個人情報の拡散を防ぐ高速匿名認証技術

High-Speed Anonymous Authentication Technology to Prevent Dissemination of Personal Data

吉田　琢也　　岡田　光司
■ YOSHIDA Takuya　■ OKADA Koji

個人情報保護法が全面施行されて約４年経過するが，無数に存在するサービス事業者での個人情報の漏えい事件はなかなか減少しない。また，従来の匿名認証技術は，個人情報やID（Identifier）を使わずに認証を行えるものの，処理速度や利用者失効機能などの点で課題があり，実用性に不十分な面があった。

東芝ソリューション（株）は，従来の匿名認証技術の問題点を解決する高速匿名認証技術を開発した。この高速匿名認証技術は，効率的な利用者失効機能を持ちながら，パソコン（PC）はもちろん携帯電話やICカードのように制約が厳しいプラットフォームでも実用的な速度で認証を処理でき，新たなビジネスモデルやユースケースも考えられるようになった。

Although about four years have passed since the Personal Information Protection Law was enforced, incidents of personal data leakage from service providers still occur.　Conventional anonymous authentication technologies without the use of personal data and identification have been insufficient for practical use due to the issues of efficiency and user revocation.

To overcome these problems, Toshiba Solutions Corporation has newly developed a practical anonymous authentication technology that can achieve high-speed processing of authentication even on restricted platforms such as personal computers, cellular phones, and IC cards, and makes it possible to be applied to a broad range of business models and use cases.

1　まえがき

個人情報保護法が2005年4月に全面施行されたが，個人情報の漏えい事件が規模の大小を問わずいまだにしばしば発生している。これは，クレジットカード会社，銀行，通信キャリア，及び医療機関など，膨大な個人情報を極めて厳重に管理している個人情報取扱事業者がいる一方で，多大なリスクとコストを負いながら個人情報を適切に管理しなければならないサービス事業者が無数に存在するためである。

サービス事業者からの漏えいがなくなれば，個人情報の漏えいは劇的に減ることが予想されるが，サービス事業者に個人情報取扱事業者並みの個人情報管理を期待するのは現実的ではない。また，従来の認証技術では，サービス事業者は利用者が“誰か”を特定して認証する必要があるため，利用者に個人情報の提供を依頼し，その情報を管理しなければならない。

東芝ソリューション（株）は，保有する個人情報の漏えいを防ぐのではなく，そもそも個人情報を保有する必要をなくすという観点から，個人情報やIDを使わずに認証を行える匿名認証技術の研究・開発を行ってきた[1]。今回，処理速度などの課題を解決し，より実用的な“高速匿名認証技術”を開発した。

ここでは，この技術の概要と特長，実装評価の結果，及び新たな適用分野などについて述べる。

2　匿名認証の仕組み

匿名認証技術とは，正規の利用者であることを認証できるが“誰か”までを特定できないようにする技術であり，サービス事業者による個人情報管理を不要にして個人情報やプライバシーの保護を実現する。

