博士論文　2014 年度（平成 26 年度）

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

総合研究大学院大学
複合科学研究科　情報学専攻

島岡 政基

2014 年 7 月

本論文は総合研究大学院大学複合科学研究科情報学専攻に
博士（情報学）授与の要件として提出した博士論文である．

論文審査委員

曽根原	登	教授 （主査）	総合研究大学院大学／国立情報学研究所
越前	功	教授	総合研究大学院大学／国立情報学研究所
合田	憲人	教授	総合研究大学院大学／国立情報学研究所
山田	茂樹	教授	総合研究大学院大学／国立情報学研究所
佐藤	周行	准教授	東京大学

A dissertation submitted to the Department of Informatics,
School of Multidisciplinary Sciences,
The Graduate University for Advanced Studies (SOKENDAI)
in partial fullfillment of the requirements for
the degree of Doctor of Philosophy

Advisory Committee

Noboru SONEHARA (Chair)	National Institute of Informatics/
	The Graduate University for Advanced Studies
Isao ECHIZEN	National Institute of Informatics/
	The Graduate University for Advanced Studies
Kento AIDA	National Institute of Informatics/
	The Graduate University for Advanced Studies
Shigeki YAMADA	National Institute of Informatics/
	The Graduate University for Advanced Studies
Hiroyuki SATO	The University of Tokyo

論文要旨

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(RRA)) 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(LRA) 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．

Abstract

Information devices and sensors of every kind are connected on the network. Information is being digitized and distributed, allowing anyone to access it anytime. As a result, integration between information space (Cyberspace) and the real world (Physical world), or in other words, a Cyber-Physical Integrated Society (CPiS), is being formed. The value of information goods, including privacy in cyberspace, continues to grow more and more. Meanwhile, the impact, which has been made by an incident regarding such information goods in cyberspace, on the real world has become too large to ignore. As cyber-physical integration advances with not only increased convenience but also increased risk, identity proofing that binds an entity, e.g., human or computer, who accesses information goods in cyberspace together with the entity in the real world becomes very important.

Identity proofing has various levels of confidence by its method. For example, identity proofing in financial services requires two kinds of identity verification documents, so spoofing is hard. Confirming the ability to receive an e-mail address, which is often preferred in the consumer industry, is easier for spoofing. Thus, there are obvious differences in the confidence of identity proofing. The identity proofing consists of a verification of existing actually and an identification (non-impersonation). The difference in the confidence is standardized as four Levels of Assurance in the international standardization body, ISO, IEC and ITU-T.

Federation technology, e.g., SAML and OpenID, which assumes that an Identity Provider (IdP) and service provider (SP) are separate, is evolving and deployed. Some services do not manage a user account and are available that enable logging in with a user account provided by a third-party. Such a trust relationship in which a SP delegates authentication to an IdP is expected to become more common. Confidence in the identity proofing of an IdP is a critical factor when judging whether a SP can delegate an IdP with authentication.

Identity proofing is the process of verifying applicant information that should be verified with certain data sources to identify an entity. This process is performed by a registration authority (RA) who is delegated by an IdP with the operation of identity proofing. For a large scale IdP who has many branches and geographically distributed users, the topology of a RA can be classified into two types: remote RAs (RRAs), where an identity is proven via an online channel, and local RAs (LRA), where proof of identity is provided in-person by the applicant.

Identity proofing is expensive work, and requires higher cost with a higher level of

assurance. If reducing the cost of identity proofing without careful consideration, it may drain the level of assurance involuntarily. IdP must achieve the cost reduction of identity proofing without the degradation of level of assurance.

The topology types of RA are important for the cost reduction of identity proofing. RRA has a great advantage for labor-intensive identity proofing; but has also disadvantage of less data sources or more expensive data sources for identity proofing than LRA. LRA has an advantage for achieving higher level of assurance because having more reliable and much data sources than RRA, but has disadvantage for labor cost reduction.

This study addresses two problems. First problem is the cost reduction method of identity proofing without degrading the level of assurance, considering the difference of RA topology. Its first approach is the design of a three layers Public Key Infrastructure (PKI) architecture, which is oriented to the RA topology and levels of assurance, based on some of the applications in the University PKI project at National Institute of Informatics. The requirement of several applications in the project requires different levels of assurance has problem that causes expensive operational cost including identity proofing. The second approach is the proposal of design method for identity proofing with the cost reduction keeping its level of assurance. This approach analyzed an identity proofing of a commercial Certification Authority, and proposed the cost-oriented design method for identity proofing as the analysis result. The proposal has been implemented and evaluated to the server certificate issuance project in National Institute of Informatics. The project plans to launch the service in NII from 2015, and this study contributed it greatly.

Second problem is the modeling the cost structure for identity proofing. Tanimoto et al. quantitatively analyzed the labor cost structure of PKI, one of the typical identity proofing applications, and clarified that its dominant factor is the operation cost. They clarified also that the work of identity proofing had high man-hour rates in operation cost. Thus, there are no studies focusing on identity proofing, especially its cost structure. The quantitative cost evaluation of identity proofing is important to its reduction. This work modeled the cost structure of identity proofing, which is evaluable without level of assurance, using the evaluation item of data sources clarified by the second approach. This model has been evaluated with existing PKI services, and will be applicable to not only PKI but also other identity management systems, such as national ID systems.

Japanese Government and its extragovernmental organizations are promoting an "ID federated trust framework" that use the Japanese national ID number system. The use of national ID number system would certainly be an effective solution for the trust framework. However, there are also some problems, such as privacy and the operation cost performance of the national ID number system itself, and it is not solution where the national ID number system cannot use. This paper shows also the cost structure model is applicable to such national ID number system, and will be able to expect more social impact.

This model will be applicable to not only PKI but also other identity proofing use cases, such as national IDs.

目 次

第 1 章　序論 **3**

1.1　背景 3

1.1.1　サイバー空間におけるなりすまし問題 3

1.1.2　なりすましを防ぐ認証技術とアイデンティティ 3

1.1.3　認証の前提となる身元確認 4

1.1.4　情報空間と実社会を結ぶ身元確認の意義 5

1.1.5　フェデレーションの普及 6

1.2　身元確認と登録機関の課題 7

1.2.1　登録機関の配備方式 7

1.2.2　配備方式の比較 9

1.3　本研究が取り組む課題と目的 10

1.4　本論文の構成 11

第 2 章　準備：身元確認と保証レベルの理解 **13**

2.1　アイデンティティ管理 13

2.1.1　アイデンティティ情報 13

2.1.2　アイデンティティ情報のライフサイクル 13

2.1.3　身元確認とアイデンティティ情報の登録 14

2.1.4　登録機関の配備方式 15

2.2　フェデレーション 17

2.2.1　フェデレーションの仕組み 17

2.2.2　実装 18

2.2.3　保証レベル 19

2.2.4　トラストフレームワーク 21

2.3　サーバ証明書の基本概念 24

2.3.1　サーバ認証の仕組み 24

2.3.2　パブリック認証局とプライベート認証局 24

2.3.3　登録業務の形態 25

2.3.4　規程類の継続的な遵守 26

第 3 章　関連研究・動向 **27**

3.1　先行研究 27

3.1.1 フェデレーションにおける身元確認スキームの設計手法 27
3.1.2 身元確認のコスト構造の分析 28
3.1.3 身元確認のコスト評価 29
3.1.4 身元確認やアイデンティティ情報に関する調査分析 29
3.2 先行事例 30
3.2.1 米国政府のトラストフレームワーク政策 30
3.2.2 経済産業省の ID 連携トラストフレームワーク 31
3.2.3 その他のトラストフレームワーク 32
3.3 関連研究：UPKI アーキテクチャ 33
3.3.1 UPKI の要件 33
3.3.2 UPKI アーキテクチャの設計 35
3.3.3 まとめ 39

第 4 章 身元確認スキームのコスト指向設計手法の検討 41

4.1 商用認証局における身元確認スキームの調査分析 41
4.1.1 審査項目 42
4.1.2 保証レベル 42
4.1.3 証明書発行フロー 43
4.1.4 身元確認スキームの考察 44
4.2 コスト指向の身元確認スキーム設計手法の提案 45
4.2.1 前提条件 47
4.2.2 評価の流れ 47
4.3 提案手法の実装 48
4.3.1 前提条件 48
4.3.2 機関審査への実装 49
4.3.3 発行審査への実装 50
4.4 提案手法の評価 51
4.4.1 機関審査の評価 51
4.4.2 発行審査の評価 52
4.4.3 商用認証局の評価 52
4.4.4 コスト比較 53
4.4.5 考察 54
4.5 本章のまとめ 56

第 5 章　身元確認コスト構造のモデル化と評価 **57**
5.1　背景: 身元確認 58
5.1.1　身元確認のためのデータソース 58
5.1.2　RA の配備方式と規模の課題 58
5.2　身元確認のコスト構造モデル 59
5.2.1　パラメータの妥当性 61
5.3　評価 61
5.4　議論 63
5.4.1　UPKI サーバ証明書プロジェクト 63
5.4.2　身元確認に関連する他のケーススタディ 65
5.4.3　まとめ 66
5.5　関連研究 66
5.6　今後の展望 67
5.7　本章のまとめ 67

第 6 章　結論 **69**
6.1　今後のアイデンティティ管理におけるコスト問題 69
6.2　本研究のまとめ 70

謝辞 **72**

参考文献 **75**

図 目 次

1.1 アイデンティティ情報 [26] 4
1.2 フェデレーションの概要 7
1.3 身元確認の概要 8
1.4 登録機関の配備方式の違い 9

2.1 アイデンティティ情報のライフサイクル ([67] 図 1.1-5) 14
2.2 登録機関の配備方式の違い 16
2.3 フェデレーションの概念図 ([84] 図 3 より©2011,IEICE) 17
2.4 EAAF の概要 ([27]Figure 1 より) 20
2.5 Open Identity Trust Framework Model[49] 23
2.6 証明書パス ([83] 図 1 より©2012,IEICE) 25
2.7 RA/LRA の違い ([83] 図 2 より©2012,IEICE) 26

3.1 リスク評価による保証レベルの決定 28
3.2 保証レベルにもとづくサービスの類型化 ([22] 図表 45 より) 31
3.3 2 種類の保証レベル ([22] 図表 42 より) 32
3.4 UPKI の 3 層構造 ([84] 図 5 より©2011,IEICE) 37

4.1 典型的な証明書発行フロー ([83] 図 3 より©2012 IEICE) 44
4.2 提案手法による主なデータソースのマッピング (RRA 方式) 46
4.3 提案手法による主なデータソースのマッピング (LRA 方式) 46
4.4 提案手法によるスキーム設計 47
4.5 機関審査への実装 50
4.6 発行審査への実装 51

5.1 提案モデルのシミュレーション結果 ([61]Fig. 2 より©2014,IEEE) 60
5.2 シミュレーション結果 #1([61]Fig. 3 より©2014,IEEE) 62
5.3 シミュレーション結果 #2([61]Fig. 4 より©2014,IEEE) 63
5.4 UPKI サーバ証明書プロジェクトへの適用 ([61]Fig. 5 より©2014,IEEE) . . 64
5.5 他のケーススタディへの適用 ([61]Fig. 6 より©2014,IEEE) 65
5.6 マイナンバーへの提案モデルの適用 68

表 目 次

1.1 RRA 方式と LRA 方式の比較 10

2.1 潜在的な被害と影響 [35] 22
2.2 潜在的な被害と保証レベルのマッピング ([35]Table 1 より) 23

4.1 商用サーバ証明書の審査項目 ([83] 表 1 より©2012 IEICE) 42
4.2 商用認証局のデータソース 45
4.3 提案スキームの審査項目の分担 ([83] 表 2 より©2012 IEICE) 49
4.4 機関審査の評価 51
4.5 発行審査の評価 52
4.6 商用認証局の評価 52
4.7 コスト比較に用いた値 (単位：人・時) 53
4.8 サーバ証明書プロジェクトの実績値 54

5.1 シミュレーションに用いたパラメータ群 ([61]TABLEusepackage(able); I より©2014,IEEE) 62
5.2 UPKI サーバ証明書プロジェクトの実績 [24] 64
5.3 他のケーススタディのパラメータ群 ([61]TABLE III より©2014,IEEE) . . . 65

Copyright Information

第1章　序論

1.1　背景

1.1.1　サイバー空間におけるなりすまし問題

スマートデバイスやセンサーネットワークの開発・普及が進み，実社会の人やモノの様々な情報が日々刻々と情報空間に蓄積され，その時その場所にいなくても，情報空間を介してあたかもその時その場所に存在していたのと同じレベルの情報を，いつでもどこでも入手できるようになってきた．こうした実社会から情報空間への流れに加えて，最近ではいわゆるO2O(online-to-offline) と呼ばれる，情報空間でのユーザ体験を実社会に誘導するアプローチも広まってきており，情報空間から実社会への流れもまた形成されつつあると言える．このような実社会と情報空間が相互に融合する，いわゆるサイバー・フィジカル融合社会においては，実社会の人やモノと，情報空間におけるそれは，適切に対応づけられている必要がある．例えば，情報空間上でコミュニケーションをとっている相手が Alice だと思っていたのに，実際には Bob が Alice になりすましていたとなれば，Bob には見せるつもりがなかった写真を見せてしまうなど，Alice 以外に意図せぬトラブルが起きるであろうことは容易に想像がつく．実際に，有名人になりすましてソーシャルネットワーキングサービス (SNS) のアカウントを取得し，SNS 上で非社会的な言動を重ねることでなりすまされた本人の評判が低下する事件も起きている．こうしたなりすまし問題は，情報空間においてコミュニケーションを取っている相手の情報が不足しているが故に生じる，情報空間に典型的な問題である [34, 28].

1.1.2　なりすましを防ぐ認証技術とアイデンティティ

一般に，こうしたなりすまし対策として，パスワードや電子証明書などを用いた認証技術が知られている．認証は，あるリソースにアクセスしようとする主体が間違いなく主体そのものであることを検証するプロセスであり，パスワードや電子証明書の私有鍵など主体自身しか知り得ない情報を用いて確認する．こうした手法は，実社会においても利用されていて，古くはアリババと 40 人の盗賊における「開けゴマ」などが有名であり，また情報空間においては Time Sharing System においてユーザを特定するためにパスワードが導入されたのが最初と言われている．その後，パスワードから公開鍵暗号技術や多要素認証など，秘密情報の安全性を高める技術が進歩しているが，事前に発行した秘密情報を用いて相手を認識するという本質的な枠組みは変わっていない [69].

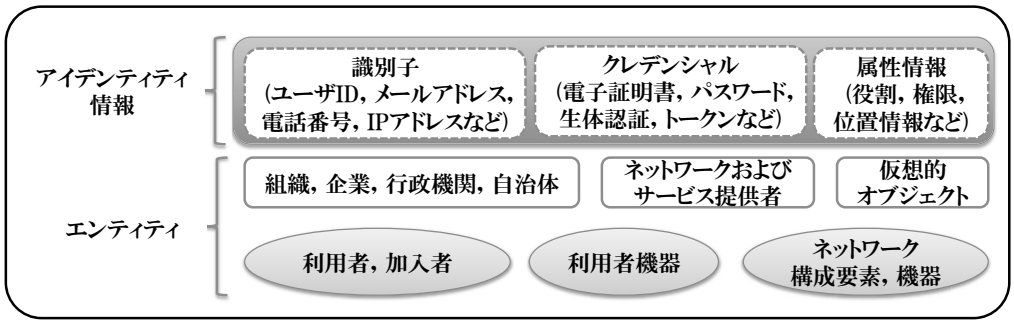


図 1.1: アイデンティティ情報 [26]

実社会では我々は，相対している人やモノを認識する際に，五感に加えて時間的・空間的文脈など様々な情報を総合して判断することができる．しかし情報空間で人やモノを認識しようとする時，物理的に相対しているのはコンピュータやスマートデバイスといった情報通信機器であり，これを通じて得られる情報は実社会で相対している人やモノから得られる情報と比較すると圧倒的に少ない．また，情報空間を介して伝わる情報は，例えば通信経路において改竄されたり，情報空間を介して対話している相手が嘘をついていてもそれを見抜くことが実社会に比べて見抜きにくい，という問題もある．しばしば示される典型的な例として，”On the Internet, nobody knows you ’ re a dog”というコンピュータの前に犬が座っている構図の風刺画はよく知られている [62].

このような実社会と情報空間の歪みを防ぐために，情報空間ではアイデンティティ情報という概念で人やコンピュータを扱い，これを管理する枠組みはアイデンティティ管理と呼ばれる [33]．アイデンティティ情報とは，図 1.1 に示すように人やコンピュータなどのエンティティを個々に識別するための識別子 (アカウント名やユーザ名など) と，事前に発行された当該エンティティだけが持ち得るクレデンシャルと呼ばれる秘密情報 (パスワードや私有鍵など)，エンティティが持つ様々な属性情報 (氏名や住所，肩書きなど) の 3 種類によって構成され，クレデンシャルと属性情報は識別子に紐付けられた形で管理される [26].

1.1.3 認証の前提となる身元確認

アイデンティティ管理では，最初にエンティティを管理対象として登録する際に，エンティティに対して「身元確認」と呼ばれる確認行為を行った上で，クレデンシャルを当該エンティティに発行する．

情報社会がそれほど発達していなかった時代には，クレデンシャルを発行する必要がある相手は限られており，もともと面識のある相手や，あるいは必要に応じて事前に面識を持つことが可能な相手であることが多く，この身元確認はそれほど問題にはならなかった．しかし，情報通信技術の急速な発達と普及に伴い，実社会でもともと面識のない相手と情報空間で対話するケースが増え始め，この身元確認の位置付けが次第に重要になってきた．

例えば，コンシューマ向けオンラインサービスなどでしばしば見られるメールアドレスの到達性確認というものがある．これは，あるサービスを利用するための利用者登録をするにあたって，特定のメールアドレスに対して空メールを送信すると特定の URL が返信され，この URL にアクセスすることで利用者を特定する仕組みである．サービス事業者側にとっては登録処理を自動化でき，登録する利用者にとっても後述の金融機関の例に比較するとすると簡便な手続きで済むというメリットがある．しかし，確認ができているのはメールアドレスだけであり，そのメールアドレスを所有しているのが誰なのかは利用者の自己申告に依存しているため，必ずしも充分な確からしさが担保されていない，というデメリットがある．

これに対して，金融機関で我々がしばしば体験する煩雑な身元確認手続きは，例えば運転免許証の提示と住民票の写しの原本の提出など複数の身元確認書類を必要としている．身元確認書類として利用できるのは，氏名・住所が記載されている公的証明書あるいはそれに準ずる書類であり，かつ本人以外が不正にこれらの書類を取得することは容易ではない．公的証明書を用いることで，利用者とその属性情報 (氏名や住所など) について一定の確からしさを担保できるメリットがある一方で，利用者が事前に身元確認書類を準備する必要があり，金融機関も身元確認書類が偽造でないことを確認する必要があるなど，双方ともに手続きが煩雑になるというデメリットがある．

このように身元確認は様々な方法があり，その方法によって身元確認の確からしさが異なる．身元確認も含めた認証技術の確からしさは「(認証の) 保証レベル」という尺度で表現される．これについて 2.2.3 節で後述する．

1.1.4 情報空間と実社会を結ぶ身元確認の意義

身元確認は，情報空間と実社会を結ぶプロセスであるが，これが今日重要な位置付けになってきたことには 2 つの背景があると考えられる．

ひとつは情報空間を介して実社会に与える影響が大きくなってきたためであり，場合によっては実社会の安全安心を脅かす可能性が増えるとともに，その場合のインパクトもまた加速的に大きくなってきている．これは，昨今の個人情報漏えい事件や SNS 炎上から実社会の刑事訴訟などの事件に至った例を見ても明らかである．そして，こうした安全安心を実現するための社会統治の仕組みは，現状では自然人あるいは法人を前提としている以上，情報空間での犯罪やトラブルが起きた場合には，それを実社会の自然人や法人に紐付けなければ，社会制度を適用できないという課題がある．

もうひとつの理由は，実社会に限らず情報空間の中に限定しても同様の問題が膨らんできているという点である．近年の情報空間においては，情報通信技術の発達と普及により，実社会とほぼ独立した仮想社会の発達が著しい．例えば，実社会の個人 A は，情報空間において実社会とはおよそ別人格の X というアイデンティティで振る舞い，またあるコミュニティで認知されていたとする．このコミュニティ内でもし他人が X になりすまして非社会的な言動を行った場合，A 氏は実社会で何ら制約を受けないものの，情報空間における当該コミュニティでは極めて活動しづらい状況に追い込まれることになる．従来は，こうしたコ

ミュニティが比較的小さく，影響範囲が少なかったためにそれほど大きな問題として捉える必要はなかったかも知れないが，昨今ではこうした問題も無視できなくなりつつある．このような問題に対しては，理想的には情報社会，それも実社会と連動することなく統治可能な社会制度の整備が必要である．つまり，実社会での刑罰などではなく情報社会上での刑罰を与えるなどの必要になってくるだろう．もちろん社会制度であるから，刑罰などのネガティブな側面だけでなくポジティブな面，つまり権利の担保などについても併せて検討していくことが不可欠である．いずれにしても，情報社会だけで完結可能な社会制度の確立が今後必要になってくると考えられる．

このように，前者であれば実社会のエンティティとの紐付けが担保されたアイデンティティ情報が情報空間には不可欠であるし，後者であれば情報社会において一意性が担保されたアイデンティティ情報が不可欠であり，そのなりすましを防ぐためにはやはり (実社会の) エンティティとの紐付けが担保されていることが不可欠である．

1.1.5　フェデレーションの普及

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．SP から IdP に認証機能を委託するということは，SP とその委託先である IdP との信頼関係の構築が不可欠になる．このような，ある信頼関係を前提に複数の組織間でアイデンティティ情報を交換する仕組みは，一般にフェデレーションと呼ばれており，その概観を図 1.2 に示す．フェデレーションでは，従来のようにサービス提供者が自前でユーザ管理を行うのと比較して，前述の身元確認も含め運用コストがかからず，認証機能の開発やそのセキュリティ対策といったアプリケーション開発とは異なったスキルを確保しなくて済む．また利用前の登録手続きが障壁とならないのでユーザ獲得がスムーズに進められるなどのメリットがあり，サービス提供者にとっては本来のサービス拡充にリソースを専念できると期待されている．

フェデレーションは，その形成にあたり IdP と SP どちらに着目するかによって，IdP 中心フェデレーションと SP 中心フェデレーションに大別できる．コンシューマサービスなど，見込みユーザが多い IdP と連携する方がメリットが大きい SP にとっては，なるべくユーザ数の多い IdP と連携する傾向にあり，このように多くの SP が少数の特定の IdP と連携するものを IdP 中心フェデレーションと呼ぶ．一方エンタープライズ市場では，それぞれに IdP を運用する多くの組織ができるだけ低コストでサービスを (ただし質は下げずに) 受けたいと考えており，そのためには合目的な複数の組織が共同で SP と契約するというアプローチがある．このように複数の IdP が共同でいくつかの SP と連携するものを SP 中心フェデ

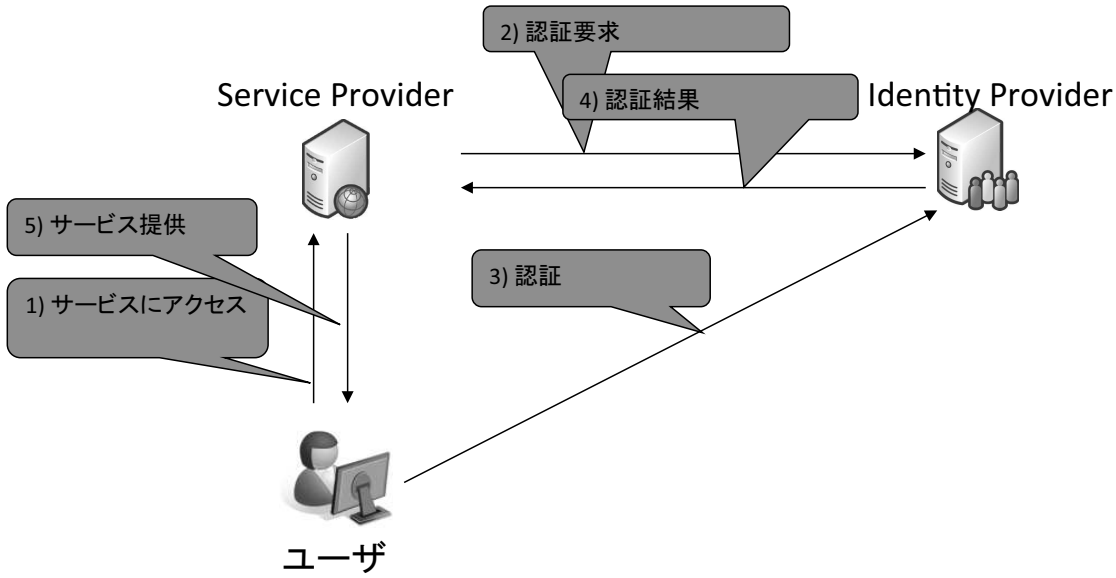


図 1.2: フェデレーションの概要

レーションと呼び，実際に日欧米を中心に学術機関が共同で学術フェデレーションを形成して，電子ジャーナルへのアクセスなどに活用されている．SP 中心フェデレーションは，SP にとっても，包括契約で多くの組織とエンドユーザを獲得できれば営業効率が上がる (他の顧客に営業リソースを投入できる) などのメリットがあり，学術機関に限らず ICT サービスを共有する医療機関連携や，グループ企業による SaaS 利用などもユースケースとして考えられる．

1.2 身元確認と登録機関の課題

1.2.1 登録機関の配備方式

あるエンティティをアイデンティティ管理するにあたっては，エンティティの身元確認を含む登録業務が発生する．この登録業務を行う組織は一般に登録機関 (RA, Registration Authority) と呼ばれる．登録機関による身元確認の概要について図 1.3 に示す．この登録機関の配備方式には LRA(Local RA) と呼ばれる地理的にエンティティに近い位置でき登録業務を行うものと，RRA(Remote RA) と呼ばれ遠隔からエンティティの登録業務を行うものに大別できる．両方式の違いを図 1.4 に示す．

身元確認の典型は対面確認であり，RA とユーザに事前の面識がある，または写真付身分証明書を同時に提出するなどの前提が必要となるが，実社会における認識と同様の総合的に判断することができる，というメリットがある．歴史的には組織内 IdP など限定された範囲で運用する IdP が自身で RA を行うことが想定されていたが，IdP の大規模化 (登録対象と

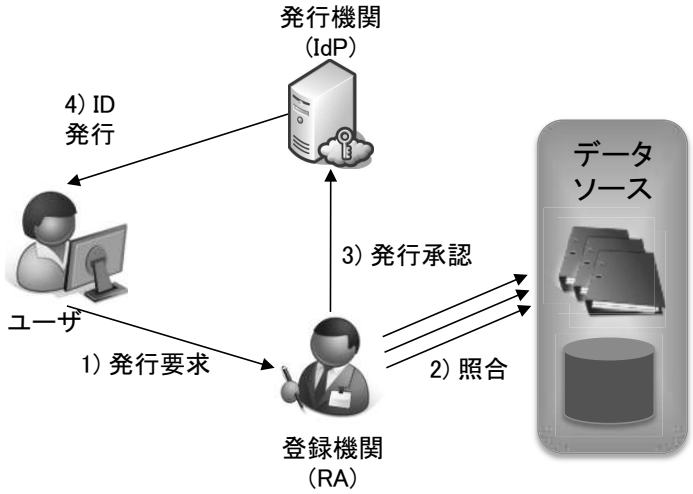


図 1.3: 身元確認の概要

するユーザの地理的広範化) に伴い，対面確認が可能な RA を明に LRA と呼ぶようになった経緯がある．このような LRA の典型例としては，本社による IdP 運用と，その下で各部署や事業所単位で LRA を運用する形態が挙げられる．LRA は対面確認に有利ではあるが，必ずしも対面確認を行うとは限らない．例えば，複数の分散したキャンパスを持つ大学において，大学教員が研究予算で短期雇用した研究員などの人事情報はキャンパス内部でしか管理しておらず，またその数が少なければ紙の台帳などで管理しているケースも珍しくない．こうした人事情報をもとに実在性確認などを行うには，RRA よりも LRA の方が低コストであることは明らかであり，そのために LRA を選択するケースもないわけではない．

