推測攻撃対策を意図したペア情報による個人認証手法の安全性・利便性評価：単語ペアと絵文字ペアの比較（第２報）

横山 佳紀[1,†1,a)]　高田 哲司[1,b)]

概要：推測攻撃に対する安全性を改善しうる個人認証手法 “AssociPass” について，単語と絵文字を秘密情報とした場合の安全性と利便性に関する比較評価について報告する．知識照合型個人認証には推測攻撃という脅威が存在し，総あたり攻撃よりも効率良くなりすましを行う手法として現実的な脅威となっている．この脅威に対する対策として我々の研究グループで提案した個人認証手法が「ペア情報の集合」を秘密情報とする AssociPass である．この手法について先行研究の成果から利便性を損なうことなく安全性を改善しうることが明らかにされているが，研究室内実験の結果であり，一般化可能な結果とは言いがたい．そこで本研究ではクラウドソーシングを通じて参加者を募り，単語ペアと絵文字ペアの２条件で評価実験をあらためて実施した．その結果，利便性と推測攻撃への安全性について，単語ペアと絵文字ペアで差がないという結果を得た．しかしその一方で，先行研究で明らかにされていた問題点が絵文字ペアを秘密情報に用いることで改善されるという結果も得られた．

キーワード：個人認証，知識照合型個人認証，推測攻撃，絵文字，ユーザビリティ

Security Evaluation of Pair-based User Authentication against Guess Attack using Words and Emojis (2nd report)

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

Abstract: One of the threats to the knowledge-based user authentication is guess attack. Human-chosen passwords or PINs are unevenly distributed. Using this bias, an attacker attempts to impersonate someone efficiently than brute-force attack. Our research group has proposed a user authentication scheme called “AssociPass”, in which the credential is a set of paired information. Our works has revealed the following two results about this scheme: (1) the scheme can improve security against guess attack without hampering usability. (2) further security improvement was suggested by using Emoji-pair credential instead of word-pair. However, the results were based on small experiments. In this study, we conducted a new experiment with participants recruited through crowd-sourcing. The results show that there is no significant difference in both usability and security against guessing attacks between word-pair and emoji-pair conditions. On the other hand, we also obtained a favorable result that one of the issues identified in the previous work could be improved by using emoji-pairs based credential. The paper reports on the conducted experiment and its results.

Keywords: User authentication, Knowledge-based user authentication, Pair-based credential, Guess attack, Emoji, Usability

1. はじめに

知識照合型個人認証には攻撃者が攻撃対象の秘密情報を推測して「なりすまし」を試みる推測攻撃という脅威が存

[1] 電気通信大学
The University of Electro-Communications
[†1] 現在，民間企業
Presently with Private Company
[a)] y.yokoyama052@gmail.com
[b)] zetaka@computer.org

在する．多くの人間にとってパスワードや暗証番号の選択は難題である．とりうるすべての候補からランダムに一つを選択すること自体困難であり，仮に選択できたとしてもそれを記憶保持することは容易ではない [1]．したがって，選択されるパスワードや暗証番号には記憶保持が優先され，結果として秘密情報として使用される情報と使用されない情報に “かたより” が発生する [2], [3], [4], [5]．このかたよりを逆手に取り，攻撃対象者が秘密情報として設定していると思われる値を推測して攻撃を行うことで，総あたり攻撃を行うよりも少ない攻撃回数で「なりすまし」を試みることを推測攻撃という．

この問題に対し我々の研究グループでは “AssociPass” とよぶ知識照合型個人認証手法を提案している [6]．この手法は推測攻撃に対する安全性を向上させることを目的とし，「情報ペアの集合」を秘密情報とする手法である．情報ペアとは，例えば（机，龍）という形式であり，２情報の組み合わせを指す．詳細は 2 章で述べるが，これにより秘密情報の記憶保持可能性を損ねることなく推測攻撃に対する安全性を向上させうることを明らかにした [6]．

しかし評価実験の結果，提案手法に起因する秘密情報による “かたより” が発生することも明らかになった．そこでその問題に対する改良案として秘密情報を「単語による情報ペア」から「絵文字による情報ペア」に変更する提案を行った．絵文字は色や形，意味解釈の多様性があるため，単語よりも多様なペア情報が作成される可能性があると考えたからである．この提案について研究室内実験を実施した結果，安全性の改善効果が期待できることを明らかにした [7]．

そこで我々は，絵文字ペアによる AssociPass の推測攻撃に対する安全性改善効果が一般化可能な結果かどうかについて，多くの実験参加者の協力のもとあらためて検証実験を行なった．その結果，単語ペアと絵文字ペアでは推測攻撃に対する安全性に差があるとは言えないという結果となった．しかし，絵文字ペアの利用により提案手法の秘密情報に起因するかたよりが減少するといった有益な結果も得られた．本論文では今回実施した検証実験とその実験結果について述べる．

2. AssociPass について

本章では山岸らによって提案された個人認証手法 AssociPass について説明する (以降，AssociPass を “*AsPs*” と略す)．AsPs の秘密情報は「ペア情報の集合」であり，(机，龍) といった情報を n 個，秘密情報として事前に決定しておく．なお我々の研究では一貫して $n = 4$ とした．

