社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (55)
2006／7／21

# 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2)

小澤 雄司[1] 荒井 大輔[1] 西垣 正勝[2]

[1]静岡大学大学院情報学研究科 〒432-8011 静岡県浜松市城北3-5-1
[2]静岡大学創造科学技術大学院 〒432-8011 静岡県浜松市城北3-5-1
E-mail: 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．本稿では，生体反射を使用した認証方式を提案する．生体反射は人間が自分で制御することができないため，不正者が他人を模倣することが困難であることから，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考えられる．すでに著者らは生体反射型認証のプロトタイプである人間の盲点位置と瞳孔の対光反射を用いた対光反射を用いた認証方式を提案している．本稿では，実際に認証システムを構築し，本人拒否率，他人受入率，なりすまし成功率を検証する．

キーワード ユーザ認証，生体反射，盲点，対光反射，バイオメトリクス

# A User Authentication using Blind Spot and Papillary Light Reflex (part2)

Yuji OZAWA[1] Daisuke ARAI[1] and Masakatsu NISHIGAKI[2]

[1]Graduate School of Informatics, Shizuoka University 3-5-1 Jyohoku, Hamamatsu, 432-8011 Japan
[2]Graduate School of Science and Technology, Shizuoka University 3-5-1 Jyohoku, Hamamatsu, 432-8011 Japan
E-mail: 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 able to control his/her own reflex. In a previous paper, we have shown a user authentication using blind spot and papillary light reflex as a prototype system of reflex-response-based authentication. Here this paper, its availability is studied.

**Keyword** User Authentication, Reflex, Blind spot, Papillary Light Reflex, 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絶対に複製ができず，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]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．そこで著者らは，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として，瞳孔の対光反射と盲点位置を用いた認証方式を提案している[5]．本方式は，認証画面内に明るい小さな点(以降，光刺激)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っている．そのため，認証システム側が光刺激を提示しさえすれば，本人の意思とは無関係に反射が引き起こされる．ユーザに要求されるのは，認証中，認証画面内のある定点を注視することだけである．このようにユーザに「受動的な認証タスク」を要求することで，不正者の訓練によるなりすましを防ぎ，同時にユーザの負担も軽減されることが期待される．

## 2. 生体反射型認証

### 2.1 生体反射とその応用

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以外のユーザがユーザ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．そこで本論文の現段階では，生体反射を誘発する刺激を提示する部分に個人差を有する生体情報を巧みに組み合わせることにより，反射の個人差を間接的に引き出し，これを認証に利用する．この場合，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される．

### 2.2 瞳孔の対光反射と盲点およびその認証への応用

瞳孔には，眼球に入る光が急に強さを増した際に縮瞳する対光反射が存在する[10]．瞳孔の収縮の程度には有意な個人差が存在することが確認されている[11]が，対光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．仮に瞳孔径の変化量に本人認証に使用できるほどの個人差あったとしても，対光反射による縮瞳反応はストレスなどの心的要因により変化する[12]ため，これを安定して捉えることはできない．

一方，人間の眼には網膜からの血管や神経束が眼球から脳へと出て行く場所が存在する．この部分は光を電気信号に変換する役割を担う視細胞が存在しないため視覚情報が欠落しており，盲点と呼ばれている．盲点によって，1m 離れた地点の映像を見た場合に直径10cm 程度の視野欠損が生じる[13][14]．両眼で見た場合は，一方の眼球の盲点部の視覚情報はもう一方の眼で補われるため，視野欠損は生じない．また，片眼視の際にも，脳の中で盲点部の視覚情報が周囲の映像によって補完されて知覚されるため，普段，人間は盲点の存在に気付くことはない．

眼球における盲点の位置は解剖学的に定点であるため，注視点(視野の中心)に対する盲点の相対位置を一度測定しておけば，注視点をリアルタイム計測することにより時々刻々の視野欠損領域を知ることができる．注視点と盲点の相対位置にはある程度の個人差が存在するが，認証に利用可能なほど有意な差ではない．しかし，現在の一般の注視点検出装置においては，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[15][16]．すなわち，眼球や瞳の位置や向きなどから注視点検出装置が注視点を検出する過程においては個人差が測定に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，注視点を正しく取

