推測攻撃対策を目的としたペア情報による個人認証の安全性評価：単語ペアと絵文字ペアの比較

横山 佳紀[1,a)]　高田 哲司[1,b)]

概要：知識照合型個人認証には推測攻撃という脅威が存在する．推測攻撃は攻撃者が攻撃対象者の秘密情報を推測・類推することにより，考えうる秘密情報に順序をつけ，その順に試行することでなりすましを試みる攻撃方法である．推測攻撃は，ユーザが秘密情報作成時に記憶保持を優先した情報の選択により生まれる脆弱な秘密情報により可能になる．この問題を改善しうる個人認証として単語ペアを秘密情報とする AssociPass が提案されたが，容易に推測可能なペアや推測攻撃に利用可能な偏りの発生が課題とされていた．そこで本研究では，AssociPass における利便性を維持しつつ推測攻撃に対する安全性を向上させることを目的とし，秘密情報に絵文字を用いることを提案する．この提案による安全性の改善効果を検証するためプロトタイプシステムを実装し，実験参加者による評価実験を実施した．その結果，秘密情報の記憶保持については 2 週間の間隔をあけても記憶保持が可能であることが明らかになった．また推測攻撃に対する安全性について人間による推測攻撃実験を行った結果，単語による手法よりも絵文字による秘密の方が推測攻撃に対して安全である傾向が見られた．

キーワード：個人認証，推測攻撃，ペア情報，絵文字，利便性

Security Evaluation of User Authentication with Pair-based Credential Against Guess Attack Using Words and Emojis

Yoshiki Yokoyama[1,a)]　Tetsuji Takada[1,b)]

Abstract: "Guess attack" is one of the threats to knowledge-based user authentication. An attacker attempts to spoof a victim by using guessed credentials, and the vulnerable situation actually exists because users tend to select a guessable credential for a better memory retention. "AssociPass" was proposed to prevent users from selecting vulnerable credential. However, AssociPass still has some issues that may become vulnerable to the attack. We, therefore, propose two improvements to address the remained issues. One is to use an Emoji-pair instead of word-pair, and the other is to put a limitation on the number of characters for making a credential. We implemented an updated AssociPass and conducted evaluation experiments with participants. As a result, we found that a memory retention of credential is possible even in two weeks interval, and we also showed a potential that the security of Emoji-pair credential is more secure than that of word-pair credential.

Keywords: User Authentication, Guess Attack, Pair-based Credential, Emoji, Usability

1. はじめに

パスワードや暗証番号を秘密情報とする個人認証は，現在も広く利用されている．このように正規利用者が持つ知識を秘密情報とする個人認証を「知識照合型個人認証」と

[1] 電気通信大学
The University of Electro-Communications
[a)] yy.azlab@uec.ac.jp
[b)] zetaka@computer.org

呼ぶが，この手法には様々な攻撃手法が存在する．その 1 つに推測攻撃という方法がある．推測攻撃とは，攻撃者が攻撃対象者の秘密情報（パスワードや暗証番号等）を推測・類推し，その情報をもとに“なりすまし”を試みる攻撃方法である．我々は複数の攻撃方法がある中で，推測攻撃に対する対策が必要だと考える．その理由は，知識照合型個人認証において現実的な脅威だと考えるからである．

攻撃者目線で考えた場合，推測攻撃は秘密情報として考えうるものを一つずつ試行する総当たり攻撃よりも効率的になりすましを成功させる可能性がある．4 桁暗証番号を例に説明する．この認証手法では，最悪の場合でも 10,000 通りの秘密情報を入力すればなりすましに必ず成功する．これが 4 桁の暗証番号認証における総当たり攻撃への安全性として示されている．これに対して攻撃者は「攻撃対象者は日付を暗証番号にしている」と類推できるならば，その値は 732 通り[*1]と 1/10 以下の試行回数でなりすましに成功することになる．また「電話番号や所有車のナンバープレート等に由来する個人情報が暗証番号になっている」と推測されるならば，その値はもっと小さな値となる．つまり，上述のような推測・類推が妥当であれば，認証手法の安全性は総当たり攻撃で想定された状況よりも低いものとなる．

そしてこのような状況は現実化している．Splash Data 社は The Top 50 Worst Passwords[1] というデータを発表している．これは漏洩したパスワード情報を基に多くの人が設定しているパスワードをランキングとして示したものである．このデータは，多くのユーザが特定のパスワードを設定する傾向があることを示しており，上で述べた「多くの利用者は日付を暗証番号にしている」と同様のことが現実に発生していることを示している．また，Li ら [2] の漏洩パスワードに関する研究によると，約 6 割のパスワードにユーザの名前や生年月日，電話番号といった個人情報が含まれていることを明らかにした．これは秘密情報にユーザの個人情報が含まれる傾向があることの証左だと言える．これらのようにユーザが作成する個人認証の秘密情報にはある種の傾向（偏り）があることが知られており，これが推測攻撃を可能にしている．

