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

2008－DPS－134 (1)
2008－CSEC－ 40 (1)
2008／3／6

プライバシー保護と個人単一IDを両立する認証基盤の提案

吉井 大介　安倍 広多　石橋 勇人　松浦 敏雄
大阪市立大学大学院創造都市研究科

インターネット上のオンライン・サービスの多くが，ユーザの登録時に厳密に個人を特定することなくユーザ固有のIDを与え，匿名アクセスを許している．そのため，匿名性を利用し，オンライン・サービスの運営者（プロバイダ）や，他のユーザへ被害を与えるような不正行為を行う者がいる．一人で複数のIDを取得できる限り，こうしたユーザを締め出すことは難しい．この対策として，ユーザのIDを厳密に一つに限定すること（個人単一ID）が考えられるが，既存の方法はその実現にユーザの個人情報を必要とするため，プライバシー保護の観点から望ましくない．そこで本論文では，信頼できる認証機関による第三者検証によって個人単一IDを実現する認証基盤を提案する．プロバイダに個人情報を提出する必要はなく，また，同一ユーザでもプロバイダが異なればIDが必ず変化するようにすることでプライバシー保護を図っている．

A Proposal of Authentication Infrastructure Which Satisfies both Privacy Protection and Strictly Unique ID per User

Daisuke Yoshii　Kota Abe　Hayato Ishibashi　Toshio Matsuura
Graduate School for Creative Cities, Osaka City University

Many online services on the Internet give users an ID without strictly identifying the user, which enables users to access the service anonymously. Therefore, under the cover of anonymity, some malicious users perform illegal act which damages online service providers and/or other users. It is difficult to shut out such users as long as you can acquire multiple IDs. While it is possible to restrict users to have exactly one single ID, existing methods to achieve this require user's privacy information, which is not desirable for privacy protection. In this paper, we propose authentication infrastructure which restricts users to have single IDs, imposed through third party verification by a trusted certificate authority. As users do not have to submit their privacy information and have different IDs for different service providers, user's privacy is protected.

1　はじめに

昨今，インターネット上の掲示板や，ソーシャルネットワーキングサービスなどのオンライン・サービスの多くがユーザの登録時に厳密に個人を特定することなく，ユーザ固有のIDを与え，匿名アクセスを許している．そのため，匿名性を利用し，オンライン・サービスの運営者（以下，プロバイダ）や，他のユーザへ被害を与える行為（誹謗中傷，詐欺など）を行う者がいる．一人で複数のIDを取得できる限り，こうしたユーザを締め出すことは難しい．

各プロバイダがユーザの氏名や住所などの個人を特定する情報を要求することで，ユーザが複数のIDを取得できないようにする（**個人単一ID**）ことは可能である．しかし，個人情報を提出することはプライバシー保護の観点から望ましいことではなく，またプロバイダにとっても個人情報の管理は負担である．このため，プロバイダに個人情報を提出せずに個人単一IDを実現できる認証基盤が望まれる．ただし，個人単一IDを実現する際，ユーザのIDが複数のプロバイダで共通だと，複数のプロバイダ同士が結託して所持するIDを照合するとユーザの行動履歴が明らかになってしまう（**結託可能性**）ことに注意する必要がある．

本論文では公開鍵基盤技術を利用して信頼できる認証機関による第三者検証を行うことで，

個人単一 ID を実現しつつ結託可能性を排除する認証基盤の実現方式を提案する．

2 既存研究と事例

本節では，個人単一 ID に関する関連事例，および，結託可能性の排除についての既存研究について紹介する．

2.1 個人単一 ID に関する関連事例

個人単一 ID の実現のためには，自動車運転免許証などの身分を証明する情報を要求する方法が一般的である．

それ以外の方法としては，例えば Yahoo!オークションでは参加資格を得るために，自分名義のクレジットカード，もしくはオフィシャルバンクの口座番号を登録する必要がある．これらの情報と，Yahoo!オークションの ID を対応付けることで本人性を確認している．また，ソーシャルネットワーキングサイトの mixi は，携帯電話の個体識別番号を登録させることで個人単一 ID の実現を図っている．

しかし，どちらもクレジットカードや携帯電話を複数用意すれば，その数だけ ID を得ることができる．また，同じクレジットカード番号や個体識別番号を複数のプロバイダが保持していると，結託可能性が発生する．

2.2 結託可能性の排除

結託可能性を排除するためには，複数のプロバイダの情報を照合しても同じユーザに結びつかないようにする必要がある．そのためには，ユーザが各プロバイダに提示する情報をそれぞれ違うものにして，情報の関連を取れないようにすることが要求される．

