社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－GN－50　(2)
2004－ EIP －22　(2)
2004／1／15

個人情報を保護しつつ活用する方法に関する一方式

林 良一†，茂木 一男†，山室 雅司†，曽根原 登†，酒井 善則‡

消費者がサービスを受ける際、サービス提供者から氏名・住所・クレジットカード番号などさまざまな個人情報の提供を求められる。しかし、個人情報の漏洩・悪用などが非常に大きな社会問題になっている。一方、個人情報を提供することにより、消費者にとっては優待など良質なサービスの享受や、サービス提供者にとっては効率的なマーケティング手法の分析などが可能となり、個人情報の保護と活用の両立が求められている。

そこで、本研究では第三者による仲介サービスに証明書を利用した認証および契約を用いることにより成りすまし・事実否認を防止すると共に情報仲介を行う手法と、仲介する第三者を多段に組み合わせ、情報を分割することにより情報漏洩のリスクなどを軽減する手法について提案を行う。

Protection and Utilization of Personal Information

Ryoichi HAYASHI, Kazuo MOGI, Masashi YAMAMURO, Noboru SONEHARA and Yoshinori SAKAI

When a consumer receives service, the service provider asks various personal information. However, a serious social problem like improper use and leakage of the personal information by service provider is caused. On the other hand, because utilizing personal information has a merit for both a consumer and a service provider, coexisting of the protection and the utilization of personal information is desired. We propose a method of anonymous trading through the trusted third party's mediation between two persons. Moreover, we also propose a method of distributing personal information by combining more than one trusted third parties' mediation.

１．はじめに

インターネット上での経済活動が活発化する中で、個人情報の保護に関する問題が顕著になりつつある。消費者がサービス提供者のサイトにおいて商品購入や資料請求といった何らかのサービスを受けようとすると、氏名・住所・電話番号・クレジットカード番号など、様々な個人情報の提示が求められる。これらの個人情報は、サービス提供者が決済・商品の配送・顧客の販売動向の分析と言ったマーケティング処理などに主に用いられるが、単にメールサービスなどにおける会員リストとして使用されることも多く、近年、このようなサービス提供者が管理する個人情報の漏洩事件が後を絶たず、社会的な問題となっている。

一度サービス提供者に提示した個人情報の削除や不正利用、漏洩を防止することは非常に困難である。特に複数のサービス提供者に個人情報を提供した場合には、同一の個人情報が複数のリストにより管理されるため、どのサービス提供者から個人情報が流出したか特定することは難しく、個人情報の売買を防止することはできない。そのため、消費者は個人情報の提示の際に、自分自身で情報提示のメリットと情報漏洩のデメリットのトレードオフを常に考慮しなければならない。

たとえば、デジタルコンテンツ流通ネットワークの場合、コンテンツの保護を目的とするDRM (Digital Rights Management)によって、コンテンツ提供者は誰が、いつ、どんなコンテンツを視聴したかを詳細に把握することができるため、プライバシを重視する視聴者にとってはサービスを受ける際の障害となっていると考えられる。その一方で、コンテンツの流通によ

†日本電信電話株式会社 サイバーソリューション研究所
NTT Cyber Solution Laboratories
‡東京工業大学 大学院理工学研究科 集積システム専攻
Faculty of Engineering, Tokyo Institute of Technology

って生じる情報の増加により、One to One マーケティングなど CRM (Customer Relationship Management)を用いたサービスが消費者の特性やニーズに即応できるようになることから、サービス提供者および消費者の双方からの期待も大きい。

本稿では、消費者を特定することなく、決済・配送・個別化サービスの提供を実現することが可能な手法を提案する。提案手法により、消費者は個人情報の流出を心配することなく安全かつ便利にサービスを利用できると同時に、サービス提供者も従来同様の顧客情報を用いたマーケティング処理や顧客の囲い込みを行うことが可能である。

提案する手法を構成する２つの方式、“ 第三者による仲介方式 ”および“ 多段階の仲介方式 ” についてそれぞれ２章、３章で述べる。

２．第三者による仲介方式

第三者による仲介方式については、さまざまな提案[1-3]がなされているが、

1. 仲介する第三者が完全に信頼できる
2. 仲介者に情報が集中する
3. サービス提供者は、消費者の情報を入手できない
4. 成りすましや事実否認の対策などが不十分