このような傾向（偏り）が生まれる理由は，秘密情報作成時のユーザの行動を考えれば説明可能である．ユーザは，（step 1）ユーザが知りうる情報群を秘密情報候補の母集団とし，（step 2）その中から記憶保持が可能と思うものを選択する，と考えられる．step 1 で言えることは，秘密情報として取りうる値すべてが秘密情報の候補になるわけではないことであり，step 2 の段階で選択されうる候補は step 1 で用意された母集団の中からさらに少数に絞られるということである．したがって，何らかの工夫がなされない限り選択される秘密情報に一定の傾向（偏り）が生まれるのは避けられないと言える．辞書攻撃と呼ばれる攻撃方法が存在するが，これは上述の step 1 における母集団の存在を前提にした攻撃方法だと言える．

したがって，推測攻撃に対する安全性を改善するためには以下の 3 つの方法が考えられる．

m1)　上記の step 1 における母集団を大きくする
m2)　上記の step 2 にて記憶可能と思える候補を増やす
m3)　ユーザに秘密情報を作成・選択させない

しかし，どの方法も実現は難しい．m3）はシステムが安全な秘密情報を作成し，それをユーザに利用させる方法である．しかし，システムによって作成された秘密情報はユーザが記憶保持できず，正規ユーザがログインできないという事態を招く恐れがある．m1）の実現には，新たな情報や知識を学習・獲得する必要があるため容易ではないと考える．m2）であるが，そもそも記憶可能な候補を増やすことが困難なためこのような問題が発生しているのであり，その実現が困難なことは明らかである．記憶可能性を維持しつつ step 1 の母集団に含まれない秘密情報を作成するため，Leet[*2]に代表されるような様々な置換や抽出による秘密情報生成法も提案されているが，これらも記憶保持の面で問題がないとは言えない．したがって，他の対策方法を考える必要がある．

そこで本研究では，推測攻撃に対する安全性向上を目的とし新たな手法として提案された個人認証手法 AssociPass[3][4] に注目し，その手法における問題点を改善する方法として秘密情報に「絵文字」を用いることを提案する．そして，この改善提案についてプロトタイプシステムを用いた評価実験を行い，その効果を検証した．

以降，本論文では 2 章で AssociPass とその問題点について述べ，3 章で AssociPass の改善提案について述べる．4 章では評価実験について述べる．また，5 章では評価実験の結果を踏まえて考察を行い，6 章で関連研究について述べる．

2. AssociPass とその問題点

2.1 AssociPass について

AssociPass[3][4] とは，秘密情報を正規利用者が作成する前提で，推測攻撃に対する安全性を改善することを目的とした知識照合型個人認証手法である．この手法では，秘密情報の基本要素を「単語ペア」とした．これは 2 つの名詞単語から構成されるものであり（学校，虎），（机，西）がその一例である．また制約条件とはしないものの，この 2 単語間の関連付けは利用者自身しか知り得ない「私的な関連」であることが望ましいとしている．AssociPass におけ

[*1] 月日（MMDD）と日月（DDMM）を想定したもの（732 = 366∗2）

[*2] 一部のアルファベットを似た形や発音の数字や記号に置き換える手法．例)password => p@$$w0rd

る秘密情報は，この単語ペア n 個の集合である．また認証時には，単語ペアを構成する単語群（単語 m 個）をシステムが認証画面に表示し，その状態で利用者が 2 単語を関連付ける操作を行うことで秘密情報を入力する認証方式となっている．

このように秘密情報を定義した理由は，前章で述べた改善方法を実現するためである．利用者が知りうる情報を増やすことは容易ではない，ならば知りうる情報で大きな母集団を形成することを考え，単語ペアという構成要素を考えた．また，単語間の関連付けについても制約条件を設けていない．これにより母集団の要素数は知りうる情報群の 2 乗個に拡張されることになる．また，候補群の一部が記憶困難と判断され，秘密情報の選択肢から外される可能性を低減するため，秘密情報の回答方法は画面内の単語群を認識し，その中から事前に決定していた 2 単語を関連付けるという回答方法にしている．これは画面に表示された単語群を見ることにより秘密情報を思い出す効果を期待したものであり，単語ペアを想起し入力欄に単語を入力するよりも記憶保持の点で望ましいものと考えての設計である．

AssociPass における取りうる秘密情報の数（NPC[*3]）について述べる．この逆数が本手法における総当たり攻撃への安全性となる．上記の説明から，認証画面に m 個の単語が表示され，その中から n 個の単語ペアを入力する認証手法である．ここで (m, n) = (10, 4) の条件を想定する．この場合，10 個の単語群から作成可能な単語ペアは 45 組（$= {}_{10}C_2$）であり，この単語ペア群のうち 4 組のペアが秘密情報であることから，NPC は 148,995 通り（$= {}_{45}C_4$）となる．