図 1 上図は AsPs の認証画面である．画面上に 10 個のノードが円環状に描画されており，各ノードの中にはペアの構成要素となる情報が表示される (以降，ノード内情報を「構成情報」と呼ぶ)．この 10 個のノード内に表示される構成情報は，重複のない 10 種の情報であり，その表示場所は認証試行のたびにランダムに配置される．この画面を用いて秘密情報４ペアを入力し，入力値と既定の秘密情報が「４つのペア情報の集合」として同値であれば認証成功となる．ペアの入力方法は，ノードのドラッグ操作で実現している (図 1 下図)．ペア情報を構成する構成情報の 1 つが表示されているノードをもう 1 つの構成情報が表示されているノードまでドラッグすることでペア情報が入力される．

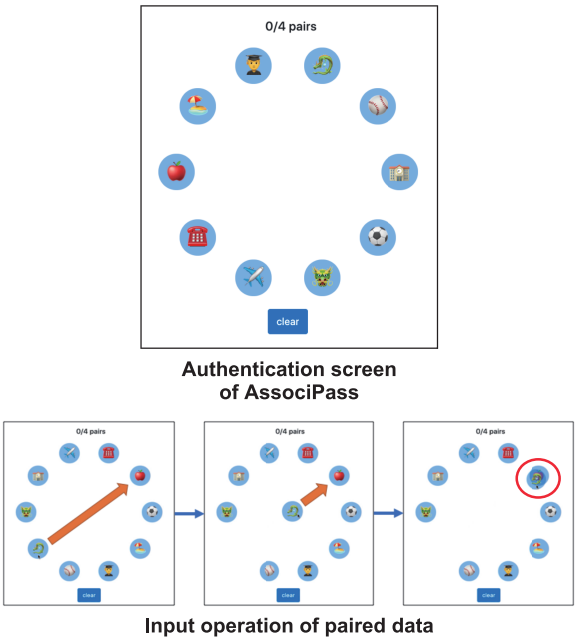

図 1 AssociPass の認証画面と入力操作

2.1 AssociPass の秘密情報と安全性

AssociPass(AsPs) の秘密情報は「ペア情報の集合」である．推測攻撃への安全性を改善する方法としてペア情報を提案した理由は，多様な秘密情報をユーザが作成可能と考えたためである．ペア情報を 1 つ作成するためには「２つの情報とその関係性」という 3 情報を決定する必要がある．よって 1 情報ですむパスワードや暗証番号よりも秘密情報に多様性が生まれる可能性がある．一方，攻撃者が推測攻撃を行う時にはこれらの情報を推測しなければならない．よって推測しなければならない情報が増えることから，推測攻撃に対する安全性が改善されると考えたのである．

AsPs の総あたり攻撃に対する安全性について述べる．AsPs における秘密情報の通り数は 148,995 ($=_{45}\ C_4$) である．10 個のノードから作成可能なペア情報は 45 通り ($=_{10}\ C_2$) であり，45 通りのペア情報から 4 ペアを秘密情報とするので上記の値となる．この値の逆数が，総あたり攻撃に対する AsPs の安全性となる．

ここで注意したいのは，秘密情報つまり 4 ペア情報の構成情報数である．４つのペア情報をいくつの構成情報で作成するかは５つのケース (4,5,6,7,8 個) が存在する．それぞ

れのケースで作成可能な秘密情報の通り数を**表 1** に示す．

表 1 構成情報数別 4 ペア情報の通り数

構成情報数	4	5	6	7	8
4 ペアの通り数	3,150	34,020	69,300	37,800	4,725

したがって，正規利用者が作成する秘密情報の構成情報数はこれら 5 つのケースに分散することが望ましい．逆に，秘密情報の構成情報数が 4 や 8 にかたよると，総当たり攻撃や推測攻撃への安全性も低下することとなる．

3. これまでの研究成果と本研究の目的

本章ではこれまでの研究成果を総括し，その延長である本研究の目的を明らかにする．山岸らの研究 (2019)[6] では，AssociPass を提案しその有用性について「単語によるペア情報の集合」を秘密情報として評価を実施した．実験の結果，(a) 作成した秘密情報の 1 週間間隔での記憶保持が可能であることと，(b) 人による推測攻撃で 496 回のシミュレーション攻撃による攻撃成功率は 10%未満であり，かつ 70 回までの推測では攻撃成功例なし，という結果をえた．一方，(c) 単語ペアでも第三者による推測が容易な秘密情報が設定されることと，(d)50%以上の実験参加者が秘密情報を「8 単語による 4 ペア構成」としていたことが明らかになった．どちらも推測攻撃を容易にしうる懸念があり，今後の課題とされた．

