生体認証の原理と課題

2014年8月2日

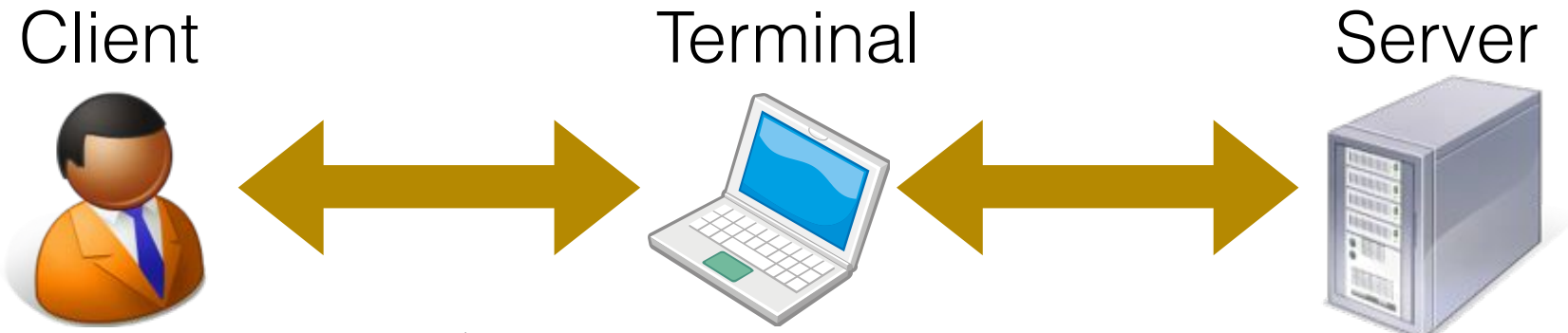
先端数理科学B『情報セキュリティの数理』講義資料

産業技術総合研究所 セキュアシステム研究部門　大木 哲史

Agenda

- 生体認証とは
  - 生体認証の特徴(モダリティ)
  - 様々な生体認証方式
  - 生体認証の課題
- テンプレート保護型生体認証
- なりすまし対策(Presentation Attack Detection)

個人認証の手段



ユーザ認証

クライアント認証
暗号プロトコルなど

What you have(所有ベース)

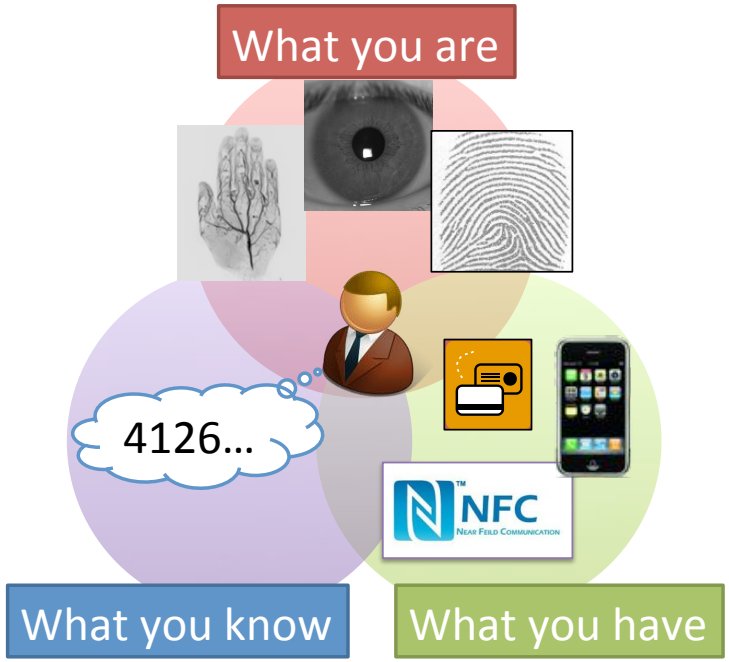
IDカードなど

What you know(知識ベース)

暗証番号，パスワードなど

What you are(生体認証)

指紋，顔，血管パターン，音声など



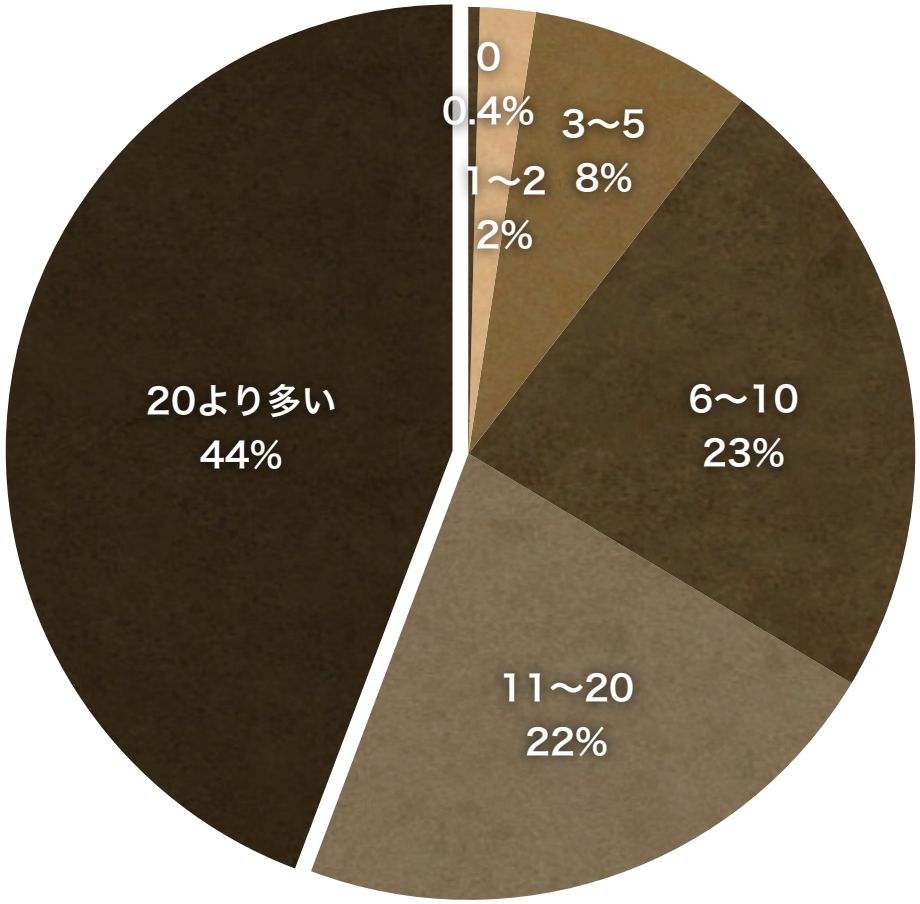
大規模サイトのパスワード漏洩事故

企業名	時期	内容	参照
WordPress sites	2009-09	large quantity of hacked sites using WordPress software and MySQL	WordPress SQL Injection – Latest Attack
eHarmony ancillary site	2011-02	user names, email addresses and hashed passwords	Some eHarmony user information stolen
MySQL.com	2011-03	unknown quantity of user credentials	MySQL Website Falls Victim to SQL Injection Attack
Barracude Networks site	2011-04	names and contact information	Hackers disclose SQL injection of Barracuda website
Sony Playstation Network	**2011-04**	**700万人分以上の氏名, 誕生日, e-mailアドレス, パスワード, セキュリティの質問等の個人情報が漏洩した。加えてクレジットカード番号が漏洩した可能性がある。**	How the PlayStation Network was Hacked
Sony Music	2011-05	"relatively small"	Sony Music Japan hacked through SQL injection flaw
Sony Pictures	2011-06	1 million user credentials	New Sony Hack Claims Over a Million User Passwords
Nokia	2011-08	unknown number of forum users credentials	Hackers breach Nokia developer community
Gamigo	**2012-03**	**1100万人分のパスワードのハッシュ値と800万人分のe-mailアドレスが2012年3月の侵入後、2012年7月にインターネットで公開**	SQL-Injection (Gamigo, Elite, FanPages) 11 million passwords from hacked game website dumped online
LinkedIn	**2012-06**	**ロシアのハッカーグループが、650万人分のパスワードのハッシュ値（パスワードファイル）をインターネットで公開**	LinkedIn hack and lessons for your company Update: LinkedIn Confirms Account Passwords Hacked
Yahoo	**2012-07**	**Yahoo Contributor Networkのアカウント450,000 人分のe-mailアドレスと平文パスワードをWebに公開（有効なパスワード5%）**	Yahoo fixes password-pilfering bug, explains who's at risk
FBI, Nasa	**2012-12**	**Hactivist “Team Ghostshell”がNASA, FBI, Pentagon, Interpol等から160万人分のEmailアドレス＋パスワードを窃取し，pastebin.comに公開したと声明**	http://news.cnet.com/8301-1009_3-57558338-83/ghostshell-claims-breach-of-1.6m-accounts-at-fbi-nasa-and-more/

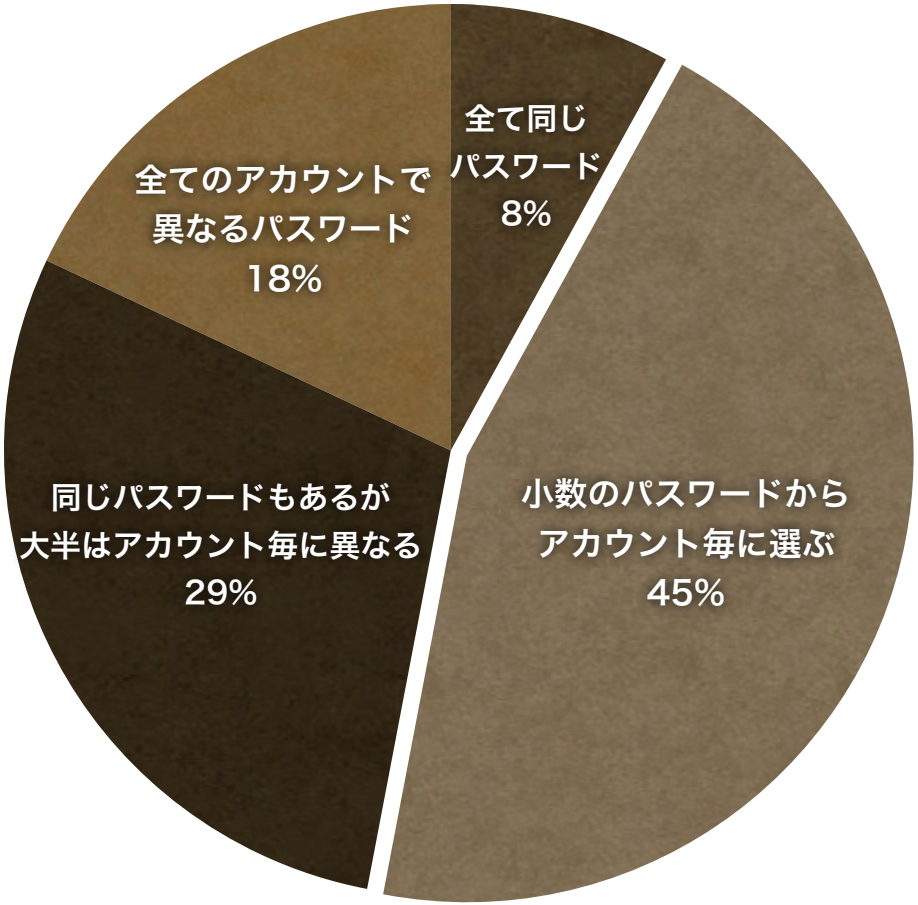
出所）The Code Curmudgeon, “SQL Injection Hall of Shame,” 2013年8月を元に作成.

パスワード使い回しの実態

パスワードを登録しているサイト数



パスワードの選び方

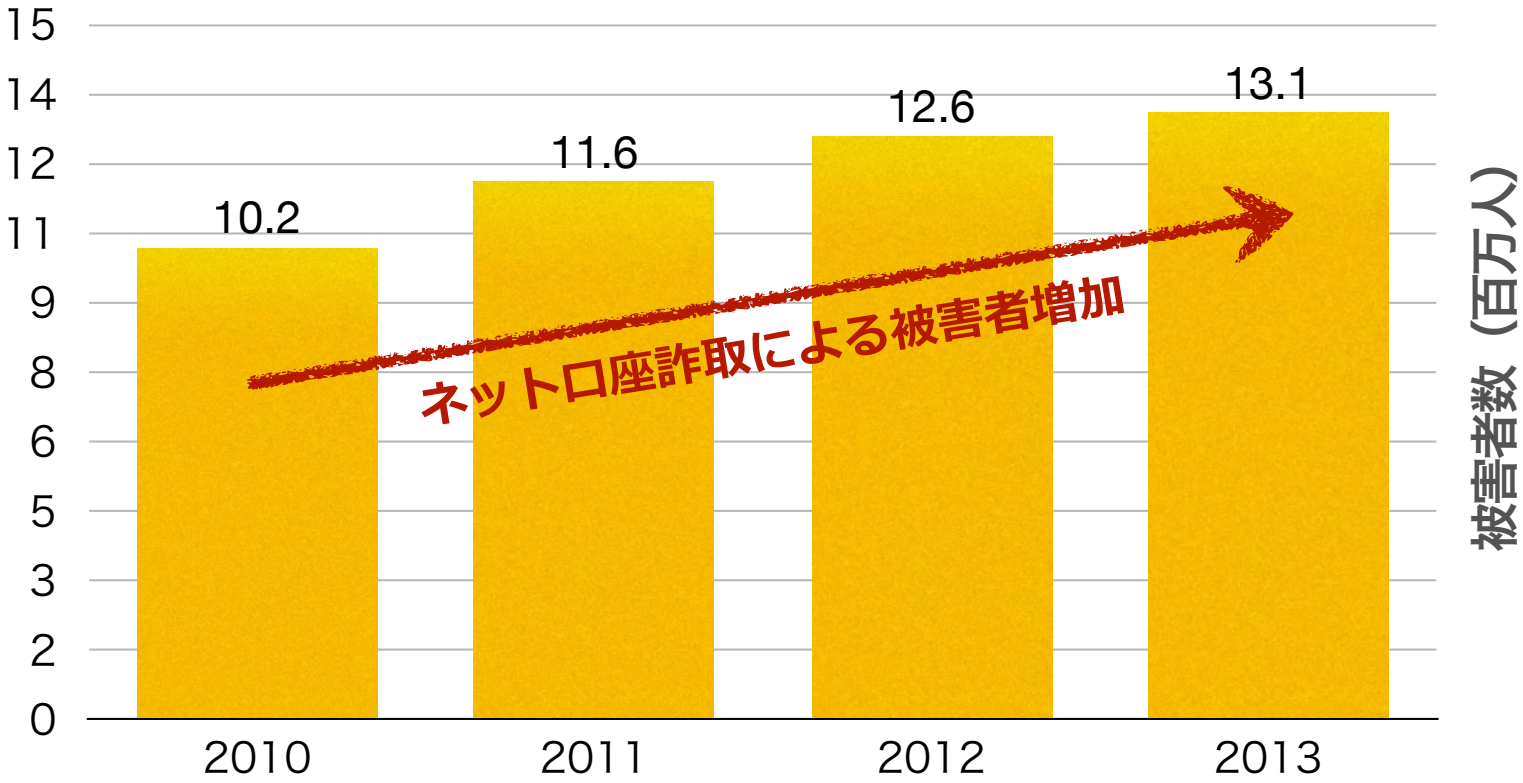


Source: Symantec official blog, “Password Survey Results”, 2010.3.

多くのユーザーは小数のパスワードを複数のサイト登録している。
大規模サイトからのパスワード漏洩で利用者のパスワード文字列が解読された場合には、金融機関等でも不正ログインの危険が高まる。

Identity Theft の深刻化(米国)

米国では2013年に**1,310万人(被害総額1.8兆円)**がIdentity Theftの被害に遭っている (オンラインID詐取を含む)。主な要因は、管理不能なほど多数のパスワードを記憶することを人々に強いていることである。このような現状をうけて、米国では**NSTIC**(National Strategy for Trusted Identities in Cyberspace)の枠組みでの中で、現在の**認証技術を発展させ**、複数の民間Identity Providerと国のIdentity Providerが共存し、個人を証明するクレデンシャルを発行するIdentity Ecosystemの構築を目指している。



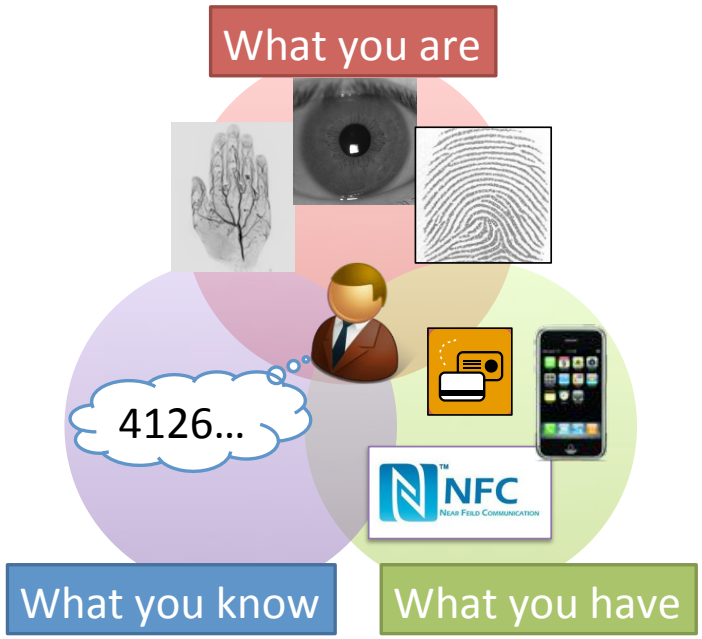
Source: Javelin Strategy & Research, 2013.

2010-2013の被害数の伸びは，New Account FraudとAccount Takeover Fraudが主因と推定

New Account Fraud: 被害者の個人情報を利用して被害者名でアカウントを開設する詐欺

Account Takeover Fraud: 被害者のアカウントへのアクセス権を詐取して，アカウント情報を変造する詐欺

個人認証の3要素



	パスワード (What you know)	所有物(ICカード) (What you have)	生体認証 (What you are)
忘却・紛失・盗難	✕ 記憶の限界	△ 紛失のリスク 盗難のリスク	◯ 忘却・紛失・盗難のリスクなし
推測・偽造	✕ パスワード使い回し	◯ 偽造困難	△ 偽造による被害事例あり
コスト	◯ 追加装置必要無し	✕ 読み取り装置必要 カード発行費用必要	✕ 読み取り装置必要

3要素の利点をセキュリティ強度や利用シーンに応じて活用することで高度かつ利便性の高い認証が実現可能

生体認証

バイオメトリクス(BIOMETRICS) とも
biology + metrics

1.**普遍性**(universality:誰もが持っている特徴である)
2.**唯一性**(uniqueness:本人以外は同じ特徴を持たない)
3.**永続性**(permanence:時間の経過とともに変化しない)

の3つの条件を備えている生体的な測定結果を用いて
本人を自動的に確認する技術

cf. 人工物メトリクス(artifact-metrics)
基材にランダム分散した磁性ファイバの磁気パターン等

参考）"Automatically recognizing a person using distinguishing traits (a narrow definition)", The Biometric Consortium (http://www.biometrics.org/)

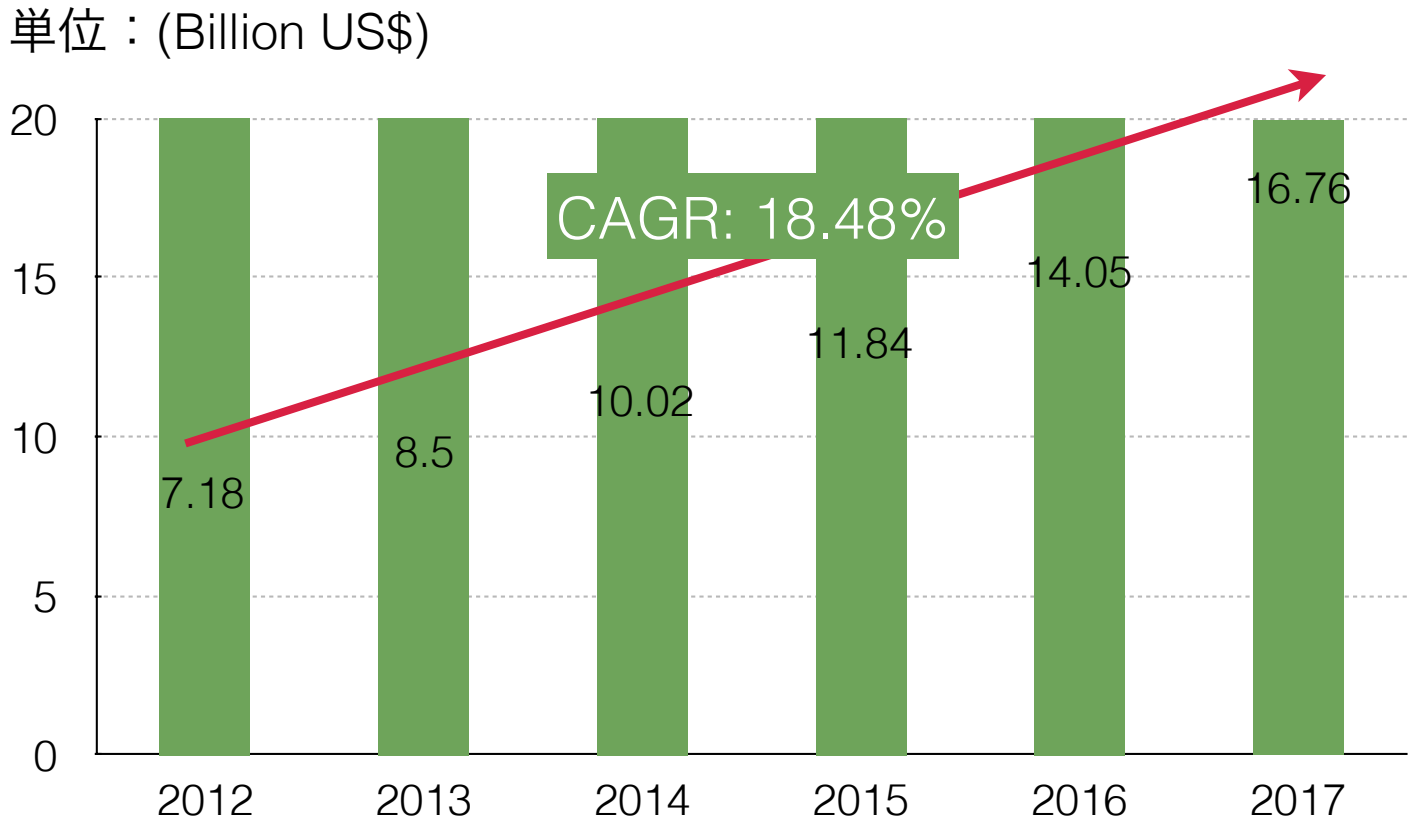
生体認証の歴史

B.C.6000頃	・中国、古代アッシリアで粘土板上の拇印を使って個人認証を行っていた
B.C.300～2000	・(B.C.1000～2000頃) 古代バビロニア時代の取引に指紋を利用 ・(B.C.300頃) 古代中国で署名に拇印を使用
～17世紀	・(1684)ヘネミア・グルー(イギリス)や(1686)マルチェロ・マルピーギ(イタリア)が指紋に特徴が存在することを発見
～19世紀	・(1823)ジョン・パーキンジ、指紋が円形や渦巻状の隆線で構成される渦状紋、また弓やりになった弓状紋等、9種類のパターンに分類するできることを発見 ・(1874～80)ヘンリー・フォールズ(スコットランドの宣教医師)、指紋により世界で初めて犯人の特定を行う。また数千人の指紋セットを相互比較することで「万人不同性」を確認する。 ・(1880)ウイリアム・ハーシェルによって指紋が「終生不変」であることが確認される。Nature論文「指紋による公的な個人認証」の発表。 ・(1891)フランシス・ゴールトンがマニューシャ(隆線の端点と分岐点)の存在と、別人のマニューシャが一致する確率が640億分の1であることを数学的に証明する。 ・(1892)アルゼンチン警察のジョアン・ブセチッチ、マニューシャによる最初の犯人識別 ・(1897)インド政府は指紋法を発布 ・(1897)英国のエドワード・ヘンリーの助手のインド人のアジール・ハクとヘムチャンドラ・ボーズにより、10本の指に紋様分類のコードを当てはめる10指分類方法が開発される。このヘンリー分類システムは英国で採用されて以降、基本概念としてほとんどの国で採用されている。
～20世紀以降	・(1918) エドモンド・ロカード、二つの指紋の間でマニューシャ12個が一致すれば同一人物と見なしてよいと述べる(この考えは現在でも「12点法」として日本の警察庁など多くの国で使われている)。 ・(1962) AT&Tベル研究所のカースタが声紋による話者認識の可能性を発表 ・(1973) 京都大学金出教授らにより、顔画像による人物識別法が提案される ・(1976) 米国 Identimat 社が機械式の掌の長さを識別する装置、Identimation を発表 ・(1978) 米国 アイデンティファイ社から網膜認証に関する基本特許が提出される ・(1979) NEC、マニューシャの位置や方向の他に、マニューシャ間の隆線数を照合に利用する方式を開発 ・(1993) ジョン・ドーグマンが虹彩コードによる認証方式をIEEEに発表 ・(1993) Kirby, Sirovichga, 固有顔による顔認証の研究開始 ・(1997) 明治大学映像処理研究室にて崔教授が手の甲静脈による認証アルゴリズム開発に着手 ・(2000) シドニーオリンピックのドイツ選手村で虹彩認証システム(米国 Eye Ticket社)利用 ・(2001) スキポール空港(オランダ)で虹彩認証を利用した出入国管理システム導入 ・(2002) 米国で入国する外国人に対して生体情報の提示を義務付ける法律が成立 ・(2003) 成田空港にてe-チェックイン実証実験 ・(2003) US-VISITプログラム発表。出入国時のセキュリティを生体情報を用いて強化する ・(2004) 富士通が手のひら静脈認証を用いたATMシステムを販売開始

