IMES DISCUSSION PAPER SERIES

生体認証における生体検知機能について

宇根 正志（うね まさし）・田村 裕子（たむら ゆうこ）

Discussion Paper No. 2005-J-15

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

IMES Discussion Paper Series 2005-J-15
2005 年 8 月

生体認証における生体検知機能について

宇根　正志†・田村　裕子‡

要　旨

生体認証技術は、各個人に固有とみられる身体的特徴等を用いて自動的に個人を認証する技術であり、金融分野では銀行の窓口や ATM 等における顧客の本人確認手段の 1 つとして注目されている。しかし、本技術を安全に利用していくためには､身体的特徴の偽造に十分留意する必要がある。実際、安価に作製された人工指を一部の指紋照合装置が高い確率で本物と判定してしまうという実験結果が示されており、他の身体的特徴を用いた装置においても同様の脆弱性が今後顕現化する可能性は否定できない。

こうした脆弱性への有力な対策の 1 つとして、生体検知機能の利用が挙げられる。生体検知機能は、脈拍等の生体固有の特性を用いて、身体的特徴等が生体によって提示されたか否かを確認する機能である。本機能を適切に活用すれば、身体的特徴の偽造に対して一定の効果を期待することが可能であろう。

しかし、生体検知機能の効果をどのように評価するかについては、これまで学会等のオープンな場ではあまり議論されてこなかった。今後、生体認証技術を適切に活用していくためには、生体認証システムのセキュリティ・レベルの維持・向上を図ることが重要であり、その手法の 1 つとして生体検知機能について検討することが求められる。

本稿では、そうした検討の端緒として、生体検知機能の概念整理を行うほか、生体検知機能のセキュリティ要件やそれに基づく生体認証システムの分類法を検討する。さらに、最近の特許情報からいくつかの生体検知機能の手法を紹介するとともに、生体検知機能に関する今後の検討の方向性を示す。

キーワード：生体認証、生体検知、セキュリティ、脆弱性、指紋、静脈パターン、虹彩

JEL classification: L86、L96、Z00

† 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）
‡ 日本銀行金融研究所情報技術研究センター（E-mail: yuuko.tamura@boj.or.jp）

本稿の作成に当たっては、横浜国立大学の松本 勉教授、早稲田大学の小松尚久教授、日立製作所の瀬戸洋一主管研究員、立命館大学の藤枝一郎教授から有益なコメントを頂いた。ここに記して感謝したい。本稿に示されている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個人に属する。

目　次

1．はじめに

携帯電話やパソコンの起動時における本人確認から空港における入国者の審査に至るまで、生体認証技術を実現するシステム（生体認証システム）が利用される場面が急速に増えてきている。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を自動的に認証する技術であり、「各個人に固有の特徴」として、指紋、虹彩、血管パターン、顔、声紋、動的署名等が挙げられる。金融分野においては、大手の銀行を中心に、窓口や ATM における顧客の本人確認の手段として生体認証技術を採用する、あるいは、採用を予定する動きが 2004 年半ば以降目立っている。スルガ銀行と東京三菱銀行は、手のひらの静脈パターンを利用した生体認証システムを 2004 年 6 月、同年 10 月にそれぞれ導入しているほか、広島銀行と池田銀行も 2005 年 4 月、同年 6 月に手のひらの静脈パターンを利用した生体認証システムをそれぞれ導入している。また、みずほ銀行、三井住友銀行、日本郵政公社等は、指の静脈パターンを利用した生体認証システムを今後導入する方針を明らかにしている。

金融業務において生体認証システムを長期間にわたり安定的かつ安全に運用していくためには、仮にそうしたシステムにおいて脆弱性が顕現化した場合でも、その脆弱性を早急に回避できるように体制を整備しておく必要がある。生体認証システムに固有の脆弱性は、日立製作所[2004]において網羅的に整理されている。その中でも、物理的に偽造された身体的特徴を誤って本物と判定してしまうというタイプの脆弱性への対策について検討することが重要であると考えられる（宇根・松本 [2005]）。指紋照合装置については、コップや携帯電話等の残留指紋から作製された人工の指を高い割合で受け入れてしまうものが存在するとの結果が複数の研究者から報告されている（van Putte and Keuning [2000]、Matsumoto *et al*. [2002]、Ligon [2002]、Thalheim, Krissler and Ziegler [2002]、Blommé [2003]、Sandström [2004]、堀内 [2005]）。一部の虹彩照合装置においても、虹彩の画像を印刷した上質紙によって作製された人工の虹彩を高い割合で受け入れてしまうことが示されている（Thalheim, Krissler and Ziegler [2002]、松本・平林 [2003a, b]、松本・平林・佐藤 [2004]）。さらに、指の静脈パターンの照合装置に関しては、生きている人間の指ではない提示物の内部形状を高い確率で誤って静脈パターンとして読み取ってしまうものが存在するとの実験結果が報告されている（松本ほか [2005a, b]）。

こうした脆弱性への有力な対策として、生体検知（liveness detection）の機能の活用が挙げられるケースが多い。生体認証技術の文脈における生体検知機能

は、生体認証システムによって読み取られた情報が生きている人間によって提示されたものか否かを自動的に確認する機能と捉えられることが多い（例えば、Valencia and Horn [2003]）。こうした機能を実現する代表的な手法として、例えば、生きている人間の体の電気特性（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・透過率等）、生理的特性（脈拍、体温、発汗等）に基づくものが挙げられる。こうした手法を生体認証システムに適用すれば、人工指や人工虹彩等の人工物を誤って生体であると判定してしまうという脆弱性を軽減することが可能になると期待される。

ただし、仮に、銀行をはじめとする生体認証システムの運営者が生体検知機能を採用しようとした場合、数ある生体検知機能の実現方式の中から、当該アプリケーションにおいて要求されるセキュリティ・レベル、利便性、コスト等の条件を満足するものを適切に選択することは容易でないのが実情である。生体検知機能の実現方式をセキュリティの観点から分析・評価した結果が学会等のオープンな場で報告される事例（例えば、Derakhhani *et al*. [2003]、田井ほか [2005]）は少なく、最近の生体検知機能をサーベイした公表文献も筆者らが知る限り存在しない。また、生体認証システムを開発・提案している企業の多くは、生体検知機能を当該システムに実装しているか否かを明らかにしていない、また、実装しているとしても技術の詳細を明らかにしていない（IBG [2003]、Valencia and Horn [2003]、Sandström [2004]）といった事情もある。こうしたことから、生体認証システムの運営者が参照可能な情報は非常に限定され、生体検知機能の各種実現方式を評価して当該システムへの組込みの是非を自ら判断することが困難な状況となっている。

今後、金融分野において生体認証技術を適切に活用していくためには、生体認証システムのセキュリティ・レベルの維持・向上を図ることが重要であり、そのための手法の 1 つとして生体検知機能について検討することが求められる。こうした検討を進めていくうえでは、生体検知機能の技術的な課題や研究成果について、学会等のオープンな場での議論を活発化させることが求められる。これまでの経緯を踏まえると、オープンな場での議論を活発化させることは一朝一夕に実現できることではないと考えられる。しかし、生体認証システムを安心して利用できる環境を整備するうえでは極めて重要であり、具体的な方策について検討することが必要であると思われる。例えば、生体認証システムの運営者が学会の議論に積極的に参画するといったことがまず必要と考えられる。これに加えて、生体検知機能に関する最新の情報を入手し、各種の実現方式をさまざまな角度から評価することができるように体制を整備していくことが重要である。

本稿は、そうした検討・体制整備の出発点として、金融機関をはじめとする生

体認証システムの運営者を含め、生体検知機能に関心をもつ人々に、その現状と今後の課題についての解説を主な目的としている。

本稿の構成は以下のとおりである。2 節において、生体認証技術や生体認証システムの基本的な概念について説明するとともに、身体的特徴の偽造に関する研究成果や、生体検知機能をはじめとする対策について現状を説明する。3 節においては、既存の文献等を参考にしつつ生体検知機能を定義するとともに、生体検知機能のセキュリティ要件について検討し、同要件に基づいて生体検知機能を搭載した生体認証システムの分類法を提案する。4 節においては、金融分野において特に注目を集めている指紋、静脈パターン、虹彩に着目し、これらのいずれかを利用した生体認証システムに組み込まれる可能性が高いとみられる生体検知機能を取り上げ、具体的な実現方式としてどのようなものが提案されているかをわが国の特許情報を参照しながら紹介する。5 節においては、本稿における検討結果を踏まえ、今後生体検知機能についてセキュリティの観点から検討を深めていく際の方向性を示す。最後に、6 節において、本稿の検討結果とそのポイントを再度強調して本稿を締めくくる。

2．生体認証とその脆弱性

(1) 生体認証技術とそれを実現するシステム

イ．生体認証技術

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機械による自動処理によって個人を認証する技術であり、バイオメトリクス（biometrics）[1]、あるいは、バイオメトリック個人認証技術とも呼ばれる。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]）。

①普遍性（universality：その特徴を誰もが有していること）
②唯一性（uniqueness：本人以外は同一の特徴を有していないこと）
③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）
④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）
⑤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、日本自動認識システム協会 [2005]、情報処理推進機構 [2004, 2005]、瀬戸 [2002, 2003, 2005]、Bolle *et al.* [2003]）。こうした文献では、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、耳形状等が挙げられているほか、代表的な行動的特徴として、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。これらのうち、指紋、虹彩、血管パターン、顔、声紋、動的署名に関しては、認証精度の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。

金融分野における最近の事例をみると、手のひらや指の静脈パターンを利用した生体認証システムに注目が集まっている。スルガ銀行と東京三菱銀行がそれぞれ2004年6月、同年10月に手のひらの静脈パターンを利用した生体認証シ

---

[1] 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。

ステムを顧客の本人確認向けに採用したほか、広島銀行と池田銀行もそれぞれ2005年4月、6月に手のひらの静脈パターンを利用したシステムを導入している。また、三井住友銀行、みずほ銀行、日本郵政公社等は、指の静脈パターンを利用した生体認証システムの導入を予定している旨の発表を行っている。

ロ．認証の形態

（イ）照合の形態

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、生体認証技術を実現するシステムに提示された身体的・行動的特徴の持ち主があらかじめ登録された個人か否かを確認するものである。被認証者は、自分の身体的・行動的特徴のアナログ情報（以下、生体特徴情報＜biometric data＞と呼ぶ[2]）から抽出された各個人固有のデータ（以下、固有パターンと呼ぶ）を、個人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。固有パターンや個人識別 ID 等は被認証者ごとに 1 つのデータ・セットとして保管されることが多く、テンプレートと呼ばれる。被認証者は、認証時には、自分の身体的・行動的特徴とともに個人識別 ID 等を生体認証システムに提示する。システム側では、センサで読み取った生体特徴情報から固有パターンを抽出し、テンプレートの固有パターンと照合する。

1 対 *n* 照合は、個人識別 ID を提示せず、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）だれのものかを照合・識別するものである。被認証者の固有パターンは、個人識別 ID とともにあらかじめ当該システムに登録される。認証時には、生体特徴情報のみが提示され、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。一致すると判定される固有パターンが存在する場合、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か否かを上記と同様の手続で確認するケース（ネガティブ識別と呼ばれる）も 1 対 *n* 照合の 1 種と位置づけられる。

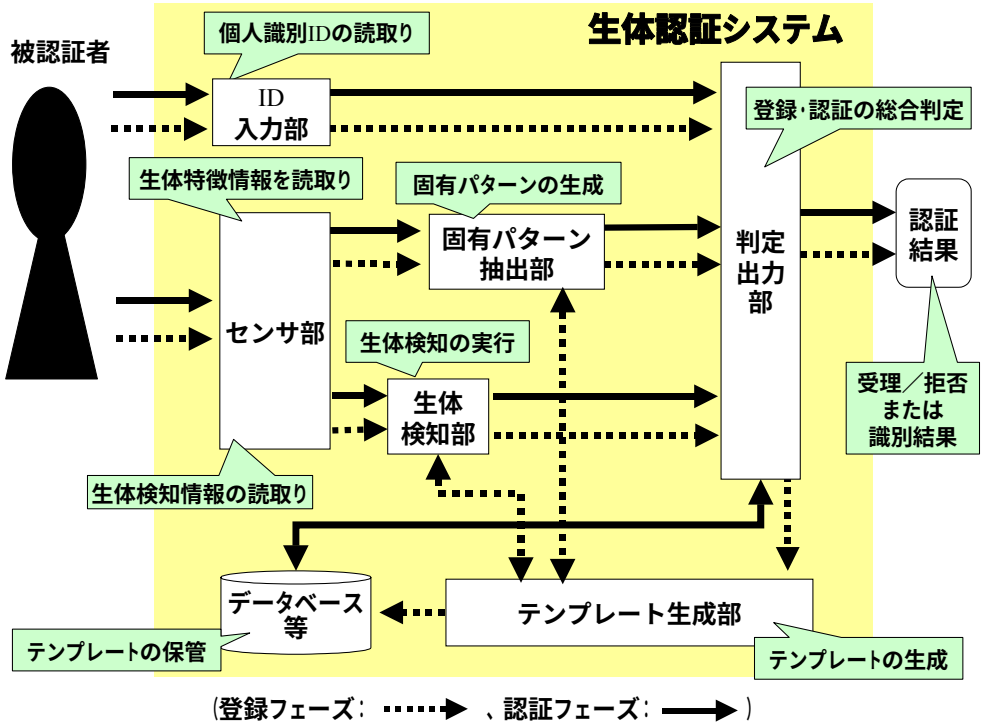
（ロ）生体を特定するレベル

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

---

[2] ここで挙げられている“ biometric data ”という用語は、一般に「生体情報」と翻訳されて広く利用されている。ただし、本稿では、後段において、生体検知を実行するために利用される情報を別途定義し、その情報と“ biometric data ”との違いを明確にする必要があることから、「生体情報」という用語ではなく、あえて「生体特徴情報」という訳語を“ biometric data ”に当てることとした。

図 1　生体認証システムの基本構成（概念図）



点から、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、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を特定して認証するケースとしては、採取した血液からその個人の血液型を特定するという場合が例として挙げられる。

ハ．生体認証システムの構成

生体検知を考慮しながら生体認証システムの構成を整理する（図 1 参照）。生体検知機能の定義については次節で検討するため、ここでは、生体検知機能の具体的な処理内容には立ち入らず、被認証物から生体検知のための情報（以下、生体検知情報＜liveness data＞と呼ぶ）を読み取って一定の処理を行う抽象的な機能として考える。生体認証システムは、センサ部、ID 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、データベース等から構成される。登録と認証はそれぞれ次の手順で実行されるものとする。ただし、生体検知が行われるタイミングについては、各生体認証システムに

よって異なり、必ずしも以下の説明の順序で行われるわけではない。

（イ）登録フェーズ

・被認証者の個人識別 ID 等を読み取る（ID 入力部）。
・被認証者から生体特徴情報を読み取り（センサ部）、生体特徴情報から固有パターンを抽出する（固有パターン抽出部）。
・被認証者から生体検知情報を読み取り（センサ部）、生体検知を実行する（生体検知部）。
・固有パターンの品質を検査し、その結果と生体検知の結果から登録の可否を判定する（判定出力部）。
・登録可能との結果が出た場合、個人識別 ID や固有パターン等からテンプレートを生成し、データベースに登録する（テンプレート生成部）。なお、テンプレートを IC カード等のトークンに格納し、テンプレートに対応する被認証者が所持するケースにおいては、データベースの部分に当該トークンが位置し、トークンにテンプレートが書き込まれる。

（ロ）認証フェーズ

・1 対 1 照合の場合、被認証者の個人識別 ID を読み取る（ID 入力部）。1 対 n 照合の場合、個人識別 ID の読取りを行わない。
・被認証者から生体特徴情報を読み取り（センサ部）、固有パターンを抽出する（固有パターン抽出部）。
・被認証者から生体検知情報を読み取り（センサ部）、生体検知を実行する（生体検知部）。その際に、テンプレートに記録されている情報を用いるケースもある。
・1 対 1 照合の場合、個人識別 ID に対応するテンプレートをデータベース等（あるいは、IC カード等のトークン）から読み出し、生体特徴情報から抽出した固有パターンと比較する。両者がどの程度一致するかを表わす値を生成し、判定しきい値と比較して一致か否かを判定するとともに、生体検知の結果を踏まえて最終的な判定結果を出力する（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、一致と判定するテンプレートが存在した場合にはその個人識別 ID も出力するケースがある。

(2) 生体認証システムにおける脆弱性

生体認証システムを採用する場合、当該アプリケーションにおける要件を満足するものを選択することが求められる。主な要件としては、一般に、セキュ

リティ、利便性、コスト、社会的受容性を挙げることができる[3]。これらの要件に優先順位をつけたうえで、要件間のバランスをとりながら生体認証システムを実装することが求められる。

セキュリティの観点から生体認証システムが一定の要件を満足しているか否かを確認するためには、各システムのセキュリティ評価を実施する必要がある。その場合、アプリケーションの環境を考慮して生体認証システムに関する脆弱性や脅威を明確にし、必要に応じて脆弱性を回避するための対策を講じることが求められる。生体認証システムにおいてどのような脆弱性が想定されるかに関しては、日立製作所[2004]において検討されており、攻撃者による第三者へのなりすましにつながるおそれのある脆弱性と、生体認証システムへのサービス妨害（denial of service）につながるおそれのある脆弱性についてそれぞれ検討されている。生体認証システムのなりすましにつながるおそれのある脆弱性に関しては 19 項目に分類されており、それらを整理すると次頁表 1 のとおりである。

