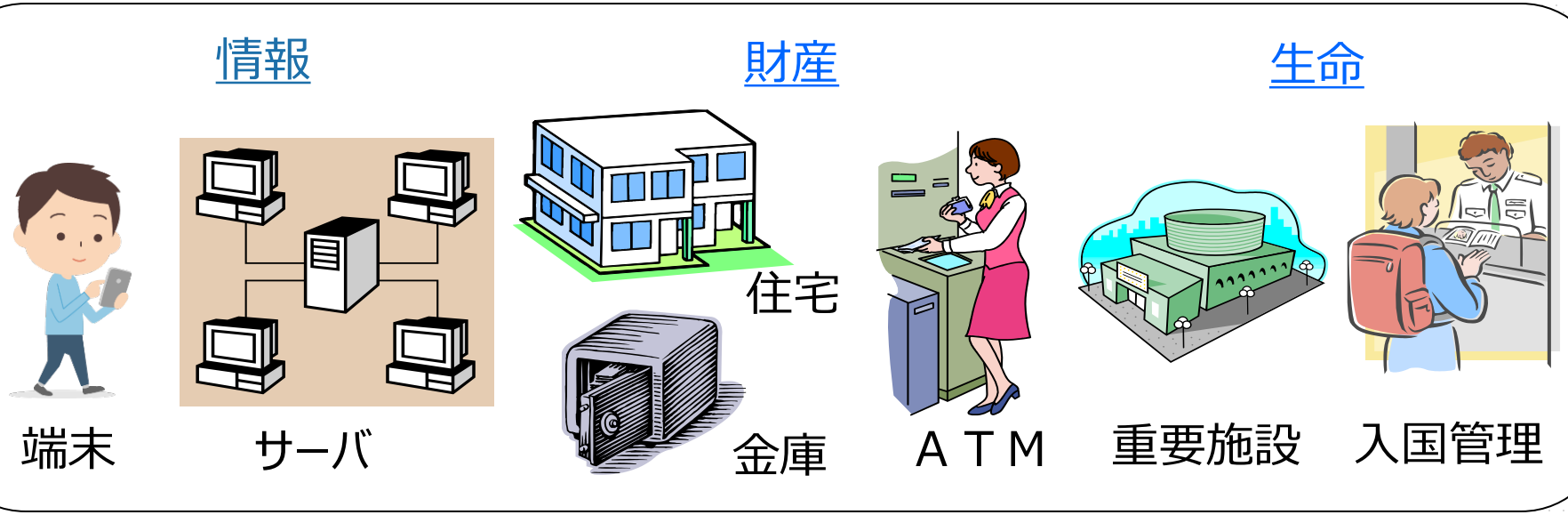
バイオメトリクスの基礎知識

CONTENTS

1. 情報化社会における本人認証の重要性

情報化社会における本人認証の使用シーン

情報化社会の進展と多様化により、電子的な本人認証が
活用されるユースケースが増大



- 偽造や盗難など、不正に使用される危険が少ない
- 本人確認手段を用いることが、個人の財産/個人の安全を守る基本

1. 情報化社会における本人認証の重要性

不正アクセス行為の発生状況

不正アクセス後の行為別認知件数

区分	平成29年	平成30年	令和元年
インターネットバンキングでの不正送金等	442	330	**1,808**
インターネットショッピングでの不正購入	133	149	**376**
メールの盗み見等の情報の不正入手	146	385	**329**
オンラインゲーム・コミュニティサイトの不正操作	83	199	60
インターネット・オークションの不正操作	28	29	47
知人になりすましての情報発信	110	24	30
仮想通貨交換業者等での不正送信	149	169	22
ウェブサイトの改ざん・消去	14	13	19
その他	97	188	269

不正アクセス行為の手口別検挙件数

区分	平成29年	平成30年	令和元年
識別符号窃用型	545	502	**785**
セキュリティ・ホール攻撃型	54	18	**2**
計	599	520	**787**

- 大半が個人の財産／安全に繋がる
- 手口の大部分は識別符号窃用

出典：経済産業省、
他：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況
（令和2年3月５日）

1. 情報化社会における本人認証の重要性

本人認証技術の種類と比較

要件＼認証方法		所有物	知識	身体的特徴
		鍵 磁気カード ICカード 証明書	パスワード、暗証番号 電子署名 	身体的： 指紋、虹彩、静脈、顔 行動的： 署名、声紋
安全性	盗難、偽造などによる悪用が困難	小	小	**大**
		紛失、盗難、偽造の恐れあり	忘失の恐れあり 管理方法により 盗難の恐れあり	偽造は困難
経済性	費用と、保護する利益が見合う	大	大	中
		ICカードなどは将来低価格化	記憶のため無償 管理は必要なものは要コスト	現時点では、他に比べ高価 用途により選択
簡便性	操作が簡単 携帯性がある	大	中	**大**
		携帯が必要 読取装置への 挿入、接触	キーボードなどから 文字・数字を入力	記憶、保持が不要 読取装置への 接触、接近

2. バイオメトリクス認証とは

バイオメトリクス認証とは、「生物個体が持つ特性」により、個人を認証する技術

- 身体的特徴を応用したもの
- 行動的特徴を応用したもの

バイオメトリクス認証技術の特徴

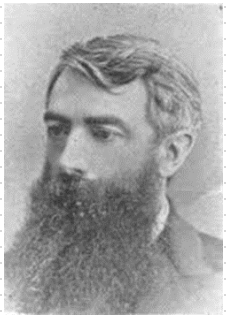
- 本人の生物学的特徴を読取り、登録してあるものと照合して個人を認証する手法のため、紛失や盗難の脅威が少なく、提示も比較的簡単

生体認証に使われる生物学的特徴とは

①普遍性：　誰でも持っている特徴
②唯一性：　万人不同　（本人以外は同じ特徴をもたない）
③永続性：　終生不変　（時間の経過と共に変化しない）

2. バイオメトリクス認証とは

バイオメトリクス認証の歴史と事例



【歴 史】

●1880年　スコットランド人H. Fauldsが、日本における拇印の習慣を研究し、指紋の不同性に気づき、犯罪捜査へ利用できることを科学誌Natureに発表（世界最初の論文）

