2005－ＣＳＥＣ－30 (66)
2005／7／22

プライバシを考慮したアイデンティティ制御方法

森藤 元† 川崎 明彦‡ 森田 豊久‡ 宝木 和夫‡

†株式会社日立製作所システム開発研究所 〒215-0013 川崎市麻生区王禅寺 1099 番地

E-mail: †{morito, akihiko, morita, takara}@sdl.hitachi.co.jp

あらまし 個人情報保護法が 2005 年 4 月に全面施行され，プライバシ保護に対するニーズがかつてなく高まっている．本稿では，実名，偽名，匿名を渡り歩く技術の一実現手段を検討している．ここでは，受信者の権限に応じて匿名から偽名，実名を復元できるレベルを決めることができ，さらに送信者の意思により実名，偽名，匿名を選択できるアイデンティティ制御方法を考案した．

キーワード 個人情報，プライバシ，実名，偽名，匿名

Identity Control Method considering Privacy

Hajime MORITO† Akihiko KAWASAKI‡ Toyohisa MORITA‡ and Kazuo TAKARAGI‡

† Systems Development Laboratory, Hitachi, Ltd. 1099 Ohzenji, Asao-ku, Kawasaki, 215-0013, Japan

E-mail: †{morito, akihiko, morita, takara}@sdl.hitachi.co.jp

Abstract With the complete introduction of the law for protecting personal information in April 2005, the needs concerning protection of privacy have become ever more demanding. Accordingly, in this paper, the authors propose an "identity control" method that can (i) set the disclosure level for revealing the real name and pseudonym from the antonym according to the receiver's authority and (ii) select the real name, pseudonym or antonym according to the will of the sender.

Keyword Personal Information, Privacy, Real Name, Pseudonym, Anonym

1. はじめに

近年，ITシステムのプライバシ問題に関する議論が盛んである．

物理的な人や物をITシステムが扱う場合，通常，対象となる人や物を特定する識別子（ID）を利用する．人や物を特定するためのIDは，その性質上，固定の値をとる固定IDとなる．人を特定するための固定IDを開示することは，本人を特定することと同義である．物を特定するための固定IDであっても長期間同一の人が所持することがわかっているならば，開示することが所有者を特定することにつながりうる．従って，人の場合でも物の場合でも固定IDの開示はプライバシの問題に絡む可能性がある．

本稿では固定IDを通信時に隠蔽する方法を提供することにより，送信者が意図しない固定IDの流出を防止する手段について述べる．また，受信者の権限や送信者の意思に応じてIDに関する情報の開示レベルを切り替えられる手段について述べる．

以下では，まずIDとプライバシに関する従来の研究について述べる．つづいて固定IDの開示をコントロールすることでプライバシを保護する提案方式について述べる．

2. IDとプライバシに関する従来の研究

固定IDが問題となる例として無線ICタグ（RFIDタグ）があげられる．無線ICタグはリーダが発する読み取り信号を受信すると，搭載するメモリの内容を返信する小型の電子回路である．現存する多くの無線ICタグは，返信内容に各無線ICタグ固有の固定IDを含む．このため，無線ICタグを一般消費者が持ち歩く物に付加した場合，例えばある場所に同じ物が繰り返し現れたという事象や，ある時刻・場所で観測された物が別の時刻・場所で観測されたという事象がその物を所有する個人の行動履歴として容易に結びつけて記録可能となるということから，プライバシ侵害につながる可能性が高いとして，昨今議論の対象となっている

[1].

これを解決するために無線 IC タグがリーダに返信する ID を頻繁に変化させるという対策が提案されている．代表的なものとして，「可変秘匿 ID 方式」[2]や「Extended Hash-chain 方式」[3]などがある．これらの方式においては，リーダが無線 IC タグに読み取り要求を発した際，無線 IC タグは固定 ID である正規の ID を返すのではなく，秘匿 ID を返す．リーダは無線 IC タグから返された秘匿 ID をバックヤードの信頼できるセキュリティサーバに送り，セキュリティサーバが許可されたリーダに対して無線 IC タグの正規の ID を答える．これらの方式では，セキュリティサーバに登録された正当なリーダによる読み取りによってのみ無線 IC タグの正規の ID を知ることができる．また，無線 IC タグが返す秘匿 ID を頻繁に変化させる仕組みが用意されることで，秘匿 ID が新たな固定 ID となることを防止している．

しかし，この方法では同じ人や物だと判断するには正規の ID まで暴露する必要がある．

ID に関する別のケースとしてユーザ ID を用いた認証がある．IT システムをユーザが利用するに当たり，システムはユーザを特定するためのユーザ ID を発行する．アプリケーション毎に本人性を確認しようとすると常に同じ固定 ID がやりとりに使われてしまい，アプリケーションを超えた名寄せが行われる可能性がある．