なりすましにつながるおそれがある脆弱性のうち、指紋、虹彩、静脈パターンといった身体的特徴に焦点を当てると、物理的に偽造された身体的特徴を生体認証システムが誤って受け入れてしまうという脆弱性（日立製作所[2004]では「偽生体検知情報」に分類されると考えられる）に、とりわけ留意する必要があるとの指摘がある（宇根・松本 [2005]）。これは、本脆弱性がいくつかの市販の生体認証システムに存在することが示されている反面、その対策に関する研究の成果がほとんど公表されておらず、脆弱性の評価手法が確立されていないという事情による。市販のいくつかの生体認証システムにおいて脆弱性の存在を示した代表的な研究成果としては、横浜国立大学の松本教授らによる一連の研究が挙げられる[4]。松本教授らは、指紋および虹彩を用いたいくつかの照合装置が人工の指紋や虹彩を高い割合で誤って受け入れてしまうことを実験によって確認しているほか（Matsumoto *et al*. [2002]ほか）、指の静脈パターンを用いたある照合装置が生体でない物質（野菜＜ダイコン＞や人工雪材）の内部形状を高い確率で誤って静脈パターンとして読み取ってしまうことも実験によって確認している（松本ほか [2005a, b]）。こうした脆弱性に伴って発生するリスクが当該アプリケーションのリスク許容度を超える可能性があると判断される場合には、脆弱性を軽減するための対策を検討することが必要となる。

---

[3] 生体認証システムを運用していくうえでの詳細な要件は、日本工業標準調査会[2004]に記述されている。

[4] 指紋や虹彩の偽造に関する一連の研究については宇根・松本 [2005]4 節に整理されている。

表 1　日立製作所[2004]において列挙されている脆弱性

脆弱性の名称	対象	概要
他人受入	生体認証システムに特有と考えられるもの	自分の生体特徴情報を提示すると、他の個人として偶然受け入れられる。
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特徴情報を有する利用者（「狼」と呼ばれる）が存在する。
子羊		複数の生体特徴情報に対して、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」と呼ばれる）が存在する。
類似性		双子等、類似の生体特徴情報を有する人が複数存在してしまう。
偽生体情報		生体特徴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		生体特徴情報が本人の同意なく容易に他人の手にわたってしまう。
推定		テンプレートや照合結果が生体特徴情報推定の手掛かりとなる。
利用者状態		生体特徴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、品質の劣る生体特徴情報を登録し、他者になりすましされる。
入力環境		生体特徴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、品質の劣る生体特徴情報を登録し、他者になりすましされる。
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	個人認証を行う各種システムに共通するもの	本人確認が不適切であり、他者の生体特徴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		生体特徴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特徴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		生体特徴情報を読み取るセンサは外部に露出しており、生体特徴情報の入手、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。

資料：日立製作所[2004]

(3) 身体的特徴の偽造への対策

イ．3 つの対策

身体的特徴の偽造への対策に関しては、既存のいくつかの文献において言及されている。英国政府傘下のバイオメトリック・ワーキング・グループ（Biometric Working Group）の報告書（BWG [2003]）においては、生体認証システム自体の技術的な対策として、生体検知機能の生体認証システムへの組込みとマルチモーダル（multimodal）認証の採用が挙げられているほか、運用上の対策として人間による登録・認証プロセスの監視（supervision）が挙げられている。米国の金融業界における生体認証技術に関する国内標準 ANS X9.84 の Annex E においては、主な対策として生体検知機能の組込みと人間による登録・認証プロセスの監視が挙げられている（ANSI [2003]）。また、瀬戸 [2003] においても、主な対策として生体検知機能とマルチモーダル認証の採用が挙げられているほか、Schuckers [2002]においては、生体検知機能の組込み、マルチ

モーダル認証の採用、人間による登録・認証プロセスの監視のほか、1 種類の身体的特徴を複数用意してそれらの中からいくつかを選択して認証に利用するという手法[5]が挙げられている。Prabhakar, Pankanti and Jail [2003]においては、生体検知機能とマルチモーダル認証が挙げられている。

これらの文献に取り上げられている対策を整理すると、生体検知機能の組込み、マルチモーダル認証の採用、人間による登録・認証プロセスの監視、1 種類の身体的特徴を複数利用するという手法の 4 つにまとめられる。ただし、1 種類の身体的特徴を複数利用する手法に関しては、採用されている身体的特徴が容易に偽造可能になってしまう可能性もある。仮に、そうしたことが起きたという状況を想定すると、登録の対象となっている複数の特徴すべてが偽造される可能性があり、その結果、本対策の有効性は大きく損なわれると考えられる。こうしたことから、以下では、対策の効果という点で相対的に有効と考えられる生体検知機能、マルチモーダル認証、人間による登録・認証プロセスの監視に絞って考察する。

ロ．各対策の特徴と検討状況

（イ）生体検知機能

生体検知機能の定義については 3 節で詳しく議論するが、ここでは、センサによって読み取られた生体特徴情報が人間から読み取られたものか否かを確認するという機能を意味すると考える。

セキュリティの観点からみると、生体検知機能を生体認証システムに適用した場合、当該システムにおいて第三者へのなりすましを試みる攻撃者は身体的特徴だけでなく生体検知情報もなんらかの形で提示することが必要になると考えられるため、なりすましが成功する可能性は生体検知機能を適用しない場合以下になると期待される。ただし、これまでに多種多様な生体検知機能の実現方式が提案されている（詳細は 3、4 節において述べる）ものの、生体検知機能の有効性について各種実現方式の提案者以外の第三者による評価結果が公表されている事例は、筆者らが知る限り非常に少ない。また、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生体検知の手法が採用されているか（あるいは、採用されていないか）に関しても、公開されていないケースが多いようである（IBG [2003]、Sandström [2004]）。

生体検知機能を実装する際に留意すべき事項を指摘する文献も、筆者らが知る限り非常に少ない。数少ない文献として、バイオメトリクス・ワーキン

---

5 例えば、両手 10 本の指からそれぞれ指紋を生体認証システムに登録し、照合の際には、いずれかの指を指定してその指の指紋を提示させるといった手法が挙げられる。

グ・グループの報告書（BWG [2003]）と Valencia and Horn [2003]が挙げられる。これらの文献においては、生体特徴情報の読取りと同一のタイミングで同一の部位から生体検知情報の読取りを行うことが必要であるといった指摘がなされている。こうした状況が満足されていない場合、攻撃者は生体特徴情報を人工物によって提示するとともに、自分の生体検知情報を提示するというタイプの攻撃が可能になると考えられる。もっとも、こうした指摘を踏まえたセキュリティ評価に関する検討結果は、筆者の知る限り発表されていないようである。

生体検知機能を生体認証システムに組み込む際のコストや利便性について考えると、採用する方式によっては生体検知用のセンサを追加的に設置したり、照合アルゴリズムを変更したりする手間やコストが必要になると予想される。また、通常の生体認証に加えて生体検知の処理も実行するために照合・判定に一定の時間が必要となり、認証処理時間が増加した結果、生体認証システムの利便性が低下する可能性がある。

（ロ）マルチモーダル認証

マルチモーダル認証は、複数の身体的特徴等を組み合わせ、それらの照合結果を総合して本人か否かを判定するという認証の手法である[6]。マルチモーダル認証を採用した場合には、当該システムにおいてなりすましを試みる攻撃者は異なる複数の特徴を偽造しなければならない。このため、なりすましが成功する可能性は単一の特徴を用いる認証方式（ユニモーダル認証と呼ばれる[7]）以下になると期待される。ただし、マルチモーダル認証における誤受入率（false accept rate）や誤拒否率（false reject rate）等の認証精度がユニモーダル認証に比べてどの程度向上するかに関しては、既に数多くの研究結果が発表されているものの、なりすましへの耐性がどの程度向上するのかに関する検討結果は筆者等が知る限り発表されていないようである。

ユニモーダル認証からマルチモーダル認証へ移行する場合のコストや利便性への影響に関しては、生体検知機能の組込みと同様の状況が発生すると考えられる。まず、複数の特徴を読み取るためにセンサを追加的に設置する必要があるケースが多いと考えられる。さらに、認証処理も複数の特徴に関して実行することになり、認証処理時間が増加する可能性が考えられる。

---

[6] マルチモーダル認証に関しては、瀬戸 [2002]3 章や Hong and Jain [1999]において詳細に述べられている。

[7] ユニモーダル認証という用語は、生体認証の種類を議論する際に、マルチモーダル認証と対比する形で用いられるケースがある（Hong and Jain [1999]）。

（ハ）人間による登録・認証プロセスの監視

運用上の対策として挙げられている人間による登録・認証プロセスの監視は、身体的特徴がそれを有する人間によって生体認証システムに提示されているか否かを、別の人間が自分の目で確認するというものである。また、ビデオ等によって登録・認証プロセスを録画しておき、何か問題が発生した場合には後日人間が確認できるようにする仕組みも、本対策に含まれる。

本手法を採用する場合、上質紙で作製した人工の虹彩やグミ製の人工指を用いた攻撃等、人間の目でみて明らかに不正行為であると判断できる攻撃については比較的容易に検知可能であり、高い効果を期待することができると考えられる。ただし、人間の目では不正行為をみつけることが困難なケースも想定される。例えば、指紋を利用した生体認証システムにおいて、指紋付きの薄膜を指に装着してセンサに指を置くといった攻撃（Sandström [2004]）が実行された場合には、監視人が近距離から目視によって攻撃者の行動をチェックしていたとしても攻撃を検知できない場合も考えられる。

人間による監視を採用する場合のコストや利便性への影響については、センサの追加等の生体認証システムにおける技術仕様の変更には直接結びつかないと考えられるものの、被認証者による認証プロセスの監視を行う人員を配置するためのコストを新たに負担することが必要となる。その結果、自動化された生体認証システムの導入に伴うコスト削減のメリットが監視のための人員配置によって損なわれてしまう可能性がある。ただし、認証プロセスは通常の生体認証のプロセスのみで実行可能であり、認証処理時間の増加にはつながりにくいケースが多いとみられる。

ハ．考察のまとめ

セキュリティの観点では、いずれの対策においても、身体的特徴の偽造に対する耐性をどの程度向上させることができるかに関する分析結果がほとんど公表されていないのが実情である。このため、生体認証システムの運営者や利用者が、どのような対策を選択すればよいかについて客観的な情報に基づいて判断を下すことが事実上困難な状況にあるとみられる。今後、セキュリティの観点から各対策がどのような効果を有しているかに関する研究を進めていくことが重要である。

コストや利便性の観点では、いずれの対策を適用しても生体認証システムにとっては別の処理を追加することになり、コストの増加や利便性の低下につながることとなる。ただし、こうした影響の度合いや形態は対策によって変わってくると考えられる。生体検知機能やマルチモーダル認証に関しては、これらを実現するためのセンサやソフトウエア等を生体認証システムに適宜組み込

むことが必要であり、そうした組込みに伴ってコストや利便性にどのような影響が及ぶかについて評価する必要がある。一方、人間による監視に関しては、生体認証システムにおける自動処理自体に及ぼす影響は少ないものの、監視のための人員配置に伴うコストや利便性への影響について考慮することが必要となる。どの対策がコストや利便性の観点から望ましいかは個々のアプリケーションに依存することになるが、機械の自動処理によって効率的な個人認証を実現することが生体認証システムの主たる特長であることを考慮すると、そうした特長を活かすという観点から、生体検知機能やマルチモーダル認証を選択するケースが現実には多くなるのではないかと考えられる。

こうした考察を踏まえると、身体的特徴の偽造への主たる対策の中でまず検討することが有用と考えられるのは、生体検知機能とマルチモーダル認証であるいえる。本稿では、これらのうち、オープンな場における検討や議論が相対的に遅れていると考えられる生体検知機能に焦点を当てることとする。

3．生体検知機能に関する概念整理と分類

(1) 概念整理

イ．2 つの確認項目

2 節の冒頭において、生体認証技術を、身体的特徴や行動的特徴を利用して個人を自動的に認証する技術であると定義した。これに基づき、生体認証技術においてどのような事項の確認が必要かについて生体検知機能を意識しつつ考えると、次の 2 項目の確認が必要であると考えられる（次頁図 2 参照）。

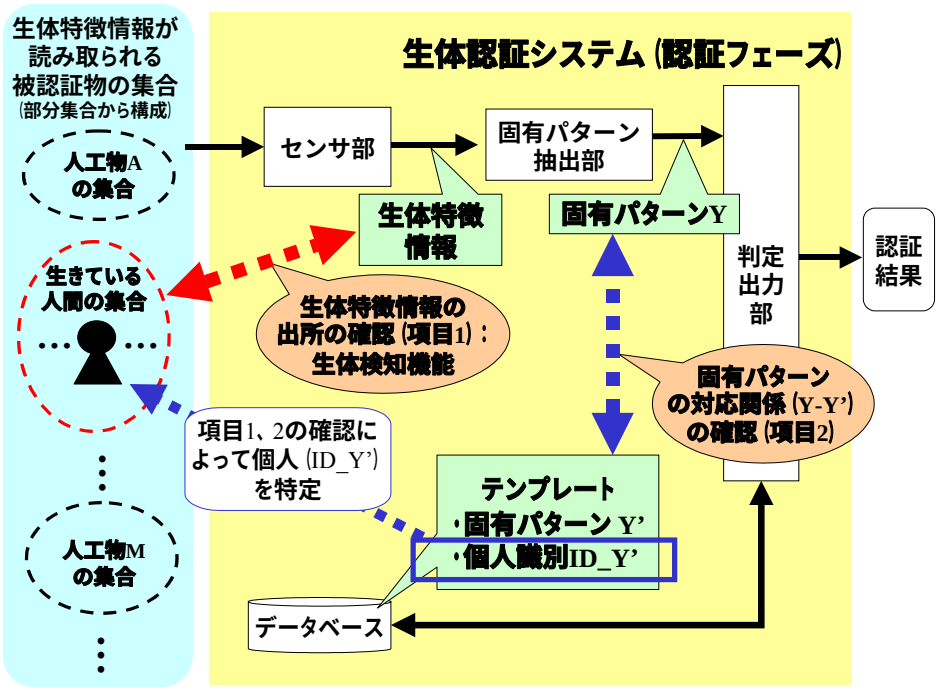
> 【項目 1】生体特徴情報が生きている人間から読み取られたものか否か
>
> 【項目 2】生体特徴情報から抽出される固有パターンが、特定のテンプレートの固有パターンと一致するか否か

項目 1 の確認は、生体特徴情報を読み取った被認証物が「生きている人間」という集合に属しているか否かを明らかにするものである。生体特徴情報は、生きている人間からだけではなく、人工物等から生体認証システムによって読み取られる可能性がある。このため、生体特徴情報が読み取られる可能性がある被認証物の集合のうち、生きている人間という部分集合から生体特徴情報が読み取られたことを確認することが求められる。

項目 2 の確認は、生体特徴情報から抽出された固有パターンに対応する個人識別 ID を特定するものである。仮に、本確認を実行する前に、項目 1 の確認によって生きている人間から生体特徴情報が読み取られたと判定されていた場合、項目 2 の確認によって、生きている人間という部分集合の中で、当該固有パターンを有する個人を特定することが可能となる。これに対して、仮に項目 1 が確認できていない場合には、当該固有パターンを有する被認証物が生きている人間なのか、それとも人工物なのかが不明確なままとなり、生体特徴情報が偽造されて提示されたものである可能性を否定することができない。こうした可能性は、人工指や人工虹彩を一部の市販の照合装置が受け入れてしまうという実験結果によっても示唆されている。また、1 対 1 照合だけでなく、1 対 n 照合の場合においても同様の問題が発生しうる。

項目 1、2 のうち、生体検知機能は項目 1 をカバーするものと位置づけることができる。この場合、生体検知機能は生体認証システムにとって必須の機能と考えられる。従来の生体認証システムの中には、「生体検知機能が搭載され

図 2　生体認証システムにおける 2 つの確認項目の関係



たシステム」といった表現に代表されるように、生体認証システムのオプション的な機能として生体検知機能を位置づけるような表現が用いられるケースが少なくない。生体検知機能がシステムに明示的に搭載されていない場合においては、「生体特徴情報が生きた人間に固有のものであり、人工物等を用いて生体特徴情報を偽造することが困難である」という期待に基づき、生きた人間から読み取られたことを別の手段で追加的に確認する必要がないと考えられているものと思われる。

ロ．先行文献における生体検知機能の位置づけと定義

生体検知機能について触れている代表的な文献を参照し、生体検知機能がどのように位置づけられているかを調べる。生体認証技術に関連する主な文献から、生体検知機能についての記述を抜き出してみると以下のとおりである。

・Valencia and Horn [2003]の p. 139

「生体検知テストは、生体認証システムに提示される生体特徴情報のサンプルが、登録時に生体特徴情報を提示した（生きている）人間から読み取られたものか否かを自動的に確認するためのテストである。」

・BWG [2003]の p. 7

「この機能（生体検知機能）は、生きている人間によって提示される生体特徴情報と人工物によって提示される生体特徴情報とを判別するシステムの能力を指す。」

・瀬戸 [2003]の 166 頁

「指紋認証を行う際に、指が生きている人間の指なのか否かを検知する生体検知技術に関する研究がある。」

・Sandström [2004]の p. 35

「生体認証システムにおける生体検知は、登録・認証時において、提示された生体特徴情報のサンプルが生体のものか否かを検知するシステムの能力を意味する。」

・Schuckers [2002]の p. 60

「生体検知テストの目的は、読み取った生体特徴情報が当該生体特徴情報に対応する（生きている）人間から実際に計測されたものであり、その人間が生体特徴情報の読取時にその場に存在していたことを確認するというものである。」

以上のように、生体検知機能の捉え方は文献によってまちまちであるものの、基本的には項目 1 を対象としている点で共通しており、項目 1 をカバーする機能として生体検知機能を位置づけるという考え方と整合的であるといえる。なお、Valencia and Horn [2003]は、「登録時に生体特徴情報を提示した人間」から読み取られたことを確認する機能（すなわち、項目 2）も生体検知機能に含める考え方を採用している。ただし、項目 2 は、生体検知機能の有無にかかわらず生体認証システムの基本的な機能として議論されることが多いため、ここでは生体検知機能に含めない扱いとする。

以上の整理を踏まえて、本稿では生体検知機能を次のように定義する。

【生体検知機能】 生体認証システムにおいて、生体特徴情報の登録・照合時に読み取られた生体特徴情報が、生きている人間から読み取られたものか否かを自動的に確認する機能

