TweetPass: ツイートから想起性と安全性の高いパスワード作成を支援するシステムの提案

坂松春香[†1]　小倉加奈代[†1]　B.B.ビスタ[†1]　高田豊雄[†1]

現在，普及している Web サービスの多くは，パスワード認証方式を採用している．この方式の場合，不正アクセスなどの攻撃に対処するため，ユーザは他者からの推測が困難なパスワードを用いることが望ましいとされている．しかし，多くのユーザは，覚えやすさから辞書にある単語や個人情報をもとにしたパスワードを使う傾向にある．特に若年層のユーザは，強固なパスワードを作成するためのルールを使用しない傾向にある．そこで本論文では，若年層に馴染みのある Twitter と，安全性と想起性の二点を考慮した語呂合わせパスワードを組み合わせたパスワード作成支援システムを提案する．

TweetPass: A Proposal of Secure and Memorable Password Creating Support System Using Tweets

HARUKA SAKAMATSU[†1]　KANAYO OGURA[†1]　BHED BAHADUR BISTA[†1]
TOYOO TAKATA[†1]

Many web services that are currently popular use a password-based authentication method. In order to prevent attacks, such as unauthorized access, the services expect users to create passwords that are difficult to guess and crack. However, many users tend to use a password that is based on the personal information or dictionary words for easy remembering. Young users, especially, tend not to use rules to create strong passwords. In this paper, we propose a password creating support system to create a password which is secure and also easy to remember. In particular, the system supports the creation of a password by using mnemonic phrase-based rules to enhance the safety of the password. Twitter which is a kind of life-log and is used by many people is used as a source for creating the password.

1. はじめに

パソコンやインターネットの普及に伴い，様々な Web サービスが利用されている．その Web サービスの多くは，ID とパスワードを用いたパスワード認証が主流である．認証に用いるパスワードは，他者からの推測を困難にするために，安全性の面から，以下の 3 つのルールを満たしていることが望ましいとされている[1].

1. 英文字（大文字，小文字），数字，記号のような複数の文字種を利用
2. 最低 8 文字以上の文字列
3. 個人情報をもとにした単語や辞書にある単語を利用しない

しかし，多くのユーザは，パスワード設定の煩雑さや，設定したパスワードを覚えやすくするため，単純な文字列や，誕生日などの個人情報に類する単語を用いたパスワードを設定することが多い．2012 年の 1 年間に個人から寄せられた不正アクセスの届け出の中で目立ったものは，「オンラインサービスのアカウントの乗っ取り」に関する届け出であり，原因の 1 つとしてパスワードが単純だったために，パスワードが推測されたことがあげられている[2]．特に，10 代やパソコン習熟度のレベルが低い利用者は，前述の 3 つのルールを使用しない傾向にある[3]．不正アクセスに対処するためには，パスワードを使用するすべてのユーザが安全性の点で適切なパスワードを作成する必要がある．

また，1 人で複数の Web サービスを利用することが多いが，サービス毎に異なるパスワードを設定しているユーザは全体で 2 割強しかいない[3]．複数のサービスで同じパスワードを使いまわしていると，パスワードリスト攻撃と呼ばれる，複数のサービスで同一の ID とパスワードを使い回している状況を悪用し，不正に取得した ID とパスワードのリストから不正アクセスを試みる攻撃に遭う危険性がある．パスワードリスト攻撃に対処するためには，パスワードを使い回しせずにパスワードを作成，利用する必要があり，そのために，高い安全性と想起性をあわせもつパスワードを作成する必要がある．

本研究では，想起性を高めるために，Web サービス等に蓄積されたユーザのログ（以下，ライフログ）の 1 つである Twitter から抽出した特徴的な単語をパスワードの素として利用し，安全性を高めるために，語呂合わせルールを用いてパスワードを作成する手法を提案する．

本稿では，本章以下，次章では，関連研究として，想起性，安全性に着目したパスワード生成システム，手法に関する研究を概観する．第 3 章では，提案システムの概要について述べ，第 4 章では，提案システムを用いた予備実験とその結果について述べ，第 5 章ではまとめと今後の課題について述べる．

†1 岩手県立大学ソフトウェア情報学部
Iwate Prefectural University, Faculty of Software and Information Science

