# 7 常時ユーザ認証

## ―視線誘導型なりすまし検知に関する研究―

西垣正勝 （静岡大学創造科学技術大学院） 高田愛美 （静岡大学大学院情報学研究科）

ユーザ認証とは，本来，単なるサービス利用開始時の「不正アクセス検知」として実施されるものではなく，ユーザがサービスを利用している全期間中の「なりすまし検知」として機能するべきものである．ログイン後も継続的に正規ユーザであることを検証する方法としては，キーボード操作における本人性を利用するものなどが提案されているが，人間の動作は基本的に曖昧であり，その認証精度の限界が指摘されている．筆者らは，常時ユーザ認証の実現にはユーザの表層的な挙動特徴だけではなく，心理的な側面を考慮した挙動特徴を捉えていくことが肝要と考えている．本稿では，その一例として，ユーザの興味対象に対する視線の動き（眼球運動）に着目したなりすまし検知に関する研究を紹介する．

## 既存の常時ユーザ認証技術

ユーザ認証技術とは，事前に登録された情報を用いて本人であることを確認する技術である．ユーザ認証技術は，(1) 本人の知識による認証，(2) 本人の所有物による認証，(3) 本人の身体的特徴による認証の 3 つに大別される．しかし，従来のユーザ認証技術のほとんどは，ユーザがシステムまたはサービスへログインするその一時点のみにおいて正規ユーザ本人であることを確認しているに過ぎない．セキュリティの観点からは，本人認証とは単なるサービス利用開始時の「不正アクセス検知」に限るものではなく，ユーザがサービスを利用している全期間中の「なりすまし検知」として機能するべきものである．

ログイン後もユーザに認証行為（パスワードの入力，認証トークンの提示，生体情報のスキャン）を定期的に繰り返し要求すれば，サービス利用中の継続的ななりすまし検知は可能である．しかし，ログイン時に 1 回の認証行為が求められるだけでも，それを不便に思うユーザは少なくない．よって，常時認証の実装においては，利便性の確保が特に肝要である．すなわち，ユーザに能動的な認証行為を求めることのない，何らかの「サービス利用中に定常的に観測されるユーザの特徴」を利用する必要がある．この条件を満たすユーザの特徴は実は非常に限られており，既存研究においては，ユーザのキーストローク [1), 2)] またはマウス操作 [3)] を利用するものが主であった☆1．

キーストロークやマウス操作を利用した常時認証は，キーボード，マウスなどの入力デバイスから取得した正規ユーザ特有の操作パターンをテンプレートとして学習，記憶しておき，サービスを利用しているユーザの入力デバイスの操作パターンがテンプレート（正規ユーザの操作パターン）に一致するかどうかを常に検証し続ける方法である．キーストロークやマウス操作に含まれる個人のくせは指紋などの静的な生体情報と比較して他人が真似（偽造）することは難しいため，常時認証への適性に加え，テンプレートが漏洩してもある一定のなりすまし耐性が期待されるという特長も有する．しかし，同一ユーザであってもキーボードやマウスの操作パターンは常に一定ではなく，特に使用しているアプリケーションによって（たとえば，ブラウザを利用している場合とワープロを利用している場合とで）大きく異なる．このため，正規ユーザ本人であっても使用時の操作パターンがテンプレートと一致しにくく，認証の本人拒否率を下げようとすると他人受入率が増加することになる．また，ユーザの習熟度（たとえば，キーボード操作に習熟しているか否か）等によって認証精度が左右されるという問題も存在する．さらに，ユーザがその入力デバイスを利用している間しかなりすまし検知を行うことができない．

このように，ユーザの動作を単純に利用するだけでは常時認証の実現は難しい．よって筆者らは，ユーザの表層的な挙動特徴に加え，心理的な側面を考慮した挙動特徴を捉えていくことが肝要と考えている．本稿では，その取り組みの一例として，ユーザの興味対象に対する視線の動き（眼球運動）に着目した常時認証の研究を紹介する．

