利用者の匿名性を考慮したアカウント管理手法

渡辺 龍[†1] 三宅 優[†1]

ID 管理の技術において、利用者情報の安全な管理及びプライバシの保護は重要な課題の一つである。利用者のアカウント管理に関して、情報漏洩のリスク低減を目的として、Dey らによりブラインド署名を用いたアカウント管理手法が提案されている。これは、ID 管理において認証を担う認証プロバイダ (Identity Provider: IDP) での漏洩リスクの低減のために、IDP でのログイン ID に匿名的な ID を利用する手法である。Dey らの手法では、ブラインド署名の技術を用い申請内容を秘匿することでアカウント管理での匿名性を実現している。しかしながら、利用者が不正な申請をすることにより複数のアカウントを生成することが可能であるという問題がある。この問題の解決として、著者らは、生成数の管理を導入したアカウント管理手法を本稿で提案する。

A User Account Management Method with Enhanced User Anonymity

Ryu Watanabe[†1] and Yutaka Miyake[†1]

Risk reduction of information leak is one of the most important functions on identity management systems. For this purpose, Dey et. al. have already proposed an account management method for federated login system with blind signature scheme. In order to give anonymity on accounts for authentication provider called IDP (identity provider), blind signature scheme is utilized for generate an authentication token on an authentication service and the token is sent to an IDP. However, there is a problem on the proposed system. Malicious users can make multiple accounts on IDP by requesting the accounts. As a measure for this problem, in this paper, the authors propose an account checking method before account generation.

†1 株式会社 KDDI 研究所
KDDI R&D Laboratories, Inc.

1. はじめに

IT 技術の発達と情報通信インフラの整備により、近年、インターネットを利用したサービスは広く浸透し、利用可能なサービスも多岐多様となった。こうした状況において、利用者による複数サービスの利用時の安全性と利便性の向上を目的として、ID 連携によるシングルサインオン技術が普及しつつあり、そのための実装や仕様が公開されている[1)2)]。ID 連携によるシングルサインオンでは、利用者の認証を実施するアイデンティティプロバイダ (Identity Provider: IDP) とサービスを実際に提供するサービスプロバイダ (Service Provider: SP) が連携し、IDP での認証状態を SP が受け入れることで SP での認証も完了する。IDP での利用者の認証状態を保持しておくことで、別の SP を利用する際にもその認証状態を活用することができるため、利用者の認証は一度で済むというメリットがある。このため、IDP はアカウント生成にあたり利用者の身元を適切に確認した上でアカウント生成を実施することが必要がある。この ID 連携によるシングルサインオンのアカウント管理の問題として、IDP がクラックされた場合に、IDP で管理されている IDP と SP 間の ID の紐付けから SP でのアクティビティを含めて本人の情報が開示される可能性があるという問題が指摘されている。このアカウントの管理における問題の解決策として、Dey らは PseudoID と呼ぶアカウント管理手法を提案している[3)]。IDP でのアカウント生成において、IDP に対しても身元を秘匿し、利用者に匿名性を与えることで、IDP がクラックされた場合のリスクを低減するものである。PseudoID では、この IDP での匿名性を実現するために、利用者の身元確認する機関を別に用意し、IDP はその結果を匿名的に受け入れて、IDP でのアカウント生成を実施する。利用者の身元確認についての情報は、署名対象を署名者に秘匿するブラインド署名の技術を利用して作成されており（このため、PseudoID では、この身元確認を実施する機関をブラインド署名サービス (Blind Signature Service: BSS) と呼んでいる。)、IDP と BSS 双方のアカウントが紐づけることがない。このため、BSS あるいは IDP がクラックされた場合でも、双方のアカウントの関係性を辿ることができず、クラックによる情報漏洩のリスクを低減できるという特徴を持つ。しかしながら、PseudoID では、アカウント生成数の管理を行っていないがゆえに、利用者が BSS に IDP でのアカウント生成を重複して申請することで、利用者が重複して IDP のアカウントを取得できてしまうという問題がある。複数アカウントの利用は利用するサービスにも依存するものの、不正な行為につながりかねない。この問題の解決のために本稿で、著者らは、BSS でのアカウント生成数の管理の導入について提案する。本提案では、BSS は IDP での生成済みで

