

IT 企業内認証の利便性評価観察

大神 渉^{1,a)} 五味 秀仁^{1,b)} 山口 修司^{1,c)} 日暮 立^{1,d)}

概要：W3C(World Wide Web Consortium) が標準化した Web Authentication (WebAuthn) API を利用し生体認証などで安全に Web ページへのログインする方法が提供されており、我々の以前の研究では、WebAuthn はパスワードや SMS OTP などと比べて素早く認証できることがわかっている。しかし、WebAuthn を使う認証にはまだ普及の余地があると考えられる。そこで、IT 企業で WebAuthn とパスワードを拡張した複数要素認証 (MFA) を社員が任意にいずれかを選択できるシステムを提供した。また、彼らが日常的に利用する様子をシステムログ解析や有志によるアンケート調査を行い、結果を分析した。社員は画面ロックなどの経験から生体認証の利便性への期待や利用する意向を示したものの、MFA の利便性を拡張した機能を使える場面が多く、MFA を利用する機会が多いことが推測できる。また、利用の促進にデバイスや環境の整備が必要な一方、認証方法を選択する際に安全性が検討されることは少なかった。

キーワード：FIDO 認証, WebAuthn, 複数要素認証, ユーザビリティ評価

Usability Evaluation of Authentication in an IT Company

WATARU OOGAMI^{1,a)} HIDEHITO GOMI^{1,b)} SHUJI YAMAGUCHI^{1,c)} TATSURU HIGURASHI^{1,d)}

Abstract: The Web Authentication (WebAuthn) API, standardized by the W3C (World Wide Web Consortium), provides a secure method of log into Web pages using biometric authentication. However, authentication using WebAuthn is still considered to have room to spread. To solve this, we provided a system in an IT company that allows employees to choose between WebAuthn and password-enhanced multi-factor authentication (MFA). We also evaluated the results of system log analysis and questionnaire surveys conducted by volunteers to find out how the employees use the system on a daily basis. Although the employees expressed their expectation and intention to use biometric authentication, it can be inferred that they often use MFA because there are many situations in which they can use functions that extend the convenience of MFA. In addition, while devices and environments were necessary to promote the use of MFA, security was rarely considered when selecting an authentication method.

Keywords: FIDO, WebAuthn, Multi-Factor Authentication, Usability evaluation

1. はじめに

ユーザ名とパスワードによるユーザ認証は、Web サービスへのログインにおいて最も主要な方法の 1 つである。しかし、パスワード認証には多くの問題が指摘されている

ものの、代替となる認証方法はパスワードほどには十分に浸透していない [1]。パスワード認証を強化する方法の 1 つに、MFA(Multi-Factor Authentication) がある。これはパスワードによる知識認証に加えて、ハードウェアトークンやスマートフォンのアプリなどによる所持認証を加える 2FA (Two-Factor Authentication) が主に利用されるが、その利用は非常に限定的である。例えば、Google のアクティブなアカウントのうち、2FA を利用しているユーザは 10% である [2]。

一方、ブラウザの標準機能として提供される WebAu-

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

thn(Web Authentication) API を利用して、生体認証などの便利な認証方法が普及し始めている。WebAuthn は、W3C(World Wide Web Consortium[3]) によって 2019 年 3 月に標準技術となり、Chrome, FireFox, Edge, Safari などの主要なブラウザがサポートしている。指紋や顔などの生体情報は画面ロックの解除に利用されることが多く、WebAuthn を用いることで、Web サービスのログインにも利用することができる。生体認証を始めとする認証方法の利便性や公開鍵暗号方式をベースとした安全性についてはそれぞれの分野において研究が進んでいる一方、パスワードを使わないパスワードレス認証はそれを置き換えるほど多くのユーザには使われていない。例えば、ヤフーのアクティブユーザ約 5,100 万人のうち、WebAuthn を含めたパスワードレス認証を使っているユーザは約 2,700 万人である [4]。パスワードレス認証には WebAuthn の他に、SMS (Short Message Service) などを利用する認証が存在するが、パスワード認証を使っているユーザが WebAuthn を利用する際の課題について十分に明らかになっていない可能性がある。

そこで、日常的に利用する認証方法の 1 つとして WebAuthn を IT 企業に導入した際にどのように社員が活用するのか観察・分析することで、パスワードに代えて WebAuthn を導入した際の課題を明らかにする。特に、WebAuthn が認証方法として負担が少なく、利用者が受け入れやすいものであるかという観点から以下の点に着目した。

