本資料について

- 本資料は下記書籍を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

  - 著者：　瀬戸　洋一
  - 書籍名：サイバーセキュリティにおける生体認証技術
  - 出版社：共立出版
  - 出版日：2002年5月25日

サイバーセキュリティにおける生体認証技術

渡邊研究室　00J075
鈴木　秀和

本発表について

- 「サイバーセキュリティにおける生体認証技術」（瀬戸洋一　著/共立出版）の内容をまとめたものである。
- 本書籍は以下の項目について説明されている。
  1. 情報セキュリティにおける生体認証技術の位置付け
  2. 生体認証技術の概要
  3. 生体認証技術の新しい展開（マルチモーダル化）
  4. 生体認証技術の新しい展開（ICカード）
  5. 標準化の状況
  6. 社会基盤へ展開する上での生体認証技術への期待

サイバーセキュリティにおける本人認証

- サイバー空間で行われているClick and Mortarでの商取引の世界では、全ての情報がディジタル化される。
  - 実世界と異なる本人性の確認
  - データの改ざん検知

情報セキュリティ（サイバーセキュリティ）技術が重要

本人性を確認する技術の1つとして生体認証技術

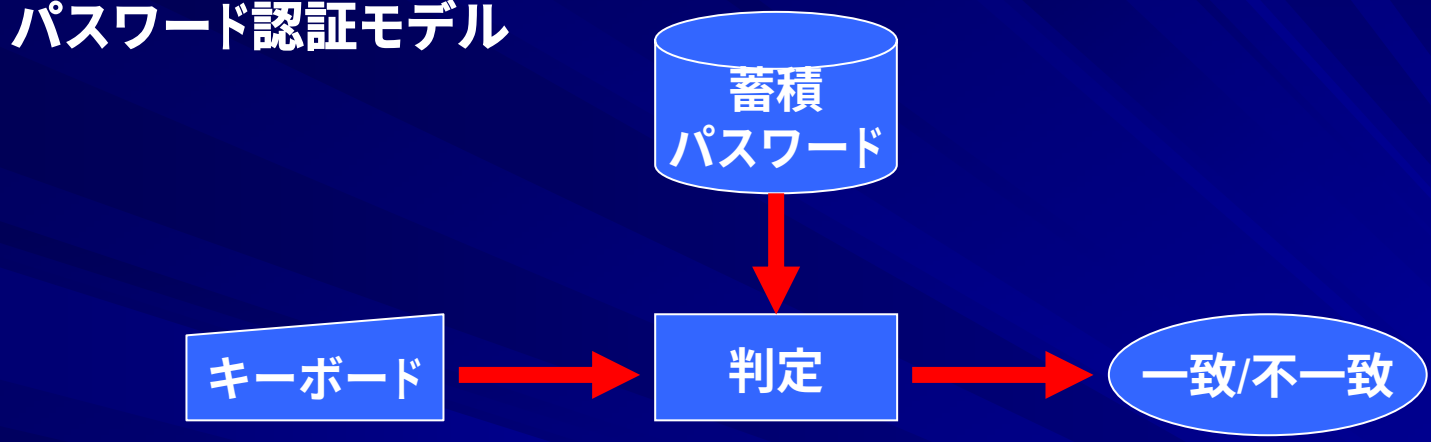
サイバー空間における脅威と対策

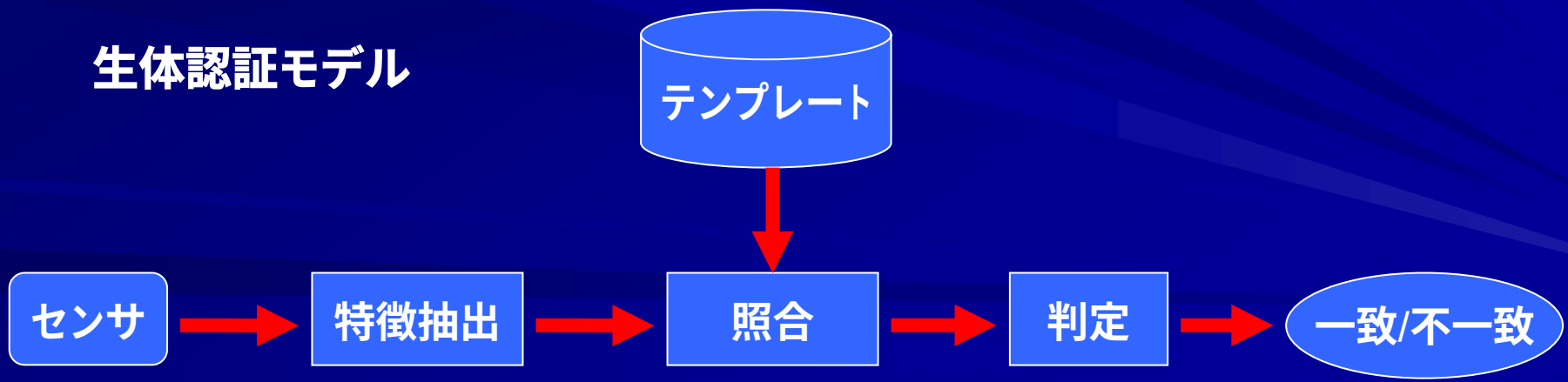
不正者	脅威	対策技術
第3者	機密性の喪失	暗号化/アクセス管理
	完全性の喪失	アクセス管理
	可用性の喪失	アクセス管理
当事者	証拠性の喪失	ディジタル署名
	原本性の喪失	ディジタル署名

