情報処理学会論文誌 Vol.60 No.4 1119–1128 (Apr. 2019)

推薦論文

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

山岸 伶[1,a)] 高田 哲司[1,b)]

受付日 2018年7月16日, 採録日 2019年1月15日

概要：知識照合型個人認証の脅威として推測攻撃が存在し，これはとりうる秘密情報から，攻撃者が利用者の秘密情報だと考える順序をつけ，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，多くの利用者が設定している秘密情報を優先する傾向型推測攻撃と正規利用者の属性や好みに基づいて順序をつける個人情報型推測攻撃に分類される．推測攻撃は，秘密情報の偏りや利用者の個人情報に基づいた脆弱な秘密情報により可能となる．これらの脆弱な秘密情報は作成・記憶保持可能である点を重視する利用者の秘密情報設定戦略に起因する．本研究では，a) 推測攻撃に対する安全性改善，b) 秘密情報の記憶保持が可能，c) 利用者が秘密情報を作成可能の 3 要件を満たす個人認証を目的とし，単語ペアを秘密情報とする個人認証を提案する．単語ペアを秘密情報とすることは選択する情報を 2 つに増やし，そのペア間の関連も利用者が定義可能な点から，自由度が増加して推測攻撃に対する安全性が向上すると考えた．この提案に基づいてプロトタイプシステムを実装し，要件 a) と b) の観点で評価実験を実施した．その結果，提案手法は 70 試行までは推測攻撃の成功例がなく，1，2 週間隔での利用でも記憶保持が可能という結果を得た．

キーワード：個人認証，推測攻撃，単語ペア，情報間の関連，利便性

Word-pair Based User Authentication System for Better Security against Guess-attack

Rei Yamagishi[1,a)] Tetsuji Takada[1,b)]

Received: July 16, 2018, Accepted: January 15, 2019

Abstract: “Guess-attack” is one of threats to a knowledge-based user authentication. In this attack, attackers attempt credential candidates that the attackers with the order that attackers suppose users’ credentials. The guess-attack is enabled by vulnerable credentials based on a bias of confidential and users’ personal information. These vulnerable credentials are caused by the user’s strategy for credential setting that users focus on creation/memory retention. We consider that we could realize a user authentication that meets the following three requirements ((a) security improvement against guess-attack, (b) memorability of a credential, (c) users create their credentials by themselves). And we propose a novel user authentication that uses a set of word-pairs as a user credential. We also have implemented a prototype authentication system based on the ideas and conducted an evaluation study with subjects. We have got two results from the study. One of results is about security against guess-attack. No subject can identify target credentials by guessing within 70 trials. The other result is a memorability of a proposed credential. All subjects can keep their own credential even in using it at one or two week(s) interval.

Keywords: user authentication, guess-attacks, word-pair, usability

[1] 電気通信大学
The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[a)] r-yamagishi0@mail.uec.jp
[b)] zetaka@computer.org

本論文の内容は 2017 年 10 月のコンピュータセキュリティシンポジウム 2017（CSS2017）にて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

1. はじめに

パスワードや暗証番号など知識を秘密情報とする個人認証は，現在でも幅広く利用されている．本論文では，知識を用いる個人認証手法を「知識照合型個人認証」と呼ぶ．知識照合型個人認証に対する攻撃方法として総あたり攻撃が存在する．総あたり攻撃ではとりうるすべての秘密情報を順番に試行することで，正規利用者へのなりすましを試みる．この総あたり攻撃を効率化する手法として「推測攻撃」があり，攻撃者が秘密情報の候補から正規利用者の秘密情報だと考える順序をつけ，その順に試行することでなりすましを試みる．

推測における順序のつけ方で，秘密情報の推測方法を大きく以下の 2 種類に分けて定義する．

(A) 傾向型推測攻撃
(B) 個人情報型推測攻撃

(A) の傾向型推測攻撃は多くの利用者が設定している秘密情報を正規利用者が利用している，と仮定して秘密情報を推測する方法である．この攻撃方法に基づき，攻撃を自動化するツール [1], [2] も存在している．(B) の個人情報型推測攻撃は，攻撃対象が誰であるかが既知であるとし，その人物の属性や好みに基づいて対象の秘密情報を推測する方法である．たとえば，「彼はお酒が好きなので，好きなお酒の銘柄をパスワードにしているだろう」と考える．

推測攻撃が可能な理由は，正規利用者が設定する秘密情報が，偏りや正規利用者の個人情報を持つからである．偏りを持つという事実は傾向型推測攻撃を可能にし，多くのユーザが利用しているパスワードランキングからも見てとれる [3]．ランキング上位に見られるキーボード配列や数字，アルファベットの規則的な羅列は，正規利用者にとって秘密情報設定時に取得可能な情報であると考える．一方で，正規利用者の個人情報を含む秘密情報も存在しており，この事実が個人情報型推測攻撃を可能にしている．Wang らは情報漏洩したパスワードデータセットを調査し，パスワード中に正規利用者の姓名や誕生日が含まれることを明らかにした [4]．

推測攻撃を可能にする秘密情報は，以下の 2 点の秘密情報選択・作成戦略により生じると考える．

(a)「既知」または「取得可能」な情報を選択
(b) (a) を満たす情報の中で，記憶保持が可能な情報を選択

上記 (a) の理由により正規利用者が思いつかず，秘密情報の候補にならない情報群が存在する．また，上記 (a) を満たす情報群であっても，(b) を満たしうるものはさらに限定される．このように候補が限られることが推測攻撃につながりうる秘密情報の生成につながっているといえる．

推測攻撃を困難化する方法として考えられるのは，秘密情報の選択・作成に正規利用者を関与させないことである．代わりに，システムが推測攻撃に安全とされる秘密情報を生成し，秘密情報として利用させることである．しかし，この方法では秘密情報の記憶保持が困難という問題が生じる．秘密情報の記憶保持は，知識照合型個人認証の利用における必要条件であり，この要件を緩和することは望ましいとはいい切れない．利用者は記憶保持が困難だとすれば，秘密情報を紙に書き留める，パスワードマネージャを利用するなど別の方法で秘密情報を維持する必要が生じる．これは知識照合型個人認証の利点を損ねるとともに，情報漏洩や紛失など別の懸念を持ち込むことになる．

