Vol.2022-IOT-56 No.23
2022/3/8

位置情報を利用した動的な質問による認証の提案

山口 修司[1,a)]　大川 悠人[2,b)]　五味 秀仁[1,c)]　上原 哲太郎[3,d)]

概要：本稿では，1) ユーザが自ら事前に認証情報を設定する必要がなく，2) パスワードや秘密の質問のように恒久的な記憶が必要ない認証手段として，行動情報から動的に秘密の質問を生成し回答を求めることで認証とする手法を提案する．提案手法の認証システムには WebAuthn の認証技術を利用し，WebAuthn の認証器の認証手段として，位置情報を利用した動的な質問を適用する．本稿では，システム実装の前段階の実験として，スマートフォンから得られる位置情報から質問を動的に生成し，参加者に回答を求めるラボ実験を行った．加えて，参加者に対するアンケートを通じて，本提案手法の定性的な評価を行った．結果，提案手法が参加者に受け入れられていることが確認でき，質問作成の方法等，システム実装に向けた課題も抽出することができた．

キーワード：WebAuthn, 秘密の質問, 位置情報, アカウントリカバリー

Developing Personal Knowledge Questions Using Location Trajectory

Shuji Yamaguchi[1,a)]　Yuto Ookawa[2,b)]　Hidehito Gomi[1,c)]　Tetsutaro Uehara[3,d)]

Abstract: We propose a method that dynamically generates secret questions from a user's location trajectory. Our proposed method aims at an authentication method that 1) does not require users to set up their own authentication information in advance, and 2) does not require permanent memory like passwords or static secret questions. The authentication system of the proposed method uses WebAuthn protocol and adapts dynamic questions based on location information as an authentication method for WebAuthn authenticators. In this paper, we conducted a lab study, generating questions from location trajectory obtained from its participants' smartphones as a preliminary experiment to implement the system. In addition, we conducted a qualitative evaluation of our proposed method through a questionnaire to the participants. As a result, we confirmed that our proposed method was accepted by the participants and identified issues for the implementation of the system, such as ones in creating questions.

Keywords: WebAuthn, Secret questions, Location trajectory, account recovery

1. はじめに

Web サービスの増加に伴い，ユーザは Web サービスのログインや買い物の前の再確認など様々なシーンで認証を行っている．また，何らかの理由でログインできなくなった時の復旧時にも認証が必要であるため，復旧用の認証手段が必要であり，サービス提供者は複数の認証手段を提供することが求められるようになっている．

パスワードや秘密の質問と答えのようなユーザの記憶を利用した記憶認証がある．記憶認証は，ユーザの記憶が必要であるだけでなく，パスワードや秘密の質問とそれに対する答えをユーザが事前に作成し登録する作業が必要であるため，大変煩雑である．また，セキュリティの面においてもリスト型攻撃のような不正利用の対象にされやすく課題が指摘されている [9].

[1] ヤフー株式会社 Yahoo Japan Corporation
[2] 立命館大学大学院情報理工学研究科 Graduate School of Information Science and Engineering, Ritsumeikan University
[3] 立命館大学情報理工学部 College of Information Science and Engineering, Ritsumeikan University
[a)] shyamagu@yahoo-corp.jp
[b)] ookawa@cysec.cs.ritsumei.ac.jp
[c)] hgomi@yahoo-corp.jp
[d)] t-uehara@fc.ritsumei.ac.jp

パスワードを使用しない認証として，W3C によって Web Authentication（WebAuthn）[26] が提案された．この規格により，Web サイトでパスワードなしに認証できるため，認証の使いやすさが向上すると期待できる [25]．WebAuthn が呼び出す認証器は生体認証が利用できる．

生体認証は，ユーザの生体情報を利用するため，記憶認証と比較して不正利用されにくい利点があるが，ユーザビリティにおいていくつか課題がある．具体的には，暗い環境下では顔がカメラに写りづらく認証が失敗するなど，生体情報は使えないシーンがある点がある．また，記憶認証と同様に，事前に生体情報の登録の作業が必要となるため登録が煩雑である点も挙げられる．加えて，自分の顔等の生体情報を利用することに対する抵抗感を持つユーザもいる．

