セキュリティとプライバシを両立させる匿名認証技術について

解説

佐古和恵（NEC）
k-sako@ab.jp.nec.com

米沢祥子（NEC）
s-yonezawa@da.jp.nec.com

古川　潤（NEC）
j-furukawa@ay.jp.nec.com

セキュリティのために本人確認がいたるところで行われているが，これは誰がどこで何をしていたかという情報が管理されてしまうことになり，プライバシの問題を引き起こしかねない．そこで，本稿では，セキュリティとプライバシの両立を考慮した匿名認証技術について，グループ署名と呼ばれる暗号プロトコルを中心に紹介する．

従来の認証技術と匿名認証技術

ユビキタス社会というのは，「いつでもどこでも誰とでも」つながる夢のような世界であるが，一方で「いつでもどこでも誰からでも」攻撃が可能になりかねないという恐れがある．そのために，認証技術を研鑽し，不正な人のアクセスを防止しようという策がとられている．

認証技術としてよく使われているものにID・パスワード方式がある．この方式では，正当なユーザのIDとパスワードを登録する．ユーザがアクセスするときには，IDとパスワードを入力してもらい，登録されたパスワードとの一致を確認することによってユーザ認証を行っている．ほかに，ディジタル署名[1]による認証技術も普及している．この方式では，正当なユーザのIDと公開鍵を登録する．ユーザがアクセスするときには，登録した公開鍵に対応する秘密鍵を用いて「ディジタル署名」を発行する．この署名が，登録した公開鍵を用いて検証できるかによって，正当なユーザかどうかを認証している．

これらの既存の認証技術に共通することは，「登録されたIDと認証情報があり，認証対象のユーザが，登録IDのいずれかに該当するか否かを判定する」という手順がとられていることである．したがって，ユーザのIDが認証サーバに伝わらざるを得ないのである．しかし，社会のユビキタス化に伴い，このような情報がいたるところで採取され大量に蓄積されると，誰がどこで何をしていたかというプライバシ情報となり，プライバシ問題を引き起こしかねない．

そこで，本稿では，グループ署名と呼ばれる新しい認証技術に基づいた匿名認証方式について紹介する．これは，アクセス権のある人をグループ化し，このグループに属しているかどうかでアクセスを許諾する方式である．この方式では個人を特定する必要がなく，認証サーバに対してもユーザのIDが秘匿されるので，匿名で認証が可能になる．もちろん，従来の認証技術を用いた場合でも，グループ全員に同じパスワードや同じ秘密鍵を配付すれば同じ効果が得られる．しかし，問題があった場合に誰であったかをさかのぼって特定することは不可能になる．グループ署名では，認証履歴から本人を特定することのできる特権者が配置されている．これによって匿名が悪用されない抑止力になっている．また，単にユーザに実名ではないIDを付与する「仮名方式」とは異なり，グループ署名では2つの認証履歴が同一ユーザを認証したものか，2人のユーザを認証したものかの区別も秘匿することができる．

本稿では，グループ署名を導入することによって得られるメリットについてのユースケースに基づいて述べる．次にグループ署名アルゴリズムの概要を紹介し，最近の方式の効率を比較する．また，グループ署名のバリエーションとして，制限回数を超えた不正ユーザの匿名性を剥奪できる方式を紹介する．最後にグループ署名の課題について述べる．

グループ署名のユースケース

➲ 図書貸し出しシステム

グループ署名は，上述したとおり，アクセス権のあるユーザをグループ化し，認証サーバがそのユーザがグループに所属しているかどうかを判定する技術である．さらに，特権者を設定して，匿名性を剥奪することが可能である．本章では，図書貸し出しシステムにおいて，ユーザの趣味嗜好を反映する貸し出し書籍履歴を保護する例を紹介する．

図書館では，本がきちんと返却されれば，誰がどのような本を借りているのか知る必要はない．ただし，期限が過ぎても返却されない人がいれば，督促状を送るなどのアクションを起こしたい．従来のシステムでは，後者の機能を実現するために，誰がどの本を借りたかをすべて明らかにしている．グループ署名を用いると，不正があったときにだけ，不正をしたユーザの氏名が判明するようにできるのである．