そこで本論文では，利用者が作成・記憶保持可能でありつつ，推測攻撃に対する安全性を改善しうる知識照合型個人認証の実現に取り組み，「単語ペアの集合」を秘密情報とする新たな知識照合型個人認証を提案する．このアイデアに基づきプロトタイプシステムを実装し，推測攻撃に対する安全性と秘密情報の記憶保持可能性について被験者による評価実験を行った．以降本論文では，2 章で提案手法のコンセプトやプロトタイプシステムについて述べ，3 章で評価実験について述べる．また，4 章では評価実験の結果をふまえて考察を行い，5 章で関連研究について述べる．

2. 提案手法

2.1 提案手法のアイデア

繰り返しになるが，本論文における目的は以下の 3 要件を満たす知識照合型個人認証を実現することである．

a) 推測攻撃に対する安全性改善
b) 秘密情報の記憶保持が可能
c) 利用者が秘密情報を作成可能

そこで我々は，「単語ペア」を秘密情報の基本要素とすることを提案する．ここでいう単語ペアとは，2 つの名詞単語から構成される「組情報」であり，(学校，虎)，(地下鉄，時計) がその一例である．要件 c) を満たすために，単語ペアは利用者が自ら設定し，ペアとする 2 単語間に「関連」があるものとした．また，制約条件とはしないものの，一般的によく知られている関連よりも「私的な関連」であることが望ましい．この「単語ペア」という秘密情報が残り 2 要件を満たしうる理由について述べる．

要件 a) を満たしうる理由は，「単語ペア」という秘密情報は以下の 2 点の選択の自由度を高めると考えたためである．1 つ目は選択する情報の増加による自由度の増加である．個人認証において秘密情報を決定する場合，多くの利用者は「1 つ」の情報を選択・作成していると考えられる．これに対し，秘密情報が 2 つ以上の情報によって構成されれば，攻撃者が推測しなければならない情報が増えることになり，当該攻撃への安全性向上できると考えたからである．一方，3 以上の単語からなる「組情報」に関しては，単語ペアよりも作成が容易ではないと考えた．もう 1 つは，単語間の「関連」も自由に定義可能という点にある．なぞなぞや質問・回答形式による認証手法が提案されているが，

それらの手法は単語ペアのうちの 1 つとその関連をユーザに開示したうえで，残りのもう 1 つの情報を回答する形式と見なすことができる．この場合，ユーザが設定できるのは回答となる情報 1 つのみとなり，推測攻撃に対して安全とはいい難い．これに対して本提案では，2 単語とその単語間の関連を利用者が自由に決定することができる．これらの自由度の高さは，秘密情報の推測を困難にするうえで有益であると考える．

要件 b) を満たしうる理由は，単語ペアが記憶保持の面でも利点を持つことにある．認知心理学の研究によると，1 つの事柄を思い出すことと比較し，2 つの関連した事柄を思い出す方が容易である [5]．関連のある単語ペアを秘密情報とすれば，記憶負担を増やすことなく秘密情報を保持できると考えた．

2.2 プロトタイプシステム

本研究では，前節のアイデアを基に個人認証のプロトタイプシステムを iOS アプリケーションとして実装した．前節で秘密情報は「単語ペア」としたが，プロトタイプシステムにおいて 1 組の単語ペアではなく複数組の単語ペアとする．

図 1 左は，ユーザ名入力後に表示される秘密情報入力画面である．図に示すとおり，画面内には円として描かれた単語ノードが複数個表示される．認証時には，これらの単語ノードから秘密情報である単語ペアを入力する．単語ペアの入力は，単語ペアを構成する 2 単語を見つけだし，そのノード間を線で結ぶ動作をすることで入力する（図 1 右参照）．この際，ノード間の始点，終点の順序はどちらでもよい．つまり単語ペアが（学校，虎）とした場合，学校ノードから虎ノードへ結ぶ場合とその逆の場合がありうるが，どちらの場合であってもシステムは単語ペアとして入力を受け取る．

秘密情報の登録方法について述べる．

(1) 単語ペアの作成：システムから指定される数の単語ペアを作成する．この際，秘密情報は単語ペアの集合なので同一単語ペアを複数回を複数個登録することはできないが，1 つの単語を複数の単語ペアに含めることは許容する．つまり（学校，虎），（学校，虎）という 2 ペアを秘密情報に登録することはできないが，（学校，虎），（学校，虹）の 2 ペアは秘密情報にできる．

(2) ユーザ名の登録（**図 2** 上部）

(3) 単語群の登録：単語設定画面（図 2 下部）に必要な単語群をシステムに登録する．(1) で作成した単語ペアの単語群を登録し，次に不足分の単語を登録する．たとえば，画面に表示される回答候補数を 10 として，秘密情報の 4 組の単語ペアとした場合，必要な単語数は 4 から 8 単語となる．したがって，回答候補数が 10 になるまで不足分の単語（2〜6 個）を追加登録する．この単語を「おとり単語」と呼ぶが，名称のとおり攻撃者が単語ペアを推測する際に迷う可能性の高い単語を設定することが望ましい．

(4) 単語ペアの登録：図 1 に示す画面を用い，単語間に線を描画する操作を通じて 2 単語をペアにする．これを秘密情報に必要な数になるまで繰り返す．

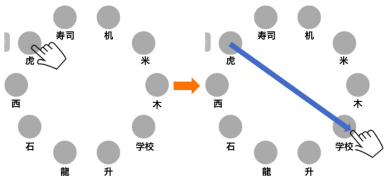

図 1 プロトタイプシステムの関連の登録，認証画面
Fig. 1 Word-pair credentials input operation.

図 2 プロトタイプシステムの単語の登録画面
Fig. 2 Screen snapshot of word registration interface.

