コンピュータセキュリティ　9－4
（2000．5．10）

属性情報開示における公平性について

須賀 祐治[†]　岩村 恵市[†]　櫻井 幸一[‡]

[†]キヤノン株式会社 画像技術研究所　[‡]九州大学大学院 システム情報科学研究院

近年インターネットの普及に伴い，電子商取引などの経済活動が手軽に行えるようになり個人情報がインターネット上を流れる場面が多くなってきた．個人情報はプライバシ情報でもあるため開示は極力抑えたいという要求がある．しかし，自らの属性情報を公開するかどうかの判断材料としては通信相手の属性情報とすることが多いため，属性情報の開示にはジレンマを生じてしまう．

そこで本稿では公平に個人の属性情報を交換するプロトコルについて考察し，その一つの解決方法を提案する．公平な情報交換プロトコルの一つである ASW プロトコル [1] [2] 上で知識対話証明プロトコルによる属性情報を開示する方式を適用することで，効率的で公平な属性情報開示方法を実現した．

On the fairness in the case of opening attributes

Yuji SUGA[†]　Keiichi IWAMURA[†]　Kouichi SAKURAI[‡]

[†]Visual Information Technology Development Laboratory, CANON INC.

[‡]Graduate School of Information Science and Electrical Engineering, Kyushu University

In recent years, due to the rapid growth of the Internet, it become possible to do economy activity (e.g. the electronic commerce) easily, whereas the service for which it is necessary to confirm identity increased. One wants to suppress to open his own individual (private) information on the network. However, the dilemma has occurred because it makes often the attributes of the communication companion as the judgement material whether to open own attributes.

Therefore, in this paper, we consider about the protocol to exchange the attributes fairly and propose the one way of being solved. We realized the way of opening the attributes efficiently and fairly where two parties, by using zero-knowledge intractive proofs over the ASW fair exchange protocol.

1　はじめに

インターネットの普及に伴い，電子商取引（EC）などの身元確認の必要なサービスがネットワークを介して行われるようになってきた．決済のためにクレジット番号などの決済情報が，また商品配送に必要なために住所や電話番号等の個人情報が商店サーバに送付されている．これらの情報は SSL プロトコル [3] などにより暗号化されて送信されるため通信路上の第 3 者による盗聴を防いでいるが，商店側では収集した顧客情報がどのように管理されているかはユーザ側からは知ることはできない．そのためインターネット上で安心して自らに関する個人情報を公開するしくみが要求されている．

EC などのサービスにおいて，利用者が商店サーバを信用するしくみは信用ラベル方式 [4] [5] や（認証局により発行された）公開鍵証明書 [6] [7] などにより提供されている．つまりサーバを信用するかどうかを判断する基準が公開されているため，クライアントは自らの個人情報を送付するかどうかを判断することができる．しかし，判断材料がない状況の例としてオークションなどのサービスが挙げられる．EC などのクライアント・サーバという通信形態ではなく，クライアント・クライアント間通信を主としており，送信相手の情報を判断材料とするためお互いに同時に自らの個人情報，つまり属性情報を交換するしくみが要求されている．ここで同時交換が保証されない場合，個人情報の流出という不利益を被ることになる．

そこで本稿では公平に個人の属性情報を交換するプロトコルについて考察を行う。属性情報に限らずあらゆるデータを公平に交換する Fair Exchange プロトコルは，先行研究として契約文書の交換（contract signing）や送達確認メール（certified mail），電子マネーによる商品購入（payment with receipt）等のアプリケーションを想定したいくつかの方式が提案されている．しかしこのような同時交換をネットワーク上で実現するのは現実的に不可能である．そこで，同時交換を満たす代わりに「情報を交換する 2 者間の通信において，いかなる状況でデータ送受信が終了したとしても両者のうちどちらか一方に不利益を生じることがない」という **公平性** を定義して擬似的に同時交換を実現している．

