PIDを用いた安全な社会システムの構想

浜崎, 陽一郎
九州大学大学院システム情報科学研究院情報工学専攻

安浦, 寛人
九州大学大学院システム情報科学研究院情報工学部門

出版情報：九州大学大学院システム情報科学紀要. 7 (2), pp.139-148, 2002-09. 九州大学大学院システム情報科学研究院
バージョン：
権利関係：

PIDを用いた安全な社会システムの構想

浜崎　陽一郎* ・ 安浦　寛人**

A Proposal of Secure Information Infrastructure based on PID

Yoichiro HAMASAKI and Hiroto YASUURA

(Received June 26, 2002)

Abstract: As a background of the rapid progress of the network,various electronic services proceed steadly. It thinks that we become more convenient, and more efficient by the introduction of these services. But on the other hand, it is a big subject that there are many security problems because of electronic. It is very important to build the society which keeps those damages to a minimum. So we don't only apply security technology to the existent society. Building of the secure information infrastructure as a cause of the definite concept. By this thesis, we proposed some concepts, modelled, and verified.

Keywords: IT-Society, Infrastructure, Security, Personal-ID(PID), PID subsequence(subPID),

1. はじめに

インターネットをはじめとするネットワークの急速な普及を背景に，様々なサービスの電子化が着々と進んでいる．このサービスは多岐に渡り，従来紙ベースで行っていた処理を電子ベースに移行したり，あるいは金融機関がインターネットを通じて金融サービスを行うインターネットバンキングなど，我々の身近な生活に大きな影響を与えるものである．

これらのサービスの導入により，我々の生活はより便利により効率的になると思われる．しかしその反面，電子的であるがために発生する安全性の問題も大きな課題である．痕跡を残さない改竄，成りすまし，盗聴など，数々の脅威が存在する．我々が留意しなければならないのはその点であり，被害を最小限に留める社会の構築は重要であると考える．

安全性を保つための研究は盛んに行われているが，これらは技術的な観点からのアプローチであるものが多いと思われる．我々はこのような技術的なアプローチだけでは，十分に安全な社会を構築できるか疑問に思っている．これらのアプローチは現状の社会システムに対して新しい技術を埋めこんでいくものであるが，社会システムそのものに目を向けると，必ずしも最適な社会システムの設計とはなっていないと考える．従来の「既存の社会システムの部分的な電子化」というアプローチから「情報技術の利用を前提とした新しい社会システムの構築とそのための技術開発」という立場への転換が求められている．

平成14年6月26日受付

* 情報工学専攻修士課程

** 情報工学部門、システムLSI研究センター

例えばインターネットにおいても，その急速な技術的進歩によって，社会的影響を見越すことがほとんど不可能な状態で技術の商用化・製品化が進められているのが現状である[1)]．利用者が法に触れるような問題，倫理的問題，セキュリティ，ディジタルディバイド，個人のプライバシ保護，違法・有害情報の流布など，インターネットの技術とは別に社会システムの問題として取り扱うべき課題も数多く顕在化してきている．

そこで，我々は現在の社会システムが将来の電子的な世界において弊害となるであろう問題点を探り出し，電子・情報技術の存在を前提とした社会システムの構築を目指している．問題点は多岐に渡ると思われ，そのすべてをカバーする理想の社会システムの構築を一気に行うことは困難と思われるが，いくつか重要と思われる問題点を分析し，それに対応した社会システムの提案を行う．

2. 問題点の分析

本論文では，企業や行政等のサービスを提供する側(以下サービス提供者)と，そのサービスを受ける個人(以下ユーザ)の関係を主として取り扱う．これは電子商取引の1つとして挙げられるBtoC(Business to Consumer) 等を含んでいる．BtoCの市場規模は2005年には13兆円になると予測され[2)]，今後大きな期待が寄せられる．

2.1 社会におけるユーザの立場

我々はまず社会におけるユーザとサービス提供者の比較を行った．比較要素は多々あるが，その中で重要と思われ，かつユーザとサービス提供者との間に大きな開きがあると考えられる部分に注目した．

第一に社会的信用度である．ユーザとサービス提供者を比較した場合，明らかに社会的信用度においては企業・

自治体の方が大きいと考えられる．

この信用度の違いはユーザを非常に弱い立場にしている．ユーザはサービス提供者が要求する金額を支払い(モノの値段)，必要な書類を提出している．ある意味ユーザはサービス提供者の言いなりになっているような感があるが，これらが受け入れられている背景にはユーザとサービス提供者の信用度の大きさに依存している．つまり社会に認知された(信用度の高い)サービス提供者が提供する物であるから，ユーザはモノの価値に加え，サービス提供者自身の信頼性・信用度を受け入れて購入する．またクレジットカードの発行や各種会員証の発行に際して，ユーザは往々にして個人情報の提出を行う必要がある．これは信用度の低いユーザを，サービス提供者が，成りすましなどない個人として信用するために必要な手続きである．社会的に信用度の高いサービス提供者はそのような行為を取り立てて行う必要がない．このように信用度は現在の社会システムの中で大きな役割を果たしており，我々の生活はその上で機能している．

第二に資本力の差が挙げられる．一般的にサービス提供者の方が大きな資本力を有している．この差は自分の利益の保護・安全性の確保といった部分に大きな影響を及ぼす．大きな資本力を持たないユーザは極めて弱い立場にあると言える．現在の社会システムがユーザを保護してきたとは言い難いし，電子的な世界においては，自分の安全性を確保するのに，今までより遥かに高度な知識や多くの資本が必要となる．その場合，ユーザはますます脆弱な立場に追い込まれる可能性がある．