これに対して，コンシューマ市場で LRA を実現できるプレイヤーは限られるため，RRA による遠隔の身元確認が発展してきた経緯がある．多数の，場合によっては不特定多数のユーザと事前に面識を持つことは困難であり，また写真付身分証明書を遠隔で提示されてもユーザとの同一性を確認することは難しく，あくまでも証跡として残す場合などもあり，RRA では LRA と異なる身元確認方式が発達してきた．1.1.3 節で触れたメールアドレスの到達性確認も，RRA において発展してきた方式と思われる．RRA における異色な身元確認方法のひとつに，認証局による証明書発行時の Outboubd-Call と呼ばれるものがある．これは，組織 X に所属するユーザ A を，他組織である RRA が身元確認するケースに用いられるもので，RRA からは意図的に組織 X の代表窓口や人事部などに電話をかけて，ユーザ A を呼び出してもらう，という方法であり，これによって組織 X にユーザ A が実在すること，また呼び出したユーザ A 本人と対話することで同一性を確認できる．組織外の RRA は，セキュリティや社員のプライバシーの観点から組織 X の社員名簿などを開示してもらえないケースも多いこと，一方で証明書を発行する認証局には高い保証レベルが期待されることなどから，こうした身元確認方法が確立された，と言える．

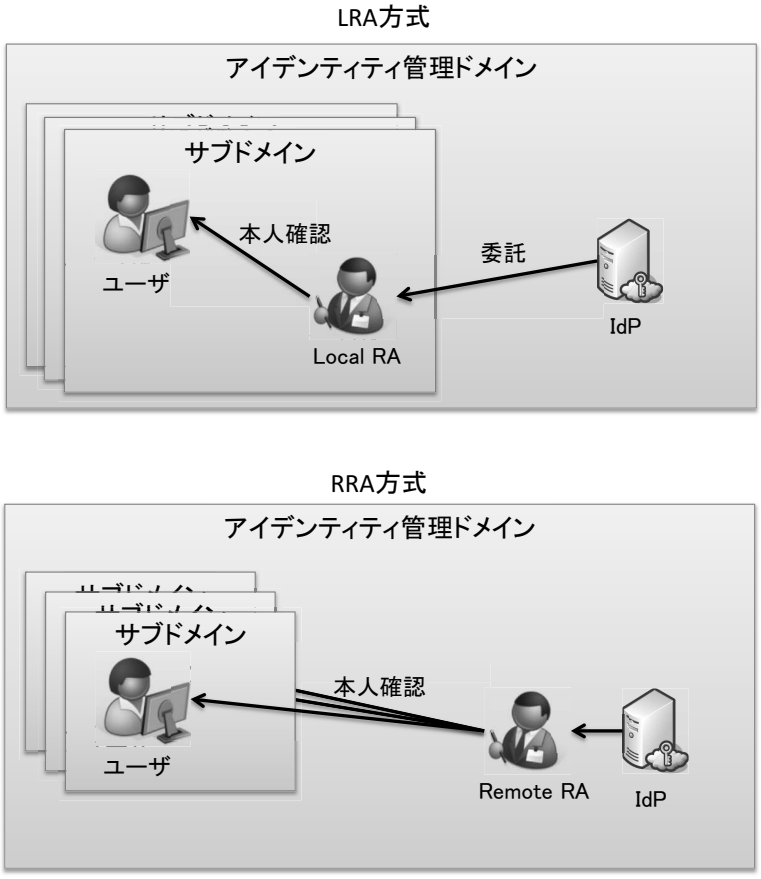


図 1.4: 登録機関の配備方式の違い

1.2.2 配備方式の比較

LRA はエンティティに近いために高い保証レベルの身元確認が行いやすく，エンティティに対する情報付が比較的豊富なので柔軟な身元確認が行い易いといったメリットが挙げられる一方で，各拠点に配備されるために人件費がかかる，といったデメリットがある．RRA は，遠隔で登録業務を行うため労働集約効果が期待でき，このため LRA よりも少ない員数で対応できか人件費が抑えられるというメリットがある．一方で LRA と比較するとエンティティに関する情報源は少なくなるため，例えばいくつかの身元確認書類についてエンティティ側で用意して提出することが求められるなど手続きが煩雑になりやすい，といったデメリットもある．このような身元確認に用いる情報源をデータソースと呼ぶ．

一般には，商用認証局などでも採用されていてコストメリットの高い RRA 方式が知られているが，RRA 方式では身元確認に利用可能なデータソースの制約が大きいという課題がある．RRA が直接参照可能なデータソースは限定されるために，前述のようにエンティティ側で身元確認書類を用意して提出することが求められたりする．あるいは RRA が参照可能なデータソースを新たに用意する選択肢もあり得るが，準備するにしても構築コストも運用コストもかかるため，既存のデータソースあるいは共用可能なデータソースでない限りは現実的ではない．これを整理すると表 1.1 のようになり，端的には RRA はコストメリット，

表 1.1: RRA 方式と LRA 方式の比較

	メリット	デメリット	アドバンテージ
RRA	員数が少ない 稼働率が高い	身元確認が煩雑になりがち 柔軟な身元確認が困難 データソース選択肢少	コストメリット大
LRA	高い保証レベルが容易 データソース選択肢多	員数が多い 稼働率が低い	高い保証レベル

LRA は保証レベルにそれぞれアドバンテージがある，ということがわかる．一方で，身元確認コストだけにフォーカスを当てて両方式を比較した場合，RRA よりも LRA の方が有利になりやすい．これは，RRA は参照可能なデータソースが限定される，あるいはプライベートなデータソースに関するアクセスコストが一般的に LRA よりも不利だからであり，さらに身元確認コストの比較においては，配備方式の員数による違いなどが考慮されないためである．このように，身元確認を設計するには RA の配備方式，保証レベル，参照するデータソース，個別および総合的な身元確認コストなど様々な点を考慮しなければならない．

過去の調査研究においても，適切なデータソース選定の難しさや運用コストの高さが指摘されている．日本情報経済社会推進協会では，データソースが網羅するエンティティの範囲や検証可能な属性情報の種類とその保証レベル，参照コストなどの難しさなどについて指摘するとともにするとともに，高い保証レベルの身元確認を行うシステムはそのシステム構築や運用にコストがかかることも指摘している [94, 97]．谷本らは，認証局を事例とした IdP の運用コスト構造を分析し，運用コストの中でも身元確認にかかる人件費が高いことを定量的に示した [64, 63]．このように，身元確認スキームの設計は難しく，またその結果は運用コストに反映されることになるため，影響は大きい．

1.3 本研究が取り組む課題と目的

これまで述べてきたように，フェデレーションの普及に伴い，IdP における身元確認の重要性はますます高まり，一方でその身元確認スキームの設計は難しく，また運用コストへの影響も大きい．そこで本研究では，SP に期待される保証レベルを損なうことなくコスト合理的な IdP 運用を可能とする，保証レベルに応じた身元確認スキームの設計手法の検討を目的とする．

身元確認コストに影響する大きな要素として RA の配備方式があり，その配備方式を決め

る制約としてデータソースがあることを 1.2.2 節で示した．基本的には RRA 方式にコストメリットがあるものの，保証レベルを保つ上では LRA 方式を補完的に組み合わせることで，よりコスト合理的な身元確認スキームが実現できるはずである．そこで本研究のひとつめのアプローチとして，保証レベルを保ちながらよりコスト合理的な身元確認を実現するために，RRA 方式と LRA 方式をよバランスよく組み合わせた身元確認スキームの設計手法を検討する．

一方，コスト合理的な設計が実現できたとして，運用を続ける IdP にとってはそのスキームの範囲で様々なコスト改善を行っていく必要があり，そこでは身元確認そのものの運用コスト構造を評価する必要がある．谷本らは，IdP の運用コストにおける身元確認の人件費の高さを定量的に示したが，身元確認そのものの運用コスト構造までは分析していない．そこで本研究のふたつめのアプローチとして，身元確認のコスト構造の定量的なモデル化について検討する．

1.4 本論文の構成

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．はじめに身元確認を議論するにあたって必要な概念としてアイデンティティ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．最後に，4 章のサーバ証明書における身元確認を議論するにあたって必要な技術としてサーバ認証の仕組みと証明書を発行する認証局について概説する．

第 3 章では，アイデンティティ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，保証レベルに応じた認証基盤のアーキテクチャ設計事例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，さらに身元確認コスト構造の分析例として，アイデンティティ管理の一応用としての UPKI においてキャンパス PKI と呼ばれる大学の学内認証基盤におけるコスト構造分析について先行研究として示す．

第 4 章では，IdP においてそ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コスト指向設計手法について提案する．はじめに商用認証局の身元確認スキームについて調査を行い，身元確認コストと保証レベルの両者に関連の深いデータソースの評価項目を分析した．この評価項目から与えられた，データソースのコスト合理的な選定を可能とするマトリクスをもとに，コスト指向の身元確認スキーム設計手法を提案した．本提案手法は，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」に対して実装・評価を行い，その実用性を明らかにした．

第 5 章では，前述の評価項目をもとに，保証レベルに影響を与えない身元確認のコスト構造をモデル化する．これによって保証レベルを変更を伴わないコスト評価やコスト改善が可

能となる．このコスト構造モデルを実際にいくつかの事例に当てはめることでモデルの妥当性を実証評価した．

第 6 章では，本研究が取り組むサイバーフィジカル融合社会におけるアイデンティティ管理の運用コストに関する問題について改めて概観し，本研究の寄与について示した上で，最後に本研究についてまとめる．

第2章　準備：身元確認と保証レベルの理解

本章では，本研究を議論するにあたって必要な概念や技術について述べる．はじめに身元確認を議論するにあたって必要な概念として，アイデンティティ管理について概説し，この中で身元確認がどのような位置付けにあるのか述べる．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し，この中で保証レベルがどのような役割を果たしているのか述べる．最後に，4 章で述べるサーバ証明書における身元確認を議論するにあたって必要な技術として，その利用形態であるサーバ認証の仕組みと，サーバ証明書を発行する認証局について述べる．

2.1　アイデンティティ管理

本節では，1.1.2 節で触れたアイデンティティ管理について，具体的に解説する．

2.1.1　アイデンティティ情報

アイデンティティ管理においては，1.1 に示したように，人やモノなどのエンティティを，エンティティが持つ様々な属性情報と，個々のエンティティを識別するための識別子，その識別子と紐付いたクレデンシャルのの 3 種類の要素によって構成されるものとして扱い，個々のエンティティについての 3 つの要素の集合をアイデンティティ情報と呼ぶ．即ちアイデンティティ管理とは，人やモノなどのエンティティを情報空間で扱い易いアイデンティティ情報に紐付けて，そのアイデンティティ情報の管理を行うことである．ここではアイデンティティ管理を行うものをアイデンティティ管理者，管理されるエンティティを管理主体，アイデンティティ管理者が管理する管理主体の範囲をアイデンティティ管理ドメインとそれぞれ呼ぶ．

2.1.2　アイデンティティ情報のライフサイクル

このエンティティをアイデンティティ情報に紐付ける作業は，アイデンティティ管理において登録 (Enrollment または Registration) フェーズと呼ばれる．登録フェーズを含むアイデンティティ情報のライフサイクルを図 2.1 に示す．アイデンティティ情報は，基本的にこのライフサイクルに従って管理される．

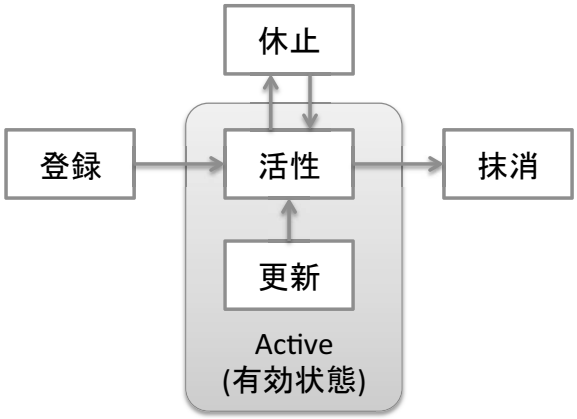


図 2.1: アイデンティティ情報のライフサイクル ([67] 図 1.1-5)

登録 エンティティからのアイデンティティ情報の発行要求などをトリガとして，所定のアイデンティティ情報について身元確認を行い，アイデンティティ情報の登録と発行を行う．ここで行われる身元確認については，2.1.3 節で後述する．

活性化 登録されたアイデンティティ情報を活性化することによって，アイデンティティ情報が有効となり，各エンティティはアイデンティティ情報を利用してサービスを利用可能になる．サービス提供者は，アイデンティティ情報をもとにサービスの提供を行う．例えばサービス提供者は，サービスリソースへのアクセス権限の確認にアイデンティティ情報を参照することが可能である

更新 アイデンティティ情報は，エンティティの状態や意向，サービス提供者の意向などによって更新される場合がある．更新は所定のポリシに従って行われる．

休止および抹消 エンティティの状態や意向，サービス提供者の意向などによってアイデンティティ情報は休止あるいは抹消される場合がある．いずれの場合もアイデンティティ情報は非活性化され，各エンティティはアイデンティティ情報を利用できなくなる．休止は，将来的にアイデンティティ情報を復活させる可能性が高い場合などに用いて，再活性化する場合にアイデンティティ情報を再利用できるようにするものである．抹消は，アイデンティティ情報が再利用できないように削除するものである．[1]

2.1.3 身元確認とアイデンティティ情報の登録

登録フェーズでは，登録対象となる管理主体について，所定の身元確認ポリシに従って身元確認に必要な情報を収集し，これらの情報をもとに所定の判定基準にもとづいて身元確認

[1]ただし，電話番号などのように識別子の資源が限られている場合には，一定の使用不能期間を経て同一識別子を別のエンティティに割り当てるケースもある．

を行う．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いる [90].

身元確認を行うものは一般に登録機関 (Registration Authority, RA) と呼ばれ，アイデンティティ管理者自身が務める場合と，第三者に委託する場合がある．登録機関は，身元確認に成功したエンティティについて，一意な識別子を割り当て，収集した情報のうち所定のものを属性情報としてこの識別子に紐付けて管理する．

(1) クレデンシャルの発行

管理主体のみが知り得るクレデンシャルは，この登録フェーズの中でアイデンティティ管理者によって発行され，身元確認された管理主体に安全な方法で配付されるか，あるいは登録の過程において，管理主体が生成・管理し，クレデンシャルの検証に必要な情報をアイデンティティ管理者に送付する，などいくつかバリエーションがある．アイデンティティ管理者は，管理主体が当該クレデンシャルを所有していることを検証するための検証情報を，識別子に紐づけて管理する．

2.1.4 登録機関の配備方式

アイデンティティ管理ドメインが地理的に広範な場合などには，管理ドメインを管理主体の近隣組織や部署など複数のサブドメインに分割して，サブドメイン毎に登録機関を配備して運用する場合がある．このように管理主体の近隣に配備される登録機関は一般に LRA(Local RA) と呼ばれ，これに対して管理主体から地理的に離れた場所から遠隔で身元確認などを行う登録機関を本論文では便宜上 RRA(Remote RA) と呼ぶ．両者の違いを図 2.2 に示す．LRA は，管理主体の近隣に位置するため，対面確認が比較的容易であるというメリットがあるが，サブドメイン毎に配備されるため人員の頭数が必要になるのと，RRA と比較して一人あたりの処理件数が少なくなりがちのため，習熟度が上がりにくい，教育効率が悪いなどのデメリットがある．RRA は，管理主体との接点が少ないあるいはまったくなく，また遠隔での運用になるため，対面確認が困難というデメリットがあるが，管理主体が多いほど労働集約効果が効き，また習熟度も上がりやすいといったメリットがある．LRA は，全国に複数の事業所を持つ組織が事業所毎に LRA を配備しつつアイデンティティ管理は本社で一括して行う，というケースなどでしばしば用いられる．RRA は，商用認証局の多くがサポートしているが，一方で代理店制度などを持つ認証局の場合は，これらの代理店が LRA に近い位置付けと捉えることもできる．

典型的なフローとして，公的個人認証サービスにおける電子証明書の発行の例を挙げる．なお，管理主体となる市民は，事前に住民基本台帳カード (住基カード) および IC カードリーダ・ライタなど必要なものは予め入手しているものとする．まず市民は，住基カードと所定の発行申請書を用意して，在住自治体の市区町村窓口で発行申請を行う．発行申請を受けた行政担当者は，提示された住基カードを用いて身元確認を行い，電子証明書に記載する氏名・性別・生年月日・住所を属性情報として管理する．この時，市民は住基カードを窓口

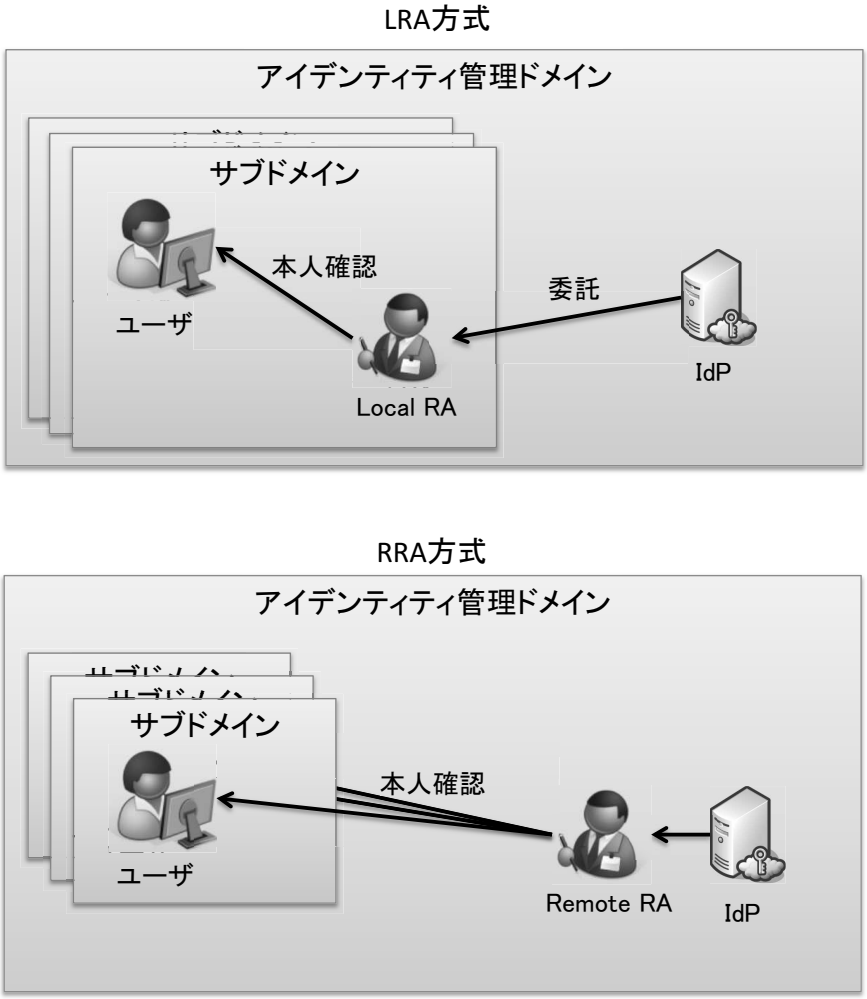


図 2.2: 登録機関の配備方式の違い

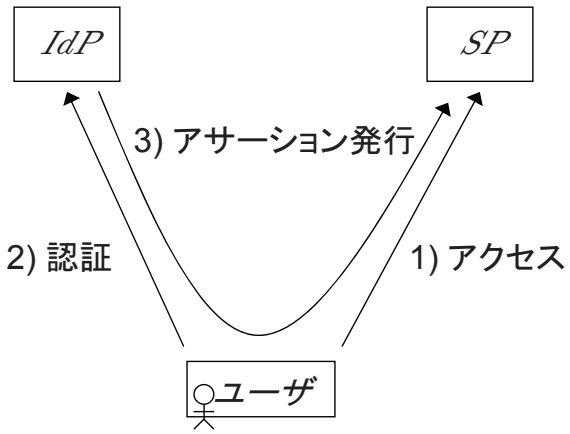


図 2.3: フェデレーションの概念図 ([84] 図 3 より©2011,IEICE)

の IC カードリーダ・ライタにセットして住基カード内で私有鍵と公開鍵の鍵ペアを生成する．公的個人認証サービスによって，ここで生成された公開鍵に対して電子証明書がその場で発行され，ここで発行された証明書も属性情報と併せて自治体によって管理される．

2.2 フェデレーション

フェデレーションでは，認証を必要とするサービス提供者 (Service Provider: SP) は，ユーザを直接認証するのではなく，図 2.3 に示すようにアイデンティティ情報提供者 (Identity Provider: IdP) に問い合わせてアサーションと呼ばれる認証結果を取得し，その内容にもとづいてアクセス制御を行う．

近年では，サービスにおける認証機能の独立化が進み，外部のアイデンティティ情報を活用するサービスが増えている．こうした複数の組織間でアイデンティティ情報を交換する行為は一般にフェデレーション連携と呼ばれ，組織間の信頼関係が不可欠となる．本節では，このフェデレーションの概観について示す．

2.2.1 フェデレーションの仕組み

一般的なフェデレーションの関係者は以下によって構成される．

エンティティ サービスを利用とする人やモノ．

サービス提供者：Service Provider(SP) エンティティにサービスを提供する人や組織．IdP が提供する認証結果を信頼する．

アイデンティ情報提供者：Identity Provider(IdP) エンティティを認証し，SP に対して認証結果と，必要に応じてエンティティのアイデンティティに紐付いたアイデンティティ情報を提供する．

フェデレーションの仕組みは，図 2.3 にもとづき以下のような流れで実現される．エンティティがサービスを利用しようと SP にアクセスした場合，SP は直接エンティティを認証するのではなく事前に信頼関係を構築した IdP に認証を依頼する．エンティティは IdP に対して所与のアイデンティティ情報を用いてログインすることで，IdP から SP に認証結果等が返される．SP は IdP からの認証結果を信頼し，エンティティにサービスを提供する．

2.2.2 実装

本方式には SAML[38] や WS-Federation[20]，OpenID[57] など様々な標準仕様が存在するが，いずれもアサーションのフォーマットやプロトコルなどを標準化することにより，SP はユーザに応じて異なる IdP に問い合わせることが可能である．安全性向上のために，アサーションは IdP による署名や SP のための暗号化が可能であり，そのためには署名検証に必要な IdP 証明書や暗号化に必要な SP 証明書を，事前に安全な方法で入手しておく必要がある．

(1) SAML

Security Assertion Markup Language (SAML) は，Organization for the Advancement of Structured Information Standards (OASIS) のセキュリティサービス技術委員会 [10] によって，通信を行うユーザの認証・認可に対する XML ベースのフレームワークとして標準化されたもので，複数組織間での認証認可を行う規格である．SAML は，Web サービス間で認証情報の他に，認可などに用いる属性情報の交換や，交換した属性情報にもとづいて決定されるアクセス制御情報の交換を行うプロトコルを規定しており，メッセージの送受信には HTTP または Simple Object Access Protocol (SOAP) を用いる．これら認証情報，属性情報，アクセス制御情報はアサーションと呼ばれ，プロトコルは要求とレスポンスによって構成される．アサーションは XML 形式で記述され，ユーザと IdP の間での具体的な認証方法については規定せず拡張可能性を持たせている．IdP と SP の間では，予めメタデータと呼ばれる XML 形式の情報を共有しておく必要がある．これはある種の信頼関係の構築と言ってよい．メタデータには，相互に連携可能な IdP や SP について，それぞれのエンドポイント URL や公開鍵情報が記載される．IdP のエンドポイント URL には，SP から IdP に認証情報を要求する際にアクセスする URL が記述され，SP のエンドポイント URL には，IdP が発行するアサーションに記載する SP の URL(アサーションののリダイレクト先) が記述される．IdP や SP の公開鍵情報には，SP が IdP に，あるいは IdP が SP にアクセスする場合に必要な TLS サーバ認証のためのトラストポイントなどを記載する．

SAML では，認証コンテキストクラスを用いてユーザと IdP の間で利用する認証方法を指定することができ，指定可能な認証方法は [47] で規定されている．

(2) Shibboleth

Shibboleth は，Internet2/Middleware Architecture Committee for Education のプロジェクト名であり，同プロジェクトが開発したオープンソースソフトウェアの名称 (以下，単に Shibboleth) でもある [13]．Shibboleth プロジェクトでは，プライバシー保護を目的として，ユーザのアイデンティティを IdP が管理し，ユーザ認証後に SP が必要とする属性のみをアサーションに含めて SP に送信する仕様を策定し，この仕様は最終的に SAML 2.0 に取り込まれた．Shibboleth には，IdP，SP その他のコンポーネントが含まれており，Shibboleth v2.0 以降では SAML 2.0 に準拠したアサーション交換が可能である．即ち，Shibboleth は基本的に SAML 2.0 をベースとした仕様と言える．Shibboleth の特徴は，IdP から SP に提供される属性情報の種類をユーザ自身が選別できるなどプライバシー保護に重点をおいていることと，学術機関での利用を想定した eduPerson と呼ばれる属性情報のオブジェクトクラスを定義している点にある．このため，日欧米をはじめ世界中の学術機関で広く導入されており，例えば日本の学術認証フェデレーション「学認」[75] においても Shibboleth を前提とした設計 [46] になっている．

(3) OpenID Connect

OpenID Connect は，OpenID Foundation[12] が策定した規格であり，クライアントアプリケーションに対する認可フローを提供する OAuth 2.0 の上でエンドユーザの認証情報を交換する機能を追加したものである．SAML が SOAP ベースでシステムの状態やセッションに依存した複雑な仕様になりがちなのに対して，OpenID Connect はシステムの状態やセッションに依存しない，いわゆる RESTful な仕様になっている．なお，OpenID Connect では，IdP のことを OpenID Provider(OP)，SP のことを Relying Party(RP) と呼ぶが，本論文ではそれぞれ IdP および SP で表記を統一する．

2.2.3 保証レベル

フェデレーションを実現するには，技術の実装だけではなく，異なる組織である IdP と SP の間に事前の信頼関係の構築が必要である．SP にとっては IdP の認証結果がどの程度の確からしさ (なりすましにくさ) を持つのかが重要となるが，IdP の認証結果を信頼するためには技術仕様だけでなく認証情報 (パスワードや認証に使用する暗号アルゴリズム) の強度や，内部不正や外部からの攻撃に対する IdP のセキュリティ対策，ID 発行時の身元確認の確からしさなどを総合的に判断する必要がある．

こうした認証情報の確からしさを表す尺度と，それを構成する要素をを含めた Entity Authentication Assurance Framework (EAAF) が，ISO/IEC　29115 および ITU-T X.1254 として標準化されており [6, 27]，その概要を図 2.4 に示す．認証情報の確からしさを表す尺度は「(認証の) 保証レベル」と呼ばれ，以下の項目のリスク評価にもとづいて決定される．

