クラウドソーシングを用いた WebAuthnベース生体認証のユーザビリティ調査

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

概要：我々は，先行研究で 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，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) で比較して WebAuthn ベー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．本稿では，さらなるユーザビリティの調査のため，クラウドソーシングによるアンケートを活用して，1) パスワード認証に関して，パスワードを手動で入力しているユーザとブラウザやその他ツールの入力補完機能を使用しているユーザ，2) SMS 認証に関して，OTP を手動で入力しているユーザと入力補完機能を使用しているユーザ，3) 生体認証に関して，顔認証や指紋認証等の各認証手段を使用しているユーザ，を識別できる仕組みを提案し，認証手段の利用形態ごとに比較を行った結果，WebAuthn ベー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．

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 using crowdsourcing

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

Abstract: We conducted a study to evaluate usability after introducing passwordless authentication based on Web Authentication (WebAuthn) standardized by W3C in previous research, and confirmed that the usability of WebAuthn-based biometric authentication is superior compared to three types of authentication methods (WebAuthn-based biometric authentication, password authentication and SMS authentication) . In this paper, in order to further investigate usability, we used a questionnaire by cloud sourcing to identify following users: 1) users who manually enter passwords and users who use the completion function of browsers and other tools regarding password authentication. 2) For SMS authentication, users who manually enter OTP and users who use the completion function 3) Regarding biometric authentication, we propose a mechanism that can identify users who are using each authentication method such as face authentication and fingerprint authentication. As a result of comparing each usage pattern of the authentication method, we confirmed that WebAuthn-based biometric authentication improved the usability of user authentication.

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

1. はじめに

様々なサービスを提供する Web システムの増加に伴い，ユーザの認証の機会が増加しているため，セキュリティのみでなく高いユーザビリティを兼ね備えた認証手段を実現することが重要になっている．最も広く使用されているパスワードを用いた個人認証は，パスワードの記憶の困難さや入力の煩雑さなどから，ユーザビリティに関しての問題が報告されている [9]．そのため，パスワードよりも優れたユーザビリティをもつ認証手段を提供するための研究が

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

行われているが，その際にユーザビリティの評価方法自体も研究の対象となっている．

パスワード認証を置き換える認証手段のユーザビリティを評価する試みが行われている．パスワードに加えて，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の第 2 の要素認証が使用される 2 要素認証 [18] のユーザビリティに関する調査が活発に行われている [7]．2 要素認証を公開鍵暗号方式をサポートする仕組みとして拡張する FIDO Universal 2nd Factor（U2F） [2] についてもいくつかのユーザビリティに関する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 によって策定された新しい認証規格が Web Authentication（WebAuthn） [21] である．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，認証の使いやすさが向上すると期待でき，Chrome，Edge，Firefox，Safari などの現在利用者の多いプラットフォームに普及している．

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]．

生体認証を利用した WebAuthn ベースの認証に関しては，我々の研究グループが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) のユーザビリティの比較を行った [22]．この研究で WebAuthn ベースの生体認証のユーザビリティがパスワード認証と比較して優れていることを確認したが，下記のように各認証手段ごとにユーザの利用形態の詳細な区別を行い，より正確に解析・比較することが課題となっていた．

(1) パスワード認証に関して，パスワードを手動で入力しているユーザとブラウザやその他ツールの入力補完機能を使用しているユーザ
(2) SMS 認証に関して，OTP を手動で入力しているユーザと入力補完機能を使用しているユーザ
(3) 生体認証に関して，顔認証や指紋認証等の各認証手段を使用しているユーザ

そこで，本稿では，大規模なクラウドソーシングを使用したアンケートにより評価対象者を募集し，SUS スコアによるユーザビリティ評価，そしてシステムログの評価を組み合わせた手法で各認証手段のユーザビリティのさらなる評価を実施する．

本稿の貢献は下記の通りである．

(1) WebAuthn ベースの生体認証のユーザビリティを評価するため，大規模なクラウドソーシングによるアンケートと SUS 評価，システムログ解析を行う手法でパスワード認証，SMS 認証と詳細に比較するユーザビリティ調査を実施した．
(2) 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. 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 [1,5–7,10,11]．