得することができない．したがって，注視点を検出することにより視野欠損領域を測定するにあたって，キャリブレーションデータの個人差を含めて考えた場合には，盲点位置には有意な個人差があるとみなしてよいと考えられる[4]．

個人差を有する生体情報である盲点位置を対光反射の誘発に用いることにより，生体反射型認証の一方式を実現することが可能である．すなわち，正規ユーザAの盲点内および盲点外に視標を表示し，その際に生じる対光反射(縮瞳)を計測することによってユーザ認証を行う．盲点位置に個人差が含まれるため，視標の表示位置と縮瞳量の関係にユーザ間で差が生じる．その差をもって本人と他人を識別できる．本方式においては，有意な個人差を有する盲点位置を「対光反射を誘発するトリガ」として利用し，盲点位置に起因する認証情報を「人間が自分の意思で制御することが困難である生体反射」に変換して観測することにより，なりすましが困難な認証を実現している．認証方式の詳細は次章にて述べる．

## 3. 対光反射と盲点位置を利用した認証方式

### 3.1 認証方式

対光反射と盲点位置を利用した認証は以下の手順によって行われる．なお，本人認証は盲点を利用するため，片眼で認証画面を見て認証を行う．

【登録フェーズ】

① 認証装置は正規ユーザの注視点をリアルタイムで計測できるように，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，正規ユーザの注視点に対する盲点位置(視野欠損領域)の相対位置を測定する．

③ 認証装置は，①の注視点検出用のキャリブレーションデータと②の相対盲点位置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，被認証者の注視点のリアルタイム計測を開始する．認証装置は，検出された注視点と登録されている相対盲点位置データから，被認証者の盲点位置をリアルタイムで補足することが可能である．

③ 認証画面には定点に注視目標が表示されており，被験者は認証中，注視目標を注視するように指示される．認証装置は，真暗(RGB の輝度レベル(0,0,0))な認証画面において，被認証者の盲点内もしくは盲点外に光刺激(RGB の輝度レベル(255,255,255))を提示する．

④ 認証装置は，被認証者の瞳孔径の変化を光刺激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，盲点外に光刺激が提示された場合，対光反射が起こる．一方，盲点内に提示された場合には対光反射は起こらない．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，盲点位置に個人差が含まれるため，次のような反応が得られる．

- ユーザAの盲点外かつユーザBの盲点内に光刺激が提示された場合:ユーザAならば対光反射が起こるはずであるのに，ユーザBは光刺激を感知できず，対光反射が起こらない．
- ユーザAの盲点内かつユーザBの盲点外に光刺激が提示された場合:ユーザAならば光刺激を感知できず対光反射が起こらないはずであるのに，ユーザBは対光反射が起こる．

正規ユーザAの盲点内をBa，盲点外を¬Ba，不正者Bの盲点内をBb，盲点外を¬Bbとした場合，光刺激の表示位置と反応の関係は表1のようになると考えられる．したがって，表1に示したような「反応の差」を考慮することで，正規ユーザAの認証が可能である．具体的には，ユーザAのキャリブレーションデータおよび相対盲点位置データを参照して光刺激を提示した際に，「刺激が盲点内に提示された場合には対光反射が起こらず，光刺激が盲点外に提示された場合には対光反射が起こる」という反応が高い確率で得られたならば，被認証者をユーザAとして認証する．

不正者Bが正規ユーザAの盲点位置を知り得たとしても，自分の盲点位置を変化させることは不可能であるため，なりすましは基本的に不可能である．例えばAの盲点に相当する領域のみを遮光したコンタクトレンズなどを作成し，Bがこれを装着したとしても，B自身の盲点を消すことは不可能であるため，正規ユーザAの盲点外かつ不正者B自身の盲点内に光刺激が提示された場合に，Bの対光反射が起こらず，なりすましが発覚する．

