パスワードと乱数を組み合わせたユーザ認証方式の提案

150441161　渡邉 悠雅
渡邊研究室

1. はじめに

インターネットは我々の生活に欠かせないインフラの一つとなった．このような環境で，個人を認証する技術はきわめて重要である．ユーザパスワードを利用した認証はセキュリティが弱いため，生体認証などの要素を組み合わせた多要素認証システムとする場合が多いが，費用がかかるなど利便性が低下する課題がある．本稿ではユーザパスワードと，ユーザ端末で生成した乱数でハッシュ値を取り，従来のパスワードと同じ扱いでサーバに登録する認証方式を提案する．本提案は一種の多要素認証になるためセキュリティが高い．また，既存のパスワード認証と同様な使い勝手で利用可能である．

2. 提案方式

本提案はユーザ端末で乱数を生成し，端末にのみ保存しておく．サーバには乱数とパスワードのハッシュ値を登録する.乱数はサーバに分からない点が特徴である．

(1) アカウントの生成方法

ユーザ端末では十分に長い乱数 r を生成し，不揮発メモリ内に保存する．次に乱数 r とパスワードでハッシュ値を求め(以下ハッシュ rp とする)，この値をサーバに登録する．登録手順は様々な方法があるが例えば次のように行う．ユーザ端末からメールアドレス，ユーザ ID，ハッシュ rp をサーバに送信する．このハッシュ rp をサーバに登録するパスワードとして扱わせる．登録メールアドレスが正規のものであると確認したら，ハッシュ rp を更にハッシュ関数にかけてデータベースに登録する．

(2) 認証手順

図 1 に提案方式における認証時のシーケンス図を示す．

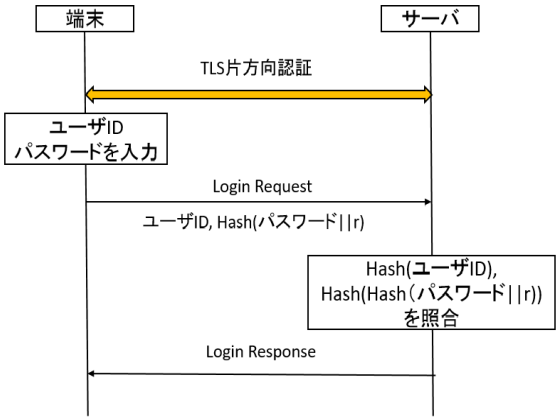


図 1: 認証時のシーケンス

まず，TLS によりサーバを認証する．次に，ユーザはユーザ ID とパスワードを入力する．ユーザ端末はハッシュ rp を生成し，ユーザ ID と共にサーバに送信する．サーバはログイン情報をデータベースの内容と照合し，ログイン情報が正規のものであると確認されれば正規ユーザと判断する．

(3) 別端末からのログイン

提案方式では生成した乱数がユーザ端末内の不揮発メモリ内に保存されるため，このままでは別端末からのログインができない．これを可能とするため，1 アカウントに対し，複数のハッシュ値を登録可能とするように拡張する．この拡張により， 同じパスワード入力により複数端末からのログインを可能にできる．

3. 評価

提案方式をセキュリティ，導入時または運用時に発生する費用，手間や煩わしさ(以下利便性とする)の三項目で既存方式と比較し表 1 に示す．比較対象はパスワードのみ，パスワード+生体認証,パスワード+OTP(*One Time Password*)とした．

表 1: 既存方式との比較

	セキュリティ	費用	利便性
PW	×	○	○
PW＋生体認証	○	×	○
PW＋OTP	○	○	×
提案方式	○	○	○

パスワードのみの認証は，ユーザの利便性が高く専用機器などの費用が必要ない．しかし，攻撃者にパスワードを推測されるなどセキュリティが脆弱である.パスワードと生体認証の組み合わせは，専用機器を使い生体情報を読み取る．ユーザの手間は少ないが，初期費用がかかる．OTP はセキュリティが固く，初期費用は必要ないが，一定時間内にコード入力をしなければならず利便性が低い．

提案方式では，パスワードと乱数の多要素認証でありセキュリティが高い．ユーザは二段階要素の入力をする必要はなく，パスワードのみの認証と同じ利便性で扱うことができる．