といった問題がある。この章では、第三者による仲介方式において、3, 4 の解決方法について述べる。

2.1　三者匿名仲介方式

ここでは、証明書を用いた相互認証および書名を用いた契約を導入することで成りすましや事実否認を防止する第三者による仲介方式について述べる。認証と契約を分離することで、事実否認や架空請求などのトラブルを回避することができる。

消費者が他者と取引を行う場合、たとえば消費者がサービス提供者から商品の購入などのサービスを受ける場合を想定する。販売店では、消費者が現金で商品を購入し、商品を自身で持ち帰れば、販売店に対して個人情報を提示することなくサービスを享受することができる。しかし、クレジットカードなどの決済サービス、商品の配送、ポイントカードなどの優待サービスなどを受ける場合には、カード番号、氏名、住所、電話番号などの個人情報の提示を求められる。ただ、これらの情報はいったん提示してしまうと、提示した相手が取得した情報をどのように利用するか、提供者自身が制御することができず、法律によって保護するしかないのが現状である。そこで、図１に示すような、第三者である与信者が取引を仲介する方式を導入する。

・利用者 1, 2：互いに取引を行う主体
　たとえば、利用者 1 は消費者、利用者 2 はサービス提供者であり、オークションや P2P など個人間取引であれば双方とも消費者である。
・与信者：利用者の身元や支払能力などを担保する主体
　たとえば、銀行やクレジットカード会社(決済系)、郵便局や宅配業者(配送系)など、利用者間の決済、配送などを仲介する機関である。

2.2　取引相手からの個人情報保護方法

図 1 における取引の手順を以下に示す。

1. 利用者 1, 2 はそれぞれ与信サービスを受けるために与信者と契約を結び、与信者が利用者を識別するための ID(以下、PID)および証明書の発行を受ける。
2. 利用者は、与信者から上記 ID とは異なる取引用 ID(以下、匿名 ID)および証明書の払出しを依頼する。
3. 利用者は、お互いに PID または匿名 ID およびその証明書を相手に提示し、相互認証を行い、与信者から与信を受けていることを確認する。

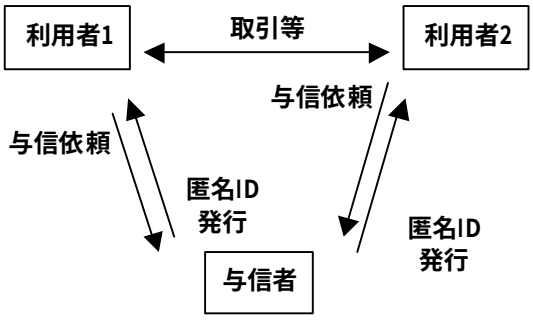

図 1　第三者による仲介取引モデル

4. 利用者は、与信者からの担保を元に取引を行う。このとき、取引内容に署名した契約書類を相手に渡すことにより、取引の正当性の確認を可能とする。
5. 与信者の代行処理が必要な場合、利用者が上記の相手の利用者の署名入り契約書類を与信者に渡し、与信者が署名の検証の後に処理を行う。

手順 1 は、クレジットカードの発行手続きに対応する。そのため、利用者は与信者に対して、与信をしてもらうのに必要な個人情報の提示を行う必要もある。プリペイドカードのように支払能力を直接担保可能な場合は個人情報の提示は必須とはならない。ID や証明書は、IC カードのような耐タンパ性や演算能力を備えた媒体に格納するのが望ましく、IC カードを利用することによりネットワークサービスだけではなく、通常のサービスにも適用が可能になる。なお、消費者は、PID は利用者の特定が可能な情報なため、発行者である与信者以外に提示してはならない。

手順 2 において、匿名 ID を用いるのは、カード番号のように一意に利用者を特定し、名寄せが行われるのを防ぐために、取引毎や取引相手毎に使い分けるためである。これは、利用者 1 が利用者 2, 3 と取引を行う場合、同じ ID を用いてしまうと、利用者 1 が誰であるかはわからないが、同一の人物であることが利用者 2, 3 にわかってしまうことを防ぐためである。上記手順では、与信者が匿名 ID を発行するが、利用者が相手に対して発行する ID を匿名 ID として与信者に登録することも可能である。与信者が発行する匿名 ID は使い捨て ID 的な利用法が、利用者が相手に発行する匿名 ID は、囲い込みを目的とした顧客 ID 的な利用法が適しているが、双方どちらの利用方法も可能である。

