

個人情報保護委員会 事務局 御中

生体データの利用に関する動向調査 最終報告書

株式会社野村総合研究所

ICT・コンテンツ産業コンサルティング部

2025年12月26日



最終報告書サマリ

- (1) 国内外における生体データの利用動向 | 利用事例
- (1) 国内外における生体データの利用動向 | 市場規模・普及度
- (2) 国内外における生体データの技術動向
- (3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否

参考文献リスト

「本人が関知しないうちに容易に取得することが可能なデータ」として、顔特徴データが当てはまる可能性が高い。また、現時点で新たに個人識別符号として拡充すべきデータは見受けられなかった

(1)
国内外における
生体データの
利用動向

- ✓ 個人識別符号では、**指紋>DNA*>虹彩≧顔>声紋>掌紋>静脈>歩容**の順に市場規模が大きい
 - DNA・虹彩は、普及率が比較的高いだけでなく、導入・運用コストも高いため、規模が大きく出ている
 - **一般的な本人認証で用いられることが多いのは、(表皮)指紋・顔**である。両者とも1台約1,000円で導入でき、スマホ等の日常的に利用するものに搭載されていることから、普及が進んでいる
 - 歩容の商用化事例は稀であるが、さまざまな研究機関や事業者によって実証が進められている
- *DNAは法医学機関の鑑識、医療・農業分野での研究開発市場の数値が含まれる値であることに留意

(2)
国内外における
生体データの
技術動向

- ✓ ①取得に要する費用等、②本人の関知なく取得される可能性をもとに、**「本人が関知しないうちに容易に取得することが可能なデータ」かを確認**
- ✓ **顔特徴データは「本人が関知しないうちに容易に取得することが可能なデータ」と評価できる可能性が高い**

(3)
特定の個人を識別
することができる
水準での利用が
見込まれる身体
の一部の特徴に係る
データの存否

- ✓ 現行の個人識別符号には定められていないが、各国法にて言及されている身体の一部の特徴に係るデータを対象として、特定の個人を識別することができる水準での利用が見込まれるデータの存否を調査
- ✓ 一意性、不変性、普及度合い、現状のユースケース、導入・運用コスト、データ取得・識別の容易性を基に調査すると、**いずれも新たに個人識別符号として拡充すべきデータとは評価できない可能性が高い**

個人識別符号ごとに、取得に要する費用等や、本人の関知なく取得される可能性を調査。顔特徴データは、「本人が関知しないうちに容易に取得することが可能なデータ」と評価できる可能性が高い

類型	生体データ	①取得に要する費用等	②本人の関知なく取得される可能性
イ	DNA	C：費用等の制約が多い	D：非常に低い
ロ	顔特徴データ	A：費用等の制約が非常に少ない	A：非常に高い
ハ	虹彩データ	B：費用等の制約が少ない	C：低い
ニ	声紋データ	B：費用等の制約が少ない	B：高い
ホ	歩容データ	C：費用等の制約が多い	A：非常に高い
ヘ	静脈データ	B：費用等の制約が少ない	C：低い
ト	指紋データ	B：費用等の制約が少ない	C：低い
	掌紋データ	B：費用等の制約が少ない	C：低い

最終報告書サマリ | (3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否
各国法で言及のあるデータや認証用途での研究が進められているデータを対象に、個人識別手段としての精度や一般的な利用度合いを調査。現時点で新たに個人識別符号とすべきデータは見当たらない

- 網膜データ・耳音響データは一意性・不変性共に高いものの、2030年代にもあまり普及が見込めないため、現時点で個人識別符号として拡充する意義は小さい。また、網膜データは取得時のコストの高さと侵襲性*も課題である
- 脳波データは一意性・普及度合い共に高いが、不変性が低いため、一時点のデータを取得しても個人識別符号とはみなしづらい
- 筆跡データは既に普及が進んでいるが、一意性・不変性共に中程度のため、単体で個人識別符号とはみなしづらい

検討対象	①個人を識別する手段としての精度が高いか		②一般的に利用されうるか			
	一意性	不変性	普及度合い (2030年代の市場規模)	現状のユースケース	導入・運用コスト	データ取得・識別の 容易性
データ 網膜	○	○	✕ 市場データなし	✕ 本人認証用途での 実証はなし	✕ 数十～数百万円単位	✕ 侵襲性の高いスキャナの利用かつ15秒程度で取得
データ 耳音響	○	○	✕ 市場データなし	△ 認証用途での 実証が進行中	△ 商用化前だが業務用に 導入可能な価格帯を予定	○ イヤホン等で音の反響を 測定。約1秒で取得
データ 脳波	○	✕	△	△ 複数のスタートアップで認証 用途での実証が進行中	△ 商用化前だが業務用に 導入可能な価格帯を予定	△ ヘッドバンドやイヤホン等を 装着。取得時間に幅あり
データ 筆跡	△	△	○	○ 商用化が浸透	○ 市販の筆跡認証パッドは 250～500USD前後	○ 数秒間（サイン記入時間） で取得し、0.2秒間で識別

*侵襲性：生体の内部環境に外部から刺激が与えられること

最終報告書サマリ

(1) 国内外における生体データの利用動向 | 利用事例

(1) 国内外における生体データの利用動向 | 市場規模・普及度

(2) 国内外における生体データの技術動向

(3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否

参考文献リスト

(1) 国内外における生体データの利用動向 | 利用事例 | 調査の観点 (1/2)

■ 生体データ別の利用事例について、以下の項目を調査した

調査項目（大項目）	調査項目（小項目）	記載内容
基本情報	生体データを利用する企業・団体名	生体データを利用する企業・団体名を記載
	生体データを利用するサービス名・概要	生体データを利用するサービス名・概要を記載
生体データ利用の目的	生体データ利用の背景・目的	犯罪捜査・防犯・本人認証など、生体データ利用の背景・目的を記載
生体データの情報源	生体データ主体の属性	全市民・受刑者・容疑者・子どもなど、生体データ主体を記載
	生体データの出所	インターネット・民間団体・個人など、生体データの出所を記載
	生体データ取得方法	遠隔・生体データ取得専用ブースなど、生体データ取得方法を記載
	データ取得の事前告知有無・方法	事前告知の有無を確認した上で、告知を実施している場合は、告知のタイミング及び媒体等を記載
	データ取得時の本人認識有無	データ取得時に本人が認識しているかを記載
	生体データの大量取得有無	生体データを「一度」に大量に取得できるかを記載（データベースの蓄積数を記載する項目ではない）
照合用のデータベース	データ主体に関する追加情報源	(1)イ〜トに該当する生体データ、(2)生体データとして定めるべきデータの案に当てはまるもの、(3)生体データ以外のデータの三つに分けて、同時に取得されている情報源を記載
	特異性	一般目的・犯罪分野特化など、特異な点を記載
	データベースの構築経緯（法的根拠含む）	データベースの構築経緯を法的根拠の整理も含めて記載
	データベースの目的変更の有無	本来は私有財産保護目的だったが、犯罪捜査目的に変更された場合など、目的に変更が生じている場合にその経緯を記載

(1) 国内外における生体データの利用動向 | 利用事例 | 調査の観点 (2/2)

■ 生体データ別の利用事例について、以下の項目を調査した

調査項目（大項目）	調査項目（小項目）	記載内容
生体データ取得・認証の アルゴリズム	処理タイプ	1対1認証・1対多での識別・1対多の検索照合など、処理タイプを記載
	精度に関する考慮事項	人種や環境条件等により誤検知が発生した事例など、精度に関する考慮事項がある場合に記載
	技術的な安全対策	暗号化や元データの破棄など、技術的な安全対策が施されている場合に記載
生体データ利用の結果	生体データ利用の影響	直接的影響（データ主体が逮捕等）及び間接的影響（統計モデルに使用等）を記載
	自動化された意思決定の有無	生体情報からその人の属性に応じた傾向等を読み取り、自動化した対応が取られているかを記載 ※入退館管理のように、人の属性に応じた傾向等を判断する対応ではないものは非該当
	取得データの保存期間	取得データの保存期間を記載
本人請求への対応	本人請求への対応	利用停止請求・消去請求等への対応状況を記載

(1) 国内外における生体データの利用動向 | 利用事例 (1/5)

類型	技術	利用事例		
		企業・サービス名	サービス提供国	調査結果概要 (利用目的・利用データ・処理の特徴等)
イ	DNA	法科学鑑定研究所 / DNA JAPAN (子会社)	日本	犯罪捜査や身元不明遺体の同定等の法的鑑定のほか、親子鑑定・浮気調査・ルーツ検査・美容や教育目的での遺伝子検査といった私的鑑定を行っている。
		FBI「Combined DNA Index System (CODIS)」	アメリカ	犯罪捜査や身元不明遺体の同定等の法的鑑定を行っている。
		イギリス内務省「National DNA Database (NDNAD)」	イギリス	犯罪捜査等の法的鑑定を行っている。
		フランス国立法医学局「Fichier national automatisé des empreintes génétiques」	フランス	犯罪捜査や身元不明遺体の同定等の法的鑑定を行っている。
		ジェネシスヘルスケア「GeneLife」	日本	個人の体質・疾患リスク・母方祖先のルーツ等をDNA解析を用いて検査するキットを個人向けに販売している。
ロ	顔	渋谷書店万引対策共同プロジェクト	日本	渋谷3書店共同で、万引き防止を目的とした防犯カメラシステムを運用している。参加店間における共同利用データを参照し、対象者を検知すると店員に通知される。
		JR東日本 駅構内の顔認証カメラシステム	日本	JR東日本が、2021年7月に東京五輪開催に向けて、駅構内での犯罪防止を目的とした防犯カメラシステムの運用を開始した。出所者を検知対象に含んでいたことが批判され、途中で検知対象から除外した。外部企業との契約期間満了に合わせ、2025年10月に運用が廃止された。
		Rite Aid 店舗内の 顔認証カメラシステム	アメリカ	米ドラッグストアチェーンRite Aidが、万引き防止を目的とした防犯カメラシステムを運用していた。告知不十分や誤検知多発が批判され、2020年に運用が廃止された。
		キングスクロス地区における 顔認証監視システム	イギリス	キングスクロス地区開発事業者が、犯罪関連人物の検知を目的とした監視カメラシステムを運用していた。告知なしで顔認証を実施していた点が批判され、2018年に運用が廃止された。
		Clearview AIによる 巨大顔画像データベース	アメリカ	ウェブ上の公開画像から取得した巨大顔画像DBを警察等の法執行機関・政府機関に提供する検索サービスを行っている。2019年には銀行や小売業などの非政府機関の顧客が存在したが、2020年以降はこれら民間の顧客への提供は中止し、政府・法執行機関に限定している。同意なしでインターネット上の顔画像がDB化される点がプライバシー侵害であると批判されているが、行政から法執行を受けたことはない。

(1) 国内外における生体データの利用動向 | 利用事例 (2/5)

