2004－DPS－119　(15)
2004－EIP－　25　(15)
2004／9／3

個人情報保護・活用のための契約方式

林 良一†，茂木 一男†，山室 雅司†

消費者がサービスを受ける際、サービス提供者から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。この問題を解決するために、我々は第三者による匿名仲介方式とこの方式を多段階に組み合わせることによる情報分散を図る多段仲介方式を提案している。本稿では、多段仲介方式において、様々な契約を安全に行うことを可能とする電子署名を用いた契約方式について提案を行う。

Contract Method for Protection and Utilization of Personal Information

Ryoichi HAYASHI, Kazuo MOGI and Masashi YAMAMURO

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 have proposed a method of distributing personal information by combining more than one trusted third parties' mediation. In this paper, we propose a method of contract by using the electronic signature, which makes it possible to perform various contracts safely.

1．はじめに

オンラインサービスが普及するようになり、インターネットに接続されたサーバに様々な個人情報が蓄積されるようになったことによって、個人情報漏洩などが頻繁に生じるようになってきており、社会問題になっている。しかし、消費者がサービス提供者からオンラインで何らかのサービスを受けようとするとき、またポイントサービスなどの特典などを受けようとするとき、サービス提供者から氏名・住所・生年月日・電話番号・クレジットカード番号など、さまざまな個人情報の提示を求められる。このため消費者は、個人情報を提供することによるメリットと情報を提示する相手であるサービス提供者の信頼度や信用度に基づく情報漏洩に対するリスクをトレードオフすることによって情報を提供してサービスを受けるか、情報を提示せずサービスを受けることをあきらめるかを選択することになる。このような個人情報は、複数のサービス提供者に対して提供されており散在しているため、個人情報が漏洩した場合、どのサービス提供者から流出したか特定することは困難となるため、個人情報の漏洩や売買を防止することは非常に困難である。

これらの情報は、サービス提供者が、決済・商品の配送・顧客の購買動向の分析といったようなマーケティング処理などに用いると考えられるが、購買動向分析を効果的に行うために複数のサービス提供者が持つ顧客の行動履歴情報を寄せ集める“名寄せ”が行われ、重大なプライバシ侵害が起こる危険性がある。一方、消費者の行動履歴情報などを収集することによって、One to One マーケティングなど CRM (Customer Relationship Management)を用いたサービスは、消費者の特性やニーズに即応できることから、サービス提供者側ばかりでなく消費者側からも期待されている。

以上のような問題点を解決するために、我々

†日本電信電話株式会社 サイバースペース研究所
NTT Cyber Space Laboratories

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で、消費者のプライバシを保護しつつ、サービス提供者もこれまで同様に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などが可能な方式として、第三者による匿名仲介とこの三者仲介方式を多段階に組み合わせることにより情報を分散する多段仲介方式[1]の提案を行ってきた。本稿では、多段仲介方式において、仲介サービスを行う第三者がある程度信頼できない場合にも、取引を安全に行うための契約方式について提案する。

2．多段仲介方式

本章では、参考文献 1 にて提案を行っている三者匿名仲介方式および多段仲介方式の概要について簡単に説明する。

2.1　三者匿名仲介方式

三者匿名仲介方式とは、図 1 に示すように、利用者 1 と利用者 2 が取引を行う際に、与信者が仲介することにより、互いにまたは一方の利用者が匿名の状態で安全に取引する方式である。匿名で取引を行いたい利用者は、名寄せされないように取引相手または取引毎に異なる匿名 ID を用いて取引を行う。認証は PKI を用いた相互認証を用いることで匿名 ID の盗難を防ぐ。ここで、消費者がオンラインショッピングなどを行う場合を例に説明する。消費者（利用者 1）は、カード会社（与信者）からクレジットカードに相当する匿名 ID を複数発行してもらう。消費者は、匿名 ID を提示してオンラインサイト(利用者 2)にて商品の購入を行う。決済および配送は匿名 ID および電子署名によって与信者を仲介して行うため、利用者１は一切、個人情報を出すことなく利用者 2 から商品の購入を行うことが可能となる。一方、サービス提供者（利用者 2）が顧客の販売動向調査などのマーケティング処理を行う場合、消費者から個人情報を縮退（個人を特定不可能なレベル：たとえば住所→居住地域）したものを提供してもらい、処理を行うことで匿名状態のまま従来のマーケティング処理が可能となり、個人情報の保護と活用を両立が実現される。利用者 1 が望むのであれば匿名 ID をキーに与信者を仲介することでダイレクトマーケティングも可能である。