対策技術

- 暗号化技術
  - 共通鍵暗号方式：暗号鍵＝複合鍵
  - 公開鍵暗号方式：暗号鍵≠複合鍵
- アクセス管理技術
  - 本人認証
    - 知識による認識：what you know
    - 所有物による認識：what you have
    - 身体的特徴などによる認識：what you are
  - アクセス制御
- ディジタル署名
  - 署名生成：送信メッセージと自分用秘密鍵で署名生成
  - 署名検証：受信メッセージと送信者側公開鍵で署名検証

パスワード認証モデルおよび生体認証モデルの比較





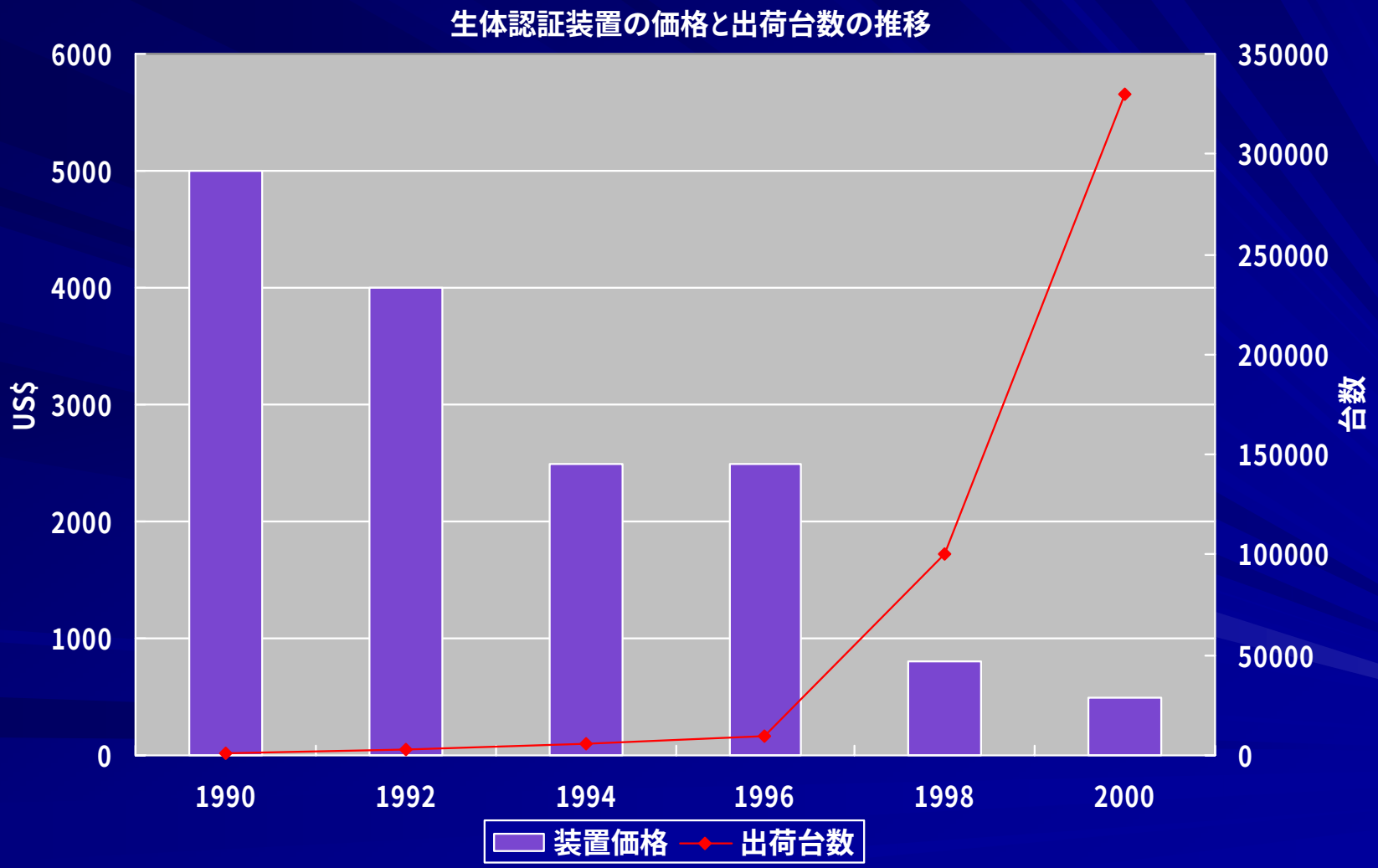
生体認証技術の導入基準

- 本人認証システムへ導入する場合の検討
  - 安全性：Safety
  - 経済性：Economy
  - 簡便性：Handiness
  - 社会的受容性：Public Acceptance
- 照合精度に生体認証製品特有の問題
  - タイプⅠエラー（false rejection rate：本人拒否率）
  - タイプⅡエラー（false acceptance rate:他人受け入れ率）

