九州大学全学共通ICカードにおける新しい個人識別のしくみ

馬場, 謙介
九州大学大学院システム情報科学研究院

出版情報：SLRC プレゼンテーション, 2006-09-05. 九州大学システムLSI研究センター
バージョン：
権利関係：

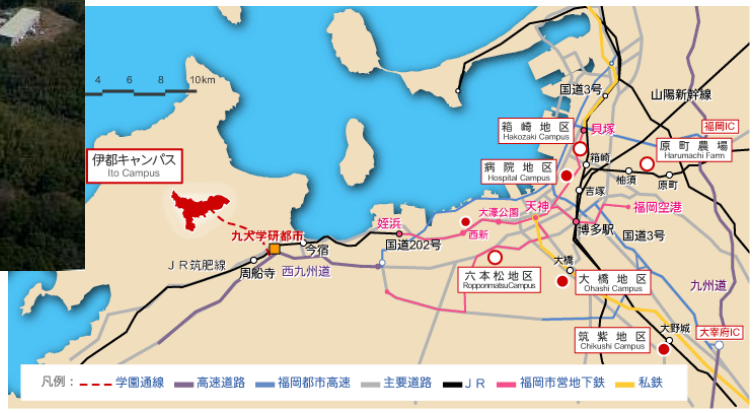
九州大学全学共通ICカードにおける新しい個人識別のしくみ

馬場謙介
九州大学大学院システム情報科学研究院
baba@i.kyushu-u.ac.jp

九州大学新キャンパス

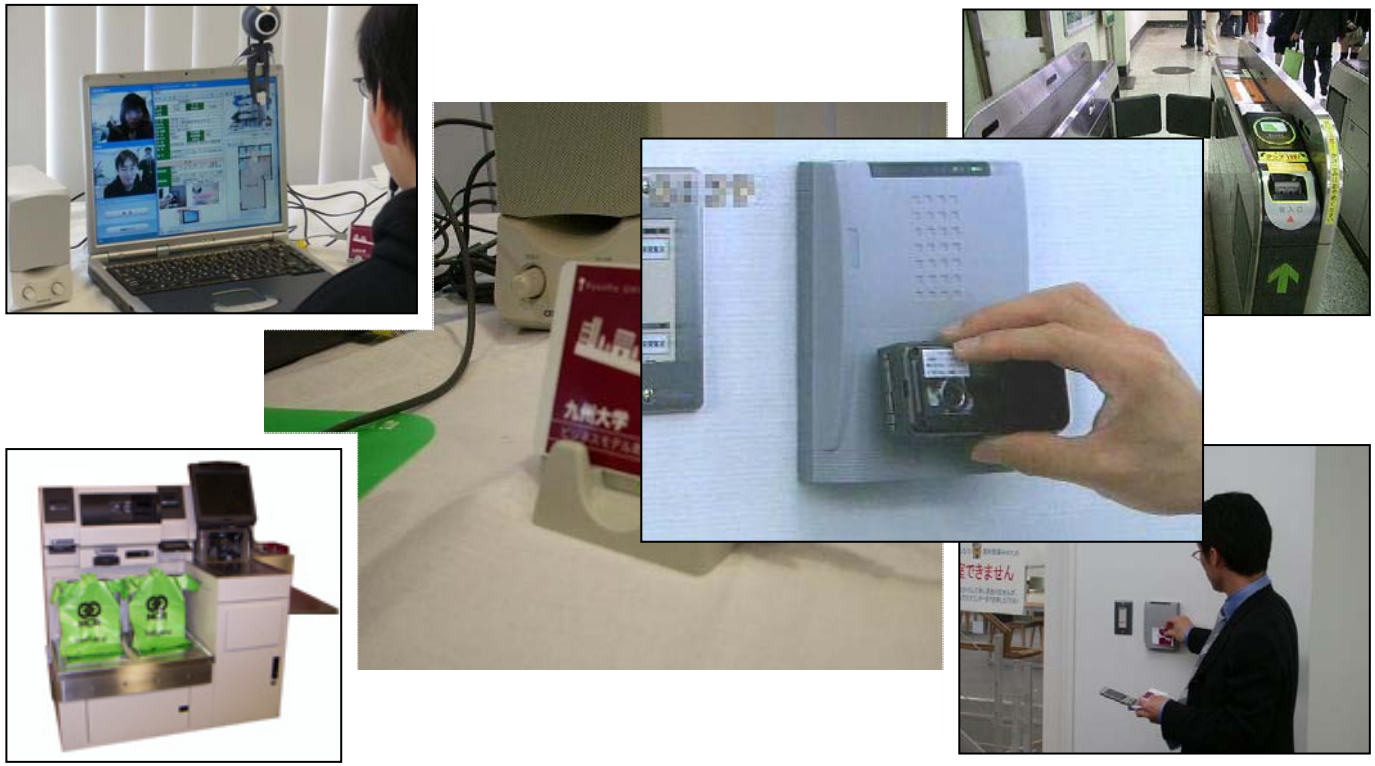
新たな挑戦と試行の実験都市

福岡市西区元岡



全学共通ICカードシステム

QUPID: KYU(Q)shu University Personal IDentification



電子的識別システムへの要求

- サービスを受ける者（ユーザ）の視点から
  - 様々なサービスを受けたいが，カードを何枚も持つのは煩わしい
  - 「なりすまし」による不正な使用は防ぎたい
  - 個人情報はもちろん，使用履歴もなるべく他人に知られたくない
  - ある程度融通の利くサービスの受け方をしたい
- サービスを提供する者の視点から
  - ユーザの囲い込みをしたい
  - ユーザの行動履歴は欲しいが，個人情報は保持したくない
  - 既存のシステムにできるだけ手を加えたくない

もちろん，まだまだあるはずだが．．．

「アイデンティティ・マネジメント」

少なくとも2つの観点での重要性

- 安全性
  - 権限にそってサービスが提供される（なりすましを防ぐ）
  - 個人情報が保護される
  - 履歴の追跡によるプライバシの侵害が防がれる
- 利便性
  - 管理コストの削減
  - 複雑で柔軟な権限管理の実現

QUPIDの特徴

- 基本概念
  - PID (Personal IDentification)
    ユーザのプライバシを守る安全な個人識別
  - MIID (Media Independent IDentification)
    メディアに依存しない便利な個人識別
- 特徴
  - 携帯デバイスの種類や通信の規格といったメディアへの依存性がない
  - 利用者間の委譲等の柔軟な権利・権限の管理が可能である
  - 相互認証および履歴情報保護の観点での安全性を考慮している