2.2 ユーザのプライバシ

ユーザについてのプライバシの問題を考える．ここで言うプライバシとは，ある情報が第3者に盗聴・盗み見されることなく相手に伝わるという意味でのプライバシではない．問題にするのは，ユーザの個人情報が非常に安易に流出している点である．前述したローンの手続きなどの重要な取引の場合ならまだしも，アンケートなどの簡易なものによる個人情報の要求に対して，ユーザが応えることに慣れすぎてしまっている．多くのホームページや電子メールによるアンケートが個人情報収集の便利な手段として利用されている．

これまでの社会において，相手を確かめる事は現在よりもさほど難しいものではなかった．相手の声を聞き，顔を見ればよく，またその機会も確実に存在した．しかし，相手の顔もわからず，声も聞けない電子社会において，相手を確かめるのはその人が持つ固有の情報の確からしさのみである．その固有な情報には当然のことながら個人情報も含まれている．したがって，個人情報の安易な流出は成りすましの危険性を増大させる原因となりうる．

3. 提案する社会システムの目的と基本方針

一般的に社会基盤の条件として以下の項目が満たされることが必要であると我々は考えている．

- 個人と社会の双方を守るためのしくみでなければならない．(個人の権利と社会の秩序)
- しくみは単純で理解しやすいものでなければならない．(弱者にも不利にならないしかけ)
- 長期的に安定して運用が可能でなければならない．(柔軟性と拡張可能性)
- 攻撃や災害に対して強くかつ復旧が簡単に行えなければならない．(危機対応能力)
- 経済的に成り立たなければならない．(経済性)

この条件と前節の問題点を踏まえ，これから提案する社会システムの目的およびそれを達成するための基本方針を述べる．

我々の目的は

◇ 弱い立場にあるユーザを守るシステムの構築

である．現在，ユーザを保護する制度はいくつかある，クーリングオフなどはその例である．裏を返せばユーザは非常に脆弱な立場にあり，そのような制度による保護の必要性が極めて高いということにもなる．特に電子化された社会では，直感が働く余地が小さくなりがちであり，知識や資本力に劣るユーザの立場が益々弱いものとなる．我々が考える社会システムもこの点を第一に考える必要がある．

次にこの目的を達成するための基本方針として以下の点を挙げる．

⋆ ユーザにとってわかりやすい仕組み

しくみは単純で理解しやすいものでなければならない．しくみを理解すればユーザは自己責任のもとで，何をすれば自分が安全でいられるか認識することができる．

⋆ サービス提供者からの一方的な認証ではなく，ユーザもサービス提供者を認証できる双方向認証のシステム

前節において現在の社会システムがユーザとサービス提供者信用度の格差，特にサービス提供者の信用度の高さの上に成り立つシステムであると述べたが，果たして電子的な世界において，このような信用度の関係が保持されるのは難しいと考える．電子的な世界の大きな問題点はネットワークの向こう側の人間の顔が見えにくい点にある．これが成りすましなどの問題を生むのであるが，これにより例え企業や行政のような信用度の高いとされてきたサービス提供者であっても，その信用度は低下する．もちろんユーザの信用度も同様である．その場合，サービス提供者の信用度の高さゆえに成り立ってきた既存の

一方向的な認証はもはや通用せず，ユーザがサービス提供者を認証するという双方向的な認証が必要になる．

⋆ 個人情報の流出を防ぐプライバシの保護

サービス提供者はユーザに対して，個人情報の提供を求める場合が多々ある．クレジットカードの発行の際，あるいは各種会員への入会の際など，その都度個人情報の提出が必要となる．このような重要な取引の場合ならまだしも，これが成り立つのもサービス提供者は信用できて，個人情報を悪用することはないという考えに基づく．しかし電子的な世界では，サービス提供者の信用度は大きく揺らぐ．そしてもう１つ留意しなければならないのが，一旦個人情報が悪用された場合，電子的な世界では，瞬時に，広範囲に，多大な被害が起きる可能性を秘めている．名前，住所などという個人の基本的な情報は容易に変更することはできず，取り返しのつかない被害を被る可能性もある．安易な個人情報の流出を防ぐことは，弱い立場にあるユーザを保護する重要な手段である．我々が考えるプライバシの保護は，重要な情報を途中で盗み見，改竄されることを防ぐという役割ではなく，そもそも重要な情報を極力流さないで済む仕組みを意味している．

⋆ 単一方式による複数のサービスの提供と個々のサービスの独立性の確保

個人認証の方式としては，公開鍵暗号を用いる方法や指紋などのバイオメトリクスを用いる方法などが提案されている．これらはすべてユーザに対応する1つの情報を複数のサービスの提供において共用することが前提となっている．このため，この情報が破られた場合，ユーザはすべてのサービスに関して危険にさらされることになる．一人のユーザに対してすべてのサービス提供者がユーザに対する同じ情報を共有していることが問題である．現在の多くの社会システムでは，ユーザはサービス提供者に対して名前，住所，電話番号といった自分の情報を提供しなければならないし，どのサービス提供者もそういった個人情報の提供を求める．このような社会の現状が結果として個人情報の共有を生み，一つのサービス提供者から情報が漏洩した場合の多方面に渡る被害を生んでいる．

サービス提供者の信用度が低下する電子化された環境では，個々のサービス毎に異なる情報をベースとして事故が発生した場合の影響を最小限にくい止めるシステムの構築が求められる．一方，経済性や使いやすさの観点からは基本となる方式は1つに統一されていることも重要である．統一された方式でしかもユーザとサービスとの個々のリンク毎に独立した安全性を保証するシステムが必要となる．

