所属先情報の分散秘匿型資格確認サービスの提案

安細 康介　　渡辺 夏樹

株式会社 日立製作所 研究開発本部
244-0817 横浜市戸塚区吉田町 292

{kosuke.anzai.jd, natsuki.watanabe.ch}@hitachi.com

あらまし 医療保険等の社会保障分野における番号制度活用に向け，情報保有機関（自治体，医療保険者，保険医療機関等）が各個人の資格情報（所属先情報および個人属性情報）を取得可能とする資格確認サービスが必要とされている．ここで，特に社会保障分野では所属先情報が機微な個人情報となり得るため，本来は情報管理元以外には秘匿しておくべきであるが，所属先情報を資格確認サービス提供機関が一括管理することで本サービスを実現する従来方式ではプライバシー上の課題がある．本課題を解決するため，ランダムに設定したルート情報を複数機関で分散秘匿し，情報管理元以外には所属先情報を秘匿したまま資格確認サービスを実現する方式を提案する．

Proposal for the concealed distributed service verifying affiliation information

Kousuke Anzai　　Natsuki Watanabe

Hitachi, Ltd. Research & Development Group
292 Yoshida-cho, Totsuka-ku, Yokohama 244-0817, JAPAN

{kosuke.anzai.jd, natsuki.watanabe.ch}@hitachi.com

Abstract To utilize the Social Security and Tax Number System in fields such as medical insurance, a verification service that allows information holding organizations (e.g. local governments, health insurers and medical organizations) to acquire individuals' qualification (affiliation information and personal attribute information) is needed. The affiliation information could especially be sensitive personal information in a social security field. Since it should be confidential to other organizations, there is a privacy problem in the conventional method in which a single verification service collectively manages all affiliation information. To solve this problem, we propose the method in which organizations distributedly share concealed random route information for the verification service while the affiliation information is kept confidential.

1　はじめに

日本政府は，国民生活の安心確保や負担の公平性実現を目的として「社会保障・税一体改革」[1]を進めており，2011 年 6 月の「社会保障・税番号大綱」閣議決定を経て，2013 年 5 月には「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号法）」[2]が成立した．

番号法に基づく番号制度は，全国民に一意な個人番号を付番した上で住基カードに代わる個人番号カードを配布し，「情報保有機関」と呼ばれる省庁，地方公共団体，および医療保険者等がそれらを活用して，新たな国民サービスの拡充や各機関間の情報連携による業務効率化を実現していための制度である．現在は，番号制度に則ったシステム構築が進められると共に，将来的な番号利活用の検討も進められている．

2014 年 12 月には，厚生労働省の「医療等分野における番号制度の活用等に関する研究会」中間まとめ[3]において，番号利活用の一つのユースケースとして，医療保険のオンライン資格確認の早期導入が示されたところである．医療保険のオンライン資格確認とは，保健医療機関の窓口において，患者の医療保険資格を番号制度のインフラを活用することで効率的・一意的に確認可能とするサービスである．

情報連携の際，情報照会元の情報保有機関は情報照会対象の個人の情報を持つ情報保有機関を情報照会先として指定する必要があるが，住基ネットにより個人の住所情報を参照することで情報照会先を特定することが出来る地方公共団体間の情報連携に対し，医療保険者（社会保障分野の医療保険を管理している情報保有機関）に対する情報連携では，情報照会対象の個人がどの医療保険者に加入・所属しているのかを解決することが現状できない．このため，医療保険者等の社会保障分野における情報照会先の所属先の解決し，個人の保険資格情報を取得可能とする仕組み（以下，「資格確認サービス」と呼ぶ）が必要となると想定されている．

