バイオメトリクス
I

目次

バイオメトリクス技術と本人認証

バイオメトリクスとは？

定　義

行動的あるいは身体的な特徴を用い、個人を自動的に同定する技術。
Biometrics deals with identification of individuals based on their biological and / or behavioral characteristics.

性　質

●普遍性(Universality)：誰もが持っている特徴。
●唯一性(Uniqueness)：本人以外は同じ特徴をもたない。
●永続性(Permanence)：時間の経過とともに変化しない。

Biometrics = Biology + Metrics

認証の分類

■認証とは、真正性(Authenticity)の証明。
- サービスなどの要求者が適正である。

■認証 ＝ 識別(Identification) ＋ 検証(Verification)
- 識別(Identification)：類似度がしきい値以上でもっとも近いものの探索。
  - システムに提示された情報とあらかじめシステム内に登録された情報を比較し、閾値以上のものを探索。
- 検証(Verification)：類似度がしきい値以上の特定。
  - 本人の特徴を示す情報とシステム内の登録情報との1対1の対応関係確認

■認証
- 本人認証（本人であることを認証）
- 権限認証（権限の保有を認証）
- 同一性認証（情報が同一であることを認証）

本人認証

■知識(秘密情報の保持)・・・What you know

- ●パスワード(暗号番号)、合言葉。
- ●紛失や他人による盗み見、不注意に書き残して漏洩などの危険性。

■所有物(唯一物の所持)・・・What you hare

- ●IDカード、印鑑、証明書。
- ●奪われたり、貸し借り、紛失、偽造などの危険性。

■バイオメトリクス・・・What you are

- ●身体的特徴、行動的特徴。
- ●忘失や紛失の危険性がない、他人による成りすましが困難。
- ●組み合わせにより高い安全性が確保。
- ●非対面、疎結合なネットワークほどセキュリティ対策が困難。

本人認証方式の比較

	パスワード	ICカード	バイオメトリクス
認証媒体	知識	所有物	身体的・行動的特徴
安全性	× 盗用・忘失の危険	× 盗用・紛失・破損・偽造	◎ 偽造は他の方式に比べ困難
簡便性	△ キーボード入力	○ カードリーダへの挿入の危険	○ 登録に時間がかかる場合あり
経済性	◎ パスワード管理コスト	△ メンテナンスコスト発生	○ 初期コストが高くても ランニングコストが低い
社会的受容性	○ これまで使ってきた	○ カード利用は馴染んできた	△ 他の方式より 抵抗感を感じる人は存在

バイオメトリクスの種類と概要

特徴	種類	概要
身体的特徴	指紋	認証精度は高い。 高齢者・幼児・手荒れ指・乾燥肌対応が課題。
	掌形	手の物理的大きさ。 入力が簡単。
	虹彩	虹彩模様をコード化。 認証精度は高い。
	顔	顔部品配置・輪郭の特徴点。入力が簡単。 認証精度、耐環境性などが課題。
	静脈	比較的新しい認証方式。新規採用事例が増加。 指紋認証に比較し、偽造困難・使えない人がいない。
	その他	網膜、耳介、DNA。
行動的特徴	音声	音声波形を分析。コード化。電話での認証可。 雑音の影響を受ける。
	署名	署名時の書き順、筆圧等動的特徴。 模倣される可能性。欧米では利用実績がある。

バイオメトリクスの歴史と事例

歴　史

- 1980年初～　犯罪捜査(指紋)
- 1980年中～　重要施設入退室管理
- 1990年中～　ネットワークでの本人認証

事　例

- 社会福祉カードなどでの多重登録防止(年金)
- 出入国管理(US-Visit)
- 金融(ATM)
- 監視(防犯カメラ)

バイオメトリクス技術の歴史

■指紋認証の歴史

- ●1685年　ネミヘア・グルーが、皮膚紋理に関する論文を発表。
- ●1858年　ウイリアム・ハーシェルが、年金の支払いの適正化の為に、指紋採取・照合を利用。
- ●1880年　ヘンリー・フォールズによって学会に発表された。
  （人間の指先の腹の部分には渦の文様があり、世界中の人間の紋様は全て違う。）
- ●1891年～　指紋を画像として採取し、その画像を処理し、様々な分析方法を考案。
  ガルトン法・ヘンリー法・ヴィセッチ法・ロッシェル法。以降各国で、様々な処理方法を解析。
- ●1911年　日本においても指紋法が成立。
- ●1971～74年　警視庁は、コンピュータ処理による指紋鑑定を本格的に開始。
- ●1995年～　入退室からPC等、急激に実用化が進展。

■顔認証の歴史

- ●顔認証は、日本の金出教授(現在米・CMUロボティックス研究所所長)が、京大で行った研究から始まる。
- ●1993年～　米・陸軍研究所が中心となって行った顔認証アルゴリズム・コンテスト共通の
  評価データベース基盤を持ったことにより、急速にアルゴリズムが発展。
- ●1997年～　Visionics Miros Viisage などの米国メーカーが商品化を開始。

■虹彩認証の歴史

- ●虹彩認証は、ドーグマン博士(John Daugman)のアルゴリズム、イリディアン社(Iridian Technologies)。

■静脈認証の歴史

- ●1998年　韓国明知大学の崔煥洙教授　手の甲静脈。
- ●2002年8月　富士通　手のひら静脈。
- ●2003年9月　日立　指静脈。

バイオメトリクス認証技術の比較

種類	唯一性	永続性	コスト	データ量（バイト）
指紋	◎	◎	◎	250–1,000
掌形	○	○	△	10
顔	△	△	○	2,000–3,000
虹彩	◎	◎	△	256
声紋	△	△	◎	1,500
署名	△	△	○	1,000
静脈	○	○	△	500

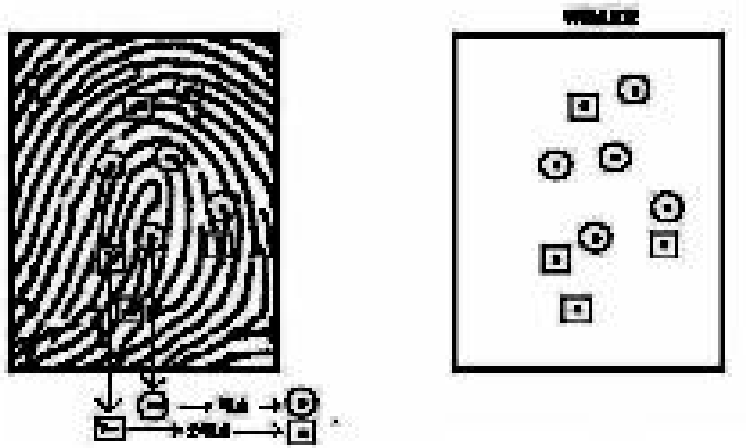
バイオメトリクス技術の比較

生体情報	一般性	ユニーク性	永続性	収集性	精度	受容性	脅威耐性
顔	○	△	○	◎	△	○	△
指紋	◎	◎	◎	○	◎	○	◎
掌形	○	○	○	◎	○	○	○
静脈	○	○	○	○	○	○	◎
虹彩	◎	◎	◎	○	◎	△	◎
網膜	◎	◎	○	△	◎	△	◎
耳	○	○	◎	○	○	◎	○
顔の赤外画像	◎	◎	△	◎	○	◎	◎
DNA	◎	◎	◎	○	◎	△	△
動的署名	△	△	△	○	△	◎	△
声紋	○	△	△	○	△	◎	△

バイオメトリクス技術

指紋認証　まとめ

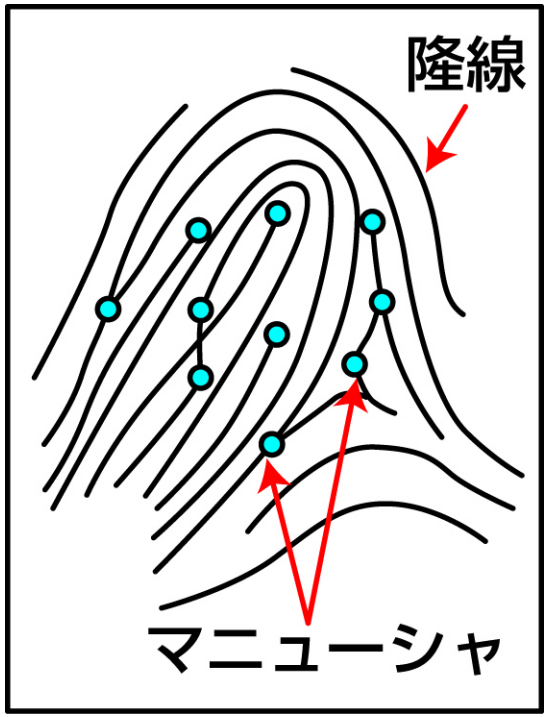
(1)職業柄及び肌荒れ体質等、
　指紋登録・照合の不可能な人の
　存在があり、システム上の考慮が
　必要。
(2)過去、犯人捜査利用の観点から、
　指紋採取の悪イメージがあったが、
　普及とともに薄れつつある。
(3)指紋は顔・虹彩等と異なり、
　10本（個）のデータ採取が可能。
(4)センサは光学式と半導体方式、
　および平面型とスウィープ型。
(5)代表的なアルゴリズム
　・マニューシャマッチング方式
　・マニューシャリレーション方式
　・パターンマッチング方式



●指紋の盛り上がった部分を
「隆線」(Ridge)と呼ぶ。
●この隆線の始まりあるいは終わりの
部分を「端点」(Ridge ending)と呼ぶ。
●隆線が分岐しているところを
「分岐点」(Ridge bifurcation)と呼ぶ。
●これらを総称して「特徴点」
(Minutia)と呼ぶ。

指紋認証　歴史

- 19世紀、植民地時代のインドで体系的に利用。
- ヘンリー・フォールズ学会発表(1880)
- 紋様の分類、隆線の端点・分岐点に注目。
- 20世紀に検索用コード化、統計的一致率の推定。

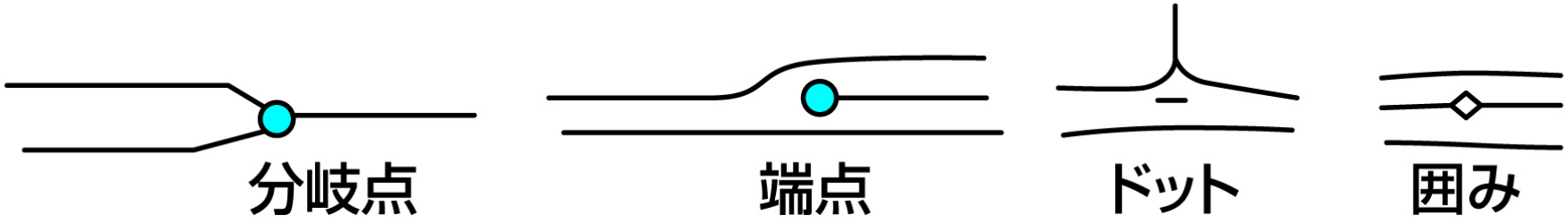


AFIS: Automated Fingerprint Identification System.

