想起性と安全性を両立するパスワード生成過程の分析
An analysis of the process for creating memorable and secure passwords

小倉　加奈代† 坂松　春香† ベッド バハドゥール ビスタ† 高田　豊雄†
Kanayo Ogura, Haruka Sakamatsu, Bhad Bahadur Bista, Toyoo Takata

†岩手県立大学
Iwate Prefectural University
{ogura_k, bbb, takata}@iwate-pu.ac.jp
s231g017@s.iwate-pu.ac.jp

Abstract

As a personal identification method, one of the most widely used authentication methods is a password-based authentication method. In this method, it is necessary to set a random character string using variety of letters and special characters as a password to make it difficult to crack. However it is difficult to remember such passwords and as such inconvenience for users. Therefore many users tend to set memorable passwords based on a simple character string and personal information. To solve this problem, we proposed a password creating support system, which helps to create mnemonic phrase-based password from Twitter. In this paper, we reveal obstacles to memorizing strong passwords by analyzing the process for creating passwords using our proposed system.

Keywords — Password-based authentication, Mnemonic, Long-term Memory, Short Term Memory

1. はじめに

現在，タブレット端末やスマートフォンの普及に伴い，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方式を採用している．この認証では，他者からの推測を困難し，安全性を確保するために，以下ルールに基づいたパスワードを設定し，利用することが望ましいとされている[1]．

(1)最低6文字,通常8文字以上の文字列使用
(2)英文字（大文字，小文字），数字，記号のような複数の文字種使用
(3)個人情報をもとにした単語,辞書に載っている単語を使用しない
(4)最低3ヶ月に1回の変更

しかし，上記ルールを全て盛り込んだパスワードを作成することは一般ユーザには困難である．多くのユーザは，パスワード設定の類雑さや，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傾向にある．実際に，2012年の1年間に個人から寄せられた不正アクセスの届出で目立ったものは,「オンラインサービスのアカウントの乗っ取り」に関する届出である．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挙げられる[2]．また，10代やパソコン習熟度のレベルが低い利用者の多くは，簡粗なパスワードを設定する傾向にある[2]．

また，大半のユーザは，複数のWebサービスを利用するが，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割強である[2].複数のサービスで同じパスワードを使い回すと，パスワードリスト攻撃と呼ばれる，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あらゆるWebサービスに不正アクセスを試みる攻撃に遭う危険性がある．以上から，パスワードは，高い安全性と記憶保持性をあわせもつ必要があるといえる．

この高い安全性と記憶保持性をあわせもつパスワード作成を支援するために著者らは， 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つであり，若年層を中心に利用者の多いTwitterを用いたパスワード作成支援システムを構築，提案した[3]．

本稿では,著者らが提案したシステムおよび,安全性の高いパスワード生成方法の 1 つである単語の素を変形させる方式の 2 つのパスワード生成方法を利用し，ユーザがパスワードを生成する過程および，パスワード生成 1 週間後にどの程度再現可能かを分析する．これにより，生成したパスワードのどの部分が想起に関わりをもつかを明らかになることで，想起性と安全性の高いパスワード作成を支援する際に取り入れるべき点，留意すべき点を具体化することができるとともに，著者らの提案システムの改良にも有用となる．

本稿は，本章以下，2 章では，著者らが提案したパスワード作成支援システムの概要について説明する．3 章では，2 章で説明した提案システム使用群とパスワードの素となるフレーズを作成した後に語呂合わせルールを適用しパスワードを作成する群によるパスワード生成および再現実験の手続きと結果について述べる．4 章では 3 章の実験時のパスワード生成に関わる過程の分析とその結果について述べ，5 章では本稿のまとめと今後の課題について述べる．

2. 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の提案

著者らは，想起性と安全性の高いパスワード作成支援システムを提案した[3].提案したシステムでは想起性を高めるために，利用ユーザが多いライフログの 1 つである Twitter のユーザ自身の投稿文の特徴語を用い，安全性を高めるために，抽出した特徴語に語呂合わせルールを適用し，パスワード作成を支援する．

2.1 パスワードの素となる特徴語の抽出と選択手順

各ユーザの Twitter の投稿文から特徴語の候補を提示し，ユーザ自らパスワードの素となる特徴語を候補の中から複数選択する．具体的には，以下の 2 つの処理を行う．