[†]E-mail: {suga,iwamura}@cts.canon.co.jp

上記の公平性に基づいた Fair Exchange プロトコルには大きくわけて 3 つのアプローチに分類することができる．(a) 段階的秘密交換方式 [8][9][10]：情報を交換する 2 者間のみで通信が行われ，段階的に情報を開示して近似的に公平性を得る方式である．ゼロ知識対話証明や一方向性関数などにより構成することができるが，一般的に通信量，計算量が膨大になる点や計算量的等価を前提としているなど非現実的なアプローチである．(b) 信用のおける第 3 者機関（Trusted Third Party, TTP）を経由する方式 [11]：すべての通信を TTP を介するアプローチであるが TTP の負荷が大きくなるデメリットがある．

以上のようなデメリットを解消するため上記 (a), (b) の中間的なアプローチとしてオプチミスティック (optimistic) なアプローチ [1] [2] [12] [13] が提案されている．通常時は情報を交換する 2 者間のみのプロトコルで構成されるが，ユーザの不正や通信路の不備などのイリーガルな状況が起こった状況下では TTP との通信が発生するという方式である．TTP に完全に信用を置くのではなく TTP への信用の依存度を下げる考え方に基づいている．

本稿ではオプチミスティックアプローチとして ASW プロトコル [1] [2] を取り上げ，2 者間でお互いの属性情報を公平に交換する方式を提案する．

次章からの流れを紹介する．まず 2 章で ASW プロトコルについて説明する．3 章にて属性証明モデルを提案し，必要な要件を洗い出して既存方式の分類と分析を行い，4 章では特に対話的属性証明プロトコルについて取り扱う．5 章にて本稿におけるアイデアと公平な属性証明プロトコルの提案とセキュリティ面の考察を行い，最後に 6 章で問題点，今後の課題について報告する．

2 ASW プロトコル

オプチミスティック (optimistic) アプローチに分類される ASW プロトコル [1] [2] について詳細に述べる．ASW プロトコルは公平性を確保するために否認防止トークンをお互いに得ることで実現する方式である．

2.1 準備

情報を交換する 2 者を $\mathcal{O}$ (Originator)，$\mathcal{R}$ (Recipient) とし，信用のおける第 3 者機関 (TTP) $\mathcal{T}$ の存在を仮定する．また前提条件として，何らかの公開鍵暗号方式系を用いた公開鍵インフラ（Public Key Infrastructure, PKI）[7] が整備されているとする．つまり各エンティティは公開鍵と秘密鍵の対を保持しており，データの暗号化と署名の検証を正当に行えるとする．

以下の説明で用いる表記法を次に示しておく．

表記法の説明

- i_P：$\mathcal{P}$ が相手に渡したい情報
- e_P：$\mathcal{P}$ が相手に要求する情報を説明するデータ
- $desc(i_P)$：i_P を説明するデータ
- $h(\cdot)$：一方向性関数
- $comm(key, item)$：コミットメント関数．鍵 key で $item$ を暗号化したデータ
- $Sign_{\mathcal{P}}(\cdot)$：$\mathcal{P}$ による署名データ

2.2 要件

公平性と否認防止を含め ASW プロトコルに求められる要件は以下の 5 つ [2] [14] が定められている．$(\mathcal{P}, \mathcal{Q})$ は $(\mathcal{O}, \mathcal{R})$ または $(\mathcal{R}, \mathcal{O})$ のいずれかを示す．

R1. 有効性（Effectiveness） $\mathcal{Q}$ が正しい振る舞いをし $\mathcal{P}, \mathcal{Q}$ ともに中断することがない場合には $\mathcal{P}$ は $desc(i_Q) = e_P$ となる i_Q を得ること．

R2. 公平性（Fairness） 正常にプロトコルを終了した場合 $\mathcal{P}$ は $desc(i_Q) = e_P$ となる i_Q を得ること．

R3. 適時性（Timeliness） プロトコル開始時に適切な時間内でプロトコルが終了することを確認できること．

R4. 否認防止（Non-repudiability） $\mathcal{P}$ が $desc\ (i_Q) = e_P$ となる i_Q を得た場合，$\mathcal{P}$ は $\mathcal{Q}$ から i_Q が送付されてきたこと（NRO, NR of Origin）と $\mathcal{Q}$ が i_P を受領したこと（NRR, NR of Receipt）を証明できること．

R5. TTP 不正検出可能（Verifiability of TTP） $\mathcal{T}$ が不正に振る舞い $\mathcal{P}$ が公平性を失う事態になった場合 $\mathcal{P}$ は第 3 者に $\mathcal{T}$ の不正を証明できること．