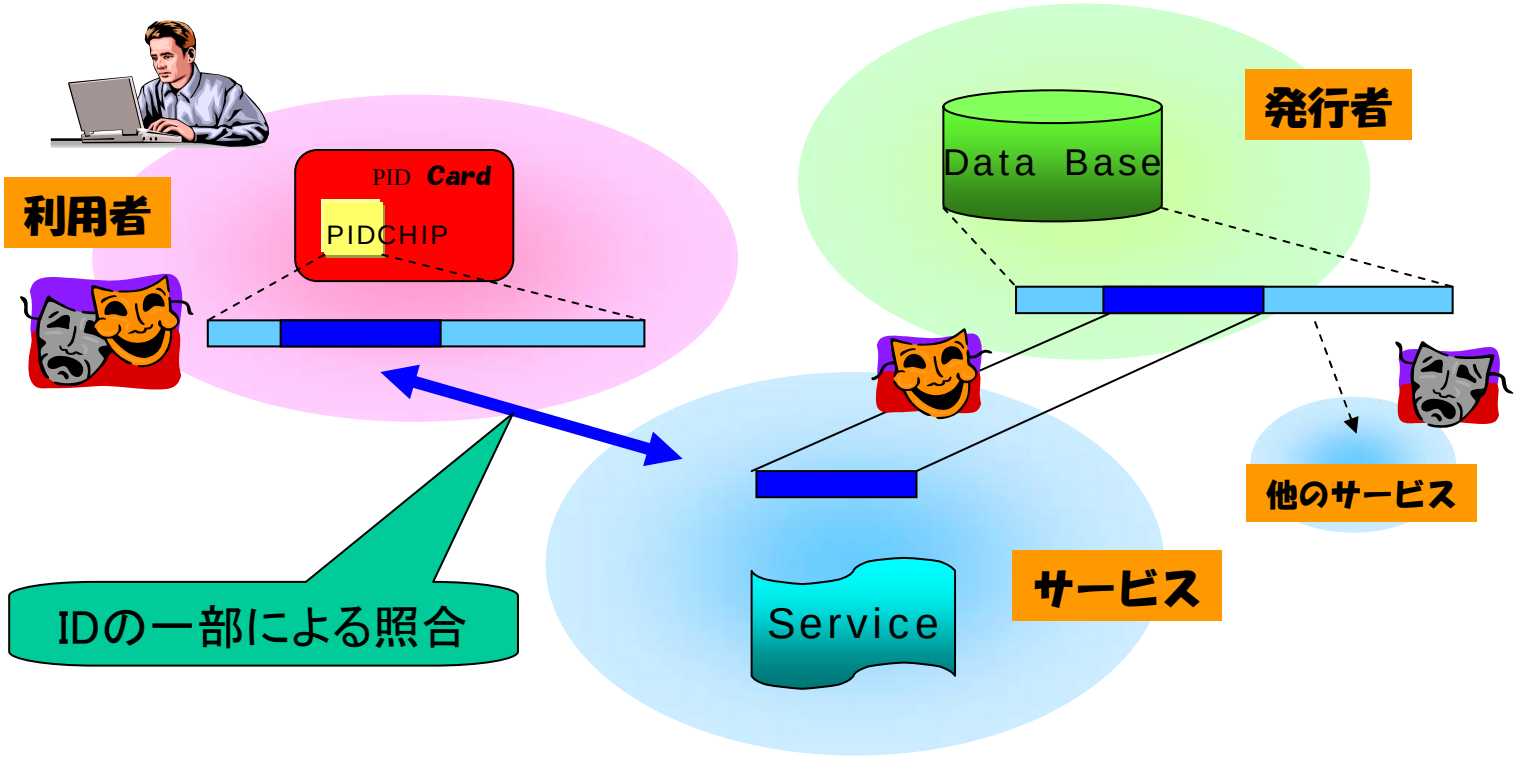
複数サービス用カードの問題点

複数サービス用カードには，なりすましとは別の脅威が存在

- 誰かは分からなくても，どういうサービスを受けたかが分かってしまう
- 人によっては，いくらコストをかけてでも守りたい「安全性」に対する脅威

PIDのアイデア

サービス毎に異なる識別子（ID）を用いることで解決

