2005－CSEC－31（10）
2005／12／9

虹彩認証システムのセキュリティ評価用テスト物体セットについて

松本　勉　　佐藤健二

横浜国立大学大学院環境情報研究院
〒240-8501 横浜市保土ヶ谷区常盤台 79-7
電子メール: tsutomu@mlab.jks.ynu.ac.jp

あらまし：虹彩認証システムのセキュリティを評価することを目的とする一揃いのテスト物体（テスト人工虹彩）を開発する際の検討事項につき考察する.

On the Set of Biometric Test Objects for Security Evaluation of Iris Authentication Systems

Tsutomu Matsumoto　　Kenji Sato

Yokohama National University
Graduate School of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
Emil: tsutomu@mlab.jks.ynu.ac.jp

Abstract: This paper discusses an experimental study on developing a set of biometric test objects --- Test Artificial Irises --- for security evaluation of iris authentication systems.

1. はじめに

指の指紋，眼の虹彩，指や手のひらや手の甲の静脈などの身体的特徴を用いた個人認証技術（バイオメトリクス，バイオメトリック認証技術，生体認証技術）のセキュリティを評価する際には，当該身体部分の偽造や偽装の困難性（あるいは容易性）について検討することが必須である[1].

筆者らは 2000 年 7 月から指紋認証技術に関して[2]，また 2003 年 7 月から虹彩認証技術[3]に関して[4][5][6]，さらに 2005 年 3 月から静脈認証技術に関して[7][8]身体的特徴の偽造に関するセキュリティ研究報告を行ってきた. その多くの結果は内外の研究者により追試され妥当であることが確認されている．たとえば 2005 年3月時点での各種指紋認証システムに対する調査結果については記事[9]を参照されたい.

バイオメトリック認証技術を具現化した個々のシステムを，バイオメトリック認証システム（Biometric System）とよぶことにする．バイオメトリック認証システムは生体情報の取得と処理とそれらに基づく個人認証管理を行う機器とソフトウェアなどから構成される. 用いる身体的特徴の種類が M であるときは M 認証システムとよぶ.

一連の研究から，あるバイオメトリック認証システムの開発・製造・試験などの各段階において必要となるセキュリティ評価の方法として，人工的に作成しておいたテスト物体（Biometric Test Object）を用いて次のような実験の結果を用いる方法が有用であることを見出した. すなわち，テスト物体がそのシステムに登録できるか，登録できたら再び提示した同じテスト物体が照合されるか，登録した人間の身体部分に対してそれを模擬して作られたテスト物体が照合されるか，そのテスト物体を登録し，対応する

人間の身体部分で照合されるか, といった事項についての実験である.

そこで, このような目的に用いることのできるテスト物体が満たすべき条件の整備や作製の方法を確立することが求められる.

これまで指紋認証システムに対してはテスト物体（テスト人工指）に関する検討をまとめ, 指紋読取装置の品質及び読取装置が出力する画像の品質についての評価基準について規定した日本規格協会発行の標準仕様書(TS X 0101:2005)[10]の一部分として公表した.

本稿では, 与えられた虹彩認証システムのセキュリティを評価するためのテスト物体のセット（紙製人工虹彩などの組）を開発する際の基本的検討事項につき考察する.

虹彩認証技術（あるいは虹彩照合技術、虹彩認識技術と呼ばれることもある）は, 誤拒否率や誤受理率が低いとされることから, 空港等での入出国管理や施設へ入退出管理などを中心として広く用いられつつある.

2. バイオメトリック・テスト物体

バイオメトリック認証システムでは対象とする身体部分を，光などを用いて計測している. 従って, 光などで見て身体部分と同じように見える対象物であれば, バイオメトリック認証システムに受入れられる可能性があるが, バイオメトリック認証システムに提示される対象物が生体であるかどうかを検知する何らか“生体検知” 機能がうまく組み込まれ，うまく働いているならば, そのような対象物は登録も照合もできないことになる.

しかし，バイオメトリック認証においては, 利用者・管理者の利便性を重視し，登録失敗 (Failure to Enroll) や誤拒否 (False Rejection) ができるだけ少なくなるような設定がなされることが多い. このため, バイオメトリック認証システムに本来提示される人間の身体部分の代わりに人間の身体部分とは限らない何らかの対象物が提示された場合でも, 生体検知のメカニズムがうまく働かず, これを拒否することに失敗することがある. この関係を詳しく見てみる.

