平成１７年度経済産業省　産業技術研究開発委託事業－１
生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化

第７部　共同研究（横浜国立大学）

平成１８年３月

財団法人ニューメディア開発協会

バイオメトリクスの脆弱性に関する分析、研究

2006 年 2 月 27 日

松本　勉
横浜国立大学大学院環境情報研究院

1. はじめに

生体認証技術、バイオメトリクス、あるいはバイオメトリック認証技術とは、ひとりひとりの人間に固有の身体的な特徴（指紋、掌形、顔、虹彩、網膜、静脈（血管）パターン、耳形状など）や行動的な特徴（声紋、手書き署名、キー・ストローク、歩行パターンなど）を用いて、個人の認証を機械が行う技術を指す。

生体認証技術の適用の歴史は長く、機密情報を扱う建物や部屋への入退室管理や、サーバ計算機や監視カメラの使用に関するアクセス管理などの、限定された利用者を対象とする組織の情報システムでの利用を中心として、古くから行われてきたが、最近では、携帯電話や銀行カードの利用者認証、ノートＰＣへのログインやアプリケーションの利用者認証、ネットワーク上の取引での個人認証、集合住宅における入室管理、さらには空港等における入出国管理の本人確認手段としての利用など、利用の裾野が爆発的に広がってきている。

生体認証技術を活用する際には、生体認証技術の利点や注意点をよく理解し、システム構築者や運用者はそのセキュリティポリシーに見合った生体認証技術を採用するようにすることが望ましいといえよう。そこで以下では生体認証技術の概念的整理とセキュリティ評価について考察する。また、虹彩認証システムを例にとりセキュリティ評価の方法論につき具体的に論じる。

2. 生体認証システム

生体認証技術を具現化した個々のシステムを、生体認証システムあるいはバイオメトリック認証システム（Biometric System）という。生体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。用いる身体的あるいは行動的特徴とその利用の方法を総合した様式（modality）がＭであるとき、Ｍ認証システムという。

生体認証システムの働きには登録(enrollment)と認証(authentication)の２つの段階がある。生体認証システムは一般に、身体情報取得部、固有パターン抽出部、生体検知部、テンプレート生成部、身体情報記録部、照合部、登録総合判断部、認証総合判断部から構成されると考えられる。

生体認証には、1 対 1 照合（verification）と 1 対 n 照合（identification）の区別がある。生体認証システムに提示された特徴の持ち主があらかじめ識別された個人であるかどうかを確認することが 1 対 1 照合である。利用者の固有パターンは、利用者の

ID と結び付けられて、テンプレートとして保管される。認証時には、被認証者となる利用者は、自分の生体情報と ID を生体認証システムに提示する。生体認証システム側は、提示された生体情報から固有パターンを抽出し、対応する ID のテンプレートと照合する。

生体認証システムには利用者の ID なしで生体情報だけが提示され、生体認証システムがそれから抽出した固有パターンが、登録されている（n 人の候補のうちの）いずれかの ID の利用者に対応するものであればその ID を出力し、誰にも対応しない場合はそうだという結果を返す方式が 1 対 n 照合である。被認証者がブラック・リスト等に登録されている個人でないこと示す目的で使うこともある。

3. 生体認証システムの特徴

個人認証の基本的方法は大別して、本人だけが知っている情報によるもの、本人だけが所持している物によるもの、それから生体認証である。もちろん、これらを単独で用いるだけでなく、組合せて利用することも非常に多い。

生体情報は、パスワードのように記憶する必要がないし、ＩＣカードのように紛失の危険が少ないが、本人が確実に本人と認められないことや、一定割合で特定の生体情報を利用できない人々がいることなど、他の技術との違いがある。また、生体認証においては、生体情報の偽造が困難であることが求められるが、現実には、利用者および管理者の利便性を追及すると、生体認証システムにとって本物の生体部分のように見えるものが提示された場合に完璧に受入を拒否するような生体認証システムを、許容できるコストで作ることが、必ずしもうまくできるとは限らない。パスワードやＩＣカードは無効化し再発行することができるが、たとえば顔が偽造されたことがわかっても、顔を新しいものに変更することはできないことは、特筆すべき生体認証システムの注意点である。

