米国における生体認証技術利活用の動向

和田恭＠JETRO/IPA New York

1．はじめに

米国では、情報システムへのログインなど個人の識別が必要とされる場面において、血管、虹彩、指紋や顔つきなど人体の一部を測定することで得られる生体情報（生体サンプルという）に基づき個人を認証する生体認証技術（バイオメトリクス）の利用が検討されてきている[1]。バイオメトリクスでは、トークンベース[2]やナレッジベース[3]の個人認証方法と比較して、誤認証の確率が低いこと、被認証者にかかる負担が少ないこと（他の手法では ID カードの取得・保持やパスワードの記憶などが求められる。）、また ID 盗難・不正使用の可能性が低いことなどの利点があることから、セキュリティの強化上、生体認証技術は有望な技術と考えられている[4]。これは、認証に用いられる生体サンプル（指紋や虹彩など）について、ほぼすべての人間が持っているものであり（普遍性）、個人ごとに異なっており（唯一性）、通常終身変わらない（永続性）という特徴を利用したものである[5]。

一方で、セキュリティ以外の場面でも、Facebook を始めとするソーシャルメディアが普及している中で、日々大量の写真・映像がインターネット上にアップロードされるようになっており、それらのコンテンツを分類・整理することがユーザー間のネットワーキング上も有効な手段となってきている。そのため、これらの写真・映像に写っているユーザーを識別するため、顔（画像）認識技術[6]が用いられるようになってきている。

以上を踏まえ、本稿では、米国の生体認証に利用される技術の概要、官民における生体認証技術の利用事例などについて報告する。

[1] http://www.biometrics.gov/Documents/BioHistory.pdf
[2] ID カードなどのそのユーザーしか保有し得ない「固有のトークン（認証を行うための鍵となる物理的デバイスやワンタイムパスワードのような電子データなど。）」を用いた認証方法を指す。
[3] パスワードなどのそのユーザーしか保有し得ない「固有の知識」を用いた認証方法を指す。
[4] http://www.thirdfactor.com/2012/03/15/biometric-market-to-grow-21-by-2014
[5] http://www.jstage.jst.go.jp/article/jsmbe/44/1/3/_pdf/-char/ja/
[6] この顔認識は厳密には認証まで行うわけではないが、顔画像に基づき個人を特定するところまでは上述の顔認証と同じであるため、同等のものとして扱っている。なお、英語では顔認証も顔認識も通例は Face Recognition である。なお、カメラのピント合わせなどのため、人間の顔が画像に含まれているか判定する技術は「顔検出(Face Detection)」。

2. 生体認証技術のこれまでの経緯と、注目の背景

本章では、米国で生体認証技術が利用されてきた経緯、および生体認証技術が注目されている背景について紹介する。

(1) これまでの経緯

1800 年代半ばより、都市の近代化・人口密度増大により、犯罪捜査での利用を中心に、個人を特定するための生体認証技術の研究開発が世界各地で行われるようになった。生体認証技術の中で最初に導入されたのは指紋による認証技術であり、米国では 1903 年に New York 州立刑務所で、囚人管理の目的で国内初の指紋認証システムが導入されている。その後、1936 年には虹彩認証技術、1960 年代には顔認証技術が開発されるなど、指紋以外の生体サンプルによる認証技術の開発が進んだ。1970 年以降になると、掌形、虹彩、などの認証技術が研究者によって開発・特許申請されるなど、様々な生体認証技術の商用化への動きが活発化している。

1990 年から 2000 年にかけて、コンピューターの普及が一般市民および事業者の間でも拡大するとともに、生体認証技術は米国市民生活の様々なシーンで利用されるようになったと言える[7]。1994 年には、不法移民取締りの目的で掌形認識システム「INSPASS（Immigration and Naturalization Service Passenger Accelerated Service System）」が米国内の一部空港に導入されたほか、1996 年の Atlanta 五輪でも、選手村に掌形認識システムが設置され入退管理に活用されたことで、生体認証技術の利用が一般的に広く認識されるようになった。

(2) 生体認証技術が注目されている背景

上述のように、生体認証は、主に犯罪捜査や空港などの重要インフラにおけるアクセス管理を中心に導入が進んでいるが、さらに最近、様々な生体認証関連機器メーカーによる研究開発により、新しい関連製品及びアプリケーションの普及が拡大している。調査会社 Companies and Markets 社によると、各国・地域政府による ID 管理及びセキュリティ需要を原動力として、世界の生体認証技術の市場規模は 2010 年の 50 億ドルから 2015 年には 120 億ドル規模にまで拡大すると予測されている。中でも指紋認証システム（Automated Fingerprint Identification System、AFIS）の市場規模の伸びが最も大きく、2015 年に 66 億ドルと全体の半分を占め、ついで顔、虹彩、血管、音声などによる認証技術の市場も 35 億ドル規模まで拡大するとされている[8]。

[7] http://biometrics.gov/Documents/FAQ.pdf
[8] http://www.companiesandmarkets.com/Market/Information-Technology/Market-Research/Biometrics-Technologies-and-Global-Markets/RPT840599
http://www.homelandsecuritynewswire.com/biometrics-market-expected-hit-12-billion-2015-0

これとは別に、調査会社 Global Industry Analysts 社の世界の生体認証市場の売上予想によると、同市場は 2017 年には 164 億 7,000 万ドル規模にまで成長すると見込まれている。そこでは、各国政府のテロ対策やセキュリティ管理ニーズ以外にも、一般消費者向けサービスでの生体認証技術の応用などが成長を牽引するとされている。具体的には、携帯電話、PDA、ノート PC などモバイル端末への指紋認証センサー需要が伸びるほか、生体認証技術が組み込まれた、企業による従業員出退勤管理用途のいわゆる「タイムカード」需要が今後数年間で急増することが見込まれている。一方で、セキュリティ管理向けの生体認証アプリケーションとしては、政府職員及び国民向け ID カードの開発に各国政府が予算を投入するとみられている。これらの生体認証技術については、新興国におけるセキュリティ需要が増大する一方で、米国が世界市場をリードする状況が続くとみられている[9]。

[9] http://www.planetbiometrics.com/article-details/i/917/

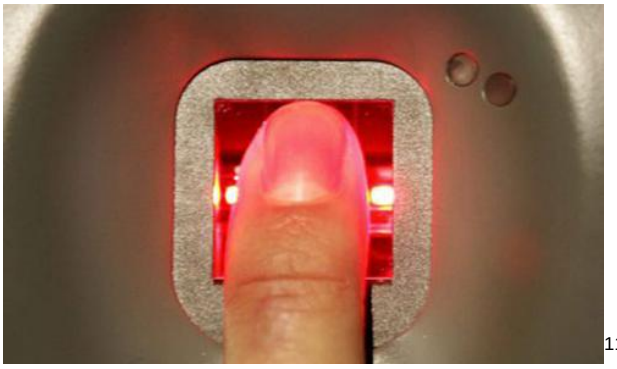
3. 主要技術および活用分野・アプリケーション

本章では、生体認証技術の種類、活用分野やアプリケーション、および技術に関連する標準化活動について紹介する。

(1) 主要技術

生体認証技術では個人を特定するために身体の一部を計測し、検出結果を生体情報（サンプル）として得る必要がある。取得される生体情報の種類別に、各種存在する生体認証技術の特徴について解説し、これらの認証技術の長所・短所について述べる。

【図表 1: 生体認証技術の概要】

指紋（Fingerprint）認証[10]	概要	指の先端にある指紋のパターンを認識して個人を特定する認証方法  [11]
	長所	• 最も汎用的に導入されている生体認証システムであり、その認証精度の高さも実証済み • 認証用データが豊富 • 認証プロセスが容易
	短所	• 犯罪捜査に広く用いられているため被認証者の抵抗感が強い • 対象者の年齢や職業によっては正確な生体サンプルの収集が困難 • 切り傷など生体サンプルが損傷しやすい

[10] http://biometrics.gov/Documents/BioOverview.pdf
http://biometrics.gov/Documents/FAQ.pdf
[11] http://fingerprint-security.net/2011/01/15/fingerprint-scanner-2/

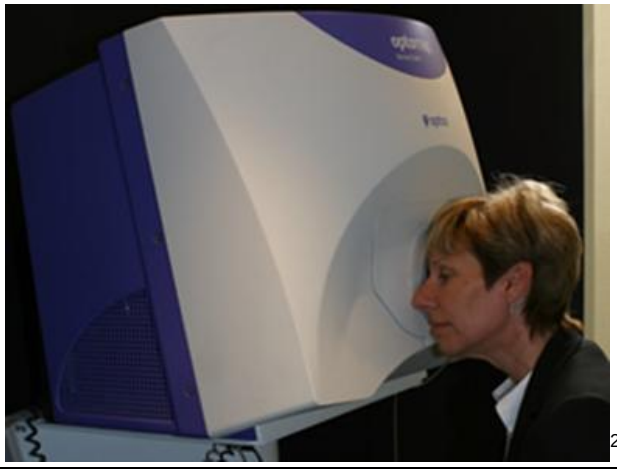
<table>
<tr><td rowspan="3">顔（Face）認証[12]</td><td>概要</td><td>目、耳、鼻、口、などの顔の特徴を認識して個人を特定する認証方法
 
