WebAuthnを用いたパスワードレス生体認証のユーザビリティ調査

山口 修司[1,a)]　日暮 立[1,b)]　五味 秀仁[1,c)]　大神 渉[1,d)]

概要：W3C で標準化された Web Authentication (WebAuthn) をベースとしたパスワードレス生体認証を導入した後の ユーザビリティを評価する調査を実施した．既存の認証手段と比較を行うため，システムログ解析とクラウドソーシングによる SUS 評価という 2 つの視点から，3 種類の認証手段 (WebAuthn ベースの生体認証，パスワード認証，SMS 認証) のユーザビリティを調査した．システムログ解析により，認証時間と認証成功率に関して，WebAuthn ベースの生体認証がパスワード認証，SMS 認証より優れていることがわかった．クラウドソーシングによる SUS 評価では，WebAuthn ベースの生体認証と SMS 認証がパスワード認証よりもユーザビリティが優れていることを確認した．以上から，WebAuthn ベースの生体認証は、パスワード認証よりもユーザビリティが良いことが確認できた．

キーワード：WebAuthn 認証，パスワードレス，パスワード認証，SMS 認証，ユーザビリティ，FIDO

Usability Study of WebAuthn-based Passwordless Biometric Authentication

Shuji Yamaguchi[1,a)]　Tatsuru Higurashi[1,b)]　Hidehito Gomi[1,c)]　Wataru Oogami[1,d)]

Abstract: We conducted a study to evaluate whether usability improves after introducing WebAuthn-based biometric authentication standardized by W3C. The usability of such authentication was investigated from two aspects; system log analysis and system usability scale (SUS) of three different authentication methods. We analyzed the authentication time and authentication success rate for accessing our web services based on the system log of our server. We also investigated the SUS in our service via crowdsourcing. We found that the usability of WebAuthn-based biometric authentication records in the system log was the best, and the average SUS of such biometric authentication was significantly better than password authentication. The results of the two investigations indicate that WebAuthn-based biometric authentication improved the usability of user authentication.

Keywords: WebAuthn, passwordless, password, SMS, usability, FIDO

1. はじめに

Web サービスの増加に伴い，ユーザは多くのアカウントを持ち，またログインする機会が多くなっている．そのため，セキュリティとユーザビリティの両方を向上させる認証方法を導入することが重要になっている．

パスワードを用いた個人認証は，最も広く使用されている認証方法だが，セキュリティとユーザビリティに関しては問題が報告されている [9]．

パスワードを使用して従来の認証手段を置き換える方法の 1 つに，2 要素認証 [18] がある．2 要素認証には，認証の 3 要素（知識，所持，生体）のうち 2 つが必要となる．認証方式としては，SMS ベースのワンタイムパスコード（OTP）やハードウェアトークンなどが一般的に使用さ

[1] ヤフー株式会社 Yahoo Japan Corporation
[a)] shyamagu@yahoo-corp.jp
[b)] thiguras@yahoo-corp.jp
[c)] hgomi@yahoo-corp.jp
[d)] wogami@yahoo-corp.jp

れる．

2 要素認証は公開鍵暗号方式をサポートする FIDO Universal 2nd Factor（U2F）[2] の仕組みによって拡張された．ユーザはセキュリティーキーを使用して認証される [1]．U2F のユーザビリティに関してはいくつかの調査が行われている [13,14,16]．

U2F と FIDO UAF(Universal Authentication Framework) [3] を強化するために，W3C によって新しい認証規格 Web Authentication（WebAuthn） [20] がリリースされた．この規格により，一般的な Web ブラウザーを介して，Web サイトでパスワードなしに自分自身を認証できるため，2 要素認証と同様に，認証の使いやすさが向上すると期待できる．

WebAuthn の規格を使用したユーザビリティの調査としては，セキュリティキーを用いた認証の調査が行われている [8,17] が，生体認証に関するユーザビリティは我々の知る限り調査されていない．

そこで，本稿では WebAuthn ベースの生体認証のユーザビリティを評価する．

本稿の貢献は下記の通りである．

(1) WebAuthn ベースのパスワードレスの生体認証について，システムログ解析とクラウドソーシングによるユーザアンケートを使用してパスワードおよび SMS 認証と比較するユーザビリティ調査を実施した．
(2) システムログ分析とクラウドソーシング結果の評価により 上記 3 つの認証方式のユーザビリティを調査した結果，WebAuthn ベースのパスワードレスの生体認証のユーザビリティが優れていることを確認した．

2. システム設計

ここでは，我々の認証システムについての概要と導入した WebAuthn ベースの生体認証について記述する．

2.1 認証システム概要

今回対象とする Yahoo! JAPAN ID の認証システムは，Yahoo! JAPAN のサービス利用のために提供されており，現時点で月間ログインユーザ数が 4000 万以上と非常に大規模なシステムとなっている．従来はパスワード認証のみが提供されていたが，近年，パスワード認証のセキュリティとユーザビリティの課題から，パスワードを使用しない認証（パスワードレス認証）も合わせて導入されている．