☆1 最近では，ユーザの脳波を用いた常時認証方式などの研究も報告され始めている [4)]．しかし，認証精度などの観点からこれらの方式はまだ開発途上の技術であることから，本文では取り上げていない．

## 視線の動きと興味

視線の動きと興味には（意識のレベルに差はあるが）相関があるといわれており，さまざまな研究がなされている[5), 6)]．文献5）によると，注視対象物に対して，「普通，人は興味を持つと，一点を注視した後，周りを見て，それから再び興味のある一点に戻り，注視する」という挙動が現れる．また，対象物に「あまり興味がなければ，すぐに別の点に移動し，視線が戻ることはない」ということが報告されている．これは，人間の視線は，注視する対象への興味の有無によって，その挙動に差が出ることを示唆している．

そこで今回は，正規ユーザが興味を引く視覚刺激に対する被認証者の視線の挙動（眼球運動）を利用して，常時認証を行う方式を検討していく．具体的には，ユーザがPC上で任意のアプリケーションソフトを利用して何らかの作業をしている最中に，ディスプレイの非作業領域（表示領域内の外周付近等，ユーザの作業の妨げにならない場所）に，正規ユーザにとって非常にアトラクティブな画像を複数の囮画像といっしょに表示する．正規ユーザであれば，興味をそそられる画像（通常の画像認証におけるパス画像に相当する画像）にちらちらと目が行くことが予想される☆2ため，ユーザの視線を常時検出し，当該画像に対する注視頻度が判定閾値よりも大きいかどうかを常に検査し続けることにより，継続的ななりすまし検知が可能であると考えられる．本方式は，ディスプレイの非作業領域に正規ジョブとは別に表示される独立な視覚刺激を利用しているため，ユーザが利用するアプリケーションやデバイスの種類，習熟度による影響も受けにくいと予想される．

## ユーザの興味を引く視覚刺激の選定

人間の顔に対する認知能力の高さはよく知られ，研究されている[7)]．人間が生活の中で最も多くの時間を費やすのはコミュニケーションであると言われており，それゆえに，対面的なコミュニケーションを行う上で必須となる「顔の認知」の能力が発達しているのだと言われている．　また，人間には恋愛感情や親愛感情があり，コミュニケーションの相手が誰であるかによって，興味の度合いが大きく変わるだろうと考えられる．そして，その興味の対象（誰のことが好きか）は個人ごとに有意な差がある．たとえば，自分の顔とまったく知らない第三者の顔を比較した場合や肉親の顔と遠縁の顔を比較した場合，自分にとっての興味の強さ（関心の度合い）は，自分に身近な人間であるほど高いのではないだろうか．

そこで本研究の現時点では，ユーザの興味を引く視覚刺激として人間の顔画像を用いることとした．今回は，「友人や親類の顔は，自分とのかかわり合いの強弱によって，自分がその顔にどれくらい興味が引かれるかが変わってくる」という仮説をたて，これに基づいてシステムを構築する．また，人間同士のかかわり合いの強弱を測る絶対的な尺度がないため，「自分自身」と「赤の他人」の2つを対象として用いることとした．このため今回は，被認証者自身の顔画像を視覚刺激として採用し，被認証者がまったく知らない第三者の顔画像を囮画像として用いる．本方式は視覚刺激に対する興味の個人差によってなりすましを検知するものであるため，正規ユーザの興味の対象が不正者に漏洩した場合には，不正者のなりすましを許すことになる．よって，本来であれば，正規ユーザ自身の顔画像を用いることは適切ではない．今回は，提案方式の実現可能性を評価することが第一義であるため，あえて本人の顔画像を利用して実験を行うこととする．

## 視覚刺激に対するユーザの興味を持続させる仕組み

本研究の目的は，ユーザがシステムまたはサービスを利用している間，常に本人認証を継続することにある．すなわち，ユーザが定常的に視覚刺激を注視し続けるという状況を用意しなければならない．しかし，正規ユーザにとって非常にアトラクティブな興味対象を視覚刺激として採用したとしても，その刺激が同じ形で常にディスプレイに表示されていた場合には，通常，時間とともにその刺激に対する興味は薄れていってしまう．よって，何らかの方法でユーザの視覚刺激に対する興味を常にリフレッシュし，ユーザの視線を誘引し続けるための工夫が必要となる．