13</td></tr>
<tr><td>長所</td><td>• 非接触で認証できるため認証される側の抵抗感が弱い
• 認証用データが豊富
• 認証結果を肉眼で検証できる</td></tr>
<tr><td>短所</td><td>• 髪の毛、眼鏡、スカーフ、帽子など認証時の画像検出の妨害になる要素が多い
• 認証される側の顔の位置及び表情、背景の照明、加齢などで認証精度が低下する</td></tr>
<tr><td>虹彩（Iris）認証[14]</td><td>概要</td><td>目の中の色のついた部分を認識して個人を特定する認証方法
 
15</td></tr>
</table>

[12] http://www.biometrics.gov/Documents/FaceRec.pdf
http://biometrics.gov/Documents/FAQ.pdf
http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/prosncons.html
[13] http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/
[14] http://biometrics.gov/Documents/BioOverview.pdf
http://biometrics.gov/Documents/FAQ.pdf
http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/prosncons.html
[15] https://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html

	長所	• 非接触で認証できるため認証される側の抵抗感が弱い（カメラはサンプルから約 30 センチ離れた所に設置可能） • 瞼に保護されているため、生体サンプルが損傷する可能性が低い • 認証精度が高い
	短所	• まつ毛、まぶた、眼鏡、コンタクトレンズなど検証の妨害になる要素が多い • 認証用のデータ蓄積が不足しているため、身元調査や人物照会としての利用が困難 • 認証結果を肉眼で検証できない
掌形（Hand geometry）認証[16]	概要	手のひらの幅や指の長さを認識して個人を特定する認証方法  17
	長所	• 主にアクセス管理に利用されているため認証される側の抵抗感が弱い • 成人については生体サンプルが安定しているため認証精度が高い • 認証プロセスが容易
	短所	• 認証システムが高価 • 認証システムの設置に大規模なスペースが必要な場合あり • 発育期の子供の認証には不向き

[16] http://biometrics.gov/Documents/BioOverview.pdf
http://biometrics.gov/Documents/FAQ.pdf
http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies#HandGeometry
http://360biometrics.com/faq/Hand-Geometry-Biometrics.php

[17] http://sandiacontrolsystems.com/page3.html

血管（Vascular / Vein）認証[18]	概要	手のひらや指の血管パターンを認識して個人を特定する認証方法  19
	長所	• 認証精度が高い • 非接触で認証できるため被認証者の抵抗感が弱い • 生体サンプルの偽造が困難
	短所	• 認証システムが高価 • 認証システムの設置に大規模なスペースが必要な場合あり • 認証アルゴリズムが複雑なため、大規模な人数を対象とした認証には向かない
網膜（Retina）認証[20]	概要	目の内部の毛細血管パターンを認識して個人を特定する認証方法  21

[18] http://www.biometrics.gov/Documents/VascularPatternRec.pdf
http://www.biometrics.gov/Documents/VascularPatternRec.pdf
http://ezinearticles.com/?Finger-Vein-Recognition&id=4399575
http://www.freewebs.com/kdypveinbiometrics/advantagesdisadvantages.htm

[19] http://www.theregister.co.uk/2007/07/23/biometrics_vein_recognition/

[20] http://www.biometrics.gov/Documents/BioOverview.pdf
http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/prosncons.html
http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies#HandGeometry

[21] http://www.itblogs.in/biometrics/retina-recognition-technique/

	長所	• 認証精度が高い • 生体サンプルデータのストレージ容量への負担が少ない • 生体サンプルの偽造が困難
	短所	• 認証システムが高価 • 目に損傷を与えるというイメージがあるため、被認証者の抵抗感が非常に強い
掌紋(Palm Print)認証[22]	概要	手のひらの皮膚隆線のパターンを認識して個人を特定する認証方法  [23]
	長所	• 指紋よりも認証時に検出対象とする範囲が広いため認証精度が高い
	短所	• 認証システムが高価 • 認証システムの小型化が困難

なお、上記のような身体的特徴に基づく生体情報(生体サンプル)を用いた認証手法(Physiological Biometrics)に加えて、音声(Voice)、キーストローク(Keystroke)、署名(Signature)、筆跡(Handwriting)、歩き方(Gait)、心拍パターン(Heart Pattern)といった個人の行動的特徴に基づく生体情報(行動学的サンプル)を用いた生体認証技術(Behavioral Biometrics)についても、研究開発及び商用化が進められている[24]。その背景には、正確性という点では生体サンプルを使用した認証手法の方が勝るものの、同認証方法のような特殊な読取装置が不要、コスト、プライバシー保護などの観点からは、行動学的サンプルを使用した認証手法に優位性があることがあげられる。

[22] http://www.biometrics.gov/documents/palmprintrec.pdf
http://360biometrics.com/faq/Palmprint-Biometrics.php
[23] http://sipl.technion.ac.il/Info/News&Events_1_e.php?id=465
[24] http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/2011%20HSSP%20Plenary%20and%20Workshop/HSSP%202011%20Plenary%20Meeting/Tilton%20Presentation.pdf
http://www.igi-global.com/viewtitlesample.aspx?id=36917

例えば北米では、指紋及び虹彩を認証するスキャナが生体認証（生体サンプル・行動学的サンプル両方含む）市場の売上シェアの大部分を占めているものの、2010 年頃より音声認識による生体認証のアプリケーションが市場で注目を集めるようになったようである[25]。

(2) 主要活用分野と具体的なアプリケーション例

生体認証技術の主要活用分野について、近年導入されているアプリケーションの例を紹介する。

① ID マネジメント強化（犯罪捜査・未然阻止、アクセスコントロールなど）

米国では、政府レベルでの犯罪捜査や出入国管理、公共施設の監視やアクセスコントロールといった目的を中心に、顔認証や指紋認証といった生体認証技術が利用されている。これらの目的に関連する ID マネジメント強化分野での生体認証技術の活用事例を以下に紹介する。

＜DMV などによる顔認証技術の導入＞

米国では、各州の車両登録や運転免許を管理する陸運局（Department of Motor Vehicles、DMV[26]）によって生体認証を利用した ID マネジメントの強化が図られている。例えば、Illinois 州の DMV では、偽造の身分証明書による身元詐称犯罪を防止する目的で、1997 年より、運転免許登録者やその他の身分証に用いられる顔写真の大規模なデータベースを用いた顔認証プログラムが導入されている。同プログラムでは、同州民が免許の更新などの際に DMV に証明写真を提出すると、生体認証ソリューション開発会社の Viisage Technologies 社[27]の開発した顔画像照会システム FaceExplorer により、データベースに記録された顔写真と照会され、身元を詐称しようとするケースが特定される仕組みとなっている。同プログラムでは、1997 年から 2007 年までに 5,000 件以上の身元詐称のケースが特定されており、全米 20 州以上で同様の顔認証プログラムが導入されることに貢献したという[28]。

なお、同プログラムでは、顔写真のデータベースが州内の警察機関と共有されており、犯罪捜査時に監視カメラなどでキャプチャされた画像や犯人のスナップショットを、同データベースに照会することで個人の特定に役立てることもできるようになっているという。

---

[25] http://www.plurilock.com/blog/how-behavioral-biometrics-will-transform-network-and-it-security
[26] 陸運局の呼称は Department of Transportation など州により異なる場合がある。
[27] 同社は、その後競合の L-1 Identity Solutions 社に買収され、現在はフランスの国営企業 Safran 社の一部門となっている。
[28] http://www.govtech.com/pcio/Biometrics-Stems-Drivers-License-Fraud.html

金融詐欺、自動車窃盗などの犯罪者は複数の偽造した身分証を使い分けて犯罪を行うことが多く、身元の特定が困難であったが、同システムの検出機能により 7 つの身分証を使い分けていた自動車窃盗犯が逮捕できたなどの成果があがっており[29]、単なる偽造 ID 発行防止以外の治安向上の効果も現れているようである。

なお、米国連邦政府は、2005 年に成立した REAL ID 法に基づき、各州政府の身分証明書（運転免許証、州政府発行の ID カードなど）発行に際して、遅くとも 2013 年 1 月までに連邦政府が定める一定基準を満たすことを義務付けている。これは、パスポートなど一部の例外を除き、米国では一般市民が使用する身分証明書の大半が州政府によって発行されていることを踏まえ、9/11 の教訓から、州ごとの身分証明書発行にあたっての確認情報の統一や州間での情報共有を進めようとする取り組みである。同法では、州政府発行の身分証明書における生体データの記録を義務付けてはいないものの[30]、上記の Illinois 州のように、REAL ID 法の要求項目に加え独自に生体データを取り込んでいる州も見られる。