2.3 プロトコル構成

ASW プロトコルは $\mathcal{O}$ と $\mathcal{R}$ との間で情報交換が行われる交換プロトコル *exchange* と $\mathcal{O}$ のみによる中止プロトコル *abort* と $\mathcal{T}$ を介して通信される回復プロトコル *resolve* の 3 種類のサブプロトコルから構成される．通常は *exchange* のみが実行される．

2.3.1 *exchange* サブプロトコル

（入力）$\mathcal{O}$ は $i_O, desc(i_O), e_O$ を $\mathcal{R}$ は $i_R, desc(i_R), e_R$ を準備する．

（**Step 1**）$\mathcal{O}$ は r_O, key_O をランダムに選択し $c_O := comm(key_O, i_O)$ を生成する．$m_1 := Sign_{\mathcal{O}}(\mathcal{T}, \mathcal{R}, h(r_O), c_O, desc(i_O), e_O)$ を $\mathcal{R}$ に送信する．

（**Step 2**）$\mathcal{R}$ は $desc(i_O) = e_R$ かどうか判断し満たさない場合はプロトコルを中止する．それ以外の場合は r_R, key_R をランダムに選択し $c_R := comm(key_R, i_R)$ を生成する．$m_2 := Sign_{\mathcal{R}}(h(m_1), h(r_R), c_R, desc(i_R), e_R)$ を $\mathcal{O}$ に送信する．

（**Step 3**）有効な m_2 が返却されなかった場合（$desc(i_R) = e_O$ を満たさない場合も含む）$\mathcal{O}$ は *abort* サブプロトコルを実行する．それ以外の場合 $m_3 := i_O, key_O$ を $\mathcal{R}$ に送信する．

（**Step 4**）有効な m_3 が返却されなかった場合 $\mathcal{R}$ は *resolve* サブプロトコルを実行する．それ以外の場合 $m_4 := i_R, key_R, r_R$ を $\mathcal{O}$ に送信する．

（**Step 5**）有効な m_4 が返却されなかった場合 $\mathcal{O}$ は *resolve* サブプロトコルを実行する．それ以外の場合 $m_5 := r_O$ を $\mathcal{R}$ に送信する．

（**Step 6**）有効な m_5 が返却されなかった場合 $\mathcal{R}$ は *resolve* サブプロトコルを実行する．

（出力）$\mathcal{O}$ は i_R を得るとともに NRO トークンとして m_2, key_R, c_R を NRR トークンとして m_1, m_2, r_R を得る．$\mathcal{R}$ は i_O を得るとともに NRO トークンとして m_1, key_O, c_O を NRR トークンとして m_1, m_2, r_O を得る．

2.3.2 *abort* サブプロトコル

$\mathcal{O}$ は $\mathcal{T}$ に対してプロトコルの中止要求を行う．$\mathcal{T}$ は既に $\mathcal{R}$ から回復要求があるかどうかを調査し，ある場合には $\mathcal{O}$ に *resolve* サブプロトコルを代わりに実行するように要請する．無い場合には要求を受理し $\mathcal{O}$ から中止要求があったことを記録しておく．

2.3.3 *resolve* サブプロトコル

$\mathcal{P}$ ($\mathcal{O}$,$\mathcal{R}$ のいずれか) は $\mathcal{T}$ に対し m_1, m_2 を送信して回復要求を行う．$\mathcal{T}$ は既に中止要求がないか調査し，受理されている場合は要求を棄却する．m_3 以降のメッセージをすべて $\mathcal{T}$ を介して再送するように指示し，プロトコルを監視する．この状況下で情報の交換に均衡が取れていないと判断した場合には $\mathcal{P}$ に対し アフィディヴィットトークン (affidavit token) を発行する．アフィディヴィットトークンは $\mathcal{P}$ に相対する $\mathcal{Q}$ が i_P, r_P を受領したのに対し，$\mathcal{P}$ は i_Q, r_Q を受領しておらず公平に交換されていないことを意味する署名文書である．トークン発行後の $\mathcal{Q}$ に対する制裁などは $\mathcal{T}$ のポリシーやシステム，実装に依る．

3 属性証明

サーバの管理下にあるリソースのアクセスコントロールにおいて，属性情報を認可情報や権限情報として扱うシステムが多く見受けられる．属性情報を開示する方式には様々な提案がされている．本章では既存方式の分析を行い，提案モデル上での分類を行う．

3.1 モデル

本稿では次の定義に基づいた属性情報開示モデルを提案する．

ID 現実世界のエンティティ (Real Entity) とバインドされたある名前空間 namespace における元* .