パスワードレス認証として，携帯電話のショートメッセージサービスを用いた認証手段 (SMS 認証) が提供されている．我々の提供する SMS 認証は，認証行為を実施するたびに，4 桁の数字の確認番号 (PIN コード) が記載されているショートメッセージをユーザに送信し，それをユーザが認証画面に入力することにより個人認証を行う手法である．都度異なる PIN コードが使用されるため，ユーザはパスワードのように記憶をする必要がなくユーザビリティの向上が見込まれる．

一方で，SMS 認証は PIN コードの確認・入力の手順が煩雑であるため，さらなるユーザビリティの改善を目指し，WebAuthn ベースの生体認証も合わせて導入された．WebAuthn は，認証に関するグローバルなコンソーシアムである FIDO アライアンスからの技術提案をもとにして，W3C（World Wide Web Consortium）において策定された標準仕様であるため，標準仕様に準拠した実装にすることでユーザのセキュリティとプライバシーに配慮した実装が可能となるだけでなく，仕様に準拠する製品やサービス間の相互接続性の確保できる． また，生体認証と組み合わせることで，さらなるセキュリティやユーザビリティの向上が見込まれる． 詳細は 2.2 に記載する．

今回対象とする我々の認証システムは，上述の 3 種類の認証手段をユーザが選択できるシステムとなっている．

2.2 WebAuthn ベースの生体認証の概要

ここでは，WebAuthn の認証技術について述べ，次に，Yahoo! JAPAN ID の認証手段として導入した WebAuthn の実装について述べる．

2.2.1 WebAuthn の認証技術

パスワードの課題に対して，パスワードへの依存度を減らしながら，利便性と安全性を同時に解決するのが WebAuthn の認証技術である [21]．WebAuthn は，WebAuthn の認証技術を主要な Web プラットフォーム（OS や Web ブラウザーなど）に組み込み，ユーザがデバイスを購入すれば直ちに利用できる環境にしていく方針に従って策定された．現在，Chrome，Edge，Firefox，Safari などの主要ブラウザーが標準機能として WebAuthn の機能をサポートしており，普及が見込まれる．

WebAuthn の認証の特徴を，パスワード認証の手順と比較して説明する．パスワード認証では，ユーザはユーザ ID とパスワード情報を，通信路を介して認証サーバに対して送付していた．認証サーバは受け取った ID を識別し，パスワード情報が先の ID にひも付いた適切な情報であるか否かを検証する．この場合，ユーザのパスワード情報は，あらかじめ認証サーバが保管し，識別と検証の処理は認証サーバで行う．

一方 WebAuthn では，ユーザのデバイスなど手元にある「認証器」が，ユーザの本人性を検証する機能を持つ．認証器によるユーザの検証結果は認証サーバに送付され，認証サーバは検証結果の妥当性を確認し，認証が完結する．よって WebAuthn の認証では，ネットワーク上にクレデンシャル情報が流れることはない．

以下，WebAuthn の認証の詳細を説明する． 概要を図 1 に示す．

WebAuthn の認証の大きな特徴は，ユーザの検証結果の

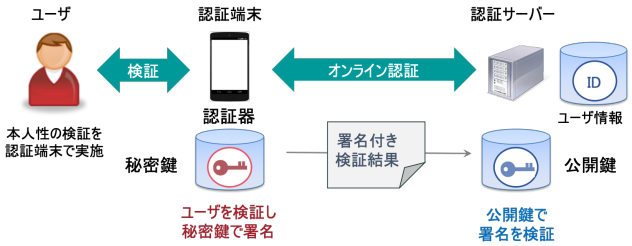

図 1　WenAuthn の認証の概要

図 2　Yahoo! JAPAN の生体認証の画面遷移

妥当性確認のために，公開鍵暗号方式を活用している点にある．ユーザは，認証のために認証器を使って認証用の秘密鍵と公開鍵のペアを作成し，秘密鍵は厳正に保管する．公開鍵は WebAuthn の認証に対応した認証サーバに ID と関連づけて保管する．秘密鍵は，TEE (Trusted Execution Environment) など，通常の動作領域とハードウエア的にも隔離された安全な領域に保管することが想定されている．つまり，秘密鍵が認証器から外に漏えいすることはないように管理する．認証の際に認証サーバは，一度だけ有効なランダムな文字列 (チャレンジ) を認証器に送付する．認証器は，ユーザの本人性を検証できた場合に，このチャレンジに対して保管していた秘密鍵で署名を生成し，署名付きのチャレンジを認証サーバに返送する．認証サーバは，秘密鍵に対応した先の公開鍵を用いて署名検証を行い，適切な署名である場合にのみ認証は成功する．公開鍵を用いて適正な署名であることを検証できれば，その公開鍵とペアの秘密鍵を確かに所持しているということを暗号学的に確かめることが可能となる．また，秘密鍵と公開鍵のペアは，ユーザと登録した認証サーバにだけ有効な情報となり，ユーザの複数のアカウントやサーバ間で共有されない．異なる認証サーバには異なる鍵ペアが発行されるため，ユーザのプライバシーにも配慮した方式になっている．