すべての対象物（３次元的な形を有するもの, 身体部分を含む）の集合をΩとする. 種類 M の身体部分（指，手の甲，手のひら，眼，顔，など）を対象とするバイオメトリック認証システムのすべてからなる集合を Ｂ[M] と書く. システムＳ∈ Ｂ[M]への提示の仕方や環境が適切であればＳに登録できる対象物の全体をΩの部分集合 Enroll[Ｓ]で表すことにする. 種類 M の身体部分のすべての個人にわたる集合をΩの部分集合 Human[M]で表すことにする.

システム Ｓ ∈ Ｂ[M] が普通に使えるためには, FER: Failure to Enroll Rate, すなわち,

FER[Ｓ]
= #(Human[M]－Enroll[Ｓ])/ # Human[M]

が十分に小さいこと（理想的には ０ ）が条件となる. ただしここでは集合 Human[M]を有限集合であると考え，その元の総数 #Human[M]が定義できるとした.

システム Ｓ ∈ Ｂ[M] が種類 M の身体部分以外を排除することも望まれるが，これは,

Enroll[Ｓ]－Human[M]

が十分に小さいこと（理想的には空集合Φ）と表せる. 考察すべきポイントは, この集合をΦにするようにEnroll[Ｓ]を作るとFER[Ｓ]が大きくなる傾向があることである（図１参照）.

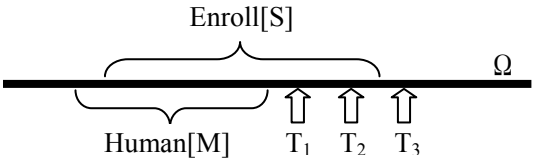

図１．Ｓは身体部分でない物体も受け入れる

与えられたバイオメトリック認証システムが身体部分の偽造に対してどれほどのセキュリティを有するかを実験的に把握する必要が生じた場合に考えられる評価の方法には, 次の２段階が考えられる：

<u>第１段階</u>

バイオメトリック認証システムにテスト物体を提示し,

（A）登録できるかどうか,

（A-A）登録できた場合，再度提示して照合できるかどうか

について調べる.

<u>第２段階</u>

バイオメトリック認証システムに

（A-L）テスト物体を登録し，身体部分で照合できるかどうか,

（L-A）身体部分を登録し，テスト物体で照合できるかどうか,

について調べる.

ここで，記号Ａは「Artificial Object」の略であり人工のテスト物体を意味する．また記号Ｌは「Live Object」の略であり生体の身体部分を意味する．また，記号（Ｌ-Ｌ）で，身体部分を登録し身体部分で照合する普通の使い方を表現することにする．

図１に例示される状況はテスト物体T_1, T_2について(A)および(A-A)に成功し，テスト物体T_3については(A)に（したがって(A-A)にも）失敗したということであるが，バイオメトリック認証システムＳにテスト物体を提示する実験により集合Enroll[S]に関する情報が増えたことを示している．よって，適切なテスト物体の組（セット）を揃えることは有益である．

なお，第１段階の（A）が成功しないテスト物体，すなわち，システムに登録ができないテスト物体については自動的に（A-A）や（A-L）が成功しないが，第２段階の（L-A）は成功する可能性があることに注意が必要である．たとえば図１のテスト物体T_3については（L-A）が成功する可能性がある．

3. 虹彩と虹彩認証

眼はおおよそ図２のような構造をしている．眼を用いた個人認証には網膜と虹彩が利用される．カメラのレンズに相当する水晶体の奥に位置する硝子体で満たされたボールの底の視神経の集まった部分が網膜である．網膜上の血管のパターンが個人認証に用いられる．実は網膜認証の適用はあまり広がっていない．装置を覗き込む形で網膜パターンを調べる方式が一般的であり，利便性が高くないことがその主要な理由であるようである．

