平成30年度　卒 業 論 文

和文題目

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

英文題目

Proposal of User Authentication Method Combining Random Number and Password

情報工学科　渡邊研究室

(学籍番号: 150441161)

渡邉　悠雅

提出日: 平成31年2月8日

名城大学理工学部

概要

ユーザ認証を確実に行うにはパスワードだけではなく別の要素を組み合わせる必要がある．しかし，認証専用機器を用意する必要があることや，認証手順が複雑になるという課題があった．そこで，パスワード以外の要素として，ユーザ端末内で生成する乱数を用いる方式を提案する．乱数はユーザアカウント作成時に作られ，パスワードと乱数を組み合わせたハッシュ値を，サーバ側にパスワードとして登録させる．乱数の生成およびハッシュ値の算出はユーザ端末内で自動的に処理される．

一般にセキュリティとユーザの煩わしさの少なさはトレードオフの関係にあり，両者を両立させることは難しい．提案方式はログイン情報入力時に二段階要素の情報入力がない分，ユーザに対してわずらわしさを与えることがない．一方，多要素認証であるためセキュリティが高い．本稿では提案方式と他の認証方式をセキュリティや使い勝手などの項目で比較した．

Abstract

In order to ensure user authentication, it is necessary to combine not only the password but another element. However, there is a problem that it is necessary to prepare a device dedicated to authentication and the authentication procedure becomes complicated. Therefore, we propose a method using random numbers generated in the user terminal as an element other than the password. A random number is created at the time of user account creation, and hash value combining password and random number is registered as a password on the server side.

In general, there is a trade-off between security and less troublesome user, so it is difficult to make both of them compatible. In the proposed method, since there is no information input of the two-step element at the time of inputting the login information, it does not give trouble to the user. On the other hand, security is high because it is multi-factor authentication. In this paper, we compared the proposed method and other authentication methods with items such as security and usability.

目 次

第 1 章　序論 **1**

第 2 章　既存の認証方式 **3**

2.1　認証要素 3

2.1.1　生体認証 3

2.1.2　IC カード認証 3

2.1.3　OTP 認証 3

2.1.4　SMS 認証 3

2.2　FIDO(Fast IDentity Online) 4

第 3 章　提案方式 **6**

3.1　概要 6

3.2　アカウントの生成と認証手順 6

3.2.1　アカウントの生成手順 6

3.2.2　認証手順 7

3.2.3　別端末からのログイン 7

第 4 章　評価 **10**

4.1　評価項目 10

4.2　比較表と考察 11

第 5 章　まとめ **12**

謝辞 **13**

第1章　序論

インターネットは我々のインフラの一つであり，パソコン以外にもスマートフォンや家庭用ゲーム機など様々な機器からアクセスできるようになった．インターネットの普及とともに，個人を認証する機会は飛躍的に増えている．多くの認証方式がある中で，ユーザ ID とパスワードを使った認証方式はもっとも使われることの多い個人認証である．しかし，インターネットには様々なセキュリティ上の弱点があり，不正アクセスや情報漏えいから個人を守るにはパスワードだけの認証では不十分である．現在のアプリケーションや Web サービスでは，多要素認証による個人認証を取ることが多い．多要素認証とは性質の異なる複数の認証要素を組み合わせる認証である．認証要素は性質により知識要素，生体要素，所持要素に分類され，多要素認証ではセキュリティ的に異なる分類のものを組み合わせることが良いとされる．[1] パスワード認証では知識要素である PIN 認証よりも生体認証，IC カード認証と組み合わせられる．

認証技術はセキュリティだけではなく，ユーザの使いやすさや分かりやすさが重要になっている．セキュリティと使いやすさは相互背反の関係であり，両立させることが困難である．多要素認証は認証手順が増える分ユーザに手間や煩わしさを与えやすい．例えば，ネット証券取引所や仮想通貨取引所ではそのセキュリティの高さから，ユーザに OTP(One Time Password) を使う二段階認証アプリを推奨する．しかし，その煩わしさから二段階認証アプリを設定せずアカウントが不正アクセスされる事件が多い．