＜DHS による US-VISIT プログラムの導入＞

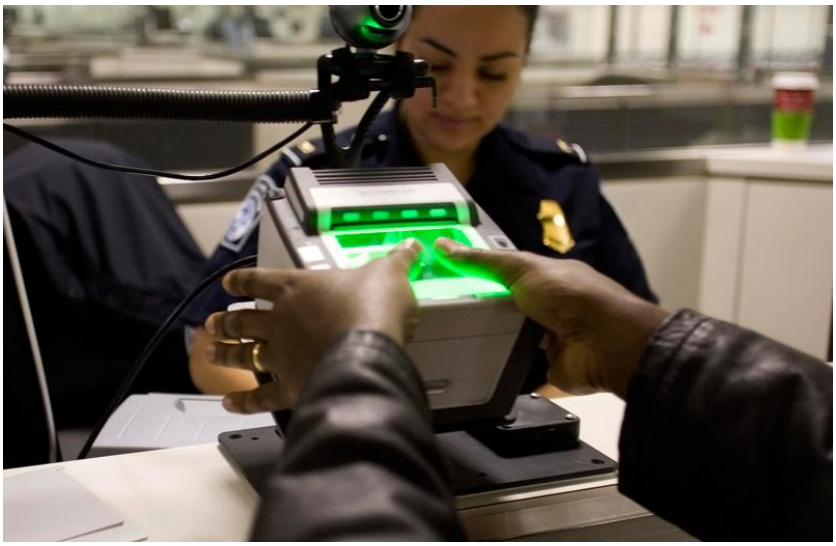
国土安全保障省（Department of Homeland Security、DHS）は 2004 年より、米国を訪問する外国人に関する政府の情報収集能力を強化する目的で、国内各地の空港や国境などの出入国審査所に生体認証技術を導入する United States Visitor and Immigrant Status Indicator Technology（US-VISIT）プログラムを実施している。同プログラムのもと、DHS は国内の 115 か所の空港、15 か所の海港で米国に出入国する外国人の指紋収集を開始し、その後最も交通量の多い 50 か所の国境チェックポイント（陸路）でも指紋収集を開始した他、段階的により多くの空港・海港でも同プログラムを導入している。DHS は、同プログラムで指紋認証による人物照会を行っており、収集されたデータは重要犯罪人約 600 万人を登録したデータベースとマッチングされるという。また、DHS は 2012 年末までに、連邦捜査局（Federal Bureau of Investigations、FBI）と協力の上、マッチング対象のデータベースに FBI が管理する犯罪人データベース（約 6,700 万人登録済）も加える予定となっており、DHS としてはより厳密かつ正確な認証が行えるよう取り組んでいることがわかる[31]。更に、現在 DHS は Texas 州 McAllen 市の国境チェックポイントで顔および虹彩認証の試験展開も行っており、今後技術の成熟化や導入コストの低下が確認された場合、US-VISIT プログラム全体で顔または虹彩認証を行う可能性もあるとのことである[32]。

US-VISIT プログラムの成果であるが、開始から間もない 2005 年 1 月の時点では、US-VISIT を通じて 1,690 万人の外国人のデータが記録されており、DHS によると、

[29] http://www.govtech.com/pcio/Biometrics-Stems-Drivers-License-Fraud.html
[30] http://www.biometrics.gov/ReferenceRoom/FederalPrograms.aspx
[31] http://securitydebrief.com/2012/01/05/us-visit-advances-in-biometrics-tighten-border-security/
http://epic.org/privacy/us-visit/
[32] http://securitydebrief.com/2012/01/05/us-visit-advances-in-biometrics-tighten-border-security/

そのうち犯罪者や不法移民など合計 372 人の摘発につながったという[33]。次いで、2008 年 1 月には、2007 年度のプログラム実施状況が DHS によって公開されている。これによると、2007 年には合計で 46,298,869 件の指紋が空港及び海港にて収集され、そのうち約 0.5%に相当する 236,857 件が「違法滞在の可能性あり」と判断されたという。また、上記 46,298,869 件のうち、39,327 件は DHS によって追加の身元調査を受け、そのうち 273 件が対象者の摘発に至ったという[34]。

【図表 2: US-VISIT プログラムにおける指紋採取の様子】



＜カナダ・米国間国境渡航優遇プログラム「NEXUS」での虹彩スキャナの導入＞

米国税関・国境警備局（United States Customs and Border Protection、CBP）とカナダ国境サービス局（Canada Border Services Agency）が 2004 年より開始した共同プログラム「カナダ米国間国境渡航優遇プログラム（NEXUS）」では、予め登録された旅行者の情報に基づいて両国間の出入国審査の迅速化が図られており、両国の一部の空港では虹彩スキャナによる生体認証が実施されている[35]。旅行者は、空港内に設置されたキオスクで虹彩認証を行えるようになっており、記録された虹彩データは両国が管理する既存のデータベースと照合される仕組みとなっている[36]。

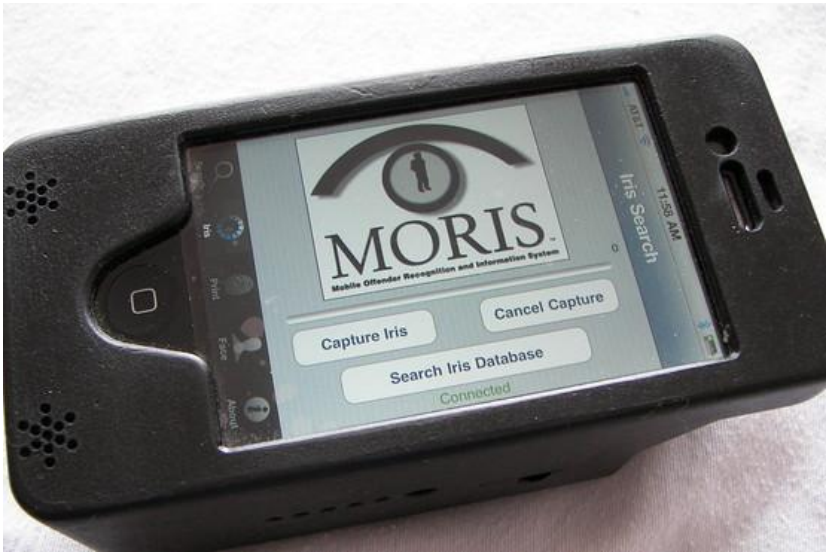
＜地方警察による携帯型生体スキャナの導入＞

米国では、携帯型生体スキャナの導入も進みつつある。一例として、生体認証システム開発大手の BI2 Technologies 社が開発した「Moris（Mobile Offender Recognition and Identification System）」と呼ばれる製品（下図参照）が存在し、2012 年内には米国各地の地方警察機関により、巡回先での不審者などの身元確認

[33] http://epic.org/privacy/us-visit/
[34] http://www.cis.org/vaughan/USVISITNumbers
[35] http://www.cbp.gov/xp/CustomsToday/2004/Dec/nexus.xml
[36] http://www.cbsa-asfc.gc.ca/prog/nexus/air-aerien-eng.html#sup

目的に採用される予定となっている。Moris とは、Apple 社製スマートフォン「iPhone」に外付けする形で利用可能なスキャナであり、虹彩、指紋、顔の 3 種類の生体サンプルを認識することができるという。Moris の価格は 1 機あたり約 3,000 ドル、また Moris によってスキャンされたデータの照会に必要なデスクトップシステムの価格は 1 基あたり 9,995 ドルと比較的高額な価格設定となっているようであるが、同社は既に多数の発注を受けており、2012 年 3 月時点では、生産能力にして今後 8 か月分の予約が入っているとのことである。具体的な発注元としては、Massachusetts 州 Plymouth 郡保安官事務所、Arizona 州 Pinal 郡保安官事務所などがあり、BI2 Technologies 社は、今後このような警察機関のみならず、ヘルスケア業界や金融業界の潜在顧客に対しても Moris の有効性を訴求していきたいとしている[37]。

【図表 3: 生体スキャナ「Moris」の外観[38]】



＜連邦政府による Super Bowl での顔認証システムの導入＞

2001 年に Florida 州 Tampa 市で開催された、プロアメリカンフットボールリーグ・NFL（National Football League）の決勝戦では、会場の Raymond James スタジアムに Viisage Technologies 社の開発した顔認証システム「FaceFinder」が導入されたという。これは、Illinois 州 DMV が利用しているシステムと同じもので、同スタジアムではカメラが入場口の回転扉に設置され、ここで撮影された入場客の映像は、連邦政府が同イベント用に臨時に設立した司令室（law-enforcement command center）で犯罪人リストとの照会が行われたという。同システムは、上記の Illinois 州 DMV の他にも、入国管理局（Immigration & Naturalization Service、現在は Bureau of Citizenship and Immigration Services と呼ばれる）、刑務所など各種連邦政府機関によって様々なセキュリティ管理手法として既に利用されていた実績があったため、米国スポーツ界