生体情報の一つの形態として，ユーザの行動情報を用いて認証を行う行動認証がある．スマートフォンや IoT の普及により行動情報をリアルタイムにかつ精密に収集できるようになった．また，機械学習など AI 技術の発展により行動情報を解析する手法が多数提案されている．このような状況下で，近年，行動情報を解析することで個人認証に活用することが可能となってきた [20, 22]．ユーザの同意の元で行動情報を取得し，自動的に解析することによって，ユーザの手間をかけず認証することが期待できる．この点は記憶・生体認証と比較して大きな利点である．

上記の行動認証と記憶認証の利点を備える認証方法として，ユーザの行動履歴を元にして，ユーザに特有の秘密の質問を動的に作成し，ユーザに回答させることで認証する「行動履歴ベース記憶認証」も考案されている [4, 24, 27, 28]．この認証では，ユーザ本人はパスワードは覚えることが難しいが，ユーザの日常生活の特徴的な行動に関しては想起しやすいであろうという発想に基づいている．

そこで本稿では，WebAuthn の認証器の認証手段として行動履歴ベース記憶認証を適用し，1) ユーザが自ら事前に認証情報を設定する必要がなく，2) パスワードや秘密の質問と答えのように恒久的な記憶が必要ない手法を提案する．この提案手法は，WebAuthn を使用した生体認証が利用できない場合等に補完できる認証手段となることを目指す．

本研究では行動情報として位置情報を採用する．近年，GPS (Global Positioning System) センサーを装備したスマートフォンが広く普及し，位置情報を容易に取得できるようになっている．また，商用アプリケーションが位置情報を利用することや位置情報を利用したゲーム（Pokemon Go 等）が普及していることから，位置情報が社会的に受容されてきており，ユーザの抵抗感が下がっているという点も考慮して選択した．

本研究の貢献は下記の通りである．

(1) WebAuthn の認証器の認証手段として，位置情報を利用した動的な秘密の質問を適用する手法を提案．
(2) 提案手法の有効性を調査するため，実際にユーザに質問を出題する実験を行った．
(3) 本提案手法に対する評価をアンケートベースで求め，定性的な評価を行った．

2. 関連研究

認証に用いるパスワードの紛失などの場合のアカウントへのアクセス復旧のために，ユーザ本人だけが知っている秘密の質問を認証サービスに登録しておくという手法は実際のサービスでよく使われている．しかし，それらの秘密の質問は多くの場合セキュリティレベルが十分ではないことが指摘されており，パスワードよりもはるかにセキュリティレベルが低いという実験報告もある [3]．上記のような固定的な秘密の質問のセキュリティ強度が低いという課題を解決するため，ユーザのスマートフォンから得られる行動履歴やライフログを元に動的に作成した質問をヒントとして認証する方法が提案されている [2, 27]．

記憶に依存する認証方法は，パスワードなど認証に用いる情報をユーザが忘れてしまう課題があり，これを解決するべく，ユーザの行動履歴からユーザに特有の行動を抽出することで認証しようとするアプローチ（行動認証）が提案されている [20, 22]．

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]．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が，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 [13, 14, 16]．

WebAuthn [23] 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，一般的な Web ブラウザーを介した Web サイトにおいて，パスワードを使わずにユーザを認証できる（パスワードレス認証）．上記セキュリティキーのみならず，スマートフォンや PC に搭載される指紋や顔などの生体認証を利用でき，ユーザビリティの向上が期待されている [8, 17, 21]．

ユーザ本人の生体情報を利用する生体認証は，常に利用可能で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，保管された生体情報は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り，盗難や紛失からの回復は困難であるという研究報告もある [18]．

3. WebAuthn の認証技術

WebAuthn は，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ことを目的とした認証技術である [26]．以下，WebAuthn の認証の詳細を説明する． 概要を図 1 に示す．