4. まとめ

乱数とパスワードを組み合わせたユーザ認証方式を提案した．乱数とパスワードでハッシュ値をとり，この値をパスワードとしてサーバに登録する．乱数はユーザ端末にのみ保存するため，サーバが知ることはできない．提案方式はセキュリティが高く,利便性も高い.1アカウントに複数のハッシュ値を登録することにより，別端末からのログインを可能にする．

乱数とパスワードを組み合わせたユーザ認証方式の提案

理工学部情報工学科
渡邊研究室所属
150441161
4年　渡邉 悠雅

研究背景

- インターネットの普及で個人の認証を行う機会が増えた
  - ➢様々なサイバー攻撃から個人を守ることが重要

- パスワードのみの認証では不十分
  - ➢多要素認証を行うのが当たり前の時代

多要素認証
性質の異なる複数の認証要素を組み合わせること

研究目的

- 使いやすくセキュリティが高い多要素認証方式
  - セキュリティと使い勝手はトレードオフの関係
    - 多要素認証はユーザに手間が発生しやすい

- 専用機器を使わない認証方式
  - システム導入時や運用時に費用が発生しない
  - 既存のパソコンなどの端末に適応可能

既存の認証方式

- 認証要素は性質により知識要素，生体要素，所持要素に分類
  - 多要素認証では異なる分類の組み合わせがよい
- 多要素認証の認証要素について説明
  - 生体認証，ICカード認証，OTP認証，SMS認証
    - パスワードと組み合わせられる主要な認証要素
- 普及が進んでいるFIDO認証
  - 認証情報ではなく認証結果をサーバに送信

生体認証

- 個人が持っている身体情報を鍵とする認証方式
  - 指紋認証，顔認証，虹彩認証，静脈認証

- 使用方法が分かりやすく，ユーザの煩わしさが小さい

- 生体情報の読み取り機が必要になる
  - 指紋センサーやカメラなどが必要
    - 機器がないとログイン不可
- 他人を誤認証，成長や加齢によって認証できない可能性

ICカード認証

- 専用の読み取り機でICカード内の秘密鍵を読み取る

- 使用方法が分かりやすく，ユーザの煩わしさが小さい

- 秘密情報はソフトウェアレベルとハードウェアレベルで守られる
- 専用の読み取り機やカードが必要になる

OTP認証

- OTP(One Time Password)を入力する認証方法
  - ➢一定時間のみ有効なパスワードを利用
    - ➢本稿ではソフトウェアでOTPを生成する方式を想定

- 専用機器が必要なくセキュリティが高い

- ユーザに煩わしさを与えやすい
  - 初めてのユーザには使用方法が分かりにくい
  - 短い有効時間内に操作を完了する必要性

SMS認証

- SMS(Short Message Service)で認証の鍵を受け取る認証
  - 電話回線でメッセージをやりとりするサービス
  - 4ケタまたは6ケタの数字を受け取り入力する

- 使用方法がユーザに分かりやすい

- 認証のたびにサーバに料金が発生する
  - 電話回線を使った通信を行うため
- なりすましや覗き見される可能性

FIDO認証

- FIDO(Fast IDentity Online)は認証器がユーザ情報の検証を行う
  - ➢認証器はユーザの手元にあり，認証結果をFIDOサーバに送信する
- UAF(Universal Authentication Framework)
  - 利用端末に生体情報やPINを登録し，端末をWebサービスに登録
  - ユーザは生体認証またはPINでログイン可能になる
- U2F(Universal 2nd Factor)
  - 二段階認証の認証要素として使われる
  - USBキーやスマートカードなどでFIDO認証を行う
- 従来の認証をリモート認証というのに対しローカル認証と呼ばれる

