

# 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

うねまさし まつもと つとむ  
宇根正志 / 松本 勉

## 要 旨

生体認証技術は、指紋や虹彩等の個人特有の生体情報を利用して個人を自動的に認証する技術であり、パスポートをはじめとして幅広い分野において採用されつつある。金融分野においても、銀行窓口やATMでの取引における顧客の本人確認の手段として生体認証技術の導入に踏み切る動きが一部の銀行においてみられている。

生体認証技術の活用の裾野が広がる中で、同技術を実現するシステム（生体認証システム）のセキュリティの確保・維持が一層大きな課題となっている。特に、市販の指紋照合装置や虹彩照合装置の一部において、物理的に偽造された生体情報を誤って受け入れてしまうという脆弱性が存在することを示唆する研究成果が発表されていることから、こうした脆弱性の評価や対策に関する十分な検討が必要となってきた。また、生体認証システムを長期的に運用していく際には、現時点で顕現化していない未知の脆弱性が将来顕現化することも想定し、そうしたケースに適切かつ迅速に対応するための体制整備についても検討しておくことが求められる。

本稿では、生体認証システムの脆弱性に焦点を当てて、身体的特徴の偽造の脆弱性に関する代表的な研究事例を紹介するとともに、そうした脆弱性に対応するためにどのような検討が必要かに関して考察を行う。

キーワード：生体認証技術、脆弱性、セキュリティ

本稿は、2005年3月29日に日本銀行で開催された「第7回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている内容および意見は、日本銀行あるいは金融研究所の公式見解を示すものではない。また、ありうべき誤りは、すべて筆者たち個人に属する。

宇根正志 日本銀行金融研究所情報技術研究センター（E-mail: masashi.une@boj.or.jp）  
松本 勉 横浜国立大学大学院環境情報研究院（E-mail: tsutomu@mlab.jks.ynu.ac.jp）

## 1 . はじめに

電子商取引や各種の電子的な手続における本人確認の手段として、生体認証技術（バイオメトリクス biometrics と呼ばれることも多い）を活用する動きが広がっている。生体認証技術は、身体的な特徴や行動的な特徴等、各個人に固有の特徴を用いて個人の認証を自動的に行う技術であり、「各個人に固有の特徴」の代表例として、指紋、虹彩、顔、動的署名、声紋が挙げられる。従来、生体認証技術は、セキュリティ・レベルが相対的に高いエリアへの入室管理、サーバやパソコンにおけるアクセス管理等、利用者がある程度限定される比較的狭い範囲（例えば、個々の企業の情報システム）において利用されるケースが中心となっていた。しかし、最近では、空港等における入国審査時の本人確認手段として採用される公算が高いとみられているほか、銀行窓口やATMにおける顧客の本人確認の手段としても生体認証技術を採用する動きがみられるなど、その利用の裾野が広がってきている。特に金融分野においては、キャッシュカードの偽造に対抗する手段の1つとして生体認証技術が注目を集めている（金融庁[2005b]、全国銀行協会[2005]）。

こうした状況を踏まえると、今後、生体認証技術を実現するシステムや装置（以下、生体認証システムと呼ぶ）のセキュリティをどのように確保し、維持していくかという課題が一層大きなものになっていくと考えられる。生体認証システムの導入を検討する際には、その時点で入手可能な最先端の技術情報を参照しつつ、導入対象のアプリケーションにおいて想定される脅威を明確にするとともに、当該システムにおける脆弱性の有無とその影響度合いについて分析することがまず必要となる。こうした分析結果を踏まえ、どのような種類の生体情報を用いたシステムとするか、照合アルゴリズムとして何を採用するか、判定しきい値等のセキュリティ・パラメータをどう設定するか等について検討を行い、コスト等の他の要素も考慮しながらシステムの詳細な仕様を決定することとなる。生体認証技術自体の分析に加えて、生体認証システム全体として十分なセキュリティ・レベルを確保しているか否かの確認も行うことが求められる。

生体認証システムにおいて想定される各種の脆弱性の中でも、物理的に偽造された生体情報を受け入れてしまうというタイプの脆弱性の評価が特に重要と考えられる。このタイプの脆弱性の評価についてはこれまで公表されている研究成果が少なく、評価方法の確立までには至っていないが、その一方で、市販されている指紋照合装置や虹彩照合装置において生体情報の偽造による脆弱性が深刻なものとなっている実情を示す研究結果が報告されている<sup>1</sup>。筆者の1人である松本の研究チームでは、比較的入手が容易な材料や機器を用いて指紋や虹彩を物理的に偽造する手法について検討するとともに、実際に市販されている指紋照合装置（19

1 本稿のメインパートは2005年3月15日の時点で入手可能な情報をベースとして執筆しており、指の静脈パターンを利用した認証方式における脆弱性については触れていない。ただし、メインパート執筆後、こうした静脈パターンの照合装置の脆弱性を指摘する重要な研究成果（松本ほか[2005a, b]）が発表されている。

機種)や虹彩照合装置(3機種)に偽造した特徴が受け入れられるか否かを実証した。研究結果は、偽造した指紋や虹彩がいくつかの装置において比較的高い確率で受け入れられたというものであり、特に指紋に関しては、コップや携帯電話といった媒体上の残留指紋からもいくつかの指紋照合装置に受け入れられる指紋を偽造することが可能であるとしている。一連の研究成果は、偽造された生体情報を受け入れてしまうという脆弱性に関する評価研究を今後活発化し、こうした脆弱性を軽減する手段について検討していくことが重要であることを示している。例えば、こうした手段の1つとして、生体検知機能(生体情報が生きた人間によって提示されているものであることを確認する機能)が挙げられる。

こうした脆弱性に関する分析を十分に行い、その結果を考慮して設計された生体認証システムは、導入当初は想定したセキュリティ・レベルを達成していると期待することができる。しかしながら、そうした状態を長期間維持するためにはこれだけでは十分とは言えない。生体認証システムの設計段階では「考慮する必要はない」と考えられていた、あるいは、考慮すらされていなかった脆弱性が、技術革新やその他の環境変化によって顕現化し、深刻な影響を引き起こす可能性がある。その結果、当該システムのセキュリティ・レベルが低下し、十分な対策が講じられるまでの間に当該脆弱性を突いた攻撃にさらされるという事態に陥る可能性がある。また、当該システムを利用している顧客からのレピュテーションが低下するおそれもある。

新たな脆弱性が発見された場合であっても生体認証システムのセキュリティ・レベルを可能な限り維持するためには、脆弱性に関する最新情報を正確かつ迅速に収集したうえで、現行システムへの影響について分析し、必要な対策を講じる必要がある。現行システムにおいて問題となっている要素技術や装置を安全なものに取り替えるといった対応が可能となるように、生体認証システムにあらかじめ拡張性を持たせておくことも有用であろう。また、脆弱性に対応するための体制が整備され、適切に運用されていることを顧客等に適切なタイミングで説明することは、サービスに対する信頼性の維持という意味で望ましい。今後、生体認証技術の活用を検討するに当たっては、こうした体制の整備について検討を行うことが求められる。

本稿の構成は以下のとおりである。まず、2節において、生体認証技術の概要、利用される生体情報の種類、生体認証システムの構成、関連する標準規格やガイドラインの策定動向等について紹介する。3節では、生体認証システムに対する脅威や脆弱性としてどのようなものが想定されるかについて既存の検討結果を紹介したうえで、脆弱性の中でも、物理的に偽造した生体情報を生体認証システムが受け入れてしまうという脆弱性に関してまず検討を行う必要があることを示す。4節では、生体情報の物理的偽造の脆弱性を評価したいいくつかの研究を紹介したうえで、代表的な研究結果として、筆者の1人である松本の研究チームによる指紋照合装置と虹彩照合装置における脆弱性評価研究の内容を紹介する。こうした研究結果を踏まえ、5節では、生体認証システムを今後安全に活用していくうえで脆弱性に対してどのように対処していけばよいかに関して考察を行い、具体的な検討項目を提示する。6節では、本稿における考察結果を整理して本稿を締めくくる。

## 2. 生体認証技術に関する標準化と金融分野における活用

### (1) 生体認証技術と認証の形態

#### イ. 生体認証技術とは

生体認証技術は、身体的特徴や行動的特徴等、各個人に固有の特徴を用いて個人の認証を行う技術であり、近年では、バイオメトリクス、あるいは、バイオメトリック個人認証技術と呼ばれるケースも多い<sup>2</sup>。上記の定義のもとでは、専門家による筆跡鑑定や指紋照合等も生体認証技術に含まれると考えられる。ただし、最近広く議論の対象となっているのは情報システムにおけるアクセス管理等のセキュリティ機能を提供するものであり、被認証者によって認証のために提示されるアナログ情報（以下、生体情報と呼ぶ）等を機械によって読み取り、生体情報から抽出されたデータ（以下、固有パターンと呼ぶ）に基づいて自動的に本人確認の処理を実行するという形態の技術である。本稿においても、機械を用いた自動処理を行う生体認証技術に焦点を当てて議論することとする。

#### ロ. 身体的および行動的特徴

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に求められる特性として、次の5項目が挙げられるケースが多い（例えば、小松 [2004]、瀬戸 [2002]、Bolle *et al.* [2003]）。

普遍性（universality：その特徴を誰もが有していること）

唯一性（uniqueness：本人以外は同一の特徴を有していないこと）

永続性（permanence：時間の経過とともに変化しにくい特徴であること）

収集可能性（collectability：その特徴をセンサ等によって容易に読取可能であること）

受容性（acceptability：その特徴を認証に利用することが一般に抵抗なく受け入れられるものであること）

こうした特性を備えた特徴とその利用方法に関しては、これまでに膨大な研究の蓄積があり、数多くの文献において整理・紹介されている（例えば、情報処理推進機構 [2004]、瀬戸 [2002, 2003]、Bolle *et al.* [2003]）。こうした文献においては、代表的な身体的特徴として、指紋、掌形、顔、虹彩、網膜、血管パターン、耳形状、DNA等が挙げられているほか、代表的な行動的特徴としては、声紋、動的署名、キー・ストローク、歩行パターン等が挙げられている。指紋、虹彩、血管パターン、顔、声紋、動的署名に関しては、これらを活用した生体認証システムの精度評価方法に関する日本工業標準・標準情報（JIS TR）が既に策定されている（日本工業標準調査会 [2002a, b, 2003a, b, 2004a, b, c]）。複数種類の特徴を組み合わせることで認証に

<sup>2</sup> バイオメトリクスという用語は、指紋や虹彩等、認証に利用される身体的あるいは行動的特徴そのものを指す場合もある。

利用するケースもあり、そうした認証はマルチモーダル（multi-modal）認証と呼ばれる。

金融分野における生体認証技術の利用の現状に関しては、金融情報システムセンター（FISC）が平成16年3月に実施した金融機関（回答数471）を対象としたアンケート結果から垣間みることができる。生体認証技術に関して、「導入済」、「平成16年度導入予定」、「検討中」のいずれかの回答を行った金融機関の割合をみると、指紋（14.5%）、静脈パターン（10.5%）、虹彩（3.6%）が上位を占める結果となっている（FISC [2004]）。これらの身体的特徴に関しては、金融機関の注目を相対的に集めているものということから、本節(1)ホ．においてやや詳しく説明する。

## ハ．認証の形態

### (イ) 1対1照合と1対 $n$ 照合

認証の形態には、1対1照合（verification）と1対 $n$ 照合（identification）の2種類がある。1対1照合は、生体認証システムに提示された身体的あるいは行動的特徴の持ち主があらかじめ識別された個人であるか否かを確認するというものである。この場合、生体認証システムの利用者は、自分の身体的あるいは行動的特徴を反映した固有パターンを、その利用者を識別するための情報（以下、個人識別IDと呼ぶ）とともに当該システムにあらかじめ登録しておくことになる。固有パターンや個人識別ID等は利用者ごとに1つのデータ・セットとして保管されることが多く、そうしたデータ・セットはテンプレートと呼ばれる。認証時には、被認証者となる利用者は、自分の生体情報とともに個人識別ID等を生体認証システムに提示する。生体認証システム側では、提示された生体情報から固有パターンが抽出され、個人識別IDに対応して登録されているテンプレートの固有パターンと照合される。

1対 $n$ 照合は、個人識別IDを提示することなく、生体認証システムが抽出した固有パターンが（ $n$ 人の候補のうち）どの利用者のものかを照合・識別するというものである。生体認証システムの利用者は、自分の固有パターンを個人識別IDとともにあらかじめ当該システムに登録しておき、認証時には、生体認証システムに生体情報のみが提示され、それに対応する固有パターンが候補となるテンプレートの固有パターンと順次照合されることとなる。一致すると判断される固有パターンが存在する場合には、照合結果として、そのテンプレートに紐付けされている個人識別IDが出力されるケースが多い。また、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上記と同様の手続で確認するものはネガティブ識別と呼ばれるが、これも1対 $n$ 照合の一種と位置づけることができる。

### (ロ) 生体を特定するレベル

生体認証を行う際に生体をどのレベルまで特定して認証するかという観点からは、個人を特定して認証するケースと、個人まで特定することはなく、その個人が属するグループを特定して認証するケースに分けられる。

個人まで特定して認証するケースとしては、例えば、銀行のATMにおいて利用

者から静脈パターンと預金口座情報が提示され、その利用者が当該預金口座の持ち主であるか否かを確認するという場合が考えられる。また、どのグループに属するかまでを特定して認証するケースとしては、犯罪捜査において、現場に残された血痕から容疑者等の関係者の血液型を特定するという場合が例として挙げられる。

金融分野をはじめとして活用の範囲が今後広がるとみられている生体認証技術は、どの個人かを特定して認証するという形態が中心となっている。そこで、以下でも、どの個人であるかを特定して認証するケースに焦点を当てることとする。

#### (八) 生体検知

生体認証システムにおいては、身体的あるいは行動的特徴の照合だけでなく、生体情報が生きた人間の身体から直接提示されているか否かを確認する機能（以下、生体検知機能と呼ぶ）を利用して認証を行うケースがある。生体検知機能の実現方法は、認証時に用いられる生体情報に依存し、多種多様な手法が提案されている。具体的な手法に関しては、Schuckers [ 2002 ]、Valencia and Horn [ 2003 ]、Sandström [ 2004 ]、Daugman [ 2004b ] といった文献において紹介されている。ただし、市販されている生体認証システムにおいて実際にどのような手法が採用されているかについては、公開されていないケースが少なくない（IBG [ 2003 ]）。

生体検知機能の実現方法はいろいろな観点から分類することができる。ここでは、生体情報読取用のセンサのみで実現するか否かという観点から次の2つに分類して説明する（Schuckers [ 2002 ]）<sup>3</sup>。

- ・生体情報読取用のセンサのみで実現する方法（固有パターンを生成するために読み取った生体情報を別途処理・加工し、その結果得られるデータを基にして生体か否かを確認する）

本分類に含まれる手法として、例えば、指紋照合時における指紋画像の色の变化を利用するという手法（藤枝・松山・田口 [ 2003 ]）が提案されている。その他の代表的な手法として、Schuckers [ 2002 ] において、指紋照合時における汗腺からの発汗に伴う生体情報の变化を利用するもの、顔画像の照合時における頭部の動きや顔の3次元画像を利用するものが紹介されている。また、虹彩に関しては、照合時における瞳孔の動きを利用するという手法がDaugman [ 2004b ] において紹介されている。

- ・生体情報読取用のセンサとは別に、生体検知のためのデータを得るセンサを用いて実現する方法

本分類に含まれる手法として、例えば指紋の場合、指先の脈拍、光の吸収率の変化量等を計測するセンサを用いる手法がValencia and Horn [ 2003 ] におい

3 このほか、(1)生体に固有の性質（例えば、皮膚における光の吸収・反射、色の变化）を利用するもの、(2)生体から自然に発せられる情報（例えば、脈拍、体温）を利用するもの、(3)外部からの刺激に応じて生体から発せられる情報（例えば、光に対する瞳孔の変化）を利用するものに分類して議論されるケースもある（Valencia and Horn [ 2003 ] ほか）。