専用機器を必要とする認証技術は使用方法を簡単にし，かつセキュリティを高めることができる利点があるが他の欠点が発生する．専用の読み取り機やカードなどが必要になる認証技術は導入時に費用が発生する．紛失時や故障時にはデバイスの再発行をする必要がでてくる．また，認証技術に対応した端末以外ではログインすることが困難である．デバイスの貸し借りや盗難される可能性がありセキュリティホールとなりうる．

本稿では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とり，ハッシュ値をパスワードとしてサーバに送信するユーザ認証方式を提案する．乱数の生成およびハッシュ値の算出をユーザ端末内で自動的に行うことにより，ユーザが二段階要素を入力する手間を省略することができる．パスワードのみの認証と同じ使い勝手でユーザは利用することができ，ユーザが新しく覚えることが少ない．提案方式は専用機器の用意をする必要がないため，既存のパソコンや携帯電話で利用することができる．サーバは乱数を知らないので，サーバサイドから情報が漏れることがない．そのため，パスワードを推定する攻撃に強い耐性を持っている．

以降，第 2 章ではパスワード認証と組み合わせられる主要な認証技術について述べる．また，近年普及が進んでいる FIDO 認証について述べる．第 3 章では，シーケンス図を用いて提案方式について述べる．第 4 章では提案方式と既存の認証技術をセキュリティ，使い勝手の観点から比較

し評価する．第 5 章では全体のまとめを述べる．

第2章　既存の認証方式

本章では，パスワード認証と組み合わせられる主要な認証要素について概要と課題を述べる．また，類似技術として FIDO の概要を述べる．

2.1　認証要素

2.1.1　生体認証

生体認証は個人が持っている身体情報を鍵として認証に活用する方法であり、生体認証には指紋認証、虹彩認証、静脈認証、顔認証といったものがある。ユーザが使用する際の煩わしさは小さく，使用方法がわかりやすい．身体情報の事前登録が必要であるが，顔認証などユーザが二段階要素を情報入力する手間がないことがある．指紋認証であれば指紋読み取り機，顔認証や虹彩認証であればカメラが必要になるなど，機器の導入費用が発生する．身体の変化で認証不可能になることや、精度によっては別の人を認証する問題がある．

2.1.2　IC カード認証

IC カードによる認証は, 専用の読み取り機を使いカード内の秘密鍵を読み取ることで認証を行う. カード内の情報はハードウェアレベルとソフトウェアレベルの両方から守られており, 外部から秘密情報の参照を防いでいる.[1] カードの事前発行と読み取り機の用意が必要でありユーザに費用が発生する．

2.1.3　OTP 認証

OTP は一定時間のみ有効なパスワードを生成する認証技術である．本稿では最も普及している二段階認証アプリの Google Authenticator による OTP の生成を想定する. ユーザはサーバとあらかじめ OTP 生成用の鍵を共有する．ユーザ端末とサーバは，それぞれ共有した鍵と時刻カウンターを元に 6 桁数字の OTP を生成する．OTP は一定時間ごとに更新されるようになっており，有効時間が定められている．専用機器などの用意が必要ないため，ユーザに金銭的負担がない．使用方法がわかりにくく，短い有効時間内に認証処理を行う必要があるため，ユーザに煩わしさを与えやすい．

2.1.4　SMS 認証

SMS(Short Message Service) とは、相手の電話番号を指定してメッセージをやり取りするサービスである。OTP 認証の一つと分類されることもあるが，本稿では分けて考える．SMS 認証は，サー

バからユーザが SMS で認証の鍵を受け取る認証である．SMS 認証は OTP 認証に分類されることもあるが，本稿では別の認証として扱う．ユーザは 4 桁または 6 桁の OTP を SMS で受けとり認証時に入力する。使用方法は分かりやすいが，携帯電話またはスマートフォンが必要になる．SMS は一般的なメールとは異なり、電話回線を使ったメッセージ送信のため送信者側に電話料金が発生する。そのため，SMS 認証を運用するサーバサイドに認証ごとに費用がかかる．ロック画面に SMS を通知する設定をしている場合に，他人に覗き見される危険性がある．

