

「脱パスワード」から「ゲートレス社会」の実現まで バイOMETRICS認証の可能性

バイOMETRICS認証（生体認証）はパスワードに代わる認証手段として長い間期待されており、スマートフォンのロック解除に指認証や顔認証が標準装備される等近年その利用が拡大している。最近では認証手段としての利用にとどまらず、より便利なサービスを提供するためにさまざまな領域でバイOMETRICS認証を取り入れる動きも出始めている。

1. パスワードの限界

パスワードの脆弱性はもう長いこと指摘されているが、依然として多くのオンラインサービスではIDとパスワードによる認証が行われている。ユーザーにとってストレスなのは、パスワードを忘れてしまい利用したいサービスが利用したいときに使えないことである。ある調査によれば、ユーザーの21%が自分のパスワードを2週間以内に忘れるという¹。また、オンラインショッピングでは、パスワードの失念によって決済手続きが制限時間内に完了せず多くの商品がカートに入れられたまま放棄されている。購入放棄理由の3分の1がパスワードの失念が原因だったという調査結果もある²。このことは、IDとパスワードに頼った認証技術が事業者にとっても大きな機会的損失となりうることを示している。事業者にとっては、パスワード再発行に係るヘルプデスク関連コストも無視できない。

2. バイOMETRICS認証への期待

本人認証技術は、何をもちて本人であると判定するかという観点で次の3つに分けられる。

- ①本人だけが知っている情報（パスワード、暗証番号、秘密の質問等）を利用したもの
- ②本人だけが持っている情報（ICカード、セキュリティトークン等）を利用したもの
- ③本人固有の生体情報（指紋、虹彩、顔等）を利用したもの

このうち、③本人固有の生体情報を利用した認証方法が「バイOMETRICS認証（生体認証）」と呼ばれる。

バイOMETRICS認証は、本人になりすまして認証を突破するのが難しい。また、パスワードのように忘れてしまうことも、ICカードのようになくしてしまうこともない。こうした理由から、バイOMETRICS認証は旧来のパスワード方式やICカード等を使った認証方式に比べて、セキュリティがより強固で利便性が高いと一般に考えられている。これまでは認証精度・スピード、導入コスト等の理由で利用場面が限定されていたものの、カメラやセンサーの性能向上とAIの技術進化により、近年、認証精度・認証スピードともに大きく向上している。実用化に十分耐えられるようになってきたことで、今改めてバイOMETRICS認証が注目を浴びている。

3. バイOMETRICS認証の留意点

バイOMETRICS認証は、事前に登録した個人の特徴データと認証時に入力した特徴データを照合してスコアを算出し、あらかじめ設定した閾値（判定値）と比較することで同一人物かどうかを判定する。その評価は、全く異なる人物を本人と認定してしまう「他人受入率」と本人を他人と認識してしまう「本人拒否率」を参考にする。両者は一般にトレードオフの関係にあり、他人受入率を下げると本人拒否率が上がり利便性が低下する。一方、本人拒否率を下げると他人受入率が上がる可能性がありセキュリティに懸念が生じる。

バイオメトリクス認証はなりすましが困難であるとはいえ、誤って他人を受け入れてしまう可能性は排除できない。ゼラチンで作った指紋や3Dプリンタで精巧に作った仮面によって認証が突破されるリスクはゼロではない。また、身体的特徴は変更ができないので、一度その特徴が盗み取られたら³、同様の特徴を使った他のあらゆる認証システムで悪用されるおそれが生じる。

以上のような留意点を踏まえた上で、セキュリティと利便性のバランスを見極めて適用していくことが求められる。

4. 主なバイオメトリクス認証技術

図表1は、主なバイオメトリクス認証技術の概要をまとめたものである。バイオメトリクス認証には、指紋や静脈、虹彩等身体的特徴を利用したものと、音声や歩容（歩き方）、タイピングやスワイプの癖等行動的特徴を利用したものとがある。以下、簡単に紹介する。

(1) 指紋認証

指紋認証は読み取り装置に指を置き、読み取った指紋を事前に登録された指紋パターンとマッチングして認証を行う。技術の成熟度が高く導入コストも比較的安いことから、最も広く活用されている。課題としては、水分や傷等に弱い、偽造されやすいといったことが挙げられる。

