マルチサービス環境に適したリンク不能性を実現するID管理方法

野原, 康伸
九州大学大学院システム情報科学府

井上, 創造
九州大学大学院システム情報科学研究院

安浦, 寛人
九州大学大学院システム情報科学研究院

出版情報：コンピュータセキュリティシンポジウム2004(CSS2004) 論文集, pp.139-144, 2004-10. 情報処理学会コンピュータセキュリティ研究会
バージョン：

マルチサービス環境に適したリンク不能性を実現するID管理方法

野原　康伸† 　　井上　創造‡ 　　安浦　寛人‡

†九州大学大学院 システム情報科学府
816-8580 福岡県春日市春日公園 6-1
nohara@c.csce.kyushu-u.ac.jp

‡九州大学大学院 システム情報科学研究院
816-8580 福岡県春日市春日公園 6-1
{sozo,yasuura}@c.csce.kyushu-u.ac.jp

あらまし 近年急速に，ICカードやRFIDといったIDデバイスが普及し，ユーザが一つのデバイスで複数のサービスを受けられるという，マルチサービス化が進展している．しかし，単一のユーザIDを複数のサービス提供者が共有すると，個人の行動履歴がリンクされ，個人の行動を追跡できるという問題が生じる．

本稿では，第三者やサービス提供者間に対するリンク不能性を実現しつつ，サービス提供者は自己の持つユーザ情報のリンクは可能であるようなID管理方法を提案する．提案方法は，ユーザIDをサービス提供者毎に異なるものにし，ユーザとサービス提供者間のIDの照合をハッシュ関数や公開鍵暗号を用いて安全に実現することで，マルチサービス環境に適したリンク不能性を実現する．

Privacy-protecting ID Management for Multi-service Environments

Yasunobu NOHARA† 　　Sozo INOUE‡ 　　Hiroto YASUURA‡

†Graduate School of Information Science and Electrical Engineering, Kyushu University
6-1 Kasuga-koen, Kasuga-shi
Fukuoka, 816-8580 Japan
nohara@c.csce.kyushu-u.ac.jp

‡Faculty of Information Science and Electrical Engineering, Kyushu University
6-1 Kasuga-koen, Kasuga-shi
Fukuoka, 816-8580 Japan
{sozo,yasuura}@c.csce.kyushu-u.ac.jp

Abstract Recently, ID devices such as smart cards and RFID tags are introducing multi-service environments, in which a user can receive many services by one ID device. However, there exists a problem that service providers can trace a user's behavior by linking the user's access history, if only one ID is assigned for the user.

In this paper, we propose privacy-protecting ID management scheme for multi-service environments. Our scheme provides unlinkability of users' accesses against third service providers, by preparing different user IDs for each service, and by using cryptographic protocol to exchange the ID between a user and a service provider, while linkability is assured between the user and the provider involved.

1　はじめに

近年急速に，ICカードやRFIDといったデバイス (**IDデバイス**) が普及し，ユーザが一つのIDデバイスで複数のサービス提供者からのサービスを受けられるという，マルチサービス化が進展している．しかし，単一のユーザIDを複数のサービス提供者が共有した場合，第三者やサービス提供者がデバイスのIDを読み取ることにより，個人の行動履歴がリンクされ，個人の行動を追跡できるという問題が生じる

これに対し，第三者やサービス提供者には複数のアクセスが同一ユーザによるものか判定できない，というリンク不能性の概念 [2][3] といくつかの実現技術が提案された [4]-[7]．しかし，マルチサービス環境を想定していなかったり，

個々のユーザに応じたサービスを提供するには支障をきたしたりといった問題があったと考えられる．

本稿では，第三者やサービス提供者間に対するリンク不能性を実現しつつ，サービス提供者は自己の持つユーザ情報のリンクは可能であるような ID 管理方法を提案する．提案方法は，我々が以前提案した PID システム [1] という電子サービスを行うための社会基盤システムをベースとしている．PID システムにおいて，ユーザを表す ID をサービス提供者毎に異なるものにし，ユーザとサービス提供者間の ID の照合と相互認証をハッシュ関数や公開鍵暗号を用いて安全に実現することで，マルチサービス環境に適したリンク不能性を実現する．

本稿の構成は以下の通りである．2 章でリンク不能性について説明し，既存の実現技術について述べる．3 章で我々の提案するマルチサービス環境に適した ID 管理方法を述べる．4 章で提案方法の評価を行う．最後に 5 章で本稿をまとめる．

2　リンク不能性

RFID デバイスに付けられた ID 自体には，氏名や住所といった個人情報を含まないようにすることは可能である．しかし，誰でも自由にデバイスの ID を読み取れるとすると，ユーザの意思に関わらず，第三者 (関係のない他のサービス提供者を含む．以下同じ) が様々な場所でユーザに無断で ID を読んで，ID を元にユーザの行動履歴を関連付け (リンク) することができる．その結果，ユーザの行動が追跡されてしまうというプライバシー上の問題が生じる [5].

