クラック困難なパスワードの作成を意識しないユーザでも利用可能な，2コマまんがを用いた認証方法の提案

小原 富美聡† ベッド B. ビスタ† 高田 豊雄†

†岩手県立大学大学院ソフトウェア情報学研究科
020-0193 岩手県岩手郡滝沢村滝沢字巣子 152 番地 52
g231i201@s.iwate-pu.ac.jp，{bbb，takata}@iwate-pu.ac.jp

あらまし 現在，Web サービスで広く使われているパスワード認証では，クラック困難性を確保するために，ユーザ自身がクラック困難なパスワードを作成する必要がある．しかし，Web サービスを利用するすべてのユーザがクラック困難なパスワードの知識を持っているわけではないため，容易にクラック可能なパスワードが利用される問題がある．そこで本研究では，複数のパスワードを用いることで，ユーザの知識に関わらずクラック困難性を確保し，同時に複数のパスワードを記憶することで発生する記憶の干渉を防ぐために，2 コマ漫画を用いてパスワード間に関連を持たせ，複数のパスワードの記憶保持性を向上させる手法を提案する．

A proposal of authentication method using two scene cartoons that user can use without considering the difficulty of password cracking

Fumisato Obara† Bhed Bahadur Bista† Toyoo Takata†

†Graduate School of Software and Information Science，Iwate Prefectural University，
152-52，Sugo，Takizawa，Iwate，020-0193 Japan
g231i201@s.iwate-pu.ac.jp，{bbb，takata}@iwate-pu.ac.jp

Abstract

Today，password authentication is widely used in Web services．In password authentication，users should make their passwords difficult to crack．However，many users use passwords that are easy to crack because not all of them know how to make a password difficult to crack．In our proposal，difficulty of a password crack is enhanced by using two passwords．However，when two passwords are memorized at the same time，passwords interfere each other in memory．In this proposal，a two scene cartoon is used to straighten out the problem of password memorization．In order to make the password easy to recall，two scene cartoon relates two passwords.

1 はじめに

現在，Web サービスの個人認証技術として，パスワード認証が広く使われている [1]．パスワード認証は，生体認証やトークン認証と異なり，特殊な機器を必要とせず，パソコンがあれば利用できる．そのため，インターネット環境があれば場所や時間の制限なく利用可能な Web サービスには，ハードウェアの制限がある生体認証やトークン認証よりも，パソコンのみで利

用できるパスワード認証が適しているといえる．

パスワード認証でクラック困難性を確保するためには，ユーザ自身がクラック困難なパスワードを作成する必要がある．しかし，すべてのWebサービスユーザがクラック困難なパスワードについての知識を持っているわけではないため，容易にクラックされてしまうようなパスワードが利用されてしまうという問題がある [2]．

そこで本研究では，ユーザの知識を仮定することなくクラック困難性を確保するために，複数のパスワードを用いた認証方法を提案する．複数のパスワードを用いることで，ユーザが作成した個々のパスワードが容易にクラック可能な物であっても，組み合わせの数を膨大にすることにより，クラック困難性を確保する．その際，一般的に，一度に複数のパスワードを記憶すると，記憶の干渉 [7] により記憶保持性は低くなる．

本研究では，記憶の干渉による記憶保持性の低下を防ぐために2コマまんがを用いて，パスワード間に関連を持たせる．ユーザはそれぞれのコマ画像から連想するパスワードを登録するので，2つのパスワードは関連したものになると考えられる．

