バイオメトリック認証の脆弱性と生体検知機能

日本銀行
宇根正志

1 本格化しはじめたバイオメトリック認証の利用

バイオメトリック認証を実現するシステム（以下，バイオメトリック認証システムと呼ぶ）が，本特集号の他の論文で示されているように，さまざまな分野で本格的に利用され始めている。金融分野に目を向けると，2004年秋に，一部の銀行が手のひらの静脈パターンを利用したバイオメトリック認証システムを顧客の本人確認の手段として採用した。その後，いくつかの金融機関が同様の目的でバイオメトリック認証システムを導入している[6]。

こうした動きを踏まえると，バイオメトリック認証は金融分野で今後普及し，本人確認手段として重要な位置を占めるようになる可能性が高いと思われる。バイオメトリック認証システムを長期間安定的かつ安全に運用していくことが，同システムのユーザあるいは社会一般から要請され，適切なセキュリティ対策の実施が一層重要となっているといえよう。そのためには，バイオメトリック認証システムにどのような脆弱性が存在するかを見極め，脆弱性を発見した場合にはそれを軽減・解消する努力を継続していくことが求められる。

本稿では，バイオメトリック認証システムの脆弱性，とりわけ，偽造された身体的特徴を誤って受け入れてしまうという脆弱性に焦点を当て，代表的な対策である生体検知の手法と今後の課題について説明する。

なお，本稿における意見は，筆者個人に属し，日本銀行および金融研究所の公式見解を示すものではない。

2 バイオメトリック認証システムとその脆弱性

2.1 脆弱性の種類

バイオメトリック認証システムは，個人に固有の身体的特徴（指紋，虹彩，血管パターン等）や行動的特徴（声紋，動的署名，キー・ストローク等）を用いて自動的に個人を認証することを目的としている。こうしたシステムで想定される主な脆弱性としては，第三者へのなりすましにつながるものと，システムのサービス妨害につながるものが挙げられる。具体的な脆弱性については日立製作所の報告書[9]で網羅的に整理されており，なりすましにつながる脆弱性は**表1**のように整理されている。本稿では，システムによって読み取られる，身体的特徴や行動的特徴を反映するアナログ・データを生体特徴情報と呼ぶが，仮に特定の個人の生体特徴情報を別の個人が偽造して提示可能であったならば，個人を認証することができなくなってしまう。これは，表の「偽生体情報」と呼ばれる脆弱性に対応する。この脆弱性は，いくつかの商用製品に実際に存在することが既に実験で確かめられており，バイオメトリック認証システムを導入する際には考慮することが求められる[3]。

2.2 人工物による生体特徴情報の提示

生体特徴情報の偽造の脆弱性についての体系的な研究結果として，横浜国立大学大学院の松本勉教授の研究チームによる研究がよく知られている。松本教授らは，指

紋や虹彩といった身体的特徴を模倣した特徴を有する人工物から生体特徴情報を偽造・提示し，それが市販の照合装置に受け入れられるか否かを実証するという試みを2000年ころから行っている。これまでに，指紋，虹彩，静脈パターンを利用した複数の照合装置を対象に実験を行い，その結果を情報処理学会や電子情報通信学会の研究会等に報告している。また，最近では，松本教授らが実施した実験の追試が海外の研究者によって行われており，その結果をインターネット上からも入手可能であるなど，類似の研究が世界的な広がりをみせている[3)]。

(1) 指紋

まず指紋に関して，松本教授らは，シリコーン・ゴムやゼラチンを材料として人工指を作製し，その表面に形成した凹凸のパターンによって偽の指紋を指紋照合装置に提示するという方法で一連の実験を行っている[15)]。人工指は，実際の人間の指やガラス等に残留した指紋（ディジタル・カメラ等によって撮影）から型を作製し，その型にゼラチン等を流し込むという方法で作製されている。実験対象となった約20の指紋照合装置は，いずれも，主にパソコンや携帯電話のログイン時における本人確認等の用途で市販されているものであり，指をセンサ面に押し付けるタイプのものや，指をセンサ面上で滑らせて指紋を読み取るタイプも含まれている。また，これらの装置における指紋読取や照合の方式は多岐にわたっており，読取方式としては，静電容量式，光学式，感熱式，感圧式等が含まれているほか，照合方式としては，マニューシャ方式，パターン・マッチング方式，周波数解析方式等が含まれている。本物の指紋を登録した後に人工指で偽の指紋を提示するという試行を各装置において100回ずつ繰り返したところ，いずれの装置においても，平均して6割以上の確率で一致と誤って判定されたと報告されている。

