シングルサインオンから独立した認可基盤とプライバシー保護

池田, 大輔
九州大学大学院システム情報科学研究院

中村, 徹
九州大学大学院システム情報科学府

大石, 哲也
九州大学大学院システム情報科学研究院

井上, 創造
九州工業大学大学院工学研究院

出版情報：電子情報通信学会技術研究報告. WI2-2009, pp.1-6, 2009-10. 電子情報通信学会
バージョン：
権利関係：

社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

シングルサインオンから独立した認可基盤とプライバシー保護

池田　大輔† 　中村　徹†† 　大石　哲也† 　井上　創造†††

† 九州大学大学院システム情報科学研究院　〒 819–0395 福岡市西区元岡 744
†† 九州大学大学院システム情報科学府　〒 819–0395 福岡市西区元岡 744
††† 九州工業大学大学院工学研究院　〒 804–8550　北九州市戸畑区仙水町 1-1
E-mail: †daisuke@inf.kyushu-u.ac.jp, oishi@ar.is.kyushu-u.ac.jp, ††toru@c.csce.kyushu-u.ac.jp,
†††sozo@mns.kyutech.ac.jp

あらまし　複数サービス向けの認証や認可システムには個人情報や属性情報が集中する上に，どのサービスをいつ利用したかという履歴も残るため，これらのシステムに対するプライバシー保護は重要である．本稿では，プライバシー保護を可能にしつつ，複数のサービスに対する認証及び認可機能を提供するシステムを提案する．まず，認証や認可における必要な情報を議論し，プライバシー保護に必要な要件を抽出する．次に，この要件を満たす認証認可システムを提案する．提案システムでは情報は分散され，個人特定ができないようする．さらに，プライベート情報検索と呼ばれる技術を応用し，認証局等に対し，誰の認証が行われているかを秘匿しつつ認証や認可を行うことを可能にする．
キーワード　シングルサインオン，認証，認可，プライバシー保護，プライベート情報検索

Privacy Protection of an Authorization System Independent from an SSO System

Daisuke IKEDA†, Toru NAKAMURA††, Tetsuya OISHI†, and Sozo INOUE†††

† Faculty of Information Science and Electrical Engineering, Kyushu University　744 Motooka, Nishi-ku, Fukuoka, 819–0395 Japan
†† Graduate School of Information Science and Electrical Engineering, Kyushu University　744 Motooka, Nishi-ku, Fukuoka, 819–0395 Japan
††† Faculty of Engineering, Kyushu Institute of Technology　1-1 Sensui-cho, Tobata-ku, Kitakyushu, 804–8550 Japan
E-mail: †daisuke@inf.kyushu-u.ac.jp, oishi@ar.is.kyushu-u.ac.jp, ††toru@c.csce.kyushu-u.ac.jp,
†††sozo@mns.kyutech.ac.jp

Abstract　A system for authentication or authorization maintains log data which records when someone uses some service, in addition to personal information, and therefore privacy protection for such a system is mandatory. In this paper, we develop an infrastructure system which provides authentication and authorization functions to multiple services, protecting privacy of users of the services. After deriving requirements for the privacy protection, we develop the system satisfying the requirements. In the proposed system, because information is divided into different subsystems, it is difficult for such a subsystem to identify an individual. The proposed system also utilizes Private Information Retrieval to prevent a subsystem identifying an individual who request an authentication process.
Key words　Single Sign-On (SSO), Authentication, Authorization, Privacy Protection, Private Information Retrieval

1. はじめに

インターネットやイントラネット上において多くの IT サービスが利用可能になり，利用者は様々なサービスを利用可能になってきた．サービスの増加に伴い，サービスごとにログインする手間や ID/パスワード等の認証情報を管理する繁雑さが問題になってきている．逆に，サービス提供者は独自に ID や対応する検証情報（パスワード等）を維持管理しなければなら

ず，これにかかるサービス提供者のコストが大きな負担となっている．

これらに対する解決策として，シングルサインオン（SSO）の枠組みが提案されている．SSO を用いれば，利用者は同じ SSO の管理下にあるサービスであれば，一度の認証手続きでどのサービスも利用することができ，1 組の ID と検証情報を管理するだけでよい．また，サービス提供者も独自に検証情報を管理する必要がなくなる．