社会保障分野の資格確認サービスを実現する上では，各個人がどの医療保険者に属しているかという情報（所属先情報）そのものが個人情報もしくは個人情報と同等の秘匿性が求められる情報であることを考慮しなければならない．例えば，各個人がどの医療保険に加入しているかという所属先情報により，医療保険者の名称等から，市町村国保では住所地の市町村，健康保険組合では勤務先の名称，職種等の個人情報を推測することが可能である．上記の観点から，資格確認サービスを構築する際には，各個人の所属先情報をいかに安全かつ秘匿性を高めた形で管理・運用するかということが課題となる．

本報告では，上記課題に対応した資格確認サービスを実現する方式として，ランダムに設定したルート情報を複数機関で分散秘匿し，情報管理元以外には所属先情報を秘匿したまま，情報照会元の情報保有機関に対し情報照会先を特定可能とする方式を提案し，その内容について報告する．

2　資格確認サービスの課題

2.1 資格確認サービスの概要

「医療等分野における番号制度の活用等に関する研究会」中間まとめ[3]で示されたサービスイメージを参考に，オンライン資格確認のシステム構成概要を図 2-1に示し，各構成要素の概要について以下に述べる．

オンライン資格確認では，保険医療機関等からの求めに応じて，情報照会対象の個人の情報がどの医療保険者に存在しているかをシステム的に解決し，資格情報として応答する．

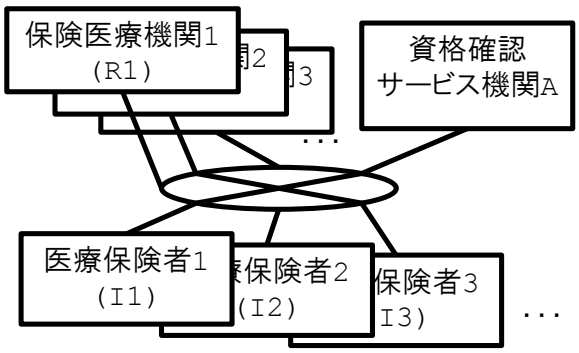

図 2-1 オンライン資格確認のシステム構成概要

(1) 資格確認サービス機関

加入者がどの医療保険者に加入・所属しているかを特定するために必要な情報を登録しておき，保険医療機関からの問い合わせに応じて提供する．

(2) 医療保険者（情報保有機関）

医療保険者毎に自機関に加入している加入者の情報を管理し，新規登録時および加入者の異動時には，資格確認サービス機関に対して，情報の登録・更新を行う．

(3) 保険医療機関（サービス利用者）

患者（加入者）の資格情報を，資格確認サービス機関に問い合わせる．

2.2 従来方式の課題

資格確認サービスを実現する従来方式として，アイデンティティ Web サービスフレームワーク（ID-WSF）におけるディスカバリサービス（DS）の仕組みを唯一の資格確認サービス機関に持つ方式が考えられる[4][5]．これは，資格確認サービスにて，個人を特定する情報と所属先の情報保有機関を特定する情報とを対応付けて，所属先情報として一括管理する方式である．各情報保有機関が資格確認サービスに対し所属先情報を登録しておくことで，情報照会元サービス利用者は情報照会対象の各個人の資格情報を資格確認サービスに問い合わせることで入手可能となる．

以下，従来方式の資格情報登録フロー及び特定フローの概要について述べる．

(1) 資格情報登録フロー（図 2-2）

各情報保有機関は，資格確認サービスに，個人を特定する情報（ユーザ ID）と所属先の情報保有機関を特定する情報（情報保有機関 ID）をセットとして登録する（a-1）．

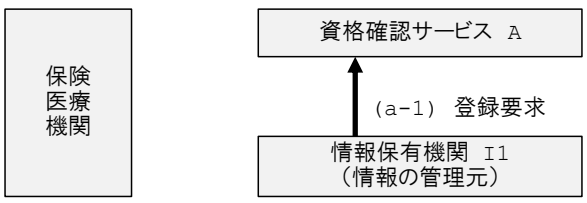

図 2-2 資格情報登録フロー（従来）

(2) 資格情報特定フロー（図 2-3）

情報照会元の保険医療機関は，個人を特定する情報（ユーザ ID）をキーに資格要求（b-1）をし，資格確認サービスから所属先の情報保有機関を特定する情報（情報保有機関 ID）を検索することで情報の管理元を特定し（b-2），該当機関から資格情報を取得する（b-3）．

