Vol.2010-GN-74 No.6
2010/1/21

個人情報保護を重視するシステムにおける他ユーザ指定手法の提案

宮島麻美† 中村亨† 爰川知宏† 大野浩† 前田裕二†

近年普及が期待されている電子公共サービスにおいては，重要な個人情報をその対象とし，厳密なアクセス制御が求められる一方で，他者による代行や他者への情報開示等，様々なシーンでの他ユーザの情報へのアクセスも想定しなければならない．本稿では，これを実現するための技術課題の一つである「他ユーザを指定すること」に着目して要件を整理し，本人が許可した以外の他ユーザに一切の個人情報を開示することなく，信頼関係のある他ユーザのみに安全に個人の識別情報を受け渡すことを可能にする新たな他ユーザ指定手法を提案する．

A Proposal of new Method for Specifying Other Users in Systems required to Protect Personal Information

Asami Miyajima† Toru Nakamura† Tomohiro Kokogawa†
Hiroshi Ohno† and Yuji Maeda†

The evolution of public services improved by broadband network technology is expected. These services are required to control access to information strictly, because these handle high-level personal information. However, the users of these services request to access other users' information in their operations, such as alternative operations. We point out specifying other users as one technological task for these requirements, and propose a new method that enables the users to specify other users without disclosing personal information to others not related.

1. はじめに

本格的なブロードバンド社会の到来により，ネットワークを用いた様々な民間サービスが登場し，ショッピングや航空券予約，証券取引等，多岐にわたる場面で利用されている．これに追従するように，これまで IT 化の遅れが指摘されてきた行政，教育，医療といった公共性の高い分野においても，ネットワーク活用への動きが加速している[1]．例えば，2009 年に策定された i-Japan 戦略 2015[2]では，エンドユーザである国民に向けた具体的なサービスイメージとして，国民電子私書箱（仮称）および日本版 EHR（仮称）について言及されており，これまでの電子政府・電子自治体の戦略からより踏み込んだ内容となっている．これらの構想では，政府内もしくは自治体内に閉じた単なる従来業務の電子化に留まらず，国民が公共機関の保有する情報を積極的に活用するという，国民に開かれた新たな公共サービスの在り方が掲げられている（本稿では，これらのサービスを総称して電子公共サービスと呼ぶ）．

普及が期待されるこれらの電子公共サービスであるが，前述したような民間サービスとは異なる要件が存在する．その内最たるものとしては，使いたい人が使う民間サービスとは異なり，電子公共サービスは老若男女問わず国民の誰もが何らかの形でサービスを享受できる必要があることが挙げられる．これを実現するための方法としては，IT リテラシが低い利用者でも操作できるようユーザビリティを向上させることが考えられるが，高齢者や子供，乳幼児までを対象とするには，この方法では限界がある．従って，本人による操作の代替手段として，本人から許可を得た他者（家族，親族等）が申請や参照等の各種操作を代行する「他者による代行」の仕組みが必要になると考える．また，操作の代行に加え，前述の日本版 EHR（仮称）[a]（以下，EHR と呼ぶ）等では，不要な検査の回避やセカンドオピニオンの目的で，本人が入手した医療・健康情報を本人が指定する医療従事者等に開示する「他者への情報開示」も想定されている[2].

上記のような利便性に関わる要件がある一方で，電子公共サービスでは，年金，税，医療情報等，個人のプライバシーに関わる個人情報を取り扱うため，基本的なセキュリティ対策のみならず，情報にアクセスするユーザを厳密に制御できることも求められる．前述した「他者による代行」や「他者への情報開示」の要件を鑑みると，本人が本人の情報にアクセスできることに加え，本人が許可した人が許可した情報だけにアクセスできるよう制御する仕組みが必要になると考えられる．現状，代行の仕組みが整っていないシステムでは，本人の ID を使って他者がログインする，という運用

† NTT サービスインテグレーション基盤研究所
NTT Service Integration Laboratories

a) EHR とは， Electronic Health Record の略．世界各国で普及に向けた取組が進められている．日本では，個人が医療機関等より電子的に健康情報を入手し，本人および医療従事者等が活用すること，および匿名化された健康情報を疫学的に活用することが将来ビジョンとして掲げられている[2].