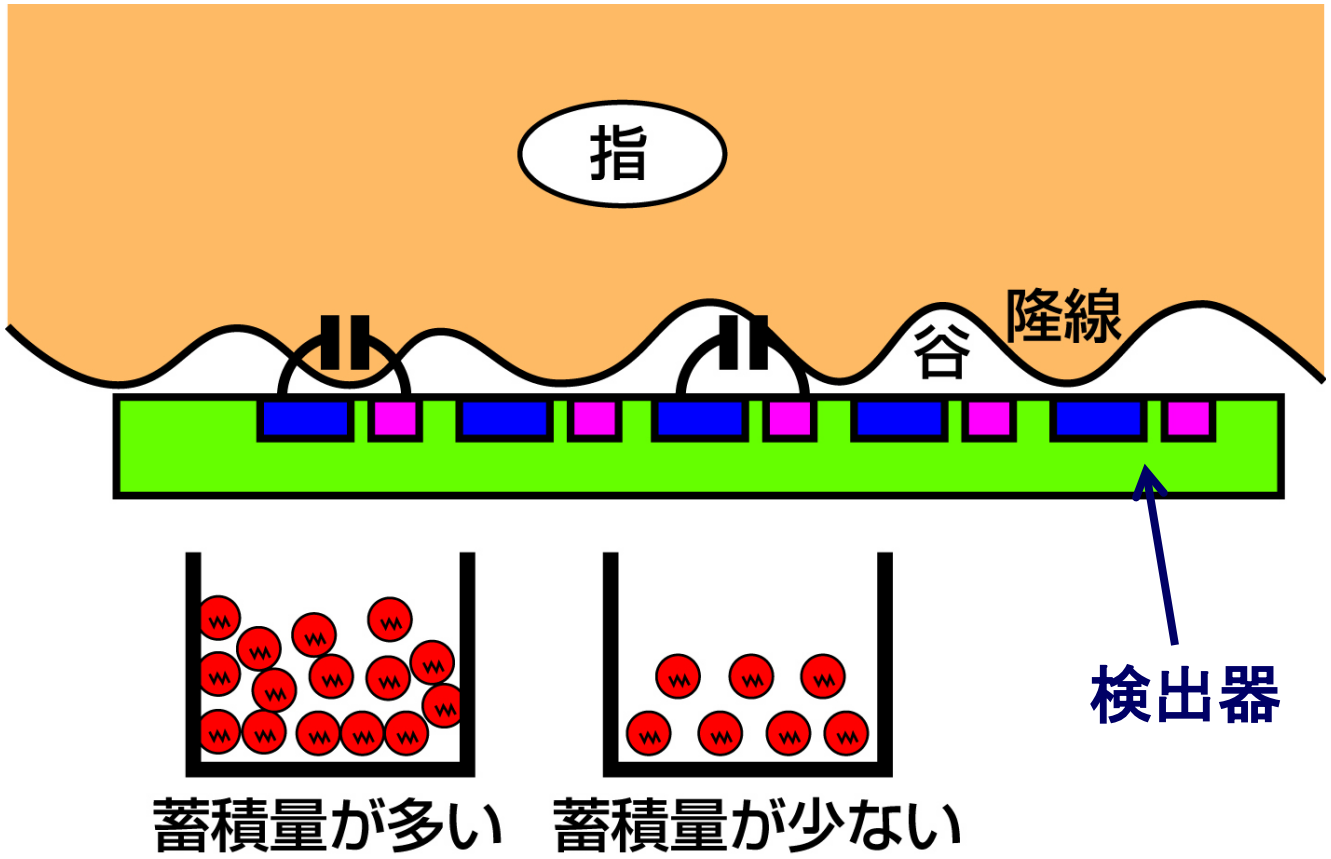
指紋認証　指紋の分類とマニューシャ

分　　類

マニューシャ：Minutia（Minutiae）

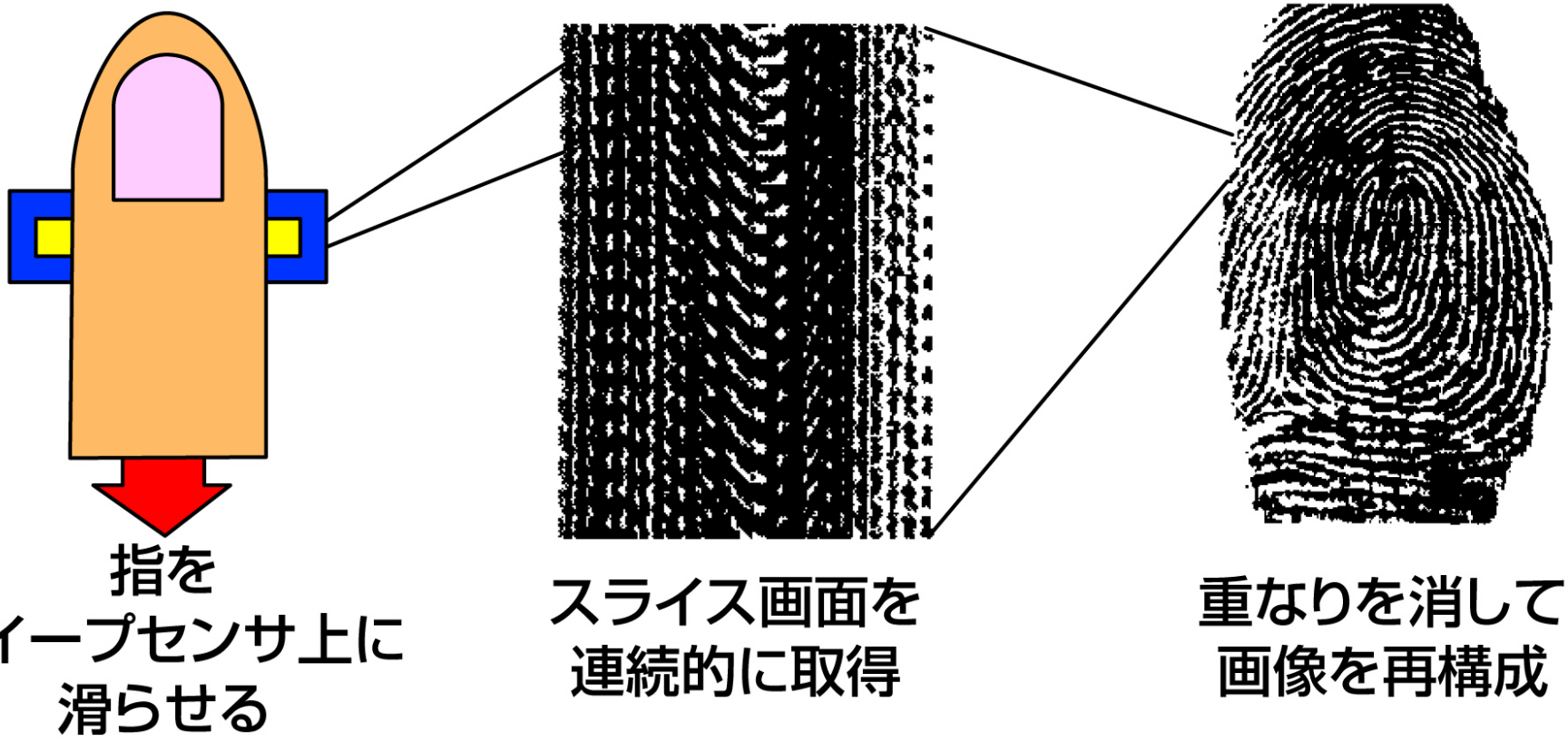


指紋認証　面型静電容量センサ



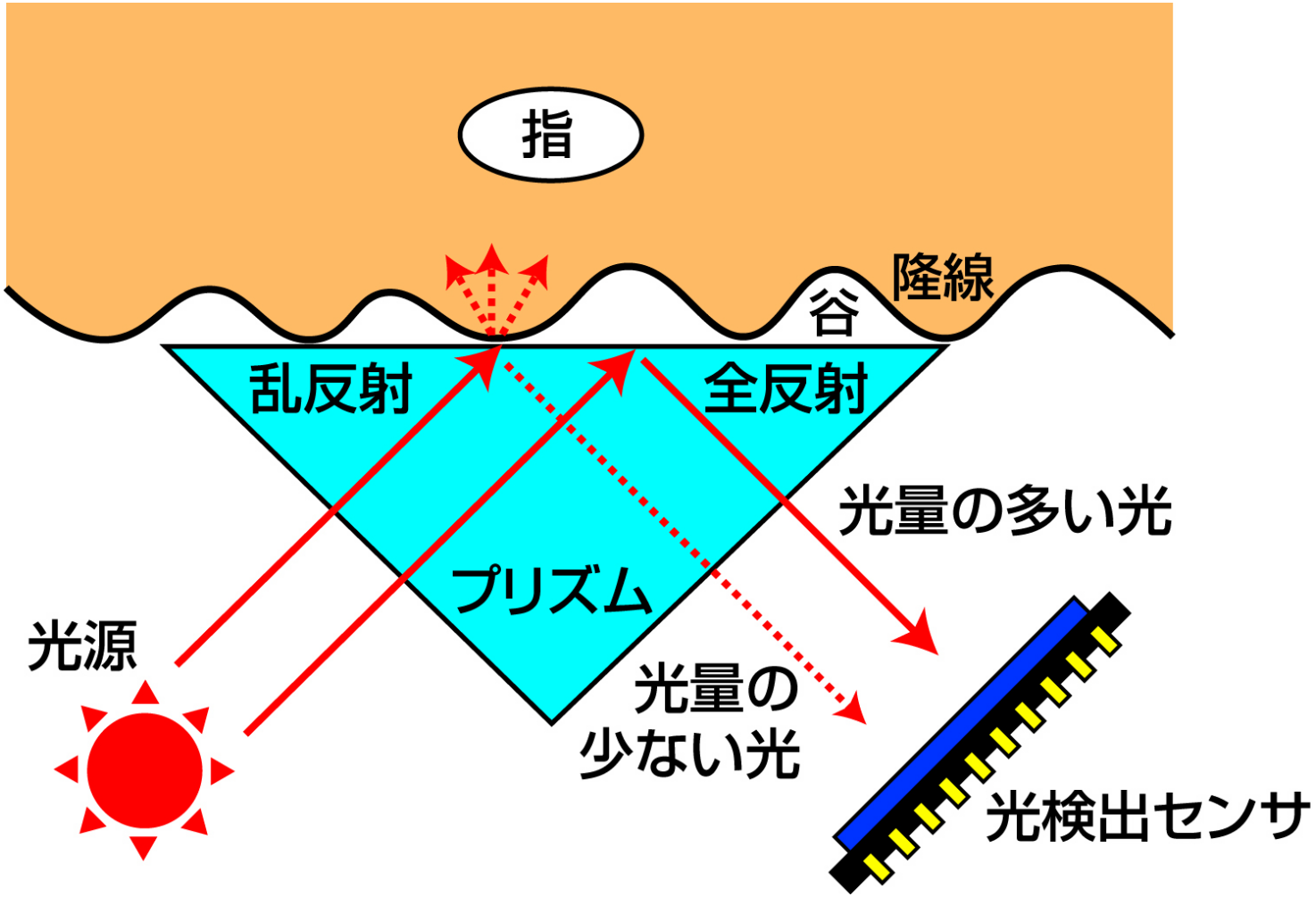
- 半導体製造プロセスで生産されるので比較的安価である。
- 面積が大きいので通常のICチップよりは高い。
- 濡れた指は不適。

指紋認証　スイープセンサ



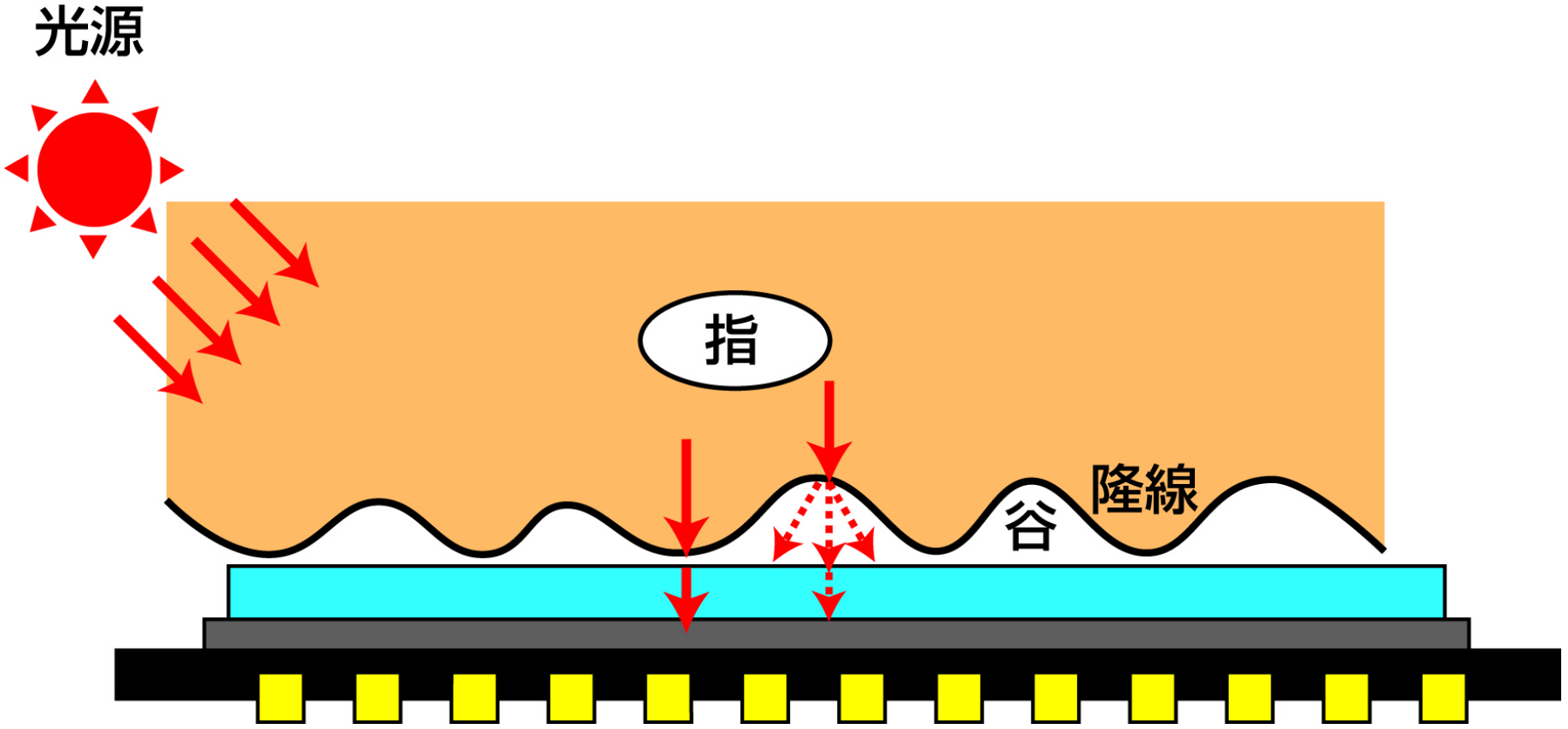
●ラインセンサでFAXのように連続的に取り込む。
●小さいのでモバイル機器のように実装する場所が小さいところに使用できる。

指紋認証　プリズム型センサ



●従来からよく使用されてきたもの。
●構造的に大きくなってしまうので、小型化は難しい。

指紋認証　指内散乱光方式センサ



●指の中を通った光の強弱から紋様を検出するので、
乾燥指や汗で濡れた指でも読み取れる。

指紋認証　照合アルゴリズム

アルゴリズム	特　　徴
マニューシャ マッチング方式	●隆線の端点や分岐点といったマニューシャを利用した方式。 ●マニューシャの個数、相対的な位置関係などの情報を 指紋データとして使用する。 ●相対的な位置関係を利用することにより、 指の置き方による変形が起こっても、 認証精度を確保できる。
マニューシャ リレーション方式	●マニューシャを使用した方式。 ●マニューシャのほかに、マニューシャ間を通る隆線の本数を 合わせて指紋データとする。 ●隆線の数を利用することにより、マニューシャの相対位置の 類似や変形による誤認証を防ぐことができる。
パターン マッチング方式	●隆線が作る紋様の一部を指紋データとして使用する方式。 ●マニューシャを利用する方式に比べ、データの容量が 大きくなってしまう。