表1:予想される反応

| | 光刺激の提示位置 | | | |
|---|---|---|---|---|
| | Ba∩Bb | Ba∩¬Bb | ¬Ba∩Bb | ¬Ba∩Bb |
| ユーザA | 無反応 | 無反応 | 縮瞳 | 縮瞳 |
| ユーザB | 無反応 | 縮瞳 | 無反応 | 縮瞳 |

### 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および相対盲点位置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．しかしそのような場合も，以下のようにユーザBのなりすましを検知することが可能であると考えられる．

なお，以下の説明では，簡単のため，ユーザAとユーザBは，盲点と注視点の相対位置(⊿u,⊿v)が全く同じである(相対盲点位置以外の眼球形状に関する各種の値は両ユーザで異なる)と仮定する．ユーザAのキャリブレーションデータおよび相対盲点位置データを用いてユーザAが注視目標(X,Y)を見た場合は，注視点検出装置はユーザAの注視点(X,Y)を正しく得ることが可能である．一方，ユーザAのキャリブレーションデータおよび相対盲点位置データを用いてユーザBが注視目標(X,Y)を見た場合には，キャリブレーションデータの個人差のために，ユーザBの注視点は誤った値(X',Y')として計測される．(X,Y)と(X',Y')の差を(⊿x,⊿y)とする．

以上の状況を例に，ユーザBによるなりすましの検知を説明すると次のようになると考えられる．

(1) ユーザAの相対盲点位置データを入手したユーザBは，自分とユーザAの相対盲点位置は同じであるため，注視目標を素直に注視すれば，自身の盲点がユーザAの盲点と一致することを知る．すなわちユーザBは，注視目標を注視することにより，ユーザAの対光反射とほぼ同じ反応を発生させることができる．しかし，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の注視点を測定する場合，注視目標(X,Y)を見ているユーザBの注視点は注視点検出装置においては(X',Y')として計測される．そこで，被認証者が注視目標を注視しているか否かを認証装置が常にチェックし，「注視目標に注視点が合わなければ認証を開始しない」，「対光反射(縮瞳)が起こった際に，注視点が注視目標から外れていた場合には認証成功としない」という運用をすることによってなりすましを防ぐことが可能であると考えられる．

(2) 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(⊿x,⊿y)であることを知る．すなわちユーザBは，意図的に認証画面上の点(X-⊿x,Y-⊿y)を注視することによって，認証装置に自分が注視目標(X,Y)を見ていると思わせることができる．しかしこの場合，認証装置のほうは被認証者の盲点位置は(X+⊿u,Y+⊿v)であると捉えているのに対し，ユーザBの実際の盲点位置は(X-⊿x+⊿u,Y-⊿y+⊿v)であり，その間に(⊿x,⊿y)の違いが生じる．よって表1に示した「反応の差」を考慮することでなりすましの検出が可能であると考えられる．

このように，生体反射型認証方式は，登録されている生体情報(キャリブレーションデータおよび相対盲点位置データ)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. 対光反射と盲点位置を利用した認証システム

### 4.1 システム構成

実験装置は，制御装置，注視点検出装置，瞳孔径検出装置，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 2000 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を受け取り，表示ディスプレイに注視目標を表示させる．登録フェーズにおける注視点検出装置のキャリブレーション，および，認証フェーズにおける光刺激の提示を行うサブルーチンを含む．
- 注視点検出装置：CCDカメラで被認証者の眼球画面を捉え，1/60ごとに被認証者の注視点を制御装置へ送信する．株式会社テクノワークス 注視点測定システムTE-9200を使用した．
- 瞳孔検出装置：CCDカメラで被認証者の眼球を捉え，カメラの画像から1/30ごとに画像解析により瞳孔径を求める．
- 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．
- 表示ディスプレイ：制御装置の制御に従い，光刺激を提示する．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．LG 16型CRTカラーモニタFLATRON 775 FTを使用した．ディスプレイのブライトネス設定は50%であり，PCの解像度設定を1280×1200ピクセルとした．ただし，認証画面は1280×1200ピクセルの画面内の640×600ピクセルの領域を使用した．また，外光の反射の防止と，認証画面内に提示する光刺激の光が正面以外に漏れることを抑えるため，ディスプレイにプライバシーフィルタを装着させた．