- 処理 1

各ユーザは普段使用している自身の Twitter 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 MeCab[4]を用いて，名詞，動詞，形容詞を原形に戻した状態で抽出する．それらの単語に対して TF-IDF 値に基づいた順位付けを行い,各品詞上位 5 位（計 15 個）の特徴語をユーザへ提示する（図 1）．ユーザは，提示された 15 個の特徴語から複数の特徴語を選択し，組み合わせて 1 つの文または句を考える．なお，ユーザが選択できる特徴語の数は n（2≦n≦15）個である．

図 1 特徴語提示画面

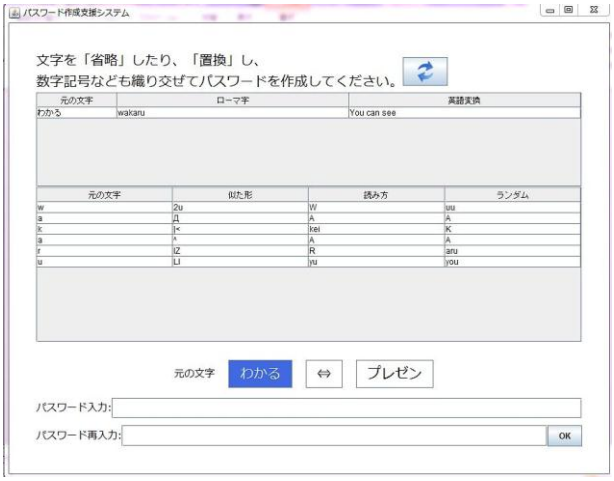

図 2 語呂合わせルール適用画面

2.2 語呂合わせルール適用とパスワード列作成手順

前述の処理 2 において，ユーザが選択した各特徴語に対して語呂合わせルールを適用し，適

用後の候補文字列をユーザに提示する（図 2）．ユーザは候補の中から使用する文字列を選択するか，ユーザ自身で文字列を考え，それぞれの文字列を組み合わせて最終的にパスワードとして利用するパスワード列を作成する．なお，提示される候補文字列パタンは，英語変換した各単語と，表 1 に示すようなアルファベットごとの置換候補である．各アルファベットと類似する形状の文字列，読み方が同じ文字列，類似形状文字列と読み方が同じ文字列からランダムに選択される文字列の 3 項目が提示される．

表 1　置換候補例

元の文字	類似形状	読み方	ランダム
u	L|	you	v

3. パスワード生成および再現実験

提案システムにより作成されたパスワードの想起性と安全性を評価するために，以下を評価項目とする実験を行った．

評価項目 1.パスワードの再現性

評価項目 2.パスワードの安全性

評価項目 3.パスワードの素が想起性にあたえる影響

3.1　実験手続き

18 歳～22 歳の大学生 18 名（男性 8 名，女性 10 名）に対し，パスワードの素となるフレーズを作成し，フレーズに語呂合わせルールを適用しパスワードを作成する「語呂合わせ群」(9 名)と，提案システムを用いてパスワードを作成する「提案システム群」(9 名）の 2 群に分けて実験を行った．具体的な実験手順は以下である．

実験手順 1.　（パスワード作成の事前準備）

パスワード作成の事前準備として，被験者に以下パスワード作成の際の注意事項を提示した．

- パスワードを長くする（8 文字以上推奨）
- 英文字（大文字，小文字），数字，記号の多くの文字種を利用する
- 紙などに作成したパスワードを書かない
- スマートフォンや PC を使ったり，記録に残したりしない

その後，語呂合わせ群には，フレーズ作成の後，語呂合わせルールを適用するパスワードの作成方法を，提案システム群の被験者には，提案システムの利用によるパスワード作成方法をそれぞれ提示した．なお，提案システム群の被験者には，自身の Twitter アカウントから最新 500 件の Twitter 投稿文を提供してもらった．

実験手順 2.　（フレーズ作成）

語呂合わせ群の被験者は，パスワード作成用のフレーズを作成した．提案システム群の被験者は，提案システムで抽出された特徴語を選択し，パスワード作成用のフレーズを作成した．また，評価項目 2 を評価するために，提案システム群の被験者は，システムから提示された特徴語について，Twitter 上で過去につぶやいた記憶があるかどうかを回答した．

