バイオメトリクス

バイオメトリクスとは

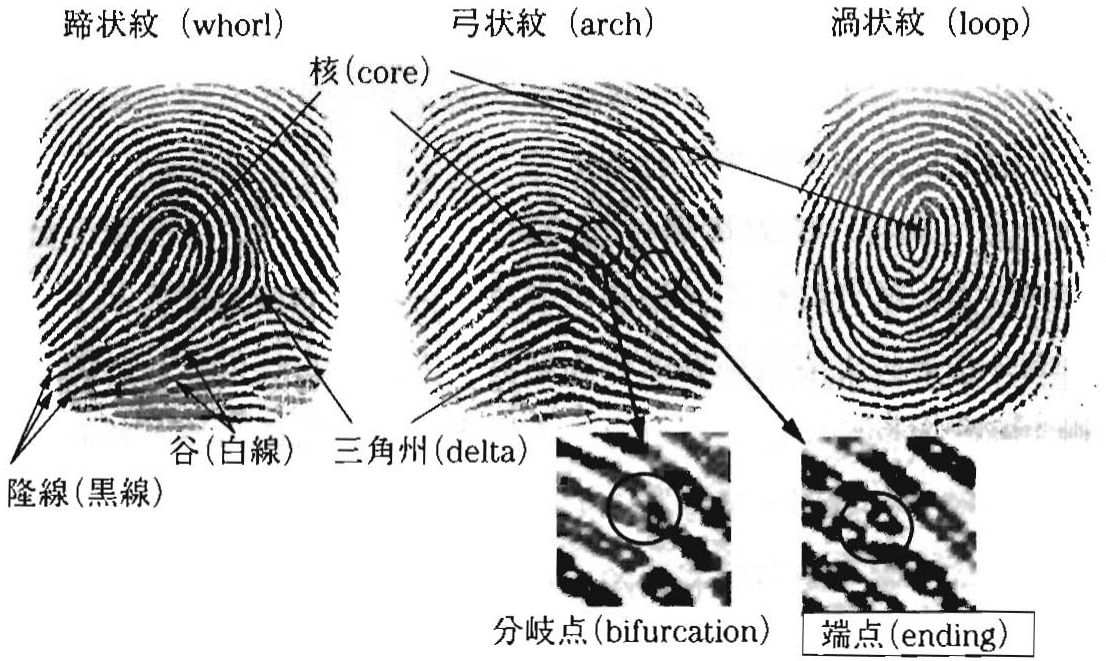
- 本人認証の方法
  - 所有物による方法：カードなど
    紛失、盗難、偽造などのおそれがある
  - 知識による方法：パスワードなど
    パスワード忘れ、流出などのおそれがある
  - 身体的、行動的特徴による方法（バイオメトリクス）
    - *普遍性：誰もが持っている特徴であること*
    - *唯一性：本人以外は同じ特徴を持たないこと*
    - *永続性：時間の経過とともに変化しないこと*

バイオメトリクスの種類

- 身体的特徴によるもの
  - 指紋　広く用いられているが抵抗感を持つ人も。偽造の研究も。
  - 顔　　抵抗感は小さいが、高精度な認証は難しい
  - 虹彩　　比較的広く用いられている。抵抗感は大きい。
  - 網膜血管　特殊な装置が必要。抵抗感が大きい
  - 耳介形状　認証精度の向上には今後の研究が必要
  - 掌、指静脈　最近よく用いられている。今後認証精度の検証など必要
  - DNA　高精度だが抵抗感は大きい。認証速度が難点。
- 行動的特徴によるもの
  - 声紋　時間、体調による変化が大きい。高精度化が課題。
  - 署名　時間による変化がある。高精度化が課題。
  - キーストローク　タイプ内容、時間による変動がある。

→複数のバイオメトリクスを組み合わせたもの
（マルチモーダルバイオメトリクス）もある

指紋の特徴点（マニューシャ）



照合モードによる違い

- 1:1の照合：入力された生体情報が、登録されている生体情報の一つと一致するかどうかを調べる
  - ID入力をともなう入退室管理など
- 1:nの照合：入力された生体情報が、登録されている生体情報のどれかと一致するか（あるいはどれとも一致しないか）を調べる
  - 犯罪者の検索
  - ID入力をともなわない入退室管理、など

バイオメトリック認証の流れ

1. データ取得：センサーから生体情報を取得する
2. 信号処理：センサーで取得した生体情報から特徴量を抽出する
3. 比較：抽出した特徴量と、登録されている特徴量を比較して類似度を算出する
4. 判定：算出された類似度から、しきい値に基づいて本人であるかどうかの判定を行う