横山らの研究 (2020)[7] では，上記 (c)(d) の問題に対する対策として秘密情報の構成情報を絵文字にすることを提案した．また秘密情報における構成情報数のかたよりを低減するため，8 情報 4 ペアによる秘密情報を禁止とし，4〜7 情報による 4 ペアに制限した．この新たな提案内容について単語と絵文字による秘密情報で比較評価を行った．その結果，人による推測攻撃で絵文字の攻撃成功例が 3/50 件 (6.0%) であったのに対し，単語による攻撃成功例は 8/50 件 (16.0%) という結果をえた．また秘密情報の構成情報数に関するかたよりについては，単語が 7/10 人が 7 単語による 4 ペアであったのに対し，絵文字では 6/10 人が 7 絵文字による 4 ペアという結果であった．どちらの結果も単語・絵文字間で有意な差はなかったが，絵文字による改善可能性が示唆される結果であった．

今回の論文 (2022) ではこれまでの研究結果をふまえ，以下の 2 点を明らかにする目的で評価実験を実施した．

(1) 一般化可能な評価結果の獲得
これまでの評価実験は研究室内実験であり，著者が直接依頼可能な方を対象に実験に参加頂いた．よって実験参加者の年齢や属性がかたよっており，人数も全体で 30 名未満と少人数であった．そこで今回は評価実験をオンラインで実施可能にし，クラウドソーシングを通じて幅広い年齢・属性を持つ実験参加者を募って実験を行なうことで一般化可能な結果を得ることを目的とした．

(2) 絵文字と単語のどちらが推測攻撃に対して安全か
横山らの研究 (2020) で，絵文字の方が単語よりも推測攻撃に対して安全である可能性が示唆されていた．しかし有意差は確認されず一般化可能な結果ではない．よって今回の実験であらためて検証を行い，どちらの構成情報が推測攻撃に対して安全かを明らかにすることを目的とした．

4. 検証実験

AssociPass(AsPs) の利用可能性と安全性について，単語と絵文字による秘密情報間で各効果に差が生じるかについて以下の 3 つの仮説をたてて検証実験を実施した．

H1）秘密情報の記憶保持可能性は同等程度である
H2）認証時間は同等程度である
H3）推測攻撃に対する安全性は単語ペアより絵文字ペアのほうが安全である

本章では，上記の仮説を検証するために実施した 2 つの実験について実験方法と実験結果を述べる．

4.1 利用可能性検証実験

本節では，前述の H1 と H2 を検証するために実施した実験について実験方法と結果を述べる．

4.1.1 実験方法

実験方法は以下の通りである．

(1) 実験説明と同意取得：新たな個人認証手法の評価実験であることと実験手順の概要を説明し，実験参加への同意を得た．

(2) 認証システムの説明：動画を用いて AssociPass の仕組みと操作方法を説明した．手法の理解を確認するため説明動画の視聴後に 3 問の選択肢問題を出題し，全問正解するまで次の手順に進めないようにした．

(3) 秘密情報作成：実験実施者が実験参加者に割りあてた情報種 (単語 or 絵文字) で 4 つのペア情報を秘密情報として作成させた．なお本作業の際，個人認証の利用シーンとして「Socail Network Service(SNS) におけるユーザアカウント作成」であると事前に説明した上で作業を依頼した．またこの手順における所要時間を「秘密情報登録時間」として測定した．そのあと認証画面に表示する１０個の回答候補に満たない分の情報（２〜６個）を「おとり情報」として追加選択させた．

(4) 計算タスク：ランダムに生成された 1 〜 3 桁の四則演算を 30 問出題し，全問正解するまで次の手順に進めないようにした．この手順は実験参加者の working memory をリセットする目的で実施した．

(5) 認証操作（I）：作成した秘密情報で AssociPass による認証を実施させた．この際，認証成否，認証成功まで

表 2　実験参加者の人口統計情報と実験時の利用機材
Table 2　Demographic Information of Participants and Used Equipment

	total	male	female	20's	30's	40's	50's	60's	others	computer	mobile phone	tablet
単語	53	37	16	4	14	19	12	4	0	29	23	1
絵文字	45	30	15	6	16	12	8	1	2	4	38	3

に要した試行回数 (最大 3 回) と認証成功時の認証時間の 3 情報を実験システム経由で記録した．なお 3 回までの試行で認証成功に至らなかった場合は認証失敗と判定した．

(6) アンケート（I）: 実験参加者の属性情報，秘密情報に関する質問を実施した．

(7) 認証操作（II）: 認証操作（I）から 1 週間以上経過した後にあらためて認証を実施させた．実施方法・記録情報は認証操作（I）と同じである．

(8) アンケート（II）: 提案手法の利用可能性に関する主観的印象について調査を実施した．

本実験は 2022 年 2 月頃にオンライン実験として実施した．実験参加者は Yahoo クラウドソーシング [13] を通じて単語，絵文字の各条件ともに 100 名を募集し，上記手順のアンケート（I）までを実施させた．その後，認証操作 (I) で認証に成功した参加者を対象に 1 週間後に行う実験（上記実験手順 7，8）への参加募集をあらためて行い，最終的に単語条件は 5 3 名，絵文字条件は 4 5 名の参加者が上記手順における手順（8）まで実施した．なお謝礼については，アンケート (I) までを実施した参加者に 25 PayPay ポイント，アンケート (II) まで実施した参加者には追加で 50 PayPay ポイントを提供した．なお本実験は実験実施前に所属組織の倫理委員会による審査を受け，承認を受けた上で実施している．