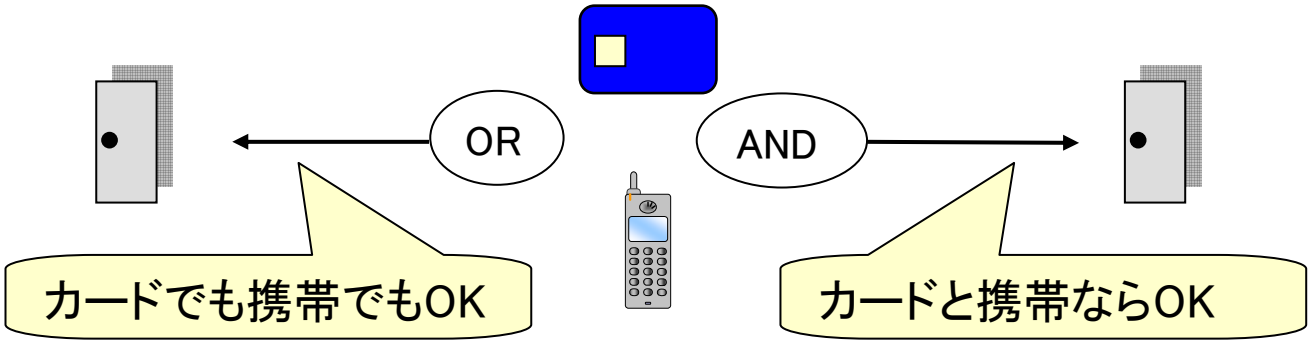


MIIDのアイデア

現実問題として，ICカードには複数の規格がある

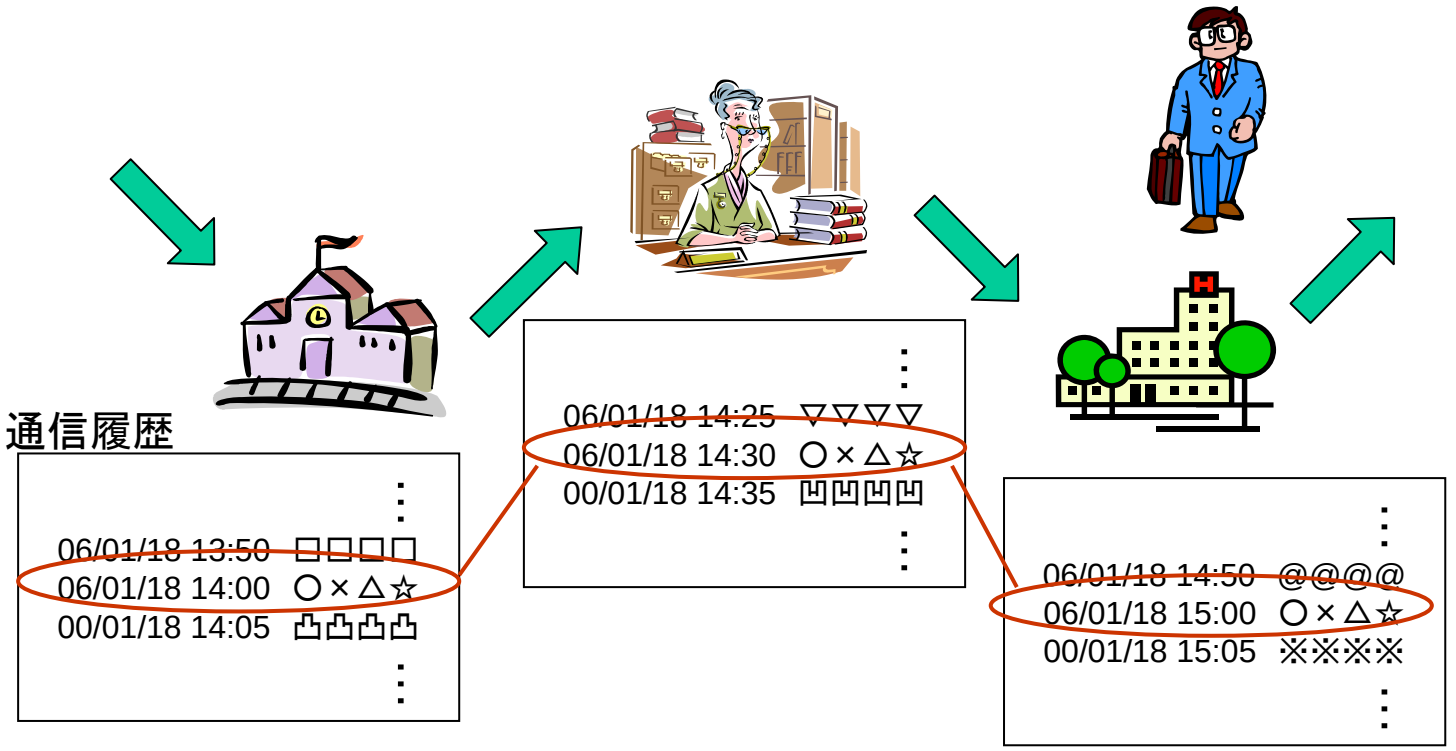
IDはデバイスではなくユーザに付与されるべきだ

- メディアに依存しないならばユーザもサービス提供者も便利
- 複数のメディアを使い分けることで，より高度な認証が可能
- デバイスの識別をしない認証ができるはずだ