[37] http://news.investors.com/article/603514/201203071552/law-enforcement-scanner-works-with-iphone.htm
[38] http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/

で最も注目されると言われる同イベントでの治安維持目的で採用される形となった。但し、同システムの利用については、入場客に対する警告や、事後結果報告なども行われておらず、主体となった政府機関の詳細も明らかになっていない[39]。

＜公的手続きにおける個人認証＞

現在 Arizona 州政府と、New York 州 New York 市政府は、いわゆる「フードスタンプ（food stamp）」プログラム（低所得者に対して食料品と交換可能な金券を付与する福祉制度のこと。正式名称は Supplemental Nutrition Assistance Program）において、申請者の指紋データ採取を義務付けている。これは、身元を偽ることで複数のフードスタンプが不正に得られることを阻止することを目的とした制度であり、2010 年 New York 市政府の集計によると、同制度によって年間約 1,900 件の不正申請（金券にして約 500 万ドル相当）が阻止されたという。ただ、フードスタンプ申請者に対して指紋データ提供を求める制度に対する反発も大きく、以前同制度を採用していた California 州や Texas 州政府は同制度の撤廃に至っている他[40]、New York 州知事は New York 市長に同制度の撤廃を求めるなど[41]、不正申請防止目的での生体データ活用傾向は、むしろ後退の状況にあるといえる。

なお、行政手続きをオンラインで行う場合も個人認証が重要となるが、わが国では確定申告、登記申請ほかの各種行政手続きをオンラインで行う際の個人認証方法として、公的個人認証制度が整備されており[42]、希望する者に対し個人ごとに異なる電子証明書を内蔵した住民基本台帳カード（IC カード）が発行される。これは、ハードウェアトークンベースの個人認証システムといえる。これに対して、米国では、確定申告などの行政手続きをオンラインで行うに当たり、元来納税者の特定目的で作成された社会保障番号（Social Security Number、SSN）[43]、および、社会保障番号作成時に紐付けられる個人情報（氏名、誕生日など）をデータベース化して組み合わせるか、またはこの組み合わせを基に作成されるユーザーID とパスワードの組み合わせを用いる場合が一般的である。これは、ナレッジベースの個人認証システムと言える。

＜一般世帯向け指紋認証型ドアロックシステム＞

米国では、家庭用防犯サービス市場でセキュリティの強化を目的として生体認証技術が積極的に導入されている。一例として、米大手ロックセットメーカーの Kwikset 社は 2007 年 2 月、指紋認証センサによるドアロックシステム「SmartScan」を発表している。同システムは、住宅に設置されたドアに容易に取り付けられるほか、最大 50 以上の

[39] http://www.theregister.co.uk/2001/02/07/feds_use_biometrics_against_super/
[40] https://www.nytimes.com/2011/10/12/nyregion/christine-c-quinn-urges-city-to-drop-rule-on-fingerprinting-food-stamp-seekers.html
[41] https://www.npr.org/2012/01/30/145905246/the-clash-over-fingerprinting-for-food-stamps
[42] http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/kojinninshou.htm
[43] http://www.americanchronicle.com/articles/view/3911

指紋を登録することができるのが特徴となっている（下図参照）[44]。ただ、同システムは現在数百ドル水準の価格で販売されており、ユーザーからは、平均価格が 50 ドル程度の通常のロックより高価なことや、技術的な問題が発生する可能性があるといった指摘もでており[45]、あくまで通常の鍵によるロックシステムの補助的な役割で利用されることが多いようである。

【図表 4: 指紋認証型ドアロックシステムの例[46]】

② 機器ロック解除、サービス利用時の認証

米国では、ノート PC や携帯電話などの各種モバイル端末を中心に、家庭用電子機器の初期認証やロック解除といった目的に生体認証技術が利用されはじめている。特に、スマートフォンやタブレット端末が普及しており、機器のロック解除やサービスログイン時におけるユーザー認証手続きが頻繁に発生することから、USB キーなどの物理的なトークンベースの認証手段より簡便で、4 桁パスコードなどのナレッジベースのものよりセキュリティ性の高い認証手段として生体認証技術に注目が集まっている。以下、電子機器分野での生体認証技術の活用事例を紹介する。

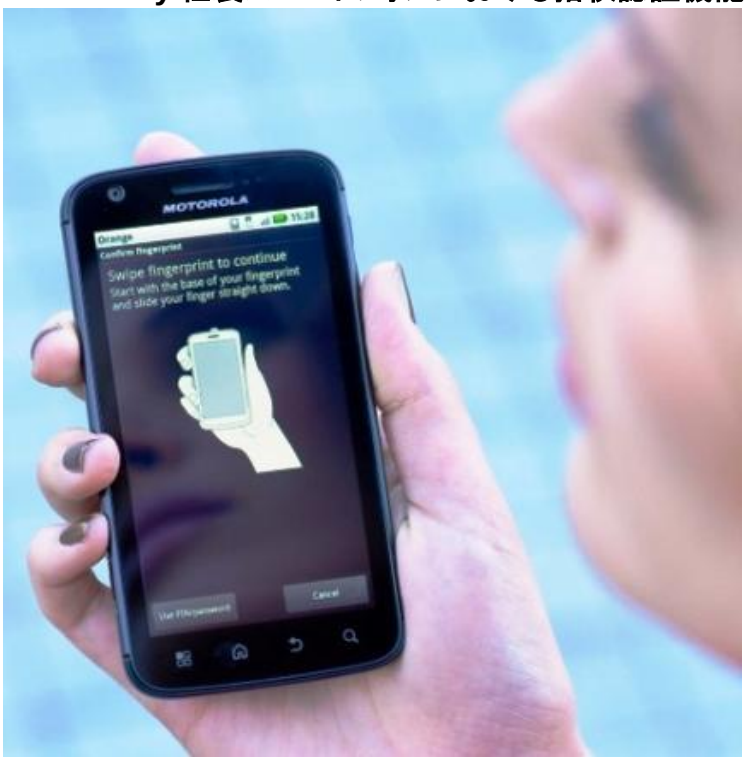
＜モバイル端末への指紋認証機能の導入＞

米国では、ノート PC やスマートフォンなどのモバイル端末において、指紋認証技術を利用したログイン及びスクリーンロック解除機能が普及しつつある。例えば、Dell 社は指紋認証スキャナ搭載のノート PC に加えて[47]、指紋認証スキャナ搭載の外付け型

[44] http://www.gizmag.com/go/6808/
[45] http://www.epinions.com/review/Kwikset_Corporation_Smartscan_Deadbolt_Satin_Nickel/content_425647443588?sb=1
[46] http://www.gizmag.com/go/6808/
[47] http://www.nytimes.com/2010/08/26/technology/personaltech/26askk.html?_r=3

USB デバイスも販売しており[48]、ユーザーは同デバイスを使用して、従来型の（生体認証技術を搭載していない）PC でも従来のパスワード入力の代りに指紋認証によるログインが行えるよう取り組んでいる。また、大手モバイル端末メーカーの Motorola Mobility 社は、2011 年に発売した Android 搭載スマートフォン「Atrix」に同様の指紋認証によるロック解除機能を搭載しており、端末のセキュリティを強化している（下図参照）[49]。

【図表 5：Motorola Mobility 社製スマートフォンにおける指紋認証機能利用イメージ[50]】

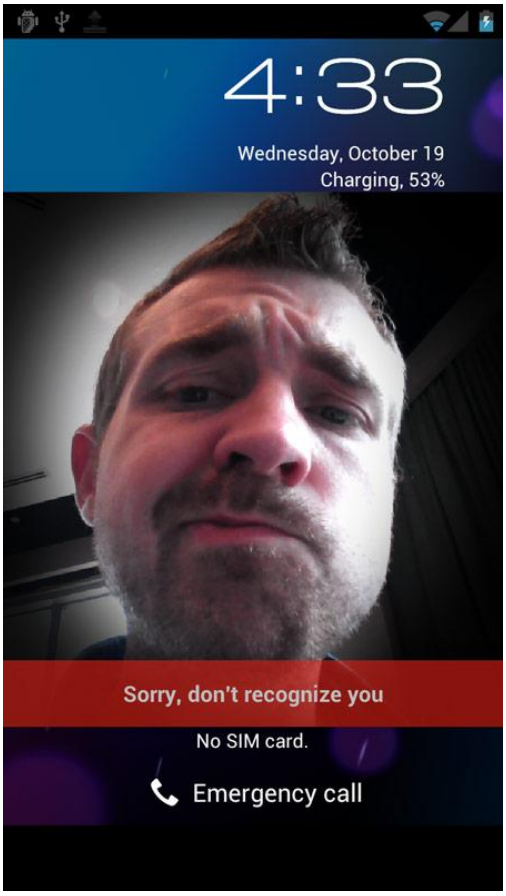


＜モバイル端末への顔認証機能の導入＞

Google 社は 2011 年 10 月、自社開発のスマートフォン・タブレット向け OS である Android の最新版（4.0、コードネーム「Ice Cream Sandwich」）を発表し、同 OS における新機能の 1 つとして、顔認証技術を用いたスクリーンロック解除機能「Face Unlock」を追加している。同技術により、Ice Cream Sandwich 搭載端末のユーザーは、端末の前面に搭載されているカメラに顔を向けることで、スクリーンロックを解除できるようになっている（下図参照）[51]。