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 [21] 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 ら [8] 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る．Oogami ら [20] は，本稿と同様に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を行い，WebAuthn の認証器登録においてユーザビリティ上の課題を報告している．

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．

3. 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．我々の先行研究 [22] と基本的に同様のシステム構成で解析を行った．

3.1 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??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．

3.1.1 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．現在，Android OS かつ，Android OS の代表的なウェブブラウザである Google Chrome と，iOS かつ，iOS の代表的なウェブブラウザである Safari が対応環境となる．

図 1 Yahoo! JAPAN の生体認証の画面遷移

4. ユーザビリティ評価

4.1 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，今回のユーザビリティ評価の評価対象ユーザを得るため，クラウドソーシングによるアンケートを実施する．アンケートは対象を限定せずに回答を募集し，利用している認証手段や認証手段ごとの利用形態に関する質問を行う．次に，定性的なユーザへの影響を評価するため，評価対象ユーザには合わせて SUS スコアを計算するための質問を行いそれによりユーザビリティの評価を行う．最後に，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，評価対象ユーザに対する当該認証システムのシステムログを取得し認証手段・利用形態ごとに解析した．

4.2 クラウドソーシングによるアンケート調査

今回，Yahoo!クラウドソーシング[*2]のサービスを利用し，インターネットを通じたクラウドワーカーを対象にアンケートを行った．

4.2.1 クラウドソーシングのタスク設計

クラウドソーシングを利用したユーザビリティ調査は下記のような設計でクラウドワーカーへアンケートを行った．

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．

[*1] https://about.yahoo.co.jp/pr/release/2018/10/231023/a/

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

ヤフーのログインのユーザビリティー調査
ヤフーの各サービスを利用する際の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．以下の設問にお答えください．

アンケートは下記のような構成とした．

(1) クラウドワーカーの属性に関する質問
(2) ヤフーのログイン時に利用している認証手段と利用形態に関する質問
(3) System Usability Scale (SUS) のスコアを計算するための質問

それぞれの詳細については次章で紹介する．このタスクがYahoo!クラウドソーシング上に表示され，クラウドワーカーが自発的にこのタスクを実施することを選択し，アンケートに回答する．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，PayPay ボーナス[*3]を 5 ポイントと設定した．

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，上記の設問にダミーの設問を追加し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．

4.2.2 クラウドワーカーの属性に関する質問

設問の設計

クラウドワーカーの属性について下記の設問を設定した．

(S1-1)性別
(S1-2)年代
(S1-3)職業
(S1-4)1 日あたりのインターネット利用時間

1 日のインターネット利用時間は，インターネットに関する知識の習熟度の指標として質問した．

結果

今回の調査では，7697 人の回答が得られた．各設問ごとの回答を統計した結果を表 1 から表 4 に示す．

クラウドワーカーの性別は，男性が 53%，女性が 45% ，年代は，30-50 代の層が多くなった．職業は会社員が多く，1 日インターネット利用時間は，大部分が 1 時間以上となりインターネットの熟練度は高いユーザー層となった．

4.2.3 利用している認証手段と利用形態に関する質問

設問の設計

ヤフーのログインに使用している認証手段と各認証手段の利用形態に関する質問を行う．こちらの質問を行うことにより，先行研究 [22] で明らかにできなかった各認証手段の利用形態ごとのユーザビリティを調査することを目的とする．今回クラウドワーカーごとに区別したい利用形態は下記の通りである．

(1) パスワード認証に関して，パスワードを手動で入力しているユーザとブラウザやその他ツールの入力補完機能を使用しているユーザ
(2) SMS 認証に関して，OTP を手動で入力しているユーザと入力補完機能を使用しているユーザ
(3) 生体認証に関して，iOS/Android それぞれの顔認証や指紋認証等の各認証手段を使用しているユーザ

