IMES DISCUSSION PAPER SERIES

生体認証システムの脆弱性の分析と生体検知技術の研究動向

鈴木雅貴（すずきまさたか）・宇根正志（うねまさし）

Discussion Paper No. 2009-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2009-J-6
2009 年 5 月

生体認証システムの脆弱性の分析と生体検知技術の研究動向

鈴木雅貴*・宇根正志**

要　　旨

身体的特徴等を利用して個人の認証を行う生体認証システムは、近年、金融分野をはじめとする幅広い分野において利用されつつある。生体認証システムを活用していく際には、生体認証特有の脆弱性としてどのようなものが知られているかを把握し、適切な対策を講じていくことが重要である。特に、生きている人間の身体部分でない物体を誤って受け入れてしまうという脆弱性が一部の市販のシステムにおいて存在する可能性が学会等において指摘されており、こうしたなりすましを目的とした攻撃法への対応が必要といわれている。

本稿では、生体認証システムにおけるなりすましに焦点を当てて、最近の国際標準化の動向や学会における研究成果等を踏まえつつ、生体認証特有の脆弱性となりすましの方法との関係を改めて整理する。その結果として、既存文献で指摘されている以外のなりすまし方法をいくつか示し、それらへの網羅的な対策の講じ方について考察する。また、人工物を用いた攻撃への対策の 1 つである生体検知技術に焦点を当てて、研究動向や本技術を導入・利用する際に留意すべき評価項目について研究事例を基に考察し、生体検知の精度の比較を可能にするための検討が今後重要であることを説明する。

キーワード：生体認証システム、ISO/IEC 19792、脆弱性、なりすまし、
　　生体検知技術、指紋
JEL classification: L86、L96、Z00

*　日本銀行金融研究所（E-mail：masataka.suzuki@boj.or.jp）
**　日本銀行金融研究所企画役（E-mail：masashi.une@boj.or.jp）

本稿を作成するに当たっては、独立行政法人産業技術総合研究所情報セキュリティ研究センターの大塚玲セキュリティ基盤技術研究チーム長と国立大学法人静岡大学創造科学技術大学院の西垣正勝准教授から有益なコメントをいただいた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行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。

目次

1．はじめに

生体認証システムは、PC へのログインや建物への入館の際の本人確認手段として広く利用されているほか、最近では、空港での入国審査における本人確認等に利用されるようになってきている。金融分野おいても、従業員の本人確認のほか、指や掌の静脈パターンを用いた生体認証を ATM における顧客の本人確認に利用する動きがみられる。生体認証システムを適切に選択し利用するためには、セキュリティ評価の実施が求められるほか、生体認証システムの脆弱性や攻撃の洗出し、攻撃への対策の整理等が必要である。国際標準策定の場においても、生体認証システムのセキュリティ評価・認証に関する標準案（ISO/IEC 19792）の審議が進められている。

こうしたなか、実際に運用されている一部の生体認証システムに対して分離された生体部位や人工物を提示するといった事例[1]が近年発生しており、従来理論上のものとみられてきた生体認証システム特有の脆弱性を現実のものとして認識することの重要性が改めて示されている。また、ウルフ攻撃（Une, Otsuka, and Imai［2008］）等の新たな攻撃法も提案されてきている。生体認証システムは、他のセキュリティ・システムと同様に、時間の経過とともに新しい脆弱性や攻撃法が提案され、そのセキュリティは徐々に低下していくという性格をもつ。上記の事例やウルフ攻撃の提案からも読み取れるように、今後中長期的に生体認証システムを利用していくうえで、新たな脆弱性を考慮しつつ、漏れのない対策を講じていくことが求められる。

本稿では、生体認証システムにおける攻撃のうちなりすましに焦点を当てて、既存の検討成果に加えて、学会で提案されている新たな攻撃法や対策の調査を行い、脆弱性となりすましの関係を整理する。具体的には、なりすましの行為を 2 つの行為に分割し、各行為を実行する方法（実行方法と呼ぶ）の組合せによって表現するという田村・宇根［2007］のアプローチを参照し、生体認証システムの脆弱性を組み合わせて各実行方法を表現するという手法を採用する。また、個々の実行方法への対策についても整理を行い、生体認証システムにおけるなりすましへの対策の講じ方について考察を行う。こうした検討結果を参照することで、なりすましへの対策を講じる際に、想定されるなりすまし方法に対して対策の漏れを減らすことができるようになると考えられる。

---

[1] マレーシアでは、イモビライザーにおける本人確認に指紋を利用している自動車の運転手が、窃盗団に襲われ指を分離されたという事件が発生している（Kent［2005］）。また、わが国では、指紋のような模様が付いたテープを貼り付けた指を提示することで、地方空港の入国審査を通過したという事件が発生している（読売新聞［2009］）。

また、なりすましへの対策のうち、近年評価の観点から研究が進展してきている生体検知技術に焦点を当てて、生体検知技術の導入・利用を検討するうえで重要になると考えられる評価項目について考察する。具体的には、生体検知の精度、利用者の利便性への影響、導入コストについて、留意すべき点を示す。そのうえで、研究事例を取り挙げ、そうした評価項目がどの程度考慮されているかを議論する。

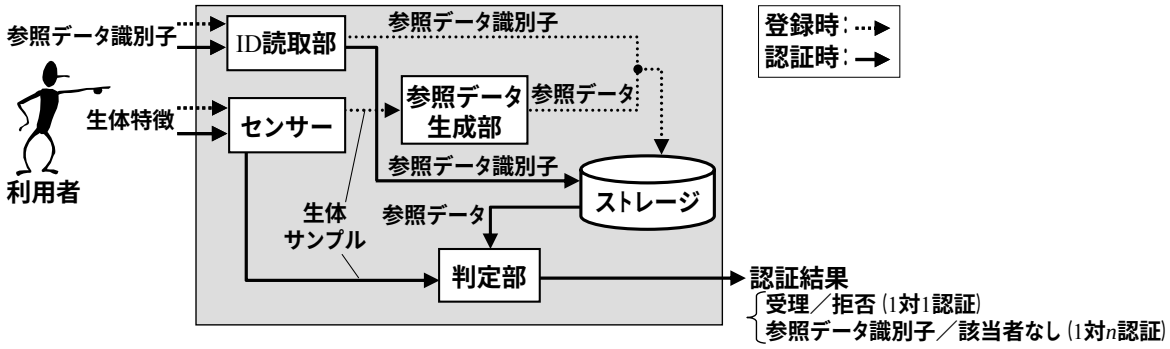
本稿の構成は以下のとおりである。2 **節**では、検討対象とする生体認証システム、攻撃、攻撃者を説明したうえで、生体認証システムの脆弱性となりすまし方法の関係を整理する。3 **節**では、各なりすまし方法への対策の講じ方について考察する。4 **節**では、生体検知技術の研究動向と生体検知の処理について概要を紹介したうえで、本技術を導入・利用する立場からの留意点について考察する。5 **節**では、2〜4 **節**の検討を踏まえて、金融機関や生体認証システムのベンダーへのインプリケーションを示す。

2．生体認証システム特有の脆弱性となりすましの方法

(1) 検討対象とする攻撃と攻撃者の設定

イ． 検討対象とする生体認証システム

まず、本稿で検討対象とする生体認証システムを示す。これまでにさまざまな生体認証システムのモデルが示されているが（例えば、JBAA［2003］、BSC［2006］、ISO［2008］）、利用者が自分の識別情報を生体認証システムに提示する処理についても明示的に扱っている宇根・松本［2005］におけるモデルを単純化して用いることとする（図表 1参照）。



図表1．検討対象とする生体認証システム

また、汎用的な生体認証技術の国際標準化を担当する ISO/IEC JTC1/SC37 では、生体認証技術に関する用語の統一化を行っている。その成果は、SC37 のスタンディング・ドキュメント 2（SD2 – Harmonized biometric vocabulary）のドラフト（ISO and IEC［2008］）として公表されている[2]。本稿では、本ドラフトを参照し、次の用語を用いることとする。

- 生体特徴（biometric characteristic）：生体認証に用いられる人間の身体的特徴または行動的特徴であり、指紋や静脈パターン等が挙げられる。
- 生体サンプル（biometric sample）：生体特徴を生体認証システムのセンサーで読み取ったデータであり、例えば、センサーで読み取った指紋画像等が挙げられる。
- 参照データ（biometric reference）：照合のために生体サンプルから生成され、ストレージに登録されるデータである。参照データの形式は個々の生体認証

[2] SD2 の最新版のドラフトは、ISO/IEC JTC1/SC37 のウェブサイトから入手可能である。

システムに依存しており、例えば、指紋画像をそのまま参照データとするケースや指紋画像から抽出した特徴点の座標を参照データとするケースが考えられる。

・ 参照データ識別子（biometric reference identifier）：利用者の参照データを識別するための情報である。

・ 照合スコア（comparison score）：照合結果を示す数値であり、認証時に読み取った生体サンプルと参照データがどの程度一致しているかを表す。

次に、利用者が不正や誤操作を行わない正常な利用を想定した場合の生体認証システムにおける登録と認証の手順を順にみていく。

(イ) 登録時の手順

e-1. 利用者は、ID 読取部に自分の参照データ識別子を入力する。

e-2. 利用者は、自分の生体特徴をセンサーに提示する。センサーは、生体特徴を読み取って生体サンプルを生成し、これを参照データ生成部に渡す。

e-3. 参照データ生成部は、生体サンプルから参照データを生成する。

e-4. 参照データと参照データ識別子のペアをストレージに登録する。ストレージは、複数のペアが登録されるデータベースとして実現される場合や個々の利用者のペアのみが登録される IC カードとして実現される場合がある。

(ロ) 認証時の手順

v-1. 1 対 1 認証の場合には、ID 読取部は、利用者が入力した参照データ識別子をストレージに渡す。1 対 n 認証の場合には、利用者は参照データ識別子を入力しない。

v-2. 利用者は、自分の生体特徴をセンサーに提示する。センサーは、生体特徴を読み取って生体サンプルを生成し、これを判定部に渡す。

v-3. 1 対 1 認証の場合には、判定部は、まず、生体サンプルから固有のパターンを抽出するなどの処理を行うとともに、参照データ識別子に対応する参照データをストレージから読み出す。これらを照合し、照合スコアを求め、予め設定されていた判定しきい値と比較して、一致か不一致かを判定する。一致の場合には「受理」を、不一致の場合には「拒否」を出力する。

1 対 n 認証の場合には、判定部は、まず、生体サンプルから固有のパターンを抽出するなどの処理を行ったうえで、ストレージに登録されている複数の参照データと順次比較し、一致と判定する場合には当該参照データに対応する参照データ識別子を出力する。一致と判定する参照データがない場合には「該当者なし」を出力する。

ロ． 検討対象とする攻撃

生体認証システムに対する主な攻撃として、まず、なりすましが挙げられる。なりすましは、登録時と認証時のそれぞれにおいて想定される。登録時においては、攻撃者自身の参照データ識別子を入力したうえで、他人の生体特徴や生体特徴を合成したもの等に対応する参照データを登録する攻撃（攻撃①）と、他人の参照データ識別子を入力したうえで、攻撃者自身の生体特徴に対応する参照データを登録する攻撃（攻撃②）が考えられる。認証時においては、攻撃者がなりすまし対象者の参照データ識別子を入力したうえで、何らかの情報をセンサーに提示する、あるいは、生体認証システム内に電気的に挿入することによって受理を出力させる攻撃（攻撃③）が考えられる。これらのうち、攻撃②については、登録時に他人になりすまして不正な登録を行うといった攻撃であるが、これは登録時の本人確認の問題であり、生体認証システム自体の機能の問題ではないことから、ここでは検討対象としない。

なりすまし可能な場合には、次のような攻撃が想定される。ただし、利用者 A は攻撃の対象となる利用者、利用者 B と利用者 C は結託している攻撃者とする。

- 特定の部屋における入退管理に生体認証システムが利用されている場合、利用者 B は、自分以外の無権限者（利用者 C）を自分の代わりに入室させるために、利用者 B の参照データ識別子と利用者 C の生体特徴に対応する参照データを登録する（攻撃①の例）
- ATM における顧客の本人確認に利用者 A が生体認証システムを利用している場合に、利用者 B が、利用者 A になりすまし、利用者 A の口座から預金を引き出す（攻撃③の例）。
- ATM における顧客の本人確認に生体認証システムを利用している場合、利用者 C が予め口座を開設しておき、利用者 C が預金を引き出すことが物理的に困難なタイミングを見計らって、利用者 B が利用者 C の口座から預金を引き出す。その後、利用者 C が他人に預金を引き出されたことを主張し、銀行に損害の補填を請求する（攻撃③の例）。