### 4.2 システム概観

システムを図1のように配置する．被認証者は認証時にはアゴ台に頭部を固定され，表示ディスプレイを片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200mmとし，認証画面の使用領域の両端が視覚で約40°となるように設置した．また，注

視点検出装置は左眼から 400mm の距離にある場所に設置した.

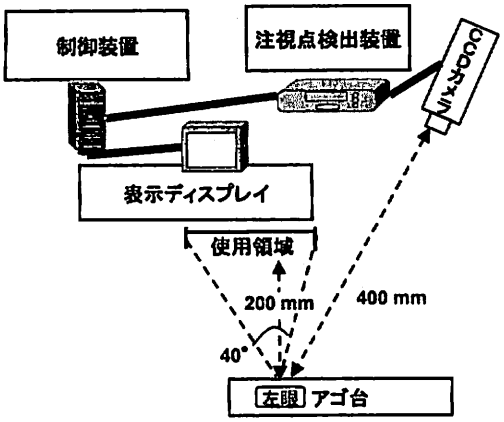


図 1：システムの概観

### 4.3 認証プログラム

本認証方式は盲点の内側ないし外側に光刺激を提示した際の対光反射による瞳孔の収縮反応の差を利用することで認証を行う．認証画面を図 2 に示す．認証画面には定点に注視目標が提示されており，被認証者は認証中，常に注視目標を注視するように指示される．破線で描かれた円は被認証者の盲点を表し，実際の認証では表示されない．すなわち認証時には，注視目標および光刺激のみが認証画面内に提示されることとなる．

光刺激の表示アルゴリズムを図 3 に示す．被認証者が注視目標に視点を移してから認証を開始する．認証を開始してから 2.0 秒後に，被認証者の盲点の中心(図 2 中の①の位置)または盲点の外側である注視目標(図 2 中の②の位置)のいずれかの位置に光刺激が提示される．提示位置の決定はランダムであり，①，②の位置が選ばれる確率はそれぞれ 50%とした．光刺激の提示期間は 1.0 秒である．ここで，光刺激は白色(RGB:255, 255, 255)の円とした．測定開始から 5.0 秒間，瞳孔径を計測する．