SSO において認証を行う組織あるいはシステムを**認証局（*IdP*）**と呼び，IdP を利用するサービス提供者を**サービスプロバイダ（*SP*）**と呼ぶ．IdP におけるセキュリティ対策は重要であり，デバイスを用いたり PKI を用いたりしてセキュリティを強化する研究もある [1]〜[3]．しかし，個人の ID と，この ID がいつどのサービスで使われているかを示す履歴が集中しているという意味で，プライバシー侵害につながり得る情報が蓄積していることにも注意を払うべきである．さらに，OpenID [4] や Shibboleth [5] といった SSO の規格では，認証だけでなく，どの情報に誰がアクセスしてよいかというアクセス制御を実現するために，IdP が個人の属性情報を提供することも考えられている．つまり，単なる ID 情報だけでなく，より詳細な情報まで IdP に集中することになり，より一層のプライバシー保護が求められるようになる．

本稿の目的はプライバシー保護を可能にしつつ，認証や認可システムを複数のサービスに提供できる仕組みを提案することである．このために，以下の 2 つの問題を解決する必要がある．第一に，認証や認可のための情報が必要以上に集中しているということである．次に，ログデータとして，利用者の行動履歴が保持されているが，このようなデータはプライバシー侵害につながりやすい．以下，これらの問題について詳細に述べる．

最初の問題は認証認可システムへの情報の集中である．SSO の本来の機能である（複数のサービスへの）認証機能に加え，認可を可能にするため属性情報も提供するようになっている [4], [5]．また，認証においては ID に対するパスワード等の検証情報のみを確認すれば十分だが，発行を認証局が兼ねる場合も多いため，ID を発行するための個人情報を取得するがある．このように発行，認証，認可において必要な情報（のペア）が異なるが，現行のシステムではこれらが集中しており，より個人が特定できやすくなっている．

次の問題は，行動の履歴が保持されている，ということである．一般に，このことはあまり問題視されてこなかったようである．システムを構築する側からすれば，ログを残すのは当然という感覚が一般的であろう．しかし，プライバシー保護の観点からすれば必ずしもそうではなく，実際に，多くの公共図書館では，プライバシー保護の観点から，図書の返却後は，その貸出履歴はデータベースから削除する．また，仮にログとして残したとしても，ID を変えるなどして，個人情報と紐づけられなければよいのではないか，という意味で問題視しない場合もある．例えば，SSO の実装の一つである Shibboleth では，各サービスと IdP の間で用いる ID として仮の ID を使う機能がある．しかし，その行動から個人を特定できる場合も多く存在

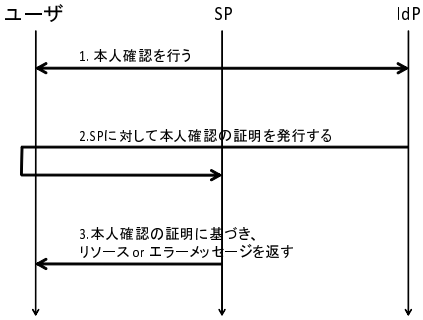

図 1　SSO における認証の概略
Fig. 1　An outline of authentication of SSO

するし，後々事故等により個人情報が流出して紐づけが可能になる場合も考えられる．このように考えると，最初の問題で指摘した個人情報だけが問題ではなく，行動の履歴に関する情報もプライバシー保護の観点から慎重に扱うべきである．

これらの問題に対し，本稿ではまず，必要な情報を議論して，プライバシー保護の対象となる情報を，個人の特定に至る**個人情報**と，個人の行動の履歴である**履歴情報**に分ける．その上で，両方が紐づけられた場合だけでなく，どちらか片方であっても，不必要に他者に取得される場合にプライバシーの侵害であると考える．次に，意味的に導出したこれらの要件を形式的に定義し，この定義を満足する複数サービス向けの認証や認可システムを提案する．提案システムは，個人情報の分散という意味で，認証と認可(注1)の機能を分ける．従来，認証と認可は別の機能であったため，別のサブシステムとして実現される例は多かったものの，本稿ではプライバシー保護に必要な要件から分ける．

しかし，このように情報を分けることにより，履歴情報を取得できることが増えてしまう．これに対し，ID 間の紐づけができないという認証プロトコル [6] を採用する．これは非常に強力であり，このプロトコルを実装したシステムでは，あるユーザが同じ IdP を利用して 2 回の認証を行ったとしても，その 2 回のユーザが同じであったかどうかが IdP には分からない．上述の個人情報の分散により，多くの場所で履歴が蓄積されることになるが，このプロトコルを複数のサブシステム（認証や認可のシステム）に拡張することで，どのサブシステムでも履歴が残らないようにすることができる．