匿名認証の仕組みを**図1**に示し，以下にその流れを述べる。

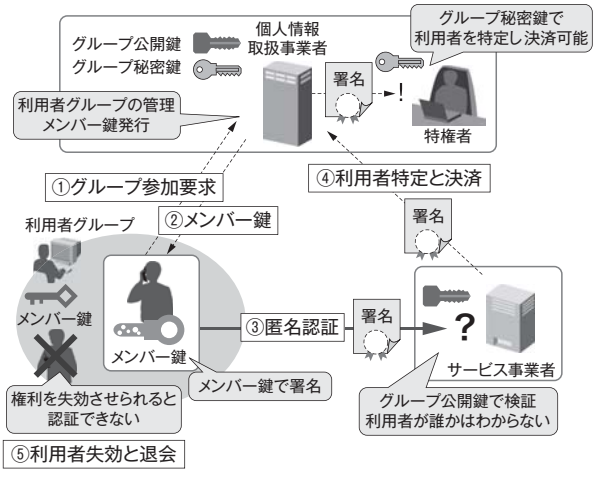

図1. 匿名認証の仕組み ― グループ署名を見ると正しい利用者による署名かどうかを判断できるが，利用者が誰かはわからない。

Scheme of anonymous authentication

ここでは，完全な匿名性を備えたグループ署名を用いているので認証の履歴も追跡できず，また，特権者だけがグループ署名から利用者を特定できる。

(1) グループ参加要求　　利用者は個人情報取扱事業者へ個人情報を送り，サービスを受ける権利を持つ正規の利用者グループへの参加を要求する。

(2) メンバー鍵　　参加要求が認められる場合，個人情報取扱事業者は，個人情報を登録すると同時に利用者へグループ署名生成のためのメンバー鍵を発行する。

(3) 匿名認証　　利用者は自分のメンバー鍵でグループ署名を生成し，サービス事業者に提示する。サービス事業者はそのグループ署名をグループ公開鍵で検証し，相手が正規の利用者かどうかを確認する。この際，個人情報やIDなど利用者個人と結びつく情報はいっさい利用されず，サービス事業者には利用者が誰かがいっさいわからない。また，正しいメンバー鍵を持っていないと，正しいグループ署名を生成できず認証もできない。

(4) 利用者の特定と決済　　一方で，グループ秘密鍵を持つ個人情報取扱事業者だけは，必要に応じてグループ署名から利用者を特定でき，課金や決済なども行える。

(5) 利用者の失効と退会　　この機能の実現方法は，利用するグループ署名方式によって異なる。また，利用者失効機能を持たない方式も少なくない。

これにより利用者は，個人情報やクレジットカード番号をそれぞれのサービス事業者に提示することなく，プライバシーも保ったまま，安全に安心してサービスを利用できる。サービス事業者は，個人情報を受け取る必要も管理する必要もなくなり，漏えいリスクや管理コストから開放される。個人情報取扱事業者は，保有している個人情報を出すことなくサービスだけを外部委託することも可能になり，個人情報を有効に活用できる。

3　従来の匿名認証技術の問題点

このように，匿名認証は個人情報保護やプライバシー保護に有効な技術であるが，現在当社が調べた範囲では，グループ署名を利用した匿名認証技術が実用化された例は見つかっていない。以下に，考えられる主な原因について述べる。

3.1　処理速度

グループ署名は通常の電子署名に比べて処理が非常に複雑で速度が遅いことが，長年にわたって問題とされてきた。処理を速めるために，処理の一部を計算能力の高いプロキシ(注1)に委託する方式[2]や，計算量自体を小さくする方式[3]-[5]などが提案されてきた。しかし，前者はオンライン利用可能なプロキシが必要であり，後者も計算能力の低いデバイスの利用を考えると計算量が十分に小さいとは言えず，まだ十分な実用性があったとは言えない。

3.2　利用者失効機能

利用者失効機能は，利用者の退会や不正者の排除などのために，運用上非常に重要な機能である。しかし，グループ署名では，匿名であることが裏目に出て，PKI（Public Key Infrastructure：公開鍵基盤）のようにIDを単純に利用するだけでは失効処理ができず，効率よく実現することが困難であった。

例えば，従来のグループ署名方式における失効機能の実現方法の一つとして，誰かひとりでも失効させようとすると，“すべての利用者のメンバー鍵（署名生成鍵）を更新”しなければいけないという方法がある。しかしこの方法では，適切なタイミングで，簡単かつ安全に，多数のメンバー鍵を更新するための運用上の問題がある。

運用上望ましいのは，個人情報取扱事業者が匿名の失効者リストをサービス事業者へ配布する方法である。この方法では，個人情報取扱事業者とサービス事業者だけの処理で失効処理が完結できるため，運用が大幅に簡素化されるが，実現が困難である。

3.3　そのほかの問題点

実際にサービスを運用する際には，署名長や鍵長のデータサイズに制約がある場合も考えられる。また，制約の多いプラットフォーム上では，実行できる演算処理が限られていたり，プログラムサイズに上限があったりもする。

