

## 生体反射型認証

### 一輻輳反射と眼球形状を利用した認証方式の提案一

青山 真之<sup>1</sup> 西垣 正勝<sup>2</sup>

<sup>1</sup>静岡大学大学院情報学研究科 〒432-8011 静岡県浜松市中区城北 3-5-1

<sup>2</sup>静岡大学創造科学技術大学院 〒432-8011 静岡県浜松市中区城北 3-5-1

E-mail: <sup>2</sup>nisigaki@inf.shizuoka.ac.jp

あらまし 生体情報は一般的に容易に漏洩するという重大な問題が存在するため、生体情報が漏洩した場合であっても絶対になりすましができないような生体情報が強く望まれる。著者らはすでに、この問題を解決する一つの方式として生体の反射を利用した認証方式を提案している。生体反射は人間が自分で制御することが難しい生体情報であるため、これが不正者に知られたとしても、その不正者が本人を模倣することが困難であると考えられる。よって、生体反射を用いた認証方式はなりすましに対して高い耐性を有すると期待できる。本稿では、生体反射型認証のプロトタイプとして、人間の眼球形状と輻輳反射を用いた認証方式を提案する。また、実験により本認証方式の実現可能性を検討する。

キーワード ユーザ認証, 生体反射, 輻輳反射, 眼球形状, バイオメトリクス

## A Proposal of User Authentication using Convergence Reflex and Eyeball Shape

Naoyuki AOYAMA<sup>1</sup> Masakatsu NISHIGAKI<sup>2</sup>

<sup>1</sup>Graduate School of Informatics, Shizuoka University 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan

<sup>2</sup>Graduate School of Science and Technology, Shizuoka University 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan

E-mail: <sup>2</sup>nisigaki@inf.shizuoka.ac.jp

**Abstract** Biometrics information could be easily leaked and/or copied. Therefore, biometrics authentication in which biometric information is not required to be secret is desirable. We have proposed a user authentication using a human reflex response as a solution that would solve this problem. It is expected that even if people know somebody's reflex characteristics, it is difficult for anybody to impersonate the somebody, since nobody will basically not be able to control his/her own reflex. In this paper, we are studying a user authentication using convergence reflex and eyeball shape as a prototype system of reflex-response-based authentication. The availability of the proposed authentication system is evaluated through basic experiments.

**Keyword** User Authentication, Reflex, Convergence Reflex, Eyeball Shape, Biometrics

### 1. はじめに

生体認証は忘却や紛失の恐れがないため、非常に魅力的な本人認証技術であると言える。しかしながら、指紋や虹彩などの生体情報そのものが容易に漏洩するという重大な問題が存在する[1]。

この問題に対処するために、(1)漏洩しにくい生体情報や、(2)動的な生体情報を用いた生体認証技術が提案されている。(1)を利用した認証には、例えば指や掌の静脈を用いた認証などが実用化されている[2]。また、(2)を利用した認証には(手書きの)署名などがある[3]。しかし、(1)のような通常では漏洩しにくいと考えられる生体情報であっても、認証

装置から漏洩する(認証装置を攻撃してデータベースに登録されているユーザの生体情報を盗み出す)可能性が否定できない。また、壁などにスキャナを隠したり、フィッシングによって、ユーザの了承なしに不正に生体情報が盗られる恐れもある。一方、(2)のような動的な生体情報であっても、署名のように随意行動に基づくものである場合、不正者が訓練により正規ユーザの筆跡を習得するなどのなりすましが考えられ得る。

したがって、生体情報が漏洩しても複製ができず、また、訓練などにより習得することもできないようななりすましに対して高い耐性を有する生体認証が

必要である。特に、最重要機密にアクセスするような場合の本人認証においては、このような生体認証が強く望まれる。この要件を満たす可能性のある認証方式の一つとして、生体反射型認証[4][5]が挙げられる。生体反射は人間が自分で制御することのできない不随意的な生体情報であり、これが不正者に明らかになったとしても、不正者が本人になりすますことは難しいと期待される。

文献[4]の生体反射型認証では、サッカード反応と盲点位置を複合的に利用している。この方法では、視標を盲点内または盲点外に提示した際のサッカード反応の有無によって本人認証を行うため、ユーザーに「認証画面に提示される視標を目で追う」という能動的な認証タスクを要求することになる。つまりこの方法は、本人の意思により引き起こされるタイプの反射を利用した生体反射型認証となっており、「ユーザーの意思」という随意的な要素が介在する分、不正者が訓練などによってなりすましを成功させる可能性を否定できない。