属性情報 (attribute) ID とバインドされた情報．ID は公開情報であるのに対し，属性情報は開示範囲を限定する必要のある情報 (プライバシ情報) であると考えることができる．

属性証明 (attribute certification) 証明者の属性情報の正当性を検証者に証明すること．

図 1 を用いて Real Entity がサーバからリソースへのアクセス権限 (Privilege) を得ることを目的としたときの属性証明方法について説明する．図中の実線はそれぞれの情報のバインドが確認できることを表わしており，Real Entity から Privilege への経路を確保することによりアクセス権限を得られるを意味する．

しかしネットワーク上で ID や Attribute の保持を証明するためには，公開鍵に対する秘密鍵を保持していることを示す (Proof Of Posession of private key, POP [15]) ことが必要である．POP が無い場合は図 2 b) のように現実世界における名刺と同じ扱いと考えることができる．

*一般的に個人を識別する情報として捉えてもよいが，namespace の管理がグローバルであるがプライベートであるにより Real Entity とのバインドが可能かどうか異なるとする．

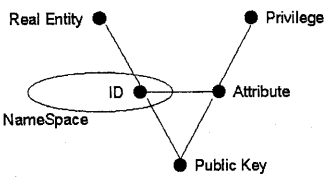

図 1: 属性証明モデル

図 2 a) は X.509 公開鍵証明書 [6] とは別に属性情報だけを切り出した X.509 属性証明書 [16] [17] の利用を示したものである．ID と Public Key のバインドを X.509 公開鍵証明書で，ID と Attribute のバインドを X.509 属性証明書で実現している．X.509 属性証明書単体での利用ではなく，POP を X.509 公開鍵証明書を用いて行う併用型である．このモデルに属する方式としては他に NetBill Project [18] [19] が挙げられる．

本来 X.509 公開鍵証明書は Public Key と ID とのバインドを認証局の署名により保証するものであるが，V3 拡張フィールドを利用して Attribute を記載することにより，図 2 c) のように 3 つのバインドを示すことも可能である．

プライバシ保護の観点から ID とのバインドを取り除いた方式は 図 2 d) で示される．匿名公開鍵証明書 [20] [21] は，公開鍵証明書から ID を省き，公開鍵と属性情報を直接バインドさせることで ID の匿名性を保持しながら属性証明を行うことができる．

その他にもこのモデルに属する既存方式を紹介しておく．グループに属するメンバーは個々に異なる秘密情報を持ちながら，グループとしての公開鍵を公開することにより，署名したメンバー (つまり ID) を秘匿してメンバーのだれかが署名したことを示すことができるグループ署名 [22] [23] という概念が提案されている．このグループを属性情報として捉えることで属性証明に用いることができる．また，SPKI/SDSI [24] [25] や Identity Escrow [26] や Subset Queries [27] などの知識対話証明プロトコルもこのモデルに属する．

3.2 ASW protocol への適用

本稿で目的としている公平な属性情報の交換を ASW プロトコル上で適用させることを考える．図 2 c) モデルで取り上げた X.509 v3 証明書は属性情報を証明書内に含んでいるため POP の時点で属性情報を公開しているため適用できないが，図 2 a) モデル上では，属性情報が X.509 属性証明書のように分離されているためこれを交換する情報 (i_P) として扱うことで ASW プロトコルに適用可能である．

図 2 d) モデル上では c) での問題点と同様に POP の時点で属性情報が公開されているために適用できないが，図 2 e) で示されているように POP で別の公開鍵を用いることにより解決することができる．しかし Identity Escrow [26] や Subset Queries [27] は知識対話証明プロトコルにより属性証明を行うが，ASW プロトコルではこのようなインタラクティブな通信データに対する交換は想定していないため適用できない．そこで次章にて対話的属性証明プロトコルへの適用を試みる．