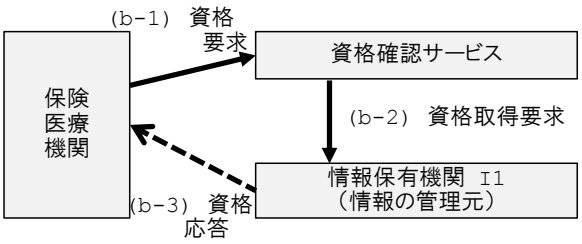

図 2-3 資格情報特定フロー（従来）

ここで，資格確認サービスを実現する上で，各個人がどの医療保険者に属しているかという情報（所属先情報）そのものが個人情報もしくは個人情報と同等の秘匿性が求められる情報であることを考慮しなければならない．従来方式では，各個人の情報の管理元である情報保有機関以外に本来知られるべきではない資格情報を，管理元とは責任範囲の異なる他の機関である資格確認サービスが管理していること自体がセキュリティリスクとなる．情報を暗号化等することで，資格情報をある程度安全に管理・運用することは可能であるものの，システム運用管理者等の内部不正者からの攻撃による情報漏えいまでを防ぐことは非常に困難である．

また，資格確認サービスのシステムに直接アクセスしなくとも，登録する通信の盗聴を行うことで登録元の機関が特定可能であり，情報の管理元すなわち所属先の情報保有機関であることが判別できてしまうという脅威も考えられる．

以上より，従来方式において以下の2つの大きな課題がある．

（課題1）各個人の情報の管理元である情報保有機関以外が本来知るべきではない所属先情報を，責任範囲の異なる他の機関が管理していること

（課題2）各情報保有機関が資格情報を登録する通信を盗聴することで，各個人の資格情報の所属先の機関で判別できてしまうこと

3　所属先情報の分散秘匿型資格確認サービスの提案

本章では，2 章で明らかにした従来方式の課題を解決する資格確認サービスの新たな方式を提案する．

3.1 提案方針

従来方式の 2 つの課題に対して，以下の方針をもって解決する．

方針1：保持する所属先情報の分散秘匿化
方針2：資格情報を登録するフローの秘匿化

(1) 方針1：保持する所属先情報の秘匿化

所属先情報を各個人の情報の管理元である情報保有機関以外の単一機関では識別できない形で保持する方針とする．具体的な解決方針を以下に述べる．

① 各個人の情報の管理元である情報保有機関が，資格確認サービス機関から他の情報保有機関をランダムに巡って自機関に辿りつく特定転送ルートを生成する．
② 資格情報登録フローにおいて，生成した特定転送ルートを単一機関では全体を把握できない形で分散秘匿して登録・保持する．
③ 資格情報特定フローにおいて，情報照会元の保険医療機関による資格確認サービスシステムへの問合せに応じて，各機関で登録・保持されている特定転送ルートに従って他の情報保有機関を順次巡ることで情報の管理元である情報保有機関に辿りつく．
④ 辿りついた先の情報の管理元である情報保有機関は，情報照会元の情報保有機関に対し，問合せ対象の資格情報を応答する．

(2) 方針2：資格情報を登録するフローの秘匿化

上記方針1の②資格情報登録フローにおいて，情報の管理元である情報保有機関から資格確認サービスシステムに特定転送ルートを直接登録するのではなく，他の情報保有機関をランダムに巡って，登録を行う方針とする．

具体的な解決方針は以下の通りである．

① 各個人の情報の管理元である情報保有機関が，自機関から他の情報保有機関をランダムに巡って資格確認サービス機関へ辿りつく登録転送ルートを生成する．
② 資格情報登録フローにおいて，生成した登録転送ルートを巡りながら，特定転送ルートを資格確認サービス機関および他の情報保有機関のいずれかに分散秘匿して登録する．