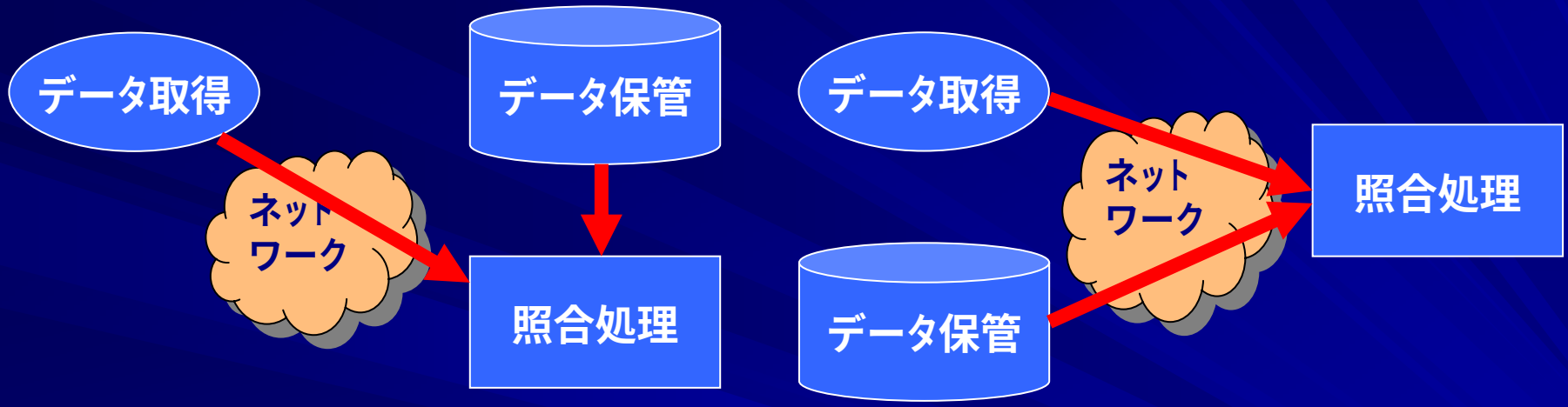
生体認証技術の比較例

生態情報	特徴量	コスト	ユーザ受容性	安全性	精度(%)		データ量 (Byte)	適用分野
					本人拒否	他人受入		
指紋	手の指の指紋の特徴点（マニューシャ）	低	登録に心理的抵抗	中	～0.1	～0.1	1000	全般
掌形	手の大きさ、長さ、厚さ比率	中	容易	低	0.15	0.15	10	低セキュリティ施設管理
顔	顔の輪郭 目や鼻の形および配置	中	容易	低	1～	1～	1000	低セキュリティ施設管理
虹彩	目の虹彩（アイリス）の放射状紋様	高	登録に手間	高	0.1	0.001	256	高セキュリティ施設管理
声紋	話者の音声特徴	中	容易	低	3～	3～	1000	電話サービス
署名	署名の字体 署名時の書き順、筆圧	低	容易	低	1～	1～	1000	低セキュリティ応用