ここでは、生体認証システムは自動化されたシステムであることから、生体検知機能も機械によって自動的に処理されることを想定している。

(2) 生体検知機能の要件

イ．セキュリティの観点からの要件

（イ）想定する脅威

生体検知機能がその役割を発揮するためにはどのような条件が満足される必要があるかについて検討する。セキュリティの観点から要件を導出するためには、どのような脅威や脆弱性が想定されるかをまず明らかにする必要がある。脅威や脆弱性は個々のアプリケーションに依存する部分も大きい。ここでは具体的なアプリケーションを想定しないで検討を進めていることから、いずれのアプリケーションにおいても共通に想定される代表的な脅威を取り上げて検討することとする。そうした脅威として次のものに焦点を当てる。

【想定する脅威】攻撃者が、生体特徴情報を偽造して提示するとともに、自分の生体検知情報を提示する、または、生体検知情報を偽造して提示することによって、第三者へのなりすましを試みる。

生体認証システムに対する脅威としてなりすましを指摘している文献は多く、同様の脅威は生体検知機能の利用を検討するうえで当然視野にいれておく必要があると考えられる。

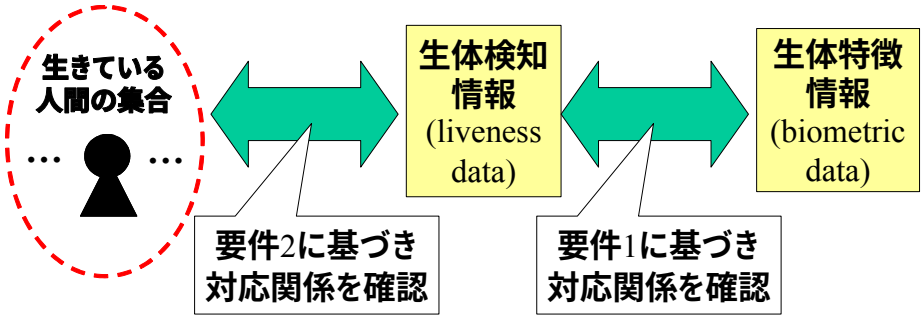
（ロ）2 つの要件

なりすましの脅威について検討する場合、次のような留意点が挙げられる。まず、攻撃者は通常生きている人間であり、生体検知情報を自分の体から読取可能であるため、「生体検知機能において生きている人間として判定されるような生体検知情報を攻撃者は容易に入手することができる」という状況を前提として検討することが求められる。こうした状況における検討のポイントとして、次の 2 点を挙げることができる。

① 生体検知情報と生体特徴情報が同一の被認証物から読み取られたことを確認可能か否か
② 人工物等から読み取られた生体検知情報が「生きている人間から読み取られたものではない」と正しく判定されるか

上記①に着目すると、生体検知情報と生体特徴情報が読み取られた被認証物が同一であることを確認困難なシステム設計となっている場合（例えば、生体検知情報を提示して生体検知が行われた後に生体特徴情報を提示する場合）、

図 3　2 つの要件によって確認されること



攻撃者は自分の生体検知情報を生体特徴情報とは別に提示して生体検知をクリアするという攻撃が適用可能になると考えられる。このため、生体検知機能のみに注目することにはあまり意味がなく、生体特徴情報の読取方法や、生体検知情報と生体特徴情報の対応関係も考慮した検討が必要であるといえる。

また、生体検知情報と生体特徴情報が同一の被認証物から読み取られたことを確認可能なシステム設計となっている場合には、攻撃者が生体特徴情報を人工物等によって提示するとすれば、攻撃者は当該人工物によって生体検知情報を提示することが必要になると考えられる。したがって、「生きている人間が提示した」と誤って判定してしまうような生体検知情報を、人工物等を通じて提示することができるか否かが重要なファクターとなってくる。これは上記②に対応する。

以上の点を踏まえると、第三者へのなりすましを想定した場合のセキュリティ上の主な要件を次の 2 つに整理することができる（図 3 参照）。

【要件 1】生体検知情報と生体特徴情報がそれぞれ読み取られた被認証物が同一か否かを確認可能であること

【要件 2】生体検知情報が生きている人間から読み取られたか否かを確認可能であること

いずれの要件においても、生体検知情報や生体特徴情報等のアナログ情報に基づいて確認が行われることから、これらの読取情報に含まれる誤差等によって、「被認証物が同一か否か」あるいは「生きている人間から読み取られたか否か」を反映する指標は読取りの都度変化する。こうした指標が個別のアプリケーションにおいて求められる判定しきい値以上となる場合に、実際に「確認できた」と判断されることになる。

ロ．セキュリティ以外の要件

セキュリティ以外の主な要件としては、利便性、コスト、社会的受容性を挙げることができる。

利便性の要件としては、認証処理時間、被認証者に要求する動作、認証精度のレベルといった項目が考えられる[8]。2 節（3）**ロ**.、**ハ**. においても説明したように、生体検知機能の搭載は利便性の低下をもたらすことも多いと思われる。具体的には、認証処理時間が長くなる、生体検知情報を読み取るための追加的な動作（あるいは静止）を被認証者に要求するといった状況が想定される。さらに、生体検知情報において誤った判定を下す可能性があるため、正しい本人であるにもかかわらずシステムを利用できなくなる可能性は、生体検知機能を搭載しない場合に比べて高まるケースも考えられる。こうした点を踏まえ、生体検知機能の搭載後の状況を勘案し、利便性が低下する程度について確認を行うことが求められる。

コストの要件としては、生体検知機能搭載にあたって必要となるハードウエアやソフトウエアの調達費用、運用・管理費用、メンテナンス費用が考えられる。コストに関しても、利便性と同様、生体検知機能の搭載はコスト増加要因となる。例えば、生体検知情報読取用のセンサの追加、ソフトウエアの購入・更新といった状況が想定される。

社会的受容性の要件として、まず、生体検知機能導入による心理的・肉体的な負荷が許容されるレベルにあることが挙げられる。生体検知は、生体検知情報を読み取る際に被認証物になんらかの刺激を与え、その刺激への反応を測定することによって実行されるというケースが多い。生体検知情報を読み取るために与えられる刺激は多かれ少なかれ心理的・肉体的な負荷となるため、刺激がなるべく少ないことが望ましいが、その場合には刺激への反応が小さくなるというトレード・オフが存在する（橋本 [2000]）。こうしたことから、身体や健康への影響や刺激による心理的な負担について評価し、どの程度の刺激であれば許容されるか、また、心理的な抵抗感が許容されるレベルにあるかといった点についても明確にしておく必要がある。

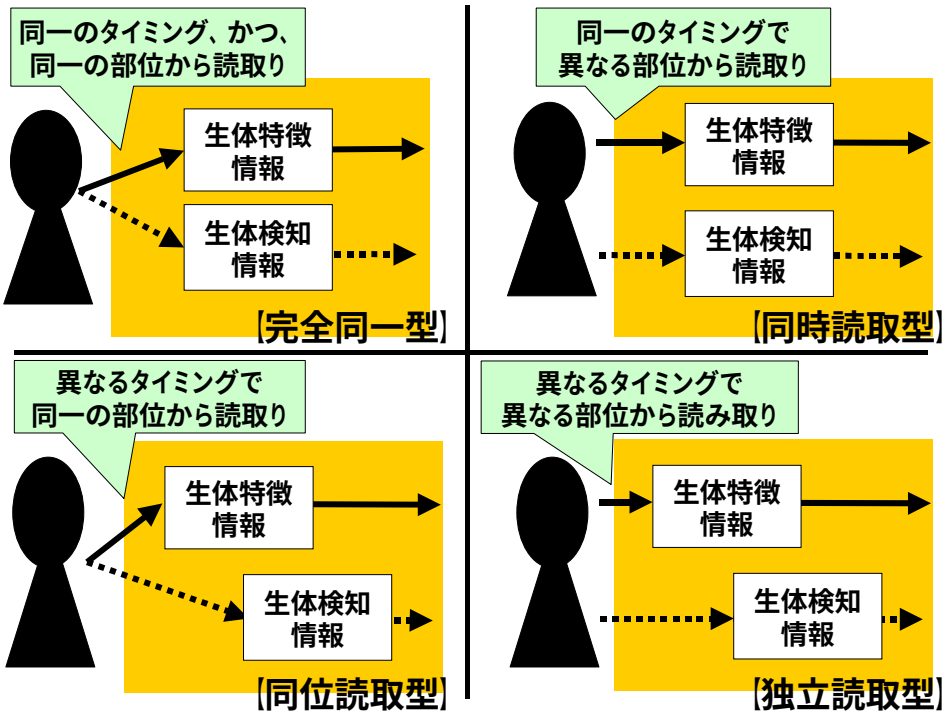
(3) 生体検知機能に着目した生体認証システムの分類

生体認証システムを生体検知機能の観点から分類することの意義は、カテゴリーごとの特徴を抽出し、異なるカテゴリーに属するシステム間の比較を行うための手掛かりを提供することにある。ここでは、なりすましに対するセキュ

---

[8] これらの要件は、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、日本工業標準調査会[2004]）において機能要件として整理されている。

図 4　生体検知情報の読取形態による生体認証システムの分類



備考：実線矢印と点線矢印はそれぞれ生体特徴情報、生体検知情報の流れを示す。

リティ・レベルという観点から生体認証システムのセキュリティを議論していることから、本節（2）**イ**．で示した要件 1、2 の満足度に影響を与えるのはどのような事項かに力点を置いて生体認証システムの分類法を検討する。

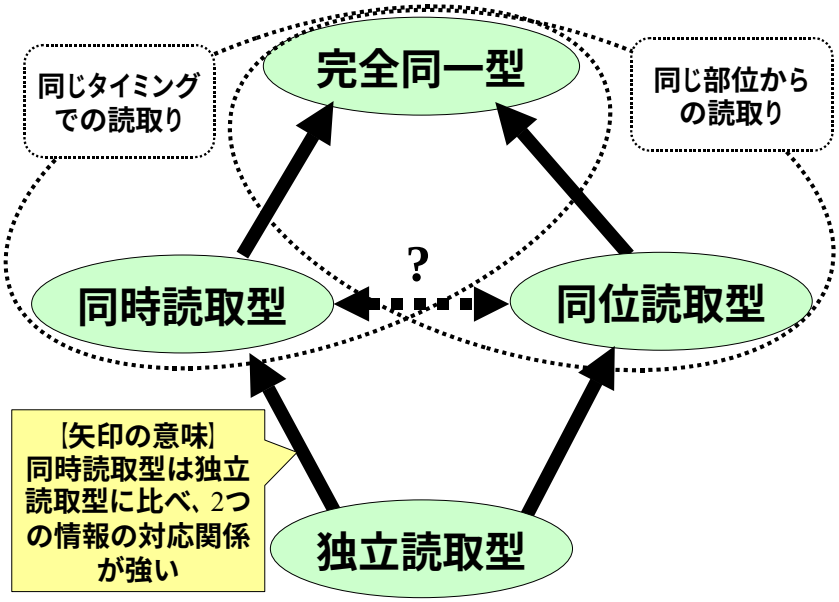
イ．2 つの要件に着目した分類法

（イ）要件 1 に着目した分類

要件 1（生体検知情報と生体特徴情報がそれぞれ読み取られた被認証物が同一か否かを確認可能であること）の達成度合いを左右する要素として、生体検知情報と生体特徴情報がどのような形態で読み取られるかという点が挙げられる。これらの情報の読取形態に着目すると、生体認証システムを次の 4 つに分類することができる（図 4 参照）。

・**完全同一型**：生体検知情報と生体特徴情報が、同一のタイミングで同一の部位から読み取られる生体認証システムの集合。ここでは、同一のタイミングとは、2 つの情報の読取期間（情報の読取りが開始されてから終了するまでの時間的間隔）が全部または一部重なっている状況を意味するものとする。また、同一の部位から情報を読み取るといった場合、2 つの情報

図 5　4 つの分類間の関係



の読取部位が全部または一部重なり合っているという状況を意味するものとする。例えば、発汗に伴う指紋画像の変化から生体検知情報を読み取り、その変化する指紋画像の一部を生体特徴情報（指紋）として用いるシステムが本分類に属すると考えられる。

- **同時読取型**：生体検知情報と生体特徴情報が、同一のタイミングで異なる部位から読み取られるというシステムの集合。例えば、虹彩と瞳孔を同時に 1 つの目画像として読み取り（虹彩の部分と瞳孔の部分は重なっていない）、虹彩の部分から生体特徴情報を、瞳孔の部分から生体検知情報をそれぞれ読み取るシステムが本分類に属すると考えられる。
- **同位読取型**：生体検知情報と生体特徴情報が、異なるタイミングで同一の部位から読み取られるシステムの集合。
- **独立読取型**：生体検知情報と生体特徴情報が、異なるタイミングで異なる部位から読み取られるシステムの集合。

これらを生体検知情報と生体特徴情報の対応関係という観点で比較すると（図 5 参照）、生体認証システムに関するその他の条件が同一であるならば、同じタイミングで、あるいは、同じ部位から読み取られる場合の方が、異なるタイミングで異なる部位から読み取られる場合に比べて、2 つの情報の対応関係は強いと考えられる。こうした点を考慮すると、生体検知情報と生体特徴情報の対応関係が最も強くなるものは完全同一型であり、相対的に最も弱くなる

ものは独立読取型であるといえる[9]。また、同時読取型と同位読取型に関しては、完全同一型と独立読取型の中間に位置することになると考えられる。ただし、同時読取型と同位読取型のどちらにおいて 2 つの情報の対応関係がより強いかは一概に判断することができない。

上記 4 つの分類間の関係をそのまま要件 1 の満足度合いとして読み換えることもできると考えられる。すなわち、2 つの情報の対応関係が相対的に強い方が、本節(2)で想定した脅威に対する安全性も相対的に高いと考えることができる。

このように、情報の読取形態による分類を行う際には、生体検知情報に加え、生体特徴情報がどのように読み取られるかに関しても考慮する必要がある。

（ロ）要件 2 に着目した分類

要件 2（生体検知情報が生きている人間から読み取られたか否かを確認可能であること）の達成度合いは、採用の候補となっている生体検知情報の種類、生体検知のアルゴリズム、判定しきい値等のパラメータに依存することになる。現時点では、生体検知情報が読み取られた被認証物が生きている人間であるか否かを判定する精度をどのように評価するかについて、筆者らが知る限り、検討結果は公表されていないのが実情のようである。こうしたことから、要件 2 の満足度合いを評価することは現時点では困難であり、本稿における分類の観点として要件 2 を直接利用することも難しいと考えられる。

ただし、生体検知情報の偽造の観点からみると、生体検知情報の読取時に攻撃者が検証に成功する生体検知情報を提示することが容易か否かという点で分類することが考えられる。この点について考察を深めるために、生体検知情報がどのようなプロセスで一般に読み取られるかについて整理する。

生体検知情報の読取りのプロセスは、まず被認証物に対してなんらかの働きかけ（刺激）を行い、その刺激に反応して被認証物から発せられる生体検知情報を検出することによって行われると一般に整理することができる。また、刺激に応じて被認証物や読取部位が状態変化を起こす場合と、起こさない場合が考えられる。例えば、指の血管における脈波を赤外光の透過光によって測定して生体検知を行う場合、刺激は照射される赤外光、読取対象は脈波、生体検知情報は透過光の光量とその時系列変化を示すアナログ情報にそれぞれ対応すると考えられる。この例は、刺激による読取部位の状態変化がほとんどないケースに対応する。目に照射される可視光の強弱による瞳孔の収縮・拡張を赤

[9] ただし、独立読取型においては、ある特定の生体特徴情報を利用する際に、読取部位やタイミングの観点で生体検知情報の選択の範囲が相対的に大きいという利点がある。

表 2　刺激の目的とその例

分類	刺激を利用した例
自発的に発信される情報を強めるため、または自発的なもの以外の情報を得るための刺激	・ 光を当てて、微細な形態を観察（光学顕微鏡） ・ たんぱく質の特異反応を利用して､特定の物質やその位置を追跡（免疫蛍光法） ・ 微小電流を流して、電気抵抗を測定 ・ 磁場を与えて、イオンの流れを測定（電磁流量計） ・ 撮影用の物質を注入して、位置を追跡
被認証物の状態を変化させるための刺激	・ 電流を流して、筋収縮の反射を測定 ・ 光を当てて、眼の虹彩の収縮・拡張（瞳孔反射）を計測 ・ 運動したときの心電図（負荷心電図） ・ 負荷を与えたときの筋電図（誘発筋電図）

資料：橋本[2000]

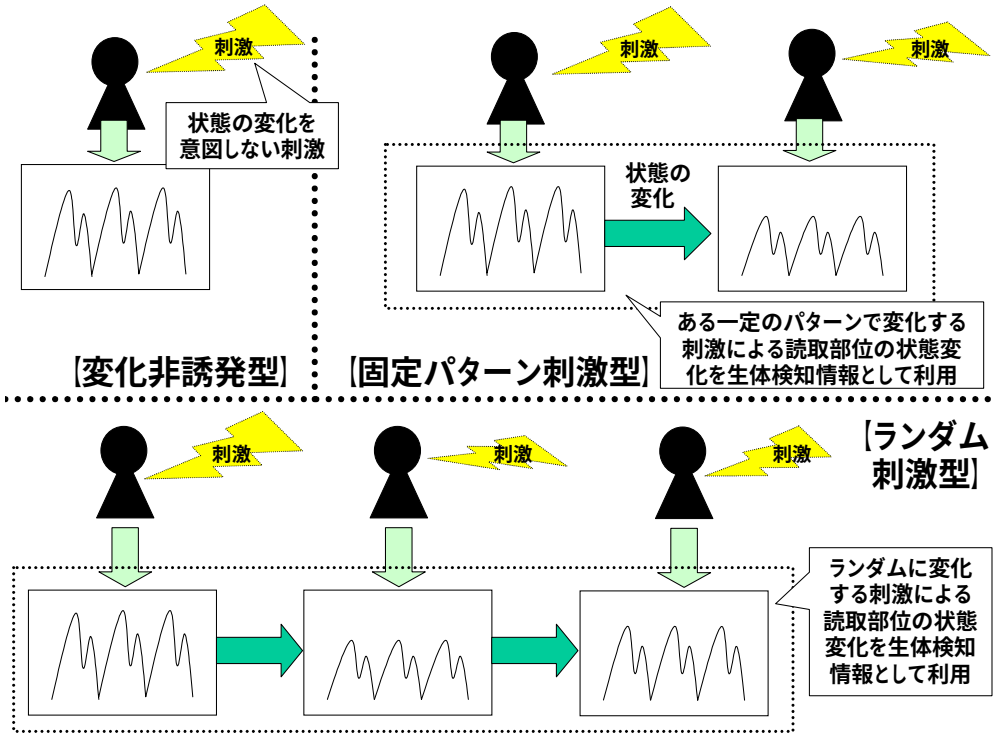
外光等によって観察して生体検知を行う場合､刺激は照射される可視光と赤外光、読取対象は瞳孔の収縮・拡張、生体検知情報は赤外光の反射光の光量とその時系列変化を示すアナログ情報にそれぞれ対応すると考えられる。この例は､刺激の強弱によって読取部位の状態が変化するケースに対応する。

生体検知情報を読み取るための刺激については､橋本 [2000]では､①自発的に発信される情報を強めるため､または自発的なもの以外の情報を得るための刺激と､②被認証物の状態を変化させるための刺激に分類されている（表 2 参照)。上記①の刺激を利用する生体認証システムでは被認証物の状態変化を誘発する意図がないのに対して､上記②の刺激を利用するシステムでは読取部位の状態変化を誘発する意図があり､その状態変化を測定して生体検知を行うものである。これらの刺激に基づいて読み取られる生体検知情報の偽造の困難さを比較すると、他の条件が一定であるとするならば､上記②のような状態変化が発生する場合は､上記①のような状態変化が伴わない場合に比べて､相対的に偽造が困難になると考えられる。このように考えると、上記①、②の刺激の形態によって生体認証システムを分類することは､生体検知情報の偽造困難性という観点から評価を行ううえで有用であると考えられる。

さらに､上記②の刺激を利用するシステムでは､刺激そのものを実行ごとに変化させるか否かによって分類をさらに細分化することができる。すなわち､刺激をランダムに変化させ､読取部位の状態もランダムに変化するか否かを測定するシステムと、刺激を変化させはするが、その変化はランダムではなく、毎回同一のパターンであるシステムとに分けることが考えられる。

以上より、読取部位に与える刺激の形態という観点から、生体認証システムを次の 3 つに分類することができる（次頁図 6 参照)。

図 6　読取部位に与える刺激の形態による生体認証システムの分類

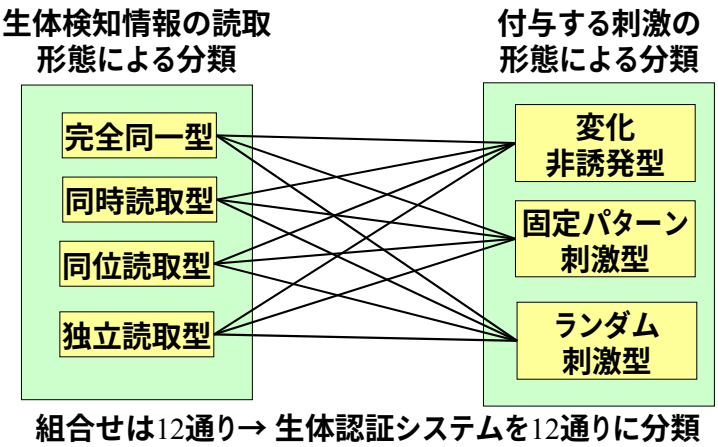


- **変化非誘発型**：読取部位の状態変化の誘発を意図しない刺激を与え、読み取られた情報を生体検知情報とする生体認証システムの集合。
- **固定パターン刺激型**：読取部位の状態変化を誘発する刺激を毎回同じパターンで与え、その変化を測定し、生体検知情報として利用するシステムの集合。
- **ランダム刺激型**：読取部位の状態変化を誘発する刺激をランダムに与え、その変化を測定し、生体検知情報として利用するシステムの集合。

上記の分類に従う場合、一般に、変化非誘発型、固定パターン型、ランダム刺激型の順でなりすましを成功させるためのハードルが高くなると予想される。読取部位の状態変化の誘発を意図した刺激が与えられる場合、攻撃者はそうした状態変化を意図的に再現する必要があり、状態変化の誘発を意図しない刺激が与えられる場合に比べて、検証を成功させる生体検知情報を提示することは相対的に困難になると考えられる。また、状態変化のパターンが固定されている場合とランダムに決定される場合を比較すると、パターンに応じた反応を意図的に発生させることは後者の場合の方が難しいと考えられる。

例えば、体温を利用する生体認証システムの場合、体温変化の誘発を意図しないで測定するケースが想定されるほか、体温変化を引き起こす発熱機能を備

図 7　本稿で採用する生体認証システムの分類法



えた装置を利用して体温の変化のパターンを測定するケースも想定される。したがって、体温を利用する生体認証システムは、変化非誘発型、固定パターン刺激型、ランダム刺激型のいずれにも属する可能性があると考えられる。また、光の強度変化に伴う瞳孔の拡張・収縮を読取対象として利用する生体認証システムにおいては、常に同じ強さの光を同じパターンで発生させる場合は固定パターン刺激型に属するが、光の強さやパターンを毎回ランダムに変化させる場合はランダム刺激型に属する。

ロ．本稿における生体認証システムの分類法

以上の検討を踏まえ、本稿では、要件 1、2 に基づく分類法を採用し、12 通り（＝4 通り×3 通り）に分類して検討することとする（図 7 参照）[10]。特に要件 1 に基づいて分類を行う際には、生体検知情報だけでなく、生体特徴情報と生体検知情報との関連づけがどのように行われているかに着目し、生体認証システムとして分類することが必要である。

生体検知機能を搭載した生体認証システムをセキュリティの観点から評価するうえで、本節において示した分類法をどのように活用することができるかについて説明する。今回の分類法では、生体検知情報の読取形態と刺激の形態

[10] 生体検知機能の実現方式の分類法については、Schuckers [2002]と Valencia and Horn [2003]において既に議論されている。ただし、いずれの分類においても、生体認証システムを対象としているわけではなく、生体特徴情報としてどのようなものを採用するか、あるいは、生体特徴情報と生体検知情報がどのように対応づけされるかが明示されていない。このため、本稿ではこれらの分類を採用しないこととする。

という生体認証システムの一部に焦点を当てて分類するというものであり、生体認証システムをあらゆる角度から検討したというわけではない。したがって、分類間の関係を、実際の生体認証システムにおける安全性の比較にそのまま適用することは適切でない。あえて比較を行うとすれば、生体検知情報の読取形態や刺激の形態以外の設定やパラメータが同一であるという状況を想定することが必要であろう。

こうした点を踏まえると、本分類法を活用する主な場面として次の 2 つを挙げることができる。

第 1 に、生体認証システムのユーザが本分類法を利用する場面が考えられる。例えば、ユーザが生体認証システムの導入を検討しており、候補となっているシステムには実装形態にいくつかのバリエーションが存在し、その中から自分の要件に見合ったものを選択する場合を想定する。ユーザが、「仮に、生体特徴情報の読取対象が将来物理的に偽造されるおそれが生じたとしても、その偽造を検知・排除できるようにしておきたい」というセキュリティ要件を設定したとする。生体特徴情報の読取対象が検知困難なかたちで偽造されたとすると、独立読取型の場合には攻撃者によるなりすましを許してしまう可能性が他の分類に比べて相対的に高いと考えられることから、独立読取型は採用しないという意思決定を行い、同時読取型、同位読取型、完全同一型を利用することが相対的に望ましいと判断することができる。こうしてシステムの形態を絞り込み、他の要件の満足度合いを勘案して、最終的にどのようなシステムを導入するかを決定することができると考えられる。

第 2 に、生体認証システムの設計者が本分類法を利用する場面が考えられる。例えば、特定の生体特徴情報と生体検知情報を採用した既存の生体認証システムを改良する、あるいは、それをベースに新たなシステムの設計を行う際に、当該システムのセキュリティ・レベルを相対的に高めたいというニーズが出てきたとする。このとき、既存のシステムが独立読取型で変化非誘発型であり、生体特徴情報と生体検知情報の読取形態や付与される刺激の形態を変更することが可能であれば、そのシステムを完全同一型、同時読取型、同位読取型に属するように、あるいは、固定パターン刺激型やランダム刺激型に属するように仕様を変更するというアイデアを本分類法から得ることができる。

4. 生体検知機能の実現方式

本節では、生体検知機能をどのように実現するかについて代表的な手法をいくつか例として紹介する。3 節において説明したように、セキュリティの観点から生体検知機能を議論する際には、生体検知機能が生体認証システムの中でどのように利用されているかを確認する必要がある。そこで、生体検知機能の代表的な手法を紹介するほか、生体検知機能を搭載した生体認証システムの事例についても特許情報を参照しながら紹介する。

以下の説明では、各生体検知機能の実現方式や生体認証システムの例として、特許情報に記載されているものをいくつか取り上げて説明している。こうした方式は、いわば一種の技術提案であり、実現可能性に関して第三者による検証を経たものでない可能性は否定できない。また、実際に、各方式の実現可能性について検討された結果も、筆者が知る限り公表されていないようである。ただし、仮に実現可能性が低い方式であったとしても、今後の技術進歩によって実現可能性が高まり、有用な方式として利用されるようになる可能性もあると考えられる。

(1) 生体検知情報とその読取対象

イ．紹介する生体特徴情報

生体認証に利用できるとされる生体検知機能には数多くのバリエーションが存在する。そうした手法の中でも、本稿では、金融分野において比較的注目を集めているとみられる生体特徴情報に焦点を絞り、それらと併用して利用可能な生体検知情報をいくつか取り上げる。ここでは、わが国の金融分野における現状を反映した調査結果として、金融情報システムセンターのアンケート調査結果を参照する。金融情報システムセンターが平成 16 年 3 月に金融機関（回答数 471）を対象に実施したアンケートでは、生体認証技術を「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において採用された生体特徴情報が紹介されており、指紋（14.5%）、静脈パターン（10.5%）、虹彩（3.6%）の 3 つが上位を占めているとの結果が示されている（金融情報システムセンター [2004]）。こうしたことから、本稿においては、生体特徴情報として指紋、静脈パターン、虹彩のいずれかを採用する場合を想定する。

ロ．生体検知機能の実現方式の例

以下では、指紋、静脈パターン、虹彩のいずれかを生体特徴情報として採用することを前提とした場合、金融機関の窓口等において比較的短時間で認証・登録が実行可能であり、小型の装置で実現可能と考えられる生体検知機能の実現方式の事例を、主として特許情報を参照しながら説明する。具体的には、生体検知情報の読取対象として、脈波、静電容量、インピーダンス、光の反射・透過・散乱度合い、皮膚表面の色の変化、目の各種特性を取り上げる。

（イ）脈波

脈波（pulse wave）は、心臓の収縮によって生じる血液の圧力変化が末梢の血管に伝わっていくときに発生する波動であり、その振動数が脈拍（pulse）である。脈波には個人差が存在するほか、当該個人の生理的状態（運動した直後か、興奮しているか、落ち着いているか等）にも依存するため、認証時の判定方法やしきい値の設定をどのように行うかについて十分検討することが必要である。

脈波を測定する代表的な手法としては、血液の光学特性を利用する手法と、血液の圧力の変化（力学特性）を利用する手法が挙げられるが（特許庁 [2005a]）、ここでは、本節（2）において紹介する生体認証システムの事例で採用されている光学特性を利用する手法について説明する。光学特性を利用する主な手法としては、被認証物に特定波長の光を照射し、①その透過・反射・散乱光の変化から直接脈波を検出するという手法（特許庁 [2005b]）や、②血液の酸素飽和度を計測し、その時間的変化から脈波を検出するという手法が提案されている（例えば、Lapsley *et al*. [1998]、比良田ほか [2005]）。以下では、上記の②の手法について詳しく説明する。

本手法では、血液中の酸素飽和度（単位血液量に存在する総ヘモグロビン量に占める酸化ヘモグロビンの割合）に着目し、酸素飽和度の時間的変化を測定することによって脈波の波形を算出するという仕組みを採用している[11]。具体的には、酸素と結合した酸化ヘモグロビンと、酸素と結合していない還元ヘモグロビンの比率の変化を計測し、この比率がどのようなサイクルで変化しているかを測定することによって脈波を算出する（Oostrom and Harris [1997]、Osten *et al*. [1998]）。酸化ヘモグロビンと還元ヘモグロビンの比率は、特定波長の光の反射・透過度合いを利用して算出するケースが一般的である。2 種類のヘモグロビンはそれぞれ異なる特定波長の光を吸収しやすいという性質を有して

[11] 2 種類の波長の異なる光を照射して酸素飽和度、および、脈波を測定する手法はパルス・オキシメトリ（pulse oximetry）と呼ばれ、本手法を実現する方式や装置は一般にパルス・オキシメータ（pulse oximeter）と呼ばれる。

おり、それらの波長の光を被認証物に照射し、反射光や透過光の光量を測定することによって比率を算出することができる。

被認証物が生きている人間か否かの判定方法の 1 つとしては、算出した脈波の波形（生体検知情報に対応）と、あらかじめ登録されていた脈波の波形とを照合し、その類似度に応じて生体か否かを判定するという手法が提案されている（例えば、比良田 [2005]）。登録される脈波としては、生きている平均的な人間のものを採用する場合のほか、各個人の脈波を採用する場合も考えられる。

本手法に対する攻撃として、脈拍によって生み出される周期で外部から光を点滅させ、生体指を模倣するというものが想定される。こうした攻撃への対策として、指から光が放出されていないことを光学式センサによって測定するという仕組みも考案されている（Lapsley *et al*. [1998]）。

（ロ）静電容量

静電容量は、単位電位あたり蓄えられる電荷量であり、当該物質においてどのくらいの電荷が蓄えられるかを示す。人間の皮膚は比較的電荷を蓄積しやすいという特性を有しており、シリコーン樹脂（人工物の材料例）等の絶縁体に比べて数十～数千倍の静電容量を示すことが知られている。こうした特性を利用して、いくつかの市販の指紋読取用センサにも静電容量が採用されている。指紋を読み取る際の基本的な原理は、指の表皮と電極とによってコンデンサを構成するというものであり、電極間の距離と電荷量とが反比例の関係にあることを利用して、電極に蓄えられた電荷量の多寡によって指紋の凹凸を読み取るという仕組みである。ただし、後述するように、皮膚表面の静電容量は発汗等にも依存することから、判定時のしきい値の設定等について十分検討することが必要となる。

生体検知に静電容量を利用する手法の 1 つとして、静電容量と電荷の放出・充電の周期との関係を利用したものが提案されている（小山 [2005]）。シリコーン樹脂等の絶縁体の場合には、一般に静電容量はほぼゼロとなり、時間の経過と関係なく一定であることが知られている。本手法においては、被対象物の表面に接触するように電極を配置し、被認証物と電極等によってコンデンサを構成したうえで、当該コンデンサにおける電荷の放出・充電の周期を測定するという仕組みが採用されている。生きている人間が被認証物の場合、絶縁体に比べて静電容量が相対的に大きく、コンデンサにおける放電・充電に比較的長い時間がかかり、その周期が相対的に長くなる傾向にあることが知られている。こうしたことから、判定しきい値として一定の周期を設定し、当該周期よりも長い周期が計測された場合には、被認証物が生きている人間であると判定するという手法が提案されている。

また、生きている人間の場合、絶縁体に比べて静電容量の時系列的変化が大きくなる傾向にある。こうした傾向に着目した手法も提案されている。例えば、①上記の電荷の放出・充電における周期を連続的に観察し、周期の時系列的な変化率をベンチマークとして判定するという手法（小山 [2005]）や、②生体における発汗に伴って皮膚表面の静電容量が変化する点に着目し、静電容量式センサによって読み取られる皮膚表面の紋様（典型的には指紋）の色合いの変化を手掛かりに判定するという手法も提案されている（Derakhshani [2005], Derakhshani *et al*. [2003]）。

このうち、上記②の手法に関しては、人間の汗が電解質を含んでいるために高い比誘電率（当該物質が電荷をどれだけ蓄積しやすいかを示す物理量）を有し、発汗に伴って生体の皮膚表面における静電容量が変化する、すなわち、汗が付着する部分により多くの電荷が蓄積されるという特性に注目したものである。例えば、静電容量式センサによって指紋を読み取る場合、指紋の隆線に沿って汗が流れ、隆線の部分に付着した汗によって指紋画像の濃淡が時間的に変化する。例えば、センサ上に指を置いている間に汗が出てくるとすれば、隆線部分の電荷が増加し、隆線がより鮮明に浮かび上がることになる。こうした画像の色合いの変化をグレー・スケール[12]の変化として捕捉し、生体か否かを判定するという仕組みである。本手法は、通常の静電容量式センサを利用できれば、そのソフトウエアを変更するだけで実現可能であるというメリットを有している。ただし、グレー・スケールの比較を行うための複数の画像をどの程度の時間的間隔をおいて撮影すべきか等の実装上の課題が残されている。

（ハ）インピーダンス

インピーダンスは、交流電流を回路に流したときに発生する交流抵抗のことであり、電圧と電流の比によって表わされる。被認証物から計測されるインピーダンスを手掛かりに、被認証物が生きている人間であるか否かの判定を行う手法が提案されている（例えば、Kallo *et al*.[2001]、長子・兼田 [2003]、上山・林 [2003]）。生体におけるインピーダンスは、人体を構成する成分によって変動する。体脂肪率が上昇するとインピーダンスも上昇する（電気が流れにくくなる）ことがよく知られており、健康器具等において体脂肪率を簡易に測定する際にインピーダンスの測定が行われるケースが多い。

インピーダンスを利用して生体検知を行う手法としては、被認証物に 2 つの電極を当てて、電極間のインピーダンスやそれを反映する交流電圧の周波数を判定に用いるという手法が挙げられる（上山・林 [2003]）。この場合、生きて