- 社員は WebAuthn を含む認証基盤をどのように利用するか？
- 社員はどのような要素で認証方法を選択するのか？
- 社員は認証基盤の安全についてどのように考えるか？

本研究では、WebAuthn を導入する際の課題を明らかにするために、企業内の認証基盤に WebAuthn とパスワード認証を拡張した MFA を同時に提供してそれらの活用状況を調査した。また、認証サーバーのログや社員へのアンケートを通じてそのユーザビリティや利用状況分析を行った。ユーザに合わせた適切な案内を行うことにより、WebAuthn による安全な認証方法を提供できる可能性があることを示唆した。

2. 関連研究

パスワードの最も一般的な拡張の 1 つにハードウェアトークンやソフトウェアなどを利用する 2 要素認証 (2FA) が呼ばれる方法が提案されている [5]。2FA は、MFA の 1 つの実装方法の 1 つであり、そのユーザビリティが評価されている [6],[7]。2FA によってパスワードの安全性を強化したが、パスワードの他に入力に使った以外のデバイスや SMS、電話番号、メールアドレスなどを使用するため、利便性が低下する。

また、パスワードレス認証の技術として W3C 標準の

WebAuthn [8] が注目されている。WebAuthn を使用することで、ユーザが Web サイトにログインする際に主要なブラウザを通じて FIDO 認証 [9] を実現する。FIDO 認証では、さまざまな認証方法を認証器 (authenticator) が提供する。認証器は、本人性の検証を、例えばユーザのスマートフォン内部などのローカルで行い、その結果情報を認証器内で保管している秘密鍵で署名して FIDO サーバへ送信する機能である。特に、指紋などの生体認証は、スマートフォンのロック解除などに広く利用されており [10]、パスワードの代替として注目されている。FIDO 認証は認証器の動作により、暗号的に安全性を担保する公開鍵ベースでの認証を行うことができ、従来のパスワードや SMS OTP を利用するよりも安全な認証を行うことができる [11]。認証器が生成した公開鍵を FIDO サーバへ登録する際、認証器はアテステーション (attestation) と呼ばれる自身の出生証明書を添付する。FIDO サーバは予め製造者などから公開されている別の公開鍵を使ってアテステーションを検証することで真に当該の認証器が署名を行っているかどうかを確認する。

FIDO 認証のユーザビリティを明らかにしようとする研究もある。Farke ら [12] は小規模なソフトハウス従業員 (8 人) に対して、FIDO2 に対応したセキュリティキーを配布し、彼らがそれを利用する様子を様々な観点から観察した。従業員は FIDO 認証による安全性よりセキュリティキーの紛失や認証時間の延長など利便性に対する不安を感じていることがわかっている。本研究は Farke らの研究を拡張し、セキュリティキーの代わりに利便性の高いスマートフォンや PC に備え付けの指紋や顔認証を使う際のユーザビリティについて明らかにすることを目的としている。

また、Oogami ら [13] は WebAuthn を用いて Android の指紋認証機能を消費者向けサービスに展開してそのユーザビリティを個別のインタビューなどを通じて明らかにしている。実験により、参加者は WebAuthn の登録作業が認証に比べて煩雑でわかりにくく、改善策として Android が表示するダイアログや Web サイトがより丁寧な案内をすることが必要であることを明らかにした。本研究では、Oogami らの研究に比べて多人数のユーザの調査する点が異なる。また、パスワードや MFA など現在主要な認証方法との比較を行うことで、WebAuthn がパスワードを代替するために必要な要素について示唆を得ることを目的とする。

また、山口ら [14] は 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として、WebAuthn による生体認証とパスワード、SMS の 3 つの手法のユーザビリティをさまざまな視点から調査を行った。システムログ解析やクラウドソーシングを用いた SUS の算出により、WebAuthn を利用した生体認証によるユーザビリティが 3 つの中で一番優れていることを示した。本研究では、山口らが行った多数の消費者を

対象する代わりに、IT 企業の社員に対して調査を行う点が異なる。本研究は公開している Web サービスではなく社内システムへの認証を対象とするため、実験を行う上で認証を利用する頻度などユーザビリティの指標をより把握しやすく、また社員を対象とすることでより深い意見や反応を入手できる可能性がある。また、山口らは主に Android を中心とした認証器について調査しており、本研究実験の iOS/Mac, Windows とは認証器の種別が異なる。