2.　複数サービス環境における認証と認可

本節では，用語の導入も兼ねて，複数サービスを対象にした一般的な認証や認可システムを述べる．シングルサインオンは，イントラネット等の単一組織内での利用も考えられるが，プライバシー保護を考えているので，複数の組織間にまたがる認証や認可を考える．

SSO において認証を行う組織あるいはシステムを認証局（IdP）と呼び，IdP を利用するサービス提供者をサービスプロバイダ（SP）と呼ぶ．図 1 に認証の概略を示す．ユーザから IdP には ID と**検証情報**が渡され，IdP はこのペアが正しく対

(注1)：あるいは必要に応じて他の機能も分けることも可能である．

応しているかどうかを確認する．例えば，パスワードや生体情報が検証情報である．検証が正しく行われると，これを SP に示し，SP はユーザに対しサービスを提供する．

ID と検証情報の対応を確認するだけでよい認証と比較して，認可，つまり，リソースへのアクセスを制御する手法はサービスに依存して数多く存在する．認可に用いられる基本的な情報として個人の属性があるが，お金を出してあるファイルへアクセスする，短い期間に限って誰にでもアクセスさせるといった手法も考えられる．このような認可の実現方法の多様性のため，SSO と比較すると，複数サービス向けの認可は広く普及しているとは言い難い．ここでは，**認可局**を，ID とリソースのペアに対し，アクセスの可否を返すものと簡単に定義する．ここで，渡される ID はすでに認証を経ていることが SSO により保証されているものとする．一般には，様々なポリシーによってリソースへのアクセス制御は実現されるが，認可局はそのポリシーをリソースと ID から $\{0,1\}$ への関数（あるいは表）として保持していればよく，個人情報や属性情報は不要である．このような関数あるいは表はアクセス制御リスト（ACL）と呼ばれる．

OpenID や Shibboleth といった SSO の規格では，認可に用いるため，IdP が個人の属性情報を提供することも考えられている．この場合，自然に IdP と認可局が同一システムあるいは同一組織により提供されると思われる．一方で，本稿で仮定している複数サービス向けの認証や認可の場合，異なる組織に所属するユーザの存在や，組織の階級とは関係のない情報による認可の手段が考えられる．そのため，プライバシー保護とは関係なく，運用の観点のみから見ても，IdP と認可局は別になることが自然である．

3. 認証認可におけるプライバシー保護の要件

本節では，認証認可を行う時のプライバシー保護に関する要件を導入する．この要件は，いわばプライバシー保護に関する概念的な要件であり，セマンティクスといえる．このセマンティクスを実現するシンタックスは，次節において導入される．

プライバシー権は，私生活への干渉に対抗する権利と理解されてきたが，他にも，自己情報へのコントロール権に対する侵害をプライバシー権侵害とする立場，私事についての自己決定権をプライバシー権とする立場，宗教的または心の静穏をプライバシー権の保護の対象とする立場などの立場がある [7]．本稿では，自己情報コントロール権を元に，プライバシー保護に必要な要件の抽出を行う．

情報を自らコントロールできないのは，自己のもとに情報がないか，他者がコントロールできる状態にある場合にいうが，ここで考える情報は自己情報なので，後者の他者が情報をコントロールできる場合のみを考える．情報をコントロールできる状態にあることを情報を保持している状態と同一視すると，他者が情報を保持している状態が自己情報がコントロールできない状態である，と定義できる．

次に，自己情報について考える．まず，個人情報は自己に関する基本的な情報であり，自己情報コントロール権でいうところの自己情報としてよいだろう．一方で，直接個人を特定する情報は含まなくても，認証や認可システムに蓄積されていくログも，見る人によっては個人を特定できる場合がある．さらに，時系列にそった個人の行動履歴は，その人の心情や思想等が十分に反映されていることが考えられる．そこで，本稿では，自己情報を個人情報と履歴情報のどちらも考えることにする．その上で，これらの情報を他人が保持している状態が自己情報がコントロールできない状態である，とする．