上記を満たすように作成した設問と選択肢の内容を下記に示す．

(S2-1)ヤフーのログインを主にどの認証手段で行っていますか．複数お使いの方は最も利用されている手段を一つだけお答えください．(選択肢：パスワード・SMS・生体認証)
(S2-2)パスワード認証の場合，パスワードの入力補完機能をつかっていますか．(選択肢：ブラウザの入力補完機能をつかっている・ブラウザ以外の入力補完ツールをつかっている・入力補完機能はつかっていない・わからない)
(S2-3)SMS 認証の場合，確認コードの入力補完機能をつかっていますか．(選択肢： 入力補完機能をつかっている・入力補完機能をつかっていない・わからない)
(S2-4)生体認証の場合，どの生体認証をつかっていますか．(選択肢： Android で顔認証・Android で指紋認証・iOS で顔認証・iOS で指紋認証・その他の生体認証)

認証手段に関しては本研究の対象のパスワード認証・SMS

表 1 性別の設問結果

性別	割合 (%)
男性	52.60
女性	45.23
教えたくない	2.17

表 2 年代の設問結果

年代	割合 (%)
10 代	2.33
20 代	9.69
30 代	22.52
40 代	33.71
50 代	21.92
60 代以上	8.33
教えたくない	1.51

表 3 職業に関する設問結果

職種	割合 (%)
会社員	54.22
該当なし	18.63
専業主婦（主夫）	14.84
自営業	8.04
学生	4.27

表 4 1 日のインターネット利用時間に関する設問結果

時間	割合 (%)
1 時間未満	8.03
1 時間〜2 時間未満	30.52
2 時間〜3 時間未満	27.00
3 時間〜4 時間未満	13.42
4 時間以上	21.03

[*3] https://paypay.ne.jp/help/c0048/

認証・生体認証を選択肢とした．S2-2, S2-3 については入力補完機能を知らない可能性を考え，わからないの選択肢を用意した．S2-4 に関しては利用可能となっている生体認証の認証器の中で主に利用されている 4 つの認証手段とその他の選択肢という形で用意した．

結果

各設問ごとの回答の統計を表 5 から表 8 に示す．S2-1 の設問の結果として認証手段はパスワードの回答が 53%と最も多くなり，つづいて SMS 認証，生体認証となった．

表 5 認証手段の設問結果

認証手段	割合 (%)
パスワード	53.10
SMS	33.36
生体認証	13.54

S2-2 の結果を表 6 に示す．「ブラウザの入力補完機能をつかっている」と回答したユーザが最も多く，46%であった．「ブラウザ以外の入力ツールをつかっている」との回答と合わせると 50%以上のユーザーがパスワード入力を補完する機能を活用していることになり，ユーザビリティを評価する上で大きな影響があることがわかった．

表 6 パスワード認証の利用形態の設問結果

利用形態	割合 (%)
ブラウザの入力補完機能をつかっている	46.22
ブラウザ以外の入力補完ツールをつかっている	5.25
入力補完機能はつかっていない	27.33
わからない	21.21

S2-3 の結果を表 7 に示す．「入力補完機能をつかっている」と回答したユーザが最も多く，43%であった．パスワードに続き，SMS も我々の想定より多くのユーザが補完機能をつかっていることが確認でき，ユーザビリティを評価する上で考慮の必要があることが確認できた．

表 7 SMS 認証の利用形態の設問結果

利用形態	割合 (%)
入力補完機能をつかっている	43.47
入力補完機能をつかっていない	35.31
わからない	21.22

S2-4 の結果を表 8 に示す．「iPhone で指紋認証」が最も多く，38%程度であった．「iPhone で顔認証」，「Android で指紋認証」も 30%程度の割合の回答となり多くのユーザが利用していることが確認できた．「Android で顔認証」は，現在の多くの Android 端末に指紋認証器がついているため，利用ユーザが少ないと考えられる．「Android で顔認証」は，十分な回答数が得られなかったため，以降の解析では除外することとした．

表 8 生体認証の利用形態の設問結果

利用形態	割合 (%)
iPhone で指紋認証	37.90
iPhone で顔認証	28.17
Android で指紋認証	30.66
Android で顔認証	2.42
その他の生体認証	0.85

4.2.4 SUS のスコアを計算するための質問

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．今回のユーザビリティ調査のためのアンケートは，この手法を採用し実施した．

