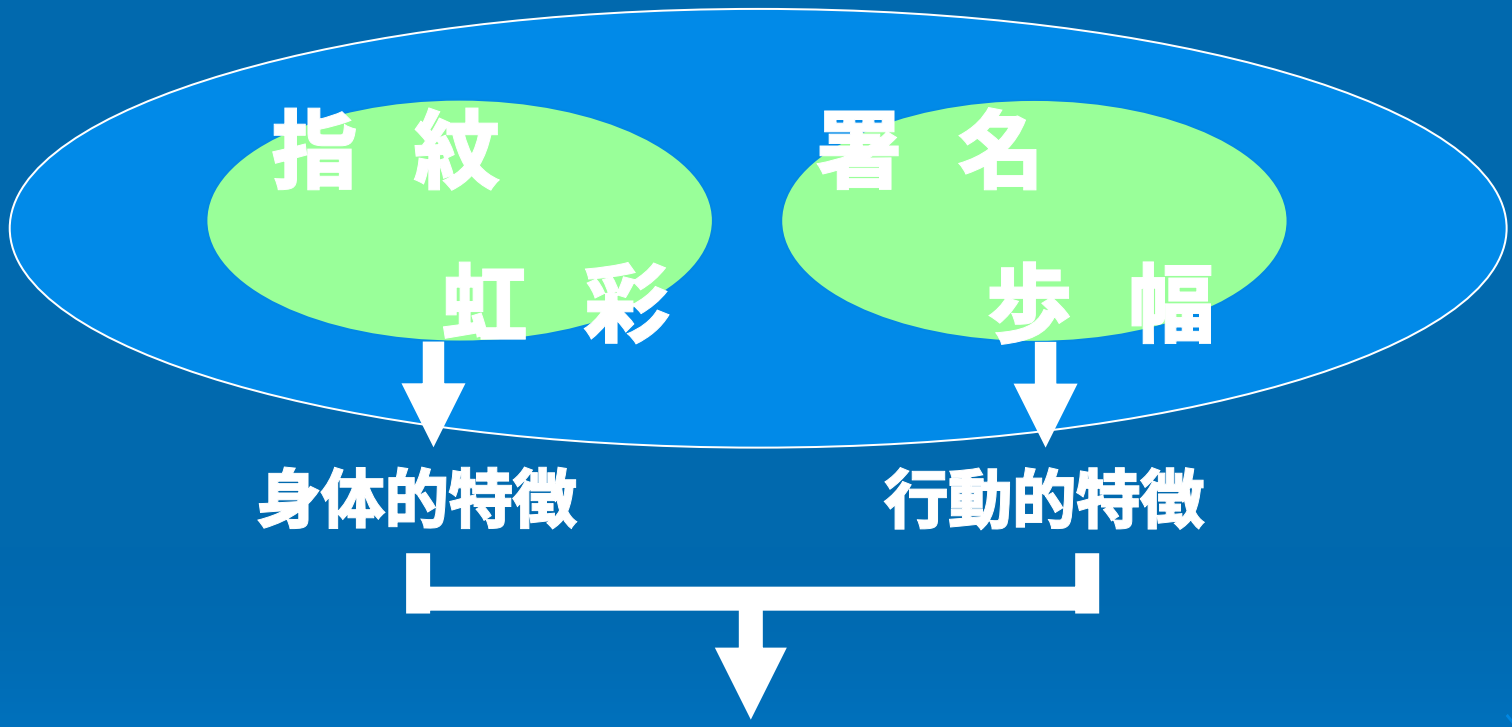
ユビキタス時代の
バイオメトリクスセキュリティ

渡邊研究室

00j124　**前羽　理克**

第1章　バイオメトリクスの概要

バイオメトリクスとは



人間の身体的特徴および行動的特徴を
利用して個人を自動的に同定する技術

歴史的背景

- ・人が他人を顔や声により同定することは昔から行われてきた。

  ＜例＞指紋　－＞

  　指紋は「万人不同」、「終生不変」という特徴をもつと経験的に理解されていたため、古くから個人同定の手段として用いられてきた。日本では拇印の習慣がいまだに残っている

- 現在では、犯罪捜査のみならず、ネットワーク社会における本人の確認手段として位置づけられ、様々な開発が行われている。

バイオメトリクスの基本的な性質

安全性の高い優れたバイオメトリクスの条件としては、次式で示されるF-ratioパラメータが大きいことが要求される

F=異なる生体間変動／同一生体間変動

- 異なる生体間変動：本人と他人との特徴の違いに比例する値。よって、大きいほうがよい
- 同一生体間変動：疲労・情緒などに起因する変動。よって、小さいほうがよい

また、“Sheep and Goats現象”を引き起こすのも特徴のひとつである

声紋認証の精度には、話者による大きな偏りがあり、誤認識のきわめて大きい、一部の話者によって全体の認証性能が決まってしまう現象

バイオメトリクスの種類

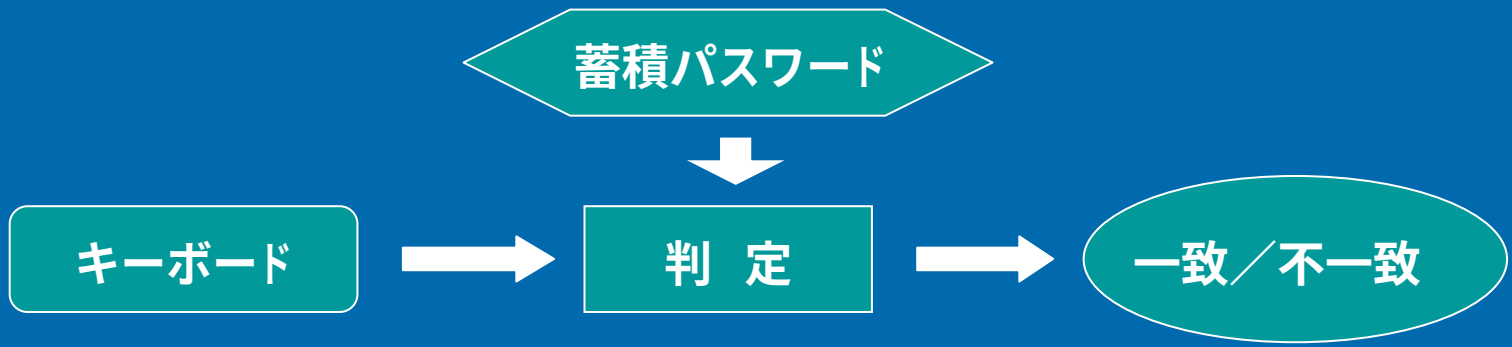
以下に主要なバイオメトリクスについて、各レベルを表示する

生体情報	普遍性	携帯性	永続性	収集性	精度	受容性	脅威耐性
指紋	Medium	High	High	Medium	High	Medium	High
虹彩	High	High	High	Medium	High	Low	High
静脈	Medium	Low	Medium	Medium	Medium	Medium	High
DNA	High	High	High	Low	High	Low	Low
声紋	Medium	High	Low	Medium	Low	High	Low
動的署名	Low	Low	Low	High	Low	High	Low