実験参加者の属性と使用機材に関する情報を**表 2** に示す．表内のデータは，上記の実験手順で手順（8）まで完了した実験参加者に関する情報である．ここで実験機材のかたよりについて言及しておく．単語条件では計算機と携帯端末の割合が同等程度であるのに対し，絵文字条件では携帯端末での実施数が多数となった．これは参加者募集における条件設定の影響である．絵文字の見た目が統一された状態で評価を行うことが望ましいと考えたため，絵文字条件の実験では「Apple 製端末所有者のみ参加可」という条件を設定して参加者を募集した．そのためこのような分布となっている．

4.1.2　実験結果

認証成功率：

表 3 に単語・絵文字の 2 条件における認証成功率と認証成功までの試行回数に関する結果を示す．この結果は認証操作 (II) におけるものであり，2 つの値で結果を示している．左側の整数値が認証に成功した人数を示し，括弧内のパーセント値はそれを認証成功率として示したものである．また “2nd trial”, “3rd trial” の各列における値は実験結果を累積値として示している．つまり 2nd trial 列の値は，2 回目の入力までに認証に成功したデータを示しており，その値には 1 回目の入力で認証に成功したデータも含まれていることを意味する．

表 3　認証試行回数と認証成功率
Table 3　Authentication success rate through the number of trials

	Over 7 days		
	1st trail	2nd trial	3rd trial
単語	32(60.4%)	44(83.0%)	49(92.5%)
絵文字	26(57.8%)	34(75.6%)	37(82.2%)

表 4　秘密情報登録時間
Table 4　Credential registration time.

	平均値 (s)	標準偏差	中央値 (s)
単語	290.6	126.0	281.9
絵文字	313.7	141.9	277.8

秘密情報を設定した日に実施された認証操作 (I) ではどちらも認証成功率が 100%で単語と絵文字の 2 条件間に差は見られなかったが，7 日以上経過した認証操作 (II) では単語よりも絵文字の方が認証成功率が低くなるという結果になった．しかし，表 3 の 3rd trial 列の値を用いてカイ 2 乗検定を行った結果，2 条件間に有意差があるとはいえない，という結果となった ($\chi^2(1) = 1.514, p = 0.219 > 0.05$).

秘密情報登録時間：

表 4 に秘密情報登録時間の結果を示す．秘密情報登録時間については，平均値では絵文字の方が 20 秒以上長くかかる結果となった．しかし，測定データに正規性がないと判断されたので Mann-Whitney の U 検定により検定を実施したところ，中央値に有意差があるとはいえない，という結果となった ($U = 1096.0, p = 0.494 > 0.05$).

認証時間：

表 5 に認証時間の結果を示す．表 5 内には二つの表があるが，上の表は認証操作 (I) における結果であり，下の表は認証操作 (II) における実験結果を示している．また各表の最右列にある “min/max” は認証時間の最小値・最大値を示している．4 条件（単語・絵文字 × 認証操作 (I)・(II)）におけるデータについてデータ群に正規性があるとは言えないことが shapiro-wilk 検定により確認できたので，Mann-Whitney の U 検定による検定を行った．その結果，認証操作 (I)(II) のどちらにおいても単語と絵文字の条件間に有意な差があるとは言えない，という結果となった．

(認証操作 (I): $U = 1446.0, p = 0.071 > 0.05$，認証操作 (II): $U = 1137.0, p = 0.695 > 0.05$)

表 5　認証時間
Table 5　Authentication time in the registration day and over 7 days

Registration day				
	平均値 (s)	標準偏差	中央値 (s)	min/max
単語	25.8	16.6	20.9	10.7/104.6
絵文字	38.5	105.5	17.3	7.9/710.2

Over 7 days				
	平均値 (s)	標準偏差	中央値 (s)	min/max
単語	74.3	73.2	43.9	12.2/376.1
絵文字	98.3	187.9	49.2	13.1/1196.3

アンケート：
以下の 3 問について，7 段階リッカート尺度でアンケートを実施した．
Q1) 秘密情報の作成負担 (「1:負担は小さい〜7:負担は大きい」と定義)
Q2) 秘密情報の記憶負担 (英数字 8 文字パスワード，4 桁暗証番号との比較で実施．「1:負担は小さい〜7:負担は大きい」と定義)
Q3) 認証時間 (英数字 8 文字パスワード，4 桁暗証番号との比較で実施．「1:短い〜7:長い」と定義)
調査結果を**表 6** に示す．表内の各値は調査結果の平均値である．なお太字は 2 条件のうち値の小さい方を示している．表内の 5 項目について Mann-Whitney の U 検定により検証を行なったが，いずれも有意差は見られなかった．したがって，絵文字を構成情報に用いることで利用可能性の面で単語よりも新たな負担が発生しているという主観的評価は見られなかった．