このほかにも、生体認証システムへの攻撃として、センサーの破壊や生体認証システムへの供給電力の遮断等によりサービスを正常に提供できないようにする攻撃（サービス妨害）が考えられる。また、不正入国者が生体認証システムに登録されているブラックリストと一致しないように変装するケースのように、ブラックリストによる検査を回避する攻撃（認証の回避）が考えられる。

サービス妨害については生体認証システムに限らず情報システム一般の課題であるほか、認証の回避については ATM における顧客の本人確認ではブラックリストによる検査を行っていないことから、本稿ではなりすましを検討対象と

する。

ハ． 検討対象とする攻撃者

なりすましを行う攻撃者の条件として、以下のものを想定する。

- 攻撃者は、なりすまし対象者の参照データ識別子を入手可能である。
  - ✧ なりすましを行うためには、なりすまし対象者の参照データ識別子を特定する必要がある。本稿では、仮に参照データ識別子が特定されていたとしても、なりすましに対抗できるか否かを検討することに重点を置くこととする。なお、参照データ識別子の入力作業については記述しないこととする。
- 攻撃者は、センサーの読取方式を知っているものの、生体認証システムの内部構造や各処理に関する知識を事前に有していない。
  - ✧ 現行の生体認証システムは、内部仕様を公開していないものが多いため、攻撃者は、内部構造や各処理に関する知識を事前には有していないとする。ただし、生体認証システムの脆弱性を利用することで内部を解析可能な場合には、こうした知識を得ることができ、例えば、攻撃者自身の生体特徴に対応する生体サンプルや参照データを生成できるとする[3]。一方、生体認証システムの内部を解析しなくとも、センサーを観察することで、センサーの読取方式（光学式、静電容量式等）を推測できるとする。

(2) なりすましを目的とした攻撃と脆弱性の関係

イ． 攻撃を構成する行為と脆弱性の関係

なりすましの方法の検討については、なりすましの行為を 2 つ（攻撃対象の生体認証システムに何らかの入力を行う行為、そのための準備を行う行為）に分割し、各行為の実行方法の組合せによってなりすまし方法を表現するというアプローチが提案されている（田村・宇根［2007］）。本アプローチは、既知の実行方法の組合せを整理し、より多くのなりすまし方法を洗い出すことができる点で優れている。田村・宇根［2007］は、定義した 7 つの基本処理の組合せ

---

[3] ウルフ攻撃の論文（Une, Otsuka, and Imai［2008］）では、攻撃対象の生体認証システムの内部仕様（照合アルゴリズム等）に関する知識を有する攻撃者を想定している。本稿では、ウルフ攻撃が実行される際には、「データの漏洩・改ざん（後述）」の脆弱性を利用することでシステムの内部仕様に関する知識を有する攻撃者を想定しており、本論文と同様の能力を持つ攻撃者となっている。

によって実行方法を設定しているが、本稿では、生体認証システムの脆弱性を利用する実行方法を既知の文献を参照しながら設定する。

指紋を用いた認証における代表的ななりすまし方法としては、なりすまし対象者の残留指紋から隆線の強調等の処理を行った情報を生成し、その情報を基に人工物を作製してセンサーに提示するという方法がある。また、生体認証システム内部の判定しきい値を改ざんしたうえで、攻撃者が自分の生体特徴を提示するという方法である。これらの方法は、なりすましに必要な情報を集めて攻撃対象の生体認証システムに入力する情報（入力情報と呼ぶ）[4]を生成し、入力情報を入力しているといえる。上記の例においては、残留指紋を観測したデータに隆線の強調等の処理を行ったデータや改ざんする判定しきい値の値が入力情報に相当する。そこで、本稿では、なりすましを構成する行為として、入力情報を入手する行為（行為 1）と入力情報を生体認証システムに入力する行為（行為 2）を想定することとする。

行為 1 と行為 2 の実現方法は、攻撃に利用する脆弱性に依存する[5]。そのため、既知の脆弱性を検討対象とするとともに、行為 1 と行為 2 における各実行方法の組合せによってなりすまし方法を表現することで、既存の文献では明示されていない方法についても検討対象にすることができると考えられる。なりすましへの対策を検討する際に、こうした整理を参考にすることで、想定する攻撃の見落としが減ることが期待される。

ロ． 生体認証システムに固有の脆弱性

生体認証システムの脆弱性は既にいくつかの文献において検討されている。まず、JBAA 報告書は、生体認証システムへの攻撃として、なりすまし、認証の回避、サービス妨害を想定したうえで生体認証システム特有の脆弱性を中心に洗い出し、各攻撃を実施する際に利用する脆弱性を整理している。宇根ら（宇根・松本［2005］）は、JBAA 報告書で取り上げられた脆弱性を紹介するとともに、留意すべき脆弱性について考察したうえで、当該脆弱性への対策の研究動向を紹介している。また、情報処理推進機構（IPA）による報告書（IPA 報告書と呼ぶ、IPA［2006］）は、国際標準 ISO/IEC 19792 のドラフトで規定された脆弱性を紹介したうえで、各脆弱性が存在する生体認証システムの処理を分析しているほか、いくつかの攻撃について関係する脆弱性と対策を紹介している。ISO/IEC 19792 は、生体認証システムに固有の脆弱性に焦点を当てて、脆弱性の洗出しとそれらを評価する際の要点等を規定する国際標準となる予定である。

---

4 こうした入力情報には生体部位を提示する順番等の情報も含まれるとする。

5 厳密には、1 つの脆弱性を利用した実行方法だけでなく、複数の脆弱性を利用することで可能になる実行方法や脆弱性を利用せずに可能な実行方法も想定される。

ISO 19092（ISO［2008］）は、金融業務において生体認証システムを利用する際のセキュリティ確保のための枠組みを規定した国際標準であり、セキュリティ上考慮すべき事項や攻撃とそれぞれへの対策を述べている。

生体認証システムに固有の脆弱性をすべて洗い出すことが理想的である。ただし、未知の脆弱性をカバーすることは困難であり、既知の脆弱性をなるべくカバーして分析するというアプローチが現実的と考えられる。本稿では、ISO/IEC 19792 や他の文献で指摘されている脆弱性を参照しつつ各行為の実行方法を検討する。ISO/IEC 19792 は、カバーしている生体認証システムに固有の脆弱性が相対的に多く、記述の抽象度が高く議論していくうえで扱いやすいほか、生体認証システムのセキュリティ評価に関する国際標準として今後参照されることが想定されると考えられる。本国際標準のドラフトにおいて規定されている脆弱性は次のとおりである。

- 「認証精度の限界（performance limitation）」は、生体認証システムの認証結果には常に一定の誤りが含まれるという脆弱性である。他人の生体特徴がセンサーに提示された場合であっても受理される可能性がある。
- 「人工物等の受入れ（artefact of biometric characteristics）」は、ゼラチンで生成した指や顔の写真等の人工物によって生体特徴を偽造したもの（擬似生体特徴と呼ぶ）や、分離された生体部位（指等）の生体特徴をセンサーに提示した場合でも、受理される可能性があるという脆弱性である。
- 「生体特徴の意図的な変更（modification of biometric characteristics）」は、整形手術、化粧、声色や筆跡の変更等、自分の身体的・行動的特徴を意図的に変更でき、それがなりすましにつながる可能性があるという脆弱性である。
- 「生体特徴の秘匿困難性（difficulty of concealing biometric characteristics）」は、グラスやセンサー上の指紋の痕跡の記録、顔の撮影、音声の録音等のように、日常生活の中で秘匿が困難な生体特徴が存在するという脆弱性である。
- 「血縁関係による類似（similarity due to blood relationship）」は、双子の顔や声が似ているといった事例のように、血縁者の生体特徴が類似している可能性があるという脆弱性である。
- 「特殊な生体特徴の存在（special biometric characteristic）」は、他人の生体特徴と高い確率で誤一致と判定される参照データ（子羊と呼ばれる）や、複数の参照データと誤一致と判定されるような生体特徴（ウルフと呼ばれる）が存在する可能性があるという脆弱性である。この脆弱性には、血縁関係により生体特徴が類似するケースは含まれない。
- 「合成された擬似生体サンプルの受入れ（synthesised wolf biometric samples）」は、参照データ生成部や判定部に入力される生体サンプルでないデータ（擬似生体サンプルと呼ぶ）が受理される可能性があるという脆弱性である。擬

似生体サンプルの例としては、2 つの生体サンプルの平均をとったデータ、幾何学模様からなるデータ、特徴点が無数に存在する偽の指紋画像が挙げられる。

- 「環境変化による認証精度への影響（hostile environment）」は、センサー周辺の環境（気温、湿度、光量等）の変化が認証精度に影響を与える可能性があるという脆弱性である。環境の変化により、なりすましに成功する確率が高くなる可能性がある。
- 「不適切な情報の登録（procedural vulnerabilities around the enrolment process）」は、不適切な情報（品質の低い生体サンプル[6]、擬似生体サンプル）の登録により、なりすましが発生する可能性があるという脆弱性である[7]。こうしたなりすましは、特殊な生体特徴の存在や人工物等の受入れといった他の脆弱性がベースとなっていることから、本稿では検討対象としないこととする。
- 「データの漏洩・改ざん（leakage and alteration of biometric data）」は、生体認証システム内のデータ（生体サンプル、参照データ、判定しきい値、照合スコア、認証結果等）が漏洩する、または、改ざんされる可能性があるという脆弱性である。この脆弱性は情報システムに共通であるものの、漏洩・改ざんの対象となるデータは生体認証システムに固有であることから、本国際標準案で取り上げられている。また、本国際標準案では、評価対象とする生体認証システムだけでなく、他の生体認証システムからのデータ漏洩もこの脆弱性に含めているが、本稿では、他の生体認証システムからのデータ漏洩をこの脆弱性に含めないこととする。なお、生体認証システム内のデータに、生体認証システムの内部構造や各処理（照合アルゴリズム等）に関する知識を含めることとする。

ハ． 各行為の実行方法

攻撃者が上記の脆弱性を利用することで、行為 1 と行為 2 をどのように実行するかを検討する。本稿では、脆弱性を利用しなくとも実行できる方法についても検討に加えることとする。

---

6 国際標準 ISO/IEC 29794-1 は、生体サンプルの品質に関する用語や規準の考え方等を規定しており、本標準のドラフトでは、生体サンプルの品質を「想定するアプリケーションにおける要件を充足する度合い」と定義している。例えば、生体特徴の状態（怪我した指の指紋等）、センサーで撮影した画像の大きさや解像度、特徴の数等が品質に関係する可能性があるとしている。

7 ISO/IEC FCD 19792 では、「不適切な情報の登録」の脆弱性を利用した攻撃として、**本節(1)ロ．**の攻撃②も挙げている。

(イ)　入力情報の入手の実行方法

入力情報を入手するうえで、なりすまし対象者本人の生体特徴から派生した情報（本人の残留指紋等）を基に入力情報を入手する方法が考えられるほか、派生していない情報を基に入力情報を入手する方法が考えられる。派生していない情報を基に入力情報を入手する方法については、なりすましのために集めた情報からなりすましの対象者を決定することも想定される。

①　本人の生体特徴から派生した情報を基にした場合

【利用する脆弱性：データの漏洩】

データの漏洩を利用することで、攻撃対象の生体認証システムから入手したなりすまし対象者の生体サンプルや参照データを基に入力情報を入手するという方法（方法 1-1、JBAA［2003］）が考えられる。

【利用する脆弱性：生体特徴の秘匿困難性】

生体特徴の秘匿困難性を利用することで、なりすまし対象者の生体特徴の痕跡（残留指紋等）から入力情報を入手する方法（JBAA［2003］）が考えられる。具体的には、生体認証システムのセンサーにおける生体特徴の痕跡から入手するという方法（方法 1-2、JBAA［2003］）と日常生活における生体特徴の痕跡から入手するという方法（方法 1-3、JBAA［2003］）が考えられる。このほか、なりすまし対象者の生体部位の分離を行わずに、日常生活において露出している生体特徴から入力情報を入手するという方法（方法 1-4、JBAA［2003］）が考えられる。方法 1-4 においては、攻撃者は入力情報の入手にあたり、音声の録音、手書き動作の記録、可視光による顔の撮影、赤外光による静脈パターンの撮影等を行うと考えられる。また、身体的特徴については、本人の意識がない時（泥酔時等）に盗取される可能性もある（遠藤・平林・松本［2003］）。