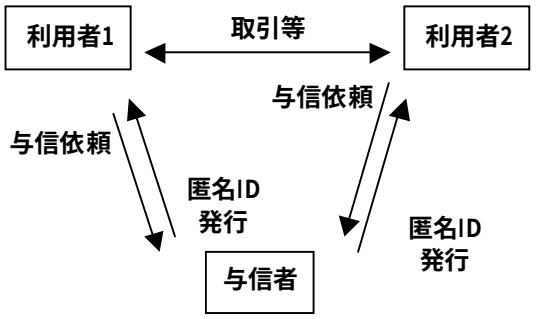

図 1　第三者による匿名仲介取引モデル

2.2　多段仲介方式

多段仲介方式とは、図 1 のような三者匿名仲介方式を、図 2 および 3 のように多段階に組み合わせることにより、与信者の知りうる情報を分割することによって、与信者からの情報リスクを分散する方式である。図 3 は、三者匿名仲

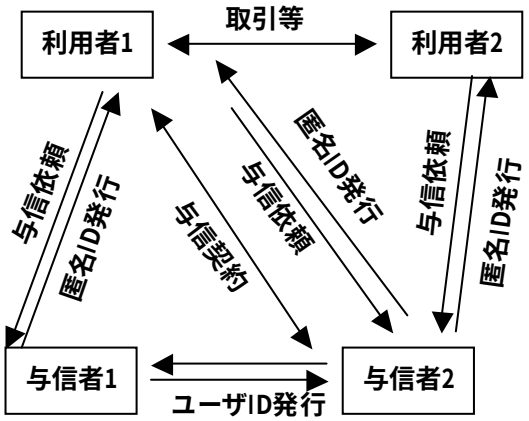

図 2　２つの与信者が介する仲介取引モデル

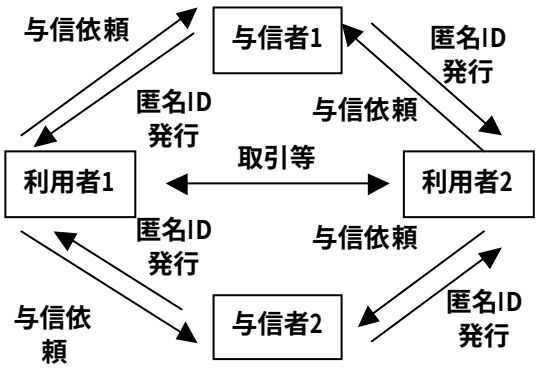

図 3　与信者を並列に用いる仲介取引モデル

介方式を直列に組み合わせた例であり、同一レイヤの仲介処理を分割することが可能である。図 3 は、並列に組み合わせた例であり、別レイヤの仲介処理を分割することが可能である。たとえば、消費者（利用者 1）とサービス提供者（利用者 2）の間の商品売買の決済代行を与信者 1，2 が図 2 のように直列に入り仲介する場合、与信者 1 は消費者が誰であるかはわかるがサービス提供者が誰であるかわからない、与信者 2 はサービス提供者が誰であるかはわかるが、消費者が誰であるかわからない、といったように与信者 1，2 の間で決済金額などの情報は共有するが、利用者の行動履歴情報を分割することになる。また、与信者 1 が決済系、与信者 2 が配送系として図 3 のように並列に仲介する場合、与信者 1 は金融情報を持ち、与信者 2 は物流情報を持つという具合に情報を分割することになる。このように与信者を直列や並列に組み合わせて配置することにより、適切に情報を保護しつつ、情報を収集・活用することが可能である。