4.2　安全性検証

本節では前述の H3 を検証するために実施した実験について，実験方法と結果を述べる．

4.2.1　実験方法

実験方法の概要は以下の通りである．
（手順 b1）攻撃用データの収集
（手順 b2）人間による推測攻撃の安全性評価

表 6　利用可能性に関するアンケート結果
Table 6　Survey result

	単語	絵文字
秘密情報の作成負担	4.42	**3.87**
秘密情報の記憶負担 (vs. Pwd)	**4.40**	4.51
秘密情報の記憶負担 (vs. Pin)	**4.74**	5.04
認証時間 (vs. Pwd)	4.13	**4.02**
認証時間 (vs. Pin)	**4.38**	4.53

（手順 b3）収集データの分析による安全性評価
各手順について説明する．

（手順 b1）：本データの収集はオンラインタスクとして 2021 年 08 月に実施した．Yahoo クラウドソーシング [13] を通じ，単語，絵文字ペアともに 150 人を募集した．この際，同一の参加者が単語ペアと絵文字ペアの両方の実験に参加できないよう条件設定をした．本タスクの詳細は，4.1.1 項で説明した実験手順のうち手順（1）から手順（6）に該当するものと同一である．ただし，本タスクにおいて作成された秘密情報が推測攻撃に利用されることについては言及しない状況でタスクを依頼した．タスク完了後に収集データを精査し，不適切な秘密情報を設定しているデータと計算タスク後の認証操作で認証に失敗しているデータを収集データから除外した．結果として，絵文字版で 143 件，単語版で 128 件の秘密情報を収集した．

（手順 b2）：人間による推測攻撃の安全性評価は，収集した秘密情報から攻撃対象データを抽出し，秘密情報作成者とは別の参加者を募った上で推測攻撃を依頼した．以下に詳細を述べる．

(b2-1): 攻撃データの選択：（手順 b1）で収集した秘密情報の中から，以下の 4 条件に合致する秘密情報を各条件ごとに 20 アカウント分づつランダム選択で抽出した．

- WdR：単語による秘密情報
- Wd8：単語による秘密情報，ただし 8 単語で 4 ペアを構成
- EmR：絵文字による秘密情報
- Em8：絵文字による秘密情報，ただし 8 絵文字で 4 ペアを構成

なお，WdR，EmR 条件で選択されたデータが Wd8，Em8 条件のデータとして再び選択されないよう配慮した．Wd8，Em8 の 2 条件を設定した理由は，多くのユーザが 8 単語で 4 ペアの秘密情報を作成する傾向があることが明らかにされており [6]，秘密情報の構成情報数が既知の場合，そうでない場合と比較して推測攻撃に対する安全性が異なるかを検証するためである．

(b2-2): 人間による推測攻撃：実験参加者に実験内容の説明を行い，その後，認証画面を見ながら攻撃対象ユーザの秘密情報を推測するよう依頼した．各実験参加者には前述の 4 条件のうち (WdR, EmR) から 1 条件，(Wd8, Em8) から 1 条件をそれぞれ割り当て，2 条件で計４０アカウント分の推測攻撃を依頼した．本実験では認証画面で回答可能な全４５種のペア情報を一覧できる実験専用 Web ページを構築し，オンライン実験として実施した．実験においては時間制限は設けず，メモ・辞書等の使用や Web ページ等の閲覧について一切制限をしなかった．本実験における収集情報は，秘密情報と推測されたペア情報１４組であり，実験参加者が秘密情報として使用している可能性が高い順に以下の三段階に分けて回答させた．

第一段階：4 pairs
第二段階：第一段階で選択したペア以外から 5 pairs
第三段階：第一，第二段階で選択したペア以外から 5 pairs

回答を三段階に分けた理由は，攻撃者視点で判断された秘密情報らしさに優先度をつけ，各段階までに回答されたペア情報を用いて推測攻撃シミュレーションを行うためである．第二段階までに回答された 9 つのペア情報を用いると 4 組の 4 ペア情報による推測回数が 100 回超 ($_9C_4 = 126$) となり，第三段階までの 1 4 個のペア情報だと 1,000 回超の推測回数 ($_{14}C_4 = 1,001$) となり（1, 100, 1000）回の三段階の推測攻撃回数に対する攻撃成功率を導出できるからである．

また実験用 Web ページでは，組みあわせ可能な全ペア情報の他に以下の 2 情報を実験参加者に提示した．

(1) 全 4 条件において，攻撃対象データを作成した人の年齢と性別（例：30 代 男性）
(2) Wd8, Em8 の 2 条件において「秘密情報 4 ペアが 8 情報で構成されている」という事実

なお推測攻撃を実施した実験参加者は，著者が所属する大学で情報セキュリティを専攻している学生および卒業生の 12 名（男性 11 名，女性 1 名）である．彼らを攻撃者役に選択した理由は，個人認証やパスワード・暗証番号等のかたよりに関する教育を受けており，攻撃者として適切な資質を持っていると考えたからである．また彼らは（手順 b1）には参加しておらず，実験用 Web ページに提示した上記 2 項目以外に攻撃データの作成者に関する情報は持っていない状況で実験を実施した．なお実験の謝礼は 1 時間あたり 1,200 円とし，さらに秘密情報の特定に成功した場合には追加報酬として 1,000 円を提供することを実験前に伝えた上で実施した．