DNA

顔

虹彩

声紋

歩容

静脈

指紋・掌紋

類型	技術	利用事例		
		企業・サービス名	サービス提供国	調査結果概要 (利用目的・利用データ・処理の特徴等)
□	顔	顔・指紋・虹彩と本人情報を紐づけたインドの個人識別番号制度「Aadhaar」	インド	行政サービスの合理化や、個人情報の偽証防止の目的で導入された、顔・指紋・虹彩認証を用いた個人識別番号制度。政府による認証記録の保存期間は、サービス開始当初は5年間であったが、2018年に最高裁で違憲とされ、6ヶ月へと変更された。
		スウェーデン・シエレフテオの高校における顔認証出席管理	スウェーデン	教員の作業時間削減を目的として顔認証による生徒の出席管理を3週間、試験運用した（2019年）。保護者の同意は得ていたが、スウェーデンDPAにより、データ主体である生徒の同意を取得していないことが問題視され、同DPAと事前協議を行わなかったこと等をふまえ、GDPR違反として罰金を科された。
		Entry/Exit System (EES)	シェンゲン協定加盟国の欧州29か国	出入国審査の効率化、違法滞在やテロ等の検知を目的とした、顔・指紋認証を利用した出入国管理システム。2025年10月より出入国管理当局における運用開始。
		会員制コワーキングスペース「point0 marunouchi」における顔認証入退管理システム	日本	株式会社point0において、コワーキングスペースへの入退管理を、社員証等を用いずに顔認証のみで行うことで、会員の利便性を向上させる目的で運用している。

(1) 国内外における生体データの利用動向 | 利用事例 (3/5)

DNA
歩容

顔
静脈

虹彩
指紋・掌紋

声紋

類型	技術	利用事例		
		企業・サービス名	サービス提供国	調査結果概要 (利用目的・利用データ・処理の特徴等)
八	虹彩	スキポール空港における虹彩認証による出入国管理サービス	オランダ	スキポール空港の有料メンバーシップ制度である「Privium」にて、虹彩認証により入国手続きを迅速化するサービスを展開している。
		株式会社セフティボックス	日本	貸金庫でのセキュリティ強化を目的として、貸金庫フロアへの入退管理に虹彩認証を利用している。顔認証を選択することもできる。
		FORVIA/Smart Eye	フランス	ドライバーモニタリング用にすでに設置されているカメラを用い、虹彩・顔認証を組み合わせることで車内決済等を行うシステムを発表している。
		Mastercard/Empik/PayEye	ポーランド	虹彩・顔認証を用いた、店舗内での決済の試験運用を行っている。店舗に設置されたeyePOS端末に一目向けるだけで決済が完了する。
		Canada Border Services Agency/ U.S. Customs and Border Protection	アメリカ・カナダ	アメリカ・カナダ間の国境通過を迅速化する有料メンバーシップ「NEXUS Program」を展開しており、サービスの一つとして虹彩認証が提供されていた（～2020頃）。現在はコスト削減等を理由に顔認証に置き換わっている。
二	声紋	英国HMRC（税関）	イギリス	コールセンターでの本人確認の迅速化・簡便化を目的とした、声紋認証システムを運用している。
		Barclays（銀行）	イギリス	コールセンターでの本人確認の迅速化・簡便化を目的とした、声紋認証システムを運用している。
		インターポール （国際刑事警察機構）	イタリア・イギリス・ ポルトガル・ドイツ等	国際的な声紋認証データベースを構築し、八百長・身代金要求・テロ予告など、様々な刑事事件において、既知の犯罪者やSNS上の公開音声と照らし合わせ、傍受対象の不特定話者が誰なのかを識別するための実証プロジェクトを実施した（2014/5～2018/4：実証プロジェクトの実施期間）。各国の情報取得・共有時の透明性を担保する仕組みがないとの批判があった。
		Aculab	イギリス	コールセンター・金融サービス・車両のロック制御などで使われる声紋認証システムを提供している。合成音声や録音音声の疑いを検知する「生体認証PAD機能」が搭載されている。
		Amazon Alexa Voice ID	欧米・日本等 Alexa提供国	利用者個人の声を識別し、パーソナライズされた体験（メッセージの送信や個人スケジュールの確認、個人プレイリストの配信等）を提供するサービスを行っている。

(1) 国内外における生体データの利用動向 | 利用事例 (4/5)

DNA

顔

虹彩

声紋

歩容

静脈

指紋・掌紋

類型	技術	利用事例		
		企業・サービス名	サービス提供国	調査結果概要 (利用目的・利用データ・処理の特徴等)
ホ	歩容	警察庁科学警察研究所・ 大阪大学 八木研究室	日本	顔が不鮮明である場合の犯人の識別のため、防犯カメラからの歩容鑑定を試験運用している。
		株式会社アジラ・ 東京工業大学 篠田研究室	日本	防犯・捜査目的だけでなく、繁華街での悪質な呼び込みへの注意喚起、高齢者施設等での利用者支援、入退館管理等のユースケースを想定した歩容鑑定システムの研究開発を行っている。
		PopEyeプロジェクト	EU	シェンゲン協定域外との国境において、乗客と不法移民の識別と検証を行い、国境のセキュリティ強化とスムーズな検問を図ることを目的としたプロジェクト。カメラ・レーダー・センサーを通じた、遠隔での歩容認証・顔認証・非接触摩擦隆起認証・虹彩認証について、EU加盟国の国境管理当局が連携し、検証している。
		Software République (Slerや自動車関連メーカー6社で 構成されるモビリティシステム開発 プロジェクト)	主にフランス	車に向かって歩いてくる人の歩容パターン・顔特徴を車が読み取り、デジタルプロフィールと照合することで、キーなしで車のロックを解除するシステムを備えたコンセプトカーを発表している。
		株式会社フリックフィット	日本	スマートインソールから取得した歩行データを解析し、個人を識別することで、セキュリティ対策やスマートホーム、認知症患者の徘徊対策に繋げるシステムの開発を行っている。
ヘ	静脈	LOTTE CARD	韓国	富士通が提供する、手のひら静脈による本人認証を利用した「HandPay 決済サービス」を導入している。利用者は会計時に電話番号を入力後、手をかざすことで決済ができる。
		Sentara Health (バージニア州を拠点とする病院ネットワーク)	アメリカ	患者の取り違え防止および診療プロセスの効率化を目的とした、来院した患者を手のひら静脈認証を用いて識別し電子医療記録を呼び出すシステムを利用している。
		三井住友銀行	日本	キャッシュカードの偽造・盗難による不正引き出し防止の目的で、キャッシュカードを用いる際、従来の暗証番号に加え指静脈認証を追加したATMを導入している。
		大垣共立銀行	日本	災害時のキャッシュカードなしでのATM利用の実現を目的とし、手のひら静脈認証・生年月日・暗証番号のみでお金を引き出せるようにしたATMを導入している。
		東京大学医学部付属病院	日本	入院患者が鍵の管理をせずに快適に過ごせるよう、全病床に指静脈認証で施錠・解錠できる引き出しを導入している。

(1) 国内外における生体データの利用動向 | 利用事例 (5/5)

DNA
歩容

顔
静脈

虹彩
指紋・掌紋

声紋

類型	技術	利用事例		
		企業・サービス名	サービス提供国	調査結果概要 (利用目的・利用データ・処理の特徴等)
ト	指紋	ウォルトディズニーワールド	アメリカ	マルチデパスポートの不正利用防止を目的とし、パーク利用者が本人であることを指紋認証を用いて確認している。
		イギリス内務省	イギリス	渡航する外国人の指紋データを、本人が事前にスマートフォンカメラで撮影し、取得する試験運用を実施している。遠隔での指紋登録の実用性及びなりすまし検知性能を検証する。
		Apple	アメリカ	ロック解除、決済などに用いる指紋認証「Touch ID」を提供している。指紋データは画像ではなく数学的データとして保存され、そのデータから指紋画像を再生することはできない。
	掌紋	FBI「Next Generation Identification」	アメリカ	犯罪捜査などを目的として、大規模な指紋・掌紋・顔・虹彩データベースを構築している。検索照合の他、教師などの信頼性が求められる職に就く個人の犯罪歴通知(通知先は州教育委員会や雇用主など、認可機関のみに限定)などのサービスも展開。監視社会化への懸念、非犯罪者データも含まれることに対する批判がある。
		日立/KDDI総合研究所	日本	スマホカメラで撮影された掌紋から一時的に秘密鍵を生成する技術を開発している。決済での利用を想定した技術であり、決済時は顔認証と組み合わせ対象者を検索したのち掌紋認証を行う。(2018/10に展示された技術)

最終報告書サマリ

(1) 国内外における生体データの利用動向 | 利用事例

(1) 国内外における生体データの利用動向 | 市場規模・普及度

(2) 国内外における生体データの技術動向

(3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否

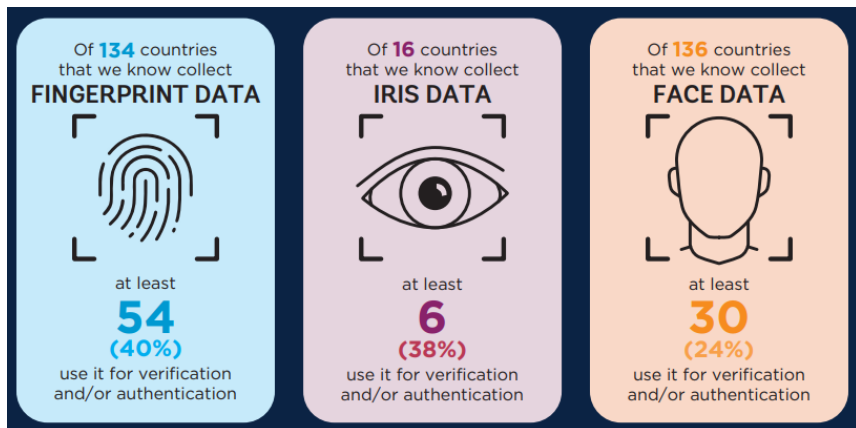
参考文献リスト

(1) 国内外における生体データの利用動向 | 生体データ別の普及度

行政機関・個人共に、虹彩認証の普及率が低い一方で、指紋・顔認証は広く普及している。
取得時の制約の少なさと、スマホ等の日常的に利用するものへの搭載が理由と想定される

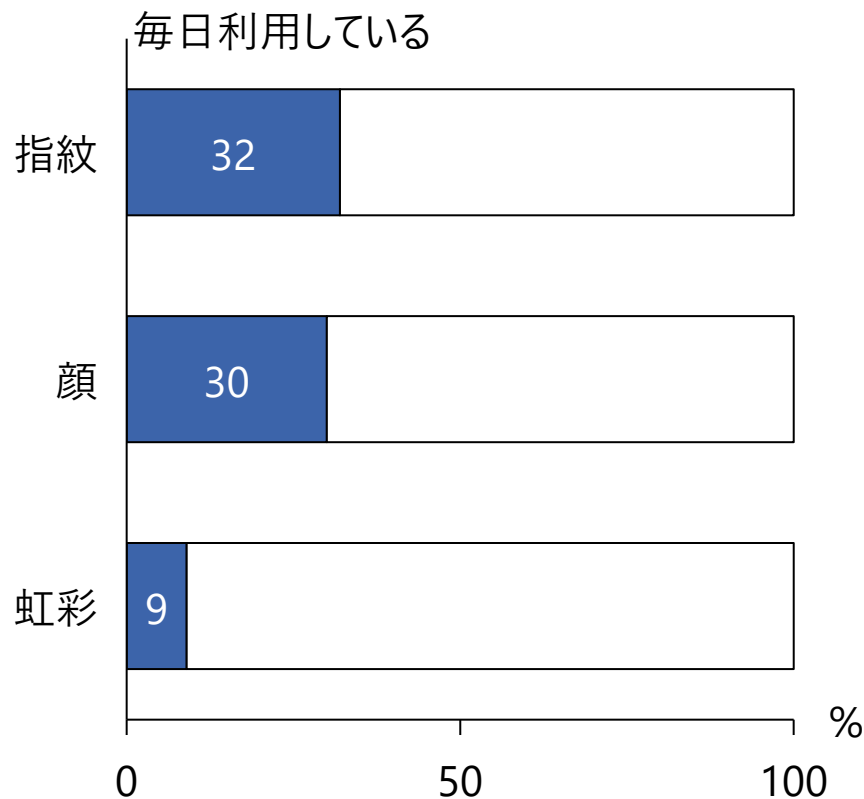
生体データを取得・利用している国数

- 2021年時点では調査対象の175か国のうち、
 - ✓ 134か国が指紋
 - ✓ 16か国が虹彩
 - ✓ 136か国が顔 のデータを取得
(国数=国内の行政・公共機関で生体データを取得している国の数)
- そのうち、個人照合/認証に使用している国は
指紋で40%、虹彩で38%、顔で24%