顔認証　まとめ

(1)顔認証の最大の特徴は、
非接触性、非拘束性。
自然な認証で心理的
抵抗感が少ない。
(2)不正に対する心理的
抑止効果。
(3)認識率は撮影条件
(向き、明暗、撮影機器等)
に左右され、一般に
認識率は低い。
(4)成長につれて少しずつ
変化し、特に幼少時は
変化が大きい。
(5)プライバシーへの配慮が
必要。

顔照合方法

学習時

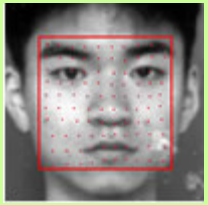
多くの人/多様な
表情・向き・照明状態の
顔画像データセット

①両目・鼻・口の位置を指定して
平均顔を構成し、サンプル点
(データ比較点)を設定。
②各画像のサンプル点の近傍
パターンを解析し、個人性を
豊かに表現できる特徴量
データの作成方法を構成。

平均顔

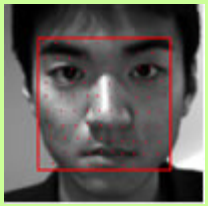
照合時

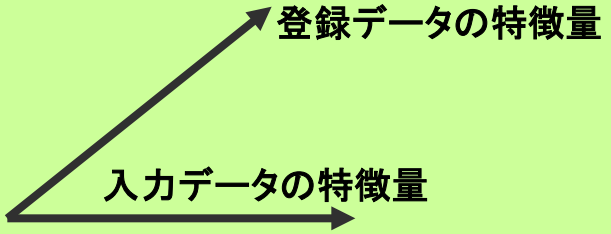
登録画像



①登録画像および入力画像の
サンプル点を検出して
特徴量データを作成。
②両特徴量データベクトルの
向きを比較し、類似度を求める。

入力画像





●特長点(量)主として鼻・眼・口の位置関係、
それらの部位輪郭付近の関係位置。
事例として平均顔との比較。

顔認証　歴史と特徴

歴史

- 金出教授が京大で研究開始（1973）。
- 米国陸軍研究所が中心となったFERETコンテスト（1993）･･･共通評価DB。
- 1997年ごろから米国で製品化（Visionics, Miros, Viisage）。
- 電子パスポートには、顔データが入る。

顔認証アルゴリズム
FacE REcognition
Technology

長所

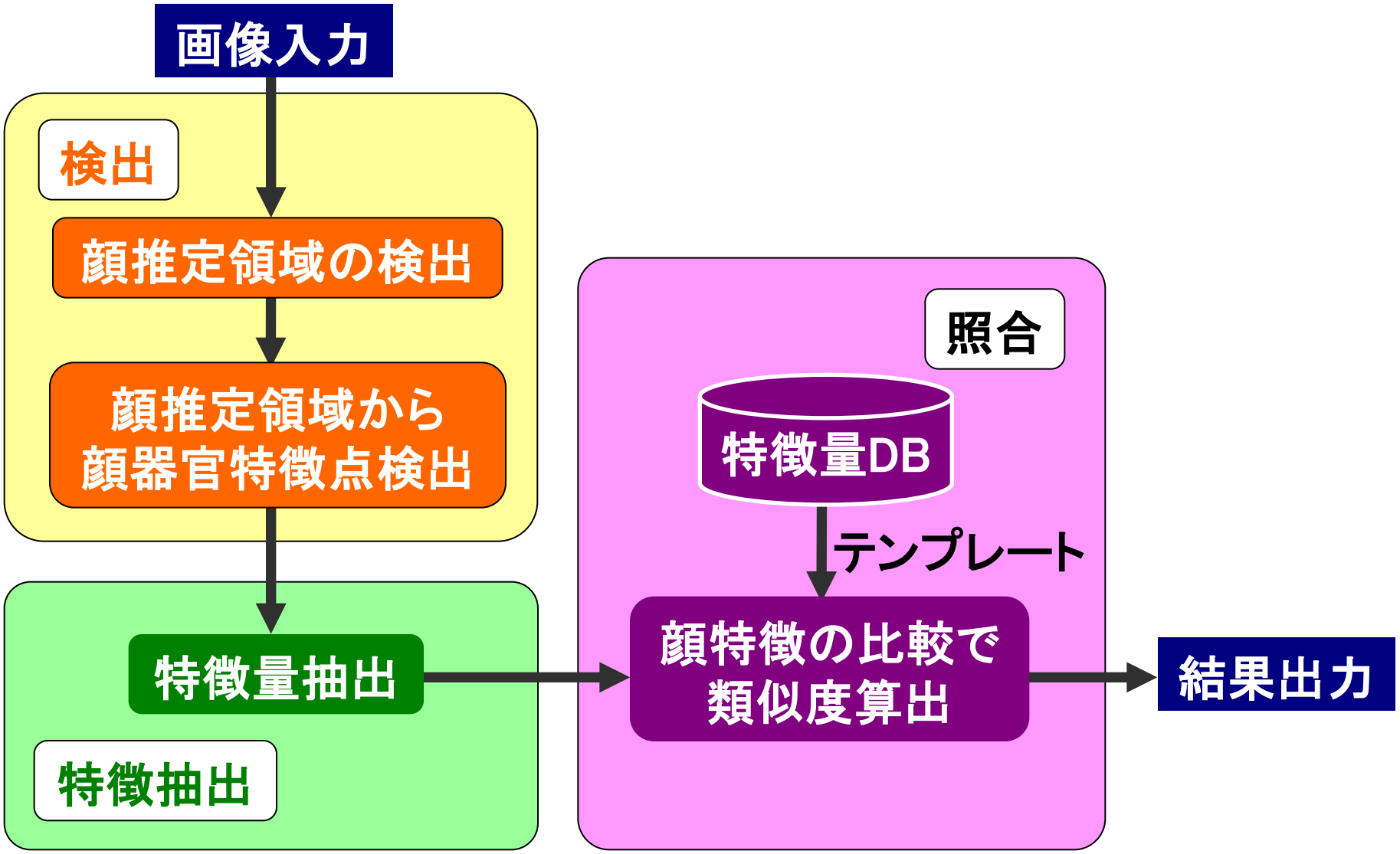
- 心理的抵抗が少ない。
- 離れたところから認識可能（気づかれずにも可能）。
- 従来から本人認証に利用されており自然。
- 映像記録できることから不正に対する心理的抑制効果。

短所

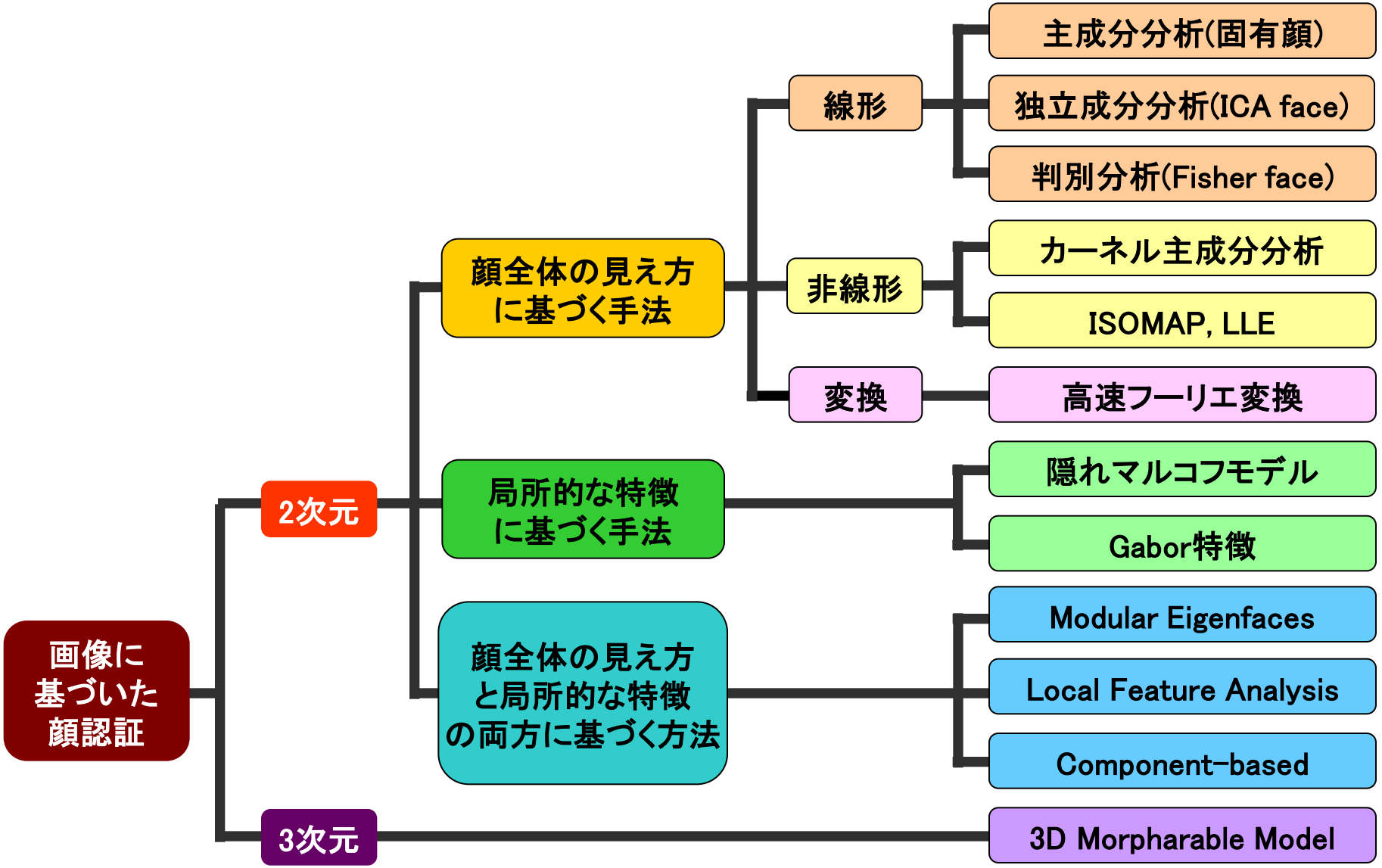
- 双子などの厳密な識別は困難。
- 照明変化、顔の向き、表情変化、サングラスやマスク、経年変化に弱い。
- 公共の場所では、プライバシー保護が問題になる可能性がある。

正面顔を対象としたものが認識率が高く、実用化も多い。

顔認証　処理フロー



顔認証　特徴量抽出に基づく分類



顔認証　特徴量抽出

顔全体の見え方による方法

●顔の領域内の濃淡情報全体を用いて、その顔の特徴とする方法。
●顔の少しの位置ずれに対して敏感。
●細かい表情の変化、髪型の変化に強い。

局所的な特徴を用いる方法

●顔画像の局所的な濃淡変化の間隔と、方向成分を特徴量として認識する方法。
●顔全体の見え方は顔の向きにより変化するが、小領域に注目すれば、あまり大きく変化していない領域があるので、顔の向きの変化に強い。

顔全体の見え方と局所的な特徴の両方に基づく方法

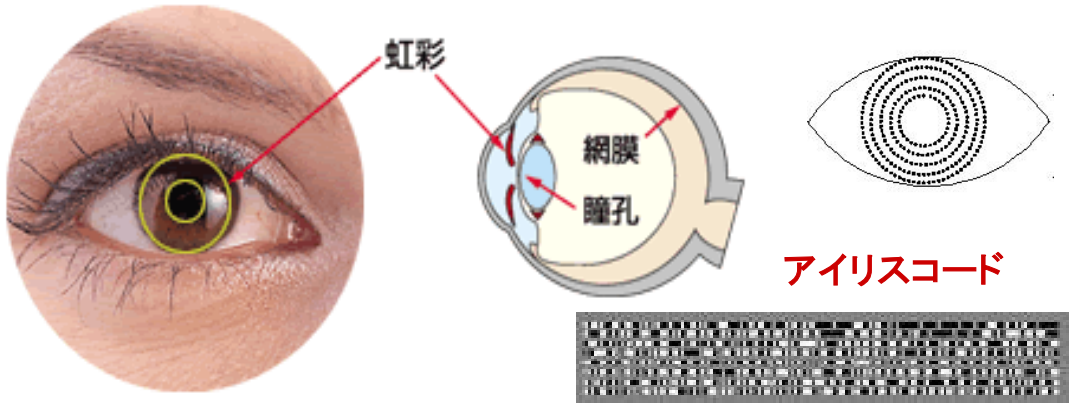
●両者の長所を生かした特徴抽出が可能になり効果的。

3次元モデルによる方法

●予め3次元形状と顔全体の見え方の2つに対して標準的なモデルを持っておき、認識時にはその両方を任意の入力顔に適合させるという方法。
●計算時間が長く、モデルを記述するためのデータサイズが大きい。

虹彩認証　まとめ

(1)認識精度が
　非常に高い。
(2)完全に非接触にて
　認識が可能。
(3)虹彩は人の成長に相
　似変化し、模様配列
　は生涯不変、周囲の
　影響は受けない。
(4)本人と他人の分布が
　はっきりしているため
　1:Nの認識に
　適した方法である。