この問題に対処するため、文献[5]では、本人の意思とは無関係に引き起こされるタイプの反射を利用した生体反射型認証が提案されている。この方法では、認証画面内に明るい小さな点を盲点内または盲点外に提示した際の対光反射による瞳孔の収縮反応の有無によって本人認証を行う。ただし、瞳孔反応を安定して捉える為に、暗室環境下で20分間程安静状態を保った上で認証を実施する必要があり、ユーザーの負担が大きいという問題がある。

そこで本稿では、本人の意思とは無関係に引き起こされ、かつ、測定におけるユーザーの負担が少ない生体反射を用いた認証方式の実現を目指す。本稿が目指したのは、物体の注視の際に起こる輻輳反射である。人は注視目標を無意識かつ自動的に両目で追う。その際の両眼の方位調節反応が輻輳反射である。本方式は、ユーザーが認証画面内の注視目標を注視した際に、注視目標と両眼の注視点の一致の有無を確認することによって認証を行う。ユーザーに要求されるのは、認証中、認証画面内の注視目標を注視することだけである。輻輳反射は本人が無意識の内に起こる。このように、ユーザーが無意識の内に起こる反射を利用することで、不正者の訓練によるなりすましを防ぐことができると思われる。また、注視点検出装置を用いたユーザーの注視点の検出は自然光下で測定可能であるため、暗室での待機は不要であり、ユーザーの負担も軽減されると期待される。

## 2. 生体反射型認証

### 2.1 生体反射とその認証への応用

反射とは、外界の作用によって感覚器が刺激されたときに、筋肉が意識とは無関係に反応を起こすことであり、常に決まった形で、自動的かつ機械的に、そして瞬間的に現れる[6]。

生体反射は、その反応を本人が意識的に制御することは難しいと考えられている。このため、例えば「ユーザーAであれば、刺激Sに対して反応速度R m/sで瞳孔がQ%収縮する」という認証用情報が漏洩したとしても、A以外のユーザーがユーザーA特有の生体反射(刺激Sに対して反応速度R m/sで瞳孔がQ%収縮する)を模倣(訓練による習得を含む)することは容易ではない。すなわち、生体反射の個人差に基づく本人認証においては、基本的に認証情報を公開したとしても他人によるなりすましは困難なものとなる。

虹彩を用いた生体認証方式の中に、対光反射をユーザーの生体検知(liveness detection)のために使用しているものもある[7]。しかし、生体検知機能は、反射の有無により、生体情報が生きている人間から読み取られたものか否かを判断しているのに過ぎず、それがゆえになりすましの成功例が報告されている[8][9]。本稿では生体反射そのものの個人差を用いて認証を実施することによってさらに頑強な生体認証の実現を提案するものであり、既存の生体検知の概念とは一線を画する。

ただし残念ながら、著者らが調べた範囲においては、現時点のセンシング技術で計測可能な生体情報の中で、実用レベルで本人認証に使用できるほどの個人差を有する生体反射は発見されていない。そこで本稿の現段階では、個人差を有する生体情報(静的な生体情報)を巧みに利用することにより、生体反射(動的な生体情報)の個人差を間接的に引き出し、これを認証に利用する方法を採っている。文献[4][5]では、生体反射(サッカード反応[4]、対光反射[5])を誘発する刺激を提示する部分に眼球形状(盲点位置)の個人差が利用されている。本方式においては、生体反射(輻輳反射)を測定する部分に眼球形状の個人差を利用する。これらの場合、反射そのものの個人差を直接利用する理想的な方法に比べると不正者による模倣の可能性が残るものの、反射を単なる生体検知のために独立に用いる既存の生体認証と比較して、なりすまし耐性の向上が期待できる。

### 2.2 輻輳反射と眼球形状およびその認証への応用

人間の眼は、視野の中心部が最も解像度が高い。このため人間は、体、顔、眼球をコントロールして、

興味の対象を視野中心部で捉えようとする。本稿では、人間の視界の中で視野中心部が捉えている点を「注視点」と呼ぶことにする。また、人間は、目標物を視野中心部で捕捉するにあたり、左右2つの眼が1つの点を注視するように、両眼の向きを適切に調整している。この視機能は「輻輳反射」と呼ばれ、人間が遠近感を測るための仕組みの一つと考えられている[10]。