虹彩は，黒目の内側で瞳孔より外側のドーナツ状の筋肉組織であり，カメラの絞りに相当する機能をもつ．人の眼は胎児のときに形成され，その時点で瞳の部分に孔があき，その開口部，すなわち，瞳孔から外側に向かって放射状の皺（しわ）ができる．この皺は生後 2 年程度で成長が止まり，それ以降は変化しないといわれている．同一人の左右の眼でもその模様は異なり，また一卵性双生児でも異なる．虹彩は，眼球へ入射する外光の光量を調節するために伸縮するが，そのパターンは伸縮してもほとんど変わらない．この「万人不同」「終生不変」の特徴が，虹彩が個人認証に用いられる理由である．

虹彩は眼から離れた場所から近赤外線を用いてきれいに撮影できる．撮影した虹彩画像をビット列に変換して記録しておき，もう一度撮影したものと比較して安定的に判断する技術が開発されたため[3]，虹彩認証システムは実用化され，さまざまな応用に使われている．

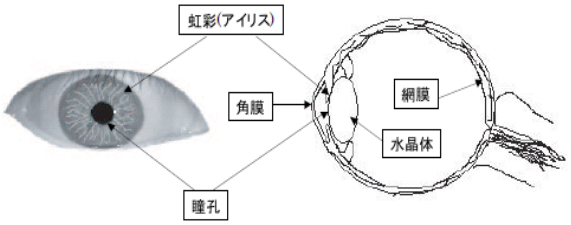

図２．眼の構造

4. 虹彩認証システムとテスト人工虹彩

本稿では，個々の虹彩認証システムのセキュリティを評価するためのテスト物体（＝ テスト人工虹彩）の作製と使用につき検討する．

4.1 利用する虹彩認証システム

利用する虹彩認証システムを表１にまとめる．システム１とシステム２はPC端末用の小型の簡易なシステムで一度には片眼だけを認証する．システム３とシステム４は両眼を用いたゲート管理等など用の本格的なシステムである．

表１．虹彩認証システム

システム名	虹彩カメラ 製造者 名称 型番 製造番号	虹彩処理ソフトウェア 製造者 名称	認証管理ソフトウェア 製造者 名称 認証タイプ	眼とカメラの推奨距離	参照URL
システム1	Oki IrisPass-h EQ50009A 202A000498	Oki OKI IRISPASS-h BSP	SAFLINK Corporation アイリスパス-h SAF2000 for Workstation ver 1.72 1:1 照合	4cm	http://www.oki.com/jp/FSC/iris/jp/irisgt_h.html
システム2	Panasonic Authenticam BM-ET100US AGB51530	Iridian Technologies Private ID	IO Software SecureSuite 3.10 1:N 照合	48cmから53cm	http://www.panasonic.com/cctv/products/bmet100us.asp
システム3	Oki IrisPass-WG カメラユニット EQ50011A 205A00002	Oki －	－ － 1:N 照合	30cmから60cm	http://www.oki.com/jp/FSC/iris/jp/iriswg.html
システム4	Panasonic BM-ET300 － DJA0008	Panasonic －	Panasonic BM-ES300 1:N 照合	30cmから40cm	http://www.panasonic.biz/security/et300/pdf/bmet300.pdf

システム１　両眼登録と片眼登録の選択ができる。両眼登録の場合，登録時に左右の眼をそれぞれ２回ずつ提示する．カメラを覗き込むと緑色の枠があり，その枠が見えるように照合させる．１回目において虹彩ビット列が生成されたとのディスプレイ表示がなされ，２回目のビット列と一致すればその虹彩ビット列が登録される．この登録時の２度目の提示の際にのみ眼の画像がディスプレイに表示される．ビープ音によるガイドを使うことができるが，音声ガイドはない．OS ログオン時に虹彩等を提示しログオンできたか否かを照合結果とした．

システム２　両眼登録と片眼登録の選択ができる。両眼登録の場合，登録時に左右の眼をそれぞれ４回ずつ提示．照合距離になると虹彩の撮影が始まり，虹彩撮影中は，カメラ下部のライトがオレンジ色から緑色に変わる．照合のときも同じ。撮影された４画像が総合的に判断され，登録虹彩ビット列が生成されその虹彩データが登録される模様．登録時・照合時ともに眼画像がディスプレイに表示される．ただし，登録時の４回目だけ虹彩画像がディスプレイに長く表示される。音声ガイドはない．専用ソフトウェアを起動する際に虹彩を提示し，起動できたか否かを照合結果とした．