●1880年　イギリス人F. Galtonは特徴点を指紋照合に利用することを提案

●1897年　世界初の指紋局がインドカルカッタに開設

●1982年　日本に自動指紋識別システム
AFIS（Automated Fingerprint Identification System）が導入

●1983年　米国にAFISが導入

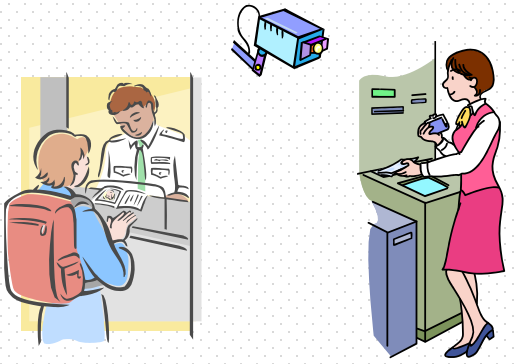
●1980年代中期　重要施設入退室管理に導入

●1990年代中期　ネットワークでの本人認証に導入

指紋研究発祥の地
（ヘンリー・フォールズ住居跡）

【事 例】

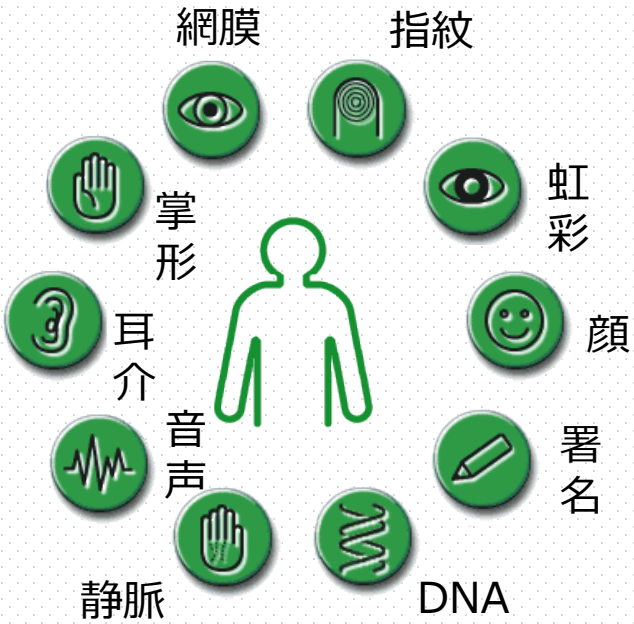
● 出入国管理 （US-VISIT、自動化ゲート）
● 金融 （ATM）
● 監視 （防犯カメラ）



2. バイオメトリクス認証とは

バイオメトリクス認証技術の種類

バイオメトリクス	生体情報と特徴量
指紋	指紋の特徴点の位置・角度・パターンなど
顔	顔の輪郭、目や鼻などの形状や位置など
静脈	手や指の静脈パターンなど
掌形	手の大きさ、長さ、厚さ、あるいは比率など
虹彩	目の虹彩（アイリス）の紋様のパターン
音声	音声パターンの時系列特徴
署名	署名の字体や署名時のペンの動き、筆圧、角度など
その他	耳介、キーストローク、網膜、歩き方（歩容）、DNAなど