この図書貸し出しシステムを例に，グループ署名を用いた手続きがどのようになるか，次に説明する．具体的には，(1) ユーザ登録フェーズ　(2) 書籍貸し出しフェーズ　(3) 延滞時対応フェーズの 3 つがある．

(1) ユーザ登録フェーズ
新規のユーザはユーザ登録を行い，メンバ証明書と秘密鍵を入手する．メンバ証明書とは，図書館に登録したメンバであることを図書館の管理者が証明したものであり，ユーザを特定する情報が記載されている．秘密鍵は，各ユーザ固有の情報である．

(2) 書籍貸し出しフェーズ
ユーザは本を借りるときに，発行されたメンバ証明書と秘密鍵と毎回新たに発生させる乱数を用いて，「匿名認証データ」を生成する．図書カウンターの司書はこの匿名認証データが正当なものか検証する．なお，このとき，ユーザ個別の認証情報を用いて検証するのではなく，全ユーザに共通の認証情報（いわばグループ公開鍵）を用いて検証する．ユーザが登録時に発行された正しいメンバ証明書と秘密鍵を用いていれば，どのユーザであってもこの検証をパスし，正当なユーザであるとみなされる．しかし，この匿名認証データをどのように解析しても，具体的にどのユーザに発行されたどのメンバ証明書と秘密鍵のペアを用いて作成されたものか，割り出すことができない．したがって，ユーザを特定しない「匿名」の認証データになっている．

(3) 延滞時対応フェーズ
書籍ごとに貸し出し時の匿名認証データを記録しておき，その書籍が返却された場合にはその認証データを削除すれば，この書籍を誰が借りたかを知らずに運営することができる．一方，書籍が貸し出し期限を過ぎても未返却の場合には，この認証データの匿名性を剥奪することができる．なぜならば，認証データ中に個人を特定する情報が暗号化されてあり，特別な秘密鍵を用いると復号できるからである．この特別な秘密鍵は，たとえば，図書館の責任者のみが管理し，問題があったときにだけ使用されることが望ましい．

➲ グループ署名の機能

上記のユースケースに沿って説明したように，グループ署名を用いて匿名認証データを生成すると
(1) 匿名認証データから登録されたユーザであるかどうかを判定できる
(2) 匿名認証データから，ユーザ名を特定できない
(3) 特別な秘密鍵を用いると，匿名認証データからユーザ名を特定できる
という機能が提供できるのである．

➲ 匿名認証技術導入のメリット

匿名認証技術を導入するメリットは，従来の認証技術と異なり，ユーザを特定することなく，ユーザのアクセス権限のみを検証できるということである．これはユーザのプライバシが保護されるという点でユーザに安心感をあたえるというメリットがある．一方で認証するサーバ側にもメリットがある．というのも個人情報を扱う場面が限定できるため，個人情報保護にかかる管理コストを低減できるということである．

「個人情報保護法」の施行に伴い，個人情報漏洩防止のためにシステムによる対策から従業員の教育まであらゆる面でコストをかける必要にせまられている．通常のパスワードベースやディジタル署名ベースの認証の場合，認証時に「登録 ID リスト」が必要だったり，認証データ中に個人が特定される ID 情報が含まれたりする．したがって管理対象となる個人情報が多くなってしまうのである．匿名認証技術を用いれば，意味のある情報のかたちでは個人情報が流通しないので，漏洩時の被害が抑えられるというメリットがもたらされる．