（b2-3）**アンケート**：推測攻撃の実施内容についてアンケートを実施した．

（手順 b3）：収集データの分析による安全性評価は，（手順 b1）で作成された秘密情報を対象に以下の 4 つの観点で収集された秘密情報の「かたより」を分析し，これにより単語と絵文字でどちらの情報種が推測を容易にしうる傾向があるのかを明らかにすることを試みた．

- ペア情報単位でのかたより
- ペア情報を構成する構成情報でのかたより
- おとり情報のかたより
- 秘密情報 4 ペアを構成する構成情報数のかたより

この分析は「暗証番号認証では，1111 や 1234 といった暗証番号を使うユーザが多い」ということと同様の秘密情報が単語や絵文字によるペア情報にどの程度発生するのかを明らかにすることでもある．もちろん，このようなかたよりが少ない方が推測攻撃に対して安全ということになる．

表 7　人による推測攻撃の攻撃結果
Table 7　The results of guess attack by human attackers

	特定回数 (特定成功率)	特定アカウント数
WdR	14/120 (11.7%)	7/20 (35.0%)
EmR	19/120 (15.8%)	7/20 (35.0%)
Wd8	19/120 (15.8%)	8/20 (40.0%)
Em8	37/120 (30.8%)	12/20 (60.0%)

4.2.2　実験結果

人による推測攻撃の安全性評価

人による推測攻撃の結果を**表 7** に示す．各条件に対し 6 名の攻撃者が推測攻撃を行うよう割り当てを行なったので，各条件における攻撃回数の母集団は 120 回 (20 アカウント ×6 名の攻撃者) となっている．表内の「特定回数」列の値は，120 回の攻撃のうち秘密情報の特定に成功した回数を示しており，「特定アカウント」列は各条件 20 アカウントのうち，秘密情報が特定されたアカウント数を示している．なお本結果は，(b2-2) で述べた三段階の回答手順のうち，第三段階までの回答に基づくシミュレーション結果であり，最短で 127 回の推測で秘密情報が特定されることを意味する．この結果について WdR-EmR 間と Wd8-Em8 間のそれぞれに対してカイ二乗検定による検定を実施した．その結果，WdR-EmR 間は有意差が見られなかったが，Wd8-Em8 間は有意差が見られた ($\chi^2(1) = 7.547, p = 0.006 < 0.05$).

かたより分析による安全性評価

（手順 b3）で実施した秘密情報のかたよりに関する分析結果を示す．まずはじめに，(手順 b1）で収集された秘密情報に関する母集団情報を**表 8** に示す．続いて実施した 4 種の分析結果を以下の各表に示す．

- ペア情報単位の分析結果: **表 9**
- 構成情報単位での分析結果: **表 10**
- おとり情報の分析結果: **表 11**
- 構成情報数の分析結果: **表 12**

これらの結果について統計検定を実施した．表 9 の結果については，ペアの重複がなかったペア情報を 1，同一ペアが 2 つ存在していたペア情報に 2, 同一ペアが 3 つ存在していたペア情報に 3... という具合にペア情報の重複数に応じてランク付けを行い，Wilcoxon の順位和検定を実施した．その結果，ペア情報の重複度合いについて有意差が見られた ($W = 164,058, p = 1.798 \times 10^{-9} < 0.05$)．したがって，単語よりも絵文字による秘密情報の方がペア情報としてかたよりが大きくなるといえる．

また表 10 および表 11 の結果についても同様の方法で検定を実施した．その結果「構成情報単位でのかたより」および「おとり情報のかたより」についても，有意差が見られた (下記参照).

- 表 10：$W = 576,592, p = 2.2 \times 10^{-16} < 0.05$
- 表 11：$W = 88,773, p = 5.563 \times 10^{-7} < 0.05$

表 8　分析対象となった秘密情報
Table 8　Overview of the collected credential information

	絵文字条件	単語条件
アカウント数	143	128
ユニークペア情報数	512	494
ユニーク構成情報数	381 絵文字	554 単語

表 9　ペア単位における秘密情報のかたより
Table 9　Credential biases based on a paired words/emojis

	絵文字ペア	単語ペア
1 アカウントのみで利用	469 (91.6%)	482 (97.6%)
2 アカウントで利用	35 (6.8%)	8 (1.6%)
3 アカウントで利用	5 (1.0%)	3 (0.6%)
5 アカウントで利用	2 (0.4%)	1 (0.2%)
8 アカウントで利用	1 (0.2%)	0 (0.0%)

表 10　構成情報単位での秘密情報のかたより
Table 10　Credential biases based on a word or an emoji

	絵文字	単語
1 アカウントでのみ利用	196(51.4%)	413(74.5%)
2-5 アカウントで利用	149(39.1%)	114(20.6%)
6-10 アカウントで利用	27(7.0%)	21(3.8%)
11-15 アカウントで利用	6(1.6%)	3(0.5%)
16-20 アカウントで利用	1(0.2%)	3(0.5%)
21-25 アカウントで利用	2(0.5%)	0(0.0%)