2　関連研究

ユーザに画像から連想するパスワードを作成させる手法に,「画像連想パスワード [3]」がある．「画像連想パスワード」では，ユーザは1枚の画像を登録し，その画像から連想するフレーズを考える．その後，フレーズから語呂合わせパスワード [4] を作成する．語呂合わせパスワードは，クラック困難で容易に記憶可能なパスワードであるため,「画像連想パスワード」も同様に，クラック困難で容易に記憶可能なパスワードをユーザが作成でき，画像からフレーズを連想させることで，ユーザが，自身の名前や生年月日，有名な歌のフレーズのような予想されやすいフレーズをパスワードを作成に用いることを防いでいる．しかし,「画像連想パスワード」を作成するためには，ユーザ自身が，クラック困難な語呂合わせパスワードの作成方法の知識を持っている，もしくは，パスワード作成時に学習する必要があり，知識のないユーザが「画像連想パスワード」を作成する場合，容易にクラック可能なパスワードが作成される可能性がある．本研究では，個々のパスワードが容易にクラック可能な物であっても，複数のパスワードを登録させることでクラック困難性を確保する．そのため，クラック困難なパスワードを作成する知識がないユーザでも，クラック困難性を確保することができる．

図 1: 2コマまんがの例

3　2コマまんがパスワードの提案

本提案手法では，ユーザは，図1のような2人の登場人物が会話を行っている2コマまんがを用意し，それぞれのコマの登場人物のセリフをパスワードとして登録する．

この手法では，2つのコマそれぞれに対応するパスワードを登録するため，ユーザは合計で2つのパスワードを登録する．また，個々のパスワードは，登場人物のセリフであるので，単語2つ以上からなるフレーズになる可能性が高いと考えられる．そのため，クラック困難なパスワードについての知識がないユーザがパスワー

ドを作成した場合でも，クラック困難性を確保できると考えられる．

2つのパスワード (セリフ) は，2コマ漫画の登場人物の会話であるため，ユーザはストーリーでつながったセリフをパスワードとして作成すると考えられる．複数のパスワードを記憶する際に，関連を持たせることで記憶保持性は向上する [8] ことが期待されるため，ストーリーで関連付けられた2つのパスワードの記憶保持性は高いと考えられる．

以上より，複数のパスワードを関連付けて記憶できる本提案手法は，クラック困難なパスワードの知識を持たないユーザでも，クラック困難性を確保でき，記憶保持性も高い認証手法であると考えられる．

3.1 パスワードの登録手順

本提案手法では，ユーザが登場人物が会話を行っている2コマまんがを用意し，それぞれのコマの登場人物のセリフをパスワードとして登録する．

パスワードの登録手順は以下のとおりである．

1. 2コマまんがを用意する
2. 2コマまんがのそれぞれのコマから連想するセリフをパスワードとして入力する
3. 確認入力を行う (表示された2コマまんがを見て，セリフを入力する)

3.2 認証手順

本提案手法では，ユーザは，表示された2コマまんがを見て，自身が登録したパスワードを答える (図2)．

認証の手順は以下のとおりである．

1. 入力されたユーザ ID をもとに，そのユーザが登録した2コマまんがを表示する
2. ユーザは表示された2コマまんがを見て，自身が登録した2つのパスワードを入力する
3. 2つのパスワードが共に登録時のものと一致すれば認証成功となる