2.2 FIDO(Fast IDentity Online)

FIDO は素早いオンライン認証を目的とした認証技術であり，ユーザの負担が少なくセキュリティが高い．図 1 は FIDO 認証を簡潔に表した図である．従来の認証は利用者が ID とパスワード等の情報を，認証サーバに送信する．認証サーバは台帳のユーザ情報と比較し，正規の情報であるか検証する．FIDO はユーザの手元にある認証器がユーザ情報の検証を行う．[2] 認証器はユーザの検証結果を認証サーバに送信し，認証サーバは検証結果が妥当のものであるかを確認することで認証が完了する．この確認処理には公開鍵暗号方式を活用している．従来の認証をリモート認証モデルというのに対し，FIDO はローカル認証モデルと呼ばれる．パスワード情報をサーバに預ける必要がなく，ネットワーク上に流れることがない．FIDO 認証には，FIDO に準じたスマートフォンや USB キーなどのデバイスを用意する必要がある．FIDO はユーザ認証方法に応じて UAF(Universal Authentication Framework) 仕様と U2F(Universal 2nd Factor) 仕様の認証がある．UAF では，生体認証または PIN(Personal Identification Number) を利用端末に登録する．利用端末を Web サービスに登録することで，ユーザは生体認証または PIN でログインすることができる．U2F はユーザ ID とパスワードによる認証後，U2F 規格に準じた認証器で簡単に二段階目の認証を使う．認証器は USB キーやスマートキーなど端末に着脱タイプや，NFC(Near Field Communication) など無線で行うタイプが存在する．UAF に対応したスマートフォンなどの端末を無線で認証器として扱うことも可能である．

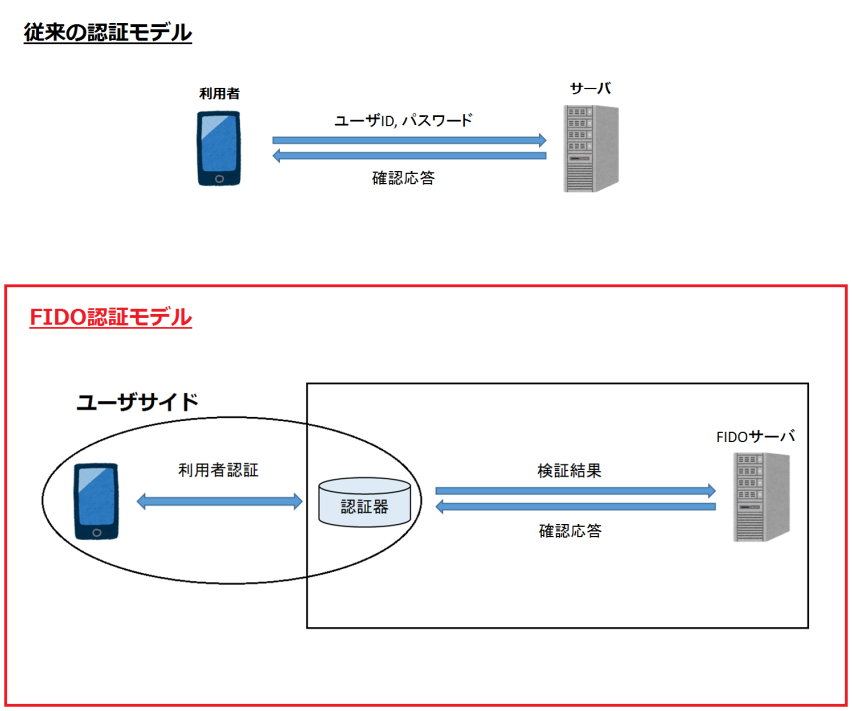

図 1　FIDO 認証の構造

第3章　提案方式

3.1　概要

本提案はユーザ端末で乱数を生成し，パスワードと乱数を組み合わせたハッシュ値を算出する．サーバにはハッシュ値をパスワードとして扱い送信する．サーバサイドには乱数元のパスワードがわからない点が特徴である．ユーザは既存のパスワード認証と同様な使い勝手で利用することができ，多要素認証によりセキュリティを向上させることができる．図 2 は提案方式の構造を表したものである．