これを解決するために本人性を持った ID を登録する機関を設け，通常利用する ID はこの機関が発行する本人性を持たない ID を使用するという対策が提案されている．代表的なものとして，「仮想 ID」[4]がある．この方式においては，ユーザは本人性に関わる情報を登録証明局（CA）にのみ開示する．CA は，ユーザの求めに応じてユーザの個人情報にリンクされた仮想 ID（VID: Virtual ID）を発行する．VID には CA の証明書がついており，VID を受け取ったアプリケーションは VID についた証明書を CA に送ることで，その VID が CA によって発行された有効な VID であることを確認する．アプリケーションは VID によりユーザの同一性を確認しつつサービスを提供できるが，VID にはユーザの本人性を特定する情報が含まれないため，ユーザはアプリケーションに対し本人性に関わる情報を秘匿できる．

しかし，この方法では VID を受け取った側が VID から本人性を特定する手段がない．

本稿では，ID に「実名」「偽名」「匿名」の 3 つのレベルを持たせ，受信者の権限や送信者の意思に応じて開示レベルを切り替えられる方法を述べる．

3. 提案方式

ID の開示がプライバシの問題として認識されやすい事例として，消費者と企業の商取引を例とする．一般的な商取引において，ID を開示する送信者は消費者であり，ID を利用する受信者は企業である．消費者側から見ると，自分の個人情報を企業にどれだけ開示するかをコントロールできることが重要となる．企業側から見ると，必要なときに必要な消費者の個人情報を閲覧できることと，個人情報の業務外での不正な閲覧や漏洩を防止することが重要となる．

本稿で使用する用語を定義する．

名前 名前とは行為主体をあらわす識別子（ID）である．

実名 実名とはそれが明らかになることで個人を特定可能な名前である．

偽名 偽名とは同じ値である限り同じ人物であることが保証されるが，それが明らかとなっても特別な知識を持たないかぎり個人を特定不可能な名前である．

匿名 匿名とは一度限り使用され，それが明らかとなっても特別な知識を持たないかぎり個人を特定不可能な名前である．同じ匿名を使用した行動は他に存在しないこととなる点で偽名と異なり，個々の行動を紐付けることは不可能である．

3.1. 機能要件

本節ではまず，ID 管理システムに求められるプライバシ機能を，消費者側および企業側それぞれの視点から列挙する．続いて，実現する機能を決定する．

3.1.1. 消費者から見た機能要件

消費者側から見ると，自分の個人情報を誰にどれだけ開示するかをコントロールできることが重要となる．

- 自分の名前を知られたくない
  - 店舗での買い物において，店員に名前を告げることなくサービスの提供を受けたい．
  - サービスとして会員への特典（ポイントやマイレージ等）がある場合は，名前を明かさないままそれを享受したい．
  - （会員制のサービスなど）名前を開示した場合でも，それを知りうる従業員を必要最小限に絞りたい．
- 自分の行動を追跡されたくない
  - 異なる企業にサービスを受けた場合に，それらを同じ人物が利用したと知られたくない．
  - 同じ企業に異なる時刻，場所でサー

ビスを受けた場合に，それらを同じ人物が利用したと知られたくない．

- 開示する情報を自分でコントロールしたい
  - あるときは実名でサービスを享受したい．何らかの理由で実名を開示する場合は，明示的にこれを指示できるようにしたい．
  - あるときは別人として（別の偽名で）サービスを享受したい．消費者の過去の購買履歴などからおすすめの商品を斡旋してくれるようなサービスを考えると，異なる嗜好に基づく購買においては別人として（別の偽名で）取引できた方が嗜好の整合性が保たれて都合が良い場合がある．
  - あるときは匿名でサービスを享受したい．通常は会員としての特典が享受できるサービスにおいても，特定の取引については特典を放棄してでも購買履歴紐付け可能な名前を残さないほうが良い場合もある．
- 使い勝手の良いものであってほしい
  - 財布の中に各種カードがあふれる現状からも理解されるとおり，店舗ごと，企業ごとに異なるものを使い分けることは煩雑である．複数の店舗，企業との取引において共通に利用できるものであることが望ましい．