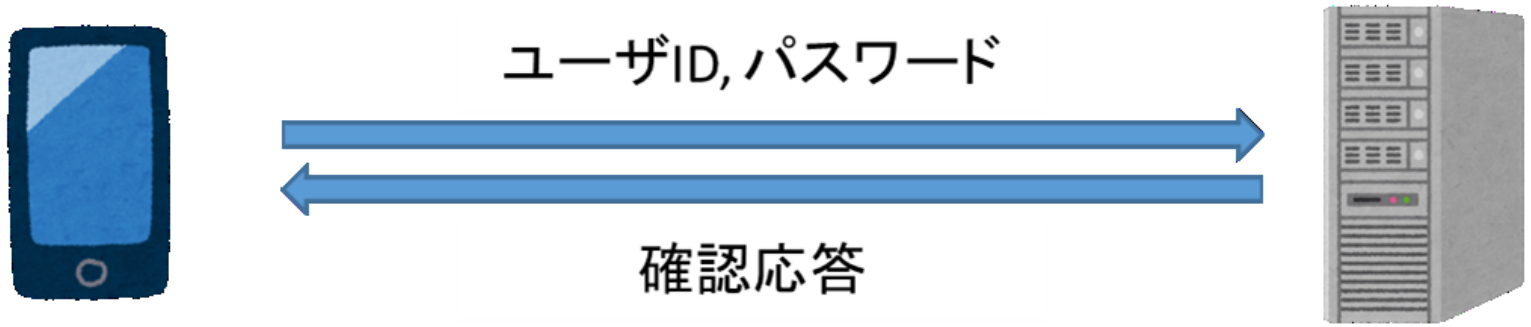
FIDO認証

- ユーザが感じる煩わしさが少ない
  - UAFでは生体認証のみでパスワード入力もいらない
- ローカル認証によるセキュリティの高さ
  - 認証器がFIDOサーバに送るのは認証結果
  - フィッシング攻撃につよい