2.2 AssociPass の問題点

山岸らは，実験参加者に AssociPass の秘密情報を設定させ，それを第三者に推測させることで AssociPass の推測攻撃に対する安全性評価を行った．AssociPass の設定条件は（m,n）=（10, 4）である．評価の結果 2 つの問題点が明らかになり，推測攻撃に対する安全性を損なう可能性があることがわかった．以降，本論文では “m” を AssociPass が認証画面に表示するシンボル（単語 or 絵文字）の数を表し，“n” は “m” 個のシンボルから関連付けることで入力するペア情報の数を表すものとする．

1 つ目の問題点は，容易に推測される関連付けによる単語ペアが作成されたことである．秘密情報となる単語ペアの関連付けに何の制約条件も設けず，推奨として「私的な関連付け」による単語ペアを作成するようアドバイスした．しかしながら，収集された秘密情報には単語ペアが容易に推測されうる関連付けによって作成されていたものがあった．「猫-哺乳類」といった名詞とその分類のような関連付けや，「裏-表」といった対義語による関連付けがその一例である．これらは，一般的な知識から容易に推測可能な関連付けであることから秘密情報として望ましくない．

もう 1 つの問題点は，4 ペアの単語を作成する上で用いた単語数に推測を容易にしうる傾向が見られたことである．4 ペアの単語を構成しうる単語数は 4, 5, 6, 7, 8 単語の 5 通りが考えられる．この 5 通りのうち，8 単語で 4 ペアを作成する場合はどの単語も 1 つのペアでのみ利用される（**図 1** 左）．これを「単語の重複利用がない」という．「単語の重複利用」とは，1 つの単語を複数のペアで使用することを意味する言葉として使用する．4〜7 単語で 4 ペアが構成される場合は，単語の重複利用が必須となる（図 1 中央，右．赤枠で囲まれた単語は全て重複利用されていることを示す）．しかしながら，収集された秘密情報を検証したところ，実験参加者の 75.6%が 8 単語を使用して 4 つの単語ペアを作成していた．この事実を攻撃者が推測攻撃に用いると，4,725 通り（$= {}_{10}C_2 * {}_8C_2 * {}_6C_2 * {}_4C_2/4!$）の秘密情報を試行するだけでなりすましに成功してしまうことになり，実質的な安全性が低くなる．ユーザにより作成される秘密情報にこのような偏りが発生することは，推測攻撃に有益な情報となりうるため望ましくない．

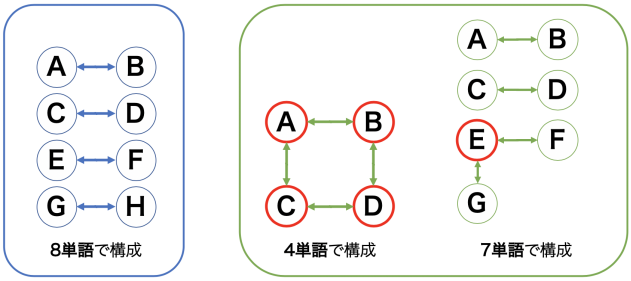

図 1 単語ペアの例

3. AssociPass の改善提案

3.1 改善提案のアイデア

前章で述べた AssociPass の 2 つの問題点に対して以下の変更を施すことで AssociPass の推測攻撃に対する安全性向上を試みた．

(案 a) 秘密情報を「単語ペア」から「絵文字ペア」に変更
(案 b) 秘密情報の構成を「4〜8 文字」ではなく「4〜7 文字」による 4 ペアに変更

(案 a) の変更は，情報の関連付けを多様化することで攻撃者による推測を困難にすると考える．その理由は，絵文字が単語と比較して多様な解釈ができる点にあると考えるからである．例えば**図 2** 左の絵文字であれば，「合掌」と解釈する人もいれば「ハイタッチ」と解釈する人もいると考えられる．Miller ら [5] の調査によると人の顔の表情を

*3 NPC=the Number of Possible Credentials

表す絵文字は人によって解釈が違うということが明らかにされている．図 2 右の絵文字は「失望」，「憂鬱」，「疑い深い」などと実験参加者によって異なる解釈がなされていた．このように絵文字を用いることにより，攻撃者は絵文字を多角的に解釈した上で関連付けを推測する必要が生じるため，推測攻撃を困難化できると考えた．

図 2　多様な解釈ができる絵文字の例

(案 b) の変更は，8 つの絵文字で 4 組の絵文字ペアを作成できないものとし，複数の絵文字ペアで同一絵文字の重複利用を必須とするものである．この変更により，ペア間で絵文字の「重複利用が必須ではない」という条件から「重複利用が必須である」という条件の下にペア作成をすることとなる．これによりユーザ間でペア作成時の条件が等しくなるため，4 ペアの作成に使用される絵文字数が 4〜7 文字に分散すると考えた．

3.2　プロトタイプシステム

本研究では，前節で述べた 2 つの改善案を AssociPass に施したプロトタイプシステムを Web アプリケーションとして実装した．提案手法では，AssociPass と同様に（m, n）=（10, 4）を採用した．