あるかどうかを確認した上で、IDP に身元確認し、アカウントを削除した場合には、BSS での生成状態がリセットされるため、一度 IDP の利用を停止した利用者であっても、再度アカウントを作成することが可能である。

2. 関 連 研 究

2.1 ブラインド署名

Dey らの提案手法である PseudoID を説明する上で必要となるブラインド署名[4] の技術について、先に説明する。ブラインド署名は、公開鍵暗号の応用技術である電子署名の拡張の一つである。電子署名技術[5] は、あるメッセージに対して署名者のみに既知である私有鍵を用いた署名処理 $S()$ と、公開情報である公開鍵による検証処理 $V()$ から構成されている。署名対象であるメッセージ m と、m への署名 $S(m)$ について、$V(m, S(m))$ を演算することで署名が検証される。

ブラインド署名の技術では、署名者に署名対象を秘匿するために、ブラインド関数 $B()$ を用いた暗号処理が導入されている。ここで、$B()$ と署名処理 $S()$ は、式 (1) の関係を満たす。また、$B^{-1}()$ はブラインド関数の逆関数である。

$$B^{-1}(S(B(m))) = B^{-1}(B(S(m))) = S(m) \tag{1}$$

ブラインド署名を利用する利用者は、あるメッセージ m に対して、その内容を秘匿したまま、署名者による署名を受けたい。このため、利用者はブラインド関数 $B()$ を用いてメッセージを暗号化し、暗号化されたメッセージ $B(m)$ を署名者に送付する。署名者は、送付されたメッセージに署名し、$S(B(m))$ を利用者に返送する。この時署名者は元のメッセージ m の内容を知ることができない。利用者は、式 (1) の関係を用いて、メッセージへの署名 $S(m)$ を得る。利用者は、m と $S(m)$ を検証者に送付し、検証処理を受ける。

ブラインド署名の一例として、RSA 署名の拡張がある。RSA 署名では、公開鍵 (n, e)、と署名者の私有鍵 (d) が用いられる。利用者はメッセージ m を暗号化するために、ブラインド処理のための乱数 r を準備し、$B(m) = mr^e$ を演算する。署名者は $B(m)$ に対して、オイラーの定理を利用し次の演算から署名を得る。