また WebAuthn 仕様では，Web ブラウザから上記ユーザの秘密鍵に汎用的にアクセスするために，Web アプリケーション向けの Web Authentication API を規格化している．これにより，ユーザの Web ブラウザは JavaScript で認証器を呼び出し，認証サーバと通信のやり取りができるようになるため，専用ソフトウエアを自ら配布する必要性がなくなるメリットがある．

WebAuthn が呼び出す認証器は主に生体認証が想定されているが，それ以外の様々な認証手段が包含されている．また，生体認証が呼び出された際，生体認証が一時的に利用できない場合などに生体認証以外の PIN コードによる認証等が利用される場合もある．これらを含めて，主に生体認証を対象とした WebAuthn ベースの認証を以下生体認証と記述する．

2.2.2　Yahoo! JAPAN ID システムの生体認証

Yahoo! JAPAN ID の認証システムは，2018 年 10 月にサービス事業者として世界に先駆けて WebAuthn ベースの生体認証が行えるシステムを開発し商用導入した[*1]．一度認証器の登録をすれば，以降は同端末を用いてパスワードなしでログインできる仕組みとなっている．画面遷移の様子を図に示す．認証が必要な際，(1) 認証画面において「次へ」をタップすると，(2) 指紋の入力による本人確認が求められ，(3) 指紋が確認されれば認証が完了する．この間，利用者によるパスワード入力欄をなくし，WebAuthn ベースの生体認証のみでシンプルにログイン/本人確認ができるようになる．対応環境は，導入時点で利用可能となっていた Android OS かつ，Android の代表的なウェブブラウザである Google Chrome[*2]となっている．

2.3　認証手段の比較

ここでは，Bonneau らの定義した評価基準 [9] を用い我々のシステムの 3 種類の認証手段 (生体認証，パスワード認証，SMS 認証) を比較する．ここで，生体認証は認証を実施する端末に内蔵されている認証器 (Platform Authenticator) を対象としている．

表 1 にまとめた結果を示す．パスワード認証と SMS 認証の評価結果は，Lang らが記述した内容 [12] を引用している．

ユーザビリティに関しては，まず，ユーザの記憶が不要，またそれに伴ってスケーラブルであるという点から，生体認証と SMS 認証が U1 と U2 において優れている．次に，U4 については生体認証が例えば，指紋認証ではタップのみ，顔認証については動作なしで認証を行えるため優れている．また，U6，U7 の項目について， 3.2 で後述するシステムログの認証時間と認証成功率の評価の結果も反映して記載した．

導入しやすさにおいては，パスワード認証について専門の装置や外部の仕組みを必要としないため最も良い結果となっている．一方で，生体認証に関しても，生体認証の認証器は必要となるものの，WebAuthn の標準仕様に従って

*1　https://about.yahoo.co.jp/pr/release/2018/10/231023/a/
*2　Android 7.0 以上かつ Chrome70 以上が対象

表 1　Bonneau らの評価基準による WebAuthn を用いた生体認証，パスワード認証，SMS 認証の比較

	Usability benefits								Deployability benefits						Security benefits										
Scheme	U1 Memorywise-Effortless	U2 Scalable-for-Users	U3 Nothing-to-Carry	U4 Physically-Effortless	U5 Easy-to-learn	U6 Efficient-to-Use	U7 Infrequent-Errors	U8 Easy-Recovery-from-Loss	D1 Accessible	D2 Negligible-Cost-per-User	D3 Server-Compatible	D4 Browser-Compatible	D5 Mature	D6 Non-Proprietary	S1 Resilient-to-Physical-Observation	S2 Resilient-to-Targeted-Impersonation	S3 Resilient-to-Throttled-Guessing	S4 Resilient-to-Unthrottled-Guessing	S5 Resilient-to-Internal-Observation	S6 Resilient-to-Leaks-from-Other-Verifiers	S7 Resilient-to-Phishing	S8 Resilient-to-Theft	S9 No-trusted-Third-Party	S10 Requiring-Explicit-Consent	S11 Unlinkable
生体認証	●	●	●	●	○	●	○	○	○	○		●	●	●	●	●	●	●	●	●	●	○	●	●	●
パスワード認証			●		●	●	○	●	●	●	●	●	●	●		○			●	●	●	●	●	●	●
SMS 認証	●	●	○		●		○	○	○			●	●	●	●	●	●	●	●	●		○		●	●

● = offers the benefit; ○ = almost offers the benefit; no circle = does not offer the benefit.