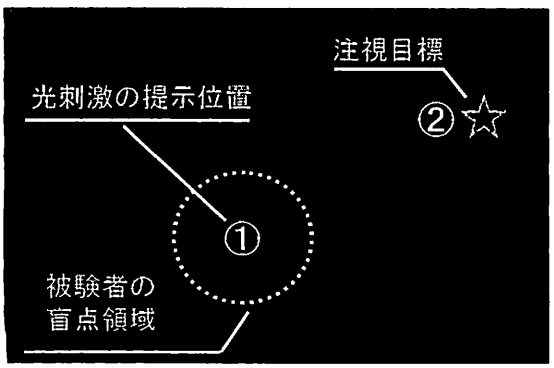


図 2：認証画面

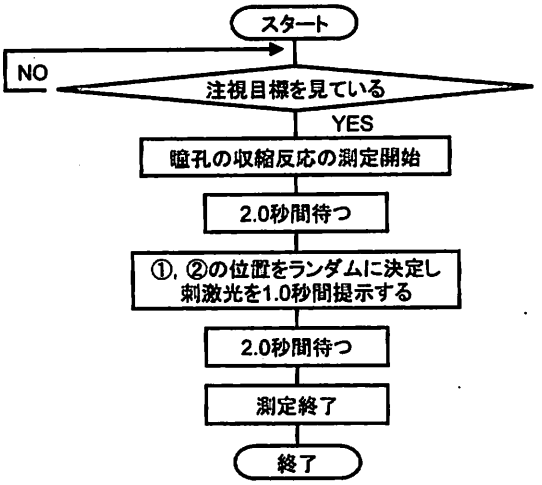


図 3：光刺激の提示アルゴリズム

## 5. 認証実験

本認証方式の実現の可能性を示すため，4 章にて実装した対光反射と盲点位置を利用した認証システムを使用して，盲点位置の個人差，本人拒否率，他人受入率，なりすまし成功率を検証した．被験者は健康な本学学生 10 名とした．照度 0.04～0.15Lux に保たれた暗室にて実験を行った．被験者は暗室に入室後，20 分間の椅座位安静状態を保った後，暗室環境下で認証実験を行った．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．

### 5.1 盲点位置と光刺激の個人差の測定

盲点位置の測定は，ディスプレイ上に順次，光刺激を提示していき，その光刺激の見えない領域を調べることにより，10 人の被験者の左眼の盲点を測定した．

次に，対光反射を誘発する光刺激の強度には個人差が含まれるため，被験者ごとに最適な光刺激の強度を求めた．すなわち，注視目標に光刺激を提示した場合には高い確率で対光反射が起こり，盲点内に提示した場合には対光反射が起こらないような光刺激強度を決定する．各被験者に対して，注視目標，盲点内に様々な強度の光刺激を与え，そのような条件を満たす光刺激の強度を求めた．ここで光刺激の強度は光刺激の円のサイズの大小により変化させることとした．10 人の被験者の注視点と盲点の中心との相対位置および最適な光刺激の円のサイズを表 2 に示す．例えば，被験者 A の盲点の中心はディスプレイ上で，A の注視点より X 軸方向に 231 ピクセル(視角で約 14.5 度)，Y 軸方向に 47 ピクセル(視角で約 2.3 度)はなれた位置に存在し，また，最適な光刺激は半径 5 ピクセルの大きさの円となる．表 1 より，相対盲点位置および最適な光刺激の大きさにはユーザの識別に使えるほどの有意な個人差

はないことが確認できる.

しかし本認証装置では，既に説明したように，注視点に対する盲点の相対位置を前もって測定しておき，注視点検出装置にてリアルタイム計測される注視点から時々刻々の盲点位置を算出する.よって，「注視点と盲点の相対位置の個人差」に「注視点検出装置における各被験者のキャリブレーションデータの個人差」が重畳されたものが，本方式における盲点位置の個人差となる.

そこで次に，被験者Aが他の被験者のキャリブレーションデータを使用した場合に,「実際の注視点」と「注視点検出装置が算出する注視点」との差がどの程度になるのかを測定した．結果を表3に示す．例えば被験者Aが被験者Bのキャリブレーションデータを使用した場合，注視点検出装置はディスプレイ上で，被験者Aの本来の注視点よりX軸方向に43ピクセル(視角で約2.7度)，Y軸方向に-68ピクセル(視角で約3.4度)ずれた点をAの注視点だと判断している．すなわち，被験者Aの実際の盲点の中心から他の被験者の盲点の中心までの距離は表2と表3の結果を重畳して表4のように換算できる.

すべての被験者に対して表3に相当するデータを測定したところ，同様の傾向が得られた．表3の距離においては被験者ごとのばらつきも十分大きく，キャリブレーションデータの個人差を考慮した形での盲点位置には有意な個人差が存在することが確認できる．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.

表2：盲点の相対位置,最適な刺激の大きさ,縮瞳率の閾値(S,T)
(単位：pixel)

| | 位置(X) | 位置(Y) | 刺激(半径) | S | T |
|---|---|---|---|---|---|
| A | 231 | 47 | 5 | 12 | 10 |
| B | 241 | 14 | 5 | 11 | 10 |
| C | 231 | 23 | 5 | 4 | 2 |
| D | 211 | 53 | 3 | 15 | 14 |
| E | 241 | 68 | 4 | 14 | 13 |
| F | 251 | 35 | 4 | 14 | 10 |
| G | 251 | 5 | 5 | 12 | 9 |
| H | 266 | 44 | 5 | 12 | 10 |
| I | 241 | 29 | 4 | 12 | 9 |
| J | 221 | 50 | 5 | 13 | 9 |

