匿名認証技術とその応用

Anonymous Authentication Technology and Its Application

加藤　岳久　　岡田　光司　　吉田　琢也
■KATO Takehisa　■OKADA Koji　■YOSHIDA Takuya

個人情報保護に関する法律が全面施行され，事業者は個人情報を厳密に管理しなければならなくなった。東芝ソリューション(株)は，このような状況に対応するため，個人情報を厳密に管理するのではなく，個人情報を使わずに認証することで個人情報の管理を不要にする，グループ署名方式を用いた匿名認証技術を開発した。また，それを用いた匿名注文システムのプロトタイプを開発し，実用上問題のないことが確認できた。更に，計算量が1/10以下になるグループ署名方式を提案し，携帯電話への実装の見通しが得られた。

With the enforcement of the Personal Information Protection Law, enterprises are obligated to strictly manage personal data. Toshiba Solutions Corp. has developed an anonymous authentication technology that employs the group signature scheme. Service providers need not strictly manage personal data because they can authenticate their clients without the use of personal data. We have developed a prototype anonymous order system based on this anonymous authentication technology. In addition, we have proposed a group signature scheme that decreases computational complexity to 1/10 or less. This scheme can be installed in a cellular phone.

1　まえがき

昨今，事業者による顧客情報の大量漏えい事件や個人情報の不正な売買，趣味や嗜好(しこう)の収集など，社会問題となっている。それを裏づけるように，総務省が行った意識調査では，インターネット利用者が抱える不安として，プライバシーの保護が第1位に挙げられている[(1)]。特に個人情報保護に関する法律が成立してからは，メディアも国民も個人情報漏えいに関して注目し，事業者も対応を迫られている状況である。

個人情報の保護に関する法律が全面施行され，各サービス提供者は**図1**のように個人情報の扱いを慎重にしなければならず，管理コストが増大する。また利用者も，個人情報をむやみやたらに提供し，個人情報が拡散することは避けたい。

東芝ソリューション(株)は利用者がサービスやコンテンツなどの提供を受けるために，サービス提供者が個人に関する情報を用いずに認証と決済を行えないか，という課題に取り組んだ[(2)]。

ここでは，ネットワーク上で個人情報やプライバシーの保護を実現するための技術である匿名認証と，決済を実現するために用いたグループ署名方式についての概略を述べ，必要な要件を満足していることを示す。次に，匿名注文システムのプロトタイプについて述べ，その実用性について考察する。最後に，匿名認証システムを携帯電話で利用するために当社が提案した方式について述べる。

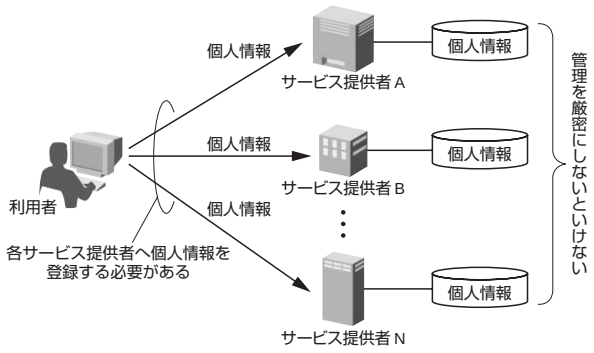

図1．従来型サービス提供の問題点 ― 利用者の個人情報が各事業者へ拡散しており，事業者は受け取った個人情報を管理しなければならず管理コストが増大する。

Problem of general service model

2　匿名認証のモデル

図2は，匿名認証・決済技術で想定する基本的なモデルである。ここで，銀行などの個人情報管理者に登録した会員が，提携したコンテンツプロバイダーなどのサービス提供者からサービスを受ける場合を考える。

このとき，個人情報管理者は，会員から預かった個人情報や個人の属性に関する情報(ID(IDentification)，パスワード，クレジット番号など)をいっさい外部に出さず，サービス提供者も会員から個人情報や属性に関する情報を受け取らずに済めば，次のようなメリットがある。