これらのことから，第三者が自由に ID を読めずに，ユーザの行動履歴をリンクできないというリンク不能性の概念が重要となる．

2.1　リンク不能性の定義

リンク不能性 (Unlinkability) は，ユーザが複数の資源あるいはサービスを使用するとき，他人がそれらを一つにリンクできないようにして使用できることを保証する性質である [2].

別の言い方をすると，二つ以上の通信やイベントがあった場合に，他人がそれらに関連があるかどうか (同一人物からのアクセスであるか等) の判定をできず，サービスの利用前も利用後も，他人が保持するユーザ情報に変化がないという性質である [3].

以下本稿では，リンク不能性について以下のように定義する．ユーザ A の持つ ID デバイスから主体 X が取得した n 番目の情報 (ID 情報や利用履歴を含む) を I^n_{AX} としたときに，主体 X が I^n_{AX} と I^m_{AX}(ただし，$m \neq n$) の送信元が同一のユーザによるものであると判定できない場合，**ユーザ A の情報は，主体 X に対してリンク不能性を有する**という．つまり，主体 X が I^n_{AX} と I^m_{AX}，I^l_{BX} を本質的に区別することができないことを意味する．

また，主体 X と主体 Y が協力して，それぞれが持つ情報を持ち寄った場合に，I^n_{AX} と I^k_{AY} の送信元が同一のユーザによるものであると判定できない場合，**ユーザ A の情報は，主体 X と主体 Y 間に対してリンク不能性を有する**という．

2.2　関連研究

RFID システムにおいて，第三者に対するリンク不能性を実現したものとして，Randomized Hash Lock 方式 [4] や可変秘匿 ID 方式 [5]，ワンタイム ID 方式 [6] がある．これらの方式は，ID に乱数を付加したものをハッシュ化または暗号化することで，秘密情報を知らない者には ID が取り出せないようにし，第三者に対するリンク不能性を実現している．しかし，マルチサービス環境を想定したものとはなっていない．

IC カードを用いた情報システムとして，グループ署名を利用した匿名認証システム [7] がある．このシステムでは，グループ署名の性質を利用して，第三者ばかりでなくサービス提供者に対してもリンク不能性を実現している．ただし，サービス提供者はユーザが正規の利用者であることの検証はできるようになっており，管理機関は，ユーザ情報のリンクが可能であるの

で，ユーザに対して課金を行う必要があるサービスについても実現できる．このシステムでは，サービス提供者に対するリンク不能性も満たしているため，高いプライバシー保護が可能であるが，サービス提供者は各ユーザに応じたサービスを実現できないという問題点がある．

2.3 マルチサービス環境におけるリンク不能性

このように，単一サービス環境におけるリンク不能性については，いままでに議論が行われてきた．しかし，今までマルチサービス環境におけるリンク不能性は議論されることは少なかった．

マルチサービス環境において新たに発生する問題として，複数のサービス提供者が持つユーザの履歴情報のリンクの問題がある．今までのIDデバイスは，デバイスに付けられた単一のIDを複数のサービス提供者で使用していた．そのため，各サービスにおけるユーザの履歴 (何をどこで買った等) を単一IDを元にリンクできることが可能である．サービス提供者間でユーザの履歴が共有されると，ユーザの行動が追跡され，ユーザのプライバシーを侵害される危険性があった．マルチサービス環境において，サービス提供者間に対するリンク不能性を実現することは重要である．

3 提案方法

3.1 システムのモデル

我々が提案するID管理方法のモデルについて述べる．本モデルは，我々が以前提案したPIDシステム [1] をベースとしている．モデルには3つの主体と，PID(Personal IDentifier) という一種の個人IDが登場する．

3つの主体とは，ユーザ，発行者，サービス提供者であり，これらは次のように定義される．

- ユーザ：サービスと取引を行う主体．発行者からPIDを発行される．複数存在する．
- 発行者：PIDの発行管理を行う主体．一者のみ存在する．
- サービス提供者：ユーザにサービスを提供する主体．複数存在する．