3．契約方式

多段仲介方式において、匿名で安全に取引を行うには、“ 代金を支払ったのにサービスを受けられない ”や“ サービスを提供したのに代金を受け取れない ”といったトラブルが起きた際に、誰が不正を行っているかを追跡できる必要がある。この章では、電子署名を用いた契約方法について述べる。

3.1 匿名 ID 発行プロトコル

この節では、契約を行う際に用いる匿名 ID の発行方法について述べる。匿名 ID は、図 4 のように利用者から一番近い与信者が、利用者を認証する主 ID から木構造的に広がっている。与信者は、ID の管理者であり、与信者が利用者を認識するときに用いる ID（上位 ID）と与信者自身または取引相手の利用者（または下位の与信者）が発行する匿名 ID（下位 ID）との関連を保証する。この関連付けを与信者が利用者に無断で行えないようにするために、一つ上位の与信者が、ID の関連付けを確認できるような匿名 ID 発行プロトコルで、下位の与信者の不正を防止する。

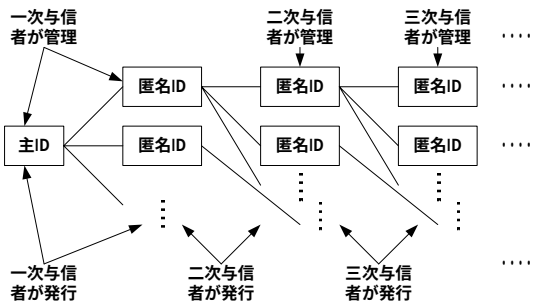

図 4　匿名 ID の関係

記号説明
ID　　:主 ID または匿名 ID
SK　　:秘密鍵
PKC　:公開鍵および ID を含んだ証明書
ID[a, b] :a=発行者、b=利用者
SK, PKC の[a, b]は、ID に対応
r：上位 ID、t：下位 ID を現す。
与信者の ID 等の発行者 y は上位与信者も含む
初期条件
与信者 :ID[y, y], SK[y, y], PKC[y, y]
利用者 1:与信者用:ID[y, r1], PKC[y, r1], SK[y, r1]
利用者 2:与信者用:ID[y, r2], PKC[y, r2], SK[y, r2]
　　匿名 ID:ID[y, t2], PKC[y, t2], SK[y, t2]
をそれぞれ所有

3.1.1 与信者が匿名 ID を発行する方法

この節では、与信者が、利用者 1 の匿名 ID 発行要求に応じて匿名 ID を発行する手順について図 5 を用いて説明する。

1. 利用者 1 が、与信者に ID[y, r1]でログインし、匿名 ID の発行を依頼する。必要があれば、利用者 1 は、発行依頼書に SK[y, r1]で署名、与信者は、発行依頼書を保存。
2. 与信者は、必要があれば発行依頼書の署名を検証し、次いで匿名 ID：ID[y, t1]を発行して、利用者 1 に送付する。必要があれば、匿名 ID 発行書に SK[y, y]で署名する。
3. 利用者 1 は、必要があれば匿名 ID 発行書の署名を検証し、次いで ID[y, t1]用の鍵ペア PK[y, t1]および SK[y, t1]を生成する。
4. 利用者 1 は、ID[y, t1]用の公開鍵 PK[y, t1]を与信者に登録する。鍵登録依頼書には SK[y, r1]により署名を行う。
5. 与信者は、鍵登録依頼書の署名を検証する。
6. 与信者は、利用者 1 の情報として鍵登録依頼