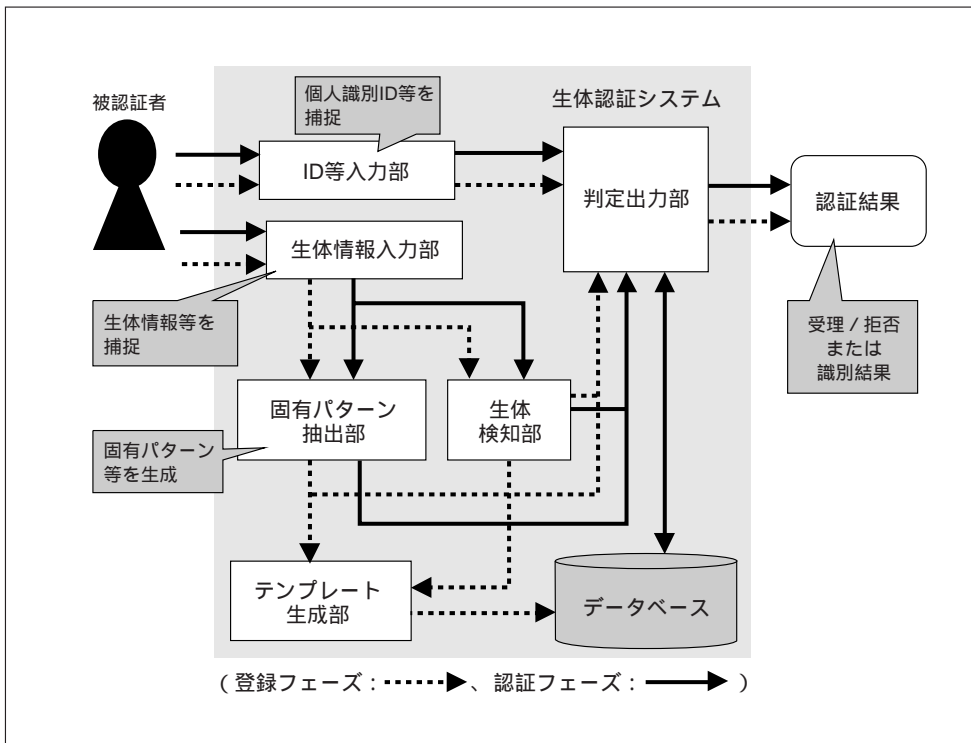
て紹介されている。顔画像の場合には、Schuckers [ 2002 ] において、温度センサによって読み取った顔表面の温度とその変化、あるいは、音声センサによって読み取った音声データが顔や唇の動きと整合的か否かを判断する手法等が紹介されている。虹彩の場合には、角膜や水晶体からの反射光を用いる方法や、網膜に反射した光によって目が赤くなって見える現象 ( red eye effect ) を用いる方法等がDaugman [ 2004b ] において紹介されている。

こうした生体検知機能は、生体認証を行う際に生体情報を偽造するといった攻撃を排除するうえで重要な役割を果たすと期待される。ただし、生体情報を読み取るセンサの高度化や別のセンサの設置等が必要となるほか、処理時間が長くなる可能性もあり、利便性やコストの面でマイナス要因となる場合がある。

## 二．生体認証システムの構成

生体認証システムは、一般に、生体情報入力部、ID等入力部、固有パターン抽出部、テンプレート生成部、生体検知部、判定出力部、データベースから構成される ( 図1参照 ) 。登録と認証はそれぞれ次の手順で実行される。

図1 生体認証システムの構成 ( 概念図 )



## 【登録フェーズ】

- ・登録対象となる被認証者の個人識別ID等を捕捉する（ID等入力部）。
- ・被認証者から生体情報を捕捉する（生体情報入力部）。また、生体検知機能が準備されている場合には、それに必要な情報も捕捉する。生体検知機能を捕捉するセンサが生体情報を捕捉するものと異なる場合もある。
- ・生体情報から、被認証者の身体的あるいは行動的特徴を反映した固有パターンを抽出する（固有パターン抽出部）。
- ・生体検知機能を備えている場合、捕捉したデータから生体であるか否かの確認を行う（生体検知部）。
- ・抽出された固有パターンの品質を検査するとともに、生体検知の結果から、登録の可否を判定する（判定出力部）。生体検知が成功しても、固有パターンの品質があらかじめ設定されたレベルを下回る場合、生体情報の捕捉、特徴の抽出を再度行う場合がある。
- ・固有パターンや個人識別ID等からテンプレートを生成し、データベース等に登録する（テンプレート生成部）。

## 【認証フェーズ】

- ・1対1照合の場合には、被認証者となる利用者の個人識別ID等を捕捉する（ID等入力部）。1対 $n$ 照合の場合には、個人識別IDを入力しない。
- ・被認証者から生体情報を捕捉する（生体情報入力部）。また、生体検知機能が準備されている場合には、それに必要な情報も捕捉する。生体検知機能を捕捉するセンサが生体情報を捕捉するものと異なる場合もある。
- ・生体情報から、被認証者の身体的あるいは行動的特徴を反映した固有パターンを抽出する（固有パターン抽出部）。
- ・生体検知機能を備えている場合、捕捉したデータから生体であるか否かの確認を行う（生体検知部）。
- ・1対1照合の場合には、個人識別IDに対応するテンプレートがデータベースから抽出され、生体情報から抽出した固有パターンと比較される。両者がどの程度一致するかを表す値を生成し、あらかじめ設定されていた判定しきい値と比較して一致か不一致かを出力する（判定出力部）。1対 $n$ 照合の場合、データベースのテンプレートと順次比較し、一致と判定する場合には個人識別IDも出力するケースがある。

ホ．主な身体的特徴：指紋・静脈パターン・虹彩

金融分野において比較的注目を集めている指紋、静脈パターン、虹彩を取り上げ、主な生体情報読取方式と固有パターン抽出方式の概要を紹介する。

### （イ）指紋

指紋は、生体認証技術において用いられる身体的特徴の中で最もよく知られてお

り、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る。既存の指紋照合装置において採用されている指紋の読取方式や固有パターンの抽出方式に関しては、瀬戸 [ 2002, 2003 ] をはじめとする各種文献において整理されている。ここではこれらの参考文献で紹介されている方式と、5節で紹介する実験の対象となっている指紋照合装置で実装されている方式を取り上げ、その概要を表1、2にまとめて紹介するにとどめる。

表1 指紋の読取方式

方式	概要
光学式	センサ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方式。
静電容量式	センサの電極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方式。隆線の部分に接する電極には比較的多くの電荷が蓄えられる。
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方式。隆線の部分が相対的に明るくなる。
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方式。
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方式。
エレクトリック・フィールド式	センサ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方式。

表2 指紋の固有パターン抽出方式

方式	概要
マニューシャ方式	隆線の端点や分岐点等を特徴点（マニューシャ）と呼び、特徴点の種類や位置、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。特徴点の情報をテンプレートと照合して一致しないしは不一致の判定を行う。
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。照合・判定時に、隆線数によって特徴点をより高い精度で特定することを可能にするといわれている。特徴点とリレーション方式と呼ばれることもある。
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し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。チップ画像を基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。テンプレートに保管される波形データとの相関度によって判定を行う。

#### (ロ) 静脈パターン

身体的特徴として静脈パターンを利用する場合、手のひら、手の甲、指に現れるものを利用する技術が提案されている。そうした技術の1つとして、森・新崎・佐々木 [2003] や楠山 [2004] においては、静脈を流れる血液中の還元ヘモグロビンが特定波長（約760ナノメートル）の光を吸収しやすいという性質を利用し、当該周波数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紹介されている。また、静脈パターンの読取方法としては、近赤外線を照射して得られる反射光を撮影する方式（森・新崎・佐々木 [2003]）やその透過光から静脈パターンを撮影して読み取る方式（三浦・長坂・宮武 [2003]）が提案されている。

固有パターンとその照合方法に関しては、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・判定する方式が楠山 [2004] において紹介されている。また、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も提案されている（三浦・長坂・宮武 [2003]）。この場合、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。

#### (ハ) 虹彩

虹彩（アイリス iris と呼ばれることもある）は、黒目の内側で瞳孔よりも外側に位置するドーナツ状の部分のことであり、瞳孔を開閉する機能を持つ（瀬戸 [2002]）。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、各個人によって異なり、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いわれている。虹彩を利用した生体認証は、この筋肉の皺のパターンによって個人を認証するというアイデアに基づいている。

虹彩における筋肉の皺のパターンは、デジタル・カメラ等によって撮影された後、虹彩ビット列（iris code）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ケースが一般的である（瀬戸 [2002]、Daugman [2004a]）。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たうえで、各領域を走査してイメージ輝度の抽出を行い、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（Daugman [2004a]）。

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によって行われる（Daugman [2004a]）。登録済みの虹彩ビット列を  $(A_1, A_2, \dots, A_n)$ 、認証時に読取りされた虹彩ビット列を  $(B_1, B_2, \dots, B_n)$  とすると（ $n$  はビット列のサイズ）、正規化ハミング距離  $HD$  は次のように表される。ただし、数式中の“ $\oplus$ ” は排他的論理和演算を意味する。

$$HD = \left(\frac{1}{n}\right) \sum_{j=1}^n (A_j \oplus B_j)$$

正規化ハミング距離は、値が一致しないビットの個数の全体に占める割合を表すものであり、登録済みの虹彩ビット列と同一のものが提示されると“0”、どのビット値も一致しないものが提示されると“1”となる。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。

## (2) 標準・ガイドライン等の策定に関する活動

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おり、それらを整理・紹介する文献も数多く存在する（例えば、瀬戸 [2002, 2003]、情報処理推進機構 [2004]、小松 [2004]、小松ほか [2003]、FISC [2005]）。本稿では生体認証技術におけるセキュリティ評価や脆弱性に焦点を当てていることから、これらに関連するものに絞って最近の動向を紹介する。

### イ．ISO関連

ISOにおいては、TC68（金融サービス）のほか、JTC1傘下のSC27（セキュリティ技術）、SC37（バイオメトリクス）が生体認証技術におけるセキュリティ評価に関連する標準案の審議を行っている<sup>4</sup>。

まず、TC68では、生体認証技術の標準化を担当しているSC2/WG10が、米国の国内標準であるANS X9.84をベースとして、金融分野において利用される生体認証技術に関する国際標準案ISO 19092（バイオメトリクス）の審議を2003年に開始している（日本銀行金融研究所 [2004a, b]、ANSI [2003]）。ANS X9.84は、瀬戸 [2003] 4章においても整理されているように、主な生体認証技術の概要、生体認証システムのモデル、セキュリティ要件、テンプレートの形式、対処すべき脅威の種類等を規定している。本稿の4節で取り上げる生体情報の物理的な偽造に関しても「付録E（参考）セキュリティ上考慮すべき事項」において触れられており、生体検知機能の採用、端末の監視といった対策例が紹介されている。

SC27においては、2004年より、傘下の3つのワーキング・グループ（WG）がそれぞれ異なるスコープに沿って生体認証技術のセキュリティに関する標準化の審議を行っている（宝木 [2004]）。WG1（情報セキュリティ要求条件と統合技術）ではセキュリティ・マネジメントの観点から、WG2（セキュリティ技術とメカニズム）では生体情報を用いた認証方式という観点から、WG3（セキュリティ評価基準）ではセキュリティ評価とテストという観点から、それぞれ標準化に関する検討が開始されている。当初WG3は、標準案ISO 19792（バイオメトリック技術のため

4 JTC1傘下のSC17においても、電子パスポートや運転免許証への生体認証技術の実装に関する標準化の審議が行われている（林 [2004]、ICAO [2004]）。ただし、これらの標準化では、ICカード等の物理特性、論理データ構造、通信方式等が主たる標準化のスコープとなっており、セキュリティの観点とは異なるため、ここでは説明を割愛する。

のセキュリティ評価およびテストに関するフレームワーク)の検討を2003年から開始していた。ISO 19792は、コモン・クライテリア(Common Criteria)の枠組みに基づいて生体認証システムのセキュリティ評価を行う際に留意すべき脅威やセキュリティ保証要件等を内容とするBEM(Biometric Evaluation Methodology、CCBEMWG[2003])を含むものであった。しかし、WG3では、BEMの検討はコモン・クライテリアの維持・管理を行っているCCDB(Common Criteria Development Board)において行うことが望ましいとの結論に至り、BEMを除いた新たなISO 19792の検討が2004年より開始されたという経緯がある。

汎用的な生体認証技術の標準化を担当するSC37では、「バイオメトリック技術の試験および報告」をスコープとするWG5において、精度評価の方法・手順を規定する標準案ISO 19795(バイオメトリクス技術の性能評価と報告)の審議が2002年より進められている(瀬戸[2004a, b])。本標準案の審議に当たっては、英国のバイオメトリック・ワーキング・グループ(Biometric Working Group)が策定した精度評価方法のガイドライン“Best Practices in Testing and Reporting Performance of Biometric Devices”(Mansfield and Wayman[2002])を参考にしているほか、わが国の標準情報(JIS TR)として策定済みの精度評価方法等も盛り込まれるとみられている(小松ほか[2003]、瀬戸[2004a])。セキュリティ評価とも関連する誤合致率(false match rate)<sup>5</sup>や誤受入率(false acceptance rate)<sup>6</sup>の精度評価指標の試験方法や報告方法等が規定される見通しである。

## ロ．JIS関連

わが国では、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が既に策定されている(日本工業標準調査会[2002a, b, 2003a, b, 2004a, b]、小松ほか[2003])。いずれのTRにおいても、生体情報の読取方法や固有パターンの生成・照合方法について具体的な方法を前提としているわけではなく、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のみである。

指紋、虹彩、血管パターンを用いた認証については、誤合致率や誤受入率等の指標のほか、照合精度特性としてROC(receiver operating characteristic)曲線<sup>7</sup>を評価

5 固有パターンの照合アルゴリズムが、異なる個人から提示された生体情報の固有パターンを1回照合し、不一致と判定すべきところを誤って一致と判定してしまう確率。ただし、何らかの手段によって偽造された生体情報が提示されるケースを想定しないで計測される場合が一般的である。なお、誤非合致率(false non-match rate)は、一致と判定すべきところを誤って不一致と判定してしまう確率である。

6 生体認証システムが、異なる個人から提示された生体情報の固有パターンを照合し、拒否すべきところを誤って受け入れてしまう確率。なお、誤拒否率(false rejection rate)は、受け入れるべきところを誤って拒否してしまう確率である。

7 誤非合致率と誤合致率、あるいは、誤拒否率と誤受入率を任意の判定しきい値のもとでプロットしたグラフであり、認証精度の表示方法として一般的に利用されている。

環境とともに精度評価レポートに記述することが求められている。同じ身体的特徴ではあるが照明条件等によって影響を受けやすい顔認証の場合には、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、発声する内容をどのように決定するかによって認証方式のバリエーションが考慮されている。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、筆跡の模倣のレベルを4段階に分類したうえでどのレベルを想定しているかを評価レポートに明記することを要求している。

また、INSTACにおいて検討された「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」もJIS TR X 0100として2004年に刊行されている（日本工業標準調査会 [ 2004c ]）。本標準情報は、生体認証システムを採用したいと考えている利用者がシステムの運用時に設定すべき要件（誤受入率、誤拒否率等の指標を含む）を決定し、当該要件を満足する生体認証システムを絞り込む方法を記述している。要件の決定プロセスとして、生体認証システムのモデルの分類、システムに求められる各種機能（未対応の可否、登録・認証処理に必要な時間、誤拒否率の許容度等）の明確化、誤受入率の明確化、要件間の優先順位の明確化が記述されており、利用者は上記プロセスの結果明らかとなった情報を生体認証システムの採用を判断する際に用いる仕組みとなっている。ただし、生体認証システムに対する脅威として、攻撃者が自分の生体情報を提示して行う攻撃のみを想定しており、生体情報の偽造による攻撃は想定外としている<sup>8</sup>。本標準情報には、いくつかの要件導出に関する具体例も記述されており、銀行のATMに生体認証システムを導入する場合への適用例も説明されている。

## 八．コモン・クライテリア関連

生体認証システムは情報システム、あるいは、その一部としてみなすことが可能であり、生体認証システムのセキュリティ評価をコモン・クライテリアの枠組みに沿って実施することが考えられる。こうしたアイデアに基づいてセキュリティ評価を行うための検討も進められており、代表的な成果物として、BEMのほかに、英国政府や米国政府によって作成・公表された生体認証システム向けのセキュリティ要件仕様書（protection profile）が挙げられる（UKGBWG [ 2001 ]、BMO/NSA [ 2003 ]）。

