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，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 パスワード認証のクラック困難性は、ユーザが作成したパスワードによって決定されるため、パスワード認証では、クラック困難なパスワードについて知識を持たないユーザや、パスワード作成時にクラック困難性を意識しないユーザは、クラック困難性を確保できず、安全に Web サービスを受けることができないという問題がある。そこで本論文では、そのようなユーザがクラック困難性を確保可能な個人認証手法として、複数のパスワードを用いた認証方法の提案を行う。また、パスワードの作成時と認証時にユーザが作成したまんがのコマ画像を用いることで、複数のパスワードを記憶する際に発生するパスワードの記憶保持性の低下を防ぐ手法の提案を行う。

A proposal of authentication method using 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 Difficulty of password cracking is decided by password that user make. If user does not know about how to make secure password, or does not considering the difficulty of password cracking when he make password, he cannot use web service safety. This article, I propose authentication method user who do not know about how to make secure password, or does not considering the difficulty of password cracking, can make password that difficult to cracking. And I also propose a method using cartoons for making passwords in order to make two or more passwords are easy to memorize.

1　はじめに

現在、Web サービスでは、個人認証技術としてパスワード認証が広く利用されている。パスワード認証において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。また、クラック困難なパスワードを作成するためには、ユーザがクラック困難なパスワードの作成方法についての知識を持っている必要がある。しかし、クラック困難なパスワードについての知識を持たないユーザは、攻撃者によって容易にクラックされてしまうパスワード作成する可能性があり、クラック困難性を確保することができない。

そこで、クラック困難なパスワードの作成方法を知らないユーザや、パスワード作成時にクラック困難性を意識しないユーザでもクラック困難性を確保可能な認証方法として、複数のパスワードを用いた個人認証手法の提案を行う。また、複数のパスワードを記憶した際に低下するといわれている記憶保持性を向上させる手法として、まんがを用いて複数のパスワード間に関連を持たせる手法を提案する。

2 本論文におけるクラック困難性と記憶保持性の定義

2.1 クラック困難なパスワード

一般にクラック困難なパスワードとは、他人に推測されない、辞書に掲載されていない、アルファベット大文字、小文字、数字、特殊文字を含む、8 文字以上のパスワードであるといわれている [1]。一般にクラック困難とされるパスワードの条件を攻撃者の視点から見た場合、他人に推測されないパスワードとは推測攻撃ができないパスワードであり、辞書に掲載されていないパスワードとは辞書攻撃ができないパスワードであり、アルファベット大文字、小文字、数字、特殊文字を含む、8 文字以上のパスワードとは、総当たり攻撃が困難なパスワードであるといえる。

アルファベット大文字（26 種類）、小文字（26 種類）、数字（10 種類）、特殊文字（32 種類）の合計 94 種類の記号からランダムに選択し、8 文字並べたパスワード（以下、8 文字のランダムパスワード）は、一般にクラック困難とされているパスワードの条件をすべて満たす。

そこで本論文では、推測攻撃、辞書攻撃、総当たり攻撃に対して、8 文字のランダムパスワードを総当たり攻撃にするよりもクラック困難であれば、提案手法がクラック困難であるとし、攻撃に対し 8 文字のランダムパスワードの総当たり数である $94^8 \approx 6.10 \times 10^{15}$ 以上のパスワード空間を有することをクラック困難性の条件とする。

2.2 記憶保持性

本論文では、対象とするユーザを、一般的に利用されている従来型のパスワードを利用することが可能なユーザとし、2.1 で述べたクラック困難性を有するパスワードの記憶保持性と同等であれば、提案手法の記憶保持性が十分であると判断する。

3 複数のパスワードとまんがを用いた個人認証手法の提案

3.1 パスワード問題とトレードオフ

パスワードを用いた個人認証手法には、パスワード問題 [2] といわれるトレードオフがあり、クラック困難なパスワードは記憶することができず、記憶が容易なパスワードは容易にクラックされてしまうといわれている。

画像連想パスワード [3] は、ユーザが語呂合わせパスワード [4] の知識があり、決められた手順に従ってパスワードを作成することでクラック困難性と記憶保持性を両立する個人認証手法であるが、知識のないユーザはクラック困難性を確保できず、ユーザに知識があったとしても語呂合わせパスワードの作成が手間であるために手順に従わない可能性がある [5]。