第2章　バイオメトリクスの本人認証技術への展開

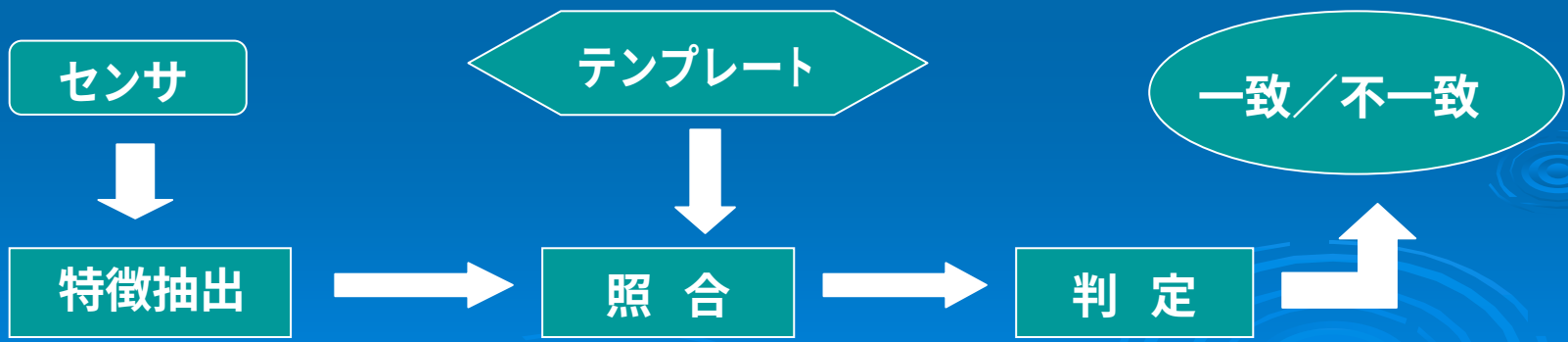
本人認証におけるバイオメトリクス技術

A) パスワードモデル



誤差：いくつかの文字が一致しない場合に生じる確定的なもの

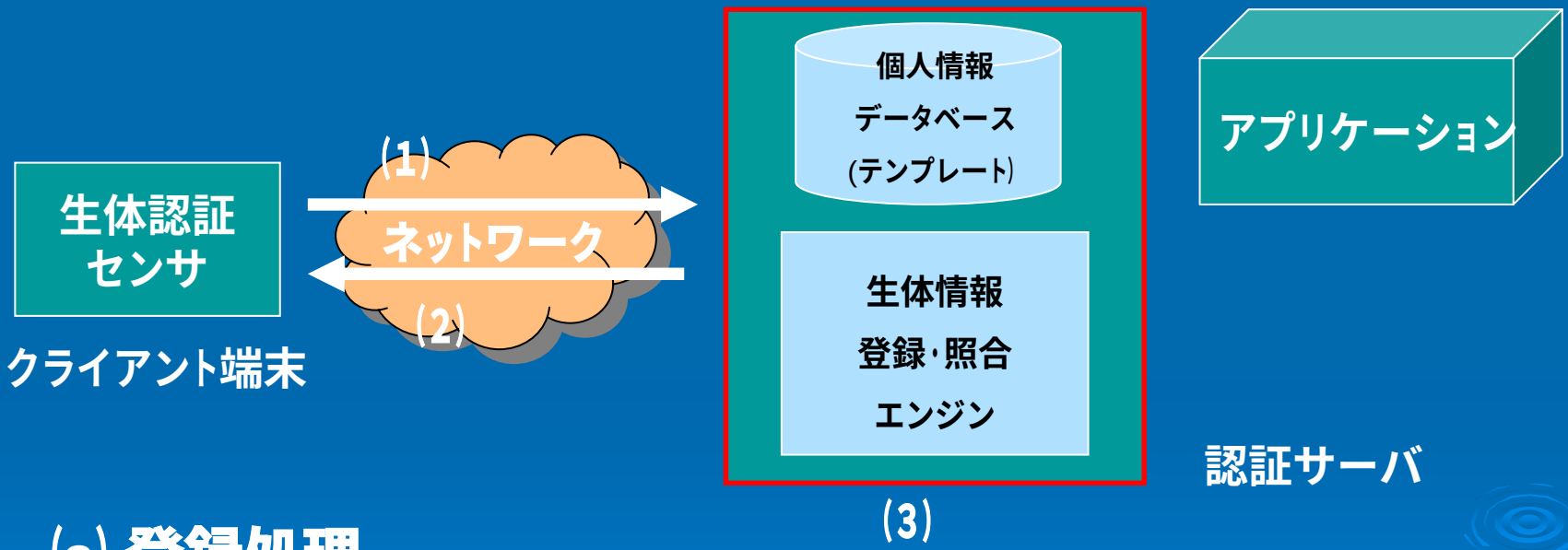
B) バイオメトリクスモデル



誤差：入力データによるパターンマッチング処理が基本なため、
これに起因する統計的な誤差が生じる

バイオメトリクス認証モデル

(Ⅰ)サーバ認証モデル：バイオメトリクスは集中管理し、検索エンジンを用いて高速認証するモデル



(a) 登録処理

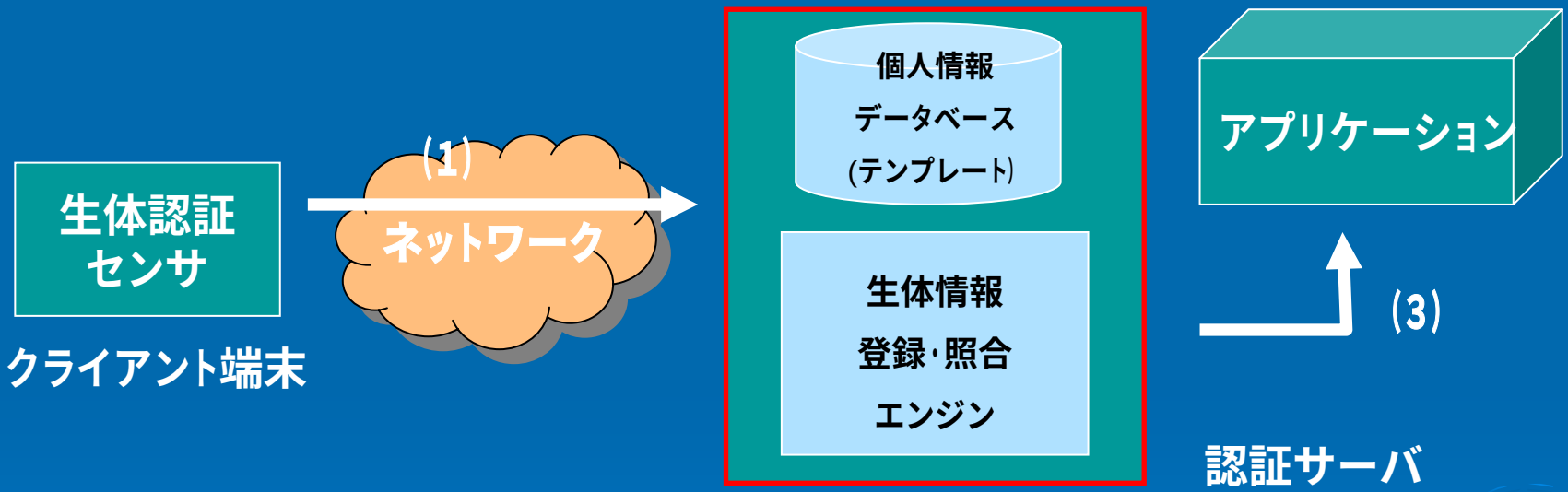
(1) 個人情報および生体情報を認証サーバに転送

(2) 認証サーバで与信紹介を行う

(3) 個人情報･ID情報･特徴量を登録する

バイオメトリクス認証モデル

(Ⅰ)サーバ認証モデル：バイオメトリクスは集中管理し、検索エンジンを用いて高速認証するモデル



(b)認証処理

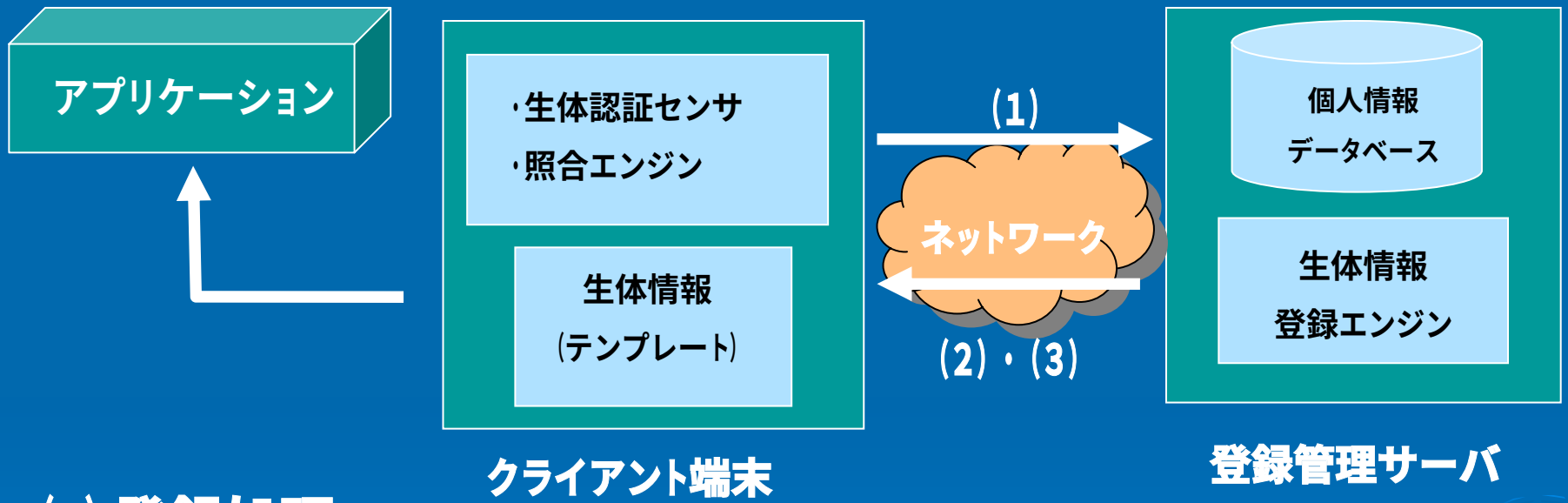
(1) ID情報および生体情報を認証サーバに転送

(2) 認証処理を行う

(3) アプリケーションを駆動する

バイオメトリクス認証モデル

(II) クライアント認証モデル：登録はサーバで行うが、認証処理・結果を端末で操作する

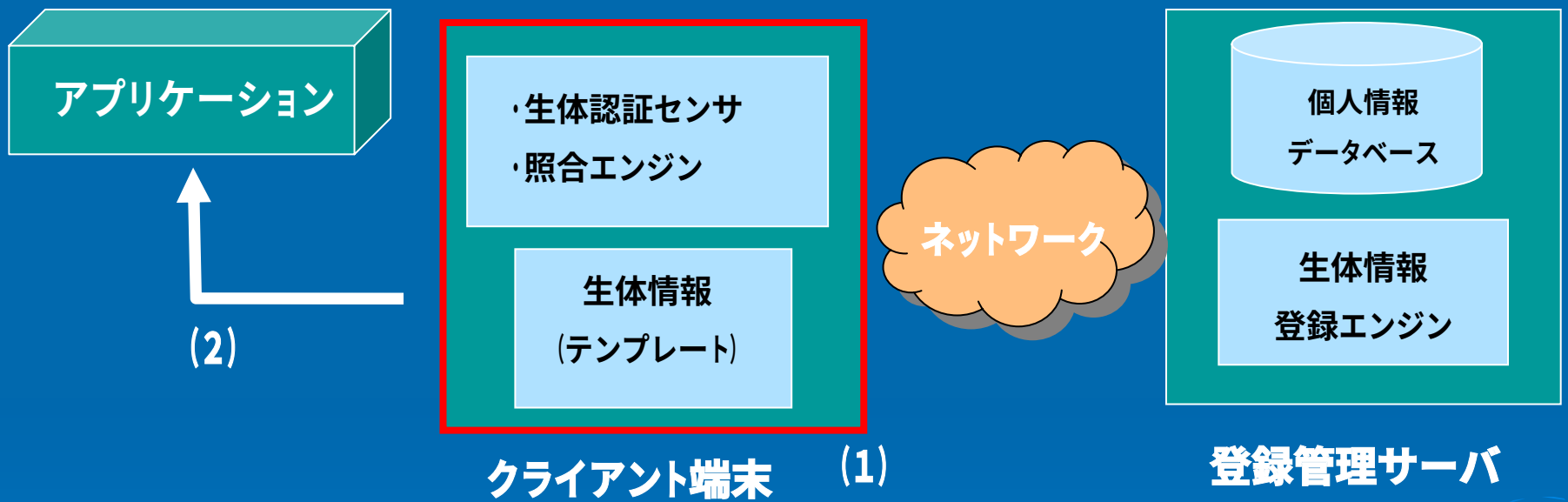


(a) 登録処理

(1) センサで入力した個人情報を認証サーバに転送する
(2) 管理サーバで与信を行う
(3) 問題ない場合はテンプレートをクライアント端末に転送しクライアント端末で保管する。
個人情報・ID情報・特徴量はシステムの安全性確保のため、管理サーバで保管する。