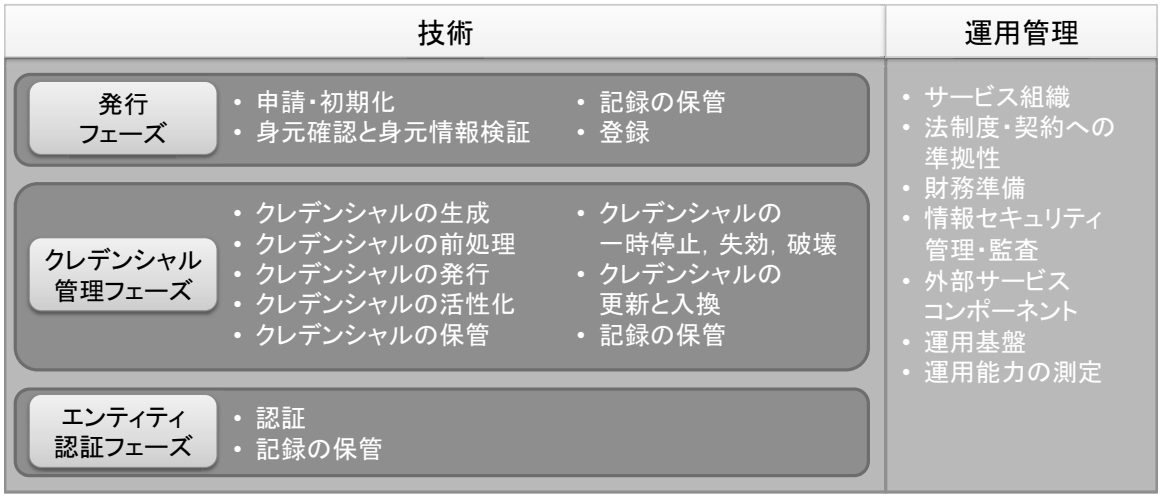


図 2.4: EAAF の概要 ([27]Figure 1 より)

EAAF(あるいは EAAF を参照するトラストフレームワークなど) に準拠しようとする IdP は，まず自身が遵守すべき保証レベルを選択した上で，EAAF からその保証レベルに応じた技術・運用要件を参照し，各要件を遵守することが求められる．EAAF では，IdP が遵守すべき要件は以下の 5 項目に分類される．

- 登録と身元確認
- 認証トークン
- トークンとクレデンシャルの管理
- 認証プロトコル
- アサーションの渡し方

各項目ごとに認証における脅威が示されており，保証レベルに応じて対策が異なる．従って，IdP は各項目の脅威に対して，保証レベルに応じた対策を実施することによって，保証レベルを満たしている，と言える．

- 認証の脅威
    - 実行中の認証プロトコルに対する攻撃などの脅威
    - 認証に用いられるクレデンシャルに対する攻撃
- 潜在的な被害
    - 不便，苦痛もしくは地位や評判に対する打撃
    - 財務上の損失または政府機関の賠償責任
    - 組織およびその活動計画または公共の利益に対する害
    - 機密情報の無許可公開
    - 身の安全
    - 民事上または刑事上の法律違反

一方の SP は，このうち「潜在的な被害」について表 2.1 にもとづき自身のサービスのリスク評価を行い，さらに表 2.2 に応じて IdP に要求する保証レベルを決定する．

従って IdP は，選択した保証レベルに応じて，アイデンティティ情報を提供できる SP の範囲が決まることになる．このようなアプローチで保証レベルに応じた身元確認要件を決定する手法は，3.1.1 節で後述するように多くの分野で採用されている．

2.2.4 トラストフレームワーク

IdP と SP の間に事前の信頼関係の構築が必要であることを 1.1.5 節で述べた．IdP や SP の数が増えればこうした信頼関係確立コストが課題となるため，一定のポリシに準拠する IdP や SP によって構成されるトラストフレームワークという組織を形成することで効率化することができる．

(1) Open Identity Trust Framework Model

トラストフレームワークを示す典型的なモデルとして，Open Identity Trust Framework (OITF) Model[49] が知られている．これは，IdP や SP がオープンにフェデレーションできるようにすることを目的に，OpenID Foundation (OIDF) および Information Card Foundation (ICF) によって開発されたモデルである．OITF Model の概要を図 2.5 に示す．従来のフェデレーションが，IdP と SP が直接連携する，いわゆるトライアングルモデルだったのに対して，OITF Model では，IdP および SP は Trust Framework Provider (TFP) と呼ばれる組織を介して契約を結ぶ．TFP は，ポリシーメーカーが策定したポリシーに基づいて運営され，契約によってこのポリシーを IdP および SP にも遵守させる．IdP および SP がポリシーを継続的に遵守していることを確認するために，TFP は査定人 (Asseessor) と契約を結んで定期的に IdP および SP の査定を行う．この査定人に対する要件もまたポリシーで定められる．このように，複数の IdP および SP が遵守可能なポリシーを策定し，これを遵守するフレームワークを整備することによって，IdP と SP の信頼関係をスケールさせることが容易になる．

(2) 学術認証フェデレーション

SAML ベースのフェデレーションでは，参加する全ての IdP および SP の証明書を含んだメタデータと呼ばれる XML ファイルを，全ての IdP および SP で共有する．IdP および SP は，メタデータに署名するフェデレーション証明書を信頼するだけで，全ての IdP および SP と信頼関係の確立が可能となる．実際に運用するには，ポリシーの策定，IdP や SP がポリシーに準拠していることの継続的な査定，増減する IdP および SP の情報のメタデータへの反映，メタデータを公開するリポジトリの運用などを行う，フェデレーション運営組織が必要になり，これは前述の OITF モデルで言うところの TFP に相当する組織と言える．

表 2.1: 潜在的な被害と影響 [35]

	Low	Moderate	High
不便，苦痛もしくは地位や評判に対する打撃	短期間における限定した損害	短期間における深刻な損害，あるいは長期間における限定した損害	長期間における深刻あるいは非常に厳しい侵害
財務上の損失または政府機関の賠償責任	あまり重要でない，取るにたらない回復不可能な金銭的ロスあるいは組織の責務	深刻な回復不可能な金銭的ロスあるいは組織の責務	非常に厳しいまたは壊滅的な金銭的ロスあるいは組織の責務
組織およびその活動計画または公共の利益に対する害	組織運用や資産，公益に対して限定されている逆の効果の波及	組織運用や資産，公益に対して深刻な逆の効果の波及	非常に厳しいまたは壊滅的な逆の効果の波及
機密情報の無許可公開	影響度の低い機密性損失における個人的，米国政府機密，商業上の機密情報の未許可組織への開示	影響度が中程度の機密性損失における個人的，米国政府機密，商業上の機密情報の未許可組織への開示	影響度の高い機密性損失における個人的，米国政府機密，商業上の機密情報の未許可組織への開示
身の安全	医療措置を必要としない傷害	たいしたことのない傷害の中程度のリスク，あるいは医療措置を必要とする限定したリスク	深刻な障害あるいは死のリスク
民事上または刑事上の法律違反	民事上あるいは刑事上の違反	法執行をうける民事上あるいは刑事上違反のリスク	法執行計画において非常に重要な民事上あるいは刑事上違反のリスク

表 2.2: 潜在的な被害と保証レベルのマッピング ([35]Table 1 より)

認証エラーによる潜在的な影響のカテゴリ	保証レベル			
	1	2	3	4
不便，苦痛もしくは地位や評判に対する打撃	Low	Mod	Mod	High
財務上の損失または政府機関の賠償責任	Low	Mod	Mod	High
組織およびその活動計画または公共の利益に対する害	N/A	Low	Mod	High
機密情報の無許可公開	N/A	Low	Mod	High
身の安全	N/A	N/A	Low	High Mod
民事上または刑事上の法律違反	N/A	Low	Mod	High

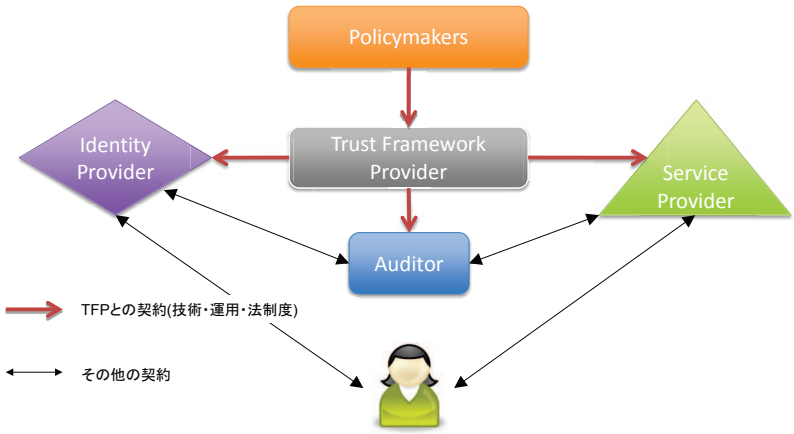


図 2.5: Open Identity Trust Framework Model[49]

2005 年頃から，世界各国の学術コミュニティで Shibboleth を利用した認証フェデレーションの構築が進み，2011 年 1 月時点で日欧米を中心とした約 25 カ国で運用が行われている [3, 8]．特に，米国の InCommon，英国の The UK Access Management Federation，スイスの SWITCHaai において様々な連携が行われている [9, 18, 15]．国内においては国立情報学研究所が運営する学術認証フェデレーション「学認」があり [75, 105, 68]，各大学でも導入が進められている [71, 93, 89]．

2.3 サーバ証明書の基本概念

2.3.1 サーバ認証の仕組み

サーバ認証の仕組みとして広く知られている技術として TLS サーバ認証 [40] がある．TLS サーバ認証は，Web ブラウザなどのクライアントがサーバへアクセスする際にサーバのなりすましがないことを確認するために行われる．具体的には，1) サーバ証明書によるサーバ名称などの確認と，2) サーバ証明書の検証によって行われる．これを実現するために，サーバは事前に PKI における認証局から，サーバ名称 (FQDN[50]) やサーバの所属組織，サーバの署名検証鍵などが記載されたサーバ証明書の発行を受けておく必要がある．その上で，1) は，クライアントのアクセス URL などが，サーバから入手したサーバ証明書の記載内容と合致することなどを確認することで実行される．2) は，1) で確認したサーバ証明書の内容が改ざんされていないこと，サーバ証明書の発行者である認証局がクライアントにとって信頼できる認証局であることを確認することで実行される．これは，サーバ証明書をその発行者である認証局の署名検証鍵で署名検証に成功し，その認証局の署名検証鍵が信頼できる認証局の証明書に記載されたそれと一致していることによって確認できる．

なお認証局は，さらに上位の認証局から証明書を発行されている場合がある．その場合は図 2.6 に示すように認証局を上位に辿っていき，最終的にルート認証局と呼ばれる認証局まで辿る必要がある．こうしたサーバ証明書からルート証明書までのシーケンスは証明書パスと呼ばれる．

ルート認証局の署名検証鍵は，基本的にクライアントが管理する「信頼する認証局リスト」に含まれている．具体的には，リストには認証局が自身に対して発行したルート証明書があり，そこには認証局の署名検証鍵が記載されている．

2.3.2 パブリック認証局とプライベート認証局

クライアントの「信頼する認証局リスト」には，予めいくつかのルート証明書が登録されており，これらは一般にパブリック認証局と呼ばれる．パブリック認証局は，クライアントのポリシ (例えば [52] など) に従い，[29] など第三者評価を必要とする認証局運用認定規準の認定を原則として取得している．パブリック認証局は，こうした第三者評価を受けることにより，不正な証明書を発行しない，あるいは万が一発行しても速やかに失効できる体制を確立するなどの運用安全性を客観的に主張することが可能となる．

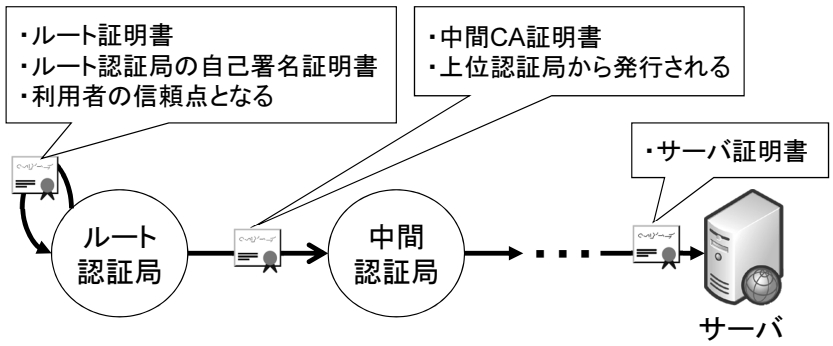


図 2.6: 証明書パス ([83] 図 1 より©2012,IEICE)

一方，一部のクライアントでは「信頼する認証局リスト」に後から利用者がルート証明書を追加登録することも可能であり，このような認証局はプライベート認証局と呼ばれる．プライベート認証局もまた，一定の運用安全性が求められるべきだが，運用安全性を評価する情報がプライベート認証局の場合は必ずしも十分に開示されていない，運用安全性を評価するには十分な認証局運用知識が必要であり一般の利用者には的確な判断が難しい，ルート証明書を利用者になりすましや改竄の危険性がない安全な経路で配付する必要がある，などいくつかの課題がある．さらに，2005 年頃からフィッシング詐欺の危険性が高まるとともに，いわゆるオレオレ証明書が問題視されたことにより [78, 86]，信頼する認証局リストへルート証明書を追加登録する作業が意図的に煩雑化されたことや，スマートフォンなどインターネット接続を前提とした携帯端末や組込み機器の出現によりサーバ認証を扱うクライアントの多様化が進み，プライベート認証局を導入した場合に発生するコストは従来よりも大きく膨らみやすくなってきている．一般に，プライベート認証局はパブリック認証局よりも運用コストが低い点が大きな魅力の一つとされていたが，こうした現状においてはプライベート認証局の方が優位な場面は，利用者数やクライアント種別を一定の範囲に制限できる場合に限られるようになってきた．

2.3.3 登録業務の形態

証明書発行における登録業務とは認証局業務の一部であり，主に 1) 加入者に対する窓口業務，2) 審査項目の確認，3) 認証局に対する証明書発行・更新・失効指示などを請け負う．この登録業務を行う組織は RA(Registration Authority) と呼ばれ，認証局業務の一部として基本的に認証局事業者が実施する．

しかし例えば身元確認において加入者への対面確認が求められているにも関わらず加入者が遠隔地に分散している場合や，負荷分散のために複数の組織で登録業務を行う場合など，認証局と一体で行うのではなく図 2.7 のように RA の一部または全部の権限を委任して登録業務を分散する，いわゆる LRA(Local RA) を設置して対応するケースもある [58].

サーバ証明書を発行する商用認証局の多くは不特定多数を対象とするため基本的に LRA を持たないが，大口顧客や代理店販売などにおいて LRA を委任するケースも存在する．プ

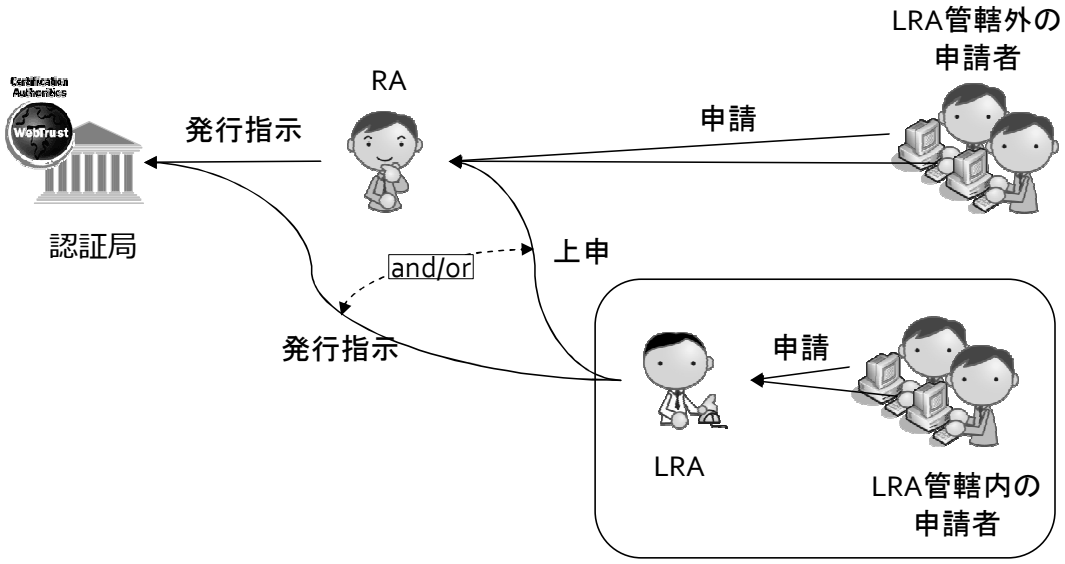


図 2.7: RA/LRA の違い ([83] 図 2 より©2012,IEICE)

ライベート認証局においては，例えば本社に認証局および RA，支社に LRA を設置して運用するケースなどがある．

2.3.4 規程類の継続的な遵守

一般に，多数の相手に所定の規程に対する継続的な遵守を求める合理的な方法のひとつとして，組織の会計や内部統制などに広く用いられている監査の仕組みがある．監査対象業務では規程に準拠する形で帳票などの証跡を継続的に作成・保管する必要があり，また一連の証跡には整合性が要求されるため，一定の準拠性を担保する合理的な方法として情報セキュリティ監査 [48] などにも広く利用されている．一方で，監査を実施するには監査実務に精通した監査人が必要とされ，監査を受ける側も監査人による膨大な量の証跡へのアクセシビリティを確保する必要があるなど，双方に相応の負担が発生する．こうした負担を軽減しつつ一定の準拠性を実現する仕組みとして，青色申告などで知られる監査権の留保が挙げられる．これは，定期的な監査は要求しないものの必要に応じていつでも監査を要求できる権利を保持しておくことで，証跡の継続的な作成・保管を義務化しつつ監査負担を最小限に抑える仕組みである．

第3章　関連研究・動向

本章では，はじめに本研究に関連する先行研究について示す．その上で研究とは違うもののフェデレーションにおける身元確認に関連する動向とを示す．最後に関連研究のひとつとして，UPKI3 層アーキテクチャについて示す．

本章では，はじめに，身元確認スキームの設計手法やそのコスト構造に関連する先行研究について述べる．次に，身元確認スキームも含めたトラストフレームワークの応用について，その動向を示す．最後に，多様な保証レベルに対応しつつコスト合理的なアーキテクチャに取り組んだ一例として，UPKI3 層アーキテクチャについて述べる．

3.1　先行研究

本節では，フェデレーションにおける身元確認スキームの設計手法および身元確認コストの分析・評価に関する先行研究・関連動向についてまとめる．

3.1.1　フェデレーションにおける身元確認スキームの設計手法

フェデレーションにおいては，SP は第三者である IdP の提供するアイデンティティ情報を信頼する必要があり，これを実現するためのフレームワークとして EAAF があることを 2.2.3 節で述べた．この EAAF の原型となった米連邦政府の OMB M-04-04 および SP 800-63 では，サービスのリスクを認証の脅威にもとづいて分析し，許容可能なリスクに対応する保証レベルを決定し，この保証レベルで規定される身元確認要件や技術要件をもとに，身元確認スキームを実装する手法を確立した [35, 43]．リスク評価にもとづいて適切な保証レベルとそれにもとづく実装の評価の概観を図 3.1 に示す．この図で示すところの 2 点目でマッピングされた保証レベルにおいて規定される身元確認要件と，3 点目で選択した技術要件によって身元確認スキームが与えられることになる．

しかしながら，このアプローチでは，与えられた身元確認要件の範囲でどのような身元確認方法を具体的に設計すればよいか，という方法論が不足しており，議論された事例も見当たらない．また，こうしたアプローチの多くは国民 ID の類を発行する行政機関において検討されており，各プレイヤーのビジネスインセンティブまでは考慮されていないという課題がある．これは，ビジネスであればインセンティブを与えないと実質的に継続が困難な作業であっても，例えば行政機関の場合には立法によって義務化が可能であったり，予算確保さえできれば受益者負担に依存することなく運用継続も可能，という点でアドバンテージにな

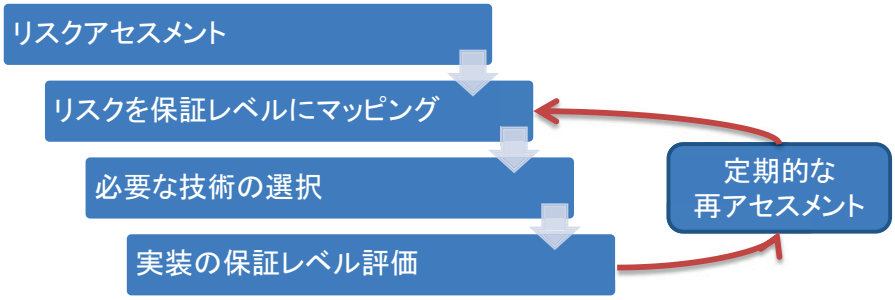


図 3.1: リスク評価による保証レベルの決定

る一方で，行政機関以外ではこれらの問題を解決しない限り同様のアプローチは難しい，ということでもある．

この手法は，国際標準化 [6, 27] されたとともに，カナダ [14, 31] やニュージーランド [53, 39] をはじめ様々な国や業界で応用されており，日本においても内閣官房によってオンライン手続を対象とした認証ガイドライン [72] が策定されている．

この手法は，IdP と SP の信頼関係を構築することが目的であり，本研究においても合目的であるが，身元確認スキームは予め規定された身元確認要件と技術要件に依存することになる．しかしながら，SP 800-63 をはじめとする関連研究においては，IdP の汎用性を保つために RRA と LRA の両方の選択肢を有しており，いずれを選択するのがコスト効率的かを判断するには別の評価基準が必要となる．5 章で後述するような RRA と LRA を比較評価できるコストモデルは先行研究では与えられていないため，コスト効率性を判断することができないという課題がある．

3.1.2 身元確認のコスト構造の分析

身元確認コストそのものについて分析・評価した先行研究は見当たらないものの，ID 管理の一応用である PKI についてはコスト分析・評価の先行研究が示されている．本節では，これら PKI におけるコスト分析・評価に関する先行研究・関連動向についてまとめる．

谷本らは大学の学内認証基盤，いわゆるキャンパス PKI[103, 102] を対象として，そのコスト構造について定量的に分析を行った [100, 101, 59, 63]．彼らはキャンパス PKI の人件費について Work Breakdown Structure にもとづいてキャンパス PKI の構築・運用にかかる作業項目を洗い出し，これをもとに人件費の見積りを行った．その上で，キャンパス PKI のプロトタイプ運用を通じて工数を実測し，見積りとの比較評価を行った．これにより，キャンパス PKI の構築・運用にかかるコスト構造を明らかにしつつ，プロトタイプ運用によってその妥当性を評価したものである．この分析評価を通じて，PKI はその運用コスト，中でも身元確認にかかる人件費の比率が高いことを明らかにした．これは，身元確認にかかるコストの課題を定量的に示す有益な研究成果である．しかしながら，本研究のスコープである身元確認そのもののコスト構造まで踏み込んだ分析は行っていない．

OASIS の PKI Education 技術委員会では，PKI の ROI(Return of Investment) 分析のた

めのガイドラインを策定した [65]．この中で彼らは PKI の導入・運用における定量化可能な指標を列挙し，初期固定費と初期従量費，運用固定費と運用従量費に分類することで，総保有コストの見積もりを容易にした．しかしながら，各指標の費目の粒度は粗く，例えば運用従量費において「ヘルプデスク」が挙げられているものの，そのパラメータまでは明らかにされていない．このため，端的なコスト積み上げによる見積もりは可能であっても，シミュレーションなどのコスト評価にはそのままでは適用が難しい．

旧 PKI Forum(現 OASIS PKI 技術委員会) では，PKI ROI 計算式のリターンに対して適度に粒度の細かいフレームワークを提供した [37]．評価指標を整理し，収入，コスト，準拠性，リスクそれぞれにおいて，数値を改善させる選択肢を示している．しかしながら，あくまで定性的な分析に留まっており，このままでは定量的評価に応用することは難しい．

その他にも PKI の ROI 分析に関する研究はいくつかあるが，いずれも OASIS や PKI Forum と同様に PKI の導入前後でのコストメリットの比較に関するものであり [44]，導入後のコスト評価・改善にかかる調査研究は見当たらない．

3.1.3 身元確認のコスト評価

Argyroudis らは，参加するエンティティ間の経済価値の交換を試すための価値モデルで PKI の分析を行い，既存の侵害リスクを理解するためにリスクベースセキュリティ評価を行った [30]，彼らの分析は，PKI のセキュリティは身元確認に依存しており，その運用コストは身元確認ポリシーが厳しいほど増えることを示した．本モデルは，その身元確認コストの増加に対する改善が期待できる．

Platis らは，PKI ベースの金融取引における運用コストの評価のための確率モデルを研究した [55]．しかしながら，彼らの運用コスト分析は，証明書検証プロセスにおける失効確認のみにフォーカスしており，身元確認に関しては何ら議論されなかった．

これらの他にも PKI や ID 管理システムのコストにフォーカスしたいくつかの研究がある．しかしそれらのフォーカスは失効 [54]，信頼関係 [45]，認証方式やプロトコルの選択 [32, 36] であり，身元確認ではなかった．

3.1.4 身元確認やアイデンティティ情報に関する調査分析

日本情報経済社会推進協会では，身元確認に関連する調査を何度か行っており，それらの中で身元確認に関する課題として以下を挙げている [94, 97]．

(a) 散在する登録機関 エンティティの属性は多様であり，各属性を管理するアイデンティティ管理ドメインは必ずしも一元的ではない．例えば国民としての情報は行政機関によって管理されるが，患者としての医療情報は病院，しかも多くの場合は症例によって複数の異なる病院に管理されている．そして，これらの管理ドメインが相互に属性情報交換をすることはプライバシー保護や交換インセンティブの不足などにより，ほとんどないと言ってよい．

(b) 身元確認書類 身元確認書類として利用可能な書類は様々にあるが，書類によって対象者や記載情報，利用可能な媒体，顔写真の有無，更新頻度，取得容易性，普及率などが異なり，汎用的な身元確認書類が存在しない．結果，複数の身元確認書類に対応できる必要があり運用コストの増加につながる．

(c) コスト 高いレベルの身元確認を行うには，必要なシステムの構築や運用にかかるコストも無視できない．自動化すれば効率化できる代わりに初期投資が必要になり，また，自動化することで属性情報をシステムに入力・更新する必要が生ずるようであれば新たな運用コストが発生することになるかも知れない．

日本情報経済社会推進協会は，身元確認に関する先述の課題を指摘した上で，平成 28 年度から導入予定のいわゆるマイナンバー (社会保障・税番号制度) を活用したトラストフレームワーク [22] を提言している．マイナンバーが導入されれば，(b) が解決され，またマイナンバーを軸としたトラストフレームワークを構築することによって (a) も大きく改善されることが期待できる．

(c) については，マイナンバーの活用によってコスト効率化が大きく期待できるとされているが，その対象は基本的にマイナンバーを活用する組織の話であり，マイナンバーそのものの導入・運用コストについては議論されていない．マイナンバーは様々な分野での活用が期待され，共用効果が高いものの，分野横断的な活用に際してはプライバシー対策など取り組むべき課題もまだまだ多く，またマイナンバーの運用コストの合理性についても今後の評価が待たれるところである．

3.2 先行事例

2.2.4 で示したトラストフレームワークは，各国政府や業界など様々なところで実装が進みつつある．本節では，日米政府におけるアプローチについて示す．

3.2.1 米国政府のトラストフレームワーク政策

米国政府は先に述べた OMB M-04-04 や SP 800-63-2 をはじめ，古くから身元確認やアイデンティティ管理に関する取組みが活発であり，その動向は非常に参考になる．2008 年には FICAM(Federal Identity, Credential, and Access Management)[4] と呼ばれる活動を立ち上げ，政府関係者には高い保証レベルの身元確認とクレデンシャルを提供する一方で，国民に対してはインターネットの普及と利便性を考慮して民間 IdP を活用した行政サービスのためのトラストフレームワークの整備を進めている [11]．民間 IdP の活用にあたっては SAML や OpenID といった多様な技術に対応するため，政府の位置づけは，図 2.5 で言うところのポリシーメーカーとして振る舞うことになる．これにより，例えば Shibboleth をベースとする学認のような TFP も，また OpenID をベースとする他の TFP も，米国政府の規定するポリシーにさえ準拠していれば行政サービスを平等に利用できるようになる．