一方、提案手法では、「クラック困難性」「記憶保持性」「登録時のユーザの負担」「認証時のユーザの負担」の 4 つの要素のトレードオフにより、パスワードの登録や認証のユーザビリティを下げることで、クラック困難性についての知識がないユーザや、意識しないユーザでも記憶保持性とクラック困難性を両立させることが可能な個人認証手法を提案する。

3.2 複数のパスワードを用いた認証

本論文では、複数のパスワードを用いて認証を行うことでクラック困難性を確保する。複数のパスワードを用いて認証を行うことで、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ものであったとしても、それらの複数の組み合わせは膨大な数となるため、ユーザに

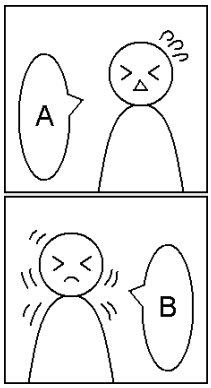

図 1: コマ画像の例

作成させるパスワードの個数を、組み合わせが $94^8 \approx 6.10 \times 10^{15}$ 以上になるように設定することで、クラック困難なパスワードの作成方法を知らないユーザや、パスワード作成時にクラック困難性を意識しないユーザであっても、クラック困難性を確保することができる。

3.3 記憶保持性の低下の原因

一般に複数のパスワードを記憶すると記憶保持性は低下する。その原因として考えられるのが記憶の干渉 [6] という現象である。記憶の中に似たような情報が存在すると、記憶や想起を困難にする干渉が起きるため、個々のパスワードが容易に記憶可能なものであっても、それを複数記憶すると、パスワードの記憶や想起が困難になると考えられる。提案手法では、パスワード間に関連を持たせることで記憶保持性を向上させる手法を提案する。

3.4 まんがを用いた認証

複数のパスワードの記憶保持性を向上させるための手法として、まんがを用いた認証手法を提案する。図 1 のようなまんがのコマの画像を用意し、画像の吹き出しにはいるセリフをパスワードとして登録する。ユーザは 1 個のコマ画像に 1 つのパスワードを入力するので、ユーザが作成するパスワードの数は、まんがのコマ数によって決まると考えられる。

まんがのコマを用いることで、複数のパスワード間に関連を持たせ、1 つのつながりのあるパスワードとして記憶することにより、記憶の干渉を防ぐ効果や、パスワードがストーリーで関連しているため、お互いを想起するためのヒントとなり、記憶や想起を容易にする効果が期待できる。また、認証時にまんがを表示し作成時の状況をユーザに再認させることで、パスワードの再生を容易にする効果も期待できる [7]。

4 複数のパスワードとまんがを用いた認証手法の評価

4.1 記憶保持性の評価方法

記憶保持性の評価では、提案手法を実装したプロトタイプを用意し、被験者はプロトタイプを用いてまんがのコマ画像とパスワードの作成を行い、1 週間後、プロトタイプで認証を行う。1 週間パスワードを記憶し、認証時に想起できた被験者の割合を調べることで、記憶保持性を評価する。

4.2 辞書攻撃に対するクラック困難性の評価方法

辞書攻撃に対するクラック困難性の評価では、提案手法を実装したプロトタイプを用意する。被験者はプロトタイプを用いてまんがのコマ画像とパスワードの作成を行う。その後、被験者により作成された複数のパスワードを、それぞれオクスフォード大学日本語パスワード解析用辞書 [8] の辞書語、辞書語を 2 つ連結した文字列と比較し、一致するか調べる。その後、辞書語の組み合わせ数が、8 文字のランダムパスワードの総当たり数 $94^8 \approx 6.10 \times 10^{15}$ 以上、または、辞書によるクラックが不可能であるパスワードの組を作成した被験者の割合を調べ、辞書攻撃に対するクラック困難性を評価する。

4.3 総当たり攻撃に対するクラック困難性の評価方法

総当たり攻撃に対するクラック困難性の評価では、提案手法を実装したプロトタイプを用意し、被験者はプロトタイプを用いてまんがのコマ画像とパスワードの作成を行う。その後、被験者により作成されたパスワードに使用されている文字の種類（アルファベット大文字、小文字、数字、特殊文字）と、合計文字長から、総当たり数の計算を行い、8 文字のランダムパスワードの総当たり数 $94^8 \approx 6.10 \times 10^{15}$ 以上となるパスワードの組を作成した被験者の割合を調べ、総当たり攻撃に対するクラック困難性を評価する。