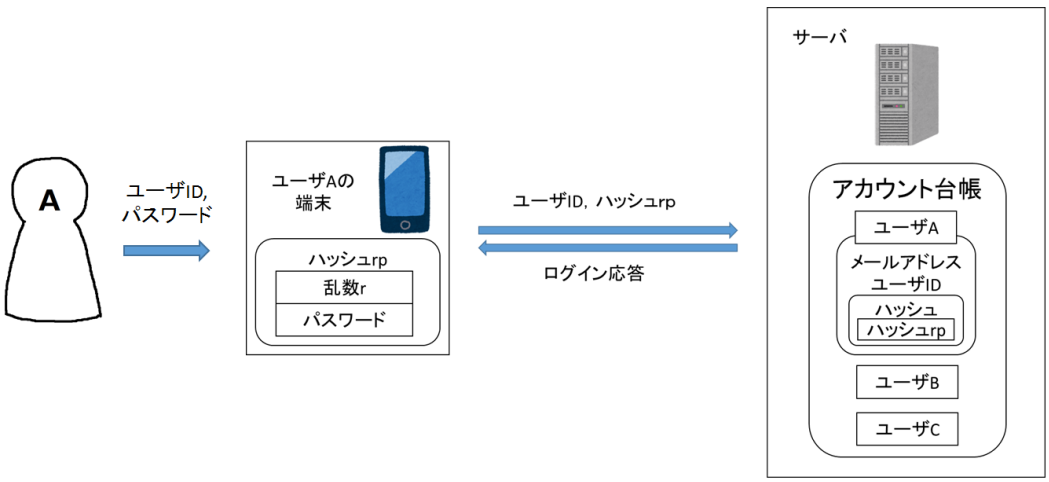

図 2　提案方式の構造

3.2　アカウントの生成と認証手順

3.2.1　アカウントの生成手順

アカウント作成方法は様々な方法があるが，例えばメールアドレスを使ったアカウント作成を行う．図 3 はメールアドレスによる提案方式のアカウント生成を示すシーケンス図である．端末は

サーバを TLS で認証した後，メールアドレス，ユーザ ID，パスワードを入力する．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とともに，乱数 r とパスワードを組み合わせたハッシュ値 (以下ハッシュ rp とする) を算出する．ユーザ端末はメールアドレス，ユーザ ID，ハッシュ rp を送信する．このハッシュ rp はサーバに登録するパスワードとして扱わせる．サーバは登録メールアドレスが正規のものであるか確認するプロセスに入る．このプロセスは既存のメールアドレス確認方法と同様の方法を適応可能である．サーバでは不規則な文字列 (以下トークンと呼ぶ) を生成し，認証用 URL の最後に付属する．ユーザが認証用 URL にアクセスすると自動的にトークンを切り取りサーバに送る．サーバはトークンを確認すると，アカウント情報をハッシュ関数にかけデータベースに保存する．