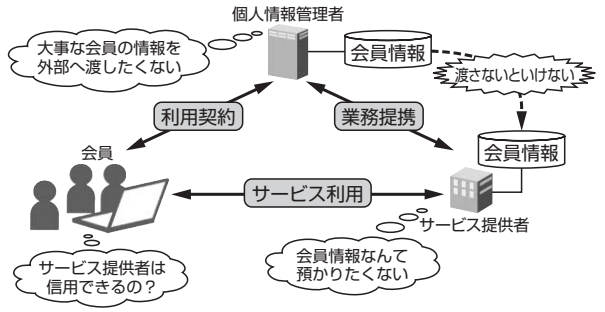

図2．匿名認証の基本モデル ― 基本モデルは，個人情報を管理する管理者，サービス提供者，利用者である会員から成る。

Basic model of anonymous authentication

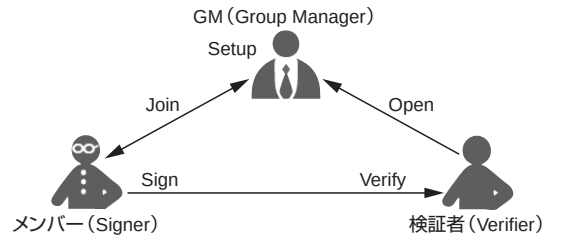

図3．グループ署名の構成 ― グループの管理者であるGM，グループ署名を生成するグループのメンバー，グループ署名を検証する検証者から成り，Setup，Join，Sign，Verify，Openのプロトコルから構成される。

Composition of group signature scheme

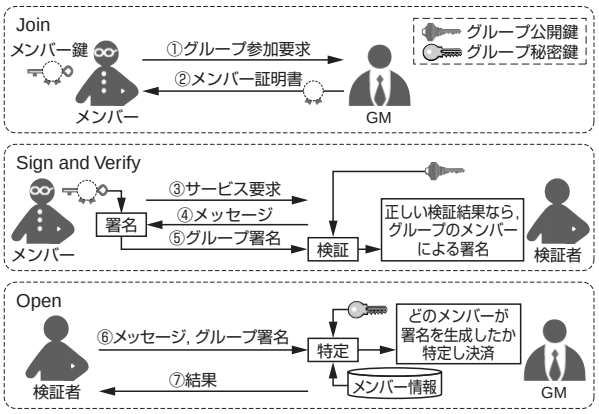

図4．グループ署名のプロトコル概要 ― メンバーは，メンバー鍵でグループ署名を生成する。検証者は，グループ公開鍵で正当性を検証する。GMは，グループ秘密鍵で署名者を特定する。

Outline of protocol of group signature scheme

⑴　個人情報管理者は個人情報をいっさい出さなくてよい。

⑵　サービス提供者は個人情報を管理しなくてよい。

⑶　会員はIDやクレジット番号などを入力しなくてよい。

この匿名認証技術は，サービス提供者にサービス権限の属性だけを示すことでサービスを受けることが可能な権限管理基盤を構築することができる。

3　グループ署名と匿名認証に必要な要件

図2のモデルで，匿名認証と決済を実現するためにグループ署名方式を用いた。グループ署名方式とは，1991年にChaumらにより提案された電子署名方式[3]で，**図3**に示すように，次の関係者から成る。

⑴　GM（Group Manager）　グループの管理を行う管理者である。図2の個人情報管理者にあたる。

⑵　検証者（Verifier）　グループ署名を検証する検証者である。図2のサービス提供者にあたる。

⑶　メンバー（Signer）　グループに参加し，グループ署名を生成する利用者である。図2の会員にあたる。

そして，以下のプロトコルにより構成される。**図4**に，GMが行うSetupを除いた手順を示す。

⑴　Setup　GMがグループの初期化を実行する。セキュリティに関するパラメータを入力として，グループ公開鍵及びグループ秘密鍵を生成する。

⑵　Join　利用者がグループへの参加を要求する際に，GMとやり取りされるプロトコルである。利用者はグループのメンバーとなることで，グループ署名を生成するためのメンバー鍵を得る。