バイオメトリクス認証モデル

(II) クライアント認証モデル：登録はサーバで行うが、認証処理・結果を端末で操作する



(b) 認証処理

(1) センサで入力した個人情報をクライアント端末で認証処理する

(2) 認証結果が妥当ならば、アプリケーションを起動する

バイオメトリクス技術の共通化

現在、多くのベンダから製品が販売されているが、互換性がなくシステムを構築・改修するのに非常に不便である。

対策

バイオメトリクス技術をセキュリティとして汎用的に使用する場合、以下の項目について標準化を行うのが望ましい

- データフォーマット基準
- プログラムインタフェース基準
- 精度評価基準
- 運用要求策定ガイドライン

データフォーマット基準

バイオメトリクスのデータフォーマット基準には、現在“ＣＢＥＦＦ”が用いられている

＜ 今 後 の 展 開 ＞

ネットワーク分野

今後グローバルネットワーク全体がひとつの情報処理システムやデータベースと化していくと考えられる。

データ表現方法の標準化が必要となり、XMLをデータ記述言語の世界基準として期待されている

バイオメトリクス分野

ネットワークを介した大規模なバイオメトリクス認証システムのニーズが期待されている

バイオメトリクスでも、データ記述法としてXMLを使うほうがよい。
ー＞CBEFFに準拠したXMLコード“XCBF”を策定している

プログラムインタフェース基準

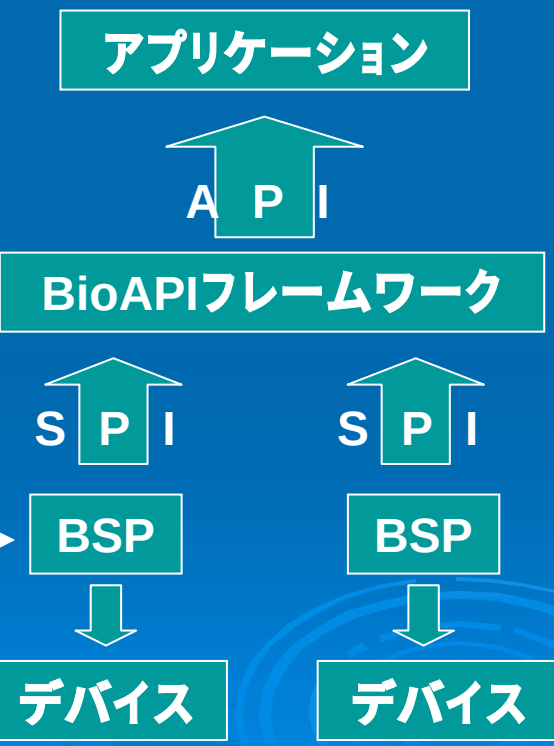
バイオメトリクスのアプリケーションプログラムインタフェース（API）として、BioAPIが採用されている

API

BioAPIフレームワークがアプリケーションプログラムに対して提供するインタフェース

SPI

BSPがBioAPIフレームに対して提供するインタフェース



アプリケーションに対し、APIフレームワークを介して機能を提供する。

精度評価基準

＜一般的な精度評価方法＞

一般的に、バイオメトリクス認証システムの精度を表すのに、

本人拒否率（FNMR） と **他人受入率（FMR）** を使用する

・本人が誤って拒否される割合。

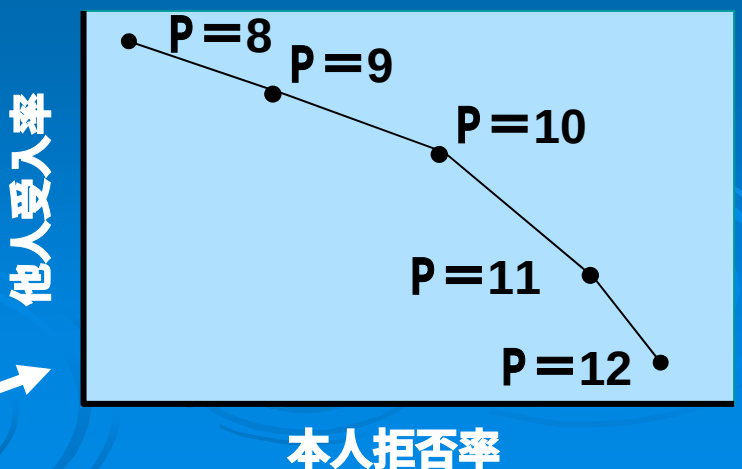
$$FNMR = \frac{\text{誤って不一致と判定した数}}{\text{照合に使用されるすべての組み合わせ（Genuine）}}$$

・他人を誤って受け入れる割合

$$FMR = \frac{\text{誤って一致と判定した数}}{\text{Genuine} \times \text{本人以外のテンプレート数}}$$

本人拒否率と他人受入率は、トレードオフな関係にある

このトレードオフな関係を表したのが右の“ROCカーブ”である



精度評価における課題および標準化

＜　精度に影響する要因　＞

要因	内容
(a) 評価対象の機能構成	評価対象となるバイオメトリクス認証システムの機能の構成
(b) 被験者の構成と数	生体情報を提供する被験者の構成と数
(c) 収集条件	入力装置の設置状態、生体情報の経時変化、被験者のシステムに対する習熟の程度などの収集条件
(d) 未対応	バイオメトリクス認証システムで登録あるいは照合できない生体情報の取り扱い
(e) 精度の表記法	本人拒否率と他人受入率の表記の方法