今回は，視覚刺激である顔画像に何らかの変化を加えることによって，刺激に対する正規ユーザの興味を持続させる方法に着目した．具体的には，顔画像に対して落書きを書き加えていく．人間は根本的に利己的であるため，自分と他人が何らかの被害を被る場合，両者の被害

☆2 本研究の認証方式においては，「ユーザにとって興味のある画像」と「興味のない画像」が通常の画像認証のパス画像と囮画像に相当する．ここで，通常の画像認証では，囮画像の中に紛れている自分のパス画像を見つけよというタスクがユーザに課される．これに対し，本研究の認証方式においては，興味のある画像を注視し続けよという指示がユーザに与えられているわけではないということに注意されたい．ユーザは，興味のある画像（パス画像）を見るも興味のない画像（囮画像）を見るも自由である．しかし，それであっても，ユーザは自分のパス画像のほうが気になって，そちらにちらちらと目をやってしまうだろう．本方式は，この人間の心理的な側面から現れる挙動を利用して，本人認証を行うのである．

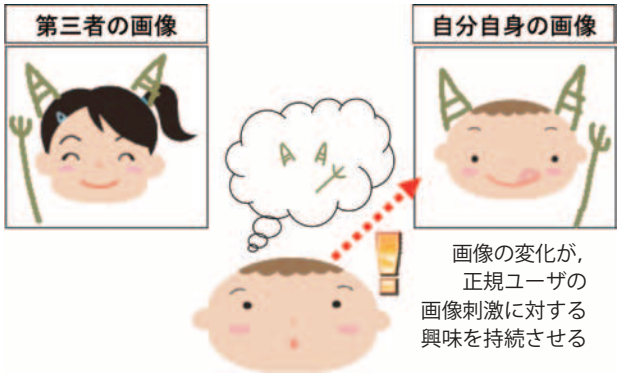


図 -1　画像変化による興味の持続と視線誘導

図 -2 使用画像例：無加工の画像（左上 1 枚）と落書きを加えた画像（①から⑩の順序で落書きが加えられていく）

が同程度のものであっても，自分が被った被害については敏感であるのに対し，他人が被る被害については鈍感であるというきらいがあるのではないだろうか．この仮定が真であるなら，自分自身の顔画像と第三者の顔画像に同時に落書きが加えられたとき，ユーザは第三者の顔画像に加えられた落書き（他人が被る被害）よりも自身の顔画像に加えられた落書き（自分が被る被害）が気になってしまうと考えられる（図 -1）．

なお，視覚刺激の画像変化が速すぎると，興味の強弱にかかわらず視線が誘引されてしまう可能性がある．逆に，画像変化がゆっくりすぎるとその変化に気づかない可能性がある．このため今回は，ユーザが興味を持つ刺激画像（ユーザ自身の顔画像）と囮画像（第三者の顔画像）のそれぞれに対して 10 種類の落書きを個別に用意し，どちらの画像にも 5 秒ごとに落書きを重ね書きしていく．画像変化の例を図 -2 に示す．常時認証をし続けるという本研究の本来の目的からは，画像を更新するなどの方法によって落書きが無数に繰り返されるようになっていないといけないが，今回の実験では 10 種類の落書きがすべて書かれるまでの視線の動きを計測することとする．また，視覚刺激の画像変化が大きすぎると，興味の強弱にかかわらず視線が誘引されてしまう可能性がある．このため今回は，画像の更新のたびに重ね書きされていく個々の落書きの大きさは顔画像の全面積の 1/5 程度以下とした．

## 基礎実験

ユーザ自身の顔と第三者の顔の変化（落書き）に対する興味の差によるユーザの視線の動きの違いに関して調査を行うため，基礎実験を行った．本研究の現段階では，なりすましに関する実験は行っていない．