いるため D3 や D4 に関して優れている．

セキュリティに関しては，生体認証と SMS 認証が優れている点が多く，パスワードの課題を解決している様子が分かる．

以上から，我々の認証システムが導入した生体認証について，主にユーザビリティとセキュリティに関して，パスワード認証よりも優れていると評価できることが確認できた．

3. ユーザビリティ評価

3.1 ユーザビリティ評価の概要

この章では，我々の認証システムにおける 3 種類の認証手段のユーザビリティに関して行った評価実験を説明する．まず，ユーザビリティが認証システムに与える影響を定量的に評価するため，当該認証システムのシステムログを上記 3 種類の認証手段ごとに解析した．次に，定性的なユーザへの影響を評価するため，クラウドソーシングによるユーザアンケートを実施した．

3.2 システムログ解析によるユーザビリティ評価

3.2.1 タスク設計

ユーザビリティが認証システムに与える影響を表す評価指標として，認証時間（以下，Authentication time: AT）と認証成功率（Authentication Success Rate: ASR）の 2 つを調査した．

我々は，当該認証システムの認証サーバからシステムログを取得して，生体認証，パスワード認証，SMS 認証の 3 つの認証方法で AT と ASR を計算した．システムログは 2019 年 12 月の 1 ヶ月分を取得して解析した． 本解析は，Yahoo! JAPAN のプライバシーポリシー[*3]に従って実施した．

AT は，取得したシステムログから，認証の開始ページの表示時間と完了ページ表示時間を取得し，表示時間の差を計算して求めた．今回，取得する表示時間は秒単位としたため，AT の値は秒単位となる．ASR は，取得したシステムログから，認証を開始したユーザと完了したユーザを取得し，開始したユーザ中の完了したユーザの割合を計算して求めた．

3.2.2 結果

図 3 に，比較対象の 3 つの認証手段 (生体認証，パスワード認証，SMS 認証) それぞれの AT の解析結果をヒストグラムで表示する．実線，破線，点線はそれぞれ平均値，中央値，最頻値を表す．平均値，中央値，最頻値の値は表 2 に示す．平均速度，中央値は生体認証が最も速いという結果が得られた．また，図 3 から，パスワード認証と SMS 認証の曲線は非常に緩やかで分散が大きいのに対し，生体認証は分散が小さく，多くのユーザは 3-8 秒で認証が完了している様子がわかる．加えて，88% のユーザは 10 秒未満で認証が完了していることから，生体認証が多くのユーザビリティを速度面において他の認証手段よりも優れていることが確認できた．

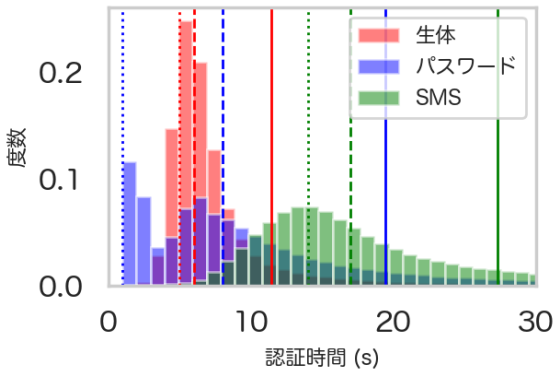

図 3　認証速度の比較)

*3　https://about.yahoo.co.jp/common/terms/chapter1/#cf2nd

表 2　認証速度の平均値，中央値，最頻値 (second)

	平均値	中央値	最頻値
パスワード認証	19.4	8	1
SMS 認証	27.3	17	14
生体認証	11.4	6	5

図 4 に各認証手段の ASR を日次で集計し，平均した結果を示す．平均値はそれぞれ，生体認証が 77.0%，パスワード認証が 72.2%，SMS 認証が 73.2%となり，ASR においても生体認証が最も良い結果を有意に得ることができた．

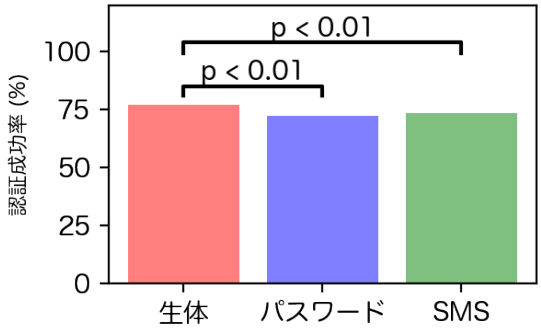

図 4　認証成功率の比較

3.3　クラウドソーシングによるユーザビリティ評価

上記システム解析に加え，Yahoo!クラウドソーシング[*4]のサービスを利用し，インターネットを通じた被験者 (クラウドワーカー) を対象に各 3 種類の認証手段に対するアンケートを行った．アンケートは SUS (3.3.1 参照) のフレームワークに則って作成し，3.3.2 に記述する方法でクラウドワーカーに提示した．