設問の設計

設問は SUS のフレームワークに則って作成し，クラウドワーカーに提示した．SUS の設問は下記のように設定した．

(S3-1)ヤフーのログインの手順は十分に統一感があると感じた．
(S3-2)ヤフーのログインの手順には一貫性のないところが多々あったと感じた．
(S3-3)たいていの人は，ヤフーのログインの手順をすぐに理解すると思う．
(S3-4)ヤフーのログインはとても操作しづらいと感じた．
(S3-5)どんな人でも，ヤフーのログインを容易に使いこなす事ができると思った．
(S3-6)ヤフーのログインを利用するには専門家のサポートが必要だと感じる．
(S3-7)ヤフーのログインを使える自信がある．
(S3-8)ヤフーのログイン時に知っておくべきことが多くあると思う．
(S3-9)ログインしてヤフーを利用する際に今後も同じ認証方法を利用したいと思う．
(S3-10)ヤフーのログインの手順は過剰に複雑であると感じた．

各設問は 1-5 点の Likert scale[*4]で解答を依頼する．これらの設問を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．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．

SUS スコアの計算方法

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

[*4] 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．

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 100 点満点で以下の通り求める．

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

結果

S2-1 の回答に基づき，各認証手段ごとに SUS スコアを計算した結果を図 2 に示す．パスワード認証が 63.5，SMS 認証が 62.9，生体認証が 65.5 と生体認証が有意に最も良い結果となった (p ¡ 0.05, 以下，Mann-Whitney U test で検証)．生体認証がパスワード認証よりよい SUS が得られることは先行研究と同じ結果となった．

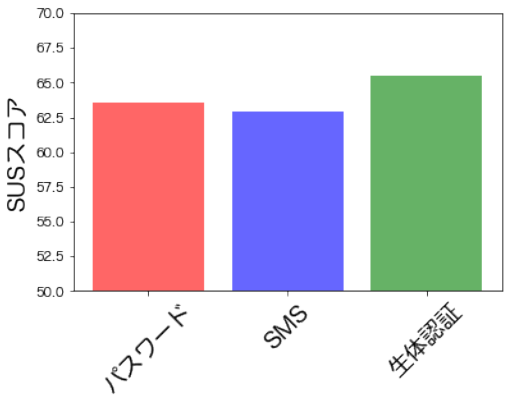

図 2 認証手段ごとの SUS スコアの比較

S2-2 の回答に基づき，パスワード認証の利用形態ごとに SUS スコアを計算した結果を図 3 に示す．「ブラウザの入力補完機能をつかっている」と回答したユーザが最も良いスコアが得られた (p ¡ 0.05)．しかし，「ブラウザ以外の入力ツールをつかっている」の回答の SUS スコアが最も低く，この点は想定外の結果となった．一方で，上記どちらも「入力補完機能をつかっていない」と比較して大きなスコアの開きがなく，パスワード入力の有無のみがユーザビリティに影響するわけではないということがわかった．

S2-3 の回答に基づき，SMS 認証の利用形態ごとに SUS スコアを計算した結果を図 4 に示す．「入力補完機能をつかっている」の SUS スコアが「入力補完機能をつかっていない」より優れたスコアとなり想定通りの結果が確認できた (p ¡ 0.05)．