3.1.2. 企業から見た機能要件

企業側から見ると，必要なときに必要な消費者の個人情報を閲覧できることと，個人情報の業務外での不正な閲覧や漏洩を防止することが重要となる．

- 必要に応じた情報の参照をしたい
  - 現金取引等により匿名で接客する接客担当など顧客情報を必要としない者には，消費者の個人情報を開示しない．
  - マーケティングユースなど顧客の行動履歴を必要とする者には，偽名による取引履歴のみを開示し，それ以上の個人情報を開示しない．
  - 顧客に直接連絡をとる必要がある部署では実名を開示する．
- 消費者へ安心感を訴求したい
  - 消費者から提供を受けた個人情報を，適切に扱っていることを証明したい．
  - 万が一情報の漏洩等の事故が発生した場合，責任の所在を明確にしたい．
- 共通かつカスタマイズが容易なプラットホームを利用したい
  - 導入コスト低減，あるいは他業種とのシナジー効果を期待できる汎用性があってほしい．

3.1.3. 実現する機能

ここでは3.1.1.および3.1.2.での要件についての考察をもとに，本稿で提案する実名，偽名，匿名を渡り歩く技術を実現する機能を述べる．

- 再現性のある偽名

  同じ店舗では同じ偽名でサービスを受けることができるようにする．これで実名は明かさなくとも会員制のサービスを享受できる．

- 通信ごとに変化する匿名

  同じ偽名を使用する場合でも，通信路を流れる名前を毎回異なるものとする．これで同じ名前を検出することによる消費者の行動の追跡を防止できる．

- 消費者が偽名を選択できる

  一人の消費者（一つの実名）が複数の異なる偽名を持てる．異なる偽名を使用した行動は互いに紐付けできないようにする．

- 消費者が開示する情報を実名とするか，偽名とするか，匿名とするかを選択できる

  消費者が望むのであれば実名を開示してサービスの提供を受けることができる．実名は開示しないが，複数のサービスの提供を同一人物として享受したい場合は偽名を開示してサービスの提供を受けることができる．複数のサービスの提供を全て別人として享受したい場合は匿名のみを開示してサービスの提供を受けることができる．

- 企業は，権限に応じて従業員に匿名，偽名，実名を参照させることができる

  消費者の実名を見る権限を有する従業員は匿名に対応する実名を知ることができる．実名を見る権限は持たないが，消費者の行動を紐付け

る権限を有する従業員は匿名に対応する偽名を知ることができる．上記のいずれの権限も持たない従業員は，匿名としてのみ認識できる．

・ 複数の企業間で共通のシステムを構築できる

個別企業ごとのカスタマイズを容易とするとともに，特定の企業，業態に特化しない汎用的な枠組みとすることで，複数の企業間で共通に利用できる．

3.2. 実現形態

3.2.1. 全体構成

送信者は実名を暗号化処理により偽名に，偽名を暗号化処理により匿名に変換して送信し，受信者は受信した匿名をそのまま，あるいは偽名や実名に復号化して利用する（図 1）．送信者は暗号化鍵を変えることにより，受信者による偽名や実名への復号化を制限できる．受信者には，権限により使用可能な鍵の制限を行うことで，業務上不必要な情報を開示しない．

3.2.2. 機能詳細

(1) 暗号化処理装置

実名から偽名を，あるいは偽名から匿名を生成する際には図 2（a）の暗号化処理を行う．暗号化処理の入力は名前 1 とパラメータである．まず名前 1 とパラメータの排他的論理和を計算し，得られた結果とパラメータを連結する．連結して得られたビット列を暗号化鍵を用いて暗号化し，得られた暗号文を名前 2 として出力する．

・ 暗号化 1 処理装置（偽名の生成）

名前 1 として実名を，パラメータとして偽名生成パラメータを入力することで偽名を生成する．実名は常に固定であるので，偽名生成パラメータを変化させて入力することで，異なる偽名を生成できる．一方，同じ偽名生成パラメータを入力することで，過去に生成した偽名を再現できる．

・ 暗号化 2 処理装置（匿名の生成）

名前 1 として偽名を，パラメータとして乱数を入力することで匿名を生成する．同じ偽名を使用する場合でも，乱数が毎回異なる限り，生成される匿名は毎回異なるものである．