書を保存する。

7. 与信者は、ID[y, t1], PK[y, t1], ID[y, y], PK[y, y]のほか与信の範囲、有効期限などを記した証明書 PKC[y, t1]を生成する。この証明書はSPKI[2, 3]のような証明書である。
8. 与信者は、利用者1の情報として匿名ID：ID[y, t1]および証明書 PKC[y, t1]を登録する。
9. 与信者は、利用者 1 に証明書 PKC[y, t1]を交付する。
10. 利用者 1 は、証明書 PKC[y, t1]の署名を確認し、記録媒体等に保存する。
11. 利用者 1 は、ID[y, t1]および PKC[y, t1]を用いて利用者 2 にログインする。

なお、ログイン時などの認証については、参考文献 1 にて述べられている相互認証に基づいて行う。

以上のように、手順 6 にて保存を行った利用者 1 の上位 ID 用秘密鍵 SK[y, r1]による署名のある鍵登録依頼書が無ければ、与信者は匿名 ID の登録ができない、また利用者 1 の上位 ID および匿名 ID 秘密鍵を知らないため、与信者が利用者 1 に成りすまし匿名 ID を生成したり、後述する契約行為を行ったりすることはできない。

3.1.2 利用者が匿名 ID を発行する方法

この節では、利用者 2 が、利用者 1 の匿名 ID 発行要求に応じて匿名 ID を発行する手順について図 6 を用いて説明する。

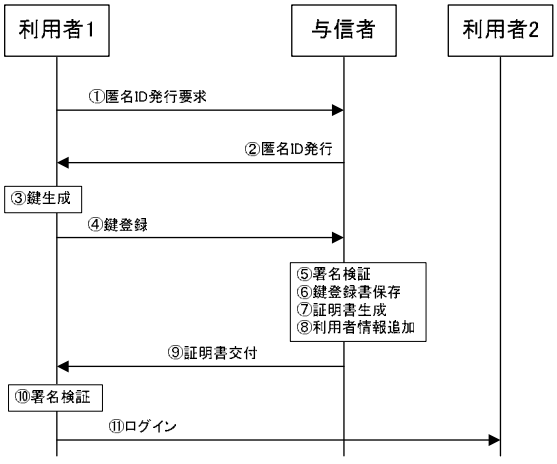

図 5 与信者が匿名 ID を発行する手順

記号の説明

x：利用者 2 が利用する ID を識別
r2 または t2 を表す

1. 利用者 1 が、ログインせずに（何も情報を出さずに）利用者 2 に匿名 ID 発行要求を行う。
2. 利用者 2 は、匿名 ID：[x, t1]を発行して、利用者 1 に送付する。必要があれば、匿名 ID 発行書に SK[y, x]で署名する。
3. 利用者 1 は、必要があれば匿名 ID 発行書の署名を検証し、次いで ID[x, t1]用の鍵ペア PK[x, t1]および SK[x, t1]を生成する。
4. 利用者 1 は、ID[x, t1]用の公開鍵 PK[x, t1]を与信者に登録する。
5. 利用者 2 は、ID[x, t1], PK[x, t1], ID[y, x], PK[y, x]のほか与信の範囲、有効期限などを記した証明書 PKC[x, t1]を生成する。この証明書はSPKI[2, 3]のような証明書である。
6. 利用者 2 は、顧客情報として匿名 ID：ID[x, t1]および証明書 PKC[x, t1]を登録する。
7. 利用者 2 は、利用者 1 に証明書 PKC[x, t1]を交付する。
8. 利用者 1 は、証明書 PKC[x, t1]の署名を確認し、記録媒体等に保存する。
9. 利用者 1 は、与信者に ID[y, r1]でログインし、匿名 ID：ID[x, t1]および証明書 PKC[x, t1]の登録依頼を行う。登録依頼書には、SK[y, r1]で署名を行う。