S2-4 の回答に基づき，生体認証の利用形態ごとに SUS スコアを計算した結果を図 5 に示す．「iPhone で指紋認証」，

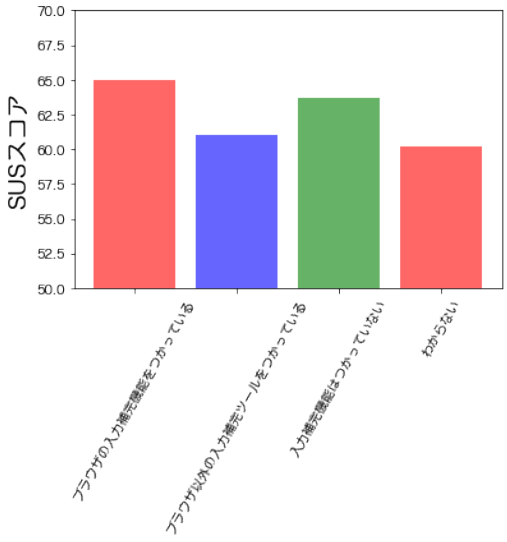

図 3 パスワード認証の SUS スコアの比較

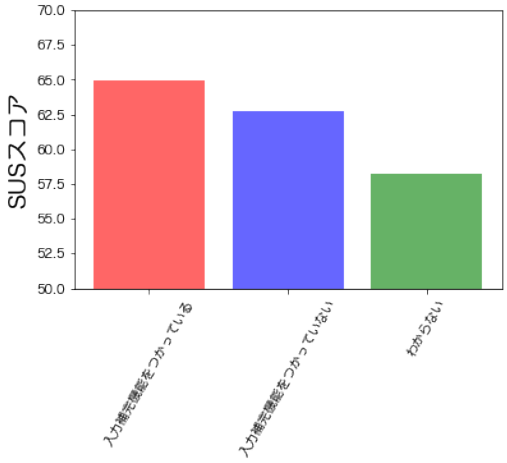

図 4 SMS 認証の SUS スコアの比較

「iPhone で顔認証」，「Android で指紋認証」それぞれ 65，有意差はみられなかった．現状普及している生体認証の認証手段ごとのユーザビリティに大きな差がないことが確認できた．

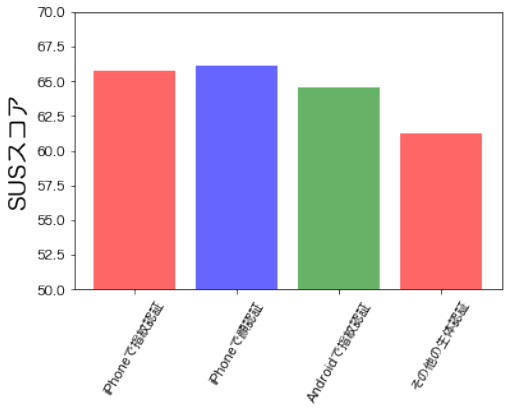

図 5 生体認証の SUS スコアの比較

4.3 システムログ解析によるユーザビリティ評価

4.3.1 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，認証時間を調査した．今回我々は，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，4.2.1 で回答が得られたクラウドワーカーごとに認証速度を取得し，生体認証，パスワード認証，SMS 認証の 3 つの認証手段をつかっているグループごとに集計を行った．システムログは 2021 年 6 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[*5]に従って実施した．認証時間は，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，認証時間の値は秒単位となる．

4.3.2 結果

図 6 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) それぞれの認証速度の解析結果をヒストグラムで表示する．点線はそれぞれ平均値を表す．平均値，中央値，最頻値の値は表 9 に示す．今回も平均速度，中央値は生体認証が最も速いという結果が得られた，その他の認証手段に関しても同様の傾向が見られることが確認できた．特にパスワード認証に関して，約 1-2 秒の非常に高速な箇所にもピークがあることも確認できた．

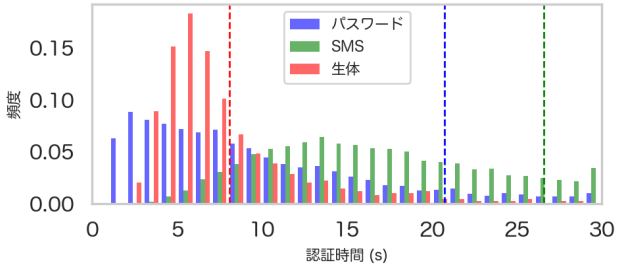

図 6 認証速度の比較

表 9 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	20.7	9.0	2
SMS 認証	26.6	18.0	13
生体認証	8.1	6.0	5

S2-2 の回答に基づき，パスワード認証の利用形態ごとに認証速度を計算した結果を図 7 に示す．平均値，中央値，最頻値の値は表 10 に示す． この結果から，図 6 でも確認したパスワードの非常に高速な箇所のピークは，主にパスワードの補完機能を利用しているユーザによるものであることが確認できた．

S2-3 の回答に基づき，SMS 認証の利用形態ごとに認証速度を計算した結果を図 8 に示す．平均値，中央値，最頻値の値は表 11 に示す． こちらも入力補完機能を利用しているユーザの認証速度が高速であることが確認できた．