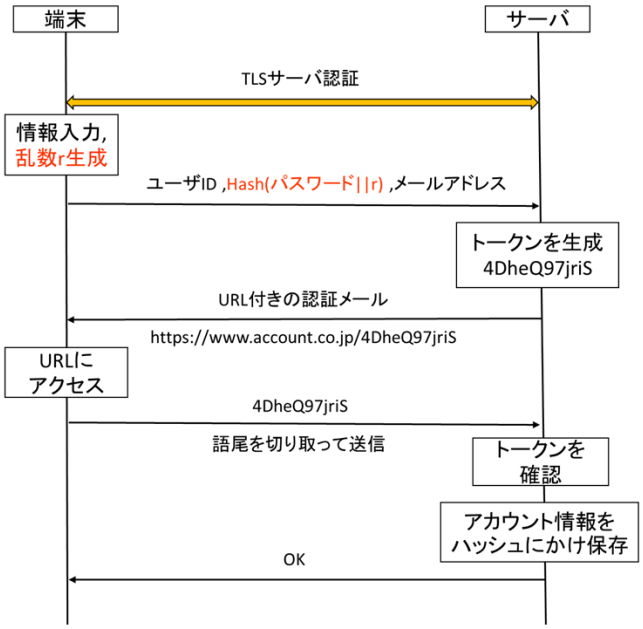

図 3　アカウント生成のシーケンス図

3.2.2　認証手順

図 4 に提案方式のログイン処理を表すシーケンス図である．ユーザは TLS によりサーバを認証した後，ユーザ ID とパスワードを入力する．ユーザ端末は保存されているパスワードと乱数 r からハッシュ rp を生成し，ユーザ ID とともにサーバに送信する．サーバは受け取ったアカウント情報をハッシュ関数にかけ，データベースと照合する．ログイン情報が正規のものであると確認されれば，正規ユーザとして認証完了する．

3.2.3　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ログインすることができない．そこで，1 つのアカウントに対して複数の端末を登録処で

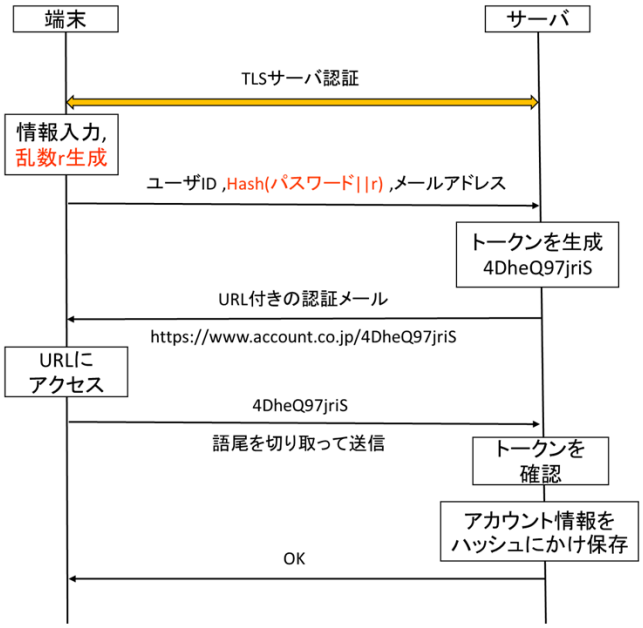

図 4　ログイン処理のシーケンス図

きるように拡張する．図 5 は別端末のログイン登録処理を表したシーケンス図である．図 6 は別端末登録した提案方式の構造を表した図である．ログイン登録をする際は，既に登録済みである端末 A と新規端末 B が近くにあることを前提としている．端末 A にてログイン登録に必要なキーを発行する．端末 B は TLS でサーバを認証後，ユーザ ID，パスワード，目視で確認したキーを入力する．なお，パスワードは端末 A と同じものを利用できる．端末 B では乱数 r2 を生成し，乱数 r2 とパスワードでハッシュ値 (以下ハッシュ rp2 とする) を算出する．その後，端末 B はユーザ ID とハッシュ rp，キーをサーバに送信する．サーバは端末 B からアカウント情報を受け取ると，端末 A にキーの一致確認を行う．正しいキーであると確認すると，端末 B から送られてきたハッシュ値を同一ユーザのアカウントとしてデータベースに登録する．