まず絵文字ペアの入力方法について述べる．**図 3** 左は，提案システムの秘密情報入力画面である．図に示す通り，画面内には円状に描かれた絵文字ノード (図 3 赤枠) が 10 個表示される．認証時には，これらの絵文字ノードから絵文字ペアを構成する 2 つの絵文字を見つけ出し，その片方のノードをタッチしたままもう片方のノードへドラッグし重ね合わせることで絵文字ペアの入力を行う (この入力動作を「ペア入力動作」と呼ぶ)．この際，ノードの始点，終点の順序はどちらでも良い．図 3 は龍の絵文字ノードをドラッグし，リンゴの絵文字ノードへ重ね合わせる操作を示したものだが，リンゴの絵文字ノードをドラッグし，龍の絵文字ノードに重ね合わせても同一の絵文字ペアが入力されることになる．

次に秘密情報登録方法について述べる．

（1）　ユーザ ID をシステムに登録
（2）　**図 4** の赤枠部分のような入力フォームに絵文字を 1 文字ずつ入力し，「ペア作成」ボタンを押してペアを登録する．
（3）　（2）の操作を 4 回繰り返し，4 組の絵文字ペアを登録する．この際，3.1 節の (案 b) の変更に則り，4〜7 絵文字で 4 組の絵文字ペアを構成しなければならない．つまり，（龍，リンゴ），（龍，電話）のように同じ絵文字を複数のペアに使用しなければならないということである．
（4）　プロトタイプシステムでは認証画面に 10 個の絵文字を表示するため，（3）で登録した絵文字ペアに用いた文字数（4〜7 絵文字）に対し不足している文字数分（3〜6 絵文字）の絵文字を登録する．この不足している文字数分の絵文字を「囮絵文字」と呼び，攻撃者が絵文字ペアを推測する際にペアの候補として迷う可能性の高い絵文字を設定することが望ましい．

最後に認証操作について述べる．ユーザ ID を入力すると，図 3 左に示す認証画面に遷移し，秘密情報登録時に登録した 10 個の絵文字が表示される．この際，10 個の絵文字は画面内のどのノードに表示されるかはランダムであり，かつ認証試行のたびに変化する．あとは秘密情報である絵文字ペアを構成する 2 つの絵文字を表示された 10 個の絵文字から見つけ出し，ペア入力動作を繰り返すことで 4 組の絵文字ペアを入力する．4 組の絵文字ペア入力が完了すると事前に登録した秘密情報との照合が行われ，秘密情報が一致すると認証成功となる．

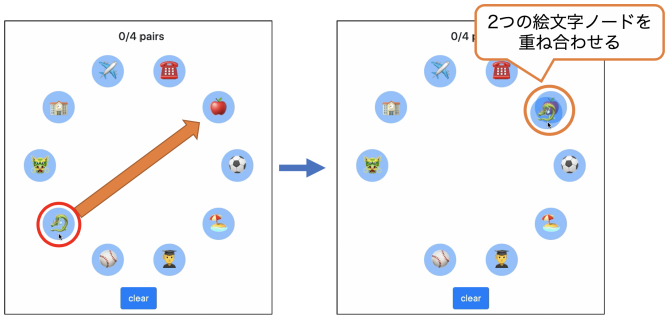

図 3　プロトタイプシステムの認証画面と秘密情報入力の様子

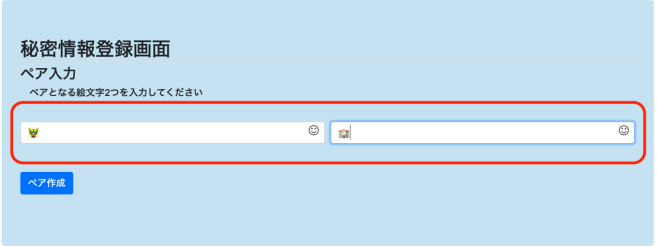

図 4　プロトタイプシステムの秘密情報登録画面

4.　評価実験

本研究では，3.1 節で述べた改善案の効果を評価するために，単語ペアを秘密情報とする AssociPass（以降，「単語版」とする）と絵文字ペアを秘密情報とするプロトタイプシステム（以降，「絵文字版」とする）を用いた比較実験

を実施した．なお今回の実験では，以下の 2 つの仮説に関する検証を目的とし「記憶可能性実験」と「推測攻撃に対する安全性評価実験」の 2 つの実験を実施した．

(H1)　秘密情報の記憶保持は，単語と絵文字で同等である．
(H2)　推測攻撃に対する安全性は，絵文字による秘密の方が単語による秘密よりも安全である．

実験に用いた単語版は絵文字版と秘密情報の構成条件を等しくするため，秘密情報の構成が 4〜7 単語となるように改変を加えた．本章では，実施した 2 つの実験について実験内容と実験結果について述べる．

4.1　記憶可能性実験

本実験では，実験参加者に絵文字版と単語版のいずれかを用いて秘密情報の設定を依頼し，一定期間後に再度認証を行わせることで自身の秘密情報を記憶保持できているかを検証した．