ICAM レベル感	分類	サービス名	相手の属性情報の確認が必要（法律、条令、自主規制など）	法律、施行規則などで、身分証明書の種類または提出数など、確認方法の限定または条件が課されている	身分証明書の発行元等に照会するかどうか
1相当程度	①-1	旅館・ホテル予約	× 情報提示のみ	×	×
	①-2	公営競技、toto（ネット投票）	○（何らかの身分証明書又はクレジットカード番号の入力により必要な属性情報を確認）	× 確認方法の限定または条件はない	×
		タバコ、酒販売、公営競技、toto販売			
		コンサート等のチケット（記名式）			
		映画館、カラオケ等の深夜利用、成人向け図書販売			
		交通機関等の（学生、シニアなど）割引利用			
		視聴年齢制限付き番組			
		オンラインゲーム			
	①-3	レンタル（DVD、車、介護用品、育児用品など）	○	△ 業界や事業者自身によって身分証明書の種類の限定または条件を課す場合がある。	×
		資格試験			
		タバコ販売（taspo）			
		結婚相手紹介			
	①-4	インターネット異性紹介		△ 身分証明書の種類の例示がある。	自己申告（保証レベル1）ではなく、一定の身元確認を行っている。
		古物（オークション）			
		質屋			
2相当程度	②	携帯電話・レンタル携帯電話契約	○	○ 条件を課している	×
		金融機関口座開設			
		ファイナンスリース口座開設			
		保険契約			
		クレジットカード契約			
		宅地建物取引			
		宝石・貴金属等取扱			
		郵便物受取サービス（私設秘書箱）			
		電話受付代行			
		電話転送サービス			
		旅館・ホテル予約（外国人）			
3相当程度	③	電子証明書の発行	○	○ 条件を課している	△ 住民票の写し、印鑑登録証等政府の登録DBの写しを求めている

図 3.2: 保証レベルにもとづくサービスの類型化 ([22] 図表 45 より)

3.2.2 経済産業省の ID 連携トラストフレームワーク

3.1.4 節で述べたように，日本では平成 28 年度からマイナンバーの導入が予定されており，これを見据えての活動と見られるが，経済産業省では日本情報社会経済推進協会とともに，インターネット利用における認証にまつわる不安や身元確認における利用者の負担やトラブルを軽減するために，マイナンバーを利活用した「ID 連携トラストフレームワーク」の普及を推進している [97]．ID 連携トラストフレームワークでは，EAAF における SP のリスク評価をより簡便にするために，図 3.2 に示すような保証レベルによるサービスの類型化を行っている．これにより，主要なサービスでは必要な保証レベルをすぐに決定することができるというメリットがある．

また，2.1.3 節で述べたように，身元確認は実在性と同一性を担保する行為として整理されており，これにもとづく形で保証レベルを，実在性を担保する「身元確認保証レベル」と，同一性を担保する「当人確認保証レベル」に区別しており，全体保証レベルは図 3.3 に示すようにいずれか低いレベルに従うものとされている．なお，本研究でいうところの身元確認の保証レベルは，まさに彼らのいう身元確認保証レベルに相当する．

このように，ID 連携トラストフレームワークでは既存の EAAF をより具体的に実装するための工夫がなされている．しかしながら，肝心の身元確認スキームそのものについては，国民を広く対象としており，そのデータソースや登録機関の配備方式は暗黙にほぼ固定である．具体的には，データソースに用いるものは住民票や運転免許証などいわゆる公的証明書[1]を想定しており，また登録機関についても自治体などが担当する (実際には法定受託事

[1]厳密に言えば，日本版 LoA2 では EAAF の身元確認要件に加えて携帯電話事業者のデータベースが新たに許容された事実はあるが，いずれにしても自然人が暗黙裡の対象である．

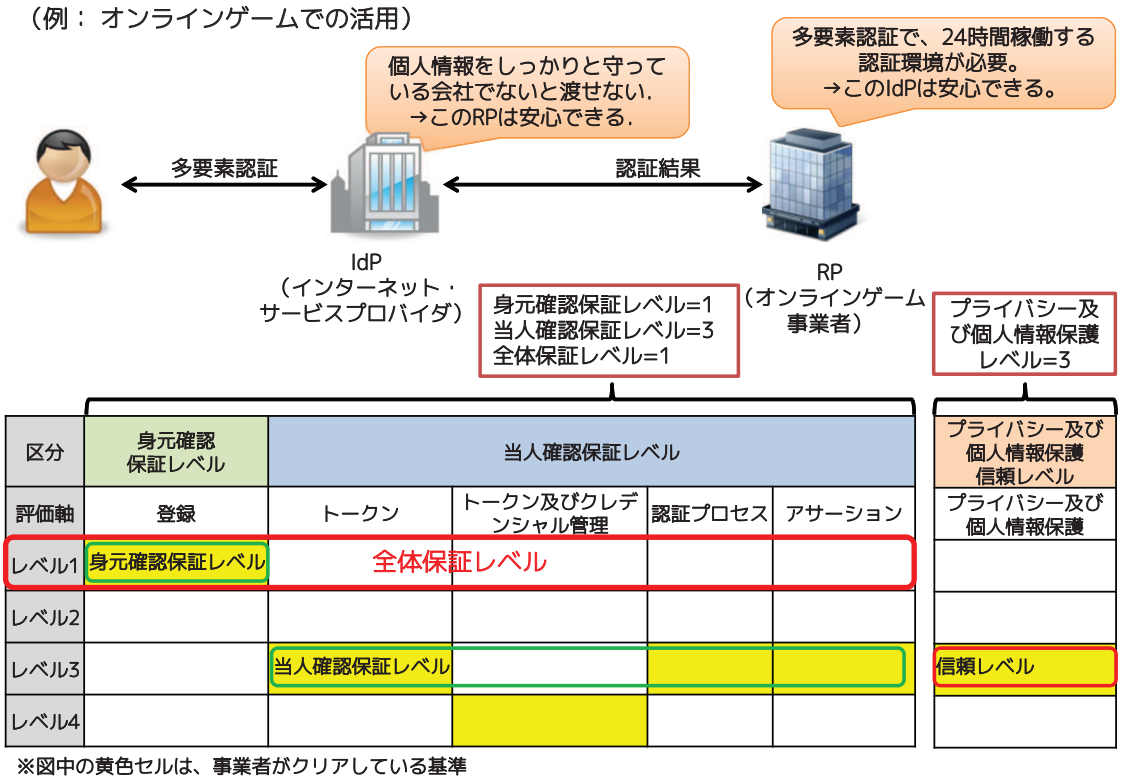


図 3.3: 2 種類の保証レベル ([22] 図表 42 より)

務) などの暗黙の前提がある．このため，コミュニティや組織などより限定的な範囲のユーザの身元確認を行う場合や，Web サーバやネットワーク機器などモノの身元確認を行いたい場合に利用可能なデータソース，さらにはその身元確認を行う登録機関として RRA の選択肢について，十分に考慮されているとは言えない．

3.2.3 その他のトラストフレームワーク

これら政府の主導するトラストフレームワーク以外にも，トラストフレームワークに関する研究はいくつか行われている．金岡らは，ID ベース暗号におけるトラストフレームワークを提案した．ID ベース暗号の公開鍵を発行する鍵生成局が複数存在する環境において，利用者が鍵生成局を如何に信頼するか，という問題を解決するために，ID ベース暗号の信頼構築のためのフレームワークを提案した [77]．また，島岡らは，現状のトラストフレームワークの多くが実際にはアイデンティティ情報のうち識別子の交換のみであるのに対して，属性情報を含めたアイデンティティ情報が本格的に交換されるようになった時に必要な属性交換フレームワークを提案した．アイデンティティ情報の中に属性情報を含めて交換する際には，IdP が提供するアイデンティティ情報を，SP が如何に安全に管理するかが問題となる．同フレームワークでは，SP が IdP に対する信頼を構築するための保証レベルという概念に対して，IdP が SP に対する信頼を構築するための保護レベル (Level of Protection) を導入し，学認のトラストフレームワークを拡張する形で提案したものである [95].

3.3 関連研究：UPKI アーキテクチャ

大規模なアイデンティティ管理ドメインにおいては登録機関の配備が大きな課題であり，また RRA 方式を検討するにあたっては利用可能なデータソースの有無や参照コストがポイントとなる．本節では，こうした大規模なアイデンティティ管理ドメインの設計事例として，国立情報学研究所が実施した「大学間連携のための全国共同電子認証基盤 (UPKI)」プロジェクトについて示す．

UPKI には 3 種類の用途が挙げられており，それぞれに身元確認ポリシや利用可能なデータソースが異なるため，身元確認スキームについては用途毎に独立させたレイヤ構造としつつ，レイヤ間の相互運用性が確保できるよう全体アーキテクチャの設計を行った [87, 84]．

例えばサーバ証明書などを利用するオープンドメイン PKI は，ブラウザなどに予め信頼されたパブリック認証局を利用する必要があることから，アイデンティティ管理ドメインは全国共通とする必要がある一方で，サーバ証明書発行時の身元確認に必要なデータソースを RRA から参照するのはコスト不合理であることから，各大学に LRA を委託することでコスト合理化を目指した．一方の学内の教職員を対象とするキャンパス PKI は，もともとアイデンティティ管理ドメインが学内に閉じていること，身元確認に必要なデータソースも学内に揃っていることから，オープンドメイン PKI とは別のレイヤとして扱うことにした．また大規模計算資源を利用する研究者を対象とするグリッド PKI は，アイデンティティ管理ドメインは全国規模であるものの，厳格な身元確認ポリシが要求されることから RRA よりも LRA 方式を採用した．このように，それぞれのアイデンティティ管理ドメインやデータソースおよびその参照コストなどの違いを考慮した結果，用途毎に異なるレイヤ構造とすることで課題を解決した．

3.3.1 UPKI の要件

本節では，UPKI を設計する上で考慮すべき要求要件について説明する．

(1) 学内認証基盤の整備

UPKI が幅広い連携を実現するには，その構成要素となる各機関の学内認証基盤にも高い相互運用性が求められる．他大学との連携には，認証局同士の相互認証や IdP と SP 間のフェデレーションなど複数の方式があり，各機関の担当者がこうした様々な方式に対応可能な認証基盤を設計するには，認証技術に対する深い理解と運用ノウハウが必要であり，多くの大学に認証基盤が整備されていない現状でそれを求めることは難しいと考えるべきである．

また，各機関の認証基盤の保証レベルに著しい差異があるようだと，技術的に連携可能であってもセキュリティポリシの観点から連携が許容されないことも考えられる．例えば，A 大学の認証基盤では，証明書発行時に対面による身元確認を行うとともに，利用する鍵ペアも IC カードなどの耐タンパ性装置に保管する一方で，B 大学の認証基盤では，証明書発行時の身元確認をメールの到達性だけで判断し，利用する鍵ペアも PC の HDD 上に複製自由

な状態で保管されるとしたら，A 大学は B 大学になりすましのリスクがあるとして信頼関係の確立を拒むかも知れない．

こうした課題を解決するには，一定の保証レベルを担保する各大学共通の運用ポリシーを策定するとともに，高い相互運用性 [60] を実現するためのシステム要件を策定し，各機関はこれをもとに学内認証基盤の整備を進めることを前提とする．

(2) グリッド PKI との整合

グリッドコンピューティングの分野では，利用権限を持つ正しいユーザが複数の異なる組織に分散した資源を連携して利用するため，PKI 技術をベースにしたセキュリティ機構の実装が進んでいる．グリッド認証基盤では，ユーザ証明書[2]により本人認証と権限確認を行い，このユーザ証明書からユーザの権限を委譲することを示すプロキシ証明書を発行することで，複数のグリッド資源上でのユーザが介在しないジョブ実行を実現している．このためプロキシ証明書とその私有鍵はグリッドシステム上で発行，管理が行われることになる．また，ユーザ証明書を発行する認証局は，複数の異なるグリッド資源提供機関から信頼されることが求められる．特に，日本の機関が世界規模でグリッド資源共有を行うためには，全世界のグリッド認証局の運用要件を規定する International Grid Trust Federation (IGTF) の下で Asia Pacific Grid Policy Management Authority(APGrid PMA) の承認を受けることが必要である．

一般的な PKI では認証局以外が証明書を発行することは禁じられているのに対して，グリッド認証基盤では，ユーザによるプロキシ証明書の発行を許可している．また，多くの PKI ではユーザ証明書と私有鍵を IC カードに格納するなどユーザ自身が管理することを求めているのに対して，グリッドシステムではプロキシ証明書だけでなくユーザ証明書もシステム上で管理している実装が多い．一方で，IGTF が規定するグリッド認証局の運用要件は，パブリック PKI の運用要件の一例として知られる WebTrust for CA よりも厳しい部分があるなど，グリッド PKI は PKI の中でも特異な位置づけであり，技術的には PKI を活用しているものの，運用ポリシの観点からは既存の PKI とは独立した認証基盤として運用することを前提とする．

(3) パブリック PKI との整合

主要な PKI アプリケーションに信頼点として予め登録された認証局 (あるいはその下位認証局) 群は，一般にパブリック PKI と呼ばれ，その発行対象は SSL/TLS サーバ認証に用いるサーバ証明書や，電子メールの署名・暗号に用いる S/MIME 証明書である．パブリック PKI の最大の利点は利用者を限定しない点にある．このため，不特定多数の利用者からアクセスされるサーバや，不特定多数の利用者が受信する可能性がある電子メールで効果を発揮する．大学の場合，サーバ利用者が必ずしも不特定多数でないにしても，構成員数の多い大

[2] ここでいうユーザ証明書は，キャンパス PKI から発行されるそれではなく，グリッド認証基盤から発行されるユーザ証明書である．

学や，学生に対しては必ずしも信頼点となる認証局証明書の登録を強制できない場合があるなど，パブリック PKI を活用する効果は大きい．更には，学外，特に産官民と連携する際に用いるサーバ証明書や S/MIME 証明書には明らかにパブリック PKI が求められる．

一方で大学から見たパブリック PKI の課題はコストにある．例えばサーバ証明書は，発行元や種類によっても価格は様々であるが，著名なベンダから購入する場合，一枚あたり年間数万円が相場と言える．NII が 2006 年に学術情報ネットワーク加入機関 218 機関に対して行った調査 [88] によれば，サーバ証明書を利用すべきにも関わらず導入できていないサーバがある，という機関が約 4 分の 3 を占めていることがわかった．

UPKI では，こうした大学における証明書の不適切な利用を改め，パブリック証明書の利用を普及させることも目標の一つである．

(4) その他の要件

連携による管理コスト UPKI により大学間で様々なサービス連携を連携して安全安心に利用が可能とするためには，連携する認証事業者とサービス事業者における管理コストが問題となる．この管理コストは認証のための ID 管理コストと認可のための属性管理コストがあり，認証基盤全体として必要な認証の保証レベル，属性の保証レベルを確保しつつ，上記両管理コストの低減を実現することが求められる．

構築コスト，運用コスト UPKI の構築，運用にあたっては，中心となるシステムの構築，運用だけでなく，国内の多くの大学がキャンパス PKI およびそれを利用するサービスに必要なシステムを構築，運用することが不可欠となる．しかし，各大学で新たなシステムを構築，運用するためにはシステムの予算化，構築要員，運用要員の確保，学内の関連組織間の調整や全学判断等も必要となり，各大学の状況により課題や障壁の高さも大きく異なってくる．そのため，全国共同の基盤として実現，普及していくためには，各大学におけるこれらのコストを低減した設計や，各大学が個々の状況に応じて導入計画を立てられるような配慮が求められる．

3.3.2 UPKI アーキテクチャの設計

前節までの要求要件を，連携によらず単独の認証基盤で実現するには仕様が重厚になってしまい，各機関における実現可能性が低下してしまう．特にパブリック PKI やグリッド PKI など，すでに導入普及が進んでいるシステムとの整合は，調整できる余地が限られる．このため，UPKI では単独の認証基盤で要求要件を実現するのではなく，既存のパブリック PKI やグリッド PKI を活用・連携することによって要求要件を実現することを目指した．その結果として設計されたのが，図 3.4 に示すオープンドメイン層，キャンパス層，グリッド層の 3 層で構成される UPKI アーキテクチャである．3 層の PKI はそれぞれ独立しており，さらにキャンパス層はキャンパス毎に独立している．UPKI では，キャンパス層を中核として，2.2 節で示した任意の方式を用いて各層と連携することを想定する．これにより，厳格な身

元確認にひもづいた証明書発行を各層で実現するとともに，既存の様々な認証基盤との高い相互運用性を実現することができる．本節では，各層の認証基盤の役割について説明する．

(1) キャンパス層

キャンパス層は，大学毎に設置される学内認証基盤について，大学間での連携を実現する，UPKI の中核をなすレイヤである．各大学は，学内の教職員・学生等を対象とした学内認証基盤を配備し，学内に提供するサービスでの認証に利用することができるものとする．また，各大学は，2.2.2 節のアサーション方式を利用することにより大学間で認証連携を実現することができる．更に，各大学は PKI ベースの学内認証基盤即ちキャンパス PKI を実装することで，将来的に 2.2.1 節 a)∼c) のいずれかの方式を用いて，署名や暗号を必要とするサービスの連携にも対応することが可能となる．

他の 2 層と異なりキャンパス層即ち大学は，学生・教職員に対して最も近い関係にある組織として，対面またはそれに準じた高い本人性確認が可能であるとともに，在籍・所属などについても人事情報等と整合した実在性確認が可能である．つまり学内認証基盤は高い保証レベルを実現することが可能であり，この学内認証基盤の認証情報をもとにオープンドメイン層やグリッド層と連携することで，いずれの層でも保証レベルを低下させることなく証明書発行を実現することが UPKI アーキテクチャの狙いである [103, 104]．キャンパス層の学内認証基盤は，各大学で導入が進められている [79, 70, 73, 81, 98, 92, 99, 76, 80]．

(2) オープンドメイン層

オープンドメイン層は，各大学における，不特定多数からのアクセスかつサーバ認証を必要とするサーバや，不特定多数を対象に署名・暗号を行う電子メールアドレスなどに対して証明書を発行するレイヤである．オープンドメイン層で利用する証明書は，Web ブラウザなど主要な PKI アプリケーションに予め登録された「信頼されたルート認証局」を信頼点として検証できる，いわゆるパブリック証明書であることが求められる．「信頼されたルート認証局」は，主要な PKI アプリケーションに登録されるために認証局の国際的な運用基準である WebTrust for CA[29] あるいはこれに相当する基準に準拠 [85] する必要があり，そのための運用コストは小さくない．各大学ごとに，既存の「信頼されたルート認証局」の下位認証局を構築することも可能であるが，運用コストの削減を考えると，既存の「信頼されたルート認証局」の下に全国で 1 つの下位認証局を用意し，その下位認証局において，各大学のサーバに対するパブリックなサーバ証明書を発行する方法も考えられる．そこで，NII では，既存の「信頼されたルート認証局」の下位認証局として「NII オープンドメイン認証局」を構築・運用し，各大学向けのパブリックなサーバ証明書の発行を行うこととした[3]．パブリックな証明書を発行する認証局に要求される運用基準では，厳格な本人性確認と実在性確認が求められることから，証明書発行の際の審査が煩雑になりやすい．
そこで「NII オープンドメイン認証局」では，キャンパス層に配備された高い保証レベルを

[3]電子メールアドレスを対象とする S/MIME 証明書の発行は現在準備中である．

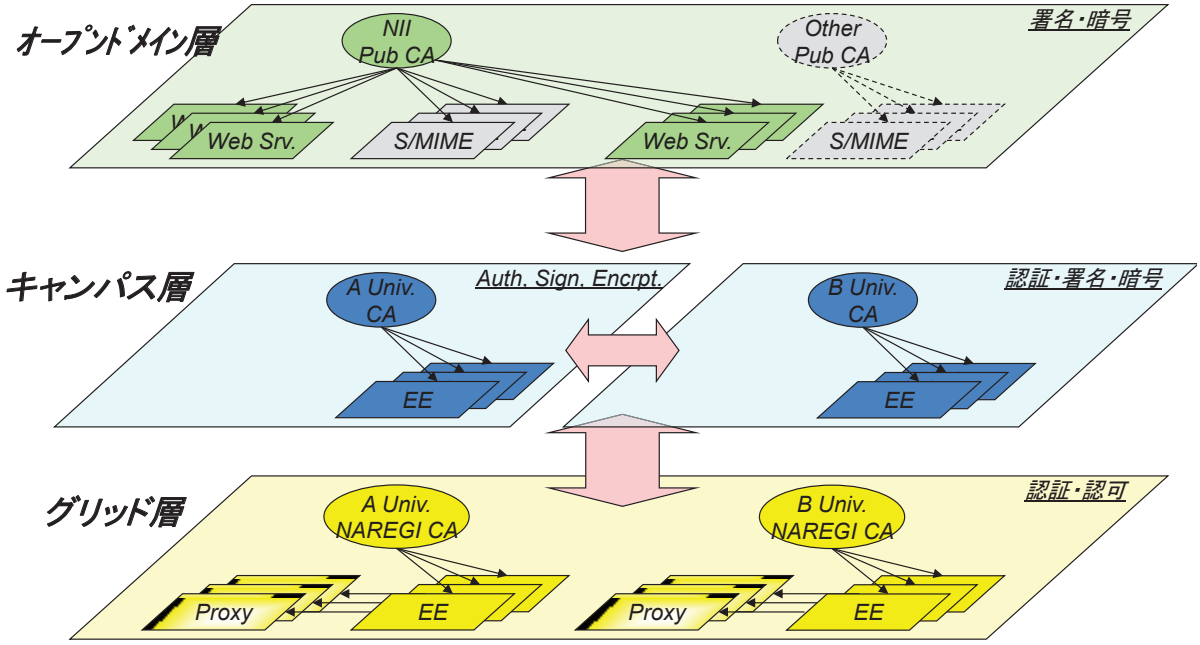


図 3.4: UPKI の 3 層構造 ([84] 図 5 より©2011,IEICE)

持つ各大学のキャンパス PKI と連携することで，パブリック証明書発行における身元確認作業の自動化し証明書発行にかかるコストを低減する [23, 19, 96, 88, 74, 82].

(3) グリッド層

グリッド層は，学術機関が運用するグリッドコンピュータを利用するための証明書を発行するレイヤである．グリッド層では，グリッドコンピュータを運用する学術機関がグリッド認証局を構築・運用し，グリッドコンピュータを利用するユーザに対してユーザ証明書を発行する．グリッド認証局は，海外のグリッドコンピュータを利用するために必要となる海外のグリッド認証基盤とも連携できるよう APGrid PMA の運用基準に準拠する必要がある．またユーザ証明書に基づいて，グリッドミドルウェアにおけるジョブ実行の認可に必要なプロキシ証明書を発行できる必要がある．グリッド認証局は，オープンドメイン層の「NII オープンドメイン認証局」と同様に，キャンパス層に配備される各大学のキャンパス PKI と連携することで，グリッド証明書発行における身元確認作業を自動化する．

(4) 方式検討の議論

本節では，UPKI アーキテクチャ設計にあたり，検討した主要な論点について解説する．

統合 PKI 方式 vs. ブリッジ方式 UPKI の命題は，各大学がキャンパス PKI を構築することを前提に，これらが連携可能な基盤を如何にして構築するか，相互運用性をどのように確保するかであり，初期は PKI 方式を前提として検討を進めていた．この場合，[84] で示された PKI 方式のうち，直接方式は，全国 800 余の大学に適用するには運用負担が大きいことから，統合方式とするかブリッジ方式とするかが論点となった．

統合方式は，階層構造で既存 PKI アプリケーションとの親和性が高く，上位認証局にパブリック認証局を採用すると利便性が大きく向上することから，パブリック認証局を前提に検討を行った．

1. NII が WebTrust for CA 認定を取得し，パブリックルートを構築・運用
2. パブリックルートの下位認証局として統合認証局を NII が構築・運用

(1) 案では，パブリックルート認証局の運用要件である WebTrust for CA 認定を取得する必要がある．認定は毎年更新する必要があり，外部監査が必須であるため，運用負担が大きい．(2) 案では，商用認証局事業者による既存のパブリックルート認証局から横断認証された下位認証局を NII が構築・運用することで，パブリック PKI の恩恵を受けながらも NII が直接 WTCA 認定を取得する手間が省ける．しかし一方で，上位認証局に対するサービス利用コストや上位認証局の CP/CPS に準拠する必要があるなど一定の制約が課されることになる．

一方，ブリッジ方式は，利用者に必要とされる複雑な証明パスの構築・検証機能が主要な PKI アプリケーションにも実装されていないこと，ブリッジ認証局における各認証局に対する審査負担が大きく運用コストの確保が難しいことなどが課題となる．

アサーション方式 vs. PKI 方式　UPKI 設計当時，アサーション方式には Internet2 の Shibboleth 1.3 や OASIS の SAML 1.0，WS-Federation，OpenID などに加え，アサーション方式ではないものの Yadis[21] や CardSpace[1] など様々な関連規格・実装が乱立状態にあり，実装まで踏み込んだアサーション方式の選定は時期尚早であった．また，アサーション方式はあくまで認証にフォーカスしたものであり，署名や暗号には適用しづらいという課題もあった．

しかしながら，学術界においては電子ジャーナルサービスの利用者認証で Shibboleth が普及し始めていたこと，設計当時における OpenID の急速な台頭など，近い将来認証に関してはいずれかのアサーション方式が普及するだろうことは疑いがなく，UPKI としてもアサーション方式に対応可能なアーキテクチャを設計しておくことは不可欠であった．

アサーション方式に対応可能としておくためには，IdP として振舞うことになる各大学のキャンパス PKI が提供する認証情報の保証レベルが一定水準を満たしている必要がある．そこで UPKI では，UPKI 共通仕様として，CP/CPS ガイドラインを策定し，各大学がこれに準拠した CP/CPS を策定することで，一定水準を満たす認証情報を提供できる枠組みを整備しておくこととした [103, 102]．

アサーション方式は，署名や暗号に適用することが難しいという課題があるが，署名・暗号は学内だけでなく他大学や企業など学外の利用者とやり取りする可能性が高く，またその方が利便性も高い．このため，署名・暗号に関してはキャンパス層で実現するよりも，キャンパス層のキャンパス PKI と連携するなどしてオープンドメイン層から各大学の教職員や学生などに署名・暗号用証明書を発行することが理想的である．

3.3.3 まとめ

こうした議論の結果，署名・暗号に関しては PKI 方式が不可欠である一方，キャンパス層における連携用途を認証に限定することでアサーション方式も選択肢として有効になった．更に，アサーション方式であれば，学内認証基盤が必ずしも PKI ベースのキャンパス PKI で構築されていなくても連携が可能となることから，キャンパス層における認証連携は PKI 方式への対応可能性も留保しつつ，アサーション方式を採用することとした．

第4章　身元確認スキームのコスト指向設計手法の検討

IdP の課題のひとつとして，その運用コストにおける身元確認の人件費削減がある．しかし，身元確認コストを削減しすぎてその保証レベルを低下させることになれば SP からのニーズに対応できなくなるというジレンマがある．本章では，保証レベルを保ちながら身元確認コストを削減する，というジレンマを解消する身元確認スキームのコスト指向設計方法について検討を行う [83].

