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

2006－ＤＳＭ－42／2006－ＱＡＩ－20（１）
2006／7／20

[招待講演]
[Invited Talk]

生体認証システムのニセモノ拒否能力をどう測るか
Measuring Biometric System's Power to Reject Fake Objects

松本　勉

Tsutomu MATSUMOTO

横浜国立大学大学院環境情報研究院

YOKOHAMA NATIONAL UNIVERSITY

〒240-8501 横浜市保土ヶ谷区常盤台 79-7

E-mail: tsutomu@mlab.jks.ynu.ac.jp

あらまし　生体認証システムのセキュリティ（あるいは，そのレベル・クラス）を測定する方法があることが望ましい．なぜなら，これを用いて個別の生体認証システムの設計・実装のセキュリティ目標を客観的に記述することが可能となり，設定されたあるセキュリティ目標に従って設計・実装された実際の生体認証システムが確かにその目標を達成しているかどうかを，セキュリティ測定に基づく試験により客観的に確認することが可能となるからである．一例としてテスト物体を用いた最新のセキュリティ測定方法の研究につき紹介する．

キーワード　生体認証，本人確認，セキュリティ設計，セキュリティ評価，セキュリティ測定，静脈，生体検知

1. 生体認証システムとセキュリティ測定

バイオメトリック認証システム（Biometric System，以下本稿では生体認証システムと記す）は，個人に固有の身体的な特徴や行動的な特徴を用いて機械が個人の認証を行うバイオメトリクスないしバイオメトリック認証技術（Biometrics，以下本稿では生体認証技術と記す）を具現化した個々のシステムのことである．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．ある生体認証システムが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（例えば「指紋」「顔」「虹彩」「静脈」「音声」「手書き署名」など）であるとき，その生体認証システムをＭ認証システムとよぶ．

生体認証システムの利用者，生体認証システムを含む情報システムの構築者や運用者は，生体認証システムに関する技術的ポリシーを設定し，それに見合った生体認証システムを採用することが望ましい．また，生体認証技術の提供者はそれらのニーズに合致した生体認証システムを提供できることが望ましい．これらを合理的かつ効率よく行うためには，利用者，情報システム構築者，運用者，そして生体認証技術の提供者や研究者が，生体認証技術の利点や注意点につき論じるための共通の枠組みを構築することが重要であろう．

セキュリティ面に議論を絞ると，上記の共通の枠組みの整備に当たっては，生体認証技術のセキュリティの特質を明らかにし，どのようなセキュリティのレベル・クラスが存在し，技術的に達成可能な高度なセキュリティレベル・クラスの可能性や注意点を捉えることが重要ではないかと考える．一般にある特定の生体認証システムを設計する際にはセキュリティ面に限らず様々な制約の中での最適化が求められる．セキュリティ設計に当たっては，どのような選択肢が存在するのかをまずは明らかにしておくことが必要であろう．

そのためにはセキュリティ（あるいは，そのレベル・クラス）を測定する方法があることが望ましい．これを用いて個別の生体認証システムの設計・実装のセキュリティ目標を客観的に記述することが可能となり，設定されたあるセキュリティ目標に従って設計・実装された実際の生体認証システムが確かにその目標を達成しているかどうかを，セキュリティ測定に基づく試験により客観的に確認することが可能となる．（図１参照）．

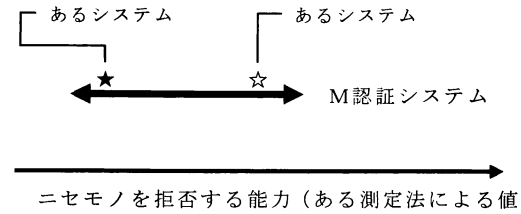


図１．技術的可能性と実際の設計・実装の違い

以下では，生体認証システムを概観した後に，生体認証システムが持つセキュリティ上の脆弱性，とりわけ生体（身体部分）を模擬したニセモノを受け入れる可能性とその本質的なメカニズムを考察し，それを踏まえ，生体認証システムのセキュリティを評価・測定する方法の開発と活用が大切であることを記述する．