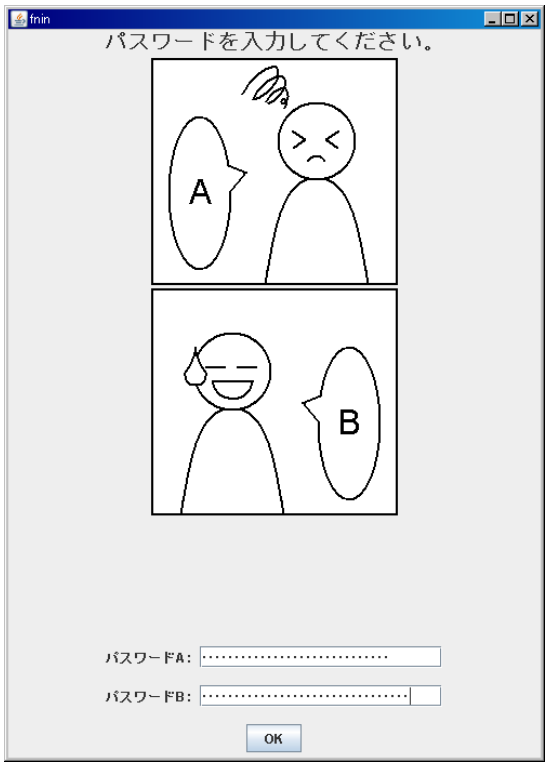

図 2: 認証：パスワード入力画面

4 プロトタイプシステムの実装

本提案手法では，パスワードを登録する前に2コマまんがを用意する必要がある．2コマまんがを用意する方法には以下の方法が考えられる．

- 画像検索を用いて多くの画像の中から認証で利用する2コマまんがを探し出す
- 普通の画像を用意し，それを画像編集ソフトで加工して2コマまんがを作成する
- ユーザ自身がまんがのコマを描く
- 既存の漫画から，好きな2コマ選び，スキャナやカメラでパソコンに取り込み，画像編集ソフトでセリフの文字を消す

上記のような方法で2コマまんがを用意することはユーザにとって負担である．そこで，実装したプロトタイプでは，あらかじめ用意されたパターンの中からコマ画像を選択することで，2人の登場人物が会話を行っている2コマまんがの作成を行う．これにより，2コマまんがを

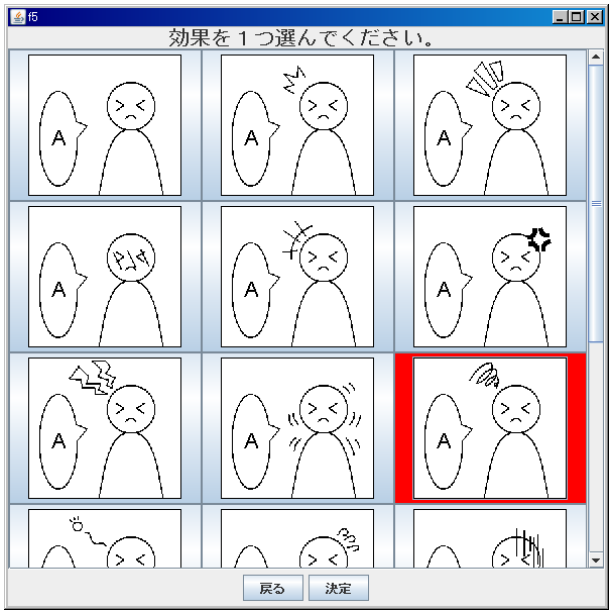

図 3: 画像作成画面 (効果の選択)

用意しなくても，パスワード登録前に容易に作成でき，ユーザが 2 コマまんがを用意する負担を軽減する．

プロトタイプでは，ユーザは，コマ画像に描かれる登場人物の目，口，効果を選択肢の中から選び 2 コマまんがを作成する (図 3)．選択肢は，既存の漫画で頻繁に用いられる登場人物の表情から，目を 7 パターン，口を 7 パターン，効果を 16 パターンを作成した．

本プロトタイプを使ったパスワードの作成手順は以下のとおりである．

1. 1 コマめの登場人物の目を 7 パターンから 1 つ選ぶ
2. 1 コマめの登場人物の口を 7 パターンから 1 つ選ぶ
3. 1 コマめの登場人物の効果を 16 パターンから 1 つ選ぶ
4. 2 コマめも 1 から 3 と同様に選択し，2 コマまんがを作成する
5. 2 コマまんがのそれぞれのコマから連想するセリフをパスワードとして入力する
6. 確認入力を行う (表示された 2 コマまんがを見て，セリフを入力する)

5　クラック困難性の考察

本提案のクラック困難性を考察する前に，本研究でのクラック困難性の基準を定める．

一般的に，クラック困難なパスワードというのは，以下の条件を満たすパスワードであるといわれている [5]．

- 予想されやすい情報 (名前，年齢，誕生日，家族やペットの名前，好きな色や曲など) が入っていない
- アルファベット小文字，大文字，数字，特所文字を含む
- 長さが 8 文字以上である
- 辞書に載っていない