身元確認コストにおいては RA の人件費の比率が高いことが谷本らによって明らかになっており，この人件費を削減することは一つの大きな課題である．人件費を削減する手法のひとつとして，RA の配備方式に RRA 方式を選択することが知られている．しかし RRA は利用可能なデータソースが限られること，さらにデータソースを変えれば身元確認の保証レベルにも影響を及ぼす場合があり，一概に RRA 方式がよいとは言い切れない．そこで，本章ではまず，RRA 方式で高い保証レベルを実現している商用認証局の身元確認スキームについて調査分析を行った．この結果から身元確認においてコスト合理的なデータソースを選定するための評価項目を洗い出し，コスト合理的なデータソースにもとづく身元確認スキームの設計手法を提案した．

また，この提案手法を用いて，国立情報学研究所のサーバ証明書プロジェクトの身元確認スキームの設計を行った．同プロジェクトでは，学術機関向けサーバ証明書発行スキームとして実装し，3 期にわたるプロジェクト運用を通じて，提案手法によって実装された身元確認スキームのコスト合理性が示された．同プロジェクトは平成 27 年から事業化が確定しており，本提案はこの事業化に大きく貢献したと言ってよい．

4.1　商用認証局における身元確認スキームの調査分析

本節では，商用認証局における身元確認スキーム (以下，商用スキーム) について調査を行った．サーバ証明書は Web サーバをはじめ多くのクライアントサーバ間通信を暗号化する TLS と呼ばれる暗号化通信プロトコルに用いられるもので，インターネットに広く普及している．商用認証局においては，身元確認スキームを規定する CP/CPS は一般に公開されるものであり，このため情報量が豊富で調査に向いている．CP/CPS はそのフレームワークが RFC 3647[51] において規定されていることから，複数の CP/CPS を横串で比較分析しやすいというメリットもある．

表 4.1: 商用サーバ証明書の審査項目 ([83] 表 1 より©2012 IEICE)

		商用認証局				定義
		DV		OV/EV		
		登録局	加入者	登録局	加入者	
組織	本人性	×		○		当該組織からの申請であり、機関の長の承認が得られていることを確認する。
	実在性	×		○		当該組織が実在することを確認する。
ドメイン	本人性	○		○		(a)申請するドメインが機関の所有であること、(b)ドメイン下のサーバへの証明書発行について機関の許諾を得ていることを確認する。
	実在性	○		○		加入者サーバが機関ドメインに実在(登録)していることを確認する。
加入者	本人性	×		○		発行申請が加入者本人の意思であり、なりすましでないことを確認する。
	実在性	×		○		加入者が組織に実在することを確認する。
加入者サーバ	本人性		○		○	加入者サーバの鍵ペアが、加入者サーバだけが管理し得る状態にあることを加入者自身が確認、自己申告する。
	実在性		○		○	加入者サーバが、組織の所有または管理下にあることを加入者自身が確認、自己申告する。

4.1.1 審査項目

サーバ証明書には，証明書主体者名としてサーバの FQDN [1]が記載されるとともに，サーバの所属する機関名などが記載される．サーバ証明書はサーバの真正性確認に用いられるものであり，その証明書に記載される主体者名としてのサーバ FQDN やサーバ所属機関などは，証明書を発行する認証局によって担保，即ち発行時に十分な身元確認がなされていることを前提としている．

こうした身元確認を行うための審査項目を表 4.1 に示す．なお，ここでいうドメインとは当該組織がレジストリ [56] から取得したドメインを，加入者とはサーバ証明書をインストールする加入者サーバの管理者を指す．また，クライアントを用いて加入者サーバにアクセスするものを利用者と呼ぶ．

実在性確認は，基本的に証明書に記載する内容を担保する上で必要とされ，本人性確認はなりすましを防ぐために必要とされる．本章において単に身元確認と記した場合は，実在性確認と本人性確認の両方を含む意味とする．各審査項目の具体的な定義は表 4.1 に示した．

4.1.2 保証レベル

パブリック認証局によるサーバ証明書の身元確認は，前述の審査項目の組み合わせによってレベルの低い方からドメイン認証 (DV, Domain Validation)，組織認証 (Organization Validation)，厳密組織認証 (Extended Validation) の 3 段階に分類される [41]．

[1]Fully Qualified Domain Name. 例えば https://upki-portal.nii.ac.jp/という URL では upki-portal.nii.ac.jp が FQDN に，nii.ac.jp がサーバの所属するドメインに該当する．

OV は組織，ドメイン，加入者それぞれについて本人性と実在性の審査を受けた証明書を指す．EV は OV に加えて組織の実在性について登記事項証明書などを用いた法人格の審査が必要であり，また EV 証明書を発行する認証局には EV 独自の認証局運用認定規準 [42] の認定が必要とされる．DV は，ドメインの本人性・実在性のみについて審査を受けた証明書を指す．

商用認証局は，発行するサーバ証明書についてこうした保証レベルのいずれを取り扱うか予め規定した上で，証明書を発行している．

4.1.3 証明書発行フロー

図 4.1 に典型的な商用認証局によるサーバ証明書発行フローを示す．フローは主に 1) 準備，2) 申請，3) 審査，4) 発行，5) 配付，6) インストールから成り立つ．証明書の発行を受ける加入者は，事前に申請に必要な準備として，申請に必要な情報の収集，(必要に応じて) 登記事項証明書などの証明書類の入手，(必要に応じて) 申請書類への押印などを準備した後，これらの情報を Web や郵便などで認証事業者に送付する．

認証事業者は，受領した申請情報や書類に基づいて証明書発行のための審査を行う．具体的には表 4.1 で示すように，発行する証明書の保証レベルに応じた審査項目について審査を行う．

審査項目の具体的な実施手順は認証事業者によって様々であるが，例えば組織の実在性およびドメインの本人性 (a)(表 4.1 参照) については，企業情報データベースや WHOIS サービスなどの第三者情報を積極的に活用することで客観的かつ効率的な審査を行っているケースもあるようである．しかしながら，加入者や加入者サーバの実在性などはこうした第三者情報に依ることが難しいために審査コストがかかりがちである．こうした中，煩雑な審査作業をできるだけ効率化した手法として Outbound-Call (OBC) がある．これは，例えば加入者組織の代表電話や人事部経由などで加入者に電話するもので，加入者の実在性と本人性を同時に確認することができる．

審査を通れば，申請内容にもとづいた証明書が認証局から発行され，加入者に配付される．加入者は受領した証明書を対応する私有鍵とともにサーバへインストールすることで，はじめてサーバ証明書が利用可能となる．

サーバ証明書を発行する商用認証局の多くは LRA を用いない RA 型であるため，上記審査項目は全て RA が審査するが，RA 業務の一部を LRA に委任する形の LRA 型の場合は，表 4.1 に示す審査項目について，1) 全ての審査項目を LRA で審査，2) 一部の審査項目のみ LRA に委任し残りの審査項目は RA で審査，という 2 方式が考えられる．特に 2) の場合は，どの審査項目を LRA で審査するかが重要となってくる．

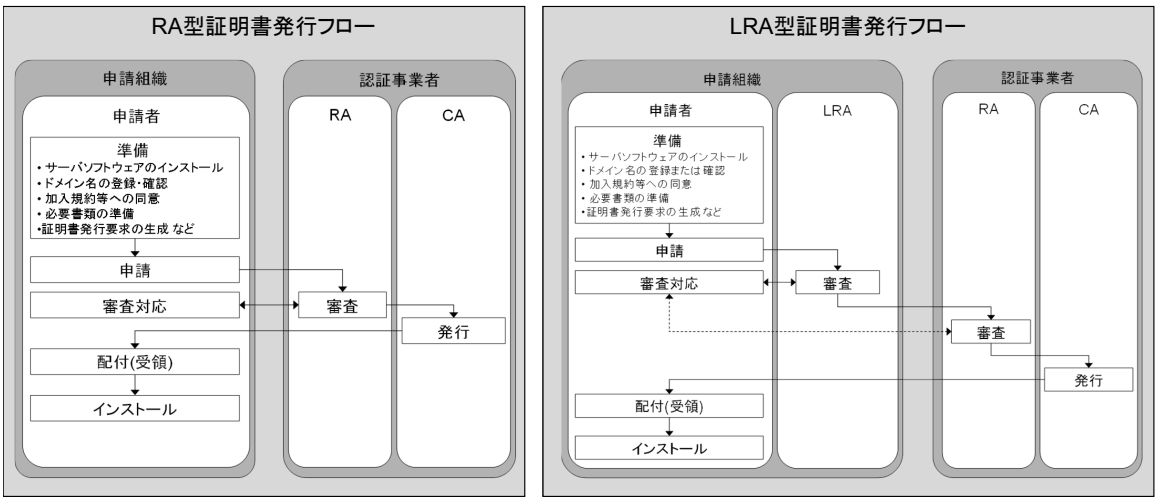


図 4.1: 典型的な証明書発行フロー ([83] 図 3 より©2012 IEICE)

4.1.4 身元確認スキームの考察

調査の結果，商用認証局では組織の身元確認に企業情報データベースを，ドメインの身元確認には WHOIS データベースを，また加入者の身元確認には OBC をそれぞれデータソースとして用いていることを一例として確認した．商用認証局がこれらのデータソースを選択した理由について考察を行い，その結果データソースを選択する際の評価項目として，以下の 4 項目に分類した．

1) RA の配備方式 RA の配備方式として，1.2.2 節に挙げた RRA と LRA の 2 方式がある．後述のアクセスコスト 3) は，誰がそのデータソースにアクセスするかによって大きく変わる場合があり，ここでどちらの方式でアクセスするかを与えておく必要がある．

2) データソースの所在 データソースが誰でもアクセス可能なパブリックな情報か，限定されたエンティティしかアクセスできないプライベートな情報か，は選定にあたって重要である．社員の人事情報は社外からはアクセスできないことがほとんどであろうし，サーバ証明書の発行における身元確認に用いられる WHOIS データベースは，何処からでも誰でもアクセス可能なオープンデータベースである．

3) データソースへのアクセスコスト 部外者によるアクセスが制限されているデータベースや，物理的に外部からのアクセスが困難な紙の台帳など，いわゆるプライベートなデータソースは RRA からアクセスする場合には，LRA からのアクセスと比較すると無視できないコストが発生する．一方，パブリックなデータソースであっても多くの企業情報データベースでは有償アクセスの仕組みをとっているなど，必ずしもアクセスコストはデータソースの所在と RA の配備方式だけでは決定できないため，ここで改めて評価する．

4) 属性情報およびデータソースの真正性 照合先のデータソースに十分な真正性がなければ，それと照合した属性情報の確からしさは，照合先データソースと同等もしくはそれ以下とみなすべきである．データソースの真正性はその程度によって以下の 3 種類に大別される [67].

権威ある源泉 (Authoritative Source) からの属性情報 厳密には属性情報の一次発行者が管理するデータソースであり，例えば社員の職権については人事情報データベースが権威ある源泉とみなせる[2].

検証された (verified) 属性情報 登録機関以外の第三者によって何らかの方法で検証された属性情報であり，例えば社員の自宅住所を確認するために社内の人事情報データベースを参照するケースなどはこれに当たるといえる[3].

未検証の (unverified) 属性情報 文字通り検証されていない情報であるが，例えば趣味のようにそもそも検証不可能な属性情報もある．

この分類にもとづいて，先の調査結果を整理したものを表 4.2 に示す．

これらの評価項目のうち，4) の真正性は，それ自身直接コストに影響するものではなく，逆に保証レベルに影響する要素である．そこで，4) を除く 1)~3) のみを評価項目とすることで，保証レベルに影響を与えない形でデータソースの選択ができるようになると考えた．さらに，データソースは RA の配備方式によって選択候補が異なる場合もあり，配備方式によって整理するため 1) を除く 2) と 3) の 2 軸にデータソースをマッピングする．表 4.2 のデータソースも含め，主要なデータソースをマッピングしたものを図 4.2 および 4.3 に示す．

4.2 コスト指向の身元確認スキーム設計手法の提案

4.1.4 節で考察したマトリクスをベースとした，コスト指向の身元確認スキーム設計手法を提案する．提案手法は，図 4.4 に示すように，データソースをコスト合理的に選択するこ

表 4.2: 商用認証局のデータソース

審査項目	組織	ドメイン	加入者
データソース	企業情報データベース	WHOIS データベース	Outbound-Call
RA 配備方式	RRA 方式	RRA 方式	RRA 方式
所在	パブリック	パブリック	プライベート
コスト	基本的に有償	無償	問い合わせ工数
真正性	検証済	検証済	権威ある源泉

[2]なお，運転免許証に記載された住所などは議論が分かれるところである．これは，公的証明書とみなせば権威ある源泉と言えるが，そもそも運転免許証に記載される住所は発行時に提出された住民票等にもとづいて記載されるものと考えれば「検証済」とみなすことも可能だからである．

[3]ここで人事情報データベースは，入社時または転居時などに社員から住民票の提出を受けているものと仮定する．

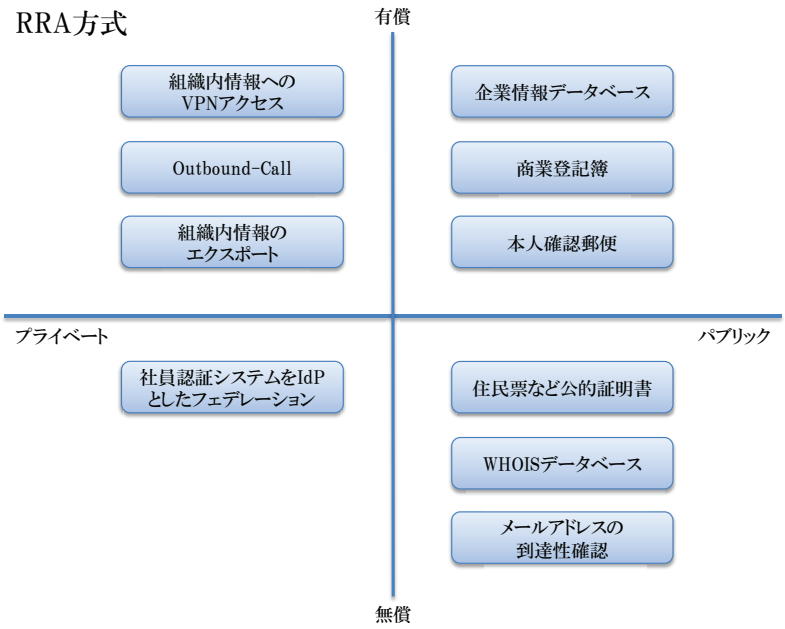


図 4.2: 提案手法による主なデータソースのマッピング (RRA 方式)

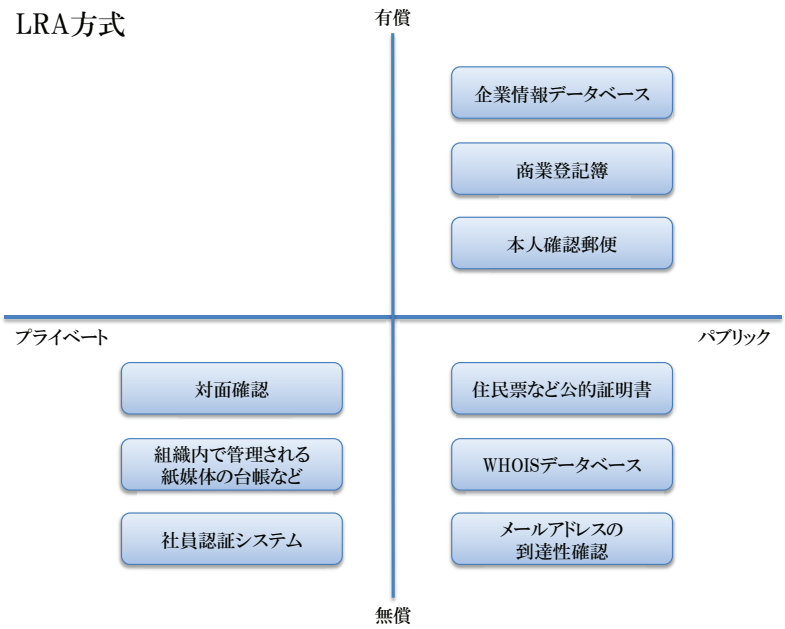


図 4.3: 提案手法による主なデータソースのマッピング (LRA 方式)

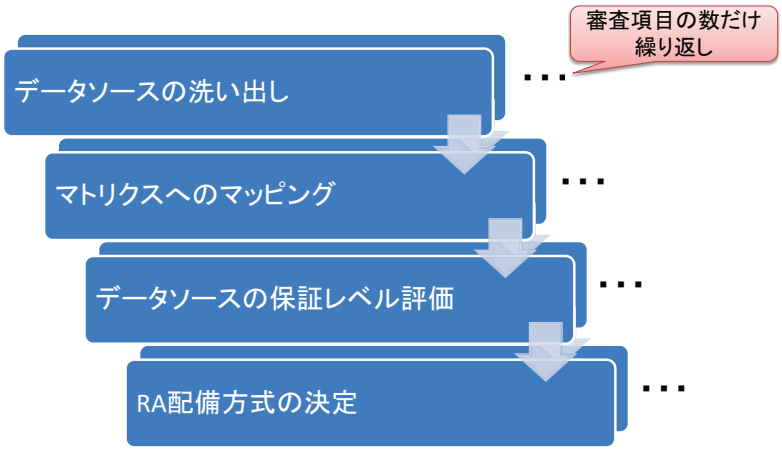


図 4.4: 提案手法によるスキーム設計

とによって身元確認スキームを簡便に設計する手法である．

4.2.1 前提条件

提案手法の前提条件として，身元確認で行うべき審査項目と，IdP が準拠すべき保証レベルは所与のものとする．

4.2.2 評価の流れ

以下の流れに沿ってデータソースの評価を行う．

1) 保証レベルに応じたデータソースの洗い出し 身元確認に利用可能なデータソースの洗い出しを行う．ここでは，データソースの所在や RA の配備方式，アクセスコスト，真正性といった点については考慮せず，各審査項目において利用可能なデータソースを可能な限り列挙する．

2) マトリクスへのマッピング 1) で洗い出したデータソースを，その所在とアクセスコストのマトリクスにマッピングする．マトリクスは RRA 方式と LRA 方式の 2 種類を用意し，配備方式が限定されるデータソースは，限定された一方の配備方式のマトリクスにのみ記載する．例えば対面確認は LRA 方式のみのデータソースとして，RRA 方式にマトリクスには記載しない．

3) データソースの保証レベル評価と選定 各審査項目について，コストが無償のもの，あるいは無償のデータソースがない場合には有償のデータソースの中でアクセスコストの最も低いものから順に，当該データソースが所与の保証レベルに準拠可能かどうかを評価する．準拠可能な場合，これを当該審査項目におけるコスト合理的なデータソースとして選定する．準拠しない場合，次にアクセスコストの低いデータソースについ

て同様に保証レベル評価を行い，準拠するまでこれを繰り返す．これを RRA 方式と LRA 方式のマトリクスについてそれぞれ行う．

4) 配備方式の決定 3) により保証レベルを満たす審査項目毎に保証レベルを満たすコスト合理的なデータソースが，配備方式毎に選定された．最後に，審査項目毎に配備方式を決定する．1.2.2 節で示したように，基本は RRA 方式としつつ補完的に LRA 方式を採用するという方針にもとづいて，審査項目毎に両方式の身元確認コストを比較しながら総合的に評価を行う．具体的には，RRA 方式で無償あるいは有償であっても十分に低いアクセスコストで身元確認可能な審査項目には RRA 方式を選択し，LRA 方式の方が顕著にコスト優位とみなせる場合に限り当該審査項目に LRA 方式を選択する．

4.3 提案手法の実装

前節で述べた，身元確認スキームの設計手法を，その実用性評価を目的として，国立情報学研究所 (NII) が平成 19∼20 年度に行った「サーバ証明書の発行・導入における啓発・評価研究プロジェクト」(以下，実証実験)[23] に対して実装した．実証実験は，国立情報学研究所が認証局となって，学術情報ネットワーク (SINET) 加入機関を対象にサーバ証明書を発行するプロジェクトである．

4.3.1 前提条件

提案手法では，4.2.1 節で述べたように保証レベルと審査項目を所与とする．なお，実証実験ではサーバ証明書の発行について，一般的な商用認証局と異なる審査方法を採用している．これによって審査項目も若干異なっているため，はじめに保証レベルについて示した後，審査項目について述べる前に審査方法について示す．

(1) 保証レベル

実証実験で扱うサーバ証明書の保証レベルは 4.1.2 節に示されている．実証実験においてはサーバ証明書が学術機関のものであることが識別できるよう OV を選択した．

(2) 審査方法

学術機関は，商用認証局からサーバ証明書を入手する一般的な組織と異なり，ひとつの組織で複数枚の証明書を利用することが多く，またその証明書入手時機は証明書を利用するサーバ管理者 (以下，加入者) によって異なる．このため，実証実験では身元確認を効率化するために，審査を機関審査と発行審査の 2 段階に分けることにした．実証実験において NII からサーバ証明書の発行を受けたい学術機関は，事前に実証実験への参加申請を行い機関審査を受けるものとする．機関審査をパスした機関からは，任意の加入者が任意のタイミング

表 4.3: 提案スキームの審査項目の分担 ([83] 表 2 より©2012 IEICE)

			商用認証局				学術スキーム			
			DV		OV/EV		機関審査		発行審査	
			登録局	加入者	登録局	加入者	登録局	機関責任者	登録担当者	加入者
①	組織	本人性	×		○		○			
②		実在性	×		○		○			
③	ドメイン	本人性	○		○		● →	○		
④		実在性	○		○		● →		○	
⑤	機関責任者	本人性					○			
⑥		実在性					○			
⑦	登録担当者	本人性						○		
⑧		実在性						○		
⑨	加入者	本人性	×		○		● →		○	
⑩		実在性	×		○		● →		○	
⑪	加入者サーバ	本人性		○		○				○
⑫		実在性		○		○			○ ←	●

で何度でも証明書の発行を要求することができるものとし，この時に行う審査を発行審査とする．

(3) 審査項目

審査項目と審査方法の関係を表 4.3 に示す．機関審査は，表 4.3 における①～⑧，発行審査は同じく⑨～⑫とした．機関審査では，組織と機関責任者，登録担当者の身元確認をそれぞれ行う．また，ドメインについても本人性の確認のみ行う．機関責任者は実証実験への参加に責任を持つ学内担当者であり，登録担当者は，参加後に学内の加入者からの発行審査を主に行う学内担当者である．発行審査では，ドメインの実在性確認と，加入者の身元確認，加入者サーバの実在性確認を行う．

機関審査は NII が行い，発行審査は各機関内の登録担当者が行うものとする．即ち，NII が RRA，各機関の機関責任者および登録担当者が LRA という位置づけになる．審査項目と審査方法の関係を表 4.3 に示す．

4.3.2 機関審査への実装

機関審査に対して提案手法の実装を行った．(2) で示した審査項目について，利用可能なデータソースを洗い出し，マトリクスへマッピングしたものを図 4.5 に示す．なお，わかりやすさのために，マトリクスには保証レベル評価を行ったもっともコスト合理的なデータソースのみを示した．

機関審査に共通の確認作業として，表 4.3 の①～③ を予め RA で確認する．

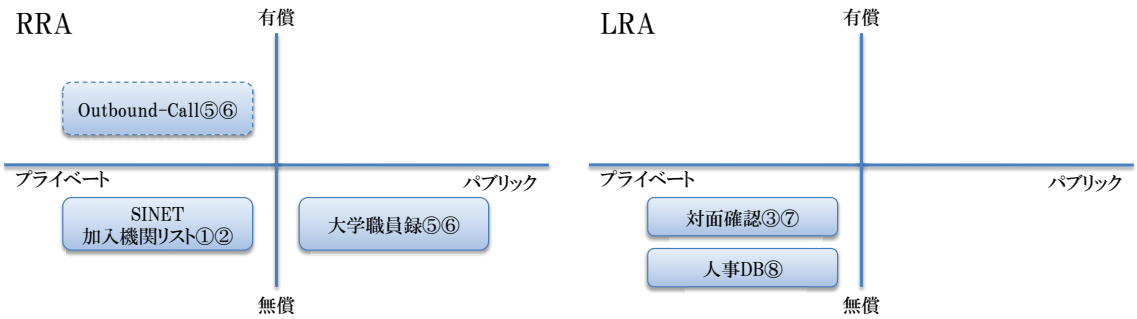


図 4.5: 機関審査への実装

機関審査においては，RRA(NII) は，組織と機関責任者の身元確認を行う．機関の身元確認には，NII 自身が所有する SINET 加入機関リストを用いることで，そのアクセスコストを無償で実現した．SINET には 2011 年 3 月末時点で全国 740 の学術機関が加入しており，その加入時には一定の審査が行われることから，信頼できる情報源として活用するものとした．機関責任者については，スキーム設計当時刊行されていた廣潤社の「全国大学職員録」[91] をデータソースとした．これは当時一般に入手可能な書籍のため，購入後のアクセスコストは無償であった．全国大学職員録では，課長職以上の職員，准教授以上の教員が掲載されており，機関責任者の資格をこれに合わせることで，データソースの対象とする範囲と審査対象の基本的なギャップについては解決した．しかしながら，プライバシーの関係で前述の資格を有していても職員録への掲載を拒否する教職員もおり，こうした場合の補完として，例外的に Outbound-Call を使うことにした．

一方 LRA(機関責任者) は，登録担当者の身元確認とドメインの本人性確認を行う．登録担当者の身元確認には，登録担当者の実在性確認に学内の人事データベースなどを，また登録担当者とドメインの本人性確認については対面確認を行うものとした

4.3.3 発行審査への実装

発行審査に対して提案手法の実装を行った．(2) で示した審査項目について，利用可能なデータソースを洗い出し，マトリクスへマッピングしたものを図 4.6 に示す．なお，わかりやすさのために，マトリクスには保証レベル評価を行ったもっともコスト合理的なデータソースのみを示した．

発行申請にあたり，LRA では表 4.3 の④，⑨，⑩，⑫ を確認する．①~③については既に機関審査で確認済みであることから，発行申請の都度の確認は省略できる．④は機関内部での DNS におけるホスト名の割り当て問題であり，DNS 未登録時点での発行申請なども想定されるため，機関内部のサーバ管理データベースあるいは相当の情報を用いることとした．⑨および⑩は，LRA であれば加入者の実在性確認に必要な教職員台帳など信頼できる情報源へのアクセスが RA よりも明らかに容易であり，また加入者と直接対話できる可能性も高いなど多様な本人性確認が実現できる．⑫は，④同様に機関内部のサーバ管理データベース (相当) を用いることとした．これらの確認作業は，LRA 内部で機関責任者から登録

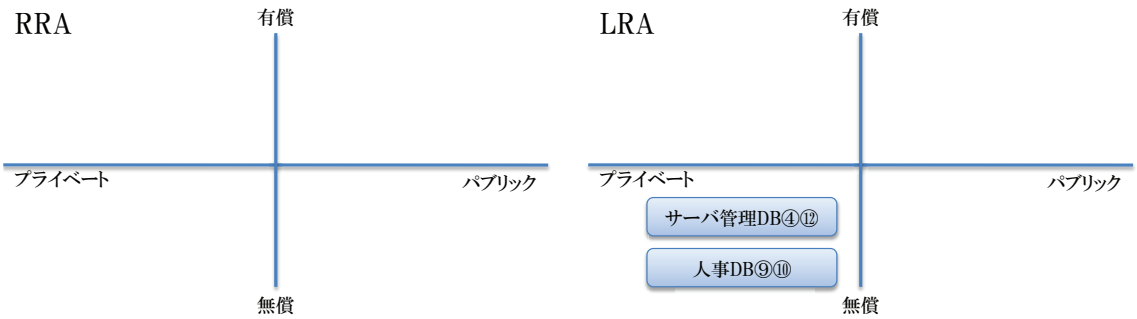


図 4.6: 発行審査への実装

表 4.4: 機関審査の評価

	審査項目	データソース
RRA	組織の身元確認コスト 機関責任者の身元確認コスト	SINET 加入機関リスト 大学職員録または OBC
LRA	ドメインの本人性確認コスト 登録担当者の身元確認コスト	対面確認 対面確認および人事情報 DB