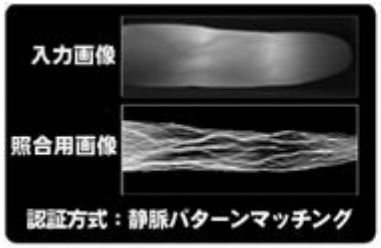


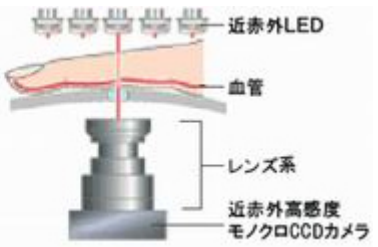
●照合アルゴリズムに用いる特徴量としては、ドーナツ状部分を帯状に広げたアイリスコード（Iris code)を用いる。
●カメラからの得られた目画像から、アイリス部分を抽出する。
●目蓋等により隠された範囲を割愛して、特徴量を用いる。
●黒目の外側からアイリス部分を8層のリング状のエリアと、中心から放射状の線に区切られた微細なセルがあり、個々の濃淡を抽出する。
●この濃淡変化配列を、デジタル化してデータ化する。

静脈認証　まとめ

(1)指紋等バイオメトリクスの使えない人の存在があったが、**対応率が極めて優秀**。
(2)身体内部情報であり、他のバイオメトリクスに比べ**偽造が困難**。
(3)接触部分が少なく、利用者の心理的抵抗感は少ない。
(4)歴史は浅く、実績は乏しいものの、金融機関で採用。

指
静脈





手のひら
静脈

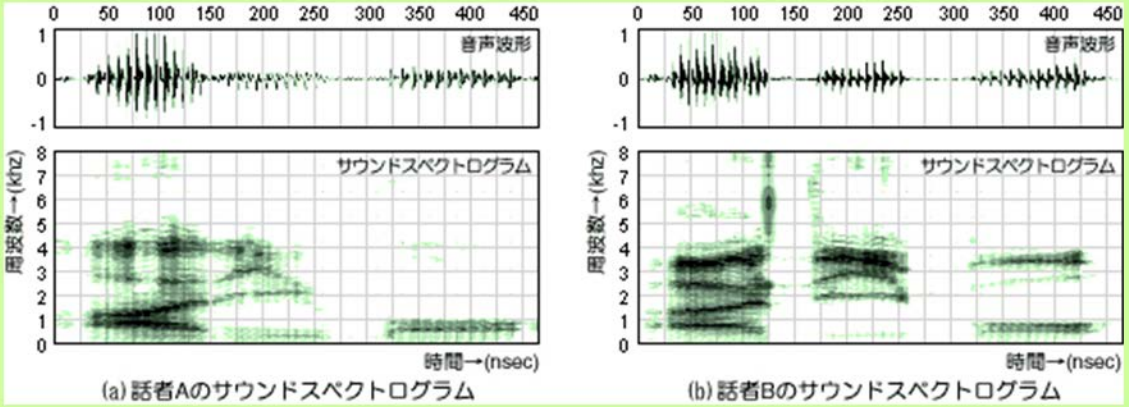
- 指静脈は透過光、手の甲、手のひら静脈は反射光を用いている。
- 血管には酸素を多く含んだ血流（動脈）と、酸素が少ない部分（静脈）があるが、近赤外線を照射した場合の吸光度合いの違いが、パターンとなって現れる。
- そこに現れた平面的な血管分岐点における分岐角度や分岐点間の血管長を、特徴量としている。

静脈認証　静脈パターン認証比較

部位	指	手のひら	手の甲	網膜
光源	近赤外線	近赤外線	近赤外線	近赤外線
画像取得方式	透過光	反射光	反射光	反射光
認証方式	パターンマッチング	パターンマッチング	分岐特性比較及びパターン比較	パターンマッチング

声門認証　まとめ

(1)課題は周囲の雑音。
　(背後の他人の声、
　電話のベル音や騒音)
(2)登録時の雑音は
　致命的。
(3)朝の寝起きの声や
　風邪引きの声
　(かすれた声・鼻声)は
　通常とは異なる。
(4)電話やネット取引の
　ために活用されていく
　傾向は注目。



※横軸は時間、縦軸は周波数

- 人間の声には個人差があり、
  発する音声を構成する音声信号の
  周波数成分が、人それぞれ異なる。
- この周波数成分から抽出した
  声紋データを事前に登録し、
  同じ言葉の声紋データと照合する
  話者照合方式。

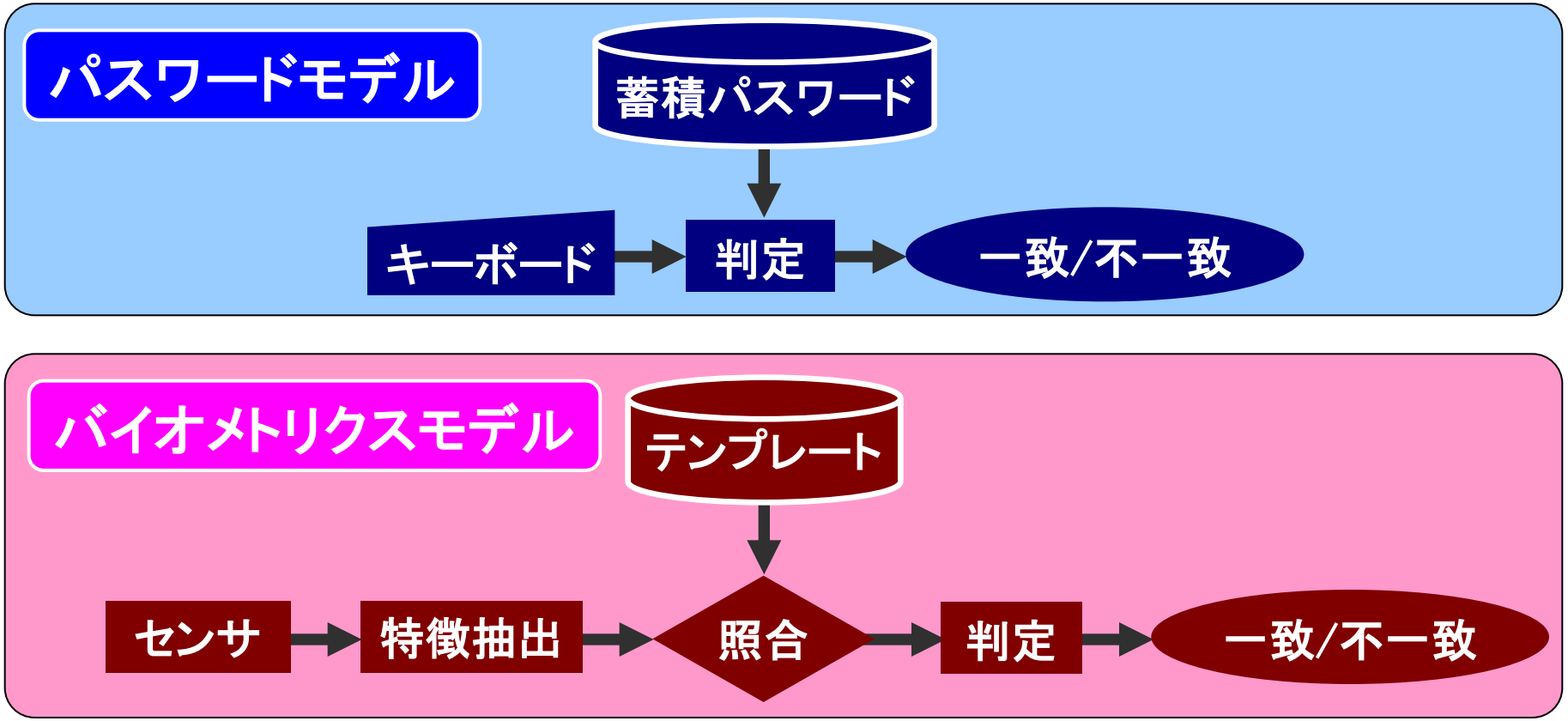
バイオメトリクス装置の選択

項目	評価指針
利便性	簡単に提示でき、短時間で結果が出る。
適用性	万人が使うことができる。
精度	個人識別精度が高い。
頑健性	詐称などの攻撃に強い。
経済性	守る価値に対して十分安価である。
安全性	利用者への影響がない。

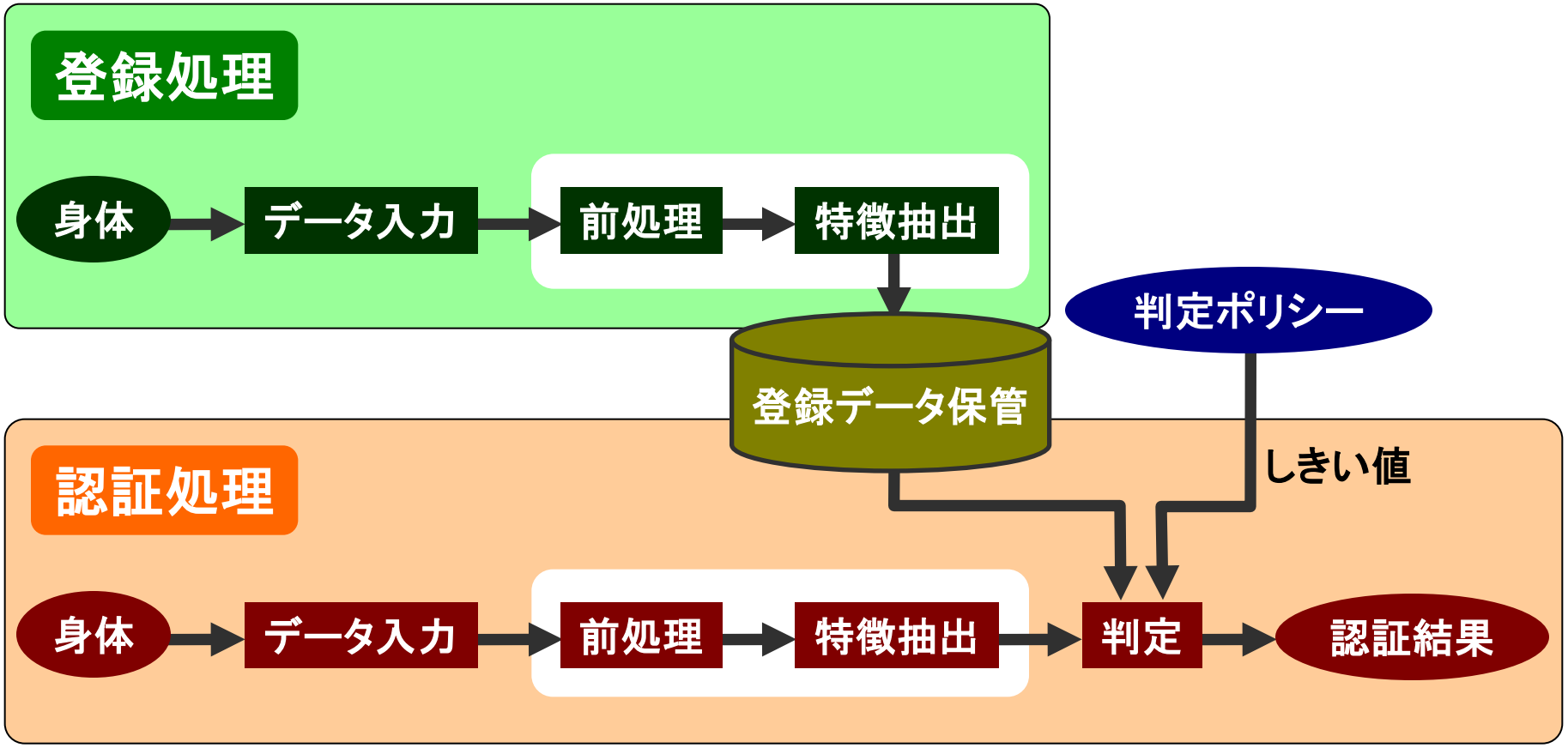
バイオメトリクス認証モデル

認証モデル

●認証(Verification):1対1照合・・・2つが同一であるか否か。
●識別(Identification):1対N照合・・・複数のどれと同一であるか。
Watch list:1対N (DB内に登録されているかの判定)。