システム３　カメラ部分の装置に顔を提示すると自動的に顔から眼画像が抽出される．登録時に顔を２回提示する．１回目において登録虹彩ビット列を生成し，２回目のビット列と一致すればその虹彩データが登録される模様．照合時には装置に顔を提示することで自動的に装置が起動し，顔・眼画像を抽出する．どちらか片方の虹彩が照合されれば，認証ＯＫの結果が出る．機械音と LED ランプによるガイドが使える．　登録時に撮影された眼画像が接続 PC に保存される．登録者の情報を管理するページで眼画像を表示して確認できる。

システム４　顔を装置のカメラ部分の前にもっていきある程度位置をあわせる。登録時に両眼を４回提示する．撮影された画像に基づく総合的な判断によりビット列が生成されその虹彩データが登録される模様．照合時には装置に眼を提示すると自動的に装置が起動し，眼を撮影する．どちらか片方の眼が照合されれば認証ＯＫとなる．合成音声と LED ランプによるガイドが使える．撮影された眼画像は接続サーバに置いておける．

4.2 テスト人工虹彩の作製

テスト物体を作製するために，お手本となる身体部分の情報を利用することは自然な考え方であろう．テスト人工虹彩の場合，

１．眼画像の取得（照明，カメラ，距離）
２．眼画像の整形（大きさ，左右反転）
３．眼画像の処理（明るさ，コントラスト）
４．眼画像の印刷（プリンタ，紙）
５．テスト人工虹彩の組立(印刷画像の瞳孔部分の穿孔，メガネフレームへの貼付け)
６．テスト人工虹彩の提示（距離，角度）

といったステップからなる流れと各ステップにおける検討項目が考えられる．

4.3 眼画像の取得と画像処理

眼画像取得には，独自に構成した赤外線撮影システムで撮影する方法と，虹彩認証システムから画像を取り出して利用する方法を検討した．なお，画像処理には汎用のソフトウェアである“Adobe Photoshop 6.0”を用いた．

赤外線撮影システム s

ディジタルマイクロスコープ“SZ-7000”
　レンズ：x0～x30　赤外線レンズ
　製造元：スカラ株式会社
赤外線照明“LED LIGHTING　810nm”
　製造元：有限会社シマテック
　製造番号：LT309127

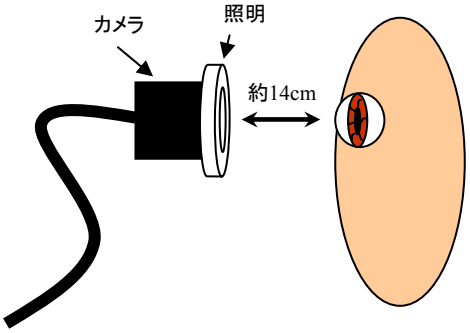

図３．システムsによる撮影方法

虹彩認証システムからの眼画像の取り出し

システム 1 の虹彩登録時にディスプレイに表示される眼画像を bmp 形式で保存する。横長に変形されて表示される画像の縦横比を調整して使用する．

システム 2 においてディスプレイに表示される画像は，画質・大きさが十分でないと判断し，システム２は眼画像の取り出しには適さないと判断した．

システム３およびシステム４に登録されている虹彩画像を閲覧する際にディスプレイに表示される眼画像を bmp 形式で保存する．左右が反転して表示される眼画像の左右を再び反転して利用する．

整形以外の画像処理

必要に応じ，“Adobe Photoshop 6.0”により明るさとコントラストを調整する．

4.4 眼画像の印刷とテスト人工虹彩の組み立て

保存した眼画像を実際の眼のサイズに近くなるようにサイズを調整して，レーザープリンタで紙に印刷する．使用するプリンタと紙は以下の２種類ずつとする．

カラーレーザープリンタ

1 “EPSON Intercolar LP-8800c” 600dpi
2 “EPSON Offirio LP-9000c” 600dpi

プリンタ用紙

1 インクジェットプリンタ用
“スーパーファインマット紙”
製造元：日本ビクター株式会社
型番：PF-SF110A4F
2 インクジェットプリンタ用
普通紙“マルチ OA ペーパー”
製造元：コニカフォトイメージング株式会社
型番：KIK250A4MP