➲ 企業間による新たな協業形態

グループ署名技術を導入することによって，企業間の新たな協業形態が実現する可能性がある．たとえば，イ

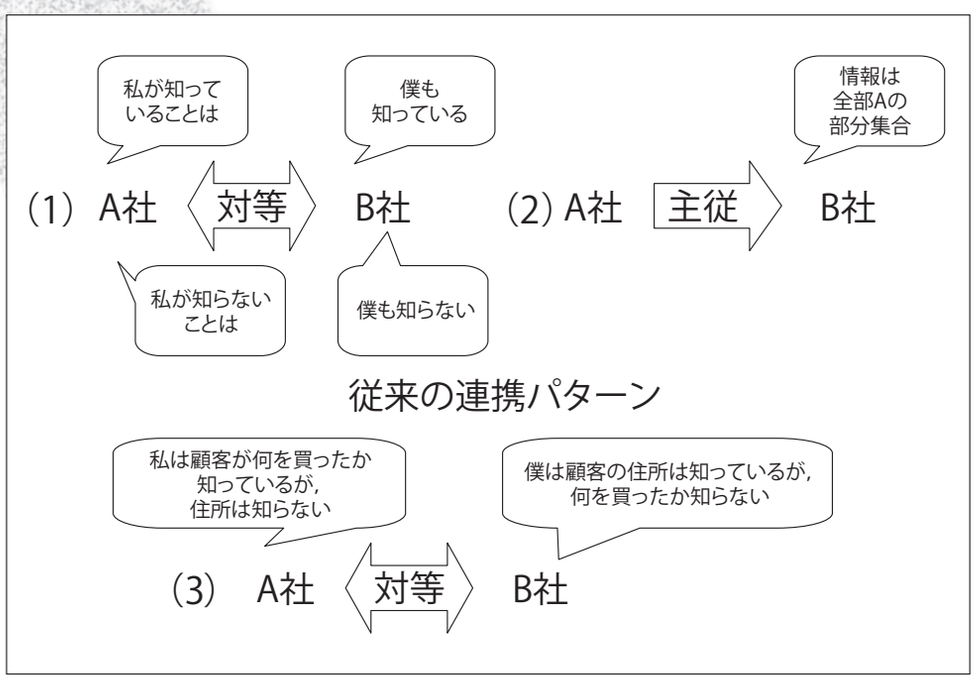

図 -1 従来の連携と新たな協業形態

ンターネットショッピングにおける Web 店舗と配達業者などのように，A 社と B 社が協業して 1 人のユーザにサービスを提供する場合を考える．従来の認証方式を利用した場合，(1) 両方とも対等の立場となる．この場合，両社とも顧客の個人情報を知るか，個人情報を扱わない場合は両社とも扱わない．(2) 一方が従属的な立場になる．この場合，従たる会社は常に主たる会社から部分的な顧客情報のみ知らされる，の 2 種類の連携しか存在し得なかった．今回のグループ署名では，新たな協業方法として (3) 両社とも独立の立場であるが，一方は個人情報を扱い，一方は個人情報を扱わなくてもよい，という連携が可能になる（**図 -1**）．これによって，個人情報を扱わない企業には，個人情報管理コストの低減が，個人情報を持つ企業には，顧客情報の独占が可能になる．

前述のインターネットショッピングを例にとって，グループ署名を用いると具体的にどのように 2 社が協業できるかを紹介しよう．

A 社として，インターネット上の Web 店舗を考える．Web 店舗はよい商品を顧客に販売し利益を上げることが目的である．そして実際の店舗と同様，必ずしも顧客の名前や住所を知る必要がないのである．顧客も，ふらっと立ち寄った店で名前を明かすことなく購入することができるように，必要以上の情報は店舗に提供したくないものである．一方，Web 店舗ではディジタルコンテンツを除くと購入した物品はネット上で持ち帰ることができない．したがって物品を配送するために届け先の住所を報告する必要がある．そこで，宅配業者 B 社のサービスとタイアップし，B 社サービスの顧客からは A 社は氏名住所を受け取らずに，B 社サービスの会員であることの匿名認証データを受け取る．A 社はこの匿名認証データが検証できれば，商品とともに B 社に送る．B 社はこの匿名認証データから秘密鍵を用いて顧客の氏名と住所を特定し，商品を届けることが可能になる [2]．

Web 店舗では物品の配送のみならず，支払いを行わなくてはならない．前述の配送業者 B が代引き配達をすることも考えられるが，クレジットカードによる支払いも一般的になりつつある．一方で，Web 店舗 A が顧客のクレジットカード番号を預かるのはリスクを伴う．そこで A 社はカード会社 C とも連携し，A 社は顧客が C 社のクレジットカード会員であることの匿名認証データを受け取れることにする．匿名認証データから A 社は代金回収が保証され，顧客は自分のカード番号そのものを A 社に知られずにすみ，相互に安心できる商取引ができる．A 社は後日 C 社に匿名認証データを送ると，C 社は匿名認証データから会員を特定しユーザ本人に請求書を送ることができる．