3.3.1　SUS スコア

System Usability Scale (SUS) [4] とは，Web サービスのユーザビリティを定量的に測定するフレームワークである．クラウドソーシングのタスクで設定した設問のインデックスを i，クラウドワーカーが回答した各設問のスコア x_i とする． 各設問に対してスコア s_i を以下のように計算する．

$$s_i = \begin{cases} x_i - 1 & (i \in \{1,3,5,7,9\}), \\ 5 - x_i & (i \in \{2,4,6,8,10\}). \end{cases} \quad (1)$$

各問題の変換した点数を合計し，2.5 倍して SUS の点数 SUS を以下の通り求める．

$$SUS = 2.5 * \sum_{i=1}^{10} s_i. \quad (2)$$

3.3.2　タスク設計

今回のユーザビリティ調査では下記のような設計でクラウドワーカーへの質問及び SUS の算出を行った．

タスクの提示方法

[*4] https://crowdsourcing.yahoo.co.jp/

今回実施したクラウドソーシングの説明ページでは，クラウドワーカーは下記のような指示を受ける．

> 【生体認証によるログイン機能の利用者限定】ユーザビリティーの調査
> ヤフーの各サービスを利用する際の、生体認証によるログイン機能のユーザビリティーに関するアンケートです。 以下の生体認証に関するヘルプページを参照した上でお答えください。 ※本アンケートは生体認証によるログイン機能の利用者限定です。

Web サービスのユーザビリティはヘルプページの内容にも関係があるため，それぞれの認証手段の実際のヘルプページをインストラクションとして利用した．

設問の設計

SUS の手法に則り，SUS の設問は下記のように設定した．[認証手段] には各対応する認証手段の名称が入る．

(S1) [認証手段] によるログインを利用するためのナビゲーションは十分に統一感があると感じた．
(S2) [認証手段] によるログインのナビゲーションには一貫性のないところが多々あったと感じた．
(S3) 多くの人は、[認証手段] によるログインの操作方法をすぐに理解すると思う．
(S4) ウェブサービスを利用する際には，[認証手段] によるログインはとても操作しづらいと感じた．
(S5) どんな人でも，[認証手段] によるログイン機能は容易に使いこなす事ができると思う．
(S6) [認証手段] によるログイン機能を利用するにはサービスのサポートが必要だと感じる．
(S7) ウェブサービスを利用する際には，[認証手段] によるログインを活用できると確信する．
(S8) ログイン時に [認証手段] の利用するには知っておくべきことが多くあると思う．
(S9) ログインしてウェブサービスを利用する際には [認証手段] を利用したいと思う．
(S10) [認証手段] によるログインを利用するには説明が必要となるほど複雑であると感じた．

設問は 1-5 点の Likert scale[*5]で解答を依頼する．これらの設問をパスワード認証，SMS 認証，WebAuthn による生体認証の 3 つの認証手段それぞれに対して用意し，各クラウドワーカーが使用している認証手段に対して質問し解答を得た．

認証のユーザビリティに関する 10 の設問以外にユーザの性別，年齢に関する属性情報，およびコンピュータに関する知識をどれくらい有するかを回答してもらった． コンピュータの専門知識に関するレベルは 3 段階 (上級，中

[*5] 1 点は設問に対して “非常にそう思わない” を示し，5 点は “非常にそう思う” を示す．

級，初級) で回答してもらった．また，認証のユーザビリティに関する意見を自由に記述できる入力フォームも用意した．

クラウドソーシングでは解答が非常に容易な設問をダミー設問として意図的に設問にまぜ，それに正しく回答を行っているかを確認することにより悪質なクラウドワーカー (設問を読まずにランダムに解答する等のクラウドワーカー) を排除することが行われる．今回も，上記の 10 の設問にダミーの設問を追加し，ユーザには実際の 10 の設問に対しダミー設問を 1 つ解答を依頼している．ダミー設問に正しく解答していないクラウドワーカーには報酬を与えず，今回のユーザビリティ評価の対象からも除外する．

対象クラウドワーカーの選定方法

3 つの認証手段それぞれに用意したクラウドソーシングタスクに解答を依頼するため，各認証手段を使用するクラウドワーカーの選定が必要となる．我々の認証システムでは複数の認証手段を同時に利用可能に設定できるため，今回は以下の条件で 3 つのグループを抽出し，それぞれの認証手段を主に利用しているクラウドワーカーに絞った．

(A) 生体認証を設定しており，SMS 認証を設定していない
(B) SMS 認証を設定しており，生体認証を設定していない
(C) SMS 認証も生体認証も設定していない