以上のように，我々は取り組むべき問題に対しての解決法について，その目的と基本方針を提案した．次節以降はその具体化および提案手法に対する検証を行う．

4. 提案する社会システムの基本モデル

我々が提案する社会システムの基本的なモデルを述べる．このモデルには3つの主体と，PID(Personal IDentify)という一種の個人IDからなる．

3つの主体とは，ユーザ，発行者，サービス提供者である．これらは以下のように定義できる．

- ユーザ：サービス提供者と取引を行う主体．発行者に属し，PIDを発行される．
- 発行者：発行者とは，一般社会において社会的に認知された集団(社会的集団)を代表するものである．ユーザはこの集団の一員であり，発行者はユーザを保証する義務を負う．
- サービス提供者：ユーザにサービスを提供する主体．

ここで社会的集団とは，市や学校といった公共団体，企業やサークルといった私的団体を問わず，社会的に団体あるいは集団として認知された集団のことを指す．従って発行者とは，市であるなら市長，企業であるなら社長，サークルであるなら代表のことを指す．

PIDは発行者がユーザに対して発行する長いビット列である．これは各ユーザに対して固有のものである．発行者はデータベースに，ユーザはICカードなどの安全なハードウェアに保管しておく．またPIDの一部分のビット列のことをsubPID(PID Subsequence)と呼ぶ．

4.1 ユーザとサービス提供者が取引を行うまでの手順

我々が提案するシステムは最終的にはユーザとサービス提供者が安全に電子的なやり取りが行える環境を構築することである．しかしユーザとサービス提供者の2者間だけでは安全な電子サービスは実現しにくい．そこで前述した発行者というものを間に置くことで安全な電子サービスを実現する．

我々が提案する発行者は，従来のTTP(Trusted Third Party)と呼ばれる，2つの主体の間に立つ公正･中立な第三者機関(例えばPKIにおけるCA(Certification Authority)のような機関)とは大きく異なる．定義からもわかる通り，発行者とはユーザが属する集団の長である．よって発行者はユーザの権利の保護や利益の拡大を行うのが義務であり，ユーザを保護する立場にある．以下ではユーザとサービス提供者が安全に電子サービスを行うまでに踏む手順を説明する．

Step1 まず最初はユーザが発行者からPIDを取得するためのプロセスである．ユーザは自分が属する社

会的集団(あるいは自分が属したいと思う社会的集団)に対して，名前や住所といった個人情報を提供する．この情報を元に発行者はユーザの本人性を確認し，その本人に対してPIDを発行する(**Fig.1**)．発行されたPIDはユーザにはICカードなどの安全なハードウェアなどに保存して提し(以下ではICカードに保存して配布すると仮定する)，発行者側は厳重に管理されたデータベースに保存しておく．

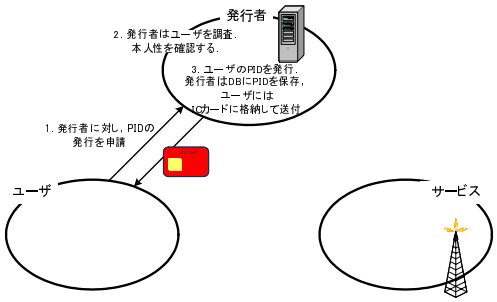

Fig.1　The process of PID issue

以上のようなプロセスにより，ユーザはPIDを取得することができた．**Fig.2**にあるように，この時点での各々の状態は，ユーザはICカードに保存された形でPIDを保持し，発行者はデータベースにユーザのPIDを保存している．サービスはこの時点では何も情報を持たない．次

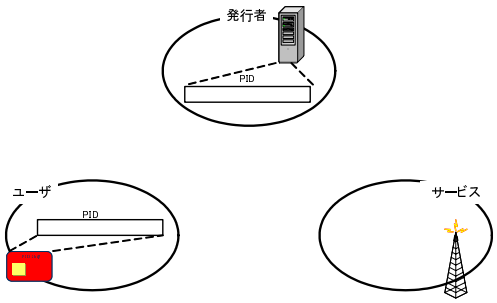

Fig.2　Standing : As of PID issue to users

はサービス提供者がユーザとサービスを行うプロセスである．まずサービス提供者は直接ユーザと取引する前に発行者に許可を得る必要がある．

Step2　サービス提供者がユーザにサービスを行いたい場合，サービス提供者はユーザの属する集団の発行者に対して，ユーザとの取引を打診する．発行者は調査の結果，このサービスがユーザに不利益をもたらさないと判断し，ユーザとの取引を認めると，サービス提供者に対してユーザのPIDの一部分を提供する．このPIDの一部分をsubPIDと呼ぶことにする．サービス提供者は発行者からはsubPID以外のユーザに関する情報は受け取ることができない．subPIDとユーザの本人性については発行者が保証するものとする(**Fig.3**)．

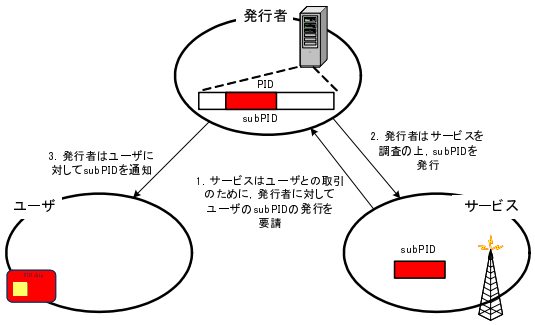

Fig.3　The process of services taking out subPID

これによりサービス提供者はユーザのsubPIDを受け取ることができた．この時点では**Fig.4**にある通り，ユーザおよび発行者はPIDを保持し，なおかつsubPIDの情報も保持している．サービス提供者は発行者から発行されたsubPID のみを保持している．