表3：キャリブレーションデータの比較
(単位：pixel)

| A | | B | | C | | D | |
|---|---|---|---|---|---|---|---|
| X | Y | X | Y | X | Y | X | Y |
| 0 | 0 | 43 | -68 | -134 | 210 | -279 | 178 |
| E | | F | | G | | H | |
| X | Y | X | Y | X | Y | X | Y |
| -44 | 178 | -125 | 119 | -88 | 50 | -153 | 131 |
| I | | J | | | | | |
| X | Y | X | Y | | | | |
| -95 | 250 | -96 | -267 | | | | |

表4：キャリブレーションデータを考慮した上での盲点位置
(単位：pixel)

| A | | B | | C | | D | |
|---|---|---|---|---|---|---|---|
| X | Y | X | Y | X | Y | X | Y |
| 0 | 0 | 53 | -101 | -134 | 186 | -299 | 184 |
| E | | F | | G | | H | |
| X | Y | X | Y | X | Y | X | Y |
| -34 | 199 | -105 | 107 | -68 | 8 | -118 | 128 |
| I | | J | | | | | |
| X | Y | X | Y | | | | |
| -85 | 232 | -106 | -264 | | | | |

## 5.2 本人拒否率の測定

4章にて実装したシステムを使用して，本人拒否率を測定した．各被験者には5.1節の予備実験により盲点位置と最適な光刺激を求めてから，1日後，8日後，15日後にそれぞれ連続で10回ずつの認証試行を行ってもらった．すなわち，盲点の内側もしくは注視目標に光刺激を提示し，縮瞳反応を測定するという試行を10人の被験者それぞれに対して計30回の試行を実施し，全体で300試行分の縮瞳反応の結果を得た.

光刺激を盲点の内側，注視目標に提示したときの縮瞳反応の分布を示した典型的な例として被験者Aの実験結果を図4に示す．図4は横軸を光刺激に対する縮瞳率，縦軸を度数とするヒストグラムである．また，縮瞳率は「光刺激を提示する直前の瞳孔径の値」と「光刺激提示期間の間の瞳孔径が最小となった値」の差分を「直前の瞳孔径」で割った値である.

実験結果に対し，「$\ell$ 回の試行を 1 回の認証とした場合，注視目標に光刺激を提示した際の縮瞳率がS%未満であった回数がm以下であり，かつ，盲点内に光刺激を提示した際の縮瞳率がT%以上であった回数がn以下であったときに認証成功する」という判定基準を採用した場合の，$\ell$ とmとnの値に対するそれぞれ

の平均本人拒否率(FRR)を表5に示す．なお，本来であれば，1日後，8日後，15日後の認証試行ごとにそれぞれの認証率を測るべきであるが，今回は基礎実験ということで延べ3日間の30回の試行全体に対する認証率を計算している．また，SとTの値については，被験者ごとに最適な値を実験的に求め，これを用いた．各被験者のSとTの値は表2に併記してある．

### 5.3 他人受入率の測定

他人受入率を調べるために，10人の各被験者が自分以外の9人として認証されることが起こりえるか測定した．被験者iが被験者jとして認証フェーズを行うにあたっては，被験者jのキャリブレーションデータを用いて注視点が計測されることになる．また，光刺激が提示される位置および光刺激の強度も被験者jの相対盲点位置データ，光刺激強度を基準として設定される．

しかしながら，本手法は被験者が注視目標を注視したことをトリガとして認証が開始するようになっている．そのため，被験者jのキャリブレーションデータを用いて被験者iの注視点検出を行う場合には，注視点が正しく計測されず，被験者iが注視目標を注視しても認証が始まらない．すなわち本手法においては，キャリブレーションデータが個人を識別するためのテンプレートの一部となっており，テンプレートと被験者との差異があまりにも大きかったため他人許容が発生しなかった．