生体認証技術の市場動向

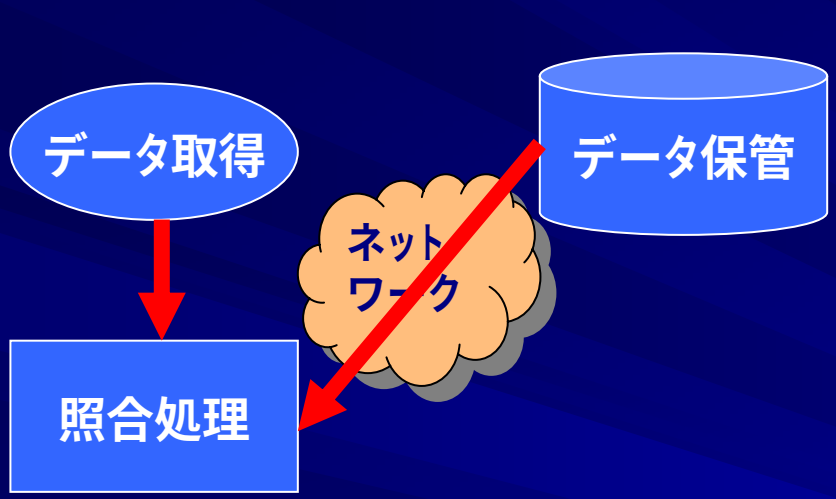


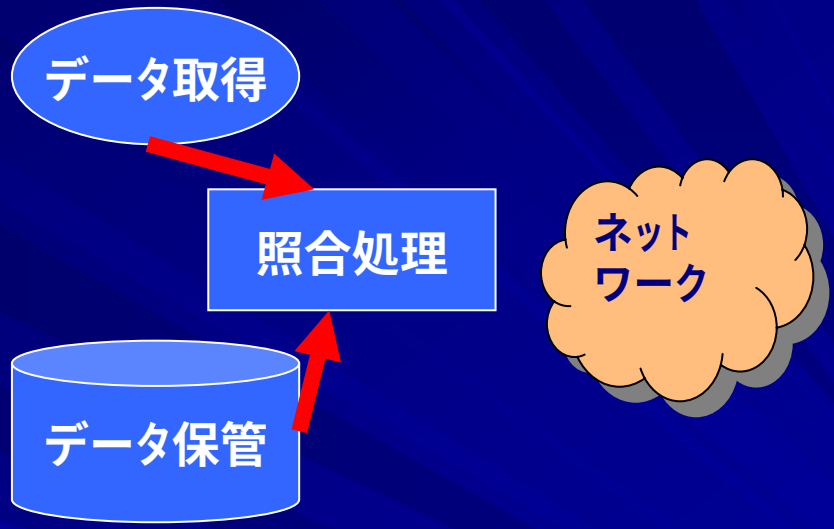
生体認証モデル



- サーバ認証モデル1
  - ネットワーク転送負荷：高
  - サーバ処理負荷：高
  - クライアント処理負荷：低
  - 低コスト
- サーバ認証モデル2
  - ネットワーク転送負荷：高
  - クライアント端末は耐タンパ性を持った構造が必要（ICカードなど）

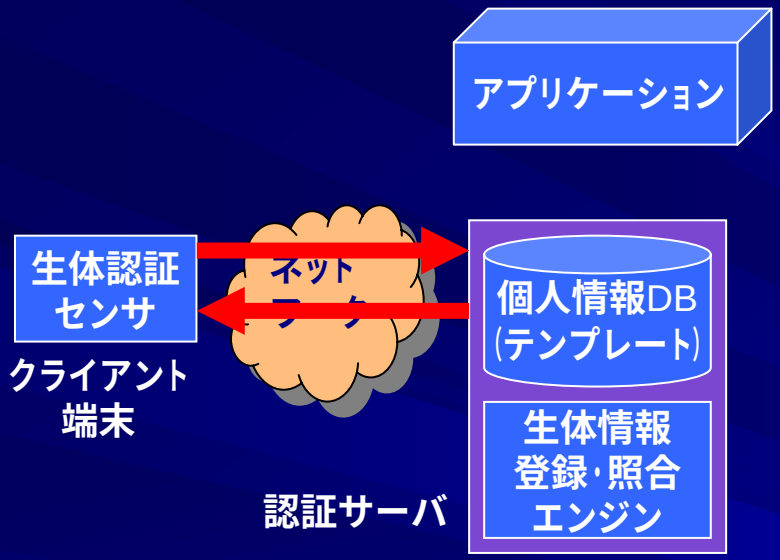
生体認証モデル

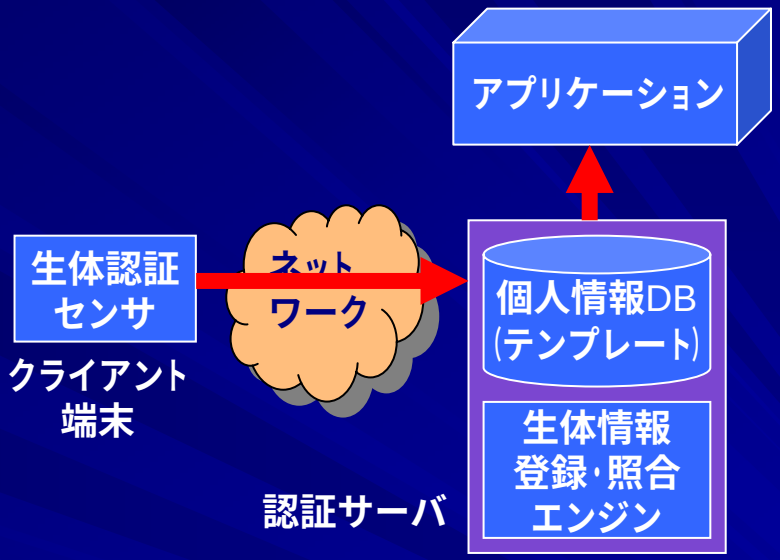




- クライアント認証モデル1
  - ネットワーク転送負荷：低
  - サーバ処理負荷：低
  - クライアント処理負荷：高
- クライアント認証モデル2
  - ネットワーク転送負荷：低
  - クライアントにICカードを用いる場合に有効