実験手順 3.　（パスワード作成）

語呂合わせ群の被験者は，手順 2 で自身が作成したフレーズに対し，「i」を「1」に置換する，「a」を「@」に置換する等の語呂合わせルールを取り入れてパスワードを作成した．提案システム群の被験者は，システムが提示する変換候補を用い，パスワードを作成した．また，パスワード認証の練習として，各群の被験者は 5 回の認証を行った．

実験手順 4.　（ログイン）

実験手順 1～3 を行った 1 週間後，全被験者は，自身が作成したパスワードを使用しログインした．前述の 2 つの評価項目を評価するために，被験者がログインに失敗した回数（以降，ログイン失敗回数）とログインに掛かった時間（以降，ログイン試行時間）を記録した．ただし，最大ログイン失敗回数は 5 回とした．

3.2 実験結果：パスワードの再現性

各群の被験者が作成したパスワードの文字数，1 週間後のログイン失敗回数，ログイン試行時間について，平均と標準偏差を表 2 に示す．なお，一元配置分散分析および t 検定において，有意水準はすべて 0.05 とした．

表 2 各群のパスワード文字数，ログイン失敗回数と試行時間

		語呂合わせ	提案システム
パスワード長（文字）	平均	12.6	14.6
	標準偏差	2.4	2.1
ログイン失敗回数（回）	平均	1.3	0.7
	標準偏差	2	1.54
ログイン試行時間(sec.)	平均	28.8	41.6
	標準偏差	28.2	50.5

ログイン失敗回数において，F=0.38，t=0.65 より，語呂合わせ群と提案システム群の間に有意差はない．また，ログイン試行時間においても，F=0.21，t=0.65 より，有意差はないといえる．この結果について，実際の結果はどうなったのか，ログインに 1 回以上失敗した人数を調べた．語呂合わせ群では，1 週間後のログインに失敗した被験者(ログイン失敗回数が 5 回)は 2 人，ログイン成功まで複数回ログインを行った被験者は 2 人であった．提案システム群では，ログインに失敗した被験者は 1 人，ログイン成功までに複数回ログインを行った被験者は 2 人であった．

3.3 実験結果：パスワードの安全性

パスワードの安全性を評価するために，被験者が作成したパスワードが，1 章で述べた以下の IPA が推奨する安全性の高いパスワード作成基準を満たすかを調査した．

基準1 8 文字以上の文字列の使用

基準2 英文字（小文字，大文字），数字，記号の複数の文字種を使用

基準3 個人情報をもとにした単語や辞書に載っている単語を使用しない

基準 2 にある「複数の文字種」とは，ここではアルファベットの大文字，小文字，数字，記号のことを指し，1 つでも使用していない文字種がある場合は「複数の文字種を利用していない」こととする．調査結果を表 3 に示す．語呂合わせ群（9 名）では，9 名全員が基準 1 を満たし，基準 2 を満たす被験者が 6 名，基準 3 を満たす被験者が 8 名であった．一方，提案システム群（9 名）の場合も，9 名全員が基準 1 を満たし，基準 2 を満たす被験者が 6 人，基準 3 を満たす被験者が 7 人であった．

表 3 安全性の高いパスワード作成基準を満たす被験者数

	基準 1	基準 2	基準 3
語呂合わせ	9	6	8
提案システム	9	3	7

また，パスワードが強力かを判定するパスワードチェッカー[5]を用いて作成したパスワードを，「弱い」，「普通」，「強い」，「とても強い」の 4 段階で評価を行った結果を表 4 に示す．いずれの群も「弱い」と評価されたパスワードはなかったが，「強い」または「とても強い」の評価数をみると，語呂合わせ群では 5，提案システムのほうが 7 と提案システムを用いて作成したパスワードのほうが強力なパスワードが作成しやすい可能性があることがわかった．

表 4 パスワードチェッカーによる作成パスワードの強度評価

	弱い	普通	強い	強力
語呂合わせ	0	4	2	3
提案システム	0	2	5	2

*「とても強い」は「強力」と表記

さらに，パスワードのクラック困難性を評価するために，作成されたパスワードに対して，John the Ripper[6]による辞書攻撃を行った．その結果，作成されたすべてのパスワードは解析されなかった．