このように，新匿名認証技術によって，複数の独立した企業が，それぞれ相手に過度に依存することなく，明確に情報の扱いを分担することができる．

グループ署名アルゴリズム

ここでは，前述の性質を提供するグループ署名アルゴリズムを紹介する．

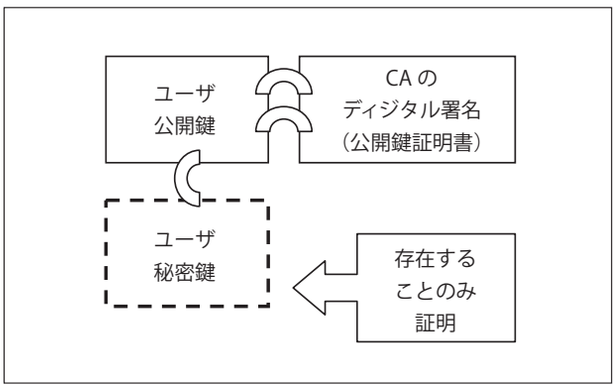

図 -2　ディジタル署名の構成概念図

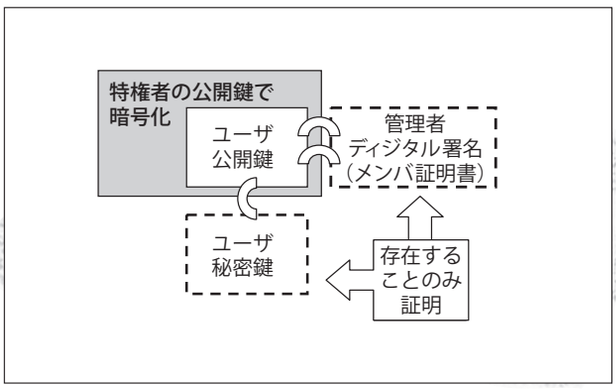

図 -3　グループ署名の構成概念図

➲ アルゴリズムの概略

グループ署名を通常のディジタル署名と対比させて説明する．通常のディジタル署名には，**図 -2** に示すように，個人の公開鍵と，この公開鍵が本人のものであるという認証局（CA, Certificate Authority）のディジタル署名が付加された公開鍵証明書が存在する．認証時には，認証データとして，ユーザは公開鍵と公開鍵証明書を開示した上で，この公開鍵に対応する秘密鍵を持っていることを証明するディジタル署名を提出するのである．認証サーバには，登録されたユーザの公開鍵と公開鍵証明書のリストがあり，開示されたものが登録されていることと，公開鍵に対する正しいディジタル署名かどうかを検証するのである．

このように，ディジタル署名では，ユーザの公開鍵が開示されるので，匿名性は持たない．一方，グループ署名では匿名性を持たせるために，ユーザの公開鍵を特権者の公開鍵で暗号化して開示する（**図 -3**）．この結果，通常の人に対しては匿名性があるが，特権者であれば匿名性を剥奪することが可能になる．なお，この暗号文が同一ユーザで同じ暗号文にならないように，毎回異なる暗号文を生成する確率暗号方式で暗号化する．

しかし，単に公開鍵を暗号化するだけでは不十分である．なぜならば，暗号文を見ても，「正しい公開鍵」が暗号化されているかどうかを確認できないからである．まず，登録を行ったユーザの公開鍵かどうか分からない．未返却のユーザを特定しようとしたのに，復号結果が該当者のいない公開鍵になってしまうのは困る．さらには他人の公開鍵になりすまして暗号化しているかもしれない．したがって暗号化された状態で，登録された公開鍵に正しく復号できることが保証され，かつ，公開鍵を持つ本人が暗号化していることが分かるような仕掛けが必要である．

