個人情報保護の視点からの認証システムの検討

中村, 徹
九州大学大学院システム情報科学府

メスバ, ウッディン モハマッド
九州大学大学院システム情報科学府

馬場, 謙介
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

SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

個人情報保護の視点からの認証システムの検討

A Consideration on Authentication Systems from the Viewpoint of Personal Data Protection

中村 徹 * ウッディン モハマッド メスバ * 馬場 謙介 † 安浦 寛人 †
Toru Nakamura Uddin Mohammad Mesbah Kensuke Baba Hiroto Yasuura

あらまし 個人情報の流出問題などのプライバシ問題を防ぐ手法として，グループ署名やブラインド署名などを用いた多くの匿名認証技術が提案され，様々なサービスへの応用が考案されている．しかし，膨大な計算量が必要となることや，権利の失効の困難さ，仕組みのわかりにくさなど問題点もある．我々の研究グループは，ユーザの ID と個人情報を一括に管理する主体を設けることによって，サービスの提供者には ID のみが提出され，個人情報の移動が最小限に抑えられる認証システムを提案した．本稿では，認証システムに求められる性質を定義し，グループ署名を用いた認証と ID を用いた認証の特徴を明確にする．さらに，これらの認証方式を用いた注文システムに注目して，実用の観点からの詳細な比較を行う．

キーワード プライバシ，個人情報保護，匿名認証，ID 管理

1 はじめに

家庭用コンピュータやブロードバンドネットワークの急速な普及により，様々なサービスの授受をコンピュータ上で行う機会が増加している．一般にサービスを提供しようとする主体 (サービス提供者) は，サービスを受けようとする主体 (利用者) を確認するために ID やパスワードを用いて認証を行う．サービス提供者は利用者にサービスを受ける権利を与える際に，個人を特定できるだけの情報を提出させることが多いため，新たなサービスを享受しようとする度に，この意味での個人情報が流出するリスクも増すことになる．これは利用者にとっても大きな問題であるが，個人情報保護法の成立した現在では，サービス提供者にとっても個人情報の管理コストが増大するので好ましい状況ではない．

個人情報の流出に加え，購入履歴から趣味嗜好が知られてしまうようなプライバシ問題を防ぐ手法として，グループ署名 [1] などの公開鍵暗号ベースの匿名認証技術に基づいたサービスが考案されている．グループ署名とは，検証者に対し匿名性を有する，特権者にのみ匿名性を剥奪する権利を持つ，という特徴を持つディジタル署名の一種である．グループ署名を用いた匿名認証方式 [2] では，利用者を特定する必要がないため，サービス提供者は個人情報を管理する必要がない．しかし，膨大な計算量が必要となることや，権利の失効の困難さ，仕組みのわかりにくさなど問題点もある．

我々の研究グループでは前述の個人情報流出問題に対し，各サービス提供者に対して異なる ID を対応させる認証システム (**PID システム**) を提案した [3]．ここで ID とは，利用者とサービス提供者間で共有する秘密情報とする．以下本稿では，ID はこのような意味で用いる．このシステムでは，概念的に，各利用者は，長いビット列を ID とし，その部分 ID を各サービス提供者と共有する．ID と個人情報は信頼できる管理者 (発行者) が管理し，サービス提供者は割り当てられた部分 ID のみを受け取る．サービスの提供に必要な個人情報については必要な個人情報だけが管理者からサービス提供者に渡される．

本稿では加藤らの匿名注文システム [4] を例に取り上げ，グループ署名を用いたシステムと部分 ID を用いたシステムについて比較・検討を行う．まず，2 つの認証システム及びそれらを用いた注文システムについて説明を行う．次に，認証システムを比較するために着目する認証の性質を定義する．最後に，定義した性質により 2 つの認証システムの比較を行う．

本稿は以下の構成からなる．2 章で本稿で扱う認証モデルと認証方式について述べ，3 章で匿名注文システムについて説明し，部分 ID を用いた注文システムを提案する．4 章で認証の性質を定義して特徴を明確にし，5