印刷した眼画像の瞳孔部分をカッターで切り抜いた紙を，メガネフレームに貼り付ける．このとき，図４のように眼画像の周りに余白を十分に残しておく．

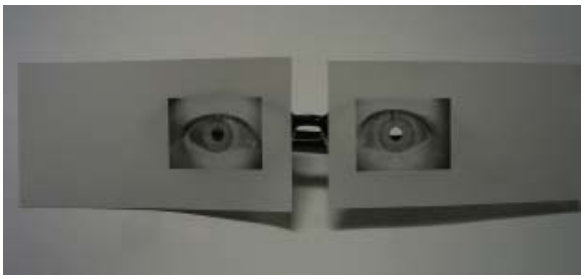

図４．テスト人工虹彩(メガネ貼付型)の例

4.5 作製したテスト人工虹彩

同一人の眼をサンプルとして用い，眼画像取得手段，眼画像の明るさやコントラストの調整の有無，および，プリンタと紙の種類を変化させ，表２に定義する多様な人工虹彩を作製した．

表２．作製したテスト人工虹彩

人工虹彩の名称	眼画像取得手段	明るさ・コントラスト調整	プリンタ・紙
A(1)	システム１	なし	１・１
A(1b)	システム１	なし	１・２
A(1c)	システム１	なし	２・１
A(1d)	システム１	なし	２・２
A(3)	システム３	なし	１・１
A(4)	システム４	なし	１・１
A(4e)	システム４	明るさ+40 コントラスト+20	１・１
A(4f)	システム４	明るさ+60 コントラスト+40	１・１
A(s)	赤外線撮影システム s	なし	１・１

5. 虹彩認証システムを用いた実験

本格型の虹彩認証システムであるシステム３とシステム４に対して，表２の様々なテスト人工虹彩を提示して実験を行った．

5.1 虹彩認証システムへの虹彩等の提示方法

人工虹彩を提示する位置のずれによる照合率の変化を押さえるため，実験者の顔をガイドで固定して，虹彩認証システム３および 4 のカメラ部と眼（人工虹彩）との位置関係（それぞれ 57cm，43cm）を一定に保ち，同一の実験者がすべての実験を行った．

5.2 虹彩認証システムの(L-L)実験結果

生体虹彩（両眼）を登録し，同じ生体虹彩（両眼）で照合をする（L-L）実験を行い，

システム３： 97 回成功/100 回試行
システム４：100 回成功/100 回試行

という結果を得た．このように，両システムとも正常に利用できるものであることを確認した．

5.3 テスト人工虹彩による実験結果

第１段階の実験(A)，(A-A)および第２段階の実験(A-L)，(L-A)を各種のテスト人工虹彩を用いてシステム３およびシステム４に対して行った結果をそれぞれ表３と表４に示す．

実験(A)の結果欄はテスト人工虹彩が登録できる場合に○を，できない場合に×を示した．実験(A)が×であると自動的に実験(A-A)および(A-L)は実行できないので対応する結果欄にーを配置した．その他の結果欄には，100 回の試行のうちで受入が成功した回数を示した．

プリンタの機種や紙質については本実験の範囲では A(1), A(1b), A(1c), A(1d)の結果から，大幅な違いが現れないことが確認できた．

眼画像の取得方法については，自作の赤外線撮影システム s であっても虹彩専用のカメラとして開発されたシステム１，システム３と遜色のない結果を得ているため，十分な品質の眼画像取得が行えることがわかる．よって，このような赤外線撮影システムをテスト人工虹彩作製用眼画像取得の目的に使用できる可能性が示唆される．

また，システム４から得た眼画像そのままを利用して作製したテスト人工虹彩 A(4)は，実験結果からわかるように他の眼画像取得手段で得た画像から作製したテスト人工虹彩とはかなり異なる特性を有する．しかし，A(4d)，A(4e)の結果から，画像処理を行えば他の眼画像取得手段並みの品質に変換できることもわかる．この結果，画像処理により様々な特性をもつテスト人工虹彩を作製できる可能性が示唆される．