⑶　Sign　グループのメンバーがメンバー鍵を用いて，メッセージに対するグループ署名を生成する。

⑷　Verify　グループ公開鍵を用いて，メッセージに対するグループ署名の正当性を検証する。

⑸　Open　メッセージ，グループ署名とグループ秘密鍵を入力として署名を生成したメンバーを特定する。

これまで，多くのグループ署名方式が提案されてきた。その中でも，2000年にAteniese らにより提案されたグループ署名方式[4]は，署名サイズや鍵サイズがグループのメンバー数に依存せず，更に，強RSA（Rivest-Shamir-Adleman）仮定（注1）及びDecision Diffie-Hellman問題（注2）の困難性仮定のもとで，次の安全性要件をすべて満たすことが証明され，効率と安全性の両面で優れている。

⑴　Correctness　グループのメンバーだけがメンバー鍵を用いて，グループ公開鍵で検証可能なグループ署名が生成できる。また，グループ公開鍵による検証が真ならば，グループ秘密鍵でメンバー情報が取り出せる。

（注1）　$n=pq$，$p=2p'+1$，$q=2q'+1$（p，q，p'，q'：素数）を満たすn，平方剰余群$QR(n)$（位数$p'q'$）の任意の元$u \in QR(n)$が与えられたとき，$z \equiv u^e \pmod n$を満たすe（>1）を見つけることが困難という仮定。

（注2）　巡回群$G=\langle g \rangle$（ここでは上記nの平方剰余群$QR(n)$）について，g，g^x，g^y，$g^z \in G$が与えられたとき，g^{xy}とg^zが等しいかどうかを決める問題。

⑵ Anonymity　グループ署名から署名を生成したグループのメンバーを特定することはできない。
⑶ 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ーが署名したか判別できない。
⑷ Unforgeability　メンバー鍵を知らなければ，検証できるグループ署名が生成できない。
⑸ Traceability　グループ秘密鍵で，グループ署名から署名を生成したグループのメンバーが追跡できる。
⑹ Coalition-Resistance　複数メンバーが結託しても，結託したメンバー以外をトレースできるグループ署名が生成できない。
⑺ Exculpability　GMであっても，グループのメンバーになりすまして検証できるグループ署名を生成することができない。

4 匿名注文システム[5]

4.1 概要

オンラインショッピングで，販売店に対して個人情報を渡すことに抵抗を感じる購入者は多い[6]。そこでグループ署名方式を用い，匿名でオンラインショッピングができる匿名注文システムのプロトタイプを開発した。

図5と以下に，匿名注文システムの概要を示す。

物流会社は，Setupとなる匿名注文のグループを設定し，対となるグループ公開鍵と秘密鍵を生成する。この操作は，グループごとに最初に一度行う。

販売店は，匿名注文サービスの提供を始める前に，物流会社に販売店の情報を登録し，匿名注文用グループのグループ公開鍵を取得する。

会員となる利用者は，あらかじめ物流会社へ会員登録をする(①)。会員審査が通ると，利用者は物流会社とセキュアな通信を行い，メンバー鍵を生成して物流会社が発行するメンバー証明書を受け取る。物流会社は，会員の個人情報と共にメンバー証明書をデータベースなどに保存する。登録の操作は，最初に一度行えばよい。

会員は販売店サイトへアクセスし，欲しい商品を選択する。そして，販売店から送られる注文情報に対するグループ署名を生成し，匿名注文情報として送る(②)。この注文情報は，注文基本情報と注文詳細情報から成る。

