個人情報のアナグラム化による質問解答型個人認証手法の提案

磯部智史† 鈴木優† 川越恭二†
†立命館大学 情報理工学部

1 はじめに

Webサービスの多様化に伴い，個人認証を必要とするWebサイトが増加している．現在の主な個人認証は，アカウント名とパスワードを入力する手法である．しかし，この個人認証手法では，利用者がパスワードを正確に記憶する必要があるため，利便性は低い．そこで，利用者が容易に記憶でき，他人に推測の困難なパスワードの生成が必要である．そして，これらを考慮した研究として，複数の画像から利用者がパスワードとして設定した画像を選択する画像選択型認証が注目されている．

画像選択型認証手法であるあわせ絵[1]では，利用者が撮影した写真をパスワードとして設定することにより，利用者の記憶量を削減している．しかし，選択肢として提示される画像群と利用者の撮影した写真では，写真に利用者の趣味・嗜好が反映されるため，利用者の知人からなりすまされる可能性がある．一方，画像選択型認証手法のDeja Vu [2]では，数式によって求められた抽象画をパスワードとして設定することにより，他人によるなりすましが困難になる．しかし，抽象画はパスワードとして記憶することが困難なため，利用者は抽象画を正確に記憶する必要があり，利用者の記憶量が増加する．つまり，利用者の記憶することが容易な画像は他人になりすまされる可能性があり，他人になりすましの困難な画像は利用者にとって記憶することが困難なため，画像自体の使用が問題であると考える．

そこで，他人が推測困難で利用者の記憶負担を抑えるパスワードを生成するために，本研究ではアナグラム化された個人情報をパスワードとして利用する認証手法を提案する．アナグラムとは，文字列を別の文字列に変換することであり，それにより利用者以外はパスワードを解読することが困難となる．また個人情報とは，利用者が既に記憶している情報であるため，利用者の記憶量を抑えることができる．

Proposal of Inquiry Answer Personal Authentication Technique Using Anagrams of Personal Information
Satoshi ISOBE†,Yu SUZUKI†and Kyoji KAWAGOE†
†College of Information Science and Engineering,Ritsumeikan University.
†{isobe,suzuki,kawagoe}@coms.ics.ritsumei.ac.jp

2 個人情報のアナグラム化による選択型個人認証

2.1 個人情報とアナグラム

提案手法では，アナグラム化された個人情報を利用することにより，他人が推測困難で利用者の記憶負担を抑えたパスワードを生成する．

個人情報とは，利用者自身の既に記憶されている情報である．このことにより，個人情報をパスワード生成に適用した場合新たに文字列を記憶する必要がないため，利用者の記憶量を抑えることができると考えられる．しかし，個人情報を利用するだけでは利用者の知人が利用者の個人情報を知っている場合が多く，なりすまされる可能性が非常に高い．そこで，ある文字列を別の文字列に変換するアナグラムを使用する．このことにより，認証の際に使用される個人情報がアナグラム文になっているため，利用者以外の認識が困難となる．

2.2 アナグラムルール

文字列を別の文字列に変換することを目的に，任意の数だけアナグラムルールを設定する．アナグラムルール設定の条件として，元の文字列が他人にとって推測困難である必要がある．提案手法では，六つのアナグラムルールを用い，そのルールを表1に示す．なお，並び替えは，文字の位置をランダムに入れ替える．また，携帯電話ボタン変換は，“abc” は2，“def” は3のように携帯電話の数字ボタンに表記されているアルファベットと数字を対応させて変換する．文字の組合せは，パスワードに適用する文字列の後ろにシステムが自動で単語をつなげる．

表 1: アナグラムルール

ルール	適用例 (ritsumeikan)
子音のみ	rtsmkn
逆読み	nakiemustir
並び替え	smeknriitua
母音を乱数	r9ts3m29k7n
携帯電話ボタン変換	74878634526
文字組合せ	ritsumeikanoita