表 11　おとり情報のかたより
Table 11　Frequetly used words / emojis for decoy

	絵文字	単語
1 アカウントでのみ利用	201(66.3%)	206(83.4%)
2-5 アカウントで利用	102(33.7%)	38(15.4%)
6-10 アカウントで利用	0(0.0%)	3(1.2%)
おとり情報の総数	303	247

表 12　4 ペアに用いた構成情報数の分布
Table 12　The number of words/emojis for making 4-pairs

構成情報数	絵文字ペア	単語ペア
8 情報	72(50.3%)	**96**(75.0%)
7 情報	**15**(10.5%)	13(10.2%)
6 情報	**13**(9.1%)	8(6.2%)
5 情報	**34**(23.8%)	9(7.0%)
4 情報	**9**(6.3%)	2(1.6%)

次に 4 ペアを構成する構成情報数のかたよりについて統計検定を実施した．表 12 の結果について Fisher の正確確率検定を実施した結果，絵文字と単語の構成情報数に有意差が見られた ($p = 7.682 \times 10^{-5} < 0.05$)．そこで，どの構成情報数で単語と絵文字に差があるかをカイ二乗検定で個別に検証したところ，構成情報数 4,5,8 で秘密情報数の割合に有意差が見られた．

- 8 情報：$\chi^2(1) = 17.419, p = 2.999 \times 10^{-5} < 0.05$
- 5 情報：$\chi^2(1) = 14.187, p = 1.655 \times 10^{-4} < 0.05$
- 4 情報：$\chi^2(1) = 3.882, p = 0.049 < 0.05$

5. 考察

5.1 仮説検証

4 章冒頭で設定した仮説について 4 章の実験結果から結論を述べる．まずはじめに 4.1 節の結果から，仮説 H1，H2 は肯定されたと考える．仮説 H1 の肯定理由は，認証成功率の結果から 1 週間以上の間隔においても秘密情報の記憶保持可能性について単語と絵文字の 2 条件間に有意差は見られなかったためである．仮説 H2 についても，単語と絵文字ペアの条件間で秘密情報登録時間および認証時間に有意な差は見られなかったことから，仮説 H2 は肯定されると結論づけた．

次に仮説 H3 だが 4.2 節の結果から否定されたと考える．人による推測攻撃実験では，ランダム選択された秘密情報に対する攻撃成功率について単語と絵文字条件間で有意な差は見られなかった．また収集された秘密情報のかたより分析では，ペア単位，構成情報単位，おとり情報の 3 種の分析において有意差が見られ，どれも絵文字の方が複数アカウントで同一情報が使われる傾向にあるという結果となった．ただし，かたより分析の結果は絵文字と任意の単語における母集団の差が大きいため，それを考慮すると今回の結果を推測攻撃を容易にしうるほどのかたよりとみるべきかは議論の余地が残ると考える．

一方，構成情報数の分布ではこれまでの研究とは異なる結果が得られた (表 12 参照)．単語ペアでは 75%の秘密情報が 8 情報で 4 ペアを構成していたのに対し，絵文字の方は 8 情報による秘密情報は 50.3%にどどまり，かわりに 4,5 情報による秘密情報が単語条件と比較して多い結果となった．この分布は推測攻撃を困難にする上で望ましい結果である．人による推測攻撃の結果 (表 7) から Em8 条件の特定成功率は最も高い結果であったが，その対象者は単語条件と比較して少なくなることから実質的な脅威度は懸念されるほど高いとは言えない．すべての秘密情報が 8 情報で構成されていると想定して推測攻撃が行われた場合の攻撃成功率は以下の通りになると考えられるからである．

- 単語条件　：11.85% = 15.8%(Wd8) × 0.750
- 絵文字条件: 15.49% = 30.8%(Em8) × 0.503

しかし，この議論も H3 を肯定することにはならない．よって絵文字ペアによる秘密情報は単語と比較して推測攻撃に対する安全性を改善しうるとは言えない，と結論づける．

5.2 今後の課題

今後の課題について 2 点述べる．1 つめは秘密情報作成方法に関する工夫を考えている．今回の実験ではペア情報の作成を依頼したためペア単位で個別に情報を作成していた．これに対し，複数の構成情報とその関係を示す「情報グラフ」を一定の条件のもとで先に作成し，その中から

秘密情報にする情報ペアを選択する方法が考えられる．3 ノード 3 ペアの情報グラフを作成し，その中から最大 2 ペアを秘密情報として選択可能にする，という具合である．またこの工夫により構成情報数のかたよりも低減する可能性があると見込んでいる．

もう 1 つは，単語・絵文字以外の構成情報の導入である．今回絵文字による秘密情報の安全性は単語と同等程度であったが，構成情報数のかたよりは軽減されるという結果を得た．今回の結果をふまえ単語・絵文字以外の構成情報を用いることや，構成情報を 1 種に限定せず多種混合を認めるなどの方法についても検討を進めていく．