処理速度や利用者失効機能に加え，これらの制約があることで，従来の方式はPCでの利用が前提となっており，ICカードや携帯電話での利用は現実的ではなかった。このように，適用範囲が限定されていたことも実用化への障害となっていた。

4　高速匿名認証技術の特長

従来の様々な問題を解決するため，当社は高速匿名認証技術を開発した。これは，メンバー鍵を利用者自身も取り出せないように安全に保存できる環境で利用可能な，新たな独自のグループ署名方式[6]により実現するもので，以下の特長を持っている。

(1) 世界最速の認証処理速度　　署名生成と検証速度が従来のグループ署名方式[3]-[5]と比較して約2倍で，世界最速の認証処理速度(注2)を持ち，実用的な時間で処理することが可能となる。

(2) 効率的な利用者失効機能　　退会者や不正会員をグループから排除する際は，管理者が匿名の“失効者リスト”をサービス事業者へ配布するだけの，効率よい処理

(注1)　処理の一部を代理で行ってくれる外部モジュールやサーバ。

(注2)　2009年5月現在，当社調べ。

が可能である。

(3) 小さいデータサイズ　　認証のたびに頻繁に送受信される情報である署名と，利用者が保持する秘密情報であるメンバー鍵は，運用上特に小さいほうが望ましく，これらのデータのサイズは世界最小クラスである。

(4) 容易な実装　　既に広く利用されている単純な演算処理の組合せだけで実装できる。

これらの特長から，モバイルPCだけでなく，携帯電話やICカードなどのように，処理速度，データサイズ，プログラムサイズなどで制約が多くて厳しいプラットフォームでも，実用的な匿名認証が可能になる。

5　高速匿名認証技術の実装評価と実用性の見込み

5.1　携帯電話

高速匿名認証技術が携帯電話上でも動作することを確認するため，東芝の携帯電話モデルA5523T上で，CDMA (Code Division Multiple Access) 携帯電話向けアプリケーションのプラットフォームであるBREW®3.1(注3)を利用して，当社グループ署名方式の実装評価を行った。

その結果，当社方式が正常動作することを確認し，更に処理速度も，署名生成時間が1秒未満と携帯電話でも十分に実用的であることも確認した。また，携帯電話向けに実装を最適化すれば，更なる処理時間の短縮も期待できる。

5.2　ICカード

高速匿名認証技術をICカード上で実装する場合，当社グループ署名方式の署名生成計算量はRSA(注4)署名生成の4倍程度であることから，十分に実用的な速度が出ることが期待できる。また，当社方式は，多倍長演算やハッシュ関数など，ICカードのコプロセッサに実装されている処理を利用できる。そのため，ほかの方式と比べて，小さなプログラムサイズで高速な処理の実現が期待できる。

6　高速匿名認証技術で広がる適用先

今や誰もが携帯電話を持っており，次々と新しい携帯電話向けサービスが提供されている。一方，ICカードは，接触型だけでなく非接触型のICカードの普及も進みつつあり，次々と新しいサービスが開始されている。このように，携帯電話やICカードを使いモバイル環境でもサービスを利用できるということが，今後よりいっそう重要度を増していくと思われる。

高速匿名認証技術の開発により，従来実現できなかったような，モバイル環境で携帯電話やICカードを利用した新たなビジネスモデルも考えられるようになったことは，今後の普及展開に向けて大きな意味を持っている。更に，高速匿名認証技術は，個人情報取扱事業者とサービス事業者が異なる事業者であるモデルだけではなく，一つの事業者の中で閉じたサービスモデルへの適用も考えられる。以下，これらの具体的な例について述べる。

6.1　匿名注文システムの適用範囲拡大

匿名注文システム(7)では，個人情報やプライバシーが守られた商品の注文が可能である。利用者は，販売店に対して個人情報やクレジットカード番号を渡さずに匿名で注文でき，購入履歴を知られることもない。