手順 3 において、匿名 ID を用いる利用者は消費者であり、PID を用いる利用者はサービス提供者であることが想定される。PID を用いる場合、一意に特定可能なため、プライバシ保護が困難になるため、消費者は匿名 ID を利用するが、サービス提供者は広く多くの利用者に知ってもらう必要があるため、PID を用いると考えられる。双方の利用者が消費者である場合（たとえば個人間売買）、双方が匿名 ID を用いることになる。

特定のサービス提供者用に利用する匿名 ID を用いる場合、ID の盗難を防ぐための**相互認証**が非常に重要になる。これは、本方式においてプライバシ保護を要求する利用者は非常に多くの ID を所有することになるため、ID の管理・利用方法が重要になる。特に、サービス提供者が囲い込みのために、同じ ID を用いてサービスを受ける消費者に対して優待サービスを提供している場合、同じ ID を使いまわすため、相手に応じて利用する ID を自動的かつ安全に選択する必要が生じるためである。

認証方法としては PKI のチャレンジ・アンド・レスポンス（C/R）を用いた方法たとえば SPKI[4, 5]などの利用を想定している。

相互認証の方法：

i) ある利用者 x が ID を提示して他の利用者のアクセスを待つ。
ii) 利用者 x に対してアクセスする利用者 y は、まず C/R などによって利用者 x の示す ID が正しいものであるか確認する。
iii) 利用者 y は、確認した ID に対応する自身の ID を検索し、利用者 x に提示する。
iv) 利用者 x は、C/R により利用者 y が提示した ID が正しいものであることを確認する。

以上のような手順により、利用者は取引相手に対応した ID のみが自動的に相手に提示でき、ID を盗み見られ名寄せされるのを防ぐことが可能である。

手順 4 は、**署名を用いた契約**を示しており、クレジットカードを利用した場合に行うサインに相当する。利用者 1(以下、消費者)は支払に同意したことを示すために署名を行い、利用者 2(以下、サービス提供者)は提供するサービス内容を記した書類に署名を行い交換することになる。クレジットカードにおいては、前者は支払確認のための書類(以下、支払同意書)で、後者は利用控えやレシートに相当する。

手順 5 は、決済処理などに相当する。サービス提供者は、消費者の署名入りの支払同意書を与信者に渡すことにより決済処理を依頼する。与信者は、支払同意書の署名を検証し、匿名 ID から利用者 1（PID）を特定し、決済処理を行う。

以上のような手順により、与信者が仲介することにより、利用者は互いに誰と取引をしているのか特定することなく、匿名で安全に取引が

可能となる。また、取引上において不正やトラブルがあった場合、契約書類の署名を検証することにより、誰が不正を行っているかや、どこでトラブルが起こっているかを検証することが可能である。ただし、本方法では、取引相手からの個人情報保護を目的としており、与信者にはある程度情報が集まってしまうため、与信者からの情報漏洩を防ぐことはできない。与信者からの個人情報保護方法については、３章にて述べる。

2.3　個人情報の活用方法

前節では、個人情報の保護方法について述べたが、ここではその上での個人情報活用方法について述べる。

既存の第三者による仲介方法では、消費者が与信者を介することによって匿名でサービスを享受できるが、サービス提供者等がマーケティング処理やリコメンデーションサービスなど消費者の嗜好情報を用いたサービスを行うことができない。そうなると消費者もその恩恵を受けることができなくなってしまうため、既存の第三者による仲介方式が普及しない一因になっていると考えられる。そこで、情報与信および情報縮退を組み合わせた与信者の仲介による情報活用手法を提案する。