[48] http://accessories.us.dell.com/sna/productdetail.aspx?c=us&l=en&s=gen&sku=311-6065
[49] https://motorola-global-portal.custhelp.com/app/answers/detail/a_id/62441/~/atrix---fingerprint-smart-sensor
[50] http://www.cellphonehits.net/site/uploads/Motorola-Atrix-Orange-UK-launch.jpg
[51] http://arstechnica.com/gadgets/news/2011/10/first-look-android-40-sdk-opens-up-face-recognition-apis.ars

【図表 6：Android OS 搭載端末における顔認証機能利用イメージ[52]】



これに対して、Apple 社が iOS そのものに顔認証機能を組み込む動きは今のところないが、同社は 2010 年に顔認証サービスを行うスウェーデンの Polar Rose 社を買収しており、開発者向けツールキットに Polar Rose 社の技術が含まれているとのことである[53]。また、現在、Apps Store からの正規ダウンロードはできないが、顔認証による端末ロック解除機能を実現するアプリケーション RecognizeMe が開発されている。

機器のロック解除以外の用途としては、わが国では、任天堂製の携帯型ゲーム専用機「NINTENDO 3DS」用「nintendogs + cats」（2011 年発売）などのゲームソフトにおいては、3DS 内蔵カメラにより操作中のユーザーの顔で個体識別を行い、登録済みの主ユーザーとそれ以外のユーザーとでゲーム上のキャラクターの反応が異なるという仕組みが導入されている[54]。ただし、ゲームのため、登録ユーザー以外の利用が禁止されるわけではなく、厳密な個体識別も行っていないものと思われる。

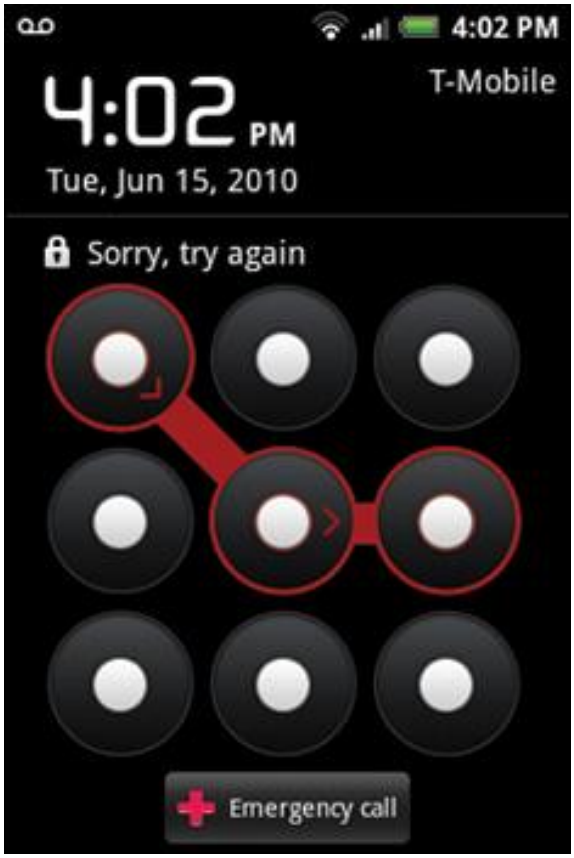
[52] http://www.androidtapp.com/whats-new-in-ice-cream-sandwich-android-4-0/android-4-0-face-unlock/
[53] http://www.readwriteweb.com/archives/facial_recognition_comes_to_ios_5.php
[54] http://nintendo-okie.com/2010/06/15/nintendogs-cats-to-feature-face-recognition/

また、2012 年の CES では、サムスン電子がスマート TV の方向性として、音声・動作認識に加え、顔認識により家庭内ネットワークをカスタマイズする方向性を打ち出している[55]。これらを見ると、単なるスマートフォンやタブレットのスクリーンロック解除機能に留まらない顔認証活用例も登場していることがわかる。

一方、PC・モバイル端末のロック解除手法に関しては、生体認証ではないが、パスコードの入力と比較して、よりセキュリティレベルの高いナレッジ型の認証手段によるものも登場している。例えば、モバイル OS の Android や Windows 8（2012 年内にリリース予定）では、端末の初期画面に表示される点を一定の順番でスワイプしたり（次図参照）、アイコンを一定のパターンに従ってクリックしたりすることでロックを解除する機能も搭載されている[56]。2012 年 3 月上旬のメディア報道によると、FBI がある被疑者より押収した Android 端末のロック解除を試みたものの正しいスワイプの順番を解読できず、裁判所を介して Android OS を開発する Google 社にロック解除方法の開示を求める令状を発行するに至ったとのことであり、民生用技術といえども相当水準のセキュリティ性が確保されていることがわかる[57]。

[55] http://ceron.jp/url/www.youtube.com/watch?v=5C1nADiC6OE
[56] http://www.mostlyblog.com/windows-8-to-come-with-pattern-based-logins
http://www.laptopmag.com/advice/tips/use-swipe-to-lock-your-android-phone.aspx
[57] http://arstechnica.com/tech-policy/news/2012/03/fbi-stumped-by-pimps-androids-pattern-lock-serves-warrant-on-google.ars

【図表 7: Android 搭載端末におけるロック解除画面[58]】



③ 決済時（クレジットカード・ATM 使用時など）における認証

ID 盗難やクレジットカード偽造などによる賠償保険が充実している米国では、電子決済のセキュリティ強化にコストをかけるインセンティブが働かないためか、米国では決済時における認証手段としての生体認証技術の活用は進んでいなかった[59]。しかし、最近では近距離無線通信（Near-Field Communication、NFC）技術を利用した非接触型の決済端末・アプリケーションが普及する兆しが見え始めているなど、決済関連の技術革新の動きがある中で、対応する新型の ATM や POS 端末などにおいて生体認証技術も同時に取り入れられる例が見られる。例えば、Ohio 州を拠点とする ATM 開発大手の Diebold 社は 2011 年 8 月、指紋認証システムを搭載した先進 ATM のプロトタイプを発表しているが、この ATM は、NFC 技術をベースとした非接触式のモバイ

[58] http://www.laptopmag.com/advice/tips/use-swipe-to-lock-your-android-phone.aspx
[59]クレジット・デビッドカードに対する 接触型・被接触型 IC カード導入についても同じことが言える。ニューヨークだより 2011 年 2 月号参照のこと。
http://www.cutimes.com/2011/09/14/smart-chips-still-slow-to-catch-on-at-us-cus
http://www.cutimes.com/2011/09/14/smart-chips-still-slow-to-catch-on-at-us-cus?page=2

ル決済サービスをサポートするほか、親指の指紋をベースに個人認証を行える機能を搭載していることが特徴となっている。指紋データは個々の ATM 内部ではなく、クラウド上で一元管理されるため、同社は世界初の仮想化 ATM と称している。なお、このATM の導入時期などの詳細は明かされていない[60]。

米国外を見ると、我が国や欧州などにおいて、決済時のセキュリティ強化方策として生体認証技術の採用が進んでいる。最も身近な例としては、生体認証技術を用いたATM があげられ、わが国では 2011 年第 1 四半期の時点で約 8 万台が設置されていたということであり[61]、世界でもっとも生体認証技術の導入が進んでいると考えられる。なお、生体認証技術を利用した ATM の製造者はほぼ完全に日本企業によって占められており、2008 年時点のデータによると、その世界市場シェアは日立が約 81%、富士通が約 7%、その他が約 12%であったとのことである[62]。

我が国以外では、ポーランドの大手銀行 BPS 社は、日立製の指血管（finger vein）認証技術を搭載した ATM（【図参照）を、2010 年 5 月に欧州で初めて設置しており、最終的には 350 の支店に合計 350 機の同 ATM を導入する予定であるという[63]。次いで、トルコ最大の銀行 Isbank 社は 2012 年 2 月、BPS 社が導入したものと同型の ATM を国内 1,000 の支店に合計 2,400 機導入したことを発表しているなど[64]、決済時セキュリティ強化に向けた生体認証技術の活用が進みつつある。

[60] http://www.digitaltransactions.net/news/story/3183
[61] http://www.homelandsecuritynewswire.com/biometric-atms-appearing-poland-us-lags-far-behind
[62] http://docbox.etsi.org/workshop/2009/200901_securityworkshop/sony_sato_fingerveinauthentication.pdf
[63] http://www.popsci.com/technology/article/2010-05/poland-installs-europes-first-biometric-fingerprint-scanning-atm-machines
[64] http://www.marketwatch.com/story/isbank-completes-implementation-of-more-than-2400-biometric-atms-using-hitachi-finger-vein-scanning-technology-biggest-biometric-atm-network-in-emea-established-2012-02-09