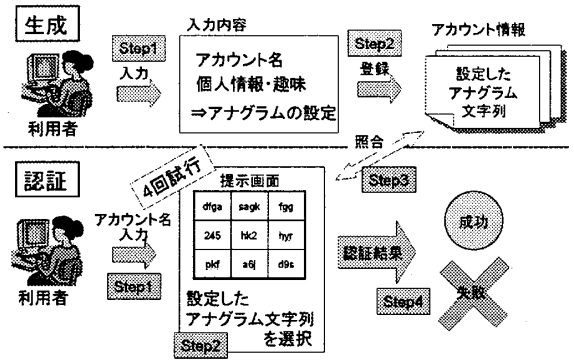

図 1: 手法概要図

2.3 提案手法の概要

本提案手法は，パスワード生成部と認証部により構成され，以下に詳細を示す．また，提案手法による概要図を図 1 に示す．なお本提案手法は，画像パスワードとの比較を行うため，あわせ絵と同じ値を使用している．そのため，パスワード生成数は 4 個，認証回数は 4 回，選択肢の提示数は 10 個必要になる．

2.3.1 パスワード生成部

パスワード生成部では，個人情報や趣味をアナグラムルールに適用することにより，アナグラム化されたパスワードを生成する．まず，利用者は利用者自身の出身地や生年月日などの個人情報と，好きな食事やスポーツなどの趣味を設定する．次に，パスワードを 4 個生成するため，複数設定した個人情報・趣味の中から四つの項目を利用者は任意に選択する．そして，利用者は選択した四つの項目に六つのアナグラムルールの中から一つを任意に適用する．これにより，4 個のアナグラム化されたパスワードが生成される．このとき，アナグラムルールの適用数を二つ以上にすると，個人情報ごとにどのアナグラムを適用したかという点を記憶する必要がある．このことにより，利用者の記憶負担を増加させてしまうため，本研究ではアナグラムルールの適用数を一つに限定する．

2.3.2 認証部

認証部では，利用者の生成したアナグラムパスワードに加え，システムが自動生成した 8 個のアナグラム文字列および，解なしの 10 個から，利用者に正解を選択させる．またシステムは，利用者の行う選択作業が 4 回全て正解した場合，利用者本人と認識する．まず，利用者は 9 個のアナグラム文字列と解なしの 10 個の選択肢から利用者自身が生成したアナグラムパスワードを選択する．このとき，提示された選択肢の中に利用者自身の設定したアナグラムパスワードが含まれていない場合，利用者の正解は解なしとなる．解なしを含める理由は，認証を複数回連続で行った場合，選択肢に提示されるアナグラム文字列の出現頻度によりパスワードを認識させないためである．そして，1 回目の選択の正解・不正解に関わらず，利用者は 1 回目から 4 回目までの選択作業を連続して行う．次に，利用者の選択したアナグラム文字列，もしくは解なしが正解であるかをシステムが判断する．最後に，利用者の 4 回の選択結果が正解していた場合，システムは利用者本人であると認識する．

3 おわりに

本研究では，個人情報や趣味をアナグラムルールに適用した文字列をパスワードとし，提示された選択肢の中から正解を選択する個人認証手法を提案した．提案手法により，画像の種類による記憶の困難さとなりすましの可能性を解消し，利用者にとって記憶することが容易で，他人になりすましの困難なパスワードを生成する．今後は，個人情報のアナグラムによる個人認証と写真や抽象画を使用した個人認証の評価実験を行い，本人認証率となりすまし率により，本手法の有効性を示すことを考える．

参考文献

[1] 高田哲司: "セキュリティとユーザビリティ特集 個人認証におけるセキュリティとユーザビリティ", ヒューマンインターフェース学会，Vol.9 No.1, pp. 5-10, (2007)

[2] R.Dhamija, A.Perring: "Deja Vu:A User Study Using Images for Authentication", Proceeding of the 9th USENIX Security Symposium, (2005) http://www.ischool.berkeley.edu/ rachna/dejavu/