最後に認証操作について述べる．ユーザ名を入力すると，図 1 左に示す画面が表示される．この際，各回答候補の単語が画面内のどの位置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．あとは前述したとおり，秘密情報である単語ペアを回答候補群から見つけ出し，線を結ぶ操作を通じて入力する．この操作を必要回数繰り返し，入力結果が設定した秘密情報と同一であれば，正規利用者として認証する．

2.3 理論的安全性

知識照合型個人認証における理論的安全性は，一般的にとりうる秘密情報の数の逆数となる．しかし，プロトタイプシステムは回答選択方式による秘密情報の入力となるため，パスワードなどとは異なり入力インタフェースによる制約も受ける．本節では，入力可能な秘密情報数を明らかにすることで，プロトタイプシステムの理論的安全性を示す．まずはじめに，単語ペアを 1 つ入力する際のとりうる数を考える．ここで変数となるのは秘密情報入力画面の回答候補数である．これを w とすると今回のプロトタイプシステムでは，w=10 である．この w の中から 2 つの単語を選択して単語ペアを入力するので，とりうる単語ペアの数 (m) は以下の式 (1) で表すことができ，w=10 の場合には 45 通りとなる．

$$m = {}_w\mathrm{C}_2 \tag{1}$$

このとおり，秘密情報が単語ペア 1 つだけでは安全性が十分とはいえない．そこで本研究では複数の単語ペアからなる集合を秘密情報としている．この集合が含む単語ペアの数を v とすると，とりうる秘密情報の数 (n) は式 (2) で表すことができる．

$$n = {}_m\mathrm{C}_v \tag{2}$$

3. 評価実験

本研究では，2.1 節で述べた 3 要件のうち「推測攻撃に対する安全性」と「秘密情報の記憶保持」について評価実験を実施した．本章では，実施した実験の詳細とその結果について述べる．

3.1 記憶保持評価実験

本実験では，被験者に秘密情報の設定とその一定期間後に記憶保持しているかの検証としてプロトタイプシステムを通じて個人認証を 3 回行わせた．

3.1.1 実験方法

本項では，実験手順について述べる．

(1) 事前準備：被験者に対し，実験目的とプロトタイプシステムについて説明を行った．被験者は被験者は 2.2 節で述べた方法に基づき，秘密情報をプロトタイプシステムに登録した．秘密情報を登録後，登録した秘密情報の再確認とプロトタイプシステムの操作に慣れてもらう目的で，認証に 3 回成功するまで練習を行わせた．

(2) 1 回目実験：(1) を終了してから 15 分後に，1 回目の記憶保持検証を行った．検証方法はプロトタイプシステムを通じた個人認証であり，その認証成否を結果として記録した．

(3) 2，3 回目実験：1 回目の実験終了後，x 週間間隔を空けて 2 度，記憶保持検証を行った．

記憶保持検証において，操作失敗をしても再度入力が認められ，認証の失敗は 3 回目で判定される．つまり，2 回までの操作失敗を許容し，3 回連続して認証操作に失敗した場合に「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．本実験では被験者を 2 つのグループに分けた．1 つは x=1 と（Group1 とする），もう 1 つは x=2 とした（Group2 とする）．1 および 2 週間間隔における記憶保持実験は，提案手法の想定する主な利用シーンである Web システムにおいて，60 日にわたり Web システムにおけるパスワードの利用を調査した研究 [6] から不適切ではないと考えた．この調査の研究で，ユーザは平均して 25 個のユーザアカウントを所持し，2 週間という期間でこれらのアカウントの 70%を利用することが明らかにされている．このことから 2 週間の記憶保持が可能であれば，ユーザが利用するサービスの 70%で，我々が提案する個人認証が適用できると考える．また，記憶保持について比較検証を行うためにより短い 1 週間間隔を設定した．被験者は 19 名（男性 15 名，女性 4 名）の大学生であり，Group1 が 7 名，Group2 が 12 名とした．

表 1 各記憶保持検証での認証成功数（成功に要した試行回数）と失敗数

Table 1 The result of the credential memorability experiment: the number of cases in a successful and a failed authentication.

条件	1 試行	2 試行	3 試行	失敗
Group1-Exp1	7	0	0	0
Group1-Exp2	6	0	1	0
Group1-Exp3	7	0	0	0
Group2-Exp1	12	0	0	0
Group2-Exp2	11	1	0	0
Group2-Exp3	12	0	0	0

3.1.2 実験結果

それぞれの検証時に，個人認証に失敗した数と「認証成功」の中でも認証操作に要した試行回数の内訳を**表 1** に示す．なお表中の条件列に記載されている文字列 “Exp” の右の数字は，何回目の実験かを意味している．結果，すべての被験者がすべての実験において認証に成功した．また，1 回の認証試行で認証成功しなかった事例は，計 52 回の認証中 2 例だけであった．

3.2 推測攻撃に対する安全性評価

提案手法の秘密情報を他者が推測可能かを検証する目的で，安全性評価実験を実施した．1 章で述べたように推測攻撃は，「傾向型推測攻撃」と「個人情報型推測攻撃」に分類される．「傾向型推測攻撃」は秘密情報の偏りに起因するため，設定された提案手法の秘密情報を利用し，その偏りを分析することで安全性を評価できる．したがって，3 章の記憶保持評価実験で収集した秘密情報の偏りを分析することで評価する．「個人情報型推測攻撃」は正規利用者に関する情報に起因するため，正規利用者が設定した単語が提示される提案手法では特に懸念される．これは，正規利用者が秘密情報を思い出す手がかりとなると同時に，攻撃者にも秘密情報を推測する手がかりを与えることになるためである．したがって，本研究では記憶保持評価実験で収集した秘密情報に対して，別の被験者が「推測攻撃」を行うことで検証する．以降では，個人情報型推測攻撃に対する安全性評価実験方法について説明する．

3.2.1 実験方法

記憶保持評価実験で収集した秘密情報に対して，別の被験者が攻撃者となり「推測攻撃」を行うことで評価を行った．各攻撃者は単語ペアの候補（2.3 節で述べたように 45 ペア）から正規利用者が秘密情報として設定しうる優先順位をつけることで，推測攻撃をシミュレートする．つまり，

攻撃者の選択した優先順位が高いものほど推測攻撃では先に試行し，低いものほど後に試行されると見なして，優先順位を試行回数に変換する．したがって，各攻撃あたり，試行回数とその試行回数における攻撃成功可否（あるいは，4 ペアすべてではないが特定できているペア数）が測定できる．以下では，攻撃者と被攻撃者（秘密情報の正規利用者）の関係，攻撃者の優先順位のつけ方（実験方法），実験条件について説明する．