以上の要因に対して、具体的な指針および試験方法を定めることによって、精度の再現性を保障しようというのが精度評価の標準化の目的である

現在、精度評価ガイドラインを原案にバイオメトリクス標準化調査委員会において、標準方法 (Techical　Report) の策定が進められている

運用要求策定ガイドライン

標準化の背景

バイオメトリクス認証装置を情報システム分野など、さまざまなアプリケーションへの展開を想定すると、以下のような要求がでてくると想定され、明確な指針が求められる

・安全性だけでなく、利便性の要求

・どの程度の精度が必要であるかの要求

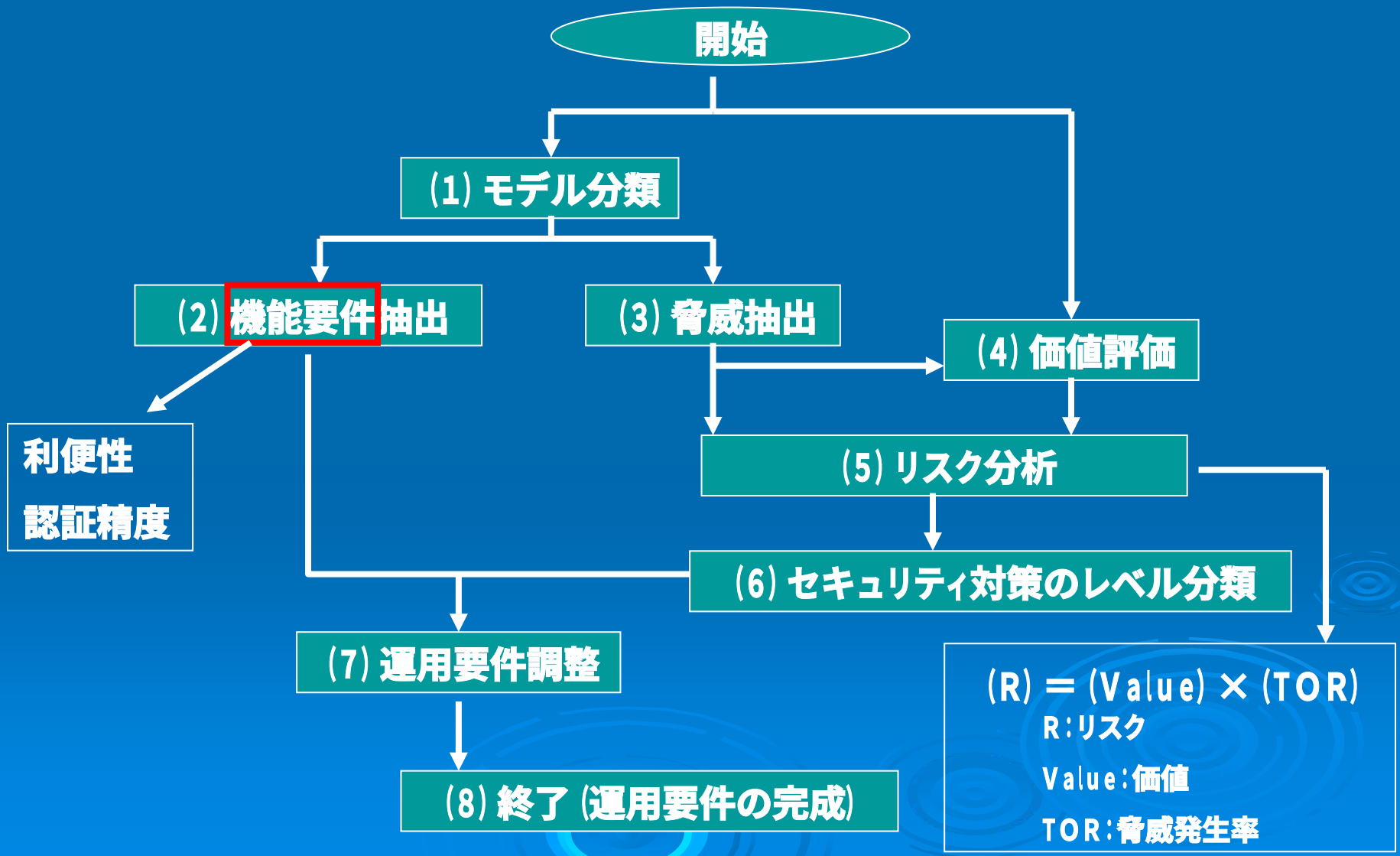
対　策

・セキュリティ対策の観点でそれぞれのアプリケーションのリスクを評価して、バイオメトリクスの認証精度に関する要件の明確化

・アプリケーションに必要なバイオメトリクスを選択するための指針の明確化

運用要求策定ガイドラインを作成

運用要件策定フロー


開始
(1) モデル分類
(2) 機能要件抽出
(3) 脅威抽出
(4) 価値評価
利便性
認証精度
(5) リスク分析
(6) セキュリティ対策のレベル分類
(7) 運用要件調整
(8) 終了 (運用要件の完成)
(R) = (Value) × (TOR)
R:リスク
Value:価値
TOR:脅威発生率