- FIDO対応スマートフォンや専用物理デバイスの用意
  - ユーザが費用を負担する

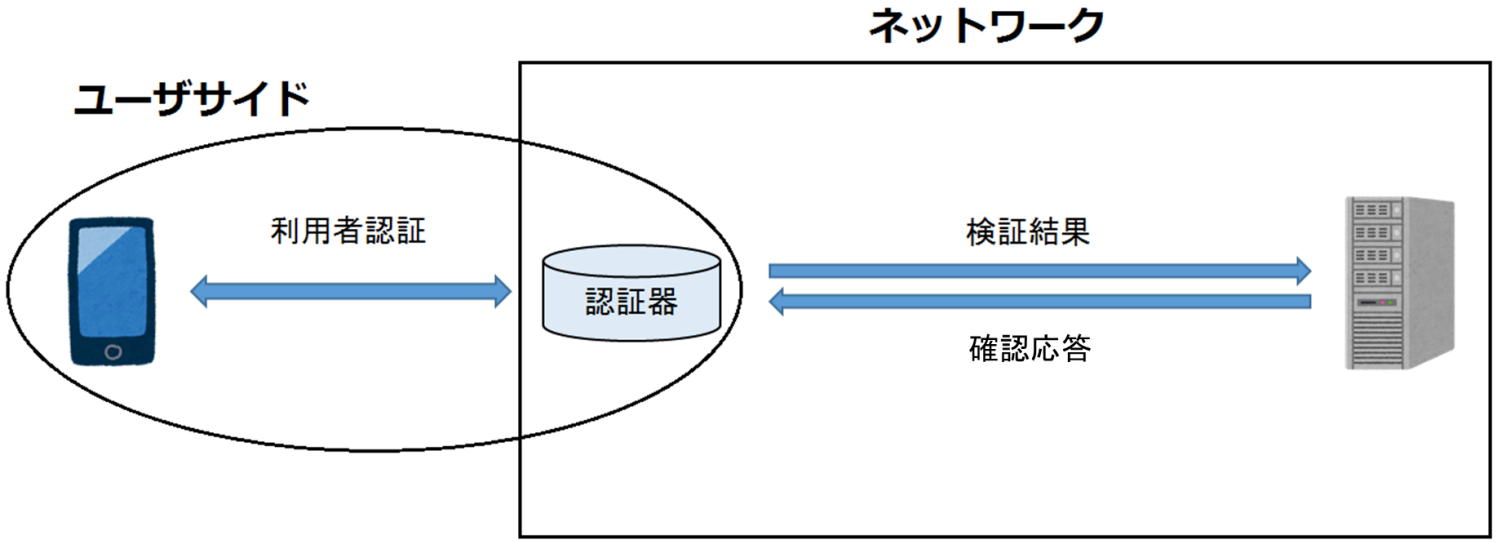
FIDO認証

- 従来の認証方法
  - ➢リモート認証モデルと呼ばれる



FIDO認証

- 認証結果をサーバに送信するFIDO認証
  - ローカル認証モデルと呼ばれる
  - FIDOサーバは認証結果の妥当性を確認

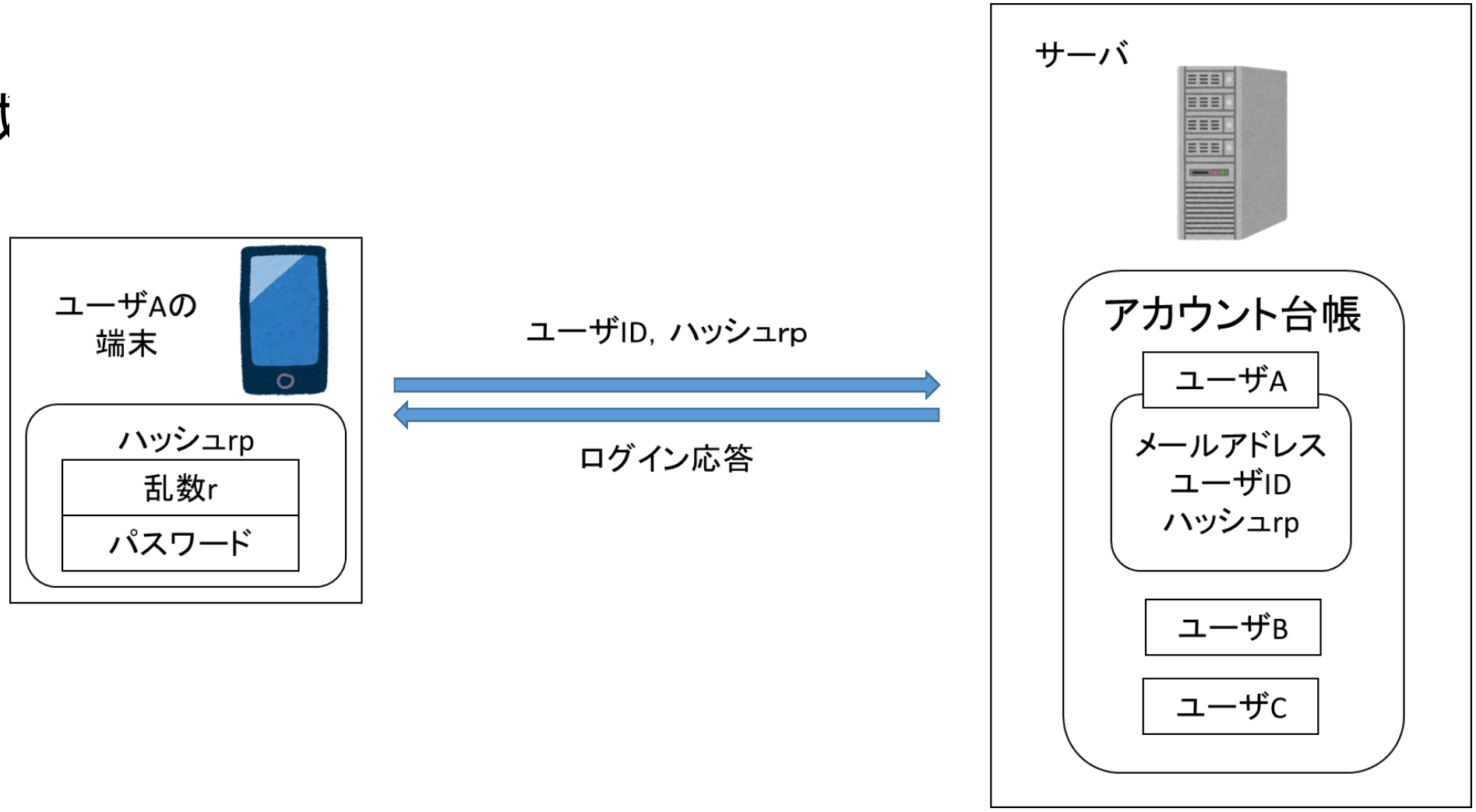


提案方式

- 乱数とパスワードでハッシュ値をとり，ハッシュ値をサーバに登録するパスワードとして扱う
  - 乱数とハッシュ値はユーザ端末で自動生成
  - 乱数は不揮発メモリ内に保存
  - サーバに送る情報はメールアドレス、ユーザID, ハッシュ値
- ユーザは既存のパスワード認証と同じ使い勝手で使用可能
- サーバサイドは乱数と元のパスワードを知ることができない