注文基本情報は，物流会社が商品の配送や決済を行うのに必要な最低限の情報であり，注文を一意に識別する注文IDを含む。注文詳細情報はそれ以外の詳細な情報で，会員のプライバシーの観点から，物流会社に対しては秘匿される。

会員が計算する匿名注文情報は，注文基本情報と注文詳細情報のハッシュ値に対し，グループ公開鍵，会員のメンバー鍵とメンバー証明書で計算されるグループ署名である。

販売店はグループ公開鍵を使って，会員が送った匿名注文情報の正当性を検証する。そして，注文情報と匿名注文情報をデータベースに保存し，匿名注文情報と注文IDが記載された伝票を梱包した商品にはり付け，決済要求としてグループ署名を物流会社へ送信する(③)。

物流会社は，販売店から送られた決済要求が重複していないことを確認し，決済要求であるグループ署名の正当性をグループ公開鍵で検証する。正しければ，グループ秘密鍵を使って注文した会員を特定し，注文IDの荷物を販売店から集荷し，注文を受けた住所へ商品を配送する(④，⑤)。次に，登録されている個人情報を元に代理決済を行い，商品代金を販売店へ支払う(⑥，⑦)。また，販売店へ個人が特定できない形でマーケット情報を提供する(⑧)。

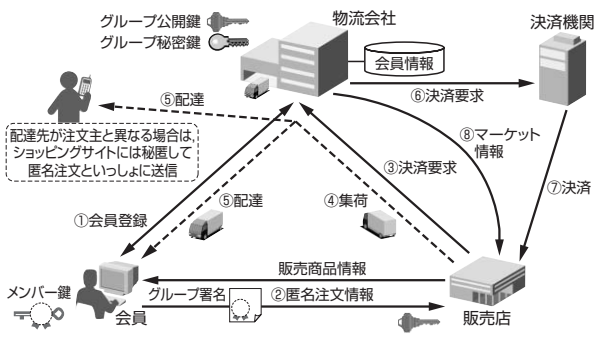

図5．匿名注文の流れ ― 購入者は物流会社へ会員登録し，物流会社と提携している販売店から匿名で商品を購入し配送を受けられる。配送先が会員以外でも対応できる。
Flow of anonymous order

4.2 特長

匿名注文システムには，次のような利点がある。
⑴ 物流会社は，展開している会員型サービスの個人情報と代理決済サービスを生かした新たな匿名注文サービスが行える。
⑵ 会員は，個人情報を各販売店へ登録する必要がなく，販売店も個人情報の管理が不要である。
⑶ 会員は，購入時にいっさいの個人情報を入力・送信しなくてよい。個人情報入力の簡素化技術としてCookieが知られているが，同じ販売店で2回目以降の利用に限られ，最初は入力が必要である。
⑷ 注文手続き開始のリクエストから注文確定までの間，購入者の個人情報は仮名，ID，クレジット番号などを含めていっさい送られず，また物流会社へのアクセスもない。
⑸ 匿名注文情報の検証時に，販売店はグループ公開鍵による署名の検証だけでよく，物流会社へアクセスする必要がない。
⑹ 販売店から物流会社へは，書籍やCDといった商品分類だけを送ることで，会員の商品購入に関するプライバ

シーが守られる。

⑺ 販売店は，従来の個人別マーケット情報は収集できないが，商品の販売傾向を，個人情報を管理せずに得ることができる。

4.3 プロトタイプシステム

プロトタイプシステムを開発し，評価を行った。動作環境と性能測定結果は次のとおりである。

4.3.1 動作環境 物流会社サーバ，販売店サーバ，会員のパソコン（PC）はいずれも下記の環境で動作し，Java™(注3) 1.3及びMicrosoft® Visual C++®(注4). NET Ver.7.0を用いて開発した。

