九州大学学術情報リポジトリ
Kyushu University Institutional Repository

プライバシ保護技術の評価のための権限認証モデル

中村, 徹
九州大学大学院システム情報科学府/研究院

稲永, 俊介
九州大学大学院システム情報科学府/研究院

馬場, 謙介
九州大学大学院システム情報科学府/研究院

池田, 大輔
九州大学大学院システム情報科学府/研究院

他

https://hdl.handle.net/2324/9186

出版情報：Computer Security Symposium. 2007, pp.405-410, 2007-11-01
バージョン：
権利関係：

プライバシ保護技術の評価のための権限認証モデル

中村　徹　　稲永　俊介　　馬場　謙介　　池田　大輔　　安浦　寛人

九州大学大学院システム情報科学 [府／研究院]
{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp　{baba, daisuke}@i.kyushu-u.ac.jp

概要　近年数多くのプライバシを考慮した権限認証方式が提案されているが，プライバシ保護に関する性質は形式的な定義が存在しないため，各方式の比較が困難である．各権限認証システムに対して最適な権限認証方式を選定するためには、権限認証方式をプライバシ保護の観点から包括的に評価することのできる枠組みを用意する必要がある．本稿では、プライバシ保護を考慮した形式的な権限認証モデルを提案する．提案モデルを用いてプライバシ保護に関する性質（顕名性，匿名性，仮名性，リンク不能性）を定義し，種々の実システムが有するプライバシ保護に関する性質を評価する．

An Authorization Model with Privacy Protection

Toru Nakamura　Shunsuke Inenaga　Kensuke Baba　Daisuke Ikeda　Hiroto Yasuura

Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan
{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp　{baba,daisuke}@i.kyushu-u.ac.jp

Abstract　It has been difficult to compare a lot of authorization methods recently proposed in the view point of privacy protection, since there is no formal definition of privacy protection. In order to select the optimal authorization method for each system, a general framework, which enables us a comprehensive verification of authorization methods in terms of privacy protection, is needed. In this paper we propose an authorization model designed in consideration for privacy protection. The proposed model enables us to give formal definitions of “identifiability”, “anonymity”, “pseudonymity”, and “unlinkability” that relate with privacy protection. Using the model, we show that real world system realizes which privacy protection aspects above.

1　はじめに

情報社会において，権限認証は必要不可欠な技術である．近年では，権限認証システムに対してプライバシ保護の性質が期待されることも多い．権限認証を行う際には，必ずしも個人を識別する必要はなく，認証を要求する主体の権限のみを認証できればよい場合がある．例えば，所属によって権限が異なるドアの入退室管理などのアプリケーションでは，主体の所属のみを示すことで主体の識別情報を秘匿することが出来る．個人の識別を行わない権限認証は，プライバシ保護の観点において優れている．プライバシ保護を考慮した認証技術については数多くの既存研究が存在する．しかしながら，プライバシ保護に関する性質の形式的な定義は存在せず，各認証方式の比較は困難であった．本研究では，マルチサービス環境を想定し，かつ認証方式に関わらず包括的にプライバシ保護に関する性質を評価する形式的な認証モデルの構築を目指している．本稿では特に，権限認証における検証者に対する仮名性とリンク不能性に注目

し，形式手法を用いた厳密な定義を行う．

Pfitzmann らは文献 [1] において，プライバシに関する性質の命名法を提案し，匿名性，リンク不能性，観察不能性，仮名性を定義した．仮名は，主体の識別子の代わりに用いられる．本稿では，識別子は主体を特定するために充分な情報を表す．仮名を用いることにより，識別子と仮名の対応を知らない主体に対して，識別子を秘匿することが出来る．しかしながら，仮名を元に情報を収集し主体に意識されることなく趣味嗜好を分析可能である点や，万一識別子と仮名が紐付けられた場合に，収集された情報全てが個人と結びつく危険性があることが指摘されている．リンク不能性とは認証を要求する主体と，認証の履歴を紐付けることが出来ない性質である．リンク不能性を持つ認証技術を用いた場合，仮名の問題点を克服することが可能である．リンク不能性を実現する手法として，グループ署名 [2] を用いる方法などが知られている．一方で，プライバシ保護はしばしば不正防止と相反する概念として扱われる．不正行為を抑制するために，匿名性を剥奪し主体の追跡を可能にする仕組みが考案されている．このような性質を追跡性と呼ぶ．ID エスクロー [3] は，追跡性の概念を取り入れ，プライバシ保護と不正防止のバランスが考慮された認証技術の一つである．