的対処を行っていることが多い．しかし，電子公共サービスのように，誰が誰の情報にアクセスしたか，その時本人によるアクセス許可はあったのか，等の証跡管理や監査も重要視されるシステムにおいては，この方法は好ましいとは言えない．

このように，電子公共サービスでは，重要な個人情報をその対象とし，厳密なアクセス制御が求められる一方で，他者による代行や他者への情報開示等，様々なシーンでの「他ユーザの情報へのアクセス」も想定しなければならない．この点が，電子公共サービスに特有の難しさの一つであると考える．

2. 技術課題

2.1 着目する技術課題

まず，ユースケースに基づいて「他ユーザの情報へのアクセス」を実現するための技術課題を抽出し，本研究の着眼点を絞り込む．ユースケースとしては，電子公共サービスの必須要件と考えられる「他者による代行」を想定する．以下は EHR サービスの場合の例である．

・市民 A：市民 B の親．高齢で IT 利用に不慣れなため，自らの医療・健康情報の操作（参照，登録等）は離れて暮らす子（市民 B）に任せたい．
・市民 B：市民 A の子．親である市民 A に代わり，市民 A の医療・健康情報を操作（参照，登録等）したい．

前述したように，証跡管理や監査が重要視される電子公共サービスでは，本人の許可を受けた他者が，自らのアカウントの権限で情報にアクセスする必要がある．

1) 情報のオーナーである市民 A が市民 B に対して自らの情報へのアクセス許可を設定する
2) 市民 B が自らの ID でログインし，市民 A が設定したアクセス許可に基づいて市民 A の情報にアクセスする

ユーザ操作 1)2)の目的は，「他ユーザの情報へのアクセス」即ち，本人が許可したユーザが本人の許可した情報のみにアクセスできるようにすることであるから，当然，アクセス制御の仕組みは必要となる（表 1①）．これは例えば，ユーザごとにその医療･健康情報へのアクセス条件を規定したアクセス制御ルールを設定できるようにし，本人がアクセス許可したい他ユーザの識別子をルールに追加して（上記 1）），他者による情報へのアクセス時にはそのルールと照合してアクセス可否判断を行う（上記 2）），等の手法が考えられる．

また，これらのアクセス制御の仕組みを使うためには，その前段で解決すべき技術課題がある．操作対象とする「他ユーザを指定する」ことである（表 1②）．上記のユーザ操作 1）において，アクセス許可を設定する場合，市民 A は，許可したい他ユーザ（市民 B）の識別情報（ユーザ ID 等）を何らかの方法で取得しなければならない．

また，上記 2）において，市民 B が他ユーザ（市民 A）の情報を参照，登録するためには，その情報の所有者（市民 A）の識別情報を取得する必要がある．この「他ユーザの指定」は，他者への情報開示においても同様に解決すべき技術課題となる．本稿では，上記 2 点の技術課題の内，②に着眼し，それを解決するための手法を提案する．

表 1　「他者による代行」実現のための技術課題

	ユーザ操作	技術課題	
		①アクセス制御	②他ユーザ指定
1)	市民 A が，自分の情報に市民 B がアクセスできるよう設定する．	市民 B を自らのアクセス制御ルールに追加する．	市民 B をシステム上で特定する．
2)	市民 B が自分の ID でログインし，市民 A の情報にアクセスする．	市民 A の情報を操作する．	市民 A をシステム上で特定する．

2.2 関連動向

システム上で登録済みの他ユーザを指定する従来手法は，その用途や条件によって様々である．利用者や使い方が限定されたシステムにおいては，他ユーザを指定することは容易である．例えばサイボウズ[3]等のグループウェアでは，会社の組織内メンバ等，信頼できる特定ユーザのみが利用することを想定し，各ユーザは氏名，所属等を他ユーザに公開することを前提としている．そのため，ユーザは氏名等を直接指定して，システム上の他ユーザを指定することができる．

また，多くの病院・診療所で利用されている電子カルテシステムでは，患者本人が来院し，診察券を提示するというフローが確立しているため，診察券に記録された患者 ID からユーザを特定でき，診療録や検査結果の記録等を行うことができる．また，院内の職員という限られたユーザが業務目的で利用するため，ユーザ（権限のある職員）は業務用に用意されたリストから患者を検索することができる[4] ．