* 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 番地 Graduate School of Information Science and Electrical Engineering, Kyushu University 744 Motooka Nishi-ku Fukuoka 819-0395
† 九州大学大学院 システム情報科学研究院 Faculty of Information Science and Electrical Engineering, Kyushu University {toru,mesbah,baba,yasuura}@c.csce.kyushu-u.ac.jp

章で 2 つの認証システム及び注文システムを比較し，6 章でまとめる．

2 認証方式

本章では，本稿で取り上げる認証モデル，及び認証方式について説明する．本稿では，証明者・管理者・検証者の三者についての認証モデルを考える．

2.1 認証モデル

認証とは，二者の間のある手続きの結果，片方の者がある人物であることを，もう一方の者が信じることである．本稿では，上の認証のための手続きを，ある文字列を保持していることの証明とする．これによって，便宜上，認証される者を**証明者**，認証する者を**検証者**と呼ぶ．また，この文字列をこの証明者の**証明情報**と呼ぶ．

個人情報: 個人情報とは，証明者が，証明情報を得るために提出する情報とする．

認証子: 認証子とは，証明者が，証明情報を保持していることを検証者に信じさせるための文字列である．

証明者: 証明者は，管理者に個人情報を提出することにより証明情報を得る．さらに検証者に対し，認証子を提出することで証明情報を保持することを証明する．

管理者: 管理者は，証明者から個人情報を受け取り証明情報を発行する．

検証者: 検証者は，証明者の提出した認証子から証明情報を保持するかどうかを検証する．

2.2 従来の ID を用いた認証

従来の ID を用いた認証は，管理者と検証者は同じ主体が行う．ここではこの主体を検証者と呼ぶことにする．

準備: 証明者は検証者に個人情報を提出し，証明情報として ID を得る．検証者は渡した ID と受け取った個人情報を紐付けする．

検証: 証明者は ID から認証子を作成し，認証子を検証者に提出する．検証者は認証子を元に，ID リストに受け取った ID があるか検索する．

特定: 検証者は一致した ID に紐付けされた個人情報を得る．

証明者は，ID を検証者から受け取る際に，個人情報を提出する必要があるので，証明者は検証者の数だけ個人情報を提出する必要がある．

2.3 部分 ID を用いた認証

本節では，我々の研究グループが提案した，部分 ID を用いた認証システム [3] について概要を説明する．部分 ID を用いた認証は以下のように行う．

準備: 証明者は管理者に個人情報を提出し，証明情報として検証者ごとに異なる ID 群を得る．管理者は渡した ID 群と受け取った個人情報を紐付けする．検証者は管理者から，自らに割り当てられた部分 ID リストを得る．

検証: 証明者は検証者に対応した部分 ID から認証子を作成し，認証子を検証者に提出する．検証者は認証子を元に，部分 ID リストに受け取った部分 ID があるか検索する．