4.4 推測攻撃に対するクラック困難性の評価方法

推測攻撃に対するクラック困難性の評価では、提案手法を実装したプロトタイプを用意し、1 人のユーザ役の被験者はプロトタイプを用いてまんがのコマ画像とパスワードの作成を行う。その後、数名の被験者は、攻撃者役となり、作成されたまんがのコマ画像を見て、パスワードを推測し、思いつく限りのパスワードを入力する。攻撃者役の被験者が入力したパスワードの中に、ユーザ役の被験者が作成したパスワードと一致または類似したものがあるか調べ、コマ画像からのパスワード推測可能性について判断を行う。

4.5 予備実験

クラック困難性の確保に必要なコマ画像の数と登録するパスワード数を調べるために、予備実験として、コマ画像数が 2 コマのプロトタイプを作成し、12 名の被験者にコマ画像とパスワードをの作成と、1 週間後の認証をしてもらった。そして、コマ画像数 2 コマのプロトタイプについて、記憶保持性と、辞書攻撃に対するクラック困難性、総当たり攻撃に対するクラック困難性の評価を行った。

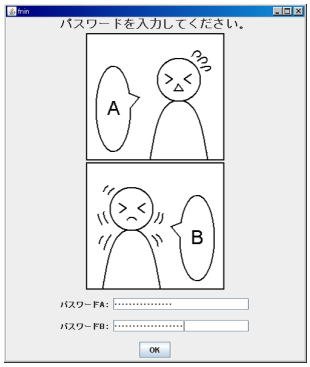

図 2: 2 コマまんが認証のログイン画面

4.5.1 プロトタイプ

2 コマまんがパスワードのプロトタイプでは、コマの登場人物の目、口、効果を選択肢から選ぶことで、コマ画像の作成を行い、作成した 2 コマのまんがから、パスワードを連想して登録する。認証は、登録時に作成した 2 コマのコマ画像が表示され、ユーザはコマ画像を見てパスワードを入力する（図 2）。

4.5.2 記憶保持性評価

12 名の被験者のうち、1 週間後の認証に成功した被験者は 10 名、認証に失敗した被験者は 2 名であった。この結果は、記憶が容易とされている語呂合わせパスワードと同等の記憶保持性であり、個人認証として利用するために十分な記憶保持性を有すると考えられる。

4.5.3 被験者のクラック困難性に対する意識

12 名の被験者が普段使用しているパスワードについてアンケートを行い、パスワードは 8 文字以上か、パスワードの個人情報を含んでいないか、パスワードにアルファベット大文字小文字の両方を含んでいるか、パスワードに数字が含まれているか、パスワードに特殊文字は含まれているか、という質問に対して、使用しているすべてのパスワードに当てはまる、使用している多くのパスワードに当てはまる、使用しているパスワードには当てはまらないという 3 つの選択肢から自分に最もよくあてはまるものを

答えてもらった結果、すべての条件を満たすパスワードを使用しているユーザはおらず、12 名の被験者は、クラック困難性に対して十分な意識を持っていないと考えられる。

4.5.4 辞書攻撃に対するクラック困難性評価

12 名の被験者が作成した、合計 24 個のパスワードについて、辞書攻撃に対するクラック困難性の評価を行った。結果、24 個のパスワードのうち、辞書語と一致したパスワードは 10 個、辞書語 2 つを連結した文字列と一致したパスワードは 5 個、一致しなかったパスワードは 9 個であった。また、被験者別にみると、12 名の被験者のうち、作成した 2 つのパスワードが両方とも辞書語と一致した被験者は 2 名、作成した 2 つのパスワードのうち一方が辞書語一致し、もう一方が辞書語 2 つを連結した文字列と一致した被験者は 3 名、作成した 2 つのパスワードが両方とも辞書語 2 つを連結した文字列と一致した被験者が 1 名、作成した 2 つのパスワードのうち、少なくとも一方は一致しなかった被験者は 6 名であった。

8 文字のランダムパスワード（$94^8 \approx 6.10 \times 10^{15}$）以上のクラック困難性を得るためには、単語数が 115600 個の辞書 [8] の、辞書語 4 つ（$115600^4 \approx 1.79 \times 10^{20}$）以上の組み合わせであればよい。そのため、7 名の被験者は、十分なクラック困難性を得ていると考えられる。しかし、辞書語 3 つ（$115600^3 \approx 1.54 \times 10^{15}$）以下の組み合わせでクラック可能な被験者 5 名は十分なクラック困難性が得られていない。