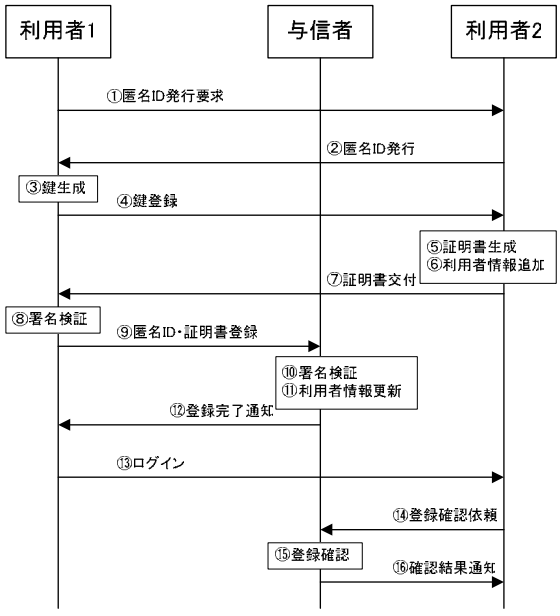

図 6 利用者が匿名 ID を発行する手順

10. 与信者は、登録依頼書の署名を検証する。
11. 与信者は、利用者 1 の情報として登録依頼書を保存して、ID[y, r1]の匿名 ID として、ID[x, t1]および証明書 PKC[x, t1]を登録する。
12. 与信者は、利用者 1 に匿名 ID の登録が完了したことを通知する。
13. 利用者 1 は、ID[x, t1]を用いて利用者 2 にログインする。
14. 利用者 2 は、ID[y, r2]を用いて与信者にログインして、ID[x, t1]の登録状況確認を依頼する。
15. 与信者は、顧客情報から ID[x, t1]を検索して ID[y, r1]（利用者 1）を特定する。次いで、PKC[x, t1]内の発行者 ID が ID[y, r2]もしくは ID[y, t2]（つまり利用者 2 の ID）であるか確認する。
16. 与信者は、ID の登録の有無を通知して、登録があれば ID[x, t1]（つまり利用者 1）の与信の範囲、契約期限（上位 ID の有効期限または仲介期限）などを通知する。

以上のように、手順 11 で保存を行った利用者 1 の上位 ID 用秘密鍵 SK[y, r1]による署名のある登録依頼書が無ければ、与信者は匿名 ID の登録ができない、また利用者 1 の上位 ID および匿名 ID 秘密鍵を知らないため、与信者が利用者 1 に成りすまし匿名 ID を生成したり、後述する契約行為を行ったりすることはできない。

3.2 契約プロトコル

この節では、匿名 ID 用秘密鍵を用いた電子署名による契約手順について述べる。

記号の説明

z：利用者 1 が利用する匿名 ID の発行者を識別　y または x（r2 または t2）

1. 利用者 1 が、利用者 2 に ID[z, t1]でログインしてサービスの提供を依頼する。
2. 利用者 2 は、顧客：ID[z, t1]に対して提供しているサービスリストを送信する。
3. 利用者 1 は、受信したサービスリストから受けたいサービスを選択する。
4. 利用者 1 は、選択したサービスを発注書の形で送信する。発注書には、必要に応じて ID[z, t1]を含め、SK[z, t1]により署名を行う。
5. 利用者 2 は、必要に応じて署名確認を行ってから発注書に応じた見積書、請求書を作成する。この見積書は、利用者 2 の ID;ID[y, x]、伝票番号、サービス明細および有効期限などの情報を含み、SK[y, x]にて署名を施したものであり、請求書は、ID[y, x]、伝票番号、請求金額などの情報に SK[y, x]にて署名を施したものである。
6. 利用者 2 は、利用者 1 に見積書および請求書を送付する。
7. 利用者 1 は、受信した見積書および請求書の署名を検証して、サービス明細および請求金額等を確認する。
8. 利用者 1 は、見積書および請求書に同意して、サービスを享受する場合、請求書に対して SK[z, t1]にて署名を行った支払同意書を利用者 2 に送付する。
9. 利用者 2 は、受信した支払同意書の署名を検証して、SK[y, x]にて署名を施した受領書を作成する。
10. 利用者 2 は、受領書を利用者 1 に送付する。
11. 利用者 1 は、受領書の署名を検証する。

