社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（41）
2005－CSEC－28（41）
2005／3／23

代理アクセスを利用した匿名認証方式

千田 浩司† 谷口 展郎† 塩野入 理† 金井 敦†

†NTT 情報流通プラットフォーム研究所
239-0847 横須賀市光の丘 1-1

{chida.koji,taniguchi.noburou,shionoiri.osamu,kanai.atsushi}@lab.ntt.co.jp

あらまし 本稿では、権限分散型の不正ユーザ追跡機能を持つ匿名認証方式を提案する。提案方式は、単純な代理アクセスによって被認証者のプライバシを保護し、フェアブラインド署名及び閾値暗号の利用により、閾値数以上の預託機関が協力してはじめて被認証者の追跡が可能となる。被認証者が認証相手に与える情報は、鍵更新する事無しに、容易に被認証者と結び付く情報を一切含まない。更に不正ユーザの署名鍵は、閾値数以上の預託機関が協力する事で即時に無効化出来る。

Anonymous Authentication System Using Proxy Servers

Koji Chida Noburou Taniguchi Osamu Shionoiri Atsushi Kanai

†NTT Information Sharing Platform Laboratories
1-1 Hikarinooka, Yokosuka
Kanagawa, 239-0847 Japan

{chida.koji,taniguchi.noburou,shionoiri.osamu,kanai.atsushi}@lab.ntt.co.jp

Abstract This paper proposes an anonymous authentication system that identifies a malicious user in a threshold manner. The proposed system protects user privacy by simply using proxy servers and employs a fair blind signature and threshold cryptosystem to identify a malicious user. In the system, each signature is separable against a verifier without updating secret/public keys and the certificate, moreover, any secret key can easily be revoked if a certain number of escrow agents collaborates.

1 はじめに

1.1 背景

健全なネットワーク社会の実現には本人認証技術の存在が不可欠であると考えられる。特にweb サービスにおいては、ユーザの行動や信頼性がサービス品質に大きく影響する場合があるため、ユーザの不正行為の抑制という意味でも本人認証は非常に有効である。しかし一方で、ユーザの不正行為の抑制を目的とした本人認証が社会に受け入れられる為には、被認証者のプライバシ保護が大きな課題と言えるだろう。本人認証技術は実際、認証機関側に悪意があれば簡単に被認証者のプライバシを侵害出来る可能性があり、この問題は無視出来ない。

被認証者のプライバシ保護を考慮した本人認証技術としては、「ID エスクロー」が有効であるとおもわれる。ID エスクローとは、被認証者の本人性を預託機関が担保する事で、被認証者は自身を認証機関に識別される事無く認証を受

けられる方式を指す [9][1]。匿名証明書やグループ署名 [5] は、ID エスクローの代表的な技術と言える。しかし実際には既存の ID エスクロー実現方式が満たすプライバシ保護要件は様々であり、用途に応じて適切に利用する事が重要である。

1.2 本稿の結果

本稿では、本人認証技術を不正ユーザの追跡手段として捉え、その中で規律正しいユーザのプライバシは最大限配慮する事を目的とした、従来に無いモデルの ID エスクロー技術を提案する。特に提案方式は運用面において以下の特徴を持つ。

(Replaceability) 認証プロトコルに用いる署名方式は限定されない (任意で良い)。

(Separability) 被認証者が認証プロトコル実行の際に認証機関に与える情報は、容易に被認証者と結び付く情報 (識別番号や公開鍵等) を一切含まない。

(Revocability) 不正ユーザの署名鍵は即時に無効化出来る。

1.3 本稿の構成

以降、先ず第 2.1、2.2 節でそれぞれ、従来の ID エスクローに関する準備と被認証者のプライバシ保護要件の分類を行い、第 2.3 節で、その分類に沿って既存の代表的な ID エスクロー技術を紹介する。そして第 3 節では、先ず第 3.1 節で ID エスクローを実現する新しいプロトコルを提案し、それに特化したプライバシ保護要件を第 3.2 節で明らかにする。第 3.3 節では、そのプライバシ保護要件を提案プロトコルがどの程度満たすか評価し、運用上の効果についての考察も行う。最後に今後の課題について第 3.4 節で言及する。

[1] [9] では後述の *Separability* の要件を満たす ID エスクローのみを考察対象としているが、本稿ではその要件を満たさない方式も考察の対象とする。

2 従来技術

2.1 準備

従来の ID エスクローの一般的なモデルは、被認証者、認証機関、及び預託機関から成る。ここで被認証者は、預託機関に対して登録を行う事を前提に多数存在するものとする。認証機関は、預託機関が担保する被認証者の本人性を受け入れる事の出来る任意の機関であり、単一または複数のどちらでも良い。そして預託機関は、単一または複数から成り、複数であれば何れの預託機関も被認証者を識別 (追跡) する事が出来ず、追跡するためには閾値数以上の預託機関の協力が必要となる。即ち、被認証者を追跡する権限は複数の預託機関に分散されていると見る事が出来る。なお [9] では、複数の預託機関の何れかは証明書発行機関として位置付けている。

被認証者の追跡権限を単一の預託機関に与えるのでは無く複数の機関に閾値付きで分散させる事は、運用上の観点から次の四つの利点があると考えられる。

(預託機関の信頼性向上) 預託機関が秘密裏にユーザ (被認証者) のプライバシを侵害する事が困難となる。

(リスク分散) 一部の預託機関の保持する秘密情報 (ユーザの Identity や暗号秘密鍵等) が内部／外部犯行または何らかの過失によって漏洩した場合でも、ユーザのプライバシは侵害されずに済む。

(システムの頑健性向上) 一部の預託機関の保持する秘密情報が復元不能な状態になったとしても、他の閾値数以上の預託機関の協力により不正ユーザを追跡する事が出来る。

(柔軟な運用体系) 認証機関が預託機関を兼ねた場合でも被認証者のプライバシは損なわれない。

表 1: 被認証者のプライバシ保護要件の分類 (I)

	匿名性	
	Pseudonymity	Separability
認証機関	レベル A1	レベル A2
認証機関 + 一部の預託機関	レベル B1	レベル B2

2.2 プライバシ保護要件 (I)

インターネット上でユーザの匿名性について論じる時は、匿名性の要件を Pseudonymity 及び Separability の観点で分けて考える場合が多い。ここで Pseudonymity はユーザの Identity を秘匿する性質を表し、Separability は複数のトランザクションが同一ユーザによるものかどうか識別困難な性質を表す。特に後者の性質が満たされれば、何れかのトランザクションにおいて匿名性が失われた際の被害が最小限で済み、リスク分散の意味で大変有効と考えられる。また後者の性質が満たされれば前者の性質も満たす事は明らかである。即ち Separability はユーザに対するより強いプライバシ保護要件と言える。

上述の議論を ID エスクローの場合に置き換えて見た時、ユーザは被認証者、そしてユーザのプライバシを侵害する可能性のある機関は認証機関及び預託機関である。そこで本稿では、従来の ID エスクローにおける被認証者のプライバシ保護要件として、先ず表 1 に示すプライバシ保護要件の分類を行う。ここで例えば表 1 のレベル A1 は、認証者に対して Pseudonymity を満たすような性質を意味する。また本分類においては、レベル A1 が最もプライバシ保護レベルが低く、レベル B2 が最も高い事は明らかである。

一方、預託機関は本来、被認証者を追跡出来る権限を持つ存在であるが、レベル B1 を満たさない方式は言い換えれば、認証機関及び単一の預託機関が結託する事で任意の被認証者の追跡が可能であり、レベル B1 を満たす方式は、閾値数以上の預託機関の協力無しでは如何なる被認証者も識別されずに済む。

2.3 既存方式の評価

ここで表 1 の分類に沿って、既存の代表的な ID エスクロー技術のプライバシ保護レベルを評価する。

先ず基本的な匿名証明書方式は、レベル A1 しか満たさないような ID エスクロー技術と言える。これは単一の預託機関が発行した、被認証者の識別情報を含まない (即ち匿名の) 公開鍵証明書を複数回の認証に繰り返し用いる方法である。その場合、同一の証明書を繰り返し用いるためレベル A2 は満たさない。しかし匿名証明書方式は、単純な応用によりレベル A2、B1、B2 を満たす事が出来る。先ず、被認証者は署名鍵をワンタイム利用とする、即ち、認証毎に署名鍵対を生成し、単一の預託機関から匿名の公開鍵証明書 (以降これを匿名証明書と略す) を発行して貰う事で、レベル A2 を満たすようになる。そして匿名証明書を発行する預託機関を複数として連鎖発行型とすればレベル B1 を満たす。ここで連鎖発行型とは、複数の預託機関が順次匿名証明書を更新する方式を指す。即ち、連鎖発行型匿名証明書を用いれば、発行に関わった全ての預託機関が協力しない限りは被認証者の追跡が困難となる事が期待出来る。そして更にワンタイム利用の連鎖発行型匿名証明書とすればレベル B2 を満たす事も可能だが、その場合 Separability の要件を満たすためには、認証回数の限度が預託機関の総数以下となるだけで無く被認証者は頻繁に鍵更新をする必要があるため、利便性及び管理コストに難があると言える。これに対して、権限分散型のグループ署名及びその類似技術 ([3] 等) は、被認証者の鍵更新は不要ながらレベル B2 を満たす、利便性、管理コストに優れた技術である。しかし認証時の処理手続きがオリジナルの電子署名と比べ一般に複雑である事、そして不正ユーザの署名鍵を無効化するための安全かつ効率的な仕組みが確立されていないといった課題もある。

以上、上述の既存方式に対するプライバシ保護レベルの評価を表 2 にまとめる。

表 2: 主な ID エスクローの要件分類

	匿名性	
	Pseudonymity	Separability
認証機関	複数回利用 匿名証明書	ワンタイム 匿名証明書
認証機関 ＋ 一部の預託機関	連鎖発行型 匿名証明書	権限分散型 グループ署名

3 提案技術

本節では、第 1.3 節でも述べたとおり、先ず ID エスクローを実現するための提案プロトコルを第 3.1 節で説明した後、第 3.2 節でそれに特化した被認証者のプライバシ保護要件を明らかにする。そして第 3.3 節でそのプライバシ保護要件を提案プロトコルがどの程度満たすか評価し、運用上の効果についての考察も行う。最後に今後の課題について第 3.4 節で言及する。

3.1 提案プロトコル

本稿で提案する ID エスクロー実現のためのプロトコルは以下の手続きから成る。尚ここで、各通信における送受信の事実は、署名付与により否認出来ないものとする。

【セットアップ】

預託機関 $T = \{T_1, \ldots, T_n\}$ は協力して、フェアブラインド署名 [4] の秘密鍵／公開鍵の組 (SK_{FB},PK_{FB})、及び閾値暗号 [8] の秘密鍵／公開鍵の組 (SK_{TC},PK_{TC}) を生成し、PK_{FB}, PK_{TC} を公開する。

【仲介機関登録】

1. 仲介機関 A_i $(i = 1, 2, \ldots)$ は任意の署名アルゴリズムを用いて署名生成鍵／検証鍵の組 (GK', VK') を生成し、VK' を T に送信する。
2. T は協力して、VK' の証明書 $CERT'$ を生成して[2] A に返信し、A の Identity と VK' とを対応付けて分散保管する。

【ユーザ登録】

1. ユーザ (被認証者) P_j $(j = 1, 2, \ldots)$ は任意の署名アルゴリズムを用いて署名生成鍵／検証鍵の組 (GK, VK) を生成し、VK を PK_{FB} よりブラインド化し、その結果 $\widetilde{VK}$ を T に送信する。
2. T は協力して、$\widetilde{VK}$ を元に VK のブラインド化証明書 $\widetilde{CERT}$ を生成して P_j に返信し、P_j の Identity と $\widetilde{VK}$ とを対応付けて分散保管する。
3. P_j は $\widetilde{CERT}$ をアンブラインドして VK の証明書 $CERT$ を取得する。

【認証】

1. P_j は認証毎に適当な仲介機関を一つ選び (これを A_k とする)、$(GK, VK, CERT)$ を用いてチャレンジ＆レスポンス認証を行う事で A_k に対して P_j の本人性を証明し、認証機関 V のアドレス $ADDR_V$ 及びメッセージ MSG を A_k に送信する。
2. A_k は P_j との認証時のログを PK_{TC} より暗号化し (ログ情報及びその暗号文をそれぞれ LOG, C_{TC} とする)、$ADDR_V$ に従って V にアクセス後、$(GK', VK', CERT')$ を用いてチャレンジ＆レスポンス認証を行う事で V に対して A_k の本人性を証明し、MSG 及び C_{TC} を V に送信する。

【不正ユーザ追跡】

1. V は C_{TC}、MSG、及び A_k との認証のログ LOG' を T に送信する。
2. T は MSG、LOG' から被認証者の追跡の妥当性を検証し、追跡する必要があると判断した場合は協力して以下を行う。
   (a) C_{TC} を復号し、復号結果 LOG に含まれる VK を取得する。

[2] ここで $CERT'$ は閾値数以上の預託機関によって保障された証明書であるとする。これは例えば多重署名 (具体的な実現方式は [10] 等を参照) を用いる事で実現出来る。

(b) VK が被認証者の署名検証鍵である事を認証のログ情報 LOG から確認する。

(c) VK に対応する $\widetilde{VK}$ をフェアブラインド署名技術により特定し、最終的に $\widetilde{VK}$ に対応する P_j の Identity を得る。

上記プロトコルにおける不正ユーザ追跡の頑健性については、第 3.3 節で考察する。またここで上記プロトコルに関して幾つか補足しておく。先ずフェアブラインド署名とは、簡単に言えばユーザ以外にもアンブラインド可能な機関が存在するブラインド署名であり、提案プロトコルではアンブラインド権限は $T_1, \ldots, T_n$ に閾値付きで分散されているものと仮定する。具体的な実現方法については、紙面の都合上、本稿では省略する。なおフェアブラインド署名の技術動向については、例えば文献 [2] に詳しい。また閾値暗号は、復号権限が閾値付きで分散された暗号方式の総称であり、Desmedt らが 1989 年に提案して以来、様々な方式が提案されている。詳しくは文献 [7] 等を参照されたい。一方、被認証者は認証機関との通信路間に仲介機関を多段に中継させて効果的にプライバシを高める事も出来る。しかしその実現方法は [6] で提案された手法を直接適用すれば良く、ここでは説明を省略する。

3.2 プライバシ保護要件 (II)

第 3.1 節から分かるように、提案方式は従来の ID エスクローのモデルに仲介機関が加わった新しいモデルである。そこで表 1 の分類方法に基づき、提案方式のモデルにおける被認証者のプライバシ保護要件について表 3 に示す分類を行った。ここで被認証者のプライバシを侵害する可能性のある仲介機関は複数存在する場合があるため、一部の仲介機関を対象とした要件を含めた。なお全仲介機関とは、ここでは預託機関に登録した全ての仲介機関では無く、被認証者のプライバシを侵害する可能性のある全ての仲介機関を意味するものとする。即ち、被認証者が認証時に選んでいない仲介機関は被認証者のプライバシ侵害に関わる情報を一切持たないため、考察の対象から外して良い。

表 3: 被認証者のプライバシ保護要件の分類 (II)

	匿名性	
	Pseudonymity	Separability
認証機関	レベル A1	レベル A2
認証機関 + 一部の仲介機関	レベル A1’	レベル A2’
認証機関 + 全仲介機関	レベル A1”	レベル A2”
認証機関 + 一部の預託機関	レベル B1	レベル B2
認証機関 + 一部の仲介機関 + 一部の預託機関	レベル B1’	レベル B2’
認証機関 + 全仲介機関 + 一部の預託機関	レベル B1”	レベル B2”

3.3 考察

ここでは先ず提案方式が満たすプライバシ保護要件を表 3 に基づいて評価し、次に第 3.1 節で与えた提案プロトコルにおける不正ユーザ追跡の頑健性の考察を行い、最後に提案方式の運用上の効果を述べる。

【Pseudonymity】 被認証者の Identity は、フェアブラインド署名によって閾値数以上の預託機関が結託しない限りは秘匿される。従って提案方式はレベル B1” を満たす。

【Separability】 認証機関は、非認証者では無く仲介機関と認証を行うため、閾値暗号の秘匿性に基づき、認証機関単独では複数のトランザクションが同一ユーザによるものかどうか識別困難である。また仲介機関はその数が十分大きく[3]、かつ被認証者は認証毎に異なる仲介機関を選ぶと仮定すれば、認証機関が非認証者の同一性を識別するためには当該認証に関わった複数の仲介機関の協力が必要となる。更に [6] で提案された方式を用いれば、被認証者の同一性を識別するための仲介機関の閾値数を任意に設定出来る。従って提案方式はレベル A2’ を満た

[3]実際、仲介機関は数に制限が無く預託機関に登録するだけで良いため、多数のユーザが仲介機関の役割を兼ねる事も可能である。またこれにより仲介機関の数は預託機関の数よりも十分大きいと見る事が出来る。

すと言える。また、閾値数以下の預託機関は被認証者の同一性を識別するための有意な情報を持たない事から、結局、提案方式はレベル B2' を満たすと言える。

【不正ユーザ追跡の頑健性】　仲介機関が第 3.1 節で示した認証手続きを正しく行い正常に認証処理が終了した場合は、同節の不正ユーザ追跡手続きを認証機関及び閾値数以上の預託機関が正しく行う事によって確実に不正ユーザを追跡する事が出来る。なお仲介機関は不正処理する事で不正ユーザの追跡を妨害する事は可能だが、その場合は認証時のログより仲介機関の不正が露呈するため、罰則規定等の運用対処により仲介機関の不正はある程度抑止出来ると考えられる。

【運用上の効果】　提案方式では、認証プロトコルは任意の署名方式によるチャレンジ＆レスポンス認証で良いため、運用が比較的容易と成る事が期待出来る。また仲介機関を通信路に中継させるため、IP アドレスの秘匿等ネットワークレベルの匿名性も高まる。更に、不正ユーザ追跡処理により特定されたユーザの署名鍵は、単純にその証明書 $CERT$ を失効証明書として仲介機関に公開する事で無効化出来る。

3.4　今後の課題

提案方式の大きな課題は、表 3 のレベル B2" を満たす改良方式の実現である。そしてもう一つは、有効期間やユーザが所属する組織名といった公開情報を署名鍵に結び付けるための技術拡張が挙げられる。具体的に言えば、提案プロトコルでは預託機関がユーザの署名検証鍵の証明書を発行する事から、単純にはその証明書に公開情報を埋め込む方法が考えられるが、実際は証明書発行手続きがフェアブラインド署名を用いた特殊な形態であるため容易には埋め込む事が出来ない。ブラインド署名に対して公開情報を埋め込む方法は、部分ブラインド署名と呼ばれる技術があるが [1]、フェアブラインド署名に対して同様の埋め込みを行う、安全性が保障された「部分フェアブラインド署名」方式は知られていないようである。

参考文献

[1] M. Abe and E. Fujisaki, “How to date blind signatures,” ASIACRYPT ’96, LNCS 1163, pp. 244–251, Springer-Verlag, 1996.

[2] M. Abe and M. Ohkubo, “Provably secure fair blind signatures with tight revocation,” ASIACRYPT ’01, LNCS 2248, pp. 583–601, Springer-Verlag, 2001.

[3] J. Camenisch and A. Lysyanskaya, “An efficient system for non-transferable anonymous credentials with optional anonymity revocation,” EUROCRYPT ’01, LNCS 2045, pp. 93–118, Springer-Verlag, 2001.

[4] J. Camenisch, J.-M. Piveteau, and M. Stadler, “Fair blind signatures,” EUROCRYPT ’95, LNCS 921, pp. 209–219, Springer-Verlag, 1995.

[5] D. Chaum and E. V. Heyst, “Group signatures,” EUROCRYPT ’91, LNCS 547, pp. 257–265, Springer-Verlag, 1991.

[6] 千田浩司, 小宮輝之, 林徹, “匿名性確保と不正者追跡の両立が可能な通信方式” 情報処理学会論文誌, Vol.45 No.8, pp. 1873–1880, 2004 年 8 月.

[7] I. Damgård and M. Koprowski, “Practical threshold RSA signatures without a trusted dealer,” EUROCRYPT ’01, LNCS 2045, pp. 152–165, Springer-Verlag, 2001.

[8] Y. Desmedt and Y. Frankel, “Threshold cryptosystems,” CRYPTO ’89, LNCS 435, pp. 307–315, Springer-Verlag, 1990.

[9] J. Kilian and E. Petrank, “Identity escrow,” CRYPTO ’98, LNCS 1642, pp. 169–185, Springer-Verlag, 1998.

[10] K. Ohta and T. Okamoto, “Multi-signature schemes secure against active insider attacks,” IEICE Trans. Vol. E-82-A, No. 1, pp. 22–31, 1999.