本稿ではまず，形式的な権限認証モデルを導入し，議論の核となるプライバシ保護に関する性質を定義する．さらにいくつかの認証システムについて，定義した性質を用いてプライバシ保護の観点から評価を行う．

2　権限認証モデル

本章では，プライバシ保護を考慮した権限認証モデルを提案する．

2.1　権限認証の定義

本稿で提案する認証モデルは大きくは以下の集合からなる．

- エンティティ集合 E
- 知識集合 Z

本節では権限を所持していることを証明する証明者と，それを検証する検証者に関する権限認証について定義を行う．

まず知識についての関数について，いくつか定義を行う．

定義 1 (知識関数) 知識関数 $k : E \times I \to \{\mathtt{true}, \mathtt{false}\}$ は以下の関数である．

$$k(x,z) = \begin{cases} \mathtt{true} & x \text{ が } z \text{ を知っているとき,} \\ \mathtt{false} & x \text{ が } z \text{ を知らないとき.} \end{cases}$$

定義 2 (信用関数) 信用関数 $b : E \times E \times I \to \{\mathtt{true}, \mathtt{false}\}$ は以下の関数である．

$$b(x,y,z) = \begin{cases} \mathtt{true} & x \text{ が } k(y,z) = \mathtt{true} \text{ と} \\ & \text{信じられるとき,} \\ \mathtt{false} & \text{それ以外のとき.} \end{cases}$$

定義 3 (知識伝達関数) 任意の $x, y \in E$ と $z \in I$ に対して，**知識伝達関数** $t(x,y,z)$ は，$k(x,z) = \mathtt{true}$ のとき $k(y,z) = \mathtt{true}$ かつ $b(y,x,z) = \mathtt{true}$ とする手続きを表す関数である．

ある証明者 $u \in U \subset E$ がある検証者 $s \in S \subset E$ に対する証明情報 $c \in C \subset Z$ を知っている，すなわち $k(u,c) = \mathtt{true}$ とする．検証者は証明情報 c を検証するための検証情報 $v \in V \subset Z$ を知っている，すなわち $k(s,v) = \mathtt{true}$ とする．$c \in C$ と $v \in V$ が対応関係にあることを，$c \approx v$ と表す．u は c を s に伝達する，すなわち $t(u,s,c)$ より権限認証を行う．

定義 4 (権限認証関数) 権限認証関数 $Auth : S \times U \times C \to \{\mathtt{true}, \mathtt{false}\}$ は以下の関数である．

$$Auth(s,u,c) = \begin{cases} \mathtt{true} & b(s,u,c) = \mathtt{true} \text{ かつ,} \\ & \exists v \text{ に対して} \\ & k(s,v) = \mathtt{true} \text{ かつ} \\ & c \approx v \text{ のとき,} \\ \mathtt{false} & \text{それ以外のとき.} \end{cases}$$

但し，権限認証関数を用いる際には，初期状態は $\forall c_i \in C$ について $b(s,u,c_i) = false$ であるとする．これは権限認証を行う前に，検証者が証明者について何も信じていない状態を表す．

2.2 識別子と仮名の定義

各証明者 $u_i \in U \subset E$ は**証明者 ID** と呼ばれる識別子を持つと仮定し，$D \subset Z$ を証明者 ID 集合とする．証明者 ID 変換関数 $e : U \to D$ は単射である．任意の $u_i \in U$ に対して $e(u_i) = d_i \in D$ とする．直感的には d_i は u_i に対して一意であるから，証明者 ID を用いることで証明者を一意に特定することが出来る．

各検証者 $s_j \in S \subset E$ は**検証者 ID** と呼ばれる識別子を持つと仮定し，$L \subset Z$ を検証者 ID 集合とする．検証者 ID 変換関数 $n : S \to L$ は単射である．

ある検証者 s_j に対して，各証明者が**仮名**を持つ場合がある．このとき，$P \subset Z$ を仮名集合とする．仮名関数 $g : D \times L \to P$ は単射であり，任意の $d_i \in D$ に対して $g(d_i, \ell_j) = p_{i,j} \in P$ とする．

本稿では以下，各証明者は証明者 ID または仮名に対応する証明情報を持つと仮定し，証明情報関数を $q : D \cup P \to C$ とする．また，q^{-1} を q の逆関数とする．

一方，各検証者は各証明者の証明情報に対応する検証情報を持つと仮定し，検証情報関数を $w : D \cup P \to V$ とする．

2.3 プライバシ保護に関する性質

本節では，検証者が定義 4 の権限認証関数を用いて証明者を認証する際の，証明者のプライバシ保護に関する用語を定義する．以下本章では，ある検証者 $s_j \in S$ と証明者 $u_i \in U$ に対して，$Auth(s_j, u_i, c) = \texttt{true}$ と仮定する．以下，$d_i = e(u_i)$，$\ell_j = n(s_j)$，$p_{i,j} = g(d_i, \ell_j)$ であることに留意する．