[12] グレー・スケールは、白黒画像における対象部分の色（灰色）の濃さを表す指標である。

いる人間を被認証物としてインピーダンスや交流電圧の周波数をあらかじめ測定し、生きている人間を対象とした場合における交流電圧の周波数の範囲を見積もったうえで、その範囲をカバーするように判定しきい値（周波数）を設定することとなる。このため、判定しきい値の範囲を適切に設定するうえで、どの程度の計測のサンプルが必要になるか等について十分な検討が必要となってくる。

また、別の手法としては、電極に指等が触れた場合における回路のインピーダンスの変化を測定して判定に用いるというものも提案されている（笠井[2004]）。本手法においても、生きている人間の場合に想定されるインピーダンスの変化の範囲をあらかじめ計測することが必要であり、その範囲をカバーするように判定しきい値を設定することになる。

（二）光の反射・透過・散乱度合い

生体に光を照射した場合、生体特有の光学特性や生体の形状・材質等に基づき、光は反射、透過、散乱する。こうした被認証物における光のふるまいを測定し、例えば反射光、透過光、散乱光の光量を時系列的に測定することによって、被認証物が生きている人間か否かを判定するというアイデアが提案されている。特に、赤外光等の波長が比較的長い光を皮膚に照射した場合には、皮膚の内部へ光が透過し、皮膚の真皮や血管のパターンを反映した光を観測することができる。こうした特性を、生体検知情報だけでなく生体特徴情報として利用する手法も提案されている。例えば、指紋パターンと同一の真皮の形状を読み取る手法（滝口 [2003]）、異なる波長の光を順々に照射し、各反射光の光量のパターンを生体特徴情報とする手法（Nixon *et al.*[2004]）、静脈パターンを読み取る手法（三浦・長坂・宮武 [2003]、森・新崎・佐々木 [2003]）が挙げられる。

光学特性を生体検知に用いる手法としては、生体に照射された光が生体内部において伝播・拡散し、ランダムに反射・散乱するという現象を手掛かりとする手法が提案されている（加藤ほか [1996]、Nixon *et al.*[2004]）。

加藤ほか [1996]においては、生体内部における反射・散乱によって照射部分だけでなくその周辺部分も明るく輝くことを利用し、①明るく輝く部分の大きさ、②明るく輝く部分の中心位置と光の照射部分との変位、③反射・散乱光における偏光の度合いを生体検知情報として判定を行うという仕組みが提案されている。③の反射・散乱光の偏光の度合いを利用した手法をやや詳しく説明すると、本手法は、光を一定方向に偏光させて被認証物に照射したうえで、その反射光および散乱光を、偏光の方向が異なる（例えば直交する）2 種類の偏光フィルタをそれぞれ通して捕捉し、各光の光量を比較して判定を行うという

仕組みである。加藤ほか [1996]においては、被認証物が生きている人間の場合とシリコーン樹脂の場合を比較すると、シリコーン樹脂の場合には内部での散乱が相対的に少なく、特定方向に偏光した反射光、散乱光が大部分を占めることとなり、2 種類の偏光フィルタを通過した光のいずれか一方で強い光が検出される（もう一方のフィルタではほとんど検出しない）と説明している。これに対して、生きている人間の場合には、特定方向に偏光した反射光や散乱光が相対的に少なく、偏光フィルタを通過した 2 種類の光の光量に偏りが相対的に小さくなる傾向があるとしている。偏りの度合いを判定しきい値として設定し、測定値がその値よりも小さくなる場合、被認証物が生きている人間であると判定する。

また、Nixon *et al.*[2004]では、被認証物に波長の異なる光を照射し、その反射光の光量を測定することによって生きている人間か否かを判定する手法が提案されている。物質からの反射光の特性はその波長や照射対象の物質の内部構造に依存することが知られており、本手法は、生きている人間の皮膚の内部構造が他の物質の内部構造と異なっている点に着目したものである。具体的には、あらかじめ生きている人間の皮膚にさまざまな波長の光を照射してその反射光の光量を測定しておき、認証時には被認証物からの反射光の光量を測定し、両者を比較することによって生体検知を行う仕組みとなっている。本アイデアに基づく生体検知装置が実際に開発されており、Nixon *et al.*[2004]では、その有効性を検証するための実験の結果も報告されている。

その他の手法としては、被認証物からの反射光や透過光によって撮影した画像の明暗の分布状況を手掛かりに判定を行うという手法（例えば、ヒストグラム分布特性比較法、特許庁 [2005b]）も提案されている。この手法は、主に、血管パターンを生体特徴情報の読取対象として利用する場合に併用されるケースが想定されている。

いずれの手法を適用するにあたっても、生きている人間からの反射光や透過光が人工物等の場合とどの程度異なっているかを当該アプリケーションの環境下において明確にしておくことが求められる。

（ホ）目の特性

目から得られる代表的な生体特徴情報としては、虹彩や網膜上の血管パターンが挙げられるが、目は、生体特徴情報だけでなく生体検知情報の源でもある。目の各種特性を生体検知に活用するさまざまなアイデアが提案されているが（Daugman [2005]、Toth and Seelen [2005]）、それらの中から代表的な事例として、次の 5 つを挙げることができる。

① 照射される光の光量に応じた瞳孔（眼球における黒目の部分）の拡張・収縮の動きを手掛かりとする手法
② 瞳孔に照射された光の反射の有無や位置を手掛かりとする手法
③ 瞳孔から入った光が網膜を照射し、網膜の血管を流れる血液の色を反映した光が反射した結果、瞳孔の部分が赤く輝いてみえるという赤目現象（red eye effect）の発生を手掛かりとする手法
④ 照射した光に対する角膜・水晶体における反射によって、光源の像（プルキニエ像と呼ばれる）を眼球上に複数観察することができるという現象を手掛かりとする手法
⑤ 眼球やまぶたが外部からの刺激に反応して動作する様子を手掛かりとする手法

これらの生体検知機能の実現方式は、主として虹彩や網膜の血管パターンを生体特徴情報の読取対象として用いる生体認証システムにおいて活用されることが想定されているとみられる。目から読み取られたアナログ情報を生体特徴情報として採用し、生体検知情報を捕捉する際に必要となる発光器や受光器を共有させることによって、照合装置の小型化につながるといったメリットが期待される。

以下では、各種手法の中でも、特許情報において具体的な実現方式が記載されている上記①の性質を利用した手法を取り上げて説明する（例えば、小田[2002]、スン・ジャン [2002]、草刈・脇山 [2003]）。

草刈・脇山[2003]によって提案された手法は、光量を変化させながら可視光を連続して 2 回照射し、その際に撮影した眼画像から瞳孔の大きさの変化を捕捉するというものである。瞳孔の大きさが変化している場合には、被認証物は生きている人間であるとの判定を行う。

同様の原理に基づく手法が小田 [2002]によっても提案されているが、本手法では、上記①の性質だけでなく、上記②の性質も併用して生体検知が行われている点が異なる。まず、近赤外光を発生させる複数の光源と可視光を発生させる 1 つの光源を準備したうえで、可視光の光量をランダムかつ連続的に変更させながら瞳孔に照射し、瞳孔の大きさがどのように変化しているかを観測するというものである。この場合、光量の変化と瞳孔の大きさの変化が整合的であるか否かが確認される。さらに、複数の近赤外光を瞳孔に照射し、被認証物が近赤外光を適切に反射しているか否かの確認が行われる。これら 2 つの確認が複数回実施され、それらの結果に基づいて被認証物が生きている人間か否かが最終的に判定される。本手法における生体検知情報は、瞳孔のサイズの変化のパターンと、近赤外光の反射のパターンから読み取られることになる。

（へ）皮膚表面の色の変化

センサの表面に指を押し当てると、指の血流の変化等によって指表面の色が変化する。例えば、指を硬い物質に押しつけると、押しつけられた指の表面の色が赤色から白色に変化するという現象が生じる。こうした生体の色の時間的な変化を手掛かりとして生体検知を行う手法が提案されている（藤枝・松山・田口 [2003]、藤枝ほか [2004]、栗田ほか [2005]、田井ほか [2005]）。

皮膚表面の色の変化を生体検知に利用する手法として、まず、読取部位（指を想定）における各色相（赤、緑、青）の色信号と、画像センサ面に押しつけられた被認証物の面積とを計測し、両者の間の相関関係をベンチマークとする手法が提案されている（藤枝・松山・田口 [2003]）。藤枝・松山・田口[2003]は、指を画像センサの読取面に密着させる密着光学系において撮像する場合、色信号の変化と、画像センサに押しつけられた指の面積の変化との間に有意な相関があることを実験によって示している。

また、別の手法として、皮膚からの散乱光を捕捉する散乱光式センサを利用し、指をセンサ面に押しつけて離すまでの間における色信号の変化がヒステリシス特性を有している点に着目した手法も提案されている（藤枝ほか [2004]、栗田ほか [2005]）。ここでのヒステリシス特性とは、指をセンサ面に押しつけたときにたどる色信号の変化の軌跡と、指をセンサ面から離したときにたどる色信号の変化の軌跡が一致しないという特性を意味する。本手法においては、これらの変化の軌跡における色相の差分をとり、その差分の最大値を判定しきい値に設定するという仕組みが採用されている。判定時には、測定した色信号の差分の最大値が判定しきい値を上回った場合、被認証物が生きている人間の指であると判定する。

上記の 2 番目の手法に関しては、実際に人工指をどの程度排除する（生きている人間であると判定しない）ことができるかについての実験結果も発表されている（田井ほか [2005]）。本実験においては、①肌色のシリコーン樹脂製人工指、②ウレタン製人工指、③木棒を芯としたウレタン製人工指、④木棒を芯としたウレタン製人工指に透明なシリコーン樹脂をかぶせたもの、⑤生きている人間の指に透明な薄膜のシリコーン樹脂をかぶせたもの、⑥表面を肌色に塗装したシリコーン樹脂製人工指が実験の対象とされた。実験の結果、上記①、③、④の人工指に関しては、生きている人間ではないとの正しい判定が比較的高い割合で得られたものの、その他の人工指に関しては、正しく判定することが困難であるとの結果が得られている。

また、上記 2 つの手法のいずれに関しても、判定しきい値をどのように設定するかという問題が残されている。判定しきい値を適切に設定するためには、

そのベースとなるサンプルの測定をどのように行うかが重要となってくる。サンプル数をどの程度に設定するか等に関しては、照合時間に関する条件等のアプリケーションに依存する部分も大きいことから、十分な検討が求められる。

(2) 生体検知機能を搭載した生体認証システム

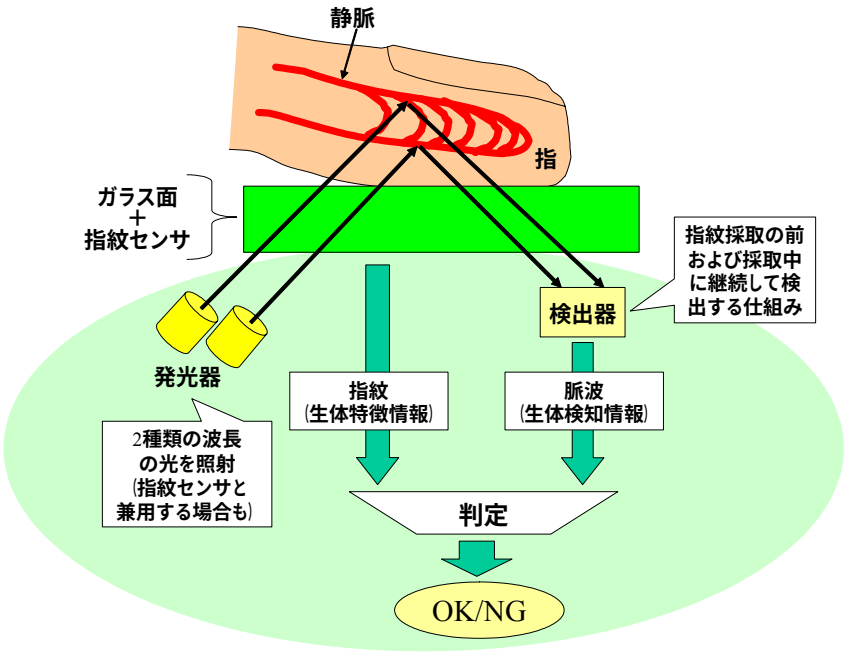
生体検知機能が有効に機能するか否かは、生体検知情報自体の偽造の困難性（3 節（3）**イ**.（**ロ**）の要件 2）に加え、生体検知機能が生体認証システムの中でどのように生体特徴情報と結び付けられているか（同要件 1）に依存すると考えられる。したがって、生体検知機能の有効性を議論する際には、生体認証システムがどのように構成されているかに着目する必要がある。以下では、本節（1）において取り上げた生体検知情報を利用している生体認証システムの具体例を紹介する。生体認証システムにおいて生体検知機能がどのように実装されているかについて詳細に記述した公開資料としては、特許情報に限定されてしまっているのが実情である。ただし、こうした特許情報は膨大に存在し、それらを本稿において網羅的に紹介することは困難である。以下では、生体認証システムの実現形態の例として、わが国における最近の特許および公開特許の中から、生体検知機能の実現方式、生体認証を実行するプロセス、生体検知情報と生体特徴情報の関係が明示されているものを選んで紹介する。

ただし、特許となっている装置・方法・システムが実際にある程度のセキュリティを確保しているか否かについては、現時点では明らかになっていないほか、実際のセキュリティ・レベルは実装環境にも依存するため、こうした点を考慮しないで判断を下すことは適切でない。以下で取り上げるものについても、「このようなシステムが提案されている」という事例紹介の意味で取り上げるものであり、十分なセキュリティ・レベルを確保しているものとして取り上げるわけではない点をあらかじめ断っておく。

イ．脈波

脈波を生体検知情報の読取対象として利用する生体認証システムの公開特許として、「生体検知方法」（特開 2005-46234）を挙げることができる（比良田ほか [2005]）。本公開特許は方法に関する 20 の請求項を含んでいる。請求項 1〜13 は、パルス・オキシメータを利用した生体検知方法を対象としており、その中でも請求項 8〜13 は指紋認証装置を含む生体検知方法を、請求項 14、15 は指静脈認証装置を含む生体検知方法を、請求項 16、17 は手の甲静脈認証装置を含む生体検知方法をそれぞれ対象としている。請求項 18〜20 については、掌形認証装置を含む生体検知方法を対象としている。

図 8　脈波を生体検知情報の読取対象とする指紋照合方法（概念図）



本公開特許の発明における生体検知の原理、すなわち、パルス・オキシメトリを利用した脈波の測定は、本節（1）**ロ**.（**イ**）において説明したように、2種類の波長の異なる光を照射し、その透過光あるいは反射光を測定することによって実行される。本特許における生体検知方法としては、「発明の実施の形態」において、①脈波から脈拍を抽出し、その脈拍から被認証物が生きている人間か否かの判定を行うという手法と、②登録時に脈波による信号の絶対値の平均値を算出・登録しておき、認証時に得た平均値と登録されていた平均値との差が一定範囲内に収まっているか否かを確認することによって判定するという手法が記載されている。

指紋認証装置における生体検知方法の処理の流れを整理すると以下のとおりである（図 8 参照）。

① 生体検知をまず実行する。パルス・オキシメータの発光体から被認証物に 2 種類の赤外光を照射し、その透過光あるいは反射光を手掛かりに生体検知を行う。
② 上記の生体検知によって被認証物が生きている人間であると判定した場合には指紋認証を開始する。その際に、上記①の生体検知も継続して実行する。
③ 指紋の読取りが完了するまでの間に生体検知を実行し、その間生体検知

の処理が継続して成功した場合に、読み取った指紋のデータと登録されていた指紋のデータの照合が行われる。生体検知の処理が継続して成功しなかった場合、本処理を停止し、上記①の生体検知から再度開始する。

④ 指紋の照合が成功した場合、被認証物が生きている人間であり、登録されている本人であると判定する。

以上の処理の流れを考慮すると、本生体認証システムは 1 対 1 照合を実行するものであり、指紋の読取りが完了するまで生体検知が継続して実行されることから、同じタイミングでそれら 2 つの情報が読み取られるといえる。また、生体特徴情報と生体検知情報が異なる部位（指の表面と指の内部）から読み取られている。したがって、生体検知情報の読取形態という観点からみると、同時読取型に属すると考えることができる。また、脈波の信号を読み取る際に、その刺激となる赤外光の光量を変化させる、あるいは、それに応じた脈波の信号の変化を検知するといった記述は本公開特許に明示されていないことから、被認証物への刺激の形態という観点からみると、変化非誘発型に属すると考えられる。

指静脈パターンを生体特徴情報の読取対象として採用する生体認証システムの場合、生体検知や認証のプロセスは基本的には上記の指紋を用いるシステムの場合と同様である。ただし、生体検知情報と生体特徴情報が同じタイミングで同じ部位から読み取られるため、完全同一型に属する。被認証物への刺激の形態という観点からは変化非誘発型に属する。生体特徴情報の読取対象が手の甲静脈パターンの場合も同様である。

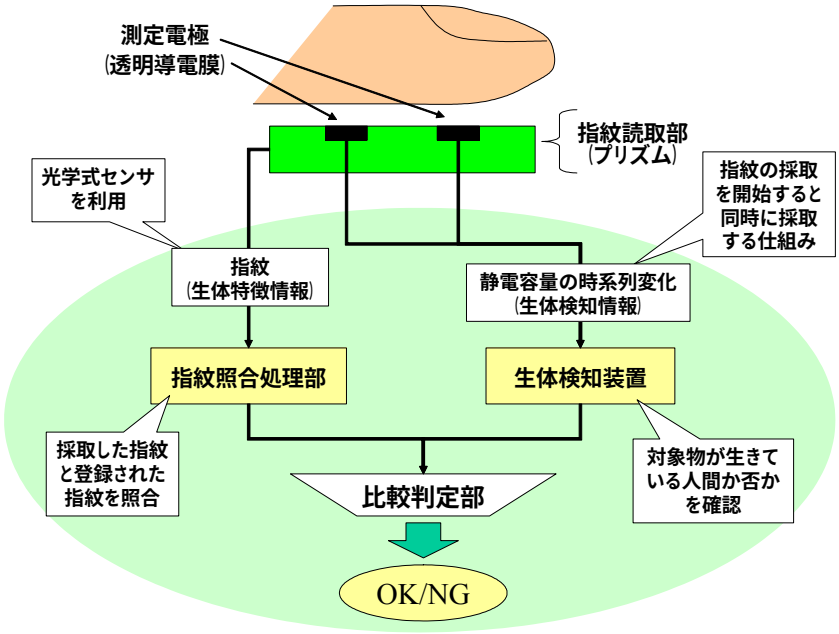
ロ．静電容量

静電容量を生体検知情報の読取対象として利用する生体認証システムの特許として、「生体検知装置」（特許第 3620558 号）が挙げられる（小山 [2005]）。本特許は 2 つの請求項を含んでいる。請求項 1 には、被認証物の静電容量を用いた生体検知装置が記述され、請求項 2 には、被認証物が生きている人間か否かを判定する方法が明示された当該生体検知装置が記述されている。