4.1.1　実験方法

(1)　事前準備: 実験目的とシステムの操作方法について説明を行った．その後，実験参加者を単語版と絵文字版のグループに分け，3.2 節で述べた方法に基づき，秘密情報をシステムに登録させた．秘密情報登録後，システムの操作に慣れてもらう目的で，3 回認証に成功するまで操作練習を行わせた．

(2)　操作実験 1: 事前準備を終了してから 10 分後に，1 回目の操作実験として評価対象のシステムを通じた認証を行った．認証成否を結果として記録し，記憶保持の検証に用いた．なお，事前準備と操作実験 1 は研究室内で実施した．

(3)　操作実験 2，3: 操作実験 1 終了から 1 週間後に操作実験 2 として，再度実験参加者に認証を依頼した．また操作実験 2 終了から 2 週間後に操作実験 3 として，同様に認証を依頼した．なお，操作実験 2，3 はオンライン実験として実施した．

各操作実験では 3 回認証を試みても認証に成功しなかった場合に「認証失敗」と判定した．これは銀行 ATM で許容されている入力回数と同じである．また本実験では操作実験の時間間隔として 10 分，1 週間，2 週間という 3 つの間隔を設定した．10 分間というのは，短期間でも覚えられないような秘密情報を実験参加者が登録していないかを確認するためである．また，個人認証の記憶可能性実験にて期間設定としてよく用いられる 1 週間より長い期間をあけると記憶可能性にどう影響するかを調査するため，2 週間という間隔を設定して実施した．本実験で使用する端末は macOS もしくは iOS が利用できる端末とした．これは絵文字版における絵文字のレンダリングの違い (**図 5**) による記憶可能性への影響を考慮する必要をなくすためである．実験参加者は大学生 20 名 (男性 16 名，女性 4 名) であり，両システム 10 名ずつとした．

図 5　絵文字レンダリングの違いの例

4.1.2　実験結果

実験結果を表 1 に示す．表内では秘密情報別に「何回目の試行で認証に成功したか？」と「認証失敗数」を示している（表の列ラベル順に説明）．実験から以下のことが明らかになった．

(結果 a1)　全実験参加者が，全操作実験（1, 2, 3）において認証に成功した．
(結果 a2)　全ての認証試行は，2 回までの試行回数内に認証に成功した．

表 1　各操作実験での認証成功数（成功に要した試行回数）と失敗数

条件		1 試行	2 試行	3 試行	失敗
絵文字版	操作実験 1	9	1	0	0
	操作実験 2	8	2	0	0
	操作実験 3	7	3	0	0
単語版	操作実験 1	10	0	0	0
	操作実験 2	9	1	0	0
	操作実験 3	9	1	0	0

4.2　推測攻撃に対する安全性評価実験

絵文字ペアによる秘密情報が単語ペアによる秘密と比較して他者による推測が困難であるかを検証するため，実験参加者を募り秘密情報の推測を行わせることで安全性評価実験を実施した．

4.2.1　実験方法

(1)　事前準備: 「実験回答用紙」を用意した．これは 4.1 節の記憶可能性実験で得られた登録情報に基づき，10 個の絵文字（または単語）で生成可能な 45 ペアの情報をリスト形式に書き出したものである（**図 6** に用紙の一部を示す）．なお 4.1 節で実験参加者が秘密情報を設定する際，設定した秘密情報が攻撃実験に利用されることは知らされていない．ただし，設定された秘密情報を利用することについては事前に同意を得ている．また本用紙には，この秘密情報を設定した人物についての 3 つの属性値（年齢，性別，職業）も記載した．

(2)　推測実験: 攻撃者役の参加者に「実験回答用紙」を渡し，秘密情報としている絵文字ペア（または単語ペア）を推測させた．この際，回答方法としては 4 ペアの選択を 4 回繰り返すという回答方法とした（図 6 は 3 ペ

アを選択している様子を表す）．これは秘密情報に設定している可能性が高いと推測した順に回答させることを意図したためである．したがって，最終的に 45 ペア中 16 ペアが回答として選択されることになる．なお以降では，k 回目の回答（k=1, 2, 3, 4）を「第 k 候補」と言及する．

なお第 1 候補の回答は，4〜7 文字の絵文字（または単語）で構成される 4 ペアを選択するよう参加者に制約を課した．これは第 1 候補として選択した 4 ペアが 1 回の推測攻撃として成立させるためである．

図 6　実験回答用紙

本実験には著者の研究室に所属する男性 5 人が攻撃者役として参加した．つまり，実験参加者は攻撃対象となる認証システムについて十分な知識を有していた．また各実験参加者は絵文字版 10 アカウントと単語版 10 アカウントの計 20 アカウント分の推測を行った．すなわち 4.1 節で収集された各秘密情報あたり 5 人の攻撃者による攻撃データが収集されたことになる．また推測を行うにあたって行動の制約は特に設けなかった．