サーバ認証モデル

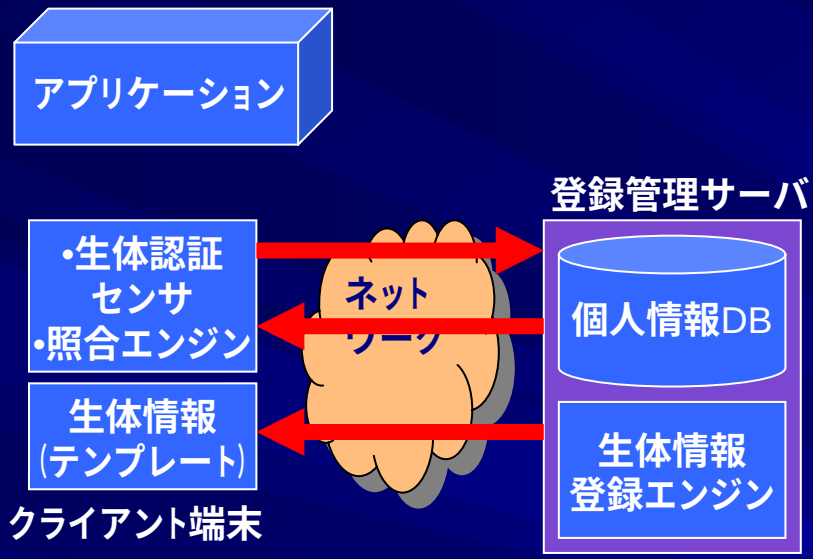


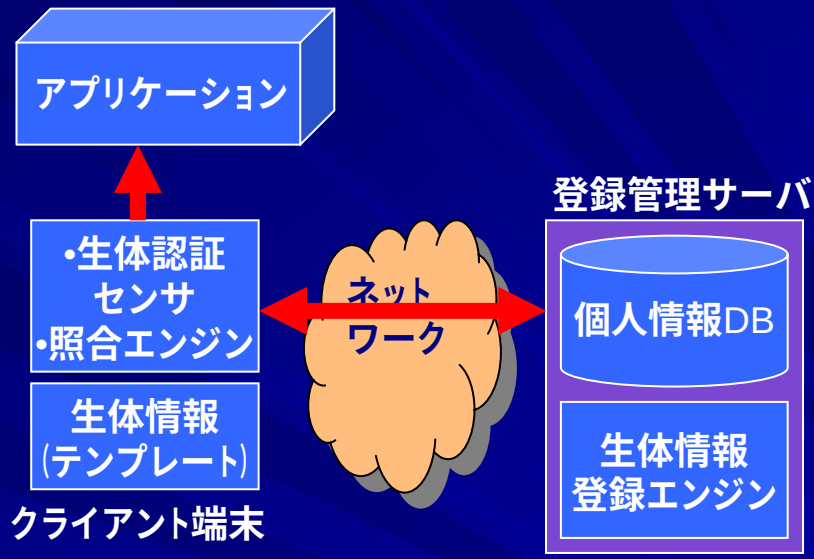


- **登録処理**
  1. 個人情報の転送
  2. 与信照会の実行
  3. 個人情報、ID情報、生体情報の登録

- **認証処理**
  1. 生体情報の転送
  2. 認証処理の実行
  3. アプリケーションの駆動

クライアント認証モデル





- **登録処理**
  1. 個人情報の転送
  2. 与信照会の実行
  3. テンプレートの転送･保管

- **認証処理**
  1. 生体情報の処理
  2. アプリケーションの駆動

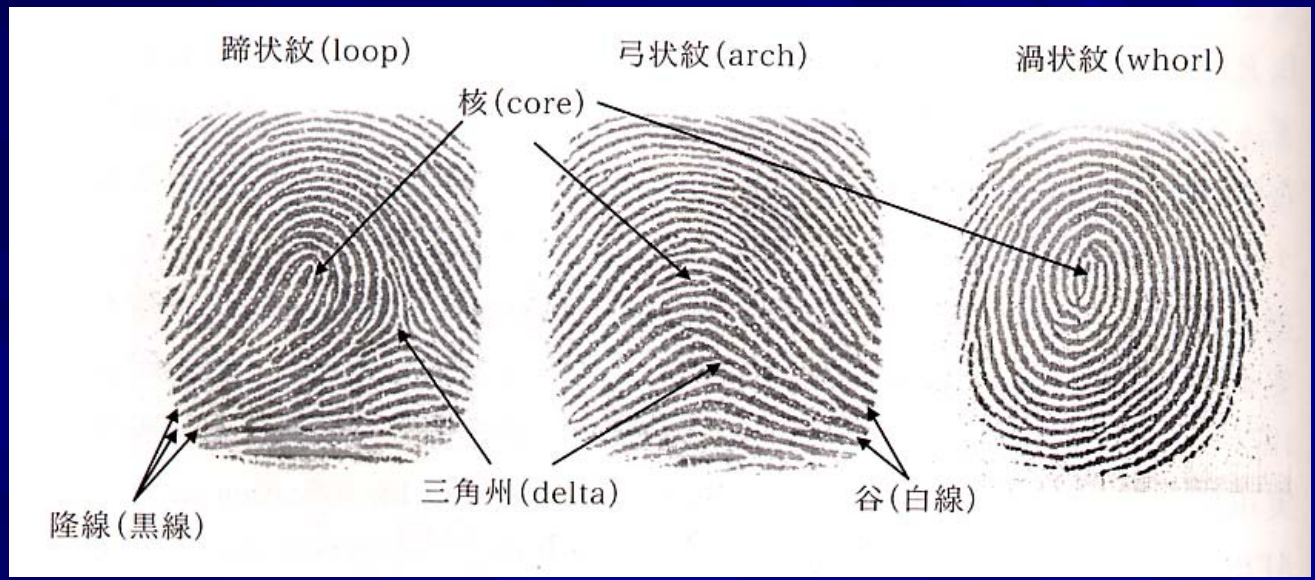
サーバ認証モデルとクライアント認証モデルの比較

	サーバ認証モデル	クライアント認証モデル
メリット	■クライアント端末の処理負荷の軽減 ■コスト削減	■認証サーバ不要によるコスト低減 ■利用者の高受容性 ■システムの安全性