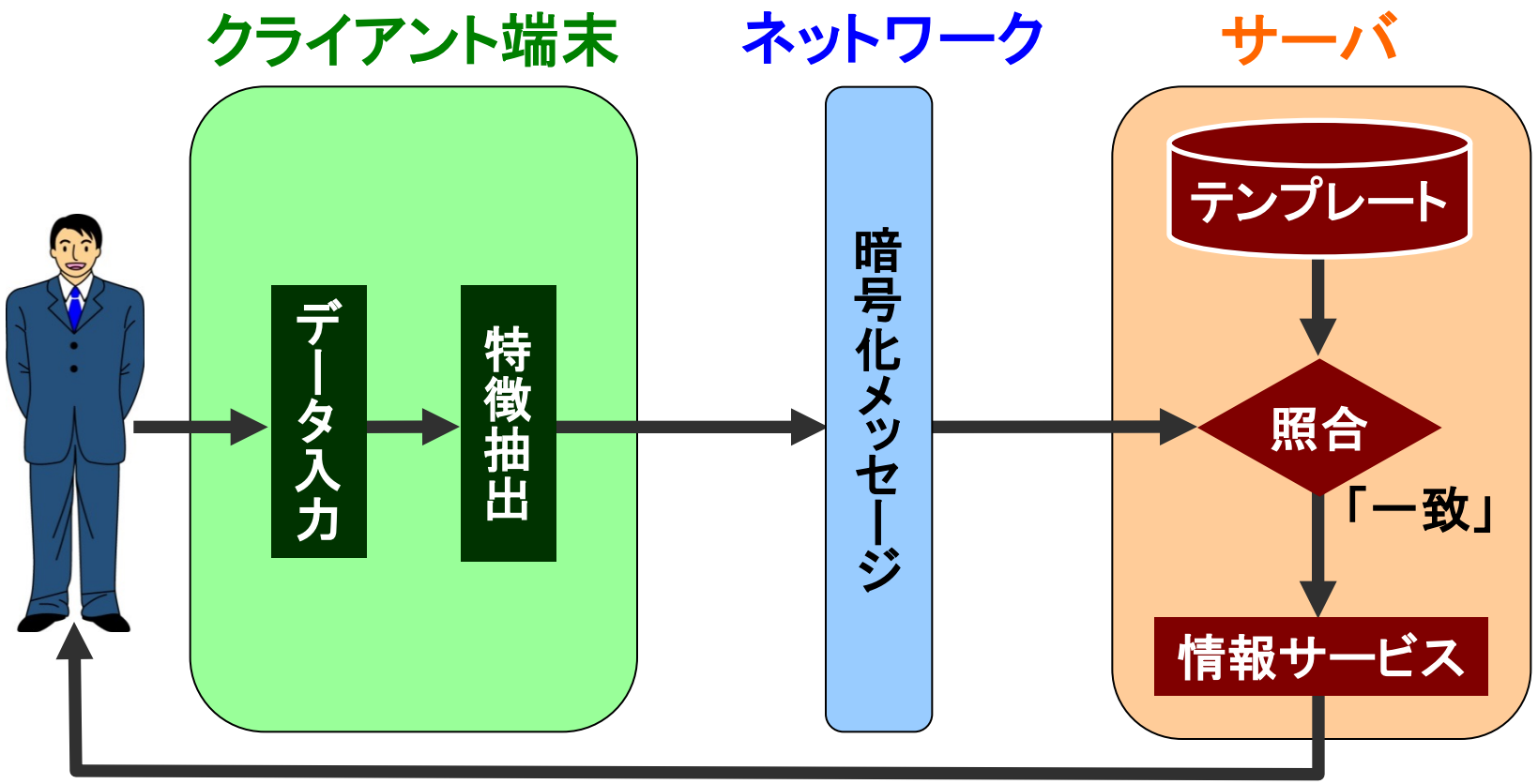
認証基本的処理フロー



特徴抽出機能

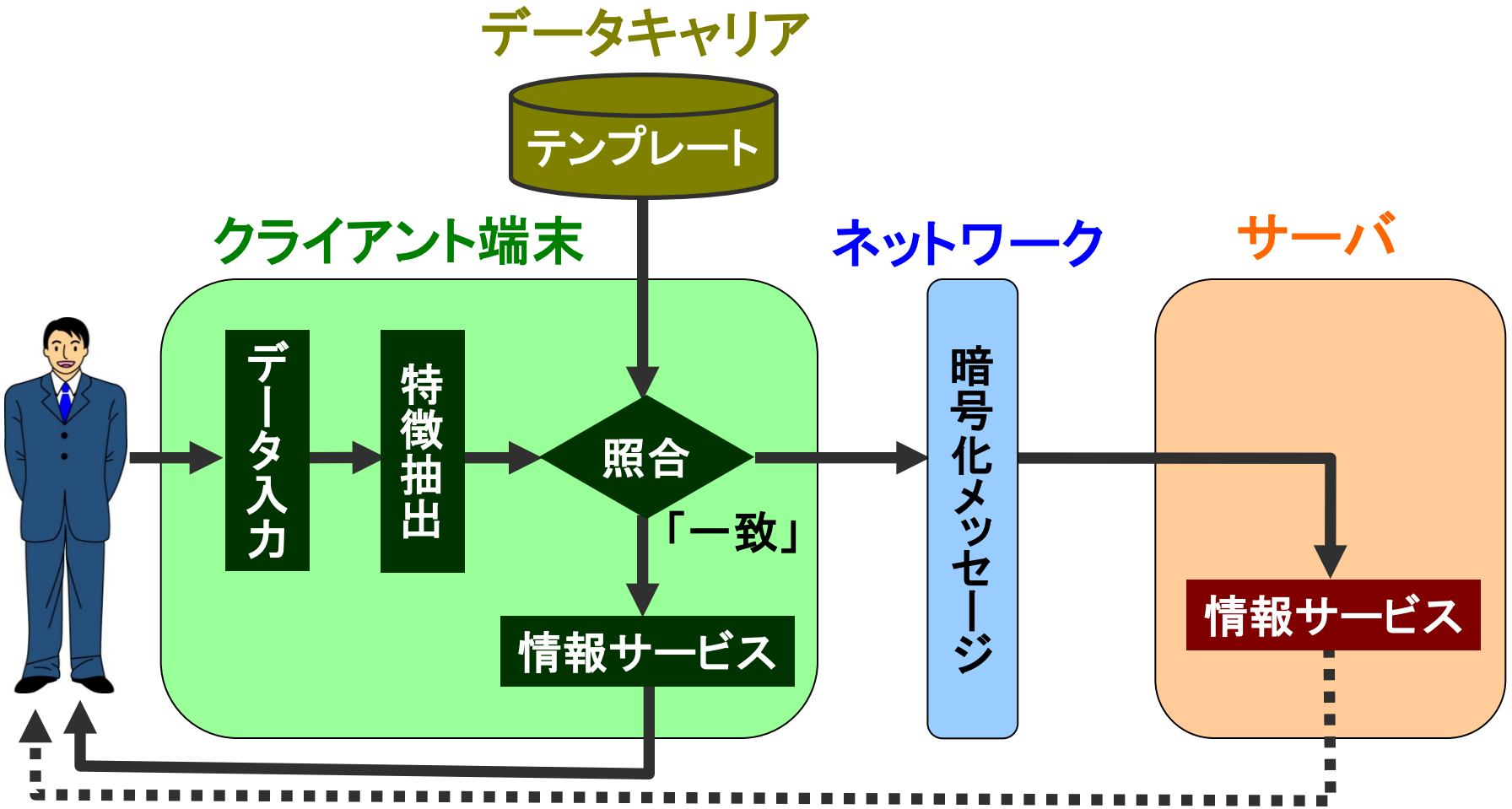
- ●前処理：判定処理に不要な環境要因の除去、空間的位置や大きさ、時間的変化などを正規化する処理。
- ●特徴抽出：判定処理に必要な個人の特徴を抽出する処理。

サーバ認証モデル



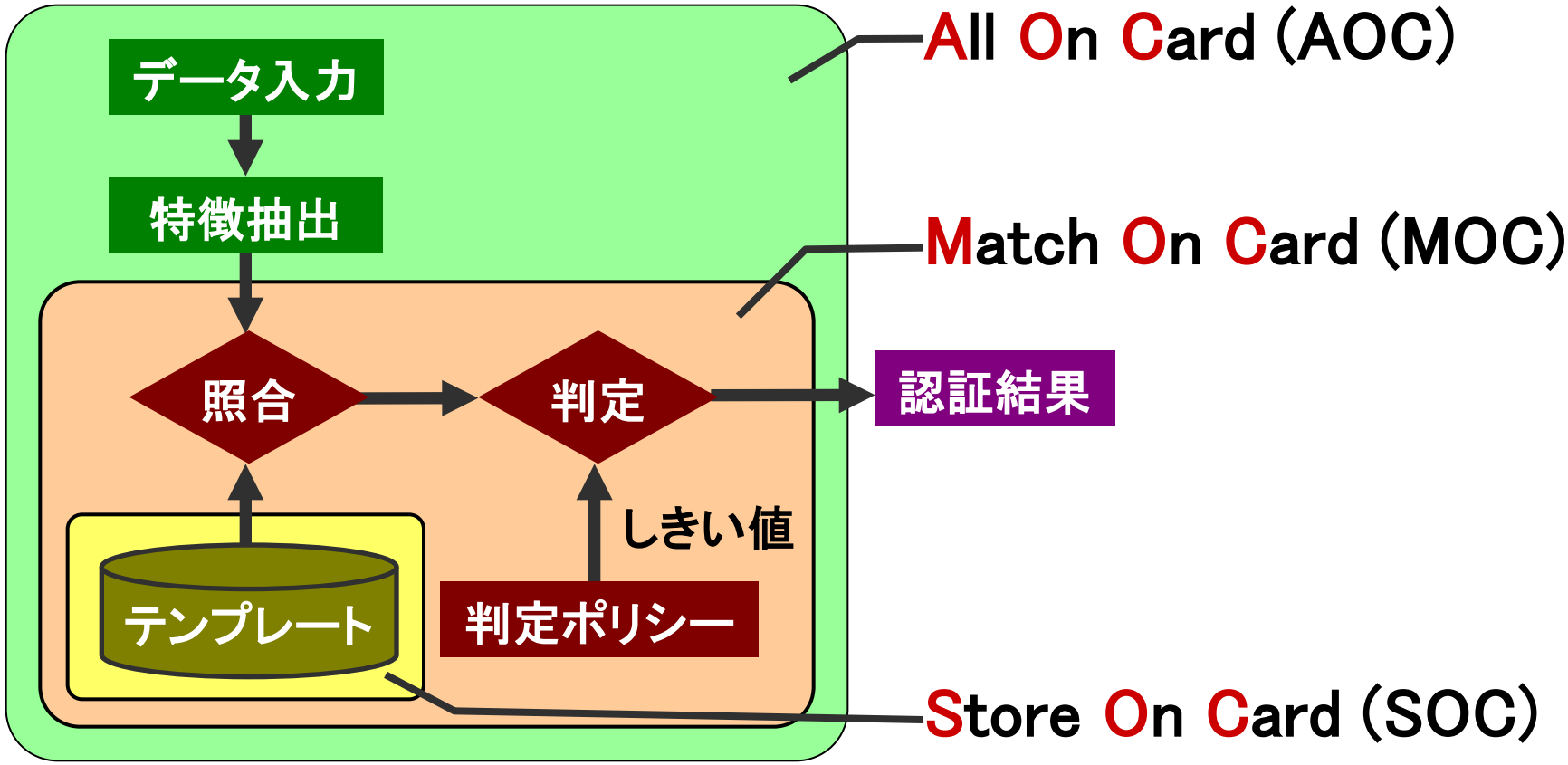
- クライアント端末の負担低減。
- クライアント端末のコスト低減。
- 利用者が多い場合、ネットワーク、サーバ負荷が大。
- 一括管理のためセキュリティ対策が重要。

クライアント認証モデル



- 本人のテンプレートをデータキャリアに格納。
- クライアント端末では登録処理ができない(してはいけない？)。
- ネットワークを使用しないで処理が可能。

ICカードを利用した認証モデル



- SOC：ICカード内のテンプレートと新たに入力したデータを、ICカードの外部処理装置（クライアント端末）で照合する。
- MOC：テンプレートの保管及び照合処理をICカード内で行う。テンプレートが外部に漏れない。
- AOC：センサもICカード上に実装され、すべての処理をカードで行う。ICカード自体のコストと、センサ電源などの問題がある。

データおよびプログラムインターフェイス

APIの概要

目的

- 生体認証システムの互換性確保。
- 開発コスト削減。
- 汎用的な生体認証モデルを実現するAPIの提供。
  - ・サーバ認証モデル、クライアント認証モデル、識別。

適用範囲

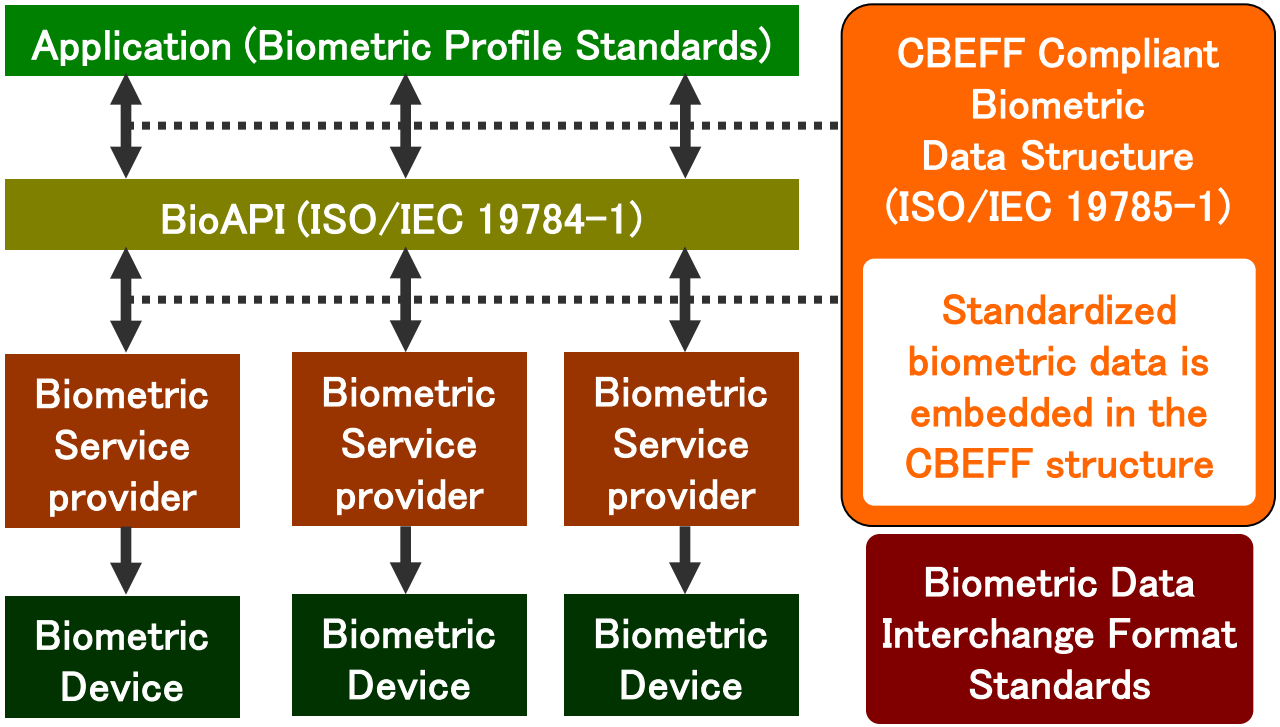
- 任意のバイオメトリクス技術。
- バイオメトリクスの登録、照合、識別、保存。