3.4 実験結果：パスワードの素が想起性に与える影響

パスワードの素が想起性に与える影響を調べるために，提案システム群の被験者（9 名）に対して，各被験者の Twitter 投稿文から抽出し，システム上に提示した特徴語に対する記憶に関する調査を行った．具体的には，システム上に提示された抽出特徴語 15 個について，Twitter 上で何の話題について投稿したのか，明確な記

憶が残っている場合には○（以下，記憶にある語),投稿した記憶はあるが何の話題について投稿したのか記憶にない場合は△（以下，あいまいな語)，まったく記憶にない場合は×（以下，記憶にない語）として調査した．その結果を表5に示す．表5より，システム上に提示される特徴語のうち，最低3個は，自分が過去にTwitter上でつぶやいたと記憶に残っている単語であることがわかる．

表 5　抽出した特徴語記憶に関する調査結果

	最小	平均	最大
記憶にある語（個）	3	5.3	7
あいまいな語（個）	1	5	11
記憶にない語（個）	0	4.6	9

また，ログインに失敗した1名の被験者が，パスワードの素として選択した特徴語の記憶について調べると，完全なパスワードを想起することができなかったが，パスワードの素となった抽出特徴語2語について，語順も含め正しく記憶しているという結果であった．なお，語呂合わせ群のログインに失敗2名の被験者についても同様に，パスワードそのものを想起できなかったが，パスワードの素となるフレーズを正しく記憶しているという結果であった．

4. パスワードの素と語呂合わせルール適用，変換過程の分析

本稿でのパスワード作成手順は，提案システム群,語呂合わせ群ともに(1)パスワードの素を作成する（提案システム群では抽出特徴語から単語を選択,語呂合わせ群では,フレーズ作成),(2)語呂合わせルールを用いてパスワードの素を変換し，最終的なパスワードを作成するという2つの作成手順がある．本章では，どのようにパスワードの素が選択され，どのような変換過程を経て最終的なパスワードが作成されるか,それらが想起性にどのように影響するかを分析,検討する．

表 6　語呂合わせ群の作成フレーズと理由

人/認証	フレーズ（上）/理由（下）
A/成功	いちごといったらとちおとめ
	出身地の名産だから
B/失敗	空は青い
	特になし
C/成功	ポップなキャンディーカラー
	響きが好きだったから
D/成功(2)	白鳥の湖
	バレエ曲
E/成功	ライブに行きたい
	今の心境
F/成功(2)	冬はこたつ
	冬はこたつがないと生活できない
G/成功	艦隊これくしょん
	流行しているゲーム
H/成功	レジにて半額
	スーパーの売り文句
I/失敗	ジンギスカンが好き
	好きな食べ物だから

*認証の「成功」は1回目で認証に成功した場合,「成功(2)」は2回目で認証に成功した場合,「失敗」は5回ログインに失敗した場合を示す.

4.1 パスワードの素の分析

パスワードの素の作成方法については，3.1節の実験手順2で述べたように，語呂合わせ群は，各自で自由に作成したフレーズをパスワードの素として利用した．一方，提案システム群は，システム上に提示される被験者自身のTwitterから抽出された特徴語15個（名詞，動詞，形容詞各5個）から2個以上の特徴語を被験者自身が選択し，パスワードの素とした．語呂合わせ群(9 名)が作成したフレーズとフレーズ作成理由を表 6 に，提案システム群(9 名)がパスワードの素として選択した特徴語とそれぞれの記憶の有無,選択理由について表7に示す．なお，提案システム群の記憶の有無の調査方法については，3.4節の調査方法と同様である．

表6の語呂合わせ群の作成フレーズと理由をみると，出身地の名産と関連づけるといった再

生が容易であると思われるフレーズを作成する被験者，その場で思い浮かんだものをフレーズとする被験者がいることがわかる．

表 7 の提案システム群のシステム上で提示された特徴語から各被験者が選択した語とその記憶の有無，理由についてみると，ほとんどの被験者は，Twitter 上で過去につぶやいた記憶のある語を選択しており，記憶にない語でも，「響きがいい」，「語呂がいい」といった印象に残る語を選択していることがわかる．

4.2 語呂合わせルール適用，変換過程の分析

パスワードの素を選んだ後に，どのような語呂合わせルールを適用し，パスワードへ変換したかについて，語呂合わせ群について表 9 に，提案システム群について表 10 に示す．