結託攻撃に耐性のある属性認証用電子署名方式 [1] では，属性証明書への署名を，生成する証明書ごとに変えることで属性証明書同士の関連が取れない属性証明手法を提案している．しかし，属性証明書は匿名のままサービスを利用する権利などの属性を証明するものであり，ユーザを特定する ID としては利用できない．

また，ユーザのプライバシー保護を考慮した総合的な認証基盤の研究として，信頼できる第三者による中央集約型の認証を核としたセキュアサービスプラットフォーム [2][3] (以下，SSP) がある．SSP では，認証基盤が発行した利用者の SSP へのログイン ID と，任意の情報を連結して暗号化したものを，サービス対応 ID として発行している．この任意の情報として各プロバイダが持つ公開情報などを対応させれば，プロバイダ毎に違う ID が発行されるため，結託可能性を排除できる．しかし，何らかの障害により認証基盤が利用できない場合，プロバイダに異常はなくともユーザはサービスを利用できなくなるという問題がある．

3 提案方式の概要

本論文では，以下の要件を満たす方式を提案する．

匿名性 ユーザはプロバイダに匿名で登録し，サービスを利用できる．

個人単一 ID の実現 同じプロバイダのサービスを利用するための ID を一つに限定する．

結託可能性の排除 複数のプロバイダが持つユーザの情報を照合しても，異なるプロバイダでの同じユーザの ID を関連付けることはできない．

追跡可能性 認証機関によって定められた手順を踏むことで，悪質なユーザを特定できる．また，必要に応じて各プロバイダにそのユーザの ID を通知できる．

サービスの可用性 何らかの原因で認証機関が停止しても，各プロバイダでの認証には支障がない．

なりすましの排除 第三者が他のユーザになりすますことはできない．

3.1 概要

本節では提案方式の認証基盤の概要を述べる．認証基盤の参加者には，プロバイダ，ユー

ザ，そして信頼できる第三者である認証機関が存在する．また，参加者はそれぞれ自分の公開鍵と秘密鍵のペアを保有する．

プロバイダは認証基盤上でサービスを提供するため，認証機関へ登録を行う．認証機関はプロバイダが提出した情報を十分に確認し，公開情報である**プロバイダ公開 ID** を発行する．一方，ユーザも同様に認証機関への登録を行い，認証機関はユーザの本人性を十分に確認し，ユーザを特定するためのユーザ ID（**認証機関用非公開 ID**）を発行する．

ユーザがサービスを利用する際にはまず，その利用したいサービスのプロバイダへ登録を行う．ユーザは認証機関から発行された認証機関用非公開 ID と，プロバイダ公開 ID を組み合わせて，登録するプロバイダだけで用いる ID（**サービス対応 ID**）を自ら生成し，プロバイダへ登録申請を行う．サービス対応 ID は，ユーザとプロバイダの組み合わせによって異なるため，サービス対応 ID から結託可能性は発生しない．

プロバイダは，登録を申請したユーザが認証機関に登録済みのユーザであるかを確認するため，サービス対応 ID の検証を認証機関に依頼する．認証機関に登録済みのユーザであることを確認できれば，プロバイダはユーザを自身のデータベースなどに登録する．

以後，ユーザがサービスを利用するときは，認証機関とやり取りをすることなく，ユーザとプロバイダ間で認証を行う．

プロバイダは，登録しているユーザによるサービスの悪用を発見した場合，そのユーザのサービス対応 ID を認証機関に報告することができる．認証機関は通報されたユーザのサービス対応 ID からユーザを特定し，各プロバイダへそのサービス対応 ID を通知する．

3.2 既存事例との差異

提案方式が第 2 節で紹介した既存事例と異なる点は，信頼できる認証機関を導入することでユーザがプロバイダに個人情報を提供しなくても個人単一 ID を実現でき，またユーザの ID はプロバイダごとに異なるため，結託可能性が生じないという点である．

SSP との違いは，プロバイダに登録済みのユーザがサービスを利用するための認証は，認証機関を介さずユーザとプロバイダ間で完結する点である．これにより，認証機関が何らかの原因で停止しても，サービスの提供が直ちに止まることはない．

4 提案方式の詳細

4.1 語句の定義

- **認証機関用非公開 ID**：認証機関がユーザを特定するために発行する非公開 ID
- **プロバイダ公開 ID**：認証機関がプロバイダに発行する，プロバイダを識別するための公開 ID
- **サービス対応 ID**：ユーザがプロバイダに登録する際，認証機関用非公開 ID とプロバイダ公開 ID から生成するサービスを利用するための ID
- **検証情報**：プロバイダがユーザから受信したサービス対応 ID を，認証機関に検証してもらうために生成する情報
- **サービス対応公開鍵/サービス対応秘密鍵**：ユーザが各プロバイダとの間で用いる公開鍵/秘密鍵（プロバイダ毎に異なる）