【図表 8: ポーランドの銀行が導入した日立製 ATM の使用イメージ[65]】

④ ソーシャルメディアにおける利用

米国では、大手ソーシャルメディアを中心に、画像や動画内の人物を自動的に特定する目的で、生体認証技術が利用されている。同分野での生体認証技術の活用事例は以下の通りである。

＜Facebook 社と Google 社による顔認証技術の導入＞

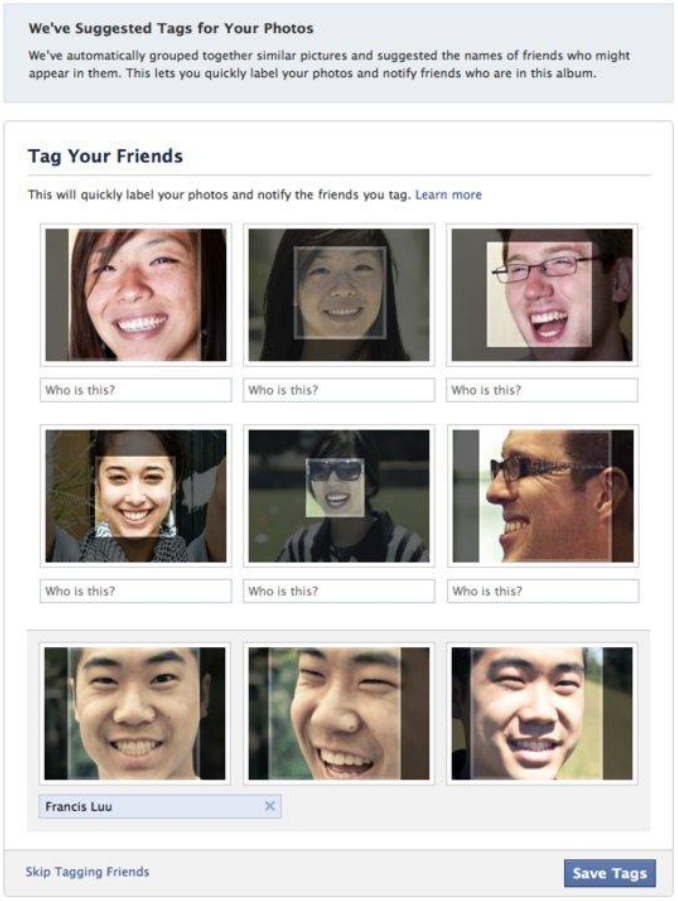
Facebook 社は 2010 年 12 月、顔認証技術による Facebook 上での写真の自動タグ付与機能を追加したことを発表している。これは、既に Facebook にアップロードされているユーザーの顔写真をもとに、新たにアップロードされた写真内の人物に自動的に「タグ」を付与するもので、Facebook ユーザーは大量の写真に手入力ではなく自動的にタグを付けることができるようになっている（参照）[66]。

なお、Facebook での顔認証技術による写真の自動タグ付与機能については、ドイツ・Hamburg 州政府の幹部が 2011 年 11 月、同機能はプライバシー侵害となるため違法であるとの見解を発表すると同時に、Facebook 社はそれ以前に同州政府が求めていた自動タグ付与機能の削除に応じなかったため、同社を提訴する意向を表明してい

[65] http://www.popsci.com/technology/article/2010-05/poland-installs-europes-first-biometric-fingerprint-scanning-atm-machines
[66] http://www.csmonitor.com/Innovation/Horizons/2010/1216/Facebook-knows-your-face.-Is-that-a-problem

る。同政府は、同機能による顔認証データが悪意のある第三者に入手された場合に Facebook ユーザーの個人情報が不正に特定される恐れがあること、また Facebook 社が事前にユーザーの同意を得ずに全ユーザーに同機能を適用し、希望者に同機能の解除を認める「オプトアウト」制で同機能を導入したことを特に問題視しており、提訴と同時に Facebook 社に 30 万ユーロ（約 40 万ドル）の罰金を課すことも検討しているという[67]。

【図表 9：Facebook の自動写真タグ付与機能[68]】



一方、Google 社も 2011 年 12 月、自社の SNS「Google+」に顔認証技術による写真の自動タグ付与機能を追加している。Google+上での写真の自動タグ機能は、Facebook 上でのものと類似しているが、ユーザーに対してその利用を事前に確認する「オプトイン」制度（初期設定では自動タグ機能がオフである制度）が採用されているため、「オプトアウト」制度（初期設定では自動タグ機能がオンである制度）を採用する

[67] http://www.csmonitor.com/Innovation/Horizons/2011/0803/Facebook-biometrics-feature-is-illegal-German-regulator-says
https://www.zdnet.com/blog/facebook/german-state-to-sue-facebook-over-facial-recognition-feature/5187
[68] https://blog.facebook.com/blog.php?post=467145887130

Facebook 社と比較して、プライバシーにより配慮した設計となっている点が特徴といえる[69]。これらのほか、画像ベースのソーシャルメディアとして、同社の Picasa にも画像認識機能は搭載されており、Picasa に保存された写真を、人物ごとに整理して見る事ができる。ただし、この顔認証プログラムはリモート環境で実行され、グーグルサーバーには情報発信を行わないなど、個人情報の保護に配慮した形になっている[70]。

また、同社は、入力した画像に基づく検索サービス「Google Goggles」を運用しており、画像中の人物を特定するために、同サービスにも顔認証技術を導入する可能性は考えられる。

同社は、2011 年 7 月には、顔認証技術をもつ Pittsburgh Pattern Recognition 社を買収している[71]。

(3) 認証技術標準化の動向

生体認証技術の利活用が拡大する中で、各種連邦政府機関や業界団体などにより、生体認証関連技術の標準化に向けた活動が行われている。代表的な例として、以下の取り組みについて紹介する。

＜NSTC による活動＞
大統領府の国家科学技術諮問委員会（National Science and Technology Council、NSTC）傘下には、生体認証及び ID 管理小委員会（Subcommittee on Biometrics and Identity Management）と呼ばれる組織が編成されており、ここで生体認証技術に関して以下のような業務が行われている[72]。

- 連邦政府向けの生体認証システムにおける相互運用性の開発と導入について、技術的な視点からリーダーシップを発揮すること。
- 政府・民間のニーズに応えるため、複数省庁間による生体認証技術研究開発への投資戦略を立案・主導すること。
- 同小委員会が作成する、「生体認証標準の開発・導入・利用に関する指針（Policy for Enabling the Development, Adoption and Use of Biometric Standards）」に基づき、生体認証の標準規格を開発・導入すること。

[69] http://techcrunch.com/2011/12/08/google-introduces-automatic-face-recognition-to-photo-tagging-but-its-completely-opt-in/
[70] http://googlesystem.blogspot.com/2009/09/picasa-35-adds-face-recognition.html
[71] http://www.mobiledia.com/news/99646.html
[72] http://www.biometrics.gov/NSTC/Overview.aspx

- 年次業界会議（Biometric Consortium Conference）などイベントの主催、ウェブサイト（biometrics.gov）におけるコラボレーションなどを通して、生体認証技術に関する様々な働き掛けを行うこと。

この中で、特に標準化との関連性が高い「生体認証標準の開発・導入・利用に関する指針（Policy for Enabling the Development, Adoption and Use of Biometric Standards）」の目的は、連邦政府が生体認証技術を採用する際の技術標準に関わるコンセンサスを、連邦省庁間で確立するための枠組み策定、とされている。連邦省庁では、同小委員会が推奨する生体認証標準を採用することで、省庁間での生体認証システムの相互運用性の向上や、生体認証システムの効率性の向上などが期待されている。同小委員会はこれまでに、この指針を 2008 年、2009 年、2011 年の 3 回にわたって発表しており、省庁の生体認証技術に対するニーズの変化に合わせる形で同指針をアップデートしていることがわかる[73]。

＜NIST による活動＞
国立標準技術研究所（National Institute of Standards and Technology、NIST）では、傘下の情報技術研究所（Information Technology Laboratory）情報アクセス部門（Information Access Division）のイメージグループ（Image Group）が中心となって、生体認証に関する標準規格の開発プロジェクトを実施している。同プロジェクトでは、生体認証データの交換用フォーマット、生体サンプルの質、認証プロセスプロトコルなど、連邦省庁が生体認証技術の運用上必要とする仕組みや要素についての標準規格が開発されている。同グループの具体的な取り組み例として、2011 年には、連邦政府の利用する入退管理カード「PIV（Personal Identity Verification）スマートカード」に組み込まれる生体認証技術に関する仕様及び要件をアップデートした文書「NIST Special Publication 800-76-2」が発表されている[74]。