なお，本実験の結果は，虹彩認証システムのセキュリティ評価についてもある程度の結果を示している．すなわち，システム３では表 2 のすべてのテスト人工虹彩が登録できないが，(L-A)はすべてのテスト人工虹彩で成功している．これに対し，システム４では A(4)以外のすべてのテスト人工虹彩が登録でき，(A-A)，(A-L)，(L-A)の各実験の成功割合も高い．

表３．システム３のテスト人工虹彩による評価

人工虹彩	(A)	(A-A)	(A-L)	(L-A)
A(1)	×	−	−	96
A(1b)	×	−	−	93
A(1c)	×	−	−	91
A(1d)	×	−	−	79
A(3)	×	−	−	82
A(4)	×	−	−	2
A(4e)	×	−	−	84
A(4f)	×	−	−	83
A(s)	×	−	−	75

表４．システム４のテスト人工虹彩による評価

人工虹彩	(A)	(A-A)	(A-L)	(L-A)
A(1)	○	88	100	87
A(1b)	○	96	100	93
A(1c)	○	96	100	97
A(1d)	○	91	98	93
A(3)	○	95	75	76
A(4)	×	−	−	0
A(4e)	○	92	98	94
A(4f)	○	95	98	91
A(s)	○	100	97	89

6. まとめ

本稿では，虹彩認証システムのセキュリティを評価するためのテスト人工虹彩のセットを開発する際に考慮すべき基本的事項につき，眼画像の取得手段，眼画像の整形，眼画像の画像処理，眼画像の印刷，テスト人工虹彩の組立，テスト人工虹彩の提示方法などの面から考察した．

文　献

[1] 宇根正志，松本 勉，“生体認証システムの脆弱性について―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.35-83，日本銀行金融研究所, July 2005.
http://www.imes.boj.or.jp/japanese/kinyu/2005/kk24-2-2.pdf

[2] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino, "Impact of Artificial "Gummy Fingers" on Fingerprint Systems," Optical Security and Counterfeit Deterrence Techniques IV, Rudolf L. van Renesse, Editor, Proceedings of SPIE Vol. 4677, pp.275-289, SPIE --- The International Society for Optical Engineering, 2002. http://www.spie.org/web/abstracts/4600/4677.html, http://spie.org/Conferences/Programs/02/pw/confs/4677.html

[3] John Daugman, “Recognition Persons by Their Iris Patterns, ”in Biometrics Personal Identification In Networked Society, Kluwer Academic Publishers, pp.103–121, 1999.

[4] 松本勉，平林昌志，“虹彩照合技術の脆弱性評価(その 1),” 電子情報通信学会，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，第 1 回研究発表会予稿集，pp.53–59, July 2003.

[5] 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 2003, Vol.2003, No.15, pp.187–192, Oct. 2003.

[6] 松本勉，平林昌志，佐藤健二，“虹彩照合技術の脆弱性評価(その 3), ” 2004 年暗号と情報セキュリティシンポジウム，SCIS2004, Vol.I, pp.701–706, Jan. 2004.

[7] 松本 勉，鉢蝋拓二，田辺壮宏，森下朋樹，佐藤健二，“バイオメトリクスにおける生体検知と登録失敗--- 静脈認証に関する速報 ---，” 電子情報通信学会技術研究報告，ISEC2004-141, March 2005.

[8] 松本 勉，鉢蝋拓二，田辺壮宏，森下朋樹，佐藤健二，“バイオメトリクスにおける生体検知と登録失敗（２）--- 静脈認証システムに関する研究（その１） ---，” 電子情報通信学会技術研究報告，ISEC2005-5, May 2005.

[9] 堀内かほり，BYTE LAB 「濡れた指，乾燥した指----指紋認証の実際」NIKKEI BYTE，2005 年 4 月号，pp. 60-67，日経ＢＰ社（2005 年 3 月 22 日発行）．

[10] 標準仕様書(TS X 0101:2005)「指紋読取装置の品質評価方法」，日本規格協会，2005 年 5 月 20 日．http://www.webstore.jsa.or.jp/webstore/Com/FlowControl.jsp?lang=jp&bunsyoId=TS+X+0101%3A2005&dantaiCd=JIS&status=1&pageNo=0