4.2 記号の意味

- U_i：ユーザ $i\,(i:1\ldots m)$.
- S_j：プロバイダ $j\,(j:1\ldots n)$.
- C：認証機関.
- UID_i：C が U_i に発行した非公開 ID.
- SID_j：C が S_j に発行した公開 ID.
- $\mathrm{STI}_{(\mathrm{U}_i,\mathrm{S}_j)}$：$\mathrm{UID}_i$ と SID_j から生成するサービス対応 ID.
- $\mathrm{V}_{(\mathrm{U}_i,\mathrm{S}_j)}$：$\mathrm{S}_j$ が U_i の $\mathrm{STI}_{(\mathrm{U}_i,\mathrm{S}_j)}$ を検証するために，C に送信する検証情報.

- $\mathrm{PK}_x/\mathrm{SK}_x$: x の公開鍵/秘密鍵.
- $\mathrm{PK}_{(\mathrm{U}_x,\mathrm{S}_y)}/\mathrm{SK}_{(\mathrm{U}_x,\mathrm{S}_y)}$: ユーザ x がプロバイダ y との通信時のみ利用する，サービス対応公開鍵/サービス対応秘密鍵.
- $\mathrm{SIG}_{SK_x}(\mathrm{X})$: SK_x を使って，データ X に電子署名を施したもの.
- $\mathrm{E}_{PK_x}(\mathrm{X})$: 公開鍵暗号方式における鍵 PK_x を使って，データ X を暗号化したもの.

4.3 設計

4.3.1 サービス対応 ID の生成方式

本提案方式では文献 [3] を参考に，ユーザ U_i はプロバイダ S_j に対して登録時に次のようにサービス対応 ID $\mathrm{STI}_{(U_i,S_j)}$ を生成する.

$$\mathrm{STI}_{(U_i,S_j)} = \mathrm{E}_{PK_C}\left(\mathrm{SIG}_{SK_{U_i}}(\mathrm{UID}_i) \| \mathrm{SID}_j\right)$$

ただし，$\|$ は連結，$\mathrm{E}_{PK_C}()$ は認証機関の公開鍵による暗号化，$\mathrm{SIG}_{SK_{U_i}}()$ はユーザ i の秘密鍵による署名を示す.

サービス対応 ID は認証機関の公開鍵で暗号化して生成されるため，認証機関と ID を生成するユーザ以外はサービス対応 ID からユーザとプロバイダとの対応関係を知ることは困難であり，匿名性を確保できる．また，認証機関は自身の秘密鍵でサービス対応 ID を復号することにより認証機関用非公開 ID を得られるため，生成したユーザを特定できる.

同一のユーザとプロバイダの組み合わせでは，常に同じサービス対応 ID が生成されるため，個人単一 ID を実現できる.

プロバイダ公開 ID は各プロバイダごとに異なるため，あるユーザのサービス対応 ID はプロバイダごとに異なるものが生成される．これにより，結託可能性の排除を実現する．また，認証機関用非公開 ID にはユーザの秘密鍵で署名を行っているため，認証機関が署名を検証することによって，悪意の第三者によるなりすましを検知できる.

4.3.2 プロバイダおよびユーザの認証機関への登録

プロバイダ S_j およびユーザ U_i が認証機関 C に登録する手順を図 1 に示す.

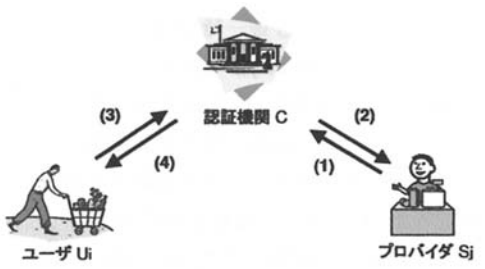

図 1 プロバイダとユーザの認証機関への登録

プロバイダ，ユーザ，認証機関はそれぞれ自分で生成した公開鍵および秘密鍵のペア $(\mathrm{PK}_{S_j}, \mathrm{SK}_{S_j})$，$(\mathrm{PK}_{U_i}, \mathrm{SK}_{U_i})$，$(\mathrm{PK}_C, \mathrm{SK}_C)$ を持っている．認証機関は PK_C を公開している.