定義 5 (顕名性) $b(s_j, u_i, d_i) = \texttt{true}$ かつ $k(s_j, d_i) = \texttt{true}$ のとき u_i は s_j に対して**顕名性**を持つという．

u_i が s_j に対して顕名性を持つとき，s_j は u_i を**識別**できるという．

定義 6 (匿名性) $b(s_j, u_i, d_i) = \texttt{false}$ のとき，u_i は s_j に対して**匿名性**を持つという．

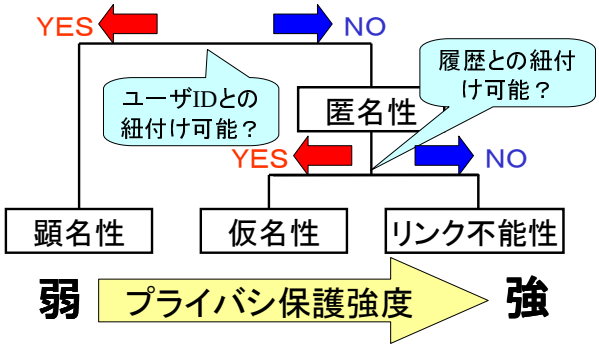

図 1: 顕名性，匿名性，仮名性，リンク不能性の関係．

d_i は u_i を特定可能な情報を含むため，証明者が検証者に対して顕名性を持つ場合，個人と行動履歴が紐付けられ，プライバシ侵害に繋がる可能性がある．したがって，匿名性を満たす権限認証の実現がプライバシ保護の観点から極めて重要である．匿名性はさらに，仮名性とリンク不能性に細分化される（図 1 参照）．

定義 7 (仮名性) $b(s_j, u_i, d_i) = \texttt{false}$，$k(s_j, p_{i,j}) = \texttt{true}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{true}$ のとき，u_i は s_j に対して**仮名性**を持つという．

定義 8 (リンク不能性) $b(s_j, u_i, d_i) = \texttt{false}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{false}$ のとき，u_i は s_j に対して**リンク不能性**を持つという．

証明者 u_i が検証者 s_j に対して仮名性を持つ場合，$b(s_j, u_i, d_i) = \texttt{false}$ であるため，s_j は仮名 $p_{i,j}$ から証明者を識別することはできない．一方，証明者 u_i が検証者 s_j に対してリンク不能性を持つ場合，s_j は u_i を識別できないだけでなく，u_i と履歴を紐付けることもできないため，リンク不能性はより強いプライバシ保護の性質であるといえる．

プライバシ保護技術は，不正防止と相反する技術となる恐れがある．そのため，通常時には証明者 ID を秘匿していても，不正検出時には証明者 ID を追跡できる仕組みが必要な場合も考えられる．

定義 9 (追跡性) ある $x \in E-U$ と $u \in U$ について，$k(x, d = e(u)) = \texttt{true}$ かつ $b(x, u, d) = \texttt{true}$ のとき，x は u 対して**追跡性**を持つ.

証明者の追跡を行うエンティティは，必ずしも検証者である必要はなく，第三者が追跡を行う場合もある．本稿では第三者として管理者のみを仮定しているが，管理者と追跡者を分離する技術も知られている [3].

3 提案モデルによる権限認証システムの評価

本章では，2 章で提案した権限認証モデルを用いて，種々の権限認証システムが満たすプライバシ保護の性質を明らかにする.

前提として，すべての権限認証システムにおいて，初期状態では $\forall s_j \in S$ と $\forall z \in D \cup P \cup C \cup V$ に対して $k(s_j, z) = \texttt{false}$ と仮定する.

3.1 アカウント名とパスワードを用いる権限認証システム

以下に，アカウント名とパスワードを用いる権限認証システムの一例を挙げる.

準備

1. ある証明者 u_i がある検証者 s_j に個人情報を提出する.
2. s_j は u_i の個人情報と紐付いたアカウント名 $AN_{i,j}$ とパスワード $PW_{i,j}$ を生成する.
3. s_j は u_i に $AN_{i,j}$ と $PW_{i,j}$ を提出する.

認証プロトコル

1. 証明者 u_i が検証者 s_j に $AN_{i,j}$ を提出する.
2. u_i は s_j に $PW_{i,j}$ を提出する.
3. 提出された $PW_{i,j}$ と一致する登録済みのパスワードが存在するとき，s_j は u_i を権限認証し，そのようなパスワードが存在しないときには s_j は u_i を権限認証しない.