● 詳細は、JAISA Webサイト

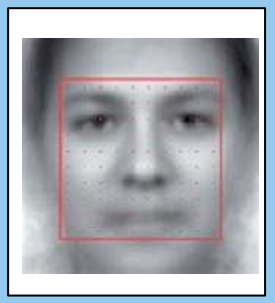
バイオメトリクスとは

2. バイオメトリクス認証とは

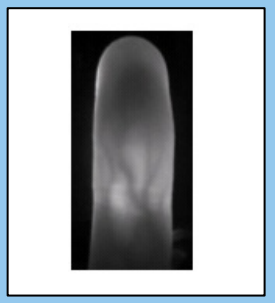
バイオメトリクス認証技術の分類

身体的特徴を応用

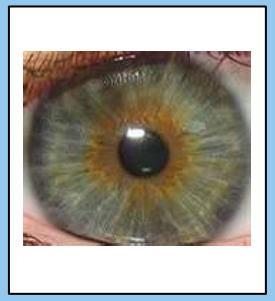
指紋



顔

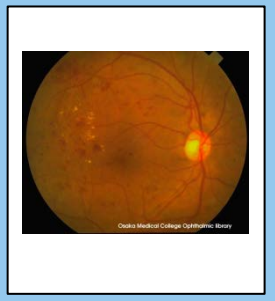


静脈



虹彩

掌形

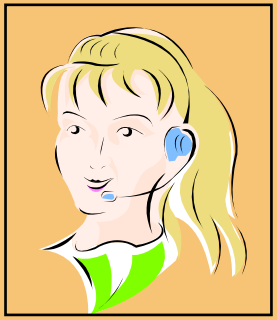


網膜

耳介、DNA、におい・・・

行動的特徴を応用

手書署名
キーストローク



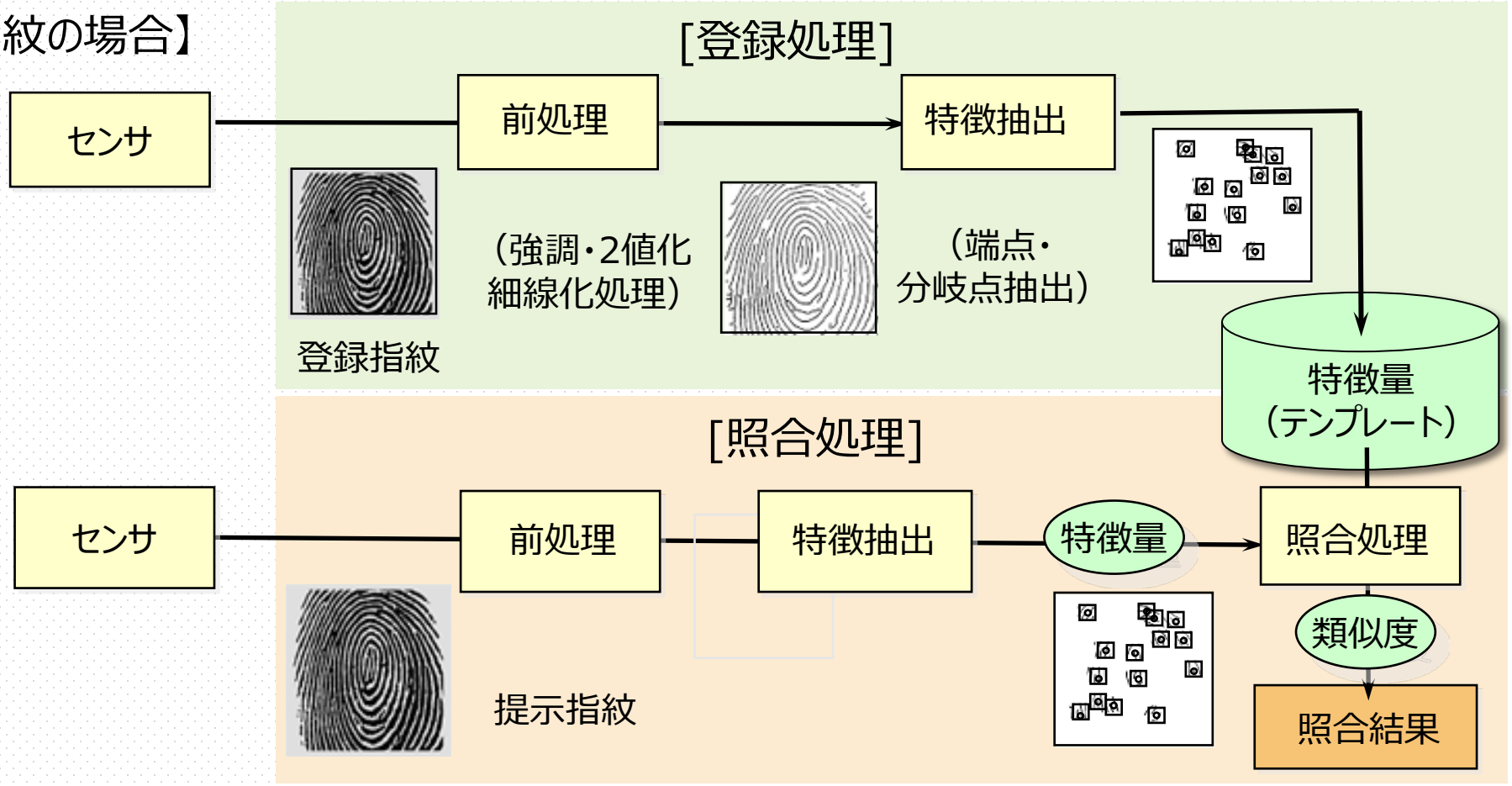
音声（声紋）

2. バイオメトリクス認証とは

バイオメトリクス認証技術の基本的考え方

画像処理・認識技術により、登録してある特徴量と入力される特徴量が「どの程度似ているか」照合し、本人確認する技術

【指紋の場合】

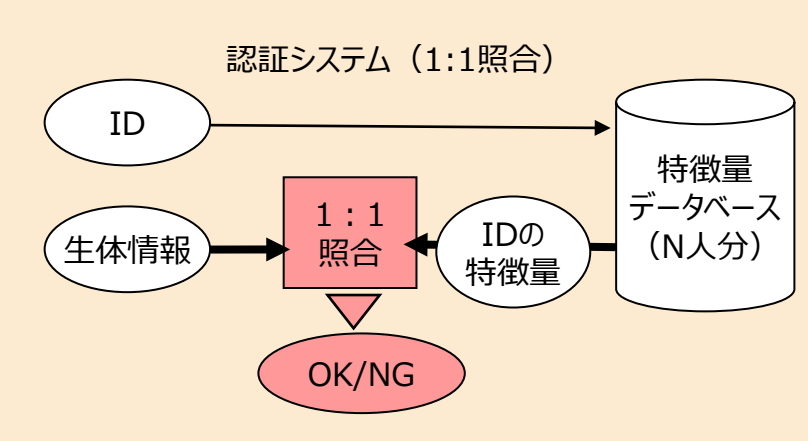


2. バイオメトリクス認証とは

バイオメトリクスモデルの種類

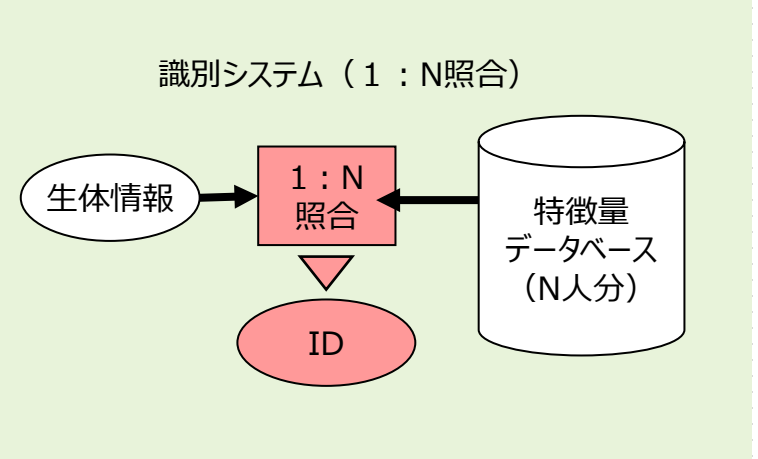
認証システム（1：1照合）

- 利用者のIDと生体情報を提示して、あらかじめ登録した利用者の特徴量と照合して本人を確認
- IDを提示するための手段が必要
- 精度はユーザーの数に依存しない