バイオメトリクス認証における脅威

バイオメトリクス認証に対する脅威は、一般的な情報システムにおける脅威と同様に、情報セキュリティ上の要件を損なう攻撃や事故があげられる

＜ 例 ＞

(1) 利用者の真正性を損なう脅威

生体情報の偽造によるなりすましや、他人受入率を制御する認証パラメータの不正な変更

(2) 可用性を損なう脅威

生体情報入力装置の破壊、生体情報の変化による本人拒否率の頻繁な発生

(3) 機密性・安全性を損なう脅威

ハッキングなどの電子的な生体情報の流出、テンプレートデータからの生体情報の再構成

バイオメトリクス認証の脆弱性

バイオメトリクス認証特有の脆弱性は、個人認証情報として用いている生体情報の性質に起因する

(1) 生体情報は他人にさらされる

この性質が起因の脆弱性は、生体認証の取得が挙げられる。この脆弱性は、そのまま生体情報の偽造による“なりすまし”などの脅威につながる

(2) 生体情報の数には限りがある

バイオメトリクス認証の場合、一人当たりの生体情報に限りがある（例：指紋では最大１０個）。よって、利用者の生体情報の更新回数の制限が脆弱性として上げられる。

(3) 生体情報は変化する

生体情報は体のコンディションによって変化するため、認証一致の条件には幅を持たせている。このため、他人受入誤差が発生することになり、これが脆弱性となる。

第3章　セキュリティ技術とバイオメトリクス認証のシナジー技術

セキュリティ技術と
バイオメトリクス技術のシナジー技術

- ICカードへのバイオメトリクス技術の組み込み
- 暗号技術とバイオメトリクスの融合
- PKI（公開鍵基盤）とバイオメトリクスの連携

暗号とバイオメトリクス

バイオメトリクスと暗号技術の接点

(1) 生体情報の秘匿とプライバシ保護

生体認証技術の広域化に伴い、使用する生体情報の的確な秘匿と正当な情報管理のために、暗号技術は欠かせない手段になっている

(2) 生体情報によるデジタル署名

デジタル署名をより厳格に実施するために、生体情報による本人確認を行ったうえで本人の秘密鍵を施錠し、署名演算をおこなう

(3) 生体情報を暗号鍵に組み込む技術とその効用

ＤＮＡ情報のように個人識別子がデジタル確定値である場合は、
生体情報を暗号化して暗号鍵に組み込む事ができる。

この暗号鍵でデジタル署名を行うことは、あたかも血判を押したような効果をもたらす

ＤＮＡ情報の暗号鍵への組込

ＤＮＡ情報の特徴

	原情報の特性	特徴点データ長	一意性	分析時間
ＤＮＡ情報	デジタル情報	20バイト	～1/（10の18乗）	１日～３Ｈ
指紋・虹彩の紋様	アナログ情報	250バイト	～1/（10の６乗）	リアルタイム