提案モデルを用いた記述.

準備 $\exists i, \exists j$ について，

1. $t(u_i, s_j, d_i)$.
2. $k(s_j, p_{i,j} = g(d_i, \ell_j)) = \texttt{true}$ かつ $\mathrm{y}k(s_j, c_{i,j} = q(p_{i,j})) = \texttt{true}$. ただし，$k(s_j, p_{i,j}) = \texttt{true}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{true}$ は $k(s_j, d_i) = \texttt{true}$ かつ $b(s_j, u_i, d_i) = \texttt{true}$ を意味する.
3. $t(s_j, u_i, p_{i,j})$ かつ $t(s_j, u_i, c_{i,j})$.

権限認証関数 $Auth(s_j, u_i, c_{i,j})$:

1. $t(u_i, s_j, p_{i,j})$.
2. $t(u_i, s_j, c_{i,j})$.
3. **if** $\exists v$ s.t. $k(s_j, v) = \texttt{true}$ and $c_{i,j} \approx v$ **then** return `true`.
   else return `false`.

定理 1 アカウント名とパスワードを用いる権限認証システムでは，証明者は検証者に対して顕名性を持つ.

証明 権限認証関数の 1 行目より，$k(s_j, p_{i,j}) = \texttt{true}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{true}$. 準備 2 より，$k(s_j, d_i) = \texttt{true}$ かつ $b(s_j, u_i, d_i) = \texttt{true}$. 定義 5 より，定理は示された. □

定理 2 *ID* とパスワードを用いる権限認証システムでは，検証者は証明者に対して追跡性を持つ.

証明 定理 1 と同様. □

3.2 PID システム [4]

PID とは，仮名の一種である．PID システムは，証明者の権限認証の際に第三者に対して PID を秘匿することによって，PID そのものを証明情報として用いる権限認証システムである.

準備

1. ある証明者 u_i が管理者 m に自らの個人情報を提出する．
2. m は，u_i の個人情報と紐付いた，各検証者 s_j に対応する PID $PID_{i,j}$ を生成する．
3. m は u_i に，各 $s_j \in S$ に対応する $PID_{i,j}$ を提出する．
4. m は s_j に，各 $u_i \in U$ に対応する $PID_{i,j}$ を提出する．

認証プロトコル

1. 証明者 u_i が検証者に s_j に $PID_{i,j}$ を提出する．
2. 提出された $PID_{i,j}$ と一致する登録済みの PID が存在するとき，s_j は u_i を権限認証し，そのような PID が存在しないとき s_j は u_i を権限認証しない．

提案モデルを用いた記述．

準備

1. $\exists i$ について，$t(u_i, m, d_i)$.
2. $\forall j$ について，$k(m, p_{i,j} = g(d_i, \ell_j)) = \texttt{true}$. ただし，$k(m, p_{i,j}) = \texttt{true}$ かつ $b(m, u_i, p_{i,j}) = \texttt{true}$ は $k(m, d_i) = \texttt{true}$ かつ $b(m, u_i, d_i) = \texttt{true}$ を意味する．
3. $\forall j$ について，$t(m, u_i, p_{i,j})$.
4. $\forall j$ について，$t(m, s_j, p_{i,j})$.

権限認証関数 $Auth(s_j, u_i, p_{i,j})$:

1. $t(u_i, s_j, p_{i,j})$.
2. **if** $\exists p$ s.t. $k(s_j, p) = \texttt{true}$ and $p_{i,j} \approx p$ **then** return `true`.
   else return `false`.

定理 3 *PID* システムでは，証明者は検証者に対して仮名性を持つ．

証明 権限認証関数の 1 行目より，$k(s_j, p_{i,j}) = \texttt{true}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{true}$．初期条件より，$k(s_j, d_i) = \texttt{false}$．定義 7 より，定理は示された． □

定理 4 *PID* システムでは，管理者は証明者に対して追跡性を持つ．

証明 権限認証関数の 1 行目より，$k(s_j, p_{i,j}) = \texttt{true}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{true}$．ここで，$t(s_j, m, p_{i,j})$ とすると，初期条件より，$k(m, p_{i,j}) = \texttt{true}$ かつ $b(m, u_i, p_{i,j}) = \texttt{true}$ を得る．準備 2 より，$k(m, d_i) = \texttt{true}$ かつ $b(m, u_i, d_i) = \texttt{true}$．定義 9 より，定理は示された． □