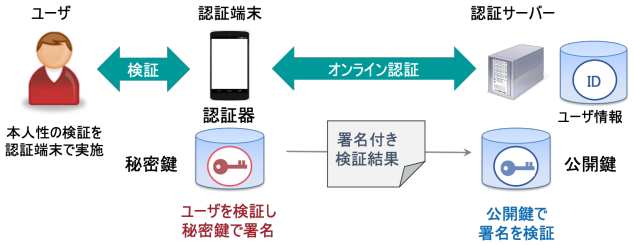

図 1 WenAuthn の認証の概要

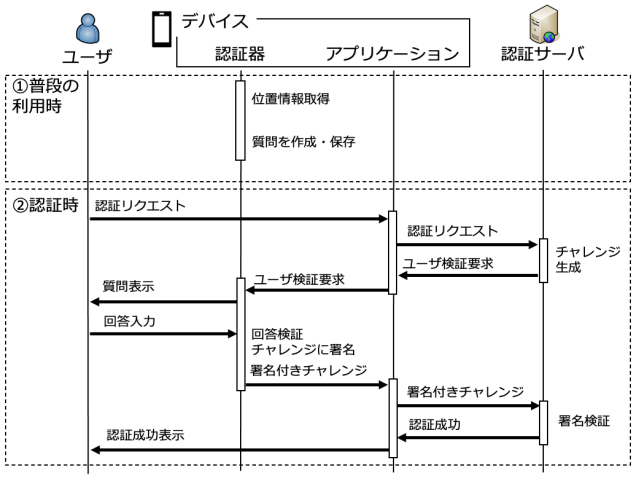

図 2 提案手法のシーケンス図

WebAuthn の認証の大きな特徴は，ユーザの検証結果の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．

4. 提案手法

4.1 提案手法の概要

提案手法のシーケンスを図 2 に示す．ユーザ，ユーザのスマートフォン等のデバイスにインストールされた認証器，デバイス上で認証を行うアプリケーション，認証サーバがある．認証器は，普段から自動的にユーザの位置情報を取得する．そして，定期的に位置情報から動的に質問を生成し，認証器内に保存する．このとき，生成した情報は TEE 等の安全な領域に保存される．

認証時のフローは 3 章に示した WebAuthn の認証技術のフローに従う．認証器がユーザに提示するユーザ検証の内容が，位置情報から動的に生成した質問になる．

4.2 質問の作成方法

4.2.1 質問に使用する地点の選択

動的な質問を適切な難易度にするために，質問に使用する地点の選択が非常に重要となる．まず，滞在している位置が最も多く得られている地点を自宅，次に多い地点が職場や学校等のよく訪れる場所であると想定した．この 2 点は，本人にとって容易過ぎ，また攻撃者にも知られやすい情報であると想定されるため，質問に適さないと定義し，極力除外する方針とした．

質問に使用する地点について，地点の名称を取得する必要がある．地点名は次のような優先順位で選択した．

(1) ランドマークとなる施設名があれば利用する（商業施設や学校等）
(2) 駅があれば駅名を利用する
(3) 市区町村名を利用する

4.2.2 質問の回答依頼方法

質問の回答依頼方式は，次のように設定した．

まず，質問文は，次のようなフォーマットを想定する．

- 「何月何日にあなたが行ったのはどの場所付近ですか？」
- 「何月何日にあなたが行ったのはどのショッピングモールですか？」

質問する地点名の名称に合わせて内容を適切に変更する必要がある．また，日付は実際に位置情報が得られた日付を入力する．

次に回答の形式は，選択肢形式とする．固定的な秘密の質問の回答に関しては一般的に自由記述が求められることが多いが，これは本人が回答を設定しているため可能になっており，システムが動的に生成する本提案手法においては適さない．選択肢の提案形式においては，地点名を文字列で表示する，地図等の画像で表示する等のバリエーションが考えられる．