語呂合わせ群については，被験者自身がパスワードの素から最終的なパスワードへ変換したが，3 章の実験手順 3 説明時に，「作成したフレーズに対し，「i」を「1」に置換する，「a」を「@」に置換する等の語呂合わせルールを取り入れてパスワードを作成する」という説明を受けたため，表 9 では，ほとんどの被験者が，説明例と同一の「i→1」，「a→@」，「o→0」というルールを利用した．説明例以外に使用された変換方法としては，長い単語を短縮するために，頭文字のみを採用する方法や，音としてとらえた際の平仮名の行と何段目か（実際の例では「は」はハ行 1 段目であるので「H１」）を変換に使用する方法が使われていた．

提案システム群については，被験者は，2.2 節で説明したとおり，システム側から提示される変換ルールを用いた候補を参照し，最終的なパスワードへの変換を行う．したがって，表 10 の各被験者が行った変換方法は，共通した語呂合わせルールに基づいたものである．しかし，語呂合わせ群と同様に，長い単語を短縮するための各種方法や，語順の入替が行われていた．

表 7 提案システム群が選択した特徴語と記憶の有無，選択理由

人/認証	選択語（上）/記憶有無，理由（下）
A/成功	中村／美しい
	○最近の愚痴り／×インパクト
B/成功(2)	流れる／つく／おいしい／ずさん／ばっちい／課題
	○4 月に流れるプールにいったこと／×短くて数字に置き換えやすい／×頻繁につぶやいている／×響きがいい／×響きがいい
C/成功	カイ／モモンガ／ムササビ
	○飼い始めた猫の名前／○モモンガとムササビの違いを調べていた／○（前に同じ）
D/失敗	カルシウム／走る
	○カルシウムせんべい／○朝ジョギング
E/成功	チェック／度胸／切ない
	○チェック柄の服／○診断メーカー結果／○恋愛系アニメの感想
F/成功	京都／パンツ／やわらかい
	○友達のインターン話／○後輩に対してのセクハラ話／○女性の胸がいい理由
G/成功	岩手／吹雪く／辛い
	○天気の話／○先週実家が吹雪いた／○ゼミ資料の作成
H/成功(2)	ネギ／みそ／ける
	○食べきれなくて困っている話／○親から送られてきた，好きとつぶやいた／×語呂がいいから
I/成功	iPad／とぐ／おいしい
	○iPad を買った時／○10 月ごろ米をといでいる時の話／×外食した話だと思うが覚えてない

*認証の記述は表 5 と同様である．

5. 考察：認証に失敗したパスワード

認証に失敗したパスワードは，語呂合わせ群 2 個（以下「語呂 F1」,「語呂 F2」），提案システム群で 1 個（以下「提案 F3」）である．表 8 に認証に失敗した 3 つのパスワードとパスワード長(PW 長)，試行時間，安全性の高いパスワード 3 基準達成状況，強度を示す．

表 8　認証に失敗したパスワードのパスワード長，試行時間，3 基準達成状況，強度

	PW 長	試行時間	基準	強度
語呂 F1	13	28.1	3/3	普通
語呂 F2	9	20.1	3/3	普通
提案 F3	14	36	2/3	強い
語呂平均	12.6	11.3	-	-
提案平均	14.6	21.3	-	-

表 8 よりパスワード長をみると，認証に失敗したパスワードと成功したパスワードの長さに大きな差はない．ここから，認証失敗の理由がパスワードの長過ぎといったパスワード長とは無関係であるといえる．次に試行時間については，認証に失敗したパスワードについてそれぞれの平均値よりも時間を要していることがわかる．前述のパスワード長と試行時間から，パスワード入力時に思い出せない，もしくは入力誤りの修正のために時間を要している可能性があることがわかる．また，安全性の高いパスワード作成のための 3 つの基準の達成状況とパスワード強度についてみると，基準達成状況については提案システム群の認証失敗パスワードのみ「複数の文字種を使用」が未達成であり，強度についてみると，語呂あわせ群の 2 つともに「普通」，提案群は「強い」であり，パスワードの使用文字列が極端に複雑でも安全性を阻害するような単純なものでもないことがわかる．