輻輳反射は、両眼の注視点をリアルタイムで計測し、両注視点の一致を検査することで確認可能である。ただし、輻輳反射は万人に起こる生体反射であり、本人認証に利用可能なほどの個人差を有していない。しかし、現在の一般の注視点検出技術においては、ユーザによる眼球の物理的な形状の差異や生理的な固体異差を補償するために、あらかじめユーザごとに注視点の校正（以降、キャリブレーション）が要求される[11]。すなわち、眼球の位置や向きから注視点を検出する過程においては個人差が大きく影響することが分かる。このため、ユーザAのキャリブレーションデータを用いてユーザBの注視点を検出しようとしても、両眼の注視点を正しく取得することができず、左眼と右眼の注視点はそれぞれ別の位置にあるものとして測定される。すなわち、他人のキャリブレーションデータを用いて注視点を検出した場合には、輻輳反射を確認することができない。

以上のように、輻輳反射そのものには有意な個人差が存在しないが、輻輳反射を測定する部分に、個人差を有する生体情報である眼球形状を適切に関与させることにより、生体反射型認証の一方式を実現することが可能である。本方式では、ユーザが注視目標を注視した際に、検出した両眼の注視点が共に注視目標と一致するかによって本人認証を行う。眼球形状の個人差が注視点の個人差として検出できるため、その差をもって本人と他人を識別できる。なお、人間の眼球形状は左右で少なからず異なるため、両眼の注視点を検出するためには、両眼それぞれのキャリブレーションが必要となることに注意されたい。ユーザAとユーザBの眼球形状（キャリブレーションデータ）が似ている場合には他人受入れが発生するが、本方式においては、どちらか一方の眼の形状が似ているだけでは誤認証は発生しない原理となっている。よって、片眼の形状の個人差のみを利用する文献[4][5]の方式と比べ、他人受入れの発生確率は低く、なりすましの困難性も向上していると考えられる。

### 3. 輻輳反射と眼球形状を利用した認証方式

#### 3.1 認証方式

輻輳反射と眼球形状を利用した認証は以下の手順によって行われる。

##### 【登録フェーズ】

- ① 認証装置は正規ユーザの両眼の注視点をリアルタイムで計測できるように、それぞれの眼に対して注視点検出用のキャリブレーションを行う。
- ② 認証装置は、①の両眼のキャリブレーションデータをユーザ名とともに登録する。

##### 【認証フェーズ】

- ① 被認証者は認証装置にユーザ名を入力する。
- ② 認証装置は、登録されている両眼のキャリブレーションデータを注視点検出装置にセットして、被認証者のそれぞれの眼の注視点計測を開始する。認証装置は、両眼の注視点を同時にリアルタイムで検出可能である。
- ③ 認証画面中の一点に注視目標が表示される。被験者は認証中、注視目標を注視するように指示される。なお、注視目標の表示位置（定点にするか/任意の点とするか）や表示回数などは、認証装置に要求されるセキュリティ強度によって決定される。
- ④ 認証装置は、検出した両眼の注視点位置を注視目標の提示位置の情報とともに記録する。
- ⑤ ③、④を必要な回数、繰り返す。

ユーザAが正規ユーザであれば、検出された両眼の注視点はどちらも注視目標と一致するはずである。これに対し、ユーザBがユーザAとして認証フェーズを実施した場合には、眼球形状（キャリブレーションデータ）の差異のため注視点を正しく取得することができず、検出された両眼の注視点は注視目標と一致しないであろう。したがって、右眼の注視点と注視目標の距離、左眼の注視点と注視目標の距離、右眼と左眼の注視点の距離を検査することで、正規ユーザAの認証が可能である。

#### 3.2 なりすまし耐性

ユーザBが能動的な不正者であった場合、正規ユーザAのキャリブレーションデータを盗んだ上でユーザAへのなりすましを試みるであろう。今、ユーザAとユーザBのキャリブレーションデータの差を左眼： $(\Delta X_L, \Delta Y_L)$ 、右眼： $(\Delta X_R, \Delta Y_R)$ とする。すなわち、ユーザBがユーザAのキャリブレーションデータを用いて注視目標 $(X, Y)$ を注視した場合、注視点検出装置においては、ユーザBの注視点は左眼： $(X + \Delta X_L, Y + \Delta Y_L)$ 、右眼： $(X + \Delta X_R, Y + \Delta Y_R)$ として検出される。