4.3 想定される脅威

本提案手法では，WebAuthn と動的な質問を組み合わせた手法を採用しているため，多要素認証が行われている状態になる．WebAuthn の認証技術を採用しているため，固定的な秘密の質問に実施されるようなリスト型攻撃等による攻撃は困難になる．また，位置情報等の行動情報をデバイスから外に送信しないため，フィッシング等の攻撃も困難であり，オンラインの攻撃に対しては強固なセキュリ

ティが実現できている．

攻撃として想定されるパターンに，物理的にデバイスに対して攻撃されるパターンがある．ユーザがデバイスを落とす，または攻撃者に盗まれる等した結果デバイスを搾取され，さらに攻撃者がデバイスのロックを解除できた場合，本提案手法の認証器への攻撃が可能となる．この攻撃を行う攻撃者が家族や知人などのユーザに近い人物である場合，ユーザの行動や位置情報を知っている可能性があるため注意が必要となる．この点においては実験 (5 章) で検証する．

5. 実験

位置情報を利用した動的な質問の認証を行う認証器を実装する前段階の実験として，今回は位置情報から生成した動的な質問を実際に出題し，参加者の回答の状況の調査と定性的な評価を行う実験を行った．

5.1 実験概要

実験は，参加者の日常生活で得られる位置情報を利用するため，実験用の Android アプリケーションを作成し，参加者にインストールしてもらい実施する．

本実験では，4.3 章で記述した脅威に対する調査も合わせて行うため，参加者には知り合いと 2 人組で参加してもらうように依頼した．2 人組の間で，本人を対象に作成された質問の回答のみでなく，お互いにペアの相手の質問にも回答を実施し，これを不正利用攻撃に見立てた実験とした．

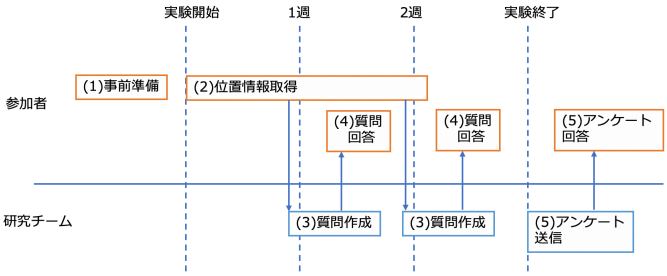

図 3 実験の流れ

図 3 に実験の流れを示す．また，それぞれの詳細を下記に示す．

(1) 事前準備
参加者を募集し，実験参加の同意を得た上で実験用の Android アプリケーションのインストール手順を配布しインストールを依頼する．実験の参加者募集について 5.2 章で，使用した Android アプリケーションについて 5.3 章で詳細を記述する．

(2) 位置情報の取得
実験用の Android アプリケーションの位置情報取得設定を ON にしてもらい，位置情報取得を開始する．実験期間中は基本的に位置情報取得設定が ON のまま過ごしてもらい，位置情報は Android アプリケーションが定期的にサーバにアップロードする．

(3) 質問作成
研究チームはサーバにアップロードされた位置情報から質問を作成する．質問の作成方法は 5.4 章に記載する．質問の作成後，本人を対象に作成された質問と 2 人組の相手を対象に作成された質問を 2 問 1 セットにし，配布用に Web 上で回答可能な入力フォームを作成する．今回は Google Form を使用した．

(4) 質問回答
研究チームは，作成した質問を掲載した入力フォームを参加者に配布する．参加者は，この入力フォームに入力し，本人向けの質問と 2 人組の相手への質問に回答する．実験期間中，(3)-(4) の手順は複数回実施する．

(5) アンケートによる定性評価の実施
実験期間終了後，提案手法の定性評価のためのアンケート調査を行う．アンケートの詳細について 5.6 章に記述する．アンケート回答後に実験参加の報酬を支払う．

5.2 参加者の募集

今回，我々の共著者が所属する立命館大学の在学生を対象に参加者を募集した．日常からある程度の移動を行っている学生を対象とし，加えて 5.1 章で示した手順の実験が行えるように，参加の条件は下記の通りとした．