参考) 星野幸男, “指紋認証技術”, 画像電子学会編

バイオメトリクスの市場予測

- Global Biometrics Market Size Forecast in 2013(forecast): **8.5 Billion US$**
- Compound Average Growth Rate(CAGR) : **18.48% (2012 - 2017)**



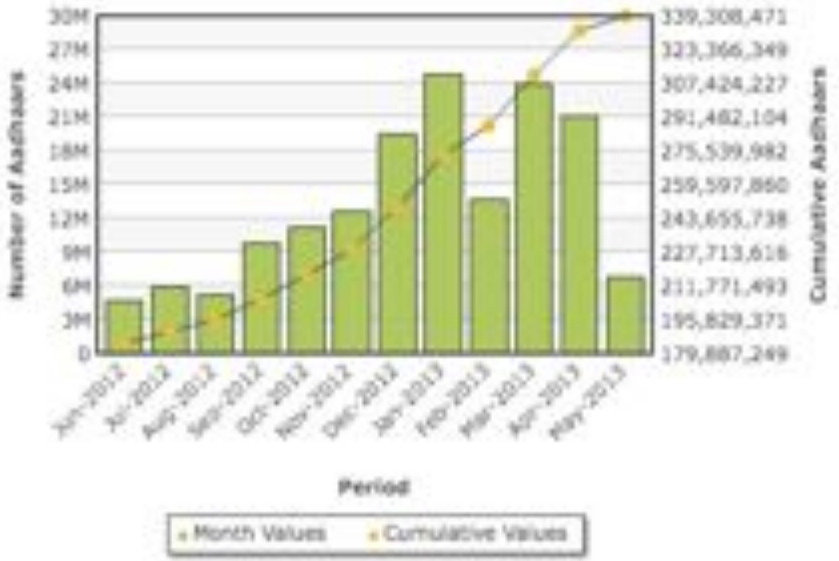
(Source: Global Biometric Systems Market Forecast & Opportunities, 2017 (c) TechSci Research)

インド国民IDにおけるバイオメトリクス活用

UIDAI Unique Identification Authority of India
Planning Commission, Government of India

出典：UIDAI Webサイトより

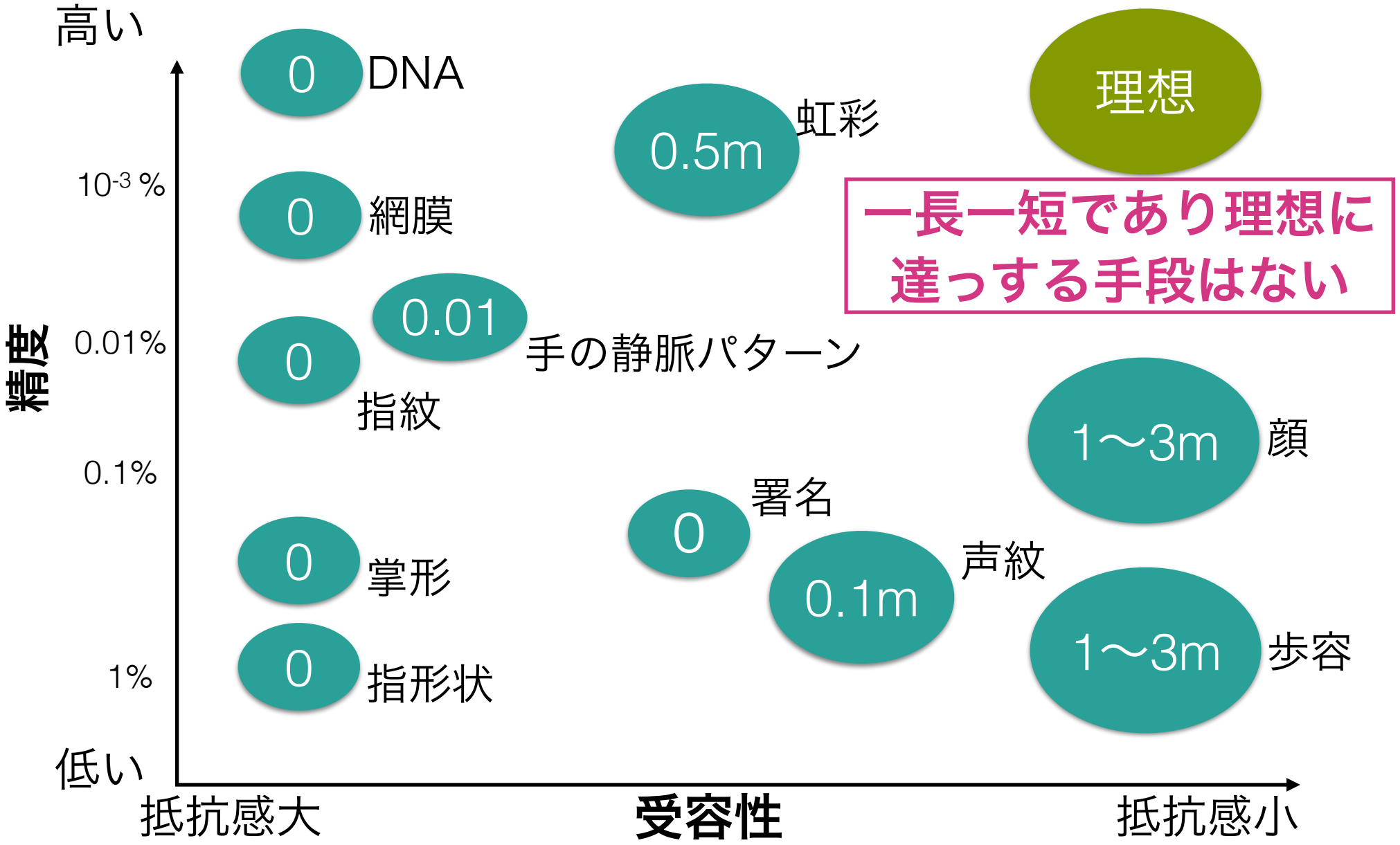
出典：UIDAI Webサイトより



社会保険の二重受給等の問題から生体認証が不可欠

今後は遠隔医療・社会福祉の基盤として利用

生体認証の特徴(モダリティ)

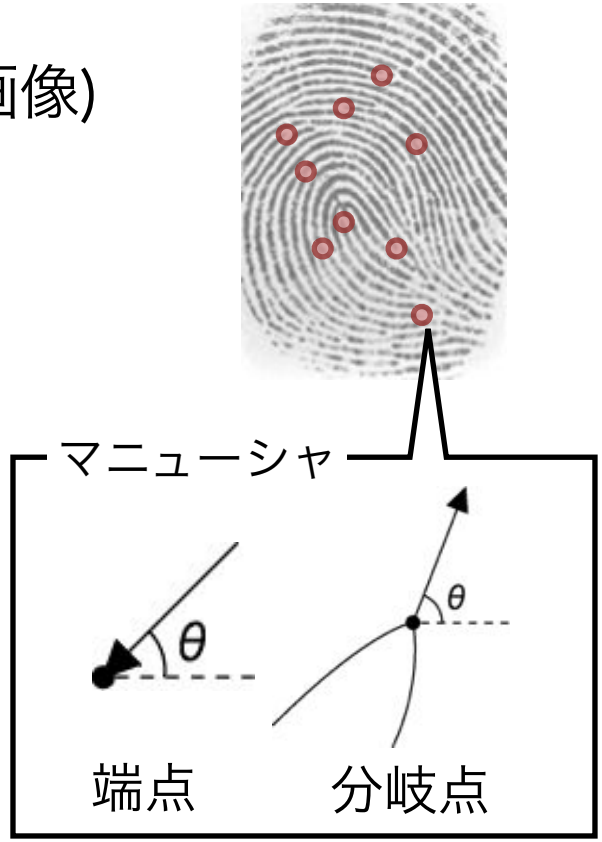


生体認証の研究事例と特徴

	パラメータ	特徴	課題
指紋	・特徴点(マニューシャ)の位置 ・リレーション	・万人不同，終生不変 ・犯罪捜査での利用	・指紋画像の品質 ・衛生面の確保 ・社会的な受容
網膜	・毛細血管パターン	・万人不同，終生不変 ・コピーが困難	・眼底撮影と同様の専用装置が必要
虹彩	・瞳孔の開きを調節する筋肉のパターン	・万人不同，終生不変 ・眼球内部の疾病等の影響がない	・睫毛の影響
血管パターン	・静脈パターンの直接照合 ・静脈の分岐点・方向	・非接触で認証可能 ・心理的抵抗が少ない ・コピーが困難	・体毛，脂肪層の影響
掌形	・掌の幅，厚さ ・指の長さ等	・操作が容易	・信頼性の確保 ・衛生面の確保
顔	・主成分分析を用いた固有顔 ・目，口，鼻の位置や形状等	・非接触で認証可能 ・心理的抵抗が少ない	・時間的な変化 ・メガネ，ひげ等の影響 ・照明や撮像角度，背景等の制約
音声	・スペクトル包絡 ・ピッチ，発音レベル，発声速度等	・非接触で認証可能 ・心理的抵抗が少ない	・時間的な変化 ・体調の影響 ・環境ノイズによる影響
筆跡	・筆順，筆速，筆圧等	・操作が容易(小型タブレット等) ・心理的抵抗が少ない	・時間的な変化 ・偽筆対策

指紋認証

1) **マニューシャ方式**： 特徴点(マニューシャ)の位置・方向
2) **マニューシャ・リレーション方式：**
   マニューシャの位置・方向 + マニューシャ間の隆線数
3) **チップマッチング方式：**
   マニューシャの位置 + 周囲の小画像(チップ画像)
4) **周波数マッチング方式：**
   フーリエ画像同士の相関を計算



隆線：Ridge Line

- 指紋の紋様を京成する皮膚の盛り上がったところ

特徴点：Minutiae (マニューシャ)

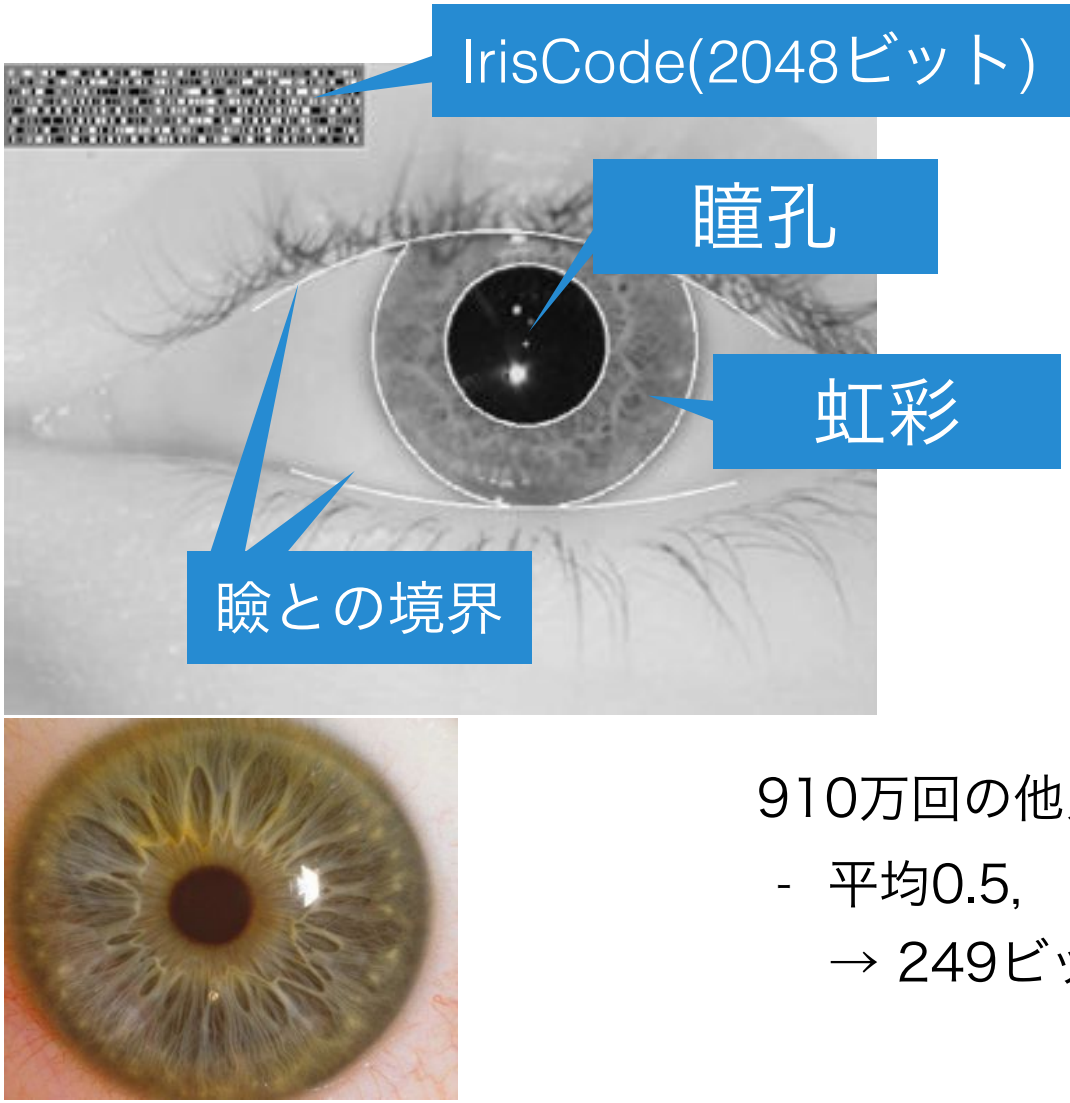
- 端点：隆線が途切れているところ
- 分岐点：隆線が分かれているところ

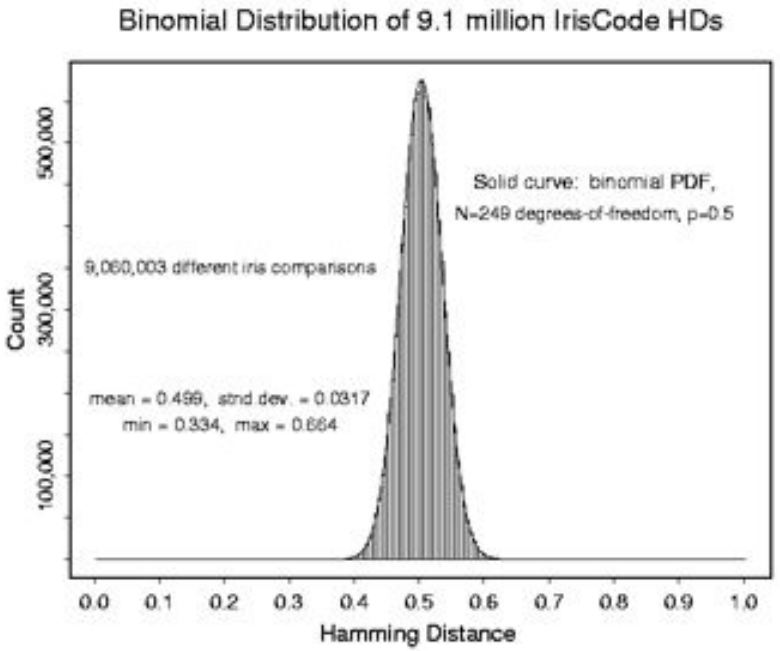
特徴点の情報：

- 特徴点の位置と方向

虹彩認証

IrisCode: 虹彩から2048ビットのビット列を生成





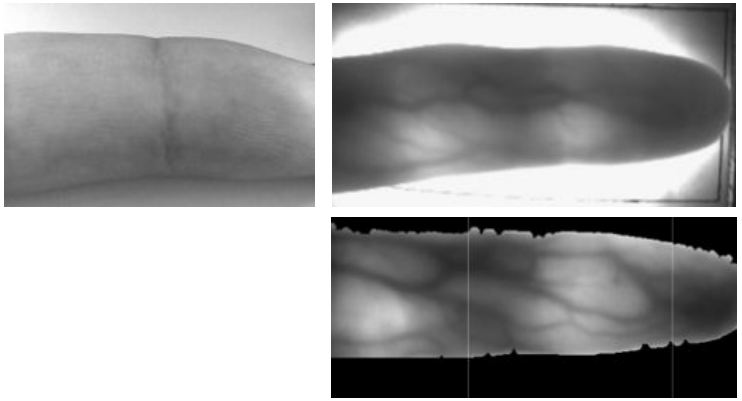
910万回の他人照合による正規化ハミング距離分布

- 平均0.5，自由度N=249の二項分布とほぼ一致
  → 249ビット程度が実際に使われているビット数

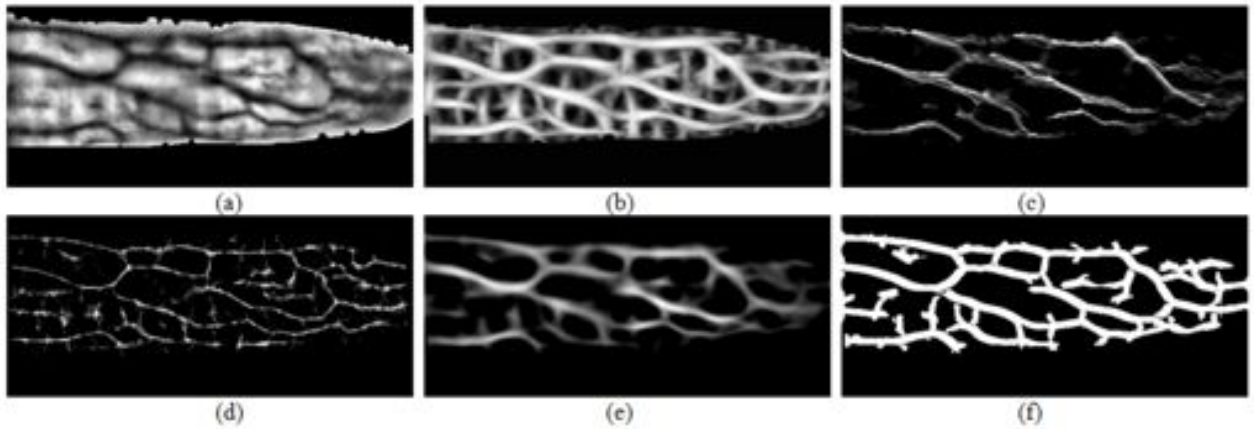
参考) John Daugman, “How Iris Recognition Works,” IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, Vol.14,No.1, Jan, 2004

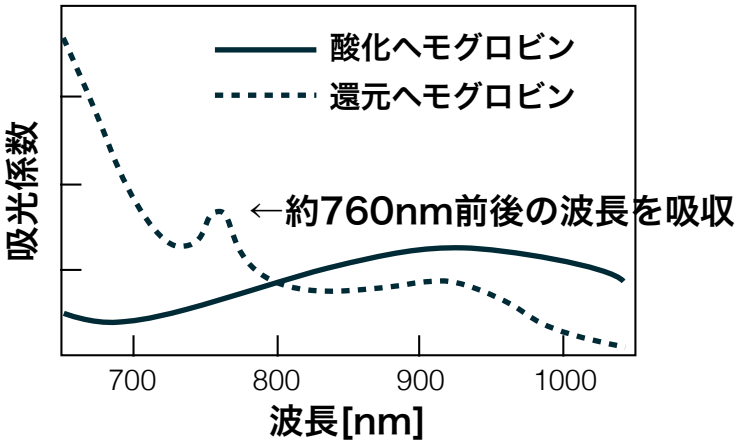
血管パターン認証(指静脈・手のひら静脈)