本特許の「発明の実施の形態」および「実施の形態の具体例」に、生体検知機能の原理として本節（1）**ロ**．（**ロ**）において説明した手法が記述されている。すなわち、被認証物が電極に触れると被認証物と電極等によってコンデンサが構成され、そのコンデンサにおける電荷の充電・放出の周期を測定し、当該周期が時系列的にどの程度変化するかを基準として判定が行われるという仕組みとなっている。

本特許の生体検知装置の構成は生体特徴情報の読取対象としてどのような

図 9　静電容量を生体検知情報の読取対象とする指紋照合装置（概念図）



資料：小山 [2005]

ものを採用するかによって異なるが、「実施の形態の具体例」には、プリズムを利用した光学式読取りによる指紋照合装置の例が記述されている。この指紋照合装置は、生体検知装置、測定電極、指紋読取部、指紋照合部、比較判断部から構成され、測定電極と指紋読取部としてそれぞれ透明導電膜とプリズムが利用されており、プリズム上に透明導電膜が形成されるかたちとなっている。したがって、指紋を読み取る部位と、コンデンサにおける放電・充電の周期の変化率を測定する部位が同一になっていることがわかる。

また、生体認証の手続が「実施の形態の具体例」に記載されており、それらをまとめると次のとおりとなっている（図 9 参照）。

① 指紋読取部において光学式センサによって指紋の凹凸情報を読み取る。
② 指紋の凹凸情報は、指紋照合処理部において既に登録されている凹凸情報と照合され、合致するか否かが判定される。
③ 上記①の処理が開始されると同時に、測定電極を通じて生体検知装置において、静電容量の時系列的変化を反映する情報が計測され、被認証物が生きている人間か否かの判定が行われる。
④ 最後に、比較判断部において、上記②と③の判定がいずれも成功した場合に限り、“ OK ”との照合結果が出力される。

このように、1 対 1 照合を採用しているほか、生体検知情報と生体特徴情報の読取りは同じタイミングで同じ部位（皮膚の表皮）において 実行される。したがって、本生体認証システムは、生体検知情報の読取形態の観点から完全同一型に分類される。また、本システムでは、生体検知情報を読み取る際に被認証物に与えられる刺激は交流電圧となるが、その交流電圧を認証時ごとにランダムに変化させるといった記述はなく、生体検知情報を意図的に変化させるために刺激を変化させるといった仕組みが組み込まれているわけではない。このため、被認証物に付与される刺激の形態の観点からは、本生体認証システムは変化非誘導型に属すると考えられる。

ハ．インピーダンス

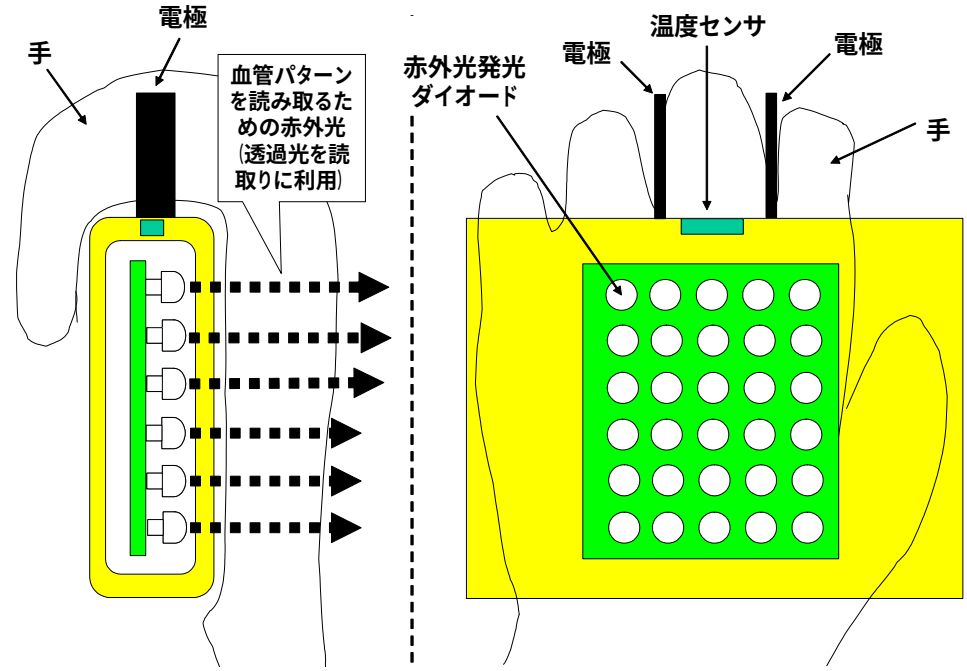
インピーダンスを生体検知情報の読取対象として利用する生体認証システムの特許として、「生体認証装置」（特許第 3396680 号）が挙げられる（長子・兼田 [2003]）。本特許は 3 つの請求項を含んでおり、このうち、請求項 1 には、手や指に赤外光を照射し、その反射光や透過光を読み取って画像を生成する手段のほか、手や指の温度、（直流）電気抵抗、インピーダンスのうち少なくとも 1 つを計測し、被認証物が生きている人間であることを確認する「生体確認手段」等を備えた装置が記載されている。また、請求項 2 においては、上記の請求項 1 の装置に、データベースから登録画像を取り出す手段を追加するとともに、読み取った画像と登録画像との照合を行うことが明示された装置が記載されている。このように、本特許においては、生体検知情報の読取対象として、インピーダンスに加え、温度と直流電流における電気抵抗を採用している。

生体検知機能の原理に関しては、本特許の「発明の実施の形態」に記載されている。温度を利用した生体検知は、手の表面に接する温度センサ（サーミスタ[13]）によって電圧を測定し、測定された電圧が特定の範囲に入っているか否かを確認するという手法によって実行される仕組みとなっている。電気抵抗については、2 本の電極をそれぞれ指と指の間に挟み、一方の電極に所定の直流電圧をかけたときに他方の電極に発生する電圧を測定し、測定された値が特定の範囲に入っているか否かを確認するという手法が採用されている。インピーダンスについては、電気抵抗の測定に用いた電極を利用し、一方の電極に所定の交流電圧をかけ、他方の電極に発生する交流電圧の位相や振幅が一定範囲内に収まっているか否かを確認することとしている。

本装置において利用することが想定される生体特徴情報の読取対象として

[13] 温度のデータを電気抵抗値に変換するセンサ。本センサから出力される電気抵抗値と電流の値から電圧を測定することができる。

図 10　手のひらの血管パターンによる生体認証装置の一部（概念図）



資料：長子・兼田[2003]

は、手のひらや指の血管パターンが想定されている。「発明の実施の形態」においては、まず手のひら（手根および指を除く部分）を透過した赤外光によって生体特徴情報を読み取るという形態が記述されており、生体特徴情報の読取対象として血管パターンを利用することを想定しているとみられる。本実施例における認証処理のフローを整理すると次のとおりである（図 10 参照）。

① 被認証物から ID の入力を得る。
② 当該 ID に対応する認証データ（固有パターンに対応）を読み出す。
③ 被認証物の直流電流による電気抵抗を中指の中央付近から測定する。
④ 被認証物のインピーダンスを中指の中央付近から測定する。
⑤ 被認証物の温度を指の付け根付近から測定する。
⑥ 上記③～⑤の測定結果から、被認証物が生きている人間であるか否かをそれぞれ判定する。いずれの測定結果からも被認証物が生きている人間であるとの結果が得られた場合に限り、認証データの読取フェーズに進む。
⑦ 手のひらに赤外光を照射し、その透過光を検出して赤外光の画像を取り込む。

⑧ 赤外光の画像から、血管パターンの端点や分岐点等の情報（固有パターンに対応）を抽出する。
⑨ 測定して得た固有パターンと上記②で読み出した固有パターンとを比較し、一致するか否かを判定する。一致と判定した場合にはOKを出力し、対応するアプリケーションを提供する。

このように、本生体認証システムにおいては、1対1照合を行っているほか、3 種類の生体検知を実施した後に、血管パターンによる認証を実行している。このことから、生体検知情報と生体特徴情報の読取りは異なるタイミングで実施されると考えられる。また、これらの情報の読取部位については、特許に記載されるセンサの配置図を見ると、中指の中央付近から電気抵抗とインピーダンスに関する情報を、指の付け根付近から温度の情報をそれぞれ読み取るほか、生体特徴情報は手のひらの内部から読み取る構成となっている。こうしたことから、生体検知情報と生体特徴情報はそれぞれ別の部位から読み取られるといえる。以上の考察より、本システムは独立読取型に属するといえる。

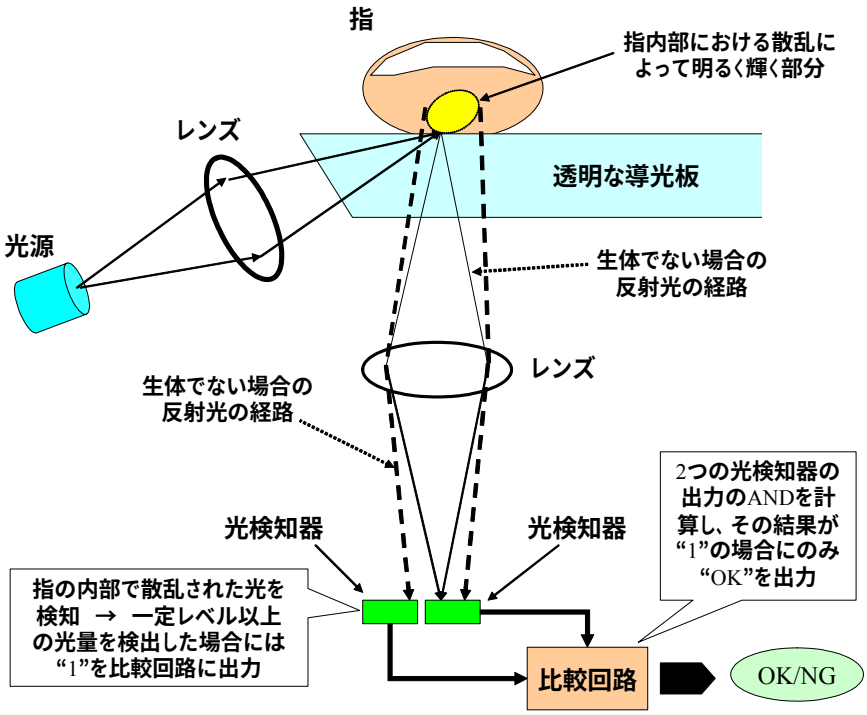
また、各種生体検知情報の読取りに際し、読取部位の状態変化の誘発を目的として、センサ側からの刺激を変化させる等の特別な措置が講じられているといった記述がない。このため、本システムは、付与される刺激の形態という観点から変化非誘発型に属するといえる。

「生体認証装置の第2実施例」として、指の血管パターンを認識する装置が記述されている。この場合に関しても、基本的には手のひらの血管パターンを利用した生体認証システムの場合と同様の生体検知および認証の処理が実行される。電気抵抗とインピーダンスについては指の付け根付近から、温度については指先から読み取られる構成となっている。血管パターンは指の中央部から読み取られることとなっている。このように、生体検知情報と生体特徴情報の読取部位が異なっており、本生体認証システムも独立読取型に属するといえる。また、被認証物に付与される刺激の形態の観点からは変化非誘発型に属するといえる。

ニ．光の反射・透過・散乱度合い

「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）は、指紋から生体特徴情報を読み取るほか、指の反射光や散乱光から得られる情報を生体検知情報として採用する生体認証システムを対象とした特許である（加藤ほか [1996]）。本特許は9つの請求項を有しており、このうち、請求項1〜8が生体検知装置を対象としている。やや詳しくみると、請求項1〜3は、指から反射・散乱した光から検出された像の大きさを手掛かりに生体検知を行

図 11　指内部における光の散乱を用いた生体検知の仕組み（概念図）



資料：加藤ほか[1996]

う装置を記載しているほか、請求項 4～6 は、反射・散乱した光から検出された像の大きさに加え、反射・散乱光によって明るく輝く領域の中心部分と照射した光の中心部分との変位の度合いを手掛かりに生体検知を行う装置を記載している。また、請求項 7～8 は、反射・散乱した光の偏光度合いを手掛かりに生体検知を行う装置を記載している。請求項 9 は、当該生体検知装置を搭載した指紋照合システムを対象としている。

生体検知の原理については、本節（1）**ロ.（ニ）**において説明したように、生きている人間の皮膚に照射された光が内部で伝播・拡散し、ランダムに反射・散乱するというものである。本特許の「課題を解決するための手段」には、上記に整理した請求項に記述されている 3 種類の生体検知の手法を実現する方法が記述されている。これらの手法のうち、請求項 1～3 において対象となっている生体検知装置を利用した指紋照合システムの処理手順が「実施例」に記載されている。指紋の読取りについては、光学式センサによって実行することとなっているが、生体検知情報を読み取る際に利用されるものとは別構成となっている。生体検知から指紋照合に至る一連の処理の流れを整理すると以下のとおりである（図 11 参照）。

① まず生体検知を行う。指に光を照射してその反射光や散乱光を集光し、2つの光検知器によって光量を測定する。
② 各光検知器によって検知した光量が一定水準以上となっている場合、光検知器は“1”を比較回路に対して出力する。比較回路においては、両方の光検知器の出力がともに 1 であった場合に限り、被認証物が生きている人間の指であると判定する。
③ 次に指紋照合を行う。光学式の読取手法によって指紋を読み取ったうえで指紋画像に変換する。
④ 上記③で得た指紋画像があらかじめ登録されていたものと一致するか否かを判定する。

このように、本生体認証システムにおいては、指紋による 1 対 1 照合が行われているほか、生体検知情報と生体特徴情報は異なる部位から読み取られていることがわかる。すなわち、生体検知情報は、照射した光が指の内部でランダムに反射・散乱したか否かを反映する情報であり、指の指紋を読み取る部位（指の表皮）とは異なる。2 つの情報を読み取るタイミングについては、最初に生体検知情報、次に生体特徴情報という順序になっている。ただし、「実施例」には、「生体検知、指の照明、指紋像の取り込みは、それぞれ数 10 ミリ秒以内といった短時間で行うように設定する。これによって、生体検知後にレプリカと交換して照合させるといった不正行為を防止することができる。」と記述されている。本生体認証システムでは、生体検知情報と生体特徴情報の読取りが実行される時間差が十分に小さくなるように配慮されている。以上を踏まえると、生体検知情報の読取形態の観点からは、本生体認証システムは同時読取型に属すると考えられる。

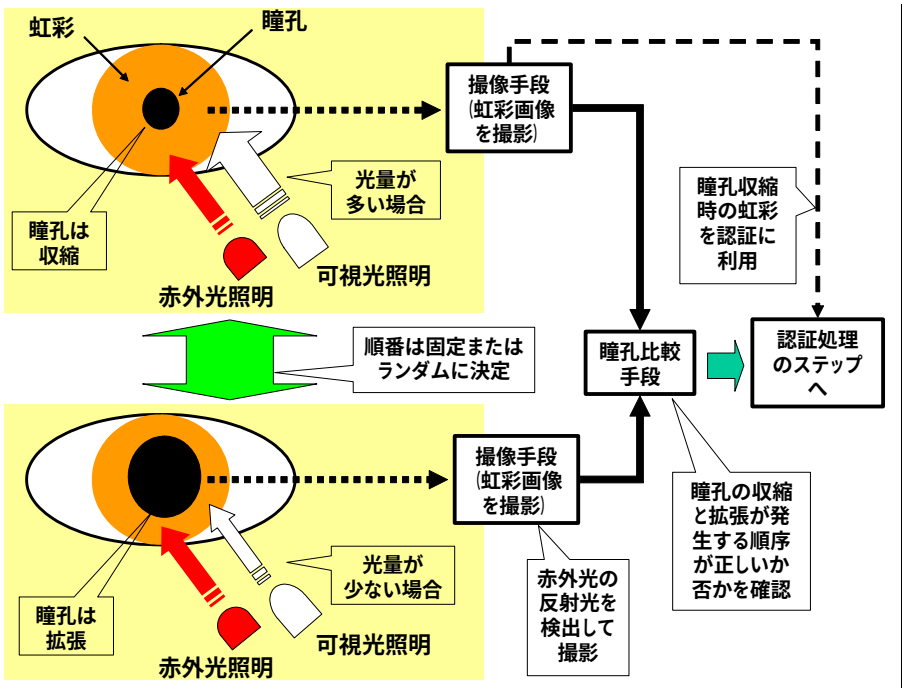
また、生体検知情報を読み取る際の刺激となる照射光に関して、読取部位の状態変化を観察することを企図して、照射光の光量や方向等を認証時に毎回変化させるといった実施例は、本特許には記載されていない。したがって、本生体認証システムは、被認証物に付与される刺激の形態という観点から変化非誘発型に属するといえる。

ホ．目の特性

（イ）瞳孔の収縮

瞳孔の収縮を手掛りに生体検知機能を実現する生体認証システムの特許として、「虹彩認証装置及び虹彩撮像装置」（特開 2003-30659）が挙げられる（草刈・脇山 [2003]）。本特許は 10 の請求項を有しており、このうち請求項 1〜5 は、虹彩画像を撮影する撮像手段、瞳孔の大きさの変化を測定する瞳孔比較手