プライバシへのさらなる脅威

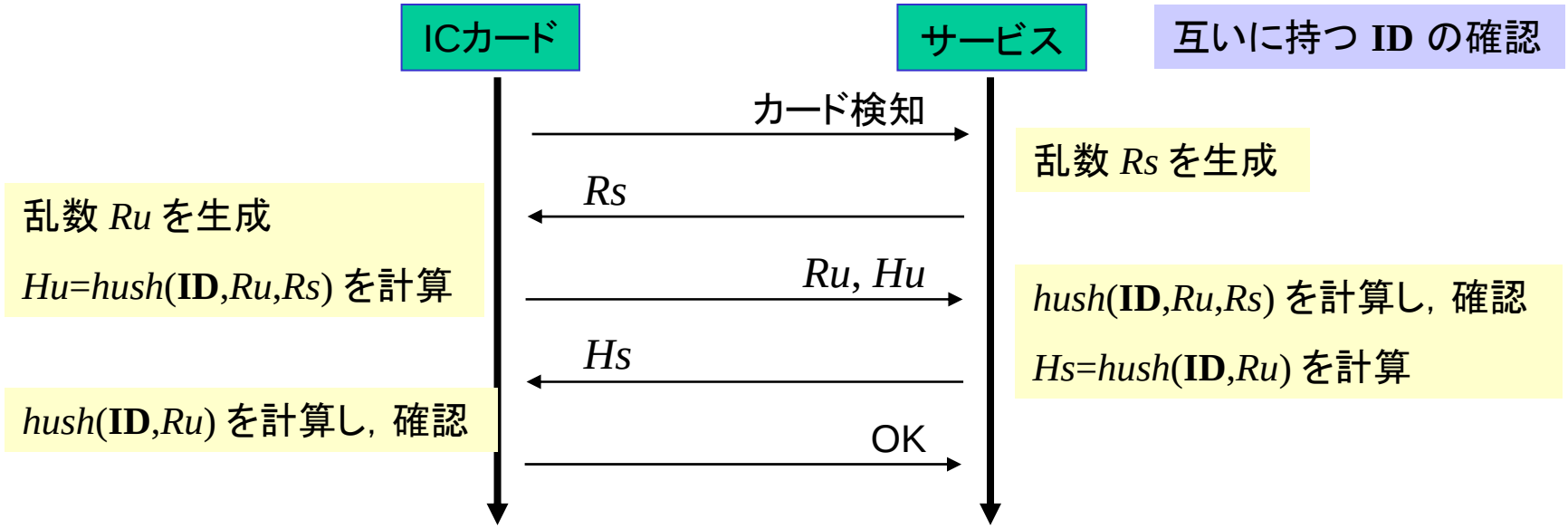
サービス提供者でなくても履歴の紐付けができてしまう



QUPIDを支える技術（1.1）

リンクを防ぐ認証プロトコル [Nohara *et al.* 04]