- 対面の講義 (ゼミも含む) を受講している方
- 知り合いと二人組で参加できる方
- 日常的に使っている Android スマホ（Android OS 9 以上）を実験に使える方
- 実験参加期間中に取得する位置情報を基本的に全て提供できる方
- 下記に同意いただける方
  - 研究チーム内で位置情報やアンケート結果の共有
  - 二人組間で不正利用のシミュレーション実験を行うこと
  - 実験結果について論文等で成果報告の実施

本実験への参加の報酬は 5,000 PayPay ボーナス[*1]とし，募集要項をキャンパス内に掲示して募集を行った．募集の結果，4 組 8 名からの応募があり，この参加者で実験を行った．

5.3 位置情報取得 Android アプリケーションの概要

位置情報の取得のために専用の Android アプリケーションを開発し，参加者に配布・インストールしてもらい，実験に必要なデータの収集を行った．Android アプリケーショ

[*1] PayPay ボーナス: https://paypay.ne.jp/help/c0048/

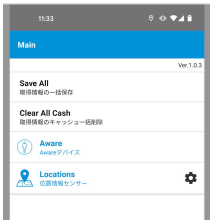

図 4 位置情報取得 Android アプリケーションの画面例

ンの画面例を図 4 に示す．

参加者は所有するスマートフォンに Android アプリケーションをインストール後，Android アプリケーションに位置情報を利用する権限を付与し位置情報の収集を開始する．Android アプリケーションの位置情報取得部分の実装には，オープンソースのモバイルセンシングフレームワークである AWARE Framework を利用した [19]．今回の対象の Android OS は Android 9 以上とした．また，今回の実験中に取得する位置情報の頻度は約 1 分に 1 度と設定した．

5.4 質問の作成方法

今回は，少人数のラボ実験であり，参加者の同意が得られていることから，研究メンバーが参加者の位置情報を閲覧し，質問作成ルールに従って質問を作成した．この際，参加者のプライバシーに配慮し，位置情報の緯度経度は小数点第 2 位までを利用した．質問は 4.2 章の質問作成ルールに従って作成した．

質問に使用する地点の選択について，今回は参加者が学生であるという性質上，滞在している位置が最も多く得られている地点が自宅，次に多い地点が学校であると想定した．この 2 点は質問に適さないため除外し，自宅から極力離れた地点を利用する方針とした．ただし，上記の条件に相当するような地点が得られていない参加者については，得られている他の地点から出題する．

回答の選択肢は 8 種類とした．正解の選択肢を質問に使用する地点の地点名とし，不正解の選択肢をそれとは別に 7 種類用意する．不正解の選択肢に関して，例えば正解の地点名がショッピングモールの場合は，不正解の選択肢もショッピングモールの名称にする等，正解の選択肢の地点名と同じジャンルの地点の名称を選び利用した．下記に実際に出題した質問の例を示す．

あなたが 2022/01/17 に行ったのはどのショッピングモール付近ですか？
- イオンタウン羽倉崎
- イオンタウン諏訪の森
- イオンタウン小阪
- イオンタウン東大阪
- イオンタウン平野
- イオンタウン淀川三国
- イオンタウン豊中緑丘
- イオンタウン茨木太田

5.5 質問の回答結果

質問は実験期間中に 2 回出題し，参加者 8 名中 7 名の回答が得られた．各回，本人向けの質問と，2 人組の相手向けの質問の 2 つに回答してもらった．参加者の回答をまとめたものを表 1 に示す．本人の回答は，1 回目は 5 名が正解，2 名が不正解となり，2 回目は 6 名が正解，1 名が不正解となった．相手の回答は，1 回目は 3 名が正解，4 名が不正解となり，2 回目は 5 名が正解，2 名が不正解となった．

5.6 アンケートによる定性評価

参加者への質問の出題と回答が全て終わった後，参加者の提案手法に関しての定性的な評価のため，アンケートによる定性評価を実施した．アンケートは Yahoo! クラウドソーシングのサービスを利用し作成した[*2]．アンケートの設問は表 2 の設問内容の列に示す 8 種類とした．