⑴ CPU Intel® Pentium®4(注5) 2.4 GHz
⑵ メモリ 768 Mバイト
⑶ 磁気ディスク装置（HDD） 40 Gバイト
⑷ 基本ソフトウェア（OS） Windows®(注6) XP SP1

ウェブサーバには，Tomcat 4.1を用いた。強RSA仮定及びDecision Diffie-Hellman問題にかかわる$n(=pq)$のビット数は，1,024ビットである。

4.3.2 性能測定結果 会員PCのグループ署名生成時間は約1.5秒，販売店サーバのグループ署名検証時間は約1.5秒，物流会社サーバの署名者特定時間は約0.5秒であった。

5 携帯電話への応用(5)

匿名注文のプロトタイプシステムでは，会員が所有する端末としてPCを想定した。しかし，国内ではIP（Internet Protocol）接続可能な携帯電話所有者が二人に一人という状況である。

そこで，グループ署名による匿名認証をPCに比べ計算能力が低いデバイスでも演算する方式として，Atenieseらのグループ署名方式を改良し提案した(7)。

5.1 Atenieseらのグループ署名方式(4)

強RSA仮定が成立する下で，$n=pq(p, q$：素数）とする。また，gをZ_n^*の巡回部分群とし，位数を$\#G$，$\lceil \log_2(\#G)=l_G \rceil$とする。$l_p$，$k$，$\varepsilon(>1)$をセキュリティパラメータとし，$H:\{0,1\}^* \rightarrow \{0,1\}^k$を一方向性ハッシュ関数とする。また，$\lambda_1$，$\lambda_2$，$\gamma_1$，$\gamma_2$を，$\lambda_1 > \varepsilon(\gamma_2+k)+2$，$\lambda_2 > 4\ l_p$，$\gamma_1 > \varepsilon(\gamma_2+k)+2$，$\gamma_2 > \lambda_1+2$を満たすパラメータとし，$\Lambda=]2^{\lambda_1}-2^{\lambda_2}, 2^{\lambda_1}+2^{\lambda_2}[$，$\Gamma=]2^{\gamma_1}-2^{\gamma_2}, 2^{\gamma_1}+2^{\gamma_2}[$とする。

以上の前提の下で，グループ署名の具体的な手順は次のようになる。

⑴ Setup GMは以下の手順でグループ公開鍵$Pk_G=(n, a, a_0, g, h)$とグループ秘密鍵Sk_Gを計算する。
ⓐ $n=pq$，$p=2p'+1$，$q=2q'+1$（$|p'|=|q'|=l_p$，p'，p，q'，q：素数）をランダムに選ぶ。
ⓑ $a, a_0, g, h \in_R QR(n)$をランダム選ぶ。
ⓒ $x \in_R Z^*_{\phi(n)}$をランダムに選び，$y=g^x \pmod n$を計算する。

⑵ Join グループのメンバーは，メンバー鍵$Sk_m=x_m \in \Lambda$を秘密に得る。GMはSk_mに対する下記のメンバー証明書$cert_m$を生成してグループのメンバーへ送信し，メンバー証明書と会員情報のペアを秘密に保管する。

$cert_m=(A_m, e_m)$，$A_m=(a^{x_m}a_0)^{1/e_m} \pmod n$，
$e_m \in_R \Gamma(e_m \in \Gamma$：素数）