PIDは発行者がユーザに対して発行する長いビット列であり，各ユーザに対して固有のものである．PIDの一部分のビット列のことをsubPIDとよび，このsubPIDが各サービス提供者に割り当てられる．

ユーザ i のPID(PID_i) のうち，サービス提供者 j に割り当てられたsubPIDを sid_{ij} とすると，$sid_{ij} = f(PID_i, ID_j)$ で与えられる．ここで，ID_j はサービス提供者 j を特定するためのIDであり，f は PID_j から ID_j に対応するアドレスの sid_{ij} を取り出す関数である．

subPIDは，ある同一のサービス提供者 j において重複せず，唯一となるように割り当てられる．すなわち，任意の $i \neq i'$ 及び j について，$sid_{ij} \neq sid_{i'j}$ である．

ユーザとサービス提供者が取引を行うための手順は以下の通りである．

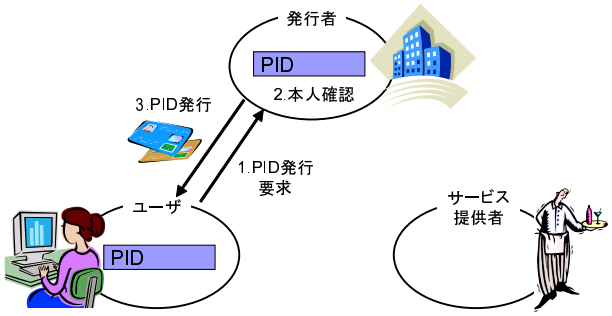

図 1: PID 発行までのプロセス

STEP1: まず，発行者はユーザの本人性を確認し，本人に対してPIDを発行する (図1参照)．発行されたPIDは，IDデバイスに保存されて，ユーザに提供される．また，発行者側はPIDを厳重に管理されたデータベースに保存しておく．

STEP2: サービス提供者がユーザにサービスを行う場合，サービス提供者は発行者に対してユーザとの取引を打診する．発行者

はサービス提供者 j に対して subPID のリスト $SID_j = \{sid_{1j}, sid_{2j}, \cdots, sid_{nj}\}$ を提供する (図 2 参照).

サービス提供者は，subPID を厳重に管理されたデータベースに保存する．サービス提供者は，subPID 以外のユーザに関する情報は原則として受け取ることができない．subPID とユーザの本人性については発行者が保証を行う．

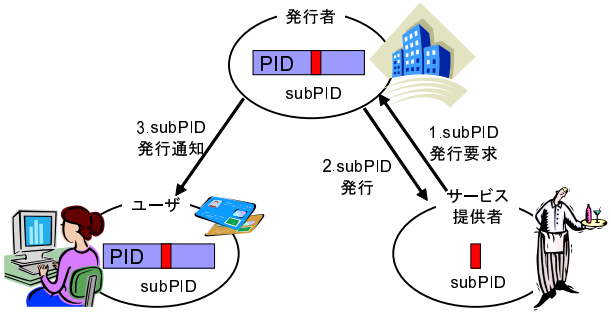

図 2: サービス提供者の subPID 取得までのプロセス

上記の手順により，ユーザ及び発行者は PID，サービス提供者は PID の一部である subPID という情報を共有することができる．ユーザとサービス提供者はお互いの持つ subPID を利用して，次節で示す ID 照合を始めに行い相手を特定する．その後ユーザとサービス提供者の間で認証や ID デバイス内のデータアクセスといった通常のサービス提供が行われる．

各サービス提供者には，利用者の PID のうち異なるアドレスの subPID が与えられる (図 3 参照)．それぞれの subPID は，サービス提供者ごとに異なる．すなわち，任意の i 及び $j \neq j'$ について，$sid_{ij} \neq sid_{ij'}$ である．

ユーザとサービス提供者の保有する情報をまとめると，次のようになる．

- ユーザ: PID 及びサービス番号とサービス提供者の保有する subPID のアドレスの組
- サービス提供者: 各ユーザに対するサービス番号と subPID のリスト

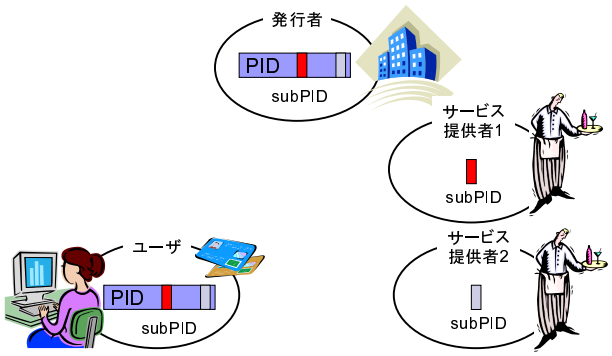

図 3: 1 人のユーザが複数のサービスを受ける場合の subPID の発行

3.2 ID 照合・認証プロトコル

本節では，ハッシュ関数を用いて，第三者に対するリンク不能性を満たすように，ユーザとサービス提供者の間で相手の識別と相互認証を行う，ID 照合・認証プロトコルについて説明する (図 4 参照).

