プライバシーを保護する匿名認証技術

個人情報を用いずに認証しプライバシーを守る匿名認証技術

これまで，サービスを受けるときに，本人であることを保険証や運転免許証で確認したり，固定のID（IDentification）やパスワードを照合して認証してきました。このため例えば，誰が，いつ，どのようなサービスを受けたか，という情報が収集され漏えいすると，プライバシー侵害などの大きな社会問題となります。インターネットを利用した会員がサービスを受ける場合には，誰からの要求かわからなくすれば，サービスと個人とを結びつけることができず，プライバシーが保護できます。

当社は，会員がサービスを受けられるかどうかという属性だけを示すことでサービスが受けられる，匿名で認証するシステムを開発しました。

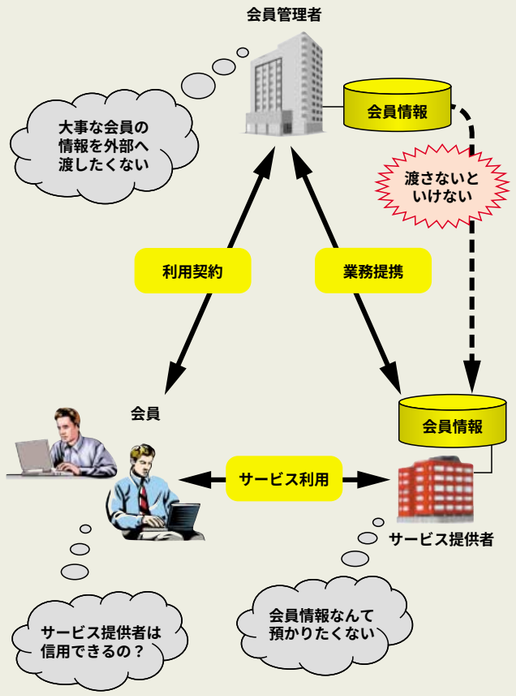

図1．従来の認証における問題点 ― 会員管理者は，会員情報をサービス提供者に渡さなければなりませんでした。会員は履歴などのプライバシーが守られているか不安でした。

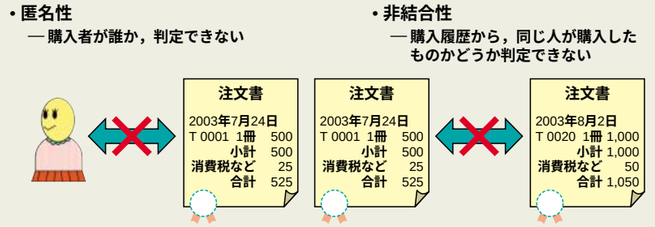

図2．匿名で認証するために必要な要件 ― 購入した人を特定できなくする匿名性と，購入履歴から同じ人が購入したかどうかわからなくする非結合性が，匿名で認証するための要件です。

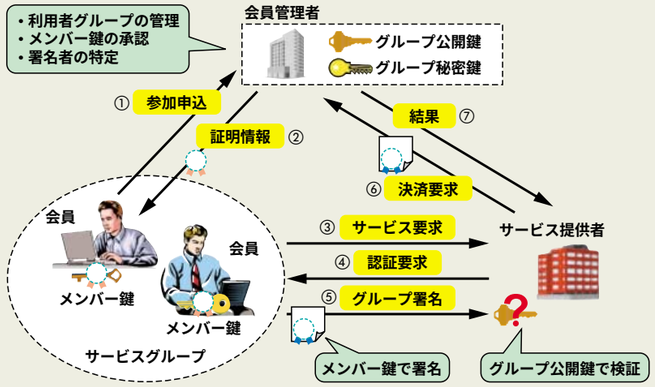

図3．グループ署名を用いた認証と決済の処理 ― サービス提供者は，グループ公開鍵だけで認証するので，アクセス元が誰かを特定できませんが，サービスを受けられる正しい会員からであることは検証できます。

ますます重要となる個人情報やプライバシーの保護

現在，事業者などによる顧客情報の漏えいや個人情報の売買が社会問題となっています。また，総務省が行った意識調査では，会員がインターネットを利用する際の不安として，プライバシー保護が第1位に挙げられています。