3.3 グループ署名を用いる権限認証システム

ここでは，グループ署名 [2] を用いる権限認証システムを取り扱う．グループ署名とはディジタル署名の一種である．検証者はグループ公開鍵を用いることによりグループ署名から署名者がグループに所属することは検証できるが，署名者を特定することは出来ない．またグループ秘密鍵を持つ特権者のみグループ署名から署名者を追跡することが出来る．

準備

1. ある証明者 u_i が管理者 m に個人情報を提出する．
2. m は，u_i の個人情報と紐付けされた各検証者 s_j に対応するグループ証明書 $Cert_{i,j}$ を生成する．
3. m は u_i に $Cert_{i,j}$ を提出する．
4. m は s_j にグループ公開鍵 P_{G_j} を提出する．

認証プロトコル

1. 証明者 u_i が検証者 s_j にグループ署名 $Sign(Cert_{i,j})$ を提出する．
2. s_j は提出された $Sign(Cert_{i,j})$ をグループ公開鍵 P_{G_j} を用いて検証し，権限認証する．

提案モデルを用いた記述．

準備

1. $\exists i$ について，$t(u_i, m, d_i)$.
2. $\forall j$ について，$k(m, p_{i,j} = g(d_i, \ell_j)) = \texttt{true}$. ただし，$k(m, p_{i,j}) = \texttt{true}$ かつ $b(m, u_i, p_{i,j}) = \texttt{true}$ は $k(m, d_i) = \texttt{true}$ かつ $b(m, u_i, d_i) = \texttt{true}$ を意味する．また，$k(m, c_{i,j}) = \texttt{true}$ は $k(m, p_{i,j}) = \texttt{true}$ を意味する．
3. $\forall j$ について，$t(m, u_i, p_{i,j})$.
4. $\forall j$ について，$t(m, s_j, v_j = w(p_{i,j}))$.

権限認証関数 $Auth(s_j, u_i, q(p_{i,j}))$:

1. $t(u_i, s_j, c_{i,j} = q(p_{i,j}))$.
2. **if** $c_{i,j} \approx v_j$ **then** return `true`.
   else return `false`.

定理 5 グループ署名を用いる権限認証システムでは，証明者は検証者に対してリンク不能性を持つ．

証明 権限認証関数より，明らかに $b(s_j, u_i, d_i) = \texttt{false}$ かつ $b(s_j, u_i, p_{i,j}) = \texttt{false}$．定義 8 より，定理は示された． □

定理 6 グループ署名を用いる権限認証システムでは，管理者は証明者に対して追跡性を持つ．

証明 権限認証関数の 1 行目より，$k(s_j, c_{i,j}) = \texttt{true}$ かつ $b(s_j, u_i, c_{i,j}) = \texttt{true}$．ここで，$yt(s_j, m, c_{i,j})$ とすると，準備 2 と $k(m, c_{i,j}) = \texttt{true}$ より，$k(m, p_{i,j} = q^{-1}(c_{i,j})) = \texttt{true}$ かつ $b(m, u_i, p_{i,j}) = \texttt{true}$ を得る．準備 2 より，$k(m, d_i) = \texttt{true}$ かつ $b(m, u_i, d_i) = \texttt{true}$．定義 9 より，定理は示された． □

4 終わりに

本稿では，プライバシ保護を考慮した形式的な権限認証モデルを提案した．次に，提案モデルを用いてプライバシ保護に関する性質の定義を行った．さらに，提案モデルを用いていくつかの認証システムについて評価を行った．本稿では記載することが出来なかったが，追跡性を持たない権限認証方式も含め，より多くの方式について考察する予定である．今後の課題として，マルチサービス環境でのサービス間の連携などで生じる問題点の考察と，時間の概念の導入を考えている．

謝辞

本研究は平成 19 年度〜平成 21 年度, 基盤研究 A, 課題番号 19200004 「価値と信用を搭載するディペンダブルな LSI の設計手法の研究」によるものである．

参考文献

[1] A. Pfitzmann and M. Köhntopp, “Anonymity, unobservability and pseudonymity - a proposal for terminology”, Proc. Workshop on Design Issues in Anonymity and Observability, LNCS 2009, Springer-Verlag, pp.1–9, 2000.

[2] D. Chaum and E. van Heyst, “Group Signatures”, Proc. Eurocrypt’91, LNCS 547, Springer-Verlag, pp.257–270, 1991.

[3] J. Kilian and E. Petrank, “Identity Escrow”, Proc. Crypto ’98, LNCS 1462, Springer-Verlag, pp.169–185, 1998.

[4] Y. Nohara, S. Inoue, and H. Yasuura. “Toward unlinkable ID management for multi-service environments”, Proc. PerCom’05 Workshops, IEEE Press, pp.115–119, 2005.