【利用する脆弱性：認証精度の限界、データの漏洩、合成された擬似生体サンプル】

照合スコアは、本人の参照データとの類似度（あるいは、距離）を示す値であり、本人の生体特徴から派生した情報とみなすことができる。データの漏洩により照合時の照合スコアを入手できる場合には、擬似生体サンプル探索用の生体認証システムに初期値として（擬似）生体サンプルを適当に与え、照合スコアが改善されるように初期値に修正を加えることで擬似生体サンプルを探索し、これを基に入力情報を入手するという方法（方法 1-5、Hill［2001］）が考えられる。こうした探索方法はヒル・クライミング攻撃と呼ばれる。なお、本稿では、照合スコアを出力しない生体認証システムを想定しているが、認証結果の一部として照合スコアを出力している生体認証システムの場合には、データ

の漏洩を利用することなく本方法を実行することができる可能性がある。

このほか、上記の脆弱性を利用せずに入力情報を入手する方法がいくつか考えられる。別の生体認証システムや生体特徴を用いた他のアプリケーション（拇印、直筆のメモ等）から入手した情報を基に入力情報を入手するという方法（方法 1-6）、なりすまし対象者の生体部位（指等）を分離し、それを基に入力情報を入手するという方法（方法 1-7、JBAA［2003］）、偽端末を設置してなりすまし対象者に生体特徴を提示させ盗取した情報を基に入力情報を入手するという方法（方法 1-8、FISC［2006］）、なりすまし対象者を脅して得た情報を基に入力情報を入手するという方法（方法 1-9、JBAA［2003］）、なりすまし対象者と結託し、同意のもとで得た情報を基に入力情報を入手するという方法（方法 1-10、JBAA［2003］）が考えられる。なお、なりすまし対象者を脅す（方法 1-9）、あるいは、結託する（方法 1-10）際には、なりすまし対象者の生体部位の分離（方法 1-7）を行わないとする。

② 本人の生体特徴から派生していない情報を基にした場合

【利用する脆弱性：データの漏洩】

データの漏洩を利用して、システム内部において認証結果を生成する処理が行われる部分とそのためのデータを特定したうえで、任意のセンサーへの入力に対して「受理」を出力する処理部分とデータを決定する。こうしたデータを入力情報として入手するという方法（方法 1-11、JBAA［2003］）が考えられる。

【利用する脆弱性：認証精度の限界】

「認証精度の限界」の脆弱性を利用して、なりすまし対象者以外の利用者をランダムに選択し、当該利用者の生体特徴を基に入力情報を入手するという方法（方法 1-12、JBAA［2003］）が考えられる。

【利用する脆弱性：認証精度の限界、血縁関係による類似】

なりすまし対象者の血縁者の生体特徴から派生したデータを基に入力情報を入手するという方法（方法 1-13、JBAA［2003］）が考えられる。ただし、血縁者の生体特徴の痕跡、生体サンプル、参照データ等を入手するために、血縁者について上記の方法 1-1～1-10 を併用する。これらの方法を実行するためには、それぞれ対応する脆弱性を利用可能であることが条件となる。

【利用する脆弱性：認証精度の限界、合成された擬似生体サンプルの受入れ】

合成された擬似生体サンプルの受入れを利用する場合には、生体特徴を模した擬似生体特徴や幾何学模様等を基に入力情報を入手するという方法（方法 1-14）が考えられる。

【利用する脆弱性：認証精度の限界、合成された擬似生体サンプルの受入れ、特殊な生体特徴の存在】

特殊な生体特徴の存在を利用しつつ、生体サンプルの品質が低い場合には期待した認証精度が得られない可能性があることが指摘されている。そのため、品質の低い（擬似）生体サンプルを基に入力情報を入手するという方法（方法 1-15）が考えられる。データの漏洩により照合アルゴリズムの解析を行ったうえで、品質の低い生体サンプルを求める方法は含めない。

【利用する脆弱性：認証精度の限界、データの漏洩】

データの漏洩を利用して複数の参照データを入手できる場合には、攻撃者自身の生体特徴と類似している参照データを探索したうえで、対応する参照データ識別子を特定し、攻撃者自身の生体特徴を入力情報とするという方法（方法 1-16、ISO［2008］）が考えられる。このほか、複数の参照データの比較により類似したペアを探索し、一方をなりすまし対象者にしたうえで、他方の参照データに対応する利用者を特定し、当該利用者の生体特徴を基に入力情報を入手するという方法（方法 1-17、ISO［2008］）が考えられる。

【利用する脆弱性：認証精度の限界、データの漏洩、特殊な生体特徴の存在】

データの漏洩により複数の参照データを入手したうえでそれらを比較し、最も多くの参照データと誤一致する参照データを探索し、これを基に入力情報を入手するという方法（方法 1-18、門田・黄・吉本［2005］）が考えられる。このように複数の参照データと誤一致する参照データの基となる入力情報はウルフに相当し、誤一致する参照データの数が多いほど強いウルフとなる。また、こうした入力情報を与えてなりすましを試みる攻撃はウルフ攻撃と呼ばれている。

【利用する脆弱性：認証精度の限界、データの漏洩、特殊な生体特徴の存在、合成された擬似生体サンプル】

データの漏洩により照合アルゴリズムに関する情報を入手したうえで解析を行い、任意の参照データを想定した場合になりすましの成功確率が高くなるような（擬似）生体サンプルを探索し、これを基に入力情報を入手するという方法（方法 1-19、Une, Otsuka, and Imai［2008］）が考えられる。こうした（擬似）生体サンプルもウルフとなる可能性があり、本方法もウルフ攻撃の 1 つといえる。

(ロ)　入力情報を生体認証システムに入力する方法

【利用する脆弱性：人工物の受入れ】

人工物等の受入れを利用する場合には、入力情報（擬似生体サンプル等）を

基に人工物を作製しこれをセンサーに提示するという方法（方法 2-1、JBAA［2003］）と、分離した生体部位（指の分離等）をセンサーに提示するという方法（方法 2-2、JBAA［2003］）が考えられる。なお、方法 2-2 では、なりすまし対象者から分離した生体部位のほか、入力情報とする（擬似）生体特徴等に類似する生体特徴を持つ利用者から分離した生体部位を用いることが考えられる。

【利用する脆弱性：生体特徴の意図的な変更】

生体特徴の意図的な変更を利用する場合には、入力情報を基に攻撃者が自分の生体特徴を意図的に変更してセンサーに提示するという方法（方法 2-3、JBAA［2003］）が考えられる。例えば、撮影した顔写真を参考に化粧や整形手術等を行うことで攻撃者の身体的特徴を変更することや、記録した音声を参考に攻撃者の声色を変えることが挙げられる。

【利用する脆弱性：データの漏洩・改ざん】

生体認証システムにおいてデータの挿入・改ざんを行うとともに、必要に応じて攻撃者が自分の生体特徴をセンサーに提示するという方法（方法 2-4、JBAA［2003］）が考えられる。例えば、盗取しておいた生体サンプルをそのまま電気的に挿入すること（リプレイ攻撃と呼ばれる）や、センサーへの任意の入力に対して「受理」が出力されるように判定しきい値や認証結果を改ざんしたうえで攻撃者自身の生体特徴を提示することが挙げられる。

【利用する脆弱性：認証精度の限界】

本人以外の利用者[8]を脅して当該利用者の生体特徴をセンサーに提示させるという方法（方法 2-5、JBAA［2003］）と、入力情報が攻撃者や結託者の生体特徴と同一あるいは類似している場合には、攻撃者や結託者の生体特徴をセンサーに提示するという方法（方法 2-6、JBAA［2003］）が考えられる。なお、方法 2-5 では、入力情報とする（擬似）生体特徴等に類似する生体特徴を持つ利用者を脅すことが考えられる。

【利用する脆弱性：環境変化による認証精度への影響】

上記の方法2-1～2-6を実行する際、センサー周辺の環境を変化させることで、なりすましの成功確率が高くなる可能性がある。センサー周辺の環境を変化させたうえで、方法 2-1～2-6 を実行するという方法（方法 2-7、JBAA［2003］）が考えられる。

---

8 本人を脅して生体特徴をセンサーに提示させる攻撃（JBAA［2003］）は、なりすましではないため本稿では検討対象としない。

ニ． 行為 1 と行為 2 に基づくなりすまし方法の洗出し

行為 1 と行為 2 の各実行方法を組み合わせることでなりすまし方法を表現することができる。行為 1 の実現方法と行為 2 の実現方法の間には従属関係があり、想定困難な組合せも存在すると考えられることから、上記の各実行方法について想定される組合せを検討する（図表 2参照)。行為 2 の実行方法（方法 2-1～2-7）を軸に組合せをみていく。

			行為 2						
			2-1 人工物	2-2 分離	2-3 変更･模倣	2-4 挿入･改ざん	2-5 脅し	2-6 提示	2-7 環境
行為 1	本人の生体特徴から派生した情報からの入力情報の入手	1-1 当該ｼｽﾃﾑから漏洩				JBAA			
		1-2 ｾﾝｻｰ上の痕跡	JBAA			JBAA			
		1-3 日常生活における痕跡	JBAA			JBAA			
		1-4 露出	JBAA						
		1-5 ﾋﾙ･ｸﾗｲﾐﾝｸﾞ攻撃				JBAA			
		1-6 他ｼｽﾃﾑから漏洩							
		1-7 分離		JBAA					
		1-8 偽端末							
		1-9 脅し	JBAA						
		1-10 結託	JBAA						
	本人の生体特徴から派生していない情報からの入力情報の入手	1-11 認証ﾊﾟﾗﾒｰﾀの漏洩				JBAA			
		1-12 本人以外の生体特徴						JBAA	JBAA
		1-13 血縁者						JBAA	
		1-14 擬似生体特徴	JBAA						
		1-15 低品質			JBAA				JBAA
		1-16 攻撃者の生体特徴と類似						JBAA	
		1-17 類似ペア							
		1-18 参照データからｳﾙﾌを探索	JBAA						
		1-19 照合ｱﾙｺﾞﾘｽﾞﾑからｳﾙﾌを探索							

（備考）背景が灰色のセルは想定困難な組合せであることを、「JBAA」は JBAA 報告書で記述されているなりすまし方法であることをそれぞれ示す。

図表2. 行為 1 と行為 2 の組合せによるなりすまし方法の洗出し

・ 方法 2-1（人工物の提示)、方法 2-2（分離した生体部位の提示)、方法 2-3（意図的に変更した生体特徴の提示)、方法 2-5（脅しによる生体特徴の提示)、方法 2-6（攻撃者等の生体特徴の提示）は、（擬似）生体特徴や（擬似）生体サンプル等を基に入力情報を入手するという方法との組合せが想定される。方法 1-11 はこうした方法に該当しないためこれらの方法との組合せは想定困難である。

・ 方法 2-4（データの挿入・改ざん）については、（擬似）生体サンプル、参照データ、改ざんしたい判定しきい値や認証結果等を入力情報とする方法との組合せが想定される。
・ 方法 2-7（センサー周辺の環境の変更）については、方法 2-1～2-6 が実行可能な場合には、併せてセンサー周辺の環境を変化させることが考えられる。そのため、方法 2-1～2-6 との組合せが想定される場合には、方法 2-7 との組合せも想定される。

まず、本稿で洗い出したなりすまし方法がどの程度のバリエーションをカバーできているのかを既存の文献と比較しながら考察する。ここでは、多くのなりすまし方法を洗い出している既存文献として JBAA 報告書を取り上げる。本報告書で示されているなりすまし方法と比較すると、方法 1-6、1-8、1-17、1-19 を用いた方法について今回追加的に整理したといえる。また、行為 1 の各実現方法と行為 2 の各実現方法の組合せによって、JBAA 報告書では想定されていないものの想定されうるなりすまし方法（図表 2において「JBAA」と書かれていない白色のセル）が存在することを示した。

今後、新しいモダリティの登場や攻撃の高度化等により、新たななりすまし方法が出現することが予測される。その場合には、当該なりすまし方法を構成する行為を分析し、図表 2に行為 1 あるいは行為 2 を実行する新たな方法として追加することで、検討対象を拡張することができる。また、実行方法を行う際に盗取・改ざんするデータの種類（生体サンプル、参照データ、判定しきい値等）や攻撃法に着目して、図表 2に示した各実行方法を明確にしていくことも考えられる。このように具体的なデータや攻撃法に基づいて実行方法を明確化・細分化して表を再構成することで、より具体的なりすまし方法を検討するという使い方も可能である。