今回の実験では，強膜反射法を利用した視線検出装置を使用した．刺激表示時の視線の動きが x 軸方向，y 軸方向に対応する電圧の時系列データとして取得される．被験者には，視線検出装置のセンサを右目側に装着したゴーグルを着用してもらい，視線の動きを測定した．また，今回使用した視線検出装置は，被験者の頭の動きによる影響を受けやすいため，アゴ台を用いて被験者の頭部を固定した（図 -3）．視線検出装置から得られたデータは，アナログ－デジタル変換機を通し，視線の x 座標，y 座標として PC に送信される．データの解析は PC 上で行った．実験で用いたディスプレイは 15 インチで，解像度は 1024 × 782 ピクセルである．

実験における画面構成を図 -4 に示す．今回は，ユーザが Web ブラウザを利用している（すなわち，被験者は

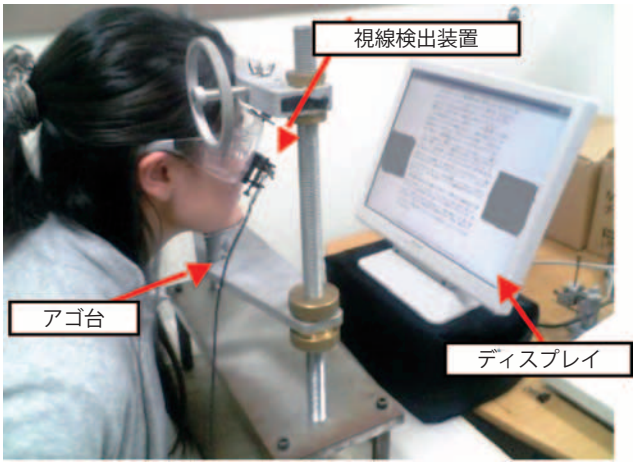


図 -3　実験風景

図 -4　実験画面

Web ページを閲覧するという作業をしている）シーンを想定している．画面中央に Web ページの文章が提示され，その左右に刺激画像が配置される．刺激画像は，右に被験者自身の顔画像，左に第三者の顔画像が表示される．顔画像のサイズは 220 × 220 ピクセルである．いずれの顔画像も，まず無加工の顔画像が表示されてから 5 秒後に加工画像①が表示され，さらに 5 秒ごとに加工画像②→③→④…の順に画像が更新されていく．文章は，ある物語の一部であり，無加工の顔画像が提示されると同時に画面中央に表示される．被験者には，実験中，この文章を黙読するという作業を行ってもらった．被験者本人の顔と他人の顔の無加工画像が表示されてから加工画像⑩が表示されるまでの間（計 55 秒）の被験者の視線を測定した．

被験者は，本学学生 2 名である．うち 1 名（被験者 B）は，視力が弱いせいで 1 回目の実験の途中まで自分の顔と他人の顔の区別ができていなかったため，2 回実験を実施している．また，実験後には，視覚刺激に対する興味などについてヒアリングを実施した．

強膜反射法を用いた視線検出では，瞬きをした際に取得値が不安定になる．このため，測定した視線データから瞬き時のデータを差し引き，実験データとした．実験データから，画像が変化するたびに被験者の視線が被験者自身／他人のどちらの画像の方に先に動いたかを調べ，まとめたものを表 -1 に示す．また，ヒアリングの結果，変化に気づかなかった画像があった場合には，表 -1 にその旨を記した．