2. 関連研究

本章では，想起性を高めるためのパスワード生成手法および，安全性を高めるためのパスワード生成手法に関する関連研究を概観する．

2.1 想起性に着目したパスワード生成手法

想起性に着目したパスワード生成手法として，エピソード記憶にもとづく秘密の質問を使ってパスワードを生成/管理するシステム「EpisoPass」が提案されている[4]．EpisoPass では，秘密の質問とその回答にもとづいて，シード文字列を換字することでパスワードを生成する．シード文字列や質問への回答によって異なるパスワードが生成されることを利用し，複数のサービスに対してそれぞれ異なるパスワードを生成/管理することができる．また，シード文字列を逆計算することにより，元々使用していたパスワードの管理も行うことが可能である．生成されるパスワードは英文字（大文字，小文字），数字，記号の多くの文字種を利用した強固なパスワードであるが，ユーザにとって記憶することは困難であると思われる.また，実際に使用する場合，利用しているサービスへログインするたびに EpisoPass を用いてパスワードを確認しなければならず，利便性は低いと考えられる．

2.2 安全性に着目したパスワード生成手法

安全性に着目したパスワード生成手法として，語呂合わせを利用したパスワード生成手法がある[5]．語呂合わせを利用したパスワード生成では，最初にフレーズ（文や句）を考え，文字の省略（例えば，「you」を「u」）や置換(例えば，「l（エル)」を「1（イチ)」）することにより，フレーズを変換してパスワードを作成する[5]．また，語呂合わせを利用したパスワード生成の研究として，画像から単語を連想し，語呂合わせによりパスワードを作成する手法が提案されている[6]．この提案では，語呂合わせパスワードを作成する際，ユーザは推測されやすい有名フレーズを使う傾向にあるという点に着目し，画像をヒントとし，その画像を元にフレーズを考え，語呂合わせパスワードを作成することで，ユーザ自身がオリジナルのフレーズを考えることを容易にしている．しかし，この提案では，できるだけ多くの単語を連想できる画像を用意しなければならず，作成までに手間がかかるという問題点がある．

3. 提案手法

本研究では，高い想起性と安全性の両立を目指したパスワード生成手法を提案する．具体的には，想起性を高めるために，Twitter で発信されたユーザの投稿文中の特徴語を抽出し，安全性を高めるために，抽出した特徴語に対し，語呂合わせルールを用いてユーザがパスワードの最終決定を行う．

3.1 想起性を高めるための工夫

想起性を高めるために，近年ユーザ数が多く，多くの人々に馴染みがあり，身近に利用されているライフログである Twitter を利用する．

パスワードを作成する際に Twitter と同様のライフログを利用する際に以下 2 つの利点があると考える．

1. パスワードを記憶する負荷を軽減
2. リアルタイムで変化するために，ある程度のタイムスパンで異なるパスワードの作成が可能

ライフログはユーザ自身が発信してきた過去の情報であり，既知で忘却されにくいエピソード記憶の一つである．したがって，ライフログを利用することはユーザにとって記憶負荷の軽減に繋がると期待できる．また，ライフログは逐次ユーザによって増加し続け，リアルタイムで内容が変化し続ける．この特性を利用することで，このシステムを利用するたびに異なるパスワードを作成することが可能であると考える．

3.2 安全性を高めるための工夫

安全性を高めるために，第 1 章で述べた安全性の面から推奨されているパスワード生成のルール[1]を踏襲した語呂合わせを利用したパスワード生成手法を利用する．なお，本提案では，複数の語呂合わせの候補からユーザ自ら最終的に利用するパスワード列を選択することで，想起性に配慮する．

3.3 提案手法概要

本稿では，前述のとおり，高い想起性と安全性の両立を目指したパスワード生成支援を行うため，大きく以下 2 つの手順をふむ．

手順 1：パスワードの素となる単語の抽出と選択

各ユーザの Twitter の投稿文から特徴的な単語の候補を提示し，ユーザ自らパスワードの素となる単語を候補の中から選択する．

手順 2：選択単語の変換とパスワード列の作成

手順 1 でユーザが選択した各単語に対し，語呂合わせルールを適用し，適用後の候補文字列パタンをユーザに提示する．ユーザは候補の中から使用する文字列パタンを選択し，選択した文字列パタンを組み合わせて最終的なパスワード列を作成する．