### 5.4 なりすまし成功率の測定

生体反射型認証方式は，登録されている生体情報が漏洩したとしても，なりすましが困難である．これを確かめるために，不正者が正規ユーザのキャリブレーションデータおよび相対盲点位置データを盗んだ上で，正規ユーザへのなりすましを試みる場合の成功率を測定する．5.3節と同様に，不正者iが正規ユーザjとして認証フェーズを行うにあたっては，正規ユーザjのキャリブレーションデータを用いて注視点が計測されることになる．また，光刺激が提示される位置および光刺激の強度も被験者jの相対盲点位置データ，刺激強度を基準として設定される．

本実験では，10人の各被験者が不正者となり，自分以外の9人として認証されるように能動的になりすましを試みた際の成功率を測定する．ここで3.2節にて述べたなりすまし(1)，(2)について検討する．

まず，(1)は「不正者が正規ユーザの盲点と自身の盲点を一致させる」という方法のなりすましである．5.1節におけるキャリブレーションデータを考慮した上での盲点位置には有意な個人差が存在することが確認されたことから，不正者が正規ユーザの盲点と自身の盲点を一致させつつ，さらに注視点検出装置が算出する注視点を注視目標に合わせることはできないと考えられる．よって，「対光反射(縮瞳)が起こった際に，注視点が注視目標から外れていた場合には認証成功としない」という運用をすることによって，なりすましの成功率を0とすることができるはずである．これは5.3節の実験と等価となるので，ここでは改めて実験を行うことは省略した．

次に，(2)は「不正者が，注視目標(X,Y)の代わりに(X-⊿x,Y-⊿y)の点を見ることにより，注視点検出装置によって測定される不正者の注視点を注視目標に合わせこみ認証を行う」という方法のなりすましである．この場合，3.2節で説明したように，表1に示した「反応の差」を考慮することでなりすましを防ぐことが可能であると考えられる．被験者10人に対して実験を行い，これを確かめる．ただし，何の目印もない点(X-⊿x,Y-⊿y)を注視することは被験者の負担が大きいので，被験者には素直に注視目標(X,Y)を見てもらい，認証装置における盲点位置の算出式を(X+⊿u,Y+⊿v)から(X+⊿x+⊿u,Y+⊿y+⊿v)に代えることにより，同等のなりすまし環境を実現することとする．

4章にて実装したシステムを使用し，自分以外の被験者9人に対して30回ずつ，計270回のなりすまし試行を10人の被験者それぞれに対して実施し，全体で2700試行分の縮瞳反応の結果を得た．なお，被験者の疲労を考慮して，10試行ごとに2分以上の休憩を挟んだ．

なりすましを行ったときの縮瞳反応の分布の典型的な例として，被験者Bが被験者Aになりすましを行ったときの実験結果を図5に示す．実験結果に対して，5.2節と同様に「ℓ 回の試行を1回の認証とした場合，注視目標に光刺激を提示した際の縮瞳率がS%未満であった回数がm以下であり，かつ，盲点内に光刺激を提示した際の縮瞳率がT%以上であった回数がn以下であったときに認証成功する」という判定基準を採用した場合の，ℓ とmとnの値に対するそれぞれの平均なりすまし成功率(FAR)を表5に示す．

図4，図5より，正規ユーザの縮瞳反応の分布となりすまし者の縮瞳反応の分布には明らかな違いが存在することがわかる．しかしながら，正規ユーザの縮瞳反応の分布においてもその分散が大きく，かつ，正規ユーザとなりすまし者の分布に重なりがあるため，正規ユーザとなりすまし者を識別するためにはℓ，m，nの値をある程度大きく設定する必要がある．今回の5.2節と5.4節の実験では，ℓ =10，m=1，n=0を採用することによって，10人の被験者による計3000回の試行(ℓ =10であるため300回の認証に相当)において本人拒否率=7.5%，なりすまし成功率=1.1%とすることができるという結果となった．