特定: 検証者は受け取った部分 ID を管理者に提出する．管理者は一致した部分 ID が属する ID 群に紐付けされた個人情報を得る．

我々の研究グループは，ハッシュ関数を利用した，部分 ID を用いた認証システムを提案した [5]．システムの概要を図 1 に示す．

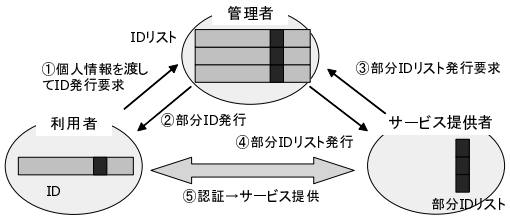

図 1: 部分 ID を用いた認証システムの構成

このシステムでは，証明者は，検証者に個人情報を提出することなく権利を証明できる．

2.4 グループ署名を用いた匿名認証

本節では，加藤らの提案した，グループ署名，及びグループ署名を用いた匿名認証システム [2] について説明する．

2.4.1 グループ署名

Chaum ら [1] により提案されたグループ署名方式では，グループのメンバは管理者が生成したメンバ証明書を用いて，検証者に対し

- グループからの有効な署名であることを証明できる．
- グループ内のどのメンバであるか特定できない．

といった性質を持つグループ署名を生成する．

加藤らの採用した，Ateniese らによって提案されたグループ署名方式 [6] の満たす安全性要件として以下のようなものがある．

Correctness: グループのメンバのみが管理者の発行したディジタル署名を用いて，グループ公開鍵で検証可能なグループ署名を生成することができる．

Unforgeability: 管理者の発行したディジタル署名を知らなければ，検証できるグループ署名が生成できない．

Anonymity: グループ署名から署名を作成したメンバを特定することはできない．

Unlinkability: 二つの異なるグループ署名から，グループの同一メンバが署名したのかどうか判別することはできない．

Exculpability: メンバも管理者もグループの他のメンバになりすますことのできるグループ署名を作成することはできない．

Traceability: 管理者の秘密鍵により，グループ署名から署名を作成したグループのメンバを追跡することができる．

Coalition-Resistance: 複数のメンバが結託しても結託したメンバ以外になりすますことのできるグループ署名を作成することはできない．

2.4.2 匿名認証

上記のような性質を持つグループ署名を用いることにより匿名認証を実現することができる．

準備: 証明者は管理者に個人情報を提出し，証明情報としてグループ証明書を得る．管理者は渡したグループ証明書と受け取った個人情報を紐付けする．検証者は管理者から，グループ公開鍵を得る．

検証: 証明者は，検証者にグループ証明書から作成したグループ署名を提出する．検証者は，受け取ったグループ署名とグループ公開鍵から検証する．

特定: 検証者は受け取ったグループ署名を管理者に提出する．管理者はグループ署名と秘密鍵からグループ証明書を特定し，グループ証明書に紐付けされた個人情報を得る．

匿名認証の概要を図 2 に示す．

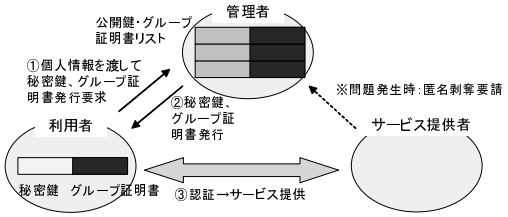

図 2: 匿名認証の概要

3 注文システム

本章では，匿名認証システムを応用した注文システム [4] を説明し，部分 ID を用いた認証システムを応用した注文システムを提案する．本稿で議論する注文システムは，いわゆるオンラインショッピングシステムを想定しており，利用者が，販売店に実際に訪れることなく注文，配送，決済を行うことを目的にしている．一般的には，利用者は購入の際，名前・住所・クレジットカード番号などを販売店に提出するが，個人情報保護の観点からは，流出のリスクが増大するので好ましくない．

3.1 匿名注文システム

匿名注文システムでは，証明者は利用者，管理者は運送業者，検証者は販売店である．利用者はまず運送業者にユーザ登録を行う．利用者は運送業者を信頼し，個人情報を提出する．利用者は販売店から商品を購入する際にグループ証明書により作成したグループ証明書により，個人情報を提出することなく注文することができる．運送業者はグループ署名から利用者を特定し，商品を配送すると共に商品の代金を販売店に代わって決済する．また，個人のプライバシにかかわらない程度の商品情報を販売店から受け取り，マーケット情報を分析して販売店に渡す．図 3 に匿名注文システムの概要を示す．

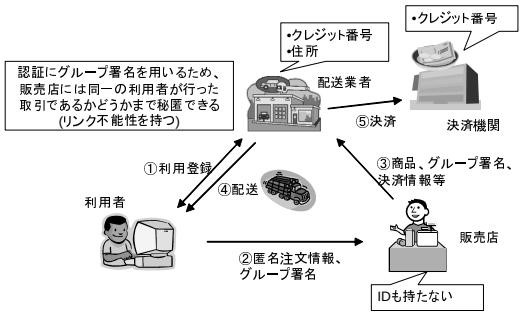

図 3: 匿名注文システムの概要

3.2 部分 ID を用いた注文システム

本節では加藤らの手法をそのまま適用し，注文システムへの応用を考える．すなわち，証明者を利用者，管理

者を運送業者，検証者を販売店とする．以下に注文システムの手順を示す．

STEP1:利用者は運送業者に個人情報を提出し利用者登録を行い，ID を受け取る．

STEP2:販売店は運送業者に販売店登録を行い，販売店に割り当てられた部分 ID のリストを受け取る．

STEP3:利用者が販売店から商品を購入する際，利用者は販売店に割り当てられた部分 ID を提出することで，運送業者に登録した利用者であることを販売店に証明する．

