研究指導　中澤 真 准教授

身近な生体認証の利便性と安全性に関する実験的検証 -Android の顔認証を用いて-

植田　武留

1.　はじめに

情報化の進展に伴って，PCやスマートフォンなどの情報機器は身近な存在となり，これらの機器内に格納される個人情報や機密情報も大幅に増加した[1]．このため，これらの情報を守るための認証技術の重要性がますます高まっている．近年では，暗証番号やパスワードに代わり生体認証技術を用いたセキュリティシステムも数多く利用されている．特に，これまで金融機関など企業が提供するサービスでしか目にしなかった生体認証が[2]，スマートフォンなどの個人所有の機器にも実装されるようになったことは注目に値する．具体的には，Android4.0以降のOSのスマートフォンやタブレットでは顔認証が，またiOSのスマートフォンではiPhone5s以降から指紋認証が導入されている[3][4][5]．こうした動きから，生体認証は今後も身近で利用される場面が増え，さらに重要性が高くなると考えられる．しかし，携帯機器に搭載されている生体認証は導入コストの制約から，安全性・利便性の品質が十分ではない可能性がある．

そこで本研究では，生体認証の中でも，特に安全性が低いとされている顔認証に焦点を当て，この認証方法を採用しているAndroid端末を対象に，安全性・利便性についての評価・検証を行う．そして，スマートフォンやタブレットのあり方やその利用方法についても考察する．

2.　生体認証について

生体認証とは，人々が生まれながらにして持っている唯一無二の生体情報を用いる，個人認証のことである．生体認証に用いる生体情報には顔，虹彩，網膜，指紋，静脈，声紋などの身体的特徴から，筆跡，キーストローク，瞬き，口の動きのような行動的特徴などさまざまな種類がある[6]．

生体認証の導入事例としては，オフィスやセキュリティエリア，マンションの入退室時，金融機関の取引時など主に企業で導入されていることが多い[2]．しかし，現在ではこれらの生体認証はスマートフォンやタブレット機器にも搭載されるようになり，より身近な存在になってきている．具体的にはGoogleでAndroid4.0から顔認証が，AppleではiPhone5sから指紋認証が導入されている[3][4][5]．

2.1 生体認証の利点

生体認証の利点としては，他のパスワードなどの個人認証と比べ利便性に優れているという点である．この点を比較するために，認証方式別に認証情報が忘却しないか，紛失しないか，盗難にあわないかを表1に記した．この表1より，認証に必要な情報を紛失すること，認証に必要な生体部位が盗難にあうこと，認証に必要な情報を記憶する必要がないことから忘れることもないなどの，生体認証の利点が確認できる．特に，従来のパスワード認証やトークン[1]などの所持による認証と比較すると，全ての項目において利便性や安全性に優れていることがわかる．

表 1:認証方式による利便性の差異[7]

認証方式	忘却	紛失	盗難
知識認証（パスワード）	する	しない	あう
所有物認証（トークン）	しない	する	あう
生体認証（生体部位）	しない	しない	あわない

このほかにも，生体認証は認証時の利用者の手間が従来の認証方式よりも少ないというメリットがある．なぜなら，認証に必要な情報を認証者自らが入力する必要がないからである．また，顔認証は遠くを歩いている個人を見分けることもでき，ゲートを通過するだけで認証が行えるほど利便性に優れている．

2.2　生体認証の課題点と精度の評価基準

生体認証には多くの利点があることを先に述べたが，課題点も多く存在する．まず1つ目に，認証に用いる生体情報はパスワードと違って基本的に変更ができないという点である[7]．万が一，生体情報が第三者に盗難されてしまった場合には，パスワードやトークンのように変更することができないため，被害が大きくなる可能性が高い．このため，生体情報の保管方法には十分な注意が必要である．

2つ目の課題点は認証精度についてである[8]．パスワードは文字を入力するため，認証が受理されるのは登録時と認証時の文字列が完全に一致したときに限られる．しかし，生体認証は登録時と認証時の生体情報の類似度によって本人かどうかの判断をする．そのため，顔のような部位を生体情報とした場合には，双子などの区別がつかないことも起こりえる．また，本人の認証時においても，登録されている生体情報と完全に一致することはないため，一定のずれを許容する必要がある．このずれの許容範囲を閾値で設定することになるが，その設定が甘いと他人を受け入れてしまう確率（他人受入率），設定が厳しいと本人すら受け入れてもらえない確率（本人拒否率）が高くなるという問題が生じる．これら2つの確率は以下の式のようにトレードオフの関係にあり，両方を同時に下げることは容易ではない．この二つの値が認証精度の評価指標となる．なお，他人受入率が安全性に関する指標，本人拒否率が利便性に関する指標を意味することになる．

---

[1] 一定時間ごとに新たにパスワードを生成する携帯機器

他人受入率(%)
＝他人受入回数/試行回数*100

本人拒否率(%)
＝(試行回数-本人受入回数)/試行回数*100

一般的に，顔認証は導入が容易な認証方式であるが，他の生体認証と比較して精度が低いという問題がある．スマートデバイスの中で顔認証を採用しているのはAndroid OSを搭載した端末であるが，顔認証そのものの問題に加えて，認証装置のコストの制約の面からも精度が十分ではない可能性がある．

3. Androidに導入された顔認証の概要

本研究で対象としているAndroidの顔認証は，バージョンが 4.0 の時期に導入された．しかし，Android4.0 に導入された顔認証は顔写真でも認証を通過することが可能だということが指摘されている[9]．つまり，登録した本人の顔写真を第三者が手に入れることにより，なりすまし認証が可能となってしまうのである．写真ならば他の生体情報と違って比較的に手に入れやすいため，なりすましにおいて大きな課題点となっていた．そこで，Google は Android4.1 からは顔認証に生体検知という新機能を追加した[5]．生体検知とは，顔写真か本物の顔かを判断するための新機能である．証時に本人の瞬きを必要とさせることで写真と顔を識別し顔写真による認証を防止する．

しかし，この生体検知を導入した Android4.1 の顔認証も，瞬きをした登録者の動画を用意することができれば認証を通過できる可能性があることが報告されている[9]．つまり，最新の Android を搭載したスマートフォンを使用する場合でも，セキュリティ上の不安を抱えていることになる．

4. 顔認証に悪影響を与える要因の分析

4.1 顔認証精度に影響を与える要因

顔認証は一般的には明るさ，マスクや眼鏡の装着によって精度が左右される傾向にある．そこで，以下に示した要因が認証時の他人受入率や本人拒否率にどのような影響を及ぼすか検証する．

・登録時と認証時の明るさの違いによる影響
・登録する特徴のパターン数による影響
・マスクや眼鏡の装着による影響
・顔写真を認証する可能性

1 つ目の「登録時と認証時の明るさの違いによる影響」とは，明るさを照度計で数値化(単位:lx)し，登録時の明るさと認証時の明るさの違いが認証精度に与える影響についての評価項目である．一般的に，顔認証は暗い場所での認証精度が低いことが指摘されているため[10]，スマートフォンのように屋内・屋外と多様な使用環境が想定される場合には，特にその影響について検証しなければならない．

2 つ目の「登録する特徴のパターン数による影響」とは，登録者から 2 つ以上の顔の特徴パターンを登録することで，認証にどのような影響を与えるかを明らかにする評価項目である．多様な利用環境が想定されるモバイル機器の場合，登録時と認証時の外部環境や顔の特徴に違いが生じる場合が多い．そのため，どのような利用場面であっても本人拒否率が上昇しないように，複数の特徴パターンを登録する機能が用意されている．しかし，登録パターン数の増加によりどれだけ本人拒否率を下げることができるのか，また逆に他人受入率の悪化の可能性はないのかということは明確になっていない．これを明らかにするために登録パターン数の他人受入率や本人拒否率への影響について検証する．

3 つ目の「マスクや眼鏡の装着による影響」とは，登録者と認証者にそれぞれ同じマスクや眼鏡を身につけて認証させることで，マスクや眼鏡を身につけた他人の顔が他人受入率や本人拒否率にどれほど影響を与えるのかを明らかにするための評価項目である．

4 つ目の「顔写真を認証する可能性」とは，登録した本人の顔写真もしくは，それに限りなく近い特徴をした本人の顔写真を認証の際に提示することで，本人として受け入れられてしまうかを明らかにする評価項目である．Android4.0 の顔認証機能では，顔写真によるなりすましが可能だということは既に述べたが，Android4.1 から導入された生体検知を利用してなお，顔写真による認証が受理されるのであれば，認証精度が改善されていないことになる．そこで，Android4.0 の顔認証と Android4.1 の顔認証のそれぞれの認証精度を比較・検証し，この問題を明らかにする．

4.2 顔認証精度に関する検証方法

検証に用いた Android の機種や OS バージョン，そのインカメの性能，また，実験器具は以下のとおりである．

Android 端末:Optimus G LGL 21
OS バージョン:Android 4.04（生体検知なし）
インカメ:約 130 万画素

Android 端末:ASUS MeMO Pad8 ME581C
OS バージョン:Android 4.4（生体検知あり）
インカメ:約 120 画素

デジタル照度計: OHM LUX-01-A
測定精度:±8%

本研究では，これらの器具を用いて，登録時・認証時の明るさを 3 ないし 5 段階で変更し，他人受入率と本人拒否率を求める．このとき，各条件での試行回数を被験者一人につき 100 回としている．また，他人受入率を求める際には，複数被験者によるなりすまし認証を試行し，その平均値を用いることとする．なお，屋外などからの自然光の変化の影響を避けるため，外部からの光を遮断できるスタジオで検証は行う．