.....  
 8 本標準情報では、「これら（生体情報を偽造する攻撃）はバイオメトリクス認証のぜい（脆）弱性と密接な関係があり、この種的不正アクセスには一般的な誤受入率を適用できないことが多い。ベンダは、この様なぜい弱性に関する情報をシステム管理者又はシステムインテグレータに対して積極的に開示し、システム管理者又はシステムインテグレータ側もベンダに対して情報提供を求めることを推奨する」と記述されている。

英国政府作成のセキュリティ要求仕様書は、汎用向けの生体認証システムを対象としたものであり、評価保証レベル ( evaluation assurance level ) 1 ~ 4 に対応するセキュリティ保証要件が記述されている。また、なりすましやサービス妨害を目的とした脅威として18項目が挙げられており、人工物を利用して生体情報を偽造し、他者になりすますという攻撃も含まれている。これに対応して、偽造された生体情報を検知・排除する手段を準備する旨のセキュリティ対策方針が記述されている。本要求仕様書の内容については、瀬戸 [ 2003 ] において詳細に説明されている。

米国政府のセキュリティ要求仕様書は、国防総省の下部組織であるバイオメトリクス管理局 ( Biometrics Management Office ) と国家安全保障局 ( National Security Agency ) によって作成されたものであり、米国政府内で採用される生体認証システムのうち、中位の堅牢性 ( medium robustness )<sup>9</sup>が求められる1対1照合タイプのものを対象としている。本要求仕様書では、生体認証システムの初期設定ミス、設定変更に伴う未知の問題の発生等、21項目の脅威が想定されており、これらの中には、英国政府のセキュリティ要求仕様書と同様に、人工物 ( artifact ) を使った生体情報の高度な偽造も含まれている。また、セキュリティ対策方針には、人工物を用いた生体情報の偽造に対抗するための手段の採用に関する項目が含まれており、その手段として生体検知機能の搭載が要求されている。本要求仕様書では、評価保証レベル4に対応する生体認証システムが対象とされており、セキュリティ保証要件においては、脆弱性分析テストの実施および結果報告に関する要件が準備されている。

こうしたセキュリティ要件仕様書等を作成する、あるいは、生体認証システムのセキュリティ評価を行う際に、参考にすることができるガイダンスとして作成されたのがBEMである。BEMは、まず、生体認証システムに特有の脅威として45項目を列挙しており、人工物によって生体情報を偽造し、なりすましを行うという攻撃も含まれている。また、セキュリティ要求仕様書やセキュリティ設計仕様書 ( security target ) において記述されるセキュリティ保証要件のうち、開発 ( ADV )、ガイダンス文書 ( AGD )、テスト ( ATE )、脆弱性評価 ( AVA ) の4項目を検討したり評価したりする場合に生体認証技術の特性を踏まえた配慮が必要であるとしている。例えば、脆弱性評価の中でも機能強度 ( strength of function ) の項目 ( AVA\_SOF ) に関しては、機能強度を「被認証者を正確に認証する性能」と定義したうえで、機能強度の尺度として誤受入率や誤拒否率を用いることができるとしている。また、脆弱性分析 ( AVA\_VLA ) の内容を検討するに当たっては、45項目に

9 堅牢性のレベルは、保護の対象となる情報 ( 生体認証システムによってアクセスの可否が決定されるもの ) の価値の大小、被認証者の信頼度、想定される脅威等によって総合的に決められると記述されているものの、どのようなアプリケーションが想定されているかについて明確な説明がない ( BMO/NSA [ 2003 ] )。中位の堅牢性が要求されるケースについては、情報価値や被認証者の信頼度が相対的にみて中庸と判断される場合といった主旨の説明にとどまっており、軍事関連の情報システムといった極めて高度なセキュリティが求められるケースではないが、政府部門の基幹となる情報システムへのアクセス制御に用いられるケース等が想定されていると考えられる。

整理された一般的な脅威の中でどれを実際に想定すべきかについて十分に考慮しなければならない旨を明記しており、具体例として人工指 (artificial finger) を用いた攻撃について触れ、指紋を使った生体認証システムを評価する場合にはこうした攻撃を想定した評価試験を行う必要があるとしている。

## 二．その他の動向

以上のほか、生体認証システムの脆弱性評価に関連する検討の成果として、日本バイオメトリクス認証協議会 (JBAA) の「バイオメトリクスシステムの脆弱性に関する報告書」が挙げられる (JBAA [2003])。本報告書では、一般的な生体認証システムのモデルを定義したうえで、生体認証システムに特有の脅威 (36項目) と脆弱性 (16項目) を抽出・列挙し、両者の関係を明確化している。これらの脅威や脆弱性については、3節において改めて詳しく説明する。

### (3) わが国の金融分野における動向

生体認証技術の金融分野における活用に関しては、従来から、一部の銀行において事務センター等における職員の入退室管理等の手段として指紋認証技術等が採用されていた。こうした状況に加えて、最近では、銀行の窓口やATMにおける顧客の本人確認の手段として静脈認証技術が採用されるといった事例もみられ、生体認証技術が活用される場面が増えてきている (中山・小松 [2000])。金融分野での生体認証技術の動向については、金融情報システムセンターによるアンケート調査や調査報告において具体例を交えつつ紹介されている (FISC [2004, 2005])。以下では、金融分野における生体認証技術の活用例の中でも、顧客向けサービスへの適用をスタートしているという意味で最近注目を集めているものとして、手のひらの静脈パターンを用いた生体認証技術を採用しているスルガ銀行と東京三菱銀行の事例を紹介する<sup>10</sup>。

また、本年4月に施行された「個人情報保護に関する法律」に先立ち、金融庁が、「金融分野における個人情報の保護に関するガイドライン」(以下、単にガイドラインと呼ぶ、金融庁 [2004]) を2004年末に公表したほか、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」(以下、単に実務指針と呼ぶ、金融庁 [2005a]) を本年初めに公表しており、金融サービスにおける顧客の本人確認等に用いられる生体情報の管理方法について規定している。これらのガイドライン、実務指針における生体情報の取扱方法の概要についても以下で紹介する。

10 このほか、三井住友銀行、みずほ銀行、日本郵政公社が、指の静脈パターンを利用した本人確認方式の採用を予定している (三井住友銀行 [2005]、みずほ銀行 [2005]、日本郵政公社 [2005]) ほか、広島銀行、池田銀行、北海道信金共同事務センター加盟の19の信用金庫が、手のひらの静脈パターンを利用した本人確認方式の導入を予定している (広島銀行 [2005]、池田銀行 [2005]、北海民友新聞社 [2005])。

#### イ．スルガ銀行の事例

スルガ銀行が2004年6月にサービス提供を開始した「バイオセキュリティ預金」では、預金の払戻し時における顧客の本人確認手段として手のひらの静脈パターンを利用している（スルガ銀行〔2004〕）。顧客が銀行窓口においてバイオセキュリティ預金の口座開設申込みを行う際には、当該顧客の静脈パターンから固有パターンを抽出し、口座番号等の顧客情報とともにスルガ銀行のサーバに登録される。このほか、顧客の印鑑の印影も登録されるほか、暗証番号の設定も行われる。預金の払戻しに関しては、口座開設を行った店舗の窓口においてのみ行われる点が特徴であり、他の店舗やATMにおいて払戻しを受けることができない。顧客は、自分の名前や口座番号を提示するとともに、手のひらを読取装置にかざす。このとき採取される静脈の固有パターンは、顧客情報と紐付けられてサーバにおいて管理されている固有パターンと照合される仕組みとなっている。ただし、固有パターンを生成する具体的なアルゴリズムやその照合方法については公開されていないようである。このほか、顧客は、口座開設時に設定した暗証番号を提示する必要があるほか、登録した印鑑の印影も提示することとなっており、これらの手段の組合せによって最終的に本人か否かの判定が行われる。

#### ロ．東京三菱銀行の事例

東京三菱銀行では、キャッシュカード機能、クレジットカード機能等を備えた多目的ICカード「スーパーICカード」のサービスを2004年10月に開始しており、預金の払戻し時における顧客の本人確認手段として、手のひらの静脈パターンによる認証方式を採用している（東京三菱銀行〔2004〕）。本サービスでは、静脈の固有パターンは顧客が保有するICカードに保管され、銀行のサーバには保管されないという特徴があるほか、口座開設店舗の窓口だけでなく、他の店舗やICカード対応ATMにおいても静脈認証を実行して預金の払戻しを受けることが可能となっている。本サービスを利用するに当たっては、まず、利用申込みを行い、銀行からICカードと通帳の発行を受ける必要がある。顧客は、当該ICカード、通帳、印鑑等を銀行窓口持参し、静脈の固有パターンの抽出とICチップへの封入を行う。預金の払戻し時には、顧客は、ICカードと暗証番号を提示するとともに、手のひらを読取装置にかざし、静脈の固有パターンを提供する。顧客から提供された静脈の固有パターンは、ICカードに保管されている固有パターンと照合され、本人のものと判定されると、次に暗証番号の入力による本人確認も行われる。ただし、固有パターンを生成する具体的なアルゴリズムやその照合方法については公開されていないようである。

#### ハ．金融庁のガイドライン・実務指針

金融庁のガイドライン・実務指針においては、「機械による自動認証に用いられる身体的特徴のうち、非公知の情報」が「生体認証情報」と定義され、個人情報の一種として管理方法が規定されている。まず、ガイドラインの第10条において、「金融分野における個人情報取扱事業者は、その取り扱う個人データの漏えい、滅

失又はき損の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規定等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じなければならない」とし、組織的、人的、技術的な観点から安全管理措置を実施しなければならないと規定している。

組織的な安全管理措置の具体的な内容は、実務指針において規定されており、個人データの管理における責任と権限の明確化、安全管理に関する規定の整備、監査体制の整備等が挙げられている。人的な安全管理措置としては、金融機関において個人データを取り扱う担当者との非開示契約の締結、役割・責任等の明確化、教育・訓練、管理手続の遵守状況の確認等が内容として盛り込まれている。技術的な安全管理措置としては、個人データの利用者の識別・認証、個人データへの内外からのアクセス制御、アクセス権限の管理、個人データの漏洩・改ざん対策、個人データのアクセスの記録・分析、システム監査の実施等が挙げられている。

こうした措置に加えて、生体認証情報に関しては、追加的に次の措置について規定に盛り込まなければならない旨が実施指針の別添2に規定されている。

- ・生体認証情報を登録する際における、なりすましによる登録の防止策、本人確認に必要な最小限の生体認証情報のみの取得、生体認証情報の取得後に基となった生体情報の速やかな消去に関する事項
- ・認証時における、偽造された生体認証情報による不正認証の防止措置、登録された生体認証情報の不正利用の防止措置、残存する生体認証情報の消去、認証精度設定等の適切性の確認に関する事項
- ・生体認証情報の保存時における、生体認証情報の暗号化、氏名等の個人情報との分別管理に関する事項
- ・生体認証情報を本人確認に用いる必要がなくなった場合における、生体認証情報の速やかな消去に関する事項

### 3．生体認証システムにおける脆弱性

生体認証システムを適切に設計・運用するためには、当該システムが必要とされるセキュリティ・レベルを満たしていることを適正に評価することが求められる。こうした評価を行う際には、当該システムに内在する脆弱性としてどのようなものが想定されるかを明確にする必要がある。ただし、現時点では、生体認証システムにおける脆弱性を網羅的に検討した文献は少なく、2節で紹介した日本バイオメトリクス認証協議会報告書（以下、JBAA報告書と呼ぶ）が挙げられる程度である。そこで、本節では、JBAA報告書において列挙されている脆弱性について紹介するとともに、それらの中でどの脆弱性について留意する必要があるかを考察する。

## (1) 想定される脆弱性

JBAA報告書では、生体認証システムにおいて想定される脆弱性を次の2つの観点から分類している。1つは、生体認証システム特有の脆弱性と一般の個人認証システムに共通する脆弱性に分類するというものである。もう1つは、当該脆弱性によって引き起こされると考えられる攻撃に着目し、なりすましにつながるもの、サービス妨害につながるもの、これら両方につながる可能性があるものの3つに分類するというものである。

生体認証システムが正常に稼働するためには、なりすましとサービス妨害のいずれに対しても十分な対策を講じることが求められるが、生体認証システムの本来的な機能は個人を正確に認証することであり、その意味で、なりすましという攻撃をまず考慮することが必要であると考えられる。そこで、以下では、なりすましに関連する19項目の脆弱性(表3参照)に焦点を絞って議論する。

### イ. 他人受入、狼、子羊、類似性

JBAA報告書において「他人受入」と呼ばれている脆弱性は、攻撃者が自分の生体情報をそのまま提示した場合に、なりすましの対象となっている別の個人の生体情報として受け入れてしまうというものである。生体認証システムが他人を本人と誤って判定してしまう確率を示す誤受入率や、生体情報の照合アルゴリズムが1回の照合において他人の生体情報の固有パターンを本人のものと誤って判定してしまう確率を示す誤合致率が、本脆弱性の深刻度を示す指標になると考えられる。本脆弱性を軽減するためには、生体認証システムが実装される環境を想定した条件のもとで誤受入率や誤合致率を測定し、その結果を基に判定しきい値等のパラメータを設定することが求められる。誤受入率や誤合致率の測定に関しては、2節(2)において紹介したように、各種生体情報に応じた認証精度評価方法の標準情報(JIS TR)が既に策定されている。また、どのように誤受入率等をアプリケーションの要件側から決定すればよいかについては、運用要件に関するガイドラインJIS TR X 0100(日本工業標準調査会[2004c])が策定されており、参考にすることができる。

「狼(wolf)」と呼ばれている脆弱性は、複数の他人のテンプレート(固有パターン)に対して一致すると高い確率で判定される生体情報を有する個人が存在してしまうというものであり、このような個人は狼と呼ばれる<sup>11</sup>。これに対して、「子羊(lamb)」と呼ばれている脆弱性は、複数の他人の生体情報と一致すると高い確率で判定されてしまうテンプレートを有する個人が存在してしまうというものであり、このような個人は子羊と呼ばれている<sup>12</sup>。また、「類似性」と呼ばれている脆弱性

11 狼という用語は、音声による本人確認技術の研究の文脈において定義されたものであり(Doddington [1998]、古井[1999]、瀬戸[2002])、他者の声色を模倣して、音声による本人確認において他者になりすますことができる個人を指す。

12 子羊という用語は、狼と同様に、音声による本人確認技術の研究の文脈において定義されたものであり、他者に模倣されやすい声色・話法を持つ個人を指す。

表3 JBAA報告書において列挙されている脆弱性

JBAA報告書における脆弱性の名称	脆弱性の特性	概要
他人受入	生体認証システムに特有	自分の生体情報をそのまま提示した場合、他の利用者として偶然受け入れられてしまう。
狼		複数のテンプレートに対して、高確率で他人受入を可能にする生体情報を有する利用者（狼）が存在する。
子羊		複数の生体情報に対して、高確率で他人受入を可能にするテンプレートを有する利用者（子羊）が存在する。
類似性		双子等、類似の生体情報を有する人が複数存在してしまう。
偽生体情報		生体情報を物理的に偽造し、それが受け入れられてしまう。
公開		生体情報が本人の同意なく容易に他人の手に渡ってしまう。
推定		テンプレートや照合結果が生体情報推定の手掛かりとなる。
利用者状態		被認証者の生体情報が自身の事情で変化し、システムに受け入れられない。また、そうした品質の劣る生体情報を登録することによって、他者になりすましされてしまう。
入力環境		被認証者の生体情報の読取データが環境要因で変化し、システムに受け入れられない。また、そうした品質の劣る生体情報を登録することによって、他者になりすましされてしまう。
認証パラメータ		不適切な認証パラメータの設定によって他人受入の可能性が高まる。
登録	個人認証システム一般に共通	本人確認が不適切であり、他者の生体情報が登録されてしまう。
データ漏洩		システム内部で処理・保管されるデータが漏洩してしまう。
データ改ざん		システム内部で処理・保管されるデータが改ざんされてしまう。
単独		生体情報のみを提示する場合、ICカード等のトークンを利用する方式に比べて攻撃を相対的に容易に実行することができる。
代替手段		代替手段による本人確認手段のセキュリティが生体認証の場合に比べて低くなっている場合がある。
提供		利用者本人の意思で自分の生体情報を他者に提供できてしまう。
サイド・チャネル		システムから各種情報（処理時間、消費電力量等）が漏洩する。
センサ露出		生体情報を採取するセンサは外部に露出しており、生体情報の入手、破壊等の対象になりうる。
構成管理		システムを構成する要素間の整合性が取れていない場合がある。