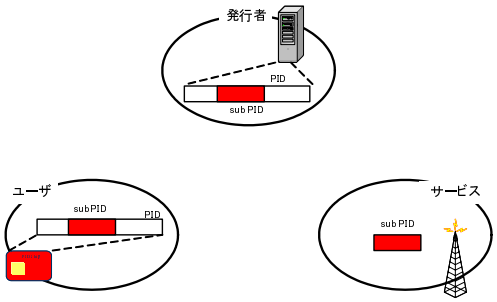

Fig.4　Standing : As of subPID issue to services

これでユーザの持つPIDとサービス提供者の持つsubPIDを用いて安全なサービスが可能になる．

ユーザから見れば，サービス提供者の安全性は発行者によってある意味で保証されている．またユーザの個人情報(住所など)はサービス提供者側に知られることはない．サービスから見れば，ユーザの信用度は発行者に依存していることになる．subPIDを用いてどのようなプロトコルで具体的なサービスの提供を行うかは，本論文の範囲外である．ワンタイムパスワードや共通鍵暗号の利用など種々の方法が考えられる．

4.2 複数のユーザ，サービス提供者が存在するモデル

現実の社会においては複数のユーザが同一のサービス提供者のサービスを受ける場合や，あるいは一人のユーザが複数のサービス提供者のサービスを受ける場合が考えられる．

4.2.1 複数のユーザが同一のサービスの提供を受ける場合

同じ発行者に属する複数のユーザが同一のサービス提供者のサービスを受ける場合(**Fig.5**)，サービスはそれぞれのユーザのsubPIDを発行者から発行してもらう必要がある．subPID 発行は各々のユーザについて前述した手順を踏んで得られる．サービス提供者は発行されたそれぞれのsubPIDを用いてサービスを行う．subPIDはユーザによって異なるので，一人のユーザのsubPIDに事故があっても，他のユーザに影響がない．

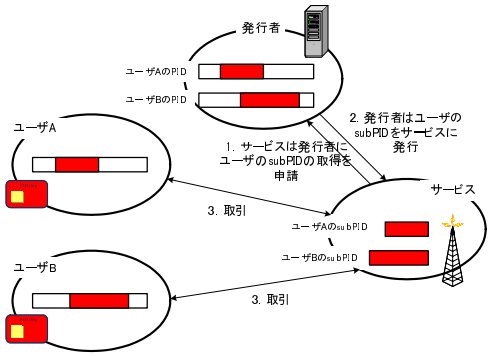

Fig.5 When two or more users receive service

4.2.2 １人のユーザが複数のサービスの提供を受ける場合

次に一人のユーザが複数のサービス提供者のサービスを受ける場合を考える(**Fig.6**)．サービス提供者側は発行者からユーザのsubPIDを取得するのは今までと変わらないが，発行者のsubPIDの発行の仕方に3つの特徴がある．これはPIDが長いビット列であるという特性に基づいている．

1つ目は，発行するsubPIDは，他のsubPIDと重複しないようにするという発行の仕方である．

PIDは長いビット列であり，subPIDはその一部分である．例えば**Fig.7**のように4つのサービス提供者にそれぞれsubPIDを提供する場合，お互いが重複しないように提供している．こうすることにより，何らかの形で一つのサービス提供者からsubPIDが漏洩しても，他のsubPIDと独立しているので他のサービス提供者のサービスに影響がでることはない．各サービス間で同一情報を用いている現在のシステム(クレジットカードなど)の場合，一つのサービス提供者から個人情報が漏洩した場合，当該

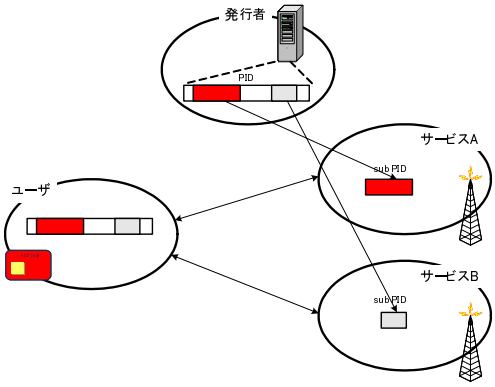

Fig.6 When one user receives two or more services

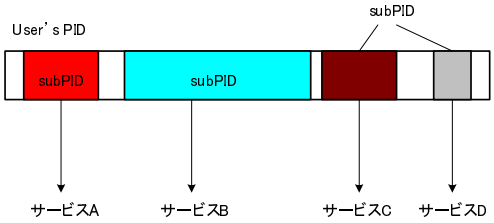

Fig.7 User's subPID assigned without overlapping

ユーザの他サービスに影響する危険は十分考えられる．一人のユーザに対してすべてのサービス提供者がユーザに対する同じ情報を共有していることが問題である．現在の多くの社会システムでは，ユーザはサービス提供者に対して名前，住所，電話番号といった自分の情報を提供しなければならないし，どのサービス提供者もそういった個人情報の提供を求める．このような社会の現状が結果として個人情報の共有を生み，一つのサービス提供者から情報が漏洩した場合の多方面に渡る被害を生んでいる．

2つ目は**Fig.8**にあるようにsubPIDの重複を許してもかまわないという発行の仕方である．重複している部分のどちらかのsubPIDが漏洩した場合，前述した重複しない場合のような安全性を得ることはできないが，簡易的なサービスを提供する場合や，同一サービス提供者の複数のsubPID取得の場合など，リスクは増えるが，簡便になり，経済性に優れるメリットもある(**Fig.9**)．