この段階でサービス授受契約は成立したことになる。以下は、決済などの代行処理であり上記手順とは非同期であってかまわない。

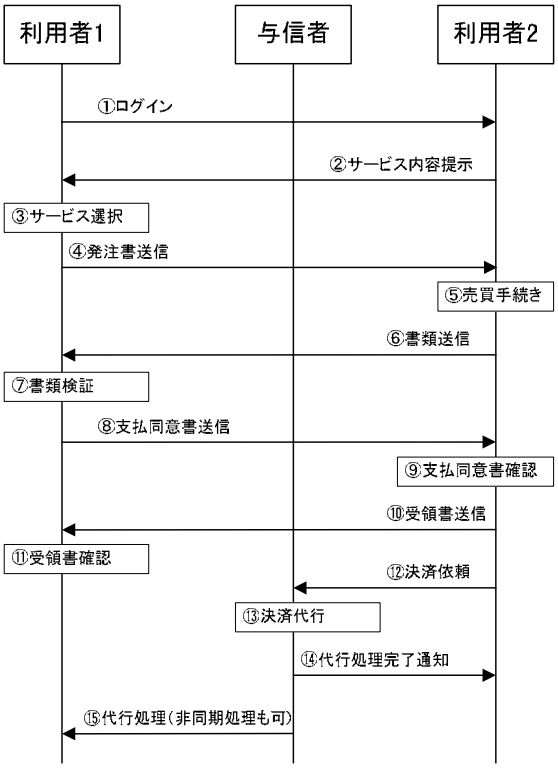

図 7　契約処理手順

12. 利用者 2 は、与信者に ID[y, r2]でログインして、手順 9 にて受信した支払同意書を送信し代行処理の依頼を行う。
13. 与信者は、支払同意書の署名の検証、請求者の ID が利用者 2 の ID かどうか確認を行い、代行処理を行う。
14. 与信者は、利用者 2 に代行処理の官僚を通知する。
15. 与信者は、利用者 2 から依頼を受けた代行処理を利用者 1 に対して行う。この代行処理は、利用者に対して直接かもしくは、上位の与信者に対して行うことになる。手順 12-14 とは独立に非同期であってもかまわない。

以上のような手順により、署名による書類を保存しておくことで、利用者間で“対価を払ったのにサービスを受けられない”や“サービスを提供したのに対価を受け取れない”といったトラブルが起こった場合、互いに署名入り書類を与信者に提示することで、どちらに非があるか突き止めることができる。

図 2 のように与信者が直列に仲介している場合、手順 15 にて与信者が上位の与信者に対して手順 12-14 の代行処理依頼を行うことになる。この際、与信者が利用者 1 に請求書を発行して利用者 1 の署名を施した支払同意書を受け取ってから上位の与信者に代行処理を依頼する方法と、利用者 1 の支払同意書を入手せずに直接上位の与信者に代行処理を依頼する方法がある。前者の場合、利用者 1 が定期的に与信者と契約処理を行う必要があるが、不正の発生は防げる。後者の場合、定期的な処理は必要ない代わりに、不正請求などが起こる可能性がある。不正が行われた際には、利用者 1 の告発により仲介した与信者すべてが、関連した情報の名寄せをして利用者 2 との署名検証まで行うことにより、どこで不正が行われたか検証可能になるが、名寄せされプライバシ情報が与信者に対して明らかになるという問題がある。

3.3 情報与信プロトコル

与信者が利用者に対して行うサービスは、名寄せ防止のための匿名 ID によるサービス、事実否認などのトラブル防止のための電子署名による契約を用いた代行サービスのほかに、参考文献 1 でも述べているように利用者の情報が真の情報であることを他の利用者に対して保証する情報与信サービスがある。この節では、情報与信の詳細な手順について述べる。