一方，不特定多数のユーザが利用するようなサービスにおいて，ユーザの個人情報を保護しながら，一意に他ユーザを特定するためには工夫が必要である．例えば，不特定多数のユーザが利用する mixi[5]等の SNS（Social Network Service）サービスでは，ユーザがそれぞれ自身のニックネームや氏名，性別，写真等，一部の個人情報（プロフィール）を公開することで，このプロフィール等に基づいて自分に近い趣向を持つ他ユーザを検索できるようにしている．

2.3 電子公共サービスの他ユーザ指定における課題

上記の従来手法をふまえ，電子公共サービスにおいて，システム上で他ユーザを指

定することを考えてみる．全国民を対象とする電子公共サービスにおいては，ほとんどのユーザ同士に関係性がなく，本人が許可した極わずかなユーザ（家族等）以外には一切の個人情報を公開することが許されない．そのため，前述のグループウェアやSNS のように，全ユーザに氏名やプロフィール等を公開する手法は用いることができない．氏名等を入力させ，絞り込んでから提示するようにしたとしても，同姓同名の場合等に誤検出が起こることを完全に排除することは難しい．また，業務も利用者の権限も限定されていないため，電子カルテのようにユーザの権限内で参照可能なリストから選択させる手法も適用できない．このように，電子公共サービス等の個人情報保護を重視するシステムにおいては，個人情報を公開させたり検索させたりすることなく，システム上で他ユーザを指定することが困難な課題となる．

システムにログイン中の操作のみで他ユーザを指定することが困難なのであれば，他の方法として，ユーザの識別情報をシステム外に取り出し，所望のユーザのみにシステム外で受け渡す方法が考えられる．最も簡易な方法は，識別情報（ユーザ ID 等）を直接受け渡すことである．しかし，流出した場合にシステム上で直接的に利用できるユーザ ID を，IT リテラシの低い市民を含むユーザ同士に自由に交換させることは，ユーザ ID を悪用されるリスクを高め，ひいては個人情報の流出やシステム全体の信頼性失墜に繋がりかねない．また，ユーザ ID が流出した場合には，ユーザが利用中のユーザ ID を失効させ，再発行する等の手続きが必要になり，円滑なシステム利用を妨げてしまう．このことから，システム外で識別情報を受け渡す方法においては，受け渡し方法に関する利用者の自由度を確保しつつ，流出時にもシステム利用に支障をきたさないよう，識別情報のシステム外への取り出し方等を検討する必要がある．

3. 他ユーザ指定手法の提案

以上の考察をふまえ，本稿では以下を特徴とする他ユーザ指定手法を提案する．

- システム上でユーザを一意に特定できる識別情報を含む「ユーザ指定子（TUS: Temporary User Specifier と呼ぶ）」をシステム外に取り出し，ユーザ間で受け渡すことができる．
- システム外に取り出したユーザ指定子（TUS）は直接システム上のユーザ識別子として利用はできず，悪用を防止するセキュリティ対策が施されている．

基本的な利用イメージは図 1 の通りである．尚，本稿では，TUS の正当性を検証し，システム上のユーザ識別情報として利用できるよう変換することを「解決」と呼ぶ．

図 1 の手順により，ユーザは所望の他ユーザを指定することが可能になり，指定した他ユーザを対象としたアクセス制御ルールの設定や情報参照を行うことができる．②については，電子メールや URL に埋め込む，二次元バーコードに埋め込んで配布する等，用途に応じた方法が考えられる．本稿では，②の自由度と安全性を確保することを目的とし，システムの機能として実装可能な①③をその検討範囲とする．