個人における生体データ認証の利用率

(n=1,008、米国のみ)



(1) 国内外における生体データの利用動向 | 生体データ認証市場の成長要因

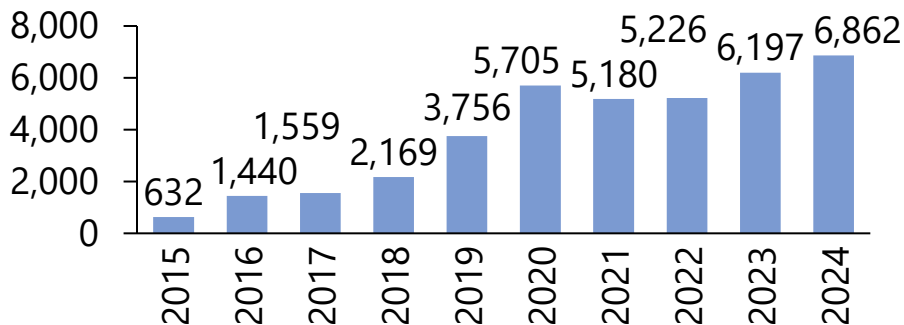
サイバー攻撃・パスワード攻撃が増加する中、セキュアな認証方式が求められていること、技術進化・市場拡大に伴い、導入コストが低下していることから、生体データ市場が拡大

サイバー攻撃・パスワード攻撃の増加

- NICTERで観測されたサイバー攻撃関連パケット数*は**2024年に6,862億パケット（2015年の11倍）**
- Microsoftによると**1日あたり6億件のID攻撃のうち、パスワードベースの攻撃が99%以上**を占めている

NICTERにおけるサイバー攻撃関連の通信数の推移

(億パケット)



* 未使用のグローバル IP アドレス宛の通信を観測することでインターネット上の不正な活動を捉えることでサイバー攻撃を観測。NICTERで観測しているダークネットの範囲に届いたパケットの個数をカウントしており、日本全体や政府機関に対する攻撃件数ではない

技術進化・市場拡大に伴う導入コストの低下

- 普及度の高い指紋・顔認証に関わる**センサーやシステムの価格は1,000円前後まで低下**
- その他データも市場拡大と共にコストが下がり、さらに市場を拡大させる循環が生じる

指紋

- 2013年発売のiPhone 5sにTouch IDが搭載
- 指紋認証センサーの平均コストは**US\$5（2013）からUS\$3（2016）に下落**（Yole調査；グローバル・表皮認証の価格）

顔

- 2017年発売のiPhone XにFace IDが搭載
- Metalenz（米）の顔認証システム「Polar ID」では、1台あたり**US\$5にまでコストを低減**
 - 光学技術の強みを活かし、顔の偏光の特徴に基づいて個人を識別
 - SamsungやQualcommとも連携

最終報告書サマリ

(1) 国内外における生体データの利用動向 | 利用事例

(1) 国内外における生体データの利用動向 | 市場規模・普及度

(2) 国内外における生体データの技術動向

(3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否

参考文献リスト

技術動向調査の目的、及び総合評価

個人識別符号ごとに、取得に要する費用等や本人の関知なく取得される可能性を調査。顔特徴データは、「本人が関知しないうちに容易に取得することが可能なデータ」と評価できる可能性が高い

- 目的：現行の個人識別符号のうち、
本人が関知しないうちに容易に取得することが可能であると評価できるデータの有無を確認すること
- 調査項目：以下4点を設定（詳細な調査項目・評価基準は[18頁及び19頁](#)ご参照）
 - ① 取得に要する費用等（金銭的費用だけでなく、時間的費用や機器の物理的制約なども含む）
 - ② 本人の関知なく取得される可能性
 - ③ 取得・利用する際のリスク
 - ④ 今後の見込み

✓ ①・②から「本人が関知しないうちに容易に取得することが可能なデータ」かを判断し、Aに近いほどその可能性が高いと評価する

類型	生体データ	①取得に要する費用等	②本人の関知なく取得される可能性
イ	DNA	C：費用等の制約が多い	D：非常に低い
ロ	顔特徴データ	A：費用等の制約が非常に少ない	A：非常に高い
ハ	虹彩データ	B：費用等の制約が少ない	C：低い
ニ	声紋データ	B：費用等の制約が少ない	B：高い
ホ	歩容データ	C：費用等の制約が多い	A：非常に高い
ヘ	静脈データ	B：費用等の制約が少ない	C：低い
ト	指紋データ	B：費用等の制約が少ない	C：低い
	掌紋データ	B：費用等の制約が少ない	C：低い

生体データの技術調査項目（1/2）

■ 以下の観点から、生体データ別に調査を行った

調査項目（大項目）	調査項目（小項目）	技術の評価の観点
① 取得に要する費用等	a. 同時取得量	○. 不特定多数から同時かつ自動的に取得可能 △. ー ×. 1対1での個別取得が前提
	b. 導入・運用コスト	○. 低（安価な設備（市販のカメラやマイク等）で対応可能） △. 中（中程度のコストが掛かる専門の設備が必要） ×. 高（高価な設備・専門人員が必要）
	c. 本人識別までの所要時間	○. リアルタイム処理が可能 △. 数秒～10秒程度を要する ×. 分析に時間や複数ステップが必要
	d. 安定取得の容易性	○. 人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい △. ー ×. 行動的特徴であるため、安定したデータを取得しにくい
	e. 商用化の度合い	○. 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 △. ー ×. 実証・実験段階であり、商用化された機器・システム・サービスは稀である ・ 前提：コストを掛ければ、誰でも認証を利用できるかを確認する項目であり、コストの高さは考慮しない
② 本人の関知なく 取得される可能性	a. 非接触取得の可否	○. 完全非接触で遠距離（5m以上）からでも取得可能 △. 非接触だがある程度の距離・姿勢条件が必要 ×. 直接的な接触・近接が必要
	b. データ取得の所要時間	○. 瞬時～数秒以内に取得可能 △. 数秒以上の静止・発声・操作などが必要 ×. 採取に手間・時間を要し、複数ステップが必要
	c. 本人操作の有無	○. 明示的な操作が不要であり、本人が気づかぬうちにデータを取得され得る △. ー ×. 明示的な操作を伴い、データを取得されていることを本人が認識する
	d. 機器のサイズ・組込可否	○. 本人が意識しないと知覚できない(目に留まらない)形でデータを取得できる △. ー ×. 本人が意識しないと知覚できない(目に留まらない)形でデータを取得できない

生体データの技術調査項目（2/2）

■ 以下の観点から、生体データ別に調査を行った

調査項目（大項目）	調査項目（小項目）	技術の評価の観点
③ 取得・利用する際の リスク	a. 特徴量データの 漏えい時のなりすまし・ 不正アクセスのリスク	○. 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクが 小さいとまではいえない △. – ×. 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい
	b. 元データの復元リスク	○. 特徴量データから元データを復元されるリスクが小さいとまではいえない △. – ×. 特徴量データから元データを復元されるリスクは小さい
	c. 元データそのものの 偽装・模倣の可否	○. 技術的には偽装・模倣が困難ではない （顔・虹彩・声紋・指紋・掌紋） △. – ×. 偽装・模倣が極めて困難（DNA・歩容・静脈） 前提：あくまで技術的に偽装・模倣が困難かどうかを確認する項目であり、 実際に認証を欺けるか、プレゼンテーション攻撃にどこまで耐性があるかは考慮しない
	d. 機微情報の推定リスク	○. 機微情報（障害・健康情報・血族情報等）を推定されるリスクが小さいとまでは いえない（○の場合、推定される情報も併せて整理する） △. – ×. 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい
調査項目（大項目）	調査項目（小項目）	調査の観点
④ 今後の見込み	a. 取得技術の革新 （センサー技術）	今後の見込みについては評価が困難なため、 取得技術・分析技術において、それぞれ先進的な研究事例を掲載
	b. 分析技術の革新 （識別精度）	

注：③・④は総合評価を置かず、参考情報として整理

(2) 国内外における生体データの技術動向 | イ：DNA (1/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	1対1での個別取得が前提	×	C 情報の取得に要する費用等の制約が多い
	b. 導入・運用コスト	- 高（高価な設備・専門人員が必要） - 根拠：個人情報を作成するには高価な試薬が必要。民間用途では、高値のまま購入する必要がある、浮気調査や親子鑑定等は1回5万円の価格帯	×	
	c. 本人識別までの所要時間	- 分析に時間や複数ステップが必要 - 根拠：最新の設備でも2時間前後かかる」とされている	×	
	d. 安定取得の容易性	人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい 【ゆらぎを生じさせる因子】 ➤ 環境条件：DNAの取得量（遺留物では取得量が少なくなる可能性が高い） ➤ 本人条件：一卵性双生児（研究レベルでは認証可能）	○	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：犯罪捜査や親子鑑定等に一般的に利用されている	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 直接的な接触・近接が必要 - 根拠：歯ブラシ・タバコの吸い殻・毛髪等で非接触で取得することも可能だが、口腔粘膜がほぼ100%の成功率であるのに対し、上記は50-70%の成功率のため、口腔粘膜の細胞や体液等から取得することを想定	×	D 本人の関知なく取得される可能性が非常に低い
	b. データ取得の所要時間	- 採取に手間・時間を要し、複数ステップが必要 - 根拠：一般的には口腔に10秒程度綿棒をこすりつけてDNAを取得	×	
	c. 本人操作の有無	明示的な操作を伴い、データを取得されていることを本人が認識する	×	
	d. 機器のサイズ・組込可否	本人が意識しないと知覚できない(目に留まらない)形でデータを取得できない	×	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の**凡例は18頁をご参照ください**

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | イ：DNA (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	—	—	—
	b. 元データの復元リスク	—	—	
	c. 元データそのものの偽装・模倣の可否	- 偽装・模倣が極めて困難 - 根拠：DNAを盗むことは可能だが、偽装・模倣したもので鑑定・認証を突破することは困難	×	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクが小さいとまではいえない - 根拠：血族情報、疾病リスクなどを推定可能	○	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	2時間以内にDNA IDを自動で生成可能な機器が開発されるなど、本人識別までの所要時間を短縮させる動きあり	—	—
	b. 分析技術の革新（識別精度）	ただし、DNAは他の個人識別符号とは異なり、犯罪捜査や浮気調査等、正確性が求められるため、所要時間の短縮ニーズは高くない	—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の[凡例は19頁をご参照ください](#)