本稿ではサービスを受けるための認証や認可を考えているため，SP や IdP 等に自己の情報を開示する必要がある場合がある．そのため，本人の同意があって開示した場合は，他人が自己情報を保持していないと考えることも可能だが，全てのユーザが同意書等を熟読した上でサービスを利用しているとは限らないし，また，ユーザが受けたいサービスの SP がサービス提供には不必要な自己情報を要求する場合もあるだろう．そこで，ユーザの同意の有無とは関係なく，SP や IdP 等がサービスを提供するのに最小限の個人情報や履歴情報を保持しているかどうかを問題にする．

本稿では認証や認可システムは複数サービス向けのものを考察しているが，これらのシステムはユーザが受けたいサービスからは直接見えない可能性がある．例えば，OpenID では自分でメールアドレスを登録して ID を発行するが，学術認証フェデレーション [8] のように，大学等の機関が ID を発行し，IdP を別途立ちあげた場合，IdP に渡される情報は機関から渡されることになり，個人では直接知ることができない，ということも考えられる．そのため，ユーザのプライバシーに配慮しているか否かは，SP に対してではなく，認証や認可を実現するためのシステムに対する性質として定義する．

これらの議論をまとめると以下のようになる．まず，あるサービスを実現するシステムが複数のサブシステムから構成されているとする．サブシステムとしては IdP や認可局がある．このようなサブシステムの一つが，ユーザのプライバシーを侵害しているとは，このサービスの任意のユーザに対し，このサブシステムが提供する機能に必要以上に個人情報または履歴情報を蓄積している時にいう．

4. プライバシ保護を考慮した複数サービス環境における認証認可

本節では，個人情報の分散に関し，前節で導入した要件を満足するように形式的な定義を導入し，実際に認証及び認可について，これを満たす情報を与える．次に，履歴情報についても同様に，形式的な定義を与え，これを満たす認証及び認可システムを提案する．IdP による履歴情報の収集を防ぐ認証として，プライベート情報検索 [9] を用いた認証手法 [6] が提案されている．この手法では認証のみであり認可は考慮されていないが，まず説明のためにこの手法の概要を述べる．次に，認証局と認可局が分離している場合への応用を考える．

4.1 個人情報の分割

本節では，個人情報を関係データベースと同様，属性情報の組からなるものとし，前節でプライバシー保護の要件とした個

人情報の分散について形式的に定義する．

個人情報 A_i をフィールド，個人をレコードとして持つデータベース $\mathcal{D}(A_1, A_2, \dots)$ を考える．IdP や認可局等を**システム**と呼ぶ．システム S が用いる個人情報（のフィールド）の集合 $\{A_{S_1}, A_{S_2}, \dots\}$ を $\mathcal{D}_S$ で表し，S は $\mathcal{D}_S$ 以外の属性情報へはアクセスできないものとする．例えば，$\mathcal{D}$(名前, 住所, 所属, ...) といったデータベースがあり，あるシステムはこの中の名前と所属のみにアクセスできるが，他の属性の属性値にはアクセスできない．

［定義 1］ 属性 $\{A_1, A_2, \dots\}$ の部分集合 $\mathcal{D}_S$ が，**システム S に対し必要十分である**とは，$\mathcal{D}_S$ 内の属性に対する属性値を用いて S がシステムとしての機能を提供でき，かつ，$\mathcal{D}_S$ から任意の属性 A_{S_j} を除いた属性集合の属性値のみでは S が機能を提供できない時にいう．

本稿で考察する認証及び認可システムには，属性としてユーザ ID の集合 I，検証情報の集合 V，(SP が提供する）リソース R の集合があればよい．具体的には，認証システムには $I \times V$ 上の関係，認可システムには $I \times R$ 上の関係が必要十分である．まず，認証について見ると，I または V のいずれか一方がないと認証ができないが，これらの対応関係を見れば認証が可能である．例えば，多くのシステムでは，ID とパスワードの組が対応しているかどうかを確認している．

次に，認可について検証する．$(i, r) \in I \times R$ が与えられた時，(i, r) が認可システムが持つ関係内に存在するかどうかを見ればよい．逆に，I または R がなければ認可することはできない．しかし，これだけでは $I \times R$ 上の関係が必要十分であることを示したことにはならない．というのは，ユーザ ID を使わない認可も考えられるためである．例えば，(物理的なリソースに対する）認可を実現する物理的な鍵は，誰が利用したかは分からない．しかし，このような認可の場合でも，ユーザ ID とリソースの関係に落とすことが可能である [10]．このようにすることで，このシステムに対しては，匿名性を犠牲にすることになるが，匿名性の担保については，次節以降で述べる ID の対応づけを不可能にする認証や認可プロトコルによって対応する．また，ユーザ ID を使わない認可でも，どのリソースにアクセスするかの情報と，アクセスの可否に関する情報の二つが必要であり，一つの属性では不十分である(注2)．例えば，上述の鍵の場合では，鍵とリソースのペアが必要である．よって，$I \times R$ 上の関係は必要十分である．