3.3.1 手順 1：パスワードの素となる単語の抽出と選択

手順 1 では，大きく以下 2 つの処理を行う．

処理 1:

各ユーザは自身のアカウントにおいて，Twitter の投稿文を取得するアプリの使用を許可し，システムは許可を出したユーザアカウントから最新 500 件の投稿文を取得する．

処理 2:

システムは取得した投稿文から形態素解析器 MeCab[7]を用いて，名詞，動詞，形容詞を原型に戻した状態で抽出．それらの単語に対し TF-IDF 値に基づいたランキング付けを行い，各品詞上位 5 位（計 15 個）の単語をユーザへ提示する（図 1）．ユーザは，提示された単語から複数の単語を

選択し，組み合わせて 1 つの文または句を考える．なお，選択できる単語の数に制限はない．

処理 1 において，使用する Twitter の投稿文からは，「@付きの TwitterID」，「#マーク付きのハッシュタグ」，「http://もしくは https://から始まる URL」，「(,)，^，_などの記号」を事前に削除する．これは，抽出される単語に，TwitterID などのユーザ自身の言葉で発信したわけではない単語や顔文字が抽出されるのを防ぐためである．

処理 2 において，デフォルトの IPA 辞書（mecab-ipadic）では，人名などの固有名詞の形態素解析が難しいため，ユーザ辞書として，Wikipedia データベース[8]と，はてなダイアリーキーワードふりがなリスト[9]からダウンロードした csv ファイルを MeCab の辞書形式に整形したものを利用した．なお，Wikipedia データベースは約 135 万語，はてなダイアリーキーワードふりがなリストは約 39 万語であり，はてなダイアリーキーワードふりがなリストのファイル名および公開日付は 2006 年であるが，ファイルの内容は 2013 年の用語も含まれている．

図 1 抽出単語表示画面

3.3.2 手順 2：選択単語の変換とパスワード列の作成

手順 2 では，前述の手順 1 の処理 2 において，ユーザが選択した単語に対し，語呂合わせルールを適用した文字変換候補を提示する．ユーザは，提示した候補もしくは自身で考えた置換ルールを用いて，文字の省略や置換を行うことにより最終的に利用するパスワードを作成する（図 2）．

4. 予備評価実験

6 名の大学生に対し，本提案システムを利用してパスワードを作成する予備評価実験を行った．予備評価実験で作成したパスワードをもとに，想起性と安全性に関する評価を行った．

図 2 語呂合わせルールを適用したパスワード作成画面

4.1 作成したパスワードの特徴

被験者 6 名が作成したパスワードの文字長について調べたところ，最短 10 文字，最長 14 文字，平均 11.7 文字であった．第一章で述べた安全性の高いパスワードを作成するための推奨ルールで文字長は，「最低 8 文字以上」とされており，安全性を確保するための文字長を大きく超えている．

実際にどの単語の素から語呂あわせルールによる文字列変換パタンを選択し，最終的にどのようなパスワードを作成したかを示すため，以下にある被験者の作成例を示す．

【被験者 1】

・パスワード:5hirentantan0

・選択単語と変換方法は表 1 の通り

表 1 被験者 1 のパスワード作成過程

選択単語	変換候補
試練	shiren → 5hiren （s を似た形の 5 に置換）
たん	tan → tantan
おいしい	oishii → 0

【被験者 2】

・パスワード:PhTecthiAkeiAI

・選択単語と変換方法は表 2 の通り

表 2 被験者 2 のパスワード作成過程

選択単語	変換候補
写真	Photos → Ph
技術	Techonology → Tec
高い	takai → thiAkeiAI

4.2 想起性の評価

想起性の評価では，本提案システムを利用してパスワードを作成した 1 週間後に作成したパスワードを使用してログインできるかどうかを調査した．

調査の結果，被験者 6 名中，5 名はログインに成功し，1 人（前述の被験者 2）のみログインに失敗した．失敗した原因をインタビューしたところ,「どの部分の小文字を大文字にしたのか，思い出せなかった」という，ユーザによる最終的なパスワード列作成過程の記憶の欠落により起こっていることが原因であることがわかった．ログインに失敗した被験者 2 のパスワード生成過程（表 2）からも，作成されたパスワードの文字長は，14 文字と推奨文字列長の 8 文字, 本予備実験の平均の 11 文字よりもさらに長い文字列であり，加えて，パスワードの素として選択した単語よりも変換の際の文字数のほうが多く，最終的なパスワード列作成過程で複雑な変換を行っていることがわかる．