「個人情報型推測攻撃」は正規利用者の情報をもとに推測を行うため，「攻撃者が正規利用者について知っている情報」が攻撃の成否に影響を与えると考える．本実験では，「攻撃者が正規利用者について知っている情報」は攻撃者と被攻撃者の関係性によって異なると仮定し，その関係性に基づき被験者群を以下の 3 グループに分けて実験を実施した．

Group-A：攻撃者も被攻撃者も同じ研究室のメンバであった．

Group-B：攻撃者も被攻撃者も同じサークルのメンバであった．

Group-C：攻撃者は被攻撃者を知らない Group-A，B 以外のメンバとした．被攻撃者は Group-B のメンバとした．

このグループ分けにより，以下の 2 点の検証が可能になる．

(a) 攻撃者と被攻撃者が知人かどうかで攻撃成功可否が異なるか

(b) 知人であっても，その関係性によって攻撃成功可否が異なるか

上記 (a) は Group-B と C では推測される秘密情報を同一とし，攻撃者と知人であるかないかという点が異なるため，この 2 グループを比較することで検証が可能となる．上記 (b) は Group-A と B は共に同じコミュニティ内の知人が攻撃者と被攻撃者になるが，そのコミュニティの性質が異なり，この 2 グループを比較することで検証可能となる．

実験は，「推測攻撃用紙」（**図 3**）を攻撃者に配布した．この「推測攻撃用紙」には被攻撃者の秘密情報の候補となる全 45 単語ペア（式 (1) 参照）が書かれている．以下に述べる方法で，攻撃者は「推測攻撃用紙」に正規利用者が秘密情報として設定しうる優先順位をつけた．攻撃者は，攻撃対象者の秘密情報と思われる単語ペアを 4 つ選択し，これを第 1 候補から第 4 候補まで 4 回繰り返して回答することで優先順位をつけた．つまり，推測攻撃用紙の 45 単語ペアのうち，4 つずつ計 16 単語ペアが選択されることになる．

また，実験環境は現実の攻撃環境を考慮し以下の条件で実施した．

- 攻撃対象の秘密情報は安全性評価実験を行うことを知らされずに作成された．
- 実験時には，推測攻撃対象である秘密情報が誰によって作成されたかを被験者（攻撃者）に通知した．
- 推測攻撃に必要となる情報収集を可能とするため，攻撃者に Web ページ閲覧を許可した．

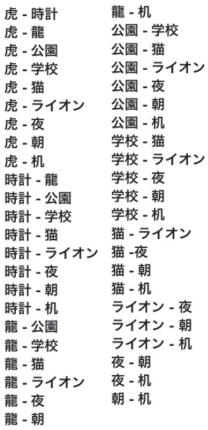

図 3 推測攻撃用紙

Fig. 3 An answer sheet for the guess attack experiment.

表 2 推測攻撃に対する安全性評価実験の被験者数と総攻撃数

Table 2 The number of subjects and attack trials in each condition at the guess attack experiment.

条件	被験者数	1 人あたりの攻撃回数	攻撃数
Group-A	7	6	42
Group-B	8	7	56
Group-C	6	8	48

表 3 攻撃の成功率と推測された被験者

Table 3 The result of the guess attack experiment(1): attack success rates in each condition.

条件	攻撃成功数	攻撃成功率（%）	推測された被験者名
Group-A	4	9.52	sub1(3)，sub2(1)
Group-B	3	5.36	sub8(1)，sub9(2)
Group-C	3	6.25	sub8(1)，sub10(2)

本実験に参加した被験者は 21 名（男性 16 名，女性 5 名）であり，3 グループのそれぞれに属する被験者人数は，**表 2** の「被験者数」列に示している．また「攻撃数」列に各グループにおいて実施した攻撃数を示している．Group-A，B では，各被験者が同一グループ内に割り当てられた攻撃者自身以外の被験者の秘密情報を攻撃するので，被験者（攻撃者）数を n とすると，攻撃数 u は $u{=}n(n-1)$ となる．また Group-C は各被験者が Group-B に割り当てられた被験者の秘密情報を攻撃するので 48 回の攻撃（= 被験者数 6 × 被攻撃者数 8）となる．

3.2.2 実験結果

グループごとに第 4 候補おける攻撃の成功数を**表 3** に示す．各グループの攻撃成功率について，カイ二乗検定を行ったところ，3 グループ間に統計的有意差はなかった

表 4 推測に成功した数と特定した候補
Table 4 The result of the guess attack experiment(2): the number of identified credential at each answer stage.

条件	第 1 候補	第 2 候補	第 3 候補	第 4 候補
Group-A	0	0	1	3
Group-B	0	0	0	3
Group-C	0	0	2	1

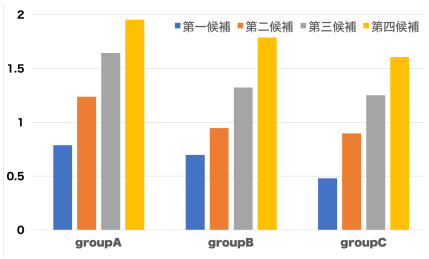

図 4 各候補での特定ペア数の平均
Fig. 4 The average number of identified word-pair(s) at each answer stage.