識別システム（1：N照合）

- 利用者の生体情報のみを提示して、あらかじめ登録した多数（N）の利用者の特徴量と照合し、利用者を特定
- 利便性は高いが、精度が利用者の数に依存する



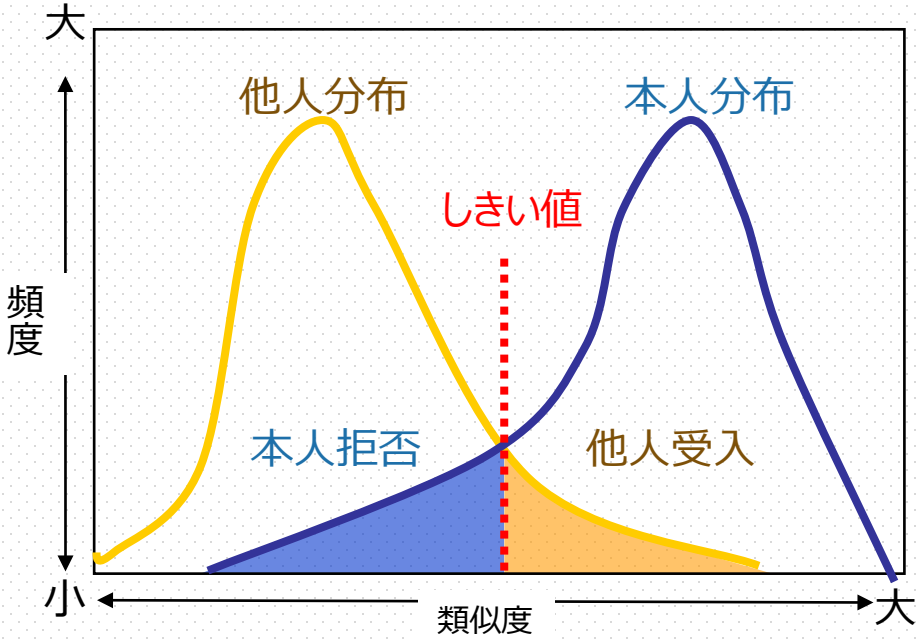
2. バイオメトリクス認証とは

バイオメトリクス認証の精度

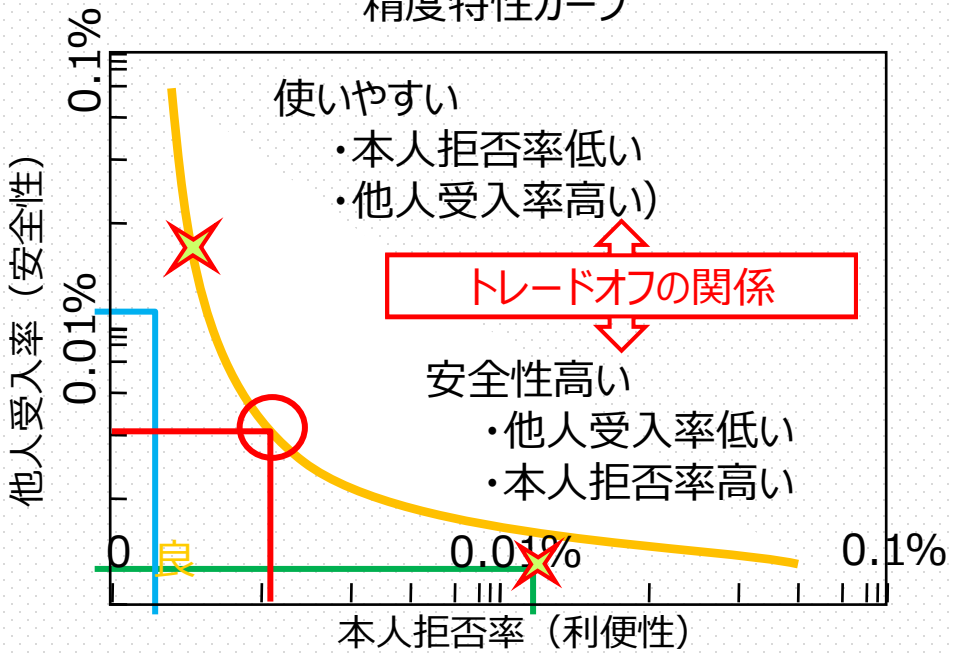
生体認証におけるエラー率

- 本人拒否率FRR（False Rejection Ratio）＝誤って本人を拒否⇒利便性に影響
- 他人受入率FAR（False Acceptance Ratio）＝誤って他人を受入⇒安全性に影響
- 登録未対応率FTER（Fail To Enroll Ratio）＝利用者を登録できない⇒運用に影響

類似度分布



精度特性カーブ



2. バイオメトリクス認証とは

バイオメトリクス認証技術の比較

	内容	コスト	安全性	精度（%）		適用分野
				本人拒否	他人受けれ	
指紋	手の指の指紋の特徴点を利用	低	中	0.5	0.01	全般
顔	顔の輪郭、目や鼻の形および位置	中	低	1	1	低セキュリティ施設管理
静脈	手や指の静脈パターン	中	高	0.1	0.0001	高セキュリティ施設管理
掌形	手の大きさ、長さ、厚さ、あるいは比率	中	低	0.15	0.15	低セキュリティ施設管理
虹彩	眼の虹彩（アイリス）の放射線状の紋様	高	高	28	0	高セキュリティ施設管理
音声	話者の音声特徴	中	低	1	0.1	電話サービス
署名	署名の字体や署名時の書き順や筆圧	低	低	0.2	0.6	PCログイン

バイオメトリクス認証のメリットと配慮する点

バイオメトリクス認証技術の特徴

●利用者の身体的／行動的特徴に基づく本人確認技術

●利用者と本人を確認するための情報（生体情報）のつながりが強い

バイオメトリクス認証のメリット

●忘れない・なくさない　⇒　高い利便性

●なりすましが難しい　⇒　高い安全性

●利用者のセキュリティ意識に依存しない安全性の確保

配慮が必要な点

●認証の精度：　本人拒否や登録未対応の発生

●運用：　本人による生体情報の登録作業が発生

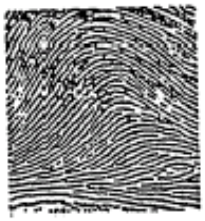
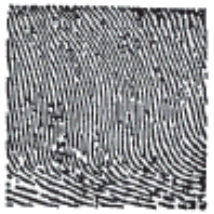
●抵抗感、個人情報保護、不完全な互換性

3. いろいろなバイオメトリクス技術

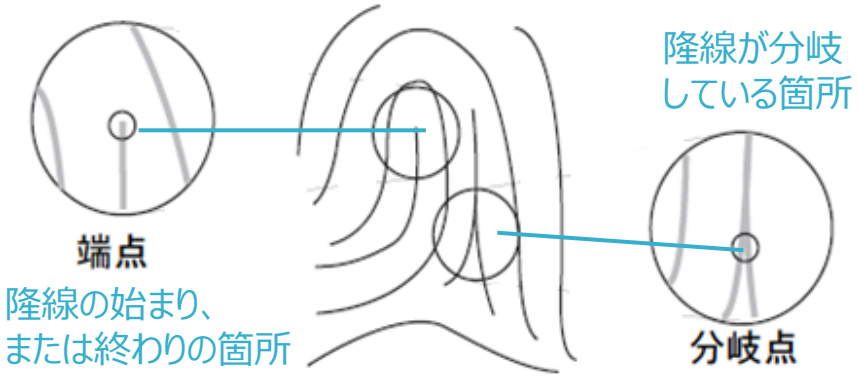
指紋認証

指紋の紋様の特徴をもとにして照合を行う技術

指紋の種類

蹄状紋	渦状紋	弓状紋	変体紋
			
左または右から起こり、馬蹄型を描いて元の方に還流する隆線で形成された指紋	中心が円、楕円、または渦巻き状の隆線で形成された指紋	左または右から起こり、反対側へ流れ去る単純な隆線だけで形成された指紋	他の三種類のいずれにも属さない指紋

指紋の特徴点（マニューシャ）



指紋認証の長所と短所

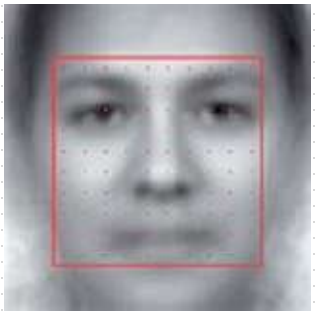
【長所】
- 小型化、低価格化した装置がある
- 認証精度が高い
- 犯罪抑止効果がある

【短所】
- 指先はケガをしやすい
- 指先が濡れていると、方式によって認証できないものがある
- 不特定多数利用で、衛生面を気にする方がいる
- 犯罪者扱いと感じる方がいる

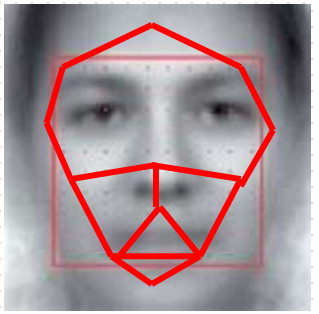
3. いろいろなバイオメトリクス技術

顔認証

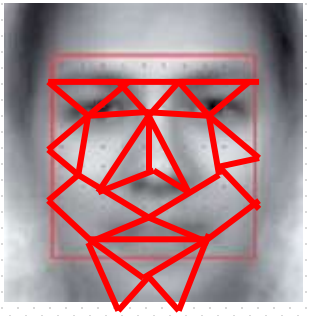
顔の輪郭、目、鼻や口の形状、位置などの
顔の持つ特徴をもとに照合を行う技術



画像入力



顔の特徴点を検出



顔画像の特徴量を抽出

顔認証の長所と短所

【長所】
- 心理的抵抗が少ない
  （顔を見て誰であるかを判断するのは、人間の自然な行為）
- 距離が離れていても認識できる
- 不正に対する心理的抑止効果がある
  （顔画像や映像が記録できる）

【短所】
- 双子などの厳密な識別は難しい
- 照明の違い、顔の向き、メガネや経年変化に弱い
- 公共の場所では、プライバシーの保護が問題になる可能性がある

3. いろいろなバイオメトリクス技術

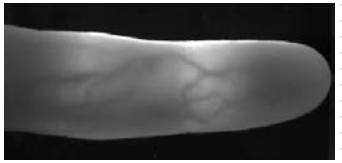
静脈認証

指あるいは手のひらなどにある静脈血管の、網目のような模様の特徴をもとにして照合を行う技術

静脈を使う理由

・静脈は、動脈よりも皮膚の表面に近いところを流れている

・静脈中の血液は、赤血球内のヘモグロビンが酸素を失っている状態（還元ヘモグロビン）である。この還元ヘモグロビンは近赤外光（波長760nm近辺）を吸収する特性を持つ



静脈中のヘモグロビンが、近赤外波長の光を吸収する → **黒く写る**

静脈認証の長所と短所

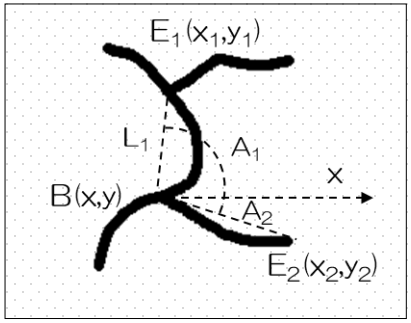
【長所】
・認証精度が高い
・体内情報のため、盗まれにくい
・濡れたりしていてもにんしょうです、
・静脈中の血液は、赤血球内のヘモグロビン

【短所】
・装置の小型が難しい
・毛深かったり貧血だと認証が難しい方がいる

静脈認証の方法（一例）

画像入力
↓
静脈パターンを抽出
↓
パターン特徴を抽出
↓
パターンマッチングや分岐特性により照合

静脈パターンの線の長さと分岐



分岐点の座標、長さ、分岐点と分岐点の間の分岐角度を使用

3. いろいろなバイオメトリクス技術

掌形認証

掌の持つ幾何学的な特徴をもとにして照合を行う技術

幾何学的な特徴の測定とは、掌大きさと形を測定すること
（指の長さ、幅、厚み、4本の指の表面積など）

掌認証の長所と短所

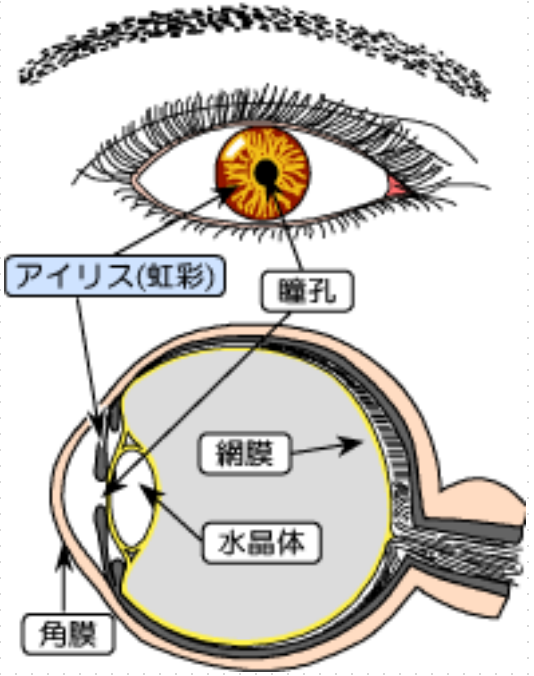
【長所】
・環境の変化を受けにくい
（幾何学的な特徴の測定のため）
・データサイズが小さい

【短所】
・装置の小型化が難しい
・不特定多数が利用する場合、衛生面を気にする方がいる

3. いろいろなバイオメトリクス技術

虹彩(アイリス)認証

目の虹彩の紋様の特徴をもとにして照合を行う技術

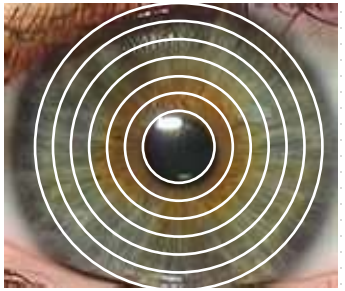


アイリスとは黒目の内側で、瞳孔より外側のドーナツ状の部分のことを言う。（瞳孔の開き具合を調節する筋肉）
妊娠６か月から２歳ごろまで成長を続け、瞳孔から外側に向かったしわ模様が形成される

虹彩認証の長所と短所

【長所】

・逆光や暗い場所に強い
・生体認証の中で、認証精度が最も高い



【短所】

・目が細いと難しい
・まつ毛が障害物になる
・サングラスは外さなければいけない

3. いろいろなバイオメトリクス技術

音声(声紋)認証

音声の音声パターンの時系列特徴(サウンドスペクトラム、声紋)をもとにして照合を行う技術

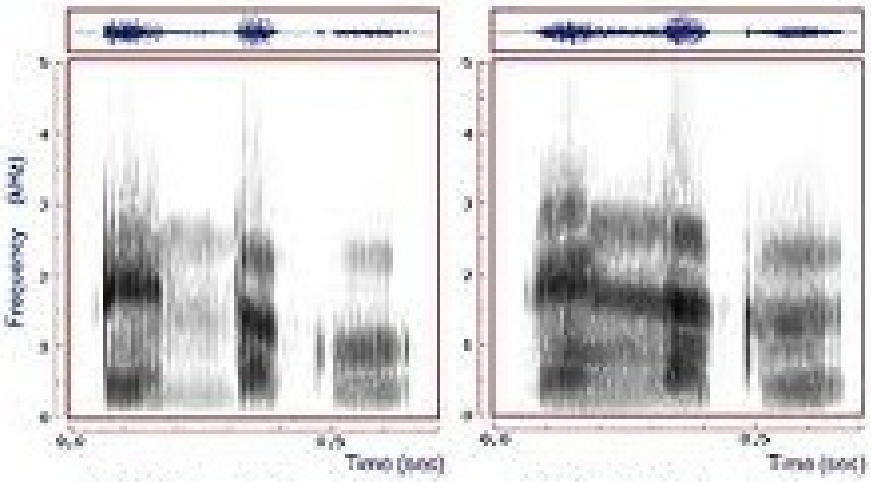
音声認証の長所と短所

【長所】

・装置の小型化・低価格化が可能
・操作が簡単で、時間もかからない
・遠隔地からでも、電話で認証できる

【短所】

・雑音に弱い
・経年変化がある(声の変化)
・録音によるなりすまし



3. いろいろなバイオメトリクス技術

署名認証

署名の個人による下記の癖（個性）をもとにして照合を行う技術
署名の形、書き順、書く速度、筆圧など

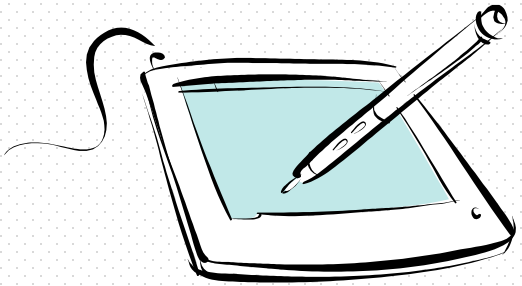
署名認証の長所と短所

【長所】

・違和感がない
・署名と認証が同時にできる
・登録データが漏えいしても変更できる

【短所】

・登録した署名を覚えておく必要がある
・経年変化がある(署名の変化)
・怪我や障害があると認識できない場合がある



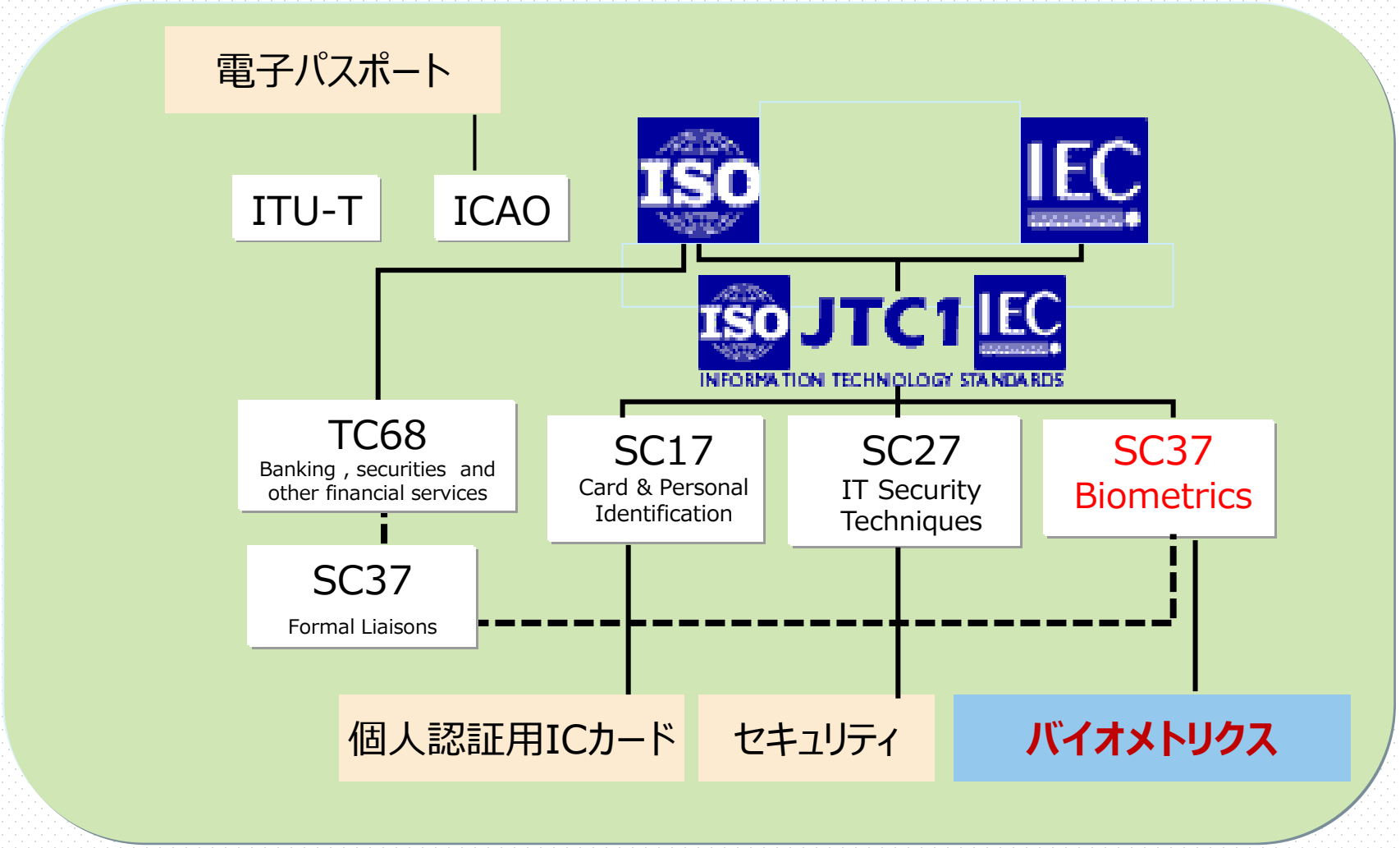
4. バイオメトリクス認証の用途

現在導入されている、おもなバイオメトリクス認証の用途

勤怠管理 （出退勤管理、タイムレコーダ）	貸金庫、貸ロッカー、鍵ロッカーの置換え
入退室管理（重要施設、マンションのドアロック）	アプリケーションプログラムの使用者認証
ATM（Automatic Teller Machine）	学校/遠隔授業の受講者認証
携帯電話の使用者認証	薬品棚、薬品カートの管理
POSレジスターの使用者認証	運転者管理のための本人確認
サーバ/端末の使用者認証	出入国管理
フィットネス機器の使用者認証	国民ID
プリンタの印刷管理	医療保険の被保険者認証

5. バイオメトリクス認証に関わる標準化

バイオメトリクス技術や運用に関わる国際標準組織



5. バイオメトリクス認証に関わる標準化

ISO/IEC JTC1/SC37について

●委員会名： ISO/IEC JTC1/SC37

●タイトル ： **Biometrics** （バイオメトリクス）

●スコープ

・応用とシステムにおける、相互運用とデータ交換を行うための一般的なバイオメトリクス技術の標準化を行う。

・一般的なバイオメトリクス技術としては、API、データ交換フォーマット、運用仕様プロファイル、性能試験などの技術項目と、相互裁判権や社会事象などを含む。

SC37のWG（ワーキンググループ）体制

	タイトル	内容
WG1	Harmonized Biometric Vocabulary and Definitions	技術用語、言語翻訳の統一
WG2	Biometric Technical Interfaces	データ、プログラムインタフェース
WG3	Biometric Data Interchange Formats	データ交換形式
WG4	Biometric Functional Architecture and Related Profiles	導入、運用仕様
WG5	Biometric Testing and Reporting	性能試験
WG6	Cross-Jurisdictional and Societal Aspects of Biometrics	管轄地域越えおよび社会的課題

