が自らアカウントを発行・管理せずに，第三者組織が発行するアカウントを用いてログインを可能とするサービスが増えてきた．この第三者組織は，情報空間で必要なアイデンティティ情報の提供を行うアイデンティティ情報提供者(IdP, Identity Provider) と呼ばれ，そのアイデンティティ情報は，アカウントなどの識別子，パスワードなどのクレデンシャル，ユーザのメールアドレスなどの属性情報の 3 種類によって構成される．このような SP から IdP に認証機能を委託する関係は，今後ますます増えてくると考えられている．ある IdP が認証機能を委託するに相応しい相手かどうかを判断する際に，身元確認の確からしさは重要な判断基準となる．身元確認は，ユーザからの申請を受けて，IdP から身元確認業務を委託された登録機関(RA, Registration Authority) が，身元確認すべき属性情報を何らかのデータソースと照合するプロセスである．IdP のユーザが全国に分散していてかつ大量にいるような大規模 IdP では，RA の配備方式として，クレジットカード発行時などのように遠隔から身元確認を行う Remote RA と呼ばれる方式と，学生証や社員証などのようにユーザの近くで身元確認を行う Local RA と呼ばれる方式の二種類に大別される．

一般に身元確認はコストがかかる作業である上に，その保証レベルを上げるほどに多くのコストが必要になる．安易に身元確認コストを削減しようとすれば，場合によっては意図せずその保証レベルまで下げてしまうというリスクが発生する．そこで，SP に期待される保証レベルを損なうことなく身元確認コストの削減を実現するという問題を解決する必要がある．身元確認コストの削減にあたって，RA の配備方式は重要な要素である．RRA は

(別紙様式 2)
(Separate Form 2)

コストがかかる身元確認作業を労働集約できる点で大きなコストメリットを持つが，身元確認に利用可能なデータソースがLRAに比較して少ない,またデータソースによってはLRAよりも参照コストがかかる，というデメリットを持つ．これに対してLRAはRRAよりも多くの，また信頼性の高いデータソースが利用できるため，高い保証レベルを実現するにはRRAよりも有利というメリットがある．一方で，RRAのような労働集約が困難なため，人件費の削減や効率化が難しいというデメリットを持つ．

そこで本研究では，ひとつめの課題として，こうしたRAの配備方式の違いに着目しながら，保証レベルを損なわない身元確認コストの削減手法について取り組む．この課題については，ふたつのアプローチを行った．まず一点目として，大学共同利用機関法人　国立情報学研究所(NII) が全国の大学と連携して推進する「大学間連携のための全国大学共同電子認証基盤(UPKI) 構築事業」におけるUPKI3層アーキテクチャの設計を行った．UPKIが対象とする複数のサービスにおいては,それぞれに異なる保証レベルを求められており，これを満たそうとすると最も高い保証レベルに合わせ，その結果身元確認を含め運用コストも高くなってしまう，という課題があった．そこで，保証レベル毎にサービスを3層に分離することでコスト合理性を保ちつつ，サービス間の相互運用性を確保するという3層構造のアーキテクチャを設計した．二点目として，身元確認の保証レベルを保ちつつ身元確認コストの削減を実現するための，身元確認スキームの設計手法について検討を行った．ここでは，商用認証局の身元確認スキームについて調査分析を行い，この分析結果をもとにコスト指向の身元確認スキームの設計手法を提案した．提案手法は，UPKIにおいて大学に存在するWEBサーバの存在証明書をNIIが発行する「サーバ証明書プロジェクト」において設計手法の実装と評価を行った．同プロジェクトは平成27年度から事業化が確定しており，本研究はその実用化に大きく寄与した．

本研究のふたつめの課題として，身元確認の定量的なコスト構造のモデル化に取り組む.谷本らは大学の学内認証基盤を事例として認証基盤のコスト構造を定量的に分析して，運用コストにおける身元確認にかかる人件費の比率が高いことを定量的に示した．しかしながら，身元確認そのものに踏み込んだ詳細な分析には至っておらず，そのコスト構造はまだ明らかになっていない．身元確認コストの削減を行うにあたりその定量的な評価は重要である．ここでは，先の商用認証局の身元確認スキームの調査分析から明らかになったデータソースの評価項目をもとに，保証レベルに依らずにコスト評価可能な身元確認のコスト構造をモデル化した．これにより，保証レベル独立なコスト評価が可能となった．本モデルはサーバ証明書発行サービスを対象として妥当性評価を行ったが，認証局に限らずアイデンティティ管理の本質である身元確認をスコープとする本モデルは，認証局に限らず広くアイデンティティ管理システムに適用可能である．