ここで，4 章で述べた本稿での 2 つのパスワード作成手順のうちのいずれに問題があるかを特定するために，それぞれの手順ごとに検討する．

まず，1 つ目の手順であるパスワードの素の作成について，表 6 および 7 より，語呂あわせ群の認証失敗パスワードの 2 つのうちの 1 つは，作成理由が「特になし」とその場で思いついた想起しにくいフレーズをパスワードの素として使用していることがわかる．残りは，「好きな食べ物」と，想起しやすいフレーズを素として使用している．提案システム群の 1 つについては，選択語のすべてが「過去につぶやいた記憶のある単語」であると評価されており，想起しやすい語を素として利用している．語呂合わせ群の想起しにくいフレーズを用いていた被験者も含め，事後アンケート結果では，認証失敗パスワードを作成した被験者 3 名全員が「パスワードの素は思い出すことができた」と述べており，パスワードの素が認証に失敗には影響していないといえる．

次に，2 つ目の手順である，パスワードの素に語呂合わせルールを適用し変換する過程について，表 9 および 10 をみると，まず語呂合わせ群の失敗パスワードの 1 つ目について，フレーズからの変換について「o→0」,「a→@」,「”ha”はハ行 1 段→H1」,「青い→ブルー」,「“bu”はバ行 3 段→b3」,「”ru”はラ行 3 段→r3」,「単語. で連結」という 7 つの変換手順を経て最終的なパスワードにいたることがわかる．また，提案システム群の失敗パスワードについて，「カルシウムを”Karu”に短縮する」,「”Karu”を繰り返す」,「r→12」,「”Run”→”Rn”」,「”Rn”を繰り返す」,「“カルシウム”と“走る”語順を入れ替える」という 7 つの変換手順を経て最終的なパスワードにたどり着くことがわかる．パスワードの素については，「好きな食べ物」や「過去につぶやいたことを思い出せる単語」といった長期記憶に類する要素であるため，想起性の点で問題はないといえる．一方，語呂合わせルールを用いた変換過程については，変換ルールがその場で使用する手続きであくまでも短期記憶に類する要素である上に，前述のいずれの失敗パスワードも 7 つの変換手順を使用していることから，手順数が短期記憶の容量を超えており，想起性に悪影響を及ぼしている可能性がある．

6. まとめと今後の課題

本稿では，著者らが提案した想起性と安全性の高さを両立するパスワード作成支援システムおよび，安全性の高いパスワード生成方法の 1 つである単語の素を変形させる方式の 2 つのパスワード生成方法を利用したパスワード生成および再現実験を行った．その結果，作成したパスワードに対し，安全性の高いパスワード作成基準の適用状況判定とパスワードチェッカーを用いた強度判定により提案システムで作成されるパスワードの安全性の高さを確認した.また，パスワードの素の作成過程，パスワードの素に語呂合わせルールを適用し，最終的なパスワードへ変換する過程の分析を行い，パスワードの素の作成過程で，提案システムを用いた群の想起性の高さを確認した．しかし，語呂合わせルールを適用し，最終的なパスワードに変換する過程で，適用ルールが多くなると，想起性に悪影響を及ぼす可能性があることを確認した.

今後は，提案システムについて，パスワードの素に語呂合わせルールを適用し，変換する過程の簡略化を検討，改良するとともに，パスワードの素から最終的なパスワードへの変換過程において，パスワードそのものの安全性と変換ルールの簡略化とのトレードオフ点を実験の積み重ねにより明らかにする予定である．また，変換ルール数，変換ルールの複雑さと短期記憶容量との関係を探るための実験も行う予定である.

参考文献

[1] 独立行政法人情報処理推進機構,(2012) “ 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（参照 2014-07-25）.

[2] 独立行政法人情報処理推進機構,(2013)“情報セキュリティ白書 2013”，pp.29-191.

[3] 坂松春香，小倉加奈代，Bista, B.B.，高田豊雄,(2014)“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”，インタラクション 2014 論文集, B6-1, pp.525-528.

[4] “MeCab”, http://mecab.googlecode.com/svn/trunk/mecab/doc/index.html(参照 2014-07-25).