⑶ Sign グループのメンバーはSk_mと$cert_m$を用いて，メッセージMに対するグループ署名$\sigma=(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$を，以下の手順で計算する。
ⓐ $w \in_R \{0,1\}^{2l_p}$をランダムに選び，$T_1=A_m y^w \pmod n$，$T_2=g^w$，$T_3=g^{e_m}h^w \pmod n$を計算する。
ⓑ $r_1 \in_R \pm\{0,1\}^{\varepsilon(\gamma_2+k)}$，$r_2 \in_R \pm\{0,1\}^{\varepsilon(\lambda_2+k)}$，$r_3 \in_R \pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$，$r_4 \in_R \pm\{0,1\}^{\varepsilon(2l_p+k)}$をランダムに選び，$d_1=T_1^{r_1}/(a^{r_2}y^{r_3}) \pmod n$，$d_2=T_2^{r_1}/(g^{r_3}) \pmod n$，$d_3=g^{r_4} \pmod n$，$d_4=g^{r_1}h^{r_4} \pmod n$を計算する。
ⓒ ハッシュ値cを計算する。
$c=H(g\|h\|y\|a_0\|a\|T_1\|T_2\|T_3\|d_1\|d_2\|d_3\|d_4\|M)$
ⓓ $s_1=r_1-c(e_m-2^{\gamma_1})$，$s_2=r_2-c(x_m-2^{\lambda_1})$，$s_3=r_3-ce_m w$，$s_4=r_4-cw$）を計算する。

⑷ Verify 検証は，グループ公開鍵$Pk_G=(n, a, a_0, g, h)$を用いて，メッセージMに対するグループ署名σの正当性を，以下の手順により検証する。
ⓐ ハッシュ値c'を計算する。
$c'=H(g\|h\|y\|a_0\|a\|T_1\|T_2\|T_3\|$
$a_0^c T_1^{s_1-c2^{\gamma_1}}/(a^{s_2-c2^{\lambda_1}}y^{s_3}) \bmod n \| T_2^{s_1-c2^{\gamma_1}}/g^{s_3} \bmod n \|$
$T_2^c g^{s_4} \bmod n \| T_3^c g^{s_1-c2^{\gamma_1}} h^{s_4} \bmod n \| M)$
ⓑ $s_1 \in \pm\{0,1\}^{\varepsilon(\gamma_2+k)+1}$，$s_2 \in \pm\{0,1\}^{\varepsilon(\lambda_2+k)+1}$，$s_3 \in \pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$，$s_4 \in \pm\{0,1\}^{\varepsilon(2l_p+k)+1}$
及び$c=c'$が成り立つことを検証する。

⑸ Open 以下の手順により，グループ署名σの署名者を特定する。
ⓐ Verifyを実行し，グループ署名σの正当性を検証する。
ⓑ $A_m=T_1/T_2^x \pmod n$を計算し，証明書A_mからグループメンバーを特定する。

5.2 携帯電話などへ実装するための当社提案方式

当社は，携帯電話など計算能力が低いデバイスでグループ

（注3） Java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。
（注4），（注6） Windows，Microsoft，Visual C++は，米国Microsoft Corporationの米国及びその他の国における登録商標。
（注5） Intel，Pentiumは，米国又はその他の国における米国Intel Corporation又は子会社の登録商標又は商標。

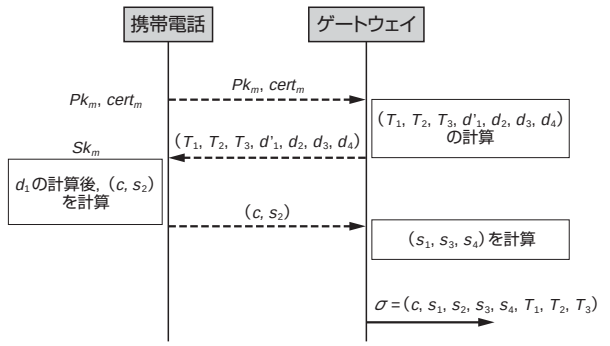

図6．携帯電話へ実装のための当社提案方式―秘密でない演算をゲートウェイで行うことにより，携帯電話内のグループ署名の演算が軽減できる。
Proposed method of installation in cellular phone

署名の生成を実現するため，Signプロトコルを改良して，携帯電話内での演算を少なくする方式を提案した[7]。

図6に示すように，提案方式は携帯電話がインターネットを介して通信する電話会社のゲートウェイと連携し，グループ署名を生成する。なお，提案方式では署名対象メッセージMは，ゲートウェイと携帯電話とで共有されているとする。