近赤外画像



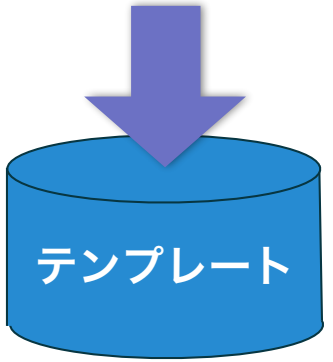
静脈画像の抽出





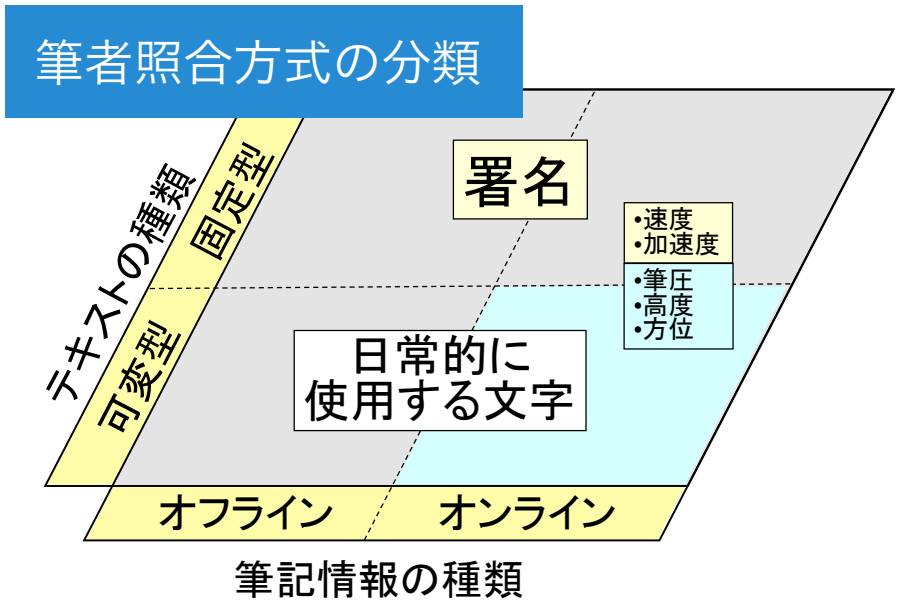
手のひら静脈

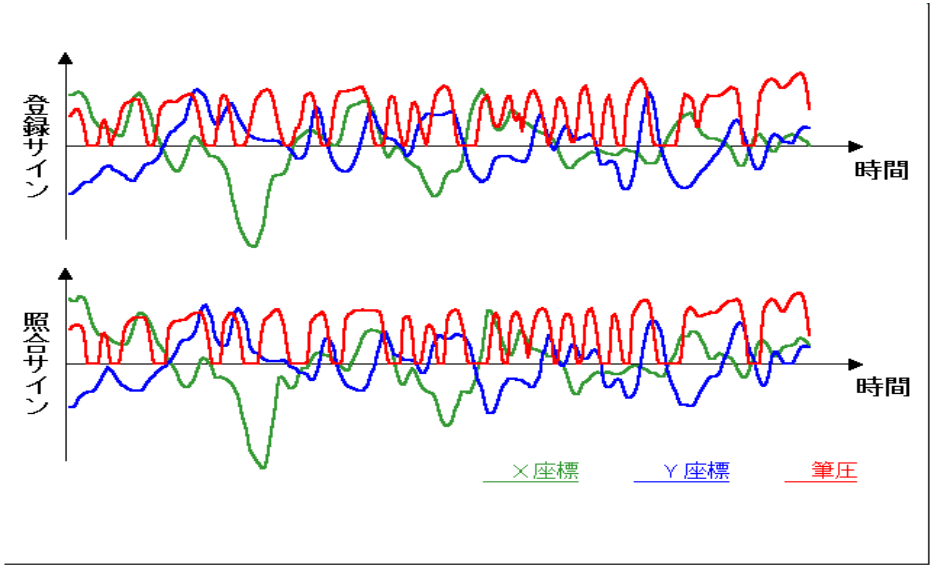
指静脈

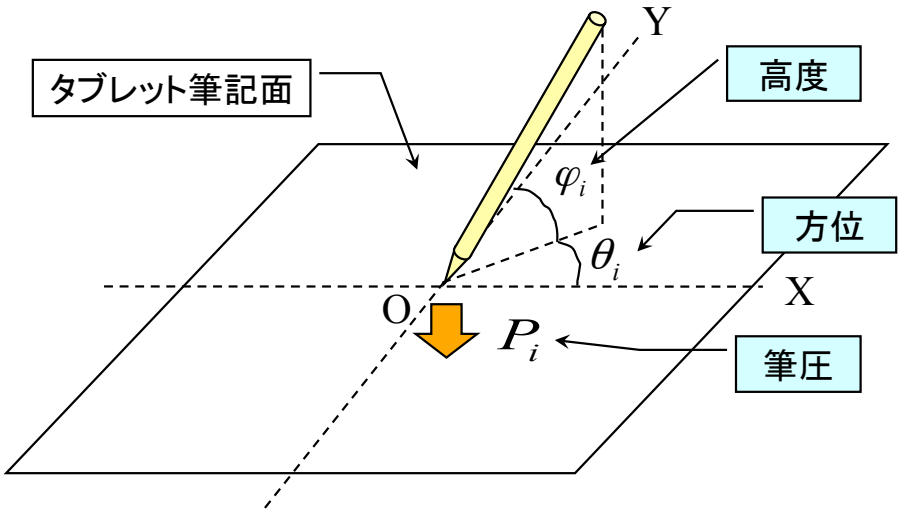


参照) Ajay Kumar and Yingbo Zhou, “Human Identification using Finger Images”, IEEE Trans. Image Processing, vol. 21, pp. 2228-2244, April 2012.

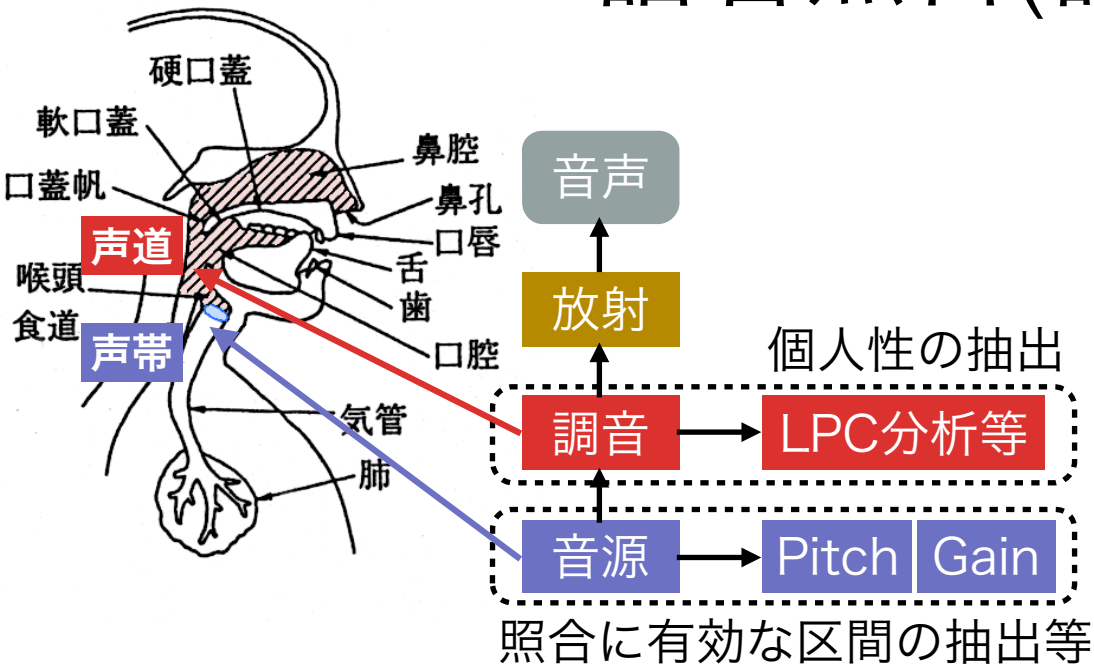
筆者照合方式


筆者照合方式の分類
テキストの種類
固定型
可変型
署名
•速度
•加速度
•筆圧
•高度
•方位
日常的に
使用する文字
オフライン
オンライン
筆記情報の種類


登録サイン
時間
照合サイン
時間
X座標
Y座標
筆圧


タブレット筆記面
Y
高度
φ_i
方位
θ_i
X
O
P_i
筆圧

話者照合(話者認識)



テキスト依存型

指定内容(パスワード等)を発話する

テキスト独立型

発話内容を限定しない

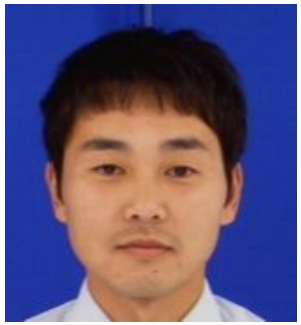
テキスト提示型

毎回異なるキーワードを発話し，本人であるかどうかとダブルチェックする

- 特定の帯域のスペクトル包絡特性をモデル化して認証するのが一般的
  → LPC分析等でモデル化した声道特性を推定する
- 音素(a,i,u,e,o など)により特性が異なる？
  → 多数音素を含む学習音声を用いて、GMM等でモデル化

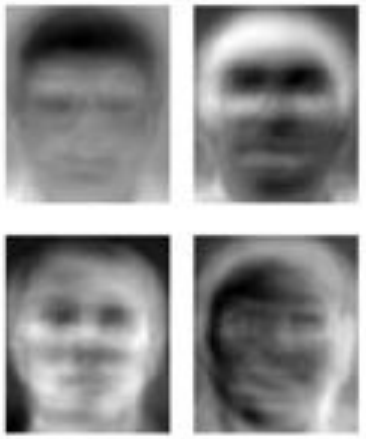
近年ではGMMのモデルパラメータから得たGMMスーパーベクトルを因子分析の入力として話者特徴を抽出するi-vectorやJFAといった手法が提案され、少量の発話データで高い認証精度を達成している。

顔認証技術



顔特徴点の抽出

固有顔(AT&T研究ＨＰより)



初期には目・鼻・口の位置やその相対的関係を特徴として認証する方式が提案された。近年では主成分分析を使って求めた固有顔を用いる方式が主流。

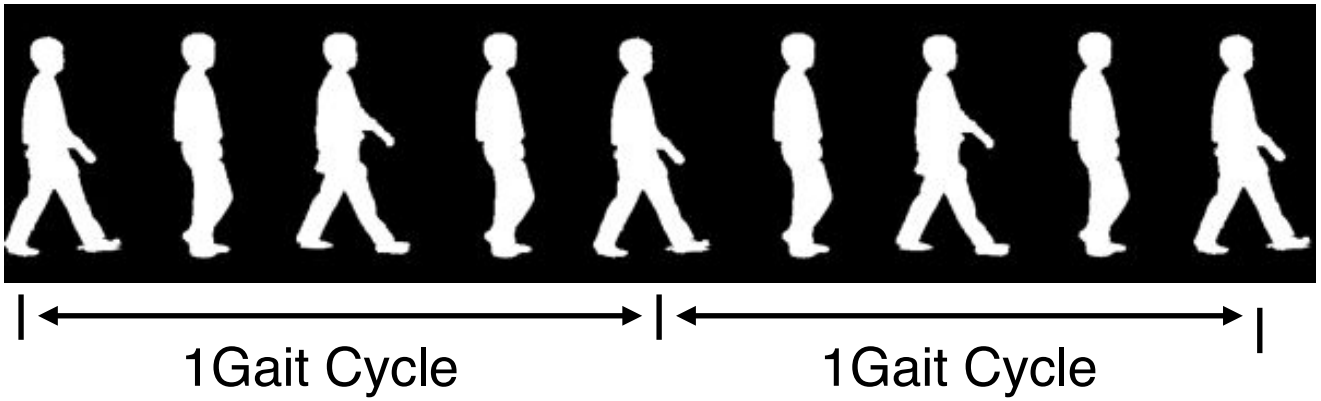
回転により顔画像の変化(XM2VTSデータベースより)

いずれの手法においても、顔の回転や、屋内/屋外における照明条件の違いによる顔画像の変化への対応が課題となっている

※ 監視カメラ等の低解像度環境においては、そもそも顔領域の検出自体が課題

歩容認証

Gait Cycle



識別対象の開始点と終了点を定める
共通な識別単位の設定

- 低解像度カメラでの認証
- 大規模サーベイランスシステム
- カメラ間の人物追跡
- 顔認証同様照明条件や撮影角度などに課題

Gait Energy Image

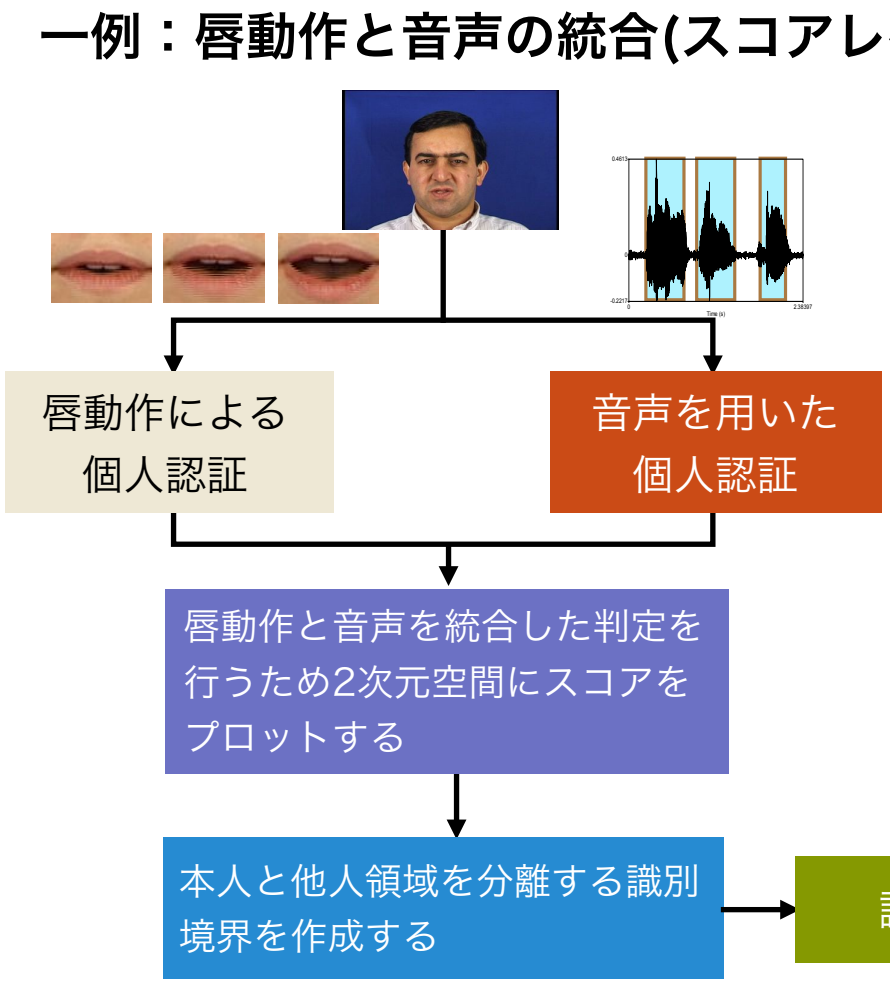
Gait Image の Moving Average

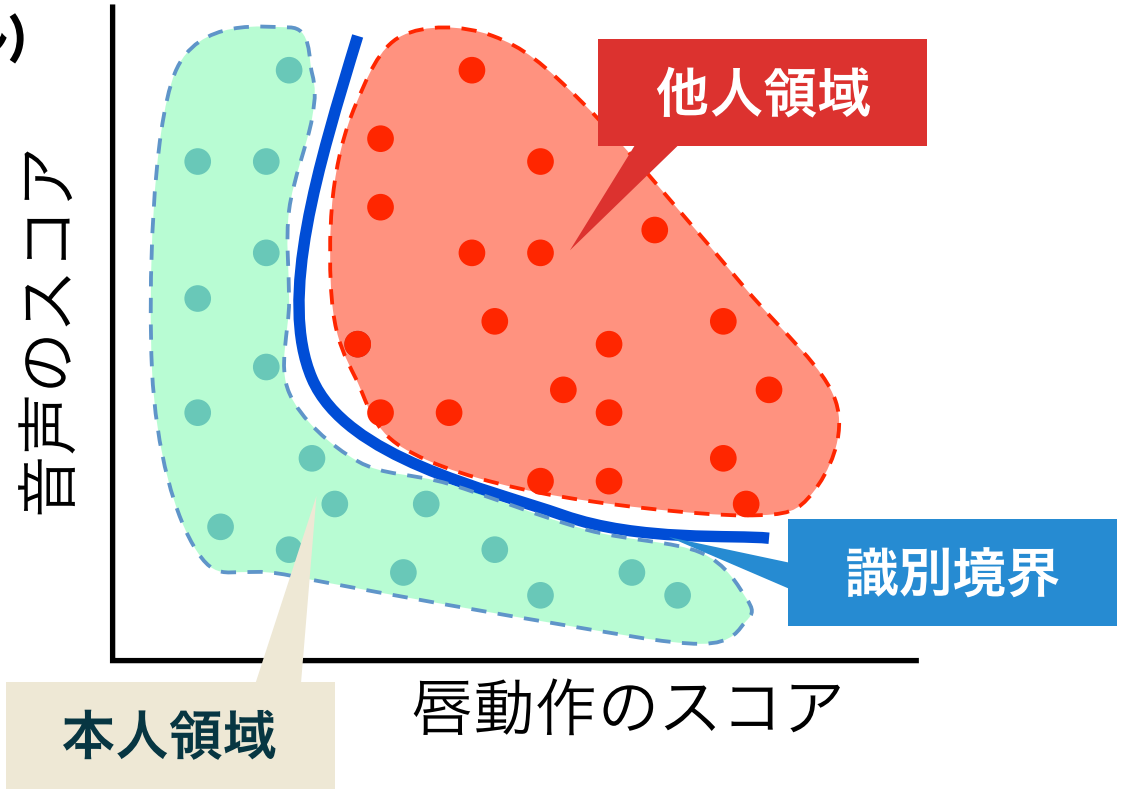
参考) Han, et al. “Individual Recognition Using Gait Energy Image”, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 28, NO. 2, FEBRUARY 2006.

マルチモーダルバイオメトリクス

- 複数のモダリティの認証結果を統合して認証精度を向上
- AND や OR では FRR/FAR を同時に改善することが困難
  → 特徴レベルやスコアレベルでの統合

一例：唇動作と音声の統合(スコアレベル)

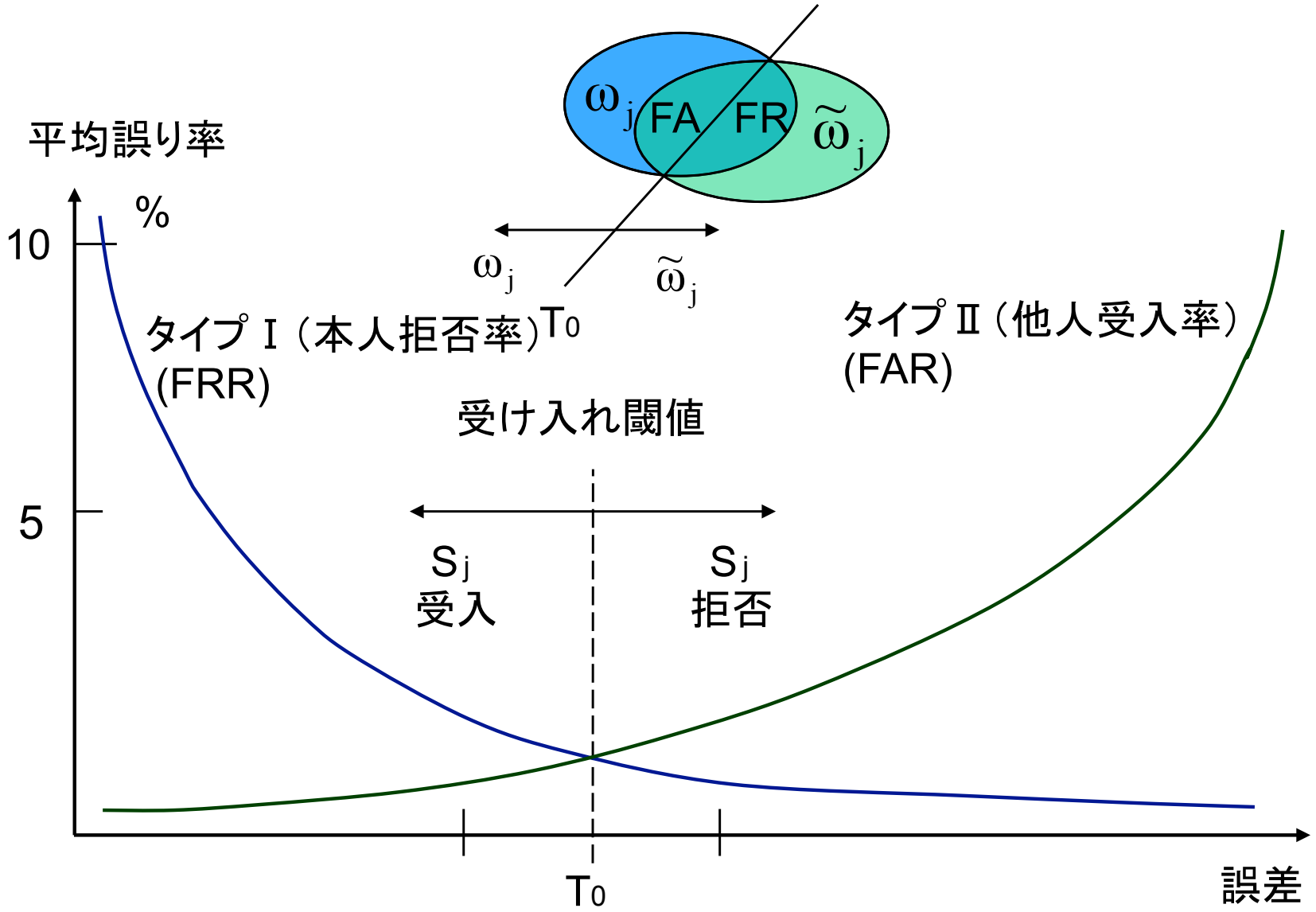




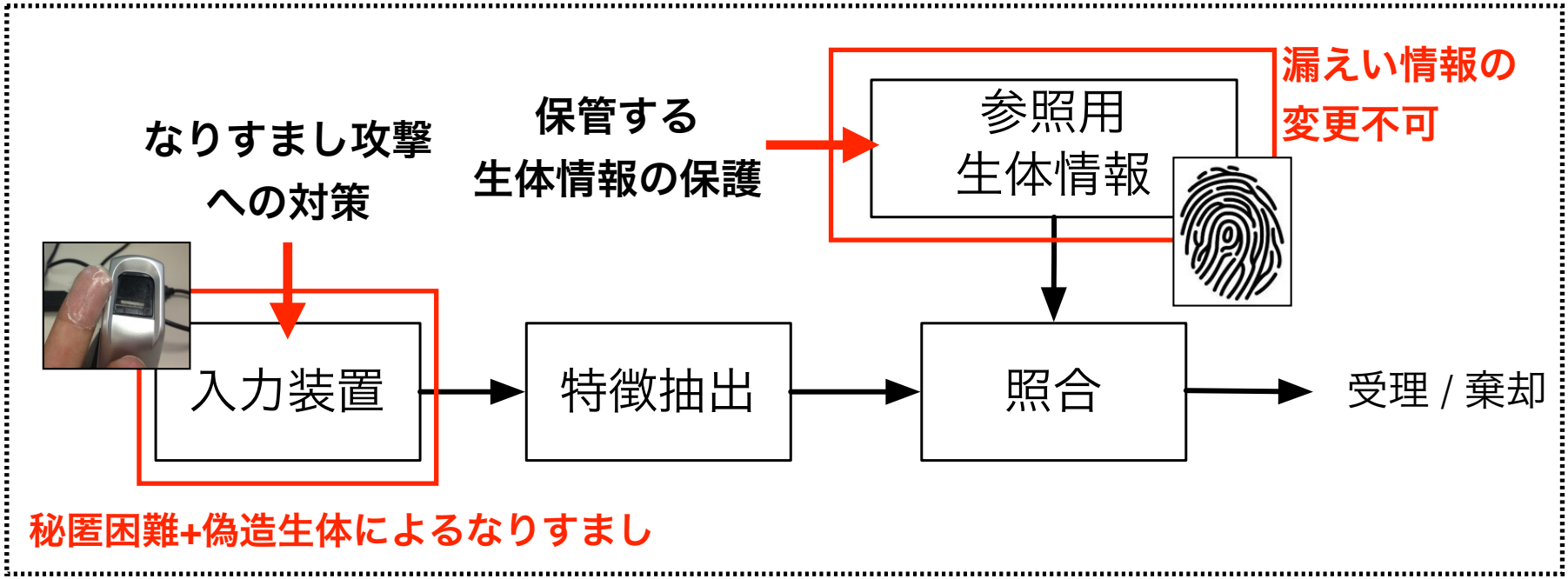
認証手段の比較

評価項目	パスワード	トークン	生体認証
識別能力	高 ・パスワード空間大 → 高いエントロピー	極めて高 ・任意の鍵長	中～高 ・モダリティに依存 ・エントロピーはFARで制限
運用強度 (ヒューマンエラー)	弱 ・短いパスワード ・推定容易なパスワード ・メモ書き ・漏えい・推定 ・ソーシャルエンジニアリング	弱 ・紛失 ・盗難 ・いつ紛失、盗難したかはわかる	強 ・本人の意識に影響しない ・管理の依存度が低い **生体認証の利点**
システム強度	強 ・長い文字列=高いエントロピー ・暗号化の適用 ・技術的強度の向上 →運用強度の低下	極めて強 ・コピー困難 ・改ざん困難 ・攻撃には高度な専門知識と技術が必要	中 ・なりすまし ・テンプレートの解析 ・登録データの不正な取得 **生体認証の課題**