3. ヤフー社内の認証

本研究では、WebAuthn と MFA のユーザビリティを比較調査するために、日常で両者を活用しているヤフーの社内認証基盤を調査に用いる。

ヤフーには、日々の業務に利用する約 1000 個の社内システムがあり、共通の認証基盤を利用して SSO (シングルサインオン) でログインできる。1 万人を超える社員は業務を行う際、各自の好みの端末・認証方法を選択して、1 日 1 回以上この認証を利用する必要がある。特に貸与スマートフォン (業務用 PC とは別のスマートフォン) の利用が始まって以降、その入力の煩雑さや複数デバイスの業務への利用のため、パスワード認証の利便性や安全性の向上が課題だった。

そこで、2019 年 12 月から WebAuthn を利用した FIDO 認証を提供している。ヤフー社内では、FIDO 認証の標準機能の実装と合わせて、利便性のために一度認証したユーザ名の自動補完機能や、FIDO のアテステーションを活用して FIDO サーバによる積極的な選別機能を実装している [15]。

さらに、2021 年 4 月からはパスワード認証の安全性向上を目指して、パスワード単体での認証の代わりに、それを拡張して貸与端末も利用した MFA を実施している。

3.1 各認証のユーザ体験

社内の認証基盤を利用する際の MFA と FIDO 認証それぞれの認証時のユーザ体験について述べる。社員は各々の好みに応じてこの認証方法のいずれかを選択する。

図 1 はヤフー社員が貸与 PC を使って MFA を利用する際の画面遷移を模した図である。まず、社内システムにアクセスした社員は、図 1a で 2 つの認証方法が提示され、いずれかを選択する。「ログイン (MFA)」を選択した場合、図 1b で登録しているメールアドレスを入力し、「次へ」を押すと、図 1c でパスワードを入力し、「サインイン」を押すことでパスワードが適切であれば図 1d へ遷移して PC のブラウザ上で承認を待つ。それと同時に、社員は貸与スマートフォンへプッシュ通知が送られる (図 1e)。その通知を開封すると、対応するアプリケーションが起動し、自身が要求した承認要求をダイアログとして確認することができる (図 1f)。内容が問題なければ、「承認」を選択するこ



図 1: MFA のユーザ体験

とで、サインインが完了し、PC のブラウザは図 1d から自動的に社内システムへリダイレクトされて利用することができる。

Boost MFA ヤフーでは、利便性とネットワークの分離などその他の安全性を検討し、前述のとおりサインインに成功した後、一定期間 Web ブラウザが認証に成功したという情報を保持しており、社員がサインイン状態を維持する意思を示したあと、利用するシステムが定めた期間内であれば、図 1b, 1c の入力と図 1d, 1e, 1f のスマートフォンでの承認作業は、いずれかもしくはどちらも省略する。これらの条件が合わさり認証がスキップされた認証要求を、利便性を増した MFA による認証という意図から、以降 Boost MFA と呼ぶ。Boost MFA を最大限適用した場合、社員は図 1a からボタンをクリックするだけで認証が完了する。

図 2 はヤフーが社員へ貸与 PC を使って FIDO 認証を利用する際の画面遷移を模した図である。社員は MFA と同様、図 2a でログイン方法を選択する。ここで、「ログイン (FIDO 認証)」を選択すると図 2b の画面へ遷移する・図 2b で登録済みアカウント名を入力して「ログイン」を押すと図 2c の画面へ遷移する。この時の表示は認証器 (FIDO 認証サーバへ登録した認証装置) やそれが搭載している OS, Web ブラウザなど社員が利用する環境によって異なるが、Web ブラウザから他のアプリケーションへ遷移することはない。図 2c で、登録した鍵を選択した後、認証器を用いた認証 (例えば、指紋認証) に成功すると、ログインして社内システムを利用することができる。図 2b で「次回以降、自



(a) ログイン方法の選択 (b) アカウント入力 (c) 鍵選択と生体認証

図 2: MFA のユーザ体験

表 1: 過去 30 日に実施した認証回数の内訳

認証方法	回数	割合
FIDO	7275	2.4%
MFA	298591	97.3%
その他	1056	0.3%

表 2: 登録されている認証器の種別

認証器	登録数
Windows Hello	147
Mac TouchID(packed 形式)	586
Apple Touch(Face)ID (fmt-apple)	491

動でログインを開始する」をチェックしてログインが成功した場合、以降の認証時にはこの画面でアカウントを社員自身が入力したり、「ログイン」を押さなくても図 2c に遷移し、認証が開始する。ただし、iOS/Mac とその標準ブラウザ Safari の組み合わせでは、WebAuthn の機能制限上、この機能は利用できないためチェックボタンが表示されない。また、単一の公開鍵をサーバへ登録している場合、図 2c で示した鍵選択は表示されないこともある。