デメリット	■利用者増大に伴うネットワーク負荷・サーバ負荷の増大 ■個人情報の一括管理体制	■クライアント端末の処理負荷が高い ■高端末コスト

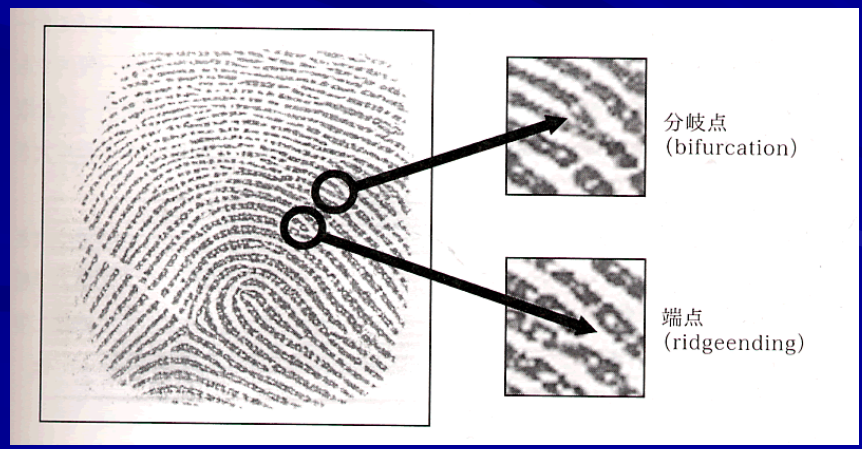
指紋認証

- 指紋 (fingerprint) は「万人不同」「終生不変」の特徴を持つ。
  - 世の中に同一指紋を持つ人間の存在確率：870億分の1
- 指紋認証技術は様々な研究開発が行われている。
  - 犯罪捜査
    - 犯罪者の登録方法 (1901：英国)
    - 犯罪者の個人識別 (1908：日本)
  - ネットワーク社会における本人認証
- 指紋を蹄状 (whorl)、弓状 (arch)、渦状 (loop) の3つに分類。

指紋の種類と紋様の特徴点



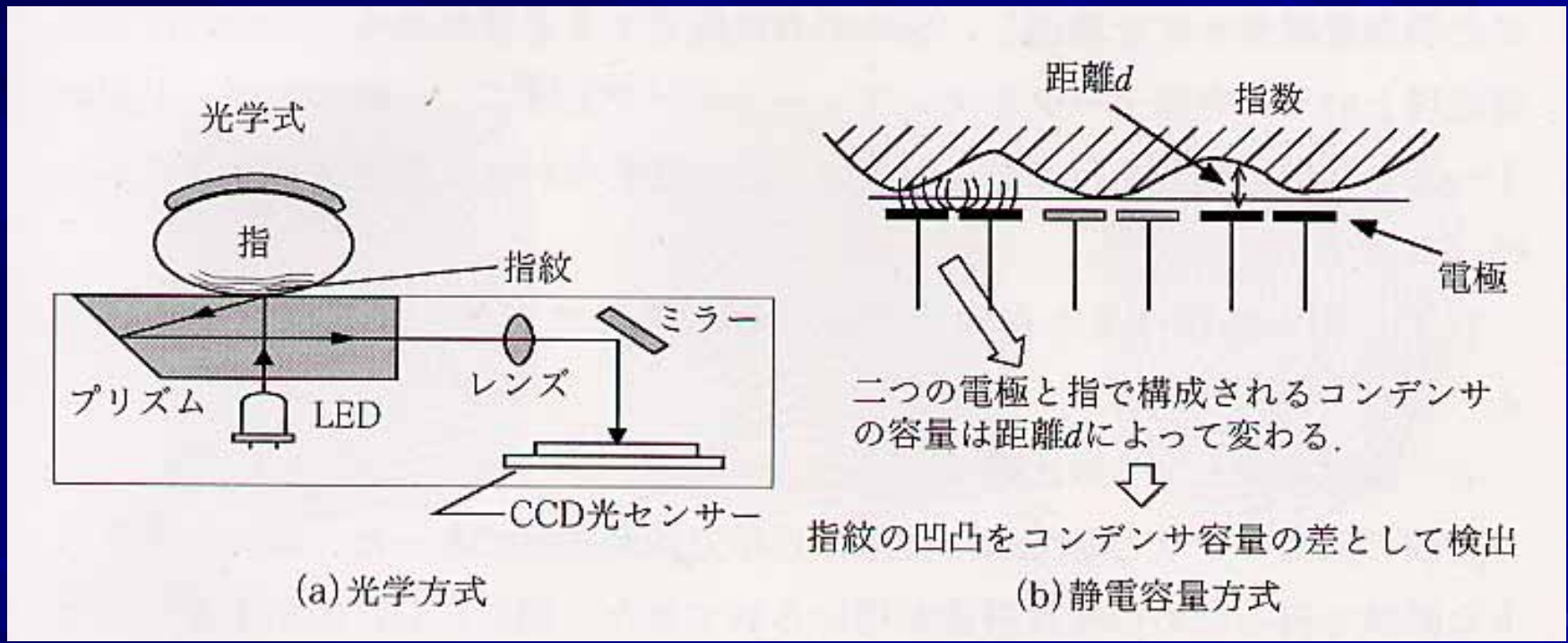
- 紋様の様々な特徴をまとめて特徴点（マニューシャ：minutia）と呼ぶ。
- 1つの指には150程度のマニューシャがあると言われている。