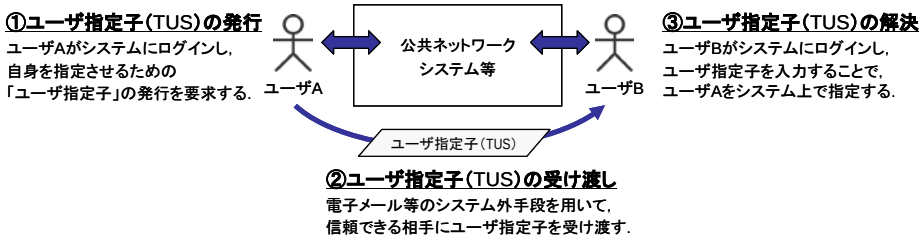

図 1　提案手法の利用イメージ

4. システム要件と基本機能

3 章までに述べた利用イメージに基づき，システム要件を明確化する．

4.1 前提条件

システム要件を明確にするため，まず設計の前提とする電子公共サービスおよびユーザを設定する．

【サービス】

現在様々な電子公共サービス普及への取り組みが行われているが，本稿では，既にフィールドでの実証事業[7]が行われている EHR サービスを電子公共サービスの典型例として取り上げる．EHR サービスについて，筆者らは既にそのサービスモデルを提案している[6]．このモデルでは，サービスを運営する事業者として次の 3 者を想定している（図 2）．本稿でも同様の構成を想定することとする．

- データプロバイダ：
  エンドユーザの医療・健康情報を保持するプロバイダ．
- サービスプロバイダ：
  データプロバイダから集めた医療・健康情報を用いて，エンドユーザに対して具体的なサービスを提供するプロバイダ．
- 情報連携基盤：
  データプロバイダ，サービスプロバイダ間での情報連携を実現する共通基盤．

【ユーザ】

他ユーザの情報へのアクセスに関連するユーザとして，図 2 のサービスモデルに従って以下を想定する．

- 一般ユーザ：医療・健康情報を有するシステム利用者．
- 代理ユーザ：親・保護者等，一般ユーザの代理人としてふるまうシステム利用者．

・ プロユーザ：
医者，保健指導師，インストラクタ等，具体的な医療・ヘルスケアサービスを提供するシステム利用者．ユーザ属性として，所属する組織の情報やロール（前記サービスにおける役割（国家資格等））の情報を有する．

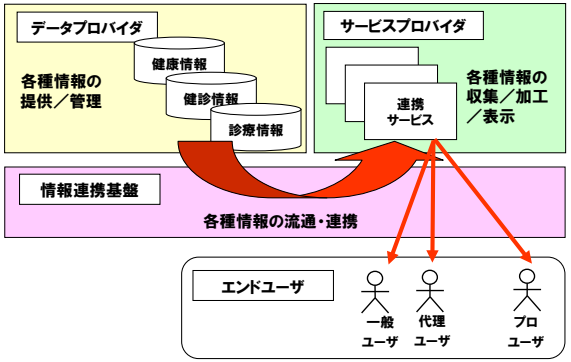

図 2　前提とする電子公共サービスモデル（[6]より引用）

4.2 システム要件

上記のサービスおよびユーザを前提として，他ユーザを指定する必要のあるユースケースを挙げ，そこからシステム要件を抽出する．

【一般ユーザー代理ユーザ（または一般ユーザ）間における要件】

EHR サービスにおける「他ユーザ指定」の一つの典型例としては，2.1 節に例示した一般ユーザと代理ユーザ（または一般ユーザ）との間の指定が考えられる．2.1 節の例では，市民 A（一般ユーザ）が自らの情報へのアクセス許可を設定する時に，市民 B（代理ユーザ）を指定する必要がある．また，市民 B（代理ユーザ）が実際に市民 A（一般ユーザ）の情報にアクセスしようとする時に，市民 A を指定する必要がある．このユースケースの特徴としては，家族や友人等の限られた相手を繰り返し指定することが多いことが挙げられる．そのため，一度 TUS で指定した相手ユーザの識別情報を個人用のリストに保存しておく等の対策が有効である．この場合，TUS は最初に一度だけ利用すれば相手ユーザを指定できる．即ち，TUS は初めに指定するまでの極めて短期間だけ有効であればよい，ということになる．