($\chi^2(2)$=0.60, p=0.74 > 0.05)．同様に，2 グループごとにカイ二乗検定を行った場合も，Group-A と Group-B 間に統計的有意差はなかった($\chi^2(1)$=0.54, p=0.46 > 0.05)．Group-B と Group-C 間にも統計的有意差はなかった($\chi^2(1)$=0.03, p=0.85 > 0.05)．

推測成功件数と推測された秘密情報の被験者との関係を表 3 内の「推測された被験者名」列に示している．表記方法について説明する．“sub1(3)” とは sub1 の部分が被攻撃者の通し番号を表し，カッコ内の数字 “3” が秘密情報を特定した攻撃者の人数を表す．この表を見て分かることは，秘密情報を特定された被攻撃者は 5 名（sub1，2，8，9，10）いたが，そのうち 1 回しか推測されなかった被攻撃者は sub2 の 1 名のみであった．

次に，攻撃成功事例が，攻撃試行時の第何候補で成功したかを**表 4** に示す．第 2 候補までの選択では攻撃成功例はなく，第 3 候補の選択において 2 グループで 3 例，第 4 候補の推測において全グループにおいて 7 例の攻撃成功例が見られ，合計 10 例の攻撃に成功している．

秘密情報となっているペアを特定した数の平均を 1〜4 候補ごとに分けて**図 4** に示す．各攻撃において選択したペアが正しい秘密情報と一致した数（特定した数）の和を攻撃数で割ったものである．第 4 候補までに特定されたペア数に対して，グループ間での結果に統計的有意差は見られなかった（$\chi^2(8)$=6.28，p=0.62 > 0.05)．

4. 考察

本章では，まずはじめに評価実験をふまえて個人情報型推測攻撃への安全性と傾向型推測攻撃への安全性，その他の攻撃に対する安全性について議論する．次に，秘密情報の記憶保持可能性や入力時間についても議論するとともに，今後の課題について述べる．

4.1 個人情報型推測攻撃に対する安全性評価

本節では，個人情報型推測攻撃に対する安全性評価について考える．まず，被験者の選んだ優先順位から推測攻撃の試行回数に変換する方法について述べる．次に，推測攻撃が成功する最小の試行回数と，検証可能な最大試行回数における安全性ついて述べる．各グループにおける推測攻撃の成功数から攻撃者と被攻撃者の関係性が推測攻撃に与える影響について考察する．最後に，秘密情報である 4 単語ペアすべてが推測されなかったとしても，うち何ペアが 1,820 回の試行で推測されたかについて述べる．

優先順位から試行回数への変換

攻撃者によって決められた 16 単語ペアの優先順位（第 1 候補〜第 4 候補）を推測の試行回数に変換する方法について述べる．第 1 候補として選択された 4 単語ペアから認証入力に要求される 4 単語ペアを選択する組合せは 1 であり，これは 1 回の攻撃試行に相当する．第 2 候補では新しく選択した 4 単語ペアと第 1 候補の 4 単語ペアをあわせた 8 単語ペア（優先順位が上位の 8 単語ペアとなる）の中から入力に必要な 4 単語ペア選ぶ組合せが，${}_8C_4$=70 通りなる．そのため第 2 候補までに順位づけられた 8 単語ペアを用いることで，70 回の攻撃試行に相当すると見なすことが可能である．同様に第 3 候補まででは 495 回，第 4 候補では 1,820 回の攻撃試行を行うことができる．

推測攻撃を成功させた最小の試行回数

推測攻撃に成功した試行回数の最小値は，攻撃者が推測攻撃に成功するために必要となる試行回数を表すといえる．本実験で第 2 候補までの攻撃成功の例はなく，第 3 候補で全 146 攻撃中 3 つの攻撃が成功した．第 2 候補は 2〜70 回の試行に相当し，第 3 候補は 71〜495 回の試行に相当する．したがって，本実験では 70 回までの攻撃による個人情報型推測攻撃の成功例はなく，攻撃に成功するためには 71〜495 回の試行が必要になるといえる．

70 試行まで推測攻撃が成功していないということは，推測攻撃に対する安全性を改善していると考える．その理由は，関連研究と比較して推測攻撃に成功するまでにより多くの試行回数が必要となるからである．以下で，個人情報型推測攻撃の検証を行った (1) Hayashi らの手法と (2) Renaud らの手法の認証方法，検証結果を説明し，本研究の結果と比較する．

Hayashi らは候補となる画像の中から秘密情報となる画像を選択する認証方式である Use Your Illusion を提案した [7], [8]．候補画像から秘密情報の画像を選択する認証方式は，攻撃者が画像を見て，正規利用者の趣味嗜好から秘密情報となる画像を推測可能だと指摘されている．そこで Hayashi らの手法では，画像候補に対して油絵のように抽象化する加工をすることで推測攻撃に対する安全性を改善

した．Hayashi らは正規利用者の知人が推測攻撃をする評価実験を実施し，10 回の試行で 15 人中 1 人（6.67%）が攻撃に成功することを明らかにした．

Renaud らは質問文（例．一番好きな食べ物は）に対してあらかじめ設定した回答を答える「秘密の質問」と呼ばれる認証方式を改良した [9]．Renaud らの手法では，「この動物は誰を思い出させる」といった共通の質問文と，複数枚の動物の画像群が用意されていて，正規利用者は秘密設定時に 1 枚画像を選択し，この画像と質問文に沿った回答を秘密として設定する．認証時には画像と質問文がシステムによって提示され，正規利用者は回答（秘密情報）を入力する．個人情報型推測攻撃実験では上記の動物の例を含む 3 種類の質問文が用意されていてそれぞれ正規利用者が秘密情報を設定した．攻撃者は各質問文に対して 3 試行が許されて推測を実施し，103 人の攻撃者のうち 3 人（2.91%）が 3 つの質問文すべてに対して推測に成功した．したがってこの結果は 3 試行の推測攻撃の成功率が 2.91%であるといえる．

Hayashi らの手法と Renaud らの手法ではそれぞれ 10 試行，3 試行の個人情報型推測攻撃で成功例が出ている．これに対して本研究では，シミュレーションではあるものの 70 試行までの攻撃で推測攻撃の成功例がないという結果を示すに至った．この結果から，提案手法は既存の手法よりも推測攻撃に対する安全性が明らかにされた手法であると考える．ただし，これらの評価実験における条件は個々に異なるため，その点は留意する必要がある．

最大試行回数における安全性

次に，本実験で測定した最大の試行回数である 1,820 回の試行における攻撃成功率について述べる．この際の推測攻撃成功率は最大で 9.52%であった．上述した Hayashi らの手法と Renaud らの手法では，10 試行までしか個人情報型推測攻撃を行っておらず，1,820 試行における比較することができない．そのため，単純比較はできないが，それぞれの試行回数における攻撃成功率は，Hayashi らの手法で 10 試行で 6.67%，Renaud らの手法では 3 試行で 2.91%であった．また提案手法の結果は，回答となる単語ペアを構成する単語がすべて開示されている攻撃者にとって有利な状況，かつ攻撃実験においても現実の攻撃状況に配慮した環境で攻撃を実施させたうえでの結果である．同じ条件での検証が必要であるが，提案手法は関連研究の安全性を改善しうると考える．