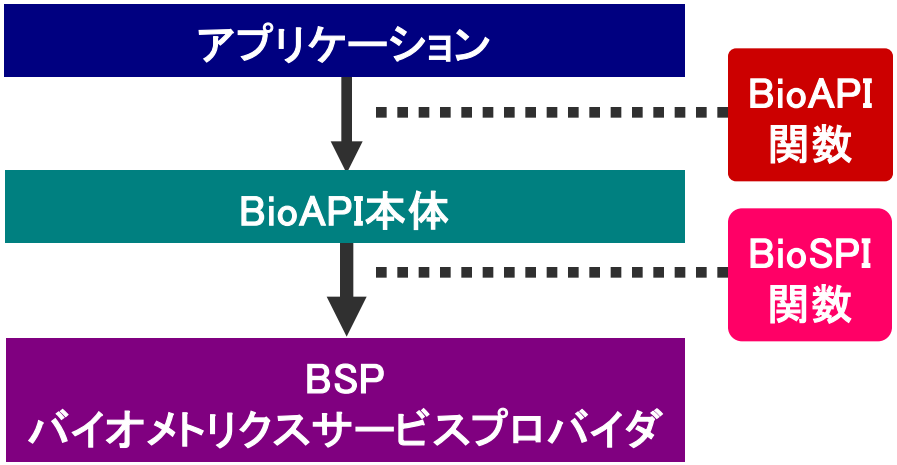
検討機関

- NISTの支援により BioAPI Consortium が検討。
- BioAPI specification ver. 1.1 を2001/3に発行。
- ISO/IEC JTC1 SC37がISO/IEC 19784-1を2005年に発行。

NIST: National Institute of Standards and Technology.（米国）

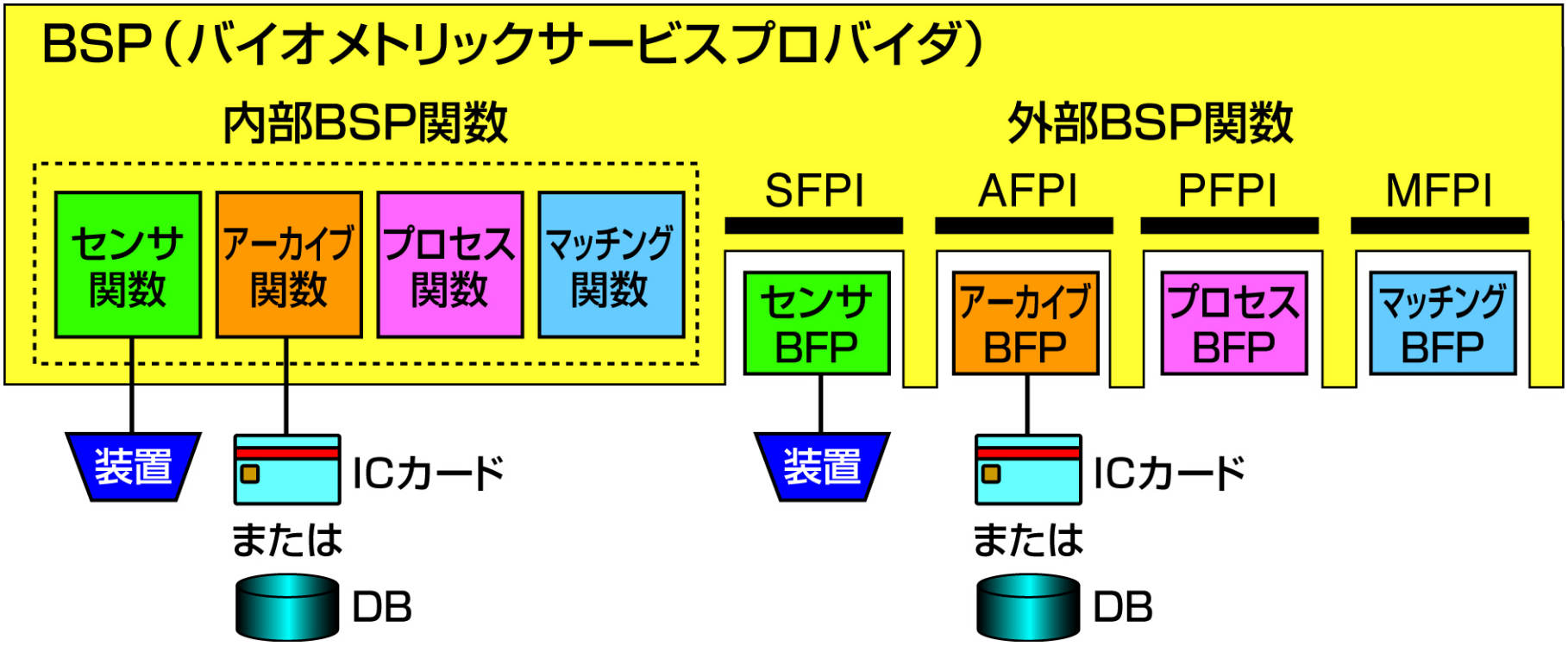
APIの構造





- API: Application Program Interface.
- BSP: Biometric Service Provider.
- SPI: Service Provider Interface.
- ISO/IEC 19784-1
  Biometric Application Programming Interface
  Part 1: BioAPI Specification.
- ISO/IEC 19785-1
  Common Biometric Exchange Formats Framework
  Part 1: Data Element Specification.

BSPの構造



BSP：Biometric Service Provider

バイオメトリクス装置制御や認証アルゴリズム

BFP：Biometric Function Provider

バイオメトリクス装置から身体情報の入手、登録データ生成

CBEFFの概要

CBEFFとは

- Common Biometric Exchange File Formatのこと。
- バイオメトリクスデータのフォーマットに関する規格。

CBEFFの目的

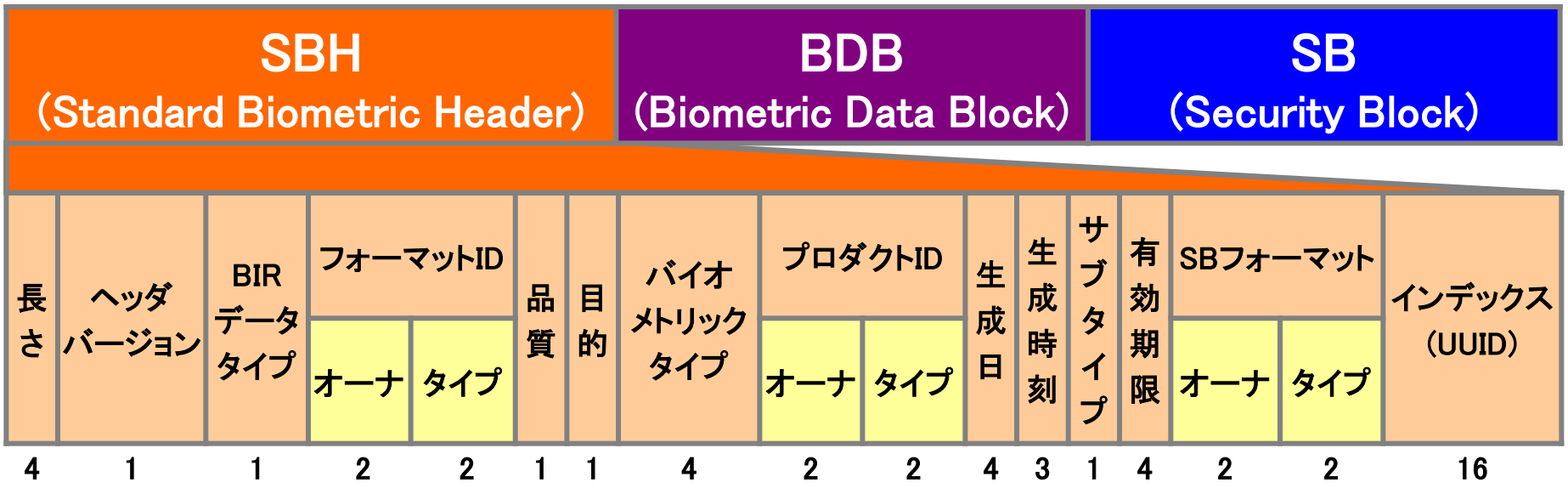
- 異なるシステム間におけるバイオメトリックデータのやりとりを可能とする。
- プログラムやシステムのインターオペラビリティの向上。
- システムインテグレートのコスト削減。

検討機関

- NISTとBiometric Consortium が支援。
- BioAPI Consortium, X9.84 WG, IBIA, TeleTrustなどの業界団体と連携。
- 2001年1月、NISTIR6529として公開。
- ISO/IEC JTCI SC37 がISO/IEC 19785-1を2005年に発行。

CBEFFの構造

- SBH (Standard Biometric Header).
  - ・CBEFFファイルのヘッダ。
- BDB (Biometric Data Block).
  - ・バイオメトリクスデータの実体を含むブロック。
  - ・ベンダ依存であり、どのようなデータでも良い。
  - ・生体情報、テンプレート、ベンダの独自ヘッダ、etc.
- SB (Security Block).
  - ・データの完全性を保証するための署名もしくは暗号化を含む。
  - ・オプション。



認証精度と
その測定方法

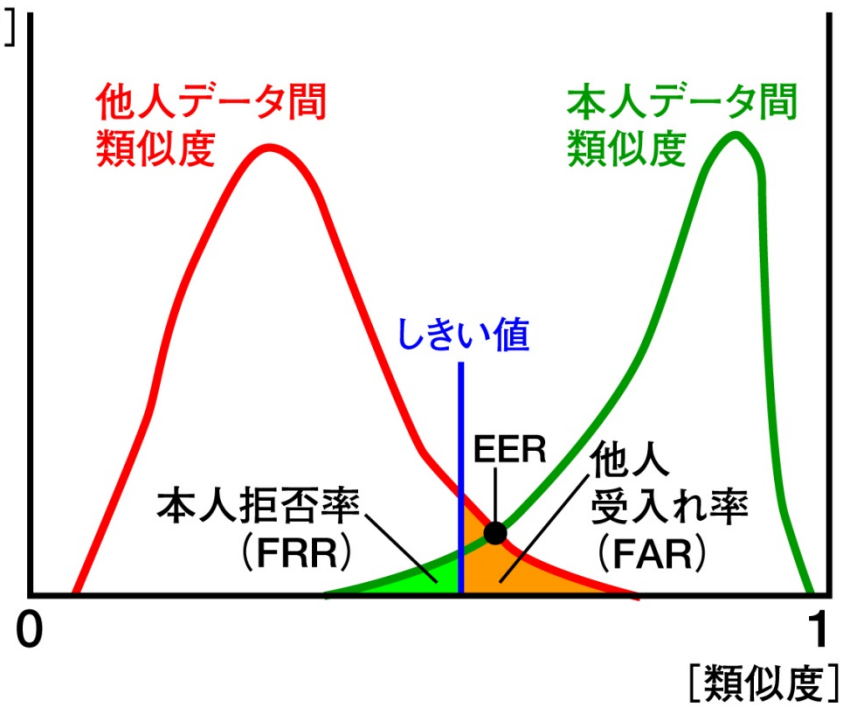
判定方式とバイオメトリクス

■他人の侵入を許さない方向に
しきい値を設定すれば、本人自身
も拒否される方向に働き、逆に
本人が拒否されることのないように
設定すれば他人の侵入を許してしまう。

●本人拒否率(FRR)
タイプⅠエラー(統計的有意性検定)
●他人受入れ率(FAR)
タイプⅡエラー(統計的有意性検定)

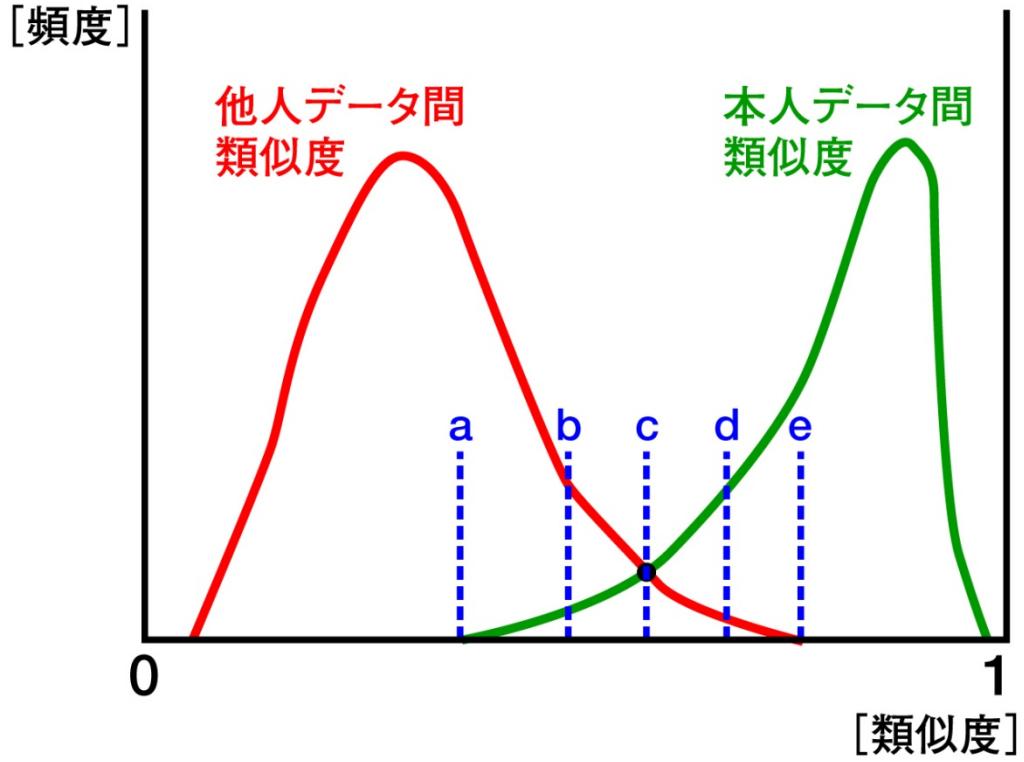
■タイプⅠエラーが高いと利用者は
フラストレーションを起こし、
タイプⅡエラーが高いと詐称を
引き起こす。