＜BioAPI コンソーシアムによる活動＞
BioAPI コンソーシアム（The BioAPI Consortium[75]）は、生体認証サービスプロバイダや生体認証アプリケーションデベロッパ向けに、Biometric（生体認証）API と称する生体認証関連アプリケーションプログラミングインターフェース（Application Programming Interface、API）の標準規格を策定する目的で、1998 年に設立された業界団体である。同コンソーシアムには、生体認証市場の発展を目指す 120 社以上の企業や組織が参画しており、幅広い生体認証技術及びアプリケーションと互換性のある API 仕様の標準規格の策定に向けた活動が展開されている[76]。

[73] http://www.biometrics.gov/NSTC/Overview.aspx
http://biometrics.gov/Standards/default.aspx
[74] http://www.nist.gov/itl/iad/ig/biometric_standards.cfm
[75] http://www.bioapi.org/
[76] http://www.bioapi.org/index.asp

BioAPI コンソーシアムがこれまでに策定した標準規格としては、米国標準規格（American National Standard）とされる BioAPI バージョン 1.1（2002 年）と、国際標準規格（International Standard）とされる BioAPI バージョン 2.2（2005 年）が存在する。米国内標準規格の BioAPI バージョン 1.1 は、生体認証に関するフレームワーク、サービスプロバイダ、アプリケーションの 3 層の仕様で構成されているのに対して、国際標準規格の BioAPI バージョン 2.2 は、フレームワーク、サービスプロバイダ、アプリケーション、ファンクションプロバイダの 4 層の仕様で構成されていることが大きな違いとなっているものの、いずれも生体サンプルの記録、認証、識別、といった基本機能や、生体認証サービスプロバイダが最適な環境でユーザーを管理できるデータベースのインターフェイス構築を実現するための仕様が規定されている[77]。

(4) 連邦政府の主要な取り組み

NIST や NSTC による標準化活動や、DHS による US-VISIT など ID 管理強化の活動以外にも、複数の連邦政府機関が生体認証技術の革新や普及に向けて取り組んでいる。連邦政府機関による生体認証技術関連の取り組みについて、以下の表にまとめる。

【図表 10：連邦政府による生体認証技術関連の取り組み[78]】

連邦政府機関	部署	取り組み
大統領府（ホワイトハウス）	**国家科学技術諮問委員会（National Science and Technology Council、NSTC）**	• 標準化（上述）
商務省（Department of Commerce）	**国立標準技術研究所（National Institute of Standards and Technology、NIST）**	• 標準化（上述）
国土安全保障省（Department of Homeland Security、DHS）	**運輸保安局（Transportation Security Administration、TSA）**	• US-VISIT プログラム（上述） • NEXUS プログラム（上述） • Transportation Worker Identification Credential（TWIC）プログラム：TSA 管理下の港湾に勤務する職員などに対して生体データを記録した ID カードを与える取り組み • Registered Traveller プログラム：年間約 200 ドルのサブスクリプション料金を支払い[79]、指紋データなどの個人情報を TSA に登録する者に対して、一

[77] http://www.bioapi.org/Version_2.0_Description.asp
[78] http://www.biometrics.gov/ReferenceRoom/FederalPrograms.aspx
[79] http://travel.usatoday.com/flights/2010-06-15-businesstravel15_ST_N.htm

		部空港におけるセキュリティチェックの順番を優遇する官民共同の取り組み
司法省（Department of Justice、DOJ）	**連邦捜査局（Federal Bureau of Investigations、FBI）**	• FBI Biometric Standards：電子指紋データの通信規格（Electronic Fingerprint Transmission Specification、EFTS）や、その他生体データに関する FBI 専用規格制定の取り組み • Integrated Automated Fingerprint Identification System（IAFIS）：犯罪歴のある米国市民の指紋データを保存するデータベース管理・運用の取り組み • Next Generation Identification System（NGIS）：IAFIS のシステム能力を拡張する取り組み
	国立司法研究所（National Institute of Justice、NIJ）	• Biometric Center of Excellence（BCOE）：FBI 向けに生体認証技術の研究開発を行う機関を運営する取り組み
国務省（Department of State）	**-**	• Electronic Passport：顔認識技術との組み合わせで利用可能な、顔写真のデータを保存したチップを内蔵する電子パスポート発行の取り組み • Secure Network Access：省内ネットワークへのアクセス管理において指紋認証技術を活用する取り組み
国立科学財団（National Science Foundation、NSF）	**Center for Identification Technology Research（CITeR）**	• 新たな生体認証技術の開発に向けた基礎研究、他省庁や民間セクタへの研究成果の伝達、研究者やエンジニアの教育などを行う取り組み

4. 今後の課題と方向性

本章では、生体認証技術の活用に伴う課題、および今後の活用分野・アプリケーションの広がりについて説明する。

(1) 課題

① セキュリティ上の脆弱性

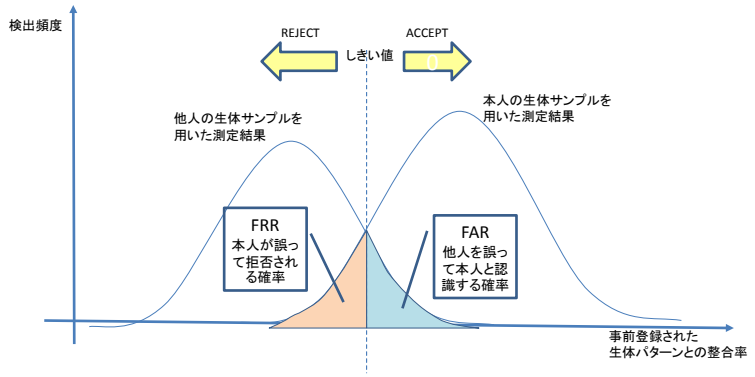
生体認証を用いたシステムに対する攻撃方法としては、以下の3つが知られている[80]。

＜トライアンドエラー攻撃＞
生体認証技術の発展・成熟化により、生体サンプルを用いた認識の精度は上がり続けているものの、統計学的な限界から、誤認識の可能性を完全に排除することは難しいと考えられている[81]。具体的には、誤認識には偽陽性（FAR）と偽陰性（FRR）の 2 種類が存在するが（下記参照）、生体認証システムにおいて片方の許容性を低下させると、もう一方の許容性が自動的に上昇するとされており、利便性向上の観点からはユーザー本人が拒否される割合を一定以上に下げることは難しく、不正ユーザーを正規ユーザーと誤認識してしまう可能性を排除できない点が、セキュリティ上の課題として指摘されている。

- 偽陽性率（FAR：false accept rate）： 提示された生体サンプルが、参照（マッチング）先のサンプルと本来は異なるにも関わらず、システムによって受け付けられてしまうタイプの誤認識の確率。
- 偽陰性率（FRR：false reject rate）： 提示された生体サンプルが、参照（マッチング）先のサンプルと本来は同一であるにも関わらず、システムによって拒否されてしまうタイプの誤認識の確率。

[80] 本分類については、久米原栄氏・三上信男氏著「ネットワーク超入門講座　セキュリティ編」を参照した。
[81] http://www.biometricnewsportal.com/biometrics_issues.asp

【図表 11:認証システムにおける FAR と FRR の関係】



このシステム上の特性を悪用すれば、まったく別人の生体サンプルを使って不正に認証を繰り返すだけで、その別人が(事前登録された人間と誤って)認証されてしまう可能性がある。このシステムとしての許容範囲を狙った攻撃を、「トライアンドエラー攻撃」という。

＜デジタルスプーフィング＞
生体認証システムでは、認証に必要な登録情報(生体サンプルの計測データ)を事前にシステムに保存しておく必要がある。これに対して、システムへの不正侵入により、事前登録された情報を盗み出す、または、本人の認証手続き中に認証に必要な情報を盗み取る(例:音声による認証の場合は「発声」の録音)といった形の攻撃が考えられる。これを「デジタルスプーフィング」という。

＜物理的ななりすまし＞
指紋の偽造など、ユーザーの身体を模倣した人工サンプルを作成するという不正も考えられる。

また、例えば、指紋認証の場合は、指紋画像そのものを画像認識するのではなく、濃淡や特定部位の紋様のパターン変化を検出することにより認証を行っているため、認証アルゴリズムによっては、本来の生体サンプルとまったく異なる人工サンプル(例:一様な肌色の紙が本人の指紋濃淡の計測結果と一致。)が、本人の生体サンプルとして認識される場合も存在する[82]。

生体認証技術固有の課題としては、以上にあげたような攻撃手段によりセキュリティが破られた場合、生体サンプルの性質上その取り消しや書き換えが困難な点がある。特に、一部の行動学的なサンプルや、トークンまたはナレッジベースのパスワードなどと違い、生体サンプルを用いた認証の場合は、なりすまされたユーザーのみ認証システ

[82] ただし、そのような人工サンプルによる攻撃事例の場合は、事前に認証アルゴリズムや対象生体サンプルを知りえなければサンプルの用意はできないため、デジタルスプーフィングとして分類することも可能とも考えられる。