ユーザAのキャリブレーションデータを入手した

ユーザBは、自分とユーザAとのキャリブレーションデータの差が左眼： $(\Delta X_L, \Delta Y_L)$ 、右眼： $(\Delta X_R, \Delta Y_R)$ であることを知る。よってユーザBは、意図的に認証画面上の点 $(X - \Delta X_L, Y - \Delta Y_L)$ を注視すれば、認証装置（注視点検出装置）に自分の左眼が注視目標 $(X, Y)$ を見ていると思わせることができ、また、認証画面上の点 $(X - \Delta X_R, Y - \Delta Y_R)$ を注視すれば、自分の右眼が注視目標 $(X, Y)$ を見ていると思わせることができるということが分かる。しかし、ユーザB自身の輻射反射があるため、ユーザBが左眼と右眼でそれぞれ異なる点を注視することは不可能に近いと考えられる。

このように、本認証方式は、登録されている生体情報（キャリブレーションデータ）が漏洩したとしても、なりすましが困難であると予想される。

#### 4. 輻射反射と眼球形状を利用した認証システム

##### 4.1 システム構成

認証システムは、制御装置、注視点検出装置、アゴ台、表示ディスプレイから構成される。各装置の詳細を以下に示す。

- 制御装置：3.1節に示した登録フェーズ、認証フェーズの各ステップを実行する認証プログラムをC++言語により実装した。プログラムはPentium4 3GHz、1GB Memory、Windows XP ProfessionalのPCにて実行される。注視点検出装置から被認証者の注視点情報を受け取り、認証の判定を行う。
- 注視点検出装置：赤外線LEDを備えた2台の特殊CCDカメラ（テクノワークス社TE-9170）により、被験者の左右の眼球をそれぞれ撮影する。撮影画像から角膜反射点と瞳孔の中心部を求め、角膜反射法[12]により被験者の注視点を算出する。撮影画像のフレームレートは毎秒30コマである。
- アゴ台：実験環境を常に一定に保つため、被認証者の頭部を顎、額、左右側頭部の4点で固定する。アゴ台の設置位置は全被験者で共通で、同じ場所にアゴ（顔）が置かれるように座ってもらう。アゴ台に顔を乗せた状態で、CCDカメラの画像が被認証者の眼球を捉えるように、カメラの仰角を設置する。なお、アゴ台の場所が固定されているため、被験者の両眼は常におよそ同じ位置にくるが、今回はカメラの仰角の微調整については認証の都度、行うようにした。
- 表示ディスプレイ：制御装置の制御に従い、注視目標を提示する。制御装置の指示を被認証者

に伝えるインタフェースでもある。SAMSUNG 32型液晶カラーモニタ SyncMaster 323Tを使用した。解像度は1280×1024ピクセルとした。

##### 4.2 システム概観

システムを図1のように配置する。被認証者は認証フェーズおよび登録フェーズ実行時にはアゴ台に頭部を固定され、表示ディスプレイを両眼で見ることとなる。眼球の位置から表示ディスプレイまでの距離を1.2mとし、認証画面の使用領域の両端が視角で約16°となるように設置した。また、注視点検出装置は両眼の前方0.7mの距離に設置した。

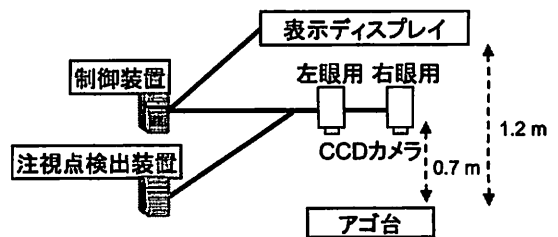


図1：システムの概観

##### 4.3 認証プログラム

本認証方式は、注視点検出装置が検出したユーザの両眼の注視点および注視目標の一致/不一致によって認証を行う。登録/認証画面を図2に示す。今回は9個の注視目標（図2の①～⑨）を提示することとした。画面は一面が黒色（RGBの輝度レベル(0,0,0)の色）であり、注視目標は白色（RGBの輝度レベル(255,255,255)の色）の円とした。被験者は登録/認証フェーズにおいて、①～⑨の順番で注視目標を注視するように指示される。それぞれの注視目標を注視してもらう時間は、およそ2秒である。登録フェーズにおけるキャリブレーション、および、認証フェーズにおける注視点検出は、2台のCCDカメラによって両眼に対して同時に実施される。