上記方針1により，資格確認サービス機関を含む情報管理元の情報保有機関以外の機関に対して，所属先情報を秘匿することが可能となる．また，上記方針2により，所属先情報の登録フローにおいて，資格確認サービスを含む他の情報保有機関に対して，情報管理元である情報保有機関が情報登録元である事を秘匿したまま登録が可能となる．

3.2 提案方式

本節では，前節の方針に基づいた具体的な提案方式について述べる．

本方式では，資格確認サービス及び特定転送ルート上の情報保有機関の各々が次に転送すべき機関の情報を「転送先情報」と定義し，特定転送ルートを各機関が共通的に識別するための識別子を，「ルート識別子」と定義する．特定転送ルートを「ルート識別子」と「転送先情報」のセットという形で各機関に分散管理することで，情報の管理元である情報保有機関以外の単一機関だけでは所属先情報を識別できない形とする．

なお，公開鍵暗号方式を使用するため，方式の前提として，資格確認サービス及び情報保有機関は，自機関の秘密鍵を保持しており，それらの秘密鍵に対応する公開鍵証明書はリポジトリ等に登録され，各機関は自由に入手できることとする．

以下では，提案方式における，資格情報登録フローおよび資格情報特定フローを述べる．

(1) 資格情報登録フロー

図 3-1にて，情報の管理元である情報保有

機関(図中の例では，I1とする)が資格確認サービス(A)に，自機関に所属している個人(ユーザID＝Sato)の特定転送ルートを登録するフローを説明する．

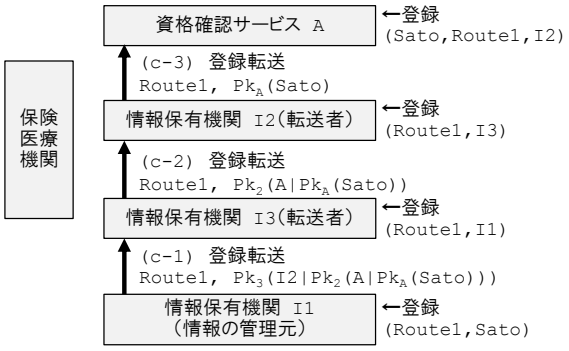

図 3-1 資格情報登録フロー(提案方式)

① 情報の管理元の情報保有機関の処理

情報の管理元である情報保有機関(I1)は事前に資格確認サービスから提供されている情報保有機関のリストを元に，複数個の情報保有機関をランダムに抽出(図中の例では，I3とI2を抽出)し，資格確認サービスから抽出した情報保有機関を経由して自機関にたどり着く，特定転送ルート(図中の例では，A→I2→I3→I1)を生成する．

次に，特定転送ルートの逆ルートを登録転送ルート(I1→I3→I2→A)とし，本システム内で一意となるルート識別子(例として Route1)を生成し，自機関の分散ルートテーブルにルート識別子(Route1)と登録対象者(Sato)を対応付けて登録する．ここで，ルート識別子は，本システム内で一意になるように留意する必要がある．

次に，匿名通信システムの The Onion Router(Tor)[6]の方法を活用し，登録転送ルート(I1→I3→I2→A)と登録対象者(Sato)の情報の暗号化を行う．登録転送ルートの暗号化は，ルート上の各情報保有機関が，自機関の転送先の情報保有機関のみしか把握できないようにするため，転送先情報保有機関の公開鍵で入れ子状に暗号化することで実現する．なおここで，情報 X を情報保有機関 z の公開鍵 Pk_z で暗号化することを $Pk_z(X)$と記述する．

図中の例では，登録対象者情報(Sato)を資格確認サービスの公開鍵Pk_Aで暗号化したPk_A(Sato)に対し，順次転送先情報を加えながら転送先機関の公開鍵で暗号化を行い，暗号化登録転送ルート情報(Pk_3(I2 | Pk_2(A | Pk_A(Sato))))を作成する．