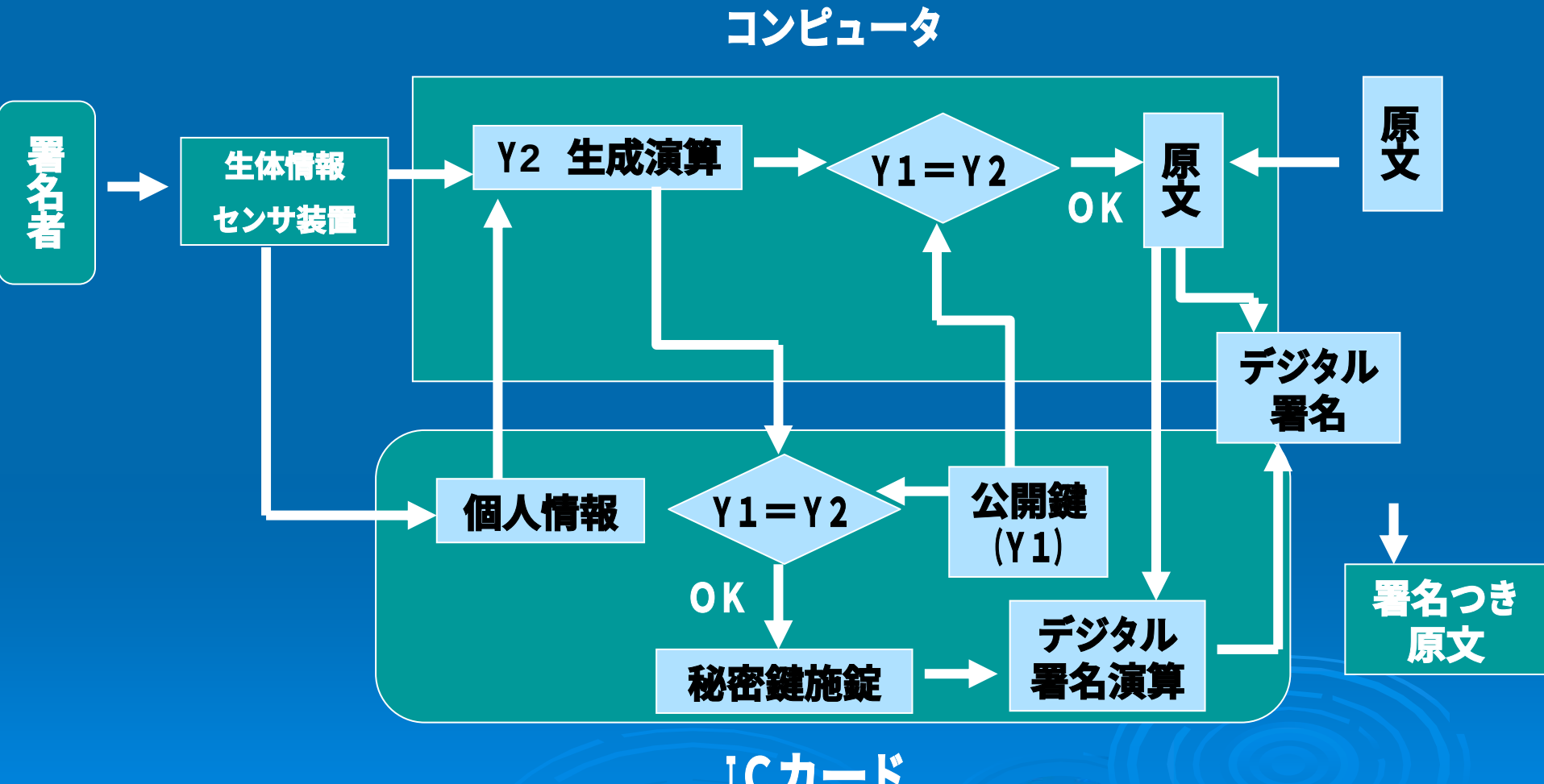
暗号鍵へ組み込む意義

（1）プライバシの保護

（2）直接組み込み可能なＤＮＡ情報のコンパクト性

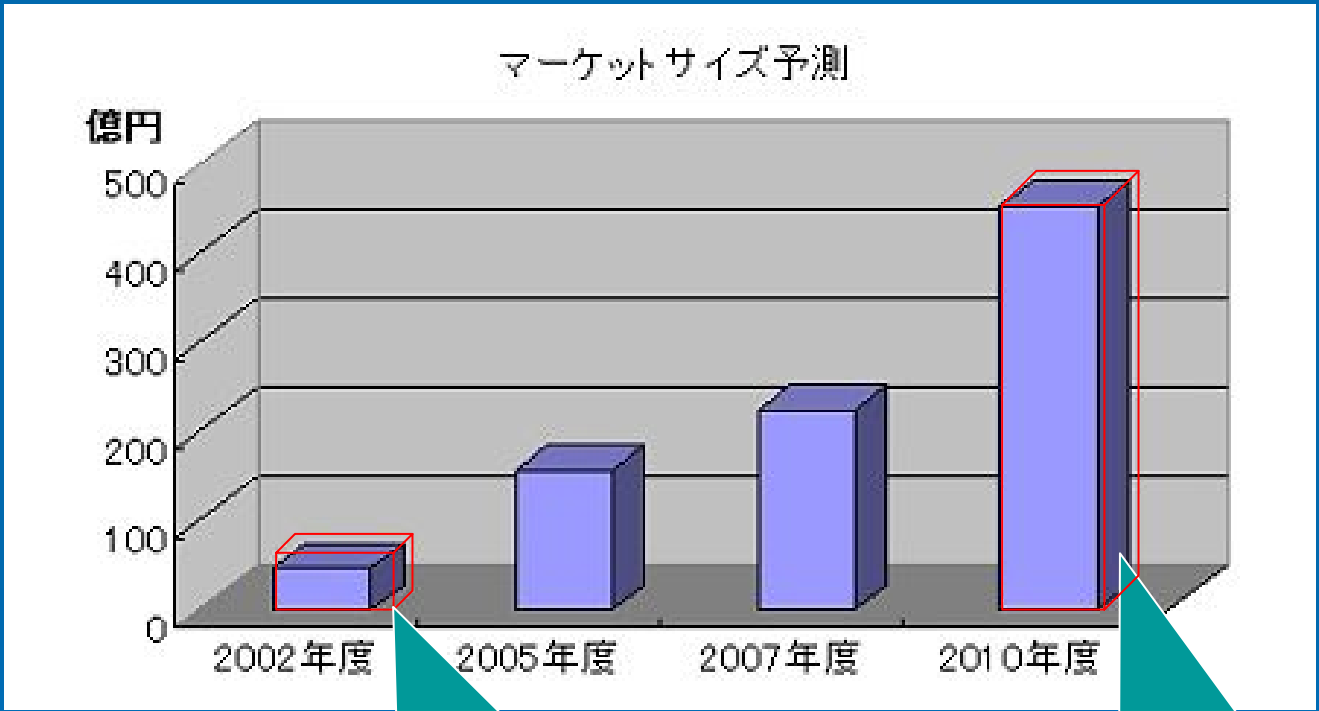
（3）生体情報ＤＢが不要

DNAバイオメトリクス本人認証/デジタル署名システム



第4章　バイオメトリクスセキュリティの今後の展開

バイオメトリクス市場の推移



8年後には約5倍に膨れ上がると予想されており、

更なる、市場規模の拡大が期待できる

今後のバイオメトリクスの位置づけ

ネットワークのユビキタス化にともない、安全で簡単な個人認証が要求されている

バイオメトリクス単体では、安全性の確保ができない

マルチモーダル化（他の個人認証技術、または複数のバイオメトリクス認証を融合する）によって、今後の社会の要求に応えていく

ま と め

- バイオメトリクス技術には、更なる可能性が秘められており、今後のネットワーク社会への展開に期待ができる
- バイオメトリクス技術は、よく究極の個人認証技術だと言われているが、実際は他の個人認証技術と大差はない。
- バイオメトリクス技術を個人認証に適用する場合は、特性をよく理解し、 他の個人認証と複合させることにより真価を発揮する

参考資料

- ユビキタス時代のバイオメトリクスセキュリティ
  ＜編著＞瀬戸　洋一
- ＭＹＣＯＭ　ＰＶ　ＷＥＢ
  http://pcweb.mycom.co.jp/

お　わ　り