この結果から、従来型のパスワード認証では、クラック困難性の確保ができない 12 名の被験者のうち、7 名の被験者は、提案手法によって辞書攻撃に対して十分なクラック困難性を持つパスワードを作成させることができた。しかし、クラック困難性を確保するためには、すべての被験者が十分なクラック困難性を持つパスワードを作成する必要があり、提案手法の改良が必要であると考えられる。

4.5.5 総当たり攻撃に対するクラック困難性評価

12 名の被験者のうち、作成した 2 つのパスワードの合計文字数が最も少なかった被験者は、11 文字であった。アルファベット小文字のみの 11 文字のパスワードの総当たり数は $26^{11} \approx 3.67 \times 10^{15}$ であり、これは 8 文字のランダムパスワードの総当たり数 $94^8 \approx 6.10 \times 10^{15}$ の約半分だが、本提案手法では、1 つ目のパスワードと 2 つ目のパスワードの間に区切り文字を入れて、ハッシュ関数に入力するため、2 つのパスワードの合計が 11 文字の場合、文字数の組み合わせが 6 パターン考えられるので、12 名の被験者は、総当たり攻撃に対して、十分なクラック困難性を得られたと考えられる。

4.6 3 コマまんがパスワード

予備実験により、コマ画像 2 つのプロトタイプでは、辞書攻撃に対するクラック困難性が不十分であることが分かった。そこで、コマ画像を 3 つに増やしたプロトタイプを実装し、25 名の被験者にプロトタイプを用いてパスワードの作成と、1 週間後の認証をしてもらい、記憶保持性、辞書攻撃に対するクラック困難性、総当たり攻撃に対するクラック困難性、推測攻撃に対するクラック困難性の評価を行った。

4.6.1 プロトタイプ

3 コマ漫画パスワードのプロトタイプでは、はじめにコマの登場人物の位置を選択肢から選択し、その後、2 コマまんがパスワードの同様に、選択肢から登場人物の、目、口、効果を選択し、3 コマまんがを作成する。その後、作成した 3 コマまんがから連想するパスワードを 3 つ登録する。その際、普段キーボードによる特殊文字の入力に慣れていないユーザがパスワード中に特殊文字を加えることを意識させるため、特殊文字入力用ボタン (図 3) を一緒に表示する。

認証は、登録時に作成された 3 コマのコマ画像が表示され、ユーザはコマ画像を見てパスワー

図 3: 特殊文字入力用ボタン

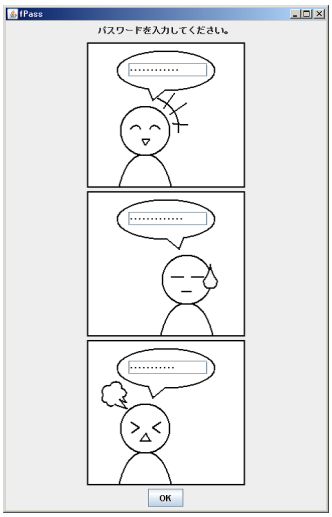

図 4: 3 コマまんが認証のログイン画面

ドを入力する（図 4)。このときも、登録時と同様、特殊文字入力用ボタン (図 3) を表示する。

4.6.2　記憶保持性評価

25 名の被験者のうち、1 週間後の認証に成功した被験者は 16 名、認証に失敗した被験者は 2 名であった。この結果は、記憶が容易とされている語呂合わせパスワードよりも低く、記憶が容易であるとは言えない。そのため、今後、記憶を容易にするための改良が必要であると考えられる。

認証時の被験者の入力を見ると、被験者は、パスワードを完全に忘れているわけではなく、同じ意味の別の言葉を入力するケースや、コマどうしのつながりや、ストーリーは合っているものの、入力のニュアンスが異なるケースが多く見られた (表 1)。これらの細かい部分での間違いを減らすことができれば、記憶保持性は向上すると考えられる。

表 1: パスワード入力間違いの例

登録	omizu	nainnda	ittadaro
認証	mizu	naiya, nainnda	ittaro
登録	sirukayo	uresiina	damareotaku
認証	nannde	yattane	otakukimoi

