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府情報工学専攻

安浦, 寛人
九州大学大学院システム情報科学研究院, 九州大学システムLSI 研究センター

出版情報：マルチメディア, 分散, 協調とモバイル（DICOMO2002）シンポジウム, 2002-07. DICOMO2002 Symposium
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 ‡

† 九州大学大学院システム情報科学府 情報工学専攻
‡ 九州大学大学院システム情報科学研究院, 九州大学システムLSI研究センター

A Proposal of Secure Information Infrastructure based on PID

Youichirou Hamasaki† Hiroto Yasuura‡

†Graduate School of Information Science and Electrical Engineering Kyushu University
‡Department of Computer Science and Communication Engineering Kyushu University,
System LSI Research Center Kyushu University

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，様々なサービスを電子的に行おうという気運が高まっている．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．

だが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。これらの技術は現状の社会システムに対して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、これからの電子的な世界において必ずしも最適なシステムではないと考える。そのような社会システムの現状を考えずして、技術のみで安全性を向上させようとすると、将来において必ず破綻をきたすと思われる。

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]．また，インターネットは開かれた技術であり，その点こそがインターネットの価値となっている．したがって，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発展とは別に取り組むべき課題も多い．

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、システムそのものを電子的な世界に沿うように最適化しようと考えた。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

これから論じる問題の前提として，我々が取り上げる社会システムは，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) の関係についてである．これは電子商取引の 1 つとして挙げられる BtoC(Business to Consumer) を考えてもらうとわかりやすい．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考えられる部分に注目した．

まず 1 つ目は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，ユーザが値段も含めて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．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．

次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と考えられる．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も考えた．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的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．

3 提案する社会システムの目的と手段

一般的に社会基盤の条件として以下の事項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手段を述べる．

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．現在世の中において，ユーザを保護する制度はいくつかあり，クーリングオフなどはそのよい例である．しかし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．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アプローチ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であるかを考えた場合，それは難しいのではないかと考える．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と思われる．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と考えられる．

⋆ **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，先ほども述べたように様々なシーンにおいてあまりにもむやみに個人情報が流出される場面が目立つ．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。しかしさきほども述べたように電子的な世界では、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十分秘めている。そうなってしまうと名前、住所などという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。我々は安易な個人情報の流出を防ぐことは，やはり弱い立場にあるユーザを保護すると考えた．従って我々が考えるプライバシの保護とは，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．

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 が登場する。

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．
- サービス：ユーザにサービスを提供する主体．サービス提供者のこと。

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個有のものである．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) と定める．

4.1 ユーザとサービス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しようと考えた．だが我々が提案する発行者とは、いわゆる 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当然である．したがって発行者は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 (図 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供し (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．

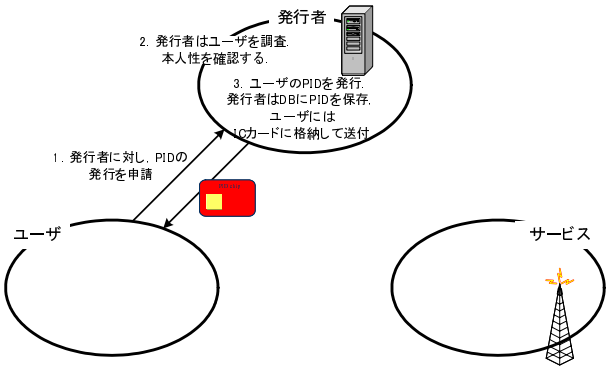

図 1: PID 発行までのプロセス

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．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.

次はサービスがユーザと電子サービスを行うプロセスである．ここでサービスが直接ユーザと取引した場合は発行者が何の意味もなさなくなる．発行者が間に入ってどのような振る舞いをするかを述べる．

Step2 サービスがユーザに電子サービスを行いたい場合，サービス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，ユーザとの取引を認めると，サービスに対してユーザの 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 (図 2).

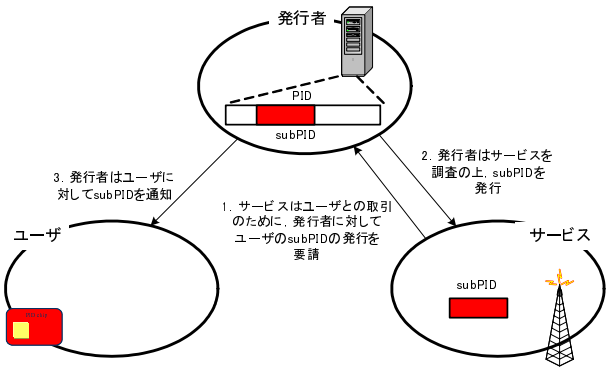

図 2: サービスが subPID を取得するまでのプロセス

これによりサービスはユーザの subPID を受け取ることができた．この時点では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．サービスは発行者から発行された subPID を保持している (図 3).