従来の匿名認証技術の性能では，PCを利用したオンラインショッピング以外は実用上現実的ではなかったが，高速匿名認証により，携帯電話からのオンラインショッピングだけでなく，携帯電話やICカードを利用した実店舗での対面決済も可能となり，利用シーンが大幅に広がる（**図2**）。また，クレジットカード番号を使わない決済が可能となるため，PCI DSS (Payment Card Industry Data Security Standard：PCIデータセキュリティ基準)(注5)で求められるセキュリティ要件を緩くできるなどの効果も期待できる。

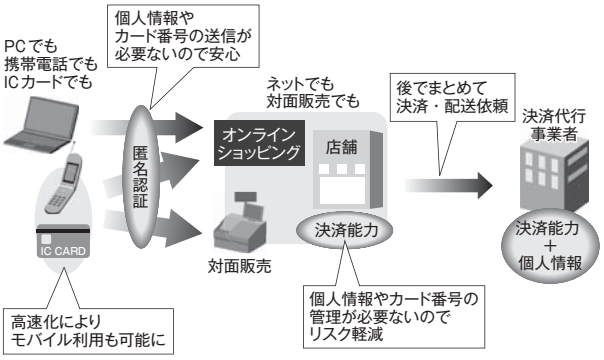

図2．匿名注文システムの適用範囲拡大 — 高速匿名認証により，携帯電話からのオンラインショッピングだけでなく，携帯電話やICカードを利用した実店舗での対面決済も可能となり，利用シーンが大幅に広がる。

Expansion of applied area in anonymous order system

6.2　モバイル端末向けアクセス認証への適用

モバイル端末でも利用可能な高速化が実現されたことにより，モバイル端末向けのアクセスポイント利用における個人情報やプライバシー保護の実現にも活用できるようになった。

サービスプロバイダーとしては，アクセスポイントでIDやパスワードを扱わないためセキュリティの向上が図れるほか，他

(注3)　BREWは，Qualcomm社の商標又は登録商標。
(注4)　Rivest氏，Shamir氏，Adleman氏の3人が開発した公開鍵暗号方式。
(注5)　クレジットカード情報及び取引情報の安全な管理を目的に，国際カードブランドによって策定されたクレジットカード業界におけるセキュリティ基準。

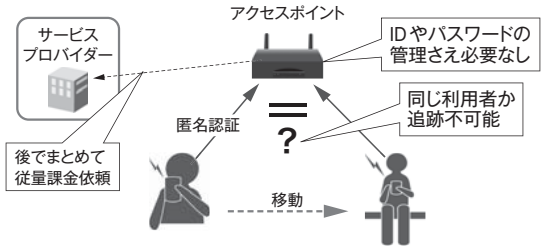

図3. モバイル端末向けアクセス認証への適用 — アクセスポイントにIDやパスワードを送らず，利用履歴も知られることなくアクセスできる。

Access authentication for mobile terminals

社のユーザーに対してローミングサービスを提供する場合にも，他社のユーザーのIDやパスワードなどを預かる必要がない。また，同じユーザーがあちこちのアクセスポイントを利用してもその行動履歴は把握されず，より高いプライバシーが保たれる（**図3**）。

6.3 アンケート収集への適用

一つの事業者内でも，個人情報を専門に管理する部門が独立して，ほかよりも厳重な情報管理を実施している場合が多い。このような場合，匿名認証技術を活用することで，個人情報を専門の部門だけに閉じて一括管理でき，ほかの部門に大きな負担を強いることなく高いセキュリティを実現できる。

その一例として，アンケート収集への適用例を**図4**に示す。サービス事業者内では個人情報を管理する部門とアンケートを収集する部門が別々であるとする。サービス利用者は匿名でアンケートに回答し，アンケート収集部門では個人情報を扱う必要がない。必要な場合にだけ個人情報管理部門が利用者を特定する。例えば，アンケート回答者の中から抽選で特典当選者を選び，その利用者へプレゼントを配送する場合など