表中，「先に注視した画像」の項の「自」「他」は，それぞれ，画像の更新時に視線が先に「被験者（自身）の顔画像」の方に動いたのか，「第三者（他人）の顔画像」の方に動いたのかを表している．どちらの画像にも視線が動かなかった場合は「×」と示した．「変化に気づかなかった画像」の項の「自」「他」は，それぞれ，画像の更新時に「被験者（自身）の顔画像」が変化したことに気づかなかったこと，「第三者（他人）の顔画像」が変化したことに気づかなかったことを表している．「－」は，両方の画像の変化に気づいた場合を示している．

| | | 表示画像 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ⑧ | ⑨ | ⑩ |
| 被験者 A | 先に注視した画像 | × | 他 | 自 | 自 | 自 | 自 | 自 | 自 | × | × |
| | 変化に気づかなかった画像 | － | 自 | － | － | － | － | 自 | 自 | 他 | 他 |
| 被験者 B | 先に注視した画像 | 自 | 自 | × | × | 自 | 自 | 他 | 自 | 自 | × |
| | 変化に気づかなかった画像 | － | － | － | 自 | － | － | 他 | 自 | 他 | 自 |

表 -1　実験結果

顔画像の変化の際に視線が自身の顔画像に向いた割合は，両方の画像の変化に気がついている場合に限定すると，被験者 A，B ともに 80% となった．また，第三者の顔画像の変化には気づかなくとも自身の顔画像の変化に気がついており，かつ，その際に自身の画像に先に目を向けてしまっている場合は，被験者 A は 57%，被験者 B は 71%であった．このことから，「興味の高い視覚刺激に対して，視線が誘引される」という傾向は確認できたと考えられる．

## 今後の展望

常時ユーザ認証の実現には，キーストロークやマウス操作などの表層的な挙動特徴のみを用いるだけでは不十分である．本稿では，ユーザの心理的な側面を考慮した挙動特徴による常時ユーザ認証の構築を目標に据え，ユーザの興味対象に対する視線の動き（眼球運動）に着目した継続的ななりすまし検知に関する研究を紹介した．

基礎実験においては，「ユーザにとって強い興味を有する視覚刺激（ユーザ自身の顔画像）」を「ユーザの興味を持続させる表示方法（ユーザ自身の顔に落書きをし続ける）」を用いて表示するという工夫を施すことによって，視線挙動に含まれるユーザ間の特徴の差を測定することができるという可能性が確認された．

今後は，まずは被験者を増やし，実験結果の確度を向上させる．そして，顔画像以外の任意の画像に対して，「正規ユーザのみが登録画像に誘引される」という状況をどのようにして作り出すかということを検討していく必要がある．これらを通じ，ユーザ心理を効果的に利用した常時認証方式を実現していきたい．

**参考文献**


1）Bleha, S., Slivinsky, C. and Hussein, B.：Computer-access Security Systems Using Keystroke Dynamics, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.PAMI-12, No,12, pp.1217-1222 (1990).
2）Monrose, F. and Rubin, A. D.：Keystroke Dynamics as a Biometric for Authentication, Future Generation Computer Systems, Vol.16, No.4, pp.351-359 (2000).
3）Pusara, M. and Brodley, C. E.：User Re-authentication via Mouse Movements, Proceedings of 2004 ACM Workshop on Visualization and Data Mining for Computer Security, pp.1-8 (2004).
4）Baba, S., Miyamoto, C. and Nakanishi, I.：Personal Authentication Using New Feature Vector of Brain Wave, Proceedings of 2008 International Technical Conference on Circuits/Systems, Computers and Communications, pp.673-676 (2008).
5）長沢伸也，森口健生：アイカメラによる視線から興味度を推定する可能性－眼球運動の専門家へのインタビューを通して－，Social Systems Studies 5, pp.73-93 (2002).
6）徳永智子，宮谷真人：顔ターゲットに対する視線注意効果，広島大学心理学研究：Hiroshima Psychological Research No.7 pp.35-42 (2008).
7）梅本堯夫：顔認知の生得的特異性，Human Developmental Research, Coder Annual Report 16, pp.99-104 (2001).


（平成 21 年 11 月 11 日受付）


西垣正勝（正会員）

nisigaki@inf.shizuoka.ac.jp

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．1999 年同講師，2001 年同助教授．2006 年より同創造科学技術大学院助教授．2007 年より准教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．

高田愛美

gs09032@s.inf.shizuoka.ac.jp

2009 年静岡大学情報学部情報科学科卒業．現在，同大学院情報学研究科 1 年．情報セキュリティに関する研究に従事．