3．なりすましへの対策

(1) 想定される対策の整理

前節のなりすまし方法（方法 1-1～1-19、2-1～2-7）への対策として考えられるものを、既存の文献を参照しながら整理する。

イ． 入力情報の入手への対策

(イ) 本人の生体特徴から派生した情報を基にした入力情報の入手への対策

- 方法 1-1（攻撃対象の生体認証システムからの漏洩）に対しては、データ漏洩の防止や検知のために、生体認証システム内のデータの暗号化・システムの耐タンパー化・ログ収集等を行うこと（宇根・松本［2005］）、漏洩した参照データをなりすましに利用できないようにする技術（テンプレート保護技術と呼ばれる）を利用すること（IPA［2006］）が考えられる。なお、テンプレート保護技術の利用にあたっては、参照データ等の漏洩を検知する必要があるケースもある。このほか、チャレンジ・レスポンス認証を行うこと（Schuckers［2002］）も考えられる。チャレンジ・レスポンス認証の例としては、予め 5 本の指を登録しておき、認証時に提示する指を生体認証システムがランダムに指定する方法が挙げられる。この方法を採用した場合、攻撃者は 5 本の指について人工指（指を模擬した人工物）や分離した指を用意する必要があるため、1 本の場合と比べて攻撃のコストが増加することが期待できる。
- 方法 1-2（センサー上の痕跡）に対しては、センサー上の痕跡を拭き取ること（宇根・松本［2005］）や提示された生体特徴を非接触型のセンサーで読み取ること（BSC［2006］）が考えられる。
- 方法 1-3（日常生活における痕跡）に対しては、日常生活において痕跡が残りにくいモダリティ（静脈パターン等）を利用すること（宇根・松本［2005］）が考えられる。
- 方法 1-4（露出した生体特徴の観測）に対しては、生体特徴をセンサーに提示する方法を攻撃者に知られないように別途決めておくこと（大野ら［2008］）が考えられる。例えば、生体認証システムに 5 本の指を登録する際、指を提示する順番も登録しておく。仮に、攻撃者に生体特徴から派生する情報が入手されたとしても、提示する順番を秘密にしておくことができれば、攻撃を防ぐことができる可能性がある。このほか、チャレンジ・レスポンス認証を行うこと（Schuckers［2002］）も考えられる。例えば、認証時に

生体認証システムから質問を行い、利用者の音声によって回答させるという対策が考えられる。これにより、記録した音声をそのまま利用する攻撃を防ぐことができると期待される。

- 方法 1-5（ヒル・クライミング攻撃）に対しては、判定しきい値をより厳しく設定するなどの方法によって認証精度を向上させ、攻撃に必要な計算量を増大させること（宇根・松本［2005］）のほかに、ヒル・クライミング攻撃に耐性のある照合アルゴリズムを利用することが考えられる（小松［2005］、村松［2008］）。例えば、小松［2005］は、認証時の照合スコアを手掛かりに擬似生体サンプルの修正を行った場合、不自然な擬似生体サンプルとなるような照合アルゴリズムを提案している。村松［2008］は、ヒル・クライミング攻撃により生成された擬似生体サンプルに耐性のある照合アルゴリズムを提案している。このほか、一定回数連続して認証に失敗した場合には新たな認証処理を開始しないといった対策（宇根・松本［2005］）が考えられる。本稿で想定する生体認証システムでは照合スコアを出力しないが、仮に照合スコアを出力している生体認証システムでは、照合スコアを出力しない（宇根・松本［2005］）、照合と照合の間に十分な時間を設け、連続して照合スコアを入手できないようにするといった対策が考えられる。
- 方法 1-6（他のシステムからの漏洩）に対しては、他の生体認証システムや他のアプリケーションで利用されていないモダリティを利用することが考えられる。また、テンプレート保護技術も対策の 1 つとなりうるが、本対策が有効に機能するためには他のシステムにおいても同様の対策が適切に講じられている必要がある。
- 方法 1-7（生体部位の分離）に対しては、分離された生体部位からは生体特徴に関する情報を得ることができないようなモダリティ（行動的特徴等）を利用することが考えられる。
- 方法 1-8（偽端末による盗取）に対しては、IC カード等を利用して利用者が端末を認証すること（田村・宇根［2006］）、「いつもとは異なる場所に設置されている端末には生体特徴を提示しないよう心掛ける」等のように利用者を啓蒙すること（FISC［2006］）、偽端末が設置されているか否かを監視によって確認すること（FISC［2006］）が考えられる。
- 方法 1-9（なりすまし対象者への脅し）に対しては、非常時通報を利用するという対策が考えられる（古江ら［2006］、國井ら［2007］）。例えば、2 本の指を生体認証システムに登録しておき、通常の認証では一方の指を提示し、脅されている場合には他方の指を提示する方法が挙げられる。
- 方法 1-10（なりすまし対象者と結託）に対しては、デジタル・フォレンジック技術等により結託していることを事後的に検知する対策が考えられる。

(ロ) 本人の生体特徴から派生していない情報を基にした入力情報の入手への対策

- 方法 1-11（判定しきい値や認証結果の入手・解析）に対しては、データ漏洩の防止や検知のために、生体認証システム内のデータの暗号化・システムの耐タンパー化・ログ収集等を行うこと（宇根・松本［2005］）が考えられる。
- 方法 1-12（なりすまし対象者以外の生体特徴の利用）に対しては、「認証精度の限界」の脆弱性による影響を軽減するために、判定しきい値の調節や照合アルゴリズムの改良等により認証精度を向上させること（宇根・松本［2005］）が考えられる。
- 方法 1-13（なりすまし対象者の血縁者の利用）に対しては、認証精度を向上させること（宇根・松本［2005］）のほかに、血縁関係による認証精度への影響がないことを確認したモダリティ[9]を利用することが考えられる。
- 方法 1-14（擬似生体特徴の利用）に対しては、認証精度を向上させること（宇根・松本［2005］）のほかに、生体認証システムが読み取ったデータを解析し、人間が取り得る値となっているか否かを検査することが考えられる。
- 方法 1-15（品質の低い生体サンプルの利用）に対しては、認証精度を向上させること（宇根・松本［2005］）のほかに、生体認証システムが読み取った生体サンプルの品質を検査すること（宇根・松本［2005］）が考えられる。
- 方法 1-16（攻撃者の生体特徴と類似する参照データの探索）と方法 1-17（類似する参照データのペアの探索）に対しては、認証精度を向上させること（宇根・松本［2005］）のほかに、データ漏洩の防止や検知のために、生体認証システム内のデータの暗号化・システムの耐タンパー化・ログ収集等を行うこと（宇根・松本［2005］）が考えられる。
- 方法 1-18（参照データを用いたウルフ攻撃）に対しては、認証精度を向上させること（宇根・松本［2005］）、データ漏洩の防止や検知のために、生体認証システム内のデータの暗号化・システムの耐タンパー化・ログ収集等を行うこと（宇根・松本［2005］）、ウルフ攻撃への耐性が確認された照合アルゴリズムを利用すること（門田・黄・吉本［2005］、Une, Otsuka, and Imai［2008］、Inuma, Otsuka, and Imai［2009］）が考えられる。
- 方法 1-19（照合アルゴリズムを用いたウルフ攻撃）に対しては、認証精度を向上させること（宇根・松本［2005］）、ウルフ攻撃に耐性のある照合アルゴリズムを利用すること（Une, Otsuka, and Imai［2008］、Inuma, Otsuka, and Imai［2009］）が考えられる。また、合成した擬似生体サンプルがウルフになる

---

9 BSC［2006］では、一卵性双生児同士の虹彩、あるいは、同一人物の左右の虹彩であっても異なると記述されている。

場合には、擬似生体サンプルを解析し人間が取り得る値となっているか否かを検査することが考えられる。このほか、照合アルゴリズムに関する知識を攻撃者に与えないために、生体認証システム内のデータの暗号化・システムの耐タンパー化・ログ収集等を行うこと（宇根・松本［2005］）が考えられる。

ロ．　入力情報を生体認証システムに入力する方法への対策

- 方法 2-1（人工物の提示）と方法 2-2（分離した生体部位の提示）に対しては、提示された被認証物が人工物や分離された生体部位か否かを識別する技術（生体検知技術と呼ばれる）を利用する（宇根・松本［2005］）、人工物や分離した生体部位を提示しているか否かを監視（IPA［2006］）するといった対策が考えられる。このほか、遠藤・松本［2002］では、静電容量式のセンサーにシリコーン製人工指を提示した場合には登録・照合ができなかったとの実験結果を示していることから、生体特徴の偽造が困難な読取方法を利用するといった対策が考えられる。
- 方法 2-3（意図的に変更した生体特徴の提示）に対しては、どのような生体特徴を模倣すればよいのか既知であったとしても模倣が困難なモダリティを利用する対策が考えられる。例えば、青山・西垣［2007］では、対象物の動きを両目で捉える際の眼球の動きが反射によって生じていること（こうした反射は輻輳反射と呼ばれる）に注目し、輻輳反射を用いた認証方法を提案している。
- 方法 2-4（データの挿入・改ざん）に対しては、生体認証システム内のデータの暗号化やシステムの耐タンパー化により改ざんや挿入を防止・検知する（宇根・松本［2005］）、システムに配線をつなぐ行為等を監視するといった対策が考えられる。
- 方法 2-5（脅しによる生体特徴の提示）と方法 2-6（攻撃者等の生体特徴の提示）は、なりすまし対象者以外の利用者の生体特徴をセンサーに提示することでなりすましを試みることから、認証精度を向上させること（宇根・松本［2005］）が考えられる。また、方法 2-5 については、攻撃者がその場にいる場合には脅されているか否かを監視する（宇根・松本［2005］）という対策も考えられる。
- 方法 2-7（センサー周辺の環境の変更）に対しては、環境状態の異常を検知する機構を準備し、検知した場合には生体認証システムを停止する（IPA［2006］）、屋外に設置するセンサーであれば光学式以外のものを利用するなどのように環境の変化を受けにくい読取方法を利用する、補助光を利用することでセンサー周辺の光量を一定に保つなどのように外部環境の影響を軽

減する工夫を行う、故意にセンサー周辺の環境を変更しようとする行為を監視する（IPA［2006］）といった対策が考えられる。

以上の対策のほかに、複数のモダリティを用いた認証を行うマルチ・モーダル認証（BSC［2006］）は、攻撃者が用意しなければならない入力情報、生体認証システムに提示する人工物や電気的に挿入するデータの数を増加させるため、行為 1 および行為 2 の各実行方法への対策になりうると考えられる。

本節(2)と(3)で示した行為 1 と行為 2 の実行方法と対策を付録にまとめる。なお、生体認証システムの内部構成や処理内容を修正する必要がある対策を技術的対策と呼ぶこととする。

(2) なりすましへの対策の講じ方

イ． 基本的なアイデア

まず、なりすましが生じた際の被害や図表 2に挙げた各なりすまし方法の顕現化の可能性を分析したうえで、対策を講じるべきなりすまし方法を明らかにする[10]。次に、対象とする各なりすまし方法に対して実施可能な対策を選択する。

2 **節**(3)に挙げた対策のなかには、技術の成熟度や運用上の制約から十分な効果が期待できないものや実施困難なものが存在する可能性がある。そうした場合であっても、なりすまし方法に対応する入力情報の入手（行為 1）と入力情報の入力（行為 2）のそれぞれの実行方法のうち、一方を実行困難にするように対策を講じることでなりすましを防ぐことができると考えられる。

ロ． 選択する対策の例

例として、生体認証システムの用途として ATM における顧客の本人確認を、対策を講じるべきなりすまし方法として図表 2に示したすべての組合せをそれぞれ想定した場合に、本稿の検討結果を採用するとどのように対策を選択することができるかを示す。

まず、金融情報システムセンター（FISC）の安全対策基準（安対基準と呼ぶ、FISC［2006］）をみると、システム内のデータの暗号化、システムの耐タンパー化、ATM 周辺の監視等が対策として挙げられている。このことから、各金融機関では既にこれらの対策が実施されている可能性が高いと考えられる。

---

10 こうした分析を行う際には、例えば、定量的なリスク分析・評価手法である FTA（Fault Tree Analysis）を利用することが考えられる（清水・瀬戸［2008］）。

・ システム内のデータの暗号化、システムの耐タンパー化
  - これらは、データの漏洩や改ざんの脆弱性を利用する方法 1-1、1-5、1-11、1-16～1-19、2-4 への対策となる。
・ ATM 周辺の監視
  - ATM が設置されている環境ではカメラや職員によって監視が行われている。こうした監視においては、利用者がセンサー周辺の環境を故意に変化させようとしているか否かにも注意が払われていることから、方法 2-7 への対策となる[11]。