誤りのタイプ(現実的な場合)



生体認証の脅威と脆弱性



生体認証システムの多くの脆弱性は既存のセキュリティ技術の組み合わせで対応可能

生体特有の性質に起因する脆弱性が課題

(1)**秘匿困難**：日常生活で利用する生体情報を他者に秘匿することは難しい(コップの指紋、声など)

(2)**変更困難**：漏えいしても、生体情報自体を変更することが難しい(外科手術等が必要)。

- **偽造生体によるなりすまし攻撃への対策が必要**
- **保管する生体情報の保護が必要**

テンプレート保護型生体認証

テンプレート保護の必要性

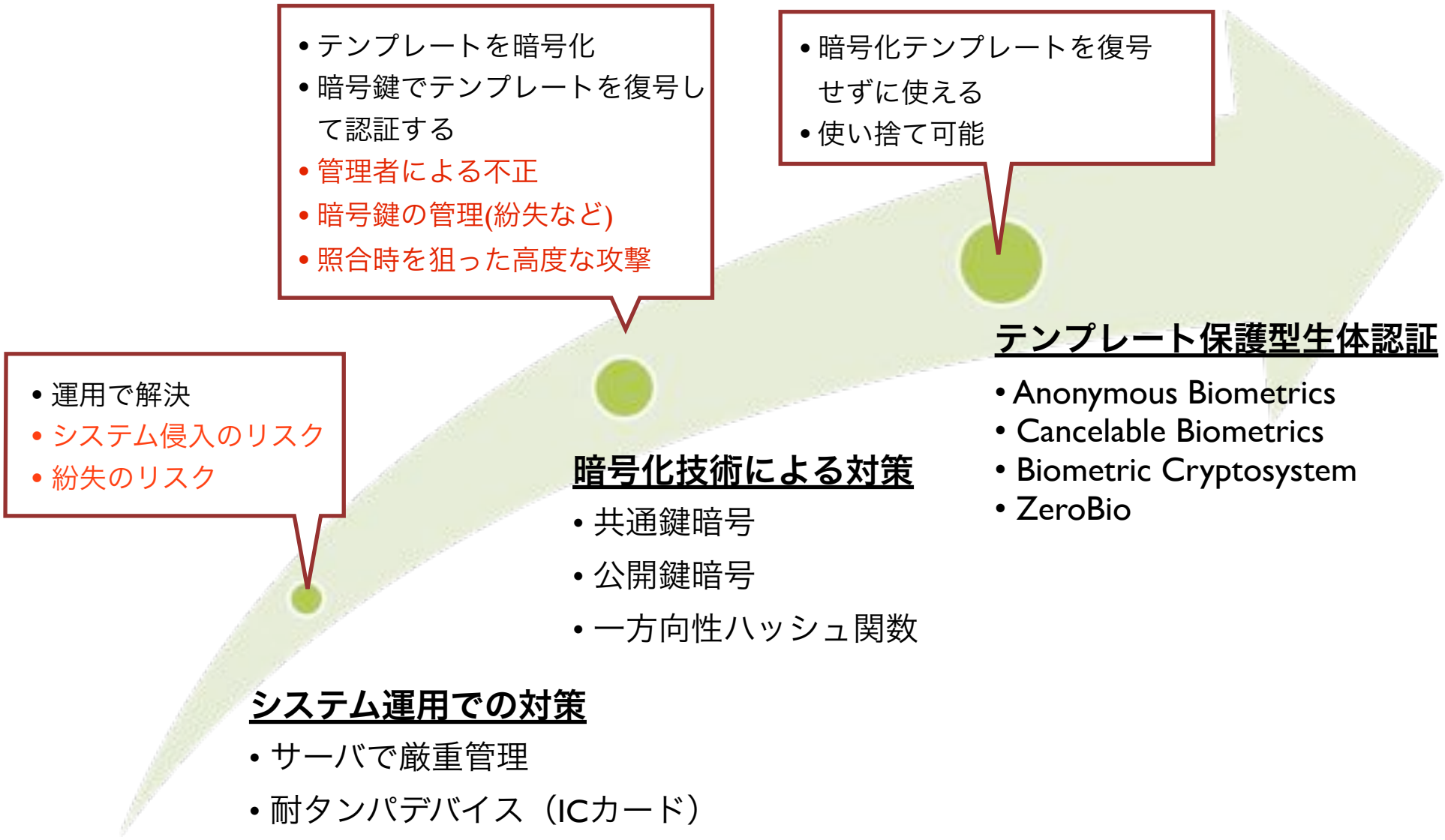
- **エンドユーザの生体情報管理能力**

ハイエンドの利用形態では生体情報は高いセキュリティレベルで管理される。 エンドユーザは実行可能か?

- **管理すべき生体情報**

ローエンドの利用形態においてもハイエンド利用と同じ生体情報が使用される。

テンプレート保護の歴史



テンプレート保護型生体認証

生体情報をサーバに保管したまま認証

- 利用者のプライバシーを保護
- サーバ管理者の不正防止

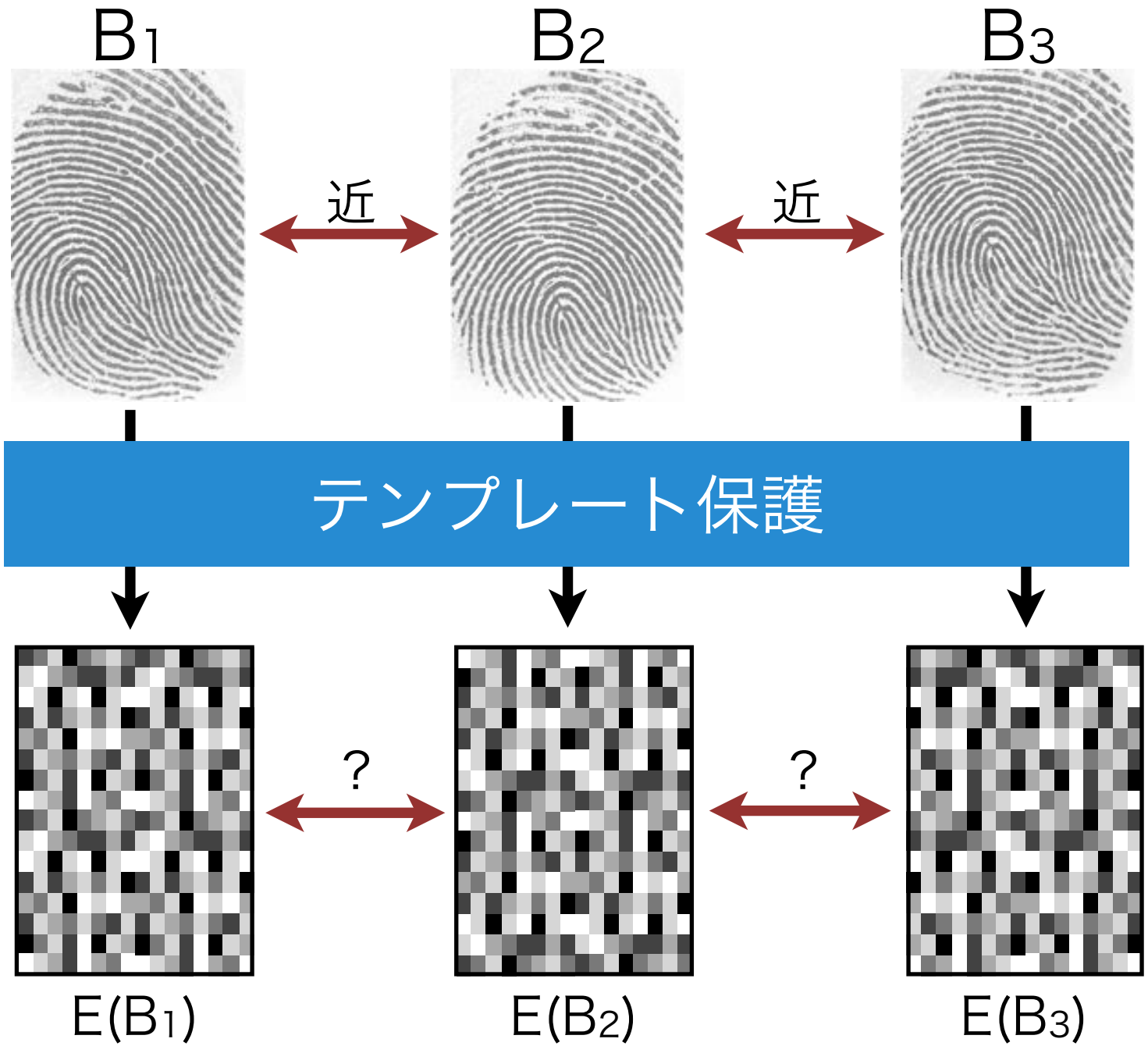
生体情報の安全性をアルゴリズムレベルで保証

- Store on Card: 安全性をハードウェア(TPM)に依存
- Store on Server(+Card): 安全性をサーバ管理者・運用方法に依存

既存研究は大きく3つに分類される

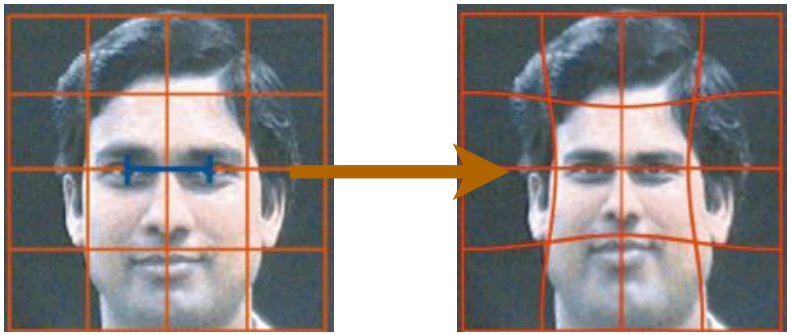
- Cancelable Biometrics(キャンセラブルバイオメトリクス)
- Biometric Cryptosystem(バイオメリック暗号)
- ZeroBIO(非対称生体認証)

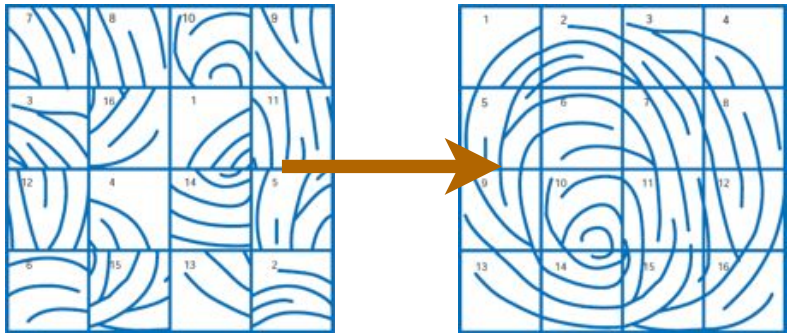
誤差のある入力を如何に考慮するか？

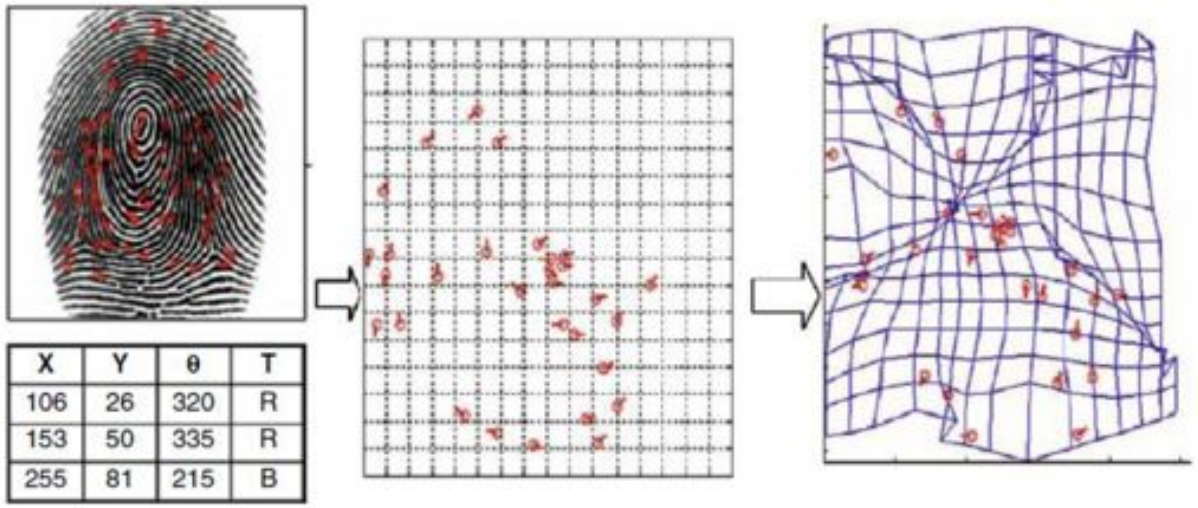


解決策1：相関を残す変換関数を定義

変換パラメータに基づく非可逆な関数を定義(Ratha, 2001)

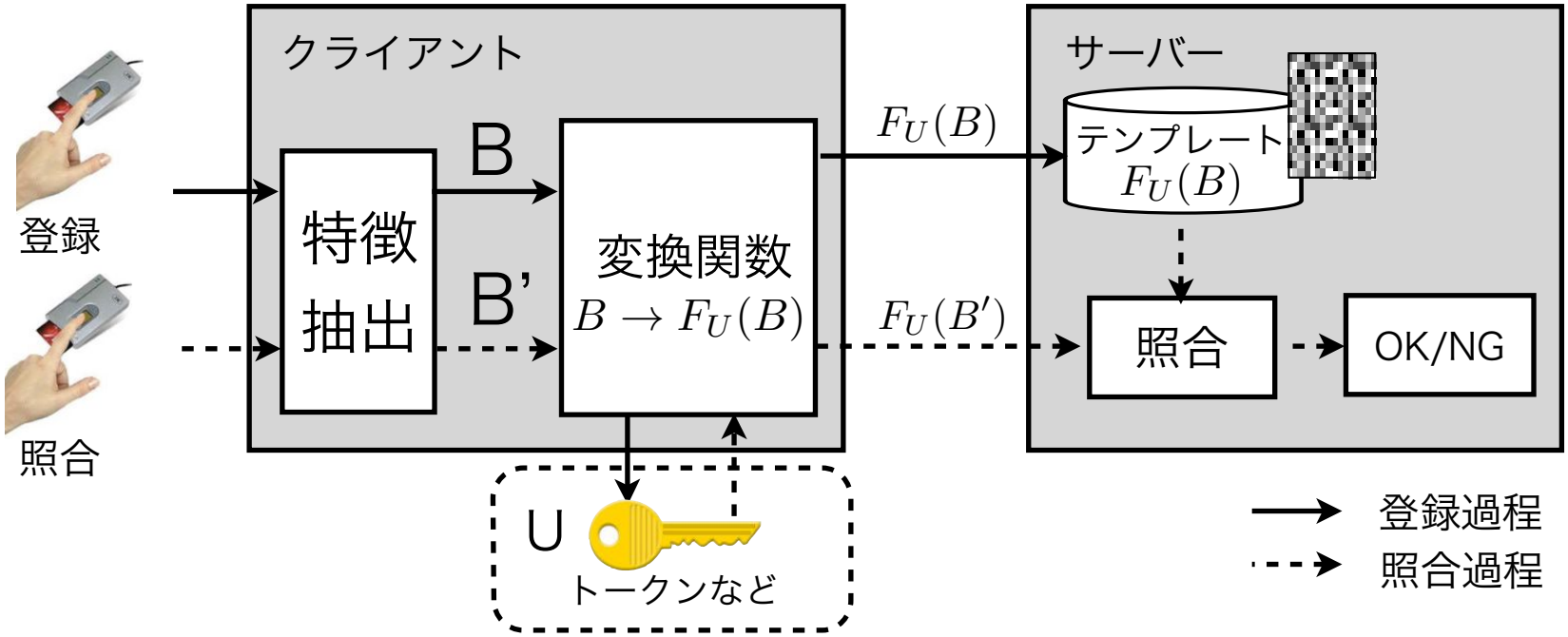






X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

Cancelable Biometrics

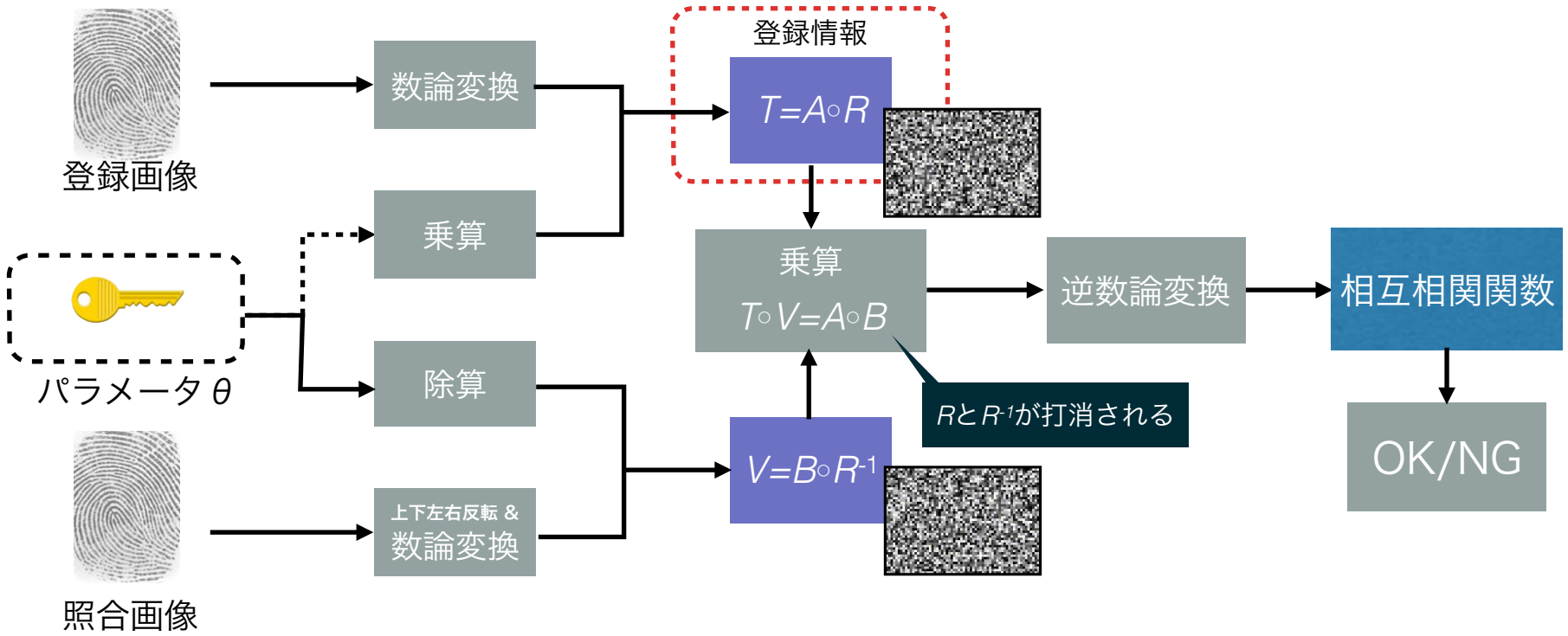


- 変換パラメータUが暗号鍵に相当
- 登録生体情報を $B \to PT = F_U(B)$ と変換してサーバに保管
- 登録生体情報を $B' \to F_U(B')$ と変換し、PTと照合(元に戻さない)

従来手法と比較して精度を保ったまま実現可能な方式が知られる

>> ただし、暗号鍵Uの管理が課題

画像マッチングに対するキャンセラブル方式

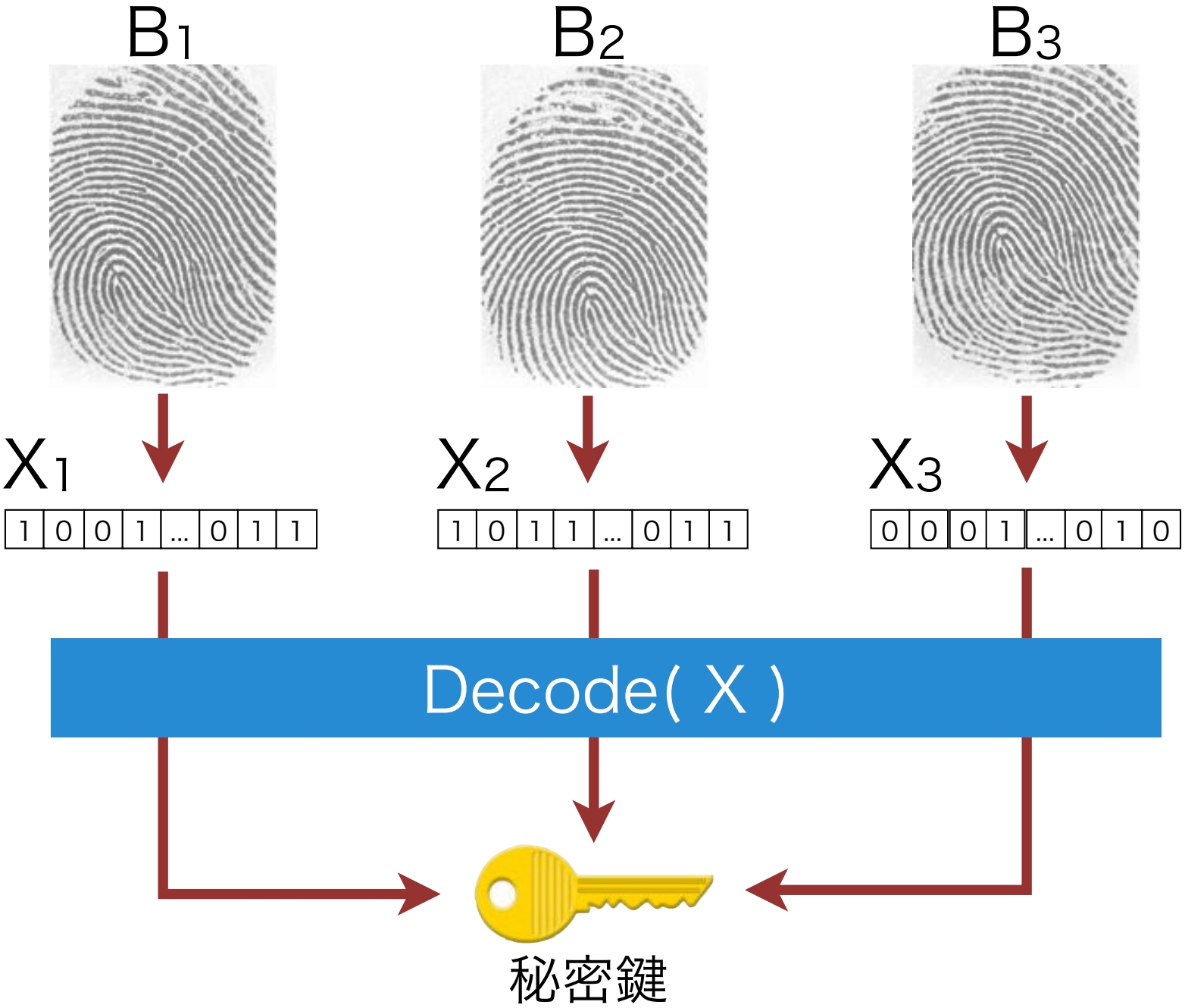


・パラメータ θ はランダム画像、任意に設定可能→再生成可能(Cancelable)
・数論変換後の画像にパラメータ θ に基づくランダム画像Rをフィルタリングする
・照合時にはランダム画像R^{-1}をフィルタリングする
・RとR^{-1}は乗算時にキャンセルされるため、登録画像と照合画像の相関が計算可能
・ネットワークを流れるデータは全てランダム画像となる