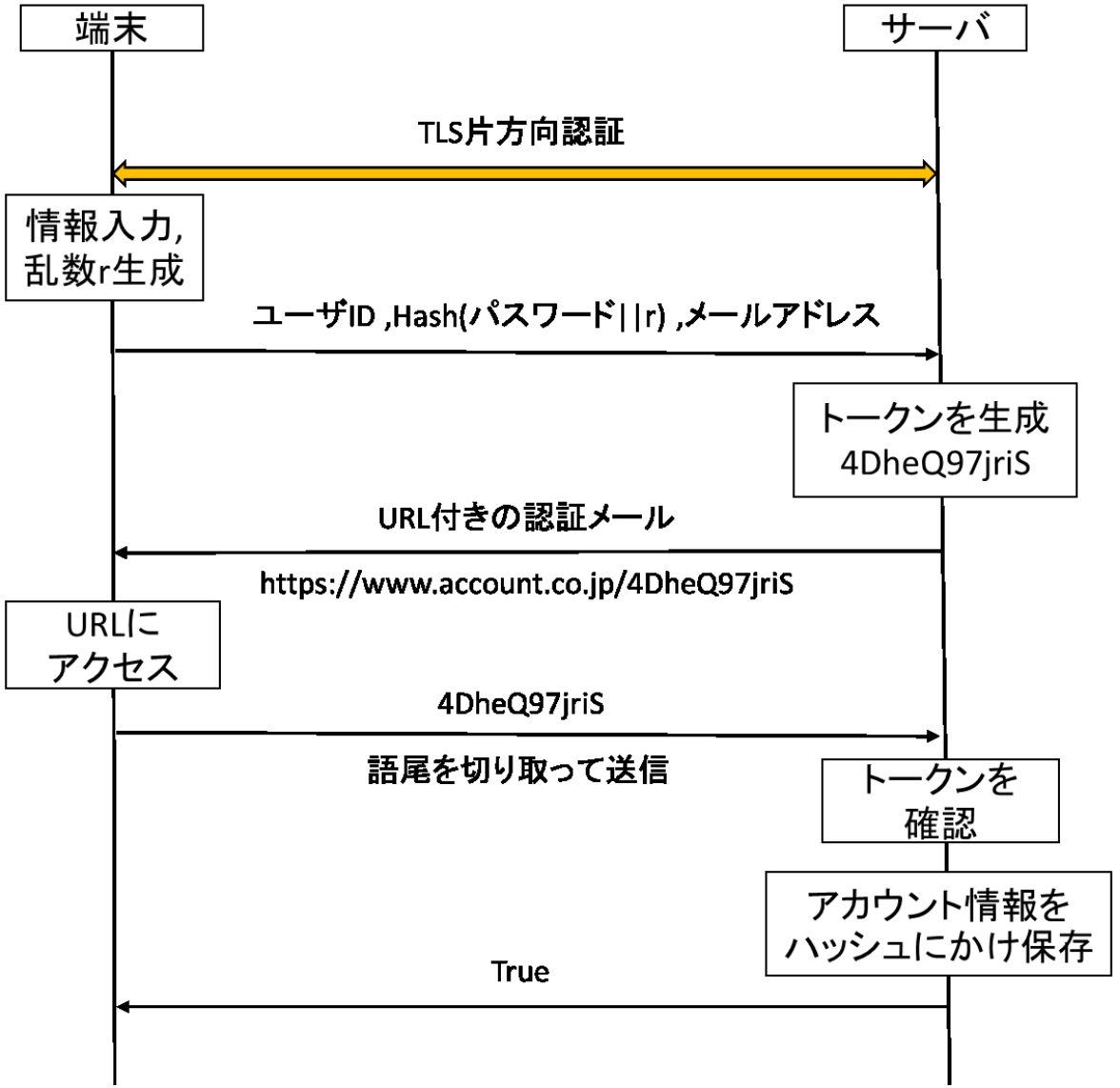
提案方式

- 構成


ユーザAの
端末
ハッシュrp
乱数r
パスワード
ユーザID，ハッシュrp
ログイン応答
サーバ
アカウント台帳
ユーザA
メールアドレス
ユーザID
ハッシュrp
ユーザB
ユーザC