【プロユーザー一般ユーザ（または代理ユーザ）間における要件】

他の典型例としては，プロユーザと一般ユーザ（または代理ユーザ）との間の指定が考えられる．市民（一般ユーザ）が自らの情報を医師（プロユーザ）に開示するためにアクセス許可を設定する時には，医師を指定する必要がある．また逆に，医師（プロユーザ）が市民（一般ユーザ）の情報を参照する時には，市民を指定することになる．前述したように，後者は業務リスト等から選択できる場合が多いが，前者については TUS を用いたユーザ指定を検討する必要がある．医師等のプロユーザは，TUS を渡す相手が複数人に及ぶため，その都度 TUS を発行することはユーザにとって負担が大きい．即ち，TUS は有効期間が長く，同じ TUS を複数の一般ユーザが利用できることが望まれる．一方，TUS を利用する一般ユーザ側から見た場合，プロユーザが有する所属組織やロール単位でアクセス許可を設定したいケースも考えられ，その時にもプロユーザ個人を指定するのと同様の操作，即ち TUS を使って設定できることが望まれる．

【ケースに依らない要件】

その他ユースケースに依らない要件としては，まずセキュリティの確保がある． TUS 自体を解読させない施策を取るのはもちろんであるが，なりすまし防止策として，TUS を利用（解決）する際に，その TUS が本当にユーザの望む他ユーザのものか否かを確認できることが望ましい．また逆に，不正利用防止策としては，TUS を利用（解決）する際に，その利用者が，TUS の発行元ユーザの許可したユーザであることを確認できることが望ましい．また，TUS 流出等に備え，TUS のみを失効させてユーザ ID はそのまま利用継続させる仕組みも必要となる．また，プロユーザが休職等の理由で TUS を失効させる場合には，失効済みの TUS を再有効化できることも望まれる．利便性の面では，複数のサービスプロバイダのいずれからログインしても，TUS を解決できることも基本的な要件として挙げられる．

4.3 要件の整理と基本機能

以上の前提・ユースケースから，3 章で述べた本手法の基本方針（表 2 の A および F）に付随するシステム要件をまとめた（表 2）．A～E は利便性に関する要件，F～H はセキュリティに関する要件である．

表 2　他ユーザ指定手法への要件

項番	要件
A	TUS を用いてシステム上で他ユーザを識別できること
B	ユーザの用途に応じて，TUS の有効期間を設定できること
C	ユーザ個人を指定するのと同様に，TUS を使って組織やロールを指定できること
D	ユーザの要望に応じて，発行済みの TUS の失効，再有効化ができること
E	システム構成に依存せず，どのサービスプロバイダからでも TUS を利用できること
F	TUS を解読・悪用されないようセキュリティ対策がなされていること

G	TUS を利用する際に，その TUS が所望の他ユーザのものであると確認できること
H	TUS を利用する際に，その利用者が TUS の発行元ユーザに許可されたユーザであると確認できること

表 2 にまとめた他ユーザ指定手法へのシステム要件より，本手法に求められる機能および TUS に格納すべき情報について，表 3 および表 4 の通り整理した．

表 3　システム要件を満たすための機能

項番	機能	対応する要件
Ⅰ	TUS を発行する（発行時には，TUS を暗号化し，署名を付与する）	A,F
Ⅱ	入力された TUS を解決する（解決時には，TUS の署名検証を行い，復号する）	A,F
Ⅲ	発行済みの TUS を失効する	D
Ⅳ	失効済みの TUS を再有効化する	D

表 4　システム要件を満たすための TUS の構成要素

項番	機能	対応する要件
1	TUS にユーザの識別情報を格納する	A
2	TUS に有効期間を格納する	B
3	TUS にユーザの属性情報（組織，ロール）を格納する	C
4	TUS に発行元サービスプロバイダの識別情報を格納する	E
5	TUS に発行元ユーザを確認するためのニックネームを格納する	G
6	TUS に発行元ユーザを確認するための質問・答えを格納する	H

G，H については，TUS の利用ユーザ自身が最終確認できることを要件と捉え，TUS の発行元ユーザと解決元ユーザとの間で，本人同士ならわかるまたは TUS 受け渡し時に通知する情報（ニックネームや質問/回答）を，TUS 解決時に確認する方式とした．

5.　システムへの適用例

4.3 節でまとめた本手法の基本機能を実システムに適用した例を示す．

5.1　システム構成と機能配置

本手法の適用対象は，システム要件抽出の前提と同様に，[6]で提案されている EHR サービスの情報連携基盤とする．この情報連携基盤では，認証連携（シングルサインオン）およびそれに基づく情報連携を実現するための要素技術として，SAML/ID-WSF に基づく通信処理を採用している．表 3 に示した本手法の基本機能は，図 3 に示す通り，[6]の情報連携基盤内の機能として配置する．