最後に，作成した暗号化登録転送ルート情報とルート識別子(Route1)のセットを，最初の転送先である情報保有機関(I3)に対し登録転送(c-1)を行う．

② 転送ルート上の情報保有機関の処理

登録転送(c-2,c-3)を受けた登録転送ルート上の情報保有機関(I3 及び I2)は，転送元の情報保有機関の情報を特定転送先情報として，受信したルート識別子と併せて自機関の分散ルートテーブルに登録する

その後，登録転送に含まれる暗号化登録転送ルート情報を自機関の秘密鍵で復号し，次の転送先の情報保有機関を把握し，ルート識別子と復号した暗号化特定転送ルート情報のセットを，次の転送先の情報保有機関に登録転送(c-2,c-3)を行う．資格情報登録フローでは，登録転送ルート上の各情報保有機関において，本処理が繰返される．

以下，登録転送ルート上の情報保有機関(I3)の処理を例示する．

登録転送を受け取った情報保有機関(I3)は転送元の情報保有機関(I1)の情報を特定転送先情報とし，登録転送に含まれるルート識別子(Route1)と併せて自機関の分散ルートテーブルに登録する．そして，自機関の秘密鍵 Sk_3 で登録転送に含まれる暗号化登録転送ルート情報(Pk_3(I2 | Pk_2(A | Pk_A(Sato))))を復号し，転送先の情報保有機関(I2)を把握し，ルート識別子(Route1)と復号した暗号化登録転送ルート情報(Pk_2(A | Pk_A(Sato)))とのセットを，次の転送先情報保有機関(I2)に登録転送(c-2)を行う．

③ 資格確認サービスの処理

登録転送(c-3)を受け取った資格確認サービスは自機関の秘密鍵 Sk_A で登録転送に

含まれる登録転送ルート(Pk_A(Sato))を復号し，登録対象のユーザ ID(Sato)を把握する．次に，転送元の情報保有機関(I2)の情報を特定転送先情報とし，登録対象情報のユーザ ID(Sato)とルート識別子(Route1)を併せて自機関の分散ルートテーブルに登録する．

(2) 資格情報特定フロー

次に図 3-2にて，(1)資格情報登録フローで資格確認サービスシステムおよび各情報保有機関の分散ルートテーブルに分散登録した特定転送ルート(A→I2→I3→I1)を利用し，情報照会元である保険医療機関からの問合せに応じて，資格情報(所属先情報および個人属性情報)を特定する処理を説明する．

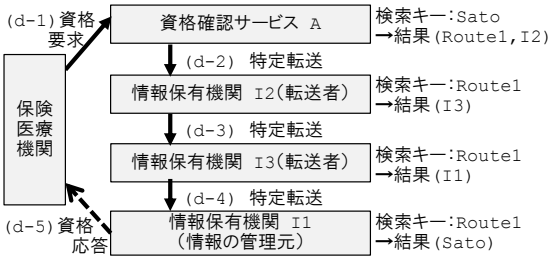

図 3-2 資格情報特定フロー(提案方式)

① 保険医療機関(情報照会元)の処理

情報照会元である保険医療機関は，資格確認サービス A に対し，対象者のユーザ ID(Sato)を指定し，資格要求(d-1)を行う．

① 資格確認サービスの処理

問合せを受けた資格確認サービスはユーザ ID(Sato)を検索キーに自機関の分散ルートテーブルを検索し，転送先情報の情報保有機関(I2)とルート識別子(Route1)を特定する．そして，特定した情報保有機関(I2)に対し，ルート識別子(Route1)を指定して特定転送(d-2)を行う．