提案方式

アカウント生成時の
シーケンス図



提案方式

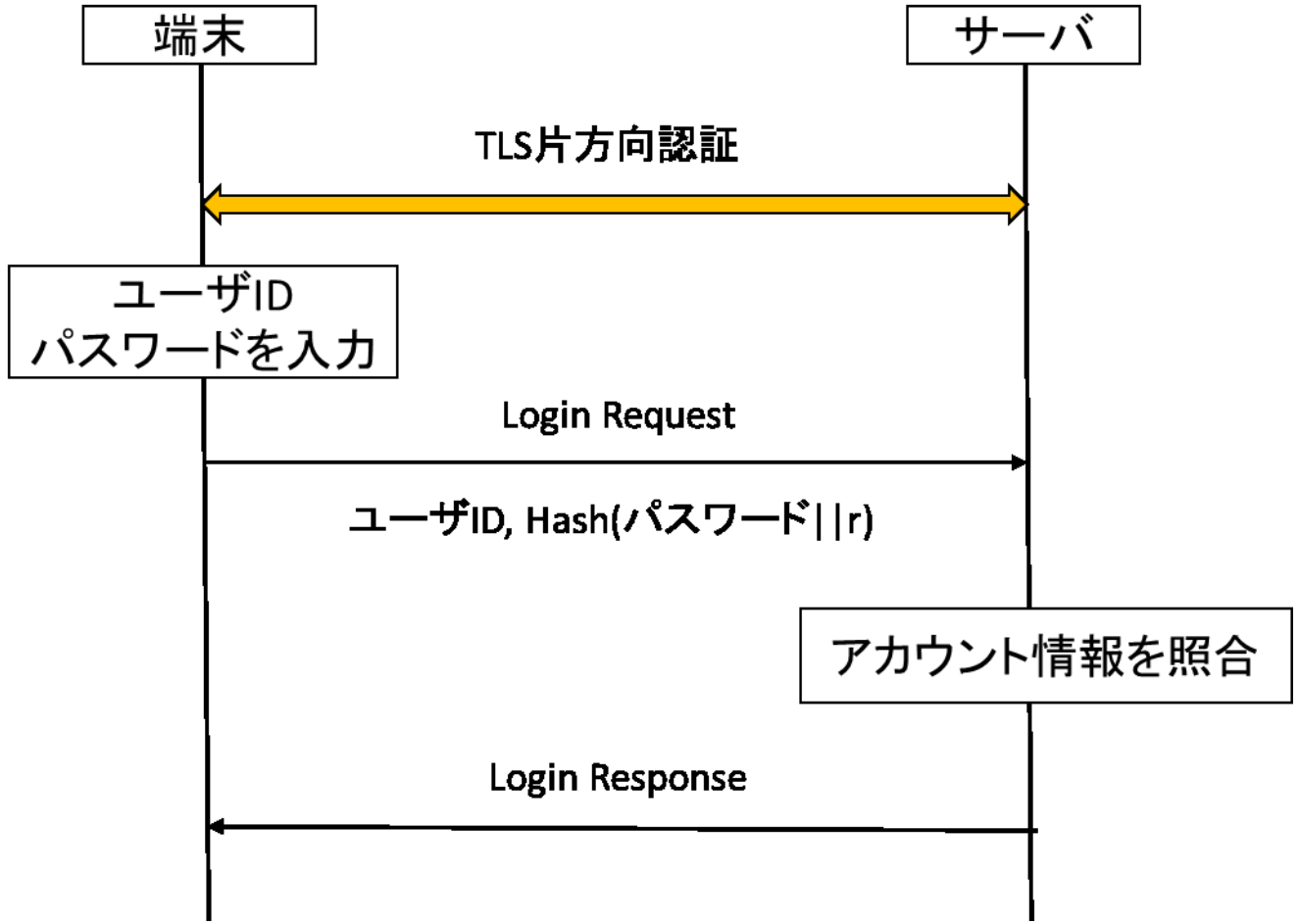
- ユーザは乱数とパスワードがないとログインできない
  - 普段使っている端末以外ではログインすることが困難

別端末登録処理を行うことで解決

- 1アカウントに複数のハッシュ値(パスワード)を登録可能に拡張
  - 端末ごとに保持する乱数とハッシュ値が異なる
  - ユーザは同じパスワードでログイン可能