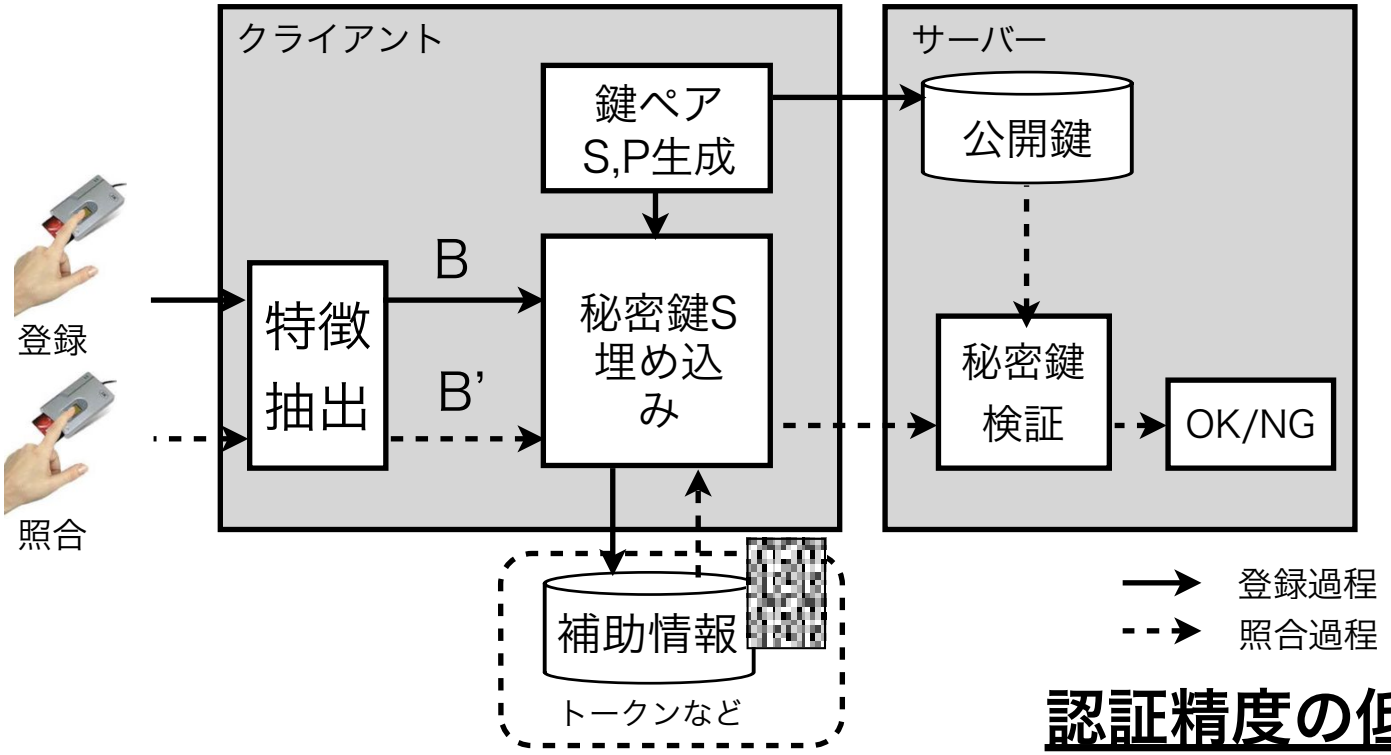
NTT=数論変換(Number Theoretic Transform)：
整数の剰余環上でのフーリエ変換
例えばGF(256)上での数論変換であれば、255を超えた値は0に戻る

参考) 日立製作所 高橋氏 提供資料より

解決策2：符号化→誤り訂正による鍵生成



Biometric Cryptosystem



認証精度の低下が課題

登録

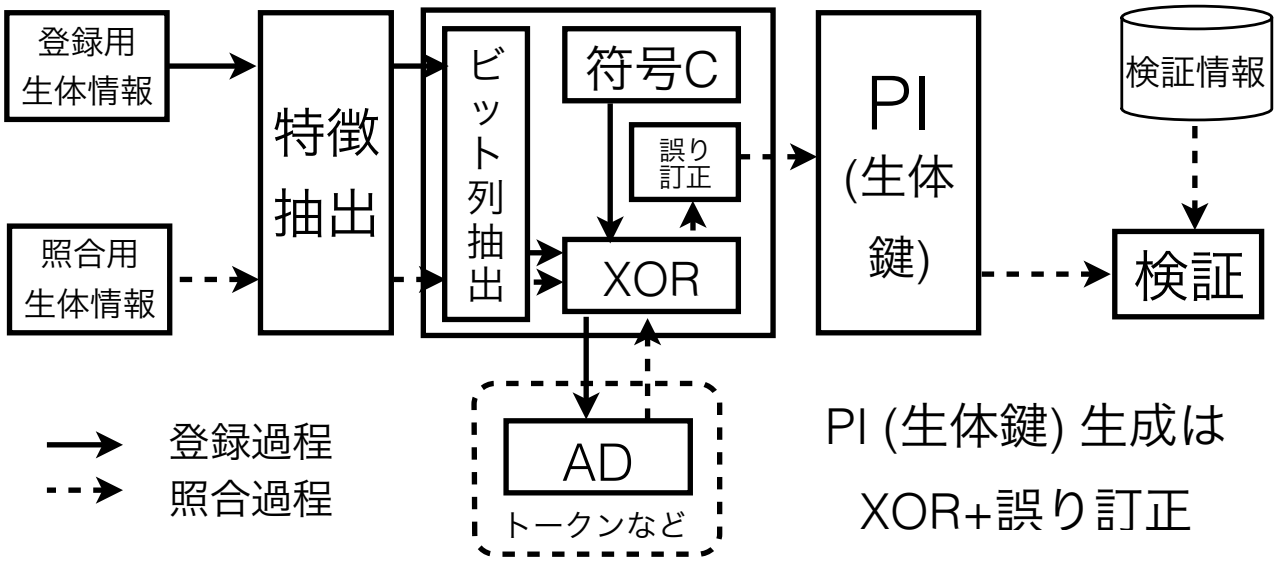
- 公開鍵Pと秘密鍵Sのペアを生成し、生体情報Bに秘密鍵Sを埋め込んで補助情報Hとして作成．公開鍵Pをサーバーに保管し，補助情報Hをトークンなどに保管し，ユーザに発行.

照合

- 利用者の生体情報B'を用いて補助情報Hから秘密鍵Sを復元する
  - BとB'が近い時のみSが復元可能(一般に誤り訂正が用いられる)
- Sが正しい秘密鍵であることをサーバの公開鍵Pを用いて検証

PKIやその他の暗号プロトコルとの親和性が高いが、認証精度の低下が課題

Fuzzy Commitment Scheme



生体特徴B, B'の変動を誤り訂正符号を用いて許容することで秘密鍵を生成するアルゴリズム。B, B'の距離はハミング距離で与えられる必要がある。

登録

$$S = Encode(C_i)$$
$$AD = B \oplus S$$

ただし、C_iはBと同じビット長を持つ
誤り訂正符号Cからランダムに選択された符号語

照合

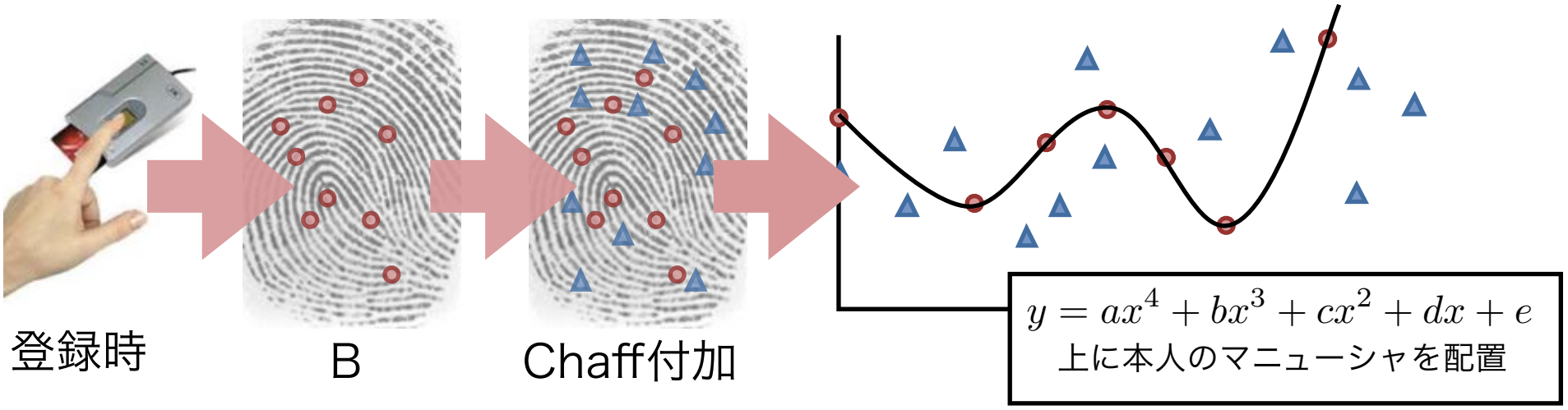
$$S' = Decode(AD \oplus B') = Decode(S \oplus B \oplus B')$$

BとB'のハミング重みが小さい(BとB'が近い)ならば
正しく誤り訂正され、S'=Sとなる

Fuzzy Vault Scheme

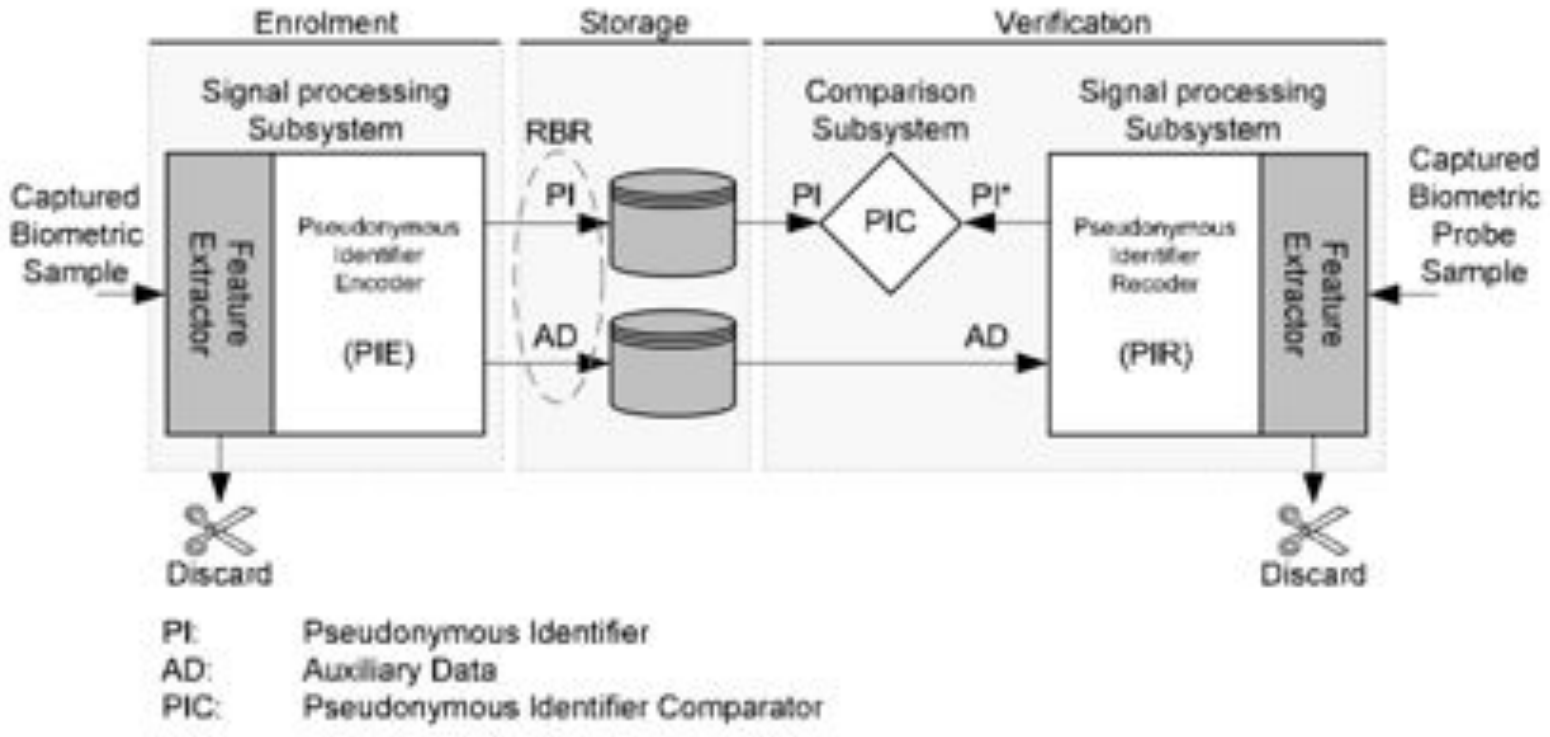
A.Juels, et.al. (RSA), “A fuzzy vault scheme”, 2002

生体情報B,B’の近さが set difference (共通の要素数)で与えられる場合に,
誤り訂正理論を用いて生体情報Bに秘密の鍵Sを埋込/復元することを可能とする.



ISO/IEC 24745: Biometric Information Protection

テンプレート保護型生体認証の一般的な構成法を定義



AD: Auxiliary Data, Cancelable Biometrics におけるパラメータや，バイオメトリック暗号における補助データ

PI：Pseudo Identifier．Cancelable Biometrics におけるパラメータやバイオメトリック暗号における生成鍵(生体鍵)

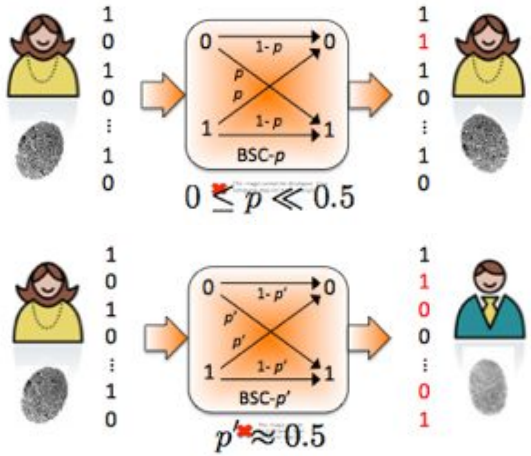
※ Cancelable Biometrics におけるパラメータはユースケースによりAD, PI, どちらとも解釈可能

ISO/IEC 30136: Performance Testing of Biometric Template Protection Schemes

テンプレート保護型生体認証の評価指標について定義

- How often does the system falsely reject a genuine user?
- How often does the system falsely accept somebody else?
- Is the stored template **irreversible**, i.e., how difficult is it for an attacker to recover the biometric from the template?
- How much storage do the templates require?
- Can an attacker combine two or more templates to gain an advantage (**unlinkability**)?
- How many templates can one extract from a given biometric (**diversity**)?

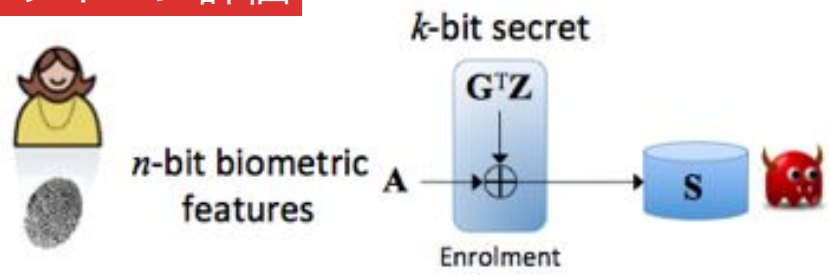
バイオメトリック暗号の誤りモデル



本人はビット反転確率に偏りあり

他人はビット反転確率がほぼ1/2

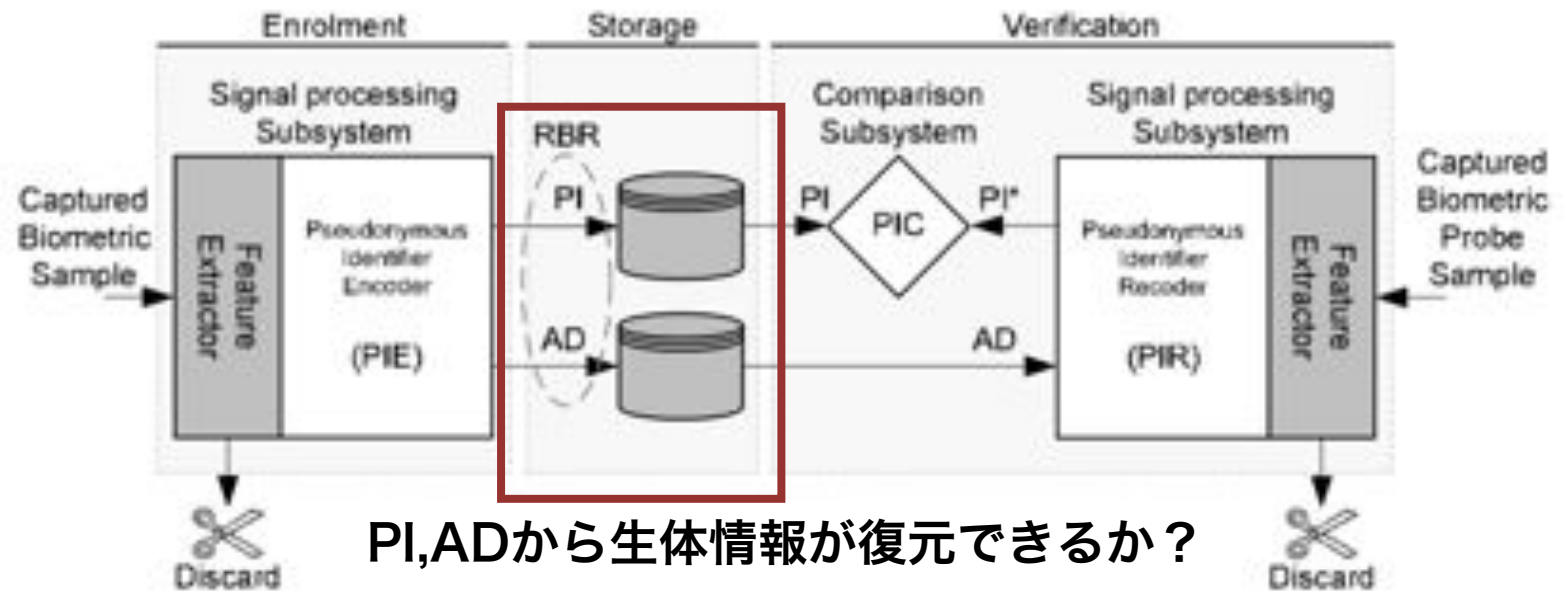
プライバシ評価



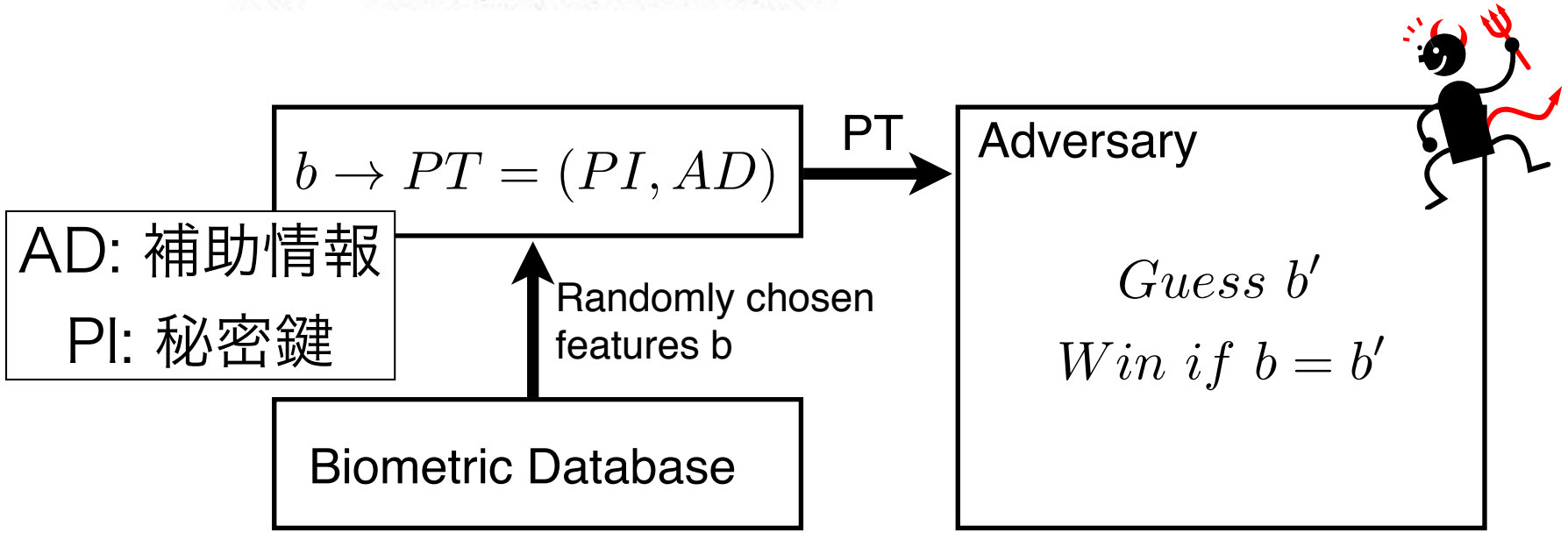
- 取り得る生体情報の総数は2^n個
- 出力可能な鍵の総数は2^k個(n > k)だった場合
  →n - kビットの情報が漏れていると考えられる

参考) Shantanu Rane, “Performance Testing of Biometric Template Protection Schemes ISO/IEC 30136”