(2) 虹彩

虹彩は，眼の黒い部分のうち瞳孔の外側に位置するドーナツ状の部分のことである。虹彩には瞳孔を開閉する機能があり，その筋肉の皺のパターンが個人を認証する際に利用される。松本教授らは，赤外線カメラ等を用いて虹彩のパターンを含む眼画像を撮影し，画像補正を行

表1　なりすましにつながる主な脆弱性

脆弱性の名称	概要
他人受入	ある個人の生体特徴情報を他の個人のものとして偶然受け入れてしまう。
狼	複数のテンプレートと高確率で一致と判定される生体特徴情報をもつ利用者（狼）が存在する。
子羊	複数の生体特徴情報と高確率で一致と判定されるテンプレートをもつ利用者（子羊）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	物理的に偽造された生体特徴情報を受け入れてしまう。
公開	生体特徴情報を本人の同意なく容易に他人に渡してしまう。
推定	生体特徴情報推定の手がかりとなるテンプレートや照合結果を第三者に渡してしまう。
利用者状態	生体特徴情報が自身の事情で変化し,誤って受け入れなくなってしまう。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てしまう。
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ってしまう。
登録	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できてしまう。
代替手段	本人確認の代替手段のセキュリティが生体認証に比べて低くなってしまう。
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	生体特徴情報の読取センサが露出し,生体特徴情報の入手や破壊の対象となってしまう。
構成管理	システムを構成する要素間の整合性が取れていない場合がある。

備考：参考文献9）をベースに作成。表中の「生体特徴情報」は，身体的特徴や行動的特徴を反映するアナログ・データを意味する。

ったうえで上質紙にカラー印刷して人工虹彩を作製するという手法を採用して実験を行っている[12, 13]。人工虹彩による照合実験では，人間の眼から直接虹彩のパターンを採取して虹彩照合装置に登録したうえで，人工虹彩によって提示された虹彩のパターンと照合するという処理が100回繰り返して行われた。実験対象には，主に端末へのログイン時における本人確認の用途で市販されている2機種（A，Bと呼ぶ）と，主にゲートにおける本人確認の用途で市販されている1機種（Cと呼ぶ）が選ばれており，AとBにおいては平均8割以上の確率で一致と誤って判定され，Cにおいては平均1～4割程度の確率で一致と判定された旨が報告されている。

(3) 静脈パターン

静脈パターンを用いる照合装置に関しては，松本教授らは，生体でない物質の内部構造が静脈パターンとして登録されるか否かを1種類の照合装置において実験している[14]。実験の対象となった照合装置は，赤外線を指先に当てて指内部の静脈のパターンを読み取って照合するというものであり，市販されている装置である。松本教授らは，照合装置に提示する生体でない物質として，安価に入手可能な野菜のダイコンと人工雪材（エポキシ樹脂を加えたもの）を選び，それぞれ100回の登録処理を試みた。その結果，いずれの物質を利用した場合も90回以上登録に成功した旨が報告されている。

3 生体検知

3.1 生体検知機能とは

偽造された身体的特徴を受け入れてしまうという脆弱性への代表的な対策として，生体検知機能を利用することが挙げられる。生体検知機能は，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と定義することができる[2]。生体検知機能を実現する際には，一般に，被認証物（人工物の場合もありうるため，あえて「被認証物」と記す）から何らかの情報（以下，生体検知情報と呼ぶ）を読み取り，その情報に基づいて被認証物が生きている人間か否かを確認するという方法が採用されているようである。生体検知情報は，生体特徴情報とは別に読み取られるケースのほかに，生体特徴情報と同時に読み取られるケースもある。