情報与信：

匿名取引においては、匿名であるがゆえに可能になる“偽りの情報提供”を防ぐために、利用者から提供された情報が正しいことを与信者が保証すること。

情報縮退：

消費者を特定可能な情報を丸め込む(縮退する)ことにより、消費者を特定することはできないが、統計的な情報利用を可能にすること。

情報縮退の対象となる情報は、他者により証明可能であり、かつ個人をある程度特定可能な、CRM に利用する情報である。下記に例を示す。

・住所
・生年月日
・契約情報

性別など、その情報単体では個人を特定することは困難であるので情報縮退の必要は無いが、非常にレアな情報、たとえば特異な趣味嗜好といった情報は、単体である程度個人が特定可能になるため、情報縮退が必要になることもありえる。

情報縮退の方法：

1) 住所：都道府県や市区町村や郵便番号レベルまで縮退、人口単位(選挙区など)のレベルで縮退。
2) 生年月日：年齢、年齢層、誕生月に縮退。
3) 契約情報：契約内容の詳細情報を簡略化。

3)については、たとえば契約金額のみにする、商品名を商品種別として記載するなど縮退の方法は契約内容個別に検討する必要がある。

情報与信の方法：

2.2 の手順 1 において、与信者がある利用者から提示を受けた情報（住所、生年月日、性別等）を、必要があれば情報縮退した形で、その利用者の正しい情報であることを保証し、他の利用者に対して提示することにより実現する。提示方法としては以下の 2 種類ある。

1) 利用者が与信者から匿名 ID と提示する情報を記載した書類に対して与信者の署名を行ったものを受け取り、その書類を取引相手である利用者に対して提示をする。
2) 他方は取引相手の利用者が、与信者が利用者の個人情報を管理している情報サーバから、匿名 ID で指定した利用者の情報の提示を受ける。

方法 1 は与信者の署名を検証することで情報が正しいことを確認することができる。情報を提供する利用者が、取引相手にどのような情報を提示するかを決めてから与信者の署名をもらうため、利用者の提供の意思を直接反映させることができる

方法 2 は与信者から直接情報を受け取ることで、情報が正しいことが保証されることになる。方法 1 とは異なり、利用者の情報が与信者から出て行くため、利用者の意思を反映させるためには、P3P[6]や開示制御技術[7-9]などを導入する必要があるが、本方式は匿名状態で縮退した情報を提示することにより保護を行っているのであり、これら開示制御機構の導入により個人情報保護レベルが上がるわけではない。

以上のように、情報縮退を行ったあいまいな情報であっても、統計処理などのマーケティング処理にしか利用できないのではなく、与信者を介することによって匿名 ID をキーに利用者を特定可能なので、その利用者が望む範囲であればダイレクトマーケティングも可能となるので、開示制御技術との組み合わせによって、消費者およびサービス提供者の双方にとって、メリットのあるサービスの構築が可能になる。また、匿名 ID を削除することで、一度提供した情報を削除することが可能であり、消費者は ID のライフサイクルを自身で制御することで、情報のライフサイクルをコントロール（登録・削除・検索など）することができる。

3．多段仲介方式

この章では、2 章であげた問題点 1, 2 の解決方法について述べる。つまり、

1. 仲介する第三者が信頼できない
2. 仲介者に集中した情報の漏洩する可能性がある

といった問題を、複数の仲介者を介することによっての個人情報を保護する多段仲介方式について述べる。多段仲介方式としては、磯谷ら[10-12]によって信頼できるである銀行二者が決済を仲介することで、取引を行う二者のプライバシを保護する方式について提案されているが、仲介者が二社に固定されている、情報活用については考慮されていないなど問題点がある。

3.1 与信者に対する情報の保護方法

図 1 のように 1 人の与信者のみが仲介処理を行う場合、与信者が利用者 1,2 双方を特定可能であるため、与信者が誰と誰が取引を行っているか、決済処理を行う場合、金銭の流れまで把握することになり、情報漏洩などの観点から望ましくない。そこで、複数の与信者が仲介する多段仲介取引手法を提案する。これは、利用者と与信者の与信契約を、図 1 に示す三者仲介取引手法における利用者の取引として扱うことで、三者仲介取引モデルを多段階に拡張することで実現する。