業務を委任された登録担当者によって行われる．

発行審査にあたって，RRA 側で行う審査は特にない．

4.4 提案手法の評価

前節では，提案手法をサーバ証明書プロジェクトの機関審査および発行審査に対して実装し，それぞれの身元確認スキームを設計した．本節では，設計した身元確認スキームのコスト合理性について既存の商用認証局の発行スキームと比較評価することで，提案手法がコスト指向性のある設計手法であることを示す．

本節では，機関審査と発行審査に分けて身元確認コストの評価を行う．

4.4.1 機関審査の評価

機関審査の身元確認コストは機関数に比例する．機関審査で対象とする審査項目と，各審査項目において参照するデータソースを表 4.4 に示す．

プロジェクトを通じて RRA における機関審査にかかったコスト $C_{機関,RRA}$ は所要時間にすると，およそ機関あたり 2/3 時間であった．LRA における機関審査のコスト $C_{機関,LRA}$ については，十分なサンプリングはできていないものの，RRA と同程度の時間で実施したという情報も得ており，本評価においては RRA と同じ値で評価することとした．

この場合，機関審査の身元確認にかかる総コスト $C_{機関,total}$ は，参加機関数を n とすると以下の式で与えられる．

表 4.5: 発行審査の評価

	審査項目	データソース
LRA	ドメインの実在性確認コスト	サーバ管理台帳
	加入者の身元確認	人事情報 DB
	加入者サーバの実在性確認	サーバ管理台帳

表 4.6: 商用認証局の評価

審査項目	データソース
組織の身元確認	企業情報データベース
ドメインの身元確認	WHOIS データベース
加入者の身元確認	Ourbound-Call

$$C_{\text{機関},total} = (C_{\text{機関},RRA} + C_{\text{機関},LRA}) * n \tag{4.1}$$

4.4.2 発行審査の評価

発行審査の身元確認コストは発行枚数に比例する．発行審査で対象とする審査項目と，各審査項目において参照するデータソースを表 4.5 に示す．

各機関での発行審査にかかるコスト $C_{\text{発行},LRA}$ は，ほぼ自動化している機関から厳格に審査している機関まで機関によっても異なるが，10˜ 30 分程度という声が多く，本評価では 1 枚あたり概ね 20 分と仮定した．

この場合，機関審査の身元確認にかかる総コスト $C_{\text{発行},total}$ は，発行枚数を p とすると以下の式で与えられる．

$$C_{\text{発行},total} = C_{\text{発行},LRA} * p \tag{4.2}$$

4.4.3 商用認証局の評価

商用認証局の身元確認コストは単純に発行枚数に比例する．商用認証局が対象とする審査項目と，各審査項目において参照するデータソースについて，表 4.4 および 4.5 と対比しやすいよう表 4.2 から抜粋したものを表 4.6 に示す．

商用認証局での身元確認にかかるコスト $C_{\text{商用}}$ は，具体的な作業時間などは明らかにされていないため，以下の仮定にもとづいて算出した．

> 商用認証局におけるサーバ証明書費用の大半は身元確認で占められると言われていることから，サーバ証明書費用を 62,500 円/枚，粗利を 20%，粗利を除く原価

表 4.7: コスト比較に用いた値 (単位：人・時)

パラメータ	値
$C_{\text{機関},RRA}$	2/3
$C_{\text{機関},LRA}$	2/3
$C_{\text{発行},LRA}$	1/3
$C_{\text{商用}}$	8

のさらに 80%が身元確認にかかるコストと仮定した．なお，サーバ証明書費用は市場価格がおよそ 3~ 12 万円/枚とばらつきが大きいことから，この範囲内において便宜上計算しやすい数値を用いている．この場合，審査費用は 62,500 円/枚 $*(1-0.2)*0.8 = 40{,}000$ 円/枚 である．一方，RA オペレータの人時単価を 5,000 円 (人月 80 万円と仮定) とすると， 40,000 円/枚/5,000 円/人時 = 8 人時で $C_{\text{商用}}$ が与えられることになる．

この場合，商用認証局の身元確認にかかる総コスト $C_{\text{商用},total}$ は，発行枚数を p とすると以下の式で与えられる．

$$C_{\text{商用},total} = C_{\text{商用}} * p \tag{4.3}$$

4.4.4 コスト比較

これらの評価をもとに，提案手法における機関審査および発行審査にかかる身元確認の総コストの合計 $C_{\text{機関},total} + C_{\text{発行},total}$ が，商用認証局の身元確認にかかる総コスト $C_{\text{商用},total}$ よりも低いかどうか比較を行う．

$$C_{\text{商用},total} > C_{\text{機関},total} + C_{\text{発行},total} \tag{4.4}$$

$$p/n > (C_{\text{機関},RRA} + C_{\text{機関},LRA}) \quad /(C_{\text{商用}} - C_{\text{発行},LRA}) \tag{4.5}$$

式 (4.4) に式 (4.1)~(4.3) を展開展開すると式 (4.5) が導かれ，これに表 4.7 の値を代入すると，およそ $p/n > 0.18$ となる．即ち機関あたり約 0.18 枚以上の証明書を発行する限りは，提案手法にもとづく身元確認スキームがコスト合理的であることが示された．

サーバ証明書プロジェクトは，4.3 節でスキームの設計を行ったフェーズ 1 の後も継続しており，各フェーズの参加機関数と発行枚数を表 4.8 に示す．いずれも機関あたりの証明書発行枚数は 0.18 枚以上であることが確認でき, 提案手法の実用性が明らかになった．

表 4.8: サーバ証明書プロジェクトの実績値

フェーズ	期間	参加機関数 (n)	のべ発行枚数 (p)	p/n
フェーズ 1	平成 19 年 4 月 ～ 平成 21 年 6 月末	97	2,413	24.88
フェーズ 2	平成 21 年 4 月 ～ 平成 24 年 3 月末	276	9,561	34.64
フェーズ 2 延長	平成 24 年 4 月 ～ 平成 27 年 3 月末	323	19,009	58.85

4.4.5 考察

本提案手法のポイントは，データソース選定マトリクスと，マトリクスも含めた 4 つのデータソース評価項目にある．

(1) マトリクスの特徴

マトリクスの各象限について考察する．第 3 象限は，高い保証レベルのデータソースの選択肢が多く，アクセスコストのかからないため，ここにマッピング可能なデータソースが最も理想的ということになる．しかし第 3 象限は所在がプライベートのため，RRA 方式においてここに無償でアクセスできるケースは極めて限られることになる．数少ない例として，当該組織が IdP としてアイデンティティ情報を提供している場合が考えられる．ただし，アイデンティティ情報の提供を受けるにあたってはエンドユーザが IdP の認証を受ける必要があるなど，通常は制約がかなり大きいと考えられる．

その次にコスト合理的なのは，第 3 象限同様に無償で参照可能な第 4 象限である．実際にコンシューマサービスではここに示されるデータソースを身元確認に用いているところが多いとみられる．しかしながら，例えば図 4.2,4.3 に示したメールアドレスの到達性確認は，1.1.3 節でも述べたように充分な身元確認とは言えず，また住民票などの公的証明書も IdP のコストはともかくエンドユーザの手間がかかるというデメリットがあるなど，この象限にマッピングされるデータソースだけで高い利便性と十分な身元確認の両者を実現することは難しいと考えられる．

このため，やはり何らかの形で第 1, 第 2 象限にマッピングされるデータソースを補完的に使っていくスキームが多くなるものと考えられる．つまり，身元確認に一定のコストをかけることは不可避であり，そうした状況においてよりコスト合理的なデータソースを選定する本提案手法は意義が大きいと言える．

(2) マトリクスの応用

4.2 節では，マトリクスの典型的な用法として，データソースを選定するケースについて説明した．しかしこのマトリクスは必ずしも指定した手順以外での応用が可能である．前述した各象限の特徴を踏まえて，予めデータソースのマッピング先となる象限を決めることで，洗い出すデータソースの要件を明確にすることも可能である．例えば，サーバ証明書プロジェクトで利用した図 4.5 にある大学職員録は，RRA による身元確認コストを削減するため，パブリックなデータソースの中で，一定の範囲の教職員の身元確認に利用可能なデータソースを探した結果に発見したものである．

実際に，データソースの洗い出しは容易ではなく，選定するほどには十分な候補を揃えられないケースも多いと考えられる．従来の EAAF のようなリスク指向設計手法では，データソースの選定などは考慮されていない．身元確認コストの合理化においては，(一定の保証レベルを保ちつつも) より低コストの代替データソースの選定が不可欠であり，こうしたデータソース選定を支援するマトリクスの意義は大きいと考えられる．

(3) 先行研究に対する新規性

身元確認スキームの設計手法として，3.1.1 節で示した EAAF やこれに類する SP-800-63-2[43] をはじめとする各国の取り組みがある．これら EAAF をベースとするアプローチは，リスク評価にもとづいて保証レベルから身元確認スキームの設計までを支援するもので，いわばリスク指向設計手法と言える．これに対して本提案は保証レベルの維持を前提としつつコスト削減を実現するためのコスト指向の設計手法を提案した．リスク指向の保証レベル導出は，ある意味合理的と言えるが，実際にリスクに着目するのは SP 側であり，IdP にとってはリスクよりも，一定の保証レベルを実現しようとした時にどれだけの投資運用コストが必要なのか，保証レベルに対応した技術要件や運用要件を確認しながら検討するのが実態である．しかしながら，EAAF はじめリスク指向設計手法では，LRA/RRA それぞれにおいて典型的な身元確認スキームを示すのみで，そのコスト合理性についてはあまり議論されておらず，また実質的な選択肢も十分ではない．これは，EAAF などは行政組織が IdP または SP として関与するフェデレーションを暗に想定しているからだとも考えられる．そこでは行政組織による認定や法制度への準拠などコスト合理性だけでない一定のガバナンスが働くことになり，コスト合理性よりも保証レベルの担保に重点が置かれている印象もある．しかしながら，少なからず民間事業者が IdP を運営する場合はその運用コストには一定の経済合理性が求められ，また行政組織であっても本質的には要求される保証レベルを逸脱しない範囲でコスト合理的であるべきで，こうした点からもリスク指向のアプローチが不可欠と考える．つまり IdP にとってはリスク指向よりもコスト指向の設計手法が合理的であるとも考えられ，その点で EAAF とは違う観点から身元確認スキームの設計が可能な本提案手法の意義は大きいと考えられる．

4.5 本章のまとめ

本章では，データソースのコスト合理的な選定にもとづく身元確認スキームのコスト指向設計手法を提案し，国立情報学研究所のサーバ証明書プロジェクトにおいて本提案手法を用いて身元確認スキームの設計を行った．同プロジェクトを通じて同スキームのコスト合理性を評価することでその実用性を示した．

商用認証局の身元確認スキーム分析を通じて，身元確認に用いるデータソースと身元確認コストの関連に着目した．保証レベルを満たす範囲でよりコスト合理的なデータソースを選定できれば身元確認コストの削減に寄与できると考え，テータソース選定における評価項目をもとに，データソース選定マトリクスを考案した．そして，このマトリクスを用いたコスト合理的なデータソースの選定と，保証レベルへの準拠性確認などを含む，身元確認スキームのコスト指向設計手法を提案した．

国立情報学研究所のサーバ証明書プロジェクトにおいて，身元確認スキームを本提案手法にもとづいて設計し，同プロジェクトを通じて設計したスキームのコスト合理性を示すことで提案手法の実用性を明らかにした．本提案手法により，保証レベルを保ちつつコスト合理的にデータソースを選定する身元確認スキームの設計が可能になった．

一方で，本手法のコスト合理性が満たされる条件として，参加機関数や発行枚数が含まれることから，これらの規模とコスト合理性の関連についても明らかにする必要がある．これについては，次章において身元確認のコスト構造と規模の関連を明らかにすることで，定量的な評価を可能とした．

第5章　身元確認コスト構造のモデル化と評価

第三者から認証情報の提供，ひいては相互にアイデンティティ情報の交換を実現するフェデレーションにおいて，相互に信頼関係を構築することは非常に重要である．信頼関係を与える枠組みとして，保証レベルにもとづく認証フレームワークが米連邦政府を中心に整備され，国際標準化に至った．

しかしながら，アイデンティティ情報の交換が促進されるほどにそのなりすましリスクは高まることになり，アイデンティティ情報を登録する段階での身元確認の保証レベルに対する期待もまた高まってくるものと予想される．

身元確認の保証レベルを高めれば，少なからずコストがかかることになるため，IdP のコスト合理的な運用においてはこれを可能な限り抑える工夫が必要である．そこで本章では，身元確認にかかるコストを適切に評価分析し，コスト改善に寄与できる身元確認のコスト構造モデルを提案する [61].

モデル化のコンセプトは，4 章で明らかになった身元確認のコストに影響するデータソースの評価項目のうち，保証レベルに影響を及ぼすデータソースの真正性を除く，データソースの所在, RA の配備方式, データソースへのアクセスコストの 3 要素のみでコスト構造をモデル化する点にある．これによって，保証レベルを変更せずに身元確認のコスト評価を行うことが可能となる．パラメータ化された異なる評価項目によるコスト評価モデルを開発し，シミュレーションにおいて提案モデルの有効性を示すことで，身元確認の典型的なユースケースとして実社会の大規模 PKI に対する提案モデルの適用可能性を示した．その結果，提案モデルの 2 つの貢献ほ示した．ひとつは RA の配備方式に依存したシステムのコスト性能の最適化ツールとして利用できること，もうひとつは既存システムの定量的評価比較方法として提供できることである．5.3 節で評価対象として扱ったのはいずれもサーバ証明書発行サービスだが，本モデルは身元確認のみを対象としていることから，証明書発行に限らず，パスワードベースのものも含め一般的な ID 管理システムのユースケースにも広く応用が期待できる．

本章の構成は以下の通りである．まず，5.1 節では大規模環境における身元確認の基本について導入する．5.2 節では提案するコスト構造モデルについて述べる．5.3 節ではシミュレーションを用いてモデルの有効性を評価する．5.4 節では，実社会の大規模 PKI に対する提案モデルの適用可能性について議論する．5.5 節では，関連研究について示し，最後に 7 節で本章についてまとめる．

5.1 背景: 身元確認

5.1.1 身元確認のためのデータソース

身元確認プロセスは，アイデンティティ情報の検証のために，何らかのデータソースから十分な情報を必要とする．データソースを場所によって以下のように分類した．

- 外部リソースは，インターネットホストのための WHOIS データベース [66]，信用調査，法人登記など，政府を含め組織外部で管理される．
- 内部リソースは，職員録やイントラネット認証システムなど申請者の組織によって管理される．

WHOIS データベースは無償だが，法人登記情報や信用調査など多くの外部リソースは有償である．これら外部リソースへのアクセスコストは RA の配備方式にかかわらず一緒である．

例えば，身元確認の典型的で信頼できる方法として，対面調査が考えられる．対面調査は，事前の面識や証明書の顔写真といったリソースを必要とする．前者は内部リソースととらえることができ，後者は社員証のような内部リソースの場合もあるし，行政機関のデータベースによる確認を必要とする国民 ID カードのような外部リソースの場合もある．

RA がアクセスすべきデータソースは身元確認プロセス，申請者からの情報，さらにはどんなリソースが利用可能なのかに依存する．内部リソースのアクセスコストは RA の配備方式によっても異なる．例えば，一般的な組織は彼らのセキュリティポリシにもとづいて内部リソースへ外からアクセスすることを禁じているかも知れない．たとえ申請者の組織の外にいる RRA が内部リソースにアクセスするにしても，RRA に十分な情報を取り出すには，例えば RRA から内部アクセスを許すような F/W のセキュリティポリシ変更や，RRA から内部へのアクセスを許す Virtual Private Network (VPN) の導入など，さらなる追加コストが発生する．

RRA は内部リソースにアクセスするためには LRA よりも多くのコストを必要とするので，つまるところ RRA は一般的に内部リソースよりも安価な外部リソースを見つける．LRA は，もちろん安価な外部リソースを使うこともできるが，内部リソースを好むものと予想される．

5.1.2 RA の配備方式と規模の課題

両方の RA タイプは一長一短があり，どちらがよいかは多数の要素に依存するため，定性的に示すことはできない．例えば，サーバ証明書を発行する商用認証局は，より地理的に広範な顧客をカバーするために RRA を好むかも知れない．商用 CA はまた，LRA と比較して労働集約によって業務効率を最大化しようとする．一方で，RRA は内部リソースへのアクセスが一般に困難なので，身元確認のために十分な外部リソースを集めなければならない．複数のキャンパスに分散する教職員や学生がおり，集約的な IT プラットフォームを共有し

ない大学では，LRA を好むかもしれない．LRA は RRA よりも多くの RA オペレータが必要で，これは経験や訓練の不足につながるかも知れないので，RRA よりも高い運用リスクを抱える．

IdM システムのスコープが広がれば，RA オペレータの数も増えるが，増える要因は RRA と LRA で異なる．RRA は典型的な集約運用である．IdM システムにおけるトランザクション件数の増加は業務効率を向上させる．何故ならオペレータ一人当たりの処理可能なトランザクションが増えれば身元確認の自動化を増やすからである．しかしながら，RRA は内部リソース外部リソースにかかわらずアクセスコストがかかる．規模によるコスト削減はアクセスコストを下回る．RRA のアクセスコストは LRA よりもかなり高いので，規模によるコスト削減がアクセスコストを下回ることはめったにない．

これに対して，LRA は分散運用において典型的に利用され，LRA 要員数は処理可能なトランザクション数よりも分散する拠点数に依存する．処理可能なトランザクション数を増やすためには，拠点あたりのトランザクションを増やす必要がある．しかしながり，LRA のアクセスコストを下げる内部リソースのみを使うか，安価な外部リソースを利用することによる LRA のアクセスコスト削減の方が容易である．

5.2 身元確認のコスト構造モデル

この分析から，トランザクション件数と拠点数に依存するコストモデルを提案する．

身元確認の年間運用コストは，人件費と *(*手作業以外の*)* 運用コストに分けられる．人件費 C_u は人的リソースのコストであり，RA が申請者を手作業で確認した場合に発生する．手作業以外のトランザクションあたりの運用コスト C_k は，RA が内部または外部のデータリソースを参照した場合に発生する．

ここで，オペレータ数として n を，年間の身元確認件数として p を，それぞれ導入して，以下のように表現する．

$$C = C_u * n + C_k * p \tag{5.1}$$

C_k に寄与する要素は以下を含む：

- 組織の履歴や与信情報などの商用データベースへのアクセス料金
- 人事管理システムなど内部データベースにアクセスする VPN 利用料金 (従量分)
- 内部データベースから情報を取り出すための運用コスト

RRA においては $n = 1$ と仮置きした．これは図 5.1 に示したように，p が大きいとき，n の効果は $C_{k,RRA}$ よりも十分に小さいためである．LRA においては，5.1.1 節で述べたように，身元確認にかかる各オペレータの稼働率は一般に RRA よりも小さいので，$C_{u,RRA}$ と $C_{u,LRA}$ の稼働率比として r を導入する．5.1.2 節で述べたように，典型的に $C_{k,RRA} \gg C_{k,LRA}$ なので，$C_{k,LRA}$ は無視できると仮定した．LRA/RRA の $C_{k/u}$ は，それぞれ $C_{k/u,LRA/RRA}$ とあらわすものとする．

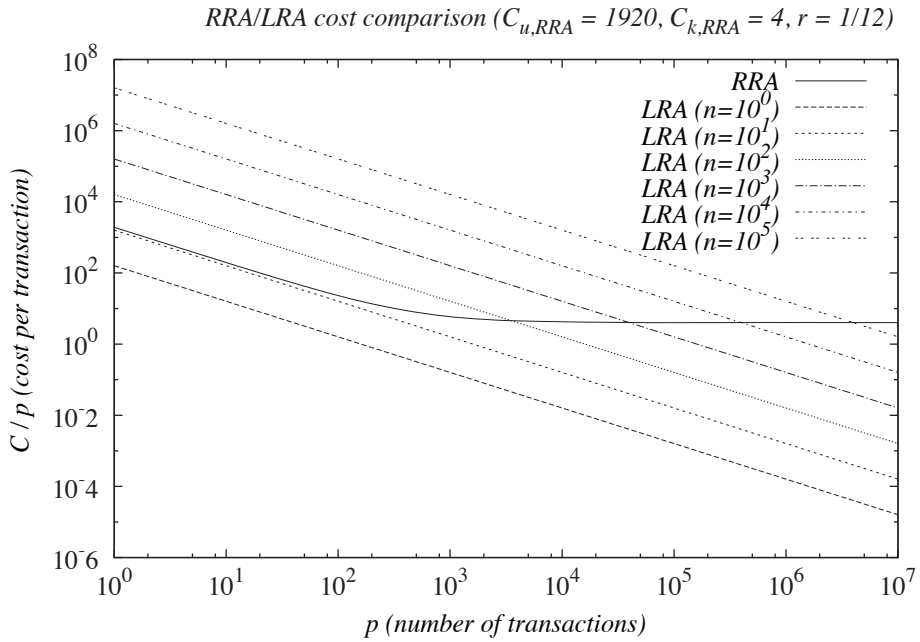


図 5.1: 提案モデルのシミュレーション結果 ([61]Fig. 2 より©2014,IEEE)

本章は，サポート時間帯やエンドユーザへのクレデンシャル配布，操作サポートなどエンドユーザサポートの運用コストは考慮しない．また，コストの曖昧さを定量的に評価する方法についても本論文の範囲外とした．組織によっては，身元確認の正しさについて，LRA または RRA はより大きな保証を提供する場合がある．

従って，式 (5.1) は，RA の各配備方式におけるトランザクションあたりのコストとしてそれぞれ式 (5.2) および (5.3) であらわされる．

$$C_{RRA}/p = C_{u,RRA}/p + C_{k,RRA} \tag{5.2}$$

$$C_{LRA}/p = C_{u,RRA} * r * n/p \tag{5.3}$$

これらの式は，2 種類の RA 配備方式の異なる因子によってパラメータ化されたコスト評価モデルを示す．以降では，人件費のコスト単位として人時を用いる．なお，$C_{u,RRA}$ は人件費ではないが，計算の便宜上人時に換算して扱う．図 5.1 は，$C_{u,RRA}$ に 1,920 人時 (1 人年相当)，$C_{k,RRA}$ に 4 人時，r に 1/12 を用いた場合の本モデルのシミュレーション結果を示す．

図 5.1 からわかるように，LRA においては p が増えるほど C_{LRA}/p は減少し，p が交点よりも大きい時は時は，C_{RRA}/p よりも小さくなる．C_{LRA}/p を一定にするには，オペレータの数が Δn 増えるごとに，p は $\Delta n * C_{u,RRA} * r/C_{k,RRA}$ だけ増えなければならない．例えば，図 5.1 では，オペレータを一人増やしたときに C_{LRA}/p を一定にするには，p は 40 件増えなければならない．

5.2.1 パラメータの妥当性

本節では，図 5.1 に用いたパラメータ $C_{u,RRA} = 1,920, C_{k,RRA} = 4, r = 1/12$ について，それぞれの妥当性を述べる．$C_{u,RRA}$ は RRA における人的リソースのコストであり，式 (5.1) で n=1 と仮置きしているので，基本的に $C_{u,RRA}$ は 1 人あたりの作業時間である．月あたりの標準稼働時間を 160h とするならば，最大でも年間 1,920h 以下ということになり，ここでは最大値で扱うことにした．

$C_{k,RRA} = 4$ は，いくつかの仮定にもとづいた値である．$C_{k,RRA}$ は手作業以外の運用コストなので，人時で表すものではないが，計算の便宜上，人時に換算している．商用認証局におけるサーバ証明書費用の大半は身元確認で占められると言われていることから，サーバ証明書費用を 62,500 円/枚，粗利を 20%，粗利を除く原価の 60%が身元確認にかかる人件費，残り 40%が運用コストと仮定した．なお，サーバ証明書費用は市場価格がおよそ 3~12 万円/枚とばらつきが大きいことから，この範囲内において便宜上計算しやすい数値を用いている．この場合，$C_{k,RRA}$ は $62,500$ 円/枚 $*(1-0.2)*0.4 = 20,000$ 円/枚 である．一方，RA オペレータの人時単価を 5,000 円 (人月 80 万円と仮定) とすると， $20,000$ 円/枚/$5,000$ 円/人時 $= 4$ 人時 で $C_{k,RRA}$ が与えられることになる．サーバ証明書費用やその原価構造，RA オペレータの単価によっても変わってくるが，いずれにしても $C_{k,RRA}$ は概ね $10^0 \sim 10^1$ のオーダーに収まると言ってよい．

r は $C_{u,LRA}/C_{u,RRA}$ で与えられる．これは n や p にも大きく依存するが，ここでは RRA オペレータのエフォート率が 100%(年間 1,920h) なのに対して，LRA オペレータのエフォート率を約 8%(年間 160h) を想定して 1/12 という値を仮置きした．ここで r の値の妥当性は本質的な問題ではなく，任意の値を設定してシミュレーションできるようパラメータとして組み込んだことが重要である．より適切な評価を行う場合には，$C_{u,LRA}$ を実測するなどしてより具体的な値を用いることが必要である．

5.3 評価

本節では，提案モデルの有効性を評価するために用いた 4 つのシミュレーションを示す．4 つのケースのパラメータを表 5.1 に示す．

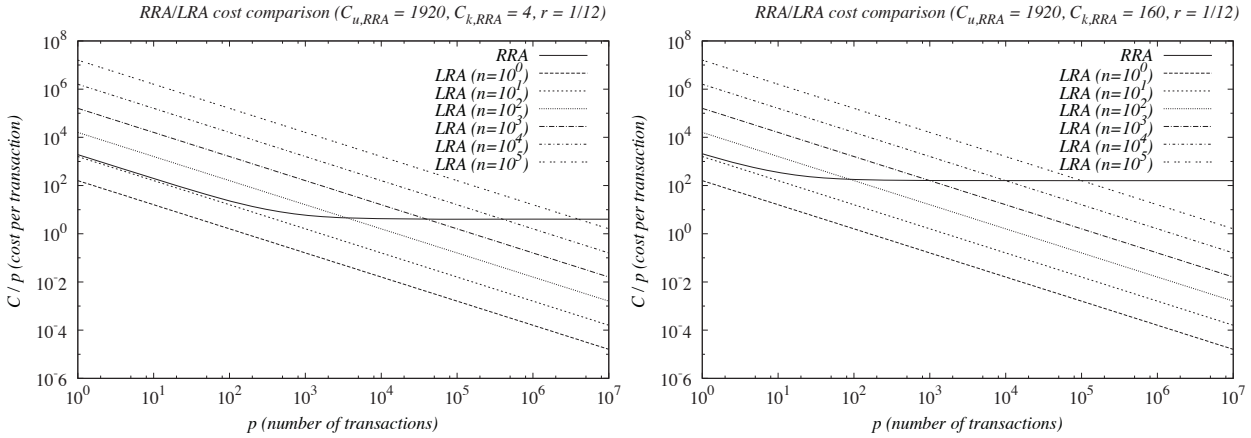
図 5.2a は，図 5.1 と同一だが，他のグラフとの比較しやすいよう再掲した．

- 図 5.2b は，LRA タイプのコストは変わらずに，$C_{k,RRA}$ だけが増加している．
- 図 5.3a は，RRA タイプのコストは変わらずに，r を小さくしたことで LRA タイプのコストだけが減少している．
- 図 5.3b は，どちらの RA タイプのコストも減少しており，$C_{u,RRA}$ が減少したので LRA と RRA の交点も左にシフトしている．

具体的に，以下の結果が本も出るから明らかにされた．図 5.2b から，$C_{k,RRA}$ が増えるとトランザクション数が少ないほど LRA がコスト優位になることがわかる．図 5.3a において，

表 5.1: シミュレーションに用いたパラメータ群 ([61]TABLEusepackage(able); I より ©2014,IEEE)