その仕掛けに「ゼロ知識証明」と呼ばれる技術を用いる．これはもらす「知識」が「ゼロ」で「証明」する技術である．実は，ディジタル署名方式にもこの技術を適用し，秘密鍵に関する知識をまったくもらさずに公開鍵に対応する秘密鍵を持っていることを証明することによって，強固なディジタル署名方式になることが知られている．

グループ署名の例では公開鍵についてもらす知識をゼロにして，正しく登録された公開鍵が暗号化されていることと，ユーザがこの公開鍵の持ち主であることを証明したいのである．まず，公開鍵の持ち主であることを証明できるようにするためには，ディジタル署名同様，この公開鍵に対応する秘密鍵を知っていることを示せばよい．次に正しく登録された公開鍵を定義する必要がある．そのために正しく登録した公開鍵には，公開鍵証明書のように，管理者のディジタル署名が付与されるものとする．これはグループのメンバであることを証明する証明書であるからメンバ証明書と呼ぶ．したがって，自分の公開鍵を暗号化し，この公開鍵にメンバ証明書が存在することと，なおかつ暗号化した人がこの公開鍵に対応する秘密鍵を持つことを証明するゼロ知識証明データを付与すれば，グループ署名のアルゴリズムになる．

認証時には，従来のディジタル署名のように，公開鍵や証明書のリストは不要で，メンバ証明書中のディジタル署名を検証するための管理者の公開鍵と，暗号化に使われた特権者の公開鍵さえあればよい．特権者が匿名性を剥奪するときには，公開鍵リストからどのユーザであったか検索する必要がある．なお，管理者と特権者は役割が違うため，あえて別の名称で呼んでいるが，同一人物がかねてもよい．

➲ アルゴリズムの具体例

図 -4 に基づき，アルゴリズムの具体例を紹介する．これは2004年に提案されたCamenisch-Grothの方式[3)]を簡略化したものである．

まず管理者と特権者の公開鍵がある．これはどのユーザに対しても共通のものである．したがってあわせて「グループ公開鍵」とみなしてもよい．管理者の公開鍵（N,

- 管理者公開鍵：$\mathsf{gpk}_1=(N, a_0, a_1, a_2, k_e, \mathcal{H})$
  特権者公開鍵：$\mathsf{gpk}_2=(g_1, g_2, g_3, P, q)$
  管理者秘密鍵：(p_1, p_2) s.t. $N= p_1p_2$
  特権者秘密鍵：y s.t. $g_2=g_1^{\,y} \bmod P$

  （$\mathcal{H}$：ハッシュ関数）
- ユーザ公開鍵：　$h=g_2{}^r \bmod P$
  メンバ証明書：　(A, e)
  ユーザ秘密鍵：　(x, r)
  s.t. $a_0a_1{}^xa_2{}^r=A^e \bmod N$

図 -4　公開鍵と秘密鍵

- $\bar{b} \leftarrow b^{c2^{k_e}+\tau'_e}a_0{}^{-c}a_1{}^{-\tau_x}a_2{}^{-\tau_r} \bmod N$
  $(\bar{u}_1, \bar{u}_2, \bar{u}_3) \leftarrow (u_1{}^{-c}g_1{}^{\tau_\nu}, u_2{}^{-c}g_2{}^{\tau_\nu+\tau_x}, u_3{}^{-c}g_3{}^{\tau_\nu+\tau'_e}) \bmod P$
- $c = \mathcal{H}(\mathsf{gpk}_1, \mathsf{gpk}_2, b, u_1, u_2, u_3, \bar{b}, \bar{u}_1, \bar{u}_2, \bar{u}_3, M)$
  が成立することを検証

図 -7　グループ署名検証アルゴリズム

- (M, Sig) の正当性を検証.
  $h= u_2 \,/\, u_1{}^y$ を計算.