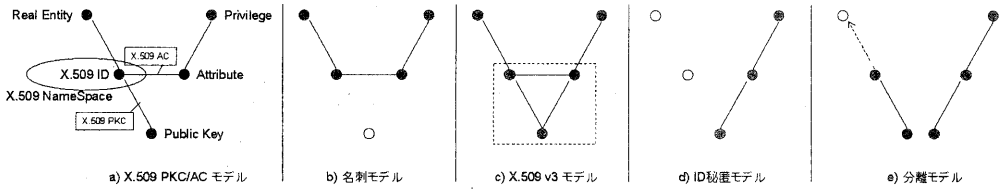

図 2: 属性証明モデルの分類

4 対話的属性証明プロトコル

4.1 属性証明における要件

以下に本稿で目的とする属性証明プロトコルの要件を列挙する.

属性情報の信頼性（完全性） 証明者の属性情報が正しいことを保証すること. 次節にて ID と 属性情報のバインドを保証する機関を仮定することで実現している.

ID の匿名性（追跡不可能性） 属性証明プロトコルの通信データから証明者の ID を特定できないこと. つまり, ID を秘匿したままで属性証明を行うこと.

4.1.1 ID の匿名性について

図 2 e) モデルでは POP で別の公開鍵を用いることが求められており, ASW プロトコルでも自らの署名が検証できる仕組みを備える必要がある. このような仕組みは PKI [7] により構築されることが多いが, ID と Public Key がバインドされた公開鍵証明書を利用することは前節で提示した要件と矛盾することとなる. そこで以降, ID に偽名（pseudoID）を用いた PKI [28] など ID とリンクしない公開鍵が利用できることを仮定する.

また本章では特に Identity Escrow を扱うが, これらの方式には論争や事件が起こった際に別のエンティティ (escrow agent) が ID を復元できるしくみを備えている. これは属性証明プロトコルにおいては必須の要件ではないが, ASW プロトコルにおいては 5.2.2で取り上げるようにアフィディヴィットトークン発行後の処理に利用することが可能である.

4.2 対話的属性証明モデル

証明者が知識対話証明プロトコルによる属性証明を行う際のモデルを次のように考える.

登場エンティティ 証明者（Prover）, 検証者（Verifier）, 属性証明機関（Attribute Authority, AA）

初期設定

- AA は公開鍵暗号系の秘密鍵と公開鍵を持つ.
- AA はあるグループの属性を特徴づけるグループ識別子（GroupID）を公開する.
- AA は証明者に対して属性証明書を発行する. AA の秘密鍵を用いて証明者固有の秘密情報（属性証明書）を作成し, ユーザの属性情報を保証する.

属性証明 証明者は検証者に対し属性証明書（＝証明者固有の秘密情報）を保持しているかどうかを知識証明を用いて証明する.

属性情報のタイプ あるグループのメンバーであるという属性情報 † のみを扱う. 属性情報を識別するためのグループ識別子を GroupID と記述する.

4.3 Identity Escrow

前節のモデルに即して Kilian らにより提案された Identity Escrow [26] を紹介する. Identity Escrow では次の点に着目して属性証明書が発行される.

- グループ G の GroupID δ を公開しておく.
- $a^e - b^e = \delta$ となる (a, b) の組を AA が証明者に発行し, 証明者のグループ G の属性を保証する.
- δ を固定したときに a, b を作るのは（e に対応した）秘密情報 d を持つ AA のみ可能である.

GroupID δ に対する (a, b) を $(a, b; \delta)$ と記述することとする. 属性証明書 $(a, b; \delta)$ を持つユーザが属性証明を行う Identity Escrow ‡ は次の通りである.

初期設定 AA は n, p, q, d, e を通常の RSA と同様に選択し（p, q:素数, $n := pq$, e: $\phi(n)$ と互いに素, $de = 1 \bmod (p-1)(q-1)$ ）, n, e を公開して p, q, d を秘密に保持する.

属性証明書の発行

（GroupID）δ をグループ G の GroupID とし, 何らかの方法で公開する.

（発行）任意の a に対し $b := (a^e - \delta)^d$ を計算し $(a, b; \delta)$ を属性証明書として証明者に発行する.

（ID 埋め込み）a^e の下位ビットに証明者の ID を埋め込んでおく. つまり ID と a^e のバインドを行う.