情報与信の流れは、図 8 に示すように、上位の与信者経由で入手した利用者 1 の与信された情報を利用者 1 から提供を受けた与信者が、利用者 1 がその与信済み情報の一部を利用者 2 に提供する際に、情報が正しいことを保証するといったように、上位から下位に与信済み情報の一部が流れていく形になっている。ただし、最上位の与信者については、現状の与信情報確認方法、たとえば郵便を用いた本人確認や公的証明書の提出などによって情報の確認を行う必要がある。利用者 1 が与信者経由で利用者 2 に与信済み情報を提供する方法は、与信者の署名を用いた方法とアクセス制御を用いた方法の 2 通りが考えられ、後者は与信者に蓄積する情報に対してアクセス制御ポリシ[4]を設定する方法と、利用者 1 が作成した情報アクセス権を利用者 2 に提供する方法の 2 通りが考えられる。以下では、この 3 通りの与信情報提供方法の手順について説明する。

図 9 に与信者の署名を用いた情報与信の手順を示す。なお、下記の手順において必要があれば、契約プロトコルに基づいて書類に署名を行うものとする。

1. 利用者 1 が、与信者に ID[y, r1]を用いてログインし、情報を提供する相手（利用者 2）用の ID：ID[y, t1]と与信を希望する情報の種類を含んだ情報与信依頼書を送付する。

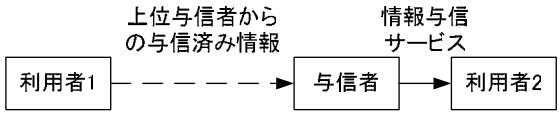

図 8 情報与信の流れ

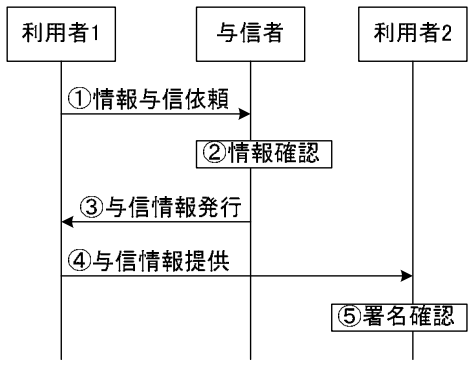

図 9 与信者の署名を用いた情報与信手順

2. 与信者は、受信した情報与信依頼書の確認を行う。（ID が利用者のものか、依頼された情報が与信済み情報として上位与信者経由で取得しているかを確認）
3. 与信者は、ID[y, t1]と与信する情報を含んだ与信情報書に対して、SK[y, y]にて署名を行い利用者 1 に送付する。
4. 利用者 1 は、与信情報書の署名を確認後、利用者 2 に ID[y, t1]を用いてログインし、与信情報書を提示する。
5. 利用者 2 は、受信した与信情報書の署名を確認し、与信者が情報の内容を保証している情報であることを確認する。

次に、図 10 を用いて情報アクセス制御ポリシを用いた情報与信の手順について示す。

1. 利用者 1 は、与信者に ID[y, r1]を用いてログインし、ID[y, t1]の利用者 2 に提供したい情報に関するアクセス制御ポリシを、“ ID[y, x]に対して開示 ” などと設定を行う。この設定を利用者 1 が与信者に依頼する際に、必要があれば、前述の契約行為を用いる。
2. 与信者は、利用者 1 からの設定要求の確認を行う。（契約行為であれば署名確認、利用者 1 および 2 の ID 確認、与信する情報が与信済みかどうか）

下記は、非同期の手順になる。

3. 利用者 2 は、与信者に ID[y, r2]を用いてログインし、ID[y, t1]の情報取得要求を行う。
4. 与信者は、ID[y, t1]から利用者 1 の情報を読み込み、アクセス制御を行う。（ID[y, t1]の要求された情報に対するアクセス制御ポリシに、ID[y, r2]または ID[y, t2]に対して開示に設定されているかどうか確認する。）
5. 与信者は、利用者 2 に対して利用者 1 の情報を、ID[y, t1]の与信済み情報として提供する。利用者 2 は、与信者から直接情報を入手することで、与信者により情報の内容が保証されることになる。