表 5：平均本人拒否率および平均なりすまし成功率
（単位：%）

| ℓ=5 | | | |
|---|---|---|---|
| m | n | FRR | FAR |
| 0 | 0 | 16.6 | 2.7 |
| 1 | 0 | 2.1 | 9.5 |
| 0 | 1 | 16.6 | 5.6 |
| 1 | 1 | 2.1 | 15.4 |
| ℓ=10 | | | |
| m | n | FRR | FAR |
| 0 | 0 | 28.7 | 0.2 |
| 1 | 0 | 7.5 | 1.1 |
| 0 | 1 | 28.7 | 0.6 |
| 1 | 1 | 7.5 | 2.0 |
| ℓ=15 | | | |
| m | n | FRR | FAR |
| 0 | 0 | 37.4 | 0.0 |
| 1 | 0 | 14.3 | 0.1 |
| 0 | 1 | 37.4 | 0.1 |
| 1 | 1 | 14.3 | 0.4 |

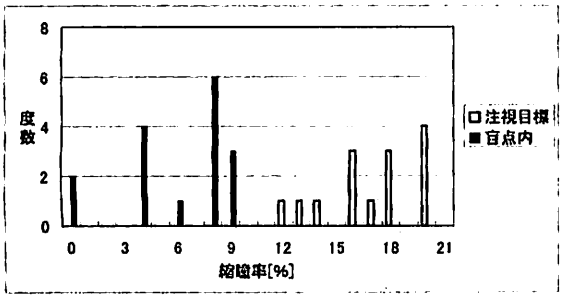

図 4：認証の際の被験者 A の縮瞳反応の内訳

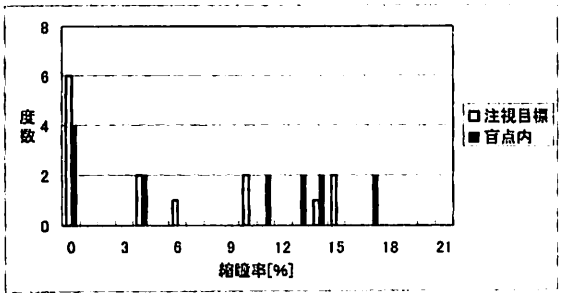

図 5：被験者 A へのなりすましの際の
被験者 B の縮瞳反応の内訳

## 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．また，生体反射型認証のプロトタイプである対光反射と盲点位置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，本認証方式の改良により認証率の改善，認証試行回数の低減，なりすまし耐性の強化を行うとともに，他の生体反射を利用した認証システムの提案を行っていきたい．

## 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] 日本郵政公社ホームページ，“日本郵政公社報道発表資料”，http://www.japanpost.jp/pressrelease /japanese/kawase/050228j301.html，確認日 2006 年 6 月 20 日．

[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] 荒井大輔，西垣正勝，“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 (2006)（掲載決定）．

[5] 小澤雄司，荒井大輔，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”，マルチメディア，分散，協調とモバイル（DICOMO 2005）シンポジウム論文集，pp. 105-108，(2005)．

[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] 苧阪良二，中溝幸夫，古賀一男 編，“眼球運動の実験心理学”，p20 p45 p101，名古屋大学出版会（1993）

[11] 玻座真忠明，小崎智照，安河内朗，“異なる色光が瞳孔の反応に及ぼす影響”，日本生理人類学会誌，9 特別号（2），pp40-41（2004）

[12] 野村幸弘，星野聖，“ストレスの瞳孔動揺に及ぼす影響”，映像情報メディア学会技術報告，Vol. 22，No. 33，pp. 7-11，June 1998.

[13] 平井有三，”視覚と記憶の情報処理”，倍風館．リチャード・L・グレゴリー著，近藤倫明・中溝幸夫・三浦佳世 訳，”脳と視覚 —グレゴリーの視覚心理学—”，ブレーン社．

[14] 株式会社クレアクトインターナショナル ISCAN 眼球運動・注視点追跡システム http://www.creact.co.jp/jpn/por.pdf，確認 2006 年 6 月 20 日．

[15] 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）