$$m^d r^{ed} \equiv m^d r \pmod{m}$$

また、利用者は、r^{-1} を用いてブラインドの処理を外すことができ、

$$m^d r \cdot r^{-1} = m^d \pmod{m}$$

最終的に、署名者による、メッセージ m への署名 $S(m) = m^d \pmod{m}$ を得る。

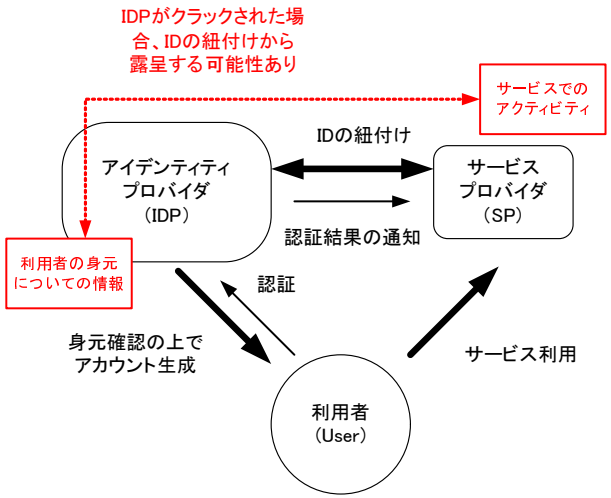

図 1 ID の紐付けによる情報漏洩

2.2 PseudoID

現状の ID 連携によるシングルサインオンでは、IDP 自身が利用者の身元管理を実施しており、また、IDP と SP 間でアカウントの紐付け情報を持つために、IDP がクラックされた場合に、紐付けを通じて様々な情報が露呈する可能性があるというセキュリティの懸念が指摘されている（図 1）。この、ID 連携によるシングルサインオンでのアカウント管理におけるリスク低減のための手法が、Dey らにより提案された PseudoID である。PseudoID では、利用者の身元確認については別の機関（ブラインド署名サービス）に移譲する。IDP との間でそれぞれのアカウントの紐付けをつくらず、IDP では匿名的なアカウントが生成される。このため、IDP あるいは BSS がクラックされた場合でも双方のアカウントの関係が露呈することはなく、個人情報の漏洩リスクを低減できる。PseudoID では、前述したブラインド署名の技術を利用することで本機能を実現している。

以下、PseudoID でのアカウント管理について説明する。PseudoID では、以下の前提を持つ。BSS は利用者の身元を確認した上で BSS へのアカウント生成を行っている。BSS の公開鍵証明書を IDP が確認でき、IDP は BSS による署名を検証できる。利用者、BSS、IDP 間の通信には暗号化通信路などを利用しており、第三者に盗聴されて内容が漏洩することはない。

表 1　記号の定義

記号	説明
ID_X	X における利用者の ID
PW_X	X における利用者のパスワード
B	ブラインド処理
$S_X(M)$	X による、署名対象 M への署名
$V(M, S_X(M))$	署名の検証処理
R_X	X が生成するユニークな乱数
$\|\|$	結合

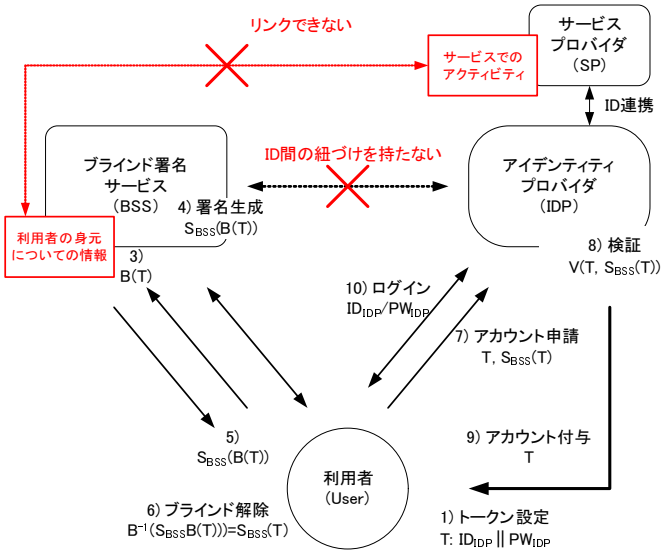

図 2　PseudoID でのアカウント作成手法

まず、利用者は IDP で利用する ID/password ペアを準備し、ブラインド処理を施したものを署名対象として、BSS に提出する。BSS は利用者を認証した上で、署名を実施し、利用者に返送する。利用者はブラインドの処理を解除し、IDP に提出する。IDP は署名を正しく検証できたならば、申請に応じて ID/password ペアを IDP での利用者のアカウントとして設定する。