生体認証，SMS 認証，パスワード認証のユーザビリティを評価するための条件として，グループ (A)，(B)，(C) をそれぞれ使用した．2019 年 10-12 月のシステムログから各認証方法を使用したユーザを選定した．

クラウドワーカーへの報酬

クラウドワーカーへの報酬は，この種のアンケートの一般的な報酬を参照し，T ポイント[*6]を 4 ポイントと設定した．

3.3.3 結果

今回の調査では，パスワード認証が 18 人，SMS 認証が 6 人，生体認証が 19 人を対象に解答を得た．クラウドワーカーの性別は，男性が 22 人 (70%)，女性が 9 人 (29%) であった．年齢は，18〜25 歳が 25 人 (80%)，26〜35 歳が 4 人 (12%)，46〜55 歳が 2 人 (6%) となり若年層が多くなった．また，ほとんどのクラウドワーカーは中級レベルのコンピュータの専門知識を持っていると解答した：初心者 9 人 (29 %)，中級 18 人 (58%)，上級 4 人 (12%)．

図 5 に，3 つの認証手段ごとに計算した SUS スコアの平均値を示す．パスワード認証の平均 SUS スコアは 58.6，標準偏差は 15.6 となり 3 つ認証手段のうち最も低くなった．SMS 認証の平均 SUS スコアは 67.1，標準偏差は 17.7，生体認証の平均 SUS スコアは 68.3，標準偏差は 15.1 となり，SMS 認証と生体認証の間には有意差がないという結果になったが，これら 2 つの認証手段はパスワード認証と比較するとユーザビリティが良いと解答されたということを示す結果になった．

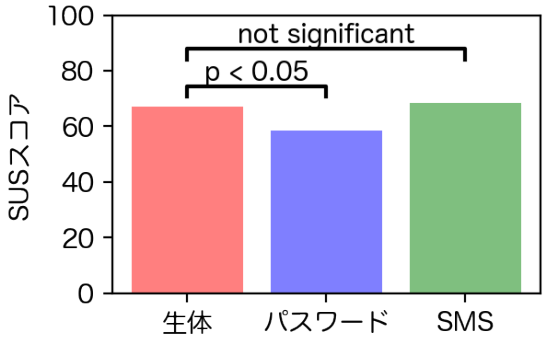

図 5 SUS の比較

図 6 に 10 個の設問ごとの式 (1) の平均のスコアを 3 種類の認証手段についてまとめたグラフを示す．

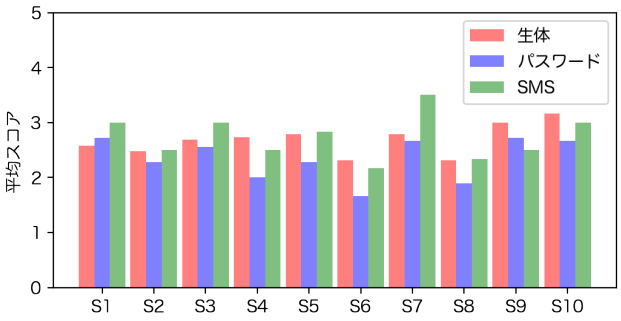

図 6 設問ごとの平均スコアの比較

すべての設問について，パスワード認証のスコアが最大になることはなかった．生体認証は (S4)，(S9)，(S10) で最も良くなった．SMS 認証については，(S1)，(S2)，(S3)，(S5)，(S6)，(S7)，(S8) の設問について最も良い結果が得られた．

4. 考察

システムログ解析から，生体認証はその他の認証手段と比較して認証時間と認証成功率の両方について最も良い結果が得られた．また，クラウドソーシングによる定性的なユーザビリティ調査の結果，生体認証の SUS スコアは SMS 認証と比較して有意差なし，パスワード認証と比較して良いという結果が得られた．以上の調査から，我々が展開する認証システムでは，生体認証は，その他の認証手段と比較して良いユーザビリティを提供できていると考える．

以下にさらなる研究トピックに対する考察と今後の課題について議論する．

*6 https://tsite.jp/r/guide/web/index.html

4.1 パスワードの入力補完機能

図 3 中のパスワード認証のヒストグラムを見ると，約 1 秒の箇所にもピークがあり，表 2 ではパスワード認証の最頻値は 1 秒となっている．このような短時間でパスワード認証を行うユーザは，ブラウザのパスワード保存機能やパスワード管理ツールによる自動補完機能を使用しているのではないかと想定する．自動補完機能を利用して非常に高速にパスワード認証を行うユーザのユーザエクスペリエンスは，生体認証よりも優れている可能性がある．上記のような補完機能を利用してパスワード認証を行っているユーザは，ある程度 PC やブラウザの操作に詳しい一部のユーザであると考えられるが，今回の評価ではパスワード認証の評価を補完機能を使うか否かで分けることなく一律で評価を行ったため，これらのユーザも含まれていると考えられる．より正確にユーザビリティを調査するためには，補完機能等の利用の有無を加味するほうが望ましく，今後の研究課題である．