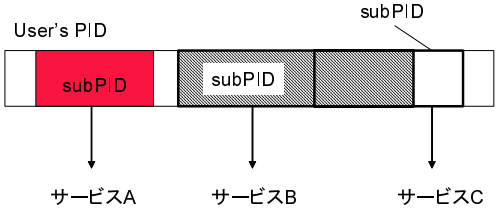

Fig.8 User's subPID assigned with overlapping

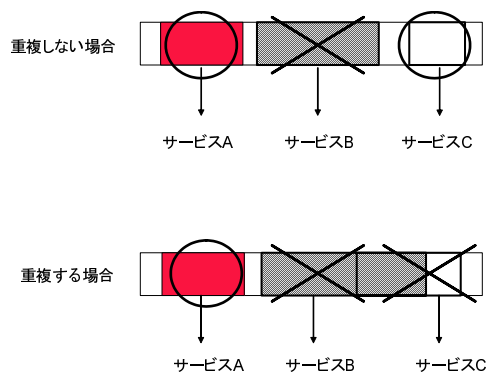

Fig.9　Comparison : User's subPID overlaps or not

3つ目は，発行するsubPIDのビット長により安全性の度合いを調節することが出来ることである．サービス提供者が安全性の高い取引を望む場合，発行者はsubPIDのビット長を長くして発行する．逆にそれほど高い安全性を求めない場合は短いビット長のsubPIDを発行する．**Fig.7**において，サービスBに対して一番長いsubPID を発行しているので図のサービス提供者の中では一番高い安全性を要求していることになる．逆にサービスDは一番安全性が低い．発行するビット長が長ければ安全性が高いという発想は短絡的ではあるが，直感的には共通鍵暗号の鍵長やワンタイムパスワードの生成などにおいて安全性を上げる余地が大きくなる．

5. 発行者について

これまで我々が提案する社会システムについての基本的な概要を述べてきた．本章では提案するシステムの大きな特徴である発行者について詳しく述べる．

発行者とは一般社会における社会的集団を代表する者であると定義した．また社会的集団とは市町村や学校，会社，組織などが考えられる．社会的集団は大きく2つに分類することができ，市や学校，企業のようにユーザが自動的に属する集団と銀行，クレジット会社，クラブなどユーザが任意に属する集団とに分けることができる (**Fig.10**).

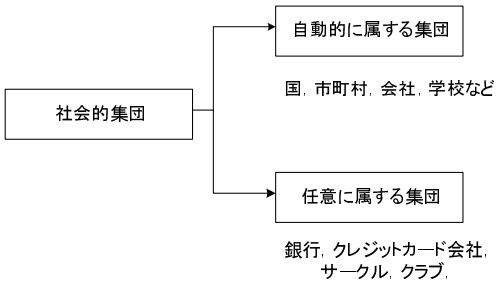

Fig.10　A social group's attribute

発行者の責任や役割について考える．発行者とは例えば市であるなら市長であり，企業であるなら社長である．ということは，発行者は集団に属する個人(本稿でいうユーザ)の権利の保護や利益の拡大を責務としなければならない．PIDにおいては具体的に発行者はどのような事を行わなければならないだろうか．

これから大きく普及する電子商取引の世界，あるいはサイバー世界の大きな性質として「匿名性」というものがある.「匿名性」とは，ネットワーク上の行為者はID，パスワード等の電子情報のみによって特定せざるを得ず，行為者の特定が困難な性質であるが，この性質によりネットワークの向こう側にいる人間が誰であるのか，信用してよいのか，といった電子商取引を行う上で障害となる大きな問題に直面する．

我々の提案では，発行者が十分にユーザの本人性を確認し，サイバー世界におけるユーザの代わりとなるPIDを発行する．しかしこれだけでは「匿名性」の解決にはならない.「匿名性」の問題点の本質は，IDやパスワードなどと，ユーザ本人の結び付きは希薄なものであり，誰でも成りすますことが可能な点にある．

そこで発行者が果たす最も重要な役割として，PIDとユーザの結び付きを発行者が保証することがある．そのために発行者はユーザに対して個人情報の提供を求める．個人情報をどこまで求めるか(名前と住所から指紋やDNAなど個人情報と言っても幅広い) は集団の性格にもよるが，いずれにしろ得られた個人情報が虚偽でないか，そして本人と対応したものであるかを十分に確認した上でPIDを発行し，外部に対してはその調査の信頼性によりユーザとPIDの本人性を保証するものとする．発行者による本人性の確認は継続的に行う必要が出てくる．

次にユーザ，サービス提供者に対してはどのような役割を背負うだろうか．各々に対して以下の点が考えられる．

＜サービス提供者に対する役割＞：各サービス提供者に対するユーザと subPID の結び付きの保証

現在の社会ではサービス提供者はユーザに対して重要な個人情報の提供を求めてきた．その情報を得ることによりサービス提供者はユーザを信用することができた．しかし提案するシステムでサービス提供者がユーザの情報として得ることができるのはsubPIDのみである．従って発行者はこのsubPIDをユーザの個人情報と同等の価値を持つ所にまで保証しなければならない．