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | □：顔特徴データ（1/2）

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	- 不特定多数から同時かつ自動的に取得可能 - 根拠：出入室管理システムは自動的に複数人の取得・認証が可能	○	A 情報の取得に要する費用等の制約が非常に少ない
	b. 導入・運用コスト	- 低（安価な設備（市販のカメラやマイク等）で対応可能） - 根拠：オフィス・学校等で導入可能な価格帯で販売	○	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：1分間に100人の識別が可能な顔認証システムが存在（※システムの性能に依存するため、必ずしもすべてのシステムでリアルタイム処理が可能ではないことに留意）	○	
	d. 安定取得の容易性	- 人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい 【ゆらぎを生じさせる因子】 ➢ 環境条件：日光、照度、照明の設置個所、遮蔽物、シャッタースピード、ブレ ➢ 本人条件：人種、マスク・サングラス等の携帯物、乳幼児、一卵性双生児	○	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：入館・入国ゲートやiPhoneのFace IDなど、商用化が進んでいる	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 完全非接触で遠距離（5m以上）からでも取得可能 - 根拠：監視カメラによる遠距離取得や、デジタル顔画像からの取得も可能（※カメラに対して顔が正面を向いている時のみ取得できるため、必ずしも常時取得できるとは限らないことに留意）	○	A 本人の関知なく取得される可能性が非常に高い
	b. データ取得の所要時間	- 瞬時～数秒以内に取得可能 - 根拠：歩行中の人物からも1秒未満での取得が可能	○	
	c. 本人操作の有無	- 明示的な操作が不要であり、本人が気づかぬうちにデータを取得され得る - 根拠：上記a.及びb.の通り、遠隔かつ瞬時～数秒での取得が可能	○	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない(目に留まらない)形でデータを取得できる - 根拠：顔認証機能付きカメラの外形寸法は20cm以内と小型	○	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の[凡例は18頁をご参照ください](#)

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | □：顔特徴データ（2/2）

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業及びシステムのバージョンごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：流出した顔特徴データに対し、テンプレート反転攻撃を用いることで元の生体情報を再生することも一定は可能¹（ただし、あくまでも一定レベル）	○	
	c. 元データそのものの偽装・模倣の可否	- 技術的には偽装・模倣が困難ではない - 根拠：NISTでは合成画像に特化した顔認証システムのテスト（Face Analysis Technology Evaluation (FATE) MORPH）を実施するなど、技術的には偽装・模倣が困難ではないデータである	○	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい - 根拠：性別・年齢・表情は推定できるが、機微情報は含まれない²	×	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	NISTでは指向性照明を備えた屋外や長距離(300m+)、見下ろす画角などでも検証を実施（FRTE Face In Video Evaluation (FIVE) 2024）	—	—
	b. 分析技術の革新（識別精度）		—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の**凡例は19頁をご参照ください**

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ハ：虹彩データ (1/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	1対1での個別取得が前提 - 根拠：複数人の同時取得は現実の運用では難しく、1人単位で両眼を一度に取得することが最大	×	B 情報の取得に要する費用等の制約が少ない
	b. 導入・運用コスト	- 中（中程度のコストが掛かる専門の設備が必要） - 根拠：ISO/IEC 19794-6は、虹彩画像データ交換フォーマットを定めており、近赤外線対応カメラ＋高解像度を必要とする。一方で、実用的には汎用的なUSBセンサーカメラを応用した低価格帯での製品提供が進む	△	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：先述のPanasonicの虹彩カメラ「BM-ET200」では約0.3秒で認証可能	○	
	d. 安定取得の容易性	- 人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい 【ゆらぎを生じさせる因子】 ➢ 環境条件：照明条件³ ➢ 本人条件：人種（虹彩の色）	○	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：入館・入国ゲートや決済システムへの導入など、商用化が進んでいる	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 非接触だがある程度の距離・姿勢条件が必要 - 根拠：虹彩の登録・認証時の距離は50cm前後が推奨	△	C 本人の関知なく取得される可能性が低い
	b. データ取得の所要時間	- 瞬時～数秒以内に取得可能 - 根拠：約0.3秒で認証可能な虹彩カメラが存在	○	
	c. 本人操作の有無	- 明示的な操作を伴い、データを取得されていることを本人が認識する - 根拠：虹彩の撮影には、カメラの正面に虹彩を向ける必要があり、本人の気づかないうちの取得は困難	×	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない(目に留まらない)形でデータを取得できない - 根拠：cと同様、本人の気づかないうちの取得は困難	×	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の凡例は18頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ハ：虹彩データ (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業及びシステムのバージョンごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：流出した虹彩特徴量データに対し、テンプレート反転攻撃を用いることで元の生体情報を再生することも一定は可能⁴（ただし、あくまでも一定レベル）	○	
	c. 元データそのものの偽装・模倣の可否	- 技術的には偽装・模倣が困難ではない - 根拠：眼画像を撮影し印刷した人工虹彩で平均8割以上の受入率となった実験結果が報告されている⁵	○	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい - 根拠：虹彩画像データから性別を識別すること⁶や、メラニン分布・虹彩色から人種を推定することも一定程度可能だが、機微情報は推定されない	×	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	撮像条件が劣悪（低ピクセル、ブレ、ノイズなど）でも、後処理で虹彩模様の復元・強調を行う技術⁷や低価格帯での製品提供が進む	—	—
	b. 分析技術の革新（識別精度）		—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の**凡例は19頁をご参照ください**

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ニ：声紋データ（1/2）

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	1対1での個別取得が前提 - 根拠：実運用されているシステムでは1対1での個別取得が前提	×	B 情報の取得に要する費用等の制約が少ない
	b. 導入・運用コスト	- 低（安価な設備（市販のカメラやマイク等）で対応可能） - 根拠：Alexa Voice ID（コンシューマー向け）のように一般的に手に入る価格帯で入手可能	○	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：Alexa Voice IDでは、呼びかけるだけで話者を識別可能	○	
	d. 安定取得の容易性	- 行動的特徴であるため、安定したデータを取得しにくい 【ゆらぎを生じさせる因子】 ➢ 環境条件：騒音 ➢ 本人条件：健康状態	×	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：コールセンター・金融機関等で商用化された製品が浸透	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 非接触だがある程度の距離・姿勢条件が必要 - 根拠：距離別の話者識別実験では、0.5m以下が高精度との評価⁸	△	B 本人の関知なく取得される可能性が高い
	b. データ取得の所要時間	- 数秒以上の静止・発声・操作などが必要 - 根拠：30秒間の会話を要求するシステムも存在。1秒間の発話でも技術的には認証可能だが、時間が長いほど精度は向上	△	
	c. 本人操作の有無	- 明示的な操作が不要であり、本人が気づかいうちにデータを取得され得る - 根拠：通話中の自然な会話から声紋を解析できるシステムが多い	○	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない（目に留まらない）サイズである - 根拠：マイクロホンのみで取得でき、本人が意識しないと知覚できない	○	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の凡例は18頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ニ：声紋データ (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業及びシステムのバージョンごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：声紋から本人の声らしき音を再現する実験あり⁹。ただし、声紋の場合は元の音声や発言内容の再現はできないことに留意	○	
	c. 元データそのものの偽装・模倣の可否	- 技術的には偽装・模倣が困難ではない - 根拠：合成音声を用いて認証を突破できるシステムも存在し、技術的には偽装・模倣が困難ではない	○	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい ※パーキンソン病の推定は可能であることに留意¹⁰	×	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	- 雑音・残響除去・話者分離機能等の開発が進行している¹¹ - 犯罪捜査のために、変換された音声から、元の声紋を復元する技術も開発¹²	—	—
	b. 分析技術の革新（識別精度）	データセット調整等により、双子の識別精度を向上させる動きあり¹³	—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の凡例は19頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ホ：歩容データ (1/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	- 不特定多数から同時かつ自動的に取得可能 - 根拠：出入室管理システムは自動的に複数人の取得・認証が可能	○	C 情報の取得に要する費用等の制約が一定存在する
	b. 導入・運用コスト	- 低（安価な設備（市販のカメラやマイク等）で対応可能） - 根拠：市販品の監視カメラにて対応可能	○	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：少なくとも2歩（通常1秒程度）の映像列があれば認証可能であり、リアルタイムでの識別も技術的に可能だが、現状は実験レベルでの運用が多い	△	
	d. 安定取得の容易性	- 行動的特徴であるため、安定したデータを取得しにくい 【ゆらぎを生じさせる因子】 ➢ 環境条件：画角（横90度から撮影された映像が望ましい） ➢ 本人条件：歩く速度、服装、携帯物	×	
	e. 商用化の度合い	- 実証・実験段階であり、商用化された機器・システム・サービスは稀である - 根拠：研究室や事業者のPoC段階のものが多い（利用動向調査ご参照）	×	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 完全非接触で遠距離（5m以上）からでも取得可能 - 根拠：監視カメラ映像からの常時取得が可能	○	A 本人の関知なく取得される可能性が非常に高い
	b. データ取得の所要時間	- 瞬時～数秒以内に取得可能 - 根拠：少なくとも2歩（通常1秒程度）の映像列があれば認証は可能	○	
	c. 本人操作の有無	- 明示的な操作が不要であり、本人が気づかないうちにデータを取得され得る - 根拠：監視カメラ映像による常時取得が可能	○	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない（目に留まらない）サイズである - 根拠：監視カメラ映像による常時取得が可能	○	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の**凡例は18頁をご参照ください**

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ホ：歩容データ (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業ごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクは小さい - 根拠：一般的な歩容認証はスケールファクターが入っておらず、同一身長で規格化されているため、元データ（人物）の復元は困難	×	
	c. 元データそのものの偽装・模倣の可否	- 偽装・模倣が極めて困難 - 根拠：体型と姿勢をまねることが非常に難しいため、偽装・模倣の可能性は低い	×	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクが小さいとまではいえない - 根拠：パーキンソン病のほか、ASD、神経筋疾患など、障害や健康情報の推定が可能¹⁴	○	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	3D骨格推定を取り入れることで認証精度を向上させる動きあり¹⁵	—	—
	b. 分析技術の革新（識別精度）		—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の凡例は19頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ヘ：静脈データ (1/2)

調査・大項目	調査・小項目	調査結果・根拠 (具体事例含む)	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	1対1での個別取得が前提 - 根拠：被験者の位置・角度が変動するため、均一な近赤外照明を当てて静脈を検出することが難しい	×	B 情報の取得に要する費用等の制約が少ない
	b. 導入・運用コスト	- 中 (中程度のコストが掛かる専門の設備が必要) - 根拠：静脈認証には専用の光学系・照明・センサー・画像処理が必要。PCログイン用センサーは1万円前後の価格帯で販売	△	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：取得～識別までの所要時間が1対1で約0.8秒、1対N (N=10,000) で約1～2秒	○	
	d. 安定取得の容易性	- 人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい 【ゆらぎを生じさせる因子】 ➢ 環境条件：自然光/蛍光灯とも3,000 lux以下など、近赤外撮像に適した照度条件を推奨 ➢ 本人条件：血栓症や傷¹⁶	○	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：入館ゲートや決済システムへの導入など、商用化が進んでいる	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 非接触だがある程度の距離・姿勢条件が必要 - 根拠：40cm以下での取得が推奨	△	C 本人の関知なく取得される可能性が低い
	b. データ取得の所要時間	- 瞬時～数秒以内に取得可能 - 根拠：取得～識別までの所要時間が1対1で約0.8秒、1対N (N=10,000) で約1～2秒	○	
	c. 本人操作の有無	- 明示的な操作を伴い、データを取得されていることを本人が認識する - 根拠：Amazon One Enterpriseは非接触型でも手のひらをかざすという意図的な動作があることを理由に静脈認証を採用	×	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない(目に留まらない)形でデータを取得できない - 根拠：縦・横・高さが30mm以内と小型でも、撮像距離や照度条件が必要	×	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の凡例は18頁をご参照ください