折しも平成28年度から社会保障・税番号制度(マイナンバー) 制度の導入が決まったこともあり，政府ではマイナンバー制度を利活用する「ID連携トラストフレームワーク」を提案している.マイナンバー制度を前提とするならば確かに有効な手法とも考えられるが，プライバシー対策やマイナンバー制度自体の運用コストの合理性評価など取り組むべき課題は多く，またマイナンバーが利活用できない分野においては有効策になり得ないという問題もある．本研究は，今後活用と普及が大きく期待されているマイナンバーにおいても適用可能なモデルであることを示しており，強い社会インパクトが期待できる．

(別紙様式 3)
(Separate Form 3)

博士論文の審査結果の要旨
Summary of the results of the doctoral thesis screening

本博士論文は、身元確認の確からしさ(保証レベル)に応じた身元確認スキームの設計手法と題し、これまで、保証レベルを低下させることなく身元確認のコストを削減する方法がないという問題に対し、本研究は、身元確認における身元確認コスト要素として、身元確認を行う登録機関の配備方式、データソースの所在、データソースへのアクセスコストを抽出し、これらをコスト変数として評価する方法を考案し、保証レベルを低下させることなく身元確認コストの削減を可能とする新たな身元確認手法を確立した研究である。

情報空間における ID(アイデンティティ)のなりすまし問題は、実社会と情報空間が相互に融合するサイバー・フィジカル融合社会において、ますますその影響が広がり、リスクが増大している。その対策として ID 発行時における、厳格な身元確認が求められるが、これには膨大なコストがかかる。従来、要求される身元確認の確からしさ(保証レベル)が決まれば、身元確認スキームがほぼ一意に与えられ、保証レベルを低下させずにコスト削減する方法がなかった。この問題に対して、商用認証局における身元確認スキームを分析し、身元確認のコストが身元確認に用いるデータソースの選定に依存していること、そのデータソース選定の評価項目が、1) 身元確認を行う登録機関の配備方式、2) データソースの所在、3) データソースへのアクセスコスト、4) データソースの真正性という 4 項目であること、さらにこのうち 1)〜3)が保証レベル独立なコスト決定要素であることを見出した。これら 3 つの要素のうち、2)と 3)を軸としたマトリクスを 1)の数だけ用意して、これに様々なデータソースをマッピングし、各データソースのコストを計量化することでコスト評価する、① 新たな身元確認スキームの設計手法の提案と、② そのコストを定量的に評価するコスト構造モデルの提案し、博士論文としてとりまとめた。本提案は、大学共同利用機関 情報・システム研究機構 国立情報学研究所が、全国の大学と連携して構築する「大学間連携のための全国大学電子認証基盤整備事業(UPKI)」において、提案①を学術機関向けサーバ証明書発行スキームとして社会実装し、システム運用を通じて同スキームのコスト優位性を実証した。また、提案②を用いて既存のサーバ証明書発行サービスの分析を行い、提案手法がコスト評価に有用であることを実証した。

博士論文は次のように構成される。第 1 章では、本研究の背景と課題、目的と本論文の構成について示す。第 2 章では、本研究の理解に必要な概念や技術について説明する。まず、身元確認を議論するにあたって必要な概念として ID 管理について概説し、次に、保証レベルを議論するにあたって必要な概念としてフェデレーションについて概説する。第 3 章では、ID 管理と身元確認に関連する関連動向として、複数組織間で認証情報を交換するための信頼関係を効率よく構築するトラストフレームワークについて、国内外の動向や標準化状況などを示す。また、学術認証基盤のアーキテクチャとして UPKI 3層アーキテクチャを提案し、さらに UPKI 学内認証基盤におけるコスト構造分析結果を示す。第 4 章では、保証レベルを保ちつつ身元確認コストの削減を可能とするための、身元確認スキームの設計手法について提案する。本提案手法は、大学に存在する Web サーバを対象とした証明書発行において実装・評価を行い、その実用性を明らかにした。第 5 章では、保証レベルに影響を与えない身元確認の定量的なコスト構造をモデル化する。これによって保証レベルの変更を伴わないコスト評価やコスト改善が定量的に可能となる。このコスト構造モデルを実際の事例に当てはめることで提案するモデルの妥当性を確認した。第 6 章では、本研究が ID 管理の

(別紙様式 3)
(Separate Form 3)

運用コストに関する問題について概観し、本研究の社会貢献について示した上で、最後に本研究についてまとめた。

本研究は、査読付きジャーナル論文 2 件、査読付き国際会議論文発表 2 件の学術貢献及び、インターネット技術標準 1 件の国際技術標準貢献を実績として有する。

今後認証基盤の社会的重要性が高まるにつれて、その身元確認における保証レベルとその運用コストもますます無視できなくなる。本研究の社会的意義は高く、また学術認証基盤だけでなく社会保障・税番号制度をはじめ行政窓口や金融機関などにおける身元確認業務にも応用可能である。よって、本論文は、情報学分野における学術貢献と学術研究実用化の方法論の新たな道を示す研究として、十分に博士の学位論文として合格と認められる。