以下に手順の詳細を記し、その概要を図 2 に、シーケンスを図 3 に示す。また、図中及び手順での各種記号の定義を表 1 にまとめる。

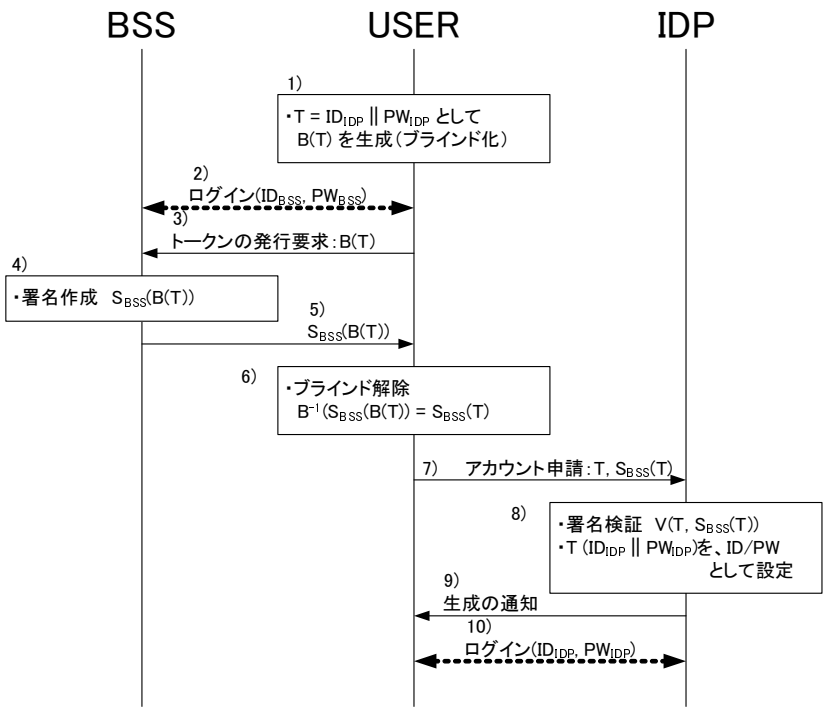

図 3　PseudoID でのアカウント作成手法

(1)　利用者は、IDP で利用する ID/password ペアを署名対象 $T = ID_{IDP}||PW_{IDP}$ として準備する。

(2)　利用者は、ID_{BSS}, PW_{BSS} を利用して BSS にログインする。

(3)　利用者は、BSS にブラインド処理を施した、$B(T)$ を BSS に提出する。

(4)　BSS は、提出された、BT に自身の私有鍵で署名 $S_{BSS}(B(T))$ を生成する。

(5)　生成した署名 $S_{BSS}(B(T))$ を、利用者に返送する。

(6)　利用者は、BSS から返送された署名のブラインド処理をはずして、T に対する BSS の署名 $S_{BSS}(T)$ を得る。

(7)　利用者は、$T, S_{BSS}(T)$ を、IDP に送付し、アカウントの申請を行う。

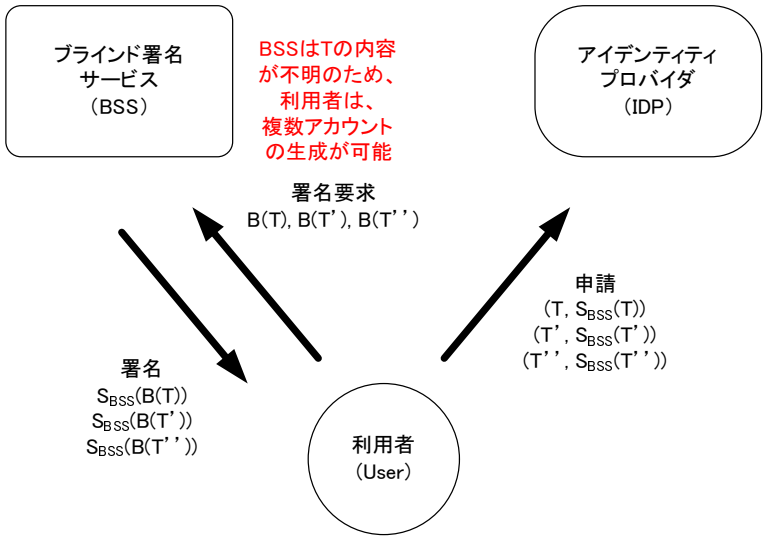

図 4　複数アカウントの生成

(8)　IDP は BSS の公開鍵を用いて署名を検証する。

(9)　正しく検証できた場合はには、T に記された、ID_{IDP}, PW_{IDP} を利用者の ID/password として設定し、利用者に通知する。

(10)　設定された ID/password により IDP を利用する。

上記手順により生成された利用者の IDP のアカウントは、BSS の持つ利用者の身元についての情報と関係を持たないため、IDP がクラックされても、サービスでのアクティビティと利用者本人がリンクされることはない。