(2) 静脈認証

静脈認証は手のひらを使う場合と指を使う場合とに大別される。赤外線カメラで血管のパターンを撮影し、事前に登録された静脈パターンとマッチングして本人であるか否かを判定する。認証精度が非常に高く、体内にある情報のため偽造が困難で外的要因による変化が少ないのがメリットで、重要施設の入退室管理やATM利用時の本人認証等に利用されている。ただし、導入コストが高いのが難点である。

《図表1》主なバイオメトリクス認証技術の概要と導入事例

分類	部位・要素	特徴	認証精度	導入例
身体的特徴	指紋	指紋のパターン	高	犯罪捜査、銀行ATMなど
	静脈	指・手のひらの静脈のパターン	高	重要施設の入退室管理、銀行ATM
	虹彩	皺のパターン	高	重要施設の入退室管理、国民登録制度
	顔	輪郭、目や鼻の配置など	高～中	出入国審査、大規模施設の入場証
	その他	掌紋、耳(音響)、体臭など	中～低	—
	音声(声紋)	話す速度・リズム・アクセントなど	中	コールセンター
行動的特徴	キーボードのタイピング	リズム、ミス傾向など	中	パソコン
	タッチスクリーンのスワイプ	開始位置、速度、圧力など	中	スマートフォン
	歩容	歩く姿勢、歩幅など	中	犯罪捜査
	その他	署名、ライフログなど	中～低	—

(注) 音声認証は身体的特徴と行動的特徴の両方を利用している。

(出典) 損保ジャパン日本興亜総研作成

(3) 虹彩認証

眼球の瞳孔の周りがある虹彩（アイリス）と呼ばれる環状の部分には細かい皺がある。虹彩認証はこの皺のパターンにより認証を行う。虹彩のパターンは複雑で経年変化が少なく、指紋認証よりも偽造が難しい。このため重要施設の入退室管理等に利用されている。インドでは国民総背番号制度「Aadhaar（アドハー）」に 13 億人の国民全ての指紋・虹彩・顔を登録するシステムを導入している。なお、虹彩認証には高解像度のカメラが必要となり導入コストが高いのがネックである。

(4) 顔認証

顔認証は、顔の形や目鼻等の位置関係を示す特徴的な点や輪郭線等を画像認識技術により抽出し、特徴点間の距離や角度、輪郭線の曲線率、顔表面の色や濃淡等により顔を識別する。登録時や認証時の利用者の負荷は少ないが、顔の角度により正しく識別できない場合があることや、加齢や生活習慣によって顔が変化することが課題である。

しかし、3D カメラで顔の微妙な凹凸まで読み取れるようになる等、近年の顔認証の技術の向上は著しい。2017 年に米国の国立標準技術研究所（NIST）が公表した動画顔認証技術のベンチマークテストで第 1 位の性能評価を獲得した NEC の顔認証システムは 99.2%の照合精度を記録している⁴。また、顔の変化についても AI が予測できるようになってきている。

認証精度や認証速度が大幅に向上したことで、厳密かつスピーディーな本人確認が必要とされる場面で顔認証を取り入れるケースが増えてきている。既に人気アーティストのライブ会場の入場ゲートでは顔認証システムが取り入れられ、チケット転売対策として有効に機能している。世界各国の空港では、出入国審査や搭乗ゲートでの本人確認に顔認証システムの導入がこの 1～2 年急速に進んでいる。2020 年の東京五輪・パラリンピックでも選手や大会関係者の会場入場時に顔認証システムが採用されることが決定している⁵。

(5) 音声認証

音声認証は、音声の周波数に着目した認証方式であり、声道の形状等個人の身体的特徴と、話す速度やリズム、アクセント等の行動的特徴とを利用して個人を識別する。マイクとソフトウェアがあればシステムを構築できるので実装コストが比較的安価である。健康状態により音声に変化することや雑音の影響を受けやすいため用途が限定されるものの、他の認証技術と違って遠隔地から認証できるため、テレホンバンキングにおける顧客の本人確認等に利用されている。

(6) 行動的特徴を利用した認証技術

キーボードのタイピングやタッチスクリーンのスワイプ・フリックの癖を利用した認証技術もある。具体的にはタイピングリズムやタイプミスの傾向、スワイプの開始・終了位置、軌跡、速度、圧力等から本人を特定する。これらは、なりすまし対策が主な用途となる。

歩容認証は、人の歩く姿を撮影した画像から歩行パターンを分析して識別する。大阪大学産業科学研究所が開発した歩容認証技術は、AI の深層学習を使うことで歩く向きが異なる場合であっても 96%の高精度で認証することに成功した⁶。歩容認証は発展途上の技術であり、現在は警察の犯罪捜査に利用されている程度であるが、同研究所は、今後より認証精度が向上すれば、商業施設等における同一人物の移動経路を解析してマーケティングや顧客に応じたサービス提供にも活用できるとしている。