備考：本表を作成するに当たっては、JBAA 報告書（JBAA [ 2003 ]）の表6、7をベースとした。

は、遺伝的な要因から双子等の血縁者における生体情報が高い類似性を有する場合、そうした個人を類似の生体情報を有する他人として受け入れてしまうというものである。

仮に、狼と呼ばれる個人が利用者のグループの中に無視できない割合で存在したとすると、この個人によるなりすましの攻撃によって当該システムの機能が低下するおそれが出てくる。また、子羊に対応する個人が無視できない割合で存在した場

合、悪意のある別の利用者によってなりすましの標的となってしまう、当該システムの機能が損なわれる可能性がある。血縁等の要因による類似度の高い生体情報を有する利用者が高い割合で存在する場合も、同様の問題が発生する可能性があると考えられる。

これらの3つの脆弱性に関しては、誤受入率や誤合致率に加え、アプリケーションの利用者になると想定される個人のグループにおいて、狼や子羊に対応する利用者、あるいは、類似度の高い生体情報を有する可能性のある利用者がどの程度の割合で存在するかについて考慮しておくことが必要である。また、狼に対応する個人のように、誤受入率が相対的に高い利用者が存在する場合には、個々の利用者の誤受入率を考慮して判定しきい値を設定することが求められる（門田・黄・吉本 [2005]）。指紋や虹彩等の一部の生体情報においては、双子であったとしても生体情報から得られる固有パターンが異なるといった研究結果が得られており、こうした事実が明らかになっている生体認証技術を利用することも有用であろう。

#### ロ．偽生体情報

「偽生体情報」と呼ばれている脆弱性は、生体認証システムが人工物等によって物理的に偽造された生体情報を受け入れてしまうというものであり、4節で紹介する人工指や人工虹彩に対する脆弱性が代表的な事例として挙げられる。偽生体情報の脆弱性がどのような形で生体認証システムに存在するかを明らかにすることは、人工物として無限のバリエーションが想定されることから容易な作業でない。現時点においては、実際に人工物を作製して偽造した生体情報がどの程度の頻度でシステムに受け入れられるかを実験するとともに、人工物を作製するためにどの程度のコストが必要となるかを明らかにするという方向で研究が進められている。

「偽生体情報」という脆弱性に対応するためには、上記のような既存の方向性の研究を続け、脆弱性評価の結果を蓄積していくことがまず必要である。そうした結果を基にして、偽造された生体情報がどの程度受け入れられてしまうかに関する評価指標を今後確立することが考えられる。類似の指標として、人工物の認証技術である人工物メトリクスの分野では、クローン受入率（clone acceptance rate）およびクローン一致率（clone match rate）<sup>13</sup>が提案されている（Matsumoto and Matsumoto [2003]）。これらの指標を生体認証技術の分野でも利用できないか今後検討することも有用であろう。

一連の評価によって偽造が比較的安価に可能であってその影響が無視できないことが判明した場合には、脆弱性を回避する対策を講じる必要がある。そうした方法の1つとして、生体検知機能の活用が挙げられる。こうした生体検知機能を採用す

13 Matsumoto and Matsumoto [2003]において、クローン受入率は、システムが拒否すべきクローン（人工物の複製物）を誤って受入する確率と定義されている。クローン一致率は、照合アルゴリズムが1回の照合において不一致と判定すべきクローンを誤って一致と判定する確率と定義されている。

るに当たっては、偽造された生体情報を確実に検知できることを再度実験等によって確認しておくことが必要である。

## ハ．公開

「公開」と呼ばれている脆弱性は、生体情報が本人の同意なく第三者によって容易に取得されてしまい、各種の攻撃に利用されてしまうというものであり、本脆弱性をどの程度考慮するかについては生体情報の特性等によって異なる。

例えば、指紋を利用した生体認証システムの場合、指で触ったもののほとんどに残留指紋が付着し、その残留指紋から当該個人の指紋を推測することが可能となる。また、顔画像を利用する場合は、当該個人の写真を撮影することによって顔画像を捕捉することが比較的容易と考えられる。こうしたケースにおいては本脆弱性を考慮することが求められる。一方、静脈パターンを利用した生体認証システムにおいては、特殊な装置を利用しない限り静脈パターンがどこかに残留するという可能性は低く、本脆弱性が問題となるケースは相対的に少ないと考えられる。

生体情報の捕捉が比較的容易と考えられる生体情報を利用している場合には、仮に生体情報が何らかの形で捕捉されたとしても、その情報が生体認証システムにとって重大な問題を引き起こさないように配慮する必要がある。例えば、残留指紋から偽造された指紋が提示されたとしても、生体検知機能等を活用して排除するといった対策が考えられよう。

## ニ．推定

「推定」と呼ばれている脆弱性は、テンプレートや照合結果から生体情報が効率的に推測されてしまうというものであり、生体認証システムの運用方法や固有パターンの照合アルゴリズムと密接な関係がある。すなわち、本脆弱性が問題となるか否かは、テンプレートや照合結果に関する情報が外部に漏れないようにシステムが設定されているか、また仮に漏れたとしても、照合アルゴリズムのセキュリティに影響するかに依存すると考えられる。例えば、本脆弱性を回避する手段としては、テンプレートを暗号化して保管する、テンプレートとどの程度一致していたかを示す情報を被認証者に開示しない、一定回数の試行において連続で失敗した場合に新たな認証処理を開始しないといった方法が考えられる。

## ホ．利用者状態、入力環境

「利用者状態」と呼ばれている脆弱性は、被験者自身の操作によって生体情報やその読取データが変化し、品質が低い、あるいは、セキュリティ上問題がある固有パターンが登録され、その結果、攻撃者によってなりすましされやすくなってしまいうというものである。例えば、指紋を利用した生体認証システムにおいて、洗剤等を頻繁に利用したために不鮮明となった指紋がそのまま登録された場合、別の個人によって提示された指紋の固有パターンと、当該指紋による固有パターンが一致すると判定される可能性が高まるおそれがある。

一方、「入力環境」と呼ばれている脆弱性は、認証を行う環境の変化によって、「利用者情報」の脆弱性と同様の結果が生じてしまうというものである。例えば、顔画像を用いた生体認証システムにおいて、顔に当てる照明の光度や角度によって本来の特徴を適切に反映していない生体情報が提示され、そのまま生成された固有パターンが登録された場合、他人によって提示された顔画像を誤って受け入れてしまうおそれが出てくる。

これらの脆弱性を軽減・回避する方法としては、登録時に提示される生体情報の固有パターンの品質を厳格にチェックし、一定水準の品質を満足しない固有パターンの登録を排除するといった方法がまず考えられる。また、当該生体情報以外の生体情報を用いた認証手段等を別途準備するという方法も挙げられる。

#### へ．認証パラメータ、登録、データ漏洩、データ改ざん

「認証パラメータ」と呼ばれている脆弱性は、生体認証システムにおける判定しきい値等のパラメータ設定が不適切に行われ、他人を本人と誤って判定してしまうというものである。「登録」と呼ばれている脆弱性は、テンプレートの登録時において利用者の本人確認が適切に行われておらず、他人の固有パターンを本人として誤って登録してしまうというものである。「データ漏洩」および「データ改ざん」と呼ばれている脆弱性は、生体認証システムにおいて保管されているテンプレートや認証時のパラメータ等が適切に管理されておらず、これらのデータが漏洩してしまう、あるいは、改ざんされてしまうというものである。例えば、テンプレートが漏洩した場合、そのテンプレートを用いて生体情報を復元するといった攻撃が想定される（例えば、Hill [ 2001 ]）。

これらの脆弱性は、いずれも生体認証システムにおけるセキュリティ管理・運用の状況に大きく依存する。「認証パラメータ」の脆弱性は、誤受入率、誤受率率、ROC曲線等の認証精度の指標を踏まえつつ、判定しきい値等を慎重に設定することによって軽減することが可能になると考えられる。「登録」の脆弱性については、登録時における利用者の本人確認の厳格な実行によって対処することになる。例えば、本人確認の業務を複数の担当者によって実行する、本人の身元を確認する資料を複数準備させるといった方法が考えられる。また、「データ漏洩」と「データ改ざん」の脆弱性に対しては、生体認証システム内部において処理されるデータの漏洩や不正な操作を防止・検知する手段を適用することが求められる。そうした手段として、例えば、データを暗号化して保管する、ハードウェア機器を外部から物理的に操作困難にする、データ処理に関するログを取得・保管するといった手段が挙げられる。また、管理者自身が攻撃者と結託するという状況を想定した場合には、複数の担当者が協力しなければ管理者権限を実行することはできないといった仕組みを導入することも検討する必要がある。このほか、登録されたテンプレートが漏洩したとしてもテンプレートから生体情報を復元困難にする技術についても研究が行われており、こうした技術についても留意しておくことが望ましい（鷲見・松山・中嶋 [ 2005 ] 大木ほか [ 2005 ]）。

### ト．単独、代替手段

「単独」と呼ばれている脆弱性は、個人を認証するシステムにおいて生体情報のみを本人確認のための情報として利用する場合、仮に、生体情報を用いた本人確認手段が破られてしまうと、当該認証システムの機能が完全に損なわれてしまうというものである。また、「代替手段」と呼ばれている脆弱性は、生体情報を提示できない利用者のために準備されている代替認証手段のセキュリティ・レベルが相対的に低く、攻撃の対象になってしまうというものである。

これらの脆弱性は、生体認証システムおよび代替認証手段のセキュリティ・レベルや認証精度がアプリケーションの要件を満足していないために生じることが考えられる。その背景としては、セキュリティ要件の設定が不適切である、または、当該システムおよび代替認証手段のセキュリティ評価が適切に実行されていないといった事情があると想定される。したがって、「単独」や「代替手段」と呼ばれる脆弱性を回避するためには、セキュリティ要件の適切な設定から始める必要がある。生体認証システムや代替認証手段のセキュリティ・レベルがセキュリティ要件を満足していないことが明確になった場合には、セキュリティや認証精度を向上させるために、別の認証手段を追加する、別の認証手段に置き換える、複数の生体情報を利用したマルチモーダル認証を採用するといった方法について検討する必要がある。

### チ．提供

「提供」と呼ばれている脆弱性は、利用者自身が自分から生体情報を他者に提供することが可能であり、攻撃者がそれを利用してしまおうというものである。こうした脆弱性が特に問題と考えられるのは、脅迫によって生体情報の提供を余儀なくさせられるというケースであろう。

生体情報の提供が本人の意思によるものである以上、その意思が強要されたものか否かを生体情報のみを用いて判定することが困難となる場合もある。具体的には、指紋、虹彩、静脈パターンのように意図的に生体情報を変化させることができない身体的特徴を利用する場合には、こうした問題が深刻なものとなる可能性がある。一方、筆跡等のように、意図的に生体情報を変化させることが可能な行動的特徴を利用する場合には、あらかじめ決められた方法で生体情報を変化させ、攻撃者に悟られないように脅迫の事実を第三者に通報する仕組み（デュレス・コントロールと呼ばれる）を準備することも考えられる。ただし、こうした仕組みの存在を攻撃者が事前に知っていることを前提として対策することが重要であり、そうした方式の実現手法に関する研究成果も発表されている（例えば、大島・松本 [ 2003 ]）。このほか、生体認証システムのセンサや装置をモニターによって監視する等の抑止効果を期待した対策も考えられる。

## リ．サイド・チャンネル

「サイド・チャンネル」と呼ばれている脆弱性は、ハードウェアから設計者の意図せざる情報、例えば処理にかかる時間、消費電力量、電磁波等が漏洩している場合、攻撃者がこうした情報を用いてハードウェア内部の情報を効率的に推測し、それを各種の攻撃に利用することができてしまうというものである。本脆弱性に関しては、いわゆるサイド・チャンネル攻撃への安全性を向上させることによって回避・軽減させることができると考えられる。サイド・チャンネル攻撃に関しては、これまでに数多くの研究成果があるほか、現在でも活発に学会等で議論されている分野であり、そうした成果をとりまとめた資料（例えば、情報処理振興事業協会 [ 2000 ]、Quisquater [ 2002 ]、INSTAC [ 2003 ]）も公表されている。こうした資料をベースとして、生体認証システムの実装環境を考慮しながら、どのようなタイプのサイド・チャンネル情報が当該システムから漏洩している可能性があるかを検討し、必要な対策を適宜実施していくことになる。

## ヌ．センサ露出

「センサ露出」と呼ばれている脆弱性は、生体情報を読み取るセンサが外部に露出する場合が多く、その中でも、指紋を利用する生体認証技術のように人体の一部をセンサに接触させるケースにおいては、生体情報がセンサに残留し、攻撃者がその残留した情報をそのまま利用してなりすましを行うことを可能にしてしまうというものである。ただし、センサに人体を接触させないケースにおいては、こうした脆弱性が問題となる可能性は相対的に小さいと考えられる。「センサ露出」の脆弱性を排除するためには、仮に生体情報がセンサ表面に残留したとしても、その情報を利用できないようにしておく必要がある。例えば、生体認証システムが利用される度にセンサ表面を拭き、生体情報が残留しないようにしておくといった対応が考えられる。また、残留した生体情報が採取されて物理的に偽造されたケースも想定するとすれば、偽生体情報の脆弱性への対策と同様に、生体検知機能を準備するといった対応も考えられる。

## ル．構成管理

「構成管理」と呼ばれている脆弱性は、生体認証システムを構成する要素（例えば、センサ等の入力デバイス、固有パターン生成モジュール、判定モジュール）間の整合性が十分に取れていないことによって発生してしまう弱点と定義されている。本脆弱性は、システムの設計時や変更時においてシステムの動作に関するテストや評価が適切に行われていないことが主な原因であると考えられる。したがって、本脆弱性を排除するためには、システムの設計・テスト・評価を適切に実施し、システム全体の整合性を確保することがまず基本となる。さらに、場合によっては、こうしたシステムの管理・評価に携わる内部者による不正行為（例えば、評価結果の改ざん）を困難にする、あるいは、検知するための対策も検討する必要があると考えられる。

## (2) 生体情報の物理的な偽造への対応

19項目の脆弱性について考察した結果、各脆弱性を排除するために重要と考えられる要素を整理すると、表4のとおりである。

これらのうち、生体認証システムに特有と位置づけられている脆弱性に着目すると、「他人受入」、「狼」、「子羊」、「類似性」と呼ばれている各脆弱性の回避・軽減を検討する際には、誤受入率や誤合致率等のいわゆる認証精度評価に関する検討が中心になるといえる。また、「偽生体情報」と呼ばれている脆弱性に対応するに当たっては、生体情報の物理的な偽造の難易度の評価、生体検知機能に関する検討が中心になるといえる。「公開」と呼ばれている脆弱性に関しては、生体情報を実際に捕捉することがどの程度困難か、あるいは、容易かについて明確にすることが中心になるといえる。ただし、「偽生体情報」の脆弱性が回避されていれば、仮に生体情報を攻撃者が捕捉したとしても、その情報を実際の攻撃に活用することは困難であると考えられることから、「公開」の脆弱性を考慮するか否かは「偽生体情報」の脆弱性への対応に依存していると考えられる。「推定」、「利用者状態」、「入力環

表4 なりすましに関する脆弱性と対策のポイント

脆弱性の名称	対策を検討する際に考慮すべき主なポイント
他人受入	・誤受入率や誤合致率等の認証精度指標とその評価
狼	・誤受入率や誤合致率等の認証精度指標とその評価 ・脆弱性を引き起こす可能性がある生体情報を有する個人が存在する割合、および、その影響度
子羊	
類似性	
偽生体情報	・生体情報の物理的な偽造の難易度の評価（クローン受率率やクローン一致率に類似の指標に関する検討等） ・生体検知機能の採用
公開	・生体情報捕捉の難易度
推定	・生体情報とその照合結果を外部に漏洩させない手段
利用者状態	・品質の低い固有パターン登録を回避する手段
入力環境	
認証パラメータ	・パラメータの適切な選択とその設定に関する管理・運用方法
登録	・登録時における本人確認方法
データ漏洩	・システム内部で処理・保管されるデータの機密性、一貫性を確保するとともに、後日再度の検証を可能にする手段
データ改ざん	
単独 代替手段	・生体認証システムおよびその代替認証手段に求められるセキュリティ要件と、適切なセキュリティ評価
提供	・脅迫等による脅威への対策
サイド・チャネル	・想定されるサイド・チャネル攻撃への対策
センサ露出	・センサに生体情報が残留しない手段 ・生体検知機能の採用
構成管理	・生体認証システムの設計・テスト・評価