アンケートは 6 名の有効な回答が得られた．集計結果と得られた自由記述の回答から特徴的な回答を表 2 に示す．

6. 考察

表 2 の設問 (1) 位置情報の利用を不快に感じたかという設問について，そう思う・ややそう思うの回答はなかった．また，自由記述からも，友人宅での利用は躊躇したという意見もあったが，適切な説明がされていれば位置情報の利用が許容されたことを確認できた．

スマートフォンへの影響は，設問 (2) の結果を確認すると，支障がないとの回答が多く得られた．電池の減りがいつもより速いと指摘している参加者がいたが，位置情報を取得する頻度等の調整でほぼ影響のない使用量にすることが可能であると考える．

また，表 2 の設問 (3) について，機会があれば利用したいが最も多い回答となり，提案した認証方法がある程度受け入れられることが確認できた．設問 (4) についても設問 (3) と同様に，機会があれば勧めたい，どちらともいえな

[*2] Yahoo! クラウドソーシング: https://crowdsourcing.yahoo.co.jp/

表 1 動的に作成した質問への回答結果

1 回目の質問			2 回目の質問		
地点の種類	本人の回答	相手の回答	地点の種類	本人の回答	相手の回答
ランドマーク（観光地）	×	×	市区町村	×	○
駅	○	○	市区町村	○	○
ランドマーク（学校）	○	×	市区町村	○	○
市区町村	○	○	市区町村	○	○
市区町村	未回答	×	市区町村	未回答	×
ランドマーク（商業施設）	×	未回答	ランドマーク（観光地）	○	未回答
市区町村	○	×	市区町村	○	○
ランドマーク（商業施設）	○	○	ランドマーク（商業施設）	○	×

いに回答が集まり，勧めたくない回答は得られなかった．

以上から，個人情報としての位置情報の利用を懸念する意見もあったが，適切な提案をすれば，本提案手法を利用したいと思っている参加者が多いことが確認できた．一方で，実験を通してさらなる研究課題が抽出できたため，以下で議論する．

6.1 位置情報の取得

今回の実験を通して，参加者により，位置情報が多く取得できないパターンがあることがわかった．自宅ともう 1 箇所程度のみの滞在地点しか取得できなかった参加者もいた．我々が確認できた原因としては次のような状態があった．まず，地下等の GPS データが得られにくい箇所にいる場合は位置情報が取得できない．また，スマートフォンの制約でバックグラウンドの処理が制限されている場合，位置情報の取得が停止する状況が起きることも分かっている．または，本当にほぼ家にいて地点数が増えていない可能性も考えられる．いずれも，実サービスに導入時にも起こりうる原因であるため，得られた位置情報が少ないユーザへの対応の検討は必須である．この点は課題であるが，本提案手法は生体認証等と併用して利用し，利用シーンによって補完するような関係で利用することが可能な手法であるため，位置情報が利用できるときに使用できる認証手段として提供する方法も可能であると考える．

6.2 質問の生成方法

ラボ実験として研究チームで質問と選択肢を生成した経験から，大きく 2 つの課題が得られた．まず， 5.4 で説明した地点とその名称の選び方について，実際に地図で位置を確認すると，次のような状況では，その地域の知識がないと選択が困難である場合があることがわかった．例えば，京都市内の場合は区の名前を利用するのではなく，通りの名前を利用しないと地元の人にはわかりずらいという例や，駅の近くの地点であるが，前後の位置から想定すると電車には乗っていないだろうと推測され駅名を利用しないほうがよい例，等が実際に生じた．

次に，選択肢の生成にも知識が必要な点である． 5.4 でショッピングモールを題材にした出題例を例示したが，当然ながらこの場合はショッピングモール名を事前に知る必要がある．今回は公式ページ等で調べたが，質問の生成の自動化を考えたときの課題となる．