乱数を用いたハッシュ化で出力を常に変化させればいい

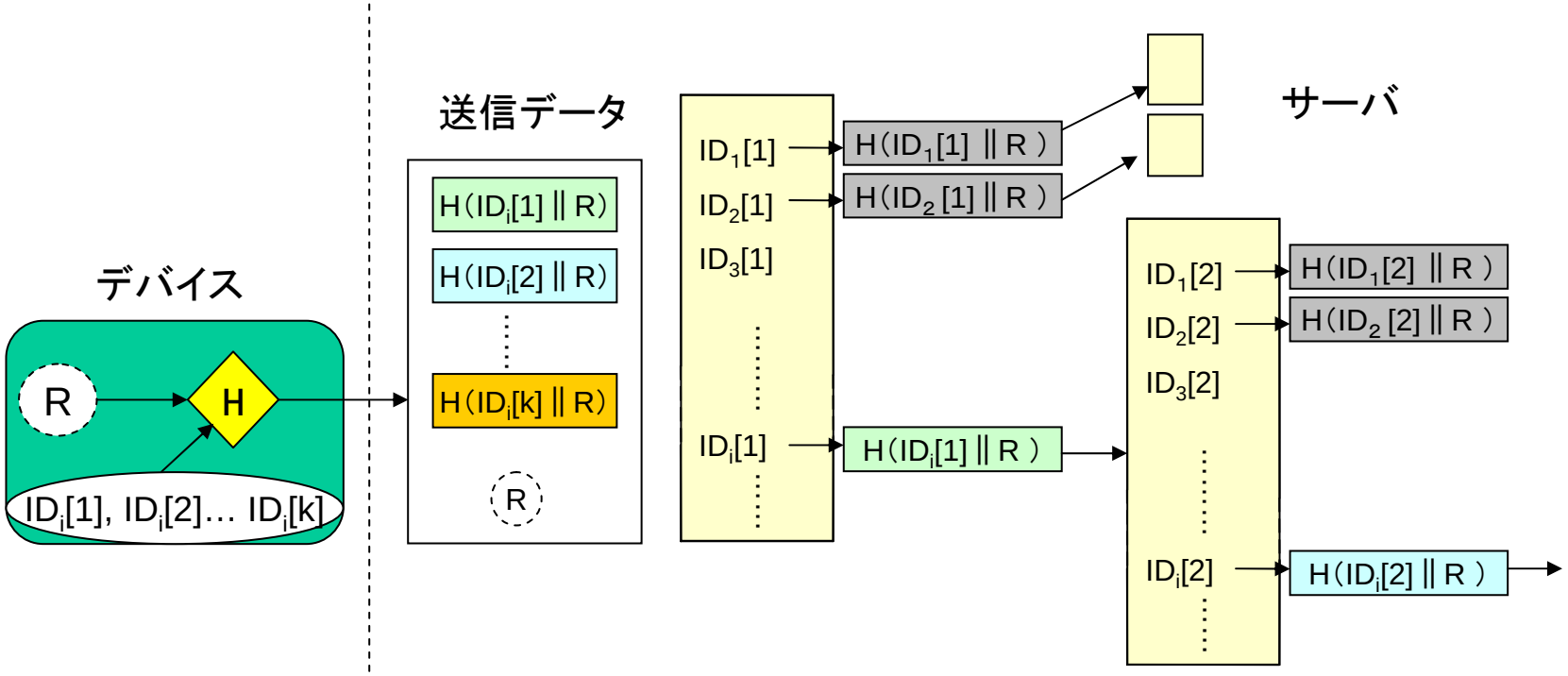


N 人のユーザに対し，最悪で N 回ハッシュ計算が必要

QUPIDを支える技術（1.2）

ID照合の高速化 [Nohara *et al.* 05]