4.2.2　実験結果

実験結果を表 2 に示す．本実験における攻撃成功とは，第 4 候補までの回答 16 ペアに攻撃対象者の秘密情報 4 ペアがすべて含まれていたことを意味する．両システムの攻撃成功数についてイェーツ補正のあるカイ二乗検定を行ったところ，システム間に統計的有意差はなかった（$\chi^2(1) = 1.634, p = 0.2011 > 0.05$）．

表 2 内の「推測された攻撃対象者名」列には秘密情報がすべて推測された攻撃対象者の情報を示した．表記方法について説明する．“sub3(1, 4)”とは sub3 が攻撃対象者の通し番号を表し，カッコ内の 1 つ目の数字“1”が秘密情報を特定した攻撃者の人数，カッコ内の 2 つ目以降の数字“4”は第何候補の回答で攻撃が成功したかを表す．つまり，絵文字版では 3 名（sub3, 5, 7）の秘密情報が特定され，そのうち第 3 候補までの選択で攻撃成功した例が 1 例，第 4 候補までの選択で攻撃成功した例が 2 例であったことを示している．単語版では 4 名の秘密情報が特定され，そのうち第 2 候補までの選択で 1 例，第 3 候補までの選択で 2 例，第 4 候補までの選択で 5 例が攻撃に成功した．

各回答候補ごとまでの回答で平均していくつの秘密情報ペアを特定できていたかを図 **7** に示す．第 4 候補までに特定されたペア数に対してイェーツ補正のあるカイ二乗検定を行ったところ，両システム間の結果に統計的有意差は見られなかった（$\chi^2(3) = 0.17, p = 0.982 > 0.05$）．だが，一貫して絵文字版の方が特定されたペア数は少ない結果となった．

表 2　人による推測攻撃の成功数と推測された攻撃対象者名

絵文字版	攻撃成功数	推測された攻撃対象者名
単語版	3（6.0%）	sub3(1, 4) sub5(1, 4) sub7(1, 3)
AssociPass	8（16.0%）	sub2(1, 4) sub4(3, 2-3-4) sub5(3, 4-4-4) sub7(1, 3)

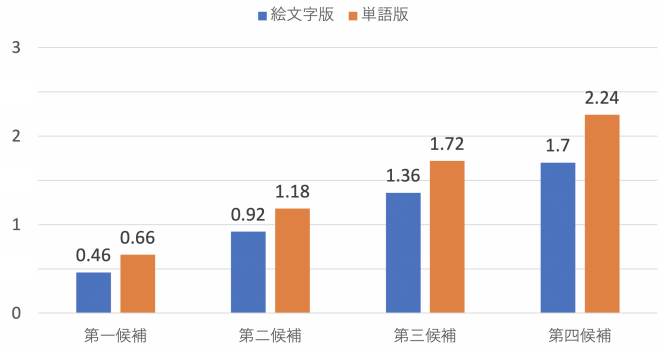

図 7　各候補での特定ペア数の平均

5.　考察

本章では 4 章で設定した 2 つの仮説を検証するため，推測攻撃に対する安全性と秘密情報の記憶保持の 2 点について絵文字版と単語版の比較考察を行う．また今後の課題についても述べる．

5.1　推測攻撃に対する安全性

4.2 節の実験結果から，絵文字版と単語版とで人による推測攻撃の成功率に有意な差は見られなかった．ただし，以下の 2 点は注目に値する点であり，さらに検証が必要だと考える．

- 成功数は倍以上の差が生じている
- 絵文字版は，複数の攻撃者から秘密情報特定される事例が発生していない

次に 4.1 節の実験で作成された秘密情報における偏りについて，山岸ら [3] が行った方法に基づき分析する．偏りが発生している場合，その事実を用いて攻撃者が推測攻撃を行うことで攻撃成功率が高くなる懸念があるからである．分析結果を表 3 に示す．

この結果から，秘密情報に発生する偏りについても絵文

表 3　秘密情報における偏りの分析結果

	絵文字版	単語版
(a) ペアの重複	40 ペアで重複なし	40 ペアで重複なし
(b) ペアを構成する文字の重複	63 文字中 10 文字重複 (16.0%)	66 単語中 11 単語重複 (17.0%)
(c) ペアを構成する文字数の重複	6/10 人が 7 文字使用	7/10 が 7 単語使用

字版と単語版で顕著な差は見られないという結果になった．これら 2 つの結果から，仮説（H2）は棄却されると考える．ただし今回の実験は小規模であり，実験参加者の属性にも偏りがあるので，より一般的な条件による大規模調査を行い再検証を行うべきだと考えている．

なお，「(c) ペアを構成する文字数の重複」について追加考察を行う．これはオリジナルの AssociPass で指摘された問題点であり，これに対して我々はペアを構成する絵文字・単語の重複利用を必須とすることで改善を試みた．しかしながら，多くのユーザが 1 絵文字・単語だけ重複利用するだけで 4 ペアを作成するという結果になり，問題改善には至らなかった．7 絵文字・単語で 4 ペアを作成した実験参加者にその理由を尋ねたところ，「絵文字の重複利用が困難であったため」(4 名) や「重複した単語でペアを作るのが面倒であった」(1 名) という回答を得た．このことから特定文字を複数のペアで重複利用することについて，何らかの負担を感じていることがうかがえる．特定文字を複数ペアで重複利用することには，記憶すべき絵文字・単語数を削減できるという利点もあると著者らは考えている．よって，利用者が重複利用に感じている負担の詳細について追加調査を行い，改善策を模索する予定である．