Irreversibility



PI,ADから生体情報が復元できるか？



Irreversibility 評価の一例

(1) BDA(Biometric Dictionary Attack):
生体情報の分布を知っている攻撃者が、分布に従った生体情報を用いて攻撃を行う

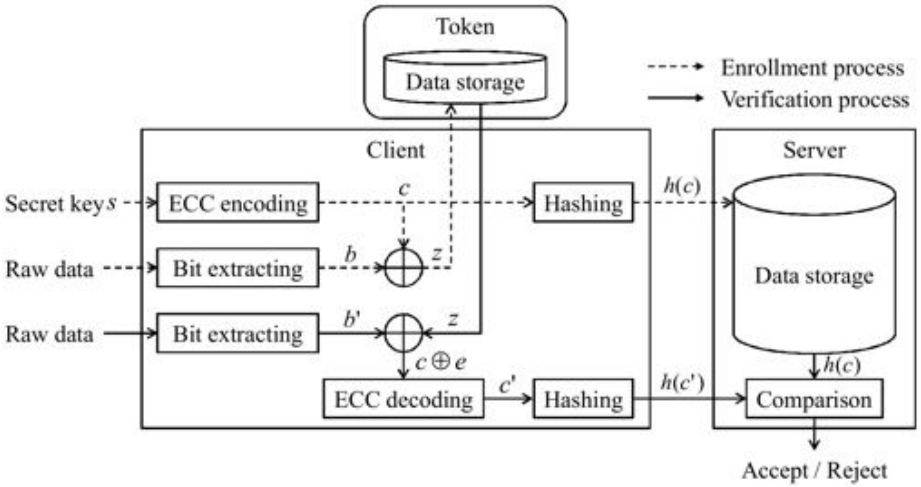
(2) ECSA(Exhaustive Codeword Search Attack):
漏えいした保護テンプレートから得られる部分情報(符号)のみを用いて攻撃を行う

(3) Decoded Biometric Dictionary Attack(DBDA):
(1)(2)を組み合わせ、漏えいした保護テンプレートから得られる部分情報のうち、生体情報の分布に従うもののみを用いて攻撃を行う

$$P_{BDA} = \frac{|\overline{\mathcal{B}}_t(b)|}{|\overline{\mathcal{B}}|}$$

$$P_{ECSA} = \frac{1}{2^n \cdot P(x \in \mathcal{C})} = \frac{1}{|\mathcal{C}|}$$

$$P_{DBDA} \approx FAR \cdot \frac{|\overline{\mathcal{B}}|}{|\overline{\mathcal{B}}_t(b)| \cdot 2^{\hat{k}}} \approx (P_{ECSA})^{\frac{\hat{k}}{k}}$$



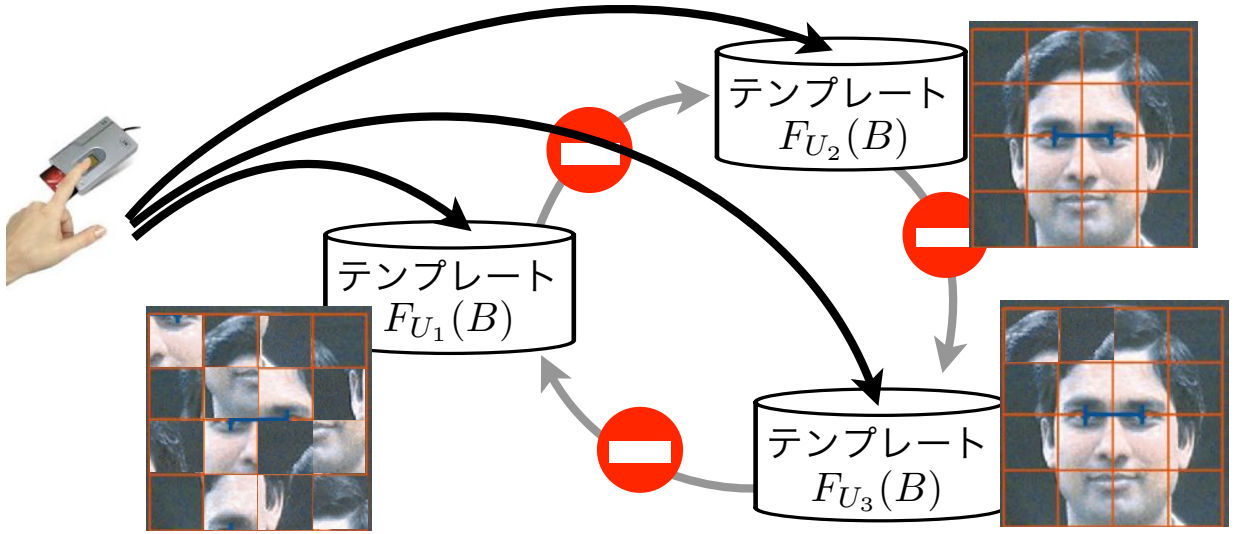
Fuzzy Commitment Schemeに対する安全性評価例

	攻撃成功確率
(1)BDA	0.1%
(2)ECSA(従来)	0.3%
(3)DBDA(提案)	20.7%

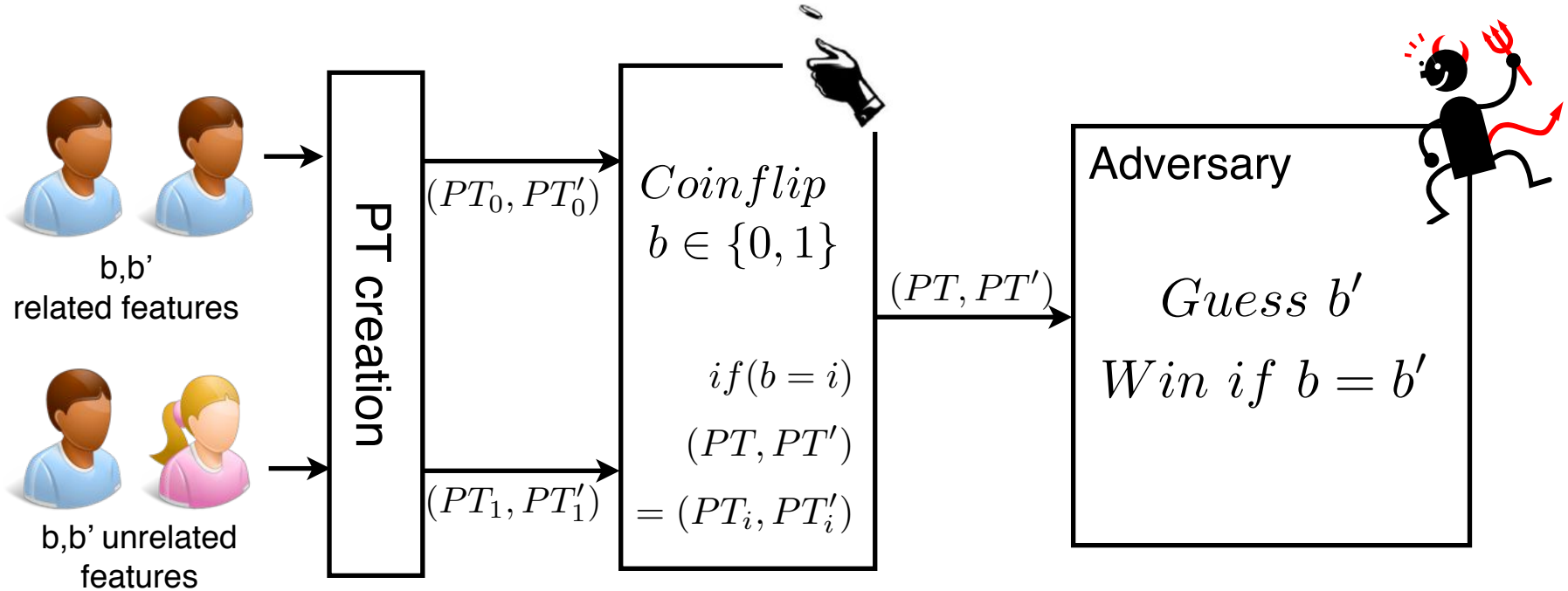
提案手法ではより正確な安全性評価が可能

「Fuzzy Commitment Schemeを用いたバイオメトリック暗号における保護テンプレートの安全性評価」,披田野清良, 大木哲史, 高橋健太, 情報処理学会論文誌, 2013年11月.

Unlinkability



単一の生体情報から生成した「**複数の保護テンプレートの独立性**」



研究・製品化・標準化の動向

- 研究動向

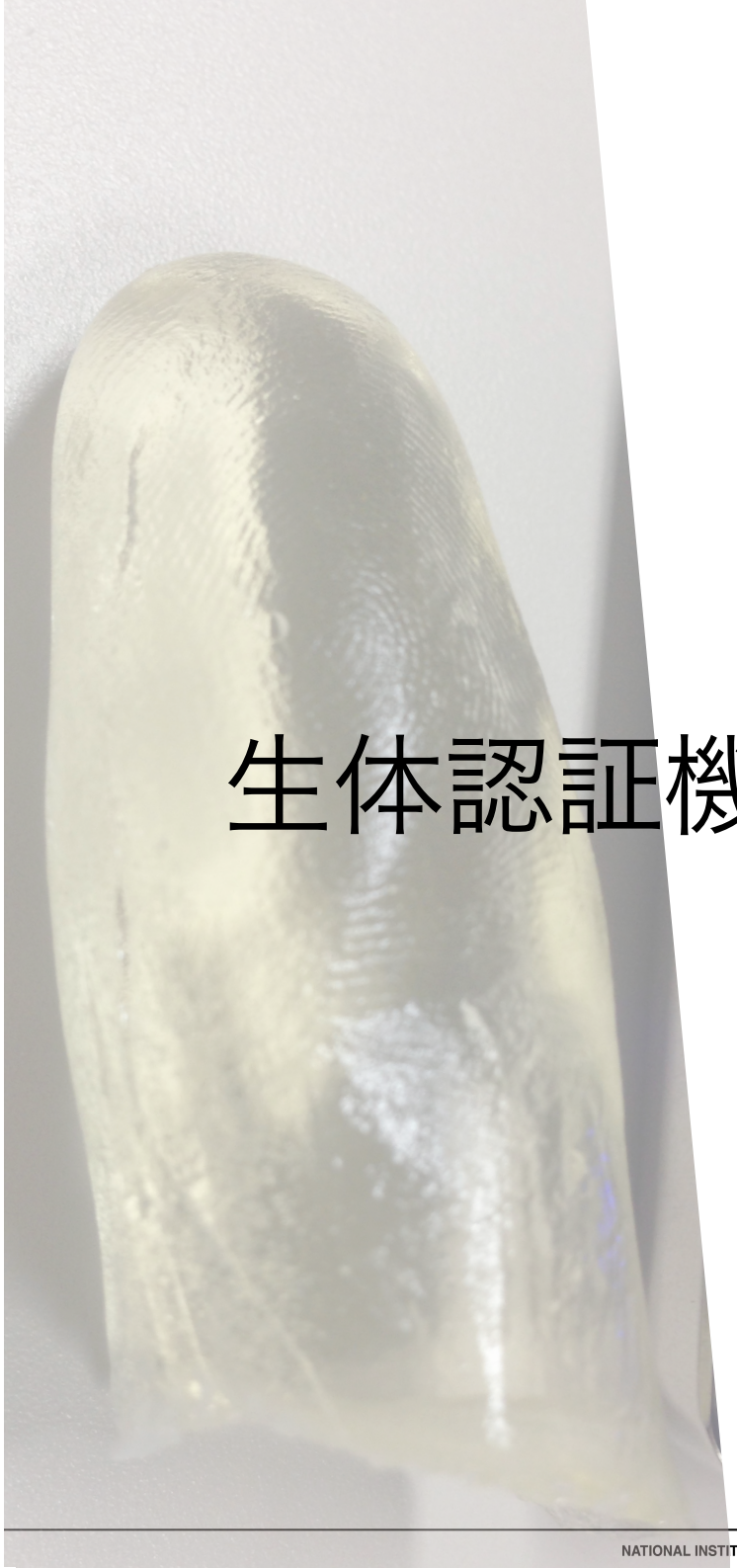
- ここ10年で企業や大学等の研究機関で研究開発が活発化
- 欧州ではFP7においてテンプレート保護技術の研究開発を目的としたTURBINEプロジェクトが実施(2008～2011)→同FP7においてBEATプロジェクトに引継. 脆弱性評価ツールの作成やCC認証のための標準文書作成などのフェーズ

- 製品化動向

- 実用化フェーズのものもいくつか存在
- 日立：クラウド型指静脈認証サービスでキャンセラブルバイオメトリクスを採用
- オランダ GenKey(PrivID)：指紋認証にバイオメトリック暗号を適用した製品を展開

- 標準化動向

- ISO/IEC 24745 Biometric Information Protection(アルゴリズムの構成法)
- ITU-T Recommendation X.1091: A guideline for evaluating telebiometric template protection techniques(保護性能評価の手順)
- ISO/IEC 30136 WD3 Performance testing of template protection schemes(保護性能評価指標)



生体認証機器へのなりすまし対策

なりすまし攻撃の事例(1)

Million Dollar Border Security Machines Fooled with Ten Cent Tape

So much for biometrics and immigr
security: A South Korean woman
managed to fool a million-dollar
fingerprint reading machine in Jap
border controls using a simple piec
tape stuck to her fingers.

It happened at Tokyo airport. The
woman has repeatedly entered Jap
using the same trick without anybo
noticing. Japanese officials say that they suspect many others have been doing the
things, demonstrating that the biometric systems they installed in 30 airports in 20
the tune of $45 million-are completely useless. The woman was deported in July 2
for illegally staying in Japan as a bar hostess in Nagano, but she entered again wit

2009年1月、テープで指紋を変えることで日本への入国審査を通過したとして外国人女性2名が逮捕された。

http://gizmodo.com/5122259/million-dollar-border-security-machines-fooled-with-ten-cent-tape

なりすまし攻撃の事例(2)

Doctor caught red-fingered, buddy-punching absent co-workers in Brazilian hospital

By Adam Vrankulj

Like 0 Tweet 4

March 13, 2013 - A Brazilian doctor has been charged with fraud, after being caught using silicone fingers to clock absent co-workers in, spoofing the biometric workforce management solution installed at a hospital outside of Sao Paulo.

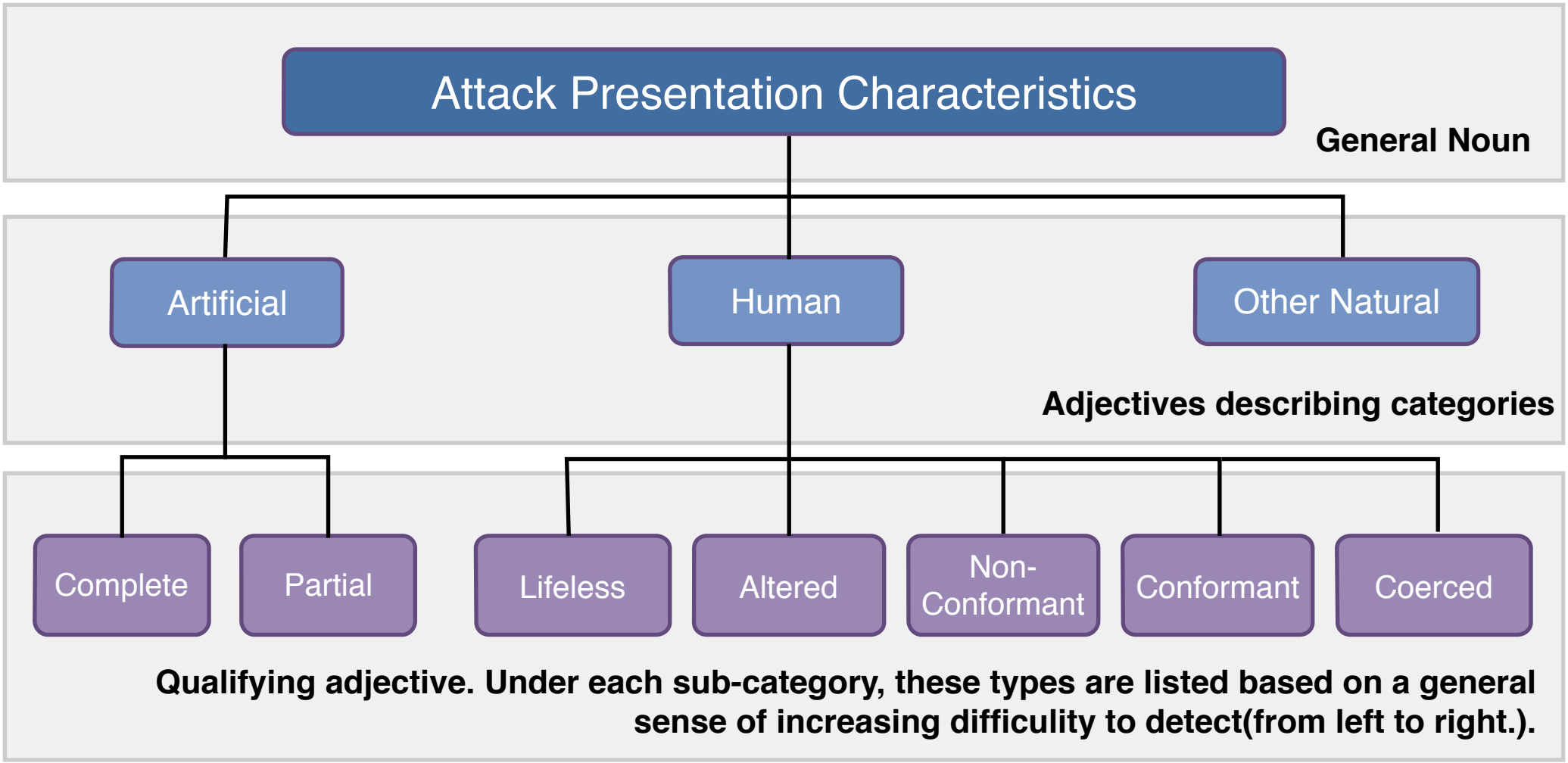
Making headlines around the world this morning, the doctor, 29-year-old Thaune Nunes Ferreira has been arrested, and according to a report in Folha De S Paulo, Ferreira told police she had been using the silicon fingers as she had been coerced by her employer to do so, as she faced losing her job.

Following suspicion that some sort of fraud had been occurring, cameras were installed near the biometric time clock and eventually caught the doctor red-handed.

http://www.biometricupdate.com/201303/doctor-caught-red-fingered-buddy-punching-absent-co-workers-in-brazilian-hospital

2013年3月、ブラジル・サンパウロの病院に勤務する医師が、シリコンで偽造した指を使うことで指紋認証をすり抜け、30人以上の同僚の勤務を偽造していることがわかった。

Presentation Attack の分類(in ISO 30107-3 WD1)



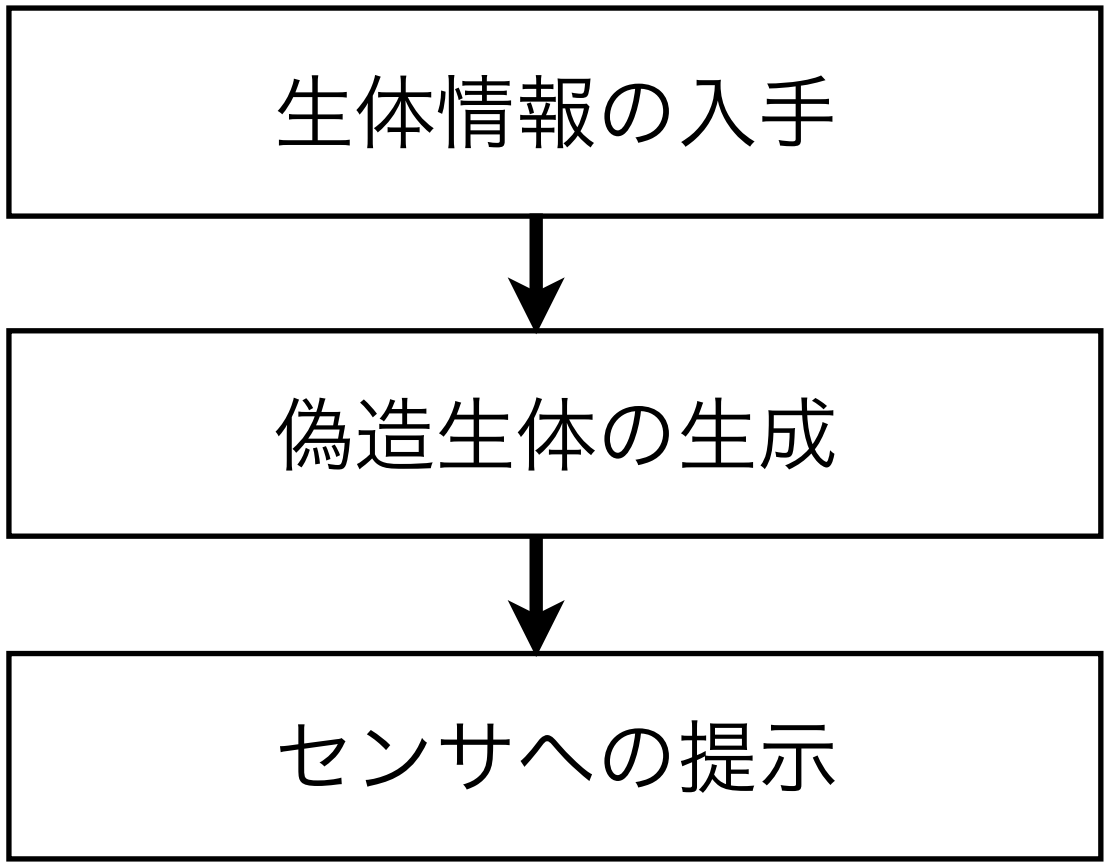
Presentation Attack の分類(in ISO 30107-3 WD1)

大分類	小分類	例
Artificial	Complete	グミ指，動画撮影された顔
	Partial	接着剤をつけた指，サングラス，パターンが印刷されたコンタクトレンズ
Human	Lifeless	死体の一部，切断された指や手
	Altered	手術によって入れ替えられたり切除された指紋
	Non-Conformant	顔の表情や指の側面といった極端な変化を含む入力
	Coerced	無意識や強制された入力
	Conformant	詐称者によるゼロエフォートの攻撃

生体特徴の入手 (in ISO 30107-3 WD1)

タイプ	内容	例
Cooperative	生体特徴を生体から直接取得して入手	型取りした指や手，顔のマスク
Latent	(遺留物から)生体特徴を間接的に取得して入手	遺留指紋，遺留手形，髪，肌，体液
Recording	何らかのメディアを用いて直接取得して入手	写真，録画ビデオ，録音音声
Template Regeneration	テンプレートから生体特徴を復元して入手	再生指紋，顔
Imporsonation	人為的な補助を受けて自分の生体特徴を他人の生体特徴に変換して入手	コンピュータアシスト音声変換
Synthetic Samples Generation	偽の生体特徴を合成して入手。作成した情報は生体特徴に似ていても似ていないくてもよい	指紋合成，虹彩合成，音声合成，ウルフ合成サンプル，三次元顔

Presentation Attack の手順



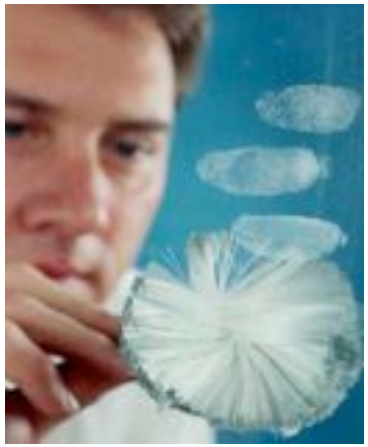
生体特徴の入手(1)