3.2 基本方式

多段仲介方式の基本形として、図 2 に示す 2 つの直列に並んだ与信者が介する仲介取引の手順を以下に示す。

1.利用者 1 と与信者 2 が 2.2 節の手順 1, 2 と同様に与信者 1 と与信契約を結び、匿名 ID を払出してもらう。
2.利用者 1 と与信者 2 が 2.2 節の手順 3, 4 の取引方法により、与信契約を結び、匿名 ID を払出してもらう。
3.利用者 2 は、2.2 節の手順 1, 2 と同様に与信者 2 と与信契約を結び、匿名 ID を払出してもらう。
4.利用者 1 は、与信者 2 から払出された匿名 ID および証明書を、利用者 2 は与信者 2 から払出された PID または匿名 ID および証明書を相手に提示し、相互認証を行い、与信者 2 からの与信を受けていることを確認する。
5.利用者は、2.2 節の手順 4 と同様に与信者 2 の担保を元に取引を行う。
6.与信者 2 の代行処理が必要なときは、2.2 節の手順 5 と同様に、利用者 1 の署名入り契約書類を与信者 2 に渡すことにより代行処理を行う。
7.与信者 2 は、手順 6 で行った代行処理に付随する処理を、利用者 1 との契約内容に基づき、与信者 1 に対して要求する。

以上のような手順により、利用者同士の取引の一種として与信契約を取り扱うことで、利用者は与信者と匿名で与信契約を結ぶことが可能である。このようにして、三者仲介取引手法

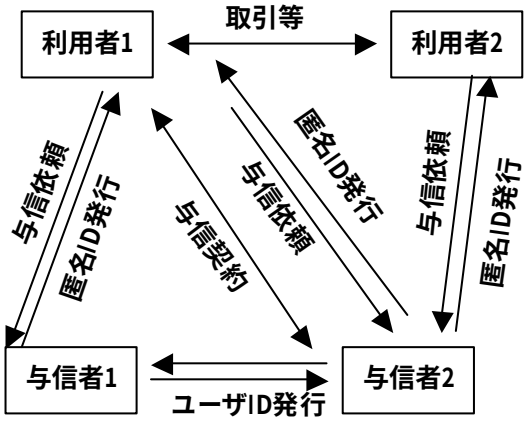

図 2　2つの与信者が介する仲介取引モデル

と同様の手順を複数組み合わせて、利用者 1, 2 の取引を 2 人の与信者が仲介することが可能になる。その結果、

1) 与信者 1 は、利用者 1 を特定することが可能であるが取引相手が誰であるかわからない
2) 与信者 2 は利用者 2 を特定することが可能であるが取引相手が誰であるかわからない

といったように図 1 の三者モデルでは与信者一人に集中していた情報が、図 2 の二段階の三者モデルでは与信者 1, 2 に分離されているため、情報漏洩などのリスクは二者に分割されるので半減する。また不正やトラブルが起こった場合、利用者等の告発に基づき、与信者 1, 2 が共同で情報を結合し、契約書類の署名検証などを行うことで、誰が不正を行っているかや、どこでトラブルが起こっているかを検証することが可能となる。ただし、この場合には利用者 1, 2 の個人情報等は保護されないことになる。つまり、与信者 1, 2 が結託した場合、情報が結合されてしまうため、与信者が結託できない、もしくはメリットが無い(デメリットがある)ようにする必要がある。たとえば、法律による規制を導入する方法なども考えられるが、次節で技術的な解決方法について述べる。

3.3 与信者が直列に並んだ仲介手法

前節で述べたように、本方式は与信者の結託に対して非常にもろいといえる。そこでさらに複数の与信者を仲介させることによって、与信者が結託する可能性および与信者からの情報漏洩リスクの軽減を図る。

図 3 は、利用者 1, 2 の取引を三者の与信者が仲介する取引モデルである。図 2 のモデルでは、利用者 2 が利用者 1 に対して一段階の仲介状態であるのに対して、図 3 のモデルは利用者 1, 2 双方が互いに二段階の仲介状態になっている。消費者とサービス提供者の取引であれば、双方の仲介段階を合わせる必要は無いと考えられるが、オークションなど個人間取引では、図 3 のように双方の利用者の仲介方式が対称であることが望ましい。このように双方合わせて三段階の仲介状態では、与信者 1, 2, 3 の三者が持つ情報を結合しなければ、完全な情報を作り出すことができないため、与信者が一者である場合に比べ情報漏洩リスクは 1/3 程度に、三者がすべて結託する可能性が $(1/2)^3 = 1/8$ 程度に軽減される。つまり、n 者の与信者が直列に並んだ場合、情報漏洩する率は 1/n 程度に、結託する率は $(1/2)^n$ 程度に軽減される。また、図４のように利用者 1 にとっての三段階の仲介状態でも双方合わせて三段階の仲介状態になるので、同様の効果を得ることができる。