これらの対策を適切に講じることで、方法 2-1～2-3、2-5、2-6 を除くなりすまし方法に対応できると考えられる（図表 3参照）。

残りのなりすまし方法（図表 3において「済」と書かれていない白色のセル）に対しては、まず、各セルに対応する行為 1 および行為 2 の実行方法への対策について技術の成熟度や利用者の不注意による影響等を分析することが考えられる。そのうえで、網羅的に対策を講じるための対策の組合せを検討し、それらのうちどの組合せが最も望ましいかについて、コストや利便性等の他の評価項目も考慮しながらアプリケーションに応じて検討を行うことが考えられる。

こうした組合せの一例として、生体検知技術の利用、認証精度の向上、模倣困難なモダリティの利用という 3 つの対策の組合せが挙げられる。生体検知技術は、近年、人工物や分離された生体部位を用いたなりすましへの対策として注目されており（宇根・田村［2005］）、方法 2-1 と方法 2-2 への対策への対策となりうる。認証精度の向上を図ることで、本人の生体特徴から派生していない情報を基に入力情報を入手する方法 1-12～1-15、および、なりすまし対象者が生体特徴をセンサーに提示する方法 2-5、2-6 への対策となりうる。さらに、模倣困難なモダリティを利用すれば、方法 2-3 への対策となりうる。ただし、生体検知技術を利用する際は、検知の精度に応じて効果が異なるためアプリケーションにおいて求められる精度を達成していることを確認する必要がある。同様に、認証精度の向上を図る際にもアプリケーションの要件を満たすことを確認する必要がある。

---

11 ATM 周辺の監視は、方法 2-1、2-2、2-5 への対策にもなりうると考えられる。しかし、読売新聞［2009］によれば、対面で監視しているにも関わらず人工指に気付かなかったケースがあるほか、攻撃者が ATM 周辺にいない場合、監視によって脅されているか否かを判断できない可能性がある。そこで、監視がこれらへの対策として有効に機能しないケースを考慮し、方法 2-1、2-2、2-5 について別の対策で対応することとした。

			行為 2						
			2-1 人工物	2-2 分離	2-3 変更･模倣	2-4 挿入･改ざん	2-5 脅し	2-6 提示	2-7 環境
行為 1	本人の生体特徴から派生した情報からの入力情報の入手	1-1　当該ｼｽﾃﾑから漏洩	済	済	済	済	済	済	済
		1-2　ｾﾝｻｰ上の痕跡				済			済
		1-3　日常生活における痕跡				済			済
		1-4　露出				済			済
		1-5　ﾋﾙ･ｸﾗｲﾐﾝｸﾞ攻撃	済	済	済	済	済	済	済
		1-6　他ｼｽﾃﾑから漏洩				済			済
		1-7　分離				済			済
		1-8　偽端末				済			済
		1-9　脅し				済			済
		1-10　結託				済			済
	本人の生体特徴から派生していない情報からの入力情報の入手	1-11　認証ﾊﾟﾗﾒｰﾀの漏洩				済			済
		1-12　本人以外の生体特徴				済			済
		1-13　血縁者				済			済
		1-14　擬似生体特徴				済			済
		1-15　低品質				済			済
		1-16　攻撃者の生体特徴と類似	済	済	済	済	済	済	済
		1-17　類似ペア	済	済	済	済	済	済	済
		1-18　参照データからｳﾙﾌを探索	済	済	済	済	済	済	済
		1-19　照合ｱﾙｺﾞﾘｽﾞﾑからｳﾙﾌを探索	済	済	済	済	済	済	済

（備考）灰色のセルは想定困難な組合せを、「済」は 1 種類以上の対策を講じていることをそれぞれ示す。

図表3．暗号化、耐タンパー化、監視によって対応可能ななりすまし方法

4．生体検知技術の研究動向

3 節で紹介した対策のうち生体認証システムに固有の技術的対策には、テンプレート保護技術、生体サンプルの品質の検査、ヒル・クライミング攻撃に耐性のある照合アルゴリズムの利用、ウルフ攻撃に耐性のある照合アルゴリズムの利用、生体検知技術、マルチ・モーダル認証の利用等が挙げられる。これらの対策は、生体認証システムのセキュリティを確保していくうえでいずれも重要な技術であると考えられる。本稿では、手始めに近年評価の観点から研究が進展してきている生体検知技術に焦点を当てることとする。

(1) 生体検知技術の研究動向の概要

2000 年前後に、人工物や分離した生体部位が一部の市販の生体認証システムに受け入れられることが学会等で示され（例えば、Wills and Lee［1998］、van der Putte, and Keuning［2000］、Matsumoto *et al.*［2002］）、現在では「人工物等の受入れ」の脆弱性として広く認識されるようになっている。また、実際に運用されている生体認証システムに対して分離した生体部位や人工物を提示するといった事例（Kent［2005］、読売新聞［2009］）が発生している。

一方、1990 年代から特許を中心に人工物等を識別する手法が提案されはじめ（加藤ら［1996］）、2000 年以降は学会でも発表されるようになってきている（Derakhshani *et al.*［2003］）。当初の研究発表では、追加的なハードウエアの有無や生体検知に利用する特徴が静的か動的かといった観点からの考察が多かった。その後、2005 年には、生体検知に用いるための情報（生体検知用サンプルと呼ぶ）の読取りに注目して、生体検知用サンプルの偽造の困難さのレベルを定性的に分類する方法が提案されている（宇根・田村［2005］）。最近では、被験者や人工物等を用いた実験により、提案方式における生体検知の精度（検知精度と呼ぶ）を定量的に評価している研究が増えてきている。検知精度の評価指標には、人工物や分離された生体部位を誤って生体と判断する確率（FAR_{FD}）、生体を誤って人工物等と判断する確率（FRR_{FD}）、これらの確率が等しくなる時の確率（EER_{FD}）が用いられることが多い。

また、モダリティごとにみると、指紋（Derakhshani *et al.*［2003］）、虹彩（Lee *et al.*［2006］）、静脈パターン（中崎・田中・松本［2008］、松本・清水［2009］）、顔（Li *et al.*［2004］）等について生体検知の研究が行われている[12]。

---

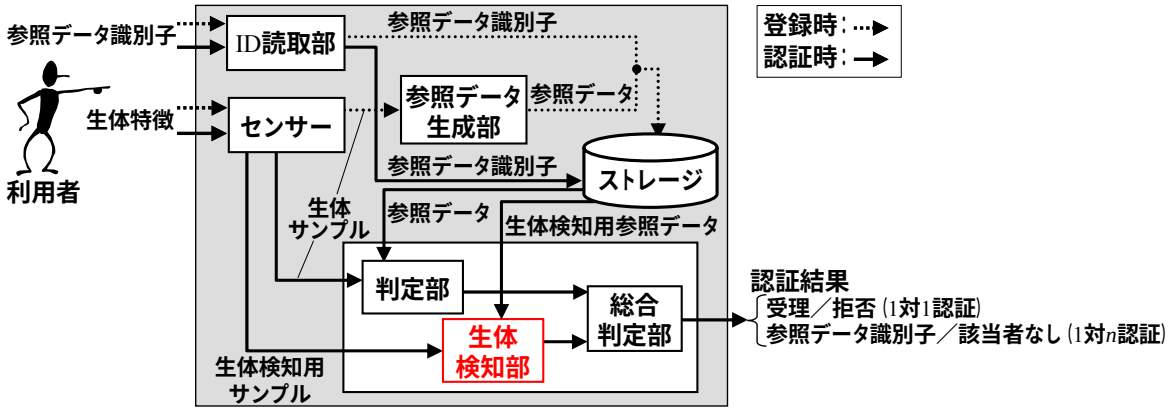
12 生体検知技術をモダリティごとにみると指紋に関する研究が最も盛んであり、例えば、生体認証技術に関する主要な国際学会である International Conference on Biometrics の第 1 回目（2006 年開催）と第 2 回目（2007 年開催）において発表された生体検知技術に関する論文（ポスターセッションを含む）をみると、指紋に関するものが 6 件、虹彩に関するものが 2 件となっている。

生体検知に用いられる人間の特徴には、例えば、電気特性（静電容量、インピーダンス、比誘電率等）、光学特性（光の反射・吸収・透過光等）、生理的特性（脈拍、体温、発汗等）等が挙げられる[13]。その他の特徴を利用した手法も多数提案されているが（中崎・田中・松本［2008］等）、どのような特徴が生体検知を行ううえでより望ましいかは明らかになっていない。

そこで、本節では、生体検知技術の導入・利用を検討するうえで重要と考えられる評価項目として、セキュリティ、利便性、コスト、社会的受容性を取り上げ（宇根・田村［2005］）、あるべき姿と研究事例を基にした現状分析を行う。

(2) 生体検知の処理の概要

図表 1に示した生体認証システムをベースに、生体検知の処理を概説する（図表 4参照）。



図表4. 生体認証システムにおける生体検知の処理

生体認証システムに提示された物体が生体か否かを識別するために利用する情報のうち、ストレージに登録しておくものを生体検知用参照データと呼ぶ。全利用者が 1 つの生体検知用参照データを共有するケースでは、システム運用者が何らかの方法によって生成した生体検知用参照データを予め登録しておく。利用者ごとに生体検知用参照データを用意するケースでは、参照データを登録する際に取得した生体検知用サンプルから生体検知用参照データを生成・登録する。どちらのケースを採用するかは、個々の生体検知手法に依存する。

認証時の生体検知の処理では、まず、提示された物体から生体検知用サンプルを読み取り、これを生体検知部に送る。生体検知部では、生体検知用参照データをストレージから読み出し、提示物が生体か否かを判断する。総合判定部

13 こうした特徴については、宇根・田村［2005］に詳しくまとめられている。

では、判定部と生体検知部の結果を基に認証結果を出力する。ただし、こうした処理の流れは一例に過ぎず、判定部、生体検知部、総合判定部間でどのような情報がどのようにやり取りされるかは個々の生体認証システムに依存する。

(3) 調達者が留意すべき評価項目

イ． セキュリティ

セキュリティについては、誤り率（FAR_{FD}、FRR_{FD}、EER_{FD}）を用いた検知精度に注目することが考えられる。さまざまな材料・製法によって作製した人工物が知られているほか[14]、特定の生体検知の手法を破るような人工物が提案されるなど、検知精度の評価には、新しい種類の人工物や分離された生体部位を含め、できるだけ多くの人工物等を用いることが望ましい。

本人を本人と判断する、あるいは、他人を他人と判断するといった認証精度に関しては、評価に用いたデータセット[15]や評価を実施した際の気温、湿度、外光、騒音、データセット等の条件（評価条件と呼ぶ）によって評価結果が変化することが知られており、評価条件を明確にすることが求められている（ISO and IEC［2006］）。検知精度も評価条件の影響を受けると考えられることから、手法ごとに検知精度に影響を与える要素を明確にすることが望ましい。また、評価結果を報告する際には、人工物の種類ごとに検知精度が異なる可能性があることから、評価に用いた人工物や分離された生体部位ごとに検知精度を示すことや、評価条件を示すことが望ましい。

生体検知機能を搭載した生体認証システムの新規調達を検討している、あるいは、運用中の生体認証システムへの生体検知機能の導入を検討しているエンティティ（調達者と呼ぶ）にとっては、生体認証システムを利用する環境の条件（利用条件と呼ぶ）における検知精度が重要である。しかし、学会等で報告される生体検知の手法の検知精度は、アプリケーションを考慮しないで特定の評価条件のもとで評価した結果となっている。そのため、導入した際に達成される検知精度と学会等で報告されている検知精度に乖離が生じる可能性がある。こうした乖離を軽減する方法の 1 つとして、報告した検知精度が得られる評価条件の範囲も報告することが考えられる。この範囲に調達者の利用条件が含ま

---

14 例えば、Nixon *et al.*［2004］は、19 種類の物体について評価を行っている。

15 データセットとは、精度評価に用いた被験者や生体サンプルの集合のことであり、データセットの規模、被験者の性別、人種、年齢、評価対象の生体認証システムへの慣れ等の要素が評価結果に影響を与える可能性があることが知られている（ISO and IEC［2006］）。