バイオメトリクス技術の評価

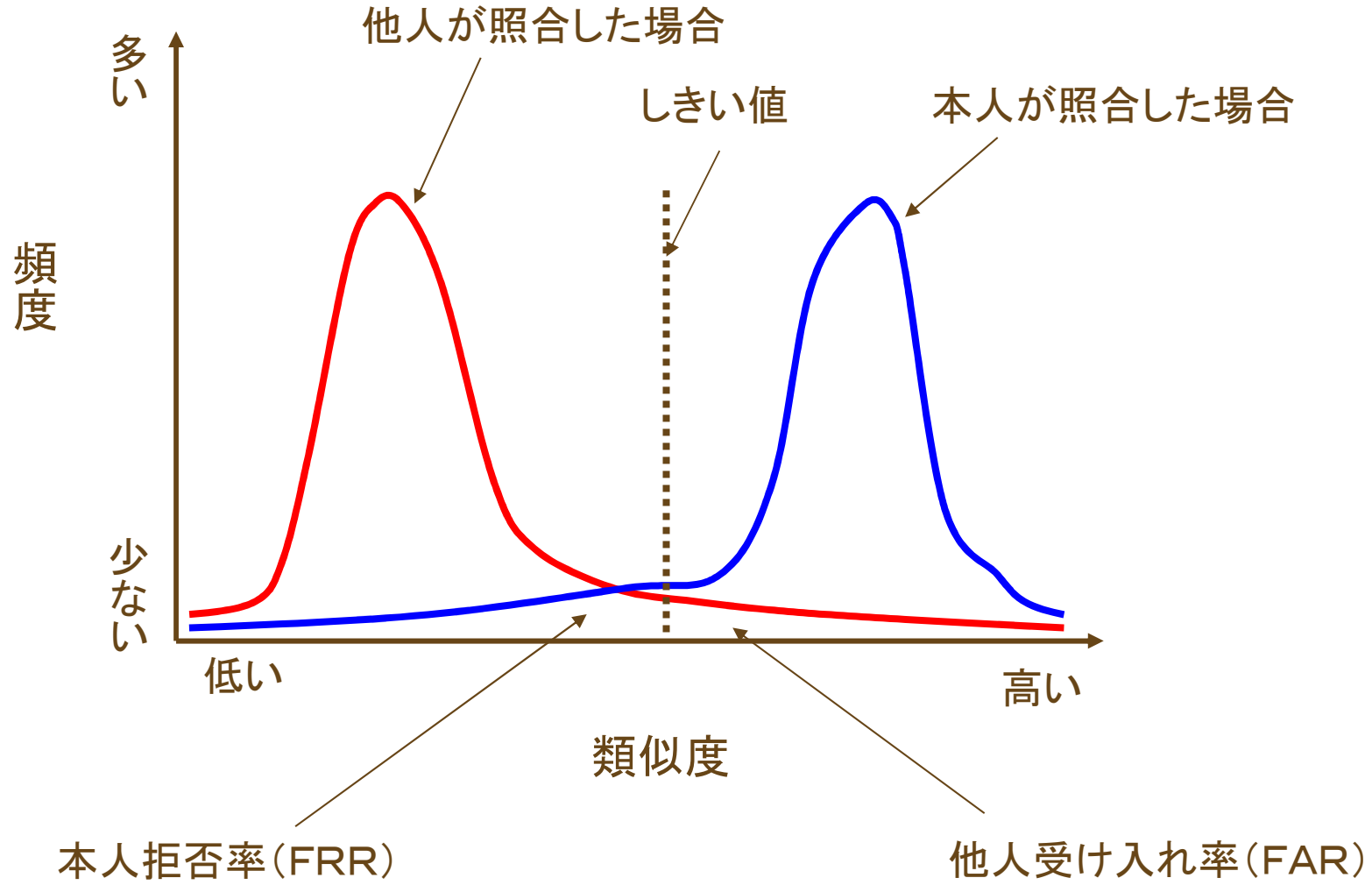
- 安全性：　照合精度が高い、偽造などが困難
- 経済性：　装置の価格や、設置費用が経済的
- 簡便性：　操作性がよい、認証時間が早い
- 社会的受容性：　違和感や抵抗感がない