「アルファベット小文字，大文字，数字，特殊文字からなる 8 文字のランダムパスワード (以下，ランダムパスワード)」は上記の条件をすべて満たすので，クラック困難であるといえる．ランダムな文字の並びを推測することはできないため，ランダムパスワードを推測攻撃で破ることはできない．また，ランダムな文字列は辞書に載っていないため，ランダムパスワードを辞書攻撃で破ることはできない．アルファベット大文字 (26 種)，小文字 (26 種)，数字 (10 種)，特殊文字 (32 種)，からなるランダムパスワードを総当り攻撃で破る場合，パスワード空間は，$(26+26+10+32)^8 \quad 6.10 \times 10^{15}$ となる．

本研究では，パスワードを攻撃する際に，ランダムパスワードと同等か，それ以上のパスワード空間があれば，クラック困難であるとする．

5.1　推測攻撃に対するクラック困難性

提案手法では，2 コマまんがのコマ画像から連想するセリフをパスワードとして登録する．ユーザがセリフを画像から連想する場合，フレーズにユーザの個人情報が入る可能性は低い [3]．そのため，攻撃者はユーザの個人情報を使ってフレーズを推測することができないと考えられる．

パスワードの連想に用いるコマ画像は，ユーザが，コマの登場人物の目，口，効果のパター

ンを選択することで作成される．そのため，画像からパスワードを推測する場合，攻撃者は，目，口，効果のパターンの情報から，ユーザが作成したパスワードを推測する必要がある．しかし，ユーザが連想するセリフを目，口，効果のパターンから正確に推測することは困難であると考えられる．

以上より，提案手法は，ユーザの個人情報やユーザが作成した 2 コマまんがの画像からパスワードを推測する推測攻撃に対してクラック困難性を確保できると考えられる．

5.2 辞書攻撃に対するクラック困難性

提案手法では，2 コマまんがのコマ画像から連想するセリフをパスワードとして登録するので，ユーザが作成するパスワードは 2 つ以上の単語からなるフレーズが使われると予想される．また，2 つのコマそれぞれからパスワードを連想するので，認証時に入力する 2 つのパスワードは少なくとも 4 つ以上の単語の組み合わせになると考えられる．

仮に，ユーザが作成した 2 つのパスワードが，「オクスフォード大学日本語パスワード解析用辞書 (115600 語)[6]」に集録されている単語 4 つの組み合わせであった場合，辞書攻撃のパスワード空間は $115600^4 \quad 1.79 \times 10^{20}$ となり，8 文字のランダムパスワードよりも広いパスワード空間となるため，クラック困難であるといえる．

また，登録単語数が少ない辞書を攻撃に使用すると，ユーザが作成したパスワードが辞書語の組みあわせになる (辞書攻撃でクラックされる) 可能性はさらに低くなる．

以上より，提案手法は，辞書攻撃に対してクラック困難性を確保できると考えられる．

5.3 総当り攻撃に対するクラック困難性

パスワードで使用する記号について指示をしない場合，多くのユーザがアルファベット小文字のみのパスワードを作成することが予想される．アルファベット小文字のみで作成されたパスワードでランダムパスワード以上のクラック困難性を得るためには，パスワードの文字数を 12 文字以上にする必要がある．

提案手法では，コマ画像からセリフを連想してパスワードとして登録する．ストーリーでつながっている 2 つのセリフを 12 文字未満で作成することは困難であり，ユーザが作成したパスワードが 12 文字未満になる可能性は低いと考えられる．そのためユーザが作成する 2 つのパスワードの合計文字数は 12 文字以上になり，総当り攻撃に対するクラック困難性は確保できると考えられる．