境」,「認証パラメータ」と呼ばれている各脆弱性に対処する際には、生体認証システムにおいて処理される情報の機密性確保や、システムのセキュリティ機能の管理・運用方法に関する検討が中心になるといえる。

このようにみていくと、各種の脆弱性の中でも今後検討が必要であると考えられるのは、「偽生体情報」の脆弱性、すなわち、生体情報の物理的な偽造に関連する脆弱性であるといえる。「他人受入」,「狼」,「子羊」,「類似性」の各脆弱性においては、主として、認証精度評価とその結果を受けて認証パラメータの設定をいかに行うかがポイントであり、これらに関しては既に多くの研究成果の蓄積が存在し、参照することができる標準規格も存在している。また、「推定」,「利用者状態」,「入力環境」,「認証パラメータ」の各脆弱性については、主に、セキュリティ機能の管理・運用方法等に関する検討がポイントであり、汎用的な情報システムにおけるセキュリティ管理・運用手法を概ね適用して検討を行うことが可能であると考えられる。これらに対して、「偽生体情報」の脆弱性に関しては、脆弱性の存在およびその影響度について研究が開始されたばかりであり、研究結果の蓄積は少なく、脆弱性評価のための確立された手法が存在しないというのが実情である。実際に、バイオメトリクス認証システムにおける運用管理の導出指針（JIS TR X 0100）においても、生体情報の物理的偽造については適用範囲外としたうえで、「...この種の（生体情報の物理的偽造による）不正アクセスには一般的な誤受入率を適用できないことが多い。ベンダは、この様なぜい弱性に関する情報をシステム管理者又はシステムインテグレータに対して積極的に開示し、システム管理者又はシステムインテグレータ側もベンダに対して情報提供を求めることを推奨する」としている。次節では、こうした脆弱性評価に関する研究事例を紹介する。

#### 4．生体認証システムにおける生体情報の物理的偽造に関する評価

本節では、生体認証システムにおける脆弱性評価の中でも生体情報の物理的偽造に関する研究成果に焦点を当てて、主な研究成果を紹介する。筆者らが知る限り、現時点では、評価の対象となっている生体情報として指紋および虹彩のみがよく知られている<sup>14</sup>。

##### (1) 生体情報の物理的偽造に関する研究

###### イ．指紋を対象とした研究

他の個人の生体情報を物理的に偽造し、当該個人になりすますという攻撃に関し

14 本稿のメインパートは2005年3月15日の時点で入手可能な情報をベースとして執筆しており、指の静脈パターンを利用した認証方式における脆弱性については触れていない。ただし、メインパート執筆後、こうした静脈パターンの照合装置の脆弱性を指摘する重要な研究成果（松本ほか [2005a, b]）が発表されている。

ては、1990年代末以降いくつかの公表されている研究事例が存在する。

初期の事例としては、ウィリス＝リーによる研究報告 ( Willis and Lee [ 1998 ] ) が挙げられる。彼らは、残留指紋から採取した指紋のパターンを透明なシートに印刷するという手法、および、ワックスの型によって指紋のパターンが表面に形成されたゴムを作製するという手法によって指紋のパターンを物理的に偽造し、市販されている6種類の指紋照合装置において、偽造した指紋が受け入れられるか否かを実験している。彼らの文献には物理的な偽造の方法に関する詳細な情報が示されていないものの、透明なシートを利用した場合には6機種のうち2つの機種に受け入れられたほか、ゴムを利用した場合には4つの機種に受け入れられたことが報告されている。

ヴァン・デア・ブッテ＝ケーニングによる研究報告 ( van der Putte and Keuning [ 2000 ] ) においては、より高度な物理的偽造の手法に関して検討が行われている。彼らは2つの手法を採用しており、1つは、実際の指から石膏によって指紋のパターンの型を作製し、その型にシリコンを流し込んで指紋のパターン付きのシリコンを作製するというものである。もう1つは、残留指紋に細かい粒子の粉を吹きかけて指紋パターンを浮き上がらせ、カメラを使って指紋のパターンをフィルムに転写したうえでフォトリソグラフィ ( photolithography )<sup>15</sup>によって型を作製し、その型から指紋のパターン付きシリコンを作製するというものである。ヴァン・デア・ブッテ＝ケーニングは、光学式の指紋読取装置を含む6機種に対して、シリコンによる指紋パターンが受け入れられるか否かを実験し、いずれの機種においても受け入れられたことを報告している。ただし、指紋付きシリコンを作製するためにはどのような材料・機材が必要か、また、作製費用はどの程度かかるかといった情報は明らかにされていない。

指紋に関する包括的な研究は、山田＝松本＝松本 ( 山田・松本・松本 [ 2000a ] ) によって開始されており、従来のシリコンを利用した指紋のパターンの偽造よりも安価で効率的に作製可能なゼラチンによる指紋のパターンの偽造が可能か否かについて幅広い検討が行われている。これら一連の研究については、本節(2)において詳しく紹介する。

山田＝松本＝松本によって開始された一連の研究を参照し、市販されている各種指紋照合装置においてゼラチンによる指紋のパターンが受け入れられるか否かを検討した文献がいくつかみられる。リゴン ( Ligon [ 2002 ] ) は、市販されている指紋照合装置1機種がゼラチンによる指紋のパターンを実際に受け入れるか否かを確認するための実験を行い、実際の指から型を作製して指紋付きゼラチンを作製する手法によって平均で60%以上の割合で受け入れられることを確認している。ブロメ ( Blommé [ 2003 ] ) も、リゴンと同様の手法を採用し、市販の指紋照合装置3機種に

15 光を利用して微細なパターンを基板や薄膜等に転写する技術。フォトレジストと呼ばれる感光性材料の薄膜を有する基板に、転写の対象となっている微細なパターンを描いたマスクを介して紫外線等を露光する。その結果、基板上で露光した部分は化学変化を起こし、パターンが基板に転写されることとなる。

においてゼラチンによる指紋のパターンが平均で40%以上の割合で受け入れられたことを報告している。また、サンドストローム (Sandström [ 2004 ]) は、フォトリソグラフィを用いて残留指紋から指紋付きゼラチンを作製する手法を採用し、光学式をはじめとする8種類の指紋照合装置においてゼラチンによる指紋のパターンが受け入れられるか否かを実験している。その結果、いずれの機種においても平均で30%以上の割合で受け入れられることが実証されている。

このほか、タールハイム = クリスラー = ジーグラー (Thalheim, Krissler and Ziegler [ 2002 ]) は、より簡便な方法による残留指紋を用いたなりすましの可能性を指摘している。タールハイムらは、残留指紋が存在するセンサ面に息を吹きかける、あるいは、薄膜に包まれた水袋をセンサ面に押し付けるといった方法によって、残留指紋をセンサ面上で強調し、いくつかの指紋照合装置において残留指紋による照合が成功するか否かを実験している。その結果、3種類の指紋照合装置において受け入れられたことを報告している。

#### ロ．虹彩を対象とした研究

虹彩を対象とした物理的偽造の可能性に関する初期の報告としては、タールハイムらによる実験とその結果に関する“*c't*” (ドイツのネット雑誌) に掲載された記事“Body Check: Biometric Access Protection Devices and their Programs Put to the Test” (Thalheim, Krissler and Ziegler [ 2002 ]) が挙げられる。タールハイムらは、被認証者の虹彩を撮影したうえで、その画像を紙に印刷して人工虹彩を作製し、一部の虹彩照合装置がその人工虹彩を受け入れてしまうという実験結果を報告している。

本報告を受けて、虹彩照合装置における脆弱性評価の研究が松本 = 平林によって本格的に開始されており (松本・平林 [ 2003a ])、その後いくつかの研究結果が続けて発表されている。これらの研究の内容については、本節(3)において詳しく紹介する。

また、虹彩ビット列の開発者であるドーグマン (Daugman [ 2004b ]) は、既存の虹彩照合装置4機種を対象に、実際に提示されている虹彩が物理的に偽造されたものか否か等を検知するための機能の有無について検討した結果を発表している。4機種のうち1機種については、虹彩の物理的偽造等を検知するための16種類の機能を搭載しているほか、別の1機種は、目が顔の一部であることを確認する機能を搭載していると説明している。また、残りの2機種に関しては、物理的偽造を検知する機能を搭載していないと説明している。

## (2) 指紋照合装置の脆弱性評価研究

### イ．一連の研究の流れ

山田・松本・松本 [ 2000a ] に端を発する指紋照合装置の脆弱性に関する一連の研究は、主に11の論文において発表されている (図2参照)。基本的な研究の枠組みについては、山田・松本・松本 [ 2000a ] において発表されており、この論文に示

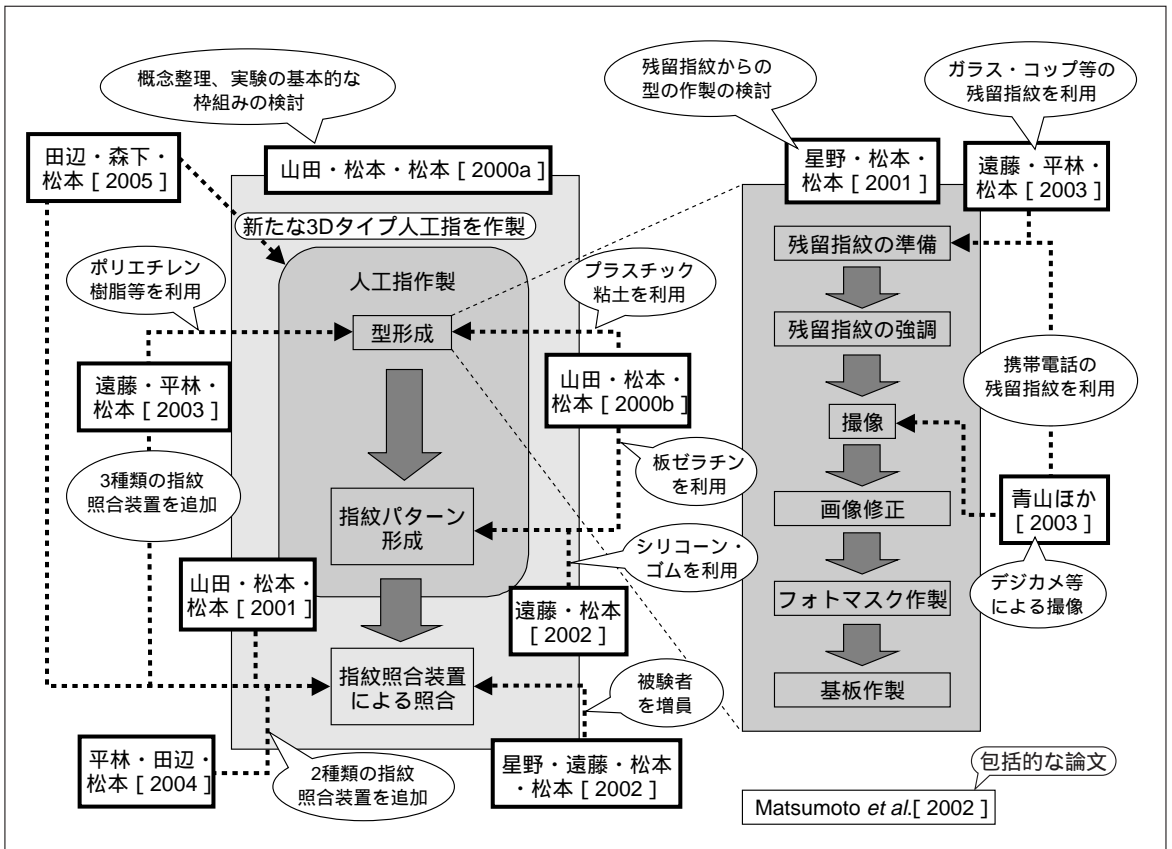
されている方法をベースとして、人工指の作製方法の改良、対象とする指紋照合装置の拡張、被験者の増員による実験結果の信頼性向上を目的とした研究が行われている。以下では、これら一連の研究の概要と関連性について説明する。

### ロ．人工指の作製プロセス

人工指による指紋照合装置の本格的な脆弱性評価研究は、山田・松本・松本 [2000a] に端を発している。本研究では、一連の研究においてベースとなる概念整理がまず行われており、指紋照合装置の構成、指紋照合装置を欺く目的で本物の人間の指（以下、生体指と呼ぶ）を模倣して作製される人工指の作製プロセス、人工指を用いた不正利用の形態が示されている。人工指の作製プロセスとして、主に次の2つが挙げられている。

- ・生体指から人工指の型を形成し、その型を用いて媒体上に指紋パターンを形成する（3Dタイプ人工指方式）
- ・生体指による残留指紋から型を形成し、その型を用いて指紋パターンを媒体上に形成する（フラットタイプ人工指方式）

図2 指紋照合装置の脆弱性評価に関する研究の流れ



## 八．人工指の作製

人工指を作製する方法として、一連の研究では3Dタイプ人工指方式とフラットタイプ人工指方式が検討の対象となっている。これらの方式はいずれも型形成と指紋パターン形成の2つのプロセスから構成されており、両者の差異は型をどのように作製するかにある。以下では、型形成と媒体上への指紋パターン形成に分けて説明する。

### (イ) 型の形成

#### (3Dタイプ人工指方式)

まず、山田・松本・松本 [2000a, b, 2001]、遠藤・平林・松本 [2003] では、3Dタイプ人工指方式による人工指(3Dタイプ人工指と呼ばれる)の作製を検討している。これらの研究では、主として、どのような材料を採用してどのように型を形成するのが効率的かという観点から検討が行われている。具体的な型材料の候補としては、シリコーン・ゴム、プラスチック粘土、ポリエチレン樹脂、歯科用アルギン酸塩印象材が用いられている。

3Dタイプ人工指方式に関する最初の研究である山田・松本・松本 [2000a] では、型の材料としてシリコーン・ゴムを採用している。シリコーン・ゴムは、電線被覆、医療用器具、模型作製材料等に用いられるゴムの一種として市販されており、比較的容易に入手可能であるとしている。シリコーン・ゴムによる型形成は次の手順で行われている。

- 1 シリコーン・ゴムの材料を攪拌し、可能な限り気泡を除去する。
- 2 シリコーン・ゴムを硬化させ、型の土台を形成する。
- 3 型の土台の上に柔らかいシリコーン・ゴムを流し込み、生体指を土台に押し付けるように埋める。
- 4 シリコーン・ゴムが硬化したら、生体指を取り外す。完全に硬化するまでに約30分かかる。

続く山田・松本・松本 [2000b, 2001] においては、型材料としてプラスチック粘土を採用している。山田・松本・松本 [2000b] では、材料をプラスチック粘土に変更することによって、材料購入費用の削減と型作製時間の短縮化が可能になるとしている。

また、遠藤・平林・松本 [2003] においては、シリコーン・ゴムやプラスチック粘土とは異なる材料の利用可能性を検討するとして、熱可塑性を有するポリエチレン樹脂と歯科用アルギン酸塩印象材を採用している。これらは、いずれも容易に入手可能なほか、数分程度で型が硬化するという特徴を有しているとしている。

さらに、田辺・森下・松本 [2005] では、後述するフラットタイプ人工指を指の形状をした媒体に接着するという手法によって3Dタイプ人工指を作製する方法を検討している。

## (フラットタイプ人工指方式)

フラットタイプ人工指方式では、残留指紋から型を作製することとなるため、指紋パターンをどのように撮影するか、また、その指紋画像から型の形成をどのように行うかがポイントとなる。基本的な方法に関しては星野・松本・松本 [2001] において検討されており、フォトリソグラフィを活用する手法が採用されている。また、その後の研究では、指紋パターンの撮影方法（デジタル顕微鏡、デジタル・カメラ）および、指紋パターンが残された媒体（板ガラス、コンパクト・ディスク、携帯電話、ガラス・コップ）を変化させた場合において、人工指を作製可能か否かについて検討が行われている。