② 転送ルート上の情報保有機関の処理

特定転送(d-2,d-3)を受けた特定転送ルート上の情報保有機関は，特定転送に含まれるルート識別子を検索キーに自機関の分散ルートテーブルを検索し，次の転送先情報保有機関を特定する．そして，特定した情報保有機関に対し，同じルート識別子を指定して特定転送(d-3,d-4)を行う．資格情報特定フローでは，特定転送ルート上の各情報保有機関において，本処理が繰返される．

以下，特定転送ルート上の情報保有機関の一つである I2 の処理を例示する．

特定転送(d-2)を受けた情報保有機関(I2)は，特定転送に含まれるルート識別子(Route1)を検索キーに自機関の分散ルートテーブルを検索し，次の転送先情報保有機関(I3)を特定する．そして，特定した情報保有機関(I3)に対し，ルート識別子(Route1)をを指定して特定転送(d-3)を行う．

③ 情報の管理元の情報保有機関の処理

特定転送(d-4)を受けた情報の管理元である情報保有機関(I1)は，特定転送に含まれるルート識別子(Route1)を検索キーに自機関の分散ルートテーブルを検索し，検索結果から資格確認対象者(Sato)が自機関に所属していることを把握する．そして，情報照会元の保険医療機関に資格確認対象者(Sato)の個人属性情報を含む資格情報を応答(d-5)する．

4 評価

本章では，提案方式を有効性，性能面，および運用面において，検討評価した内容を述べる．

4.1 有効性の検討

関係する各機関が，本提案方式において把握可能な情報を精査することで，2 章で述べた課題が解決できているかを検討し，本方式の有効性を示す．

(1) 資格確認サービス機関

資格確認サービス機関は以下の情報のセットを把握可能である．

・ユーザ ID
・ルート識別子
・転送先情報

また，資格情報登録フローにおいても，資格確認サービス機関は，登録転送の転送元の機関は把握可能であるが，それより前の登

録転送ルートは把握できないため，ユーザ ID の所属先である情報管理元の情報保有機関は把握できない．

(2) 転送ルート上の情報保有機関

転送ルート上の情報保有機関は，以下の情報のセットを把握可能である．

・ルート識別子

・転送先情報

上記のとおり転送先情報は把握可能であるが，次の転送先が情報管理元の情報保有機関であるかどうかは判別できない．

また，資格情報登録フローにおいても，転送ルート上の情報保有機関は，登録転送の転送元及び転送先の情報保有機関を把握可能ではあるが，資格確認サービス機関と同様に情報管理元の情報保有機関は把握できない（転送回数ごとの検討は4.1(1)にて後述）．

以上の検討により，課題1の管理元以外の情報保有機関が所属先情報を管理していないこと，課題2の資格情報を登録する通信を盗聴しても所属先情報が判別できないこと，が分かり，課題解決の有効な手段であることが確認できる．

4.2 性能面の検討

資格情報特定フローでは，複数の情報保有機関を巡って管理元である情報保有機関に辿りつくことで，所属先情報を秘匿している．このとき，情報保有機関を巡る数を多くすると，転送数が増え，応答性能が劣化するため，転送回数を適切に設定する必要がある．以下では，転送回数を定数にする場合及び，ランダムにする場合についてそれぞれ検討する．

(1) 転送回数を定数で固定する場合

転送回数を1回で固定する場合，従来技術とほぼ同様となるため，課題解決はできない．

転送回数を2回で固定した場合も，資格確認サービス機関から最初に転送された情報保有機関は，次の転送先が情報管理元の情報保有機関であることを判別できてしまうため，同じく課題解決はできない．

転送回数を3回で固定した場合は，資格確認サービス機関から最初に転送された情報保有機関は，次の転送先が情報管理元の情報保有機関であることを判別できない．しかし，資格確認サービス機関以外の情報保有機関から転送された機関は，次の転送先が情報管理元の情報保有機関であることを判別できてしまうため，同じく課題解決にならない．