4.2 生体認証の認証速度

図 3 に示されるように，生体認証は多くのユーザが 3-8 秒で完了し，最頻値は 5 秒となっている．近年のスマートフォンにおける指紋認証や顔認証自体の認証時間は非常に短くなってきているが，この結果をみると生体認証には，パスワード認証ほど認証完了までの時間が短いユーザは存在していない．この理由について検証するため，指紋認証を実際に行い，ログイン処理開始から完了まで，各処理にかかる時間を検証した結果下記のようになった（Google Pixel4，wifi 環境で実施）．

- ログインボタンを押してから生体認証を促すダイアログが表示される (認証リクエストを実施する) : 約 1.2 秒.
- 生体認証を実施し完了のダイアログが表示される: (実施するユーザによる)
- ダイアログが自動的に閉じ，ログインページが表示される : 約 1.3 秒.
- ログインが完了しログインページが閉じる: 約 1 秒.

この結果から，ユーザが指紋認証を実施する以外にも，WebAuthn プロトコルによるクライアントとサーバの通信の時間と，インタラクティブな画面の表示のため，今回の検証環境では少なくとも約 3.5 秒が必要であった．認証においては，操作に慣れたユーザにおいてもパスワード認証と比較し，一定の認証時間が必要となるという課題があることがわかったが，一方で，クラウドソーシングで検証した SUS スコアでは生体認証はパスワードより良い結果が得られていることから，この数秒程度のロスはユーザビリティには大きな欠点とはならない可能性がある．

4.3 生体認証の完了率

生体認証の認証完了率は 77%であった．他の認証手段と比較して良い結果ではあったが，まだまだ改善の余地がある．認証が完了しない場合には，生体認証の失敗のみでなく，生体認証をキャンセルした場合やブラウザバックを行った場合等も考えられるが，現状の仕組みではこの内容を取得できていない．生体認証の場合，思わぬタイミングでダイアログが表示されることによる心理的な影響で認証をキャンセルしてしまうことも考えられるため，さらなるユーザエクスペリエンスの向上による認証完了率の改善にはこの内訳がわかるような仕組みを作ることが必要である．

4.4 クラウドソーシングを用いたユーザビリティ評価の比較

生体認証と SMS 認証がパスワード認証よりもよい SUS スコアを得られたことで，パスワードレス認証がユーザビリティに良い影響を与えることが確認できた．

SMS 認証の SUS スコアに関して，SMS を開く・PIN コードを入力するという操作に手間がかかるにも関わらず，生体認証の SUS スコアとあまり有意差がないという結果は, 予想外であった．SMS 認証を行ったクラウドワーカーのコメントを参照すると，SMS は慣れているという意見があった．SMS は普段からユーザが使っている SMS のアプリケーションを利用しており一般的で使いやすいため，SMS に慣れ親しんでいることが，使い勝手の良さにつながるのではないかと考える．さらに，生体認証を行ったクラウドワーカーのコメントに，指紋認証は手が汚れたり手袋をするというようなユーザの状況によって失敗するというものがあった．SMS はユーザの状況に関係がなく，SMS の到達が失敗することはほとんどないため，この点でも SMS 認証と比較して生体認証のユーザビリティが悪いと感じている可能性がある．

5. 関連研究

近年，パスワードに加えて第 2 の要素認証が使用される 2 要素認証 (2FA) のユーザビリティに関する調査が活発に行われている [5–7, 10, 11].

2FA は FIDO Universal 2nd Factor (U2F) [2] メカニズムによって拡張された．公開鍵暗号方式をサポートする「セキュリティキー」によりフィッシングや中間者攻撃から保護される [12, 15]．このような新しい手法はユーザ認証のセキュリティ向上に効果的であるため、ユーザが利用する際のユーザビリティが新たな課題になる．

この課題についても近年いくつかの研究が行われている [13, 14, 16]．Reese ら [14] は，SMS，TOTP，事前生成コード，および U2F セキュリティキーを含む 5 つの 2FA 認証方法を比較した．

WebAuthn [20] は，W3C によって開発およびリリース

された認証標準であり，2 つの認証ケースを更新する：パスワードレスタイプ (FIDO UAF [3]) と 2FA タイプ (FIDO U2F)．この標準により，一般的な Web ブラウザーを介した Web サイトで，パスワードなしでユーザ認証を行えるようになった．WebAuthn を使用し，セキュリティキーを用いた 2FA タイプのユーザビリティ評価はすでに行われている．Lyastani ら [17] は，FIDO2 対応のセキュリティキーを用いた認証と従来的なパスワード認証のユーザビリティを比較する調査研究を実施した．また，Farke Farke2020 らは，小規模な企業システムにおいて，その従業員が FIDO2 対応のセキュリティキーを 6 週間継続的に使用した場合のユーザビリティ実験を実施した．これらの研究はいずれもセキュリティキーを用いた WebAuthn のユーザビリティに関する研究であり，本稿のようなスマートフォンなどのハードウェアに内蔵される認証器を用いたパスワードレス認証に関するユーザビリティ評価は，我々の知る限り調査・報告されていない．