＜ユーザに対する役割＞：サービスの選別

発行者はユーザを保護する立場にある．従って発行者はユーザにとって相応しくないと思われるサービスを排

除し，ユーザにとって安全にサービスを受けることのできる環境を整えなければならない．

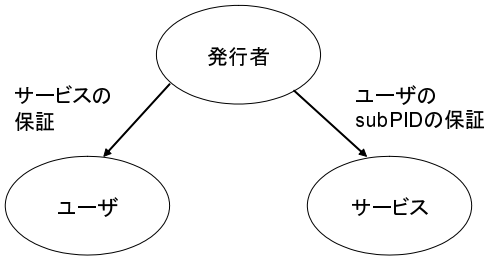

Fig.11 The duty which a publisher undertakes

5.1 ユーザの観点から見た発行者選び

次にユーザが発行者に対して求めるものについて考える．**Fig.11**において，発行者はユーザに対してサービスの保証を行うと述べた．つまり発行者は自分の安全保証範囲に見合ったサービスを選別し，それらをユーザに対して提供する．ユーザがサービス提供者に対して望むものは，ユーザにとって便利なものであり，なおかつ不当な不利益を被らないものである(ユーザにとって安全なサービスである)のは当然である．従って，そのようなサービスを揃える発行者をユーザは望むと考えられる．しかし発行者は自分の安全保証範囲に見合ったサービスを選別する．便利なサービスがユーザにとっていつも安全とは限らない．そのようなサービスは高い安全性を保証する発行者から提供されない可能性があり，それほど高い安全性を持たない発行者から提供されるかもしれない．

従って安全性の高い発行者を選ぶユーザは幅広いサービスを受けられないかもしれない．また幅広いサービスを受けようと考えるなら安全性の低い発行者を選ばなければならないかもしれない．つまりユーザにとって便宜性と安全性はトレードオフの関係にあると考えられる．ユーザが発行者を選び，自分の責任でその保証を利用することになる．

5.2 サービス提供者の観点から見た発行者選び

サービス提供者が発行者に対して求めるものは，それがサービス提供者の利益拡大につながるものであるかどうかであると考えられる．多くのユーザを抱える発行者などがそれに該当する．サービス提供者は，

- 出来るだけ大きな集団と契約を結びたい．
- 出来るだけ信用度の高いユーザ集団と契約を結びたい．
- 複数の発行者との契約による自由度の確保とリスク分散．

多くのユーザを抱える発行者と関わりを持つことは，当然多くの顧客を得ることにつながる．しかしそれにはサービス提供者自体も信用度が高くないといけない．また1人のユーザとの取引において，1つの発行者からのsubPIDを得るのではなく，複数の発行者からのsubPIDを得ると，より幅広いサービスの提供や，個々のユーザは複数の発行者から保証されているという安全面でのメリットもある．

5.3 複数の発行者が存在する場合のモデル

発行者が複数存在する場合，ユーザ，サービス提供者，発行者いずれにとってもリスクが大きく低減される．**Fig.12** は１人のユーザが3つの発行者A～CからPIDを発行され，2つのサービスA，B と取引を行う例である．

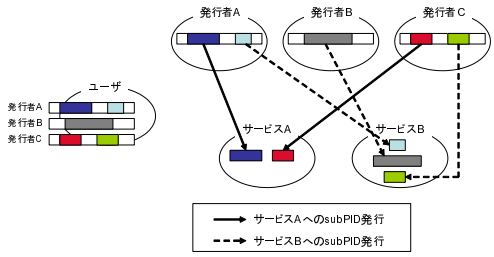

Fig.12 When two or more publishers exist

ユーザの観点から見た場合，発行者Bのセキュリティが破られPIDが漏洩した場合，発行者BからのsubPIDを受け取っているサービスBの使用はできなくなるが，サービスAには影響しない(**Fig.13**)．また，サービスAのセキュリティが破られsubPID が漏洩した場合，サービスBにおけるsubPIDとは独立しているため，サービスBは影響を受けることはない(**Fig.14**)．

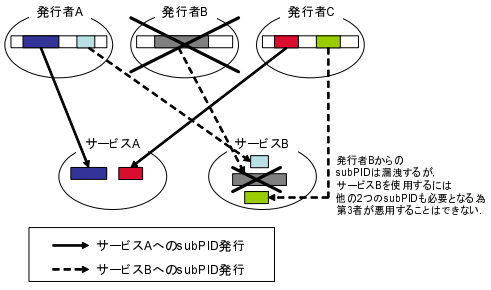

Fig.13 When publishers fail

サービス提供者の観点から見た場合，自サービスのセキュリティが破られてsubPIDが漏洩しても，他サービス提供者への影響はない．

発行者の観点から見た場合，1つの発行者がすべての

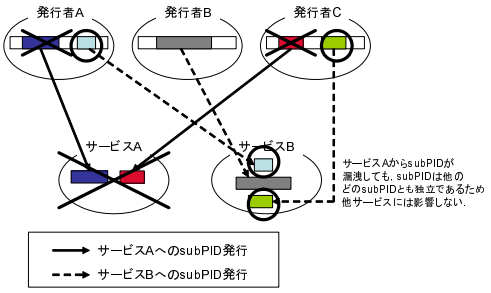

Fig.14　When services fail

PIDを発行すると，その発行者のセキュリティが破られた場合の危険性は計りしれない．しかし発行者を複数にし，なおかつユーザがサービスとの取引において，複数の発行者からのsubPID を用いるような環境であったなら，例え１つの発行者からのPIDが漏洩しても，サービスを成りすまして受けるには不充分であり，他の発行者のPIDあるいはsubPIDが必要になるため，サービスを悪用することはできない．

6. 提案する社会システムの安全性・安定性の考察

我々が提案する社会システムの安全性·安定性について考える．

6.1 PID の安全性とは

PIDが与える安全性には2つの側面があると考えられる．1つは物理的な側面であり，もう１つは情報的な側面である．

物理的な側面

1. 物理的存在を持つことによるユーザとPIDの本人性の確実化．
2. ユーザが直感的に理解しやすいしくみ．
3. subPIDを物理的に異なるハードウェアに置くことによるリスクの分散化．

PIDは長いビット列であるので，ユーザにPIDを渡す場合，ICカードのような安全なハードウェアに入れて渡すか，あるいはユーザに対して電子的に送信するかの2通りの方法が考えられる．後者の場合であるとネットワークで繋がった世界に存在する可能性が高いため，不正アクセスなどといった危険性が問題になる．したがって前者のようにICカードなどに入れてしまった方がより安全な運用が可能であると考える．