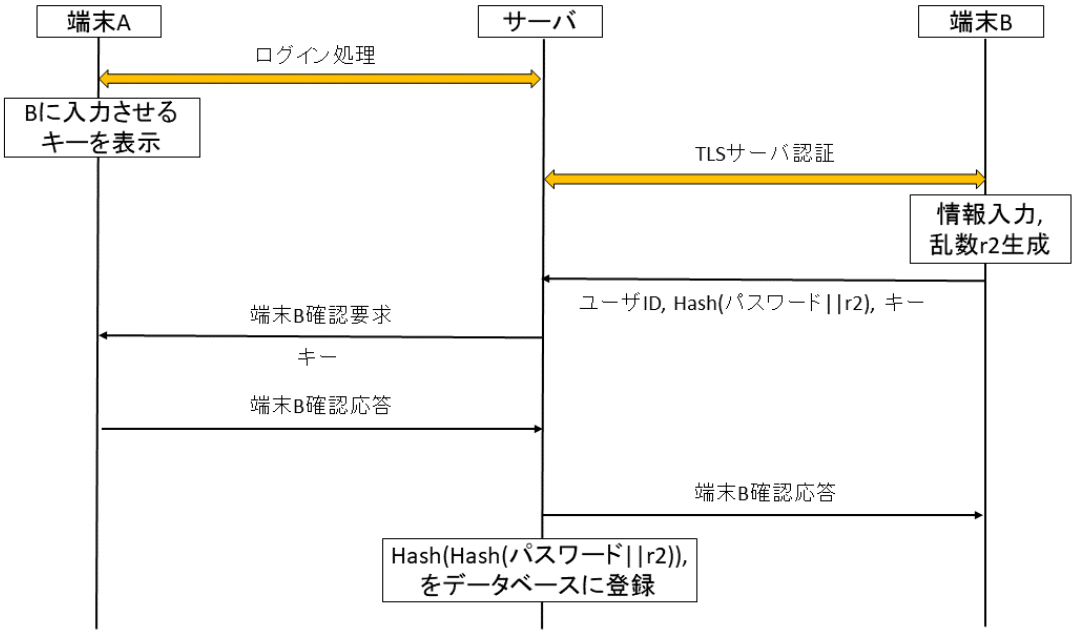

図 5　別端末登録処理のシーケンス図

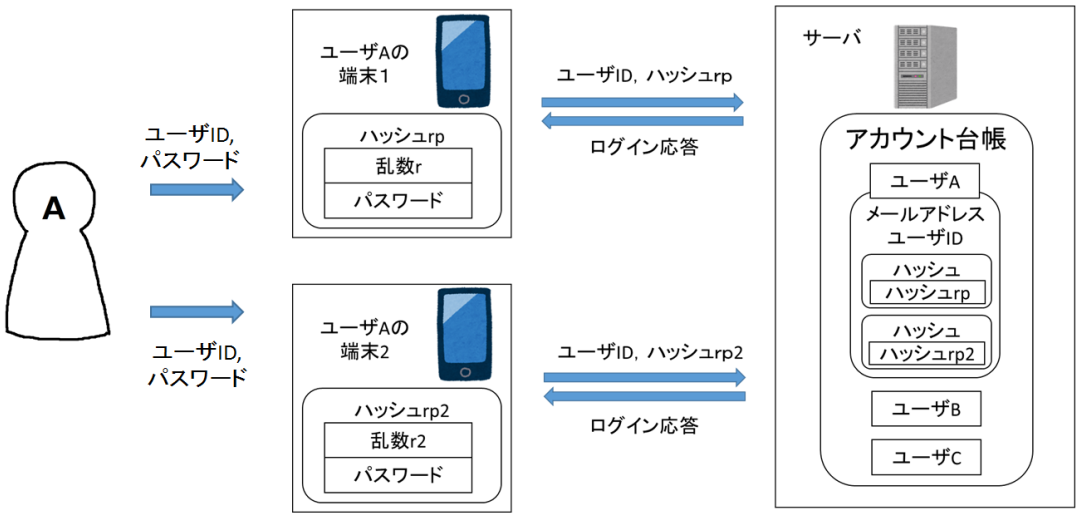

図 6　1 アカウントに複数ハッシュ値を登録する提案方式

第4章　評価

認証方式をセキュリティと使い勝手で比較して表 1 に示す．比較対象はパスワードのみ，パスワードに要素として生体認証，IC カード，OTP，SMS を組み合わせた場合，FIDO，および提案方式とした．

4.1　評価項目

辞書攻撃は辞書に載っている単語をひたすら照合することによってパスワードを解析する攻撃である．辞書攻撃は辞書に載っている単語の他に，数字を加えたものや大文字と小文字を混ぜたものまで照合する. 対策として一定回数パスワードの入力を間違えた場合に，ID を凍結する方法をとる場合が多い．しかし，サーバサイドの台帳情報が漏洩している場合に解析される可能性がある. 本稿では台帳情報が漏洩している場合も想定して評価する．パスワード等の一部情報が解析されるが，不正ログインされることがない場合に△と評価する．