ムから除外するということも難しいことから、漏洩した場合の被害は他の認証手段と比べてより大きくなる可能性も考えられる[83]。

② プライバシー侵害に対する懸念

近年米国では、一般消費者の間で、外出先で写真や映像を撮影し、SNS などのウェブサービスにその場でアップロードできる機能を持つ携帯機器（スマートフォンやデジカメ）が普及している。また、前章で述べたように、最近では SNS など一般消費者が日常的に利用するサービスでも導入されるなど、顔認証技術を活用したサービスが身近になっていることもあり、これらの技術の組み合わせによって、かつては考えられなかった形態でプライバシー侵害事案が発生するという懸念が提示されている。

例えば、Google 社が保有する顔認識アルゴリズム「PittPatt」（上述）は、ウェブ上に公開されている顔写真を収集し、写真のアップロードと同時に公開されている名前と関連付けることで顔認識のデータベースを構築する設計になっているという[84]。現在、Google 社は同アルゴリズムを一般公開しておらず、将来的に公開する予定もないとしているが、このようなアルゴリズムが、例えば変質者、ストーカー、独裁者など悪意を持つ者の手に渡り、個人特定の目的で悪用されるといった可能性は十分に考えられる[85]。

こうした懸念が高まりつつある中で、現在、連邦取引委員会（Federal Trade Commission、FTC）によって、民生用顔認識技術の利活用に対する規制の可否が検討されている。FTC は、まず 2011 年 12 月上旬に官民から有識者を招き、顔認識技術の利用状況や今後の展開に関するワークショップを開催している[86]。次いで、同月下旬から 2012 年 1 月末にかけて、FTC は顔認識技術の利活用状況、ベストプラクティス、プライバシー侵害の可能性などに関するパブリックコメントを募集した[87]。パブリックコメントの募集期間終了後、2012 年 4 月時点では FTC より本件に関する新たな発表はなされていない。

[83] http://www.biometricnewsportal.com/biometrics_issues.asp
[84] http://www.theatlantic.com/technology/archive/2011/09/cloud-powered-facial-recognition-is-terrifying/245867/#.TofORKIDQb4.twitter
[85] http://www.readwriteweb.com/archives/facial_recognition_privacy_concerns.php
[86] http://www.ftc.gov/opa/2011/11/facefacts.shtm
[87] http://ftc.gov/opa/2011/12/facefacts.shtm

(2) 今後の方向性

本項では、生体認証技術の今後の方向性について考察する。

① すでに講じられている個人認証手段の利便性向上とセキュリティ強化

多種多様な分野における生体認証技術の応用が予想されている中で、特にトークンまたはナレッジベースの認証方法を置き換える役割が注目されている。IBM 社幹部の David Nahamoo 氏によると、今後 5 年間で、従来のパスワードや ID カードに代わり、生体サンプルによる認証が通常となる時代が到来するとのことであり、認証用のサンプルには、現在幅広く利用されている指紋だけではなく、網膜、DNA などの生体的サンプルに加え、音声、歩き方といった行動学的サンプルも利用されるようになるとされている[88]。

② 決済及び電子投票などにおける個人認証手段

非接触短距離通信技術 NFC（Near Field Communication）の登場などにより、モバイル決済サービス分野の成長が期待されているが、音声認識技術が決済時のセキュリティ強化に大きな役割を果たすと予想されている。調査会社 Opus 社の 2012 年 1 月の発表によると、モバイル端末による決済サービスにおける不正行為のリスクを低減させるためには、金融機関はなんらかの個人認証ソフトウェアを利用する必要があるが、認識精度と利便性の高さから音声認識が理想的な認証方法として望ましいとしている。個人の認証方法に生体認証技術を採用することで、金融機関はモバイル決済サービスの不正利用による被害や管理コストを削減することが可能となり、コスト削減への寄与が期待されるとのことである[89]。

また、今後実現の可能性があるアプリケーション例として、電子投票における認証方法が挙げられる。米国では、今のところ電子投票での個人認証方法として生体サンプルは利用されていないものの、技術的な基盤は既に整っており、電子投票向けの生体認証システムベンダも存在する。一例として、California 州の個人認証ソリューション開発会社 DigitalPersona 社による指紋認証ベースの電子投票システムは、2010 年にブラジルで開催された国政選挙で約 18 万台導入された例があり[90]、今後米国市場でも電子投票をはじめ、オンライン化が進む各種行政手続きでの生体サンプルの利用が拡大する可能性がある。

---

[88] http://ibmresearchnews.blogspot.com/2011/12/ibm-5-in-5-biometric-data-will-be-key.html
http://www.huffingtonpost.com/2011/12/30/biometric-identification-_n_1177277.html
[89] http://www.bcs.org/content/conWebDoc/43500
[90] http://news.thomasnet.com/companystory/Diebold-Voting-System-Relied-on-180-000-DigitalPersona-Fingerprint-Readers-in-Brazil-s-Historic-National-Election-603364

③ ソーシャルメディア・マーケティングにおける利用

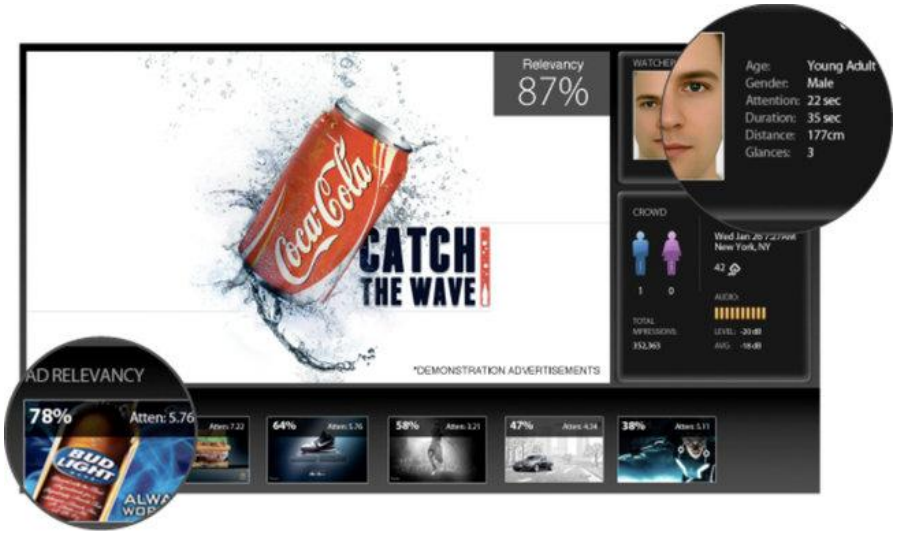
動画や画像を共有することが主眼の YouTube、Flickr, Pinterest などのソーシャルメディア普及に伴い、それらのサービス上表示される人物を簡便に特定することができれば、ユーザー同士のつながりはさらに多様化・深化するものと考えられる。また、最近では turntable.fm や picotube.tv のようなアバターを用いた SNS も登場してきており、顔認識技術をアバター作成に活用するという利用方法も考えられる。

ソーシャルメディア上表示される動画や写真上について、撮影されたユーザーの顔画像に基づくタグ付け機能の利用拡大の傾向は紹介したとおりであるが、後者については、Iowa 州立大学で情報システム管理を専門分野とする Brian Mennecke 教授によると、顔認証ベースで SNS ユーザーのアバターを作成して、ユーザー1 人 1 人に向けパーソナライズされた商品やサービスの広告やプロモーションを提供するマーケティング手法が近い将来導入されるとのことである。同教授は、マーケティング業者はこのような技術を商用化するためには Facebook 社や Google 社などの大規模な SNS ユーザーのデータベースが必要となるが、このようなアバターを利用したマーケティング手法の実現は決して不可能ではないとした上で、そのような手法に対する消費者の反発も予想されると警告している[91]。

一方、顔認証技術を用いたマーケティング手法は、消費者を個人識別するという意味では、現時点では普及に至っていない。しかし、個人の特定に至らずとも、性別、年齢を判別する認識技術については、既に一般展開可能な水準の技術が開発されている。New York Times 紙報道によると、2011 年 11 月に米国内の 3 都市（New York 市、Los Angeles 市、San Francisco 市）で、表示内容が自動的に調整される「スマートビルボード」が街中に設置された。このスマートビルボードでは、顔認識技術によってスマートビルボードを見ている人物の特徴（性別、年齢、どれだけビルボードに注意を払っているか、など）を分析し、それぞれの属性に最も適した広告を表示するものとなっている（下図参照、例えば青年男性に対してはビールを表示するなど。）[92]。

[91] http://www.businessnewsdaily.com/1839-facial-recognition-marketing.html
[92] https://www.nytimes.com/2011/11/13/business/face-recognition-moves-from-sci-fi-to-social-media.html?_r=1

【図表 12:「スマートビルボード」による広告表示のイメージ[93]】



本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。
なお、このレポートに対するご質問、ご意見、ご要望がありましたら、
takashi_wada@jetro.go.jp までお願いします。

[93] https://www.nytimes.com/2011/11/13/business/face-recognition-moves-from-sci-fi-to-social-media.html?_r=1