れていれば、示された検知精度が得られることが期待できる[16]。

ロ． 利便性

生体検知の手法の導入によって、利用者の利便性が低下する可能性がある。例えば、生体検知用サンプルの取得や生体検知部における識別処理にかかる時間により、認証処理全体の処理時間が増加する。また、生体検知用サンプルを取得するために一定の動作を要求する場合には、そうした動作に慣れる必要がある点や認証時に行う作業が増えるといった点から利便性が低下すると考えられる。このほか、運用中の生体認証システムに生体検知の手法を導入する状況において、利用者ごとの生体検知用参照データの登録を必要とする手法を選択した場合、各利用者に生体検知用参照データを登録してもらう必要がある。

こうした生体検知にかかる時間、利用者に要求する動作、生体検知用参照データが利用者ごとか否かの項目について、明らかになっていることが望ましい。

ハ． コスト

既存の生体認証システムに生体検知の手法を導入する際、ソフトウエアの変更が必要になるほか、ハードウエアの追加・変更も必要になるケースがある。ハードウエアの追加・変更の必要性については、例えば、光学式センサーによって読み取った指紋画像を生体サンプルとして用いる生体認証システムにおいて、提示された物体の電気抵抗を生体検知用サンプルとして用いる手法であれば、ハードウエアの追加が必要となる。また、指紋画像を生体検知用サンプルとする場合であっても、生体サンプルよりも高解像度の画像を必要とする手法の場合には、そうした画像が取得可能なセンサーへの変更が必要となる。

つまり、ハードウエアの追加・変更の必要性については、生体サンプルの読取りに用いるセンサーの仕様が、生体検知用サンプルの読取りに用いるセンサーの要求性能を満たすか否かがポイントとなる。そのため、要求性能が明確になっていることが望ましい。

ニ． 社会的受容性

副次的な情報が抽出される可能性のある身体的特徴[17]や犯罪捜査に利用される身体的特徴等の場合には、社会的受容性が低く、そうした特徴を利用した生体認証システムが一般に受け入れられない可能性がある。生体検知においても、

---

16 提供されている検知精度の評価条件と調達者の利用条件の乖離が大きい場合には、その乖離による影響の分析や当該利用条件に基づいた検知精度の評価を実施することが考えられる。

17 BSC［2006］では、網膜の血管パターンから糖尿病などの病歴を、顔等の皮膚の色から人種を把握できると記述されている。

例えば、脈波を用いる場合には不整脈の有無から健康状態を知られるケースも考えられる（河野ら［2003］）ことから、社会的受容性の観点からの検討が行われることが望ましい。

事例	参考文献	評価項目 1 生体検知用サンプル (抽出する特徴)	評価項目 2 検知精度	評価項目 3 データセット	評価項目 4 利用者への 要求動作	評価項目 5 処理時間	評価項目 6 生体検知用参照 データの個別性	評価項目 7 実験に用いた装置の仕様
1	Baldisserra *et al.*［2006］	指から発生した物質の大気中の濃度(濃度の変化の度合い)	EER_{FD}=7.48%	被験者：20 人(40 指) 人工指：各 4 指(ｼﾘｺｰﾝ製、ｾﾞﾗﾁﾝ製、天然ｺﾞﾑ製)	指をｾﾝｻｰに 5 秒間乗せた後離す	・生体検知用ｻﾝﾌﾟﾙの取得：5 秒 ・認証試行間のｲﾝﾀｰﾊﾞﾙ：10～15 秒	利用者ごと	・0.2 秒間隔で濃度を測定可能なｹﾐｶﾙｾﾝｻｰ
2	Antonelli *et al.*［2006a］	連続撮影した指紋画像(指の回転による指紋のひずみの度合い)	EER_{FD}=4.9%	被験者：20 人(52 指) 人工指：各 4 指(ｼﾘｺｰﾝ製、ｾﾞﾗﾁﾝ製、天然ｺﾞﾑ製)	指をｾﾝｻｰに乗せ、一定速度で反時計回りに 15 度回転する	・生体検知用ｻﾝﾌﾟﾙの取得と生体検知部の処理の合計時間：平均 2 秒		・光学式ｾﾝｻｰ (500dpi, 30fps)
3	Antonelli *et al.*［2006b］		EER_{FD}=17.65%	被験者：45 人(90 指) 人工指：各 10 指(ｼﾘｺｰﾝ製、ｾﾞﾗﾁﾝ製、天然ｺﾞﾑ製、木工用ﾎﾞﾝﾄﾞ製)				・光学式ｾﾝｻｰ (569dpi, 20fps)
4			EER_{FD}=13.58%				ｼｽﾃﾑ共通(熟練者のものを使用)	
5	Tan and Schuckers［2006］	1 枚の指紋画像(隆線に沿った濃淡のﾊﾟﾀｰﾝのﾉｲｽﾞ成分)	FAR_{FD}=7% FRR_{FD}=15.4%	被験者：33 人(33 指) ｾﾞﾗﾁﾝ製人工指：33 指	指をｾﾝｻｰに乗せて離す	(記述なし)	ｼｽﾃﾑ共通(ﾃﾞｰﾀｾｯﾄの一部を基に決定)	・光学式ｾﾝｻｰ(380dpi)
6			FAR_{FD}=0% FRR_{FD}=10%	被験者：58 人 ｾﾞﾗﾁﾝ製人工指：30 指 粘土製人工指：50 指 分離指：25 指(10 人)		・生体検知用ｻﾝﾌﾟﾙの取得：提示直後の指紋画像を撮影		・光学式ｾﾝｻｰ(500dpi) ・静電容量式ｾﾝｻｰ(500dpi) ・電気光学式ｾﾝｻｰ(403dpi)
7	Tan and Schuckers［2008］	1 枚の指紋画像(谷＜隆線と隆線の間＞に沿った濃淡のﾊﾟﾀｰﾝのﾉｲｽﾞ成分)	FAR_{FD}=1.6% FRR_{FD}=0%					
8			FAR_{FD}=0% FRR_{FD}=9.1%	生体指：28 指 ｼﾘｺｰﾝ製人工指：28 指		(記述なし)		・光学式ｾﾝｻｰ(569dpi)
9	Jia *et al.*［2007］	連続撮影した指紋画像(ｾﾝｻｰに接地した指の面積、画像の輝度情報)	EER_{FD}=4.78%	被験者：15 人(30 指) ｾﾞﾗﾁﾝ製人工指：47 指		・生体検知用ｻﾝﾌﾟﾙの取得：1.5 秒		・静電容量式ｾﾝｻｰ (500dpi, 20fps)
10	Tai *et al.*［2006］	連続撮影した指紋画像(指表面の色、ｾﾝｻｰに接地した指の面積)	EER_{FD}=0%	被験者：47 人 人工指：9 種類		・生体検知部の処理：1 秒以下		・光源：赤と緑の LED ・ｾﾝｻｰ：光学式(15fps)
11	Zhang *et al.*［2007］	5 枚の指紋画像(指紋を上下左右にひずませた時のひずみの度合い)	EER_{FD}=4.5%	被験者：20 人(120 指) ｼﾘｺｰﾝ製人工指：120 指	指をｾﾝｻｰに乗せ、上下左右の方向にそれぞれ指をひずませる	(記述なし)		(記述なし)

（備考）・「利用者への要求動作」は、生体検知を行う際にどのように生体部位を提示するかを示す。
・「生体検知用参照データの個別性」は、生体検知用参照データを利用者ごとに用意するか、生体認証システムで共有するかを示す。
・「fps」は 1 秒間に撮影できるフレームの枚数を示す。
・「dpi」は 1 インチ当たりの画素数を示す。
・Antonelli *et al.*［2006b］（事例 3、4）は、2 種類の生体検知部を用意しそれぞれについて評価を行っているが、事例 2 との比較のために、事例 2 と同一の生体検知部を用いた検知精度を引用した。
・事例 5～8 は、複数のセンサーや複数の生体検知部ごとに検知精度を示しているため、検知精度が最も高いものを引用した。

図表5．指紋を対象とした生体検知技術の研究事例

(4) 指紋と組み合わせる生体検知技術の研究事例

イ． 研究事例

こうした評価項目に焦点を当てて生体検知技術の既存研究がどのように対応しているかをみる。生体検知技術の研究の多数を占めている指紋と組み合わせた研究事例のうち、特定の生体検知技術を評価する目的で被験者や人工物を用いて検知精度を測定しているものを取り上げる。図表 5の各評価項目の内容は、次のとおりである。

ロ． 各評価項目に関する考察

(イ) セキュリティ

セキュリティの観点からみると、次のような傾向がみられる。

①評価に用いられる人工物にはさまざまなバリエーションが存在する。

評価項目 3 をみると、評価に用いた人工物のバリエーションが 3 種類以下のものが多いものの、9 種類の人工物を用いて評価を行っているものもある（事例 10）。こうした事例を参考に多様な人工物を用いることが望ましい。事例 10 で用いられている人工物は次のとおりである。

・ シリコーン製人工指（黄色のもの、肌色のもの、スプレーで着色したもの）
・ ウレタン樹脂製人工指（箸を挿したもの、コーティングしたもの）
・ 薄く透明なシリコーンを貼り付けたウレタン樹脂に箸を挿した人工指
・ 薄く透明なシリコーンを生体指に貼り付けた人工指
・ ゼラチン製人工指
・ 食紅で着色したゼラチンに白色のアクリル棒を挿した人工指

②分離された生体部位を用いた検討が始まっている。

事例 6、7 をみると、分離された生体部位を用いた評価が行われている。仮に分離された生体部位を生体と判断してしまう生体認証システムを利用している場合には、なりすまし対象者の生体部位を分離する事件（Kent［2005］）が発生するおそれもあり、こうした検討が有用となる。

③データセットの影響を考慮した評価が行われるようになってきている。

同一の生体検知の手法に対して異なるデータセットを用いて検知精度を評価している事例がある。例えば、事例 3 は、同一の手法の評価を行っている事例 2

と比較して、データセットを変えることで事例 2 より検知精度が大きく低下しており、指を一定速度で 15 度回転させるという一見単純そうな動作であっても、利用者の慣れが検知精度に影響を与えている可能性があるとの考察を行っている（Antonelli *et al.*［2006b］）。また、タン=サッカーズは、自分達の研究グループが収集したデータセット（事例 6）と他の研究グループが用意したデータセット（事例 5）の結果をそれぞれ示している。同様の試みが事例 7、8 でも行われている。

このほか、事例 7 は、事例 6 と同一のデータセットを用いることで、データセットの影響を軽減したうえで生体検知の手法の検知精度の比較を行っている。

④評価条件や評価結果の記述が十分とはいえない事例が多い。

シリコーン製人工指やゼラチン製人工指にもさまざまなバリエーションがある。例えば、色の異なるシリコーン製人工指や含水率の異なるゼラチン製人工指が挙げられる。このような人工物の状態に関する詳細な記述が十分とはいえない事例が多い。

また、評価項目 2 をみると、複数の種類の人工物を用いて検知精度を評価していても、人工物ごとに検知精度を明記していないことがわかる。ただし、生体か否かを識別するために算出したスコアを人工物の種類ごとに示している事例もある（事例 10）。

(ロ) 利便性

利便性の観点からみると、次のような傾向がみられる。

①処理時間についての記述が十分とはいえない事例がみられる。

評価項目 5 をみると、生体検知に要する全体の時間、あるいは、生体検知に関する各処理に要する時間を明記している事例がみられる。生体検知の処理時間については、生体認証システムにおける実現形態によっては判定部の処理時間の影響を受ける可能性がある。そのため、生体検知に要する全体の処理時間を示すことが困難なケースも想定されるものの、可能な限り処理時間を示すことが望ましい。なお、PC を用いて生体検知部の処理を実行した際の時間が示されていることが多いものの、よりリソースの制限された環境での利用を想定した場合には、別途処理時間を評価する必要があると考えられる。

②生体検知用参照データの個別性の評価が行われるようになってきている。

Antonelli *et al.*［2006b］は、生体検知の手法とデータセットを揃えたうえで、生体検知用参照データを利用者ごとにした場合（事例 3）とシステム共通にした

場合（事例 4）について検知精度を比較している。事例 4 の方が検知精度が高いことについて、利用者は指を回転させる速度が一定でないことが多いのに対し、熟練者は速度が一定であったことが検知精度に影響を与えた可能性があるとの考察を行っている（Antonelli *et al.*［2006b］）。仮に同レベルの検知精度が得られるのであれば、利便性の観点からはシステム共通の生体検知用参照データを用いる方が望ましいと考えられる。生体検知用参照データの個別性についても研究テーマの 1 つと考えられる。