推測攻撃はターゲットが設定すると考えられるパスワードを予想して不正アクセスを試みる攻撃である．例えば，自分の名前や誕生日，人気のキャラクターの名前をパスワードに含んでいる場合に被害に遭いやすい．

リスト型攻撃は他のサービスなどから漏洩したアカウント情報を利用して不正アクセスを試みる攻撃である．他の Web サービスのパスワードを使いまわしている人が被害に遭いやすい．

使い勝手は以下の 2 項目で比較した．

(1) 導入費用または運用費用の安さ

(2) 使用方法の分かりやすさ，使用時の手間や煩わしさ

表 1　Comparison of authentication methods

	セキュリティ			使い勝手	
	辞書攻撃	推測攻撃	リスト型攻撃	項目 (1)	項目 (2)
PW	×	×	×	○	○
PW+生体認証	△	○	×	×	○
PW+IC カード	△	○	○	×	○
PW+OTP	△	○	○	○	×
PW+SMS	△	○	○	×	○
FIDO	○	○	○	×	○
提案方式	○	○	○	○	○

4.2 比較表と考察

パスワードのみの認証はユーザサイドとサーバサイド両方の面から辞書攻撃にあう可能性がある．覚えやすい言葉をパスワードにしているユーザは推測攻撃される危険性がある．ユーザによっては同じパスワード使いまわしているのでリスト型攻撃に弱い．発生する費用や煩わしさが小さい．

生体認証は漏洩した生体情報を使われる可能性があるためリスト型攻撃に耐性がない．認証に指紋読み取り機，カメラなどが必要となるため項目 (1) を×とした．操作の手間や煩わしさが少ない．

IC カード認証はカードリーダーやカードの用意が必要になり費用が発生する．使用方法が直感的にわかりやすく手間が少ない．

OTP 認証は一定時間内のみ有効なパスワードを使うためセキュリティが高い．専用機などの用意が必要ないため発生する費用が小さい．使用手順が多く認証に制限時間があるため項目 (2) を×とした．

SMS 認証は一度きり有効なパスワードを使うため，推定する攻撃に耐性がある．電話回線を使っているため認証を行うたびにサーバに費用が発生する．使用方法は電話番号を送信し，送られてきたコードを入力するだけなので項目 (2) を○とした．

提案方式はパスワードのみの認証と同様の使い勝手で利用可能である．サーバに登録されたハッシュ値は十分に長い文字列であるため辞書攻撃は不可能である．ハッシュ値はパスワードと乱数を組み合わせて生成しているので，推測攻撃をすることも不可能である．また，認証にユーザ端末に保存されている乱数 r が必要となるためリスト型攻撃は不可能である．セキュリティと使い勝手を兼ね備えた認証方式であるといえる．

第5章　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，算出したハッシュ値をパスワードとしてサーバに登録する．乱数はユーザ端末内の不揮発メモリ内に保存されており，ネットワーク上に流れることがない．また，パスワードが直接ネットワーク上に流れることもない．サーバは元のパスワードを知るすべがなく，サーバサイドの台帳情報が漏えいした場合にも辞書攻撃されることがない．推測攻撃，リスト型攻撃に対する耐性も持ち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がなく，パスワード認証と同様な使い勝手で利用できる．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，別端末からログインすることを可能にする．

謝辞

本研究にあたり，研究の方向や進め方など終始にわたりご指導，ご助言を受け賜わりました指導教官の渡邊晃教授に心より厚く御礼申し上げます．

最後に，本研究に関して本研究室の皆様にも多くの方々から多大な助言と協力を受け賜り深く感謝しております．

参考文献

[1] SKUID by GMO 第 2 回 多要素認証の種類と方法．https://sku.id/catalog/skuid_whitepaper02.pdf

[2] fido ALLIENCE ｜ PRESENTATIONS ｜ fido 認証概要説明
https://fidoalliance.org/fido%e8%aa%8d%e8%a8%bc%e6%a6%82%e8%a6%81%e8%aa%ac%e6%98%8e/