これらの解決には，ナレッジグラフの利用や自然言語処理技術の活用が必要であると考えており，将来の課題としたい．

6.3 質問の回答結果

表 1 の実験結果から，本人の回答の正解率が高いことが確認できた．基本的に本人向けの質問として適切に質問が生成できていることが確認できたが，本人への質問であるにも関わらず不正解となる状況があることも確認できた．加えて，アンケート設問 (5)(6) で確認した自分への質問の難易度と内容の適切さについても評価が分かれる結果となっている．本人向けの質問であるにも関わらず不正解または難しいと感じる要因として，選択肢が迷うようなものであった点や，数日前の行動を覚えていないという点が挙げられていたため，こちらも質問を生成する上での課題であると考える．

次に，不正利用に見立てた実験である相手の質問への回答について，表 1 から正解率が高いことがわかる．表 2 のアンケート設問 (7)(8) をみると，相手の質問に対する難易度の評価は人それぞれであり，相手について知らない情報から出題されていたことも多いことが分かるため，難しいまたは知らない情報の質問にもある程度正解できてしまっている状況があることがわかった．難易度が大変やさしかったという回答の中に，もっと詳細な時刻・位置情報を利用するべきという指摘があったため，事前に情報を知らなくても答えを想像しやすい質問になっていた可能性が高く，この点は課題である．また，位置情報を共有するアプリをお互いに入れていて答えられたという回答もあったため，このような状況がある点も相手の質問への正解率を上げる要因になっていると考えられる．

上述した課題は，今回の実験により抽出されたさらなる研究課題であり，より詳しい原因の特定と改善のため，大規模な人数の実験を行うことが今後の課題である．

表 2 アンケートによる定性評価結果

設問内容	選択肢	回答数	自由記述例
(1) 位置情報データを活用されることに関して不快に思いましたか	そう思う	0	
	ややそう思う	0	
	どちらともいえない	2	「個人を特定されない範囲での活用ならば，不快感はない．友人宅へお邪魔しているときなど，若干情報提供に躊躇した.」
	あまりそう思わない	2	
	そう思わない	2	「目的や取得したデータの使用方法などついて具体的な説明があれば，ふかいかんはない.」
(2) 実験アプリが位置情報を取得することでスマートフォンに支障がありましたか	支障あった	1	「電源がいつもより減るのではないかと感じた」
	支障なかった	5	
(3) このような位置情報を利用した秘密の質問を利用したいと思いますか	ぜひ利用したい	0	
	機会があれば利用したい	3	「便利だと思うから.」
	どちらでもない	2	
	あまり利用したくない	1	「i would not want to use it much because sometimes i tend to forget where i was few days ago.」
	利用したくない	0	
(4) このような位置情報を利用した秘密の質問を知人に勧めたいですか	ぜひすすめたい	0	
	機会があればすすめたい	3	「非常に簡単だったため」
	どちらでもない	3	「位置情報と個人情報をより強く結びつけるのはどうなのかなと思ってしまうため.」
	あまりすすめたくない	0	
	すすめたくない	0	
(5) 自分の質問の難易度はいかがでしたか	たいへん易しかった	3	「想像できるものが多かった，親しい友人ならば，パスワードを想像されてしまいそう」
	すこし易しかった	0	
	どちらともいえない	1	
	すこし難しかった	2	「どの選択肢に当てはまるのかとても迷う質問があったのでどれに答えていいのか戸惑った.」
	たいへん難しかった	0	
(6) 自分の質問の内容はあなたにとって適切でしたか	適切だった	2	「場所は正確だった」
	やや適切だった	1	
	どちらともいえない	1	
	少し不適切だった	2	「1 週間くらい前の場所を問われると，すこし思い出すのに時間がかかった．しかし，選択式だったためそれほど手間取らなかった.」
	不適切だった	0	
(7) ペアの人の質問の難易度はいかがでしたか	たいへん易しかった	2	「非常に簡単にペアの位置情報を確認できた，もっと詳細な時刻と位置情報でのパスワード予測が必要」
	すこし易しかった	0	
	どちらともいえない	2	
	すこし難しかった	2	「一緒にいた日はいいけどいなかった日は，相手のスケジュールを，全て把握してないから.」
	たいへん難しかった	0	
(8) ペアの人の質問の内容は，ペアの人に関して，あなたが事前に知っている情報から出題されていましたか	知っている情報だった	1	「直接話してはいないが，普段の行動パターンからほぼ確定で推測できた」
	やや知っている情報だった	1	「位置情報共有アプリをお互いに入れていたため，大学にいるか家にいるかはなんとなくわかり，回答しやすかった.」
	どちらともいえない	1	
	やや知らない情報だった	0	
	知らない情報だった	3	