③指紋を対象とした生体検知の手法であっても、指の提示方法が区々である。

評価項目 4 をみると、指の提示方法が区々であることがわかる。例えば、事例 9（Jia *et al.*［2007］）は、指を提示するだけであり、利用者が指を 15 度回転させる動作（事例 2～4）よりも利用者の負担が少ないと主張している。利用者への要求動作による負担については、想定する利用者の集合や負担の検知精度への影響等を考慮して検討することが望ましいと考えられる。

(ハ) コスト

評価項目 7 をみると、実験に用いた装置の仕様を明記している事例が多いことがわかる。しかし、ハードウエアの要求性能について議論している事例はほとんどない。事例 2 は要求性能を示しているものの、複数の性能のハードウエアを用意し、各ハードウエアの検知精度を比較するなどの検討結果については示されていない。

(ニ) 社会的受容性

図表 5の事例をみる限りでは、生体検知に用いる特徴に関してプライバシー等の社会的受容性の観点から議論しているものはない。こうした点について、利用者の理解が得られるよう学会においても議論が行われることが望ましいと考えられる。

5．考察

ここまでの検討結果を踏まえて、なりすましへの対応のあり方について考察する。

(1) 研究動向のフォローの重要性

2 節において新たな研究成果を踏まえて攻撃と対策の整理を行ったように、研究動向のフォローを行い、提案される攻撃や対策についても同様のアイデアに基づく検討を行うことが望ましい。例えば、人工物等の受入れへの対策の 1 つとして金融機関職員等の人間による監視を選択した場合においても、人工物の研究動向に注視することが有用である。図表 6に示すように、指紋のパターンが付与された薄いゼラチンによって実現される巧妙な人工指が提案されており、人間による監視だけでは検知が容易とはいえないケースがありうる。このような人工物を利用した攻撃に対応するためにも、どうすれば人工物による偽造が可能となるかを知っておくことが大切である。

（備考）Sandström［2004］の図 7.4 を引用

図表6．薄いゼラチンを付けた生体指

(2) 検知精度の比較に向けた取組み

また、今後、さまざまな生体検知の手法について、それらの検知精度の比較をどのように実現していくかについて検討が望まれる。測定される検知精度には、評価条件の差異による影響が存在するため、検知精度を直接比較することが適切ではないケースが現時点では少なくない。一方、認証精度の比較についてみると、共通のデータセットを用いて各生体認証システムを比較するという取組み（FVC[18]等）や、第三者評価機関（K-NBTC[19]、IBG[20]等）が各生体認証シ

18 FVC（Fingerprint Verification Competition）：指紋認証システムの照合アルゴリズムを評価対象とする認証精度評価プロジェクトであり、主催者はボローニャ大学（伊）、ミシガン州立大学、サンノゼ州立大学、マドリッド自治大学である。2000 年から開催されている。

ステムを評価するという取組みが行われている。検知精度の比較においても、こうした取組みが参考になると考えられる。例えば、共通のデータセットを用いるアプローチについて考察すると、生体検知の手法によっては、原理的に同一のデータセットを用いることが困難なケースがありうる。前節の事例を引き合いに出せば、事例 1 では指から発生した物質の濃度を利用しているのに対し、事例 2 では連続して撮影した指紋画像を利用しており、データセットの共有化を図ることは難しい。指紋画像を用いる手法同士であれば（例えば、事例 5〜9）、データセットの共有化を図ること考えられる。こうした点についても検討を深めていくことが重要である。

(3) 検知精度に影響を与える要素の解明と記述

前節(4)で述べたように、さまざまな人工物を用いて検知精度の測定が行われているものの、測定時の環境条件（気温、人工物の状態等）や評価結果（人工物ごとの検知精度等）が論文等において十分に記述されているとはいえない。生体検知の手法の提案の論文においては、こうした情報を明記することが望まれる。また、記述が不十分である一因として、検知精度に影響を与える要素が明らかになっていないことが考えられる。そのため、影響を与える要素についての検討を深めるとともに、そうした要素がどのような条件であれば検知精度を比較する際に影響がないとみなすことができるかについても議論していくことが重要である。

---

19 K-NBTC（Korea-National Biometric Test Center）：韓国情報保護振興院（KISA：Korea Information Security Agency）内部に設立された第三者評価機関であり、生体認証システムの認証精度等を評価し認定書の発行を行っている。

20 IBG（International Biometric Group）：生体認証技術に関する米国の民間コンサルティング会社であり、第三者的な立場から生体認証システムの評価プロジェクト（Comparative Biometric Testing Round 6 等）を実施しているほか、米国国防省と共同で指紋認証システムを開発するなどの活動も行っている。

6．まとめ

生体認証システムを適切に利用していくためには、生体認証に特有の脆弱性としてどのようなものが知られているかを把握し、適切な対策を講じていくことが重要である。ただし、生体認証は現在発展途上の技術であり、学会を中心に、脆弱性の洗出しや評価のあり方に加えて、各脆弱性への対策に関する技術的な検討が進められているところである。

こうしたなか、本稿では、学会で提案されている新たな攻撃法や対策を踏まえて、脆弱性となりすましの関係を整理しなりすましの方法を検討した。また、各実行方法への対策を整理するとともに、想定するなりすまし方法に網羅的に対策を講じる考え方を示した。さらに、なりすましへの対策の 1 つである生体検知技術に焦点を当てて、研究動向を紹介するとともに、セキュリティ、利便性、コスト、社会的受容性の観点から考察した。

金融業務において生体認証システムを利用していくためには、新たな攻撃や対策の研究動向をフォローしていくことが求められる。今回紹介した生体検知技術等の技術にも注目しながら、それらを適切に活用していく方法について引き続き検討していくことが重要であろう。

【参考文献】

青山真之・西垣正勝、「生体反射型認証 －輻輳反射と眼球形状を利用した認証方式の提案－」、『情報処理学会研究報告』、情報処理学会、2007-CSEC-38、2007 年、185～191 頁

宇根正志・田村裕子、「生体認証における生体検知機能について」、『金融研究』第 24 巻別冊第 2 号、日本銀行金融研究所、2005 年、1～55 頁

――――・松本　勉、「生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に」、『金融研究』第 24 巻第 2 号、日本銀行金融研究所、2005 年、35～83 頁

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-CSEC-20-44、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』、情報処理学会、2002 年

大野敬弘・鹿嶋雅之・佐藤公則・渡邊　睦、「手形状認証によるセキュリティキー入力システムに関する研究」、『電子情報通信学会研究報告 パターン認識・メディア理解』、Vol.107、No.427、2008 年、325～332 頁

加藤雅之・新崎　卓・井垣誠吾・山岸文雄・池田弘之、『生体検知装置および該装置を用いた指紋照合システム』、特公平 8-23885、公告日：1996 年 3 月 6 日

金融情報システムセンター（FISC）、『金融機関等コンピュータシステムの安全対策基準・解説書 第 7 版』、FISC、2006 年

國井　雅・遠藤良輔・有沢大輔・四方順司・松本　勉、「非常時通報機能を有するオンライン手書き署名認証方式の提案」、『コンピュータ・セキュリティ研究会（CSEC）予稿集』、情報処理学会、Vol. 36、2007 年、369～347 頁

河野美由紀・梅村晋一郎・長野明紀・鱒沢　裕、『生体認証装置および該装置実現のためのプログラム』、特開 2003-331268、公開日：2003 年 11 月 21 日

小松尚久、「バイオメトリクスセキュリティ評価基準に関する研究」、『平成 16 年度経済産業省基準認証研究開発事業 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』早稲田大学共同研究報告書、ニューメディア開協会、2005 年

清水將吾・瀬戸洋一、「バイオメトリック認証システムにおけるキャンセラブルバイオメトリック技術の有効性の検討」、『2008 年暗号と情報セキュリティシンポジウム予稿集』、2B3-2、2008 年

情報処理推進機構（IPA）、『バイオメトリクス・セキュリティ評価に関する研究会 平成 18 年度 研究会中間報告書』、IPA、2006 年

田村裕子・宇根正志、「金融取引における IC カードを利用した本人認証について」、『金融研究』25 巻別冊第 1 号、日本銀行金融研究所、2006 年

――――・――――、「IC カードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」、『金融研究』26 巻別冊第 1 号、日本銀行金

融研究所、2007 年
中崎麻由子・田中瑛一・松本　勉、「静脈画像の圧力依存性を用いた指の生体検知」、『第 12 回バイオメトリックシステムセキュリティ研究会資料』、電子情報通信学会、2008 年、25～30 頁
日本バイオメトリクス認証協議会（JBAA）、『JBAA 技術部会 2002 年度成果報告会配付資料 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
バイオメトリクスセキュリティコンソーシアム（BSC）、『バイオメトリックセキュリティ・ハンドブック』、オーム社、2006 年
古江岳大・遠藤良輔・四方順司・松本　勉、「非常時通報機能を有するユーザ認証方式のモデル化」、『2006 年暗号と情報セキュリティシンポジウム予稿集』、3D1-5、2006 年
松本　勉・清水将太、「手のひら静脈認証システムにおける画像処理ベース生体検知機能に関するホワイトボックス認証システムとテスト物体」、『第 16 回バイオメトリックシステムセキュリティ研究会』、BS-16-08、2009 年
村松大吾、「ヒルクライミング法を用いたオンライン署名認証アルゴリズムの検討」、『2008 年暗号と情報セキュリティシンポジウム予稿集』、2B4-2、2008 年
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』、2A2-1、2005 年
読売新聞、「「生体認証」破り入国」、朝刊、1 月 1 日、2009 年
Antonelli, Athos, Raffaele Cappelli, Dario Maio, and Davide Maltoni, “A New Approach to Fake Finger Detection based on Skin Distortion,” *1st International Conference on Biometrics (ICB)*, LNCS 3832, Springer-Verlag, 2006a, pp.221-228.
――――, ――――, ――――, and ――――, “Fake Finger Detection by Skin Distortion Analysis,” *IEEE Transaction on Information Forensics and Security*, Vol.1, No.3, Springer-Verlag, 2006b, pp.360-373.
Baldisserra, Denis, Annalisa Franco, Dario Maio, and Davide Maltoni, “Fake Fingerprint Detection by Odor Analysis,” *1st International Conference on Biometrics (ICB)*, LNCS 3832, Springer-Verlag, 2006, pp.265-272.
Derakhshani, Reza, Stephanie Schuckers, Larry Hornak, and Lawrence O’Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” *Pattern Recognition*, Vol.36, Issue 2, 2003, pp.383-396.
Hill, Chirstopher James, “Risk of masquerade arising from the storage of biometrics,” Bachelor thesis, Department of Computer Science, Australian National University, 2001.
International Organization for Standardization (ISO), ISO 19092 – Financial services – Biometrics – Security , ISO, 2008.
――――, and ――――, ISO/IEC 19795-1 Information technology – Biometric performance testing and reporting – Part 1: Principles and framework, ISO and IEC, 2006.
――――, and ――――, ISO/IEC JTC1/SC37 Standing Document 2 (SD2) – Harmonized biometric vocabulary, Ver. 10, N2777, ISO and IEC, 2008.
Inuma, Manabu, Akira Otsuka, and Hideki Imai, “Theoretical framework for

constructing matching algorithms in biometric authentication systems," in submission to International Confference on Biometrics (ICB) 2009.

Jia, Jia, Lianhong Cai, Kaifu Zhang, and Dawei Chen, "A New Approach to Fake Finger Detection based on Skin Elasticity Analysis," *2nd International Conference on Biometrics (ICB)*, LNCS 4642, Springer-Verlag, 2007, pp.309-318.

Kent, Jonathan, "Malaysia car thieves steal finger," BBC News, 31 March, 2005. available at http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Lee, Eui Chul, Kang Ryoung Park, and Jaihie Kim, "Fake iris detection by using purkinje image," *1st International Conference on Biometrics (ICB)*, LNCS 3832, Springer-Verlag, 2006, pp.397-403.

Li, Jiangwei, Yunhong Wang, Tieniu Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," *SPIE Defense and Security Symposium 2004*, Vol. 5404, Biometric Technology for Human Identification, 2004, pp. 296-303.

Nixon, Kristin A., Robert K. Rowe, Jeffrey Allen, Steve Corcoran, Lu Fang, David Gabel, Damien Gonzales, Robert Harbour, Sarah Love, Rick McCaskill, Bob Ostrom, David Sidlauskas, and Karen Unruh, "Novel spectroscopy-based technology for biometric and liveness verification," *Biometric Technology for Human Identification, Proceedings of SPIE*, Vol. 5404, 2004, pp.287-295.

van der Putte, Ton, and Jeroen Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned," *Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, 2000, pp. 289-303.