図 -8　匿名剥奪アルゴリズム

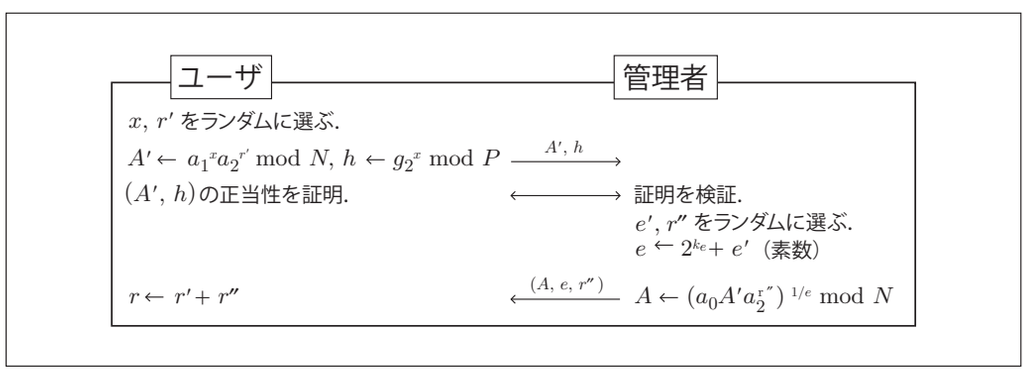

図 -5　ユーザ登録プロトコル

- s, ν をランダムに選ぶ.
  $b \leftarrow a_2{}^sA \bmod N$
  $(u_1, u_2, u_3) \leftarrow (g_1{}^{\nu}, hg_2{}^{\nu}, g_3{}^{\nu+e'}) \bmod P$
- $\rho_x, \rho_r, \rho'_e, \rho_\nu$ をランダムに選ぶ.
  $\bar{b} \leftarrow b^{\rho'_e}a_1{}^{-\rho_x}a_2{}^{-\rho_r} \bmod N$
  $(\bar{u}_1, \bar{u}_2, \bar{u}_3) \leftarrow (g_1{}^{\rho_\nu}, g_2{}^{\rho_\nu+\rho_x}, g_3{}^{\rho_\nu+\rho'_e}) \bmod P$
  $c = \mathcal{H}(\mathsf{gpk}_1, \mathsf{gpk}_2, b, u_1, u_2, u_3, \bar{b}, \bar{u}_1, \bar{u}_2, \bar{u}_3, M)$
  $\tau_x = \rho_x+cx$, $\tau_r = \rho_r + c(r+se)$
  $\tau'_e = \rho'_e+ce'$, $\tau_\nu = \rho_\nu+c\nu \bmod q$
  $\mathsf{Sig} = (b, u_1, u_2, u_3, c, \tau_x, \tau_r, \tau'_e, \tau_\nu)$

図 -6　グループ署名作成アルゴリズム

$a_0, a_1, a_2)$ は，メンバ証明書内の発行者のディジタル署名を検証するためのものであり，特権者の公開鍵 (g_1, g_2, g_3, P, q) は公開鍵を暗号化するためのものである．

次にメンバ証明書を紹介する．これはユーザの公開鍵 h に対して，管理者だけが N の素因数を用いて生成できるディジタル署名 (A, e) からなる．また，ユーザの公開鍵 $h=g_2{}^r$ に対する秘密情報 x はユーザのみが所有する．登録フェーズで，このメンバ証明書を発行するプロトコルは**図 -5** のとおりである．これにより，管理者は，登録されたユーザの ID と公開鍵 h やディジタル署名 (A, e) を紐づけることができる．

図 -6 はグループ署名生成アルゴリズムを示す．(u_1, u_2) はユーザ公開鍵 h を特権者の公開鍵 g_1, g_2 で暗号化している部分である．その他の情報は，暗号化された公開鍵 h に対する発行者のディジタル署名 (A, e) を持っていることと，この公開鍵 h に対する秘密鍵 x を持っていることを，ディジタル署名 (A, e) そのものや秘密鍵を相手に知らせずに，ゼロ知識証明で証明する部分である．ディジタル署名 (A, e) は個人に特有の情報なので，これを見せてしまうと匿名性が保持できない．したがって毎回異なる乱数 s や乱数 ρ'_e を用いて b や τ'_e に変換したものを見せて証明を行っている．また，秘密鍵を知られてしまうと他人に自分になりすまされてしまう恐れがある．そこで，同様に乱数 ρ_x を用いて τ_x に変換している．