Case	$C_{u,RRA}$	$C_{k,RRA}$	r
図 5.2a	1,920	4	1/12
図 5.2b	1,920	160	1/12
図 5.3a	1,920	4	1/240
図 5.3b	160	4	1/12



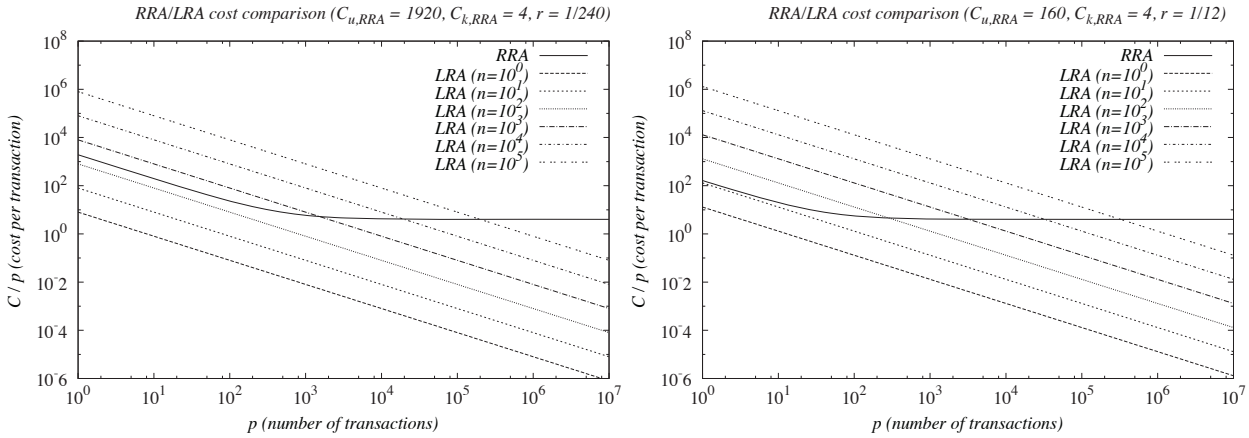
(a) $C_{u,RRA} = 1920, C_{k,RRA} = 4, r = 1/12$ (b) $C_{u,RRA} = 1920, C_{k,RRA} = 160, r = 1/12$

図 5.2: シミュレーション結果 #1([61]Fig. 3 より ©2014,IEEE)

r が減るとトランザクション数が低いほどほど LR コストメリットがあることがわかる．図 5.3b は，$C_{u,RRA}$ を小さくすると，どちらの RA タイプも全体でトランザクションあたりのコストを下げることができ，LRA にコストメリットがあることを示している．

このように，$C_{u,RRA}$, r, n and $C_{k,RRA}$ が本モデルにおけるコスト因子である．$C_{u,RRA}$ は RRA と LRA の間で共有する値なので，LRA におけるコスト因子は n と r のみである．RRA に対して LRA のコストメリットを実現するには，n と r を小さくすることが必要となる．一方で，n または r が大きくなると，ああるいは $C_{k,RRA}$ or $C_{u,RRA}$ を小さくすると，LRA よりも RRA にコストメリットが出る．

加えて，本モデルによって，LRA タイプにおいて想定した n と p の値から，コストリーズナブルな $C_{k,RRA}$ を，あるいは RRA タイプにおいて想定した $C_{k,RRA}$ の値から，n と p の損益分岐点を，それぞれ推定することが可能である．



(a) $C_{u,RRA} = 1920, C_{k,RRA} = 4, r = 1/240$ (b) $C_{u,RRA} = 160, C_{k,RRA} = 4, r = 1/12$

図 5.3: シミュレーション結果 #2([61]Fig. 4 より©2014,IEEE)

5.4 議論

本節では，本モデルを既存の証明書発行サービスに適用することで，その有効性について議論する．適用するにあたっては，$C_{u,RRA}$, $C_{k,RRA}$, and r について，図 5.2 と同一の値を用いた．

5.4.1 UPKI サーバ証明書プロジェクト

NII は，UPKI サーバ証明書プロジェクトと呼ばれる，日本の学術機関を対象としてサーバ証明書発行サービスを提供している．NII は認証局を運用し，参加機関は LRA として機関内部の申請者について必要な身元確認を行う．UPKI サーバ証明書プロジェクトは，フェーズ 1[2] が完了し，フェーズ 2[19] が延長 (2014 年 6 月時点) されており，表 5.2 にその概要を示す [24]．参加機関数を n に，証明書発行枚数を p に代入し，$n = 97$ および $n = 237$ における式 (5.3) と，これに対して C_{RRA}/p として式 (5.2) をプロットしたものを図 5.4 に示す．このケースでは，RRA モデルが若干だけ LRA よりもコストメリットがあることが明らかになった．

フェーズ 1 とフェーズ 2 の結果は，$C/p \quad = 14.15$ に収束する．つまり，$C_{k,RRA}$ が 14.15 人時以上であれば，RRA は LRA よりもコストリーズナブルである．

$C_{u,RRA}$ を変えずに LRA が RRA よりもコスト優位になるには，フェーズ 1 では $C_{u,LRA} < 99.50$，フェーズ 2 では $C_{u,LRA} < 138.57$ を満たす必要がある．LRA はが RRA よりコスト優位になるのは，p が $C_{u,RRA} * r * n/p < C_{k,RRA}$ を満たす場合に限られる．これは，フェーズ 1 であれば $p > 3,880$，フェーズ 2 であれば $p > 11,040$ である．

UPKI サーバ証明書プロジェクトをテストケースとして用いることにより，本モデルが既存システムの定量的な評価比較手法として有効であることを示した．

表 5.2: UPKI サーバ証明書プロジェクトの実績 [24]

フェーズ	Term	n	p
フェーズ 1	2007 年 4 月 2 日˜ 2009 年 6 月末	97	2,413
フェーズ 2	2009 年 4 月 1 日˜ 2012 年 3 月末	276	9,561
フェーズ 2 延長	2012 年 4 月 1 日˜ 2015 年 3 月末	317	(未計上)

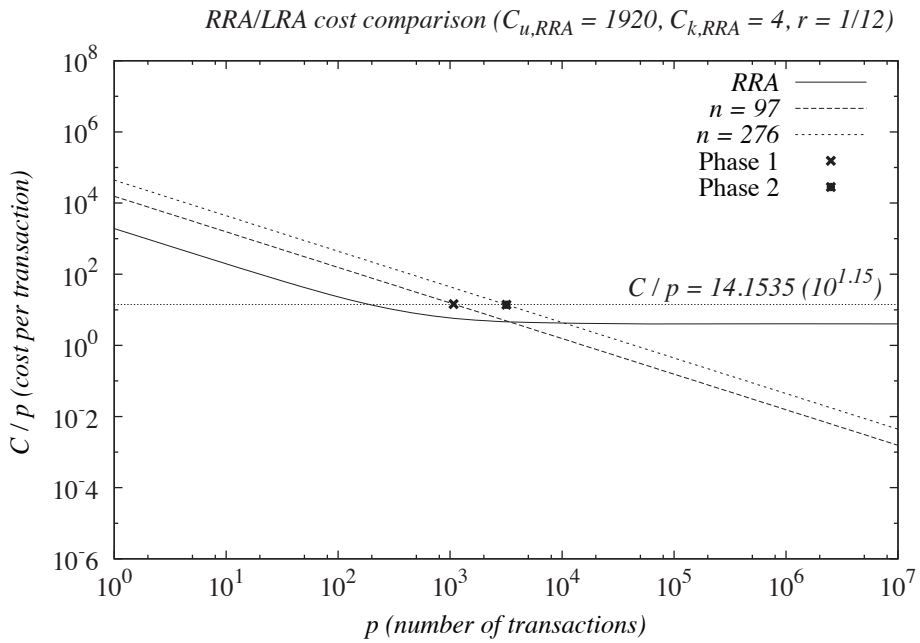


図 5.4: UPKI サーバ証明書プロジェクトへの適用 ([61]Fig. 5 より©2014,IEEE)

表 5.3: 他のケーススタディのパラメータ群 ([61]TABLE III より©2014,IEEE)

Service	n	p
TCS	25	93,333
ICS	264	80,870
住基カード	1,749	914,755

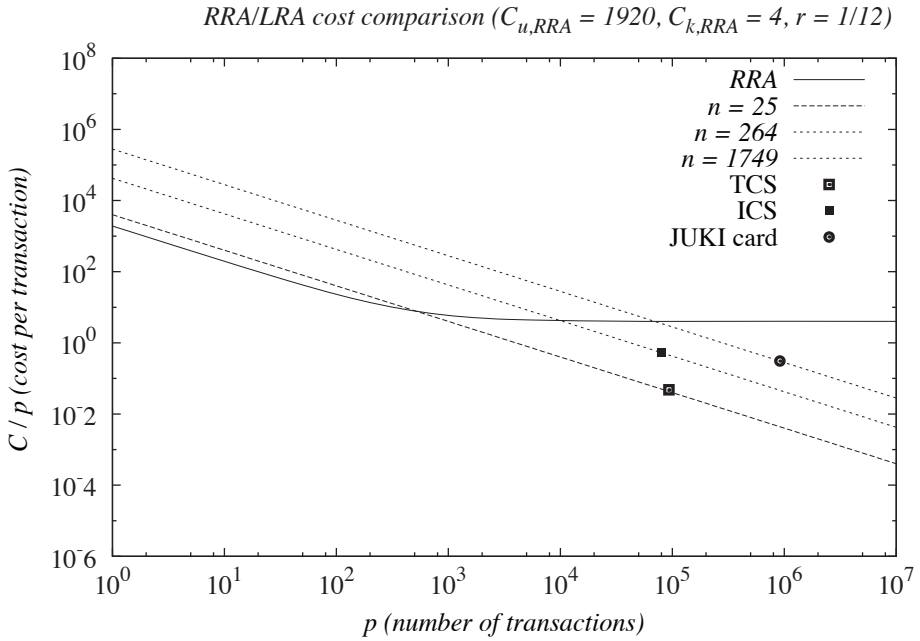


図 5.5: 他のケーススタディへの適用 ([61]Fig. 6 より©2014,IEEE)

5.4.2 身元確認に関連する他のケーススタディ

他の地域においても同様に学術機関を対象としたサーバ証明書発行サービスがある．欧州の Trans-European Research and Education Networking Association (TERENA) によって提供されている　TERENA Certificate Service (TCS) [16] や，北米の InCommon によって提供されている InCommon Certificate Service (ICS) [5] がある．これらのサービスも UPKI サーバ証明書プロジェクトと同様に，参加機関が機関内部の申請者の身元確認を行う LRA としての役割を担う．ここでも同様に参加機関または参加国数を n として，証明書発行枚数を p として扱うものとする．

また，PKI アプリケーションではないものの典型的な LRA 方式の身元確認を行う事例として，日本の国民 ID として使われている住基カードについても本モデルの適用を行った．住基カードは自治体の行政窓口で対面による身元確認が行われ，希望する全国民に発行される．

表 5.3 に，TCS，ICS，住基カードの主要なパラメータを示す [17], [5], [7, 25]．図 5.5 は，表 5.3 を式 (5.2) および (5.3) にプロットしたものを示した．

5.4.3 まとめ

5.3 節から，LRA が大規模環境においてコスト優位になるには，

- トランザクション件数の増加なしに r を小さくする (例えば LRA オペレータの身元確認業務にかかる 1 件あたりの作業時間 (Cu,LRA) を短縮する)
- トランザクション件数 p を，$\Delta n * C_{u,RRA} * r / C_{k,RRA} < \Delta p$ を満たすまで増やす

RRA 方式がコスト優位性になる唯一の方法は，$C_{k,RRA}$ を小さくすることである．

本節で本モデルを用いた既存サービスの分析により，身元確認のもっともコスト効率的な方法を定量的にために利用できることを示した．

本モデルは，入力として運用規模のパラメータ n と p を用いることで，RRA と LRA の身元確認のコストの損益分岐点の分析を可能とする．つまり，RRA のアクセスコスト $C_{k,RRA}$ や，あるいは新しくシステム設計にあたりにどちらの RA 配備方式が最適かを決定するためのトランザクション数または LRA のオペレータ数を計算することができる．

5.5 関連研究

谷本らは，予測と実測を通じて PKI の人件費を定量的に分析し，支配的な因子は運用コストであることを明らかにした [64, 63]．彼らの予測は，WBS(work breakdown structure) にもとづくワークパッケージの人時の積算によって計算され，実測はプロトタイプ PKI の運用における作業時間から算出された．実測結果から，身元確認のための証明書発行申請および失効申請業務が高い作業時間比を示した．しかしながら，彼らは RA 方式を選択するためのモデルは開発しなかった．

Argyroudis らは，参加するエンティティ間の経済価値の交換を試すための価値モデルで PKI の分析を行い，既存の侵害リスクを理解するためにリスクベースセキュリティ評価を行った [30]．彼らの分析は，PKI のセキュリティは身元確認に依存しており，その運用コストは身元確認ポリシーが厳しいほど増えることを示した．本モデルは，その身元確認コストの増加に対する改善が期待できる．

Platis らは，PKI ベースの金融取引の運用コストの評価のための確率モデルを研究した [55]．しかしながら，彼らの運用コスト分析は，検証プロセスにおける失効確認のみにフォーカスしていた．

これらの研究は，運用コストも含め PKI のコスト構造にフォーカスした研究である．しかし運用規模に応じた計算可能なモデルは開発されなかった．規模に応じてパラメータ化されたコスト計算可能なモデルを開発する既存研究は見当たらない．

PKI や ID 管理システムのコストにフォーカスしたいくつかの研究がある．しかしそれらのフォーカスは失効 [54]，信頼関係 [45]，認証方式やプロトコルの選択 [32, 36] であり，身元確認ではなかった．

5.6　今後の展望

本研究は，主にサーバ証明書を発行する認証局の身元確認コストを題材として調査研究を行ってきたが，図 5.5 で示したコスト構造モデルは住基カードにも適用可能であることを示した．これはつまり，身元確認が認証局に限らず ID 管理 (とその中での身元確認) を必要とする様々なシステムにおける基本的な要素であり，本章で示した提案モデルが身元確認を必要とする様々なシステムに広く応用可能なモデルであると言える．住基カードを適用事例として取り上げたのは，発行枚数が多くまた全国に広く展開して運用する必要がある大規模な ID 管理基盤だからである．今般法案が可決されまもなく本格的に導入されることになるマイナンバーも同様であり，本節ではマイナンバーへの適用可能性について考察する．

マイナンバーは，国民約 1.3 億人を対象に個人番号を発行する制度であり，希望する申請者には個人番号カードの形で交付される．個人番号交付時の身元確認窓口には，今のところ住基カード同様全国約 1,750 の市町村が想定されている[1]．個人番号は更新されず不変だが，やむを得ない事情が生じた際などには変更して再交付される可能性もある．個人番号コードの有効期間は 10 年 (ただし未成年に限り 5 年) とされている．

本章で示した提案モデルは LRA 員数 n と身元確認の件数 p をパラメータとする．LRA の員数は窓口の数に比例するものとしてここではひとまず $n = 1,749$ とみなす．身元確認の件数 p はマイナンバーの発行対象である総人口約 1.3 億人に加えて一定の再発行が発生するが，実際には初年度に全国民に発行した後は，毎年の人口増減分と国民側都合による再発行などだけにとどまると予想される．これは現状予想根拠がないため，任意の数字を仮置きで当てはめる必要がある．

本章での議論から定性的に明らかな点として，n は少ない方がコスト合理的であるが，逆に n をどこまで増やしてもコスト合理性を確保できるのか，ということが提案モデルを使えば試算することが可能である．例えば，市町村単位の LRA からさらに拠点数を増やして，より地域に密着した LRA 運用を検討することができる．例えば小中学校や公民館など行政窓口以外の公的施設で LRA を運用してもコストメリットが得られるのであれば，従来行政窓口ではできなかった，より多様な属性情報の身元確認を低コストに実現することも可能である．小中学校であればクラスやクラブ活動といった属性情報が容易に確認できるなど，新たな活用事例が出てくるかも知れない．あるいは，拠点数を固定して，再発行件数がどの程度であればコスト合理性を確保できるのか，という試算も可能である．

このように，本提案モデルによって，マイナンバーひとつとっても今までになかった様々なシミュレーションがコスト合理性と併せて検討可能になる．

5.7　本章のまとめ

本章では，身元確認のシステム運用のための基礎的なコスト構造モデルを提案し，いくつかの異なる因子をパラメータ化することによって，従来方式の RA のためのコスト評価モデ

[1] 今後変更の可能性もあるとのこと

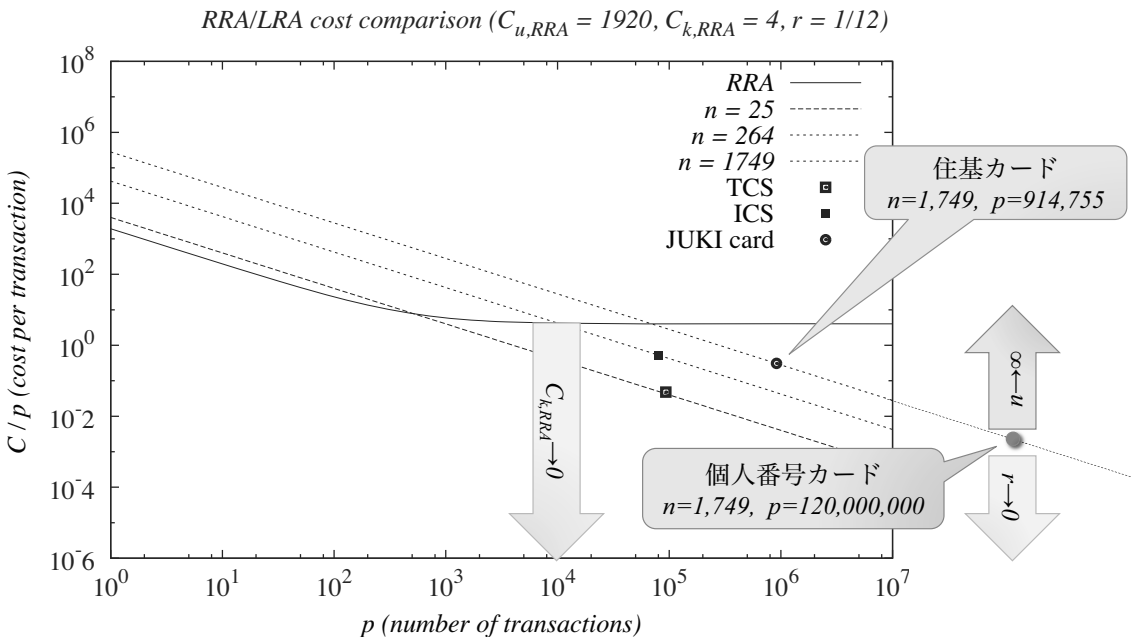


図 5.6: マイナンバーへの提案モデルの適用

ルを開発した．そして，シミュレーションにおいて評価モデルの有効性を示し，実社会の大規模 PKI に対して，モデルの適用可能性を分析した．本モデルは PKI に限らず他の ID 管理システムにも適用可能である．本モデルの主な用途は，RA の配備方式を選択するための，システムのコストパフォーマンスを最適化するツールと，既存システムの定量的な評価比較方法である．

今後の展開としては 2 種類の方向性がある．ひとつは水平方向のアプローチで，マイナンバーのような他の大規模な ID 管理システムへの適用によって，本モデルの高い適用可能性を検証する．もうひとつは垂直方向のアプローチで，本モデルの詳細を改善するための，実際のシステムを表現するより多くのパラメータの導入である．

第6章　結論

本章では，今後のサイバーフィジカル融合社会において一層その重要性が増すであろうアイデンティティ管理の運用コストに関する課題について改めて概観した上で，それに対する本研究の寄与について述べる．最後に本研究の成果を概観してまとめとする．

6.1　今後のアイデンティティ管理におけるコスト問題

実社会におけるエンティティとアイデンティティ情報を紐付ける作業は，行政の担うところが大きかった．これは，行政サービスを保障するために不可欠だからであるが，情報空間，特に実社会とは必ずしも連動しない仮想社会に対しては，行政がそのアイデンティティ情報を担保する必然性がない．情報社会においては，行政に依存しない自律的なアイデンティティ管理が必要であり，また行政のように一元的なアイデンティティ管理をするインセンティブを持つ組織がない以上は，様々な組織による協調型のアイデンティティ管理が重要になってくる．つまり，情報社会においては複数の組織が相互のアイデンティティ管理に依存しあう形になってくるとも考えられ，そこには保証レベルという概念が極めて重要になってくる．また，個々の組織においてアイデンティティ管理を行わなければならない以上は，それを継続していく上での運用コストの問題は無視できない．

アイデンティティ管理や認証基盤の導入を促進させるためのリスク分析や ROI (Return of Investment) 分析についてはいくつか調査研究があるものの，それを継続させるための工夫としてコスト改善の方法に関して，先行研究として一般に知られているものは存在しない．しかし，アイデンティティ管理や認証基盤といった要素は導入すればそれで解決という技術ソリューションではなく，運用管理ソリューションであり，そこには継続のための運用コストが必ず発生する．

従来のアイデンティティ管理は，構成員や顧客情報の管理という自組織のためのソリューションであったが，今後フェデレーションの普及が進む中でのアイデンティティ管理においては，第三者のために一定の保証レベルを担保する必要が生じてくる．担保する上で一定のコストがかかる以上は，そこにはインセンティブの確保も必要であるが，同時に多くの組織ではやはり継続のための資金獲得とコスト削減という努力が欠かせない．

本研究は，こうした問題に寄与する２つのアプローチを行った．ひとつは，行政に依存せず自律的なアイデンティティ管理を行う上で不可欠な，コスト合理的な身元確認スキームの設計手法の提案である．既存の身元確認スキーム設計手法はその多くがリスク指向であり，コスト合理性を充分に議論したものとは言い難かった．提案は，一方的なコスト合理性では

なく保証レベルを保ちつつコスト合理性を実現可能にする設計手法であり，既存の手法と直交するものではなく，相互に補完しながらの利用が可能である．

もうひとつは，フェデレーションを前提としたアイデンティティ管理を継続する上で必要なコスト改善のためのコスト評価モデルの確立である．既存のコスト分析やコスト評価は，その多くがアイデンティティ管理や認証基盤をソリューションとして捉え，その導入前後での効果を測定するためのものであったり，あるいは定量的に評価容易な部分に着目したものであった．これは，身元確認というプロセスが技術でもなく，また運用管理としてもこれまでに知見が少なかったために分析しにくかったという事情もあると思われる．提案は，アイデンティティ管理の規模とコストを軸としたコスト評価モデルである．コスト削減のためには，どの程度の規模に拡大することでコストメリットが得られるか，現状の規模でコストメリットを出すには身元確認をどの程度のコストに抑えればよいかといった改善・検討に有効である．

6.2 本研究のまとめ

ID 発行において身元確認はコストインパクトが大きく，特に身元確認を厳密にするほどコストは増える．ID 発行の役割は SP から独立して一部の IdP に収束していくものと期待されるが，依然 ID 発行を分離せずに自前で行っている SP は多いし，リスク面でもサイバー・フィジカル融合は進むと考えられており，高い保証レベルの身元確認を低コストに実現することは喫緊の課題と言える．

身元確認を簡易にすればコストインパクトを減らせることは定性的に明らかだが，身元確認を簡易にすることなくコストを減らすことが難しい，即ち保証レベルに依らないコスト評価モデルが不在という課題があった．

この課題に対して，マイナンバーに強く期待するところは大きいが，マイナンバーが扱う属性情報や活用範囲は限定的であることから，必ずしも汎用的な解決策になるものではない．また，マイナンバーそのものも身元確認を必要とする認証基盤のひとつであり，その運用モデルがコスト合理的かどうかを適切に評価できる必要があるはずである．

本研究では，この課題を解決するために，商用認証局のサーバ証明書発行における身元確認スキームを題材として調査分析を行い，身元確認にかかるコスト構造の分析と，コスト合理的な身元確認スキームの設計手法を検討し，最終的に保証レベルに依らないコスト構造の定量的評価モデルを確立した．4 章では，サーバ証明書を事例として，運用コストを合理化しつつ保証レベルを確保する身元確認スキームの設計手法について検討を行った．商用認証局におけるサーバ証明書発行の際の身元確認スキームを調査し，身元確認のコスト因子を明らかにした．これらのコスト因子をもとに身元確認スキームの設計手法の検討を行い，国立情報学研究所の UPKI サーバ証明書プロジェクトにおいて設計手法の実装・評価を行った．この身元確認スキームにより同プロジェクトでは年間 1.8 億円の費用削減効果を得て，平成 27 年度からの事業化が確定するなど本研究が実用化に大きく寄与したと言ってよい．5 章では，4 章で明らかになったコスト因子のうち，保証レベルに影響しないコスト因子のみを用

いて，身元確認のコスト構造を定量的評価モデルを提案した．これによって，保証レベルを変更せずに身元確認のコスト評価を行うことが可能となる．このコスト構造モデルを実際にいくつかの事例に当てはめることでモデルの妥当性を実証評価した．さらにこのコスト構造モデルの応用例として，今後活用と普及が大きく期待されているマイナンバーのコスト評価について考察可能性を示し，本研究が身元確認を必要とする様々なシステムに広く適用可能なモデルであることを示した．

謝辞

本研究活動を行うにあたり，多くの方々のご指導とご協力を賜りました．ここにお世話になった方々への感謝の意を表します．

まず，本研究の発端となる，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」(以下 UPKI プロジェクト) において研究活動の機会を与えていただき，総合研究大学院大学入学後も主任指導教員として熱心かつ寛容にご指導いただいた国立情報学研究所 曽根原 登教授に深く心より感謝申し上げます．特に入学後に思うような時間を確保できず十分なご指導を仰ぐことなく不十分な研究成果を示し続けてきたにも関わらず，常に包容力を持って，かつここぞというところでは鋭いご指導をいただきながら，学生生活を見守っていただきました．本当に感謝の念に堪えません．また，学会活動などでもしばしばご指導いただき，入学後も指導教員として学位取得に向けて常に気をかけていただきました国立情報学研究所 越前功教授にも心より感謝申し上げます．UPKI プロジェクトと切っても切れない関係にあった，文部科学省の推進する「最先端・高性能汎用スーパーコンピュータの開発利用プロジェクト」(NAREGI プロジェクト) をはじめグリッド PKI の立場から様々なアドバイスをいただきました，指導教員の国立情報学研究所 合田 憲人 教授にも心より感謝申し上げます．総合研究大学院大学における学生生活を通じて，また指導教員として様々なアドバイスをいただきました国立情報学研究所の山田 茂樹 教授，また途中まで指導教員としてご指導いただきました同研究所 計 宇生教授に心より感謝申し上げます．外部指導教員としてご指導いただいた東京大学 佐藤 周行 准教授には，やはり UPKI プロジェクトから常に真正面から議論に応じていただき，その後の学認や研究活動においても的確なアドバイスをいただきました．改めて心より感謝申し上げます．

UPKI プロジェクトへの参加および本学への入学も快くご許可いただきましたセコム IS 研究所の小松崎常夫所長，また入社以来つかず離れず上司として，技術者としてまた研究者として忍耐強く自由な研究活動をさせていただいた松本泰ディビジョンマネージャー，もっとも苦しい時期に沈黙と愛情を持って見守り続けていただいた伊達浩行グループリーダーをはじめ，同僚の先輩後輩社員の方々にはご迷惑をおかけするとともに，研究活動やリフレッシュなどにおいてしばしば助けていただきましたことを御礼申し上げます．

UPKI プロジェクトにおいて，曽根原教授とともに業務・研究両面で常に思慮深く丁寧かつ的確なご指導をいただきました京都大学の岡部寿男教授には，特に深く感謝申し上げます．同プロジェクトにおいて成果を残すにあたって，論文執筆や学会発表など様々なまた過分なほどの機会をいただき，研究業績を積み上げるためのご支援をいただきましたとともに，初めての本格的な論文執筆にあたって，論文のいろはから懇切丁寧にご指導いただきま

したことを改めて御礼申し上げます．

UPKI プロジェクトにおいて，同じ国立情報学研究所のメンバーとしてともに行動し，事業・研究など多岐に渡りご指導ご鞭撻いただいた高度情報科学技術研究機構の峯尾真一殿，千葉工業大学の谷本茂明教授，日本電気株式会社の片岡俊幸様，国立情報学研究所の中村素典特任教授，山地一禎准教授，岡田仁志准教授，西村健特任研究員，また旭川医科大学図書館に転任された樋口秀樹課長をはじめとしてプロジェクトの運用や研究活動など様々な後方支援をしていただいた国立情報学研究所の皆様方，そしてプロジェクトにご参画いただいた各大学の皆様にも深く御礼申し上げます．

また，身近に学位を持つ存在として強烈な刺激を受け，経験者として様々な助言と励ましをしてくれた東邦大学の金岡晃講師の存在なくして学位への挑戦は考えられませんでした．バイタリティのある素晴らしいロールモデルを身近に得られたことは，何者にも代え難い経験であり常に心の励みでした．偉大な後輩に，深く，深く感謝致します．そして，論文執筆にあたって悩み事や相談に気軽に応じ叱咤激励していただいた東京電機大学の柿崎淑郎助教，広島大学の大東俊博助教，東京大学の山口利恵特任准教授をはじめ多くの方々に，改めて感謝申し上げます．

最後に，二児の育児と介護と家事を抱えながら学位挑戦を支えてきてくれた最愛の妻と，家に帰ればどんな疲れも吹き飛ばしてくれた最愛の子供たちに心から感謝いたします．

参考文献

[1] Cardspace. http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx.