■照合精度の評価

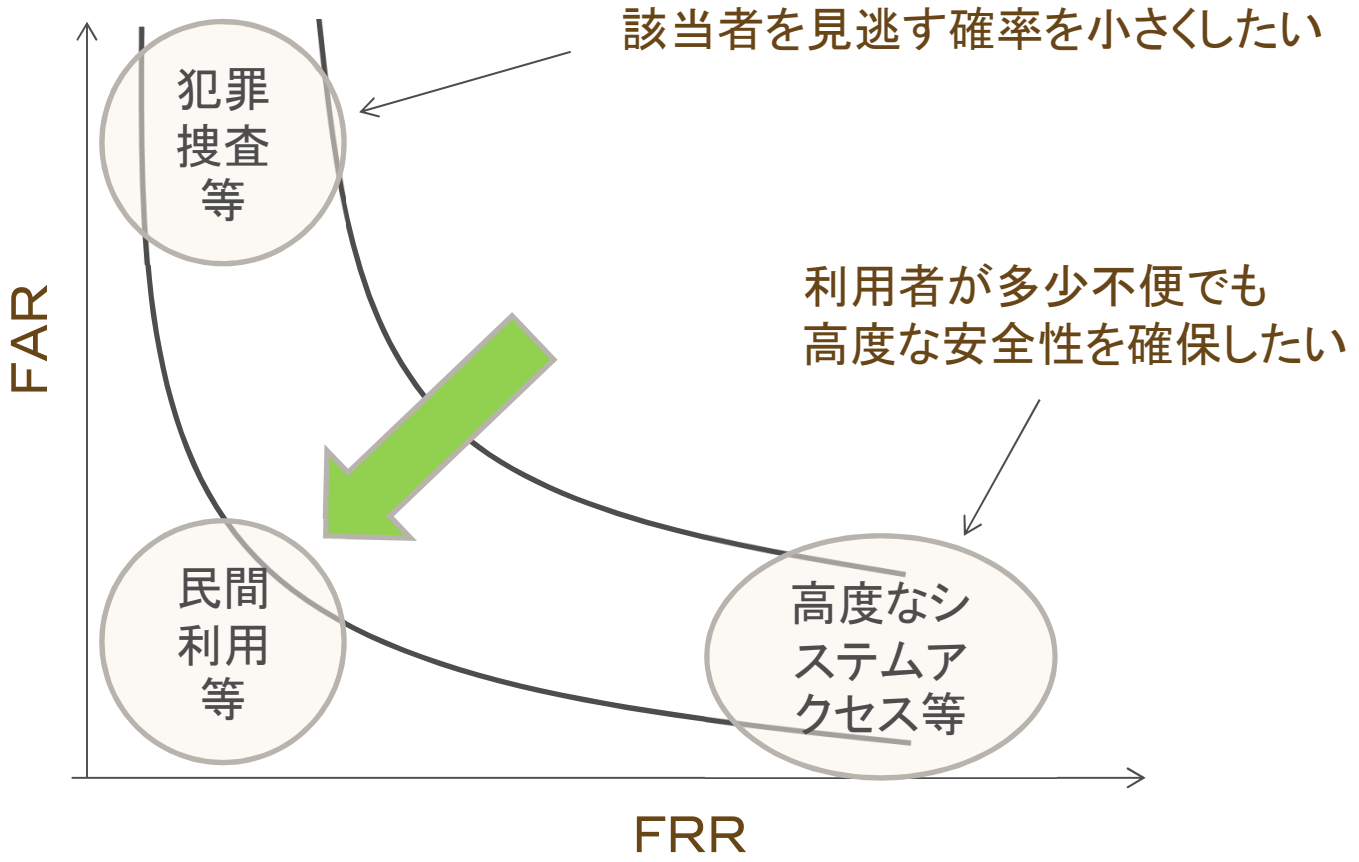
•本人拒否率（FRR）：本人の認証が失敗する割合
　これが大きいと、認証時のフラストレーションが高まる
•他人受け入れ率（FAR）：他人を本人であると誤って認証してしまう割合　　これが大きいと、安全性が低下する

◎一般に、FRRとFARはトレードオフの関係にあり、両者を適切に調整する必要がある。

照合精度と誤認識の関係



ROC(Receiver Operating Characteristic)カーブによる評価



バイオメトリック認証の安全性

- バイオメトリック認証特有の問題点
  →テンプレートの漏えい問題：
  - テンプレート情報から元の生体情報を復元できる可能性あり
  - パスワード等と異なり、生体情報は更新ができないため深刻な影響を与える
- テンプレート漏えいへの対策
  - システム運用による対策
  - 暗号化技術による対策
    バイオメトリック暗号、キャンセラブルバイオメトリクス、等