仲介者を増やし、仲介段数を増やすことによって、さらにリスクを軽減できると考えられる

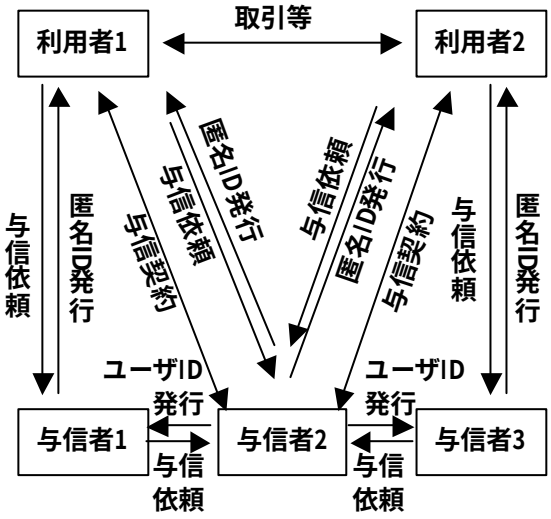

図 3 双方の利用者が複数の与信者を利用する仲介取引モデル

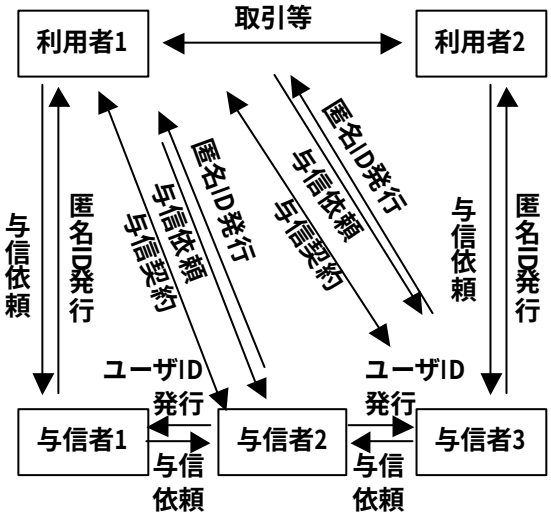

図 4 利用者 1 が三者の与信者を利用する仲介モデル

が、個人情報の分割可能数以上に仲介段階（与信者）を増やしても、情報の複製が増えるだけなので、上限は存在すると考えられる。また、仲介者の増加は、コストの増大につながるため、コストと安心度のトレードオフによって、仲介者の数が決まる。個人情報は、住所・住所・生年月日などの公的な情報、趣味嗜好情報、契約などの取引情報の３つに分割可能だと考えられるため、一人の利用者が利用する与信者の数は、３程度であろう。

3.4 与信者が並列に並んだ仲介手法

前節では、与信者が利用者間に直列に複数入り取引を仲介する手法について述べてきたが、図５では与信者が利用者間に並列に複数入り取引を仲介する手法について述べる。この場合、それぞれの利用者は独立に与信者 1, 2 と与信契約を結ぶため、与信者 1, 2 間で情報を結合することはできない。たとえば、与信者 1 が決済代行を、与信者 2 が配送代行(物流やネットワーク配送を含む)を行う場合の取引について例として示す。利用者 1(以下、消費者)が与信者 1 と個人情報を提示せず、プリペイドのような形で現金を担保に与信契約を結び、与信者 2 と氏名・住所などを提示し配送契約を結ぶ。利用者 2(以下、サービス提供者)は、与信者 1 と決済代行契約、与信者 2 と配送代行契約を結ぶ。その上で、消費者はサービス提供者と与信者 1 を介して売買契約を結び、与信者 1 が決済代行処理を行う。この契約の中で、消費者は配送方法として与信者 2 による配送代行を指定する。このような手順によって、与信者 1 は契約金額を知り、その金額がサービス提供者にわたることは知ることができるが、消費者を特定することができない。また与信者 2 は消費者を特定することができるが、金銭の流れを知ることができない。また、与信者 1, 2 は独立に与信契約を結んでいるために、互いの情報を結合することはできない。