S_j は PK_{S_j} を含む，認証機関が定めた登録に必要な登記簿などの情報を C に提示する (図 1 の (1))．C は，S_j の登録を認めるとプロバイダ公開 ID SID_j を発行し (図 1 の (2))，SID_j に対応付けて PK_{S_j} をデータベースなどに記録する.

U_i も同様に，PK_{U_i} を含む必要な情報を，C に提示する (図 1 の (3))．C はその本人性を十分に確認し，かつ，二重登録でないことを確認すると，認証機関用非公開 ID UID_i を発行し (図 1 の (2))，UID_i に対応付けて PK_{U_i} をデータベースなどに記録する．なお，ユーザは自身の公開鍵を認証機関にのみ公開すればよい.

4.3.3 ユーザのプロバイダへの登録

認証機関 C に登録が完了したユーザ U_i がプロバイダ S_j へ登録する手順を述べる．この手順は，以下の三つの処理に分割される.

(1) ユーザのプロバイダへの登録申請
(2) プロバイダによる認証機関へのサービス対応 ID の検証依頼

(3) プロバイダとの認証時にのみ用いる，ユーザのサービス対応鍵ペアの生成

図 2 に手順の概略を示す．

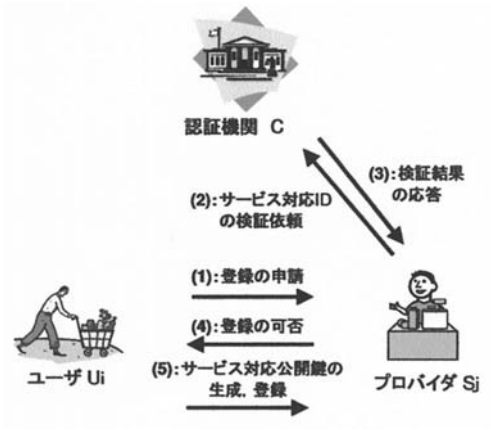

図 2　ユーザのプロバイダへの登録申請

U_i は PK_C，PK_{S_j}，SID_j を予め入手しておく．

(1) U_i はサービス対応 ID $STI_{(U_i,S_j)}$ を生成し，S_j に送信する (図 2 の (1))．S_j は多重登録の確認のため，自身の管理しているサービス対応 ID の一覧と照合する．受信した $STI_{(U_i,S_j)}$ と一致するものがあれば，そのユーザは多重登録である．

(2) S_j は，$STI_{(U_i,S_j)}$ に SK_{S_j} で署名した検証情報 $V_{(U_i,S_j)}$ を生成して，C に送信する (図 2 の (2))．

$$V_{(U_i,S_j)} = SIG_{SK_{S_j}}\left(STI_{(U_i,S_j)}\right)$$

C は S_j の登録時に取得した PK_{S_j} によって $V_{(U_i,S_j)}$ に施されている S_j の署名を検証する．$STI_{(U_i,S_j)}$ を自身の秘密鍵 SK_C で復号することで，$SIG_{SK_{U_i}}(UID_i)$ および U_i が登録しようとしているプロバイダの ID SID_j を得ると，以下の検証を行う．

a　UID_i に施されている署名を，U_i の公開鍵 PK_{U_i} を用いて検証する．これは，悪意の第三者による認証機関用非公開 ID の推測攻撃を防ぐためである．

b　サービス対応 ID に格納されている SID_j と，検証依頼のあったプロバイダの SID_j が一致しているかを検証する．これは，U_i は SID_j に対応したサービス対応 ID を生成しているかを確認するためである．

これらの検証を行い，どちらか一方についてでも正当性を確認できなければ NG 報告を，両方の正当性が確認できれば OK 報告を S_j に返信する (図 2 の (3))．

S_j は $STI_{(U_i,S_j)}$ の検証結果が NG 報告であれば，U_i の登録を拒否する．一方，OK 報告であれば，U_i の登録を了解し，$STI_{(U_i,S_j)}$ を U_i のサービス対応 ID として記録する (図 2 の (4))．

(3) S_j への登録の了解を受けた U_i は，登録した S_j と通信時のみに使うサービス対応公開鍵 $PK_{(U_i,S_j)}$ と秘密鍵 $SK_{(U_i,S_j)}$ のペアを生成し[*1]，$PK_{(U_i,S_j)}$ を S_j に送信する (図 2 の (5))．

S_j は，$PK_{(U_i,S_j)}$ を U_i の $STI_{(U_i,S_j)}$ に関連付けてデータベースに保存して，U_i の S_j への登録処理がすべて完了する．なお，サービス対応公開鍵は，対応するプロバイダにのみ公開する．