タイプⅡエラーはタイプⅠエラーに比べ、
1桁から2桁小さくする。



●FRR: False Rejection Rate
●FAR: False Accept Rate
●EER: Equal Error Rate

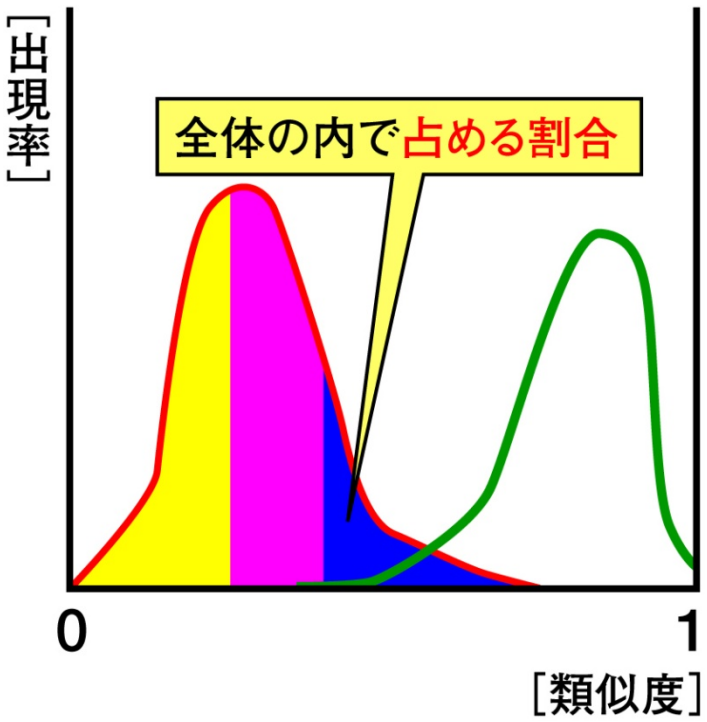
しきい値の設定

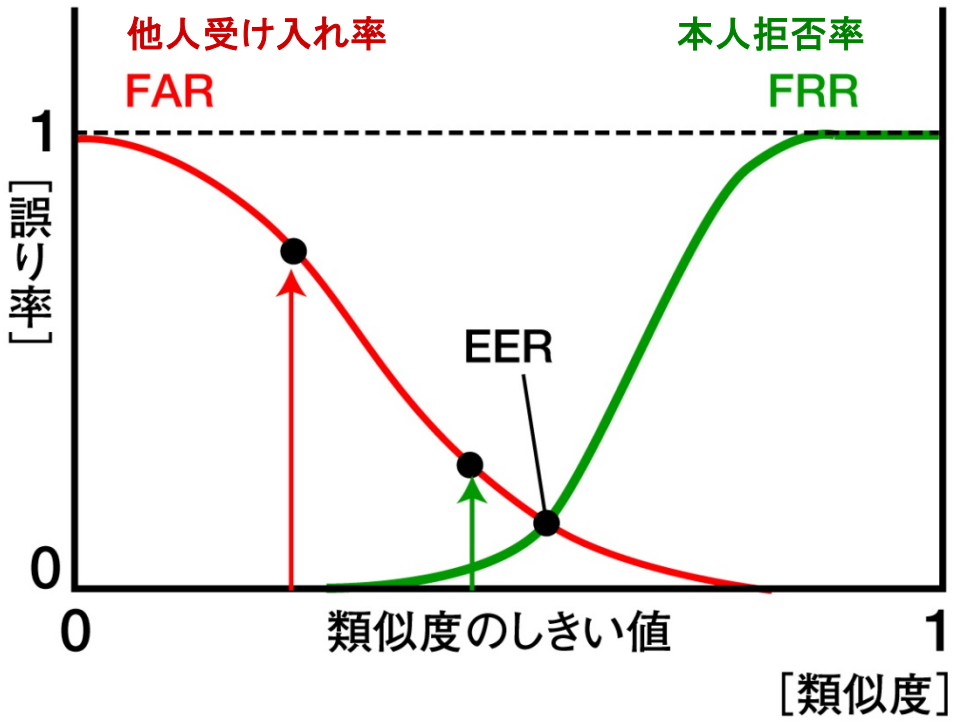


a: 本人が拒否されない
b: FAR > FRR
c: FAR = FRR
d: FRR > FAR
e: 他人の侵入を許さない

タイプⅠエラー（第一種の過誤）:
帰無仮説が正しいにもかかわらず帰無仮説を棄却するという誤り。
タイプⅡエラー（第二種の過誤）:
帰無仮説が誤っているにもかかわらず帰無仮説を採択するという誤り。

FAR曲線とFRR曲線





参　考　データ単位で扱う場合

- FARに相当するもの　FMR: False Match Rate（誤照合率）
- FRRに相当するもの　FNMR: False Non-Match Rate（誤非照合率）

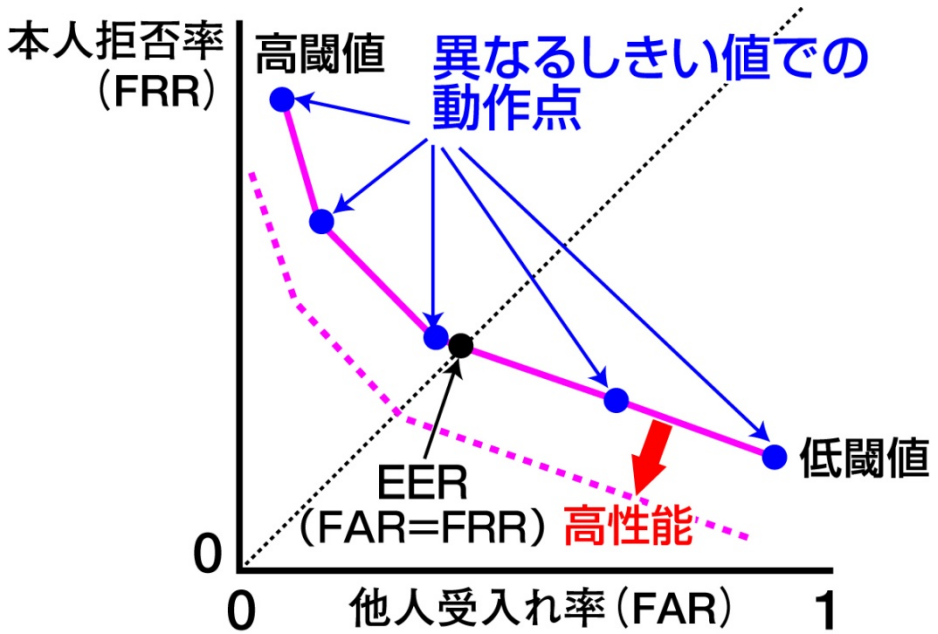
ROCカーブ

精度評価の問題点

(1)どのような精度をユーザに提示すべきか？
(2)どの程度のデータがあれば、どの程度の信頼性のある精度を得られるか？
(3)収集したデータの中に、精度を著しく劣化させる特異なデータがあった場合の扱いをどうするか？

精度評価の方法

ROCカーブは閾値をパラメータとしてFARとFRRをプロットしたグラフである。両対数グラフで書くこともある。
FARとFRRが一致する動作点でのそれらの値は2の誤認識率や誤照合率が一致することからEERと呼ばれる。



●ROC: Receiver Operating Characteristic.

サンプル数と信頼度

N min ～ 3/p

信頼度95%で誤差pの照合アルゴリズム評価に必要な最低テンプレート数と、照合用サンプルの組数(照合組数)N minの関係。

■精度誤差とサンプル数の関係(指数 6指/人)

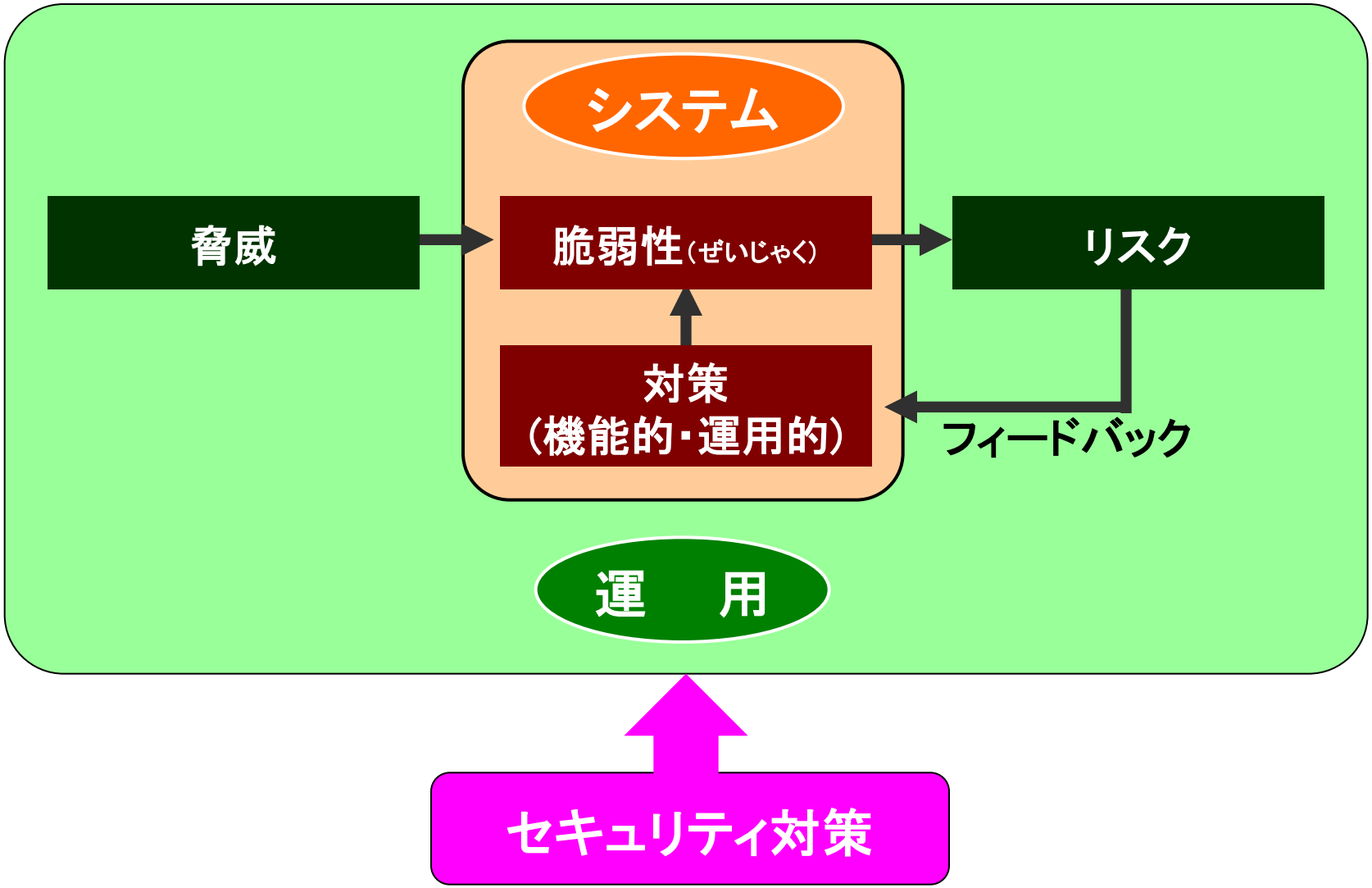
誤差	1 %		0.01 %	
認証精度	FRR	FAR	FRR	FAR
照合組数	300	300	30,000	30,000
被験者数	50	5	5,000	41