4.6.3　被験者のクラック困難性に対する意識

被験者がパスワードのクラック困難性に対してどの程度の知識や意識を持っているのかを調べるため、25 名の被験者に従来型のパスワードを普段通りに作成してもらい、辞書攻撃と、総当たり攻撃に対するクラック困難性を調べた。

その結果、辞書語と一致した（クラック困難性：115600）被験者が 25 名中 1 名、辞書語 2 つを連結した文字列と一致した（クラック困難性：$115600^2 \approx 1.34 \times 10^{10}$）被験者が 2 名いた。また、辞書語、辞書語 2 つを連結した文字列のどちらとも一致しなかった被験者 22 名のうち、総当たり攻撃に対するクラック困難性が $94^8 \approx 6.10 \times 10^{15}$ 以上になるパスワードを作成した被験者はおらず、22 名のうち最もクラック困難性が高かったパスワードは、アルファベットの小文字、数字、特殊文字からなる 8 文字のパスワード（クラック困難性 : $67^8 \approx 4.06 \times 10^{14}$）であった。このことから、被験者は普段から十分なクラック困難性を持つパスワードを使用するほどの、クラック困難性に対する知識や意識を有していないといえる。

4.6.4　辞書攻撃に対するクラック困難性評価

25 名の被験者がプロトタイプを用いて登録した合計 75 個のパスワードについて、辞書攻撃に対するクラック困難性の評価を行った。結果、75 個のパスワードのうち、辞書語と一致したパスワードは 7 個、辞書語 2 つを連結した文字列と一致したパスワードは 24 個、一致しなかったパスワードは 44 個であった。また、被験者別にみると、25 名の被験者のうち、作成した 3 つのパスワードの組み合わせが、辞書語そのものと一致するパスワード 2 個と、辞書語 2 つを連

結した文字列と一致するパスワード1個の組み合わせを作成した被験者が1名、辞書語そのものと一致するパスワード1個と、辞書語2つを連結した文字列と一致するパスワード2個の組み合わせを作成した被験者が1名、3つすべてが辞書語2つを連結した文字列と一致するパスワードも組み合わせを作成した被験者が3名、作成した3つのパスワードのうち、少なくとも1つは一致しないパスワードを作成した被験者が20名であった。つまり、すべての被験者が辞書語を4つ以上組み合わせなければクラックできないパスワードの組み合わせを作成した。このことから、本提案手法は、辞書攻撃に対するクラック困難性は確保可能であるといえる。

4.6.5 総当たり攻撃に対するクラック困難性評価

被験者がプロトタイプを用いて作成した3個のパスワードの合計文字数の平均は25.2文字であり、最小文字数は9文字であった。また、3個のパスワードを小文字のみで作成した被験者が25名中12名で最も多く、小文字と特殊文字で作成した被験者が5名、小文字と数字で作成した被験者が4名、小文字と数字と特殊文字で作成した被験者が2名、特殊文字のみで作成した被験者が2名であった。総当たり攻撃に対するクラック困難性を、使用された文字の種類の総数 (アルファベット大文字 : 26、アルファベット小文字 : 26、数字 : 10、特殊文字 : 32) を3個のパスワードの合計文字数乗して求めた場合、特殊文字のみで合計9文字のパスワードを作成した被験者1名を除く、24名の被験者が総当たり攻撃に対して十分なクラック困難性を持つパスワードを作成していた。また、クラック困難性が不十分な特殊文字のみで合計9文字のパスワードを作成した被験者1名は、パスワードを記憶することができていなかったため、実際の認証時にそのようなパスワードを作成する可能性は低いと考えられる。このことから、提案手法はクラック困難性についての知識を持たないユーザでも総当たり攻撃に対するクラック困難性を確保可能な認証方法であるといえる。

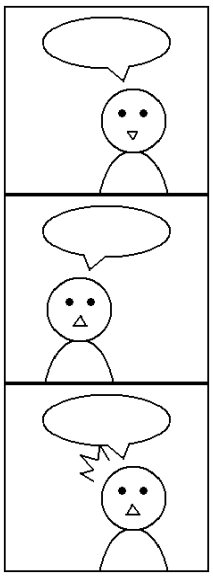

図 5: 推測攻撃用の3コマまんが

4.6.6 推測攻撃に対するクラック困難性評価

1名のユーザ役の被験者にプロトタイプを用いて、図5の3コマまんがと、3つのパスワード (1コマ目 : ohayou, 2コマ目 : mouyorudayo, 3コマ目 : mazisuka) を作成してもらい、10名の攻撃者役の被験者に、図5の3コマまんがに入るセリフを予想してもらった。結果、7名の攻撃者役の被験者が全くセリフを思いつかなかったものの、3名の被験者から合計21個のセリフを取得することができた。21個の予想されたセリフの中に、「こんにちは」「まじで!」という、作成されたパスワードに意味の近い言葉が見られたが、完全にパスワードを予想したセリフは見られなかった。このことから、提案手法では、攻撃者がコマ画像からパスワードを推測することは困難であると考えられる。