3.2 既存の生体検知手法

実際に生体検知機能を実現する手法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の中からいくつか紹介する。2節で取り上げた指紋，虹彩，静脈パターンに対応させて，皮膚，目，血管から生体検知情報を読み取る手法をいくつか紹介する。

(1) 皮膚

人間の皮膚の表面（表皮）や内部組織（真皮）の電気特性や光学特性を利用した生体検知手法が提案されている。

①電気特性

電気特性を利用する手法としては，皮膚の静電容量を手掛かりとするものや，インピーダンス（交流抵抗）を手掛かりとするものが挙げられる。静電容量は単位電位あたり蓄えられる電荷量であり，人間の皮膚はシリコーン樹脂等の絶縁体に比べて高い静電容量を有することが知られている。静電容量を利用する手法としては，例えば，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が構成されるようにして，その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ものが挙げられる[8]。測定された周期が一定範囲に収まるならば，被認証物が生きている人間であると判定する。また，インピーダンスを利用する手法としては，被認証物に2つの電極を接触させ，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計測し，計測した周波数が一定の範囲内に収まるか否かによって判定を行うというアイデアの手法が提案されている[1]。

②光学特性

光学特性を利用する手法としては，皮膚に光を照射し，生きている人間に固有の光の反射・透過・散乱が皮膚の表面や内部で発生するか否かに着目するというアイデアに基づく手法が提案されている。例えば，光を一定方向に偏光させて被認証物に照射したうえで，その反射光や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，各光量を比較

するという手法が挙げられる[5]。これは，生きている人間からの反射光には他の物質に比べて偏りが少なく，偏光フィルタを通した光の光量の偏りが相対的に小さくなる傾向にあるという性質を利用している。また，波長の異なる複数の光を照射し，それぞれの反射光の光量を測定することによって生体検知を行うという手法も提案されている[16]。この手法では，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等の光量をあらかじめ測定しておき，認証時に測定したものと統計的な手法を用いて比較することによって生きている人間か否かを測定する。このほか，センサ面等に押し付けられた皮膚の色の時系列変化を手掛かりに生体検知を行う手法も提案されている[11]。

(2) 目

目もさまざまな生体検知情報の源である。例えば，目に照射した光の光量に応じた瞳孔のサイズの変化，瞳孔における光の反射の有無や位置，いわゆる赤目現象（網膜の血管を流れる血液の色を反映した光が反射して，動向の部分が赤く輝いてみえる現象）の発生の有無等を手掛かりにするもの等が挙げられる。このうち，瞳孔のサイズ変化に着目した手法は，照射される光が強いと瞳孔が収縮し，逆に光が弱いと瞳孔が拡大するという生体反射を利用するものである[7]。照射する光の光量を連続的かつランダムに変化させ，そのパターンと整合的に瞳孔のサイズも変化するか否かを確認することによって，被認証物が生きている人間か否かを検証するというアイデアである。本手法では，瞳孔の変化を誘発する光として可視光を，目の画像を撮影して瞳孔のサイズを測定するための光として赤外光を照射する。また，赤外光の複数の光源を準備し，それらが点灯するパターンと反射光のパターンを比較して生体検知を行う手法も提案されている[4]。

(3) 血管

血管を生体検知情報の読取部位とする手法としては，心臓の収縮による血液の圧力変化が血管に伝わっていくときに発生する波動である脈波を計測する手法が代表的なものとして挙げられる。脈波を測定する代表的な手法としては，血管に特定波長の光を照射して，その光の透過・反射の度合いから酸素飽和度を測定し，酸素飽和度の変化から血流を捕捉するという手法が知られている[10]。酸素飽和度は，血液中の総ヘモグロビン量に占める酸化ヘモグロビン（酸素と結合しているヘモグロビン）の割合であり，酸化ヘモグロビンや還元ヘモグロビン（酸素と結合していないヘモグロビン）がそれぞれ特定の波長の光を吸収しやすいという性質を有している。そこで，これらの波長の光を照射し，その吸収度合いを反射光や透過光から時系列で測定して脈波を計測することができる。