木構造を使えば $O(\log N)$ 時間で照合できる



柔軟な権限管理の要求

認証で与えられる権限（サービス）を「鍵」と思うと．．．

物理鍵

メリット：
- 貸与・複製が可能

デメリット：
- 安易に複製が可能
- 履歴管理できない
- 紛失・盗難による不正使用
（個人限定利用できない）
- 物理的管理の煩雑さ

既存のソフトウェアキー

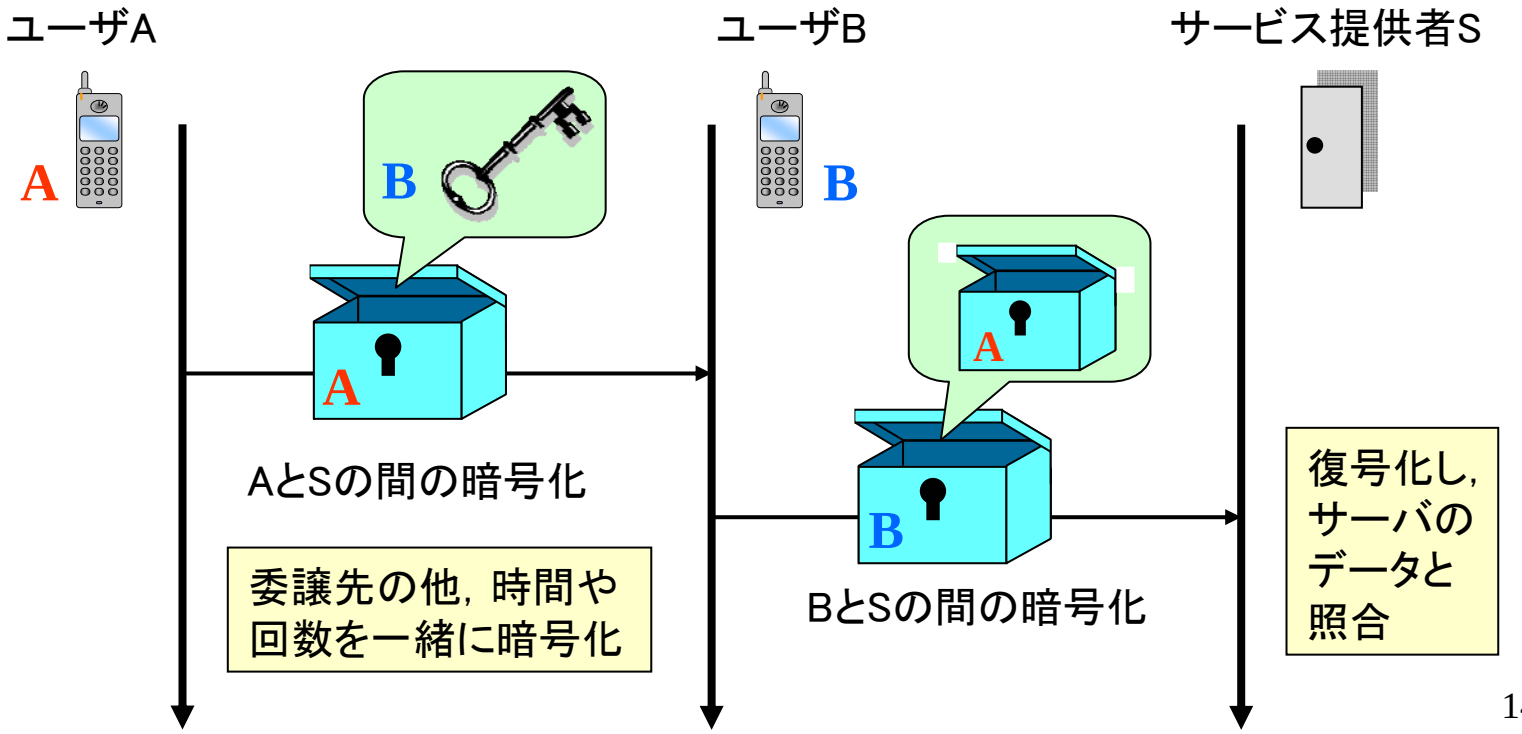
メリット：
- オンラインによる取得が可能
- センターサーバ上での履歴管理が可能

デメリット：
- 複製できなくしているものが多い
- 複製をしないと貸与ができない