星野・松本・松本 [2001] による型形成の手続は以下のとおりである。

- 1 ガラス板に指を押し付けた後、ガラス板をシアノアクリレート系接着剤と呼ばれる特殊な接着剤と同一の密閉容器内に入れ、残留指紋を白く浮き出させる。この操作は、シアノアクリレート系接着剤が少量の水分と反応し、白く変色する性質を有していることを利用している。
- 2 浮き出た指紋をデジタル顕微鏡（211万画素）で撮影し、デジタル画像化する。
- 3 指紋画像をコンピュータに取り込み、コントラストの補正、指紋パターンの欠損の補正等を行う。
- 4 補正後の指紋画像をインクジェット・プリンターによってOHPシートに印刷し、フォトマスクとして利用する。
- 5 型材料として採用する基板にフォトマスクを上から被せ、紫外線ランプによって6分程度露光する。この結果、紫外線を浴びた部分が化学変化を起こし、フォトマスクの指紋画像が基板上のフォトレジストに転写される。
- 6 基板を専用の現像液に1分程度浸し、化学変化を起こした部分のフォトレジストを剝離させ、指紋画像と同じ形状のフォトレジストだけを基板上に残す。
- 7 基板をエッチング液に20分程度浸し、フォトレジストが残っていない部分の金属（銅）を食刻させ、指紋画像と同じ形状の部分が浮き上がった基板を完成させる。

上記手順ではガラス板上の残留指紋をデジタル顕微鏡によって撮像しているが、青山ほか [2003] は、ガラス板に加えて、携帯電話の液晶部分あるいは本体部分（黒色）の残留指紋を採取の対象としているほか、デジタル顕微鏡のほかに、デジタル・カメラ（413万画素）による撮像の可能性を検討している。残留指紋が存在する場所として携帯電話を採用した点について、青山ほか [2003] は、携帯電話の利用者の本人確認手段として指紋照合装置を搭載したものが販売されていることを指摘し、そうした携帯電話を攻撃者が何らかの手段で入手し、残留指紋から人工指を作製して当該携帯電話の持ち主になりすましするという攻撃が想定されるとしている。また、デジタル・カメラを採用している点については、デジタル顕微鏡よりも画素数が多く、比較的安価に入手可能であることを挙げている。

遠藤・平林・松本 [2003] は、コンパクト・ディスクやガラスのコップの残留指紋を採取の対象としているほか、青山ほか [2003] において用いられたデジタル・

カメラよりも画素数が少ないデジタル・カメラ、あるいは、携帯電話に搭載されているデジタル・カメラによる撮像の可能性を検討している。

#### (ロ) 指紋パターンの形成

指紋パターンの形成は、人工指となる媒体を型に押し付けて硬化させるという手法が採られている。人工指の材料としては、粉末ゼラチンから生成したゼラチン水溶液をゲル化したもの（以下、グミと呼ぶ）、通常のシリコーン・ゴム、導電性のシリコーン・ゴムの3つが検討対象となっている。

山田・松本・松本 [2000a] が、人工指の媒体として最初にグミを採用しており、特に粉末ゼラチンからグミを生成するという手法を検討している。指紋パターンの形成手続は次のとおりである。

- 1 粉末ゼラチンに熱湯を加えて攪拌した後、冷却と加熱を交互に繰り返し、ゼラチン水溶液に含まれる気泡をできるだけ除去する。
- 2 ゼラチン水溶液を型に流し込む。
- 3 冷蔵庫で10分程度冷却し、完全に硬化したら取り出す。

上記手続では、粉末ゼラチンから高濃度の水溶液を生成するために、ゼラチン水溶液中の気泡を除去する作業が必要となる。この作業を簡略化する方法として、山田・松本・松本 [2000b] は、粉末ゼラチンの代わりに板ゼラチンを利用する方法を採用している。板ゼラチンはゼラチン水溶液をあらかじめ濃縮して板状に硬化させたものであり、高濃度のグミを比較的容易に作製可能とし、人工指の耐久性の向上にもつながるとしている。

また、遠藤・松本 [2002] は、グミの代わりにシリコーン・ゴムや導電性シリコーン・ゴムを利用した人工指の検討を行っている。導電性シリコーン・ゴムは絶縁体のシリコーンに導電性充填材を加えることで導電特性を付与させたものである。遠藤・松本 [2002] では、シリコーン・ゴムについては型に流し込んで30分程度硬化させて指紋パターンを形成しているものの、導電性シリコーン・ゴムの場合には、高温での処理が必要なため、専門の業者に依頼して指紋パターンの形成を行っている。

## 二．指紋照合装置での登録・照合

一連の研究では、登録・照合の際に指紋照合装置に提示される指の組合せ（生体指もしくは人工指）によって分類されるいくつかの実験を行っている。ここでは、「攻撃者が人工指を使って正当な指紋照合装置の利用者になりすます」という攻撃に焦点を当てて、固有パターンの登録は生体指で行い、照合は人工指で行うというタイプの実験結果について紹介する。いずれの実験においても、1対1照合で認証が行われている。一連の研究において用いられている指紋照合装置<sup>16)</sup>は全体で21機種であり（表5、6参照）、指紋パターンの照合だけでなく、提示された指が生体指で

16 実験の対象となった指紋照合装置の詳細については原論文の記述を参照されたい。

表5 3Dタイプ人工指の研究

研究	人工指の作製方法		指紋照合装置 ( )内は読取方式と照合方式
	型材料	指材料	
山田・松本・松本 [ 2000a ]	・シリコン・ゴム	・粉ゼラチン	・装置A (光学式、マニューシャ方式) ・装置B, D (光学式、照合方法不明)
山田・松本・松本 [ 2000b ]	・シリコン・ゴム ・プラスチック粘土	・板ゼラチン	・装置C (光学式、特徴点とリレーション方式) ・装置E* (光学式、パターン・マッチング方式) ・装置F, H (静電容量式、マニューシャ方式) ・装置G (静電容量式、特徴点とリレーション方式) ・装置I* (静電容量式、照合方法不明)
山田・松本・松本 [ 2001 ]			装置A~I、および、以下の装置J、Kが対象。 ・装置J (光学式、マニューシャ方式) ・装置K (光学式、マニューシャ方式)
遠藤・平林・松本 [ 2003 ]	・プラスチック粘土 ・ポリエステル樹脂 ・歯科用アルギン酸塩印象材		装置A~K、および、以下の装置O~Qが対象。 ・装置O (指内散乱光直接読取式、特徴点とリレーション方式) ・装置P (感圧式、照合方式不明) ・装置Q (エレクトリック・フィールド式、照合方式不明)
平林・田辺・松本 [ 2004 ]	・プラスチック粘土		・装置R (感熱式、周波数解析方式)
田辺・森下・松本 [ 2005 ]			・装置T (エレクトリック・フィールド式、照合方式不明) ・装置U (静電容量式、照合方式不明)

備考：表5、6については、山田・松本・松本 [ 2001 ]、遠藤・平林・松本 [ 2003 ] の表を参照して記載した。“\*”がついている装置は生体検知機能付きであることが明示されているものを表す。

表6 フラットタイプ人工指の研究

研究	人工指の作製方法		残留指紋から型作製の方法		指紋照合装置
	型材料	指材料	残留指紋の存在場所	撮像方法	
星野・松本・松本 [ 2001 ]、 星野・遠藤・松本・松本 [ 2001 ]	・基板 (フォトレジスト)	・板ゼラチン	・ガラス板	・デジタル顕微鏡	装置A~K
遠藤・松本 [ 2002 ]		・板ゼラチン ・シリコン・ゴム ・導電性シリコン・ゴム			
青山ほか [ 2003 ]		・板ゼラチン	・ガラス板 ・携帯電話の液晶部分と本体 (黒色) 部分	・デジタル・カメラ ・デジタル顕微鏡	装置A~N
遠藤・平林・松本 [ 2003 ]			・ガラス板 ・ガラス・コップ ・コンパクト・ディスク	・デジタル・カメラ ・携帯電話内蔵デジタル・カメラ	装置A~K、 O~Q
平林・田辺・松本 [ 2004 ]			(不明)	・デジタル・カメラ	装置S
田辺・森下・松本 [ 2005 ]					

備考：装置L：静電容量式、チップ・マッチング方式  
装置N：光学式、マニューシャ方式

装置M：静電容量式、マニューシャ方式

装置S：エレクトリック・フィールド式、パターン・マッチング方式

あるか否かを確認するための生体検知機能を搭載していることが明示されている装置も含まれている。

#### ホ．登録・照合結果

##### (イ) 3Dタイプ人工指での結果

3Dタイプ人工指を用いた実験は山田・松本・松本 [2000a, b, 2001]、遠藤・平林・松本 [2003]、平林・田辺・松本 [2004]、田辺・森下・松本 [2005] において行われており、全体で17種類の指紋照合装置が対象となっている(表5参照)。いずれの指紋照合装置も、パソコンや携帯電話等におけるログイン時での本人確認等の用途で市販されているものである。

まず、山田・松本・松本 [2000a] と山田・松本・松本 [2000b] は、同一種類の指紋照合装置(9機種)において実験を行っており、指紋パターン読取方式として光学式および静電容量式を、照合方式としてマニューシャ方式および特徴点とリレーション方式を採用している指紋照合装置を対象としている。これらの装置には、生体検知機能を搭載していることが明示されているものも2種類含まれている。上記の2つの文献では、板ゼラチンを材料とした人工指の受入率がいずれの指紋照合装置においても平均7割以上になったとの結果が示されている。ただし、実験は被験者5名による比較的小規模なものであり、「各社の製品の性能を定量的に評価するまでには至っておらず、実験結果によって各装置の性能を比較できるものではない」としている。

山田・松本・松本 [2001] は、読取方式として光学式を、照合方式としてマニューシャ方式を採用している別の2種類の指紋照合装置を追加して同様の実験を行っている。これらの装置においても人工指の受入率が平均8割以上となったとの結果が示されている。また、平林・田辺・松本 [2004] では、読取方式として感熱式、照合方式として周波数解析方式を採用している1機種を対象に同様の実験を行い、9割以上の受入率を観察している。

遠藤・平林・松本 [2003] は、型材料として、プラスチック粘土のほかにポリエステル樹脂、歯科用アルギン酸塩印象材を利用し、被験者1名で実験を行っている。指紋照合装置としては、山田・松本・松本 [2001] において採用された11機種に、異なる読取方式(指内散乱光直接読取式、感圧式、エレクトリック・フィールド式)を利用した3種類の指紋照合装置が追加されている。どの指紋照合装置においても、各型から作製された人工指の受入率が平均7割以上となったとの結果が報告されている。

田辺・森下・松本 [2005] は、フラットタイプ人工指(ゼラチン製)を指の形状をしたゼラチンに接着して作製した3Dタイプ人工指が、指をセンサ面に密着させながら滑らせて指紋を読み取るスワイプ型の指紋照合装置2機種(携帯電話に搭載)において受け入れられるか否かを実験している。実験の結果、いずれの機種においても平均8割以上の受入率が得られている。

#### (ロ) フラットタイプ人工指での結果

フラットタイプ人工指を用いた実験は、星野・松本・松本 [2001]、星野・遠藤・松本・松本 [2002]、遠藤・松本 [2002]、青山ほか [2003]、遠藤・平林・松本 [2003]、平林・田辺・松本 [2004]、田辺・森下・松本 [2005] において行われており、全体で18種類の指紋照合装置が対象となっている(表6参照)。

遠藤・松本 [2002] では、人工指の材料として、板ゼラチンのほかにシリコーン・ゴムと導電性シリコーン・ゴムを採用しており、11機種中5機種においてシリコーン・ゴム製の人工指の受入率が平均8割以上となったほか、導電性シリコーン・ゴム製の人工指についても9機種において同程度の受入率になったとの結果が示されている。これらの人工指を受け入れなかった機種が存在することも判明しており、静電容量式を採用している機種が不導体であるシリコーン・ゴム製人工指を受け入れなかったほか、光学式を採用している2つの機種が黒色の導電性シリコーン・ゴム製の人工指を受け入れなかったと報告されている。

青山ほか [2003] は、残留指紋が存在する媒体としてガラス板のほかに携帯電話(液晶部分および本体部分 黒色)を、残留指紋の撮像機器としてデジタル顕微鏡(211万画素)のほかにデジタル・カメラ(413万画素)を用いて実験を行っている。また、遠藤・松本 [2002] において用いられた11機種に、チップ・マッチング方式による照合装置を含む3機種が新たに加えられて実験が行われている。実験の結果、いずれの機種においても、媒体や撮像機器によらず平均7割以上の受入率が得られている。

遠藤・平林・松本 [2003] は、ガラス・コップやコンパクト・ディスク上の残留指紋を携帯電話に内蔵されているデジタル・カメラによって撮影することを試みている。本実験では、指内散乱光直接読取式、感圧式、エレクトリック・フィールド式を読取方式としてそれぞれ採用している3機種を加えており、これらの機種においても、残留指紋から作製されたグミ製人工指の受入率が7割以上になったとの結果が示されている。

また、平林・田辺・松本 [2004] および田辺・森下・松本 [2005] は、エレクトリック・フィールド式を読取方法として採用している1機種(携帯電話に搭載されたもの)を対象に実験を行っており、平均で8割以上の受入率を得ている。

### (3) 虹彩照合装置の脆弱性評価研究

#### イ．研究の流れ

虹彩照合装置の脆弱性に関する研究成果として、松本・平林 [2003a, b] と松本・平林・佐藤 [2004] が発表されている。まず、松本・平林 [2003a] においては、紙製の人工虹彩の作製方法について検討を行っているほか、2種類の虹彩照合装置において人工虹彩を受け入れるか否かの実験を行っている。続く松本・平林 [2003b] は、松本・平林 [2003a] によって得られた知見を基に、比較的鮮明に撮影された眼画像を利用して人工虹彩を作製し、照合実験を行っている。また、松

本・平林・佐藤 [ 2004 ] は、眼画像の撮影に赤外線カメラを利用する手法を検討しているほか、照合実験の対象となる虹彩照合装置を1機種追加して実験を行っている。

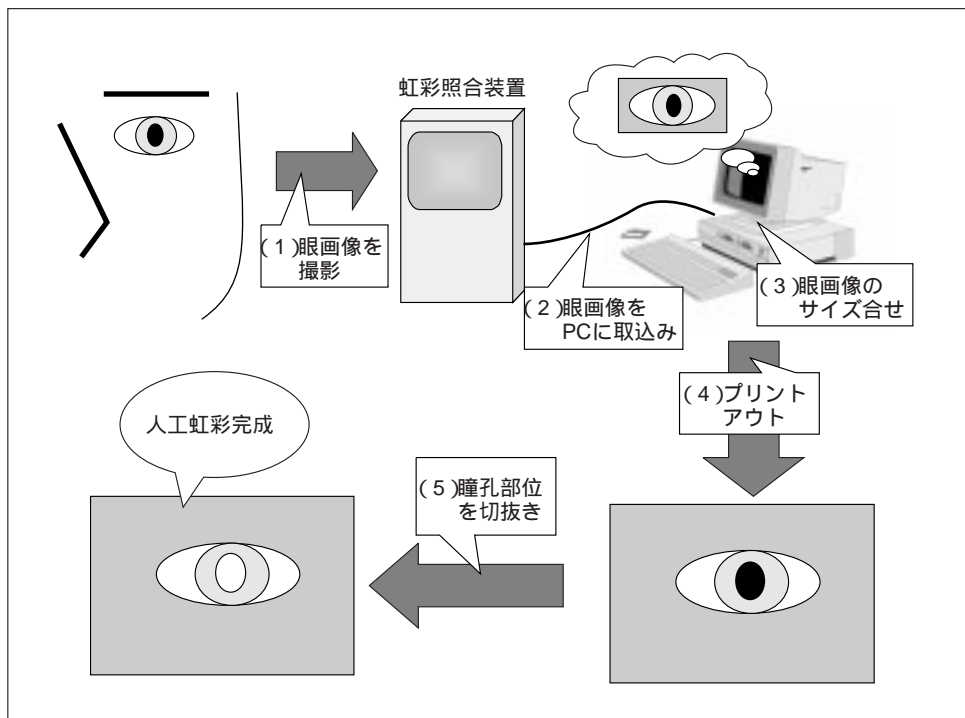
#### ロ．人工虹彩の作製方法

人工虹彩の作製方法は、一連の3つの研究に共通しており、以下のとおりである（図3参照）。

- 1 個人の（虹彩を含む）眼画像を撮影する。
- 2 撮影した眼画像をコンピュータに取り込む。
- 3 画像処理ソフトを用いて、眼画像が実際の眼のサイズと同一になるように画像サイズを調整する。
- 4 調整済みの眼画像をレーザー・プリンターによってインクジェット・プリンター用紙に印刷する。
- 5 印刷した眼画像の瞳孔部分をカッターで切り抜く。