なお、CCDカメラによって撮影される画像（左眼）の例を図3に示した。図中のプルキニエ像とは、CCDカメラより赤外線光を照射した際の角膜表面における反射像のことである。角膜反射法は、角膜の曲率中心（プルキニエ像の位置）と瞳孔中心から視線ベクトルを算出する方法である[12]。

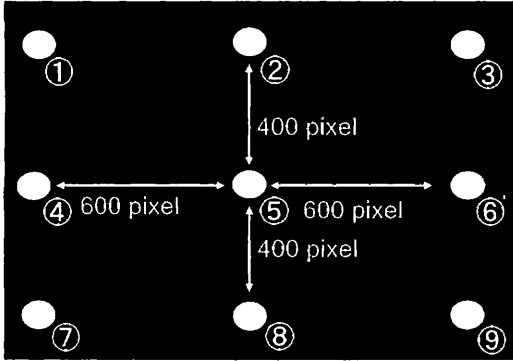


図 2：登録／認証画面

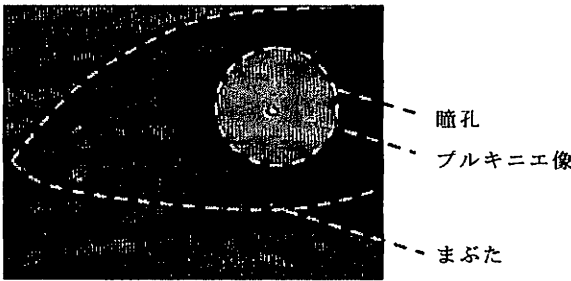


図 3：瞳孔とブルキニエ像（左眼）

## 5. 実験

本認証方式の実現の可能性を示すため、4 章にて実装した輻射反射と眼球形状を利用した認証システムを使用して、注視点検出における個人内・個人間の差に関して調査するための基礎実験を行った。被験者は健康な本学学生 4 名とした。本システムで使用している注視点検出装置は自然光下での注視点検出が可能であるが、今回はより鮮明な瞳孔画像を得るために暗室にて実験を行った<sup>1</sup>。各被験者には、実験初日に登録フェーズ（キャリブレーション）を実行してもらい、その 3 日後に認証フェーズを実施してもらった。なお、被験者には事前に本実験に関する説明を十分に行った。今回は裸眼での実験を実施した。

### 5.1 注視点の個人内および個人間の差

注視点の個人内の揺らぎ（注視点検出装置の測定誤差を含む）の大きさを測るために、各被験者に対し、初日に登録した本人のキャリブレーションデータを用いて 3 日後の認証フェーズを実施した際の、本システムにより測定された注視点の位置を調べた。

<sup>1</sup> 対光反射を用いる文献[5]の方法と異なり、本方式では暗室入出後、すぐに実験を開始して構わない。

また、注視点の個人間の差異を測るために、各被験者に対し、他人のキャリブレーションデータを用いて認証フェーズを実施した際の、本システムにより測定された注視点の位置についても同様に調べた。

各被験者が、被験者 A のキャリブレーションデータを用いて認証フェーズを実施した際の、図 2 の①の注視目標を注視した状況において、本認証システム（注視点検出装置）によって検出された注視点を図 4 に示す。図 4 においては、図 2 の①の注視目標の位置を原点として、各被験者が注視目標を注視している間の注視点位置の平均が記されている。

図 4 から、被験者 A 本人でさえ、認証フェーズの 3 日前に実施したキャリブレーションを用いた場合、注視点は完全に①の注視目標に一致していないことが分かる。これが注視における個人内の揺らぎ（注視点検出装置の測定誤差を含む）であると考えられる。しかし被験者 A の両眼の注視点は、他の被験者の注視点と比べ注視目標に近くなっていることから、個人内の揺らぎは個人間の差異よりも小さく、注視目標と注視点の距離を用いて本人と他人を切り分けることは可能であるだろうということが確認できる。これについては次節で検証を行う。

なお、全ての被験者のキャリブレーションデータ、および、①～⑨の全ての注視目標について図 4 に相当するデータを測定したところ、ほとんどの場合において同様の傾向が得られることが確認された。ただし、この結果は現時点においては、まだ万人に対して普遍的に保障されたものではないことを明記しておく。