STEP4:販売店は利用者の部分 ID と購入した商品を運送業者に渡す．

STEP5:運送業者は部分 ID から個人を特定し，運送業務や支払手続きを行う．

部分 ID を用いた注文システムの概要を図 4 に示す．

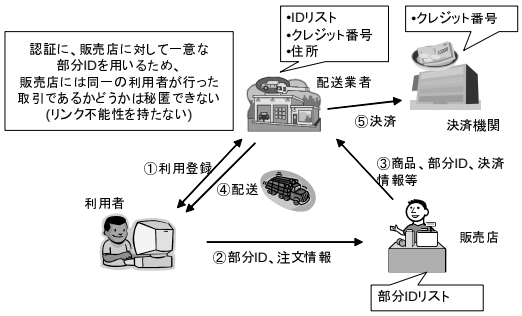

図 4: 部分 ID 注文システムの概要

しかし，本来の運送業者の業務では，個人情報のうちクレジットカード番号は必要がないので，より適切なモデルが考えられる．詳細は 4 章で述べる．

4 認証に求められる性質

本章では，認証システムを比較するために認証の性質の定義を行い，性質から導かれる認証システムの特徴を整理する．

4.1 認証の性質

まず，認証の要件と匿名認証の要件を挙げる．

- 認証の要件

  完全性: 管理者が発行した証明情報を持つ証明者は必ず認証に成功する．

  健全性: 管理者の発行した証明情報を持たない証明者は，必ず認証に失敗する．

- 匿名認証の要件

  匿名性: 検証者は，証明者の提出した認証子から，認証子を作成した証明者を特定することはできない．

  リンク不能性: 検証者は，二つの異なる認証子から，同じ証明者が認証子を作成したのかどうか判別することはできない．

匿名認証については，完全性，健全性については Correctness，Unforgerbility，Exculpabillity，Coalition Resistance，より満たすことが明らかである．匿名性，リンク不能性についてもそれぞれ Anonymity，Unlinkability より満たす．

一方で部分 ID を用いた認証では，完全性，健全性は，部分 ID が衝突しないほど十分に長い前提であれば満たす．匿名性については検証者が個人情報を持たないことから満たすことがわかる．リンク不能性については，検証者に毎回同じ部分 ID を伝えてしまうので満たさない．認証される証明者が全員同じ ID(グループ ID) を用いた場合，ID により証明者が一意に特定できないためリンク不能性を持つ．しかしグループ ID を用いた場合，検証者も管理者も認証後に証明者を特定することができない．匿名認証では，グループ署名の Traceability の性質により，管理者は認証子から，認証後に証明者の匿名性を剥奪し追跡できる．この性質を**追跡性**とする．

追跡性:管理者は認証子を作成した証明者を認証子により特定できる．

計算量に関しては，グループ署名を用いた認証では，(1) 非対話証明，(2) 匿名性剥奪機能，のために，ID とハッシュ関数を用いた認証に比べて計算コストがかかる．

認証方式と認証の性質を表 1 にまとめる．

4.2 認証の性質から生じる特徴の比較

本節では，様々な認証システムを用いた注文システムにおいて，前節で述べた性質からどのようなメリット・デメリットが生じるかを考察する．完全性・健全性については認証システムを成立させるための必須の性質であるので省略する．追跡性については，注文システムをへの応用を考える場合，管理者は個人を特定し課金などをする必要があるため，必須の性質である．以下ではこれらの性質は持つものとして議論を行う．