2. 生体認証システムの概要

2.1. 生体認証の適用分野

生体認証の適用は，最近になって始まったのではなく，実は長い歴史がある．限定された利用者を対象とする組織において，重要な情報システムでの利用を中心として，一定の利用が古くから行われている．例えば，厳重な警備が必要な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で利用されてきた．

近年の特徴は，生体認証の適用分野が多岐にわたり，適用事例も爆発的に増加の傾向にあることである．具体的には，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，多くの事例を挙げることができる．

また，生体認証技術は，セキュリティ目的だけでなく，ＩＤの自動取得手段などの利便性向上の目的でも様々な適用がなされている．

2.2. 生体認証システムのしくみ

2.2.1. 利用する生体の特徴

生体認証技術において利用される身体的および行動的特徴は，一般に，

①その特徴の種類は誰でも持っている
②本人以外は同一の特徴パターンを有さない
③特徴パターンが時間経過により変化しにくい
④その特徴の測定（読取り）が容易である
⑤受容性：認証への利用が一般に受け入れられる

を満たすことが求められる．

2.2.2. 生体認証システムの構成と働き

生体認証システムは，バイオメトリック情報取得部，固有パターン抽出部，生体検知部，テンプレート生成部，バイオメトリック情報記録部，照合部，登録総合判断部，認証総合判断部などから構成される．

また，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．

1対1照合とは，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方式である．この場合，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，自分のバイオメトリック情報と 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，提示されたバイオメトリック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．

一方，1対n照合では，生体認証システムには利用者の ID なしでバイオメトリック情報だけが提示される．この方式では，生体認証システム側は固有パターンを抽出し，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．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を示す目的で使うこともある．

●指紋認証

指紋（fingerprint）とは，指先の皮膚表面の隆線（盛り上がった部分）と谷（隆線に挟まれた部分）によって形成されるパターンであり（図２参照），

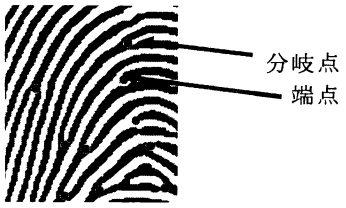


図２．指紋のあらまし

指紋認証は，最もよく用いられている生体認証技術である．代表的な指紋の読取方式を図３と表１に，また，代表的な指紋認証アルゴリズムを表２に示す．

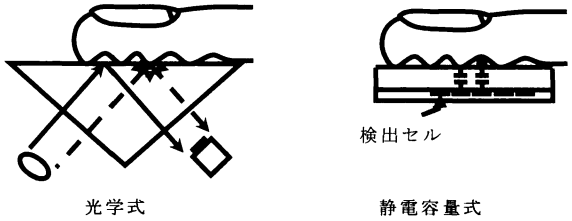


図３．指紋読取方式の例

表１．指紋読取方式の例

方式名	概要
光学式	センサーから指に向かって光を当て，その光の反射率の差によって指紋の隆線・谷のパターンを検出する．
指内散乱光直接読取式	指に光を照射し，指の内部で散乱する光の明暗によって隆線・谷のパターンを検出する．
静電容量式	センサーの電極と指の間に蓄えられる電荷量によって隆線・谷のパターンを検出する．
電界式	センサーから指に向かって電流を流し，発生した電界の強弱によって隆線・谷のパターンを検出する．
感熱式	指からの熱によって隆線・谷のパターンを検出する．
感圧式	指からの圧力によって隆線・谷のパターンを検出する．

表２．指紋認証アルゴリズムの例

方式名	概要
マニューシャ方式	隆線の端点や分岐点である特徴点(マニューシャ)の種類や位置、特徴点から伸びる隆線の方向等を固有パターンとする方式.
マニューシャ・リレーション方式	特徴点に関する情報に加え，特徴点間に存在する隆線の数を固有パターンとする方式.
パターンマッチング方式	読み取った指紋の画像を固有パターンとし，テンプレートの画像との類似度によって一致ないしは不一致の判定を行う方式.
チップマッチング方式	特徴点の位置と，各特徴点の周囲の小画像(チップ画像)を固有パターンとする方式．チップ画像をもとにしてテンプレートと対応する特徴点を特定しその数によって判定を行う.
周波数解析方式	指紋のパターンをある位置で一直線に切り，その断面に現れる隆線・谷のパターンを波形データに変換して固有パターンとする方式．テンプレートの波形データとの相関によって判定を行う.