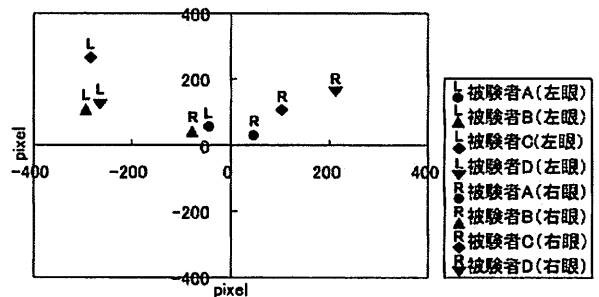


図 4：各被験者の注視点と注視目標の距離

### 5.2 本人認証に関する検証

本認証方式は注視点検出装置が検出したユーザの両眼の注視点および注視目標の一致／不一致によって認証を行う。ここで、本認証方式が機能するためには、注視点の個人間の差異が個人内の揺らぎと比べ有意であることが必要条件となる。これを確認するために、本人のキャリブレーションデータを用いて注視点を検出した場合と、他人のキャリブレーション

ョンデータを用いて注視点を検出した場合に対し、以下の(1)および(2)を評価した。

(1) 注視精度：GP( $\alpha, \beta, \gamma$ )

$\alpha$ のキャリブレーションデータを用い、被験者 $\beta$ が注視目標 $\gamma$ を注視した際の、「注視目標と検出された左眼の注視点の距離」と「注視目標と検出された右眼の注視点の距離」の和

(2) 輻輳反射精度：CP( $\alpha, \beta, \gamma$ )

$\alpha$ のキャリブレーションデータを用い、被験者 $\beta$ が注視目標 $\gamma$ を注視した際の、検出された左眼の注視点と右眼の注視点との距離

まず、各被験者に被験者自身のキャリブレーションデータを用いて①から⑨の注視目標を注視してもらった場合の注視精度 (GP( $i, i, k$ ):  $i=A\sim D, k=①\sim ⑨$ ) および輻輳反射精度 (CP( $i, i, k$ ):  $i=A\sim D, k=①\sim ⑨$ ) を算出し、その平均値、標準偏差、最小値、最大値を求めた。全被験者および全注視目標に対するGPおよびCPの各値の平均値を表1、表2に示す。続いて、各被験者に自分以外のキャリブレーションデータを用いて注視目標を注視してもらった場合に対しても同様の値 (GP( $i, j, k$ ), CP( $i, j, k$ ):  $i, j=A\sim D$ , ただし  $i \neq j, k=①\sim ⑨$ ) を算出し、その平均値、標準偏差、最小値、最大値を求めた。全被験者、全キャリブレーションデータおよび全注視目標に対する各値の平均値も表1、表2に併記する。

次に、各被験者 $i$  ( $i=A\sim D$ ) ごとに、本人のキャリブレーションデータを用いて注視点を検出した場合の注視精度 (GP( $i, i, k$ ):  $k=①\sim ⑨$ ) および輻輳反射精度 (CP( $i, i, k$ ):  $k=①\sim ⑨$ ) の最大値を閾値  $\theta_{GP}(i)$ ,  $\theta_{CP}(i)$  として設定し、 $i$ 以外の被験者 $j$ が $i$ のキャリブレーションデータを用いて注視点を検出した際に、注視精度または輻輳反射精度がこの閾値を越えた回数 (すなわち、 $i, j=A\sim D$ , ただし  $i \neq j, k=①\sim ⑨$  のそれぞれに対し、 $GP(i, j, k) > \theta_{GP}(i)$ ,  $CP(i, j, k) > \theta_{CP}(i)$  となった回数) を被験者ごとに求めた。結果を表3、表4に示す。表3、表4はそれぞれ注視精度および輻輳反射精度に関し、本人の揺らぎの中に他人が入ってくる回数を表す。

表1、表2から、注視精度GPおよび輻輳反射精度CPの本人の平均値、標準偏差、最大値は、他人に比べて十分に小さくなっていることが確認できる。また、表3、表4の結果から、①～⑨の全ての注視目標において注視精度および輻輳反射精度が本人の最大値以内に収まる (すなわち、 $i, j=A\sim D, k=①\sim ⑨$  のすべてに対し、 $GP(i, j, k) \leq \theta_{GP}(i)$ ,  $CP(i, j, k) \leq \theta_{CP}(i)$  を満たす) のは本人だけであることが分かる。この結果から、特定の注視目標においては「注視点」という生体情報に本人と他人の差が大きく現れない場合