生体認証はユーザ本人の生体情報を利用するため，常に利用可能でありユーザは覚えておく必要がないためユーザビリティが高いとされている．ただし，生体認証は生体情報の所持による認証であるため，物理的またはシステムへの攻撃によって盗まれる可能性があるが，盗難や紛失からの回復は困難であるという結果がある [19]．そのため，多くの場合，堅固なトークンなどの特別なハードウェアに依存した状態でユーザとリンクしている．結果として，生体認証のシステムは，盗難や紛失に対する脆弱性の問題，および導入コストが高いという課題がある．WebAuthn をベースとした生体認証は，これらの課題を解決する．

6. おわりに

システムログ解析とクラウドソーシングによる SUS 評価という 2 つの視点から, 3 種類の認証手段 (生体認証, パスワード認証, SMS 認証) のユーザビリティ調査を実施した，システムログ解析により，認証時間と認証成功率に関して，生体認証がパスワード認証, SMS 認証より優れていることがわかった．クラウドソーシングによる SUS 評価では, 生体認証と SMS 認証がパスワード認証よりもユーザビリティが優れていることが確認できた．以上から, パスワードレス認証は，パスワード認証と比較してユーザビリティが良いことを確認した．

今回の調査で，生体認証の認証速度が一部のパスワード認証のユーザを下回っている点, 生体認証と SMS 認証の SUS スコアに差がなかった点等の課題が明らかになった．今後，これらの課題の原因をより詳細に調査するためのシステムや実験手法の検討を行っていく．

参考文献

[1] Security keys: Practical cryptographic second factors for the modern web. In *Financial Cryptography*, 2016.

[2] FIDO Alliance. FIDO U2F JavaScript API. https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-javascript-api-v1.2-ps-20170411.pdf, 2017.

[3] FIDO Alliance. FIDO UAF Protocol Specification. https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-protocol-v1.1-ps-20170202.pdf, 2017.

[4] J. Brooke. SUS: A Quick and Dirty Usability Scale, 1996.

[5] D. Han *et al.* Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication. In *Proc. MobiCom '18*, pp. 401–415, 2018.

[6] D. Wang *et al.* The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes. In *Proc. ASIA CCS '16*, pp. 475–486, 2016.

[7] E. M. Redmiles *et al.* You Want Me To Do What? A Design Study of Two-Factor Authentication Messages. In *Proc. SOUPS '17*, pp. 1–7, 2017.

[8] F. M. Farke *et al.* "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Proc. SOUPS '20*, 2020.

[9] J. Bonneau *et al.* The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proc. S&P '12*, pp. 553–567, 2012.

[10] J. Colnago *et al.* "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proc. CHI'18*, pp. 1–12, 2018.

[11] J. Dutson *et al.* "Don't punish all of us": Measuring User Attitudes about Two-Factor Authentication. In *Proc. Euro S&PW '19*, pp. 119–128, 2019.

[12] J. Lang *et al.* Security keys: Practical cryptographic second factors for the modern web. In *International Conference on Financial Cryptography and Data Security*, pp. 422–440. Springer, 2016.

[13] J. Reynolds *et al.* A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *Proc. S&P '18*, pp. 872–888, 2018.

[14] K. Reese *et al.* A usability study of five two-factor authentication methods. In *Proc. SOUPS '19*, pp. 357–370, 2019.

[15] R. Macgregor *et al.* Evaluating the Android Security Key Scheme: An Early Usability, Deployability, Security Evaluation with Comparative Analysis. In *Proc. SOUPS '19*, 2019.

[16] S. Ciolino *et al.* Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Proc. SOUPS '19*, pp. 339–356, 2019.

[17] S. G. Lyastani *et al.* Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *Proc. S&P '20*, pp. 842–859, 2020.

[18] S. Ma *et al.* An Empirical Study of SMS One-Time Password Authentication in Android Apps. In *Proc. ACSAC '19*, pp. 339–354, 2019.

[19] S. Mare *et al.* ZEBRA: Zero-Effort Bilateral Recurring Authentication. In *Proc. S&P '14*, pp. 705–720, 2014.

[20] W3C. Web Authentication: An API for Accessing Public Key Credentials – Level 1. https://www.w3.org/TR/webauthn/, 2019.

[21] 五味, 大神. FIDO（ファイド）認証とその技術. 電子情報通信学会論文誌, Vol. 12, No. 2, pp. 115–125, 2018.