3.2 認証基盤の利用実態

社内認証基盤は 1 営業日あたり、平均 18,660 回、9,175 人の社員が利用している (2021 年 8 月 13 日から過去 30 日のヤフーの営業日実績)。社内認証基盤で利用された認証回数の内訳を表 1 に示す (2021 年 8 月 13 日から過去 30 日の実績)。社員は MFA の利用率が最も高く、FIDO 認証は十分に浸透していない。しかし、多くの社員は貸与スマートフォンの画面のロック解除のために顔や指紋を登録していると推測できる [10]。多くの社員には PC とスマートフォン両方が貸与されており、そのいずれかもしくは両方で FIDO 認証が利用可能である。社員の利用するこれらの環境から、FIDO 認証を選択する上で課題が存在する可能性がある。

現在、登録を許可している認証器の種別とそれぞれの認証器の登録台数を表 2 で示す。

表 3: 参加者の属性

年代	女性	男性	教えない/その他	総計
21-30 歳	13	39	0	52
31-40 歳	17	75	0	92
41-50 歳	5	41	0	46
51-60 歳	2	9	0	11
教えない/その他	3	0	9	12
総計	40	164	9	213

4. 実験

FIDO 認証を導入する上での課題を明らかにするため、(1) 社内認証基盤のログ分析及び (2) 社員によるアンケートを実施した。アンケートは、参加者の属性および各自が利用している認証方法の利便性を問う設問を設定し、社内のイントラネット上に Web フォームを設置した。

4.1 参加者

著者はヤフーの社員に本研究の主旨をイントラネット上の Web ページで説明し、後述のアンケートに 2021 年 7 月 29 日から 8 月 6 日の 9 日間任意のタイミングで回答を求めた。社員であれば誰でも回答が可能であり、回答に関する報酬は発生しない。アンケートの回答結果に基づく参加者の属性を表 3 に示す。

4.2 アンケート

前述した属性を除いた設問を以下に示す。設問の前提として、アンケートの“認証方法”は勤務開始時の認証体験について回答を求めた。これは 3.1 章でも述べた通り、利用する社内システムが異なる場合には、例えば直近で認証が行われても再度認証を要求されるなど、別の認証体験を要求される可能性があるためである。また、社員は毎日勤務開始時には決まった社内システムへのアクセスが義務付けられており、日常的な利用実態を観察する上で適切であると考えた。

(1) 主にどちらの認証方法を利用していますか？

- MFA
- FIDO 認証

(2) 業務開始時にどのデバイスを使っていますか？

- Windows(PC)
- Mac(PC)
- iPhone
- Android
- その他

(3) そのデバイスを使っている理由を教えてください。

(4) FIDO 認証を使うとデバイスについている顔認証や指紋認証を利用できることは知っていますか？

- はい

- いいえ
- (5) 今後 FIDO 認証を利用したいと思いますか？
- はい (これから使いたい、もうつかっている)
 - はい (デバイスが FIDO に対応していなくて使えない)
 - いいえ (使いたくない)
- (6) その理由を教えてください。
- (7) 社内認証基盤のパスワードを忘れたことがありますか？
- はい
 - いいえ
 - つかったことがない
- (8) もし社内認証基盤のパスワード認証が許可されていたら、今でもパスワード認証を利用しますか？それとも他の方法を利用しますか？
- パスワード認証を使う
 - MFA を使う
 - FIDO 認証を使う
- (9) その理由を教えてください。
- (10) 登録・ログインの手順は十分に統一感があると感じる。
- (11) 登録・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る。
- (12) たいていの方は、登録・ログインの手順をすぐに理解すると思う。
- (13) 登録・ログインはとても操作しづらいと感じる。
- (14) どんな人でも、登録・ログインを容易に使いこなす事ができると思う。
- (15) 登録・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。
- (16) 私は登録・ログインを問題なく使うことができる自信がある。
- (17) 登録・ログイン時に知っておくべきことが多くあると思う。
- (18) 登録・ログインして利用する際に今後も同じ認証方法を利用したいと思う。
- (19) 登録・ログインの手順は過剰に複雑であると感じる。
- (20) 今答えた認証方法について改善点や不満な点があれば教えてください。

以降、各設問は Q にアンケートの各設問に対応する番号を添えて、例えば Q1 と呼ぶ。

Q3, Q6, Q9, Q20 は回答が任意で、参加者はテキストエリアによるコメントを記入した。Q3, Q6, Q9, Q20 以外は回答が必須で、参加者はラジオボタンによる複数選択肢から択一で選択した。また、Q10 から Q19 は、各参加者が Q1 で答えた認証方法について 5 段階 (“5:とてもそう思う”, “4”, “3”, “2”, “1:全くそう思わない”) でそれぞれ評価し、SUS(System Usability Scale)[16] を算出した。