5.2　秘密情報の記憶保持

4.1 節の実験結果から，絵文字版と単語版における秘密情報の記憶保持について有意な差は見られなかった．このことから，秘密情報を単語から絵文字にすることで実用上の問題が発生することはなく，仮説（H1）は受容されると考える．

本実験で使用した秘密情報は最大で 7 絵文字（または単語）とその関連付けであり，暗証番号やパスワードと比較すると情報量は多い．それにも関わらず，2 週間の間隔を空けても認証に全員が成功したのは回答候補となる絵文字・単語群が認証画面に提示されるという認証方法が影響していると考える．この考えが仮に正しければ，ペアを構成する情報種には依存せずにこの記憶保持の効果が得られる可能性もある．この検証については今後の課題である．

5.3　今後の課題

今後の課題について 3 点ほど述べる．1 つ目は，大規模な評価実験の実施である．今回の評価実験は，著者の呼びかけに応じてくれた大学所属の 20 名＋ 5 名という規模で行われたものであり小規模であると言わざるをえない．また実験参加者の属性も理工系分野の知識を持ち，大半が 20 代男性という属性を持つ人であったことから偏った母集団による評価と言わざるをえない．したがって，今回の実験結果を一般化することは問題があると考える．この点については，クラウドソーシングを利用したオンライン実験を行うことを検討している．

2 つ目は，秘密情報登録用ユーザインタフェース（UI）の改善である．5.1 節内の表 3 の分析から実験参加者の多くが文字の重複利用の少ない構成の 4 ペアを選択していることが明らかになった．この理由の 1 つに秘密情報登録の UI に問題があるのではないかと考えている．図 4 に示されているが，現行の UI は，ペアを入力することを強く意識させたものになっている．これが利用者にペア情報を個別に考えさせることとなり，同一絵文字・単語の重複利用を難しくさせた可能性があると考えている．したがって，マインドマップ作成用 UI などを参考にペア情報の入力に囚われない秘密情報作成用 UI を検討し，それを用いて同一絵文字・単語の重複利用を促進できるかを検証する必要があると考えている．

3 つ目は，入力手法に起因する利用絵文字の偏りの改善である．5.1 節で分析した秘密情報の偏り以外に，絵文字版で新たに生じうる偏りの 1 つとして絵文字ペアに用いられた絵文字の「カテゴリ」に関する分析を行った．絵文字の「カテゴリ」には Unicode[6] で定義されている「group」という分類区分を用いた．分析結果を**図 8** に示す．

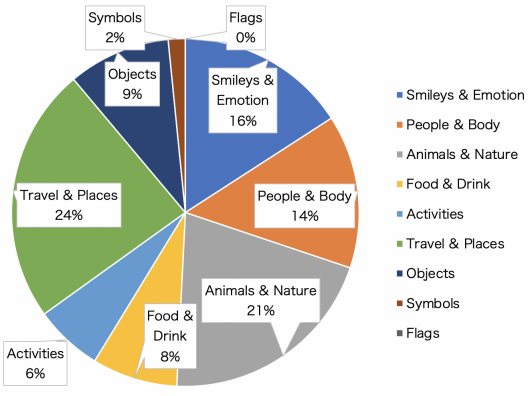

図 8　絵文字ペアに用いられた絵文字の「カテゴリ」の重複の偏り

図 8 より，「Smileys & Emotion」，「People & Body」，「Animals & Nature」，「Travel & Places」の 4 つのカテゴリに属する絵文字はより多くペアに使われ，「Symbols」，「Flags」は対照的にほぼペアに使われていないことがわかる．この結果を絵文字の入力手法の観点から考察する．本研究では絵文字の入力方法として，macOS あるいは iOS の絵文字キーボードが利用可能であった．絵文字キーボー

ドではカテゴリ毎に絵文字が参照でき，スクロールすることによりカテゴリを切り替えることができる．この絵文字キーボードに表示されるカテゴリ順は図 8 の右側に示すカテゴリの降順と同一である．つまり，図 8 の下側にあるカテゴリほど，参照するのにより多くのスクロールを必要とする．この絵文字キーボードにおけるスクロール量とペアに用いられた絵文字のカテゴリとの対応を見ると，より多くペアに使われた絵文字のカテゴリ（「Travel & Places」を除く）はスクロール量が少なく，キーボードを表示してすぐに選択可能な領域にあるカテゴリの絵文字であることがわかる．反対にほぼペアに利用されていない絵文字のカテゴリは，多くのスクロール量を要する位置に配置されている．今回の結果ではそこまで顕著な偏りがあるとは言い難い．しかしながら，このような入力方法に起因した利用絵文字の偏りは，秘密情報自体を表すものではないが，攻撃者にとっては秘密情報の推測に有用な情報となる可能性がある．そのため，今後は入力方法に起因した利用絵文字の偏りを生じないような入力方法を検討する必要があると考える．