図 -7 にあるように，生成された署名 $\mathsf{Sig}=(b, u_1, u_2, u_3, c, \tau_x, \tau_r, \tau'_e, \tau_\nu)$ はグループ公開鍵のみを用いて検証できる．ユーザが暗号化された公開鍵に対する正しい秘密鍵を知っていて，なおかつ正しいメンバ証明書を持っている場合に限り，この等式が成り立つようになっている．

図 -8 にあるように，特権者の秘密鍵 y を用いれば，暗号文 u_1 と u_2 からユーザの公開鍵 h が復元され，これからユーザを特定することができる．

	署名 データ長	署名 計算量	検証 計算量	安全性の仮定
Ateniese-Camenisch-Joyce-Tsudik 2000	23,709	12L (2700E)	11L (2475E)	Strong RSA, DDH
Boneh-Boyen-Shacham Aug. 2004 (*)	2,057	11E+3F (20E)	12E+3F+2P (33E)	q-SDH, DLDH
Camenisch-Lysyanskaya Aug. 2004	5,926	3E+13F (42E)	13F+5P (69E)	LRSW, DDH
Camenisch-Groth Sept. 2004	3,216	4E+4N (28E)	8E+5N (38E)	Strong RSA, DDH
Teranishi Sept. 2004	12,400	5E+10N (65E)	8E+13N (86E)	Strong RSA, DDH
Nguyen et al. Dec. 2004	4,782	20E+6F (38E)	13E+2F+3P (37E)	q-SDH, DBDH
Furukawa-Imai Aug. 2005	1,704	7E+4F (19E)	6E+4F+2P (30E)	q-SDH, DDH

E：楕円曲線のスカラー倍，F：素体上の冪乗剰余
P：ペアリング，N，L：合成数を法とする冪乗剰余（指数部の長さは考慮していない）
(*) 安全性をあわせるために，論文中のプロコトルを一部変更して換算
計算量の括弧内は F=3E，P=N=6E，L=225E と換算した値

表 -1　グループ署名アルゴリズムの比較

既存アルゴリズムの比較

グループ署名の概念は 1991 年に Chaum らによって初めて提唱されたが，当時提案された方式は署名長がグループの大きさに比例してしまう非効率なものであった．その後 1997 年に Camenisch らや Kilian らによって，グループの大きさに比例しない方式が紹介され，さらに 2000 年に Ateneise らにより，より現実的な方式が提案された．その後楕円曲線上に定義される双線形写像を用いた各種アルゴリズムの進展に伴い，高速なグループ署名方式の開発が盛んになった．**表 -1** に最近提案されたグループ署名方式を列挙する．署名データ長，署名生成に必要な計算量，署名検証に必要な計算量，およびそのグループ署名が基づく安全性についても併記している．

グループ署名のバリエーション

上述のグループ署名では特権者の秘密鍵があればどのユーザの匿名性も剥奪できてしまう．そこで，特権者に過度の権限の集中が起きないような方式がいくつか考えられている．

1 つ目は特権的な権限を分散する方式である．すなわち，1 人の特権者の秘密鍵ではユーザを特定することができず，複数の特権者の秘密鍵が集まって初めて匿名性が剥奪できるようにする方式である．このために，秘密分散方式を応用した閾値付暗号を導入したグループ署名アルゴリズムが提案されている [4]．

もう 1 つは，特権者の意思のみでユーザの匿名性が剥奪できるのではなく，不正が起こったときにだけ不正者の匿名性を剥奪できるようにすることである．しかし，不正の発生は常に検出可能とは限らない．1 つの検出可能な「不正」として，制限回数オーバーがある．たとえば，電子投票において有権者は匿名で投票できるが，2 度以上投票するのは不正投票であるので匿名性が剥奪できるべきである．その場合に特権者でなくても即時に不正者を判定できるように提案されているのが回数制限型匿名認証方式 [5] である．この方式では，特権者が匿名性を剥奪したくても，ユーザが不正をしない限り匿名性が守られるという強いプライバシが保たれる．電子投票以外にも，電子回数券などに応用があると思われる．また，インターネット上の試聴をたとえば 5 回までなら無料で匿名のままで視聴できるが，6 回以上視聴した場合には，匿名性が失われ，該当のユーザに課金されるというサービスにも利用できる．