さてこのように物理的なハードウェアに格納して保管する方法は3節において述べた目的とする社会システムを構築するための手段として挙げている「ユーザにとってわかりやすい仕組み」という条件にもかなう．つまり，そのハードウェアさえ保持していれば安全であり，他人に悪用されることはないと感じることができる．特に印鑑の使用を中心としてきた我が国ではわかりやすいしくみといえる．

またsubPIDを別のハードウェアに保持することも可能である．こうすることは，現在の社会における印鑑のアナロジーをイメージしてもらうとわかりやすい．実印以外に複数の印鑑を使用することでリスクを分散している．

情報的な側面

1. 個人情報のむやみな流出を防ぐ．
2. ビット列を用いることで容易に変更が可能．
3. 発行者による双方向認証とsubPID同士による双方向認証の実現．

これまでも何度も述べてきたように，既存の社会システムはユーザに対してその都度個人に関する重要な情報を求めてきた．しかし，本システムにおいてユーザの個人情報は発行者のみが知ることになり，サービス提供者には個人情報が流出することはない．個人情報はユーザのプライバシーに関わるものである．そのような情報を開示する機会は極力少ないことが望ましい．既存の社会システムにおいて，サービス提供者側がユーザに対して個人情報の提供を求めてきた背景には，組織を守る発想が考えられる．しかし組織と個人を考えた場合，より弱い立場にいるのは個人であり，我々はその個人を守るという発想の元に成り立っている．また，PIDやsubPIDは

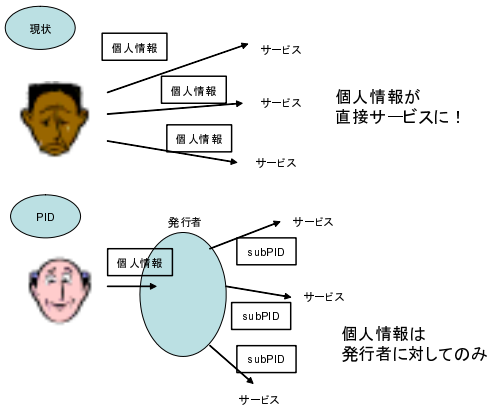

Fig.15　Comparison : The outflow of personal information

単なるビット列である．従ってこれらの情報が流出しても変更は容易であるのも大きな利点である．また発行者がPIDに対して有効期限を設けたりすることも可能になる(PIDの変更容易性)．これは3節の「個人情報の流出を防ぐプライバシの保護」という手段に該当する．

「サービス提供者からの一方的な認証ではなく，ユーザとサービス提供者を認証できる双方向認証のシステム」

について，本提案では，2重の方法でもって実現している．**Fig.16**にあるように，発行者がユーザ，サービス提供者をそれぞれ認証することで間接的ながら双方向認証を実現している点．もう一つは，ユーザはPID，サービス提供者がsubPIDというお互いしか知り得ない情報を共有している．これらを用いて双方向認証を行う方法を現在模索中である．1つのPIDをsubPIDに分けて個々のユーザ

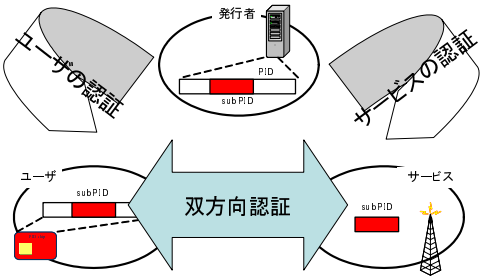

Fig.16 2-Way certification

対サービスの認証を使うことで，統一された方式が提供され，かつ個々のサービスに関する安全性の独立性が保証される．さらに複数の発行者から出されるPIDを組み合わせることによりリスクの分散もはかれる．

6.2 発行者の安全性とは

サイバー世界は顔の見えない世界である．そのような世界に対して発行者はユーザにPIDを発行することでサイバー世界における顔を与えている．

顔であるPIDのすべてのビット列をサービス提供者に渡した場合，そのサービス提供者から情報が漏洩すると，そのPIDを用いたユーザの成りすましという可能性がでてくる．しかしsubPIDをサービス提供者に渡すため，一つのサービス提供者が破綻しても，違う部分のsubPIDを使用している他のサービス提供者に影響は出ない上，PIDそのものも一部分のみが漏洩しただけであるので，その部分を変更すればよい．

では，PIDや個人情報を管理する発行者が攻撃された場合はどうであろうか?もしユーザが一つのみの発行者からPIDの発行を受け，そのsubPIDでサービスを受ける場合，発行者が攻撃されPIDが漏洩すると，成りすましが容易になり，ユーザには大きな打撃となる．そこで複数の発行者からPIDを発行してもらい，1つのサービス提供者に対して複数の発行者からのsubPIDを使用する．その場合，例え1つの発行者が破綻しPIDが漏洩しても，サービスを利用することはできないが，他人にサービスを利用されることはない．

7. 九州大学を実験場に

我々はこの提案を九州大学の新キャンパスをモデルとして実験を行うことを考えている．内容としては九州大学(厳密には九州大学学長)が発行者となり，九州大学に属する教官・職員あるいは学生を対象にサービスを提供するシステムである．

発行者は九州大学学長であり，ユーザは九州大学に属する教官・職員・学生である．ユーザには職員証あるいは学生証の形でPIDを発行する．サービスは様々な用途が考えられる．例えば**Fig.17**にあるように，成績管理，部屋の入退室管理，各種証明書の電子的な発行などである．これらは従来紙ベースで係りの人が手作業で行っていた手続きであり，電子化することにより非常に大きな作業の効率化が計れるものと思われる．また利用者にとっては，利便性の向上が望まれる．