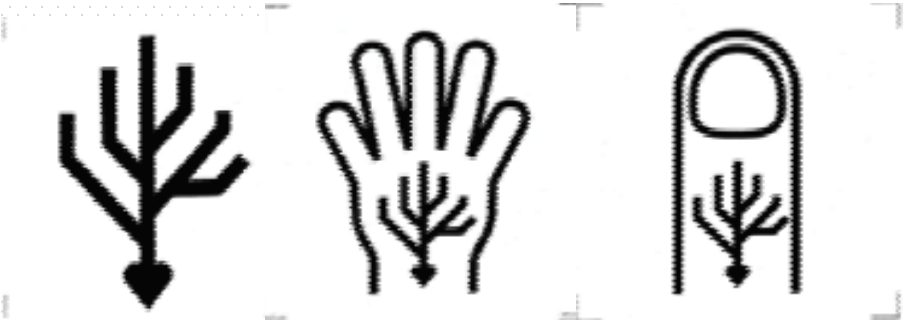
5. バイオメトリクス認証に関わる標準化

SC37の活動トピックス

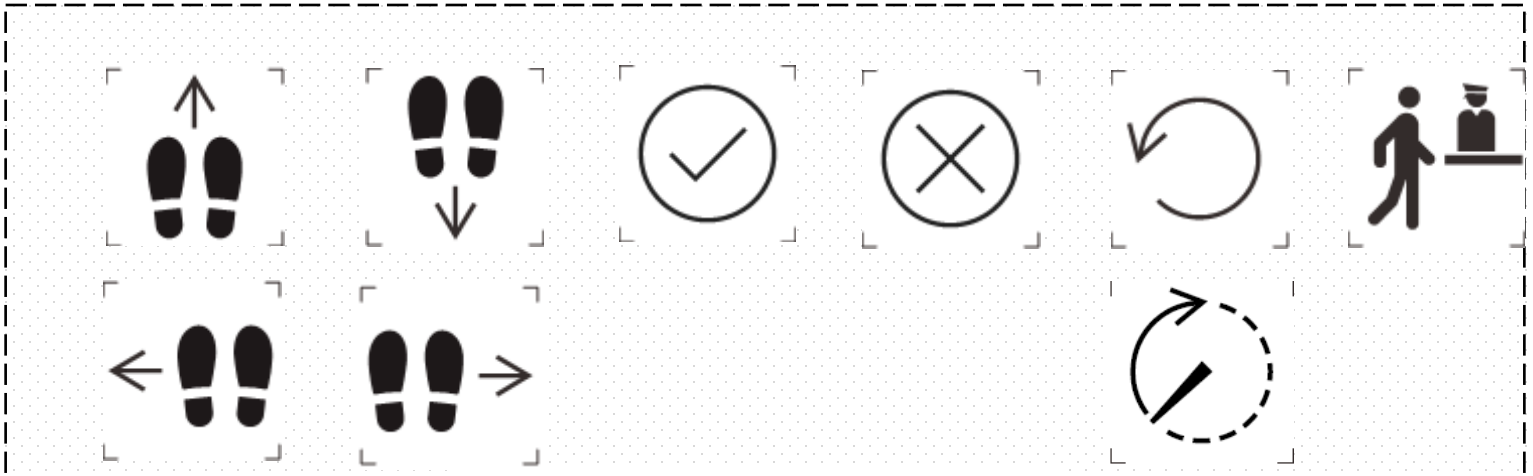
バイオメトリクス装置と関連して使用されるアイコンとシンボルの規定

指紋認証のシンボル

顔認証のシンボル



静脈認証のシンボル

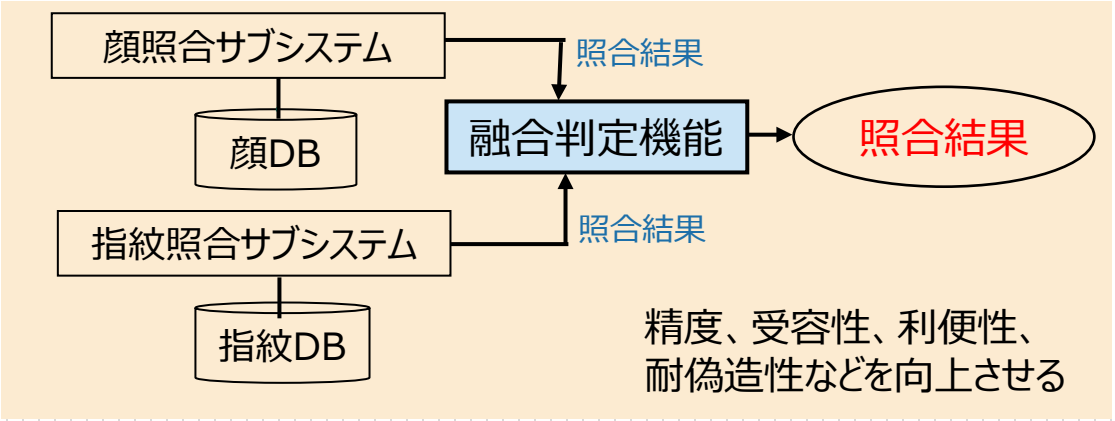


モダリティ非依存のシンボル

6. バイオメトリクス認証のトピックス

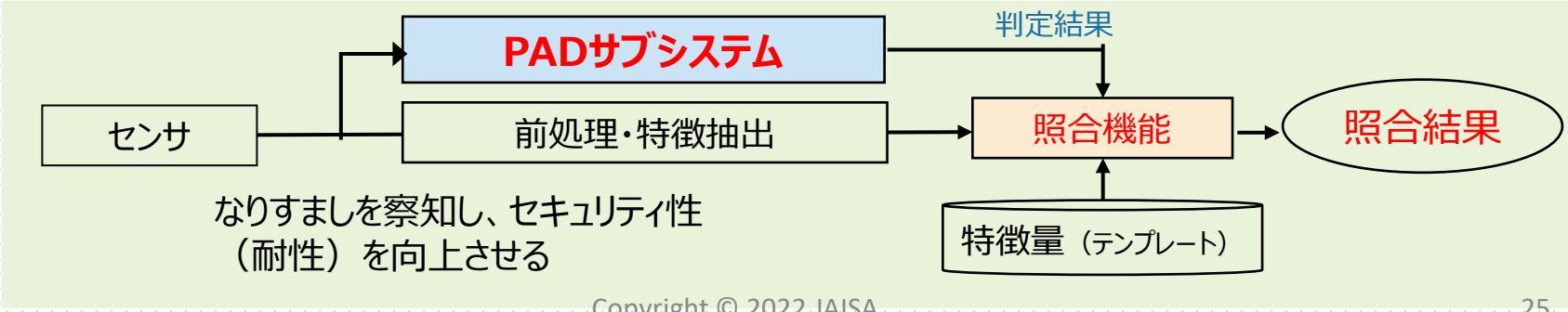
マルチモーダル（複合化）技術

複数のバイオメトリクスを組み合わせて融合判定を行い、照合結果を得る技術。



PAD（Presentation Attack Detection）技術

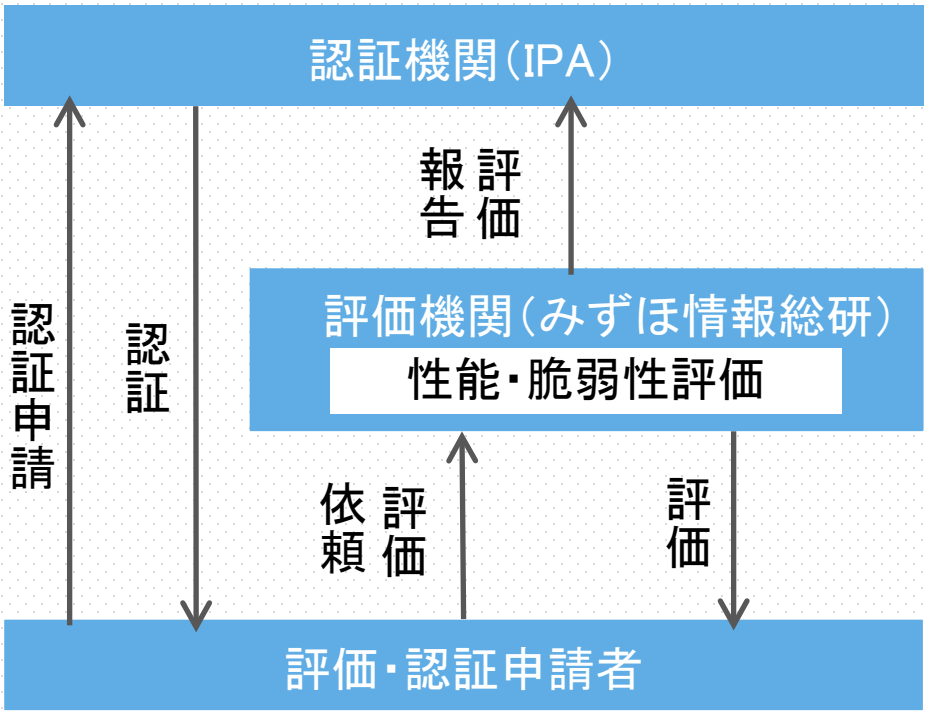
バイオメトリクス認証のためにセンサに表示されたものが「なりすまし」でないことを判定する機能。照合判定は、その機能による判定結果を含めて行われる。