攻撃者と被攻撃者の関係性が推測攻撃に与える影響

攻撃者と被攻撃者の関係性が推測攻撃に与える影響を考えるために，各グループの 1,820 回の試行における攻撃成功率について考える．Group-B と C は同一の秘密情報に対して，被攻撃者と知人関係にある攻撃者とそうでない攻撃者がそれぞれ推測を行わせたが，その攻撃成功率に有意差はなかった．これは，「単語ペア」が知人であっても推測に有利に働かない秘密情報ということを示唆している．また，Group-A と B の間にも有意差はなかった．一方で，本実験のグループ分けは「攻撃者が正規利用者について知っている情報」が攻撃者と被攻撃者の関係性によって異なると仮定したが議論の余地は残るため，今後の課題である．

最大試行回数における推測された単語ペア数

4 単語ペアすべてが推測されなかったとしても，何ペアかは 1,820 回の試行で推測されていることがあった．この個人情報型推測攻撃で 16 ペア選択した際に特定された単語ペア数と，ランダムに 16 ペア抽出した際に含まれる秘密情報の単語ペア数を比較することで，攻撃者の推測がどの程度ペアの特定に影響を与えるかが分かる．個人情報型推測攻撃で特定できたペア数の平均は Group-A：1.95 ペア，Group-B：1.79 ペア，Group-C：1.60 ペアであった．一方で，ランダムに 16 ペア抽出した場合，秘密情報が平均 1.42 ペア含まれる．これは，以下の方法で計算される．45 ペア内に 4 ペアの秘密情報が存在している場合に，その中からランダムに 16 ペア抽出すると x ペアの秘密情報が含まれる．この時 45 ペア中の 4 ペアの秘密情報と抽出された 16 ペア抽中の x ペアの秘密情報は等しいと考えられるため，x=(4/45) × 16=1.42 で求められる．2 つの結果を比較すると，ランダムで選択した場合と各条件で特定できたペア数の差は最大で 0.52 ペアである．個人情報型推測攻撃がランダムで選択した場合比較して 1 ペア以上増加していないことから，攻撃者の推測は特定ペア数に大きく影響を与えていないと考える．

4.2 傾向型推測攻撃に対する安全性評価

傾向型推測攻撃に対する安全性を 3.1 節の評価実験で収集した 21 名の秘密情報の偏りを分析することで評価する．被験者が設定した秘密情報に重複がなければ，秘密情報自体に偏りがなく，結果としてこの攻撃への安全性がある，と考えられるからである．解析結果は以下のとおりとなった．

- 「単語ペア」での重複：84 単語ペア中，重複なし
- 単語ペアに用いられた「単語」での重複：158 単語中，20 単語（7.9%）が重複
- 単語ペアに用いられた「単語」+「おとり単語」（プロトタイプシステムに登録された全単語）での重複：210 単語中，27 単語（12.9%）が重複

単語単位では重複が存在するものの，単語ペアとしての重複はなかったことは，秘密情報の偏りが少なくなる可能性があることを示しており，結果としてこの攻撃への安全性に対する懸念が少なくなる可能性が示唆される．

被験者の作成した単語ペアのうち同一の単語ペアは存在せず，単語ペア（秘密情報）に偏りはなかったが，被験者の作成した単語ペアには「単語ペアに用いられた単語数」に偏りがあり，この偏りを利用した新たな推測攻撃が懸念

される．「単語ペアに用いられた単語数」は，提案手法が1つの単語を複数の単語ペアに含めることは許容するため，4〜8単語となる．実際には21名の被験者のうち14名が8単語で4つの単語ペアを用いており，偏っていた．仮に，「単語ペアに用いられた単語数が8単語」だと仮定して推測攻撃を行う場合，この条件内での総あたりに要する試行回数は4,725（$=_{10}C_2 \times {}_8C_2 \times {}_6C_2 \times {}_4C_2/4!$）回となる．これは，以下のように計算される．まず2.3節の式(1)で計算したように回答候補となる単語ペア数 ${}_{10}C_2$ から1つ目のペアを選択する．この後，1つ目の単語ペアを構成する単語以外の8単語から作成されるペア数 ${}_8C_2$ から2つ目の単語ペアを選択し，同様に3つ目，4つ目と選択する．最後に実際は順番が考慮されず組合せであることから4!通りで割ることで導き出される．この「単語ペアに用いられた単語数が8単語」を前提とした場合の総あたりに要する試行回数（4,725回）は総あたり攻撃に要する試行回数（148,995回）と比べて約32分の1となっている．したがって，「単語ペアに用いられた単語数」に偏りが生じた場合，提案手法の安全性を低下させうる新たな推測攻撃が懸念される．

しかし，この偏りは秘密情報の内容に依存するものではなく単語ペアの集合に関する構成方法に起因するため，秘密情報設定方法の変更で偏りを軽減しうると考える．プロトタイプシステムで被験者は図2の画面で10単語を設定し，この入力欄には同じ単語を入力することができない．そのため，被験者が2つずつ並んだ単語入力欄にペアとなる単語を入力していくと，「8単語で4単語ペアを構成する秘密情報」を作成する可能性がある．また本来，4単語ペアにおける同一単語の利用は正規利用者の登録負担を軽減すると考える．これは4単語ペアにおける同一単語の利用により正規利用者は新たに2つの単語を考えず，すでに登録した単語を手がかりに，追加で1つの単語を考えてペアを作成できるからである．秘密情報設定方法の変更により期待される軽減の効果が得られるか再検証が必要である．