指紋認証の基本処理フロー

1. 入力処理：
   指紋をシステム側でセンサにより取得
2. 特徴抽出処理：
   入力データを処理、照合用の特徴算出
3. 照合判定処理：
   登録データと入力データの特徴同士の比較

指紋入力センサの比較


光学式
指
指紋
ミラー
プリズム
LED
レンズ
CCD光センサー
(a)光学方式
距離d
指数
電極
二つの電極と指で構成されるコンデンサの容量は距離dによって変わる.
指紋の凹凸をコンデンサ容量の差として検出
(b)静電容量方式

照合アルゴリズムの比較

- 指紋照合アルゴリズム：テンプレートと照合指紋を比較する判定方式
  - 指紋の大局的なパターンを比較する方式
    - フーリエ変換を用いた画像マッチング
    - 照合時の指の部分的な歪み、登録時との指の向きのずれや回転ひずみに弱い。
  - 指紋の局所的な特徴を比較する方式
    - テンプレートが小さく、高精度
    - 多くの商用指紋照合システムで実用化

照合アルゴリズムの比較

照合 アルゴリズム	マニューシャ方式	マニューシャ リレーション方式	チップマッチング方式
照合に 用いる情報	■特徴点の位置 ■特徴点の方向 ■特徴点の種類 ■指紋中心位置 ■指紋全体の方向	■特徴点の位置 ■特徴点の方向 ■特徴点の種類 ■リレーション ■指紋中心位置 ■指紋全体の方向	■特徴点の位置 ■特徴点の種類 ■コアの位置 ■チップ画像
テンプレート サイズ	250 Byte	400 Byte	500 Byte
利点	■回転に強い ■テンプレートサイズが小さい	■回転に強い ■マニューシャ方式に比べて精度が高い	■照合処理が軽い (ビット演算)
欠点	■チップマッチング方式に比べて処理が複雑	■チップマッチング方式に比べて処理が複雑	■回転に弱い
適合 システム	ICカード内保存+端末内照合型の指紋照合システム	指紋識別システム (AFIS)	ICカード内指紋照合型システム

指紋認証の脆弱性

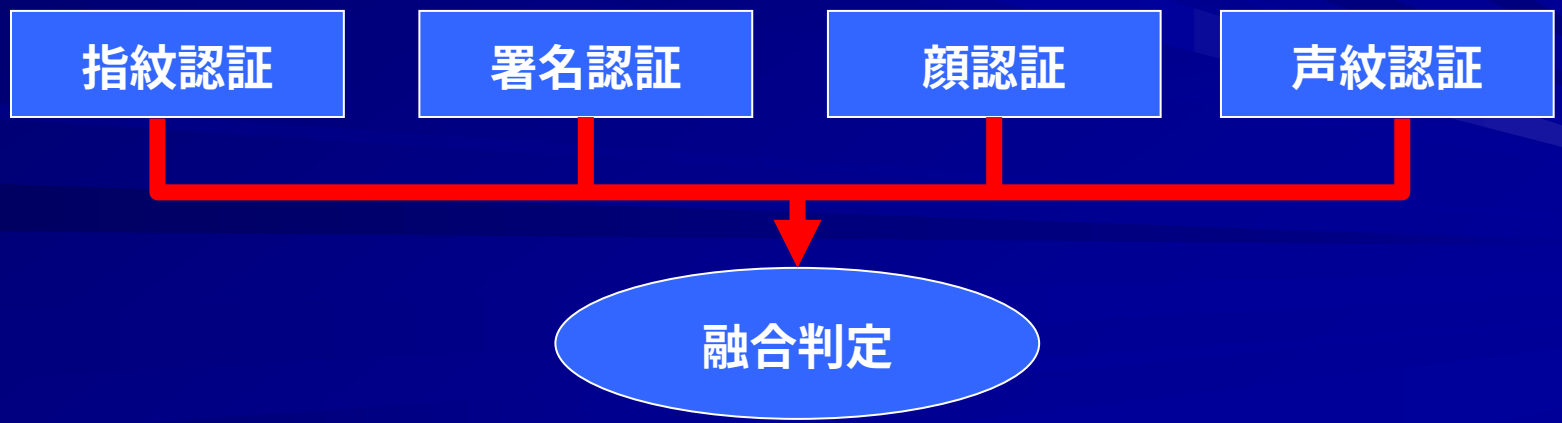
- 偽造問題は生体認証技術の根本的な問題
- 本人から直接的に採取したレプリカ指紋で実験
  - 現状レベルの指紋認証装置ではパスする確率が高い。
  - 人の指から直接作成：低コストで作成
  - 遺留指紋から直接作成：コストが高い
- 複合的な手段で実運用上はリスクを回避
  - 監視カメラによる不正発生時の事後追跡
  - ICカードの連携利用による複合認証
- 生態情報は遺留や非接触の獲得が可能で、センサが生体か偽造かを低コストで判定するのは難しい。