4.3 安全性の評価

安全性の評価として，パスワードのクラック困難性を評価した．具体的には，Microsoft 社の提供するパスワードチェッカー[10]を利用した．このパスワードチェッカーは，入力されたパスワードのクラック困難性を,「弱い」,「普通」,「強い」,「とても強い」の 4 つのスコアを表示する．なお，パスワードチェッカーの判定基準は，1）使用する文字種，2）パスワードの文字長（8 文字以上推奨），3)パスワードが辞書に記載されているかどうかの 3 つである．

評価の結果，被験者 6 名のうち 5 名が「普通」，1 名（前述の被験者 2）が「強い」パスワードを作成していることがわかった．これより，本システムのような単語の変換候補を表示したとしても，ユーザは必ずしもクラック困難性の高いパスワードを作成するわけではないということが明らかとなった．これには，日本人などの漢字圏のユーザにとって，アルファベットの置換に馴染みがないことも，原因の 1 つとして考えられる．

5. まとめ

本稿では，高い想起性と安全性の両立を目指したパスワード生成支援システムを実現するため，想起性を高めるために，Web サービス等に蓄積されたユーザのログ（以下，ライフログ）の 1 つである Twitter から抽出した特徴的な単語をパスワードの素として利用し, 安全性を高めるために，語呂合わせルールを用いてパスワードを作成する手法を提案した．

提案手法の予備評価のため，被験者 6 名に本提案システムを利用してもらい，実際にパスワードを作成する実験を行った．その結果，被験者が作成したパスワードの特徴として, 作成したパスワードの文字長は, 平均で 11.7 文字と，安全なパスワード作成の推奨ルールにある「8 文字以上の文字列」を満たすことがわかった．さらに，想起性の評価として，1 週間後に作成したパスワードを用いてログインできるかどうかを実験したところ，6 名中 5 名がログイン可能であり，ログインに失敗した被験者のパスワード生成過程を分析したところ, 最終的なパスワード文字列長が 14 文字と平均より大幅に長い文字列長であり，さらに，語呂あわせルールの提示後の変換文字列のほうが変換前の文字列よりも多い部分があるという，本提案システムの想定を超えた複雑なパスワードの作成を行っていることがわかった．また，安全性の評価として，被験者が作成したパスワードに対し，パスワードチェッカーを用いてクラック困難性の評価を行い，6 名中 1 名は「強い」，5 名は「普通」という評価結果を得た．この点について，日本人のように漢字圏のユーザにとって，安全性の高いパスワード作成の推奨ルールにあるようなアルファベットの置換に馴染みがないことも原因の 1 つとして考えられ，今後改善の余地があると考える．

今後は，本提案手法の更なるクラック困難性の評価と，それに対する改善手法の提案を行う予定である．

参考文献

1) 独立行政法人情報処理推進機構: コンピュータ不正アクセス被害防止対策集, http://www.ipa.go.jp/security/ciadr/cm01.html.
2) 独立行政法人情報処理推進機構: 情報セキュリティ白書 2013, pp.29-30, pp.184-186 (2013).
3) 独立行政法人情報処理推進機構: 情報セキュリティ白書 2013, pp.190-191 (2013).
4) 増井俊之: EpisoPass: エピソード記憶にもとづくパスワード管理, WISS2013, 入手先 <http://www.pitecan.com/episopass.pdf> (2013).
5) Yan, J. et al.: Password Memorability and Security: Emprical Results, IEEE Security & Privacy Magazine, vol.2, No.5, pp.25-31 (2004).
6) 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 (2009).
7) MeCab, http://mecab.googlecode.com/svn/trunk/mecab/doc/index.html.
8) Wikipedia データベース, http://dumps.wikimedia.org/jawiki/.
9) はてなダイアリーキーワードふりがなリスト, http://d.hatena.ne.jp/hatenadiary/20060922/1158908401.
10) Microsoft: パスワードチェッカー: 安全性の高いパスワードの利用, https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx.