生体認証導入･運用のための
ガイドライン

2009 年11月改訂

独立行政法人　情報処理推進機構

はじめに

近年、金融機関の ATM（現金自動支払機）における手のひらまたは指の静脈認証導入の流れが顕著となっており、生体認証が注目を集めています。また、従来は企業内の入退室管理に利用されていた指紋認証がマンションの共用玄関に導入される事例も登場しています。

こうした状況を踏まえた上で、本ガイドラインは、生体認証のセキュリティに係わる状況に関して、客観的に述べているものです。読者は、生体認証の導入を検討している企業の担当者および意思決定者、既に生体認証導入済みの担当者を想定しています。

現在、生体認証に関しては、非常に極端な 2 つの意見があります。一つは、生体認証は究極の認証手段であり、完璧に安全であるというものです。もう一つは、生体認証は、生体情報の偽造が可能であるとともに、流出の危険があり非常に危ないというものです。

本ガイドラインは、こうした状況に対して、客観的な情報を提供することにより、誤解を解くことを目的としています。つまり、生体認証は、完璧に安全であるわけではなく、非常に危ないというわけでもない、ということを述べています。生体認証の利用の際には、生体認証の特徴を十分踏まえた上で目的に合致した利用をすることが重要です。すなわち、生体認証導入・利用のメリットと生体認証のセキュリティ上の課題を認識することにより適切な利用法が理解できるものであると考えています。

本ガイドラインにより、生体認証の導入・構築・運用に際してのポイントを把握し、導入・構築・運用に活用して頂ければ幸いです。

目　次

1. 生体認証（バイオメトリクス）の概要

1.1.生体認証（バイオメトリクス）とは

生体認証とは、人の生体的な特徴・特性を用いて行う本人認証方式である。生体的な特徴・特性を総称して生体情報と呼ぶ。生体情報には、指紋や顔など身体的外観に基づく身体的特徴と、音声や署名など行動特性に基づく行動的特徴がある。身体的特徴は、常に本人の肉体に付随している。行動的特徴は、本人の癖であり、本人であれば再現が可能なものである。

したがって、生体認証では、パスワードなどの記憶に基づく認証における「忘れる」、「他人に知られる」といった問題や、カードなどの所持に基づく認証における「紛失」、「盗難」、「置き忘れ」の問題を回避できることが多いと言われている（ただし、IC カードとの組み合わせにより生体認証を行う場合もあり、全てのシステムが該当するわけではない）。

1.2.生体認証の導入のメリット

生体認証の導入は、以下のメリットをもたらす。

1) 利便性の高い本人確認方法を提供できること
   生体認証は、普遍性のある生体情報を用いており、生体情報の唯一性および永続性という特質により、本人確認時に利用者自身がカードの準備やパスワードの記録などをする必要が無いため、利用者にとって利便性の高い本人確認方法を提供できる。
2) 認証時に必要となる機密情報の紛失・盗難・置き忘れの可能性を低くできること
   生体認証においては、認証時に必要となる機密情報が生体情報である。そのため、機密情報の紛失・盗難・置き忘れの可能性が極めて低くなる。
3) システムの目的に合わせて、運用者が安全性と可用性を設定できること
   生体認証は、入力データと予め保管されている生体情報である保管データを照合することにより本人確認を行うが、運用者が入力データと保管データの類似度に基づく判定値（以下、閾値）を設定することにより行われる。これにより、運用者は、システム全体の目的に合致した安全性と可用性を設定することが可能である。

生体認証の利用は、必ずしも非常に安全性の高いシステムの構築に直結しているのではなく、利用者にとって機密情報の紛失や忘却、紛失・盗難等の可能性が非常に低いため本人確認時の可用性が高く、かつ運用者にとって安全性の

コントロールが可能であることがメリットである。

1.3. 生体認証による認証技術の概要

(1)生体認証の仕組み

生体認証においては、入力特徴データと登録特徴データをマッチングして算出し、類似度が高い場合に本人と一致するとの判定を行う。ここで、入力特徴データは、湿度や気温等環境条件により異なるため、登録特徴データと完全に一致することはない。

そのため、入力特徴データと登録特徴データとの類似度の計算結果は、あらかじめ設定された閾値と比較され、本人との一致/不一致が判定される。

生体認証の処理の流れは、図 1 -1 の通りである。

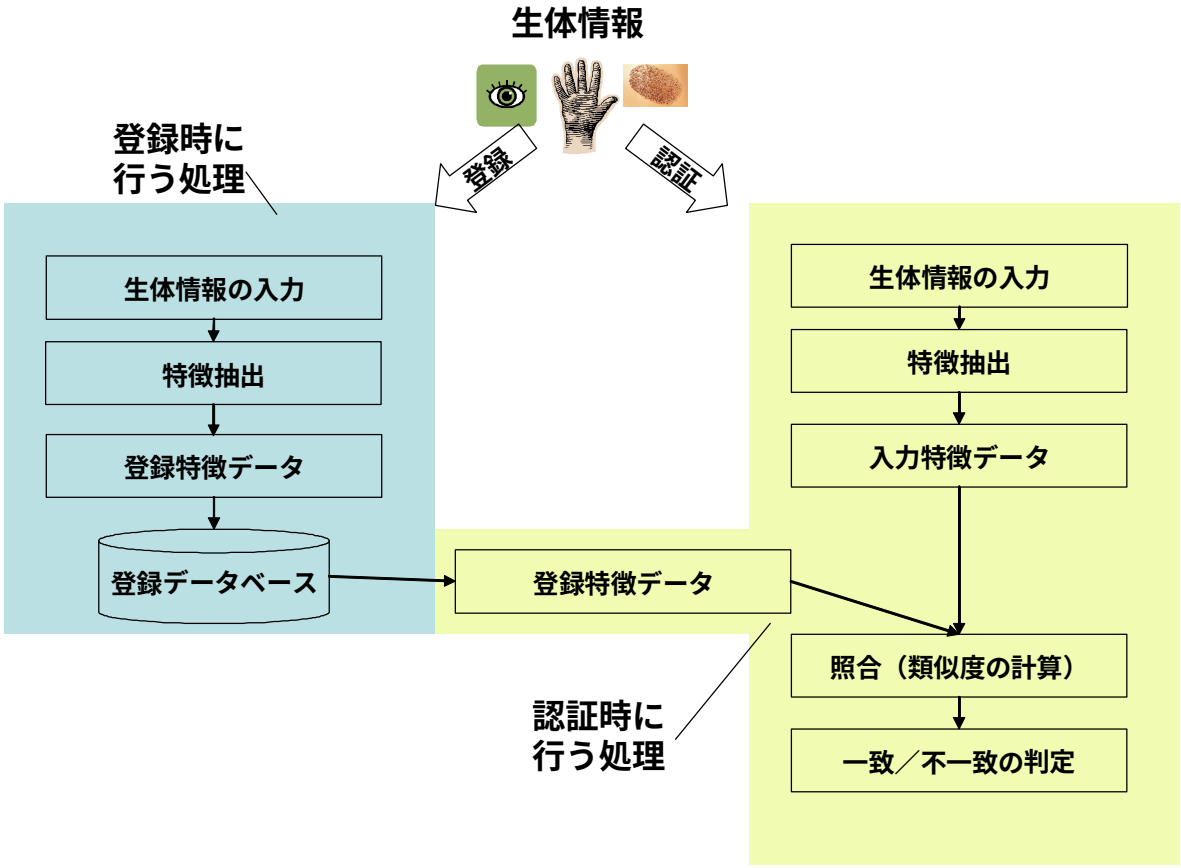


図 1-1 生体認証の処理の流れ

(2)閾値、本人拒否率および他人受入率

生体認証において、どのように閾値を定めても、誤って他人を受け入れる可

能性を 0 にし、かつ誤って本人を拒否する可能性を 0 とすることはできない。生体認証においては、エラーは不可避であるため、環境やアプリケーションに応じて、リスクと利便性の兼ね合いで適切なエラー率の設定を行う必要がある。

誤って本人を拒否する確率を、本人拒否率：FRR(False Reject Rate)と呼び、利便性要件に対応する。一方、誤って他人を受け入れる確率を、他人受入率：FAR（False Accept Rate）と呼び、安全性要件となる。

(3)利便性と安全性のトレードオフ

一般に、本人拒否率を低く抑えようとすれば、他人受入率は高くなる。逆に、他人受入率を低く抑えようとすれば、本人拒否率は高くなる。そして、本人拒否率が高く他人受入率が低い場合、安全性を重視した認証であり、本人拒否率は低く他人受入率が高い場合、利便性を重視した認証であるといえる（図 1-2 参照）。

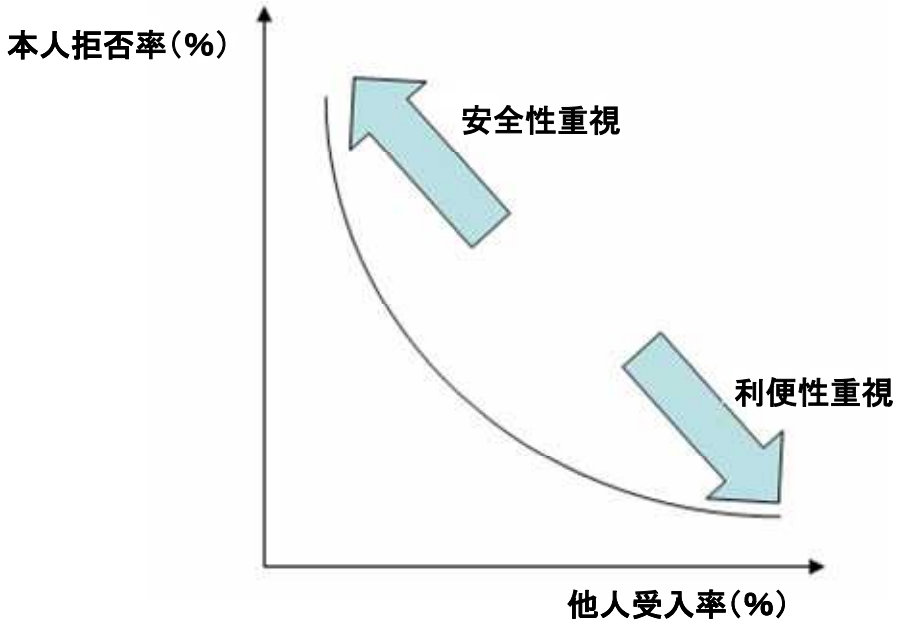


図 1-2 閾値を変化させた際の本人拒否率および他人受入率と、安全性および利便性の関係

(4)対応率

一部の人は、指紋の判別が困難な場合がある。そのため、こうした人々にとって指紋認証技術を利用することは難しい。また、他の生体情報の場合でも、一部の人に対応できないことがある。このように、生体認証の装置あるいは生体認証のアルゴリズムが生体情報を認識できない割合を、対応率と呼ぶ。

メーカでは、対応可能な生体情報のみを用いて精度評価を行っている場合もあり、システム管理者は、対応できない生体情報と対応率を確認することが望ましい。

1.4.ホワイトリスト方式／ブラックリスト方式

生体認証システムは、センサーから入力した生体情報が、システム内部に保管されている生体情報と一致するか否かを判定する。判定は大きく 2 種類に大別される。一方はカードやキー操作で、一致を判定する人物が一人指定される場合であり、照合（1:1 認証）と呼ばれる。もう一方は、一致を判定する人物がリストとして複数指定される場合であり、識別（1:N 認証）と呼ばれる。

識別の処理は、さらに、リストに登録されている人物の種類の違いにより二つの方式に分かれる。権限を与えてよい人が登録されているホワイトリスト方式と、権限を与えてはいけない人が登録されているブラックリスト方式である。

システム管理者は、システムが実現するアプリケーションに応じてホワイトリスト方式とブラックリスト方式を適切に選択することが望ましい。

(1)ホワイトリスト方式

システム内部に保管されているデータベースに登録された生体情報と一致する生体情報を持つ人に権限を与える方式である。あらかじめ登録を済ませた人にしか権限を与えることができないので、限られた人にのみ権限を与えるシステムに適している。

登録人数が多くなるとシステム内部のデータベースに保管される生体情報が増えるため、登録されていない人の生体情報が、登録されている人の生体情報と偶然に一致してしまう確率も増える。そのため、安全性を確保するためには、登録人数が多くなっても他人受入率が増大しないように技術的な配慮が必要である。

(2)ブラックリスト方式

システム内部に保管されているデータベースに登録された生体情報と一致する生体情報を持つ人には権限を与えない方式である。権限を与えたくない人の生体情報のみ登録すればよいので、権限を与えたい人が不特定大規模であらかじめ生体情報を登録できないシステムに適している。

判定のために入力された生体情報がデータベースに登録されている生体情報と一致しない場合は、すべて権限が与えられるので、安全性を確保するためには、本人拒否率を低く維持するように技術的な配慮が必要である。

2.生体認証システム構築と運用の留意点

本章は、生体認証システムの構築に係わるシステム管理者およびシステムインテグレータを対象とする。内容は、システム構築に係わる基本知識および個別対策と、システム運用に係わる基本知識および個別対策から成る。

2.1.構築フェーズに係わる事項

(1)システムの目的と生体認証の使い方の明確化

設計フェーズの最初においては、生体認証を利用したシステムの目的と生体認証の使い方を明確にすることが必要である。

例えば、データセンターのサーバルーム等における機密性の確保が優先される入退室管理システムにおいては､一般に､入退室の手続きが複雑になっても、なりすましを防止することが重要となる。逆に、企業における勤怠管理システムの場合、本人確認を迅速かつ確実に行うことが重要となる。

生体認証を利用するシステムの目的と生体認証の使い方に関しては、以下のように、本人拒否率と他人受入率を設定することにより生体認証の使い方を明確化する。

表 2-1 生体認証を利用するシステムの目的と生体認証の使い方(例)

システムの目的	生体認証の使い方
機密性重視のシステム(例:なりすましを防止し、許可を受けた者のみが確認されることを主目的とする)	他人受入率を低く抑えることに重点を置く
利便性重視のシステム(例:本人の拒否を防止することを主目的とする)	本人拒否率を低く抑えることに重点を置く

(2)認証精度の確保

生体認証において、認証精度は様々な条件により変化する。認証の対象とする生体情報により違いはあるが、以下の事項に関して、生体認証製品毎に条件を確認する。

1) 登録可能人数
2) 生体情報の利用可能年数
3) 被認証者による設定変更の可否
4) 屋外での稼動の可否
5) 耐水性
6) 温度
7) 湿度

8) 照度

千葉工業大学の事例

千葉工業大学では、生体認証機器の傍の窓にブラインドを設置し、太陽光の調整を行っている。

（事例集 p.22 参照）

東海地区信金共同事務センターの事例

東海地区信金共同事務センターでは、生体認証端末にスポットでライトを点灯させることで、調整を行っている。

（事例集 p.27 参照）

(3)生体情報の登録機能

生体情報の登録機能に関して、以下の点に留意する。

1) 生体情報の登録の際に、生体情報以外の情報が入力されないような生体検知機能の有無
2) 生体情報の再登録に際して、過去に登録された生体情報との違いを明示する機能の有無

一般に、上記 1)に関しては、他人受入率を低くすることが望まれる場合等機密性の高いシステムにおいては有していることが望ましい。2)に関しては、利用目的に係わらず有していることをチェックする。

(4)生体情報の管理機能

生体情報は機微情報であるため、生体情報の管理のために以下の機能を設定する。

1) 管理者を特定するためのアクセス制御機能
2) 管理者以外が生体情報を参照不能とする機能
3) 生体情報の改ざんを防止する機能
4) 管理者による生体情報の消去機能
5) 生体情報の保存時の暗号化機能

SBI 損害保険株式会社の事例

SBI 損害保険株式会社では個人の生体情報を暗号化して保存している。

（事例集 p.7 参照）

東陽倉庫株式会社の事例

東陽倉庫株式会社では生体認証装置とサーバの通信に生体認証専用の LAN を使用している。

（事例集 p.9 参照）

(5)生体認証の代替機能

生体認証の代替機能の設定に関して、以下の点に留意する。

1) 代替機能の実現手段の選択(生体認証では対応できない個人にも対応できることが必要である)

2) 代替機能の設定時における認証精度の変化(一般に、代替機能を設定した場合でも、生体認証装置を用いた場合と同等の認証精度を実現することがよい)

2.2.運用フェーズに係わる事項

(1)実運用環境における検証

システムの運用に際しては、実環境における検証を実施する。この検証により、認証精度の変化の様子を見極め、目的に合わせた閾値を設定する。

検証に際しては、以下の点に留意する。

1) 登録人数を実運用と同等にする

2) システム構成や機能を実運用環境と同等にする

3) 温度、湿度、照度、屋内外等の稼動環境を、一日単位、一週間単位、月単位、(可能であれば)年単位で検証する

恵佑会札幌病院の事例

恵佑会札幌病院では、職員及び模擬患者にて、約二週間の試験を行った。

(事例集 **p.16** 参照)

ジェイアール福岡メンテックの事例

ジェイアール福岡メンテックでは、システム導入前には、認証精度の確認を実施し、システム稼動後も含めて、システムの改修を実施して認証率の向上をはかった。

(事例集 **p.17** 参照)

(2)管理手順の策定

管理手順を策定し、管理者運用マニュアルを用意すると共に、管理者の教育を行う。管理者運用マニュアルには、生体情報の取扱い、その他運用等に際しての留意事項として以下の項目を記載する

1) 生体情報を含む個人情報の登録の手順

ー管理者がなすべきこと(対面や必要書類による本人確認の方法を含む)

ー一般利用者にお願いすること

2) 生体情報を含む個人情報の参照のための手順

ー参照可能とする場合の要件

ー参照のための手続きと手順

3) 生体情報を含む個人情報の変更のための手順
　－変更可能とする場合の要件
　－変更のための手続きと手順
4) 生体情報を含む個人情報の消去のための手順
　－消去の際の要件
　－消去のための手続きと手順
5) システム構成変更の手順
　－システム構成変更の要件
　－システム構成変更の手続きと手順
6) 検証の手順
　－検証が必要な場合の要件
　－検証の項目および手順
　－検証の期間
7) 監査の手順
　－監査の時期
　－監査の項目および手順
8) その他運用に際しての留意事項
　－生体認証失敗時（本人受入拒否時）における代替手段
　－事故発生時（他人受入の発覚時、システム故障時等）における対応方法

なお、金融庁が発表している「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」には、生体情報の取扱いに関する記述がある。

三井住友銀行の事例

三井住友銀行では、説明を行う行員が自ら生体認証に精通するよう、導入一ヶ月程度前から、ビデオ映像などを用いた勉強会を開催し、実際に利用する演習も実施した。

（事例集 p.14 参照）

ジェイアール福岡メンテックの事例

ジェイアール福岡メンテックでは、管理者に対して一日程度の講習を行った。

（事例集 p.18 参照）

（事例集 p.17 参照）

(3)システムの設定や変更の作業自体のセキュリティ

システムの設定や変更を行う際には、セキュリティに配慮することが必要であり、以下の事項に留意する。

1) 管理者のみが、設定や変更作業が可能なようにアクセス権限を設けること

2) 管理者の認証には、目的に応じて適切な手段を用いること
3) 設定作業を行う場所に関して、覗き見等が困難であることも考慮すること

(4)利用者向けのマニュアル作成

システムの運用に際しては、予め利用者向けのマニュアルを作成し、必要に応じて適宜改訂する。

利用者向けマニュアルには、以下の事項を含む。

1) システムの目的
   当該システムが機密性の高い場所で利用されるものであるか､利便性を重視するものであるか　等
2) 通常の利用方法
   －生体情報の登録方法(当該システムでの生体情報の登録方法を詳細に記述する)
   －生体認証の方法(当該システムでの生体認証機器を用いた生体認証の方法を詳細に記述する)
   －生体認証失敗時（本人受入拒否時）の対応方法
3) 留意事項
   －通常の運用で発生すること(気象条件や環境条件などにより､本人受入拒否が発生する等)
   －特定の生体情報は永続的ではなく、適宜更新が必要であること　等

(5)利用者向けマニュアルに沿った利用者の教育

システムの運用に際しては、利用者向けマニュアルに沿った利用者の教育を行うことが必要である。利用者の教育には、以下の項目を含むものとし、実運用環境で行うことを重視する。

1) 生体情報の登録方法
2) 生体認証の具体的方法
3) 生体認証失敗時（本人受入拒否時）の対応方法

佐賀県庁の事例

佐賀県庁では､システム導入 3 ヶ月前と 2 週間前に全職員を対象とした説明会を実施し、操作のポイントを分かりやすく解説したビデオファイルやパンフレットを配布した。

（事例集 p.13 参照）

福岡県豊前市の事例

福岡県豊前市では、システム導入時に、全職員を対象として、講習を実施した。

（事例集 p.23 参照）

(6)監査

システムの運用開始後、数ヶ月を経た段階で、システムのセキュリティ監査を実施する。監査に際しては、経済産業省が発表している「情報セキュリティ監査基準」等を参照するとよい。

生体認証システムにおけるセキュリティ監査のポイントは、以下の通りである。

- システムの目的と管理者運用マニュアルの記載事項の対比
- 管理者運用マニュアルと実際の運用の対比
- 他人受入の発生率
- その他

明和地所の事例

明和地所では、竣工後年に一度、また、状況によってはマンションの管理者の判断によって、メンテナンスを行っている。

（事例集 **p.11** 参照）

恵佑会札幌病院の事例

恵佑会札幌病院では、生体認証センサが適切に動作しているかどうかのチェックを随時実施している。

（事例集 **p.16** 参照）

3.付録

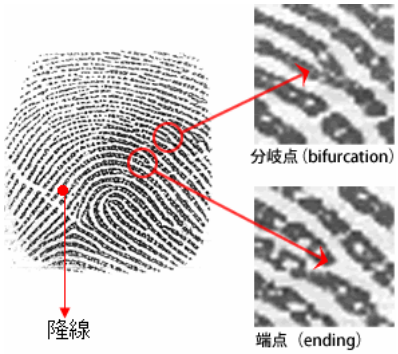
3.1.生体認証による認証技術の種類

生体認証による代表的な認証技術について述べる。

(1)指紋認証

(a)概要

指紋は皮膚が線状に隆起した隆線（りゅうせん）が多数集まったものである（図 3 -1 参照）。



オンラインマガジン「COMZINE」2004 年 3 月号
（http://www.nttcom.co.jp/comzine/no010/dragnet/）に一部加筆

図 3-1 指紋の隆線、分岐点、端点

指紋認証の方法は、隆線の分岐や終端部分を指紋特徴点（マニューシャ）と呼び、特徴点の位置・種類・方向等を計算する方式（マニューシャ方式）と、指紋全体をデータ化しパターンマッチングする方式（パターンマッチング方式）に分けることができる。

(b)特徴

指紋認証の特徴は、以下に整理できる。

- 技術の成熟度が高い
- 水分や傷等に左右されることがある
- 導入コストが安い
- 指紋登録の困難な人が居る場合がある

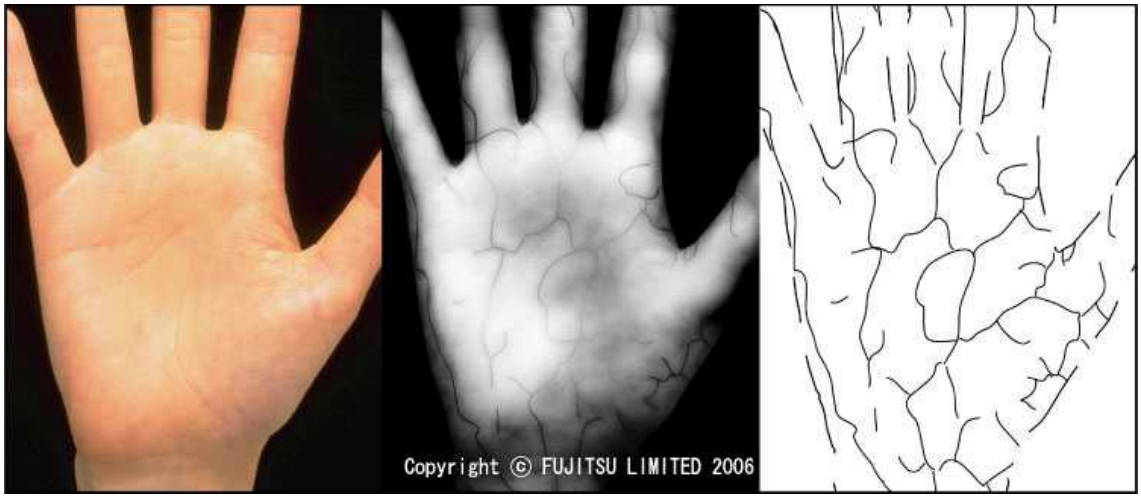
(2)静脈認証

(a)概要

静脈や動脈などの血管のパターンは、唯一性と永続性を有する。さらには、体の中の情報であるため、体の外からの覗き見されること、外的要因により変化することが少ないと考えられている。

静脈認証には、手のひら静脈認証、手の甲の静脈認証、指の静脈認証があり、金融機関では、手のひら静脈認証と指の静脈認証の導入が進んでいる。

静脈認証の方式は、赤外線カメラにより手のひらや指を撮影し、その結果から静脈のパターン（図 3-2 参照）を抽出する。抽出後の静脈のパターンのデータの取り扱い方法は、指紋認証と同様に、マニューシャ方式またパターンマッチング方式に分けることができる。



(a) 一般のカメラで撮影した画像　(b) 赤外線カメラで撮影した画像　(c) 手のひらの輪郭および抽出した静脈パターン

図 3-2 手のひらの静脈パターン

(b)特徴

静脈認証の特徴は以下に整理できる。

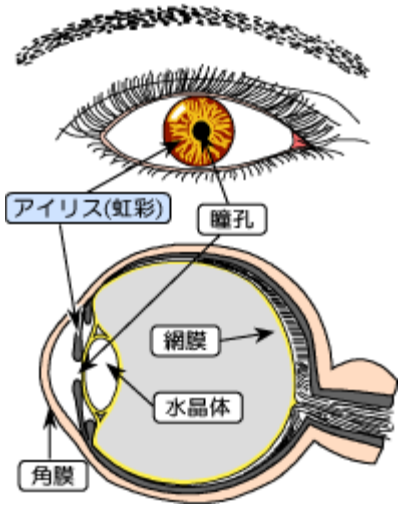
- 偽造が困難である
- 導入コストが高い
- 登録不可能な人が少ない
- 認証精度が高い

(3)虹彩認証

(a)概要

眼球の黒目部分には、瞳孔の拡大や縮小のための筋肉から成る虹彩(アイリス)（図 3-3 参照）と呼ばれる環状の部分がある。筋肉には細かい皺があり、この皺は人が 2 歳を迎える頃からほとんど変化しないことが知られている。虹彩認証は、この皺のパターンをカメラで撮影することにより認証を行うものである。コンピュータで虹彩のパターンを抽出して認証する。

第１図 アイリスとは



社団法人自動認識システム協会 JAISA

（http://www.jaisa.or.jp/action/group/bio/Technologies/Iris/Irs-00.htm）図１より引用

図 3-3 虹彩（アイリス）

(b)特徴

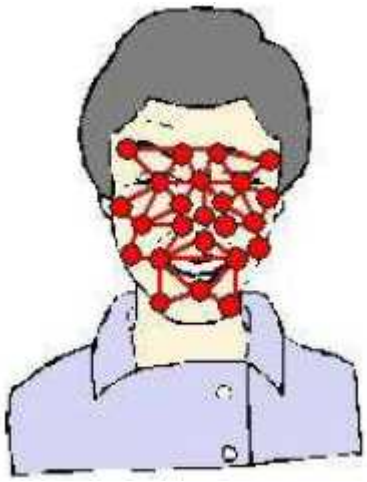
虹彩認証の特徴は、以下に整理できる。

・ 他人受入率が非常に低い
・ 偽造が困難である
・ 導入コストが高い

(4)顔認証

(a)概要

顔認証では、顔の形や目鼻などの位置関係を示す特徴的な点や輪郭線等を画像認識技術により抽出し（図 3 -4 参照）、特徴点間の距離や角度、輪郭線の曲率等や、顔表面の色や濃淡等の特徴量により顔を識別する。



平成 16 年度標準技術集「バイオメトリック照合の入力・認識」5－1－1－3－2 顔特徴点検出
（http://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/biometric/5-1-1.pdf）より引用

図 3-4 顔認証に用いる特徴点（例）

(b)特徴

顔認証の特徴は、以下に整理できる。

・ 一般の利用者の登録時および認証時の負荷が少ない
・ 角度により、本人を拒否する場合がある
・ 数年で再登録が必要となる

(5)音声認証

(a)概要

音声認証は、音声信号を時間と周波数の分布で表したサウンドスペクトログラムあるいはこれと等価な情報を持ったパターンに変換し，そのパターンの比較により、個人の照合を行う技術である（図 **3 -5** 参照）。

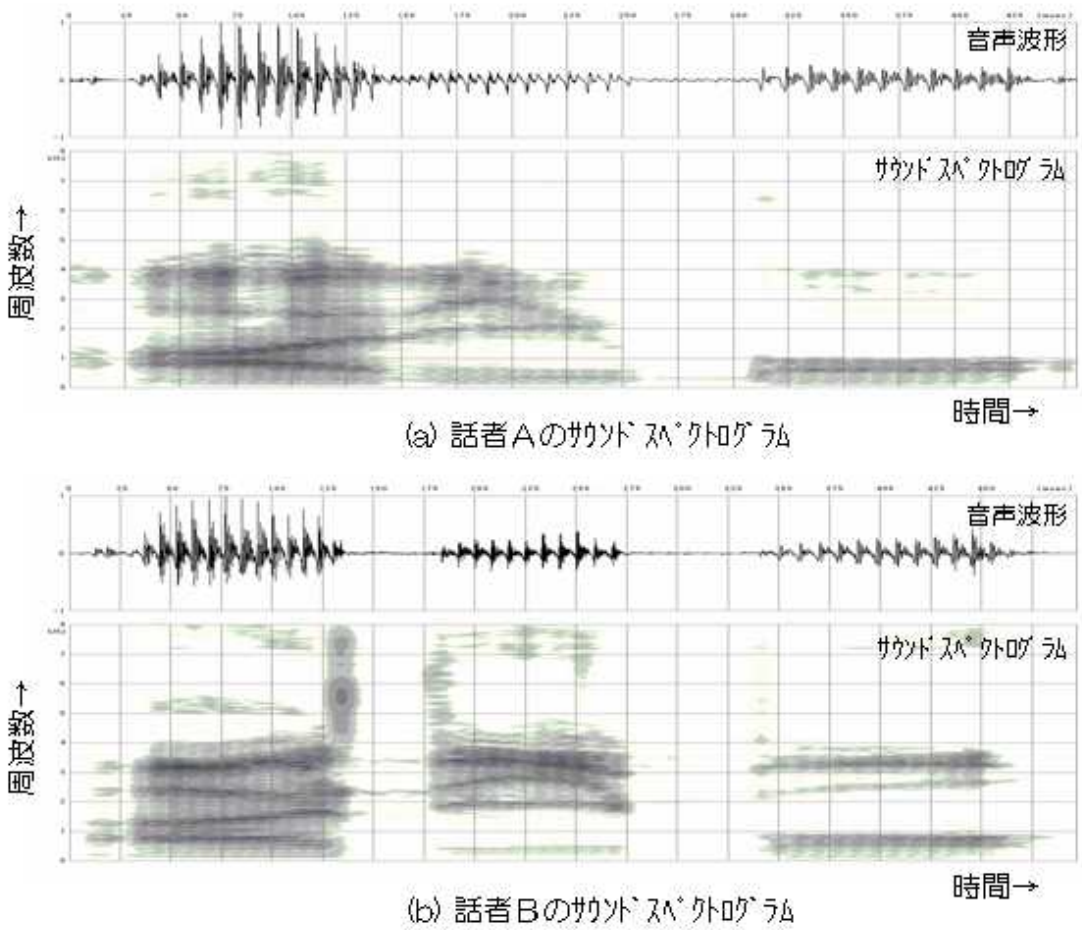


図 3-5 音声認証の個人パターン

(b)特徴

音声認証の特徴は、以下に整理できる。

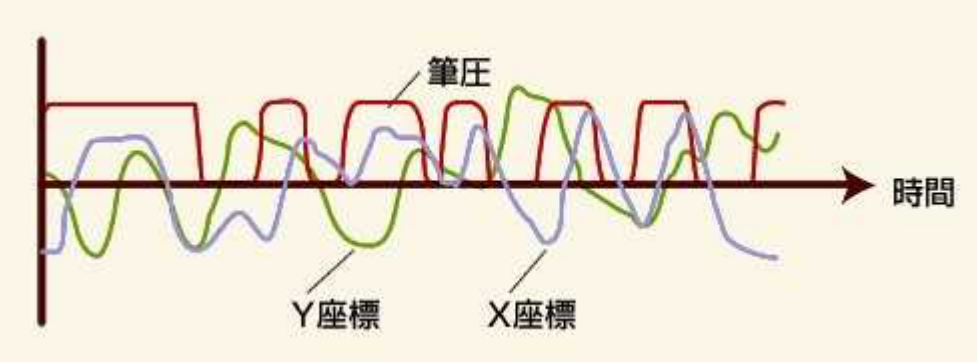
- マイクとソフトウェアの導入によりシステムを構築できるため､安価である
- 健康状態等により音声の波形が変化するため､その際には本人拒否や他人受入の可能性が高まる
- 雑音により、本人拒否率が高まる場合がある

(6)サイン認証

(a)概要

サイン認証とは、タブレットなどの座標入力装置上に筆記されたサインに関

して、ペン先の座標、筆圧等を一定時間間隔で収集して入力情報を獲得し、あらかじめ登録されている登録情報と照合することにより、本人を確認する技術である（図 3-6 参照）。



ウィッツェル株式会社ホームページ
（http://www.witswell.co.jp/cybersign/wm/syogo.htm）より引用

図 3-6 サイン認証に用いるペンの位置と筆圧の変化

(b)特徴

- 登録情報は、本人の意思により別の登録情報に置換できる
- けが等により本人が署名不可能となる場合がある
- 他人のなりすましに関しては、他の生体認証より比較的容易である