4.3 その他の攻撃に対する安全性

以降，その他の攻撃に対する安全性（汚れ攻撃，フィッシング攻撃）について議論する．

汚れ攻撃（smudge attack）

汚れ攻撃は，タッチパネル上に残った操作痕跡から，秘密情報を特定する攻撃である．操作痕跡を活用するこの攻撃は入力操作がつねに同じであることに起因している．提案手法では単語の表示位置を認証試行のたびにランダムに変化させ，見た目上の入力操作を毎回異なるものにしている．この設計により，提案手法は汚れ攻撃に対する安全性を確保している．また類似の攻撃手法として，Thermal Attackがある[10]．Thermal Attackでは，秘密情報の入力後，タッチパネルに指の熱が残ることを利用し，この温度をサーマルカメラで可視化して秘密情報を窃盗する．提案手法は入力操作が毎回異なるため，Thermal Attackに対しても安全性を確保している．

フィッシング攻撃

フィッシング攻撃に関してはパスワードと比較すると攻撃が困難になると考える．パスワードはすべての利用者が共通の入力画面を利用するため，攻撃者はフィッシング攻撃用入力画面を作成した後は，対象サービスの利用者すべてに対してその画面を用いてフィッシング攻撃を行うことができる．一方，提案手法は認証画面に提示される単語群が利用者ごとに異なるため，攻撃者は標的とする正規利用者の単語群を把握してから，その利用者のために，専用のフィッシング攻撃用入力画面を作成する必要がある．したがって，多くの利用者をフィッシング攻撃するためには，その利用者数分の攻撃用画面を作成しなければならないことから，提案手法はパスワードと比べてフィッシング攻撃を困難にする効果があると考える．

4.4 記憶保持評価

記憶保持評価実験において，1および2週間間隔で2回検証を行った場合でもすべての被験者が認証に成功していた．この結果から，利用頻度が1，2週間に一度程度の利用形態でも，実用に耐えうる認証手法であるといえる．提案手法の秘密情報は単語ペア4組であり，最大で8単語と4つの組合せを覚える必要がある．このことから，パスワードと比較してその記憶保持は容易でないと利用者は感じるであろう．しかし，秘密情報を構成する単語ペアは，関連を利用したものであり，記憶保持を支援しうる形態になっていること，また単語ペアを構成する単語は認証画面に提示されることから，記憶想起の手がかりとなる．これらの効果が奏功して今回の結果につながったと著者らは考えている．

4.5 入力時間

提案手法の入力時間について考察する．実験結果から，入力時間は平均値が19.9秒，中央値が14.4秒であった．また最短および最長時間はそれぞれ9.2秒，57.9秒であった．この結果は，若干長いように感じられるが，実用性が疑問視されるほど長い入力時間ではないと考える．その理由は2つある．

1つ目の理由は，パスワード認証の入力時間との比較で同等程度の入力時間であった点である．Shayらの論文[11]によると，複数のパスワードポリシによって生成されたパスワードによる個人認証の入力時間は，パスワード決定から3日後で中央値が11.6〜16.2秒となっている．この結果と比較すると，パスワード認証と提案手法の操作時間は同等程度であり，非現実的な操作時間が必要という状況ではないと考える．

2つ目の理由は，増加要因があるにもかかわらず，入力時間の増加は抑制的であった点である．提案手法の操作時間

には，以下の 3 つの要素が含まれると考えている．「(a) 秘密情報を思い出す時間」+「(b) 画面から秘密情報を構成する単語を探索する時間」+「(c) 実際に秘密情報を入力する時間」このうち，(b) については既存の知識照合型個人認証には存在しない操作時間要素である．このことから，提案手法はパスワード認証と比較して入力時間が長くなる可能性が高いといえる．加えてこの (b) の操作は，操作慣れによる時間短縮が成立しにくい．回答候補単語群の配置が，秘密情報の入力のたびにランダムに配置し直されるため，操作に慣れたとしても一定の探索時間がかかると見込まれるからである．このように，パスワード認証と比較して入力時間が長くなる要素が明らかに存在する状況で，提案手法の操作時間はパスワード認証と同等程度という結果が得られていることから，入力時間の点で提案手法の利用可能性に疑問を抱かせるものではないと考える．

4.6 今後の課題

今後の課題として，プロトタイプにおける問題点の改善，おとり単語設定に関する改良と実験による再評価があげられる．プロトタイプにおける問題点として 3 つある．1 つは 4.2 節で述べた秘密情報設定方法の変更である．今回の実験では「4 単語ペアを構成する単語の数」に偏りがあり新たな推測攻撃の可能性が示唆されたため，この偏りを軽減しうるプロトタイプの秘密情報設定方法の変更と再検証が必要である．これ以外の 2 つは入力時間の短縮方法の検討と覗き見攻撃の対策を考えていく必要があることである．

また，おとり単語の設定を支援することも今後の課題の 1 つと考えている．おとり単語の設定は，本手法を使用する際ユーザに対する負担になる一方で，推測攻撃への安全性にも影響する設定項目でもある．我々は，「おとり単語の候補提示と利用者による選択」を基本にしつつ，どのようにおとり単語の候補を提示すれば良いかについて推測攻撃に対する安全性の影響を測りながら，望ましい手法を模索していく必要があると考えている．

本実験は被験者が全員大学生でありまた人数も限られていたため，被験者数を増やし，大学生以外での実験による再評価が必要である．被験者数の増加は秘密情報数を増加させ，秘密情報の偏りや正規利用者がどういった情報を秘密にするかを明らかにする可能性がある．また，関連研究との同条件での比較が行えなかったため，同条件における評価も必要である．

5. 関連研究

最後に推測攻撃への安全性を向上を目的とした個人認証の研究と関連を用いた個人認証の研究について述べ，提案手法の新規性を明らかにする．

4.1 節で述べたように Use Your Illusion は候補となる画像を油絵のように抽象化する加工することで推測攻撃に対する安全性を向上を目的とした．同様に原田らは元画像に対して不鮮明化処理を行うことで，安全性を向上を目指したが，原田らとは評価している安全性が異なり，覗き見攻撃耐性について検証している [12]．そのため，推測攻撃に対する評価を比較議論することができない．

関連を秘密情報に用いた個人認証が提案されている．これらは，システムが提示した情報に対して関連する情報（秘密情報）を入力する方式（以降，「Q&A 認証」とする）をとっている点で提案手法とは異なる．4.1 節で述べた秘密の質問や Renaud らの手法も Q&A 認証である．