もあるが、複数の注視目標における注視点検出の結果を総合して判断することによって、本人と他人を切り分けることができると考えられる。

表1：注視精度 GP の比較 (単位：pixel)

本人	平均	標準偏差	最大値	最小値
	116.6	28.0	155.5	80.7
他人	平均	標準偏差	最大値	最小値
	335.1	75.0	469.2	241.5

表2：輻輳反射精度 CP の比較 (単位：pixel)

本人	平均	標準偏差	最大値	最小値
	84.1	21.0	117.2	49.7
他人	平均	標準偏差	最大値	最小値
	234.3	55.8	327.0	153.7

表3：本人の揺らぎの中に他人が入ってくる回数 (注視精度 GP)

		キャリブレーションデータ			
		A	B	C	D
被験者	A	0	0	0	0
	B	0	3	0	0
	C	0	0	0	0
	D	0	0	0	0

表4：本人の揺らぎの中に他人が入ってくる回数 (輻輳反射精度 CP)

		キャリブレーションデータ			
		A	B	C	D
被験者	A	0	0	0	0
	B	0	2	0	0
	C	0	0	0	0
	D	0	0	0	0

6. まとめ

生体情報そのものが漏洩しやすいという生体認証が抱える重大な問題を解決するために、生体の反射を利用した認証方式を提案した。生体反射は人間が自らの意思で制御することのできないため、生体情報が漏洩したとしても、不正者が本人になりすますことは困難である。本稿では、生体反射型認証のプロトタイプである輻輳反射と眼球形状を用いた認証システムを構築し、基礎実験から生体反射型認証の実現の可能性を示した。今後は、より多くの被験者における本人認証率と他人受入れ率の測定を行うとともに、なりすまし耐性についても検証を提案していきたい。

## 謝辞

本研究は一部、(財)セコム科学技術振興財団の研究助成を受けた。ここに謝意を表する。

## 文 献

- [1] 松本勉, 平林昌志, “虹彩照合技術の脆弱性評価(その2)”, コンピュータセキュリティシンポジウム(CSS2003)論文集, pp187-192(2003).
- [2] バイオメトリクスセキュリティコンソーシアム編集, “バイオメトリックセキュリティ・ハンドブック”, pp186-197, オーム社(2006).
- [3] 中西巧, 西口直登, 伊藤良生, 福井裕, “DWTによるサブバンド分解と適応信号処理を用いたオンライン署名照合”, 電子情報通信学会論文誌 A, Vol. J87-A, No. 6, pp. 805-815(2004).
- [4] 西垣正勝, 荒井大輔 “生体反射を利用した認証方式”, 情報処理学会論文誌, vol.47 no.8, pp. 2582-2592(2006).
- [5] 小澤雄司, 西垣正勝, “生体反射型認証: 対光反射と盲点位置を利用した認証方式(その3)” ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会, 研究発表会予稿集, pp. 19-26(2007).
- [6] 森宏一 編集: 哲学辞典, p. 385, 青木書店(2000).
- [7] 小田高広, “アイリスコード生成装置およびアイリス認識システム”, 特許第 3315648 号.
- [8] 松本勉, 平林昌志 “虹彩照合技術の脆弱性評価(その2)”, コンピュータセキュリティシンポジウム(CSS2003)論文集, pp. 187-192(2003).
- [9] 宇根正志, 松本勉, “生体認証システムにおける脆弱性について: 身体的特徴の偽造に関する脆弱性を中心に”, 金融研究, vol. 24, No. 2, pp. 35-84(2005).
- [10] Richard-L-Gregory 著, 近藤倫明・中濤幸夫・三浦佳世 訳: 脳と視覚 グレゴリー視覚心理学, p73, ブレーン社(2001).
- [11] 大野健彦, “視線インタフェースから視線コミュニケーションへ”, 情報研報 2001-HI-95, Vol. 2001, No. 087, pp. 171-178(2001).
- [12] 坂下祐輔, 藤吉弘亘, 平田豊: “画像処理による3次元眼球運動計測” JSEM 日本実験力学会特集号, Vol. 6, No. 3, p 26-33(2006).