4ZB-08

視線入力装置を用いた画像注視認証方式の提案

上平　大輝†　　小木　嘉原‡　　岡本　学†
神奈川工科大学大学院　情報工学専攻†
神奈川工科大学　情報メディア学科‡

１．　あらまし

情報通信機器の利用にあたっては本人確認を行う認証行為として「簡単な認証」を用いる場合がある．例えばスマートフォンのロック解除方式として，四桁の PIN 番号の入力や，指先で点を結んで描くパターン認証等がある.これら簡易な認証はブルートフォースアタックに弱い等，セキュリティ的課題は当然あるが，運用性・利便性が高い点に特徴をもつ．しかし四肢の不自由な肢体不自由者においては，たとえ簡単な認証においても実行が難しい．そこで視線入力装置を用いて，画像の特定の一点を見つめることで認証を行う画像注視認証方式の提案を行う．

２．　簡単な認証と肢体不自由者の利用課題

以下で述べる認証とはサービス提供側が本人確認を行う方法を指す．ネットワークを利用したサービスの多くでは認証手段としてパスワード方式を採用している．パスワード方式は知識認証とも呼ばれ，事前登録した文字列を入力するだけで本人確認を行う簡単な方式である．しかし忘却したり推測されたりする点が課題である．そこで指紋認証等の生体認証の利用が増えつつある．

生体認証は本人以外の第三者が利用できる可能性が極めて低い「強い認証」である．この方式では安全性が高いが，その点運用性に課題が出る場合がある．例えば代理人が認証を突破して利用することが不可能になる．しかしある種の認証の「ゆるさ」も重要要素であり，例えば認証用の IC カードを社内に忘れて社外に出てしまった社員は本来，入室カードチェックを突破して仕事に戻ることができなくなってしまうが，実際の運用上は誰か他の社員が開けてくれたドアに続いて入ることで入室することができる．セキュリティ的には問題のある行為だが，運用上は設置された監視カメラ撮影を用いて事件発生時には追跡が可能なため，このような「ゆるい運用」が事実上許されている場合が多い．

スマートフォン利用のためのロック解除認証も同様で，指紋認証等の「強い認証」をかけることも可能な一方で，緊急時に誰か他人に操作してもらうことを考え「ゆるい」認証にしておくことも可能である．「ゆるい認証」とはセキュリティ的に安全性が高いとはいえないが，運用性の高い認証方式をそう呼ぶものとする．例えば四桁の PIN 番号入力やパターン認証等がこれにあたるが，これら方式はブルートフォースアタックにも弱い単純な認証方式であるが，いざというときこれら秘密情報を第三者に暴露して代理で利用してもらうことも可能である．

つまり「ゆるい認証」も認証手段としては重要な一要素をなす．しかしここで四肢の随意運動が難しい「肢体不自由者」の利用について考えてみる．そもそも彼らはパスワードを打つことも難しく，指が欠損していれば指紋認証も不可能である．さらに健常者にとっては簡単な「ゆるい認証」ですら操作が難しい場合が多い．

そこで本論文では「肢体不自由者」にも利用可能な「ゆるい認証」の一方式として，「画像注視認証」を提案する．この方式は健常者・肢体不自由者の両者共有に利用できる簡単な認証方式で，入力に視線入力機器を用い，画像の特定の一点を注視することで認証を行う方式である．ブルートフォースアタックが可能であるので安全性が高い方式とはいえないが，「ゆるい」運用が可能であり，例えば緊急時には秘密情報を教えることで誰でも突破が可能な方式である．大多数で共有できる秘密情報として利用でき，問題発生時には秘密情報（注視位置）を簡易に変更できる点にも特徴をもつ．

３．　先行研究

簡易認証とその課題については[1]等の研究があるが，肢体不自由者向けの簡易認証の研究はまだ途上である．肢体不自由者向け認証方式としてはパスワード方式の提案[2]があり，視線入力による認証については[3]等の研究がある．

４．　提案方式

本方式では入力インタフェース装置として Tobii Eye Tracker [4] を用いる． PC の前に座

Proposal of Image Gaze Authentication using eye tracking device.
†‡ Kanagawa Institute of Technology

った操作者の視線動作を感知することができる装置で，図1に実施イメージ図を示す．

操作者として四肢が不自由な肢体不自由者を想定し，提示された画像の一点を注視することで個人認証を行う方式を提案する．なお以下の設定にてプロトタイプの開発を行った．

・画像サイズ：　1477 × 1108（図2）
・注視秒数：5秒
・注視許容：縦横±10 ピクセル
・正当許容：縦横±20 ピクセル

図1. 入力イメージ図

図2. 提示画像例
（黒いぬいぐるみの右目が注視ポイント）

5． 実験

以下の条件にて検証実験を実施した．

・ 被験者は本学学部生4名とする．肢体不自由者ではなく健常者である．
・ 今回は「共有秘密情報共有」としての「ゆるい認証」を想定し，画像の注視ポイントは全員共通の特定点とした．
・ 認証時間は画像が表示されてから注視点入力が完了するまでの時間を取得する．注視せず視線を泳がせている限り認証判定に入らない仕様である．
・ 30 秒を制限時間とし、時間が経過すると認証失敗とする．
・ 被験者1人につき3回の認証行為を実験する．
・ 被験者には事前に講習を行い，情報を収集しない練習を1回程度実施するものとする．

入力時間及び認証成功率について以下表に示す．

表1. 認証時間（秒）
Authentication Time(second)

	1st	2nd	3rd	Avg of Total
A	24	6	8	12.7
B	16	5	6	9
C	21	15	7	14.3
D	11	14	5	10

表2. 認証成功率(%)　（○が成功を示す）
Success Rate(%)(○ means Success)

	1st	2nd	3rd	Avg of Total
A	○	○	○	100
B	○	○	○	100
C	○	○	○	100
D	○	○	○	100

加えて簡単なアタック試験を実施した．

・ 画像注視位置を知らない被験者4名にて各3回実施する
・ 被験者は毎回，正当な認証者が成功する様子を観察後，推測した画像位置を注視

これらアタック試験を実施した結果，12 回の試験中，成功は 1 回であった．アタック成功してしまった要因を今後検討する必要がある．

6． 今後の課題

今後様々な画像による長期検証及び動画の利用，アタック対抗，ドアロック開錠等 PC 以外での利用の検討が必要である．

謝辞

本研究は JSPS 科研費 JP17K00194 の助成を受けて実施された研究である．

参考文献

[1] E. V. Zezschwitz, P. Dunphy, A. D. Luca, ”Patterns in the Wild:A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices”, Mobile HCI2013, pp. 261-270, 2013.
[2] 岡本学，“肢体不自由者向けパスワード入力方式の研究”，電子情報通信学会論文誌(D), Vol. J101-D, No. 02 ， pp. 386-394， 2018.
[3] 向井寛人，小川剛史，”個人認証を目的とした視線の軌跡情からの特徴抽出”，情報処理学会論文誌(デジタルコンテンツ)，Vol. 4, No. 2, pp. 27-35, 2016.
[4] Tobii Eye Tracker, https://www.tobiipro.com, 参照 Nov. 2018.