図 12　瞳孔の収縮・拡張を用いた生体検知の仕組み（概念図）



資料：草刈・脇山[2003]

段、認証処理を行う認証手段によって構成される虹彩認証装置を記載している。やや詳しくみると、請求項 4 は、近赤外光の光源を別途備え、可視光と両方を同時に虹彩に向ける機構を備える虹彩認証装置を記載しているほか、請求項 5 は、2 つの虹彩画像のうち、瞳孔のサイズが小さい方の虹彩画像を認証処理に用いる虹彩認証装置を記載している。請求項 6～10 は、瞳孔のサイズが変化したと判定した場合に虹彩画像を認証処理装置に渡す瞳孔画像選択手段、撮像手段から構成される虹彩撮像装置を記載している。

本発明における虹彩認証装置の原理は、本特許の「課題を解決するための手段」に記載されており、本節（1）**ロ**.（**ホ**）において説明した縮瞳と呼ばれる特性に基づいている。縮瞳は、照射される光の光量が増えると瞳孔が収縮するという反射現象である。本虹彩認証装置においては、光量を 1 度、あるいは、2 度変化させ、その刺激によって瞳孔がどのように反応するかを手掛かりとして生体検知を実行する仕組みとなっている。その際に、瞳孔の大きさを図る指標として、瞳孔と虹彩の境目を手掛かりに計測する瞳孔径（瞳孔の直径）を採用している。

「発明の実施の形態」においては、縮瞳を誘発させる機構として光量を調整可能な可視光の発光ダイオードと、虹彩画像を撮影するための近赤外光の発光

ダイオードを備え、虹彩および瞳孔を含む画像を撮影するためのカメラを搭載した装置が記述されている。本装置における生体検知および認証の処理プロセスは以下のとおりである（図 12 参照）。

① まず瞳孔の反応の有無を確認する。ある光量（例えば大光量）の可視光と、一定光量の近赤外光を同時に照射し、虹彩画像を撮影する。
② 上記①とは異なる光量（例えば小光量）の可視光と、一定光量の近赤外光を同時に照射し、2 枚目の虹彩画像を撮影する。
③ 上記①と②で撮影した虹彩画像からそれぞれ瞳孔径を測定し、変化の有無を確認する。
④ 上記③において瞳孔径が変化しており、その方向（小→大）が光量の変化に対応していた場合、被認証物が生きている人間であると判定する。
⑤ 生きている人間と判定された場合、上記①で撮影した虹彩画像を利用して虹彩のデータを抽出し虹彩認証処理のステップに進む。

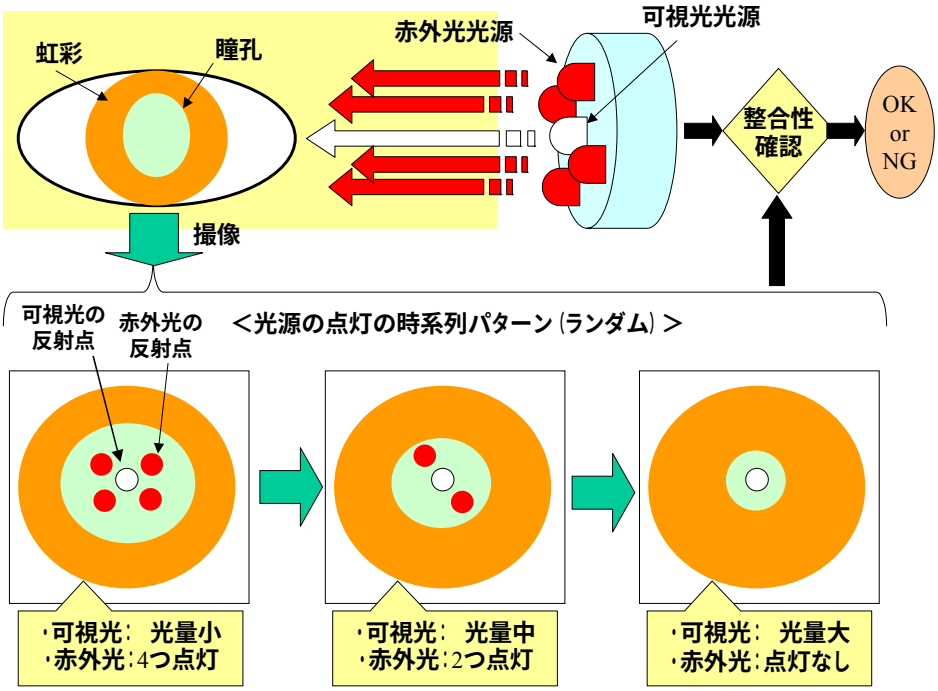
上記①と②における可視光の光量に関しては、最初に大光量で照射した後に小光量で照射する場合に加え、この逆のパターンもあり得る。本特許においては、こうした点についても言及されており、「どちらのステップ（上記の①と②に対応）の方を大光量とするかは、固定とするのではなく、ランダムにすることで偽造認証を困難にする。…（中略）…光量の大小がランダムであっても問題はなく、ランダムの方が、偽造画像の誤認証を避ける率がより一層高くなるのはいうまでもない。」と記述されている。このことから、光量の調整のパターンをランダムにするという手法も想定されていると読み取れる。

以上を踏まえると、本生体認証システムにおいては、瞳孔径の変化から読み取られる生体検知情報と、虹彩から読み取られる生体特徴情報が同一のタイミングで読み取られる仕組みとなっている。ただし、読取部位は異なっていると考えられる。瞳孔径の変化は瞳孔と虹彩の境界によって測定されるのが一般的であり、生体検知情報が直接虹彩部分から読み取られているわけではないと考えられる。これらのことから、生体検知情報の読取形態に着目すると、本生体認証システムは同時読取型に属すると考えられる。また、被認証物に付与される刺激の形態からは、光量の大小のパターンが固定の場合には固定パターン刺激型、パターンをランダムに変化させる場合にはランダム刺激型に属すると考えられる。

（ロ）瞳孔の収縮と光の反射

瞳孔に照射した光の反射の具合を手掛かりに生体検知を実行する生体認証

図 13　縮瞳と瞳孔の反射光を用いた生体検知の仕組み（概念図）



資料：小田[2002]

システムの特許として、「アイリスコード生成装置およびアイリス認証システム」（特許第 3315648 号）が挙げられる（小田 [2002]）。本特許は 11 の請求項を有している。このうち請求項 1～10 がアイリスコード生成装置を記載している。請求項 1 はアイリスコード生成装置の主要な構成要素を記載しており、同装置が、①目の画像の撮影手段、②画像処理手段、③生体反応を喚起させるための刺激手段、④刺激の内容を制御するコードを生成するチェックコード手段、⑤生体検知の判定を行う制御手段から構成されると記述されている。請求項 7 は、近赤外光が瞳孔上のどの位置において反射されているかに基づいて生体検知を行う装置を記載しているほか、請求項 8、9 は、近赤外光の光源が複数存在する装置、および、発光する光源の組合せがランダムに決定される装置をそれぞれ記載している。また、請求項 11 は、アイリスコード生成装置を搭載し、読み取ったアイリスコードをあらかじめ登録されたものと照合して個人を確認する機能を有するアイリス認証システムを記載としている。本特許における「アイリスコード」については、定義されていないが、ドーグマンによって提案されたアイリス・コード（iris code）等を利用することができると思われる（Daugman [2004]）。他の請求項をみると、その他の請求項の内容は次のとおりである。

本生体認証システムにおける生体検知の原理は、本特許の「発明の実施の形態」に記述されており、上記**（イ）**と同様の縮瞳、および、瞳孔が光を反射するという特性の 2 つを組み合わせている。「本発明の実施形態」をみると、可視光の光量を高めることによって縮瞳を誘発するほか、近赤外光を照射することによって瞳孔における光の反射を誘発するという仕組みが記述されている。実施例の 1 つとしては、可視光の光源を中心としてその周囲に複数の近赤外光の光源を配置したうえで、可視光の光量を調節して縮瞳を確認するほか、近赤外光の光源のうちどれが点灯するかをランダムに決定し、それらの点灯した光源から光の像が検出されるか否かを確認するという方式が記述されている。こうした瞳孔の動きと光の反射の有無、および、それらのパターンが生体検知情報の読取対象となる。

生体検知および虹彩を用いた認証の処理の流れは以下のとおりである（前頁図 13 参照）。

① 生体検知を行う際に、可視光および近赤外光の照射のパターンをランダムに決定する。このパターンをデータにしたものをライフチェックコードと呼ぶ。
② ライフチェックコードにしたがって、可視光あるいは近赤外光を特定の光量と特定の順序で照射し、それぞれの目画像を撮影する。
③ 目画像から、縮瞳のタイミングと反射光のパターンを測定する。縮瞳の有無については、画像のコントラスト分布から瞳孔と虹彩の境界を検出し、その境界によって構成される円のサイズを手掛かりに確認する。
④ 上記③で測定したタイミングおよびパターンと、上記①で生成したライフチェックコードが整合的か否かを確認する。整合的であった場合には、被認証物が生きている人間（の目）であると判定する。整合的でなかった場合には処理を中止する。
⑤ 上記②で撮影した目画像から、アイリスコードを生成する。
⑥ 上記⑤で生成したアイリスコードと、あらかじめ登録されたとみられているアイリスコードとを比較し、一致と判定される場合、本人確認が成功する。

このように、本生体認証システムは、1 対 1 照合を行うほか、生体特徴情報と生体検知情報を、同一のタイミングで異なる部位から読み取る。異なる部位から読み取る点に関しては、目画像における瞳孔のコントラスト分布を測定し、一定の判定しきい値に基づいて瞳孔の大きさを測定していることから、虹彩部分とは異なる部分から生体検知情報を読み取っていると考えることができる。

表 5　例に挙げた生体認証システムの分類

	変化非誘発型	固定パターン刺激型	ランダム刺激型
完全同一型	・比良田ほか[2005] （静脈パターン、脈波） ・小山[2005] （指紋、静電容量）		
同時読取型	・比良田ほか[2005] （指紋、脈波） ・加藤ほか[1996] （指紋、光の反射・散乱）	・草刈・脇山[2003] （虹彩、瞳孔の収縮）	・草刈・脇山[2003] （虹彩、瞳孔の収縮） ・小田[2002] （虹彩、瞳孔の収縮と光の反射）
同位読取型			
独立読取型	・長子・兼田[2003] （血管パターン、電気抵抗・インピーダンス・温度）		

備考：例えば、表中の“（静脈パターン、脈波）”は、当該生体認証システムの生体特徴情報と生体検知情報の読取対象がそれぞれ静脈パターン、脈波であることを示している。

以上を踏まえると、生体検知情報の読取形態の観点から、本生体認証システムは同時読取型に属するといえる。さらに、生体検知情報を読み取る際には、そのための刺激のパターンがランダムに決定され、それに応じて生体検知情報も変化するという仕組みになっている。このため、被認証物に付与される刺激の形態の観点からは、本生体認証システムはランダム刺激型に属すると考えられる。

(3)　各生体認証システムの分類

本節（2）において紹介した特許の実施例として挙げられている生体認証システムを、生体検知情報の読取形態（完全同一型、同時読取型、同位読取型、独立読取型）と読取部位に与える刺激の形態（変化非誘発型、固定パターン刺激型、ランダム刺激型）によって分類すると、表 5 のとおりである。以下では、生体認証システムが属する分類を記号で表わすこととする。例えば、生体検知情報の読取形態から完全同一型、読取部位に与える刺激の形態から変化非誘発型に分類されるシステムの集合を“［完全同一型、変化非誘発型］”と表記する。3 節（3）**ハ**. において説明したように、表 5 の分類を用いて各特許に記載されている生体認証システムの比較を行うことは適切でなく、ここでは各システムがどのカテゴリーに分類されるかを説明するにとどめる。

まず、状態変化の誘発を意図しない刺激を与えて生体検知情報を読み取る生体認証システムとしては、比良田ほか [2005]、小山 [2005]、長子・兼田 [2003] 、加藤ほか [1996]が挙げられる。

比良田ほか [2005]において実施例として挙げられている生体認証システムは、

指あるいは手のひらの内部に赤外光を照射し、その反射光を測定することによって読み取った脈波に関する情報を生体検知情報として利用している。このため、生体特徴情報として、指や手のひらの内部から読み取る静脈パターンを利用するか、指の表皮から読み取る指紋を利用するかによって、生体検知情報の読取形態による分類が異なる。静脈パターンを生体特徴情報の読取対象として利用する場合には、［完全同一型、変化非誘発型］に分類される。また、生体特徴情報として指紋から読み取る情報を利用する場合には、［同時読取型、変化非誘発型］に属することとなる。

小山 [2005]において実施例として挙げられている生体認証システムでは、静電容量を生体検知情報の読取対象として利用している。本システムは、生体検知情報と生体特徴情報のどちらも皮膚の表皮の同一部位から同一のタイミングで読取りを行うことから、［完全同一型、変化非誘発型］に分類される。

また、電気抵抗・インピーダンス・温度を生体検知情報の読取対象として利用する長子・兼田 [2003]の実施例の生体認証システムは、生体検知情報と生体特徴情報を、異なるタイミングで異なる部位から読み取っており、[独立読取型、変化非誘発型]に分類される。

光の反射・散乱を利用する加藤ほか [1996]の実施例の生体認証システムは、生体検知情報と生体特徴情報を、同一のタイミングで異なる部位から読取りを行っており、［同時読取型、変化非誘発型］に分類される。

一方、草刈・脇山 [2003]の実施例として挙げられている生体認証システムは、生体検知情報として瞳孔の収縮を利用しており、縮瞳を誘発させるように光量を変化させ、その刺激に対する反応を生体検知情報としている。本システムは、光量の調整のパターンを固定とするかランダムにするかは任意であるほか、生体特徴情報の読取対象には虹彩を利用するため、［同時読取型、固定パターン刺激型］、あるいは、［同時読取型、ランダム刺激型］に属することとなる。

また、小田 [2002]の実施例の生体認証システムは、縮瞳に加えて瞳孔における光の反射の状態も生体検知情報として利用する。本システムは、生体検知情報を読み取るための刺激（可視光および近赤外光の照射）のパターンをランダムに決定し、それに対する反応が整合的か否かを判断するという特徴を持つことから、［同時読取型、ランダム刺激型］に分類される。

5．生体検知機能の検討の方向性

(1) 検討結果を踏まえた考察

生体認証システムの安全性は、想定する攻撃者の行動（能力）に対する耐性の強さによって評価されるため、どのような攻撃を想定するかが重要となる。本稿では、生体認証システムに対する脅威として、攻撃者が「生体特徴情報を偽造して提示するとともに、自分の生体検知情報を提示する、または、生体検知情報を偽造して提示することによって、第三者へのなりすましを試みる」という状況を想定した。そのうえで、生体検知機能におけるセキュリティ要件（要件 1、要件 2）を示したほか、その要件の相対的な満足度合いを評価する軸として、生体検知情報の読取形態と読取部位に与える刺激の形態に着目し、生体検知機能を搭載した生体認証システムを 12 に分類する手法を提案した。

本分類法は、セキュリティの観点から生体認証システムの比較を行うための手掛かりとして活用することができる。例えば、生体認証システムのユーザが一定のセキュリティ・レベルを満足するシステムを選択する、または、既存のシステムにおけるセキュリティ・レベルを向上させる際に、本分類法を参考にすることが可能であろう。攻撃者による第三者へのなりすましに対しては、［完全同一型、ランダム刺激型］に属する生体認証システムが、本分類を用いた評価において他の分類に属するシステムに比べて相対的に望ましいと考えられる。ただし、本分類法は、個々の実現方式間の関係を直接示すものではなく、あくまで実現方式のある側面にのみ着目して分類した集合間の関係を示すものにすぎない点に留意する必要がある。今後は実現方式間の関係をより厳密に評価するべく検討を深めていくことが考えられる。

(2) 今後の検討の方向性

これまでの検討結果を踏まえ、今後生体認証システムの安全性に関する検討課題について技術面と運用面から述べる。

イ．技術面における課題

（イ）生体認証システムの分類法の精緻化

【分類の基準の精緻化】

本稿において示した生体検知機能における安全性の評価軸のうち、生体検知情報の読取形態に関しては、生体検知情報と生体特徴情報を①同じタイミングで読み取るか（読取期間の全部または一部が重なっているか）否か、②

同じ部位から読み取るか（読取部位の全部または一部が重なっているか）否かという 2 つの点に着目して生体認証システムを分類する方法を示した。ただし、情報の読取りの期間がどの程度重なっていれば同一のタイミングであると判断するか、また、読取部位がどの程度重なっていれば読取部位が同じであると判断するかについては、個々の実装形態に依存すると考えられるため、今回の検討では立ち入らない扱いとした。今後こうした点についても検討を深め、分類の基準を精緻化することが求められる。

【新たな評価軸の追加】

生体検知機能の有効性をより精緻に評価するうえで、今回提案した 2 つの評価軸とは別の評価軸についても検討することが有用であると考えられる。

本稿では生体検知情報の読取形態に基づいて 4 つのカテゴリーに分類する方法を示し、カテゴリー間の関係を考察した。ただし、同時読取型と同位読取型の関係については、生体検知情報と生体特徴情報の対応関係の相対的な強弱に関する比較を行うことは具体的な実装形態を想定しなければ困難であると考えられることから、それ以上の検討を行わなかった。この点に関して、別途新たな評価軸を考案し検討を深めることが今後の課題の 1 つとして考えられる。

新しい評価軸も組み合わせることでより詳細な分類が可能になれば、生体認証システムの比較、または、セキュリティ・レベルに応じたシステムの選択をより適切に実行することができるようになると期待される。

（ロ）人工物等による生体検知情報の再現困難性の評価

今回の検討では、生体検知情報を偽造することがどの程度困難かという観点で、被認証物に与える刺激の形態によって生体認証システムを分類する方法を検討した。刺激によって状態が変化するような読取対象を利用する場合、①状態変化の誘発を意図しない刺激、②同じパターンの刺激、③ランダムな刺激の順で、それらの刺激によって誘発される読取部位の状態変化（生体検知情報）を偽造することが困難になると一般には考えられる。