属性証明 次の過程を規定回数繰り返す.

（Step 1）$(a, b; \delta)$ を保持する証明者はランダムに a_1, b_1, x, y を選び, $a = a_1 a_2, b = b_1 b_2$を満た

† 属性証明を「ある属性を持つことを提示する」と考えると, 属性情報は（1）あるグループのメンバーであるという属性情報,（2）ある属性型に対し属性値を伴う属性情報（つまり属性型と属性値の組）の 2 つのタイプが考えられる.（2）は属性値を含んだグループを考えることで（1）に帰着できるため, 以降の議論においてはモデルを簡素化するために（1）のみを扱っていくこととする.

‡ 論文中で間違いと思われる 3 箇所について修正したプロトコルを紹介している.

すように a_2, b_2 を置く．次の値をゼロ知識コミットメントする．$a_1, a_2, b_1, b_2, {a_1}^e, {a_2}^e, {b_1}^e, {b_2}^e, x, y, x(a_1)^e, x(b_1)^e, x(a_1a_2)^e + y, x(b_1b_2)^e + y$．ただし ${a_1}^e$ と ${a_2}^e$ は escrow agent の公開鍵を用いてコミットメントしておく．

（**Step 2**）検証者は（1）から（5）をランダムに選択し証明者に送信する．

（**Step 3**）証明者は検証者の指示に従い，次のいずれかを開示する．
(1) $x, a_1, {a_1}^e, x(a_1)^e, b_1, {b_1}^e, x(b_1)^e$
(2) $a_2, {a_2}^e, b_2, {b_2}^e$
(3) $x(a_1)^e, {a_2}^e, y, x(a_1a_2)^e + y$
(4) $x(b_1)^e, {b_2}^e, y, x(b_1b_2)^e + y$
(5) $x, x(a_1a_2)^e + y, x(b_1b_2)^e + y$

（**Step 4**）検証者はそれぞれの値が式を満たしているかどうか確認を行う．

ID の復元 escrow agent はコメットメントされた情報から ${a_1}^e$ と ${a_2}^e$ を復元して a^e を得ることにより，証明者の ID を特定することができる．

5 提案方式

前章の Identity Escrow を ASW プロトコル上で行うことを目的とする．以下にアイデアと満たすべき要件について述べる．

アイデア 本来証明したい GroupID を隠蔽してお互いにダミー GroupID による属性証明を行い，後で ASW プロトコルにより正当な GroupID を公平に交換する．

証明者は GroupID g に対応する属性証明書を保持すると仮定する．ここでランダムな値 R を生成し，R と g からダミー GroupID g' と，g' に対する属性証明書を生成する．証明者は ASW プロトコルにおいてランダムな値 R を暗号化し，検証者にコミットメントしておく．その後，g' に対する属性証明書を用いて GroupID g' の属性証明を行う．この作業を公平な属性証明を行う 2 者間で相互に行う．つまり ASW プロトコルをランダムな値 R の公平な開示に利用する．

要件 このアイデアのもとでの要件を示す．

- ダミー GroupID g' から GroupID g に関する情報が漏れないこと．
- ランダム値 R を公開しても，GroupID g に対応する属性情報を保持すること以外の情報が漏れないこと．

5.1 ASW プロトコルへの適用

GroupID δ に対する属性証明書 $(a, b; \delta)$ を保持する証明者を考える．$(aR)^e - (bR)^e = \delta R^e$ を満たすことから，ランダムな値 R を生成し，属性証明書を $(aR, bR; \delta R^e)$ としてダミー GroupID δR^eに対する属性証明を行うことが可能である．

目的 エンティティ $\mathcal{X}, \mathcal{Y}$ 間でお互いの属性情報を公平に交換すること．

前提 エンティティ $\mathcal{X}, \mathcal{Y}$ は属性証明書としてそれぞれ $(a_x, b_x; \delta_x)$, $(a_y, b_y; \delta_y)$ を持つとする．

（**Step 1**）$\mathcal{X}$ はランダムな値 R_x を生成し，ダミー GroupID を $\delta_x {R_x}^e$とおく．$\mathcal{Y}$ も同様の操作を行い，R_y を生成する．