認証システムが匿名性を持つ場合，利用者は購入時に個人情報を入力する手間が省くことができる．販売店は詳細な個人情報を手に入れることができなくなることと引き換えに，個人情報を管理するコストを削減することができる．

認証システムがリンク不能性を持つ場合，利用者は，どのような嗜好を持つ利用者がいるかすら販売店に知られることはなく，高いプライバシ保護を得ることができる．しかし販売店は，利用者が全く見分けがつかないた

表 1: 認証システムの比較

	従来の管理者・検証者一体型認証	一意に証明者が定まる部分 ID 認証	一意に証明者が定まらないグループ ID 認証	グループ署名を用いた匿名認証
完全性	○	○	○	○
健全性	○	○	○	○
匿名性	×	○	○	○
リンク不能性	×	×	○	○
追跡性	○	○	×	○
計算コスト	○	○	○	×

め，利用者に合わせたサービスを提供することができない．これは利用者の利便性を損なう可能性もある．例えば，利用者の嗜好に合わせた推薦サービスなどは全く利用できなくなる．また，利用者の権利を失効する場合を考えたとき，権利の有無を販売店のみで判断できないことから，失効が困難になる．

認証の性質のもたらすメリット・デメリットを表 2 にまとめる．

5 部分 ID を用いた注文システムの評価

部分 ID を用いる認証と匿名認証の差はリンク不能性の有無である．リンク不能性の有無により変化する特徴は前章において述べた．本章では，その特徴について詳細に考察する．

5.1 評価

本稿で行った整理では，部分 ID を用いる認証が，グループ署名を用いる匿名認証に明らかに劣っている部分は，どのような嗜好を持つ利用者がいるかを販売店に分析されてしまう点である．各販売店で異なる部分 ID を用いるため，複数の店舗が結託しても他の店舗の購入履歴との紐付けは困難であるので，結託して広範囲にわたる購入情報等のプライバシが侵害される危険性は低いと考えられるが，同一の販売店で行う購入情報はその販売店に残る．

この点については，販売者のマーケット情報を得たい要求とトレードオフの関係になるのは不可避である．匿名注文システムでは，販売店から配送業者に送られる商品情報を，個人のプライバシに関わらない程度に制限することで解決しようとしているが，十分なマーケット情報が得られるとは考えにくい．社会に受け入れられるためには，利用者・販売店両者の立場を尊重する必要があるため，この点で妥協するのは妥当であると考えられる．

一つの解決法として，販売店が持つ部分 ID リストを複数用意し，ある一定期間ごとにローテーションしながら使う方法が考えられる．この方法であれば，管理する ID が多くなるデメリットはあるが，ある程度嗜好の分析を阻むことができる．

その他の部分 ID を用いる認証のメリットとしては，まずハッシュ関数を用いることによる計算コストの少なさが挙げられる．ハッシュ関数の計算は公開鍵暗号系の処理に比べて処理時間が短いのに加えて，回路のコストも抑えることができるため，IC カード，携帯電話などの携帯デバイスに向いていると考えられる．

5.2 管理者を独立させた注文システム

今回説明を行った注文システムでは，管理者を運送業者とし個人情報を管理させていたが，(1) 管理者は認証の信用を保証する機関となるため，複数存在し信頼のよりどころのない運送業者を管理者にするのは現実的でない，(2) 管理者の管理する情報には，運送業者の業務には必要のない情報が含まれる，などの理由から，管理者は販売店とも運送業者とも独立に存在するべきであると考える．以下に部分 ID を用いた認証を用いた，管理者を独立させた注文システムの手順を示し，概要を図 5 に示す．なお，管理者を独立させた注文システムは，グループ署名を用いた匿名認証システムを用いても同様に構築できる．