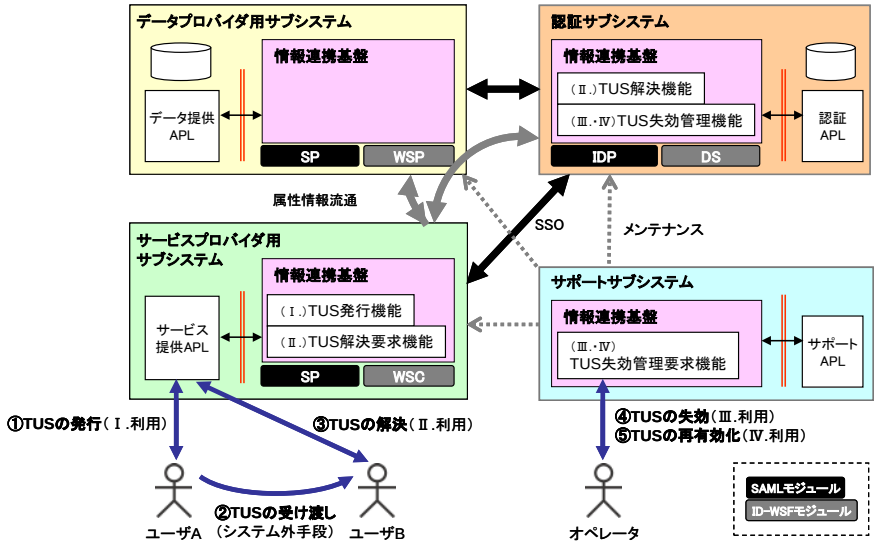

図 3　システム構成と機能配置

TUS の発行機能（Ⅰ.）は，ユーザインタフェースを有するサービスプロバイダ用サブシステムに配置する．これにより，通信を発生させず TUS を発行することができる．TUS に発行元サービスプロバイダの識別情報を格納しておけば，TUS 解決は異なるサービスプロバイダからでも可能である．TUS の解決機能（Ⅱ.）は，システム上のユーザ管理を統括している認証サブシステムに配置する．認証サブシステムはユーザ ID と仮名の対応付けも管理しているため，TUS に格納するユーザの識別情報として，ユーザ ID そのものの代わりに仮名を TUS に格納することが可能になる．仮名とは，SAML で規定されたものであり，認証サブシステムと他のサブシステムとの対ごとに規定される，ユーザ ID とは異なるユーザ識別子である．そのため，万一流出しても実ユーザ ID の漏洩を最小限に抑えられるというセキュリティ面でのメリットがある．TUS の失効・再有効化機能（Ⅲ.・Ⅳ.）は，認証サブシステムに配置し，一般/プロユーザからの申請に応じて，システム管理者であるオペレータがサポートサブシステムから利用することを想定する．TUS の解決手段と同じサブシステムに配置することにより，TUS 解決時に容易に失効状況を確認することができる．