4.3.4　ユーザ-プロバイダ間の認証プロトコル

ユーザ U_i がプロバイダ S_j に登録完了後に，サービスを要求する際の認証プロトコルを説明する．

*1 プロバイダとの認証に利用する鍵（以下，サービス対応鍵）は共通鍵方式ではなく，公開鍵方式で生成する．共通鍵方式で生成したサービス対応鍵をユーザとプロバイダで共有する場合，悪意の第三者にプロバイダが管理するユーザのサービス対応 ID と，サービス対応鍵の対応関係を知られると，容易にそのプロバイダに登録するユーザになりすますことができるためである．

U_i は S_j に，$STI_{(U_i,S_j)}$ を提示してサービスの提供を要求する．S_j はこれを受けて，以下に述べるようにチャレンジレスポンス方式で認証を行う．(1) $STI_{(U_i,S_j)}$ に対応付けて保存している，$PK_{(U_i,S_j)}$ で乱数 R を暗号化した $E_{PK_{(U_i,S_j)}}(R)$ を生成して，U_i に送信する．(2) U_i は $SK_{(U_i,S_j)}$ で $E_{PK_{(U_i,S_j)}}(R)$ を復号し，R を入手する．(3) この R を PK_{S_j} で暗号化した $E_{PK_{S_j}}(R)$ を生成し，S_j に返信する．(4) 最後に，S_j が PK_{S_j} で $E_{PK_{S_j}}(R)$ を復号して得られた R' が，U_i に送信した R と一致すれば認証成功とする．

4.3.5 悪質なユーザの報告

プロバイダ S_j はあるユーザ U_x を悪質なユーザと判断すると，$STI_{(U_x,S_j)}$ を認証機関 C に報告することができる．C は，必要と判断すれば $STI_{(U_x,S_k)}$ を生成し，他の $S_k(k:1\ldots n, k\neq j)$ へ通知する．

5 考察

本章では提案方式について考察する．

匿名性 4.3.1 で述べたとおり，プロバイダや第三者がサービス対応 ID からユーザの特定はできない．

個人単一 ID の実現 4.3.1 で述べたとおり，同一のユーザが同一のプロバイダに登録する限り，必ず同じサービス対応 ID が生成されることになる．したがって，プロバイダは登録ユーザのサービス対応 ID を参照するだけで，多重登録であるかどうかを確認でき，個人単一 ID を実現できる．

結託可能性の排除 4.3.1 で述べたとおり，同一ユーザが生成したサービス対応 ID でも，各プロバイダが保有する値は必ず異なる．したがって，サービス対応 ID からの結託可能性は発生しない．

ユーザの公開鍵，および，サービス対応公開鍵からの結託可能性は，4.3.3 で述べたとおり発生しない．

追跡可能性 4.3.1 で述べたとおり，認証機関だけは必要に応じてサービス対応 ID からユーザを追跡できる．

サービスの可用性 既にプロバイダに登録したユーザとプロバイダ間での認証手続 (4.3.1 参照) では認証機関を必要としない．このため，何らかの原因で認証機関が停止していても，既に登録したユーザはサービスを利用することが可能である．

なりすましの排除 4.3.1 で述べたとおり，認証機関用非公開 ID にユーザの秘密鍵による署名を行うことでなりすましを排除できる．

6 おわりに

本論文では，信頼できる認証機関を導入することでユーザがプロバイダに個人情報を提供しなくても個人単一 ID を実現でき，また同一のユーザでもプロバイダごとに ID が異なるようにすることで結託可能性が生じない認証基盤を提案した．

提案方式では，各プロバイダがユーザを登録するたびに認証機関が検証する必要があるため，認証機関の負荷が高い．これを軽減することは今後の課題である．

参考文献

[1] 山中晋衛. 結託攻撃に耐性のある属性認証用電子署名方式. *SCIS 2007 The 2007 Symposium on Cryptography and Information Security Sasebo, Japan*, pp. 23–26, 2007.

[2] 高田治, 鍛忠司, 星野和義, 藤城孝宏, 手塚悟. B-7-16 セキュアサービスプラットフォームにおける認証モデルの一検討 (b-7. 情報ネットワーク, 通信 2). 電子情報通信学会総合大会講演論文集, Vol. 2005, No. 2, p. 170, 2005.

[3] 渡辺龍, 窪田歩, 田中俊昭. B-7-20 セキュアサービスプラットフォームにおけるプライバシー保護のための ID 管理方式 (B-7. 情報ネットワーク, 通信 2). 電子情報通信学会総合大会講演論文集, Vol. 2005, No. 2, p. 174, 2005.