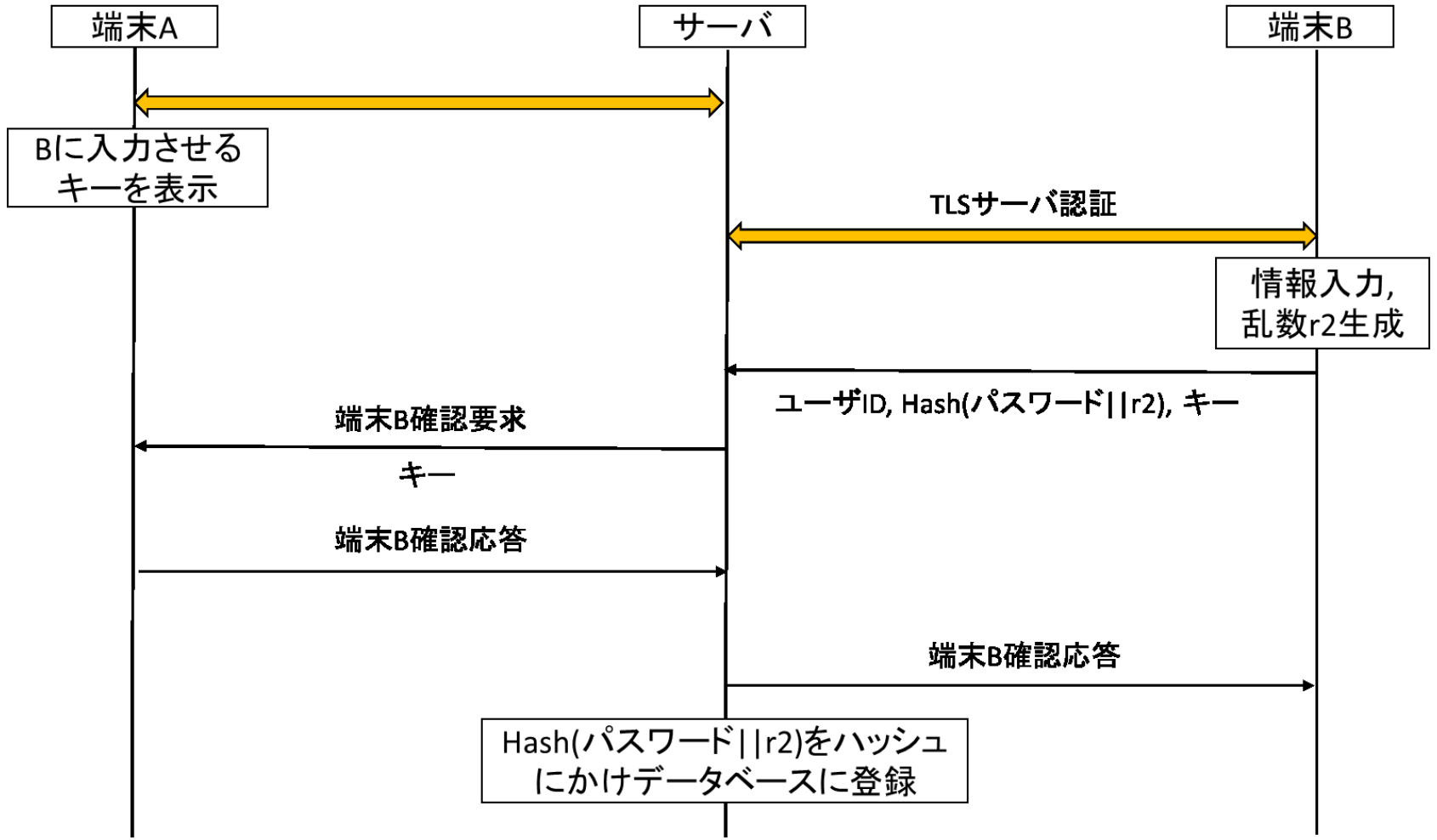
提案方式

ログイン処理時の
シーケンス図



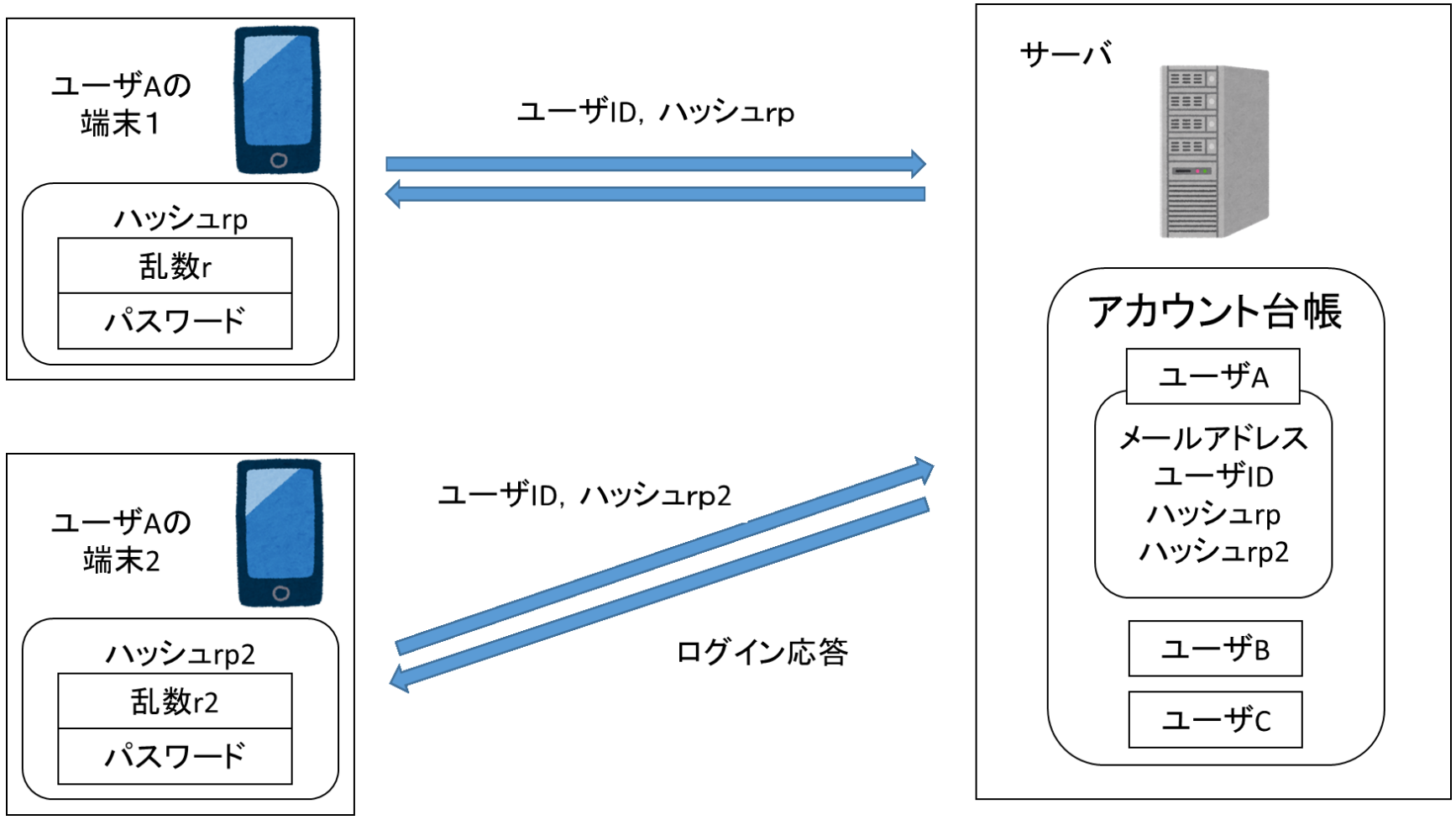
提案方式

別端末登録時の
シーケンス図



提案方式

複数端末登録した構成図



評価

- 辞書攻撃
  - 辞書に載っている単語をひたすら照合する解析攻撃
- 推測攻撃
  - パスワードにつけていると思われる単語などを推測する解析攻撃
- リスト型攻撃
  - 流出したアカウント情報を当てはめて不正アクセスを試みる攻撃

評価

- パスワードのみ，パスワードと組み合わせた多要素認証，FIDO認証，提案方式を比較

	セキュリティ			使い勝手			
	辞書攻撃	推測攻撃	リスト型攻撃	費用	わかりやすさ	煩わしさ	別端末ログイン
PW	×	×	×	○	○	○	○
PW+生体認証	△	○	×	×	○	○	×
PW+ICカード	△	○	○	×	○	○	×
PW+OTP	△	○	○	○	×	×	○
PW+SMS	△	○	○	×	○	○	△
FIDO	○	○	○	×	○	○	△
提案方式	○	○	○	○	○	○	○

まとめ

- 乱数とパスワードでハッシュ値をとり，ハッシュ値をパスワードとしてサーバに登録する
- 提案方式はセキュリティと使い勝手を兼ね備えた多要素認証
  - パスワードのみの認証と同じ使い勝手
- 専用機器が必要なく既存のパソコン等で利用可能
- 端末登録処理により別端末からのログイン可能に拡張

補足

- IPv6は