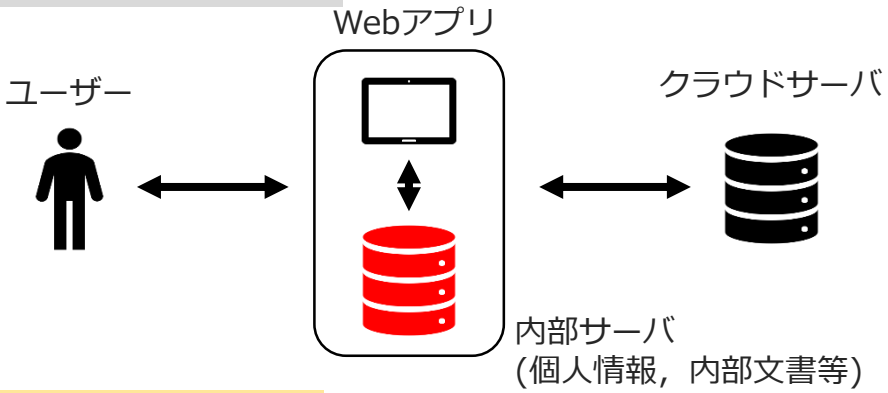
Private Digital Identity認証
~秘密計算によりクラウド化した認証アルゴリズム~

知能情報学部　講師　木原眞紀

研究の概要・特徴

従来の認証システムとPDI認証システムのちがい：

従来の認証システム



課題
- 内部サーバは高コスト
- 漏洩時のリスク
- 生体情報はネット利用しづらい

PDI認証

メリット
- **ワンタイムキー**で暗号化
- 独自の秘密計算で個人情報を**暗号化したまま照合**
- 生体情報が**ネット利用可能**

新規性・優位性

特許第 7165414号
US11,431,686 B2 (登録)　(東京理科大)
- PDI認証方式の基本特許
- 暗号化したまま認証するための情報処理プロセス
- クレジットカード，交通系ICカード，生体情報等任意の個人情報を利用可能

特許第 7384487号
US，CN，EP(審査中)　(東京理科大)
- PDI認証を用いたシングルサインオン
- 情報を分散保持，認証のクラウド化
- クレジットカード，交通系ICカード，生体情報等任意の個人情報を利用可能

実用化効果

応用分野/用途：認証のクラウド化
- Zoom会議やメタバースでの本人認証
- 個人情報を開示しない生体認証
- PDI認証ベースの応用システム
  - トレーサビリティ
  - ヘルスデータ管理

など

- 宿泊施設，レンタルスペース：フロントレス
- イベント：転売不可能なe-チケットシステム
- 住宅：スマホ不使用のスマートロック

など

【　論　文　】M. Kihara; S. Iriyama. Cryptography. 2019; 3(3):19.
M. Kihara; S. Iriyama. Cryptography. 2020; 4(2):16.
【キーワード】照合可能暗号，PDI認証，秘密計算

教員の連絡先：mkihara@konan-u.ac.jp