- 特定個人限定利用できない

QUPIDを支える技術(2)

利用者間での権限の委譲 [Noutomi *et al.* 04]

暗号技術を利用すれば，権限管理の一部をユーザが行える



より現実的な安全性の検証

高度な暗号技術やバイオメトリクスは，安全なシステム構築の十分なソリューションだろうか？

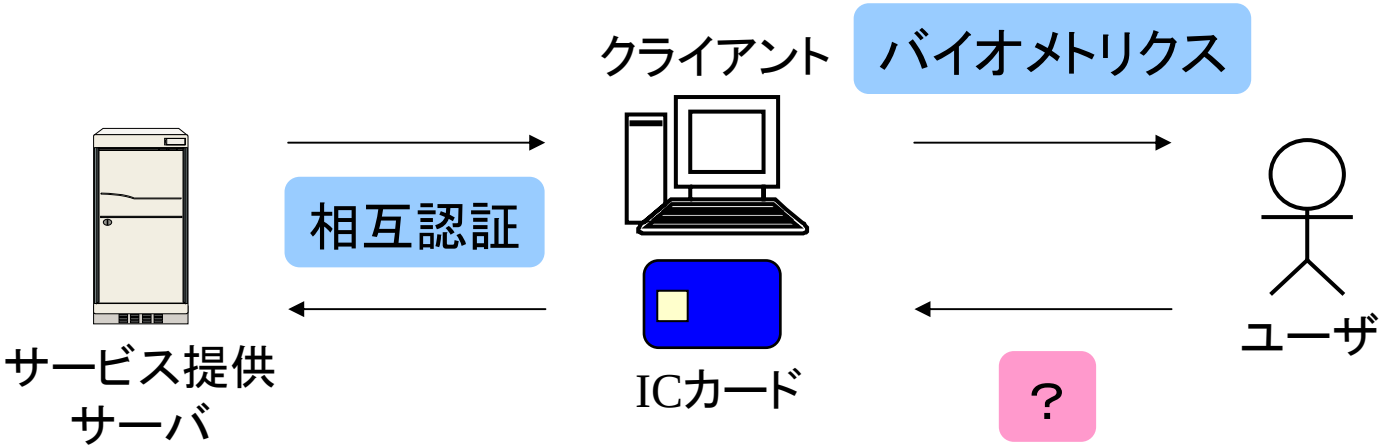
- 決して盗聴されない認証が，拾ったICカードによって行われる
- バイオメトリクスにより，詐欺にかかった人が確かにカードの持ち主だとわかる
- 「ガード番号を入力して下さい」と表示されたので入力した