（**Step 2**）$\mathcal{X}$ は交換したいデータ i_X を R_x とし，$desc(i_X)$ は空に e_X には $\mathcal{Y}$ に公開して欲しい GroupID のリストを格納して m_1 を生成し $\mathcal{Y}$ に送付する．

（**Step 3**）$\mathcal{Y}$ は GroupID リスト e_X に自分の公開したい GroupID が含まれているか判断し，含まない場合はプロトコルを中止する．それ以外の場合は i_Y, $desc(i_Y)$, e_Y を同様にして m_2 を作成し $\mathcal{X}$ に送信する．

（**Step 4**）$\mathcal{X}$ は GroupID リスト e_Y から判断してプロトコルを継続するかどうか判断する．中止要求をする場合には *abort* プロトコルを実行する．

（**Step 5**）$\mathcal{X}$, $\mathcal{Y}$ はそれぞれ GroupID を $\delta_x {R_x}^e$, $\delta_y {R_y}^e$ として属性証明を行う．複数の GroupID の証明を行う場合も同じ R_x (または R_y) を用いてダミー GroupID を生成して属性証明を行う．

（**Step 6**）以降，ASW プロトコルに基づいて $i_X = R_x$ と $i_Y = R_y$ の交換を行う．

5.2 考察

5.2.1 不正な GroupID の利用

ダミー GroupID は正規の手順に則って生成されていない場合が考えられる．Identity Escrow においてはランダムに a', b' を選択することで $\delta' = {a'}^e - {b'}^e$ を GroupID として属性証明可能である．正規の手順で生成した場合には $\delta' = {r'}^e \delta$ となる r' を知っているが，不正した場合は r' を計算することは困難であるため m_1 内で含まれるべき r' は偽造されることとなる．

5.2.2 ID 復元の可能性

ASW プロトコルにおけるコミットメント関数で利用する鍵に AA の公開鍵を用いる方法も考えられる．鍵として AA の公開鍵を用いることによりコミットメントされた R を復元することができ，本来の GroupID を知ることができる．さらにこの性質を用いて，アフィディヴィットトークンが発行されたエンティティは AA に申し出を行い ID 復元の申請を行うことができる．

不正利用を発見した AA は不正ユーザの属性情報の開示や属性証明書の廃棄などの措置が行われる．

5.3 別の属性証明方式

5.1 とは別のダミー GroupID による属性証明方式について触れる．GroupID δ に対する属性証明書 $(a, b; \delta)$ を保持する証明者を考える．$a^e - (bR)^e = \delta + (1 - R^e)b^e$ を満たすことから，ランダムな値 R を生成し，属性証明書を $(a, bR; \delta + (1 - R^e)b^e)$ としてダミー GroupID $\delta + (1 - R^e)b^e)$ に対する属性証明を行うことができる．ASW プロトコルにより本当の GroupID δ を明かす場合には R だけでなく b^e も検証者に公開する必要がある．そのため ASW プロトコル においては b^e も i_P 内に含んでおく必要がある．

本方式においては，検証者なら誰でも δ と b^e により a^e が復元できるため Identity Escrow としての仕組みが有効に活用できないが，a^e から Real Entity へのバインドは AA のみが知るように namespace がプライベートに管理されていれば匿名性は保たれる．しかしこの場合，追跡可能性は弱い条件しか満たさなくなる．つまり ID は特定できないが pseudoID（ここでは a^e）は特定でき，複数の属性証明プロトコルの通信内容から同一 ID による証明が行われていることを追跡される可能性がある．

6 まとめ

公平に個人の属性情報を交換する方式として ASW プロトコル上で知識対話証明プロトコルによる属性情報を開示する方式を提案した．属性証明方式としては現在主に X.509 属性証明書の標準化 [16] と製品化が進められているが，本提案方式の実装による評価を行い有用性を検討したいと考えている．

ASW プロトコルの改良としては，送達確認メールにおけるプライバシ保護 [14] や期日指定条件の導入 [29]，マルチパーティプロトコルへの拡張 [30] など幅広い研究が行われている．今後それぞれの提案に対して，本提案方式の適用を試みる必要があると考えている．

参考文献

[1] N. Asokan, V. Shoup, M. Waidner, Optimistic protocols for fair exchange, 4th ACM Conference on Computer and Communications Security, pp.7-17, 1997.