2.3 問　題　点

PseudoID では、利用者のプライバシと情報漏洩リスク低減のために、IDP でのアカウント自体にも匿名性を与えていることを実現している。しかしながらこの特徴のために、利用者による不正なアカウントの作成が可能となっている。利用者は BSS に対して異なる ID/password ペアでの申請をするにあたりブラインド署名を利用し、その内容を秘匿している。このため異なる ID/password ペアでの申請を繰り返すことで、IDP でのアカウントを複数作成できてしまうという問題がある（図 4）。多数のアカウントを活用できることはサービス種類にも依存するが自作自演などができてしまうため、サービス提供側としては望ましい行為ではない。

3. 提 案 手 法

3.1 要 件 検 討

前述した PseudoID でのアカウント生成における問題点の解決として、BSS において IDP でのアカウント生成の管理を導入する。利用者によるアカウントの乱発を抑制するものである。すなわち、BSS は IDP でのアカウント生成済みのユーザから申請がなされた場合は、その旨を利用者に通じてトークンの生成を行わない。本機能の付加についてと安全性と運用面を考慮して次の要件を置く。

(1)　PseudoID の概念を引き継ぎ、IDP でのアカウントを匿名的なものとするため BSS と IDP のアカウントの紐づけを双方に保持させない。

(2)　IDP のアカウントを削除した場合は BSS でのトークン発行回数を回復する。

(1) は、情報漏洩のリスク低減と利用者のプライバシ保護の観点からの要件であり、(2) が運用面での要件となる。このため、IDP でのアカウントの生成確認に加えて、IDP でのアカウント削除の機能が必要となる。以下提案手法でのアカウント生成手順と、削除手順について説明する。説明にあたり、また、IDP と BSS は信頼関係を持ち、双方の公開鍵は公開されておりお互い取得しているとの前提を置くものとする。また、利用者、IDP、BSS 間の通信には暗号化通信路が利用でき、通信内容が第三者に漏洩することはないものとする。

3.2 アカウントの生成手順

PseudoID では、まず、利用者が IDP で利用する予定の ID/password ペアをトークンの内容としていたが、本方式では、IDP が一時的に払い出すユニークな乱数を利用者が取得し代用している。このため、IDP での ID/password は IDP がトークンの署名を検証できた後に IDP 側で利用者が指定する。また、この乱数は、利用者によるトークン再利用の防止と、アカウント生成後の管理にも利用されている。

以下手順について説明する。また、そのシーケンスを図 5 に示す。

(1)　利用者は、まず IDP にアカウント生成を申請する。

(2)　IDP は、申請をうけて、IDP でユニークとなる乱数 R_{IDP} を生成し、利用者に送付する。また、生成した R_{IDP} について、生成の時間を記録しておく。この乱数には有効期限を設定しており、期限を過ぎた場合は失効される。