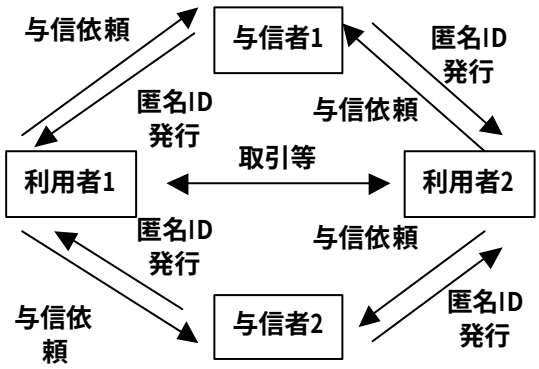

図 5　与信者を並列に用いる仲介取引モデル

以上のように、利用者間の取引に際して、取引を仲介する与信者を、直列および並列に複数・多段階に組み合わせることによって、個人情報を分割し、与信者の結託による情報復元および与信者からの情報漏洩といった問題を軽減することができる。

４．まとめ

本稿では、第三者を介することによって相手に対して匿名性を保つことで個人情報を保護する三者匿名仲介方式と、第三者を直列や並列に多段階に複数配置することにより個人情報を分割することによって、第三者による情報漏洩のリスクを軽減するとともに、情報の不正利用を困難にする多段階仲介方式により個人情報を保護しつつ活用する方法を提案した。

三者匿名仲介方式では、認証と契約を分離することにより事実否認や架空請求の防止を実現し、情報縮退および情報与信により“個人情報の保護”と“個人情報の有効な活用”の両立する仕組みの設計を行った。

多段階仲介方式により、第三者である仲介者がある程度信頼できなくても、複数の仲介者が連携することで、安全性を向上させる仕組みの設計を行った。

今後は、本方式を実現する具体的なプロトコルの設計、安全性・利便性・コストの評価方法やビジネスモデルの検討を行っていく予定である。

参考文献

(1) 特開 2002-7904, 物品配送方法、オンラインショッピング方法、オンラインショッピングシステム、サーバ、販売者サーバ
(2) 特開 2001-312606, 電子取引システムおよび電子取引方法
(3) 特開 2002-63444, 匿名による個人間取引方法及びシステム
(4) C. Ellison, SPKI Requirements, RFC2692,

1999.
(5) C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, SPKI Certificate Theory, RFC2693, 1999.
(6) W3C Recommendation: “The Platform for Privacy Preference 1.0 (P3P1.0) Specification,“ http://www.w3.org/TR/2002/REC-P3P-20020416/, 16, April 2002.
(7) 寺西、長谷川、梅本、佐藤：“ 利用制約に基づくマルチメディアコンテンツ流通システムの設計 ”、情処研報、DPS-95-6、pp.31-36、1999.
(8) 高倉、山本、難波、西田：“ 提供者の意志に基づく情報流通のための開示制御技術 ”、NTT 技術ジャーナル、Vol.14、No.10、pp.28-31、2002.
(9) 森賀、高倉、谷口、塩野入：“ コミュニティーサービスにおける共有情報の管理と活用 ”、NTT 技術ジャーナル、Vol.14、No.10、pp.46-49、2002.
(10) 磯谷、佐藤、曽根原、酒井：“ CBN における匿名決済システムの検討 ”、電子情報通信学会 2002 年総合大会、B-7-72、p.299、2002.
(11) 磯谷、佐藤、曽根原、酒井：“ コンテンツ指向ネットワークにおける販売者の匿名性を考慮した決済システムの検討 ”、電子情報通信学会 2002 年ソサイエティ大会、A-6-6、2002.
(12) 磯谷、佐藤、曽根原、酒井：“ コンテンツ指向ネットワークにおける匿名決済方法に関する検討 ”、電子情報通信学会技術報告、IN2002-55、NS2002-111、CS2002-66、13-18、2002.