4.2 プライベート情報検索

プライベート情報検索（Private Information Retrieval, PIR）とは情報検索技術の一つであり，検索要求を出すユーザのプライバシを保護しつつ，情報検索を行う．具体的に秘匿される情報は，ユーザが獲得したいデータベースのインデックスである．つまり，データベースはどのレコードが結果として検索されたかを判別できない．これを実現するナイーブな手法は，ユーザがデータベースに全ての要素を送るように要求することであり，このとき，通信量はデータベースの要素数 n に対して $O(n)$ であり，現実的ではない．Chor ら [9] は，同じ要素を持つ複数のデータベースを用いることにより，情報理論的に安全でかつナイーブな手法と比較して通信量の小さい PIR を提案した．以後，計算量理論的に安全な PIR [11] や，単一のデータベースで実現可能な PIR [12] も提案されている．

以下に, [13] に基づくシングルサーバ PIR の定義を示す．データベースの要素をビットとし，要素数 n のデータベースをビット列 $X = x_1 \cdots x_n$ とする(注3)．$p(\cdot)$ を任意の多項式とする．任意の自然数 n に対して，$[n] \stackrel{\text{def}}{=} \{1, 2, ..., n\}$ とする．任意の集合 A，任意の自然数 n に対して，$A^n \stackrel{\text{def}}{=} \overbrace{A \times A \times \cdots \times A}^{n}$ とする．

［定義 2］ $m, n, \ell_r, \ell_q, \ell_s, \ell_a \in \mathbf{N}$ について，シングルサーバ PIR は以下の 3 つの関数から構成される．

- **クエリー生成関数** $Q : [n] \times \{0,1\}^{\ell_r} \to \{0,1\}^{\ell_q} \times \{0,1\}^{\ell_s}$
- **アンサー生成関数** $A : \{0,1\}^n \times \{0,1\}^{\ell_q} \to \{0,1\}^{\ell_a}$
- **再構成関数** $R : [n] \times \{0,1\}^{\ell_q} \times \{0,1\}^{\ell_s} \times \{0,1\}^{\ell_a} \to \{0,1\}^m$

ただし，$Q_1(i, r)$ を $Q(i, r)$ の 1 つ目の要素とし，これらの関数は以下の性質を満たす．

- **完全性:** 任意の $X \in \{0,1\}^n$，任意の $i \in [n]$ について，

$$\Pr[R(i, Q(i,r), A(X, Q_1(i,r))) = x_i] > 1 - \frac{1}{p(\log n + \ell_q + \ell_s + \ell_a)}$$

である．ただし，左辺の確率は $\{0,1\}^{\ell_r}$ から一様に選択された r により決まる．

- **クエリーの識別不可能性:** 任意の $i, j \in [n]$，任意の確率的多項式時間アルゴリズム $\mathcal{B}$，任意の十分に大きい w について，

$$|\Pr[\mathcal{B}(1^w, Q_1(i,r)) = 1] - \Pr[\mathcal{B}(1^w, Q_1(j,r')) = 1]| < \frac{1}{p(w)}$$

である．ただし，左辺の確率は $\{0,1\}^{\ell_r}$ から一様かつ独立に選択された r, r' 及び $\mathcal{B}$ の動作に用いるランダムな選択（以後，コイントス）により決まる．

$Q(i, r)$ の 1 番目の要素をクエリー，2 番目の要素をシークレット，$A(X, q)$ をアンサーと呼ぶことにする．上記の定義は，簡単には以下を意味する．

- 求めたい要素のインデックス i とそれに対応するクエリー，シークレット，及びアンサーを用いることで，非常に高い確率で求めたい要素 x_i を復元できる．
- 求めたい要素のインデックスが i である場合のクエリーと，j であった場合のクエリーが識別不可能 [14] である．