5.2 機能詳細

以下では，表 3 に挙げた本手法の基本機能について説明する．

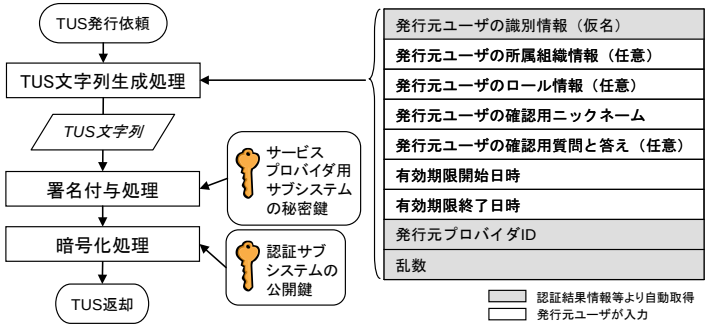

図 4　TUS の発行ロジック

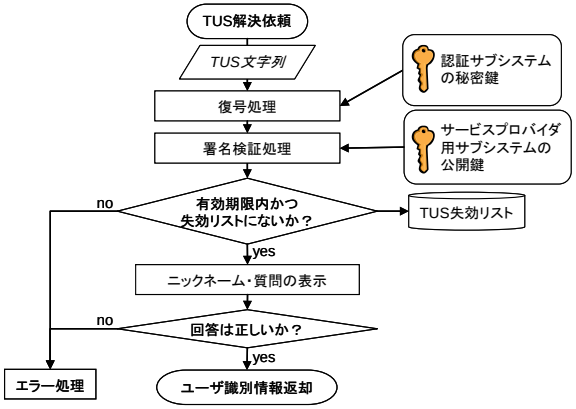

図 5　TUS の解決ロジック

Ⅰ. TUS の発行

TUS の発行ロジックを図 4 に示す．まず，表 4 に示した構成要素を”&”で連結して TUS 文字列を生成し，更に署名を連結する．この文字列を認証サブシステムの公開鍵で暗号化した後，TUS として発行する．

Ⅱ. TUS の解決

TUS の解決ロジックを図 5 に示す．まず，入力された TUS 文字列を復号・署名検証し，有効期限内であることおよび TUS が失効済みでないことを確認する．続いて，TUS から抽出したニックネームと質問を表示し，TUS 解決要求元のユーザに質問に対する回答を求める．回答が TUS から抽出した回答と一致すれば，TUS の発行元ユーザの識別情報，所属組織情報（任意），ロール情報（任意）を返却する．TUS 解決要求元ユーザは，これらの情報を用いてユーザ（または組織等）を指定し，アクセス制御ルールの設定や情報参照を行うことができる．

Ⅲ./Ⅳ. TUS の失効・再有効化

認証サブシステムに TUS 失効リストを設け，TUS 失効要求時には入力された TUS をそのリストに追加し，TUS 再有効化要求時には TUS 失効リストから削除する．また，TUS 失効リストから失効済み TUS を検索する機能も提供する．

6. まとめと今後の課題

本稿では，個人情報保護が重視される電子公共サービスにおいて，本人が許可したユーザ以外には一切の個人情報を公開することなく，実世界において信頼関係のある他ユーザのみに個人の識別情報を安全に受け渡すことを可能にする新しい他ユーザ指定手法を提案した．

今後は，本手法を適用した実システムの利用実験等を通じて，実際のユースケースにおいて本手法の目的とする安全性と利便性の双方が満たされているか，検証する必要がある．安全性の面では，例えば，一般ユーザ向けに一度利用（解決）したら再利用できない TUS を提供する，TUS 解決の用途を限定する等の機能も検討の余地がある．また利便性の面では，例えば，市民－市民間の他ユーザ指定においては，親と子が相互に指定し合う場合に，TUS の発行・解決の手順を簡略化することが可能と考える．また，本稿では詳しく言及しなかった TUS の受け渡し部分についても各種の方法を実装し，一連の利用手順の利便性を確認する必要があると考えている．

参考文献

1) ICT ビジョン懇談会: ICT ビジョン懇談会報告書,（平成 21 年 6 月）,
http://www.soumu.go.jp/menu_news/s-news/02tsushin01_000017.html
2) IT 戦略本部: i-Japan 戦略 2015（平成 21 年 7 月）,
http://www.kantei.go.jp/jp/singi/it2/kettei/090706honbun.pdf
3) サイボウズ: http://manual.cybozu.co.jp/office8/user/
4) 日立製作所: 電子カルテシステム「HIHOPS-HR」,
http://www.hitachi.co.jp/Prod/comp/app/iryou/hr/function.html
5) mixi: http://mixi.jp/help.pl?mode=item&item=467
6) 爰川知宏, 宮島麻美, 大野浩, 中村亨, 前田裕二: 医療・健康情報の流通・活用に向けた情報連携基盤の提案, 情報処理学会研究報告, Vol.2009-GN-73, No.14, pp.1-6, 2009
7) 総務省・厚生労働省・経済産業省: 健康情報活用基盤実証事業について（平成 20 年 9 月 5 日）,
http://www.kantei.go.jp/jp/singi/it2/iryou/kaisai_h20/dai2/siryou4.pdf