会員が，会員管理者と提携したサービス提供者から，サービスを受ける場合を考えます（**図1**）。

従来は，サービス提供者は会員管理者から会員情報をもらい，それを利用して認証しました。例えばパスワードや会員の公開鍵など，会員ごとに異なる情報です。これにより，少なくとも異なるアクセスが同一会員からであることを知ることができます。

一方，会員は，サービスを受けた履歴がサービス提供者に収集されたり，会員情報が漏えいしたりするなどの不安がありました。

このような問題を解決するために当社では，会員がサービスを受けられるかどうか，という属性だけを示すことでサービスを受けられる，匿名で認証できるシステムを開発しました。

匿名で認証するために必要な要件

匿名で認証するために必要な要件を，**図2**に示します。

図2では，ある会員が品物を発注して購入する場合を想定します。匿名で認証するためには，購入した人を特定できない匿名性（Anonymity）と，購入履歴から同一人物が購入したかどうかわからない非結合性（Unlinkability），という二つの要件が必要になります。

グループ署名を用いた処理の流れ

そこで当社は，匿名で認証するのに必要な要件を満たすために，電子署名方式の一つであるグループ署名を採用しました。

想定するモデルでは，グループを管理する会員管理者と，グループを構成する会員，及びサービスを提供するサービス提供者，の三つのプレーヤーが存在します（**図3**）。

会員は，サービスグループに参加してサービスを受けます。始めに，会員管理者に利用申込みをする（①）と，会員が持つ鍵がサービスグループのメンバー鍵であることを証明する証明情報が送られます（②）。

サービス提供者は，会員からのサービス要求がある（③）と，認証要求を送り返します（④）。会員は，各自が所有するメンバー鍵と証明情報を元に，認証要求に対するグループ署名を生成して送り返します（⑤）。

サービス提供者は，グループ公開鍵を使ってグループ署名を検証し，正当なものであればサービスを提供します。ここで，サービス提供者はアクセスしてきた会員を特定できないため，誰に課金すればよいか特定できません。そこで，会員から送られてきたグループ署名を決済情報として会員管理者へ送ります（⑥）。

会員管理者は，グループ署名の正当性を検証し，署名を生成した会員を，グループ秘密鍵を用いて特定します。そして，署名を生成した会員に対して，あらかじめ登録されている課金情報を元に決済を行い，結果をサービス提供者へ通知します（⑦）。

グループ署名の特長

以上のように，会員は，会員ごとに異なる承認されたメンバー鍵を用いて，グループ署名を生成します。

サービス提供者は，会員情報をいっさい持たずに，サービスグループに一つのグループ公開鍵を用いて，グループ署名を検証します。

このように，グループ署名は個々のメンバー鍵で異なる署名を生成します。しかし，グループで唯一の公開鍵で署名の正当性は検証できますが，誰が生成したかを隠蔽（いんぺい）できる（匿名性）ので，匿名で認証できます。また，異なるグループ署名から同一人物が生成したことを検証することができません（非結合性）。

グループ公開鍵に対応するグループ秘密鍵を知っている会員管理者のみが，グループ署名を生成した会員を特定できます。

利便性とセキュリティの向上

将来，携帯性と安全性を高めるためにJava™[注1]カードで実装することを視野に入れ，会員が秘密にしなければいけない情報や演算をJava™カード内に格納し演算できるように，アルゴリズムを改良し実装しました。また試作システムでは，公開鍵暗号RSAの鍵長1,024ビット相当の安全性で，実用レベルの処理速度を実現しました。

なおこの研究は，情報処理振興事業協会が実施した平成14年度次世代ソフトウェア開発事業“ 個人情報保護を目的とした属性証明による認証システムの開発 ”の委託を受け，東芝が研究開発したシステムに関するものです。

加藤　岳久

東芝ソリューション（株）
SI技術開発センター　SI技術担当主任

（注1）　Java及びその他のJavaを含む商標は，米国Sun Microsystems, Inc.の米国及びその他の国における登録商標又は商標。