PIR を用いた情報検索の具体的な手順は以下のようになる．

（1） ユーザは $r \in \{0,1\}^{\ell_r}$ をランダムに選択し，データベースに $Q_1(i, r)$ を送る．

（2） データベースはユーザに $A(X, Q_1(i, r))$ を送る．

(注2)：何の認可もせず誰でも利用可能という場合はリソースを指定するだけでよいが，これは通常の意味で認可といえず，ここでは考慮しない．

(注3)：要素がビットではなくビット列である一般的な PIR については，文献 [9] で効率のよい手法が提案されている．

（3） ユーザは $R(i, Q(i,r), A(X, Q_1(i,r)))$ を計算し，x_i を得る．

このとき，PIR の完全性の性質から，ユーザは x_i を（微小な誤り確率を除き）復元可能であり，また，クエリー識別不可能性の性質から，クエリーを得たデータベースは i についての情報を得ることができない．

4.3 PIR を用いた認証

本節では，[6] に従い，PIR の情報検索を認証に応用する．基本的なアイデアは，ユーザ ID とパスワード等の検証情報が格納されているデータベースに対し，ユーザ ID をインデックスとみなして，PIR を用いる．

ユーザ数を n とし，ユーザを $\mathcal{U}_i$ $(i \in [n])$ で表す．各ユーザ $\mathcal{U}_i$ には，一意な識別子 i と検証情報 $p_i \in \{0,1\}^m$ が割り当てられているものとする．SP は，識別子 i についての認証要求を出したユーザが本当にユーザ $\mathcal{U}_i$ であるかどうかを検証する．IdP は，全てのユーザのパスワードの列 $P = (p_1, p_2, ..., p_n)$ を持つ．

IdP に対して匿名性を持つ単純な認証プロトコルを以下に示す．

（1） ユーザは SP に (i, z) を送る．ここで，$z \in \{0,1\}^m$ である．

（2） SP は $r \in \{0,1\}^{\ell_r}$ 及び $c \in \{0,1\}^m$ をランダムに選択し，IdP に $(Q_1(i,r), c)$ を送る．

（3） IdP は SP に $A(P, Q_1(i,r))$ を送る．

（4） SP は $p_i \leftarrow R(i, Q(i,r), A(P, Q_1(i,r)))$ を計算する．次に SP は，もし $z = p_i$ であれば 1 を出力し，そうでなければ 0 を出力する．

前節で述べた手法を直接用いると，PIR の 2 番目の性質から，IdP は受け取った SP からのクエリーを用いても，SP を利用しているユーザの識別子が，i であるか j であるか効率よく判別することができない．すなわち，IdP には，現在 SP を利用しているユーザが，以前利用したユーザと同一のユーザであるか，異なるユーザであるのかを判別することができない．そのため，IdP は受け取ったクエリーから，同一のユーザのサービス利用履歴を記録することができない．しかし一方で SP は正しいパスワードを復元することができるので，パスワードを用いてユーザを認証することができる．

4.4 PIR を用いた認証及び認可

本節では，IdP に加え，認可を行う認可局がある場合に，プライバシー保護を可能にしつつ，認証及び認可を可能にするプロトコルを提案する．

前節で述べた認証手法のアイデアの，IdP と認可局が分離している場合における，複数サービス環境における認証認可への応用を考える．この場合，単純な実現方法として，SP が IdP と認可局それぞれに対してユーザ ID を送り，IdP からパスワードを，認可局からは権限の有無を得る方法が考えられる．このような単純な実現方法を用いた場合には，IdP と認可局ともに，どのユーザがどのサービスを利用したのかを把握することができる．ゆえに，履歴の保護の観点からは，認証局と認可局を分離させることによりプライバシリスクが高まる．

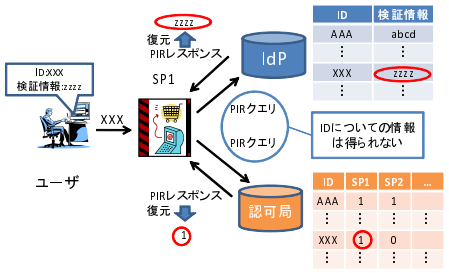

図 2 IdP と認可局が分離している場合の PIR を用いた認証と認可
Fig. 2 Authentication and authorization in case that IdPand authorization servers are separated

この問題に対して，IdP が持つ検証情報のデータベースだけでなく，認可局の持つ ACL に対しても PIR を用いることで，前述の問題を解決することができる（図 2 参照）．