●虹彩認証

虹彩（アイリス，iris，図４参照）は，黒目と瞳孔に挟まれたドーナツ状の部分のことであり，瞳孔から入る光の量を調節する，カメラでいえば絞りに相当する機能をもつ部分である．虹彩には筋肉によって形成される皺が存在し，その皺のパターンは，人毎に異なり，幼年時にいったん形成されるとその後ほとんど不変であるとされている．

虹彩パターンは，カメラによって撮影された後，虹彩ビット列と呼ばれる特徴量に変換され，固有パターンとして用いられることが多い．虹彩ビット列は，撮像された虹彩をいくつかの領域に分割し，各領域を走査して輝度の抽出を行い，そのデータを一定長のビット列に符号化するという手順で生成されることが多い．

この方式の場合，虹彩ビット列の照合は，登録済みの虹彩ビット列と読み取られた虹彩ビット列との正規化ハミング距離の値を用いて行われる．登録済みの虹彩ビット列（ｍビット）をＡ，認証時に読み取られた虹彩ビット列（ｍビット）をＢとすると，ＡとＢとで一致しないビットの個数をｍで割ったものが，正規化ハミング距離であり，“0”から“1”までの値をとる．照合では，正規化ハミング距離についてあらかじめ判定しきい値が設定され，判定しきい値よりも小さな値が得られた場合には，照合成功と判断される．

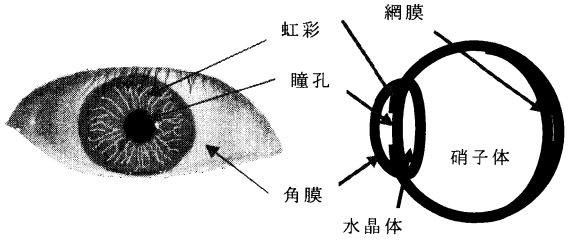


図４．目の構造：虹彩は瞳孔の周りの部分

●静脈認証

手のひら，手の甲，指に現れる静脈パターン（vein pattern）を身体的特徴として利用する生体認証技術がある．静脈を流れる血液中の還元ヘモグロビンが特定波長の近赤外光を吸収しやすいという性質を利用し，当該波長の近赤外線を照射することによって静脈のパターンを浮かび上がらせるという手法が一般的である．静脈パターンの読取には，近赤外線を照射したときの反射光や，近赤外線の透過光が用いられる(図５参照)．

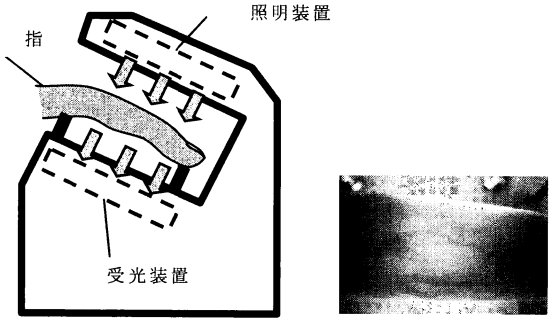


図５．指静脈認証システムの例

固有パターンとその照合方法は，静脈の分岐点や屈折点の位置，および，それらの点間の距離等を固有パターンとして照合・判定する方法や，撮影した静脈パターンの画像において静脈部分とそうでない部分を画素値によって識別する方式など提案されている．その場合，読み取った静脈パターンに対応する固有パターンをテンプレートと比較して，異なる値となる画素値の全体に占める割合に基づいて判定を行う．

2.3. 個人認証の方法としての生体認証の特徴

個人認証の基本的方法には大別して，本人だけが知る情報によるパスワード・質問応答などの技術，本人だけが所持している身分証明証，パスポート，ICカード，携帯電話機などの物による技術，それから生体認証技術がある．これらは組合せて利用することも多い．

生体認証は，パスワードのように記憶する必要がなく，またＩＣカードのように紛失の危険が少なく，極めて便利である．ただし，以下で詳しく説明するように，本人が本人と認められない場合が生じえることや，一定割合で特定のバイオメトリック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，バイオメトリック情報の偽造が困難であることが求められるが，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身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，現実の様々な制約下で作ることが，必ずしもう

まく行えるとは限らない（図１参照）.