出所) 公開情報、ヒアリングより作成 (公開情報の出所については参考文献リストを別途ご参照ください)

(2) 国内外における生体データの技術動向 | ヘ：静脈データ (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業及びシステムのバージョンごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：高解像度テンプレートや特徴ベクトルから、元の指静脈パターンを再構成する研究も進む¹⁷（ただし、あくまでも一定レベル）	○	
	c. 元データそのものの偽装・模倣の可否	- 偽装・模倣が極めて困難 - 根拠：体内情報で偽造が難しい（研究レベルでは印刷した掌静脈等によるなりすましが可能と実証されている¹⁸）	×	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい - 根拠：性別と年齢のクラスを識別可能¹⁹だが、機微情報は推定されない	×	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	通常のカメラ画像から静脈パターンを強調する波長分解能と解析により、明確な静脈パターンを抽出できる技術を富士通が開発。また、他分野で学習された特徴の転用によるデータ拡張や、ノイズ耐性改善などの技術研究が進む²⁰	—	—
	b. 分析技術の革新（識別精度）		—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の凡例は19頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ト：指紋データ (1/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	1対1での個別取得が前提 - 根拠：実運用されているシステムでは1対1での個別取得が前提	×	B 情報の取得に要する費用等の制約が少ない
	b. 導入・運用コスト	- 中（中程度のコストが掛かる専門の設備が必要） - 根拠：真皮認証用の端末は1～2万円程度で販売。なお、表皮認証用の静電容量式指紋センサーモジュールは1台数千円で販売	△	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：高速応答が要求される出入国審査、国民IDシステム、空港自動化ゲート等で活用	○	
	d. 安定取得の容易性	- 人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい 【ゆらぎを生じさせる因子】 ➢ 環境条件：照射条件（非接触型の場合） ➢ 本人条件：皮膚水分状態（表皮認証の場合）	○	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：入館ゲートへの導入やiPhoneのTouch IDとしての搭載など、商用化が進んでいる	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 非接触だがある程度の距離・姿勢条件が必要 - 根拠：NISTでは、撮影範囲で姿勢を安定させることを推奨	△	C 本人の関知なく取得される可能性が低い
	b. データ取得の所要時間	- 瞬時～数秒以内に取得可能 - 根拠：非接触型で指紋を1秒未満で取得できるシステムが存在	○	
	c. 本人操作の有無	- 明示的な操作を伴い、データを取得されていることを本人が認識する - 根拠：非接触型でも手をかざす/指定位置に手を出す動作が前提	×	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない（目に留まらない）サイズである - 根拠：スマートフォンの画面内やキーボード内など、一見すると指紋センサーとわからない形で組み込まれている製品が多数存在	○	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の**凡例は18頁をご参照ください**

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ト：指紋データ (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業及びシステムのバージョンごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：保護されていないテンプレートから元のサンプルを再構成可能²¹	○	
	c. 元データそのものの偽装・模倣の可否	- 技術的には偽装・模倣が困難ではない - 根拠：多くのユーザーの指紋に一致する合成指紋の生成²²や、シリコン等で物理的に模倣するなどのなりすましが可能	○	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい - 根拠：指紋画像からの推測として、年齢で89.1%、性別で88.7%の精度を達成する²³。ただし、機微情報は推定されない	×	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	エラー率低減などを可能とする超音波指紋センサー等、取得の技術研究が進む²⁴。また、ディープラーニングの活用²⁵や偽造検知強化²⁶等により、認識精度の高度化の余地がある	—	—
	b. 分析技術の革新（識別精度）		—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の凡例は19頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

(2) 国内外における生体データの技術動向 | ト：掌紋データ (1/2)

調査・大項目	調査・小項目	調査結果・根拠 (具体事例含む)	小項目評価	総合評価
① 取得に要する費用等	a. 同時取得量	1対1での個別取得が前提 - 根拠：実運用されているシステムでは1対1での個別取得が前提	×	B 情報の取得に要する費用等の制約が少ない
	b. 導入・運用コスト	- 中 (中程度のコストが掛かる専門の設備が必要) - 根拠：非接触型の専用端末は10万円程度で販売	△	
	c. 本人識別までの所要時間	- リアルタイム処理が可能 - 根拠：非接触型の取得・識別時間は0.35秒	○	
	d. 安定取得の容易性	- 人体の物理的特徴または生理的特徴であるため、安定したデータを取得しやすい 【ゆらぎを生じさせる因子】 ➢ 環境条件：照射条件 (非接触型の場合) ➢ 本人条件：手のひらの距離や位置²⁷ (非接触型の場合)	○	
	e. 商用化の度合い	- 商用化された機器・システム・サービスがあり、エンドユーザーが購入可能 - 根拠：スマートフォンのカメラを用いた非接触型の認証システムなど、商用化が進んでいる	○	
② 本人の関知なく取得される可能性	a. 非接触取得の可否	- 非接触だがある程度の距離・姿勢条件が必要 - 根拠：犯罪現場の照合は接触型であるが、商用製品では非接触型がみられる。非接触型であっても手をかざす、所定位置に出す等の操作は必要	△	C 本人の関知なく取得される可能性が低い
	b. データ取得の所要時間	- 瞬時～数秒以内に取得可能 - 根拠：取得・識別時間が0.35秒のシステムが存在	○	
	c. 本人操作の有無	- 明示的な操作を伴い、データを取得されていることを本人が認識する - 根拠：非接触型でも手をかざす/指定位置に手を出す動作が前提	×	
	d. 機器のサイズ・組込可否	- 本人が意識しないと知覚できない(目に留まらない)形でデータを取得できない - 根拠：非接触型ではスマホ/IPカメラで取得できるが、手を見せる動作が必要	×	

総合評価凡例：小項目評価が全て○⇒A、半数以上が○⇒B、△か×のみ⇒D、それ以外⇒C ※小項目評価の凡例は18頁をご参照ください

出所) 公開情報、ヒアリングより作成 (公開情報の出所については参考文献リストを別途ご参照ください)

(2) 国内外における生体データの技術動向 | ト：掌紋データ (2/2)

調査・大項目	調査・小項目	調査結果・根拠（具体事例含む）	小項目評価	総合評価
③ 取得・利用する際の リスク	a. 特徴量データの漏えい時のなりすまし・不正アクセスのリスク	- 漏えい時に特徴量データを用いてなりすまし・不正アクセスが行われるリスクは小さい - 根拠：特徴量データを抽出するアルゴリズムは企業及びシステムのバージョンごとに異なるため、流出しても悪用されるリスクは小さい	×	—
	b. 元データの復元リスク	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：指紋と同様に、特徴から元の摩擦隆線を推定することは可能	○	
	c. 元データそのものの偽装・模倣の可否	- 特徴量データから元データを復元されるリスクが小さいとまではいえない - 根拠：指紋と同様に、シリコン等で物理的に模倣するなどのなりすましが可能	○	
	d. 機微情報の推定リスク	- 機微情報（障害・健康情報・血族情報等）を推定されるリスクは小さい - 根拠：手の酷使の度合いを間接的に示唆する可能性があるが、機微情報は推定されない	×	
④ 今後の見込み	a. 取得技術の革新（センサー技術）	非接触型では可視光と近赤外光の2台のカメラでの取得により、偽造防止対策と認識精度を向上させる研究が進む²⁷	—	—
	b. 分析技術の革新（識別精度）	距離や手の向きなどの認証時に発生する問題へ対処する技術研究が進む	—	

※大項目③・④は総合評価を置かず、参考情報として整理。小項目評価の凡例は19頁をご参照ください

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

最終報告書サマリ

(1) 国内外における生体データの利用動向 | 利用事例

(1) 国内外における生体データの利用動向 | 市場規模・普及度

(2) 国内外における生体データの技術動向

(3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否

参考文献リスト

新たに個人識別符号となりうるデータの存否を確認するために、以下のデータを対象に調査

- 目的： 現在は個人識別符号として規定されていないが、特定の個人を識別することができる水準での利用が見込まれる**身体の一部の特徴に係るデータの存否**について確認すること
- 調査対象： 各国法にて生体データとして言及されている身体の一部の特徴に係るデータや、近年、本人認証用途での実証が進められているデータを対象とする

分類	生体データとして定めうる身体の一部の特徴に係るデータ	データの概要	対象データを生体データとして言及している各国法例
物理的又は生理的特徴	網膜データ	・網膜の静脈パターンデータ	・米CCPA ・米イリノイ州BIPA ・加ケベック州法 ・豪ALRC
	手のジオメトリデータ	・指紋・掌紋以外の手の形状（手のひらや指の長さ、幅、角度など）に関するデータ	・米イリノイ州BIPA ・加ケベック州法
	耳音響データ	・耳の内部の形状によって決まる音の反響の違いから特徴量を抽出したデータ	・豪ALRC
	体臭データ	・体臭の化学パターンに関するデータ	・豪ALRC ・加ケベック州法
	脳波（EEG）データ	・脳波パターンに関するデータ	－
	心拍（ECG）データ	・心拍パターンに関するデータ	－
行動的特徴	睡眠・健康・運動データ	・睡眠、健康又は運動に関するデータで個人を識別できる情報が含まれるもの	・米CCPA
	キーストロークデータ	・キーボードやタッチスクリーンにおける入力操作（キーを打つスピードの緩急、利用頻度の高いキー、打ち間違いの傾向など）	・米CCPA ・加ケベック州法 ・豪ALRC
	筆跡データ	・サインや文字を書く際の運筆（筆圧、速度、筆順など）の特徴量データ	・加ケベック州法 ・豪ALRC

調査結果

ただし、いずれも現時点では個人識別符号として拡充する意義はあまりないと評価できる

- 先述の調査対象のうち、一定の一意性・不変性が認められるデータのみを有力候補として選定
- **網膜データ・耳音響データは一意性・不変性共に高いものの、2030年代にもあまり普及が見込めないため、現時点で個人識別符号として拡充する意義は小さい。**また、**網膜データは取得時のコストの高さと侵襲性***も課題である
- 脳波データは一意性・普及度合い共に高いが、**不変性が低い**ため、一時点のデータを取得しても個人識別符号とはみなしづらい
- 筆跡データは既に普及が進んでいるが、**一意性・不変性共に中程度のため、単体で個人識別符号とはみなしづらい**