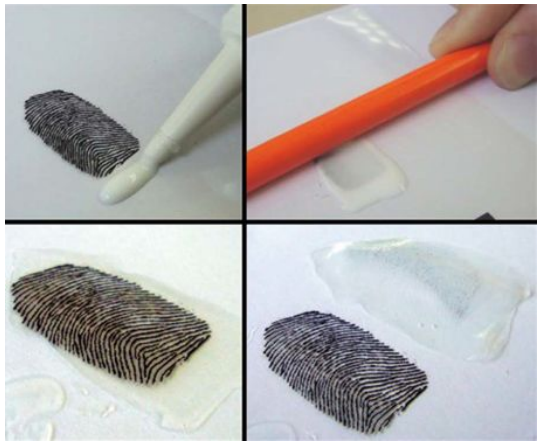
協力的なりすまし(cooperative)

攻撃者は攻撃対象者の生体サンプルを直接入手し、そこから偽造物を作成することができる。

Ref) http://prag.diee.unica.it/fldc-tset/LivDet_2013_slides.pdf

Latent





遺留物(**Latent**)から偽造物の元となる生体特徴を入手することができる。

生体情報の入手(2)

Template Regeneration

テンプレートから生体特徴を復元して入手する

Adler, et al, Biometric Conference, 2003

左上の画像から右下の画像(テンプレート)を推定する実験。照合スコアのみを用いて山登り探索で推定を行っている。

補足) 山登り探索

元画像Xに対し微小な変更を加えた画像Yを作成して照合を行う。Yでの照合スコアが元画像Xでの照合スコアを僅かでも上回ればYを新しいXとする。同様にして画像を更新していくことで照合スコアの高い生体を推定する探索手法(左図は元画像に対し0,200,500,3200回変更を加えた際の画像)

入手した生体情報を利用した偽造生体の作成

生体の模倣（造形）	Cast(two step mold/cast process)	1.型取り(Molding)- 生体特徴の三次元表現	人間からキャプチャされた顔型、医療用素材で作られた指の型、プリント基盤に印刷された指紋など
		2.成型(Casting) - 型からの再生成	演劇用マスク、粘土やゼラチン、シリコンなどの素材で作った偽造指など
	Direct Rendering	二次元プリント	虹彩や顔、指紋、静脈パターンなどを透過性のある紙にプリントしたもの
		三次元プリント	模様が印刷されたコンタクトレンズ、静脈の模様が印刷された人工の手ものなど
		エッチング	金属に指紋をエッチング加工したもの
		ペインティング - 人工器官に描かれた模様や色	人工の目に虹彩の模様を描かれたものや，人工の手に静脈の模様を描いたもの
	Mask	生体特徴の偽造物による変更や秘匿	指に接着剤をつけたもの、化粧、取り外し可能な移植組織、不透明レンズ、スキーのマスクなど
生体の模倣（動画／音声）	Computing device	ラップトップやタブレットに表示された画像やビデオ	顔・虹彩の画像や動画
	Time series player	時間軸で記録された情報	音声の録音，デジタルタブレットを用いた署名の登録，脳波の登録など
生体情報の人工合成		合成生体特徴の作成	指紋，顔，音声の合成，ウルフ合成サンプルや三次元顔の彫像など

Static physical reproduction (1)

Cast の例

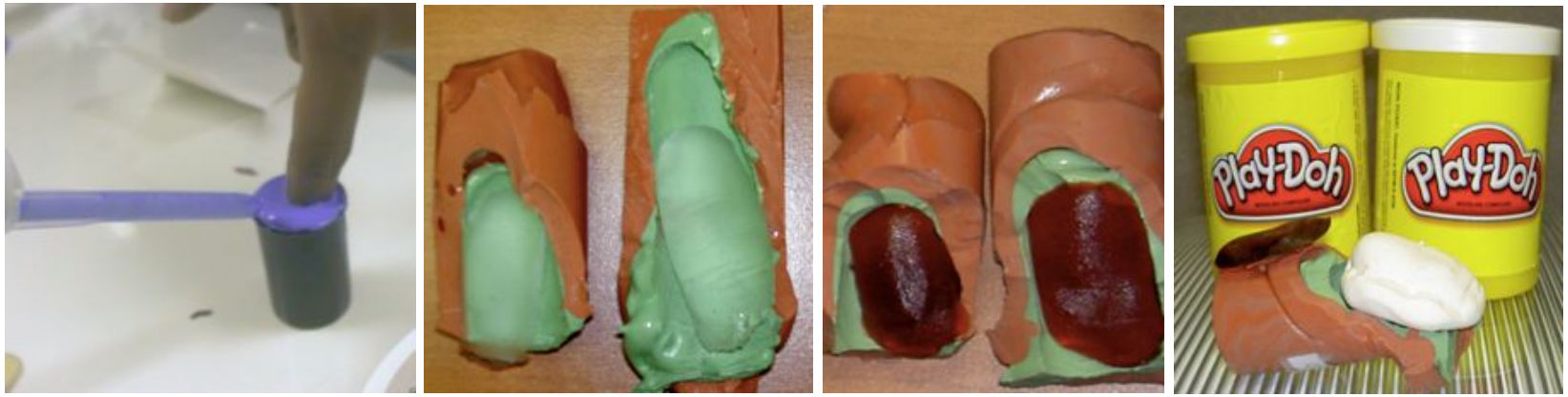
型取り(Molding)と成形(Casting)の2つのプロセスから構成される

1. 型取り

入手した生体特徴を元に型を作成する

2. 成型

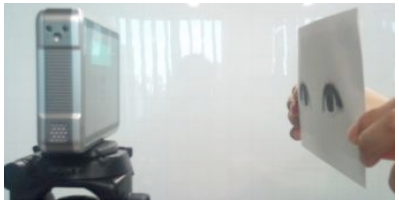
型にシリコンやゼラチンを流し込んで偽造指を作成



Static physical reproduction (2)

Direct Rendering

二次元プリント



三次元プリント

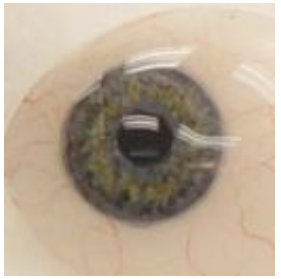
Nesli, et al, IEEE International Conference of the Biometrics Special Interest Group(BIOSIG), 2013.

エッチング

左図：プリント基板に対して指紋画像をエッチング処理したもの

http://www.atmarkit.co.jp/fsecurity/column/ueno/48.html

ペインティング



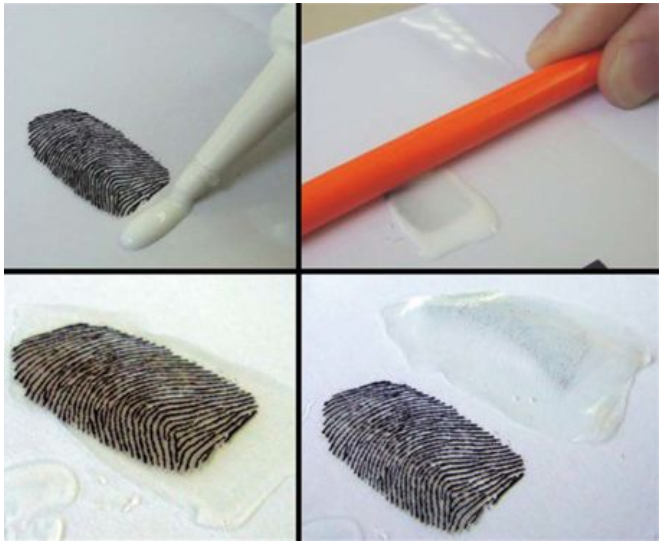
左図：義眼に対し半透過レイヤを30枚重ねて虹彩模様を作成したもの

Lefohn, et al, IEEE Computer Graphics & Applications article, 2003.

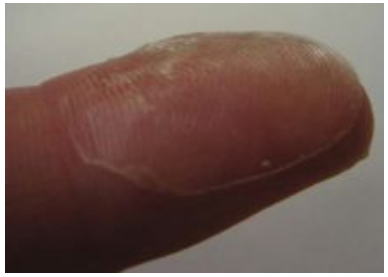
Static physical reproduction (3)

Mask

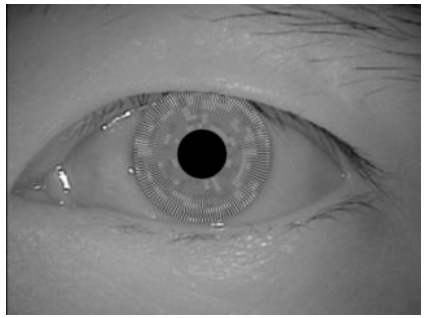
生体特徴の偽造物による変更や秘匿



例) 木工用ボンドによる
偽造指紋の作成



Source) Chaos Computer Club



Nesli, et al, IEEE International Conference of the Biometrics Special Interest Group(BIOSIG), 2013.

Liveness Detectionの分類
(1) 生体の固有特徴

生体のみが持つ固有の特徴を用いて偽造物を判定する方式

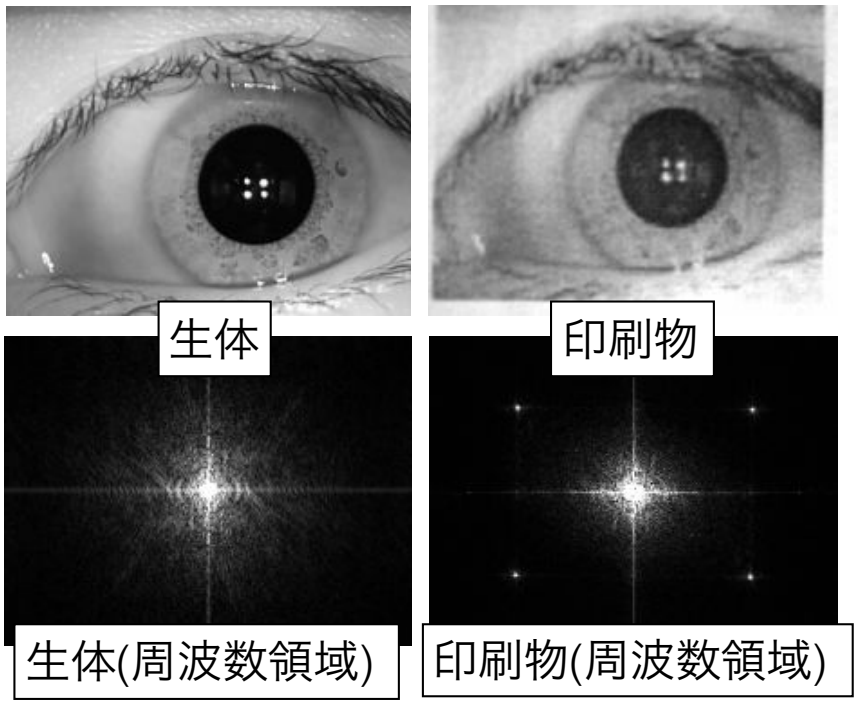
例)　- 汗腺が存在するか

- 皮膚の電気抵抗

- 隆線構造

- 光の反射や吸収

周波数領域による印刷物判定



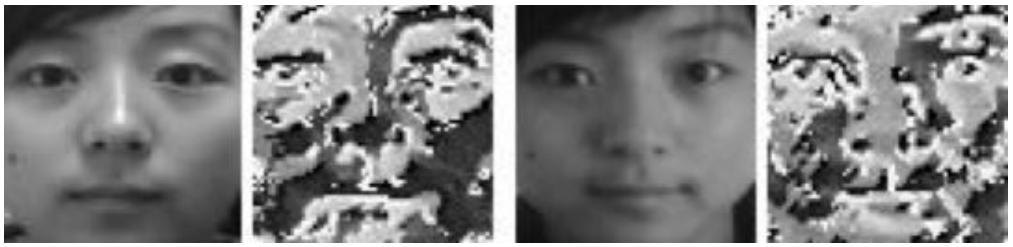
X. He, et. al, Advances in Biometrics, 2009.

PAD方式例： 顔認証におけるPAD

テクスチャベース

対象の外観を測定して検知に利用

Maatta, et.al, IJCB2011.

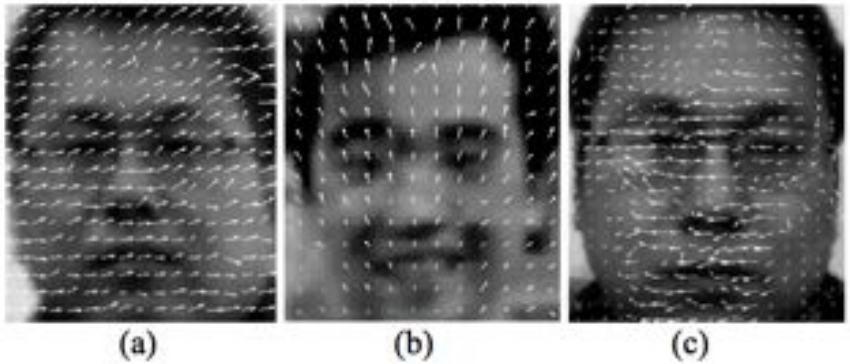


図：LBP画像空間における生体と印刷物の違い
左(生体)と右(印刷物)の顔画像は非常に似通っているが、LBP画像空間においては違いが顕著となる

モーションベース

対象の動きを測定して検知に利用

Bao, et.al, IASP2009.

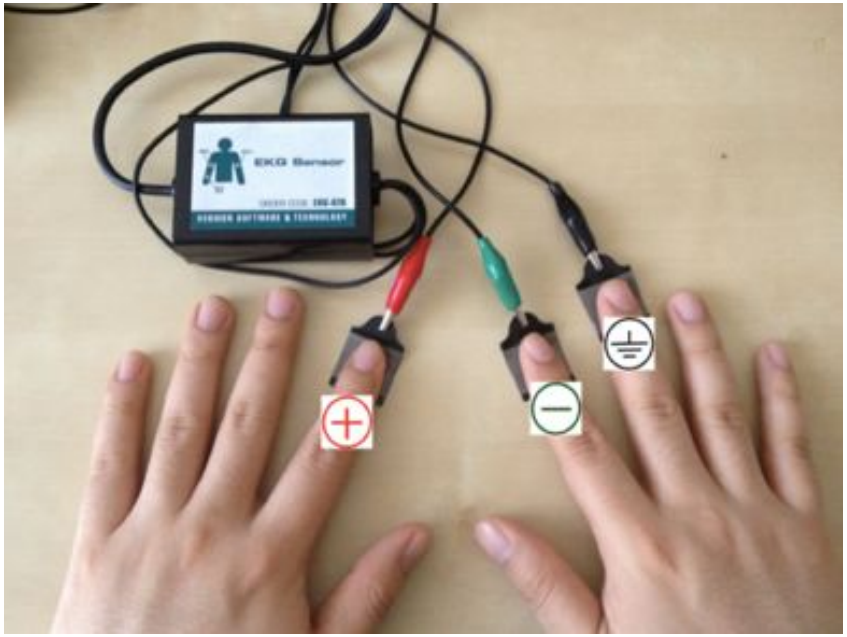


図：オプティカルフローによる動きの違いの可視化
(a)印刷物を手で持って提示したもの、(b)は同じものを固定して提示したもの、(c)は実際に生体を提示したもの。他2つと比較して複雑な動きをしていることがわかる

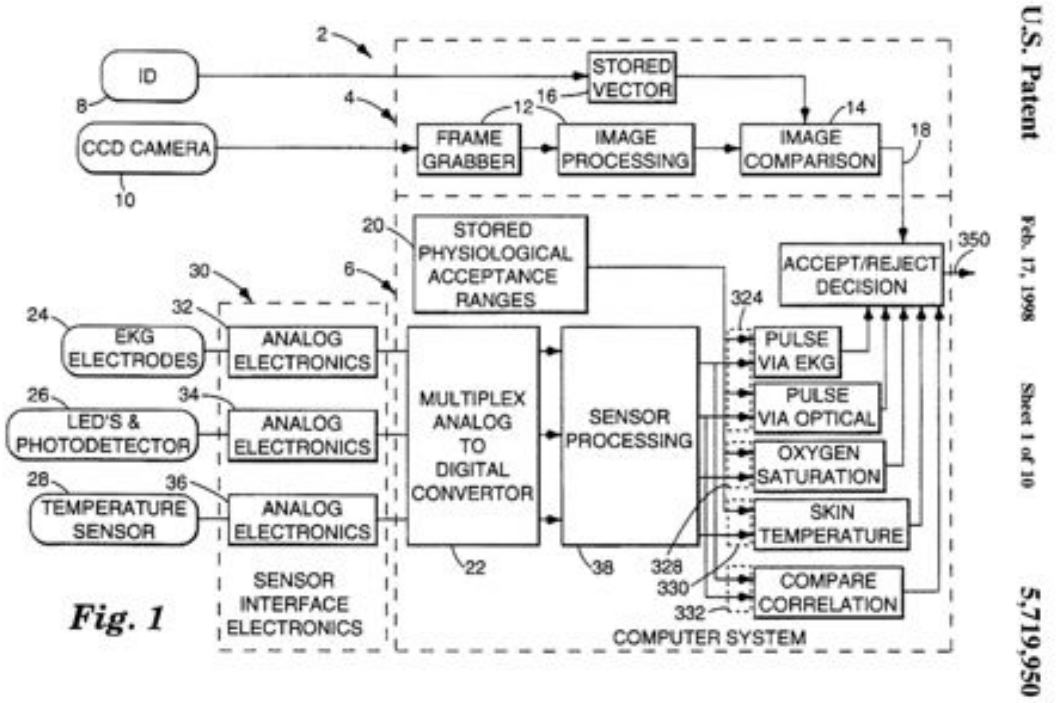
両者を組み合わせる(統合)することで更に高精度な検知も可能

Liveness Detectionの分類
(2) 生体の無意識動作

血圧，血流，脳波，心電図波形，照明の変化によらない瞳孔の収縮など



図：ECGと指紋リーダーの組み合わせ



図： 脈拍・心電図・対応の組み合わせによる検知(US Patent)

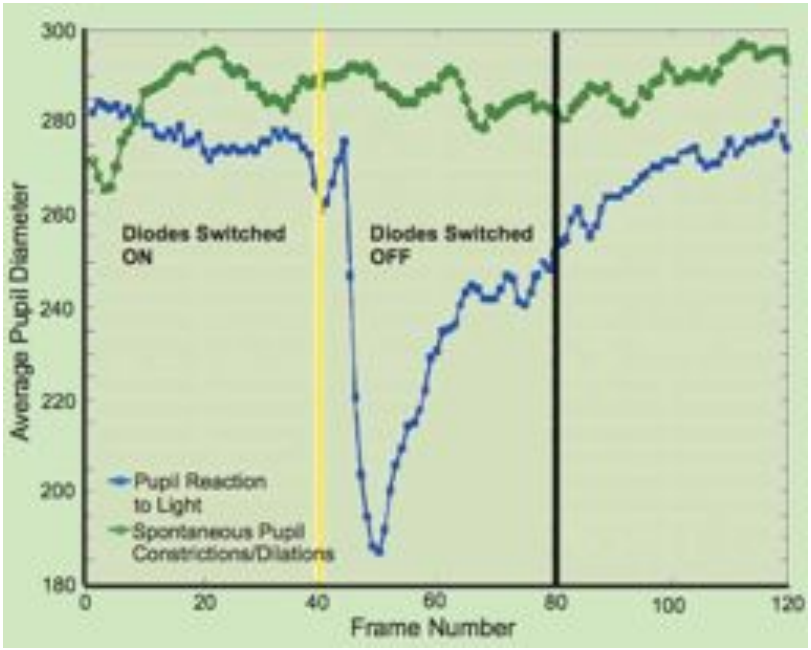
Ref 1) C. X. Zhao, T. Wysocki, F. Agrafioti, and D. Hatzinakos, “Securing handheld devices and fingerprint readers with ECG biometrics,” presented at the Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on, 2012, pp. 150–155.
Ref 2) D. Osten, H.M Carim, M.R Arneson, and B.L Blan, “Biometric, personal authentication system,” Minnesota Mining and Manufacturing Company, US Patent #5,719,950, Feb. 1998.

チャレンジレスポンス型PAD

Voluntary physiological

自然あるいは無意識な本人によってコントロールできない反応を測定することで生体検知を行う

- 光による瞳孔の収縮
- 膝蓋腱反射



図：照明をあてた際の瞳孔直径の変化
スイッチをオンにした瞬間瞳孔が収縮している

Involuntary physiological

人間の認知と意識的な行動に基づく反応を測定することで生体検知を行う

- 顔認証における瞬き検知
- 話者照合におけるキーワード発話

図：目を閉じた瞬間を検知する

強力ななりすまし(ウルフ攻撃)

通常のなりすまし

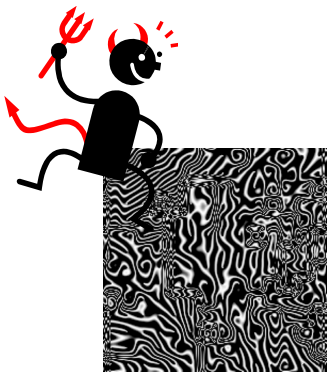

攻撃成功
User A


攻撃成功
User B


攻撃成功
User C

Aさん,Bさん,Cさん専用の
偽造生体でなりすます

強力ななりすまし(ウルフ攻撃)


攻撃失敗
User A
攻撃成功
User B
攻撃成功
User C

1つの偽造生体で
「多くのユーザになりすます」攻撃

実験によるウルフ攻撃の成功確率 2014.3時点

モダリティ	攻撃対象アルゴリズム (論文等)	ウルフ攻撃 成功確率 (これまでの実験で得られた最大値)
指紋認証	C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wil- son, R. M. McCabe, S. Janet, and K. Ko, “User ’s Guide to NIST Biometric Image Software (NBIS), ”National Institute of Standards and Technology , ” http:// fingerprint.nist.gov/NFIS/ , 2007.	42.4%
話者認証	Y. Yamazaki, Y. Fujita, and N. Komatsu, “CELP- based speaker verification: an evaluation under noisy conditions,” ICARCV 2004 8th Control, Automa-tion, Robotics and Vision Conference, 2004., vol.1,pp. 408-412, IEEE, 2004.	50%
虹彩認証	J. Daugman, “How Iris Recognition Works,”IEEE Circuits and Systems for Video Technology, Vol.14, pp21-30, 2004.	42.6%

Fingerprint Wolf

マニューシャマッチング方式へのウルフ攻撃 (Bozorth3)

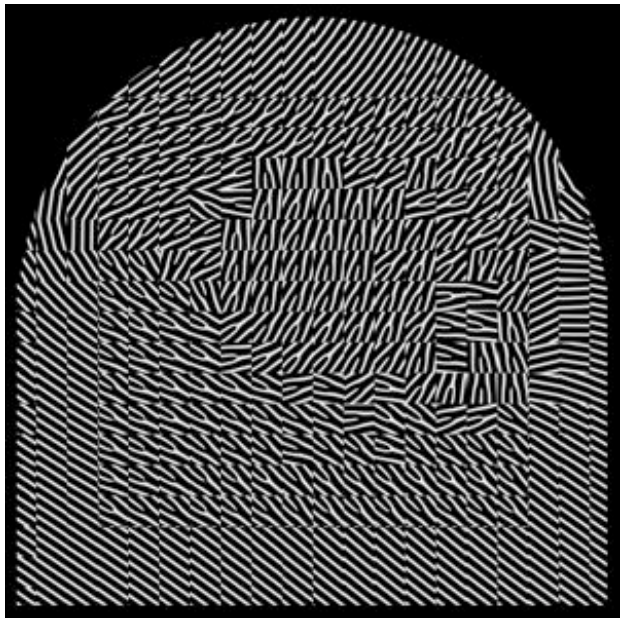
Analysis of Bozorth3

Bozorth3 was much more difficult to find wolf patterns…

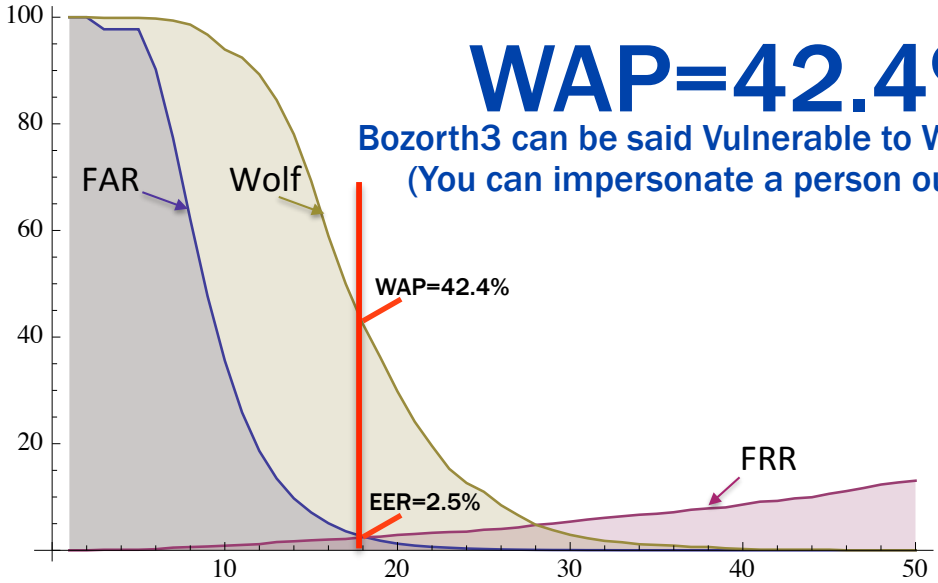
(1) Only up to 200 minutiae accepted
(2) Severer distance allowance of minutiae (within 15 pixels)
(3) Severer direction allowance within 11.25 degree (32 discrete directions)

Previous random minutiae arrangement approach doesn't work!