6. 関連研究

最後に推測攻撃に対する安全性向上を目的とした個人認証の関連研究について述べる．

Chowdhury らは 4 枚の画像を秘密情報とし，その 4 枚の画像に対しそれぞれヒントを定義できる認証方式である PHAS（PassHint Authentication System）[7] を提案した．PHAS では秘密情報である画像を含む画像群とともに秘密情報である画像のヒントが認証画面に表示され，このヒントが秘密情報を思い出す手がかりとなる．Chowdhury らは，ユーザが個人的なエピソードや記号などをヒントとして設定することで推測攻撃に対する安全性の向上を目指した．しかし評価実験の結果，80 件の推測攻撃に対し 21 件（26.3%）が推測に成功する結果となった．

Woo らはユーザの life-experience（人生経験）に関する既存の記憶を秘密情報に用いる LEPs（life-experience passwords）[8] を提案した．この手法では，ユーザが定義した life-experience に対してシステムから複数の質問が出され，その質問に対する回答が秘密情報となる（ex: Q.“パリ旅行は誰と行きましたか？”=>A.“一郎，太郎”）．認証時には life-experience に関する秘密情報登録時とは異なる質問が複数個提示され，その質問に回答し（ex: Q.“パリ旅行は何人でいきましたか？”=>A.“2 人”）目標値として設定された個数以上の回答が秘密情報と一致していた場合に認証成功となる．家族や親友による推測攻撃実験を実施した結果，その攻撃成功率は 9.5%であった．

2 つの先行研究を紹介したが，AssociPass も含めたこれらの研究の共通点は，暗証番号やパスワードとは異なり，回答候補やヒントを認証画面に提示し，その情報に基づいて回答する形態の認証手法である．回答候補が画面に提示されるため攻撃者にとって推測攻撃がしやすい認証手法であると言えるが，その中でも今回の絵文字版 AssociPass は推測攻撃成功率が低い部類ではないかと考えられる．ただし，秘密情報や評価方法が研究毎に異なるため，推測攻撃成功率の値だけを取り上げて単純比較できるものではない点には留意する必要がある．

7. おわりに

本研究では単語ペアを秘密情報とする AssociPass における記憶保持の利点を維持しつつ推測攻撃に対する安全性を向上させることを目的とし，秘密情報に絵文字ペアを用いた個人認証を提案した．プロトタイプシステムを実装し，記憶可能性・推測攻撃への安全性に関する評価実験を実施した．その結果，提案システムの秘密情報は 2 週間の間隔を空けても秘密情報の記憶保持は可能であり，AssociPass と同程度の記憶可能性を有することを明らかにした．また，実際に収集した秘密情報に対する推測攻撃の結果，有意な差は見られなかったが，単語ペアによる秘密情報よりも絵文字ペアによる秘密情報の方が推測攻撃に対して安全である可能性が示唆された．今後の課題として，秘密情報登録時のインターフェイスを再検討するとともに，多様な属性を対象にした参加者よる大規模実験を行い，その改善効果を再検証する必要がある．

参考文献

[1] TeamID: The Top 50 Worst Passwords of 2019, 入手先＜ https://www.teamsid.com/1-50-worst-passwords-2019/ ＞（参照 2020-4-17）.

[2] Li, Y., Wang, H. and Sun, K.: A Study of Personal Information in Human-chosen Passwords and Its Security Implications, *The 35th Annual IEEE International Conference on Computer Communications*, IEEE(2016).

[3] 山岸 伶，高田 哲司: 推測攻撃に対する安全性改善を目的とした単語ペアの集合を秘密とする個人認証，情報処理学会論文誌，Vol.60, No.4, pp1119-1128(2019).

[4] 山岸 伶: 推測攻撃への安全性向上を目的とした個人認証の研究:秘密情報に「情報間の関連」を用いた試み，電気通信大学平成 30 年度修士論文.

[5] Miller, H., Thebault-Spieker, J., Chang, S., Johnson, I., Terveen, L. and Hecht, B.: “Blissfully happy” or “ready to fight” :Varying Interpretations of Emoji, Proc. the 10th International Conference on Web and Social Media(ICWSM 2016), pp.259-268, AAAI press (2016).

[6] unicode: Full Emoji List, v13.0, 入手先＜ https://www.unicode.org/emoji/charts/full-emoji-list.html ＞（参照 2020-8-11）.

[7] Chowdhury,S., Poet, R. and Mackenzie,L.: Passhint: Memorable and Secure Authentication, *Proc. CHI'14*, pp.2917-2926,ACM(2014).

[8] Woo,S.S., Artstein,R., Kaiser,E.,Le,X. and Mirkovic,j.:Using Episodic Memory for User Authentication, *ACM Transactions on Privacy and Security*, Vol. 22 No. 2 Article 11.