SUS 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。Q10 から Q19 までの添字

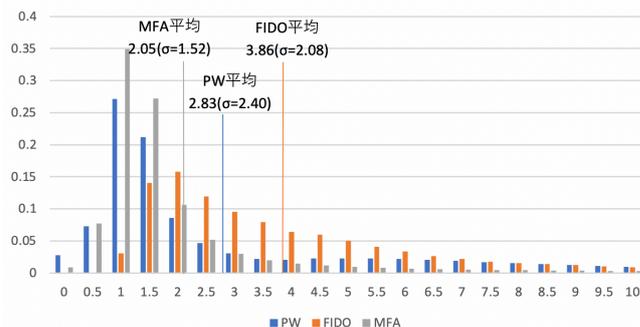


図 3: PW, FIDO, MFA の認証時間

を i とし、参加者の各設問の回答を a_i としたとき、各設問に対するスコア s_i は式 1 で計算する。

$$s_i = \begin{cases} a_i - 1 & (i \in \{10, 12, 14, 16, 18\}), \\ 5 - a_i & (i \in \{11, 13, 15, 17, 19\}). \end{cases} \quad (1)$$

SUS は 100 点が最高点となるように式 2 で計算する。

$$SUS = 2.5 * \sum_{i=10}^{19} s_i. \quad (2)$$

5. 実験結果

参加者が主に利用している認証方法 (Q1) は、FIDO 認証が 40 人、MFA が 173 人である。これは表 1 で示した利用率に比べて FIDO 認証を行う参加者の方が多い。

5.1 認証時間と利便性

認証時に取得したログから、認証の利便性の指標の 1 つとして認証を行う際にかかる時間を評価する。図 3 は、社内認証においてパスワード (PW) と FIDO, MFA それぞれ 1 度の処理にかかった時間をヒストグラムである。対象となるログは共通の画面 (図 1a) が表示されてから、各認証が完了し社内サービスヘリダイレクトされるまでの時間から計測している。また、10 秒以内に認証を完了したログを対象とし、ピンを 0.5 秒ごとに区切って各認証方法の対象ログ数が 1 となるよう正規化した。2019 年 12 月から 2021 年 7 月末までのログを利用した結果、対象となるログは全体の約 90% を含んでおり、認証にかかる時間の傾向を考察する上で十分である。それぞれの対象データ数は PW, FIDO, MFA の順に 3731102, 52591, 2371303 である。図 3 から、PW と MFA は約 1 秒を、FIDO 認証は 2 秒を頂点として減衰する傾向を確認した。注意すべき点として、図 3 中の “MFA” には Boost MFA と MFA の両方を含み、本研究の集計上ではこれらが不可分である。MFA の平均認証時間は FIDO 認証より 1.81 秒短い、これは勤務開始時にアクセスするシステムが Boost MFA を長期間許可しているためであり、MFA での認証要求は Boost MFA により実施している。参考までに、著者が 3 回 MFA による認証を行った際の認証時間は貸与 PC と貸与スマー

表 4: FIDO 認証器の登録状況

認証器の登録	Q1FIDO 認証	Q1MFA
あり	38	53
なし	2	120

表 5: 業務開始時のデバイス

Q2	FIDO	MFA	総計
iPhone	6	14	20
Mac(PC)	24	81	105
Windows(PC)	10	78	88
総計	40	173	213

トフォンの組み合わせで実施したところ、平均で 27.2 秒、Boost MFA を用いた際には平均 1.86 秒を要した。

また、社員の各認証方法の利便性を数値化するため算出した *SUS* は、Q1 で主な認証方法が FIDO 認証と答えた人の平均は 67.75、MFA の平均は 61.46 を示したが、*t* 検定の結果、この *SUS* の間に有意な差はみられなかった ($t(53) = 1.65, ns$)。

WebAuthn が利用可能な Android で指紋認証器を用いた先行研究では、登録時にユーザビリティ上の課題があることがわかっている [13]。そこで、参加者のアカウント名に基づく FIDO サーバの認証器の登録の有無と主な認証方法の関係を表 4 に示す。表 4 から、認証器を登録している参加者は 42.7% ((38+53)/213) 存在し、そのうち 41.7% (38/(38+53)) が FIDO 認証を主な認証方法として利用しているが、58.3% (53/(38+53)) は登録済みに関わらず MFA を主に利用している。