5. 関 連 研 究

複数のサービスに対する認証としてシングルサインオン（SSO）は広く知られてきており，OpenID や Shibboleth といった実装もある [4], [5]．また，実際に学術情報流通に応用する目的の実証実験プロジェクト [8], [15] も行われている．セキュリティ確保の観点から生体認証や PKI を用いたシングルサインオンが提案されるなどしているが，プライバシーの問題は一部の例外 [16] を除いて考えられていない．上述したように，これらの実装では認証だけでなく認可も行うため，不必要に個人情報が集中しており，プライバシー保護の観点からは望ましくない．また，仮名の利用などにより一部プライバシー保護に配慮しているものの [5]，履歴における ID の対応づけは可能である．

一方で SSO のような広く利用される実装はないものの，認証認可のプライバシ保護に関する研究は盛んに行われている．柿崎ら [17] は，本人情報と属性情報を分離し，SP に対しては属性管理者が発行する属性証明書のみを用いて属性認証を行う手法を提案した．この手法では，属性管理者に対しては本人証明書を用いて本人確認を行って属性証明書を発行してもらい，その属性証明書を用いて SP に対して本人情報を与えることなく，属性を持つことを証明することを可能にする．本稿の提案手法では IdP や認可局に対して情報を秘匿するのに対し，この手法では SP に対して秘匿する点が異なる．

グループ署名 [18] とは，プライバシ保護を考慮した匿名署名技術の一つであり，グループに属するメンバのみが署名可能であり，また署名から署名者の識別子に関する情報を得ることができない性質を持つ．あるグループに属することを属性とみなすと，グループ署名を用いて属性認証を行うことができる．しかしながら一般的に，その匿名性のために失効が困難であり，頻繁に属性が変更される場合には不向きである．

個人情報と行動の履歴に関する情報を分離するという観点では Personal ID （PID）と呼ばれる仕組みも同様の分離を行っている [19]．PID では，認証局に対応する発行者がサービスごとに異なる ID のリストを発行し，ユーザと ID の対応づけを管

理する．サービス提供者は発行者からリストを取得し(注4)，この ID を用いてサービスを行う．ユーザへは，耐タンパー性を持つ IC カード等に複数サービス用の複数の ID を格納して渡す．ID を複数格納できる IC カードや携帯電話等のデバイスが必要だが，個人情報は発行者にあり，（リストが渡された場合は）行動の履歴はサービス提供者のみに記録される．[20] では，PID を図書館サービスに利用した場合のプライバシー保護について議論している．

プライバシーの問題はデータマイニングのコミュニティでも広く研究されている．データマイニングにより大規模なログデータベース等から有用な知識を自動的に抽出する研究が行われてきたが，対象のデータによってはプライバシー侵害の恐れがある．そこで，プライバシー保護しながらマイニングを行う手法が多く提案されている（例えば [21] を参照）．しかし，基本的に履歴に関する情報は取得してあると仮定するため，既に他者が情報を保持している状態にあるといえる．本稿では，IdP や認可局が持つ履歴情報からは誰がアクセスしてきたのか原理的に分からないような状態にしてあり，そこが本質的に異なる．

6. ま と め

本稿では，プライバシーの意味的な要件を議論し，要件に対応する形式的な定義を与えた．これらの要件では，個人情報と履歴情報に分けられる．個人情報の分散により，複数のシステムで行動の履歴が（誰かは分からないかもしれないが）蓄積できる危険性が増える．さらに，個人情報を必要十分に制限するため，必ずしもユーザ ID が必要とは限らない認可の場合でも，ユーザ ID を用いた認可を行うようにすることで，履歴情報と ID が紐づけられるようになる．これらの問題に対し，[6] で提案された手法を使い，履歴情報における ID 間の対応がとれないような認証や認可プロトコルを実現した．

今後の課題として，SP に対しての匿名性を持つ手法の構築が考えられる．つまり，本稿で述べた手法では，SP がユーザの識別子を知っているので検証情報と属性情報の対応を知ることができた．これを単純な方法で，SP に対しても識別子を秘匿した場合には，復元した検証情報と属性情報が，本当に同一のユーザのものであるか確認できない．例えば，ユーザが認証局に送るクエリーは正しい識別子を用いて生成し，認可局に送るクエリーは異なる識別子を用いて生成することで，不正が行われる危険性が生まれる．一方で，認可局を考えず IdP のみの場合は，IdP だけでなく SP に対しても匿名性を持つ認証手法が構築できる [6]．よって，本稿で考察した複数のシステムに情報が分離された場合でも同様の手法が適用できるかどうかを明らかにすることは，重要な今後の課題である．