転送回数を4回で固定した場合は，資格確認サービス機関以外の情報保有機関から転送された機関であっても，次の転送先が情報管理元の情報保有機関であるのか，さらに転送を行う機関であるのかを判別することができない．

よって，転送回数を最低でも 4 回以上にする必要があり，性能面を考慮すれば 4 回にするのが望ましいと考えられる．

(2) 転送回数をランダムにする場合

転送回数をある一定回数以内のランダム範囲に設定する方法も考えられる．

ランダム範囲が 2 回以内の場合，選択可能な転送回数は1回と2回であり，資格確認サービスはどちらが選択されたか分からないため，転送先が管理元の情報保有機関であるかは判別できない．しかし，資格確認サービス機関から最初に転送された情報保有機関は，転送を受けた時点で2回が選択されたことが分かるため，次の転送先が管理元の情報保有機関であることが判別できてしまう．

ランダムの範囲が 3 回以内の場合は，資格確認サービス機関は 2 回以内の場合と同様に問題ない．また，資格確認サービス機関以外の情報保有機関から転送された機関であっても，次の転送先が情報管理元の情報保有機関であるのか，さらに転送を行う機関であるのかを判別することができない．

よって，ランダム範囲に設定する場合は，最低でも 3 回以内の範囲で設定する必要がある．

以上から，転送回数は定数で固定するよりも，ランダムにした方が性能面で優れていることが

分かる.

4.3 運用面の検討

本提案方式においては，情報保有機関等の統廃合に伴い，各機関の分散ルートテーブルに登録される特定転送ルートが更新・削除されるケースが考えられる.

例えば，情報保有機関の廃止または統合により，資格情報特定フローがとぎれてしまい，正常な回答が出来なくなる問題が考えられる．また，何らかの理由により，各機関の分散ルートテーブルに登録される特定転送ルートの情報が欠損してしまうことも考えられる．情報保有機関の統廃合の場合は，従来方式にはない運用上の考慮を別途行う必要がある.

上記を踏まえ，特定転送ルートを複数登録しておくことで可用性を高める方法や，安全なルートの更新・削除方法等の検討も行っていくべきと考える.

5　まとめ

社会保障分野における資格確認サービスにおいて，各個人の所属先情報を安全かつ秘匿性を高めた形で管理することを目的として，資格確認サービス機関と複数の情報保有機関とが協調しあう方式を提案した.

本提案方式は，ランダムに設定したルート情報を複数機関で分散秘匿し，情報管理元以外の機関には所属先情報を秘匿したまま資格確認サービスを実現可能とする方式である.

提案した方式は，情報管理元以外の情報保有機関に所属先情報を秘匿すること，および登録する通信の盗聴を行っても所属先情報を判別できないこと，という従来方式の課題を解決するものであり，本方式の有効性の確認も行った．また，性能面・運用面においても，適切な転送回数の検討や情報保有機関の統廃合時の運用上の検討も行った.

今後の課題としては，性能面の検討で述べた転送回数での実システムを用いた性能評価や，運用面の検討で述べた特定転送ルート情報の安全な更新方法などの検討が挙げられる.

参考文献

[1] 社会保障・税一体改革, http://www.cas.go.jp/jp/seisaku/syakaihosyou/

[2] 社会保障・税に関わる番号制度, http://www.cas.go.jp/jp/seisaku/bangoseido/index.html

[3] 「医療等分野における番号制度の活用等に関する研究会」中間まとめ, http://www.mhlw.go.jp/stf/shingi2/0000067915.html

[4] 畠山誠, ″5F-1 異なる連携プロトコルを仲介するプロキシ型属性情報管理システム(社会システムと Web，一般セッション，ネットワーク，情報処理学会創立 50 周年記念).″ 全国大会講演論文集 72.3 (2010)

[5] Liberty Alliance Project, Liberty Identity Web Services Framework 2.0 (Liberty ID-WSF), http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications/?f=resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications

[6] Tor Project: Anonymity online, https://www.torproject.org/