7. おわりに

本稿では，WebAuthn の認証器の認証手段として，位置情報を利用した動的な秘密の質問を適用する手法を提案した．実験として，8 名の参加者を対象に，提案手法で生成した質問を実際に出題し，回答を求めるラボ実験とアンケートによる定性調査を行った．結果，本人の回答は高い正解率が得られ，アンケート結果からは本提案手法を利用したい意思がある参加者が多いことが確認できた．さらなる研究課題として，不正利用に見立てた実験である相手の質問の正解率が高い点や，位置情報取得の課題，質問作成の方法等のシステム実装に向けた課題が抽出できたため，より大規模な人数の実験を通して解決していくことを今後の課題としたい．

参考文献

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

[2] Yusuf Albayram and Mohammad Maifi Hasan Khan. Evaluating the effectiveness of using hints for autobiographical authentication: A field study. In *Proc. of SOUPS*, pp. 211–224, 2015.

[3] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In *Proc. of WWW*, pp. 141–150, 2015.

[4] Sauvik Das, Eiji Hayashi, and Jason I Hong. Exploring Capturable Everyday Memory for Autobiographical Authentication. In *Proc. of UbiComp*, pp. 211–220, September 2013.

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

[6] D. Wang *et al.* The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes. In *Proc. of ASIA CCS*, 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. of SOUPS*, 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. of SOUPS*, 2020.

[9] J. Bonneau *et al.* The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proc. of S&P*, 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. of CHI*, pp. 1–12, 2018.

[11] J. Dutson *et al.* "Don't punish all of us": Measuring User Attitudes about Two-Factor Authentication. In *Proc. of Euro S&PW*, 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. of S&P*, pp. 872–888, 2018.

[14] K. Reese *et al.* A Usability Study of Five Two-Factor Authentication Methods. In *Proc. of SOUPS*, 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. of SOUPS*, 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. of SOUPS*, 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. of S&P*, pp. 842–859, 2020.

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

[19] Denzil Ferreira, Vassilis Kostakos, and Anind K. Dey. Aware: Mobile context instrumentation framework. *Frontiers in ICT*, Vol. 2, , 2015.

[20] Lex Fridman, Steven Weber, Senior Member, Rachel Greenstadt, and Moshe Kam. Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. In *IEEE Systems Journal*, pp. 1–9, 2016.

[21] 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. of SOUPS*, 2020.

[22] Shuji Yamaguchi, Hidehito Gomi, Ryosuke Kobayashi, Rie Shigetomi Yamaguchi. Effective Classification for Multi-modal Behavioral Authentication on Large-scale Data. *J. Internet Technol.*, Vol. 22, No. 5, pp. 1169–1181, September 2021.

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

[24] Simon S Woo, Ron Artstein, Elsi Kaiser, Xiao Le, and Jelena Mirkovic. Using episodic memory for user authentication. *ACM Trans. Priv. Secur.*, Vol. 22, No. 2, pp. 1–34, April 2019.

[25] 山口修司, 五味秀仁, 日暮立, 大神渉. 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. In *Proc. of Computer Security Symposium*, pp. 207–214, 2021.

[26] 五味秀仁, 大神渉. 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.

[27] 倉嶋俊, 橋山智訓, 田野俊一. ユーザの行動履歴に基づく秘密の質問の自動生成. ファジィシステムシンポジウム講演論文集, pp. 269–274, 2016.

[28] 増井俊之. EpisoPass: エピソード記憶にもとづくパスワード管理. In *Proc. of Computer Security Symposium*, pp. 933–940, 2013.