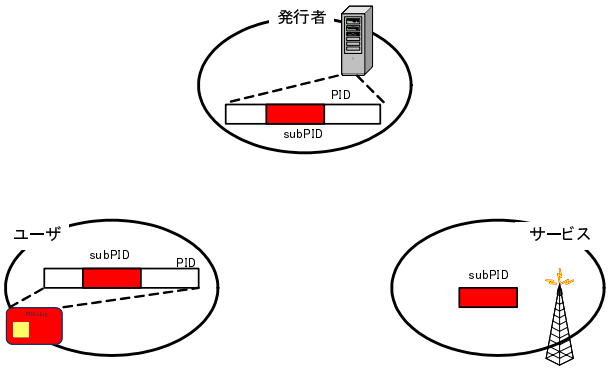

図 3: サービスに subPID が発行された時点での各々の状態

図 3 の状態において、ユーザは PID、サービスは subPID というお互いにしか知り得ない情報を共有している．この情報を利用してユーザとサービスが初めて直接的に双方向認証を行い、電子的なサービスが開始される.

5　提案モデルの考察

我々は弱い立場にあるユーザを守るシステムを構築するための手段として 3 節において以下の 3 点を挙げた.

- ユーザにとってわかりやすい仕組み
- 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
- 個人情報の流出を防ぐプライバシの保護

これが提案する基本モデルにおいて満たされているかを考える.

「ユーザにとってわかりやすい仕組み」に関して，仕組みがシンプルであるモデルを提案した．またユーザが何をすれば安全性を保てるかを判断できる仕組みという観点から見れば，ユーザは PID が保存された物理的なモノ (IC カードなどの独立したハードウェア) を大切に保管しておけば十分である．またサービス提供者に発行される subPID のみを取り出して，IC カードに保管する方法もある．この場合，PID を保存しているカードは印鑑で言うところの実印のように家に保管しておき，subPID が入っているカードを携帯してサービスとのやり取りを行う.

ユーザは今までの印鑑のアナロジーを考えればよくわかりやすい仕組みで，なおかつ安全性の判断がつきやすいと考える.

「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．図 4 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.

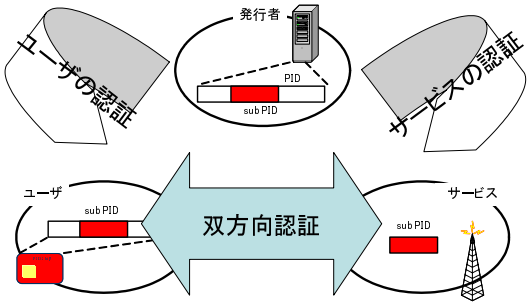

図 4: 2 重の双方向認証

「個人情報の流出を防ぐプライバシの保護」について，ユーザが個人情報を提供するのは発行者に対してのみである．サービス提供者にはユーザの subPID のみが提供される．例えば図 5 において複数のサービス提供者に subPID を発行する様子を表しているが，サービス提供者にはやはり subPID しか渡っていない.

6　まとめ

本論文において，安全な社会システムの提案を行い，基本モデルを構築を行った．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，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.

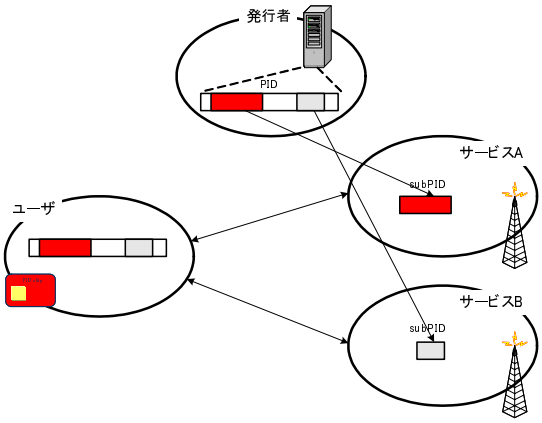

図 5: 1 人のユーザが複数のサービスを受ける場合

しかし，弱い立場にあるユーザを守る仕組みはこれからの社会において大変重要なことと考えている．この基本方針のもと，安全な社会システムの提案をこれからも行っていきたいと考えている.

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] 電子商取引実証推進協議会. http://www.ecom.or.jp

[3] 片方善治 監修. e-コマースシステム技術大系. 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