4.3　検証結果と考察

前節で述べた検証方法によって他人受入率と本人拒否率を求め，それらの値を表にまとめた結果を以下に示す．

表3：登録時と認証時の明るさの違いが与える影響

登録時の照度＼認証時の照度		100lx	300lx	500lx	700lx	1000lx
100lx	他人受入率	11%	0%	0%	0%	0%
	本人拒否率	0%	5%	0%	2%	1%
500lx	他人受入率	0%	0%	0%	0%	0%
	本人拒否率	0%	0%	0%	0%	0%
1000lx	他人受入率	0%	0%	0%	0%	0%
	本人拒否率	95%	0%	0%	0%	0%

表4：登録特徴パターン数の増加により生じる影響

登録時の照度＼認証時の照度		100lx	300lx	500lx	700lx	1000lx
100lx	他人受入率	11%	0%	0%	0%	0%
	本人拒否率	0%	5%	0%	2%	1%
100lx+1000lx	他人受入率	50%	0%	0%	0%	0%
	本人拒否率	0%	0%	0%	0%	0%
100lx+500lx+1000lx	他人受入率	49%	48%	20%	45%	39%
	本人拒否率	0%	1%	0%	0%	0%
500lx+500lx	他人受入率	0%	0%	1%	0%	0%
	本人拒否率	0%	0%	0%	0%	0%

表5：眼鏡が与える影響

登録時の照度＼認証時の照度		100lx	500lx	1000lx
100lx	他人受入率	87%	17%	0%
	本人拒否率	0%	0%	0%
500lx	他人受入率	0%	100%	0%
	本人拒否率	0%	0%	0%
1000lx	他人受入率	0%	0%	7%
	本人拒否率	6%	0%	0%

表6：マスクが与える影響

登録時の照度＼認証時の照度		100lx	500lx	1000lx
100lx	他人受入率	50%	1%	2%
	本人拒否率	0%	0%	0%
500lx	他人受入率	94%	83%	93%
	本人拒否率	58%	0%	0%
1000lx	他人受入率	83%	41%	62%
	本人拒否率	0%	68%	0%

表7：顔写真の受入率

登録時の照度＼認証時の照度		100lx	500lx	1000lx
生体検知なし 500lx	他人受入率	100%	100%	97%
生体検知あり 顔写真1枚：500lx	他人受入率	0%	0%	0%
生体検知あり 顔写真2枚：500lx	他人受入率	97%	99%	91%

まず表3から，登録と認証の際に100lxしかない暗い場所を用いた場合は11％の他人受入率が生じるという結果が示された．ここから考察できることは，暗い場所では，顔の特徴を正確に抽出することができないということである．そのため，登録時も認証時も生体認証を100lxしかない場所で行った場合，正確に特徴抽出することができず，登録者と認証者の顔の部位の特徴がほぼ同じだと判断されたと考えられる．次に，生体情報を1000lxの明るい場所で登録し，100lxしかない暗い場所で認証した場合は95％という非常に高い本人拒否率が生じる結果となった．明るい場所で登録し，暗い場所で認証をした場合では本人の登録時の正確な特徴と認証時の不正確な特徴の情報に大きな誤差が生じるため，このような高い値の本人拒否率が生じたと考えられる．登録者本人の認証が9割以上失敗することから，この条件下ではまったく利便性がないと評価することができる．次に表4から，異なった登録特徴パターン数を増やすほど，他人受入率が高くなり，本人拒否率は低くなるという結果が示された．明るさが異なる3箇所で顔の特徴パターンを登録した際の他人受入率は，認証時の照度にかかわらず20%から49%という高い値となった．また，明るさが異なる2箇所で登録した場合では，100lxという暗い認証環境において高い他人受入率を示した．一般的に異なった登録特徴パターン数を増やすことで本人拒否率を下げることができ，利便性は高くなる．しかし，それは認証受理する顔の特徴パターンの範囲を広げてしまい，他人受入率の上昇といったリスクも併せ持つ．今回の検証結果では，登録特徴パターン数を増やすことで，Android端末の認証に著しく安全性に問題が生じる可能性があることが確認できた．