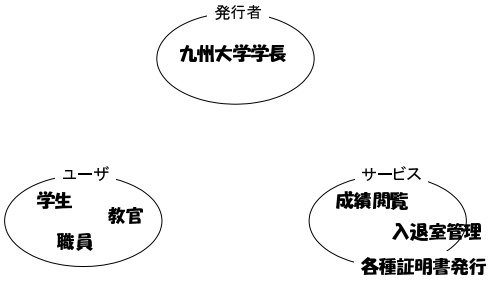

Fig.17 An example of PID use in Kyushu University

また**Fig.18**のように，例えば発行者に銀行などの金融機関を付加することにより，生協での物品購入の際のキャッシュレス化，職員証・学生証を交通機関での定期券として使用する，キャッシュカード機能など，従来の職員証・学生証の役割を越えた機能を提供することも可能である．

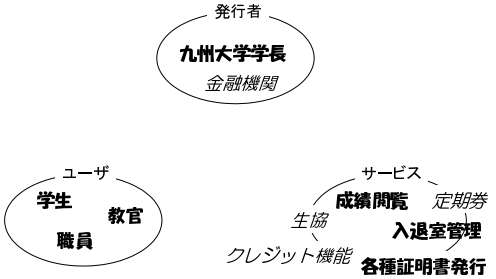

Fig.18 When financial institutions are added to a publisher

このシステムを導入することのメリットとして主に以下のことが挙げられる．

1. 個人情報および成績のプライバシーの保護

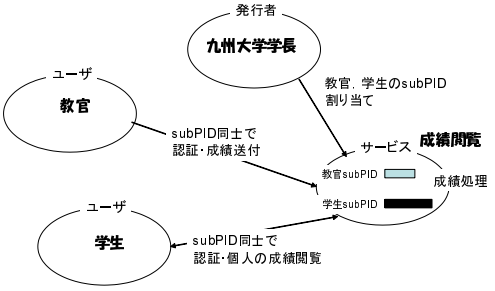

Fig.19　An example of result managements

2．成績閲覧などに関する利便性の向上
3．重要な情報を電子的に処理することが可能に
4．作業の効率化

PIDを発行する大きなメリットの１つとして個人情報のむやみな流出を防ぐことがある．教務課や生協が学生あるいは教官について得られる情報はsubPIDのみである．これは個人情報のプライバシーを守るだけでなく，内部での悪用も防ぐこともできる．

成績閲覧についてもう少し詳しく述べると(**Fig.19**)，成績とはもともと公開されるものであるが，学生や教官以外の人間もあるいは閲覧が可能な状態は好ましいとは言えない．そこでsubPIDにより学生は電子的に成績を閲覧できるようになれば，学生個人しか成績を閲覧できないようになるため，プライバシーの保護だけでなく，Web等で簡単に自分の取得した単位等を閲覧することが可能になるといった，利便性の向上にもつながる．

電子的な処理は成績閲覧に限ったことではなく，PIDあるいはsubPIDを用いることにより，従来までは安全性の問題から電子的に行うことが躊躇された処理が可能になると考えられる．

8. 技 術 的 課 題

本提案はあくまでコンセプトの提案であり，技術的アプローチは行っていない．そこで，これから必要となるであろう技術的課題を以下に列挙する．

- 基地局(リーダ)，端末(PID)用システムLSIセット開発とPIDシステムの構築
- 暗号技術，双方向認証技術の集積化と低消費電力化
- 無線通信の集積化と無線による電力供給
- 超低消費電力化技術
- 耐タンパー性の確立とテスト技術
- 安全で高信頼性を持った回路およびソフトウェアの開発技術の確立
- システム全体のセキュリティーポリシーの確立
- システム全体の低消費エネルギー化

9. お わ り に

本論文において，安全な社会システムの提案を行い，基本モデルの構築を行った．これからの課題としてはこの仕組みが，5年先，10年先の社会において安全な仕組みとして本当に有用であるか？という考察，そして複数のユーザ，サービス提供者，発行者が存在する場合の安全性の考察など課題は多い．また技術的な問題には今回は一切触れていないため，我々のシステムに沿った技術の模索，あるいは新たな技術の提案が今後必要になってくると思われる．

謝　　辞

本研究を行うにあたり，様々な角度から鋭い指摘をしてくださった，村上和彰教授，松永祐介助教授に感謝します．安浦-村上-松永研究室のセキュリティグループのメンバーである，萩原大輔氏，野原康伸氏に感謝します．物心両面に渡り支援して頂いた，当研究室のメンバー諸氏に感謝します．

本論文にて提案されているアイディアの一部は，2001年度に開催された,「超セキュリティシステム技術調査研究会」において交された議論によるものである．

この論文は平成14-18年度科学研究費補助金学術創成研究14GS0218によるものである．

参　考　文　献

1) 村田正幸; 山田英; 塚本昌彦; 塚田晃司; 星徹; 下条真司; 佐藤哲司; 名和小太郎; 篠崎彰彦; 尾家祐二：**社会基盤としてのインターネット** 岩波書店. 2001
2) 電子商取引推進委員会: *http://www.ecom.or.jp*
3) 片方善治: e-**コマースシステム技術体系** フジテクノシステム. 2001
4) Arthur E. Hutt; Seymour Bosworth; Douglas B. Hoyt: *Computer security handbook* Wiley Inc. 1995
5) 国際決済銀行 (BIS): **電子マネーのセキュリティ** ときわ総合サービス (株). 1997