最後に、ライフログ認証という風変わりな認証技術を紹介したい。これはスマートフォン等の利用履歴（ラ

イフログ) から個人の生活習慣を特定しようとするもので、東京大学大学院情報理工学系研究科ソーシャルICT 研究センターが民間会社と協働で実証実験を行っている⁷。例えば、位置情報を使って、自宅や職場等普段の行動範囲から離れていないか、いつもと違う行動をしていないかを判定する。また、利用端末、利用時間、利用内容等複数の情報から個人を認証し、クレジットカードの不正利用の発見等に活用すること等が考えられている。

行動的特徴は身体的特徴よりもさらになりすましが難しいことに加えて、本人が無意識に行っている動作を利用するためユーザーの負荷なく認証を行うことができるのが特長である。認証精度は総じて身体的特徴を利用したものに劣るものの、ユーザーに極力負担をかけない認証のニーズは高く、適切に運用すれば応用領域は広いと考えられる。

5. バイオメトリクス認証で変わる生活

バイオメトリクス認証は今後さらに様々な領域に広がる兆しが見えている。以下では、近未来の暮らしに変化をもたらすような事例を紹介する。

(1) パーソナライズ化される自動車

自動運転やコネクテッドカーなどイノベーションの波にさらされている自動車業界では、指紋認証や顔認証システムを搭載した自動車の研究開発が進んでいる。

ドイツの大手自動車部品メーカーContinentalは、クルマのキーと指紋認証を組み合わせた二段階認証によるドアロック解除やエンジン始動の仕組みの開発に取り組んでいる。従来のキーに加えて指紋を要求することで盗難防止のセキュリティを強化するのが狙いである。同社はまた顔認証による車両の「パーソナライズ化」のコンセプトを打ち出している⁸ (図表2)。これは車載カメラでドライバーの顔を識別し、シートやミラーの位置を自動的に調整し、音楽、車内温度などをドライバーに応じて設定しようとするものである。単に本人認証を行うだけでなく、本人を特定した上で最適なサービスを提供するという点が興味深い。

自動車に関しては、上記のほかにも、ライドシェアリングサービスにおける運転手の本人確認や、駐車料金の自動精算(決済)の用途で顔認証や虹彩認証の活用が検討されている⁹。また、パーソナライズ化という観点ではテレマティクス保険への影響を予想する声もある。テレマティクス保険とは、自動車に取り付けた機器・センサーから走行距離や運転特性といった運転者ごとの運転情報(データ)を保険会社が取得・分析し、その情報を基に保険料を算出する自動車保険を指す。現在のテレマティクス保険は、厳密には運転者「個人」ではなく「自動車」ごとの運転特性が保険料に反映されている。だが、バイオメトリクス認証によって実際にその自動車を運転している運転者が特定できるようになれば、運転手個人の運転特性を保険料に反映させることが可能となる。このためテレマティクス保険が真に運転手個人の運転特性を反映したものへと変わっていく可能性が指摘されている¹⁰。

(2) 顔認証決済で財布もカードもスマホも不要に

キャッシュレス化が進む中国ではALIPAY(アリペイ)やWeChatPay(ウィチャットペイ)のQR決済が普及しているが、最近では顔認証決済も広がり始めている。顔認証決済では、アリペイを運営するアリバ

《図表2》車載バイオメトリクス認証システムのイメージ



(出典) Continental ウェブサイト

傘下のスタートアップ企業 Ant Financial が杭州市の KFC（ケンタッキー・フライド・チキン）に導入した「smile to pay」が比較的良好に知られている。利用者は来店前に顔写真を登録しておき、店頭には設置されたスクリーン式販売機から商品の注文を行う。決済画面まで進むと販売機に内蔵されたカメラが利用者の顔を認識し、アリペイと連動して即時決済される。

日本では、2018年10月に富士通研究所が、顔認証と手のひら静脈認証を組み合わせた「手ぶらで決済」の技術を開発したことを発表した。深層学習（ディープラーニング）の手法で学習したモデルを使って100万人規模の処理が可能になったといい、同社では2020年度中の実用化を目指すとしている¹¹。

（3）電車の乗り降りが「顔パス」に ～ 改札ゲートがなくなる駅

ロンドンの地下鉄は、米国 Cubic Transportation System が開発した顔認証改札システム「ゲートレス・ゲートライン」を採用し、ゲートのない改札を実現しようとしている¹²。