[*5] https://about.yahoo.co.jp/common/terms/chapter1/#cf2nd

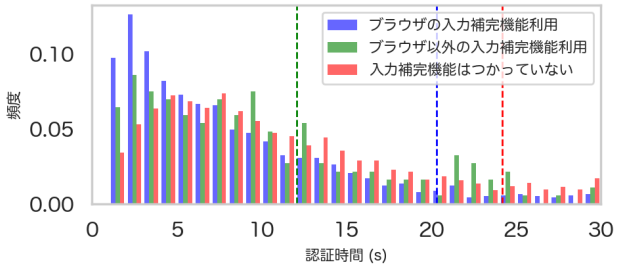

図 7 パスワード認証速度の比較

表 10 パスワード認証速度の平均値，中央値，最頻値 (second)

	平均値	中央値	最頻値
ブラウザの入力補完機能利用	20.3	7.0	2
ブラウザ以外の入力補完機能利用	12.1	9.0	2
入力補完機能はつかっていない	24.2	11.0	7

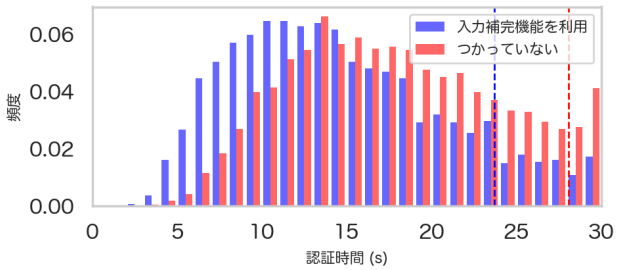

図 8 SMS 認証速度の比較

表 11 SMS 認証速度の平均値，中央値，最頻値 (second)

	平均値	中央値	最頻値
入力補完機能を利用	23.7	15.0	10
つかっていない	28.1	20.0	13

S2-4 の回答に基づき，生体認証の利用形態ごとに認証速度を計算した結果を図 9 に示す．平均値，中央値，最頻値の値は表 12 に示す．生体認証の認証手段ごとに比較すると，各ヒストグラムの山の傾向は似ており，6-7 秒程度にピークがあることが確認された．生体認証の手段ごとに比較して認証スピードは大きく変わらないことが確認できた．

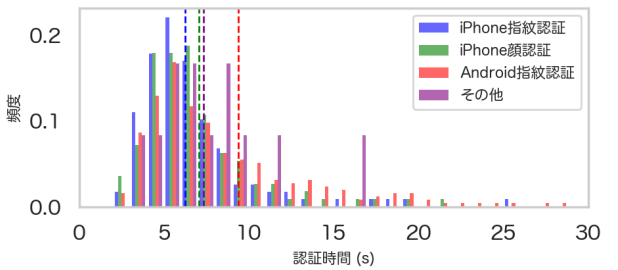

図 9 生体認証速度の比較

表 12 生体認証速度の平均値，中央値，最頻値 (second)

	平均値	中央値	最頻値
iPhone 指紋認証	6.2	5.0	5
iPhone 顔認証	7.1	6.0	6
Android 指紋認証	9.4	6.0	5
その他	7.3	6.5	8

5. おわりに

先行研究で 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，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) で比較して WebAuthn ベー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．本稿では，さらなるユーザビリティの調査のため，クラウドソーシングによるアンケートを活用して，1) パスワード認証に関して，パスワードを手動で入力しているユーザとブラウザやその他ツールの入力補完機能を使用しているユーザ，2) SMS 認証に関して，OTP を手動で入力しているユーザと入力補完機能を使用しているユーザ，3) 生体認証に関して，顔認証や指紋認証等の各認証手段を使用しているユーザ，を識別できる仕組みを提案し，認証手段の利用形態ごとに比較を行った結果，WebAuthn ベー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．

参考文献

[1] Jacob Abbott and Sameer Patil. How Mandatory Second Factor Affects the Authentication User Experience. In *Proc. CHI '20*, pp. 1–13, 2020.

[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] W. Oogami, H. Gomi, S. Yamaguchi, S. Yamanaka, and T. Higurashi. Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones. In *Proc. SOUPS '20*, 2020.

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

[22] 山口修司, 日暮立, 五味秀仁, 大神渉. 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. コンピュータセキュリティシンポジウム 2020 論文集, pp. 704–711, October 2020.