このような分類は、利用する読取対象の種類等を固定した場合において生体検知情報の偽造困難性を評価する際に有用であり、読取対象が同一であるシステム間における比較に本分類を用いることが可能であると考えられる。しかし、異なる読取対象を利用するシステムについては、そうした比較を行うことは適切でない。異なる読取対象を利用するシステムを比較できるようにするためには、各生体検知情報を人工物等によって再現することがどの程度困難であるかを個別に評価し、その結果を考慮して比較する必要がある。こうした評価を行

うための手法はまだ構築されておらず、今後検討することが求められる。

生体検知情報の再現困難性を評価する際には、再現するためにかかるコスト等を比較するという方法がまず考えられる。また、一定の読取環境（読取手法の種類、センサの精度、システム・パラメータの設定等）を想定したうえで、一定の手法によって再現された生体検知情報をどの程度の確率で正しく判定することができるかといった観点から評価するという方法も考えられる。こうした評価が可能となれば、異なる読取対象を利用している生体認証システム間での比較に加えて、各生体検知情報がどのような読取環境に適しているか、また、どのような生体特徴情報と組み合わせて利用するのが適切かといった点についての考察も深まるものと思われる。

（ハ）検討スコープの拡張

【生体特徴情報の種類の拡張】

本稿では、生体特徴情報の読取対象として、金融分野で特に関心を集めているとみられている指紋、静脈パターン、虹彩に焦点を絞り、これらと併用して利用される可能性が高いとみられる生体検知情報を取り上げて検討した。しかし、今回検討対象としたもの以外にも多種多様な生体検知機能の実現方式が提案されている。それらについても、本稿において検討した 2 つのセキュリティ要件を考慮して考察を行うことも有用であると考えられる。

【取り扱う脅威の拡張】

本稿では、想定する脅威として第三者へのなりすましを取り上げたが、日立製作所[2004]で示されているように、生体認証システムにはこれ以外にも多くの脅威や脆弱性の存在が想定されている（2 節（2）表 1 参照）。生体検知機能の包括的な評価を行ううえで、そうした脅威や脆弱性についても焦点を当てて、それらが生体検知機能の有効性にどのような影響を及ぼすかについて明らかにする必要がある。

【生体検知情報の利用形態の拡張】

今回の検討では、被認証物が生きている人間であるか否かを判断する材料として生体検知情報を利用する場合を想定した。しかし、生体検知情報に有意な個人差が存在するケースにおいては、「生きている人間」の中でも特定の属性を有する人間か否かの認証の手段として生体検知機能を利用することも可能であると考えられる[14]。このような生体検知機能は、生体特徴情報

[14] 例えば、比良田ほか[2005]においては、生体検知情報（ここでは脈波）の個人差を考慮し

に基づく本人確認の機能を補完するものとして利用することができると考えられる。こうした生体検知機能の利用の可能性について検討することも有用であろう。

（ニ）マルチモーダル認証との差異

本稿では生体検知機能を対象としたが、身体的特徴の偽造に対する他の対策手法としてマルチモーダル認証を挙げることができる。マルチモーダル認証における身体的特徴の偽造を想定したセキュリティ評価に関しては、筆者らが知る限りこれまで公表されていないようである[15]。このため、マルチモーダル認証をセキュリティの観点から評価していくことが求められる。具体的には、生体検知機能を搭載したユニモーダル認証との関連性に着目した次のような課題が挙げられる。

【各手法が有効に機能するための条件の検討】

マルチモーダル認証と生体検知機能を搭載したユニモーダル認証を比較すると、どちらも生体に関する複数の情報を手掛かりとして個人の認証を行う手法と位置づけることができる。ただし、各手法が有効に機能するための条件には差異が存在する可能性もある。

生体特徴情報が偽造可能となってしまう状況を想定した場合、各生体特徴情報による照合がすべて成功したときにのみ、特定の個人であるとの判定結果を出力するという形態のマルチモーダル認証が採用されることになると考えられる。この場合、マルチモーダル認証が有効に機能するための条件として、少なくとも 1 種類の生体特徴情報が偽造困難であることが求められる。これに対し、3 節（2）**イ**.（**ロ**）における要件 1 を満足するユニモーダル認証においては、上記の状況を想定した場合においても有効に機能するためには、生体特徴情報と生体検知情報のいずれかが偽造困難であることが必要となる。

これらの手法については、偽造可能な生体特徴情報以外の情報（生体特徴情報、あるいは、生体検知情報）の偽造の困難性の度合いが、生体認証シス

た生体検知の仕組みが記述されている。比良田ほか[2005]の方法は、パルス・オキシメータによって測定された各個人の脈拍の情報を生体特徴情報や個人識別用の ID とともにテンプレートに記録し、認証時に測定される脈拍の情報と比較することによって生体検知を実施しており、生体特徴情報（ここでは、指紋や指静脈パターン）による本人確認の機能を補完したかたちとなっている。

15 マルチモーダル認証を複数のユニモーダル認証の組合せと位置づけるならば、ユニモーダル認証の評価に注力すればよいという考え方もあり得る。

テム全体のなりすましに対する安全性の強度に影響を与えるものと思われる。ただし、生体検知機能を搭載したユニモーダル認証には、「攻撃者が自らの生体を提示することで生体検知をクリアする」という特有の脅威が存在し、こうした脅威に対抗するための条件が必要と考えられる。生体認証システムが有効に機能するための条件を導出する際に、本稿での検討結果を参考にすることも可能であろう。この場合、生体検知機能を搭載したユニモーダル認証システムが完全同一型に属することを条件として挙げることも考えられる。

このように、各手法が有効に機能するための条件の差異をより明確にすることができれば、両者をどのように使い分けることが適当か、すなわち、どのような環境下であればマルチモーダル認証を利用した方が望ましいかについての知見が深まると考えられる。また、同時に、生体検知機能を搭載したユニモーダル認証の守備範囲も明らかになってくるものと思われる。

【各手法における効果の差異に関する検討】

生体検知機能を搭載したユニモーダル認証とマルチモーダル認証に関して、要求される条件の差異だけでなく、それらの効果の差異についても検討することが有用であると考えられる。両者を比較すると、次の 2 点において差異が存在することに気づく。

第 1 に、認証に利用される情報の関係における差異である。マルチモーダル認証においては、「仮にいずれか 1 つの生体特徴情報が人工物等によって偽造可能となってしまう状況に陥ったとしても、その影響を受けないであろう」と予想される生体特徴情報を複数組み合わせて利用することが望ましいと考えられる。これに対して、生体検知機能を搭載したユニモーダル認証においては、読み取られた生体特徴情報が生きている人間によって提示されたものであるか否かを確認する必要があるため、生体特徴情報と強い対応関係をもつ生体検知情報を利用されるケースが望ましいと考えられる。

第 2 に、認証の対象をどの程度絞り込むかにおける差異である。マルチモーダル認証では、基本的には複数の生体特徴情報がいずれも個人を特定するために利用されるのに対し、生体検知機能を搭載したユニモーダル認証においては、生体検知情報は生きている人間というグループを特定するために利用されるという差異が存在する。

こうした実現形態における差異がなりすましへの耐性にどのような影響を与えるかについて検討することが考えられる。攻撃者は、なりすましを試みる際に、生体特徴情報と生体検知情報をすべて偽造することが求められるが、こうした攻撃の実現可能性が各手法において変わってくる可能性がある。

上記の検討によって、マルチモーダル認証と生体検知機能を搭載したユニモーダル認証の効果の違いが明確になると思われる。その結果、生体認証システムのユーザは、どちらの認証手法を選択すればよいかについて、より多くの情報を利用しながら意思決定を行うことができるようになるであろう。

ロ．運用面における課題

（イ）人間による監視の有効性評価

生体特徴情報の偽造によるなりすましへの運用面からの対策手法として、人間による登録・認証プロセスの監視が挙げられる。2 節（3）**ロ．（ハ）**において説明したように、本対策手法には、生体認証システムの技術仕様を変更することなく実施することが可能であるため、既に導入した生体認証システムへの適用可能性という点で有用であると考えられる。

ただし、効果を期待できるのは人間の目でみて判断できる範囲に限定されるため、生体特徴情報の種類によっては、不正行為を検知することが困難なケースも考えられる。このため、人間による監視がどのような生体認証システムにおいて有効に機能するかに関して検討を深めることが今後の課題の 1 つとして挙げられる。

（ロ）生体検知機能の検討結果に関する情報共有の場の整備

生体検知機能も、生体認証システムと同様に、オープンな場において研究成果を発表し議論する状況を醸成することが求められる（宇根・松本 [2005]）。従来から、生体検知機能については、学会等において議論されることも少なく、生体認証システムの提供者側からの情報提供も非常に限定されているといわれている。そのため、金融業界をはじめとする生体認証システムのユーザは、自発的に生体認証システムの安全性を評価・比較することが困難であるのが実情である。生体認証システムを安定的かつ長期的に利用していくためには、外部の専門家等の第三者による客観的な評価を参考にすることが重要である。

まずは、生体認証システムのセキュリティ・レベルを損なわないと考えられる範囲で、学会等を中心に生体検知機能の研究成果に関する情報を共有し、議論する枠組みを検討していくことが重要であろう。

（ハ）生体検知機能の観点で拡張性のあるシステム設計

生体検知機能は生体認証システムの一部であり、致命的なセキュリティ・レベルの低下（生体検知機能の危殆化）が将来発生する可能性を否定することができない。したがって、現在搭載している生体検知機能の実現方式を別の方式に比較的容易に取り替えられるようにしておくことが重要である。ただし、ど

のような生体検知情報であれば、そうした取替えや更新が比較的容易であるかについては、学会等において議論されているとはいえない。拡張性を意識したモジュールの設計手法等に関する研究が今後望まれる。

6．おわりに

生体認証技術は、高い安全性を持つ個人認証技術として認識され、金融分野をはじめとする幅広い分野において普及しはじめている。しかし、ある一部の生体認証システムが生きている人間と同様の生体特徴情報を備えた人工物に対して脆弱であるという研究成果が複数発表されたことから、身体的特徴の偽造を考慮した技術設計が必要不可欠となった。このような脆弱性に対しては、認証の対象となっているのが生きている人間であることを確認する生体検知機能の利用が有力な対策と考えられている。しかし、生体検知機能の実現方式をセキュリティの観点から分析・評価した結果がほとんど公表されていないため、既存の生体認証システムのセキュリティ・レベルを評価することが困難であるほか、どのように生体認証システムを構築すれば安全となるのかが不明確となっているのが実情である。

本稿では、生体検知機能のセキュリティ評価に関する検討の端緒として、身体的特徴の偽造によるなりすましを脅威として想定したうえで、生体検知機能に求められるセキュリティ要件を導出した。さらに、セキュリティ要件の達成度合いを評価する方法として 2 つの評価軸を設定し、それを用いて生体認証システムを分類する方法を提案した。生体検知機能がその役割を十分に発揮するためには、生きている人間から読み取る情報としてどのようなものを利用すれば偽造に対して安全性を確保できるか（生体検知情報の偽造の困難性）という観点からの検討だけではなく、生体特徴情報とどのように組み合わせるか（生体検知情報を読み取る部位やタイミングが同一か否か）という観点からの検討も必要であることを示した。

また、生体認証システムを今後長期間にわたり安定的かつ安全に運用していくためには、顕現化した脆弱性だけでなく、未知の脆弱性についても将来顕現化することを想定し、新たな脆弱性への体制整備を進めておくことが必要である。システム管理者の観点からみた具体的な対策方針としては、拡張性の高いシステムの採用、情報の収集・分析を行う体制の整備、脆弱性の影響等に関する情報の適切かつ迅速な提供が挙げられる。こうした点に留意し、今後も生体認証技術とその脆弱性に関する研究動向に引き続き注目していく必要があろう。

以　上

【参考文献】

上山直樹・林 正明、『熱伝導指紋センサおよび該熱伝導指紋センサを用いた生体検知装置』、特開 2003-290177、公開日：2003 年 10 月 14 日

宇根正志・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、35～84 頁

小田高広、『アイリスコード生成装置およびアイリス認識システム』、特許第 3315648 号、発行日：2002 年 8 月 19

笠井英治、『生体検知装置』、特許第 3484355 号、発行日：2004 年 1 月 6 日

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、「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

草刈 高・脇山浩二、『虹彩認証装置及び虹彩撮像装置』、特開 2003-30659、公開日：2003 年 1 月 31 日

栗田真嗣・松山悦司・田井克樹・堀 淳史・藤枝一郎、「可視～近赤外 LED を備えた指紋センサによる生体識別」、『2005 年電子情報通信学会総合大会講演論文集』、A-7-6、電子情報通信学会、2005 年

小林 充、『生体検知センサ』、特開平 8-350779、公開日：1998 年 7 月 14 日

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

小山武志、『生体検知装置』、特許第 3620558 号、発行日：2005 年 2 月 16 日

情報処理推進機構、『各国バイオメトリクスセキュリティ動向の調査』、2004 年

――――、『バイオメトリクス評価に関する調査』、2005 年

スン・ジ・ミン、ジャン・ジン・チャイ、『虹彩認識システムの偽造判別方法』、特許第 3312303 号、発行日：2002 年 8 月 5 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

――――、「解説：バイオメトリック認証技術の現状」、『情報技術標準 NEWSLETTER』No. 66、情報処理学会、2005 年、12～14 頁

田井克樹・松山悦司・栗田真嗣・堀 淳史・藤枝一郎、「指紋画像の色変化に基く生体識別と人工指」、『2005 年電子情報通信学会総合大会講演論文集』、A-7-7、電子情報通信学会、2005 年

滝口清昭、『生体パターン検出方法及び生体パターン検出装置、生体認証方法及び生体

認証装置』、特開 2003-331271、公開日：2003 年 11 月 21 日

長子欣彌・兼田祐輔、『生体認証装置』、特許第 3396680 号、発行日：2003 年 4 月 14 日

特許庁、『平成 16 年度標準技術集：新世代電子時計の基礎技術とその外延』、2005 年 a

――、『平成 16 年度標準技術集：バイオメトリック照合の入力・認識』、2005 年 b

日本工業標準調査会、『JIS TR X0100: 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

日本自動認識システム協会、『平成 16 年度基準認証研究開発委託事業-2：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』、2005 年

橋本成広、『生体計測工学入門』、コロナ社、2000 年

日立製作所、「バイオメトリクスセキュリティ評価基準の研究開発」、『平成 15 年度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（平成 15 年度経済産業省委託事業成果）』、日本自動認識システム協会、2004 年、分冊 A

比良田真史・瀬戸洋一・磯辺義明・三村昌弘・高橋健太、『生体検知方法』、特開 2005-46234、公開日：2005 年 2 月 24 日

藤枝一郎・栗田真嗣・松山悦司・堀 淳史、「指紋画像から抽出する生体識別信号」、『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 3 回研究発表会予稿集』、電子情報通信学会、2004 年、211～215 頁

――――・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

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・鉢蝋拓二・田辺壮宏・森下朋樹・佐藤健二、「バイオメトリクスにおける生体検知と登録失敗―静脈認証に関する速報―」、『電子情報通信学会技術研究報告』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（Part 2）―静脈認証システムに関する研究―」、『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

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-Ⅱ、No. 5、電子情報通信学会、2003 年、678～687 頁

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）

山越憲一・戸川達男、『生体用センサと計測装置』、コロナ社、2000 年

American National Standards Institute, *ANS X9.84: Biometric Information Management and Security for the Financial Services Industry*, 2003.

Biometric Working Group (BWG), Biometric Security Concerns, V1.0, 2003. (http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf, access date: May 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 Verlag, 2003.

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.

Derakhshani, Reza, "Spoof-proofing Fingerprint Systems using Evolutionary Time-Delay Neural Networks," *Proceedings of IEEE CIHSPS 2005 Conference*, 2005.

――――, Stephanie A. Schuckers, Lawrence Hornak and Larry O'Gorman, "Determination of Vitality From A Non-Invesive Biomedical Measurement for Use in Fingerprint Scanners," *Pattern Recognition*, Vol. 36, No. 2, 2003, pp. 383-396.

Hong, Lin and Anil K. Jain, "Multimodal Biometrics," Biometrics: Personal Identification in Networked Society, Anil K. Jain, Ruud Bolle and Sharath Pankanti eds., Kluwer Academic Publishers, 1999, pp.327-344.

International Biometric Group (IBG), *Liveness Detection in Biometric Systems*, 2003. (http://www.ibgweb.com/reports/public/reports/liveness.html, access date: January 20, 2005)

Kallo, Peter, Imre Kiss, Andras Podmaniczky and Janos Talosi, "Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus," Dermo Corporation, Ltd., U. S. Patent 6,175,641, 2001.

Lapsley, Philip Dean, Jonathan Alexander Lee, David Ferrin Para Jr. and Ned Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," SmartTouch LLC., U. S. Patent 5,737,439, 1998.

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)

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," *Proceedings of the Conference Optical Security and Counterfeit Deterrence Techniques IV*, *Part of IS&T/SPIE's Electronic Imaging 2002*, 2002. (http://cryptome.org/gummy.htm, access date: February 10, 2005)

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 Oostrom, Hans, and John G. Harris, *Biomedical signals: measurement and processing*, 1997. (http://needle.anest.ufl.edu/anest4/hans/EEL4930/, access date: April 14, 2005)

Osten, David W., Hatim M. Carim, Micheal R. Arneson and Bradford L. Blan, "Biometric, personal authentication system," Minnesota Mining and Manufacturing Company, U. S. Patent 5,719,950, 1998.

Prabhakar, Salil, Sharath Pankanti and Anil K. Jain, "Biometric Recognition: Security and Privacy Concerns," *IEEE Security and Privacy Concerns*, March/April 2003, pp. 33-42, 2003.

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, 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: August 2, 2005)

Thalheim, Lisa, Jan Krissler and Peter-Michael Ziegler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test," *c't*, p. 114, 2002. (http://www. heise.de/ct/english/02/11/114, access date: February 10, 2005)

Toth, Bori, and Ulf Cahn von Seelen, "Liveness Detection for Iris Recognition," *The Presentation Sheet of NIST Workshop, Biometrics and E-Authentication over Open Networks*, 2005.

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.