Smith は単語の関連を用いた手法 [13] を提案した．この手法において個人認証システムが利用者に提示する情報は単語であり，これに対して利用者が提示された単語と関連があるとして事前に登録した単語を回答する．Smith の手法は我々の提案手法と 2 つの単語を秘密情報として用いる点で共通している．しかし，提案手法が正規利用者に対して 2 単語を共に開示しているのに対して，Smith の手法は一方の単語しか開示していない．それゆえに，Pond らが Smith の手法に対して記憶保持検証を実施した結果，秘密情報の登録から 2 週間後に 65%の利用者しか秘密情報の記憶を保持していないことが分かった [14]．

増井はなぞなぞ認証 [15] を提案した．この手法では，質問文や画像に対して，回答候補群中から回答（秘密情報）を選択する．登録時にユーザは，秘密情報となる「答え」と「誤答」と「なぞなぞ」（文や画像）を登録する必要がある．Q&A 認証は，秘密情報であるペアとなる情報の利用の差から，提案手法と比べて脆弱だと考える．ペアとなる情報には，情報 A，情報 B，両者の関係という 3 点の情報が含まれる．Q&A 認証はこれらのうち，提示された情報である情報 A と「Q&A 関係」という両者の関係を認証利用者に開示している．提案手法では情報 A，B を候補群として提示し，両者の関係を秘密情報としていて，両者の関係性に自由度が上がり，Q&A 認証と比較して推測が困難になると考える．

6. おわりに

本研究では秘密情報として「単語ペアの集合」を用いて，a) 推測攻撃に対する安全性改善，b) 秘密情報の記憶保持が可能，c) 利用者が秘密情報を作成可能の 3 要件を満たす個人認証の実現を目的とした．プロトタイプシステムを実装して，上記 a)，b) に関する評価実験を実施した．その結果，提案手法の秘密情報は 70 試行までは推測攻撃の成功例がなく，関連研究の推測攻撃に対する安全性を改善しうることが示唆された．また，記憶保持評価実験を通して，1，2 週間に一度程度の利用形態においては，利用者が提案手法も秘密情報を記憶保持可能ということであるといえた．今後の課題として，秘密情報設定，入力時間，覗き見攻撃耐性に関する問題の改善と，被験者数を増やし，多様化し

た被験者層での実験による再評価について検討していく．

参考文献

[1] Hashcat advanced password recovery, available from ⟨https://hashcat.net/hashcat/⟩ (accessed 2018-07-13).
[2] Openwall, John the Ripper password cracker, available from ⟨http://www.openwall.com/john/⟩ (accessed 2018-07-13).
[3] TeamsID, Worst Passwords of 2017 Top 100, available from ⟨https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf⟩ (accessed 2018-07-13).
[4] Wang, D., Zhang, Z., Wang, P., et al.: Targeted Online Password Guessing: An Underestimated Threat, *Proc. ACM CCS 2016*, pp.1242–1254, ACM (2016).
[5] Bradshaw, G. and Anderson, J.: Elaborative encoding as an explanation of levels of processing, *Verbal Leading and Verbal Behavior*, Vol.21, No.2, pp.165–174 (1982).
[6] Dinei, F. and Cormac, H.: A large-scale study of web password habits, *Proc. WWW*, pp.657–666 (2007).
[7] Hayashi, E., Christin, N., Dhamija, R. and Perrig, A.: Use Your Illusion: Secure authentication usable anywhere, *Proc. SOUPS 2008*, pp.35–45, ACM (2008).
[8] Hayashi, E., Hong, J. and Christin, N.: Security through a different kind of obscurity: Evaluating distortion in graphical authentication schemes, *Proc. CHI'11*, pp.2055–2064, ACM (2011).
[9] Renaud, K. and Just, M.: Pictures or Questions? Examining User Responses to Association-Based Authentication, *Proc. 24th BCS Interaction Specialist Group Conference*, pp.98–107 (2010).
[10] Abdelrahman, Y., Khamis, M., Schneegass, S. and Alt, F.: Stay cool! understanding thermal attacks on mobile-based user authentication, *Proc. CHI'17*, pp.3751–3763, ACM (2017).
[11] Shay, R., et al.: Designing Password Policies for Strength and Usability, *ACM Trans. Inf. System Security*, Vol.18, No.4, Article 13, 34 pages (2016).
[12] 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013 (2005).
[13] Smith, S.: Authenticating Users by Word Association, Computers & Security, Vol.6, No.6, pp.464–470 (1987).
[14] Pond, R., Podd, J., Bunnell, J. and Henderson, R.: Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates, *Computers & Security*, Vol.19, No.7, pp.645–656 (2000).
[15] 増井俊之：パスワードとの闘い—パスワードなし認証システムの運用報告，コンピュータセキュリティシンポジウム 2009 論文集 (2009).

推薦文

本論文は，ユーザの知識を用いる個人認証における推測攻撃の効果を軽減するために利用者が秘密情報を自ら作成して事前登録する特徴を持ち，単語ペアの組を入力として認証を行う新しい方式を提案している．ユーザ認証を行うための入力インターフェイスとしてスマートフォンを用いる実験を行っており，ノード間を線で結ぶ動作を導入するなどして複雑な操作にならないように工夫されている．今後のユーザブルセキュリティの研究を推進する論文の一つとあると確信する．よって推薦論文として推薦する．

（コンピュータセキュリティシンポジウム 2017（CSS2017）
プログラム委員長　須賀祐治）

山岸 伶

2017 年電気通信大学情報理工学部総合情報学科卒業．2019 年 1 月現在，電気通信大学大学院情報理工学研究科在学中．在学中は個人認証の推測攻撃対策の研究に従事．ソーシャルエンジニアリング，セキュリティとユーザビリティにも関心がある．

高田 哲司　（正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士後期課程修了．博士（工学）．2003 年ソニーコンピュータサイエンス研究所研究員．2005 年独立行政法人産業技術総合研究所情報技術研究部門研究員．2010 年電気通信大学大学院情報理工学研究科准教授．現在に至る．個人認証，ユーザブルセキュリティ，情報視覚化に興味を持つ．IEEE/CS 会員．