Sandström, Marie, "Liveness Detection in Fingerprint Recognition Systems," Master thesis, Linköpings Universitet, 2004.

Schuckers, Stephanie, "Spoofing and anti-spoofing measures," Information Security Technical Report, Vol. 7, No. 4, 2002, pp. 56-62.

Tai, Katsuki, Etsuji Matsuyama, Masashi Kurita, and Ichiro Fujieda, "Dual-LED imaging for liveliness detection and its evaluation with replicas," *Applied Optics*, Vol.45, No.24, 2006, pp.6263-6269.

Tan, Bozhao, and Stephanie Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing," *Conference on Computer Vision Pattern Recognition Workshop (CVPRW 2006)*, 2006.

————, and ————, "New Approach for Liveness Detection in Fingerprint Scanners based on Valley Noise Analysis," *Journal of Electronic Imaging*, Vol.17, No.1, 2008, p.011009.

Tsutomu, Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," *In Proceedings of SPIE Vol.4677, Optical Security and Counterfeit Deterrence Techniques IV*, 2002, pp. 275-289.

Une, Masashi, Akira Otsuka, and Hideki Imai, "Wolf Attack Probability: A Theoretical Security Measure in Biometric Authentication Systems," *IEICE Trans. Inf. & Syst.*, Vol. E91-D, No. 5, 2008, pp. 1380-1389.

Wills, David, and Mike Lee, "Six biometric devices point the finger at security," *Network Computing*, Vol.9, Issue 10, pp.84-96, 1998.

Zhang, Yangyang, Jie Tian, Xinjian Chen, Xin Yang, and Peng Shi, "Fake finger detection based on Thin-Plate Spline distortion model," *2nd International Conference on Biometrics (ICB)*, LNCS 4642, Springer-Verlag, 2007, pp.742-749.

付録．なりすましを目的とする攻撃の実行方法と対策

攻撃			想定される対策
ISO/IEC FCD 19792で規定された脆弱性のうち利用するもの	具体例		
・ データの漏洩	方法1-1	攻撃対象の生体認証システムから入手したなりすまし対象者の生体サンプルや参照データを基に入力情報を入手する（JBAA［2003］）。	・ 生体認証システム内のデータの暗号化、システムの耐タンパー化、ログ収集を行う（宇根・松本［2005］）。 ・ テンプレート保護技術を利用する（IPA［2006］）。 ・ チャレンジ・レスポンス認証を利用する（Schuckers［2002］）。
・ 生体特徴の秘匿困難性	方法1-2	攻撃対象の生体認証システムのセンサーにおける生体特徴の痕跡を基に入力情報を入手する（JBAA［2003］）。	・ 提示された生体特徴を非接触型のセンサーで読み取る（BSC［2006］）。 ・ センサー上の痕跡を拭き取る（宇根・松本［2005］）。
	方法1-3	日常生活における生体特徴の痕跡（残留指紋等）を基に入力情報を入手する（JBAA［2003］）。	・ 日常生活において痕跡が残りにくいモダリティ(静脈パターン等)を利用する(宇根･松本[2005])。
	方法1-4	露出している生体特徴を観測した情報を基に入力情報を入手する（JBAA［2003］、遠藤・平林・松本［2003］）。	・ 生体特徴をセンサーに提示する方法を別途決める（大野ら［2008］）。 ・ チャレンジ・レスポンス認証を利用する（Schuckers［2002］）。
・ 認証精度の限界 ・ データの漏洩 ・ 合成された擬似生体サンプルの受入れ	方法1-5	認証時の照合スコアを参照できる場合において、擬似生体サンプル探索用の生体認証システムに初期値として（擬似）生体サンプルを与え、照合スコアが改善されるように初期値に修正を加えることで擬似生体サンプルを探索し入力情報とする（ヒル・クライミング攻撃、Hill［2001］）。	・ 判定しきい値をより厳しく設定するなどの方法によって認証精度を向上させ、攻撃に必要な計算量を増大させる（宇根・松本［2005］）。 ・ ヒル・クライミング攻撃に耐性のある照合アルゴリズムを利用する（小松［2005］、村松［2008］）。 ・ 一定回数連続して認証に失敗した場合には、新たな認証処理を開始しない（宇根・松本［2005］）。
・ なし	方法1-6	他の生体認証システムや生体特徴を用いた他のアプリケーションから、なりすまし対象者の生体特徴から派生する情報を入手し、これを基に入力情報を入手する。	・ 他の生体認証システムや他のアプリケーションで利用されていないモダリティを利用する。 ・ テンプレート保護技術を利用する。
	方法1-7	なりすまし対象者の生体部位（指等）を分離し、これを基に入力情報を入手する（JBAA［2003］）。	・ 分離された生体部位からは生体特徴に関する情報を得ることができないようなモダリティ（行動的特徴等）を利用する。
	方法1-8	なりすまし対象者を騙し偽端末に生体特徴を提示させ、得られた情報を基に入力情報を入手する（FISC［2006］）。	・ IC カード等を用いて、利用者が端末を認証する（田村・宇根［2006］）。 ・ 偽端末の有無を監視によって確認する（FISC［2006］）。 ・ 利用者を啓蒙する（FISC［2006］）。
	方法1-9	攻撃者がなりすまし対象者を脅すことで入力情報を入手する（JBAA［2003］）。ただし、生体部位の分離は含まない。	・ 非常時通報を利用する（古江ら［2006］、國井ら［2007］）。
	方法1-10	なりすまし対象者と結託し、得られた情報を基に入力情報を入手する（JBAA［2003］）。ただし、生体部位の分離は含まない。	・ デジタル・フォレンジック技術等により結託していることを事後的に検知する。

（備考）灰色のセルは技術的対策であることを表す。「マルチ･モーダル認証を行う（BSC［2006］）」は、方法 1-1～1-10 への対策となりうる。

図表7．本人の生体特徴から派生する情報を基にした入力情報の入手方法と対策の例

攻撃			想定される対策
ISO/IEC FCD 19792 で規定された脆弱性のうち利用するもの	具体例		
・ データの漏洩	方法 1-11	生体認証システム内部を解析し、任意のセンサーへの入力に対して「受理」を出力するようなデータ等を入力情報とする（JBAA［2003］）。	・ 生体認証システム内のデータの暗号化、システムの耐タンパー化、ログ収集を行う（宇根・松本［2005］）。
・ 認証精度の限界	方法 1-12	なりすまし対象者以外の生体特徴を用いる（JBAA［2003］）。ただし、なりすまし対象者の血縁者の生体特徴を用いる方法は含まない。	・ 認証精度を向上させる（判定しきい値の調節、照合アルゴリズムの改良等、宇根・松本［2005］）。
・ 認証精度の限界 ・ 血縁関係による類似	方法 1-13	なりすまし対象者の血縁者（双子等）の生体特徴から派生した情報を基に入力情報を入手する（JBAA［2003］）。なお、方法 1-1～1-10 を併せて実行する。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ 血縁関係の影響がないモダリティを利用する。
・ 認証精度の限界 ・ 合成された擬似生体サンプルの受入れ	方法 1-14	生体特徴を模した擬似生体特徴や幾何学模様等を入力情報とする。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ 生体認証システムが読み取った擬似生体サンプルを解析し、人間が取り得る値となっているか否かを検査する。
・ 認証精度の限界 ・ 合成された擬似生体サンプルの受入れ ・ 特殊な生体特徴の存在	方法 1-15	品質の低い（擬似）生体サンプルを基に入力情報を入手する。ただし、攻撃対象の生体認証システムを解析し、ウルフ等の特殊な生体特徴を求める方法（方法 1-18）は行わない。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ 生体サンプルの品質を検査する（宇根・松本［2005］）。
・ 認証精度の限界 ・ データの漏洩	方法 1-16	複数の参照データから攻撃者の生体特徴と類似したものを探索し、対応する参照データ識別子を特定し、攻撃者自身の生体特徴を入力情報とする（ISO［2008］）。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ 生体認証システム内のデータの暗号化、システムの耐タンパー化、ログ収集を行う（宇根・松本［2005］）。
	方法 1-17	入手した複数の参照データを比較し、類似するペアを探索する（ISO［2008］）。一方をなりすまし対象者とし、他方の参照データを基に入力情報を入手する。	
・ 認証精度の限界 ・ データの漏洩 ・ 特殊な生体特徴の存在	方法 1-18	入手した複数の参照データを比較する。最も多くの参照データと誤一致する参照データを探索し入力情報を入手する（ウルフ攻撃の一種、門田・黄・吉本［2005］）。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ ウルフ攻撃に耐性のある照合アルゴリズムを利用する（門田・黄・吉本［2005］、Une, Otsuka, and Imai［2008］、Inuma，Otsuka, and Imai［2009］）。 ・ 生体認証システム内のデータの暗号化、システムの耐タンパー化、ログ収集を行う（宇根・松本［2005］）。
・ 認証精度の限界 ・ データの漏洩 ・ 合成された擬似生体サンプルの受入れ ・ 特殊な生体特徴の存在	方法 1-19	照合アルゴリズムを解析し、なりすましの成功確率が高くなるような（擬似）生体サンプルを求め入力情報を入手する（ウルフ攻撃、Une, Otsuka, and Imai［2008］）。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ ウルフ攻撃に耐性のある照合アルゴリズムを利用する（Une, Otsuka, and Imai［2008］、Inuma，Otsuka, and Imai［2009］）。 ・ 生体認証システムが読み取った擬似生体サンプルを解析し、人間が取り得る値となっているか否かを検査する。 ・ 生体認証システム内のデータの暗号化、システムの耐タンパー化、ログ収集を行う（宇根・松本［2005］）。

（備考）灰色のセルは技術的対策であることを表す。「マルチ･モーダル認証を行う（BSC［2006］）」は、方法 1-11～1-19 への対策となりうる。

図表8．本人の生体特徴から派生していない情報を基にした入力情報の入手方法と対策の例

攻撃			想定される対策
ISO/IEC FCD 19792 で規定された脆弱性のうち利用するもの	具体例		
・ 人工物等の受入れ	方法 2-1	入力情報に基づき作製した人工物をセンサーに提示する（JBAA［2003］）。	・ 生体検知技術を利用する（宇根・松本［2005］）。 ・ 生体特徴の偽造が困難な読取方法を利用する（遠藤・松本［2002］）。
	方法 2-2	分離した生体部位をセンサーに提示する。	・ 人工物等を提示しているか否かを監視する（IPA［2006］）。
・ 生体特徴の意図的な変更	方法 2-3	入力情報を基に攻撃者が自分の生体特徴を意図的に変更したうえで、センサーに提示する（JBAA［2003］）。	・ 模倣が困難なモダリティを利用する（青山・西垣［2007］）。
・ データの漏洩・改ざん	方法 2-4	生体認証システムにおいてデータ（生体サンプル）の挿入やデータ（参照データ、判定しきい値、認証結果）の改ざんを行うとともに、必要に応じて攻撃者が自分の生体特徴をセンサーに提示する（JBAA［2003］）。	・ 生体認証システム内のデータの暗号化やシステムの耐タンパー化により、データの改ざんや挿入を防止・検知する（宇根・松本［2005］）。 ・ システムに配線をつなぐ行為等を監視する。
・ 認証精度の限界	方法 2-5	本人以外の利用者を脅して、当該利用者の生体特徴をセンサーに提示させる（JBAA［2003］）。	・ 認証精度を向上させる（宇根・松本［2005］）。 ・ （攻撃者がその場にいる状況であれば）脅されているか否かを監視する（宇根・松本［2005］）。
	方法 2-6	攻撃者や結託者が自分の生体特徴をセンサーに提示する（JBAA［2003］）。ただし、生体特徴の意図的な変更や生体認証システム内のデータの改ざんは行わない。	・ 認証精度を向上させる（宇根・松本［2005］）。
・ 環境変化による認証精度への影響	方法 2-7	センサー周辺の環境を変化させたうえで、方法 2-1～2-6 を実行する（JBAA［2003］）。	・ 環境状態の異常を検知し、生体認証システムを停止する（IPA［2006］）。 ・ 環境の変化を受けにくいモダリティや読取方法を利用する。 ・ 外部環境の影響を軽減する工夫を行う（補助光の利用等）。 ・ 故意にセンサー周辺の環境を変更しようとする行為を監視する（IPA［2006］）。

（備考）灰色のセルは技術的対策であることを表す。「マルチ・モーダル認証を行う（BSC［2006］）」は、方法 2-1～2-7 への対策となりうる。

図表9．入力情報をシステムへ入力する方法と対策の例