[5] Microsoft,“パスワードチェッカー”, https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx（参照 2014-07-25)

[6] “John the Ripper password cracker”, http://www.openwall.com/john/（参照 2014-07-25)

表 9　語呂合わせ群（9 名）の作成フレーズ，パスワード，変換ルール

人/認証	フレーズ（上）/パスワード（中）/変換（下）
A/成功	いちごといったらとちおとめ
	15toT0chi
	いちご→15／といったら→to(短縮)／とちおとめ→Tochiotome→T0chi (短縮)(o/0)
B/失敗	空は青い
	s0r@.H1.b3r3-
	空→sora→s0r@ (o/0,a/@)／は→ha→H1 (「は」はハ行 1 段) ／青い→ブルー→buru-→b3r3-(「ブ」はバ行 3 段,「ル」はラ行 3 段)，単語を．で連結
C/成功	ポップなキャンディーカラー
	p0pnaC@ndycol0r
	pop→p0p (o/0)／candy→C@ndy (a/@)／color→col0r (o/0)
D/成功(2)	白鳥の湖
	T@np0p0mizu-mi
	白鳥→同名の女性お笑い芸人のコンビ名がたんぽぽ→Tanpopo→T@np0p0 (a/@, o/0)／湖→mizu-mi
E/成功	ライブに行きたい
	Con2ikit@i
	ライブ→コンサート→Con(短縮)／に行きたい→niikitai→Con2ikit@i (ni/2，a/@)
F/成功(2)	冬はこたつ
	w1nter1sk0t@tu
	冬→winter→w1nter (i/1)／は→is→1s (i/1)／こたつ→kotatu→k0t@tu (o/0，a/@)
G/成功	艦隊これくしょん
	k@ntco11ecti0n
	艦隊→kant (短縮)→k@nt (a/@)／これくしょん→collection→co11ecti0n (l/1, o/0)
H/成功	レジにて半額
	Rej1_2te_1/2g@ku
	レジ→Rej1 (i/1)／にて→nite→2te (ni/2)／半額→1/2g@ku (a/@)，単語を_で連結
I/失敗	ジンギスカンが好き
	JGKg@suk1
	ジンギスカン→jingisukan→jgk(頭文字短縮)→JGK／が→ga→g@ (a/@)／好き→suki→suk1 (i/1)

表 10　提案システム群（9 名）の選択特徴語，パスワード，変換ルール

人/認証	選択特徴語（上）/パスワード（中）/変換（下）
A/成功	中村／美しい
	beautiyNAKAMURA
	中村→nakamura→NAKAMURA／美しい→beautiful→beautiy
B/成功(2)	流れる／つく／おいしい／ずさん／ばっちい／課題
	yupi29o14zu381kdeye
	流れる→yupias(プールの名前)→yupi(短縮)／つく→tuku→29（tu/2，ku/9)／おいしい→oishii→o14（i/1，shii/4)／ずさん→zusan→zu3（san/3)／ばっちい→batii→81(ba/8，tii/1)／課題→kadai→kdeye (母音省略) (ai/eye)
C/成功	カイ／モモンガ／ムササビ
	K41M0M0nms4
	カイ→kai→k41(a/4，i/1)／モモンガ→Momonga→M0M0n（短縮）(o/0)／ムササビ→Musasabi→ms4(母音省略，短縮)
D/失敗	カルシウム／走る
	RnRnka12uka12u
	カルシウム→Karusiumu→Ka12uka12u（r/12）(繰り返し，短縮)／走る→Run→RnRn(省略，繰り返し)，語順の入れ替え
E/成功	チェック／度胸／切ない
	ChEMant01SetsU
	チェック→Check→ChE（短縮)／度胸→mantol→Mant01（o/0，l/1)／切ない→setunai→SetsU (短縮)
F/成功	京都／パンツ／やわらかい
	|<yo10@1¥1s0fty
	京都→Kyoto→|<yo（k/|<）(省略)／パンツ→pantsu→10@1¥1（p/10，n/1¥1)／やわらかい→Soft→S0fty (o/0)
G/成功	岩手／吹雪く／辛い
	Iw@teyu|<12ra1
	岩手→Iwate→Iw@te (a→@)／吹雪く→hubuku→yu|<1(吹雪く→雪) (k/|<)／辛い→turai→2ra1 (tu/2，i/1)
H/成功(2)	ネギ／みそ／ける
	Neg!mi50kerU
	ネギ→negi→Neg! (i/!)／ミソ→miso→mi50 (s/5 o/0)／ける→keru→kerU
I/成功	iPad／とぐ／おいしい
	1PaD|-ogU0ishiI
	iPad→1PaD (i/1)／とぐ→togu→|-ogU (t/|-)／おいしい→oishii→OishiI