5.2 利用デバイス

各参加者が業務開始時に利用するデバイス (Q2) を表 5 に示す。多くの参加者は、PC を選択している。デバイスによって認証方法の選択に傾向はみられない。PC を選ぶ理由として、「業務をまず始めるときに PC を立ち上げて作業を開始するため」(女性、教えない/その他) のように業務形態に合わせた参加者が一番多く、PC 利用者の 36.7% (71/(213-20)) が回答しており、勤務開始時の認証機会に適したデバイスであると考えられる参加者が多い (Q3)。一方、スマートフォンを選択する人は「PC を起動するのは時間がかかるため」(女性、21-30 歳) のように答えた人が 55.0% (11/20) で最多である (Q3)。

5.3 FIDO 認証の認知と利用意向

FIDO 認証の認知と利用意向について Q4 と Q5 の結果を表 6 に示す。FIDO 認証を認知している参加者は 61.0% (130/213) で、Q1 で FIDO 認証と回答した参加者は全員が認知している一方で、MFA と回答した参加者のうち 48.0% ((45+5+33)/173) は FIDO 認証を認知していなかった

表 6: FIDO 認証の認知と利用意向

Q5	Q1	Q4 はい	Q4 いいえ
はい (使いたい、既利用)	FIDO	39	0
	MFA	38	45
はい (デバイス未対応)	FIDO	1	0
	MFA	19	5
いいえ (使いたくない)	FIDO	0	0
	MFA	33	33
総計		130	83

表 7: Q6 の代表的なコメント

Q5	デバイス	便利	現状に満足	わからない	総計
はい	10	23	2	7	147
いいえ	12	2	22	8	66

(Q4)。また、69.0% ((38+39+45+1+19+5)/213) の参加者は今後 FIDO 認証を利用する意向を示している (Q5)。また、FIDO 認証を使いたい参加者のうち、25 人は現在貸与されているデバイスの他に FIDO 認証対応のデバイスが必要としている。表 7 は Q5 で参加者が答えた FIDO 認証の利用意向に合わせて、その理由 (Q6) を集計した。ただし、1 つのコメントにつき、複数の要素を持つことに注意が必要である。利用意向のある参加者で一番多かったコメントは生体認証などを前提として「認証完了までの時間が短縮できそう」(男性 21-30 歳) など FIDO 認証の認証体験を肯定的に捉える (便利) が一番多く、一方で「以前使おうとしたときに顔をきちんと認証してくれないストレスがあり」(女性、教えない・その他)、「普段は、MBP*1 をクラッシュモード*2 で使用しているので、FIDO 認証の指紋・顔認証が使えない為」(男性、41-50 歳) など認証器での認証時の課題 (デバイス) も多かった。また、利用意向のない参加者では、「MFA 認証で特段困っていない」という (現状に満足) しているコメントが最多であった。さらに、FIDO 認証の利用意向に関わらず FIDO 認証自体がよくわからない「FIDO が何だか分からないので、使う使わないの判断ができない」(男性、31-40 歳) というコメントもあり、認証の利便性以外にも、技術の理解や認知が認証方法の選択に影響を与えることがわかる。

5.4 PW との比較

表 8 は社内認証基盤におけるパスワードを忘れた経験 (Q7) を縦軸に、もしパスワードが単体で認証が許可された場合、参加者が FIDO 認証と MFA、パスワードのいずれかを利用したいか (Q8) を横軸に、社内システムにおける社員のパスワードへの態度に関する結果を示す。まずパスワードを忘れたことのある参加者は 44.6% (95/213) で、彼らのうち 62.1% ((49+10)/95) がパスワード単体もしくは

*1 Mac Book Pro

*2 ノート PC を閉じて接続したディスプレイへ映して利用する

表 8: パスワードの忘却経験と認証方法の選択

Q7	Q8FIDO	Q8MFA	Q8PW	総計
はい	36	49	10	95
いいえ	21	70	21	112
つかったことがない	4	0	2	6
総計	61	119	33	213

はパスワードをベースとした MFA を使いたいと回答している。また、忘れたことのない参加者 (112 人) の 81.3% ((70 + 21)/112) がそれらの認証を使いたいと回答している。一方、パスワードを忘れた経験に関わらず、FIDO 認証を使いたいと答えた参加者は 28.6% (61/213) であったが、認証方法の内訳 (表 1) や Q1 の回答に比べると多くの参加者が FIDO 認証の利用意向を示した。