4　生体検知を巡る今後の課題

3.2節で紹介したように生体検知の手法としてさまざまなものが既に提案されているが，生体検知手法を利用しようとしても，どのくらいの精度で生体検知が可能なのか，また，生きている人間以外（例えば人工物）を使って意図的に生体検知情報を偽造して提示するという攻撃に対してどの程度安全なのかが，筆者が知る限り，ほとんど明らかになっていない。生体検知の手法はバイオメトリック認証システムにおける情報セキュリティ対策の1つであり，本手法を採用するか否かを適切に判断する際には，手法の導入に伴って発生するコストとその手法から得られる便益（なりすまし等の防止）の比較衡量によって決定することが望ましい。現状のように生体検知の効果が不明なままであると，本手法導入時に考慮すべきコスト・便益の比較を実行困難な状況が続き，生体検知手法導入に関する意思決定も適切に実施できない可能性が今後も残る。こうしたことから，生体検知の手法の認証精度評価とセキュリティ評価に関する研究の進展が望まれる。

生体検知手法の評価研究を進めるにあたっては，バイオメトリック認証システムのユーザの視点からは，学会等のオープンな場で研究成果が発表され議論されるようになることが望まれる。生体検知に関する研究は，学会等において議論されることは稀であり，各企業内に閉じたかたちで進められるケースが多いとみられる。このため，生体検知手法の効果や実現可能性の最先端の状況をユーザが自分で理解することは困難であるのが実情と思われる。たとえ，生体検知手法に関して各種の評価が今

後行われたとしても，それがオープンな場で公表されなければ，ユーザは生体検知手法の客観的な評価結果を参照することができず，生体検知手法の採否について自ら適切に検討・判断することも容易でないと考えられる。また，ユーザ側にも，そうした場に積極的に参加し，バイオメトリック認証システムを利用する際の問題点等を提示し，研究者や開発者と情報や意見を交換していくことが求められるといえよう。

その他の技術的な課題を参考文献2）に整理しているので，興味のある読者は参考文献2）の宇根・田村論文を参照されたい。

参考文献

1）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
2）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，1～56頁，2005年12月
3）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，35～84頁，2005年7月
4）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日
5）加藤雅之ほか，『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
6）金融情報システムセンター，「第10回コンピュータシステムの安全性対策状況調査報告書」，『金融情報システム平成17年11月増刊60号』，2005年11月
7）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
8）小山武志，『生体検知装置』，特許第3620558号，発行日2005年2月16日
9）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，分冊A，2004年
10）比良田真史ほか，『生体検知方法』，特開2005-46234，公開日2005年2月24日
11）藤枝一郎ほか，「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，211～215頁，2004年
12）松本勉・平林昌志，「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，187～192頁，2003年
13）松本勉ほか，「虹彩照合技術の脆弱性評価（その3）」，『2004年暗号と情報セキュリティシンポジウム予稿集』，電子情報通信学会，701～706頁，2004年
14）松本勉ほか，「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，81～82頁，2005年
15）T. Matsumoto, et al., “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*, pp.275-289. 2002.
16）K. A. Nixon, et al., “Novel spectroscopy-based technology for biometric and liveness verification,” *Biometric Technology for Human Identification, Proceedings of SPIE*, Vol. 5404, pp.287-295, 2004.

■ Vulnerability of Biometric Authentication and Liveness Detection

■ Masashi Une

■ Deputy Director, Center for Information Technology Studies, Institute for Monetary and Economic Studies, Bank of Japan

■ We introduce recent research results regarding a vulnerability of biometric authentication systems that the systems falsely accept a forged biometric sample presented by artifacts. Furthermore,we describe several liveness detection methods as one of major countermeasures against the vulnerability and show future research topics on the liveness detection methods.

ウネ　マサシ
所属：日本銀行　金融研究所
情報技術研究センター　企画役補佐
連絡先：〒103-8660　東京都中央区日本橋本石町2-1-1
Tel. 03-3277-3023　Fax. 03-3510-1265
E-mail：masashi.une@boj.or.jp
経歴：博士（工学）。現在，金融分野と関連が深い情報セキュリティ技術の調査・研究等に従事。情報処理学会会員。