誰が誰を認証するのかという観点で整理

QUPIDを支える技術(3)

ユーザによるサービスの認証 [Watanabe *et al*. 06]

カード・サーバ間の相互認証は，ユーザ・サーバ間の相互認証か？

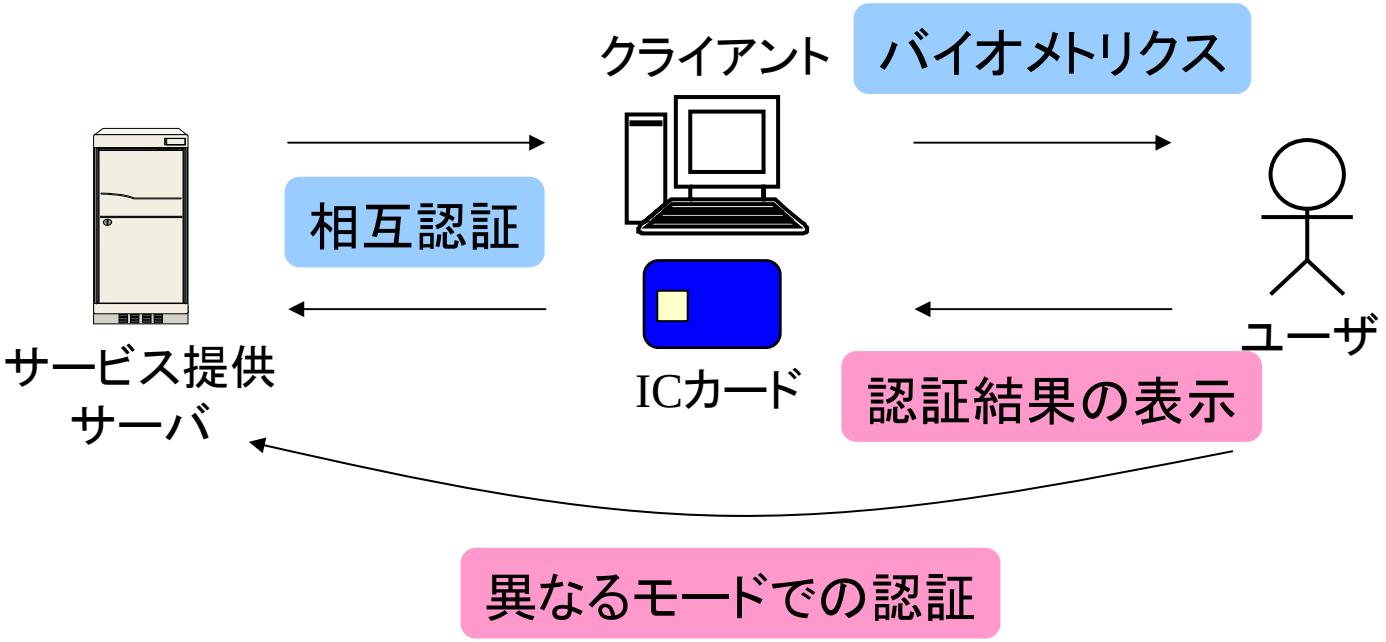


クライアントが信用できないとき，ユーザはサーバを確かめられない

QUPIDを支える技術(3)

QUPIDでのソリューション

- 携帯電話端末や電子ペーパーの利用
- マルチモーダルの利点



まとめ

QUPID：ICカードや携帯電話端末を使って，様々なサービスを受けられるしくみ

- 基本となる2つのコンセプト
  - PID（安全に）
  - MIID（便利に）
- 3つ技術の紹介
  - リンクを防ぐ認証プロトコル，その高速化
  - 貸し借り可能なソフトウェアキー
  - ユーザによるサービス提供者の認証方法の検討