さらに、Q9 のコメントの内容を分析した結果、FIDO 認証や MFA を選択した参加者は、それが共通してパスワード由来の問題にあることを示している。例えば、「パスワード入力面倒」、「パスワードは忘れがち」(男性, 31-40 歳) というコメントが FIDO 認証を選択した参加者のうち 16 人、MFA を選択した人からは 21 人が回答しており、ともにパスワードによる煩わしさを感じていることがわかる。また、パスワード単体の認証と比べてパスワードを入力しなくてよいことが推測できる。また、MFA を選択した参加者のうち 23 人は「今使っているもので不自由がないから」(女性, 31-40 歳) という MFA に特段不便を感じない、もしくは FIDO 認証へ変更することに大きな利点を感じないことを回答しており、他の認証方法 (FIDO 認証は同 1 人、パスワード認証は同 7 人) に比べて多かった。Q4-Q6 の回答と合わせて、MFA の利便性が高いことが推測できる。

6. 考察

6.1 認証時間と利便性

FIDO 認証はパスワードや SMS OTP を利用した認証方法に比べて、素早く認証できることがわかっている [14]。本研究実験では、FIDO 認証に比べてパスワードや MFA を利用した認証のほうが短時間で利用できる傾向があることがわかった。ただし、先行研究で山口ら [14] が述べているように、本研究実験においても、パスワード認証においてはブラウザなどのパスワード補完機能が利用されている割合が多いことが推測される。これは、本研究の対象が Web サービスを提供しているヤフーで日常的に利用しているシステムであり、社員ごとに利便性を追求した場合、合理的な選択である。現在ヤフー社内ではパスワードを単体で利用する認証方法は特別なケースを除いて許可されていないため、これを検証できなかった。また、図 3 に注目すると、パスワードと MFA の認証時間は特にピーク付近の傾向で近似している。前述の通り、パスワード認証はその補完機能が特に短い認証時間としてログに記録されている

と推測でき、それと近似した MFA の認証時間はパスワードに比べても非常に短く見える。前述の通り、「MFA」には Boost MFA も含まれており分けて集計することはできないため、著者が MFA を選択した場合の認証体験を調べたところ、日常的に利用する社内システムへのアクセスの場合、ボタンを押すだけで認証が完了する Boost MFA による認証の画面遷移・入力の手間が省略されており、前述のように Boost MFA 以外の認証体験では主に ID/PW の入力、別デバイスでの承認にそれぞれ長い時間をかける必要があった。著者の環境での実測時間と PW 補完機能との類似から、「MFA」の認証のうち、ピーク付近の多くの認証要求の多くが Boost MFA によって認証を行っていることが推測できる。FIDO 認証は認証要求のたびに認証器を用いて本人性の検証と署名検証を行うことが利便性高くできるため、パスワード補完機能のようにユーザの手元で入力を補助するツールを必要としたり、Boost MFA のように認証機会をスキップする必要がない。そのため、パスワードの課題点 (5.4 章) を解消したうえで (Q9)、昨今のリモート勤務環境においても本人性をユーザからみて便利に確認することができる。参加者の多くは現在の主に利用している認証 (Q1) やパスワードの失念経験 (Q7) には関係なく FIDO 認証の利用意向を示した。また、彼らは現在すでに利用している貸与 PC や貸与スマートフォンの顔や指紋認証のロック解除機能を念頭に利便性に期待するコメントが多い (表 7)。

6.2 利便性と認証方法の選択

参加者の多くは勤務形態に合わせたデバイスを選択しており (Q2, Q3)、業務内容を主に行う貸与 PC を使う参加者が最も多く、業務開始をより素早く行いたい参加者は貸与スマートフォンを選択する傾向がみられた (Q3)。また、参加者は FIDO 認証の今後の利用意向に関わらず、デバイスの生体認証時にうまく読み取りができないなどの動作や、マスク・手濡れなどの動作環境へ課題を感じている (Q5)。また、FIDO 認証の利用意向がある参加者には例えば別のモデルへ変更するなど、勤務形態で主に使うデバイスを変更する必要がある (Q4, Q5)。ここから社員のデバイスや環境を認証時に適応させていくことで、FIDO 認証をより積極的に利用する可能性がある。

また、Q1 で主な認証方法を MFA だと答えた参加者の多くが現状の MFA に満足しており、中には Q9 で「特に理由はない。変えたいモチベーションがないため現在の方法^{*3}で認証できればよい。」(男性, 31-40 歳) など MFA から FIDO 認証を選択する明確な動機がないことを明言している参加者もいた。MFA への満足は、Q6 で「MFA 認証が都度認証ではなく 1 クリックで済んでいるので、現状