Our Approach: (1) Arrange 200 minutiae s.t. area (circle of radius 15) of each minutia is disjoint and packed together, and
(2) Direction of each minutiae is determined as the most probable direction at each area around minutia, computed from Human distribution.



Artificial Fingerprint with 14x14=196 Minutiae (tentative)

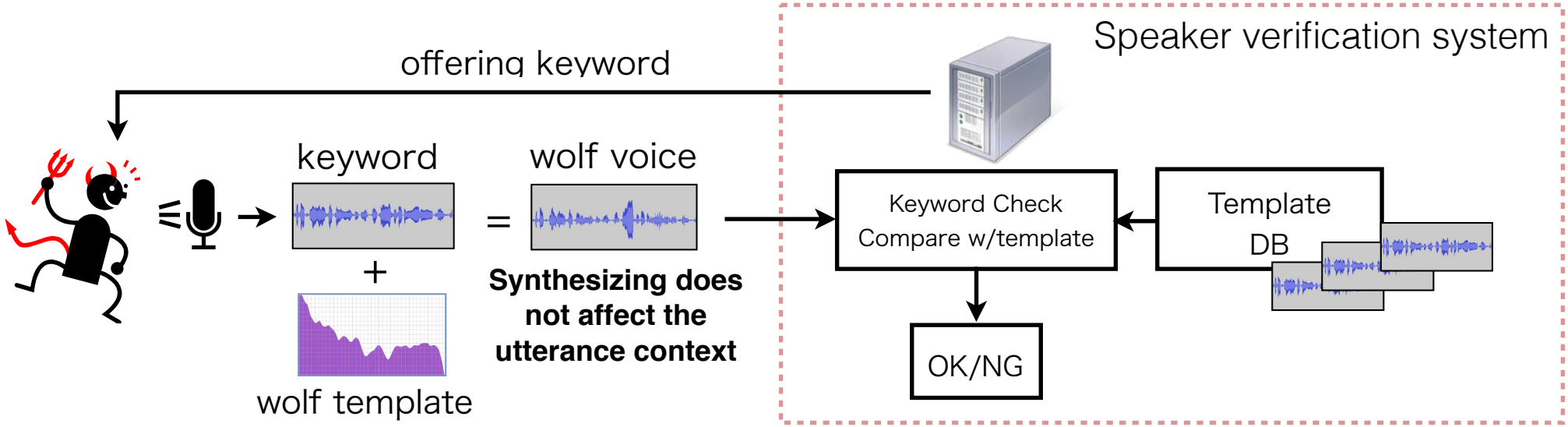


WAP=42.4%

Bozorth3 can be said Vulnerable to Wolf Attack
(You can impersonate a person out of 3!)

A Comparison of Cumulative Score Distributions of Human-Wolf (Yellow) and Human-Human (Red,Blue)

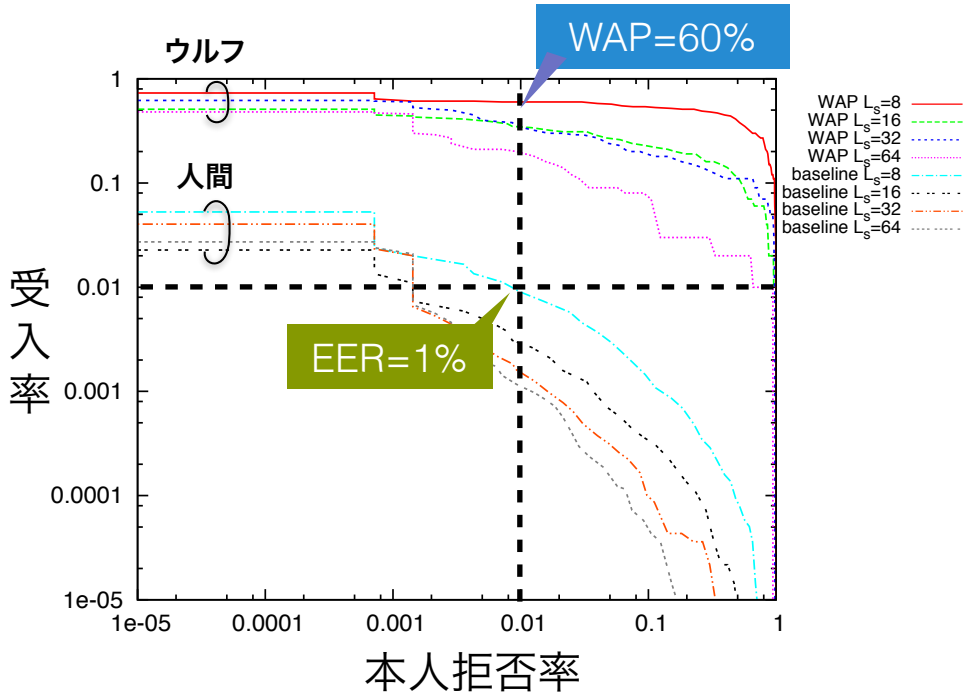
話者照合に対するウルフ



対数尤度比に基づく生体認証に対するウルフ

Given a threshold t > 0, and given an $(\epsilon, \tau) - approximation\ p^*(x)$ of a probability distribution $p(x)$, then, for some $\delta \geq \mathrm{FAR}$ there exists $(1-\epsilon)\delta - wolf, x_w \in X$, namely

$$\mathrm{AR}_t^*(x_w) > (1-\epsilon)\delta$$

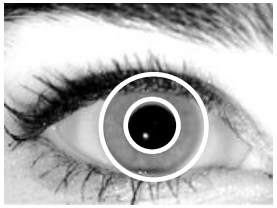


虹彩認証に対するウルフ攻撃（例）

虹彩認証アルゴリズム

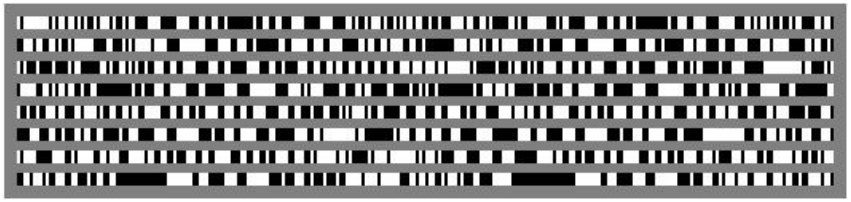
J.Daugman, “How Iris Recognition Worls,”IEEE Circuits and Systems for Video Technology, Vol.14, pp21-30, 2004.

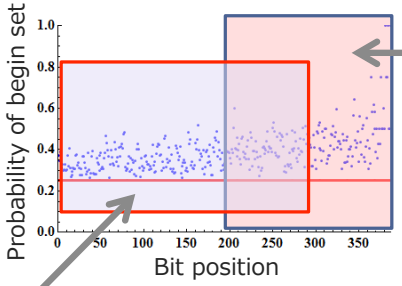
- 虹彩領域を見つける
- 白目と黒目の間にあり囲まれた領域が虹彩



- 虹彩領域を極座標変換し長方形の画像に変換

- Wavelet変換後の位相情報を抽出／2値化





ウルフが利用する虹彩領域

本研究では学習元DBのうち、85%のテンプレートでマスクされる領域を選択

通常の虹彩が利用する虹彩領域

白黒の領域…アイリスコードの1と0

赤の領域　…マスクコードによって照合から除外される領域

通常の虹彩とウルフには、マスクコードに大きな違いがある

- ウルフデータを用いたなりすまし成功確率

DB	認証閾値	EER[%]	WAP[%]
虹彩DB1	0.393	0.98	**42.6**
虹彩DB2	0.375	0.33	14.0
虹彩DB3	0.378	0.65	33.0
ウルフDB	0.393	1.66	33.3

丹, 井沼, 大塚, 今井, “虹彩照合アルゴリズムに対するウルフ攻撃”, SCIS2014.

ウルフ攻撃への対策

- 他人スコア分布の推定 -

動的な閾値決定

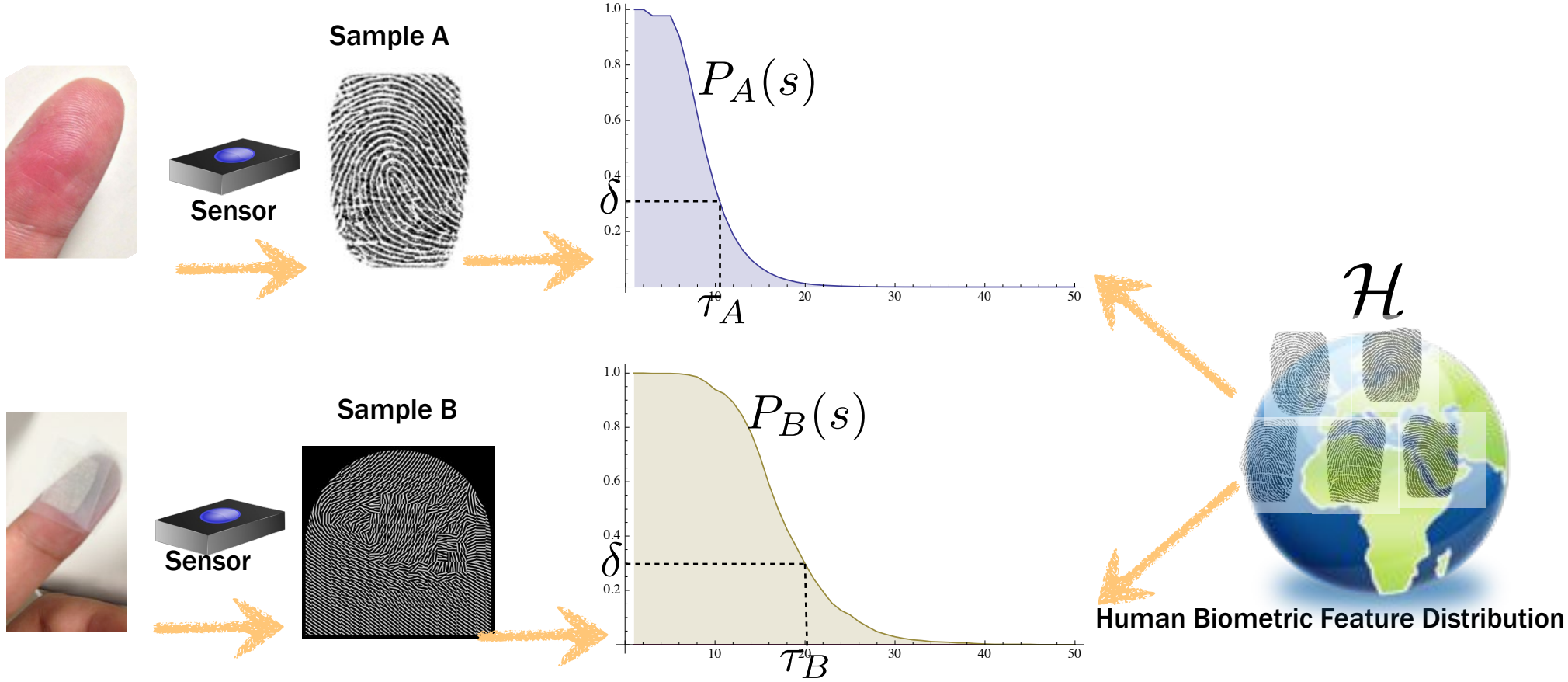
- Determine security parameter $\delta > 0$
- On input sample X, compute a *true cumulative score distribution* $P_X(s)$ and a threshold

$$\tau_X = \max\{x | P_X(x) < \delta\}$$

(computing $P_X(s)$ requires access to distribution of human biometric feature distribution)

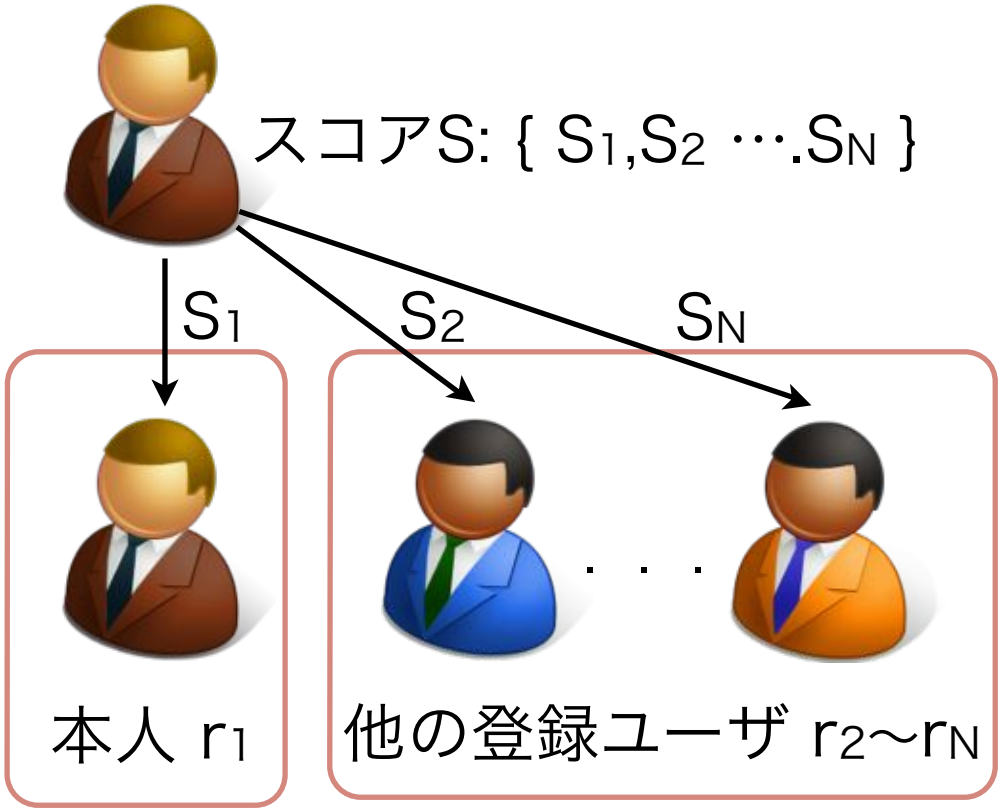
- Then,

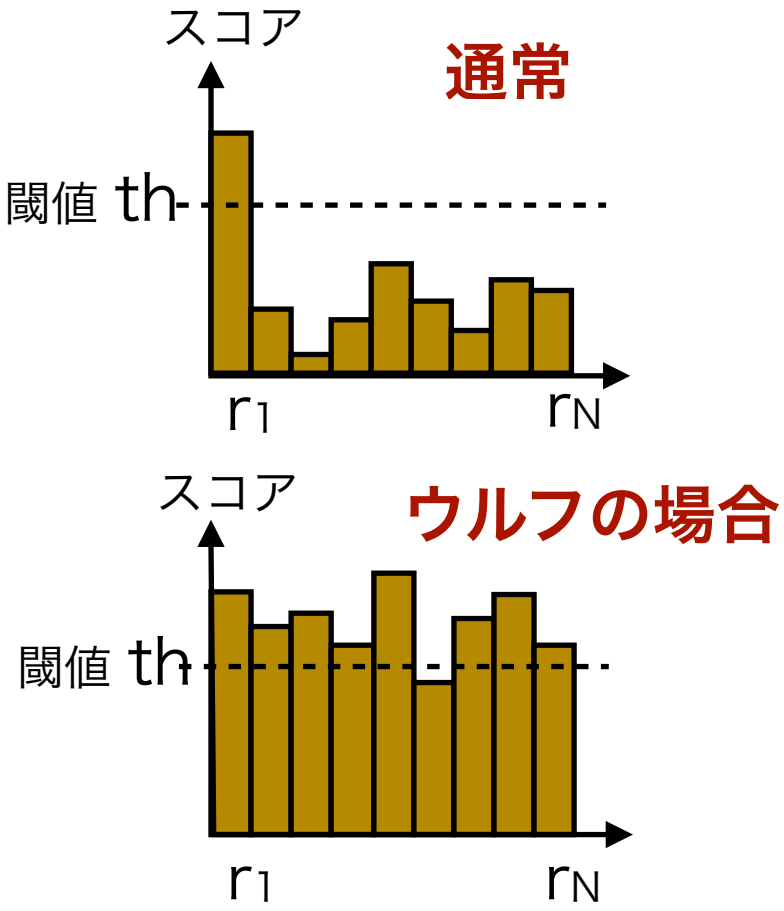
$$\mathrm{WAP} < \delta$$



ウルフ対策

他ユーザとの照合スコア比で判定





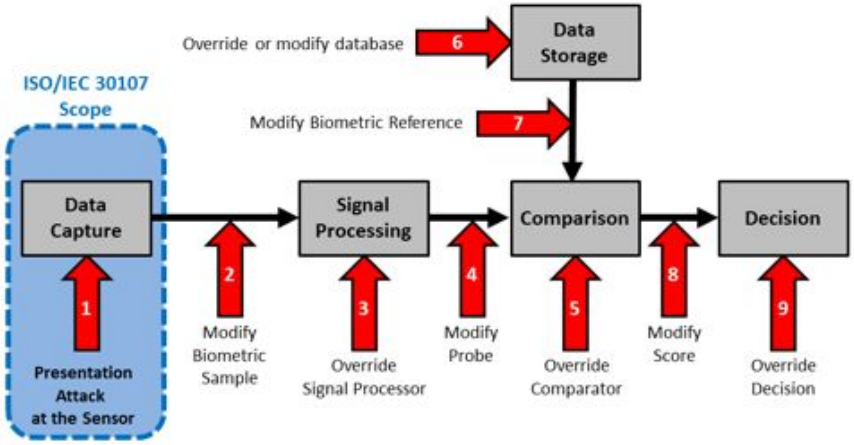
- Wolf は多くのユーザに対して高い照合スコアを示す
- 本人の照合スコアが他ユーザと比較して相対的に高ければ受入

参考： 村上隆夫,高橋健太,“ 生体認証における Wolf と Lamb に対す る安全性の高い判定アルゴリズムの提案 ”,情報処理学会論文 誌,Vol.51,No.12,pp.2319-2329,2010.

ISO/IEC 30107 Biometric Presentation Attack Detection

生体認証機器に対するなりすまし攻撃の用語定義と分類、評価方法の定義

- 2011年1月 ISO/IEC 30107 “Anti-Spoofing and Liveness Detection Techniques”が開始
- 2014年1月 文書をFramework, Data Format, Testing and Reporting の3パートに分割
- 2014年7月 ISO/IEC 30107 “Biometric presentation attack detection”へタイトル変更



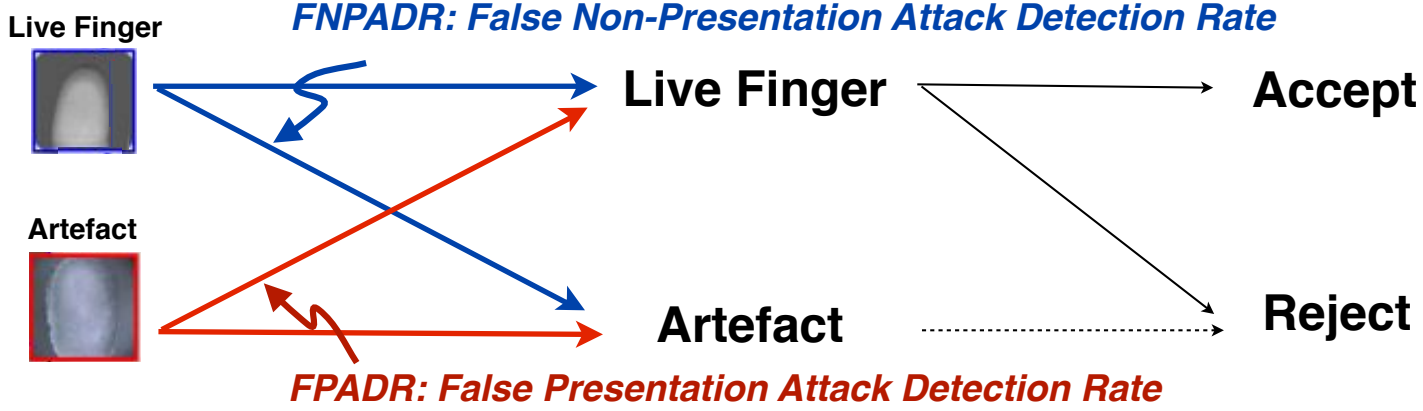
各パートの構成

Part1: Framework

Part2: Data Format

Part3: Testing and Reporting

評価指標の一例(30107-3 WD1)



まとめ

生体認証の歴史と代表的な認証技術

- **個人認証の三要素(記憶，所有，生体)**
- 安全かつ簡単な個人認証の実現には3つの要素の利点を活用した **マルチファクター認証**が重要

今後の生体認証普及に関して重要な2つの課題

- **テンプレート保護型生体認証**
  - 代表的な技術と標準化動向を解説
  - さらなる技術開発で保管情報から生体情報が漏えいする心配のない生体認証システムの実現が期待される
- **生体認証装置に対するPresentation Attack（人工物攻撃）**
  - 攻撃技術／対策技術の現状を解説
  - 認証機器に対する攻撃は現実に様々な手段で行われており、個々の認証機器への対策技術導入が重要

ご清聴ありがとうございました

ご質問等は以下の連絡先まで

tetsushi.ohki@aist.go.jp