グループ署名の生成は，以下の手順で行う。

(1) Sign　グループのメンバーは，$cert_m$を携帯電話からゲートウェイへ送る。

(2) ゲートウェイは，(T_1, T_2, T_3)と(d_2, d_3, d_4)を計算する。また，$d'_1 = T_1^{r_1}/y^{r_3} \pmod n$を計算し，$(T_1, T_2, T_3, d'_1, d_2, d_3, d_4)$を携帯電話へ送る。

(3) グループのメンバーは，携帯電話で$r_2 \in_R \pm\{0, 1\}^{\varepsilon(\lambda_2+k)}$をランダムに選び，$d_1 = d'_1/a^{r_2} \pmod n$を計算する。次に，ハッシュ値$c$を計算し，$Sk_m = x_m$で$s_2 = r_2 - c(x_m - 2^{\lambda_1})$を計算し，$(c, s_2)$をゲートウェイへ送る。

(4) ゲートウェイはs_1，s_3，s_4を計算し，グループ署名$\sigma = (c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$を出力する。

5.3 グループ署名計算量の比較

Atenieseらのグループ署名方式と当社提案方式とで，グループのメンバーが行うべき指数ビット数を比較した結果を**表1**に示す。

当社提案方式により，グループのメンバーの計算量を1/10以下に低減できる。

表1．署名生成の計算量比較
Comparison of computational complexities of group signature generation schemes

方　式	べき指数ビット数（ビット）	
	グループのメンバー	ゲートウェイ
Atenieseらのグループ署名方式	33,530	−
当社提案方式	2,762	30,768

6 あとがき

グループ署名方式を用いた匿名認証技術と，それを応用した匿名注文システムのプロトタイプについて述べた。プロトタイプの性能評価から，グループ署名の生成が約1.5秒であり，実用上問題のないことがわかった。また，携帯電話などへ実装するために，新たなグループ署名方式を提案し，携帯電話での計算量を1/10以下にできることがわかった。

今後は，実用化に向けたモデルの検討と，携帯電話での試作評価を行う。

なお，この研究は，情報処理推進機構の平成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」を受託し，その成果を元に当社が継続して研究開発したシステムに関するものである。

文　献

(1) 総務省．“平成14年「通信利用動向調査」の結果”．<http://www.soumu.go.jp/s-news/2003/030307_1.html>，(参照 2005-02-07)．

(2) 加藤岳久，ほか．“プライバシを保護する匿名認証システムの開発”．コンピュータ セキュリティ シンポジウム(CSS) 2003予稿集．北九州，2003-10，情報処理学会CSEC研究会．2003，p.569－574．

(3) D. Chaum, E. van Heyst, “Group Signatures”. Advances in Cryptology-Eurocrypt’91. Donald W. Davies. Brighton, UK, 1991-04, The International Association for Cryptologic Research (IACR). Berlin, Springer-Verlag, 1991, p.257－265.

(4) 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, Springer-Verlag, 2000, p.255－270.

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

(6) RSA Security Inc. “RSA Security Study Shows Identity Theft Awareness High, But Consumer Confidence Low”．<http://www.rsasecurity.com/press_release.asp?doc_id=3377&id=1034>，(参照 2005-02-10)．

(7) 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．

加藤　岳久　KATO Takehisa
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。課金決済，プライバシー保護，及びネットワークセキュリティの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Toshiba Solutions Corp.

岡田　光司　OKADA Koji, D.Eng.
東芝ソリューション(株) SI技術開発センター SI技術担当主任，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。電子情報通信学会会員。
Toshiba Solutions Corp.

吉田　琢也　YOSHIDA Takuya, D.Eng.
東芝ソリューション(株) SI技術開発センター SI技術担当，工博。情報セキュリティ技術の研究・開発に従事。
Toshiba Solutions Corp.