*3 この参加者は Q1 で MFA と回答している

不便を感じていないため」(女性, 31-40歳)とあるように Boost MFA による認証経験が裏付けとなっていることがわかった。

6.3 安全性の意識

前述のように, パスワードを拡張した MFA およびその利便性を高めた Boost MFA に満足している参加者が多い。一方, 継続的に本人性の検証を行うためには FIDO 認証への移行は合理的な選択であると言える。しかし, 参加者の多くは FIDO 認証や Boost MFA に対する利便性に対して肯定的なコメント (Q6, Q9) をする反面, 認証方法の安全性(「セキュリティ」と「安全」など)を言及した参加者は 10 人で, 相対的に少なかった (Q6, Q9)。こうした点から, FIDO 認証を推進していくためには, より利便性に対する強力なインセンティブやシステムに合わせた強制力を持った適用が必要である。

6.4 総括・今後の課題

本研究実験では, 社員を対象とした社内システムの認証を対象にしたが, 一般的な Web サービスにおいても Boost MFA などと同様, 従来のパスワード認証をサポートする標準的な機能が拡充されていることや, 以前と比べて長い有効期限を持つ cookie をもたせて長時間認証をスキップする Web サービスが増えている。こうした技術的な補助により, ユーザが認証の必要性を正確に把握できていないもしくは認証を不要だと捉える可能性があるが, ユーザの利便性とサービス提供者の継続的な本人性の確保を両立する上で FIDO 認証には未だ多くの普及の余地がある。

今後の課題として, Boost MFA やパスワード補完機能など既存のパスワードを補助する技術の仕様実態についても明らかにしたい。また, FIDO 認証の利用意向には技術の認知や使い方も含めた教育も必要であるというコメントが少数だが見られた (Q6)。社内で周知や講習などを通じて, FIDO 認証に触れることが社員の利便性や安全な認証を促進したい。

7. おわりに

Web サービス提供をしているヤフーで日常的に利用している社内認証基盤に WebAuthn を導入し, 観察した。ヤフーではパスワードに代えてそれを拡張した MFA, WebAuthn を用いた FIDO 認証の 2 つが社員の任意で利用することができる。実験結果から, MFA の利便性を向上させた Boost MFA が主に利用されていることが多いことを推測し, それらを背景として FIDO 認証が我々が考えたとおりには利用が進んでいない実態が明らかになった。また, 複数のコメントから社員の環境に沿ったデバイスの準備が必要であり, さらなる拡充により FIDO 認証がより選択されやすくなる可能性がある。

参考文献

- [1] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pp. 553–567, 2012.
- [2] Grzegorz Milka. Anatomy of account takeover. In *Enigma 2018 (Enigma 2018)*, Santa Clara, CA, January 2018. USENIX Association.
- [3] W3C. The world wide web consortium (w3c) – standards organization for the world wide web, october 1994., 2021. <https://www.w3.org>.
- [4] ヤフー. ヤフーが推進する「パスワードレス」その進捗と今後の展望, 2020. <https://about.yahoo.co.jp/info/blog/20200914/passwordless.html>.
- [5] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. “It’s Not Actually That Horrible”: Exploring Adoption of Two-Factor Authentication at a University, p. 1–11. Association for Computing Machinery, New York, NY, USA, 2018.
- [6] Jonathan Dutton, Danny Allen, Dennis Eggett, and Kent Seamons. Don’t punish all of us: Measuring user attitudes about two-factor authentication. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 119–128, 2019.
- [7] You want me to do what? a design study of two-factor authentication messages. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, Santa Clara, CA, July 2017. USENIX Association.
- [8] W3C. Web authentication: An api for accessing public key credentials level 2, 2021. <https://www.w3.org/TR/webauthn/>.
- [9] FIDO Alliance. Fido authentication, 2021. <https://fidoalliance.org/fido-authentication/>.
- [10] Adrian Ludwig. What’s new in android security (m and n version) - google i/o 2016, 2016. <https://www.youtube.com/watch?v=XZzLjllizYs>.
- [11] 五味秀仁, 大神渉. FIDO (フェイド) 認証とその技術. 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol. 12, No. 2, pp. 115–125, 2018.
- [12] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. “you still use the password after all” – exploring fido2 security keys in a small company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pp. 19–35. USENIX Association, August 2020.
- [13] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones. In *SOUPS 2020*. USENIX Association, August 2020.
- [14] 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.
- [15] 江川達也. 社内認証パスワードレス化のすゝめ, 2021. <https://techblog.yahoo.co.jp/entry/2021040530131208/>.
- [16] J. Brooke. SUS: A Quick and Dirty Usability Scale, 1996.