4. 生体認証システムの認証精度

生体認証システムでは、本人であるが本人であると照合されない場合（False Rejection）が存在する。これは、登録時と認証時で状況が異なるためである。登録時と認証時の装置の違い、生体情報の変化、生体情報の提示方法のばらつきなどが原因である。このため、照合を厳密にしすぎず、誤拒否率（FRR: False Rejection Rate）が適度に低く抑えられるようにシステムのパラメータを調整して用いることが普通である。そうすると、異なる人間の生体情報で厳密には異なっているものが提示された場合に、それを誤って正しい本人の生体情報であると誤って照合されることが避けられない。つまり、誤受理率（FAR: False Acceptance Rate）をゼロにすることは困難である。FRR や FAR を生体認証システムの認証精度という。

生体認証技術を対象とする標準やガイドライン等の策定は世界中で活発に行われているが、認証精度に関しては、日本国内では、日本規格協会情報技術標準化センター（INSTAC）のバイオメトリクス標準化調査研究委員会によって、指紋、虹彩、血管

パターン、顔、音声、手書き署名を用いた認証精度の評価方法について検討が行われ、関連する TR（テクニカルレポート）が作られており[1][2][3][4][5][6][7]、それらにおいては認証精度評価を行う際の留意点や評価結果の報告方法等を規定している。

指紋、虹彩、血管パターンを用いた認証については、誤受理率等の指標のほか、照合精度特性として ROC 曲線（ＦＡＲとＦＲＲの関係）を評価環境とともに精度評価レポートに記述することが、また、顔認証など、照明条件等によって影響を受けやすい生体認証技術の場合は、評価テストを再現可能にするために、人物の姿勢・挙動、表情に関する条件、照明の位置・角度等のパラメータを精度評価レポートに記述することが、それぞれ求められている。行動的特徴である音声を用いた認証の場合には、発声する内容の種類により分類される音声認証方式のそれぞれについての規定が示されている。手書き署名の場合は、第三者が他人の筆跡を模倣してなりすましを行うという攻撃が想定されており、どのレベルの模倣を想定しているかの評価レポートへの明記を要求している。

5. 生体認証システムのセキュリティ

生体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、生体認証システムに受入れられる可能性があるが、生体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、生体認証においては、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、生体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[8]。

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。様式 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。様式 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、

Human[M]－Enroll[Ｓ]

が十分に小さいこと（理想的には空集合Φ）が条件となる。

システム Ｓ ∈ Ｂ[M] が様式 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）。

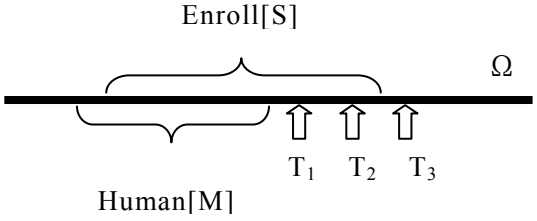

図１．Ｓは身体部分でない物体も受け入れる

6. 生体認証システムのセキュリティ評価

生体認証においては、本人を間違うことなく認めると同時に、本人でない者が本人になりすますことをいかに排除するかがセキュリティ上の焦点となる。なりすましに関する脆弱性には様々な項目がありその多くはシステム設計・運用で対処できるが、最大の懸念事項は、特定の具体的生体情報の代わりをする対象の提示である。以下では身体的特徴を用いる生体認証システムに限定して考察する。

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バイオメトリック認証システム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[9]。

筆者らは 2000 年 7 月から指紋認証システムに関して[10]、また 2003 年 7 月から虹彩認証システムに関して[11][12][13]、さらに 2005 年 3 月から静脈認証システムに関して[14][15]、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[15]を参照されたい。

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）を用いた次のような方法が有用であることを見出した[15]。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実験を行いその結果を分析するセキュリティ評価方法である。

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。

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)[17]の一部分として公表した。

また、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した[8]。

7. テスト物体を用いるセキュリティ評価方法

与えられた生体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：

第１段階

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。

第２段階

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。

8. 身体部分の情報入手に関する考察

生体認証システムに登録・照合できる生体部分を模擬したテスト物体を作製するには、生体部分の情報入手が必要であるが、第１段階の実験においては、必ずしもある特定個人の身体部分の特徴を模したものであることは求められない。この身体部分の

情報入手に際して、評価対象の生体認証システムそのものは必要とはいえず、これとは独立に、身体部分につき各種の測定を行えばよい。ただし、評価対象のシステムが特に“何を見ているのか”に関する情報が増えれば、省略可能な測定項目が増えることになる。

また、第２段階の実験においては、特定個人の身体部分の特徴を採取することが必要である。セキュリティ評価の実験においては、実験に協力する個人の身体部分を計測すればよい。