松本・平林 [ 2003a, b ] では、眼画像を撮影する方法として、実験の対象としている虹彩照合装置において撮影されたものを利用している。松本・平林 [ 2003a ] においては、2つの眼画像を撮影し、各画像に対して1つずつ人工虹彩を作製している。これに対して、松本・平林 [ 2003b ] では、いくつかの眼画像を撮影し、それ

図3 人工虹彩の作製手順（虹彩照合装置で撮像する場合）



らのうちで最も状態がよい眼画像を選択して人工虹彩を1つだけ作製している。

松本・平林・佐藤 [2004] においては、虹彩照合装置において撮影する方法に加えて、赤外線レンズを用いたデジタル・マイクロスコープによって撮影する方法も検討している。また、松本・平林 [2003b] と同様に、最も状態のよい眼画像から1つの人工虹彩を作製している。

#### 八．虹彩照合装置における登録・照合方法

虹彩を用いた認証では、虹彩ビット列と呼ばれる特徴量が用いられるケースが一般的であるといわれている（瀬戸 [2002]）。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たうえで、各領域を走査してイメージ輝度の抽出を行い、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。

人工虹彩に関する一連の研究では、3種類の虹彩照合装置が採用されているが、いずれも上記の方法によって登録・照合を実施している。

#### 二．照合実験の結果

照合実験では、いずれの研究においても、登録、照合をそれぞれ生体虹彩と人工虹彩によって行い、全体で4種類の実験が実施されている。これらの中でも、登録は生体虹彩によって行い、照合は当該生体虹彩から作製された人工虹彩によって行われるというタイプの実験結果に焦点を当てて紹介する。

まず、松本・平林 [2003a] においては、2種類の虹彩照合装置を対象に、2つの人工虹彩によって照合実験が行われた。虹彩照合装置2機種は、いずれもネットワーク端末におけるログイン時の本人確認等での利用を想定したものである。5人の被験者によってそれぞれ20回ずつ照合が行われ、作製した人工虹彩の状態によって受入率が大きく変化することが示された。すなわち、一方の人工虹彩を用いると2機種とも受入率が平均8割を上回ったものの、もう1つの人工虹彩では受入率が平均4割程度まで低下するという現象が観察された。

こうした結果を受けて、松本・平林 [2003b] は、人工虹彩の作製プロセスに注意を払い、比較的鮮明な眼画像を材料として人工虹彩を作製するとともに、各被験者の照合実験の試行回数を100回に増やして再度実験を行っている。その結果、2種類の虹彩照合装置においていずれも平均8割以上の受入率となったことが報告されている。

松本・平林・佐藤 [2004] においては、上記の研究で用いられた2機種にゲート管理用の虹彩照合装置を実験対象として追加するとともに、眼画像の撮影に赤外線レンズを用いたデジタル・マイクロスコープを採用しているほか、被験者数も従来の5人から7人に増員している。その結果、赤外線レンズを利用して作製した人工虹彩はいずれの虹彩照合装置においても相対的に受け入れられにくく、平均で1～4割程度の受入率にとどまることが示されている。また、ゲート管理用の虹彩照合装置では、平均の受入率が約5割となり、他の機種の場合（8割以上）に比べて受入率が小さくなる傾向も観察されている。

#### (4) 小括

本節において紹介したように、比較的安価な材料や機器によって作製された人工指や人工虹彩が、いくつかの市販されている照合装置において比較的高い確率で受け入れられることが実証されている。一連の研究成果は、物理的に偽造された生体情報を生体認証システムが受け入れてしまうという脆弱性が生体認証システムにおいて現実に存在し、無視できないものであることを示唆している。現在の生体認証技術に対する高い期待を前提とすると、生体認証システムのセキュリティに大きく依存した業務システムが構築される可能性が高いと考えられる。このため、物理的な生体情報の偽造による脆弱性は、生体認証システムに関連する各種の脆弱性の中でも、今後最優先で対策を検討すべき項目の1つであるといえるであろう。

### 5 . 生体認証システムの脆弱性に関する今後の対応

#### (1) 2つの方向性

前節において紹介したように、いくつかの研究成果によって、物理的に偽造された生体情報を受け入れてしまうという脆弱性が実際に生体認証システムにおいて存在するほか、こうした脆弱性を突いた攻撃が比較的容易に実行可能であることが示唆されている。こうしたことから、今後、生体情報の物理的偽造の脆弱性に関して検討を進めることが必要である。

こうした方向での検討に加えて、今後金融分野においても生体認証技術を活用する場面が増えてくる可能性があることを勘案すると、生体認証システムにおける新たな脆弱性が発見された場合への対応に関しても、同システム導入時に十分検討しておくことが必要である。従来は、生体認証システムの活用事例の多くが企業内部における入退室管理等、比較的閉じた環境においての利用であり、生体認証システムの被認証者となる個人もある程度限定されていた。このため、生体情報の物理的偽造という脆弱性が特段深刻な問題とは認識されてこなかったと考えられる。しかし、今後、生体認証システムが金融分野をはじめとする公共性の高いサービスに導入され、一般の幅広い層に利用されるようになるとすれば、生体認証システムにおける脆弱性の指摘は、同システムの関係者に対してこれまで以上に大きなインパクトを与えることになろう。こうした点を踏まえると、今後新たな脆弱性が発見される可能性を考慮し、これに備えておくことが必要であるといえる。

以下では、これらの2つの方向で検討を行っていくうえで、具体的にどのような点に注目する必要があるか、また、どのような課題が存在するかについて考察を行う。

## (2) 生体情報の物理的偽造への対応

生体情報の物理的な偽造に関する脆弱性については、まず、脆弱性の評価をどのように行うか、また、生体検知機能をどのように活用するかに関して検討することが必要である。

### イ．脆弱性評価手法の確立

生体情報の物理的偽造に関する脆弱性の評価は、これまでの研究においては、偽造に利用可能と考えられる物理媒体や機器等を使って実際に偽造を行い、生体情報を偽造したものを生体認証システムに提示した際に、当該システムにおいてどの程度受け入れられるか、また、偽造を行うために必要なコストはどの程度かを、個別のシステムごとに実験を行い確認するという手法が採用されている。その結果明らかになった情報を基に、生体認証システムを利用している個別のアプリケーションにおいて具体的にどのような攻撃が想定されるか、また、攻撃が成功した場合にはどの程度の被害が発生しうるのかを分析し、複数の生体情報を組み合わせた認証方式（マルチモーダル）の利用、別の個人認証手段との併用等、脆弱性を軽減するための手段を適宜講じていくことが求められる。

以上のような手法による評価研究を積み重ねていくことによって、脆弱性評価に関するノウハウが蓄積され、実際の評価手法も洗練されたものになり、より効率的な評価手法の確立につながっていくと考えられる。その際には、実施した評価研究を、その結果とともに、第三者が追試可能なように実験の手順や条件を詳細に公表することが必要である。

また、こうした評価研究から得られる知見は、生体情報の物理的偽造の脆弱性を回避する有効な手段を考案する際の手掛かりになる場合もある。例えば、松本・平林 [2003b] および松本・平林・佐藤 [2004] では、虹彩照合装置の脆弱性評価の過程において、紙で作製した人工虹彩による照合時間が生体の虹彩による照合時間に比べて長くなる傾向にあるという結果を得ている。こうした結果は、照合に要する時間の長短によって虹彩の物理的偽造を検知するという手法のアイデアに結びつく。

### ロ．生体検知機能の開発と評価

脆弱性の評価に関する検討を進めるとともに、生体認証システムに提示された生体情報が偽造されたものであることをどのようにして検知するかについても検討することが必要である。こうした機能を実現する生体検知機能に関しては多種多様なアイデアが提案されているほか、特許等においても公開されている。また、実際に生体検知機能を搭載していることを明示した生体認証システムも提案されている。

しかしながら、そうした生体検知機能が期待どおりの効果を発揮するか否かについては、明確になっていない場合が多く、生体認証システムの利用者が生体検知機能の有効性を確認することは困難であるのが実情である。山田・松本・松本 [2000a]

に端を発する一連の評価研究においては、生体検知機能を搭載しているとされる指紋照合装置が、指紋付きゼラチンによって提示された指紋パターンを高い割合で受け入れたとの結果が報告されている。こうした事例からも、生体検知機能の評価が重要であることを容易に理解できる。

実際の生体認証システムに実装されている既存の生体検知機能を、生体情報の物理的偽造という観点から評価することが検討の第一歩になると考えられるが、こうした検討の実効性を高めるためには、生体検知機能に関する情報を開発・設計者、評価者、利用者間において共有するとともに、評価結果等について議論する場をどのように設けるかがポイントになるであろう。これまで、学会等のオープンな場において生体検知機能の評価に関して議論されることは極めて少なかったようである。こうした背景には、生体認証システムを開発・提案している企業の多くが、生体検知機能を実装しているか否か、また、実装しているとしてもその技術の詳細を明らかにしていないという事情がある（IBG [2003]、Valencia and Horn [2003]、Sandström [2004]）。生体検知機能に関する情報共有が有効に機能しないとすれば、検討の際に利用可能な情報は断片的なものとなり、十分な評価が困難になる可能性があるほか、評価結果がどの生体認証システムに関して適用可能であるかについても不明確となるおそれがある。こうした点を踏まえると、生体検知機能に関する情報の共有を可能にするための枠組みについて検討することが必要であるといえよう。

### (3) 未知なる脆弱性への備え

生体認証システムを導入する時点では知られていなかった脆弱性が、長期間システムを運用していく過程で顕現化する可能性がある。システム運営者の観点からみると、こうした問題への主な対応方針として次の3点が考えられる。

- ・システムを構成する要素や技術を別のものに置き換えることが相対的に容易であるという意味で、拡張性の高い生体認証システムを採用する。
  - ・脆弱性に関する最新情報を正確かつ迅速に収集し、その脆弱性が生体認証システムに与える影響を分析する体制を整備する。
  - ・新たな脆弱性が発見された場合、生体認証システムの利用者となる顧客に対して、当該脆弱性がシステムに及ぼす影響やその対応について迅速に情報提供を行う。
- 以下では、これらの項目の内容について説明する。

#### イ．拡張性の高いシステムの採用

生体認証システムの設計面では、拡張性を備えたシステムの実現が求められる。新たに発見された脆弱性によって現行システムにおいて採用していた生体認証技術のセキュリティ・レベルが著しく損なわれてしまった場合、当該技術の代わりに別の技術を導入することが困難であるとすれば、システム的大幅な変更が必要となるケースが考えられる。その結果、サービスの運営者にはサービスの継続に多大なコ

ストの負担を余儀なくされる状況も想定される。こうした問題を回避する方法の1つとして、セキュリティ・レベルの高い技術をシステムに容易に導入できるよう、採用する生体認証システムに対して高い拡張性を要件として定めることが挙げられる。

例えば、生体情報を読み取るセンサを別の手法に基づくものに交換する場合、当該システムの他の要素に影響を及ぼさないこと、あるいは、システムに登録できない顧客の割合が増加しないこと（未対応率が上昇しないこと）といった要件の設定が考えられる。また、生体情報の物理的偽造に対する耐性を高める目的で生体検知機能の搭載が必要となった場合を想定し、生体検知機能をシステムに容易に追加することができるといった要件を設定することも考えられる。

こうした要件を設定する際には、生体認証システムのどの部分に対して拡張性を要求すべきかについて検討する必要がある。これは、生体認証システムの構成や採用されている生体情報の特性だけでなく、当該システムが利用されるアプリケーション等に依存することから、システムの運営者がこれらの事情を考慮したうえで決定することが求められる。

#### ロ．情報の収集・分析を行う体制の整備

脆弱性に対処するための運用面における第一歩は情報の収集・分析である。生体認証システムの脆弱性に関する情報は、情報セキュリティを対象分野とする学会において発表されるケースがあるほか、情報技術関連の科学雑誌・業界誌において紹介される場合もある。学会に関しては、わが国においては、例えば電子情報通信学会や情報処理学会が挙げられる。こうした場に継続的に参加するほか、関連分野の研究者と適宜情報交換を行い、留意すべき脆弱性に関する研究成果等が発表されていないかをチェックする必要がある。実際に留意すべき脆弱性に関する情報を得た場合には、その脆弱性が、当該システムおよびその利用環境において深刻な問題となりうるか否かを確認することが求められる。そのうえで、必要となる対策を適宜講じることとなる。

生体認証システムの運営者の中には、当該システムの管理・運用を専らベンダ等に委託し、脆弱性への対応についても大部分を任せるといったケースも考えられる。こうしたケースにおいても、生体認証システムによるアクセス制御の対象となっているアプリケーションの重要度や想定環境等に精通し、生体認証システムの設定変更等の最終決定を行う運営者が、脆弱性やその分析内容について相応の判断を行うことが必要になる場面が必ず出てくると思われる。そうした状況においても適切な対応が可能となるように、生体認証システムの運用者みずからが脆弱性に関する情報の収集と分析を正確かつ迅速に行うことができる体制をあらかじめ整備しておくことが必要である。

## 八．脆弱性の影響等に関する情報の適切かつ迅速な提供

生体認証システムの脆弱性評価の結果等に関する情報を同システムの顧客に迅速に提供することも、システムに対する顧客の信頼を維持していくうえで必要であると考えられる。仮に、既存の生体認証システムにおいて深刻な脆弱性が存在することが明らかになった場合に、顧客に対して同システムへの影響に関して適切なタイミングで説明を行わなかったとすれば、顧客は同システムのセキュリティ・レベルについて不快感を抱き、関連するサービスを利用しなくなってしまう可能性がある。こうした問題がいったん発生すると、その他の生体認証システムに対する信頼も連鎖的に低下してしまう可能性も否定できない。

どのような情報を提供することが望ましいかという点に関しては、少なくとも、次の項目に関する情報を適切かつ迅速に顧客等に開示することが求められよう。

- ・問題となっている脆弱性とはどのようなものか、どのような環境のもとでどのような弱点が発生するのか。
- ・当該脆弱性に関して、生体認証システムの設計時において考慮していたか否か、考慮していなかったとすればその理由は。
- ・当該脆弱性を排除または軽減する方法としてどのようなものが考えられるのか。
- ・生体認証システムにおいて当該脆弱性を排除するために、どのような対策を講じる方針か、また、そうした対策の実施によって既存のシステムにどのような影響が生じるのか。

こうした情報を提供するためには、システムの運営者が脆弱性に関する情報を迅速に収集・分析することが前提となる。

## 6．おわりに

生体認証技術は、個人を認証する有力な技術の1つとして現在注目を集めており、入国管理等の公共部門において今後活用される見通しであるほか、金融サービスにおいても顧客の本人確認手段として採用する動きがみられている。また、わが国では、こうした動きに先立って生体認証技術の精度評価に関する標準規格等が既に策定されたほか、ISOにおいては、関連する国際標準の審議が活発に進められているところである。

生体認証技術を採用する動きが広がる中で、それらを安全に活用していくために、生体認証システムに内在する脆弱性にこれまで以上に注意を払っていく必要がある。既に明らかになっている脆弱性の中でも、人工指や人工虹彩に代表されるように、物理的に偽造された生体情報を受け入れてしまうという脆弱性に今後注目していくことが求められる。こうした脆弱性に対抗する生体検知機能に関する研究についても、その動向を注視する必要がある。

特に、幅広い層の顧客が利用する金融サービスにおいて生体認証技術の導入を検討する場合には、少なくとも既に明らかになっている脆弱性を考慮し、候補となっ

ている生体認証システムにおいてそうした脆弱性が存在するか否かを厳格に確認することが必要であると考えられる。本稿では、指紋照合装置や虹彩照合装置の脆弱性についてかなり詳細に解説したが、こうした研究蓄積の存在は指紋や虹彩を用いる認証技術がその他の生体認証技術よりも必ずしも劣位にあることを意味しない。むしろ、こうした研究蓄積の存在は、これらの技術の安全性を客観的に評価することを可能としており、研究蓄積が存在する技術は、研究蓄積がないものに比べて相対的に信頼できるともいえる。この点、学界等において評価の対象となっておらず、脆弱性に関する報告が行われていない生体認証技術については、当該分野の学者や研究者等に評価を依頼し、その結果を慎重に検討したうえで、実際に採用するか否かを判断すべきである。