有力候補	①個人を識別する手段としての精度が高いか		②一般的に利用されうるか			
	一意性	不変性	普及度合い (2030年代の市場規模)	現状のユースケース	導入・運用コスト	データ取得・識別の 容易性
データ 網膜	○	○	✕ 市場データなし	✕ 本人認証用途での 実証はなし	✕ 1台数百万円～	✕ 侵襲性*の高いスキャナ- かつ15秒程度で取得
データ 耳音響	○	○	✕ 市場データなし	△ 認証用途での 実証が進行中	△ 商用化前だが業務用に 導入可能な価格帯を予定	○ イヤホン等で音の反響を 測定。約1秒で取得
データ 脳波	○	✕	△	△ 複数のスタートアップで認証 用途での実証が進行中	△ 商用化前だが業務用に 導入可能な価格帯を予定	△ ヘッドバンドやイヤホン等を 装着。取得時間に幅あり
データ 筆跡	△	△	○	○ 商用化が浸透	○ 市販の筆跡認証パッドは 2.5～5万円前後	○ 数秒間（サイン記入時間） で取得し、2秒間で識別

*侵襲性：生体の内部環境に外部から刺激が与えられること

①個人を識別する手段としての精度が高いか、及び②一般的*に利用されうるかを調査し、 現行の個人識別符号と同等の精度・利用が認められるものを個人識別符号として拡充

※「一般的」かは1.導入・運用コスト、2.データ取得・識別の容易性、3.現状のユースケース、4.普及度合いから判断

調査の流れ

①
個人を識別する手段
としての精度が高いか

②
一般的に
利用されうるか

調査項目

- 以下の基準に基づき、一意性が○になるデータ、または両者が○/△になるデータを有力候補データとして選定（詳細基準は次頁をご参照）
 - ✓ 一意性の評価基準：
 - . 個人ごとに極めて高い識別性を持ち、誤判定の可能性が極めて低い
 - △. 識別性はあるが、現時点では誤判定の可能性が一定程度ある
 - ×. 識別性が低く、誤判定の可能性が高い
 - ✓ 不変性の評価基準：
 - . 1年程度以上安定
 - △. 数か月単位で変わる可能性がある
 - ×. 数日～数週間単位で変わる可能性がある
- ①の有力候補データのうち、一般的に利用されうるものを個人識別符号として拡充
 - 個人識別が可能でも、何らかの理由で事業者が認証データとして利用しない・できない場合、個人識別符号として拡充する意義が薄いため、一般的に利用されうることを条件として追加している
- 「一般的」の定義として、以下4つの項目を調査
 1. 普及度合い（本人認証の手段として普及しているか、市場規模を参照）
 2. 現状のユースケース（既にユースケースが存在するか）
 3. 導入・運用コスト（導入・運用コストが安い）
 4. データ取得・識別の容易性（取得方法・所要時間における制約はないか）

①個人を識別する手段としての精度 | 評価基準

①個人を識別する手段としての精度を評価するにあたり、以下の基準を参照する

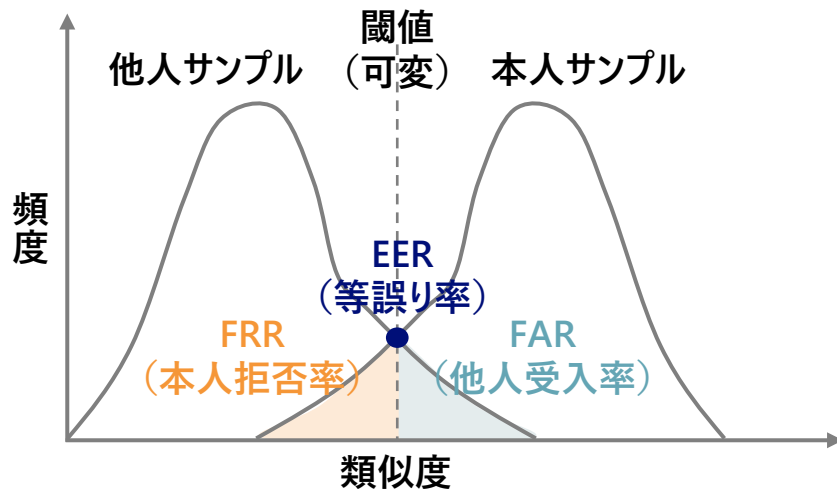
調査項目（小項目）	技術の評価の観点
a. 一意性	○. 個人ごとに極めて高い識別性を持ち、誤判定の可能性が極めて低い △. 識別性はあるが、現時点では誤判定の可能性が一定程度ある ×. 識別性が低く、誤判定の可能性が高い • FAR（≡FMR）（他人受入率）及びFRR（≡FNRM）（本人拒否率）のほか、犯罪捜査の材料や裁判の証拠として利用された実績があるか、今後の取得技術や分析技術の向上が見込めるか等の定性情報をふまえて評価
b. 不変性	○. 1年程度以上安定 △. 数か月単位で変わる可能性がある ×. 数日～数週間単位で変わる可能性がある • 前提：成長・老化の影響が少ない20-60代を対象とする。携帯物や、風邪や怪我等の健康状態による影響、スポーツや職業等による変化は考慮しない

①個人を識別する手段としての精度 | 評価基準

一意性を評価する際の定量指標としては、主にFAR・FRR・EERを参照する。
世界的な技術ガイドラインでは、 $FAR \leq 0.01\%$ かつ $FRR \leq 1 \sim 5\%$ の水準が望ましいとされる

【FAR及びFRRの水準に関する参考】

- NIST SP800-63A : Digital Identity Guidelines (NIST : 米国国立標準技術研究所が定めた、米国連邦政府がデジタルIDを導入する際の技術ガイドライン。米国連邦政府向けではあるが、セキュリティ要件の世界的なデファクトスタンダードとなっている)
 - $FAR (\equiv FMR) \leq 0.01\%$ かつ $FRR (\equiv FNRM) \leq 1\%$ を満たすべきと定義 (n数の定義なし)
- FIDO Biometrics Requirements (FIDO Allianceが定めた技術ガイドライン。Amazon・Apple等のビッグテックやNEC・富士通等の日系企業含む、複数のテック企業・金融事業者等が参画。NISTと同じく、世界的なデファクトスタンダードとなっている)
 - Biometrics Level1+/2+ (被験者245人) の場合、
 $FAR (\equiv FMR) \leq 0.01\%$ かつ $FRR (\equiv FNRM) \leq 5\%$ を満たすべきと定義



【FAR・FRR・EERとは】

- 生体認証の精度はFARとFRRで評価されることが多い
- FARとFRRはトレードオフの関係にあるため、ユースケースに応じて閾値が調整されている
(例：本人拒否率が低いと利便性が高まるが、その分他人受入のリスクが上がるため、高セキュリティの用途にはそぐわない)
- EERは、FARとFRRが一致する水準を指しており、EERが低いほど本人拒否・他人受入共に低いため、個人識別の精度が高いといえる

一意性・不変性に基づき、有力候補を選定。網膜・耳音響・脳波・筆跡データが挙げられた

分類	検討対象	一意性	不変性
		➤ 評価根拠のページ	➤ 評価根拠のページ
身体的特徴	①網膜データ	○	○
	手のジオメトリデータ	×	○
	②耳音響データ	○	○
	体臭データ	×	×
	③脳波（EEG）データ	○	×
	心拍（ECG）データ	△	×
行動的特徴	睡眠・健康・運動データ	×	×
	キーストロークデータ	△	×
	④筆跡データ	△	△

①個人を識別する手段としての精度 | 調査結果：一意性の評価根拠

分類	検討対象	調査結果・根拠（具体事例含む）	精度評価
身体的特徴	網膜データ	- 個人ごとに極めて高い識別性を持ち、誤判定の可能性が極めて低い - 根拠：一卵性双生児でも異なり、推定誤差率は1千万分の1とされる²⁸。本人認証用に行われた実験は少ないが、EER（等誤り率）は0.0557%²⁹との結果あり	○
	手のジオメトリデータ	- 識別性が低く、誤判定の可能性が高い - 根拠：24名の408枚の画像で、FARは0.18%、FRRは14.6%との実験結果あり³⁰。加ケバック州法や米イリノイ州BIPAでは、ジオメトリデータを生体データとして言及しているが、ジオメトリデータ単体は一意性がなく、知識認証との組み合わせが重要	×
	耳音響データ	- 個人ごとに極めて高い識別性を持ち、誤判定の可能性が極めて低い - 根拠：52名の被験者でEER（等誤り率）は0.39%³¹ - 豪ALRCでは耳の形状も生体認証技術の一つとして言及している	○
	体臭データ	- 識別性が低く、誤判定の可能性が高い - 根拠：13人のグループで85%の認証精度³²。体臭は警察犬による追跡に用いられ、一定の識別性があるものの、一次臭（遺伝）、二次臭（食事・ストレス等の影響を受ける臭い）、三次臭（石鹸・香水等の臭い）があり、機械では識別が困難である	×
	脳波（EEG）データ	- 個人ごとに極めて高い識別性を持ち、誤判定の可能性が極めて低い - 根拠：108名を脳波に基づいて識別する実験では、前頭葉領域間の機能的結合性を結合した場合、EC（閉眼）・EO（開眼）時共に識別率が100%、中心頭頂領域のパワースペクトル情報を結合した場合は、ECで97.41%、EOで96.26%³³。Lymbic AIやYneuroなど本人認証用途で脳波データを取得する動きがある	○
	心拍（ECG）データ	- 識別性はあるが、現時点では誤判定の可能性が一定程度ある - 根拠：FARが5%前後、FRRが2%前後³⁴	△
行動的特徴	睡眠・健康・運動データ	- 識別性が低く、誤判定の可能性が高い - 根拠：研究開発段階のため、一意性を裏付けるデータは見当たらない	×
	キーストロークデータ	- 識別性はあるが、現時点では誤判定の可能性が一定程度ある - 根拠：100,000人でEERが4.8%³⁵。キーストロークは一時点の本人認証ではなく、不正検知・連続認証（認証を解除したユーザーが継続してその端末を利用しているかを確認）のために使用されることが多い（例：TypingDNA）	△
	筆跡データ	- 識別性はあるが、現時点では誤判定の可能性が一定程度ある - 根拠：102名の1,232個の署名で、FARは1.6%、FRRは2.8%³⁶。ただし、遺言書・契約書等の筆跡鑑定や、決済時の署名等も広く浸透しており、識別性は認められる	△

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

①個人を識別する手段としての精度 | 調査結果：不変性の評価根拠

分類	検討対象	調査結果・根拠（具体事例含む）	精度評価
身体的特徴	網膜データ	1年程度以上安定 - 根拠：生涯変わらない²⁸	○
	手のジオメトリデータ	1年程度以上安定 - 根拠：成長が終わった段階で安定する³⁷	○
	耳音響データ	1年程度以上安定 - 根拠：成長が終わった段階で安定する³⁸	○
	体臭データ	- 数日～数週間単位で変わる可能性がある - 根拠：先述の通り、体臭には一次臭（遺伝）、二次臭（食事・ストレス等の影響を受ける臭い）、三次臭（石鹸・香水等の臭い）があり、二次臭・三次臭を除いて評価することが難しく、不変性が低い	×
	脳波（EEG）データ	- 数日～数週間単位で変わる可能性がある - 根拠：テンプレート劣化問題があり、1日目にTAR（真陽性率）が94.6%であったシステムが1週間後に83%、6か月後に78%に低下する³⁹など不変性が低い	×
	心拍（ECG）データ	- 数日～数週間単位で変わる可能性がある - 根拠：運動やストレスにより影響が出る³⁴ため、不変性が低い	×
行動的特徴	睡眠・健康・運動データ	- 数日～数週間単位で変わる可能性がある - 根拠：日々の体調や睡眠時間等で変わるため、不変性が低い	×
	キーストロークデータ	- 数日～数週間単位で変わる可能性がある - 根拠：タイピングの慣れやキーボードの種類などで変わる⁴⁰ため、不変性が低い	×
	筆跡データ	- 数か月単位で変わる可能性がある - 根拠：1日目にERRが4.1%であったシステムが、2か月後には16.2%に低下⁴¹。また、意識的に文字の形状や書くスピードを変えることも可能。筆跡認証の運用上は、本人の筆跡が変わって認証できなくなった場合には、再度登録を行うように推奨している	△