利用者はあらかじめスマートフォンの専用アプリにクレジットカード情報を登録し、駅に設置してある端末で顔データを登録しておく。もしくは、交通系 IC カードと顔データを事前に紐付けておく。登録を済ませた利用者がゲートレス・ゲートラインに向かって進むと、壁に設置されたセンサーがポケットやバッグの中にあるスマートフォンや IC カードをキャッチし、改札レーン通過時に顔認証が行われる（図表 3）。降車駅でも同様に改札レーンを通る際に顔認証が行われ、乗車区間に応じた

運賃が自動的に精算される。無賃乗車や料金不足と判断されると赤いランプが点灯し駅員にアラートが飛ぶ。

ゲートレス・ゲートラインが完成すれば、スマートフォンや IC カードを取り出して改札機にタッチする動作が不要となるだけでなく、通常の IC カード対応の改札機よりもレーンの幅を広くとることができるため、乗客は歩行スピードを緩めることなく、よりスムーズに改札を通過できるようになると考えられている。

ロンドンの地下鉄は、今後30年で乗客が2倍になることを見越してゲートレス・ゲートラインの導入を決めたとされる。ロンドンで混雑緩和効果と利便性が実証されれば、巨大な地下鉄網を有する日本でも将来同様のシステムが導入され、顔パスで電車を乗り降りするのが当たり前になるかもしれない。

6. おわりに

技術的な課題や社会受容性などの問題は残されているものの、今後バイオメトリクス認証がさらなる技術進化と人々の意識変化によって生活の隅々に浸透していく可能性は十分に考えられる。ビジネスサイドから見れば、セキュリティ強化はもとより利便性の向上ひいては CX 向上の観点で、まずは「脱パスワード」を目指して採用を検討してみる価値がある。「脱パスワード」が広く実現した先の未来には、顔パス・指パスで施設を出入りする「ゲートレス社会」が待っているだろう。

【副主任研究員 内田 真穂】

《図表 3》ゲートレス・ゲートラインのイメージ



（出典） designboom,
<<https://www.designboom.com/technology/facial-recognition-london-underground-cubic-gateless-gatelines-10-04-2017/>>

¹ G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman and I. Martinovic, “Mobile Biometrics in Financial Services: A Five Factor Framework”, Department of Computer Science, University of Oxford, 2017.

² Mastercard, “Mastercard identity check to simplify and strengthen online shopping”, Oct.6, 2015. (visited Nov.16) <<https://newsroom.mastercard.com/press-releases/mastercard-identity-check-to-simplify-and-strengthen-online-shopping/>>

³ 事前に登録していた特徴（これを「テンプレート」という。）が外部に流出する場合と、指や顔等体外に露出した特徴が本人

の知らない間に盗み取られる場合の両方の可能性がある。

⁴ 2017年3月16日付 NEC プレスリリース<https://jpn.nec.com/press/201703/20170316_01.html>

⁵ 2018年8月7日付日本経済新聞「NEC、顔認証システムが東京 2020 オリンピック・パラリンピック競技大会関係者の会場入場時の本人確認に採用」

⁶ 大阪大学産業科学研究所「「未来科学捜査」歩容鑑定～深層学習でどんな向きの人物も認証可能に～」
<https://www.sanken.osaka-u.ac.jp/toppage/hot_topics/topics_20171108/>

⁷ 東京大学大学院情報理工学系研究科ソーシャル ICT 研究センターウェブサイト (2018年11月16日訪問)
<<http://www.sict.i.u-tokyo.ac.jp/research/lifestyle.html>>

⁸ Continental ウェブサイト (2018年11月16日訪問)

<<https://www.continental-corporation.com/en/press/press-releases/2016-12-13-highlights-ces-101510>>

⁹ Goode Intelligence, “*Biometrics for the Connected Car*”, 2017.

¹⁰ 同上

¹¹ 2018年10月4日付富士通プレスリリース「手ぶら決済に最適な非接触の生体認証融合技術を開発」
<<http://pr.fujitsu.com/jp/news/2018/10/4.html>>

¹² Wired, “*Your face could be your ticket at the Tube station of the future*”, Sep.25,2017 (visited Nov.16)
<<https://www.wired.co.uk/article/train-station-face-recognition-gateless-gate-technology>>

<参考文献>

IPA 情報処理推進機構「生体認証導入・運用の手引き」(2013年1月)