6. バイオメトリクス認証のトピックス

バイオメトリクス認証製品のセキュリティ評価基盤

コモンクライテリアを適用したバイオメトリクス（静脈認証）装置の第三者評価・認証



セキュリティ評価・認証体制

評価機関：みずほ情報総研

【評価内容】

①性能評価

②脆弱性評価（偽造物による
なりすまし攻撃検知の評価を含む）

経済産業省　工業標準化推進事業委託費
戦略的国際標準化加速事業
（国際標準共同研究開発・普及基盤構築事業）

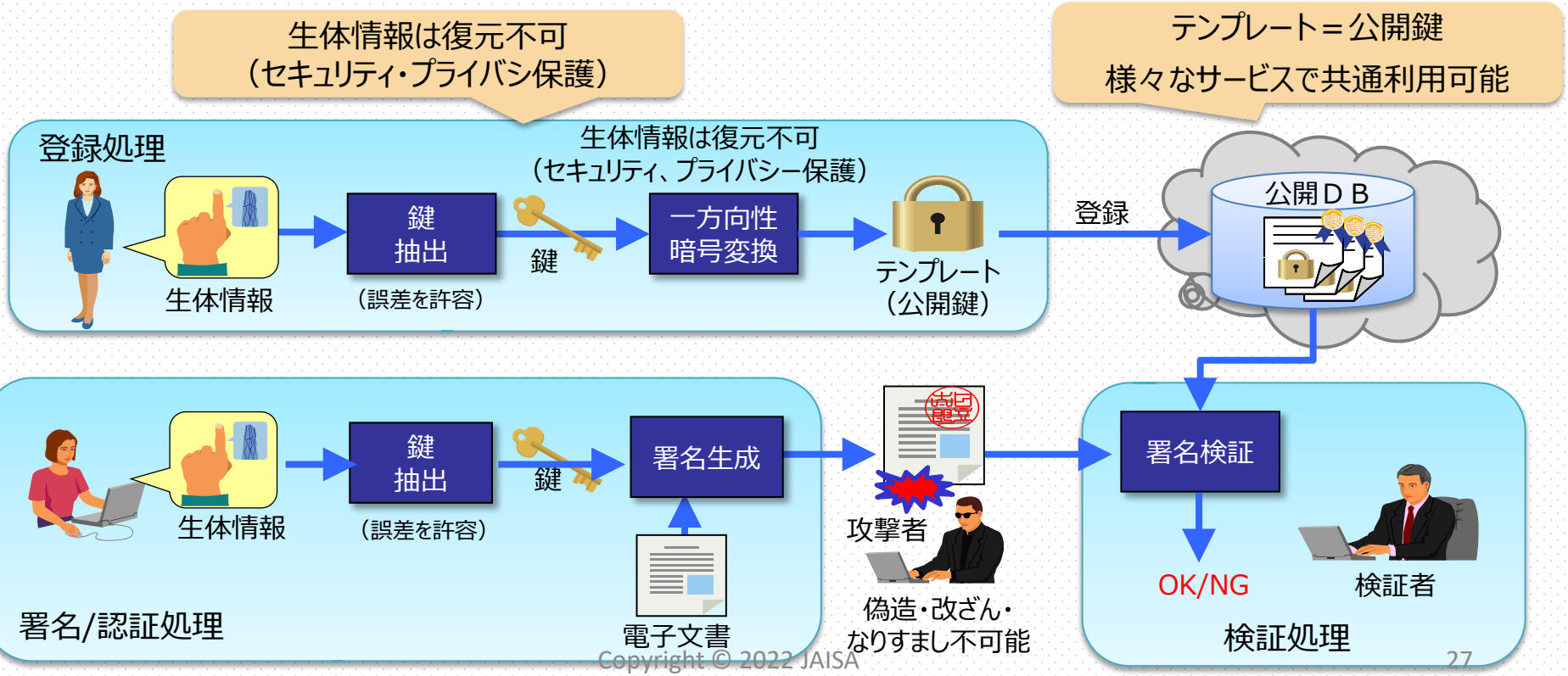
受託事業成果による実施期間
2014年4月より2017年3月（ 3年間 ）

http://www.jaisa.jp/pdfs/170331/001.pdf

6. バイオメトリクス認証のトピックス

バイオメトリクス情報を「鍵」とするPKI認証基盤（公開鍵基盤）

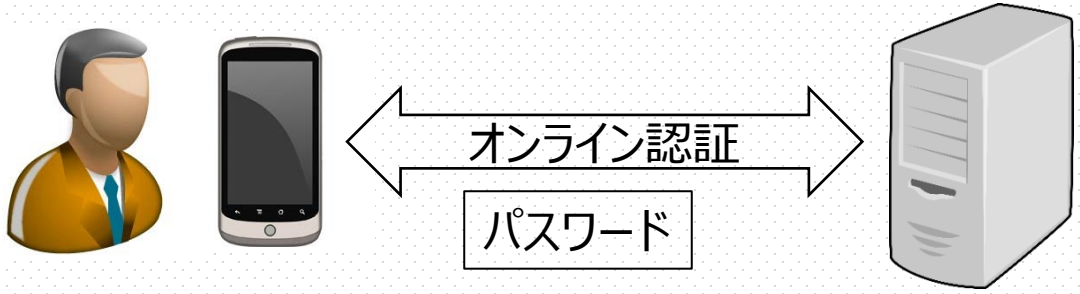
- 生体情報から「公開鍵（テンプレート）」と「秘密鍵」を生成
- 公開鍵から生成情報の復元は不可能
- 公開鍵は公開可能、または変更可能なため厳重な鍵管理不要
- PKIと同等のセキュリティ機能を持つ



6. バイオメトリクス認証のトピックス

FIDO（First IDentity Online）とバイオメトリクス認証の連携

従来（パスワード認証）



FIDO（ローカル認証と公開鍵認証の組合せ）

●オンライン認証のためにサーバにパスワードが提供されない

●ローカル認証はどのような認証技術でもよい

（利便性の面からバイオメトリック認証が適用され始めている）

以上