さらに，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，たとえば指が人工物によって偽造されたことがわかっても，指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（図６参照）.

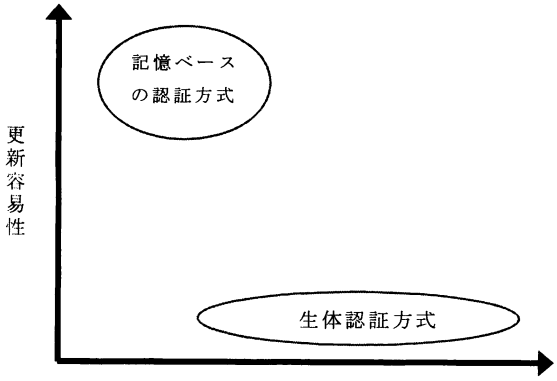


図６．総合的に評価する必要がある

3. 生体認証システムのセキュリティ

3.1. 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，環境の変化などが原因である．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．

また，ある生体の特徴を人によっては登録できない場合もあり，それを表す指標として登録失敗率あるいは対応率が定義されている．FRR や FAR などを生体認証システムの認証精度という．

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 JIS-TR（テクニカルレポート）が作られており（日本工業標準調査会 JIS TR X 0053, JIS TR X 0072, JIS TR X 0079, JIS TR X 0086, JIS TR X 0098, JIS TR X 0099），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．国際標準化機構ＩＳＯにおける精度評価の検討にも一定の貢献をしている．

3.2. 生体認証システムのセキュリティ上の脆弱性

認証精度の問題は，生体認証システムの各構成要素において，そのアルゴリズムや取得データの品質に起因するものといえる．認証精度の問題以外には，第１に，生体認証システムの各構成要素あるいはそれらの間（通信回線を含む）において、各種データの不正な読み出しと書き換え，各種機能の不正な変更などの攻撃が行われる可能性があるというセキュリティ上の問題がある．これは，暗号アルゴリズムを実装した暗号モジュールへの各種実装攻撃に対処しなければならないという問題と同様であり，実装上のセキュリティ要件を整備して対応することにより，この意味でのセキュリティの高い生体認証システムが得られるであろう．

第２に，生体認証システムの入力がニセモノであったときにそれを確実に見破れるか，という問題がある．生体認証システムでは対象とする身体部分を，光などの手段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の“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よう．

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）を対象とする生体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．考察すべき点は，この集合をΦにするように Enroll[S]を作ると Human[M]－Enroll[S]が大きくなる傾向があることである（図７参照）．

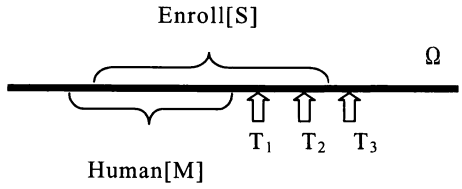


図７．生体認証システムＳとテスト物体Ｔ

3.3. 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はないかと考える．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．

特定の身体部分の代りをする対象物による攻撃のステップと対策のポイントは表３のように整理できる．

表３．攻撃のステップと対策のポイント

攻撃のステップ	対策のポイント
①身体部分に関する情報入手	偽ＡＴＭ等（によるバイオメトリック情報のフィッシング）の排除：利用者への注意喚起が必要（→3.6 節で詳述する）
②対象物の作製	個々の生体認証システムについての事実の把握 生体検知機能の充実：ただし、利便性・コストとのバランスが必要（→3.4 節で詳述する）
③対象物の使用	監視・運用面での対応：ただし、利便性・コストとのバランスが必要