4.7 ユーザビリティ評価

記憶保持性評価実験の被験者25名に、3コマまんがの作成、パスワードの作成について、「簡単につくれた」「なかなか思いつかなかった」「システムの操作が難しかった」「その他（自由記述)」の選択肢を選んでもらった。その結果、3コマまんがの作成は、11名の被験者が「簡単に

作成できた」と回答し、12 名の被験者は、「なかなか思いつかなかった」と回答した。パスワードの作成は、14 名の被験者が「簡単に行えた」と回答し、11 名の被験者が、「なかなか思いつかなかった」と回答した。

3.1 で述べたとおり、提案手法は、ユーザビリティとのトレードオフにより、記憶保持性とクラック困難性を向上させる手法であるため、4.6.3 で述べたように、これまでクラック困難性について意識せずにパスワードを作成してきた被験者の約半数が、プロトタイプを用いて 3 コマまんがや、コマ画像からパスワードを考えることを負担に感じるのは妥当な結果であると考えられる。

5 おわりに

5.1 まとめ

クラック困難性に対する知識を持たないユーザや、パスワード作成時にクラック困難性を意識しないユーザでもクラック困難性が確保可能な認証方法として、複数のパスワードとまんがを用いた認証方法について提案した。

2 コマまんが認証では、高い記憶保持性を維持したまま、クラック困難性に対する十分な知識を持たない被験者に対して、約半数の被験者に十分なクラック困難性を持つパスワードを作成させることができた。しかし、被験者すべてにクラック困難なパスワードを作成させなければ、クラック困難性の確保とは言えず、改良する必要がある。

3 コマまんが認証では、辞書攻撃に対するクラック困難性については、すべての被験者にクラック困難なパスワードを作成させることができ、総当たり攻撃に対するクラック困難性についても、1 名を除くほぼすべての被験者にクラック困難尚パスワードを作成させることに成功した。しかし、記憶保持性に関して、記憶が容易とされている既存の個人認証手法と比較すると、3 コマまんが認証は記憶が容易な個人認証手法とは言えず、今後、改良の余地がある。

5.2 今後の課題

2 コマまんが認証ではクラック困難性の改善、3 コマまんが認証では記憶保持性の改善が必要であり、まんがのコマ数によるトレードオフが発生していることがわかる。今後、十分な記憶保持性と、十分なクラック困難性をユーザに提供可能な認証手法を提案するために、2 コマまんが認証のクラック困難性を向上させるアプローチと、3 コマまんが認証の記憶保持性を向上させるアプローチの 2 通りが考えられる。また、ユーザビリティに関しても、記憶保持性とクラック困難性が十分である手法が確立した後、パスワードの作成時や認証時にユーザにかかる負担が、妥当なトレードオフであると言えるか、十分に実用的なユーザビリティであるかを検証していく必要がある。

謝辞

本研究は一部 JSPS 科研費 23500094 の助成を受けたものである。

参考文献

[1] パスワードを強化する 7 つのヒント, http://ascii.jp/elem/000/000/628/628320/

[2] 桝野隆平, ユーザの心理的負担を視野に入れたパスワードの安全性について, 情報処理学会第 49 回コンピュータセキュリティ研究発表会（CSEC49）.

[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] Jianxin Yan, Alan Blackwell, Ross Anderson, Alasdair Grant, The memorability and security of passwords . some empirical results, UCAM-CL-TR-500, UNIVERSITY OF CAMBRIGE Computer Laboratory Technical Report, 2000.

[6] 高野陽太郎編, 認知心理学 2 記憶, 東京大学出版会, 1995.

[7] 心理学辞典 Psycholopedia, http://wiki.livedoor.jp/psycholopedia/

[8] オクスフォード大学日本語パスワード解析用辞書, ftp://ftp.ox.ac.uk/pub/wordlists/japanese/, 最終更新 : 1992/12/07 午前 12:00