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

②一般的に利用されうるか | 網膜認証のユースケース・コスト・データ取得・識別の容易性

網膜は撮影時に非常に高価なデバイスが必要なため、本人認証用途では使用されていない。
また、近距離で取得することが条件となるため、離れて取得できる虹彩の方が利便性が高い

ユースケース

- 数百万円～と高価なデバイスが必要なため、セキュリティや本人認証では使用されていない
- また、既に虹彩認証で高い識別性と利便性を担保できており、網膜認証を用いるメリットが存在しないと想定される

導入・運用
コスト

- 医療用に用いられている網膜スキャナーは一台2,000万円の価格帯

データ
取得・識別の
容易性

- 侵襲性（生体の内部環境に外部から刺激が与えられること）の有無
 - スキャナーをのぞき込む形で近距離で取得するため、侵襲性が高いとみなされることが多い
- データの取得方法・取得時間
 - 10-15秒で取得可能
- データの識別に掛かる時間
 - 不明

②一般的に利用されうるか | 耳音響認証のユースケース・コスト・データ取得・識別の容易性

耳音響認証はコストやデータ取得・識別の容易性共に大きなハードルはない。
ただし、他の生体データに比べて研究主体が限られており、普及が見込めない可能性がある

ユースケース

- ・ 実証・ユースケースの検討段階
- ・ オンラインショッピングの本人認証や、工場・病院といった手袋やマスクを使用する環境下での従業員の認証が想定されている

導入・運用
コスト

- ・ 反響音をマイクで拾う専用の仕組みが必要なため、市販のイヤホンの転用はできない
- ・ ただし、耳音響イヤホンはそれほど高額ではなく、業務用に導入することは可能なレベル

データ
取得・識別の
容易性

- ・ 侵襲性（生体の内部環境に外部から刺激が与えられること）の有無
 - イヤホンで音楽を流し、音の反響を取得するだけのため、侵襲性は低い
- ・ データの取得方法・取得時間
 - 約1秒間で取得可能
- ・ データの識別に掛かる時間
 - 他の生体認証と同程度

②一般的に利用されうるか | 脳波認証のユースケース・コスト・データ取得・識別の容易性

高セキュリティ用途での実用化に向け、スタートアップが脳波認証の研究に取り組んでいる。
ヘッドホンやヘッドセットで取得できるため、比較的安価かつ侵襲性が低いと想定される

ユースケース

- 脳波はヘッドセット等を装着したまま、連続的に認証し続けられること（利用者が本人かを常に確認）が特徴であり、**防衛・金融・医療など、高いセキュリティが求められる領域でのニーズが見込まれる**
 - Lymbic AIでは、Howden（グローバル保険ブローカー）やUltra PCS（英国国防省にも納入している軍用飛行機・車両等のサプライヤー）とパイロット契約を締結。軍用ヘルメットに脳波認証を活用
- **将来的にはXRグラス等への組み込みが期待されており、一般消費者にも普及が進む可能性がある**

導入・運用
コスト

- 脳波測定デバイスは2極で6万円、5極で7.5万円、14極で15万円前後の価格帯。電極が多いほど精度が向上
- ただし、脳波“認証”システムは組み込まれていないため、上記にシステムの価格が上乗せされると想定

データ
取得・識別の
容易性

- 侵襲性（生体の内部環境に外部から刺激が与えられること）の有無
 - ヘッドホンやヘッドセットで取得できるため、侵襲性は低い
- データの取得方法・取得時間
 - Lymbic AIでは**10回連続した1秒間の脳波サンプルを解析**し、NTTデータ研究所×VIEでは**25分間「Neuro Music」という特定の音楽を聴いてもらったときの脳波を測定**するなど、事業者によって取得方法・取得時間には差がある。また、EC（閉眼）・EO（開眼）時の脳波の違いを測定する場合や、前頭葉領域や中心頭頂領域を測定する場合など、条件や部位も様々である
- データの識別に掛かる時間
 - 不明

②一般的に利用されうるか | 筆跡認証のユースケース・コスト・データ取得・識別の容易性

筆跡認証は金融決済・医療・契約時など幅広い場面で利用されており、コストとデータ取得・識別の容易性においても優れている。前述の通り、一意性・不変性の有無が論点となりうる

ユースケース

- ・ 金融決済・医療・契約時など、幅広い場面で利用
- ・ 一部の国では、投票や年金受給時の本人証明に利用されている場合がある

導入・運用
コスト

- ・ 市販の筆跡認証パッドは25,000～50,000円前後

データ
取得・識別の
容易性

- ・ 侵襲性（生体の内部環境に外部から刺激が与えられること）の有無
 - 特定の文字を書くだけのため、侵襲性は低い
- ・ データの取得方法・取得時間
 - 数秒間（サインの記入時間）で取得可能
 - 文字の形状のほか、筆圧、速度、書き順、ペンの傾き等も測定
- ・ データの識別に掛かる時間
 - 約2秒間で識別可能

①個人を識別する手段としての精度 | 現行の個人識別符号

(参考) 現行の個人識別符号においても、一意性・不変性・犯罪捜査等の実績を確認した

個人識別符号	一意性	不変性	犯罪捜査の材料や裁判の証拠としての実績
DNA	「約565京人に1人」と極めて高い識別性を持つ⁴²	生涯にわたり不変	各国の法執行機関で利用されており、DNAデータベース等を保有する国も存在（例：米国連邦捜査局の複合DNAインデックスなど）
顔特徴データ	AppleのFace IDのFARは1,000,000分の1未満⁴³であり、一意性が高いとみなせる	成年であれば10年以上は安定するとみなされている	渋谷ハロウインの軽トラ横転事件では、監視カメラ映像に顔認証システムを用い、人物を継続追跡することで容疑者を特定
虹彩データ	NIST IR 8207によると最も精度の高い製品でFAR0.0001%、FRR0.57%⁴⁴であり、一意性が高いとみなせる	18年前に撮影された虹彩画像と18年後に再撮影された虹彩画像同士が高精度に一致⁴⁵	虹彩が犯罪捜査の材料や裁判の証拠として使用された判例等は見当たらない
声紋データ	FAR0.01%未満、FRR1%未満のシステムがあり、一意性が高いとみなせる	成年であれば10年以上は安定するとみなされている	科学警察研究所では、犯人や被疑者の音声を解析し、個人を識別⁴⁶
歩容データ	- EER（等誤り率）は2.7%⁴⁷ - FARは理想環境下で0.1%程、任意の画角で0.5%前後	映像による歩容認証では、9か月は安定して個人識別可能⁴⁸。プレート上の歩き方を計測した実験では、7～16か月の間は個人識別可能⁴⁹	日本においても裁判の証拠として認められた実績がある⁵⁰
静脈データ	FARは0.000001%以下、FRRは0.01%のシステム⁵¹があり、一意性が高いとみなせる	- FBIは加齢による変化を受けにくいと紹介 - 成人後であれば殆ど変化しないが、運用上は5-10年で更新することがある	英国では、赤外線撮影された手の静脈パターンの分析結果が法廷で認められ、有罪（有罪答弁・有罪評決）に至った事例がある
指紋データ	iPhoneの指紋認証では1対1認証でFAR0.002%⁵²であり、一意性が高いとみなせる	怪我や摩耗等を除くと、成年であれば10年以上は安定するとみなされている	世界的に最も長く、かつ多くの裁判で単独証拠として利用されてきた生体情報である
掌紋データ	1対12,000識別で98.78%の認識率⁵³を達成し、一意性が高いとみなせる	怪我や摩耗等を除くと、成年であれば10年以上は安定するとみなされている	米国の法執行機関のデータベースNPPS（National Palm Print System）を通じて、捜査・起訴および有罪判決に用いられている⁵⁴

出所）公開情報、ヒアリングより作成（公開情報の出所については参考文献リストを別途ご参照ください）

②一般的に利用されうるか | 現行の個人識別符号

(参考) 現行の個人識別符号においても、一般的な利用度合いを確認した

個人識別 符号	普及度合い (2030年代の市場規模)	現状のユースケース	導入・運用コスト	データ取得・識別の 容易性
参照ページ	—	➤ 利用事例	➤ 技術動向調査②-b	➤ 技術動向調査①-b,②-c
DNA	○	○ 商用化が浸透	✕ 高価な設備・専門人員が必要	✕ 識別には最低2時間程度かかる
顔特徴 データ	○	○ 商用化が浸透	○ 安価な設備で対応可能	○ 瞬時に取得・識別が可能
虹彩 データ	○	○ 商用化が浸透	△ 中程度のコストが掛かる専門設備が必要	○ 50cm前後で瞬時に取得・識別可能
声紋 データ	○	○ 商用化が浸透	○ 安価な設備で対応可能	○ 取得時間が長いほど精度は向上するが、 1秒間の発話でも識別可能
歩容 データ	○	△ 認証用途での実証が進行中	○ 安価な設備で対応可能	△ 1秒間の動画で学習可能。リアルタイム 識別も技術的には可能だが実証段階
静脈 データ	○	○ 商用化が浸透	△ 中程度のコストが掛かる専門設備が必要	○ 瞬時に取得・識別が可能
指紋 データ	○	○ 商用化が浸透	△ 中程度のコストが掛かる専門設備が必要	○ 瞬時に取得・識別が可能
掌紋 データ	○	○ 商用化が浸透	△ 中程度のコストが掛かる専門設備が必要	○ 瞬時に取得・識別が可能

最終報告書サマリ

- (1) 国内外における生体データの利用動向 | 利用事例
- (1) 国内外における生体データの利用動向 | 市場規模・普及度
- (2) 国内外における生体データの技術動向
- (3) 特定の個人を識別することができる水準での利用が見込まれる身体の一部の特徴に係るデータの存否