3.4. テスト物体を用いるセキュリティ評価・測定方法

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生体認証システムのセキュリティを評価する際には，表３のステップ②に当たる，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 月から指紋認証システムに関して[2][5]，また 2003 年 7 月から虹彩認証システムに関して[3][6]，さらに 2005 年 3 月から静脈認証システムに関して[4][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．一連の研究から，生体認証システムの開発・製造・試験などの各段階で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．すなわち，各種のテスト物体の組を用意し，セキュリティ測定・評価対象の生体認証システムに対して，テスト物体を登録・照合する実験を行い，テスト物体の作製に要する技術やコストなどと登録・照合実験結果の対照により，結果を分析するといったセキュリティ測定・評価方法である．こうした方法の有効性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．具体的方法としては，次の２段階が考えられる：

第１段階

生体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

生体認証システムに

（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．

ここに，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．身体部分を登録し身体部分で照合する普通の使い方は記号（Ｌ-Ｌ）で表現する．

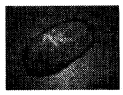
図７に例示される状況はテスト物体 T_1, T_2 について(Ａ)および(Ａ-Ａ)に成功し，テスト物体 T_3 については(Ａ)に（したがって(Ａ-Ａ)にも）失敗したということであるが，生体認証システムＳにテスト物体を提示する実験により集合 Enroll[S]に関する情報が増えたことを示している．よって，適切なテスト物体の組（セット）を揃えることは有益である．

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７のテスト物体 T_3 については実験をせずに（Ｌ-Ａ）が成功しないと言い切ることはできない．

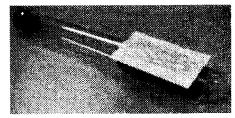
3.5. バイオメトリック・テスト物体の組の整備

テスト物体は有用であるので，テスト物体の組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．

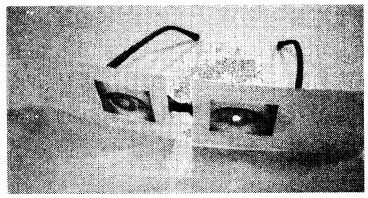
指紋認証についてはテスト物体（テスト人工指）に



ゼラチン製の人工指（指紋）



紙と試験管とビニールテープ製の人工指（静脈）



紙製の人工虹彩

図８．バイオメトリック・テスト物体の例

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（セキュリティの評価基準ではなく読取装置と出力画像の品質の基準である）について規定した日本規格協会作成の標準仕様書(TS X 0101:2005)「指紋読取装置の品質評価方法」の一部分として2005年5月に公表した．

また，虹彩認証システム，静脈認証システムを評価するためのテスト物体の組を開発するための基本的検討事項につき考察をはじめている[6][7][8]．

図８に各種のテスト物体の例サンプルを示す．

3.6. 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測定すればよい．

表３のステップ①で，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測定しなくてもよい場合と，本人の身体部分を直に測定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）を用いた生体認証は後者に分類されるといえるが，後者であっても本人の身体部分を直に測定することが攻撃者にとって困難であるとは限らない．生体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．利用者に対する注意喚起も必要であろう．

4. おわりに

生体認証システムの設計・実装・評価・使用の各段階において，セキュリティ測定が行えることの有用性を述べ，テスト物体の提示によるセキュリティ評価・測定の方法に関する研究を紹介した．第１段階の実験，第２段階の実験というステップ構成でセキュリティ評価を行うことが有益である．この方法により個々の生体認証システムのセキュリティレベルを客観的に測るためには，個々の生体認証技術が対象とする生体部分（モダリティ）毎に，評価・測定のためのテスト物体の組を吟味しその標準化を行うことが重要であろう．

参考文献

[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.

[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.

[3] 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.

[4] 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 18, 2005.

[5] 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).

[6] 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て,”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.

[7] 松本 勉，森下朋樹，李文，“バイオメトリクスにおける生体検知と登録失敗（３）--- 静脈認証システムに関する研究（その２） ---,”電子情報通信学会技術研究報告，ISEC2006-8, May 19, 2006.

[8] 松本 勉，“生体認証システムのセキュリティ設計とセキュリティ測定,”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７回研究会予稿集，pp. 57-64, June 23, 2006.