[2] N. Asokan, V. Shoup, M. Waidner, Asynchronous Protocols for Optimistic Fair Exchange, 1998 IEEE Symposium on Security and Privacy, pp.86-99.

[3] SSL 3.0 Specification, http://home.netscape.com/eng/ssl3/

[4] プライバシマーク制度, http://www.privacymark.gr.jp/

[5] オンラインマーク付与制度, http://www.jadma.org/whatsnew/olm-r.html

[6] ITU-T Recommendation X.509, "Info. tech. - OSI - The Directory: Authentication framework", 1993.

[7] R. Housley, W. Ford, W. Polk, D. Solo, X.509 Certificate and CRL Profile, RFC2459, 1999.

[8] T. Tedrick, Fair exchange of secrets, CRYPTO'84, pp.434-438.

[9] R. Cleve, Controlled Gradual Disclosure Schemes for Random Bots and Their Application, CRYPTO'89, pp.573-588.

[10] E. F. Brickell, D. Chaum, I.B. Damgard, J. Graaf, Gradual and Verifiable of a Secret, CRYPTO'87, pp.156-166.

[11] ISO/IEC JTC21/SC27, Information technology - Security techniques - Non-repudiation, 13888-1, 13888-2, 13888-3, 1996.

[12] Y. Frankel, Y. Tsiounis, M. Yung, "Indirect Discourse Proofs": Achieving Fair Off-Line Electronic Cash, ASIACRYPT'96, pp.286-300.

[13] M. Franklin, M. Reiter, Fair exchange with a semi-trusted third party, Proc. ACM Conference on Computer and Communications Security, 1997.

[14] J. Zhou, R. Deng, F. Bao, Some Remarks on a Fair Exchange Protocol, PKC'2000, pp.46-57.

[15] C. Adams, S. Farrell, Certificate Management Protocols, RFC2510, 1999.

[16] S. Farrell, R. Housley, An Internet Attribute Certificate Profile for Authorization, draft-ietf-pkix-ac509prof-02.txt, 2000 (work in progress).

[17] 須賀, 荒木, 公開鍵インフラにおける属性証明書の利用について, ソフトウエアシンポジウム'99, pp.102-107.

[18] B. Cox, J. Tygar, M. Sirbu, NetBill Security and Transaction Protocol, First USENIX WorkShop of Electoronic Commerce, pp.77-88, 1995.

[19] Y. Kawakura, M. Sirbu, I. Simpson, J. Tygar, Flexible and Scalable Credential Structures: NetBill Implementation and Experience, Cryptographic Techniques and E-Commerce, pp. 231-235, 1999.

[20] K. Oishi, Anonymous Public Key Certificates and Group Signatures, SCIS'97-27E.

[21] K. Oishi, M. Mambo, E. Okamoto, Anonymous Public Key Certificates and their Applications, IEICE Trans. Fundamentals, Vol. E81-A, pp.56-64.

[22] D. Chaum, E. van Heyst, Group Signature, EUROCRYPT'91, pp. 257-265.

[23] L. Chen, T.P.Pedersen, New Group Signature Schemes, EUROCRYPT'94, pp.171-181.

[24] P. Nikander, Y. Kortesniemi, J. Partanen, Preserving Privacy with Certificates in Distributed Delegation, PKC'99, pp.136-153.

[25] 川倉, ID 証明書と属性証明書の併用によるアクセス制御方式, CSS'98, pp.97-102.

[26] J. Kilian, E. Petrank, Identity Escrow, CRYPTO'98, pp.169-185.

[27] D. Boneh, M. Franklin, Anonymous authentication with subset queries, the 6th ACM Conference on Computer and Communications Security, pp. 113-119, 1999.

[28] 大石, 松本, 今井, 匿名通信ネットワーク上で公平に名乗り合う方法, 電子情報通信学会論文誌 Vol. J75-D-I, No.6 pp.370-379.

[29] 神田, 松本, 公平な情報交換プロトコルに関する一考察, SCIS-2K, B-13, 2000.

[30] J. Kim, J. Ryou, Multi-party Fair Exchange Protocol Using Ring Architecture Model, JW-ISC 2000, pp.117-124.