STEP1:利用者は管理者に個人情報を提出し利用者登録を行い，ID を受け取る．

STEP2:販売店は管理者に販売店登録を行い，販売店に割り当てられた部分 ID のリストを受け取る．

STEP3:利用者が販売店から商品を購入する際，利用者は販売店に割り当てられた部分 ID を提出することで，管理者に登録した利用者であることを販売店に証明する．

STEP4:販売店は利用者の部分 ID と購入した商品を一意に決定する商品 ID，決済情報を管理者に渡し，商品に商品 ID を貼り付けて運送業者に渡す．

STEP5:管理者は部分 ID から個人を特定し，運送業者に商品 ID と住所を渡し，支払手続きを行う．

表 2: 認証システムの比較

		匿名性	リンク不能性
利用者	メリット	購入時に個人情報を入力する手間なし	購入履歴からどのような嗜好を持つ利用者がいるかを販売店に分析されることがなく安心
	デメリット	特になし	利用者に合わせたサービス享受不可
販売店	メリット	個人情報を管理するコスト削減	購入履歴を管理するコスト削減
	デメリット	詳細な個人情報入手不可	利用者に合わせたサービス提供不可，権利の失効の有無の判断不可

STEP6:運送業者は，商品を紐付けされた住所に搬送する．

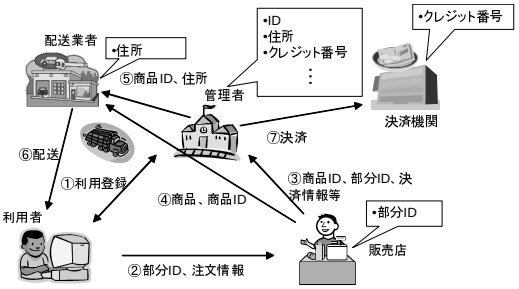

図 5: 管理者を独立させた注文システム

この方式では，運送業者がわかるのは住所だけ，決済機関がわかるのはクレジットカード番号だけとなり，業務に不要な個人情報が渡されていないことがわかる．

管理者は，国や大学など，社会的な信頼があり利用者に不利益を与える動機の薄い機関が行うのが適当である．九州大学では，e-World プロジェクトにおいて，九州大学を管理者として，PID を用いた認証方式を IC カードに実装し，教員・学生に配布して実証実験を行っている．管理者を独立させた注文方式は，実験を行っている認証方式に実装することが容易であるため，今後実装に向けてさらに議論を行っていく予定である [7].

6 終わりに

本稿では匿名注文システムを例に取り上げ，グループ署名を用いたシステムと部分 ID を用いたシステムについて比較・検討を行った．

謝辞

本研究は平成 14-18 年度科学研究費補助金学術創成研究費・課題番号 14GS0218 によるものである．

参考文献

[1] D.Chaum, E.van Heyst, “Group Signatures”, Advances in Cryptology Eurocrypt’91. Donald W. Davies. Brighton, UK, 1991-04, The International Association for Cryptologic Reserch(IACR). Berlin, Springer Verlag. 1991,p.257-270.

[2] 加藤 岳久, 岡田 光司, 吉田 琢也, “プライバシを保護する匿名認証システムの開発”, CSS2003, Oct.2003.

[3] 浜崎 陽一郎 and 安浦 寛人, “PID を用いた安全な社会システムの構想”, マルチメディア，分散，協調とモバイル（DICOMO2002）シンポジウム, Jul. 2002.

[4] 吉田 琢也, 岡田 光司, 加藤 岳久, “匿名注文システム”, CSS2004, Oct.2004.

[5] Yasunobu Nohara, Sozo Inoue, and Hiroto Yasuura, “Toward unlinkable ID Management for Multi-service Environments”, Proc. 3rd Int’l Conf. Pervasive Computing and Communications(PerCom) Workshops, pp.115-119, Mar. 2005.

[6] G.Ateniese, J.Camenisch, M.Joye, G.Tsudik, “A Practical and Provably Secure Coalition-Resistant Group Signature Scheme”, Advances in Cryptology-CRYPTO2000, Mihir Bellare, California, USA, 2000-08, IACR. Berlin, Splinger-Verlag, p.255-270, 2000.

[7] 九州大学システム LSI 研究センター, http://www.slrc.kyushu-u.ac.jp/index-j.html