表5では，眼鏡やマスクを顔に身につけて登録することで，認証時に他人受入率に大きな影響を与えることが示された．眼鏡をかけて100lxしかない暗い場所での登録した際は，100lxの認証で他人受入率が87％，500lxの場所で登録した際は500lxの場所の認証で他人受入率が100％という，非常に高い他人受入率が生じる結果が示された．ここれは，表3の考察でも述べた照度が十分でない環境では顔の特徴パターンを正確に抽出できないことが理由の一つとして挙げられる．さらに，登録時と認証時に眼鏡をかけることで，明るさにかかわらず眼鏡の特徴が同じ特徴だと判断されたことも理由の一つとして考えられる．500lxの照度で登録と認証をした場合の他人受入率が100％と高い値になった原因は明確でないが，もっとも標準的な明るさの環境でこのような結果になったことから，Androidの顔認証において眼鏡はその安全性に大きな影響を与えてしまうといえる．

続いて表6からは，マスクをかけて登録を行うと，認証時の明るさにかかわらず，他人の受入が生じてしまうという結果が得られた．これは登録と認証の際にマスクをかけることで，マスク全体を口のような顔の特徴として抽出していると考えられる．それによって，本人と他人を比較した際でも顔の下半分が同じ特徴として抽出されることになる．

最後に表7からは，Androidの顔認証は登録者の顔写真を認証時に提示することで生体検知機能の有無にかかわらず，100lxから1000lxまでのどの環境で登録をしてもなりすましが可能だということがわかった．生体検知機能を利用しない場合は登録者の顔写真を1枚，生体検知機能を利用した場合は目が開いているものと目をつぶっているものの2枚の登録者の顔写真を用意すれば，9割以上認証を通過することができた．

登録者の顔写真という情報は，生体情報と比較して容易に入手されてしまう可能性があり，Androidの顔認証において最も脆弱な部分であると考えられる．

5. むすび

本研究では，身近な生体認証として，Androidの顔認証を用いて各評価項目に対する検証を行い，安全性と利便性を評価した．これにより，顔認証の安全性と利便性を低下させる要因を示し，項目ごとにユーザが注意すべきことを考察した．生体認証はパスワードなどの個人認証と比べ利便性に優れているが，セキュリティとして利用する際に安全性が低いという検証結果を考慮しなければならない．そのため，Androidの顔認証は機密性が低い情報を守る場面での利用にとどめておくべきであり，ビジネスユースのような高い機密性が求められる場合には，別の認証手段を講じる必要があるだろう．

Androidの生体認証は特徴登録パターン数を変化させることで，ユーザ自身が安全性と利便性をコントロールすることが可能である．しかしこれはパターン数を増やすことで安全性を下げて利便性を上げるという方向にしかコントロールできない．それゆえ，メーカーが設定するAndroidの顔認証の閾値は，これまでよりも他人受入率に対して厳しく設定すべきである．これにより，始めは安全性を重視した顔認証として機能し，利便性を重視する場合は登録特徴パターン数を増やすといった対応をユーザ自身で行うことができるようになる．

また，Androidの顔認証は顔写真によるなりすましの危険性が高いという検証結果から，今後は顔認証を他の認証技術と組み合わせて使うことも検討すべきである．

今後はPC用の顔認証ソフトウェアやiOS端末の指紋認証など，Android端末以外の身近な生体認証の安全性と利便性についても検証を進めたい．

謝辞

本研究の検証にあたり，多大なご協力をいただいた会津大学短期大学部産業情報学科経営情報コース2年生山崎達也氏，金誉大氏に厚くお礼申し上げます．

参考文献

[1] 総務省,平成 25 年版情報通信白書,主な情報通信機器の普及状況, http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc243110.html

[2] 独立行政法人,情報処理推進機構セキュリティセンター, 生体認証システムの導入・運用事例集,https://www.ipa.go.jp/files/000024466.pdf

[3] Gizmodo Japan,livedoorNEWS,iPhone5s の指紋認証機能が改良か, http://news.livedoor.com/article/detail/8591677/

[4] 田中聡,ITmedia Mobile，グーグル,「Android4.0」発表,http://www.itmedia.co.jp/mobile/articles/1110/19/news062.html

[5] 平澤寿康,週アス PLUS,Android4.1 新機能を解説,http://weekly.ascii.jp/elem/000/000/097/97687/

[6] 瀬戸洋一 ，サイバーセキュリティにおける生体認証技術 ,共立出版株式会社 ,2002 年,

[7] 日立製作所, ID 入力やカードは一切不要−ID レス生体認証の利点と課題,http://www.hitachi.co.jp/rd/portal/story/idless_biometrics/01.html

[8] Richard E. Smith ,認証技術 パスワードから公開鍵までオーム社 ,2003 年,

[9] かけなびブログ,Androidの顔認証が流行らない3つの理由, http://blog.kakenavi.com/2013/09/android.html

[10] JAISA,一般社団法人日本自動認識システム協会,BIOMTRICS, http://www.jaisa.jp/action/group/bio/Technologies/Facial/Fac-f.htm