謝　　辞

本研究の一部は科学研究費補助金 基盤研究 (A)(課題番号:19200004) および科学技術振興事業団（JST）の戦略的創造研究推進事業（CREST) の支援を受けた．

(注4)：リストを取得せず，SSO の IdP のように利用時にネットワーク認証を行うモデルも考えられる．この場合，SSO と同じく，個人情報と行動の履歴が発行者に集中する．

文　　献

[1] 野林, 中村, 池永：“ハードウェアトークンと鍵管理サーバを用いたシングルサインオンシステムの開発”, 電子情報通信学会技術研究報告, 第 106 巻, pp. 7–12 (2006).
[2] 梅本, 藤野：“USB トークンによる PKI 相互認証を用いたセキュアネットワーク上でのシングルサインオンシステムの提案と実装”, 電子情報通信学会技術研究報告, 第 106 巻, pp. 49–54 (2007).
[3] 益田, 梅本, 浅田, 藤野：“秘密鍵を LSI に埋め込んだユニークデバイスを用いた PKI システムの提案とシングルサインオンシステムへの応用”, 暗号と情報セキュリティーシンポジウム (SCIS 2007) (2007).
[4] “OpenID”. http://openid.net/.
[5] “Shibboleth”. http://shibboleth.internet2.edu/.
[6] T. Nakamura, S. Inenaga, D. Ikeda, K. Baba and H. Yasuura: “Anonymous Authentication Systems Based on Private Information Retrieval”, Proceedings of the First International Conference on Networked Digital Technologies, pp. 53–58 (2009).
[7] 竹田, 堀部（編）：“名誉・プライバシー保護関係訴訟法”, 青林書院 (2001).
[8] “学術認証フェデレーション”. https://upki-portal.nii.ac.jp/SSO.
[9] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan: “Private Information Retrieval”, Jornal of the ACM, **45**, pp. 965–982 (1998).
[10] T. Yamasaki, S. Inenaga, D. Ikeda and H. Yasuura: “Modeling Costs of Access Control with Various Key Management Systems”, Proceeding of The 2009 International Conference on Parallel and Distributed Processing Techniques and Applications, CSREA Press, pp. 676–682 (2009).
[11] B. Chor and N. Gilboa: “Computationally Private Information Retrieval”, Annual ACM Symposium on Theory of Computing, ACM, pp. 304–313 (1997).
[12] E. Kushilevitz and R. Ostrovsky: “Replication is Not Needed: Single Database, Computationally-Private Information Retrieval”, the 38th Annual Symposium on Foundations of Computer Science, pp. 364–373 (1997).
[13] C. Cachin, S. Micali and M. Stadler: “Computationally Private Information Retrieval with Polylogarithmic Communication”, Advances in Cryptology - EUROCRYPT ’99, Vol. 1592 of LNCS, Springer-Verlag, pp. 402–414 (1999).
[14] O. Goldreich: “Foundations of Cryptography”, Cambridge University (2001).
[15] 国立情報学研究所（編）：“平成 20 年度シングルサインオン実証実験報告書”, 国立情報学研究所 (2009).
[16] R. R. Heckle and W. G. Lutters: “Privacy Implications for Single Sign-On Authentication in a Hospital Environment”, Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 173–174 (2007).
[17] 柿崎, 山本, 辻：“属性認証を利用したプライバシ保護方式”, 情報処理学会論文誌, **48**, 3, pp. 1038–1046 (2007).
[18] D. Chaum and E. van Heyst: “Group Signatures”, Advances in Cryptology - EUROCRYPT 1991, Vol. 547 of LNCS, Springer-Verlag, pp. 257–270 (1991).
[19] 浜崎，安浦：“PID を用いた安全な社会システムの構想”, 九州大学大学院システム情報科学紀要, **7**, 2, pp. 139–148 (2002). http://kasuga.csce.kyushu-u.ac.jp/lab_db/papers/paper/pdf/2002/hamasaki02_2.pdf.
[20] 安東, 池田：“新個人認証システム personal id が変える図書館の個人情報管理： 個人情報やプライバシーに配慮した一歩先行く図書館サービスとは”, 大学図書館研究, **81**, pp. 26–41 (2007).
[21] C. C. Aggarwal and P. S. Yu Eds.: “Privacy-Preserving Data Mining: Models and Algorithms”, Vol. 34 of Advances in Database Systems, Springer US (2008).