バイオメトリクス技術の精度

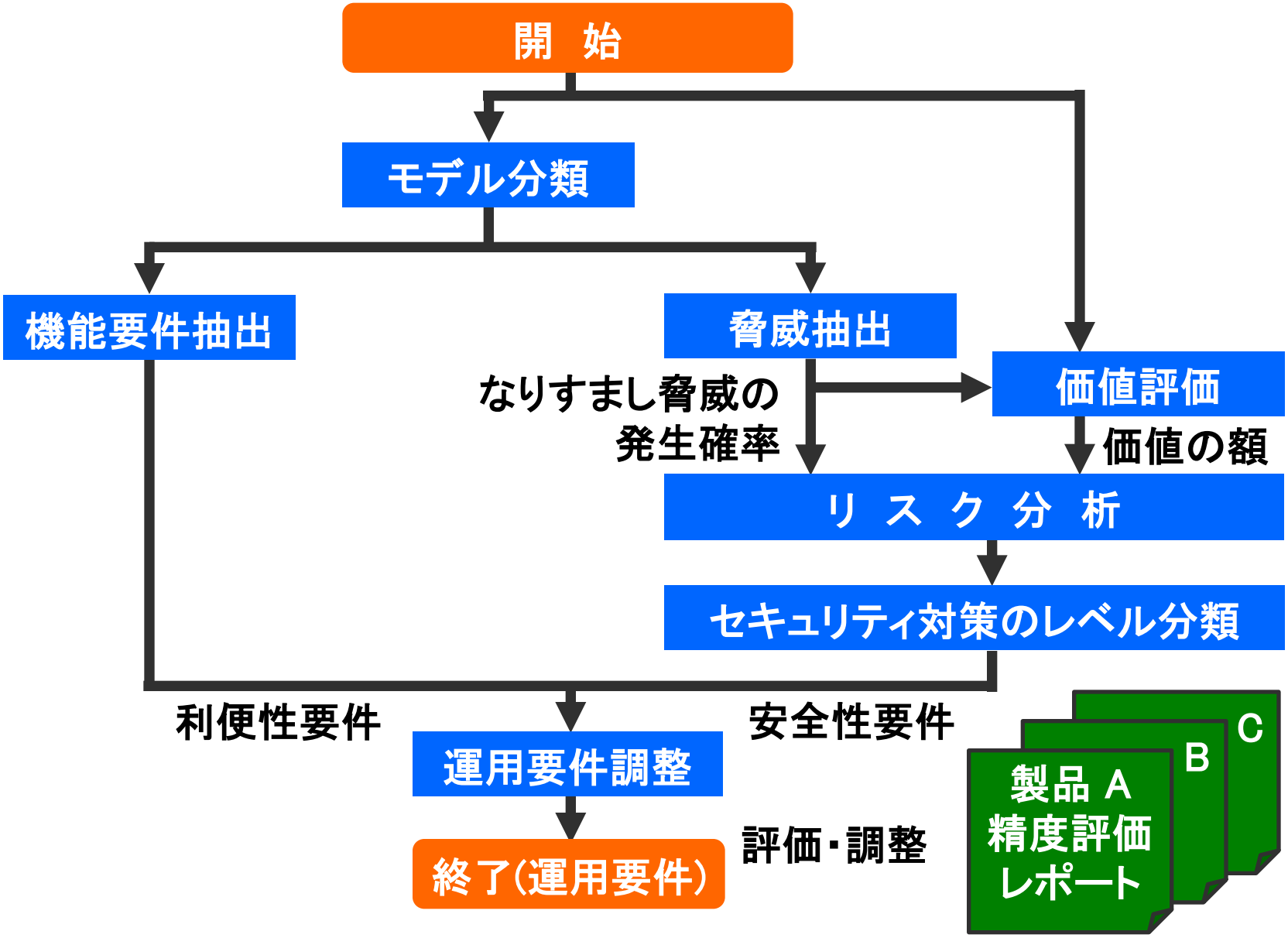
種　類	FRR (%)本人拒否	FAR (%)他人受け入れ
指　紋	0.5～1.0	0.01～0.0001
掌　形	0.1	0.1
顔	1～5	1～5
虹　彩	2～10	0.001
声　紋	10	10
署　名	5	5
静　脈	0.1～1	0.01～0.0001

認証システムにおける脅威

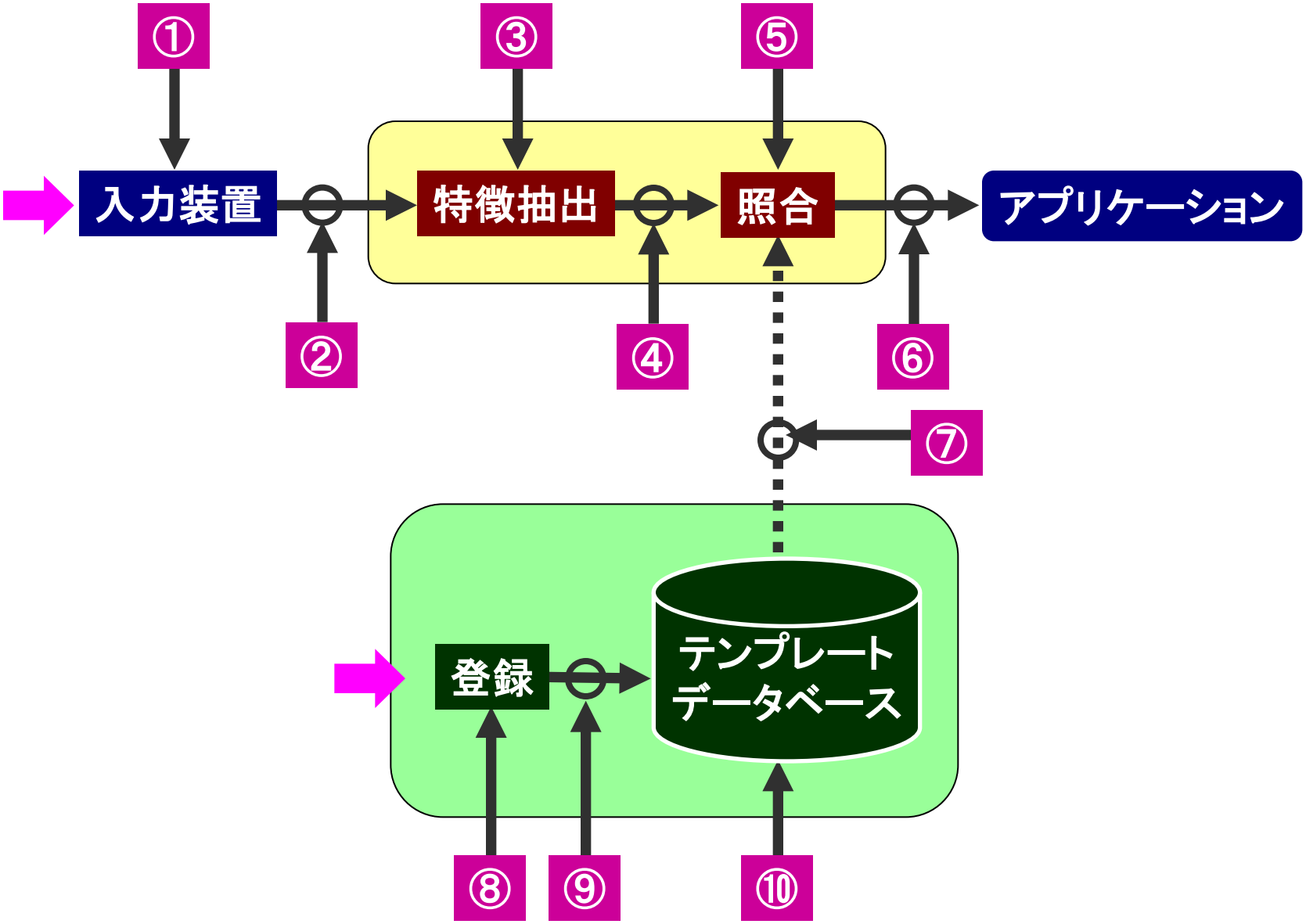
システム評価



運用要件策定フロー



認証システムにおける脅威　フロー



認証システムにおける脅威　詳細

#	脅　威	内　容	対　策
①	センサへの偽の生体情報の提示	●偽の生体情報がシステムへ入力されるなりすまし攻撃。 ●例えば、偽造の指、偽の署名、顔写真を張った覆面などが使用される。	①④⑥⑨ センサ部分およびネットワーク部分通信を暗号化することにより、少なくとも遠隔地からの生体情報の転送時の攻撃を防止できる。 ③⑤⑧⑨ の攻撃 照合処理を行うホストとテンプレートを保管しているデータベースを安全な場所に置くことで、攻撃を防止できる。ただし共謀者がいる場合の内部犯行まで防止できない場合もある。 ⑥最終決定部分 最終決定出力の暗号化を行うことにより、この部分に対する攻撃は防止できる。
②	蓄積された生体情報の再入力	●センサを介さずに、以前に入力された生体情報が入力されるなりプライアタック攻撃。 ●例えば、以前使われた指紋情報の再使用、または音声の再生などによる攻撃である。	
③ ⑧	特徴抽出処理の置き換え	●特徴抽出処理に対してトロイの木馬などによる攻撃を行い、侵入者の意のままの特徴を設定する。	
④ ⑨	生体の特徴を示す情報の不正変換	●入力信号から抽出された生体の特徴を示す情報を偽造した情報に置き換える。 ●特徴抽出処理と照合処理とは同じ場所で行われる場合が多いので、この攻撃は非常に困難である場合が多い。 ●例えば、抽出した指紋特徴点の情報がインターネット経由で照合処理が行われる場所へ転送される場合では、この攻撃が可能となる。 ●攻撃者はTCP/IP上のスヌーフィングを用い特定のパケットを摩り替えることによりこの攻撃が可能である。	
⑤	照合処理への攻撃	●照合処理が行われる場所を攻撃し、実際の照合処理の結果を生成されたスコアではなく、攻撃者が設定するスコアを設定する。	
⑩	蓄積されたテンプレートの改ざん	●認証用のテンプレートを格納したデータベースは、ローカルに設置されているか、あるいは遠隔地に設置されている。 ●また、このデータベースは、複数個所に分散配置されていることもある。 ●このデータベースを攻撃対象として、攻撃者がデータベース中に蓄えられた認証用のテンプレートを改ざんする可能性がある。 ●改ざんが行われると、不正な利用者に認証を与える可能性、もしくは正規のユーザを否認する可能性が生じる。	

脆弱性 I

脆弱性(Vulnerability)とは？

●何らかの理由により、設計者が意図した性能を
実現できなくなる原因となるシステムの特性。

生体認証システムにおける脆弱性とは？

●なりすましを引き起こす原因となるシステムの特性。
●可用性を阻害する原因となるシステムの特性。

安全な生体認証システムの構築

●全ての脆弱性が明確化されていること。
●各脆弱性に対するリスクが把握できていること。
●各脆弱性への対策が明確化されていること。

生体認証技術の脆弱性例

●他人受入誤差、本人拒否誤差。
●生体情報の偽造(人口指)。
●照合結果の偽造・改ざん。
●生体情報の偽造・改ざん・漏洩。

脆弱性 II

■身体情報に存在する脆弱性

分類	項目	定義	対策等
特有	複製	物理的に身体情報を複製できる	ライブチェック、監視、マルチバイオ
	秘匿困難	身体情報の秘匿が困難である	
	センサ残留	身体情報の痕跡がセンサ面に残留する	採取に物理的コンタクトのないシステム
	変更不可	身体情報を利用者が意識的に変更できない	
	登録未対応	身体情報をバイオメトリクス装置に登録できない	
	類似性	類似した身体情報を持つ他の利用者が存在する	類似した個人情報のペアを秘密にする
	変化	身体情報の状態が変化する	
	特異性	高確率で他人受入や本人拒否が発生する	弱いIDを検出・再登録して削除
	プライバシー情報	身体情報は個人情報の一種であり、プライバシー情報を含む	

脆弱性Ⅲ

■バイオメトリック装置に存在する脆弱性

分類	項目	定義	対策等
特有	他人受入れ	他人受入が偶発的に発生する	十分低いFAR、リトライ回数の制限
	本人拒否	本人拒否が偶発的に発生する	しきい値の調整
	推定	テンプレートや照合結果から身体情報が推定できる	テンプレートデータや照合結果の暗号化
	不定データ	身体情報でないノイズ画像などから他人受入が発生する	エラーを避けるチェック
一般	センサ劣化	センサが劣化する	
	構成管理	バイオメトリック装置の構成の変化により、精度が変化する	
	データ改ざん	バイオメトリック装置のデータを改ざんできる	
	データ漏洩	バイオメトリック装置のデータが漏洩する	転送における信号の暗号化、タイムスタンプ

脆弱性Ⅳ

■利用情報に存在する脆弱性

分類	項目	定義	対策等
特有	習熟	利用者がバイオメトリック装置の使用方法を習熟しなければならない	
	抵抗感	バイオメトリック装置の使用に抵抗感を感じる	
	動機	利用者は認証される意思をもって、身体情報の入力を行わなければならない	
	提供	利用者が第三者に身体情報を提供できる	信頼できる第三者機関による電子署名などのセキュリティ対策

■運用条件・環境条件に存在する脆弱性

分類	項目	定義	対策等
特有	入力条件	入力環境が精度に影響する	
	認証パラメータ	認証パラメータの設定が精度に影響する	パラメータのアクセス制限

セキュリティレベル

	安全性重視		利便性重視
基準	●本人認証によるリスクが天文学的に大きい ●社会的安全に寄与する	●本人認証によるリスクが大きい ●社会的信用に関わる	●本人認証によるリスクが小さい ●セキュリティへの要求がない
アプリ例	●原子力施設への入退室 ●造幣局への入退室 ●防衛・警察分野の入退室 ●ICカード発行施設への入退室 ●電子認証局における認証局秘密鍵へのアクセス	●金庫室への入退室 ●出入国管理 ●ICカードアクセス ●デビット・クレジット ●ホームバンキング ●電子カルテ・ATM ●データベース	●PCログイン ●集合住宅エントランス ●国内空港施設入退室 ●カスタマイズ ●勤怠管理 ●不正監視 ●利用端末管理
他人受入率	0.00006%	1%～0.01%	1%程度
（算出式の例）	$\frac{1}{(人口)\times(刑法犯発生確率)}$	$\frac{(許容他人受入率)}{(アクセス人数)\times(刑法犯発生確立)}$	本人拒否率のトレードオフ
本人拒否率	他人受入率とのトレードオフにより決定		機能要件により決定

平均攻撃空間

例	攻撃方法	平均攻撃空間
FARが1%(1/100)のバイオメトリクス	対話的	6ビット
ランダムな10文字の英文	オフライン	16ビット
FARが1/100,000のバイオメトリクス	対話的	16ビット
FARが1/1,000,000のバイオメトリクス	対話的	19ビット
各人が選ぶ8文字のunixパスワード	オフライン	22.7ビット
FIPS181の10文字 パスワードジェネレータによるパスワード	オフライン	39.5ビット
56ビットDES	オフライン	54ビット
128ビットAES	オフライン	127ビット

ご清聴、ありがとうございました。