既存の認証プロトコルは，認証を行うに先立って，ID の交換を行うことが前提である．そのため，第三者に対するリンク不能性を満たすことが出来ない．そこで本プロトコルでは，以下のようにして事前の ID 交換なしに相互認証を行う．

STEP1: ID デバイスは，サービス提供者に認証要求を出す

STEP2: サービス提供者は，自分のサービス番号 ID_j と乱数 R_s を ID デバイスに対して送信する．

STEP3: ID デバイスは，ID_j と自分の持つ PID_i から，当該のサービス提供者に対応した $sid_{ij} = f(PID_i, ID_j)$ を取り出す．また乱数 R_u を生成する．サービス提供者には，R_s, R_u および sid_{ij} を連結し，ハッシュ化した $H_u = H(R_s||R_u||sid_{ij})$ と R_u を送信する．

STEP4: サービス提供者は，subPID のリスト SID_j から $H_u = H(R_s||R_u||sid_{ij})$ となる sid_{ij} を検索する．

STEP5: サービス提供者は，sid_{ij} と R_u をハッシュ化した $H_s = H(sid_{ij}||R_u)$ を ID

デバイスに送信する．

STEP6: ID デバイスは，$H_s = H(sid_{ij}||R_u)$ となるか検証する．

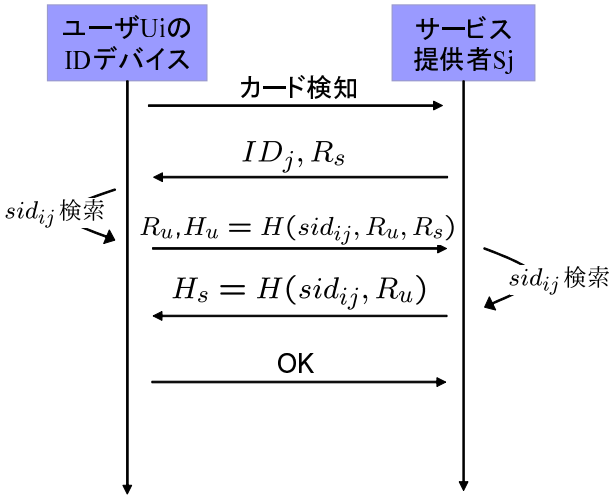

図 4: ハッシュ関数による ID 照合・認証

本プロトコルであれば，ユーザの ID がハッシュ化されており，その値も毎回変化するので，第三者に対するリンク不能性を満たすことが出来る．一方，サービス提供者は，検索した sid_{ij} でユーザ情報をリンク可能である．

本プロトコルは，サービス提供者側において，全ユーザの subPID に対するハッシュ計算 (STEP4) が必要になるため，ユーザ数が増えるほどサーバへの負担も増大する．

STEP3 において，ユーザがハッシュ関数を用いた H_u そして R_u の代わりに，サービス提供者の公開鍵を用いて暗号化した $E_{KS_j}(R_s||R_u||sid_{ij})$ を送信するようにすれば，サービス提供者が秘密鍵で復号化することにより，sid_{ij} を取り出せるためこの問題は解決する．しかし，デバイスに公開鍵暗号を実装しなければならなくなり，デバイスの実装コストと，鍵管理方法を考慮する必要がある．

4 提案方法の評価

本章では，提案方法が実現するリンク不能性と，提案方法に対して想定される攻撃とその防御策について考察する．

4.1 提案方法が実現するリンク不能性

ユーザの ID は乱数と合わせてハッシュ化されているため，ID リストを持たない第三者は ID を取得することができない．よって，第三者に対するリンク不能性を満たすことができ，第三者によるユーザの行動追跡を防ぐことができる．

サービス提供者は，ID リストを持っているため，ユーザの ID を知ることができ，サービス提供者はユーザ情報をリンクすることが可能である．しかし，各サービス提供者が結託してもそれぞれの ID は異なるため，提供者間で情報のリンクは出来ず，サービス提供者間でのリンク不能性を満たす．これらのことから，サービス提供者は，個々のユーザに応じたサービスを実現することができるが，他のサービス提供者と結託してのユーザ情報のリンクを阻止できる．