(3)　利用者は、$T = R_{IDP}$ として、ブラインドの処理を行い、$B(T)$ を作成する。

(4)　利用者は、ID_{BSS}, PW_{BSS} を用いて、BSS にログインする。

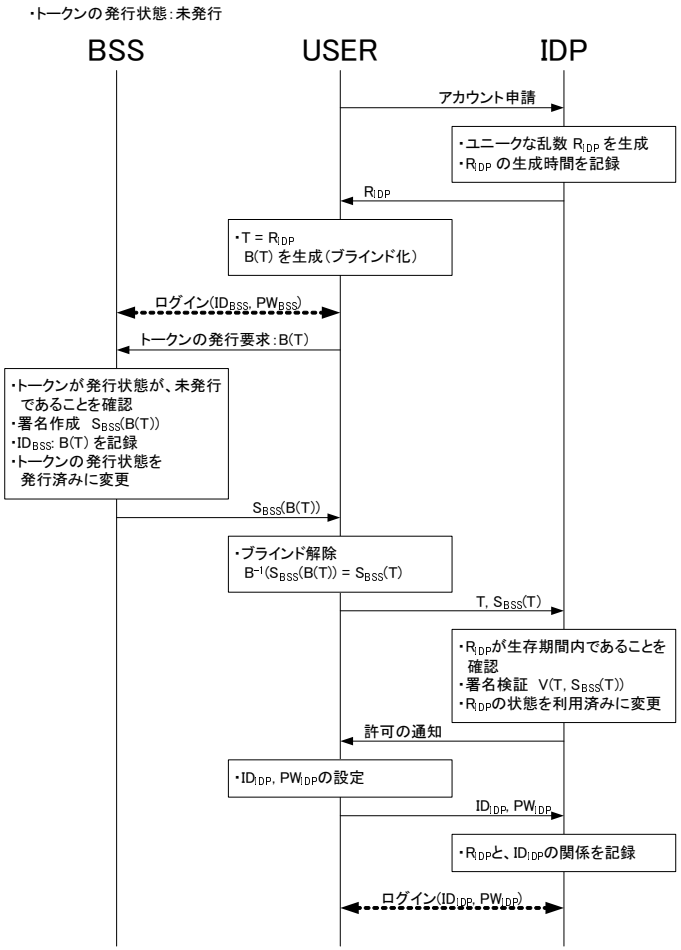

図 5 提案手法でのアカウント生成手順

(5) 利用者はトークンの発行申請として、$B(T)$ への署名を求める。

(6) BSS は、利用者のトークン発行状態を調べて、未発行であれば、BSS は、署名 $S_{BSS}(B(T))$ を生成するとともに、ID_{BSS} に紐づけて、$B(T)$ を管理する。また、利用者のトークンの発行状態を、「発行済み」に変更する。トークンの発行状態が、発行済みの場合は、処理を中止する。

(7) BSS は、生成した署名を利用者に送付する。

(8) 利用者は、B^{-1} を用いて、ブラインドを解除し、$S_{BSS}(T)$ を得る。

(9) 利用者は、IDP に対して、$T, S_{BSS}(T)$ を送付する。

(10) IDP は、T より、R_{IDP} を取得し、状態として、既にアカウントと紐づいていないか、利用済みでないか、有効期限を過ぎていないかを確認し、どの場合でもない場合は引き続き、署名の検証 $V(T, S_{BSS}(T))$ を実施する。正しく検証できたならば、R_{IDP} の状態を利用済みとする。

(11) IDP は、利用者にアカウント生成の許可を通知する。

(12) 利用者は、自身で、IDP でのアカウント (ID_{IDP}, PW_{IDP}) を登録し、以降のログインに利用する。

正しくアカウントが生成された場合には、BSS は、$(ID_{BSS}, B(T))$ を、IDP は、$(ID_{IDP}, T = (R_{IDP}))$ の関係性を保持している。

3.3 アカウントの削除手順

アカウントの削除も、アカウント生成時同様にブラインド署名を用いて実現される。削除手順の場合には、BSS が乱数 R_{BSS} を生成している。アカウント生成の手順において IDP が生成した乱数同様に、トークンの再利用を防ぐために利用されている。手順を以下に記し、また、図 6 にシーケンスを示す。