参考文献リスト

参考文献リスト

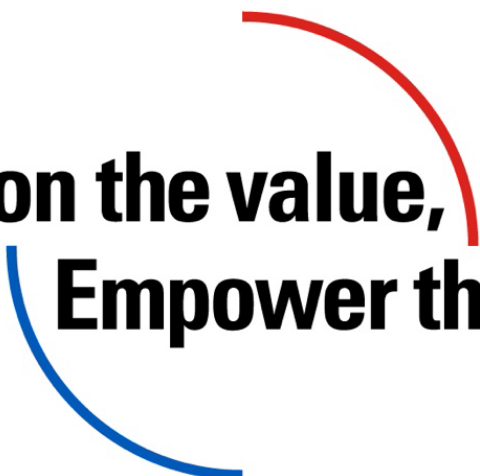
1. Guangan Mai, Kai Cao, Pong C. Yuen, Senior Member, IEEE, and Anil K. Jain, Life Fellow, IEEE, "On the Reconstruction of Face Images from Deep Face Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence (Volume: 41, Issue: 5, 01 May 2019)
2. Zohra Rezgui, Nicola Strisciuglio, Member, IEEE, and Raymond Veldhuis, Senior Member, IEEE, "Gender Privacy Angular Constraints for Face Recognition", IEEE Transactions on Biometrics, Behavior, and Identity Science, Vol. 6, No. 3, July 2024
3. Liu Xiaonan, Bai Yuchen, Luo Yuwen, Yang Zhengwei, Liu Yan, "Iris recognition in visible spectrum based on multi-layer analogous convolution and collaborative representation", Pattern Recognition Letters (2019年1月1日)
4. Sohaib Ahmad, Christopher Geiger, Benjamin Fuller, "Resist : Reconstruction of irises from templates", 2020 IEEE International Joint Conference on Biometrics (IJCB)
5. 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/2005.7』、2005年、35～84頁
6. Nour Eldeen M Khalifa, Mohamed Hamed N Taha, Aboul Ella Hassanien, Hamed Nasr Eldin T Mohamed, "Deep Iris: Deep Learning for Gender Classification Through Iris Patterns", Acta Inform Med. 2019 Jun; 27(2):96–102
7. Fernando Alonso-Fernandez, Reuben A. Farrugia, Josef Bigun, "Very Low-Resolution Iris Recognition Via Eigen-Patch Super-Resolution and Matcher Fusion", 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)
8. Khamis A. Al-Karawi, Burhan Al-Bayati, "The effects of distance and reverberation time on speaker recognition performance", International Journal of Information Technology 16(5):3065-3071, March 2024
9. Panpan Lu, Qi Li, Hui Zhu, Giuliano Sovernigo, Xiaodong Lin, "Voxstructor: Voice Reconstruction from Voiceprint", Information Security: 24th International Conference, ISC 2021, Virtual Event, November 10–12, 2021, Proceedings
10. Ifrah Naeem, Allah Ditta, Tehseen Mazhar, Muhammad Anwar, Mamoon M. Saeed, Habib Hamam, "Voice biomarkers as prognostic indicators for Parkinson's disease using machine learning techniques", Scientific Reports volume 15, Article number: 12129 (2025)
11. Keisuke Kinoshita, Marc Delcroix, Sharon Gannot, Emanuel A. P. Habets, Reinhold Haeb-Umbach, Walter Kellermann, Volker Leutnant, Roland Maas, Tomohiro Nakatani, Bhiksha Raj, Armin Sehr, Takuya Yoshioka, "A summary of the REVERB challenge: state-of-the-art and remaining challenges in reverberant speech processing research", EURASIP Journal on Advances in Signal Processing 2016(1), January 2016
12. Jiangyi Deng, Yanjiao Chen, Yinan Zhong, Qianhao Miao, Xueluan Gong, Wenyan Xu, "Catch You and I Can: Revealing Source Voiceprint Against Voice Conversion", Proceedings of the 32nd USENIX Security Symposium, August 2023
13. Mohammed Hamzah Alsalihi, Dávid Sztahó, "Effect of identical twins on deep speaker embeddings based forensic voice comparison", International Journal of Speech Technology Volume 27, pages 341–351 (2024)
14. Elsa J. Harris, I-Hung Khoo, Emel Demircan, "A Survey of Human Gait-Based Artificial Intelligence Applications", Frontiers in Robotics and AI, January 2022
15. Hongji Guo, Qiang Ji, "Physics-Augmented Autoencoder for 3D Skeleton-Based Gait Recognition", 2023 IEEE/CVF International Conference on Computer Vision (ICCV)
16. Syed Aqeel Haider, Shahzad Ashraf, Raja Masood Larik, Nusrat Husain, Hafiz Abdul Muqeet, Usman Humayun, Ashraf Yahya, Zeeshan Ahmad Arfeen, Muhammad Farhan Khan, "An Improved Multimodal Biometric Identification System Employing Score-Level Fuzzification of Finger Texture and Finger Vein Biometrics", Sensors 2023, 23(24), 9706
17. Christof Kaubaa, Simon Kirchgassera, Vahid Mirjalilib, Andreas Uhla, Arun Rossb, "Inverse Biometrics: Reconstructing Grayscale Finger Vein Images from Binary Features", 2020 IEEE International Joint Conference on Biometrics (IJCB)
18. Pedro Tome, Sébastien Marcel, "On the Vulnerability of Palm Vein Recognition to Spoofing Attacks", 2015 International Conference on Biometrics (ICB)

参考文献リスト

19. Wafa Damak, Randa Boukhris Trabelsi, Alima Damak Masmoudi, Dorra Sellami, Amine Nait-Ali, "Age and Gender Classification from Finger Vein Patterns", International Conference on Intelligent Systems Design and Applications, February 2017
20. Mustapha Hemiscor, Hamza Kheddar, Sami Bourouis, "Deep Learning Techniques for Hand Vein Biometrics: A Comprehensive Review", Information Fusion 114(32):102716
21. Marta Gomez-Barrero, Javier Galbally, "Reversing the Irreversible: A Survey on Inverse Biometrics", Computers & Security Volume 90, March 2020, 101700
22. Philip Bontrager, Aditi Roy, Julian Togelius, Nasir Memon, Arun Ross, "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution", 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)
23. Emanuela Marasco, Luca Lugini, Bojan Cukic, "Exploiting quality and texture features to estimate age and gender from fingerprints", Proceedings of SPIE - The International Society for Optical Engineering 9075:90750F, May 2014
24. Yirong Yu, Qiming Niu, Xuyang Li, Jianshe Xue, Weiguo Liu, Dabin Lin, "A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications", Micromachines 2023, 14(6), 1253
25. 島原 達也・廣川 聡、「ディープラーニング技術を用いた指紋照合技術の現状と将来」、NEC技報 Vol.74 No.1 安全・安心・公平・効率を提供する社会インフラ特集、2021年8月
26. Joshua J. Engelsma, Anil K. Jain, "Generalizing Fingerprint Spoof Detector: Learning a One-Class Classifier", 2019 International Conference on Biometrics (ICB)
27. Dandan Fan, Xu Liang, Chunsheng Zhang, Junan Chen, Baoyuan Wu, Wei Jia, David Zhang, "Smart touchless palm sensing via palm adjustment and dynamic registration", Nature Communications volume 16, Article number: 2912 (2025)
28. Innovatrics, "Retinal Scanning" (<https://www.innovatrics.com/glossary/iris-retinal-scanning/>、2026年8月閲覧)
29. Jarina Mazumdar, "Retina Based Biometric Authentication System: A Review", International Journal of Advanced Research in Computer Science 9(1):711-718, February 2018
30. Peter VARCHOL, Dušan LEVICKÝ, "Using of Hand Geometry in Biometric Security Systems", Radioengineering 16(4), January 2007
31. Masaki Yasuhara, Isao Nambu, Shohei Yano, "Bilateral Ear Acoustic Authentication: A Biometric Authentication System Using Both Ears and a Special Earphone", Appl. Sci. 2022, 12(6), 3167
32. Universidad Politécnica de Madrid, "Identity verification: Body odor as a biometric identifier", Science News, February 4, 2014
33. Daria La Rocca, Patrizio Campisi, Balazs Vegso, Peter Cserti, Gyorgy Kozmann, Fabio Babiloni, Fabrizio De Vico Fallani, "Human brain distinctiveness based on EEG spectral coherence connectivity", IEEE Transactions on Biomedical Engineering (Volume: 61, Issue: 9, September 2014)
34. Rouqiaiah Al-Refai, Pankaja Priya Ramasamy, Ragini Ramesh, Patricia Arias-Cabarcos, Philipp Terhörst, "A Comprehensive Re-Evaluation of Biometric Modality Properties in the Modern Era", 2025 IEEE International Joint Conference on Biometrics (IJCB)
35. Alejandro Acien, Aythami Morales, Ruben Vera-Rodriguez, Julian Fierrez, John V. Monaco "TypeNet: Scaling up Keystroke Biometrics", 2020 IEEE International Joint Conference on Biometrics (IJCB)
36. Anil K. Jain, Friederike D. Griess, Scott D. Connell, "On-line signature verification", Pattern Recognition 35 (2002) 2963–2972
37. Katerina Prihodova, Miloslav Hub, "Hand-Based Biometric Recognition Technique – Survey", Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 6, 689-698 (2020)
38. Ramar Ahila Priyadharshini, Selvaraj Arivazhagan, Madakannu Arun, "A deep learning approach for person identification using ear biometrics", Applied Intelligence, Volume 51, pages 2161–2172 (2021)

参考文献リスト

39. Hui-Ling Chan, Po-Chih Kuo, Chia-Yi Cheng, Yong-Sheng Chen, "Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition", Front. Neuroinform. Volume12, October 2018
40. Vinnie Monaco, Charles C. Tappert, "The Partially Observable Hidden Markov Model and its Application to Keystroke Dynamics", Pattern Recognition 7, November 2017
41. Tobias Scheidat, Karl Kümmel, Claus Vielhauer, "Short Term Template Aging Effects on Biometric Dynamic Handwriting Authentication Performance", CMS'12: Proceedings of the 13th IFIP TC 6/TC 11 international conference on Communications and Multimedia Security, September 2012
42. 法科学鑑定研究所株式会社 HP (<https://alfs-inc.com/dna/>, 2026年8月閲覧)
43. Apple Inc. HP, "About Face ID advanced technology", (<https://support.apple.com/en-us/102381>, 2026年8月閲覧)
44. George W. Quinn, Patrick Grother, James Matey, "IREX IX Part One Performance of Iris Recognition Algorithms", NISTIR 8207
45. Hunny Mehrotra, Mayank Vatsa, Richa Singh, Banshidhar Majhi, "Does Iris Change Over Time?", PLoS One. 2013 Nov 7;8(11):e78333, November 2013
46. 科学警察研究所 HP (<https://www.npa.go.jp/nrips/jp/fourth/section3.html>, 2026年8月閲覧)
47. Gunwoo Park, Kyoung Min Lee, Seungbum Koo, "Uniqueness of gait kinematics in a cohort study", Scientific Reports volume 11, Article number: 15248 (2021)
48. Chi Xu, Yasushi Makihara, Yasushi Yagi, Jianfeng Lu, "Gait-based age progression/regression: a baseline and performance evaluation by age group classification and cross-age gait identification", Machine Vision and Applications, Volume 30, pages 629–644 (2019)
49. F Horst, M Mildner, W I Schöllhorn, "One-year persistence of individual gait patterns identified in a follow-up study - A call for individualised diagnose and therapy", Gait Posture. 2017 Oct;58:476-480.
50. 大阪大学 D3センター ライフデザイン・イノベーション拠点本部 八木研究室 HP (<http://www.am.sanken.osaka-u.ac.jp/jp/gait/>, 2026年8月閲覧)
51. 富士通株式会社、「Fujitsu 生体認証 PalmSecure-F Pro+」製品シート
52. Apple Inc. HP, "About Touch ID advanced security technology", (<https://support.apple.com/en-us/105095>, 2026年8月閲覧)
53. Anum Aftab, Farrukh Aslam Khan, Muhammad Khurram Khan, Haider Abbas, Waseem Iqbal, Farhan Riaz, "Hand-based multibiometric systems: state-of-the-art and future challenges", PeerJ Comput Sci. 2021 Oct 7;7:e707.
54. International Association of Chiefs of Police HP (<https://www.policechiefmagazine.org/what-police-officers-need-to-know-about-palm-prints/>, 2026年8月閲覧)



**Envision the value,
Empower the change**