発行者は，ID 全体を保有しているので，何か問題が発生した場合は，リンクを行い，ユーザの責任を追及できる．

このように，提案方法はマルチサービス環境に適したリンク不能性を実現することができる．

4.2 ID 照合・認証に対する攻撃：なりすまし

本攻撃は，攻撃者がハッシュ値 H_u として適当な値をサービス提供者に送ることで，誰かになりすましてサービスを受けるという攻撃である．ユーザ数 N に比例して，攻撃者が送った値 H_u が，ユーザの誰かの subPID をハッシュ化したものと一致する可能性が高くなるので，N が大きいほど攻撃の成功確率が上がる．

本攻撃に対して，通常のハッシュ関数による認証と同程度の安全性を保つためには，通常のハッシュ関数による認証よりも，鍵長 (subPID の長さ) 又はハッシュ関数の出力長を $\log_2 N$[bit] 増やす必要があると考えられる．

4.3 サービス提供者間のリンク不能性に対する攻撃

提案システムは，4.1 節で述べたようにサービス提供者間に対してリンク不能性を有している．

しかし，複数のサービス提供者が事前にsubPIDリストの共有を行っていると，攻撃を行うに当たって制約があるが，以下のような攻撃によってサービス提供者間に対するリンク不能性が破られる場合がある．

4.3.1 subPID 共有

複数のサービス提供者が，ある一つのサービス提供者のsubPIDリストのみ使用してサービスを行っていくものである．本攻撃を行うに当たって，攻撃者であるサービス提供者は，サービス提供者毎に独自のサービスを実現することはできないという問題がある．

4.3.2 多重 subPID 照合

まず，複数あるサービス提供者のうち，一方のサービス提供者のsubPIDリストでID照合を行う．続けて，残りのサービス提供者のsubPIDリストでID照合を行う．複数回のID照合を行う間隔が十分短いならば，その間にIDデバイスが移動することはないといえるため (物理的制約)，それぞれのサービス提供者のsubPIDリストによるID照合によって得られた情報は，同一のユーザのものであると判定できる．つまり，サービス提供者間のリンク不能性が破られる．ただし，本攻撃を行うには，攻撃者であるサービス提供者は，IDであると同時に，相互認証のための鍵でもあるsubPIDを他のサービス提供者に開示しなければならない．

本攻撃に対する対策としては，IDデバイスが，短期間に複数のID照合がされた場合に応答を拒否するようにすることが考えられる．

5 おわりに

本稿では，マルチサービス環境に適したID管理方式を提案した．提案方法は，サービス提供者間に対するリンク不能性を実現でき，マルチサービス環境に適したID管理方法である．今後は，ID照合・認証でのサーバに必要な計算量を減らす方法について考察を行っていきたい．

謝辞

ご議論いただいたNTT情報流通プラットフォーム研究所の森田光氏，九州大学の馬場謙介助手，浜崎陽一郎・納富貞嘉両研究員をはじめとするシステムLSI研究室の諸氏に感謝します．

本研究は，平成14-18年度科学研究費補助金学術創成研究・課題番号14GS0218および，平成15-16年度科学研究費補助金若手研究・課題番号15700100によるものである．

参考文献

[1] 浜崎陽一郎, 安浦寛人,“PIDを用いた安全な社会システムの構想”, DICOMO2002シンポジウム論文集 pp535-538, 2002年6月

[2] “ISO/IEC 15408 - INTERNATIONAL STANDARD Information technology - Security techniques - Evaluation criteria for IT security - Part2: Security functional requirements”, Dec.1999

[3] Andreas Pfitzmann, Marit Hansen, “Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology”, http://www.freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf, May.2003.

[4] S.A Weis,“Security and Privacy in Radio-Frequency Identification Devices”, Masters Thesis, MIT, May. 2003

[5] 木下真吾, 星野文学, 小室智之, 藤村明子, 大久保美也子,“RFIDプライバシー保護を実現する可変秘匿ID方式”, CSS2003論文集 pp.497-502, 2003年10月

[6] 今本健二, 櫻井幸一,“信頼できる第三者機関を用いたユーザID情報保護可能な鍵共有プロトコル”, CSS2003論文集 pp.451-456, 2003年10月

[7] 加藤岳久, 岡田光司, 吉田琢哉,“プライバシを保護する匿名認証システムの開発”, CSS2003論文集 pp.569-574, 2003年10月