(1) 利用者は、まず BSS にログインする。

(2) IDP でのアカウントを削除する予定であることを通知する。

(3) BSS は、当該利用者のトークンの発行状態が、「発行済み」であることを確認し、利用者のアカウントである、ID_{BSS} から、検索し、アカウント生成の際に利用者から送付された $B(T)$ を得る。また、ユニークな乱数 R_{BSS} を生成し、ID_{BSS} と $B(T)$ と併せて管理する。

(4) BSS は、BT と R_{BSS} を、利用者に送付する。

(5) 利用者は、トークン $D(= B(T)||R_{BSS}||ID_{BSS})$ として、ブラインド処理 $B(D)$ を行う。

(6) 利用者は、ID_{BSS}, PW_{BSS} を用いて、IDP にログインする。

(7) 利用者は、IDP に対してアカウントの削除申請を行い、$B(D)$ を提出する。

(8) IDP は、提出された $B(D)$ に対して、署名 $S_{IDP}(B(D))$ を生成する。ID_{IDP} を用いて、R_{IDP} を検索し、R_{IDP} の状態を、「アカウント削除済み」とする。最終的に、

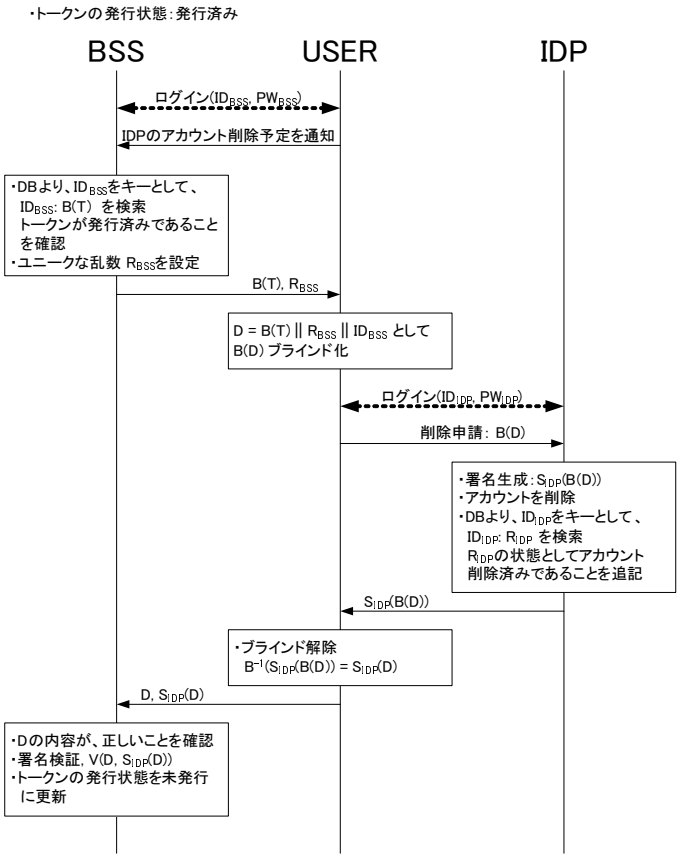

図 6 提案手法でのアカウントの削除

利用者のアカウントを削除する。

(9) IDP は、利用者に $S_{IDP}(B(D))$ を送付する。

(10) 利用者は、$S_{IDP}(B(D))$ のブラインドを解除し、$S_{IDP}(D)$ を得る。

(11) 利用者は、BSS に、$D, S_{IDP}(D)$ を提出する。

(12) BSS は、D の内容 $(ID_{BSS}, B(D), R_{BSS})$ が自身が管理している情報と一致するを確認した上で、署名検証を実施する。正しく検証できたならば、トークン発行の状態を、未発行に更新する。

本手順を用いることにより利用者は、IDP でのアカウントの削除も BSS に対してアカウント内容を秘匿したままで可能であり、一度 IDP の利用を中止し、必要に応じて再度申請することで利用を再開できることとなる。