5.3 関連研究

関連研究については紙面の都合で簡単に述べるにとどめる．知識照合型個人認証の 1 つに正規利用者しか分からないエピソードを秘密情報とし，なぞなぞ形式で認証を行う手法が提案されている [8], [10]．しかし文献 [10] による評価では，近親者による推測攻撃で 9.5%の攻撃成功率という結果が示されている．

文献 [9] では，認証画面に提示されたヒントに該当する画像を画像群の中から選択する認証手法を提案している．このヒントは秘密情報である画像に正規利用者がつけるもので，本人のみが分かるヒントとなることを期待したものである．この手法に対して推測攻撃に関する評価を行った結果，26.3%の攻撃成功率であった．

絵文字を応用した個人認証手法も提案されている [11], [12]．文献 [12] では 795 人に秘密情報を作成させ，その内容を分析している．その結果，秘密情報として利用されやすい絵文字が存在することを明らかにしている．

我々の研究と先行研究との違いは 2 点ある． 1 つはペア情報の利用により攻撃者が推測する必要のある情報を増やしている点であり，もう 1 つは，シミュレーションとはいえ 1000 回の推測に相当する推測攻撃の安全性を評価している点である．

6. おわりに

知識照合型個人認証には推測攻撃という脅威が存在し，ランダム値を用いてなりすましを行うよりも効果的に攻撃が可能なことから現実的な脅威である．この問題に対し，我々の研究グループでは “AssociPass” と呼ぶペア情報の集合を秘密情報とした個人認証を提案している．ペア情報を用いることで攻撃者が推測しなければならない情報が増え，推測攻撃への安全性が改善されると考えたためである．

先行研究の結果から，単語によるペア情報で推測攻撃への安全性が確認されたが，その一方で推測攻撃を容易にしうる問題点も明らかになった．それらの問題点に対して単語のかわりに絵文字を用いることで改善を試みた結果，改善効果が示唆される結果となった．しかし，これらの結果は研究室内実験によるものであり，一般化できるものではなかった．そこで本研究ではクラウドソーシングを通じて参加者を募り，オンライン実験にて利用可能性と安全性評価を実施した．その結果，秘密情報の記憶保持と認証時間については単語と絵文字条件間で差がないことを明らかにした．一方，安全性についても単語と絵文字条件間で差は見られず，絵文字を導入することで単語条件で明らかになった問題点を改善しうるとはいえない結果となった．しかし「構成情報数のかたより」という問題点では絵文字の導入による改善効果が見られた．今回の実験結果をふまえ，単語・絵文字以外のペア情報の導入や秘密情報の作成方法を工夫することで推測攻撃に対する安全性を有する個人認証手法の実現を模索していく予定である．

参考文献

[1] M.D.Leonhard and V.N.Venkatakrishnan, A comparative study of three random password generators, IEEE Int'l Conf. on Electro/Information Technology, pp.227-232, (2007).

[2] Y.Li, H.Wang and K.Sun, A study of personal information in human-chosen passwords and its security implications, IEEE Int'l Conf. on Computer Communications (IEEE INFOCOM 2016), 9 pages, (2016).

[3] D.Wang, Q.Gu, X.Huang, and P.Wang, Understanding Human-Chosen PINs: Characteristics, Distribution and Security, ACM on Asia Conf. on Computer and Communications Security (ASIA CCS '17), pp.372–385, (2017).

[4] M.Weir, S.Aggarwal, B.d.Medeiros and B.Glodek, Password Cracking Using Probabilistic Context-Free Grammars, IEEE Symp. on Security and Privacy, pp.391-405, (2009).

[5] Nord Security, Top 200 most common passwords, available from ⟨https://nordpass.com/most-common-passwords-list/⟩(accessed at 2022-08-20)

[6] 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, pp.1119-1128, (2019).

[7] 横山佳紀, 高田哲司: 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, コンピュータセキュリティシンポジウム 2020, (2020).

[8] 増井俊之, EpisoPass: エピソード記憶にもとづくパスワード管理, コンピュータセキュリティシンポジウム 2013, (2013).

[9] S.Chowdhury, R.Poet, and L.Mackenzie, Passhint: memorable and secure authentication, SIGCHI Conference on Human Factors in Computing Systems (CHI '14), pp.2917–2926, (2014).

[10] S.S.Woo, R.Artstein, E.Kaiser, X.Le, and J.Mirkovic, Using Episodic Memory for User Authentication, ACM Trans. on Priv. Secur, Vol.22, Issue.2, 34 pages, (2019).

[11] L.Kraus and R.Schmidt, Implications of the Use of Emojis in Mobile Authentication, Symp. on Usable Privacy and Security (SOUPS'16), (2016).

[12] M.Golla,D.Deterring,M.Dürmuth, EmojiAuth: Quantifying the Security of Emoji-based Authentication, USEC Workshop, (2017).

[13] Yahoo Japan, Yahoo クラウドソーシング，入手先 ⟨https://crowdsourcing.yahoo.co.jp/⟩(参照 2022-08-20),