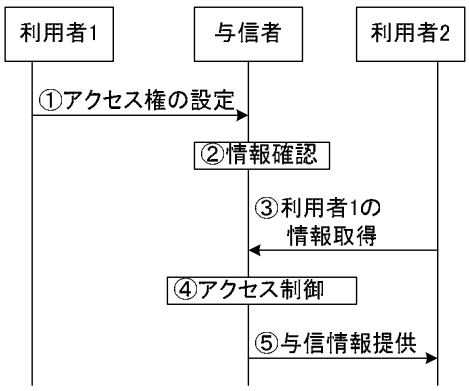

図 10　ポリシを用いた情報与信手順

最後に、図 11 を用いて情報取得件を用いた情報与信の手順について示す。

1. 利用者 1 が、利用者 2 に対して与信者から情報を取得する権利を記述した書類：情報取得権を生成する。この書類には、情報所有者 ID[y, t1]と権利者 ID[y, x]と提供する情報の種類を含み SK[y, t1]による署名が施されたものである。
2. 利用者 1 は、利用者 2 に ID[y, t1]を用いてログインし、上記の情報取得権を利用者 2 に提供する。
3. 利用者 2 は、受信した情報取得権の署名および内容を確認する。
4. 利用者 2 は、ID[y, r2]を用いて与信者にログインし、情報取得権を送信し、情報の取得を要求する。
5. 与信者は、受信した情報取得権の署名および内容を確認する。（ID[y, t1]というユーザの有無、権利者 ID が利用者 2 のものであるか、提供する情報は、与信済みの情報であるか）
6. 与信者は、利用者 2 に対して利用者 1 の情報を、ID[y, t1]の与信済み情報として提供する。利用者 2 は、与信者から直接情報を入手することで、与信者により情報の内容が保証されることになる。

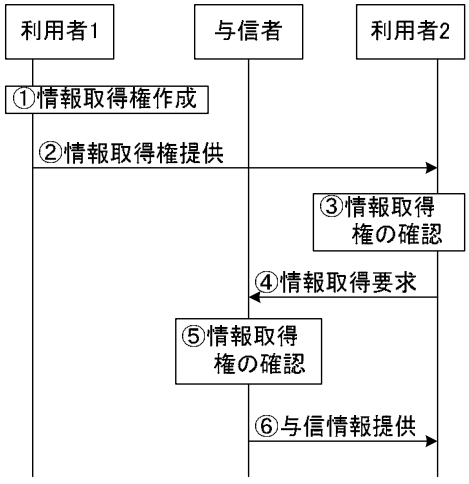

図 11　情報取得権を用いた情報与信手順

以上のような手順によって、サービス提供者（利用者 2）が消費者（利用者 1）の情報を、多段仲介方式の匿名状態であっても正しく入手することができ、質の高いマーケティングデータの分析が可能となる。

ただし、3 通りの情報与信の手順について述べてきたが、それぞれ長所短所があるためシステム設計の際には注意が必要である。

４．まとめ

本稿では、多段仲介方式における匿名 ID 発行手順により、仲介者である与信者がある程度信頼できない場合でも、不正を行うことができないような仕組みの実現方法について提案を行った。また、電子署名を用いた契約手順により、事実否認等によるトラブルを検証可能な仕組みについて提案を行った。さらに、情報が正しいことを仲介者が保証する情報与信の方法について提案を行った。これらの仕組みを多段仲介方式に適用することで、個人情報を適切に保護しつつ活用可能な便利で安全なプラットフォームを構築することができる。

今後は、本方式の安全性・利便性の評価方法の検討を行っていく予定である。

参考文献

(1) 林，茂木，山室，曽根原，酒井：“ 個人情報を保護しつつ活用する方法に関する一方式 ”，第 22 回 情報処理学会 電子化知的財産・社会基盤研究会,EIP-EIP22-2,Jan.2004

(2) C. Ellison, SPKI Requirements, RFC2692, 1999.

(3) C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, SPKI Certificate Theory, RFC2693, 1999.

(4) 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.