[2] Certificates evaluation and research project. https://upki-portal.nii.ac.jp/docs/server.

[3] Federationstatus. https://refeds.terena.org/index.php/FederationStatus.

[4] Identity, credential and access management sub committee (icamsc). http://www.idmanagement.gov/drilldown.cfm?action=icam.

[5] Incommon certificate service. https://www.incommon.org/certificates/.

[6] ISO/IEC 29115 - Information technology – Security techniques – Entity authentication assurance framework. Technical report, ISO/IEC and ITU-T. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138.

[7] Issue status of juki-card (in japanese). http://warp.ndl.go.jp/info:ndljp/pid/258151/www.soumu.go.jp/c-gyousei/daityo/pdf/050217_1.pdf.

[8] National identity management federations. http://www.internet2.edu/pubs/national_federations.pdf.

[9] National identity management federations. http://www.incommonfederation.org/.

[10] Oasis security services (saml) tc. https://www.oasis-open.org/committees/security/.

[11] Open identity solutions for open government. http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV.

[12] Openid foundation. http://openid.net/foundation/.

[13] Shibboleth. https://shibboleth.net/.

[14] Standard on identity and credential assurance. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776&section=text.

[15] Switchaai. http://www.switch.ch/aai/index.html.

[16] Terena certificate service. http://www.terena.org/activities/tcs/.

[17] Terena compendium of national research and education networks in europe. http://www.terena.org/publications/files/TERENA-Compendium-2013.pdf.

[18] The uk access management federation. http:/www.ukfederation.org.uk/.

[19] Upki オープンドメイン証明書自動発行検証プロジェクト. https://upki-portal.nii.ac.jp/docs/odcert.

[20] Web services federation language. http://www.ibm.com/developerworks/library/specification/ws-fed/.

[21] Yadis. http://yadis.org/wiki/Main_Page.

[22] 「id 連携トラストフレームワーク」の構築のための実証事業. http://www.meti.go.jp/policy/it_policy/id_renkei/.

[23] サーバ証明書の発行・導入における啓発・評価研究プロジェクト. https://upki-portal.nii.ac.jp/docs/server.

[24] 次期証明書発行サービスの全貌. http://id.nii.ac.jp/1125/00000067.

[25] 住基カード 市区町村交付窓口一覧. http://juki-card.com/madoguchi/.

[26] Ngn identity management framework. series y: Global information infrastructure, internet protocol aspects and next-generation networks, next generation networks — security. recommendation ITU-t y.2720. Technical report, 2009. http://www.itu.int/rec/T-REC-Y.2720/en.

[27] Endentity authentication assurance framework. series x: Data networks, open system communications and security, cyberspace security — identity management. recommendation ITU-t x.1254. Technical report, 2012. http://www.itu.int/rec/T-REC-X.1254/en.

[28] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee. The identity crisis. security, privacy and usability issues in identity management. *arXiv preprint arXiv:1101.0427*, 2011.

[29] Inc. (AICPA) American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (CICA). Webtrust program for certification authorities. Technical report, American Institute of Certified Public Accountants, Inc. (AICPA) and Canadian Institute of Chartered Accountants (CICA), 2000.

[30] Patroklos Argyroudis, Robert McAdoo, DonalO ' Mahony. Comparing the costs of public key authentication infrastructures. In *Proceedings of the 1st Workshop on the Economics of Securing the Information Infrastructure (WESII'06)*, 2006.

[31] Identity Assurance and Trust Working Group. Pan-canadian assurance model. `http://www.iccs-isac.org/en/km/transformative/docs/Pan-Canadian%20Assurance%20Model.PDF`.

[32] Kheira Bekara, Yosra Ben Mustapha, Samia Bouzefrane, Khaled Garri, Maryline Laurent, and Pascal Thoniel. Ensuring low cost authentication with privacy preservation in federated ims environments. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, pp. 1–5. IEEE, 2011.

[33] Elisa Bertino and Kenji Takahashi. *Identity Management: Concepts, Technologies, and Systems*. Artech House, 2011.

[34] Nicholas Bohm and Stephen Mason. Identity and its verification. *Computer Law & Security Review*, Vol. 26, No. 1, pp. 43–51, 2010.

[35] Joshua B Bolton. E-authentication guidance for federal agencies. *Office of Management and Budget,(December 16, 2003).*, 2003. `http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf`.

[36] Samia Bouzefrane, Khaled Garri, and Pascal Thoniel. A user-centric pki based-protocol to manage fc 2 digital identities. *International Journal of Computer Science Issues (IJCSI)*, Vol. 8, No. 1, 2011.

[37] Derek Brink. Pki and financial return on investment. White Paper, PKI Forum ' s Business Working Group, 2002.

[38] Scott Cantor, John Kemp, Rob Philpott, and Eve Maler. Assertions and protocols for the oasis security assertion markup language. *OASIS Standard (March 2005)*, 2005. `http://docs.oasis-open.org/security/saml/v2.0/`.

[39] State Services Commission. *Guide to Authentication Standards for Online Services*. `http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/guide-authentication-standards-online-services/`.

[40] T Dierks and E Rescorla. Rfc 5246: The transport layer security (tls) protocol. *The Internet Engineering Task Force*, 2008.

[41] CA/Browser Forum. Frequently asked questions - extended validation ssl. `http://www.cabforum.org/faq.html`.

[42] CA/Browser Forum, editor. *Guidelines For The Issuance And Management Of Extended Validation Certificates.*

[43] NIST Electronic Authentication Guideline. *NIST Special Publication 800-63-2.* NIST, 2013.

[44] CHII HSU and Yu-Ching Tung. The effect of pki benefits on competitive advantage. In *Proceedings of the 8th conference on Applied informatics and communications*, pp. 291–296. World Scientific and Engineering Academy and Society (WSEAS), 2008.

[45] Jingwei Huang and David Nicol. A calculus of trust and its application to pki and identity management. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, pp. 23–37. ACM, 2009.

[46] Toshiyuki Kataoka, Takeshi Nishimura, Masaki Shimaoka, Kazutsuna Yamaji, Motonori Nakamura, Noboru Sonehara, and Yasuo Okabe. Leveraging pki in saml 2.0 federation for enhanced discovery service. In *Applications and the Internet, 2009. SAINT'09. Ninth Annual International Symposium on*, pp. 239–242. IEEE, 2009.

[47] John Kemp, Scott Cantor, Prateek Mishra, Rob Philpott, and Eve Maler. *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2. 0. OASIS Standard, 15.03. 2005.*

[48] KPMG ビジネスアシュアランス株式会社. 情報セキュリティ監査制度：管理態勢の構築と監査の実施.

[49] Eve Maler, Anthony Nadalin, Drummond Reed, Mary Rundle, and Don Thibeau. The open identity trust framework (oitf) model. `http://blogs.technet.com/b/identity/archive/2010/03/03/open-identity-trust-framework-model-whitepaper.aspx`.

[50] G Malkin. Rfc1983: Internet users ' glossary. Technical report, RFC Editor, USA, 1986.

[51] Charles Chas R Merrill. Internet x. 509 public key infrastructure certificate policy and certification practices framework. 2003.

[52] Microsoft. Microsoft root certificate program, 2009. `http://technet.microsoft.com/en-us/library/cc751157.aspx`.

[53] Department of Internal Affairs. *Evidence of Identity Standard 2.0.* `http://www.dia.govt.nz/EOI/EOIv2Foreword&Contents.html`.

[54] Mona H Ofigsbø, Stig Frode Mjølsnes, Poul Heegaard, and Leif Nilsen. Reducing the cost of certificate revocation: a case study. In *Public Key Infrastructures, Services and Applications*, pp. 51–66. Springer, 2010.

[55] Agapios Platis, Costas Lambrinoudakis, and Assimakis Leros. A probabilistic model for evaluating the operational cost of pki-based financial transactions. In *Public Key Infrastructure*, pp. 149–159. Springer, 2004.

[56] Jon Postel. Domain name system structure and delegation. 1994.

[57] N. Sakimura and et al. Openid connect core 1.0. `http://openid.net/specs/openid-connect-core-1_0.html`.

[58] Klaus Schmeh. *Cryptography and public key infrastructure on the Internet*. John Wiley & Sons, 2006.

[59] Tanimoto Shigeaki, Yokoi Masahiko, Sato Hiroyuki, and Kanai Atsushi. Quantifying cost structure of campus pki based on estimation and actual measurement. 情報処理学会論文誌, Vol. 53, No. 5, 2012.

[60] Masaki Shimaoka, Nelson Hastings, and Rebecca Nielsen. Memorandum for multi-domain public key infrastructure interoperability. 2008.

[61] Masaki SHIMAOKA and Noboru SONEHARA. Modeling the cost structure of identity proofing. In IEEE, editor, *Proceedings of the 8th IEEE International Workshop on Middleware Architecture in the Internet, at Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th Annual*.

[62] Peter Steiner. On the internet, nobody knows you ' re a dog. *The New Yorker*, Vol. 69, No. 20, p. 61, 1993.

[63] Shigeaki Tanimoto, Masahiko Yokoi, Hiroyuki Sato, and Atsushi Kanai. Quantifying cost structure of campus pki. In *Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on*, pp. 315–320. IEEE, 2011.

[64] Shigeaki Tanimoto, Masahiko Yokoi, Hiroyuki Sato, and Atsushi Kanai. Quantifying cost structure of campus pki based on estimation and actual measurement. *Information and Media Technologies*, Vol. 7, No. 3, pp. 1274–1282, 2012.

[65] Stephen Wilson. Guidelines on how to determine return on investment in pki. *OASIS PKI Education Sub-committee*, Vol. 1, , 2005.

[66] Mykyta Yevstifeyev. Whois protocol specification. 2011.

[67] アイデンティティ管理技術解説制作委員会. アイデンティティ管理技術解説. 情報処理推進機構.

[68] 山地一禎, 片岡俊幸, 中村素典, 曽根原登. シボレスシステムを用いた属性連携基盤の開発. 情報処理学会研究報告. 情報学基礎研究会報告, Vol. 2009, No. 10, pp. 1–8, nov 2009. `http://ci.nii.ac.jp/naid/110008003390/`.

[69] 稲村雄. 認証技術: パスワートから公開鍵まで. 株式会社 オーム社, 2003.

[70] 伊東栄典. 九州大学全学共通認証基盤と全学共通 id「sso-kid」の紹介. 情報統括本部 IT マガジン, Vol. 1, No. 2, pp. 42–48, jul 2007. http://ci.nii.ac.jp/naid/120001748995/.

[71] 伊東栄典, 片岡真, 牧瀬ゆかり. Shibboleth 認証基盤構築と学術認証フェデレーションへの参加–今後の e リソースサービス基盤にむけて. 九州大学附属図書館研究開発室年報, Vol. 2009, pp. 11–15, 2009. http://ci.nii.ac.jp/naid/120002405297/.

[72] 各府省情報化統括責任者（CIO）連絡会議. オンライン手続におけるリスク評価及び電子署名・認証ガイドライン. 内閣官房, 2010 年 8 月. http://www.kantei.go.jp/jp/singi/it2/guide/index.html.

[73] 宮本貴朗, 西本隆, 金森剛志, 山本貴史, 上田博文. 組織内認証基盤の構築 : 大阪府立大学における認証基盤の構築事例. 情報処理, Vol. 49, No. 4, pp. 435–444, apr 2008. http://ci.nii.ac.jp/naid/110006652970/.

[74] 西村健, 島岡政基, 中村素典, 曽根原登, 岡部寿男. Upki 証明書自動発行検証プロジェクトのシステム移行における課題と対策 (認証技術, インターネットと情報倫理教育, 一般). 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ, Vol. 109, No. 438, pp. 225–228, feb 2010. http://ci.nii.ac.jp/naid/110007863140/.

[75] 西村健, 中村素典, 山地一禎, 佐藤周行, 大谷誠, 岡部寿男, 曽根原登. 多様なポリシーを反映可能な認証フェデレーション機構の実現 (ネットワーク応用,< 特集 > インターネット技術とその応用論文). 電子情報通信学会論文誌. D, 情報・システム, Vol. 96, No. 6, pp. 1400–1412, jun 2013. http://ci.nii.ac.jp/naid/110009611652/.

[76] 古村隆明, 永井靖浩. 京都大学の認証基盤構築の現状と今後.

[77] 金岡晃, 島岡政基, 岡本栄司. Id ベース暗号の信頼構築フレームワーク. 情報処理学会論文誌, Vol. 51, No. 9, pp. 1692–1701, sep 2010. http://ci.nii.ac.jp/naid/110007970771/.

[78] 高木浩光. Pki よくある勘違い (1)「オレオレ証明書でも ssl は正常に機能する」, 2005. http://takagi-hiromitsu.jp/diary/20050123.html.

[79] 飯田勝吉. キャンパス共通認証・認可システムが拓く高度な研究・教育のための情報通信基盤 (インターネット及び一般). 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ, Vol. 106, No. 309, pp. 13–18, oct 2006. http://ci.nii.ac.jp/naid/110004850937/.

[80] 飯田勝吉, 新里卓史, 伊東利哉, 渡辺治. キャンパス共通認証認可システムの構築と運用 (< 特集 > セキュアでサステイナブルなインターネットアーキテクチャ論文). 電

子情報通信学会論文誌. B, 通信, Vol. 92, No. 10, pp. 1554–1565, oct 2009. http://ci.nii.ac.jp/naid/110007387666/.

[81] 岡村真吾, 寺西裕一, 秋山豊和, 馬場健一, 中野博隆. 大阪大学におけるキャンパス pki の構築 (セッション 2-c:認証 (1)). 情報処理学会研究報告. CSEC, [コンピュータセキュリティ], Vol. 2006, No. 26, pp. 67–72, mar 2006. http://ci.nii.ac.jp/naid/110004683644/.

[82] 島岡政基, 西村健, 中村素典, 曽根原登, 岡部寿男. Upki サーバ証明書プロジェクトにおける証明書自動発行支援システムの開発 (認証技術, インターネットと情報倫理教育, 一般). 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ, Vol. 109, No. 438, pp. 229–234, feb 2010. http://ci.nii.ac.jp/naid/110007863141/.

[83] 島岡政基, 西村健, 古村隆明, 中村素典, 佐藤周行, 岡部寿男, 曽根原登. 学術機関のためのサーバ証明書発行フレームワーク (ネットワーク管理・オペレーション,< 特集 > 若手研究者のためのフロンティア論文). 電子情報通信学会論文誌. B, 通信, Vol. 95, No. 7, pp. 871–882, jul 2012. http://ci.nii.ac.jp/naid/110009470615/.

[84] 島岡政基, 片岡俊幸, 谷本茂明, 西村健, 山地一禎, 中村素典, 曽根原登, 岡部寿男. 大学間連携のための全国共同認証基盤 upki のアーキテクチャ設計 (< 特集 > スマートな社会を支えるインターネットアーキテクチャ論文). 電子情報通信学会論文誌. B, 通信, Vol. 94, No. 10, pp. 1246–1260, oct 2011. http://ci.nii.ac.jp/naid/110008749640/.

[85] 島岡政基, 松本泰. Ssl 証明書の事例に見る暗号アルゴリズムの移行問題：収束しない 2010 年問題. 電子情報通信学会論文誌. B, 通信, Vol. 94, No. 1, pp. 1–13, jan 2011. http://ci.nii.ac.jp/naid/110008006443/.

[86] 島岡政基, 松本泰, 高木浩光. 技術が社会基盤となるとき, 我々は何をすべきか：ウェブにおける pki 応用の例に学ぶ. B-plus：電子情報通信学会通信ソサイエティマガジン, No. 22, pp. 138–147, 2012. http://ci.nii.ac.jp/naid/40019427636/.

[87] 島岡政基, 谷本茂明, 片岡俊幸, 峯尾真一, 曽根原登, 寺西裕一, 飯田勝吉, 岡部寿男. 大学間連携のための全国共同電子認証基盤 upki における認証連携方式の検討 (インターネット及び一般). 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ, Vol. 106, No. 62, pp. 13–18, may 2006. http://ci.nii.ac.jp/naid/110004741033/.

[88] 島岡政基, 谷本茂明, 片岡俊幸, 中村素典, 曽根原登, 岡部寿男. Bs-8-3 upki プロジェクトにおけるオープンドメインサーバ証明書発行・導入 (bs-8. セキュア、スケーラブルでサステイナブルなキャンパス情報システム, シンポジウムセッション). 電子情報通信学会総合大会講演論文集, Vol. 2008, No. 2, pp. S–108–S–109, mar 2008. http://ci.nii.ac.jp/naid/110006871356/.

[89] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明. シングルサインオンに対応したネットワーク利用者認証システムの開発. 情報処理学会論文誌, Vol. 51, No. 3, pp. 1031–1039, mar 2010. http://ci.nii.ac.jp/naid/110007970705/.

[90] 総務省行政評価局. 行政手続等における本人確認に関する調査結果に基づく通知. 総務省行政評価局, 2008. http://ci.nii.ac.jp/ncid/BA88200449.

[91] 大学職員録刊行会, 広潤社編集部. 全国大学職員録. 廣潤社, 1957. http://ci.nii.ac.jp/ncid/BN05702769.

[92] 新里卓史, 飯田勝吉, 岸本幸一, 太刀川博之, 昆野長典, 山崎孝治, 伊東利哉, 渡辺治. 大学内の業務・システムと連携するキャンパス共通認証認可システムの構築と運用. 電子情報通信学会技術研究報告. NS, ネットワークシステム, Vol. 106, No. 577, pp. 201–206, mar 2007. http://ci.nii.ac.jp/naid/110006249119/.

[93] 松平拓也, 笠原禎也, 高田良宏, 東昭孝, 二木恵, 森祥寛. 大学における shibboleth を利用した統合認証基盤の構築. 情報処理学会論文誌, Vol. 52, No. 2, pp. 703–713, feb 2011. http://ci.nii.ac.jp/naid/110008507909/.

[94] 日本情報処理開発協会電子商取引推進センター. 属性情報利用システム. Technical report, 日本情報処理開発協会 電子商取引推進センター and 電子商取引推進協議会, 2004.

[95] 島岡政基, 佐藤周行. 学認における属性交換フレームワーク. コンピュータセキュリティシンポジウム 2013 論文集, 第 2013 巻, pp. 486–493, oct 2013.

[96] 島岡政基, 谷本茂明, 片岡俊幸, 中村素典, 曽根原登, 岡部寿男. Bs-8-3 upki プロジェクトにおけるオープンドメインサーバ証明書発行・導入 (bs-8. セキュア, スケーラブルでサステイナブルなキャンパス情報システム, シンポジウムセッション). 電子情報通信学会総合大会講演論文集, Vol. 2008, No. 2, 2008.

[97] 日本情報経済社会推進協会. 「本人確認をした属性情報を用いた社会基盤に関する調査研究」調査報告書. Technical report, 日本情報経済社会推進協会, 2013.

[98] 秋山豊和, 寺西裕一, 岡村真吾, 坂根栄作, 長谷川剛, 馬場健一, 中野博隆, 下條真司. キャンパス it 認証基盤の構築 : 大阪大学における導入事例と課題 (インターネット技術及び一般 ii). 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ, Vol. 107, No. 74, pp. 47–52, may 2007. http://ci.nii.ac.jp/naid/110006289210/.

[99] 秋山豊和, 寺西裕一, 岡村真吾, 坂根栄作, 長谷川剛, 馬場健一, 中野博隆, 下條真司, 長岡亨. 大阪大学における全学 it 認証基盤の構築. 情報処理学会論文誌, Vol. 49, No. 3, pp. 1249–1264, mar 2008. http://ci.nii.ac.jp/naid/120004898427/.

[100] 谷本茂明, 黒崎悟, 高本剛志, 林和範, 水原真一, 守屋利彦, 横井雅彦, 佐藤周行, 金井敦. キャンパス pki におけるコスト構造に関する研究 (マルチメディア通信, マルチメディアシステム, ライフログ活用技術、ip 放送/映像伝送, 一般). 電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム, Vol. 110, No. 207, pp. 25–30, sep 2010. http://ci.nii.ac.jp/naid/110008106769/.

[101] 谷本茂明, 黒崎悟, 高本剛志, 林和範, 水原真一, 守屋利彦, 横井雅彦, 佐藤周行, 金井敦. D-9-36 キャンパス pki のコスト構造定量化に関する検討 (d-9. ライフインテリジェンスとオフィス情報システム, 一般セッション). 電子情報通信学会総合大会講演論文集, Vol. 2011, No. 1, p. 112, feb 2011. http://ci.nii.ac.jp/naid/110008574196/.

[102] 谷本茂明, 黒崎悟, 高本剛志, 林和範, 水原真一, 守屋利彦, 内田圭介, 横井雅彦. D-9-31 キャンパス pki 構築・普及促進に関する検討 (d-9. ライフインテリジェンスとオフィス情報システム, 一般セッション). 電子情報通信学会総合大会講演論文集, Vol. 2010, No. 1, p. 118, mar 2010. http://ci.nii.ac.jp/naid/110007881208/.

[103] 谷本茂明, 島岡政基, 片岡俊幸, 西村健, 山地一禎, 中村素典, 曽根原登, 岡部寿男. 大学間認証連携のためのキャンパス pki 共通仕様 (研究速報,< 特集 > スマートな社会を支えるインターネットアーキテクチャ論文). 電子情報通信学会論文誌. B, 通信, Vol. 94, No. 10, pp. 1383–1388, oct 2011. http://ci.nii.ac.jp/naid/110008749653/.

[104] 谷本茂明, 島岡政基, 片岡俊幸, 中村素典, 曽根原登, 岡部寿男. Bs-8-2 upki 共通仕様 (アウトソースモデル) の提案 (bs-8. セキュア、スケーラブルでサステイナブルなキャンパス情報システム, シンポジウムセッション). 電子情報通信学会総合大会講演論文集, Vol. 2008, No. 2, pp. S–106 – S–107, mar 2008. http://ci.nii.ac.jp/naid/110006871355/.

[105] 庄司勇木, 山地一禎, 中村素典, 曽根原登. 共通認証基盤構築の意義と学術認証フェデレーションの直面する政策上の課題について (実装評価, 一般, コンテンツ配信, コンテキストアウェアネス,ipv6, 認証,id/名前管理及び一般). 電子情報通信学会技術研究報告. IN, 情報ネットワーク, Vol. 109, No. 362, pp. 35–40, jan 2010. http://ci.nii.ac.jp/naid/110008000288/.

本論文に含まれる発表文献

ジャーナル論文

1. 島岡政基，西村健，古村隆明，中村素典，佐藤周行，岡部寿男，曽根原登,「学術機関のためのサーバ証明書発行フレームワーク」，電子情報通信学会論文誌. B, 通信 J95-B(7) 871-882 2012 年 7 月
2. 島岡政基，片岡俊幸，谷本茂明，西村健，山地一禎，中村素典，曽根原登，岡部寿男,「大学間連携のための全国共同認証基盤 UPKI のアーキテクチャ設計」，電子情報通信学会論文誌. B, 通信 J94-B(10) 1246-1260 2011 年 10 月

査読付き国際会議論文

1. Masaki SHIMAOKA, Noboru SONEHARA,“Modeling the Cost Structure of Identity Proofing”, Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th Annual. IEEE, Jul 2014

その他本論文の内容に関連する発表文献

ジャーナル論文

1. 谷本 茂明，島岡 政基，片岡 俊幸，西村 健，山地 一禎，中村 素典，曽根原 登，岡部 寿男,「大学間認証連携のためのキャンパス PKI 共通仕様」，電子情報通信学会論文誌. B, 通信 J94-B(10) 1383-1388 2011 年 10 月

2. 島岡 政基 , 松本 泰,「SSL 証明書の事例に見る暗号アルゴリズムの移行問題：収束しない 2010 年問題」，電子情報通信学会論文誌. B, 通信 J94-B(1) 1-13 2011 年 1 月

3. 金岡 晃 , 島岡 政基 , 岡本 栄司,「ID ベース暗号の信頼構築フレームワーク」，情報処理学会論文誌 51(9) 1692-1701 2010 年 9 月

査読付き国際会議論文

1. Toshiyuki Kataoka, Takeshi Nishimura, Masaki Shimaoka, Kazutsuna Yamaji, Motonori Nakamura, Noboru Sonehara, Yasuo Okabe,“Leveraging PKI in SAML2.0 Federation for Enhanced Discovery Service”, 2009 Ninth Annual International Symposium on Applications and the Internet, 239-242, Jul 2009

国際標準

1. M. Shimaoka, N. Hastings, R. Nielsen, “Memorandum for Multi-Domain Public Key Infrastructure Interoperability”, Internet Engineering Task Force, RFC 5217, Jul 2008

書籍

1. 情報処理推進機構,「アイデンティティ管理技術解説」，アイデンティティ管理技術解説制作委員会，情報処理推進機構，2013 年 3 月

研究会等

1. 島岡政基，佐藤周行,「学認における属性交換フレームワーク」，2B3-2，コンピュータセキュリティシンポジウム 2013 論文集, 2013(4),486-493 2013 年 10 月

2. 西村健，島岡政基，中村素典，曽根原登，岡部寿男,「UPKI 証明書自動発行検証プロジェクトのシステム移行における課題と対策」，信学技報 109(438) 225-228 2010 年 2 月

3. 島岡政基，西村健，中村素典，曽根原登，岡部寿男,「UPKI サーバ証明書プロジェクトにおける証明書自動発行支援システムの開発」，信学技報 109(438) 229-234 2010 年 2 月

4. 島岡政基，谷本茂明，片岡俊幸，中村素典，曽根原登，岡部寿男,「UPKI プロジェクトにおけるオープンドメインサーバ証明書発行・導入」，2008 信学総大，通信 (2) S-108-S-109 2008 年 3 月

5. 谷本茂明，島岡政基，片岡俊幸，中村素典，曽根原登，岡部寿男,「UPKI 共通仕様 (アウトソースモデル) の提案」，2008 信学総大，通信 (2) S-106-S-107 2008 年 3 月

6. 島岡政基，谷本茂明，片岡俊幸，峯尾真一，曽根原登，寺西裕一，飯田勝吉，岡部寿男,「大学間連携のための全国共同電子認証基盤 UPKI における認証連携方式の検討」，信学技報 106(62) 13-18 2006 年 5 月