(2) 復号化処理装置

匿名から偽名，偽名から実名を復号化する際には

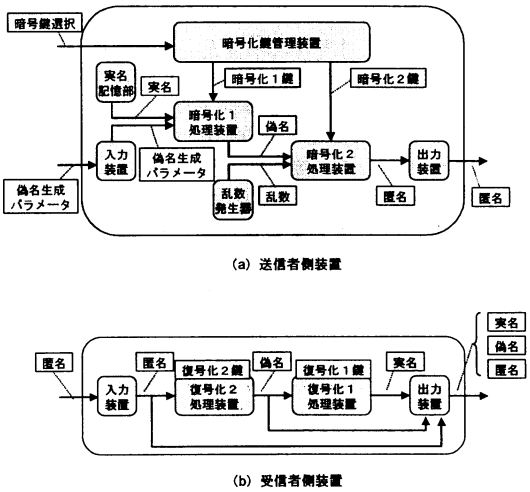
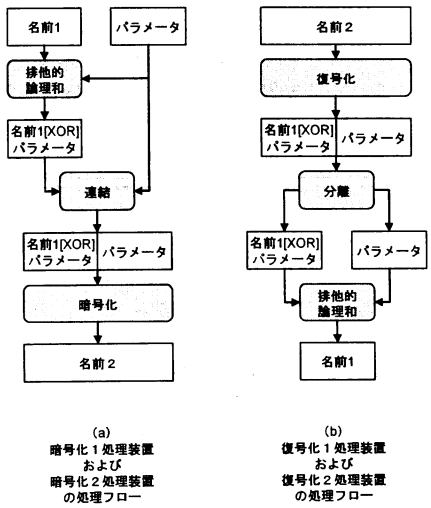


図 1　全体構成



暗号化１処理装置および復号化１処理装置においては，
名前１は実名，パラメータは偽名生成パラメータ，名前２は偽名．

暗号化２処理装置および復号化２処理装置においては，
名前１は偽名，パラメータは乱数，名前２は匿名．

図 2　暗号化処理・復号化処理

図 2（b）の復号化処理に従う．復号化処理の入力は名前 2 である．まず復号化鍵を用いて名前 2 を復号化し，得られた平文を上位ビット列と下位ビット列に二等分する．ここで，下位ビット列は暗号化処理の際のパラメータである．上位ビット列と下位ビット列の排他的論理和を計算し，得られたビット列を名前 1 として出力する．

・復号化2処理装置

名前2として匿名を入力することで偽名が復号化される.

・復号化1処理装置

名前2として偽名を入力することで実名が復号化される.

(3) 暗号化鍵管理装置

入力に従って，暗号化1処理装置または暗号化2処理装置の暗号化鍵を別のものに取り替える.

3.2.3. 機能説明

ここでは，3.1.3.で述べた機能が3.2.2.の詳細機能を用いてどのように実現されるかを説明する.

・再現性のある偽名

偽名生成パラメータとしては店舗の名前，位置情報等を入力する．同じ実名に対して，店舗の名前，位置情報等の偽名生成パラメータが一致する場合，同じ偽名が再現して生成される．これにより，消費者が過去に生成し使用した偽名で再び同じ顧客としてサービスの提供を受けることができる.

・通信ごとに変化する匿名

同じ偽名を使用する場合でも，乱数を使用しているため匿名は毎回異なるものとなる．したがって，通信路を流れる匿名は毎回異なるものとなり，同じ名前を検出することによって消費者の行動が追跡されることが防止される.

・消費者が偽名を選択できる

偽名生成パラメータを異なるものにするか，あるいは偽名を生成する暗号化処理に用いる暗号化鍵（と対応する復号化鍵）を異なるものにすることで，異なる複数の偽名を生成できる．実名を復号化する復号化鍵を持たない受信者は，異なる偽名間の紐付けを行うことができない.

・消費者が開示する情報を実名とするか，偽名とするか，匿名とするかを選択できる消費者が偽名を選択できる

匿名から偽名を復号化するのに使用する鍵，偽名から実名を復号化するのに使用する鍵を暗号化鍵管理装置で変える.

・企業は，権限に応じて従業員に匿名，偽名，実名を参照させることができる

受信者の権限に応じて復号化処理装置の復号化鍵を与える.

・複数の企業間で共通のシステムを構築できる

実名を復号化する鍵を第三者機関に預け，一般企業には匿名を偽名にするところまでの機能を持たせる.

4. まとめ

固定IDを多数の相手に開示するとプライバシ侵害の危険性が高まる．本稿では，実名，偽名，匿名を渡り歩く技術の一実現例を検討した．受信者の権限に応じて匿名から偽名，実名を復元できるレベルを決めることができ，さらに送信者の意思により実名，偽名，匿名を選択できるアイデンティティ制御方法を考案した.

文　献

[1] 高木浩光，“固定IDはデジタル化された顔――プライバシ問題の勘所，”
http://it.nikkei.co.jp/it/column/¥
njh.cfm?i=20030421s2000s2

[2] 木下真吾，星野文学，小室智之，藤村明子，大久保美也子，“ローコストRFIDプライバシ保護方法，”情報処理学会論文誌，Vol.45，No.8，pp.2007-2021，Aug. 2004.

[3] 大久保美也子，鈴木幸太郎，木下真吾，“Forward-secure RFID Privacy Protection for Low-cost RFID，”CSS2003，Oct. 2003.

[4] 石垣良信他，“特集：個人情報保護法対策シリーズ，”
http://www-6.ibm.com/jp/services/¥
security/features/index.html