また、既存の脆弱性だけでなく、未知の脆弱性についても将来顕現化することを想定し、新たな脆弱性への対応方針とそのため体制整備を進めておくことが必要である。具体的には、拡張性の高い生体認証システムの実現、脆弱性に関する情報の収集・分析や、発見された脆弱性の影響等に関する情報の迅速な提供を可能にするための体制整備等について検討することが考えられる。

こうした点に留意して脆弱性に対して適切な措置を講じ、安全で信頼性の高い生体認証システムが継続的に利用可能になることが望まれる。今後も、生体認証技術とその脆弱性に関する動向に注目していく必要がある。

## 参考文献

- 青山奈保子・遠藤由紀子・平林昌志・太田和夫・松本 勉、「指紋画像からの人工指作製（その3）：デジタルカメラを用いた場合」、『2003年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2003年、393～398頁
- 池田銀行、「セキュリティ重視「ICキャッシュカード」の実用化・本格発行開始について～ICカード“身体認証機能”を搭載し、全国初の“複数口座”対応～」、『2005年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2005年（<http://www.ikedabank.co.jp/news04/news0117.html>、アクセス日：2005年1月20日）
- 遠藤由紀子・平林昌志・松本 勉、「指紋照合装置は人工指を受け入れるか（その5）」、『情報処理学会研究報告』Vol. 2003、No. 18、2003年、251～256頁
- ・松本 勉、「指紋照合装置は人工指を受け入れるか（その4）」、『コンピュータセキュリティシンポジウム2002論文集』、情報処理学会、2002年、245～250頁
- 大木哲史・田島 賢・赤塚志郎・小松尚久・笠原正雄、「Fuzzy Biometric Vault Schemeによるテンプレートの安全性に関する一考察」、『2005年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2005年、547～552頁
- 大島康志・松本 勉、「ユーザ認証における非常時通報」、『電子情報通信学会技術研究報告』Vol. 103、No. 315、2003年、17～22頁
- 金融情報システムセンター（FISC）、「金融機関業務のシステム化に関するアンケート調査結果」、『金融情報システム』No. 273、2004年
- ・「生体認証技術の最新動向と金融機関における活用」、『金融情報システム』No. 276、2005年
- 金融庁、「金融分野における個人情報の保護に関するガイドライン」、『2004年（<http://www.fsa.go.jp/siryou/siryou/ki-hogo/01.pdf>、アクセス日：2005年1月24日）
- ・「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」、『2005年a（<http://www.fsa.go.jp/siryou/siryou/ki-hogo/04.pdf>、アクセス日：2005年1月24日）
- ・「偽造キャッシュカード問題への対応について」、『2005年b（<http://www.fsa.go.jp/news/newsj/16/ginkou/f-20050222-1/02.pdf>、アクセス日：2005年2月25日）
- 楠山倫夫、「バイオメトリクス最新認証技術：非接触型手のひら静脈認証技術の今後の展望」、『シメディア・バイオメトリクスの実用化検証セミナー発表資料、2004年
- 小松尚久、「個人認証」、『情報セキュリティハンドブック』、電子情報通信学会編、オーム社、2004年、275～283頁
- ・内田 薫・坂野 鋭・和田誓一・池野修一、「バイオメトリクス認証の評価基準」、『情報技術標準NEWSLETTER』No. 60、情報処理学会、2003年、2～5頁
- 情報処理振興事業協会、「スマートカードの安全性に関する調査調査報告書」、『2000年情報処理推進機構、電子政府行政事業化事業：各国バイオメトリクスセキュリティ動向の調査』、2004年

- 鷲見和彦・松山隆司・中嶋晴久、「バイオメトリクス認証テンプレート保護に関する検討」  
『2005年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2005年、535～540頁
- スルガ銀行、「～手のひら静脈認証～バイオセキュリティ預金」  
2004年 (<http://www.surugabank.co.jp/surugabank/prod/yokin/bio.html>、アクセス日：2005年1月14日)
- 瀬戸洋一、「サイバーセキュリティにおける生体認証技術」  
共立出版、2002年  
(編著)『ユビキタス時代のバイオメトリクスセキュリティ』、日本工業出版、2003年  
、「SC37専門委員会 (Biometrics / バイオメトリクス)」、『情報技術標準NEWSLETTER』  
No. 62、情報処理学会、2004年a、34～36頁  
、「SC37 (Biometrics / バイオメトリクス) 総会報告」、『情報技術標準NEWS LETTER』  
No. 63、情報処理学会、2004年b、20～21頁
- 全国銀行協会、「偽造キャッシュカード対策に関する申し合わせ」  
2005年 (<http://www.zenginkyo.or.jp/news/17/pdf/news170125.pdf>、アクセス日：2005年2月25日)
- 宝木和夫、「SC27 (IT Security Techniques / セキュリティ技術) 総会報告」  
『情報技術標準NEWSLETTER』No. 63、情報処理学会、2004年、13～14頁
- 田辺壮宏・森下朋樹・松本 勉、「携帯機器に搭載された指紋照合装置は人工指を受け入れるか」  
『2005年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2005年、553～558頁
- 東京三菱銀行、「スーパーICカード「東京三菱 - VISA」ご留意事項」  
2004年 (<http://www.btm.co.jp/tsukau/card/visa/ryui.htm#security>、アクセス日：2005年1月14日)
- 中山靖司・小松尚久、「バイオメトリクスによる個人認証技術の現状と課題 金融サービスへの適用の可能性」  
『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年、155～192頁
- 日本規格協会情報技術標準化研究センター (INSTAC)、「耐タンパー性調査研究委員会報告書」  
2003年
- 日本銀行金融研究所 (TC68国内委員会事務局)、「ISO/TC68/SC2-SC6国内検討委員会 (平成15年12月18日開催) 議事録」  
2004年a (<http://www.imes.boj.or.jp/iso/gijiroku/h15/gi031218.pdf>)  
、「ISO/TC68/SC2-SC6国内検討委員会 (平成16年11月2日開催) 議事録」  
2004年b (<http://www.imes.boj.or.jp/iso/gijiroku/h16/gi041102.pdf>)
- 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a  
、「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b  
、「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a  
、「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b  
、「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a  
、「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b  
、「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c

日本バイオメトリクス認証協議会 (JBAA) 『バイオメトリクスシステムの脆弱性に関する報告書Ver. 0.6』、2003年

日本郵政公社、『郵便貯金ICキャッシュカードの発行について』、2005年 (<http://www.japanpost.jp/pressrelease/japanese/kawase/050228j301.html>、アクセス日：2005年3月2日)

林 義昭、「SC17 (Cards and Personal Identification) 総会報告」、『情報技術標準NEWS LETTER』No. 64、情報処理学会、2004年、9～10頁

平林昌志・田辺壮宏・松本 勉、「指紋照合装置は人工指を受け入れるか(その6)」、『電子情報通信学会技術研究報告』Vol. 103、No. 713、2004年、151～154頁

広島銀行、『多機能カード『(ひろぎん) VALUE ONE (バリューワン)』の取扱開始について』、2005年 (<http://www.hirogin.co.jp/ir/news/paper/news050225.html>、アクセス日：2005年3月2日)

藤枝一郎・松山悦司・田口耕造、「指紋画像の色変化に基づく偽造対策の可能性」、『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』、電子情報通信学会、2003年、49～52頁

古井貞熙、「音声による本人認証：第1部 音声による本人認証のしくみと技術動向」、『情報処理』40(11)、情報処理学会、1999年、1088～1091頁

星野 哲・松本弘之・松本 勉、「指紋画像からの人工指作製」、『電子情報通信学会技術研究報告』Vol. 101、No. 311、2001年、53～60頁

・遠藤由紀子・松本弘之・松本 勉、「指紋画像からの人工指作製(その2)」、『2002年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2002年、821～826頁  
北海民友新聞社、『手をかざせば本人確認(紋別信金)』、2005年 ([http://www.minyu.ne.jp/digitalnews/050119\\_3.htm](http://www.minyu.ne.jp/digitalnews/050119_3.htm)、アクセス日：2005年1月20日)

堀内かほり、「濡れた指、乾燥した指 - 指紋認証の実際」、『日経バイト』2005 April、日経BP社、2005年、60～67頁

松本 勉、「金融取引における生体認証について」、『金融庁・第9回偽造キャッシュカード問題に関するスタディグループ(2005年4月15日)説明資料』、2005年 ([http://www.fsa.go.jp/singi/singi\\_fccsg/gaiyou/f-20050415-gingi\\_fccsg/02.pdf](http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-gingi_fccsg/02.pdf)、アクセス日時：2005年5月13日)

・鉢舘拓二・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』Vol. 104、No. 732、電子情報通信学会、2005年a、81～82頁

・ 、 「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』Vol. 105、No. 51、電子情報通信学会、2005年b、29～33頁

・平林昌志、「虹彩照合技術の脆弱性評価(その1)」、『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』、電子情報通信学会、2003年a、53～59頁

・ 、 「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論文集』、情報処理学会、2003年b、187～192頁

・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予稿集』、電子情報通信学会、2004年、701～706頁

- 松本弘之・宇根正志・松本 勉・岩下直行・菅原嗣高、「人工物メトリクスの評価における現状と課題」、『金融研究』第23巻別冊第1号、日本銀行金融研究所、2004年、61～140頁
- 三浦直人・長坂晃朗・宮武孝文、「線追跡の反復試行に基づく指静脈パターンの抽出と個人認証への応用」、『電子情報通信学会論文誌』Vol. J86-D-、No. 5、電子情報通信学会、2003年、678～687頁
- みずほ銀行、「ICキャッシュカード取引時の生体認証による本人確認手法の導入について」、2005年（<http://www.mizuhobank.co.jp/company/release/2005/pdf/news050302.pdf>、アクセス日：2005年3月4日）
- 三井住友銀行、「ICキャッシュカードへの生体認証導入について」、2005年（[http://www.smbc.co.jp/news/j500056\\_01.html](http://www.smbc.co.jp/news/j500056_01.html)、アクセス日：2005年3月2日）
- 森 雅博・新崎 卓・佐々木繁、「バイオメトリクス認証技術」、『FUJITSU』54(4)、富士通株式会社、2003年、272～279頁（<http://magazine.fujitsu.com/vol54-4/paper04.pdf>、アクセス日：2005年2月10日）
- 門田 啓・黄 磊・吉本誠司、「個別安全性を保証できる指紋の精度評価」、『2005年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2005年、541～546頁
- 山田浩二・松本弘之・松本 勉、「指紋照合装置は人工指を受け入れるか」、『電子情報通信学会技術研究報告』Vol. 100、No. 213、2000年a、159～166頁
- ・ ・ ・ ・ ・、「指紋照合装置は人工指を受け入れるか（その2）」、『コンピュータセキュリティシンポジウム2000論文集』、情報処理学会、2000年b、109～114頁
- ・ ・ ・ ・ ・、「指紋照合装置は人工指を受け入れるか（その3）」、『2001年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2001年、719～724頁
- American National Standards Institute (ANSI), *ANS X9.84: Biometric Information Management and Security for the Financial Services Industry*, 2003.
- Biometrics Management Office (BMO), and National Security Agency (NSA), *U.S. Government Biometric Verification Mode Protection Profile (PP) for Medium Robustness Environments*, Version 1.0, 2003. ([http://niap.nist.gov/cc-scheme/pp/PP\\_VID1022.html](http://niap.nist.gov/cc-scheme/pp/PP_VID1022.html), access date: February 10, 2005)
- Blommé, Johan, *Evaluation of biometric security systems against artificial fingers*, 2003. (<http://www.ep.liu.se/exiobb/isv/2003/3514/exiobb.pdf>, access date: January 19, 2005)
- Bolle, Ruud M., Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior, *Guide to Biometrics*, Springer, 2003.
- Common Criteria Biometric Evaluation Methodology Working Group (CCBEMWG), *Common Criteria - Common Methodology for Information Technology Security Evaluation - Biometric Evaluation Methodology Supplement (BEM)*, 2003. ([http://www.cesg.gov.uk/site/ast/biometrics/media/BEM\\_10.pdf](http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf), access date: February 10, 2005)
- Daugman, John, "How Iris Recognition Works," *IEEE Transactions on Circuits and Systems for Video Technology*, 14 (1), 2004a, pp. 21-30. (<http://www.cl.cam.ac.uk/users/igd1000/irisrecog.pdf>, access date: February 10, 2005)

- , "Iris Recognition and Anti-Spoofing Countermeasures," *Proceedings of Biometrics 2004*, 2004b.
- Doddington, George, Walter Liggett, Alvin Martin, Mark Przybocki, and Douglas Reynolds, "SHEEP, GOATS, LAMBS and WOLVES: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation," *Proceedings of ICASSP 98*, 1998, pp. 125-128. ([http://www.nist.gov/speech/publications/papersrc/icslp\\_98.pdf](http://www.nist.gov/speech/publications/papersrc/icslp_98.pdf), access date: February 10, 2005)
- Hill, Christopher James, *Risk of Masquerade Arising from the Storage of Biometrics*, 2001. (<http://chris.fornax.net/download/thesis/thesis.pdf>, access date: February 7, 2005)
- International Biometric Group (IBG), *Liveness Detection in Biometric Systems*, 2003. (<http://www.ibgweb.com/reports/public/reports/liveness.html>, access date: January 20, 2005)
- International Civil Aviation Organization (ICAO), TAG MRTD/NTWG, *Biometrics Deployment of Machine Readable Travel Documents: Technical Report (Version 2.0)*, 2004.
- Ligon, Aaron, *An Investigation Into the Vulnerability of the Siemens ID Mouse Professional Version 4*, 2002. (<http://www.bromba.com/knowhow/idm4vul.ntm>, access date: January 19, 2005)
- Mansfield, Anthony J., and James L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01*, 2002. (<http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf>, access date: February 10, 2005)
- Matsumoto, Hiroyuki, and Tsutomu Matsumoto, "Clone Match Rate Evaluation for an Artifact-metric System," *IPSI Journal*, 44 (8), 2003, pp. 1991-2001.
- Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems," *Optical Security and Counterfeit Deterrence Techniques IV, Proceeding of SPIE*, Vol. 4677, SPIE (The International Society for Optical Engineering), 2002, pp. 275-289. (<http://cryptome.org/gummy.htm>, access date: February 10, 2005)
- van der Putte, Ton, and Jeroen Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned," *Proceeding of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Press, 2000, pp. 289-303. ([http://www.keuning.com/biometrv/Biometrical\\_Fingerprint\\_Recognition.pdf](http://www.keuning.com/biometrv/Biometrical_Fingerprint_Recognition.pdf), access date: February 10, 2005)
- Quisquater, Jean-Jacques, *Side channel attacks — State-of-the-art —*, 2002. ([http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047\\_Side\\_Channel\\_report.pdf](http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf), access date: February 10, 2005)
- Sandström, Marie, *Liveness Detection in Fingerprint Recognition Systems*, 2004. (<http://www.ep.liu.se/exiobb/isv/2004/3557/exiobb.pdf>, access date: February 10, 2005)
- Schuckers, Stephanie A., "Spoofing and Anti-Spoofing Measures," *Information Security Technical Report*, 7 (4), Royal Holloway, University of London, 2002, pp. 56-62. (<http://www.citer.wvu.edu/members/publications/files/15-Sschuckers-Elservior02.pdf>, access date: February 10, 2005)
- Thalheim, Lisa, Jan Krissler, and Peter-Michael Ziegler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test," *c't*, 2002, p. 114. (<http://www.heise.de/ct/english/02/11/114>, access date: February 10, 2005)

- United Kingdom Government Biometrics Working Group (UKGBWG), *Biometric Device Protection Profile, Draft Issue 0.82*, 2001.
- Valencia, Valorie S., and Christopher Horn, "Biometric Liveness Testing," *Biometrics*, John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins eds., McGraw-Hill, 2003, pp. 139-149.
- Willis, David, and Mike Lee, "Six Biometric Devices Point The Finger At Security," *Network Computing*, 1998. (<http://www.nwc.com/91/910r1.html>, access date: January 19, 2005)