グループ署名技術の課題

グループ署名の課題としては，まず計算量があげられるが，表 -1 でみたような最近の進展により，通常のディジタル署名の 10 倍程度の計算量で実現可能の見込みが見えてきた [6]．

次の課題はユーザの失効である．グループに登録されたユーザ A とユーザ B のうち，ユーザ A のみを失効し

たい場合を考える．しかし，通常はグループ署名データからユーザ A とユーザ B を区別することは不可能である．そこでいくつかの対策が考えられている．以下，ディジタル署名における主な失効方法になぞらえて，（1）短い有効期間方式　（2）有効性問合せ方式（OCSP 方式）（3）失効者周知方式（CRL 方式）で紹介する．

（1）短い有効期間方式
この方式は鍵の寿命を短く設定することにより，使用中の鍵をあえて失効させなくても，新たな鍵を発行しなければよい，という考えに基づくものである．これは短い頻度で全員に新たな鍵を発行しなくてはいけないが，たとえば月極めの Web 新聞視聴などのアプリケーションに適合すると思われる．

（2）有効性問合せ方式
これは，署名の検証者が，受け取ったディジタル署名が有効であるかどうかを OCSP（Online Certificate Status Protocol）という方式によって，検証サーバに逐次問い合わせるディジタル署名の方式にならっている．グループ署名においても，同様に検証サーバを設置し，グループ署名が有効であるかどうか回答してもらうことが考えられる[7]．ただ，この検証サーバに匿名性剥奪相当の権限を譲渡する必要がある．一方，このような検証サーバを設置すれば，どのようなグループ署名アルゴリズムにも適用できるメリットがある．

（3）失効者周知方式
ディジタル署名方式では CRL（Certificate Revocation List）と呼ばれる形式で失効されたユーザを通知している．ディジタル署名を受け取った検証者が，署名者が CRL に掲載されていないか確認する方式である．これと同様にグループ署名でも失効者の情報を用いて検証することができる[8]．ただし，検証者だけではなく署名者が CRL に依存した署名計算を行う必要があることと，匿名性を保持するための特別なグループ署名アルゴリズムを採用する必要がある．

このように，グループ署名の持つ失効に関する問題も，さまざまなアプローチで解決がはかられており，日々その改良が進んでいる．

おわりに

ユーザを特定せずに認証できるという，従来の認証技術の常識をくつがえす画期的な機能を提供するグループ署名方式，およびそのアプリケーションについて紹介した．依然技術として未熟な点も多いが，サーバの都合でユーザのプライバシを犠牲にすることのない，新しいソリューションをもたらす有望な技術である．また，複数の企業が協業してユーザにサービスを提供する場合において，それぞれの企業の権限や企業秘密を守るための基盤にもなる．グループ署名技術をうまく利用することによって，ユビキタス社会において高い安全性を保ったまま，その可能性を大きく広げられる世界になると確信する．

参考文献

1）岡本，山本：現代暗号，産業図書．
2）加藤，岡田，吉田：匿名認証技術とその応用，東芝レビュー，Vol.60, No.6，pp.23-27 (2005).
3）Camenisch, J. and Groth, J. : Group Signatures : Better Efficiency and New Theoretical Aspects, SCN 2004, pp.120-133.
4）Furukawa, J. and Yonezawa, S. : Group Signatures with Separate and Distributed Authorities, SCN 2004, pp.77-90.
5）Teranishi, I., Furukawa, J. and Sako, K. : k-Times Anonymous Authentication, ASIACRYPT 2004, pp.308-322.
6）Furukawa, J. and Imai, H. : An Efficient Group Signature Scheme from Bilinear Maps, ACISP 2005, pp.455-467.
7）米沢祥子，佐古和恵：OMSP レスポンダ：グループ署名における失効メンバ確認モデル，コンピュータセキュリティシンポジウム CSS2004（情報処理学会論文誌掲載予定）．
8）Camenisch, J. and Lysyanskaya, A. : Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, CRYPTO 2002, pp.61-76.

（平成 18 年 3 月 7 日受付）