実際の攻撃者が個人の身体部分に関する情報を入手しようとした場合の困難性を論じるには、撮影された顔画像やガラス等についた指紋のように本人の身体部分を直に計測しなくてもよい場合と、本人の身体部分を直に計測しなければならない場合とがあることに留意が必要である。目（虹彩）や指や手の内部（静脈）を用いたバイオメトリクスは後者に分類されるといえる。しかし、後者であっても本人の身体部分を直に計測することが攻撃者にとって困難であるとは限らない。たとえば、バイオメトリック認証システムの利用が普及するにつれ、バイオメトリクス入力装置に自らの身体部分を提示することが日常的になると、偽のバイオメトリクス入力装置に、それとは気づかず身体部分を提示して情報取得がなされてしまう、といった危険性も考慮しなければならないからである。偽夜間金庫や偽ＡＴＭ、あるいはインターネットにおけるフィッシング詐欺事件の場合と類似の状況になるわけである。

9. 虹彩認証システムとテスト人工虹彩

以下では、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）の作製と使用に関する検討例につき論文[8]にもとづき紹介する。

9.1 虹彩

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[18]、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。

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。

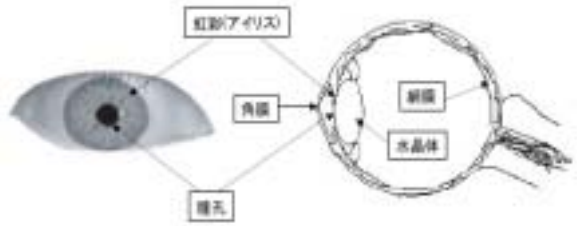

図２．眼の構造

9.2 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。

9.3 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

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

プにおける検討項目が考えられる。

9.4 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

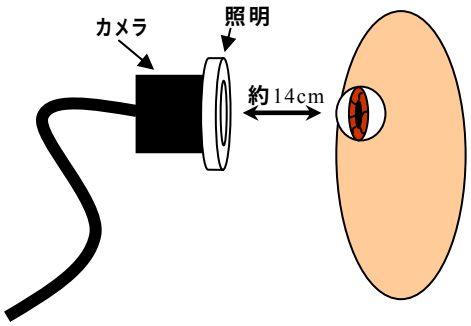

図３．システムsによる撮影方法

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。

9.5 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。

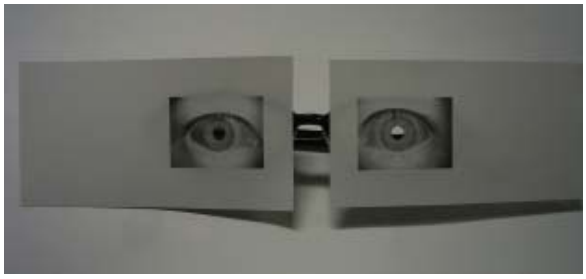

図４．テスト人工虹彩(メガネ貼付型)の例

9.6 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

10. 虹彩認証システムを用いた実験

両眼を用いる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３の様々なテスト人工虹彩を提示して実験を行った[8]。

10. 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。

10. 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。

10. 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－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

11. おわりに

生体認証技術の概念的整理と生体認証システムのセキュリティ評価方法について研究成果を報告した。テスト物体を用いることにより生体認証システムのセキュリティを具体的に計測できる可能性があることを紹介し、テスト物体を開発する際の基礎的事項を虹彩認証システムにより例示した。

参考文献

[1] 日本工業標準調査会,「JIS TR X 0053：指紋認証システムの精度評価方法」, 日本規格協会,2002年.

[2] ――――,「JIS TR X 0072：虹彩認証システムの精度評価方法」, 日本規格協会, 2002年.

[3] ――――,「JIS TR X 0079：血管パターン認証システムの精度評価方法」, 日本規格協会, 2003年.

[4] ――――,「JIS TR X 0086：顔認証システムの精度評価方法」, 日本規格協会, 2003年.

[5] ――――,「JIS TR X 0098：音声認証システムの精度評価方法」, 日本規格協会, 2004年.

[6] ――――,「JIS TR X 0099：署名認証システムの精度評価方法」, 日本規格協会, 2004年.

[7] ――――,「JIS TR X 0100：バイオメトリクス認証システムにおける運用要件の導出指針」, 日本規格協会, 2004年.

[8] 松本 勉, 佐藤健二, “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,” 情報処理学会 コンピュータセキュリティ研究会, CSEC-31, Dec.9, 2005.

[9] 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

[10] 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

[11] 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.

[12] 松本 勉, 平林昌志, “虹彩照合技術の脆弱性評価 (その2),” 情報処理学会 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.

[13] 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),” 電子情報通信学会 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.

[14] 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.

[15] 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.

[16] 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）.

[17] 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

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