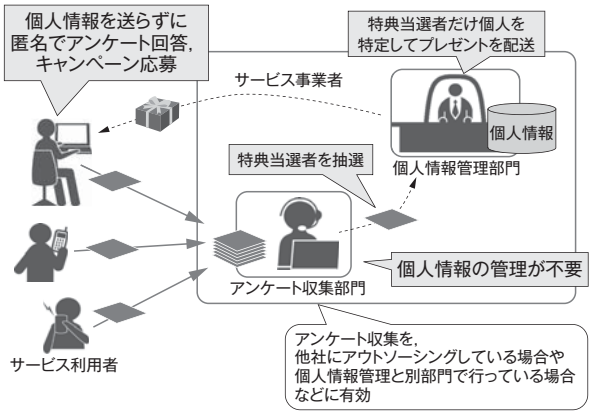

図4. アンケート収集への適用 — サービス事業者内では，個人情報を管理する部門とアンケートを収集する部門が分離されている。サービス利用者は匿名でアンケートに回答し，抽選で選ばれた特典当選者へのプレゼント配送など必要な場合にだけ，個人情報管理部門が利用者を特定する。

Questionnaire collection system

が考えられる。

7 あとがき

今回開発した高速匿名認証技術を適用すると，一般のPCはもちろん，携帯電話やICカードのように計算速度，データサイズ，実装などで制約が厳しいプラットフォームでも，実用的な匿名認証が可能になる。これにより，従来方式では実現できなかった新たなビジネスモデルやユースケースも考えられるようになった。例えば，個人情報やカード番号の漏えい防止を重視しているクレジットカード会社や銀行向けのサービス，携帯電話やモバイル端末の識別番号を利用しないモバイルサービス，及び機微な個人情報を扱い，プライバシー保護のニーズが非常に高い医療機関向けサービスなどが考えられる。

当社は，高速匿名認証技術を個人情報保護やプライバシー保護を実現するサービスとして提案し，幅広い適用先にソリューション展開を進めていく。

文 献

(1) 加藤岳久，ほか．匿名認証技術とその応用．東芝レビュー．**60**，6，2005，p.23－27.

(2) 岡田光司，ほか．“計算能力の低いデバイスに適したグループ署名方式”．暗号と情報セキュリティシンポジウム（SCIS）2005 予稿集Ⅲ／Ⅳ．兵庫，2005-01，電子情報通信学会ISEC 研究会．2005，p.1147－1152.

(3) Camenisch, J. ; Groth, J. "Group Signatures : Better Efficiency and New Theoretical Aspects". Fourth Conference on Security in Communication Networks '04 (SCN '04). Amalfi, Italy, 2004-09. Heidelberg, Springer, 2005, p.120－133.

(4) Delerablée, C. ; Pointcheval, D. "Dynamic Fully Anonymous Short Group Signatures". International Conference on Cryptology in Vietnam 2006 (VIETCRYPT 2006). Hanoi, Vietnam, 2006-09, FPT Software. Heidelberg, Springer, 2006, p.193－210.

(5) Furukawa, J. ; Imai, H. An Efficient Group Signature Scheme from Bilinear Maps. IEICE Trans. Fundamentals. **E89-A**, 5, 2006, p.1328－1337.

(6) Yoshida, T. ; Okada, K. "Simple and Efficient Group Signature Scheme Assuming Tamperproof Devices". International Workshop on Security 2008 (IWSEC 2008). Kagawa, Japan, 2008-11, IEICE and IPSJ. Heidelberg, Springer, 2008, p.83－99.

(7) 吉田琢也，ほか．“匿名注文システム”．CSS2004予稿集．札幌，2004-10，情報処理学会CSEC研究会．2004，p.403－408.

吉田 琢也 YOSHIDA Takuya, D. Eng.

東芝ソリューション（株）IT技術研究所 研究開発部研究主務，工博。情報セキュリティ技術の研究・開発に従事。電子情報通信学会会員。

Toshiba Solutions Corp.

岡田 光司 OKADA Koji, D. Eng.

東芝ソリューション（株）IT技術研究所 研究開発部研究主務，工博。情報セキュリティ技術の基礎研究及び応用開発に従事。国際暗号学会（IACR），電子情報通信学会会員。

Toshiba Solutions Corp.