3.4 考　　察

提案手法について考察する。前述の削除手段を導入することにより要件 (2) は満たされている。また、削除手段での削除申請でも、ブラインド署名が利用されており、IDP、BSS 双方のアカウントが紐づけされることもなく、要件 (1) も満足されている。本提案手法を利用することで、IDP では不作為なアカウント生成を低減できるというメリットがあり運用コストの削減を図ることができる。

BSS と IDP が生成する乱数 R_{BSS}, R_{IDP} は、トークン再利用の防止に利用されている。これらを用いない場合、利用者は、一度払いだされたトークンを再び利用することができ、BSS の許可を受けることなく、IDP でのアカウント生成ができることとなる。一度、生成及び削除で利用された乱数は、BSS 及び、IDP は利用済みの状態として以降取り扱う。以降、同じ乱数 R_{IDP}, R_{BSS} を持つトークン T 及び、D が再利用されることはない。利用者は、IDP に最初の申請をすることなく適当な値を用いて、トークン T を生成することも可能であるが、IDP で発行された乱数 R_{IDP} には期限があるため、他のユーザに配布されたアクティブな値を利用できる可能性は低い。

また、本手法では、BSS と IDP 間では直接一連のセッションの管理を実施していない。このため、手順の途中で通信障害や、処理エラーが発生した場合は、BSS でのトークンの払い出し状況と IDP でのアカウントの生成状況が一致しなくなりえるが、利用者側に不利になるよう構成されており、BSS でのトークンの払い出しの状態が未発行であるにも関わらず、IDP 側でアカウントが生成されている状況にはなりえない。この場合は、回復処理として、利用者はブラインドの逆処理を BSS に開示する。BSS は、保持している、$B(T)$ から、$T = R_{IDP}$ を得る。BSS は、IDP に R_{IDP} の状態を確認することにより、IDP でのアカウントの生成状態が確認できるため、状況に応じて、トークンの発行状態のステータスを変更する。その後、利用者はブラインド処理のための鍵を変更する。

また、本手法では、複数アカウントの生成ができなくなるように構成しているため、利用者のプライバシ保護の条件が Dey らの提案から緩和されている。オリジナルの手法では、BSS は署名を生成するだけであり、利用者がどの IDP でアカウント生成をしているかについて検知はしていない。これに対して、著者らの手法では、BSS と IDP に信頼関係がある

ことが前提であるため、BSS はどの IDP へトークンを払い出しているかが明白となっている。また、本提案のモデルでは、BSS と IDP が 1 対 1 となっているが、実際の利用を考慮した場合には、ひとつの認証機関 (BSS) が、複数の IDP へ対応することがが必要である。

4. おわりに

本稿では、利用者のプライバシ保護を目的したアカウント管理手法である PseudoID を拡張し、BSS でのアカウントの生成管理を導入することにより、利用者による複数アカウントの生成を排除した。BSS でのアカウントの削除においても、ブラインド署名を利用しているため、アカウント情報の紐づけは BSS 及び IDP に対して秘匿されており、IDP クラック時のリスクは低減される。今後は提案手法のさらなる機能拡張について検討を行うとともに、機能検証を進める予定である。

参 考 文 献

1) Security Assertio Markup Language (SAML) V2.0, OASIS (2005), http://www.oasis-open.org/specs/index.php#samlv2.0
2) OpenID Authentication 2.0 - Final, OpenID Foundation, (2007), http://openid.net/specs/openid-authentication-2_0.txt
3) Dey, A. and Weis, S.:PseudoID: Enhancing Privacy in Federated Login, *Proc. 3rd Hot Topics in Privacy Enhancing Technologies(HotPETs 2010)*, pp.95-107 (2010).
4) Chaum, D.:Blind signatures for untraceable payments. *CRYPTO,* pp.199-203 (1982).
5) Diffie, W. and Hellman, M.E.:New directions in cryptography, *Trans. on Information Theory, IEEE*, Vol. 22, Issue 6, pp. 644-654 (1976).