6 記憶保持性の考察

一般に複数のパスワードを記憶すると，パスワードの記憶保持性は低くなる．これは，記憶の干渉 [7] の影響であると考えられる．

記憶の干渉とは，似たような情報を複数記憶しようとすると，記憶同士が干渉し，記憶や想起が困難になる，または容易になる現象のことである．パスワードを記憶する際にはこの現象が記憶や想起を困難にするようにはたらくため，複数のパスワードを記憶するのが困難になると考えられる．

提案手法では，ユーザは 2 つのパスワードを記憶する．2 つのパスワードは 2 コマまんがから連想されているので，パスワードはストーリーでつながったセリフになると考えられる．そのため，2 つのパスワードはお互いに関連した物となり，一方を想起すれば，それがもう一方のパスワードのヒントになり，単純に 2 つのパスワードを記憶するのに比べて，記憶保持性と，想起性が向上すると考えられる．

複数のパスワードに関連を持たせる手法に，クロスワード認証 [8] がある．クロスワード認証では，合計の文字長が 15 文字以上になるように複数の単語を考え，その単語でクロスワードを作成することで認証する．この手法の記憶保持性に関する実験では，被験者が 15 文字のパスフレーズを記憶した場合と，被験者が合計文字数が 15 文字になる複数の単語で作成したクロスワードを記憶した場合では，クロスワードを記憶した場合のほうが一週間後のログイン成

功率は高いという結果が出ている．このことから，パスワード間に関連を持たせることで，複数の単語を記憶していても，記憶の干渉による記憶保持性の低下を防ぐことができ，1 つの長いパスフレーズを記憶するよりも高い記憶保持性が保てることがわかる．

以上より，提案手法は，ユーザがパスワードを記憶できるだけの記憶保持性を持つと考えられる．

7 おわりに

本論文では，クラック困難なパスワードを作成できるだけの知識を持たないユーザでもクラック困難性を確保できるように，複数のパスワード使った認証手法を提案を行い，複数のパスワードを記憶する際に起きる記憶の干渉を防ぐために，2 コマまんがを用いてパスワード間に関連を持たせ，記憶保持性を向上させる手法の提案を行った．

今後は，提案手法で認証を行うプロトタイプを実際に被験者に利用してもらい，記憶保持性，被験者が作成したパスワードの様々な状況下におけるクラック困難性，ユーザビリティ (パスワードの登録と認証にかかる操作時間，被験者の感じた主観的な負担) を評価する．

参考文献

[1] Steven Furnell. An assessment of website password practices, Computers & Security, No. 26, pp. 445-451, 2007.

[2] Anne Adams and Martina Angela Sasse. Users are not the enemy, Communications of the ACM, Vol. 42, No. 12, pp. 40-46, 1999.

[3] 福光正幸，加藤貴司，Bhed Bahadur Bista，高田豊雄．画像を利用したパスワード作成支援システムの提案，2009 年暗号と情報セキュリティシンポジウム (SCIS2009)，3D3-1(6pages)，2009.

[4] Yan. J., Blackwell. A., A. Anderson, and Grant A, Password memorability and security: empirical results. IEEE Security & Privacy Magazine, Vol. 2(5) Sept-Oct, pp. 25-31, 2004

[5] マカフィー株式会社．McAfee Blog - パスワードを強化する 7 つのヒント, http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1273, 最終アクセス：2011 年 8 月 23 日.

[6] オクスフォード大学．パスワード解析用辞書，ftp://ftp.ox.ac.uk/pub/wordlists/, 最終アクセス：2011 年 8 月 23 日.

[7] 桝野隆平．パスワードの脆弱性と対策－認知心理学の知見を生かして，情報処理学会研究報告 (CSEC2010)，Vol.2010-CSEC-49 No.9，pp.1-6，2010.

[8] 田澤宏尚，加藤貴司，Bhed Bahadur Bista，高田豊雄．複数個のパスフレーズと配置情報を用いたユーザ認証システムの提案，2009 年暗号と情報セキュリティシンポジウム (SCIS2009)，3D3-2(6pages)，2009.