その他の生体認証技術

- 顔認証
- 虹彩認証
- DNAパターン認証
- 掌形パターン認証
- 網膜血管パターン認証
- 耳介パターン認証
- 掌静脈パターン認証
- 汗腺パターン認証
- 匂いによる認証
- 声紋認証
- 署名認証
- キーストロークによる認証
- 手指動作による認証

生体認証のマルチモーダル化

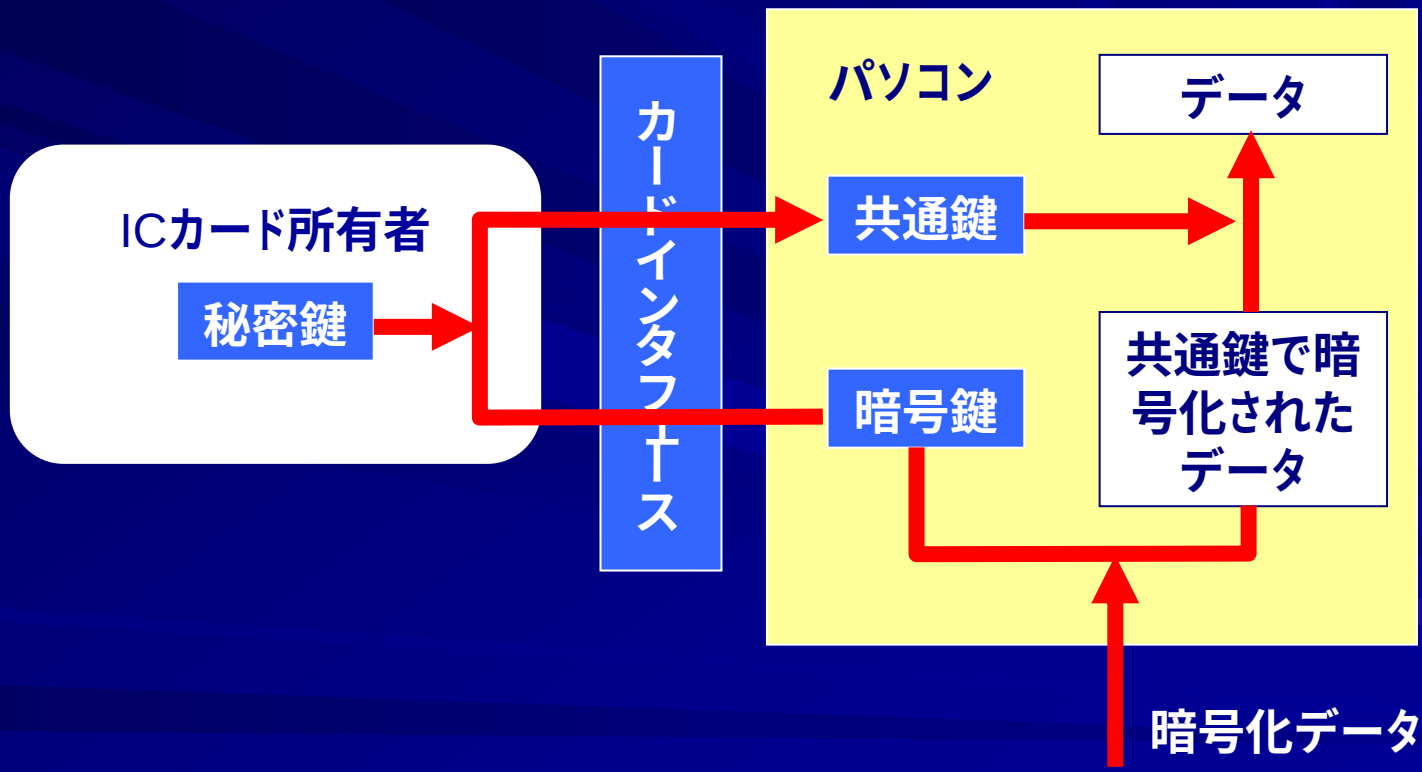
- 生体情報を複数用いて本人認証を行う技術
  - 本人拒否率や他人受入率などの精度改善
  - 識別を目的とした場合の処理時間の改善
  - 生体情報の偽造対策
  - 最適な生体情報を選択することによる利便性改善



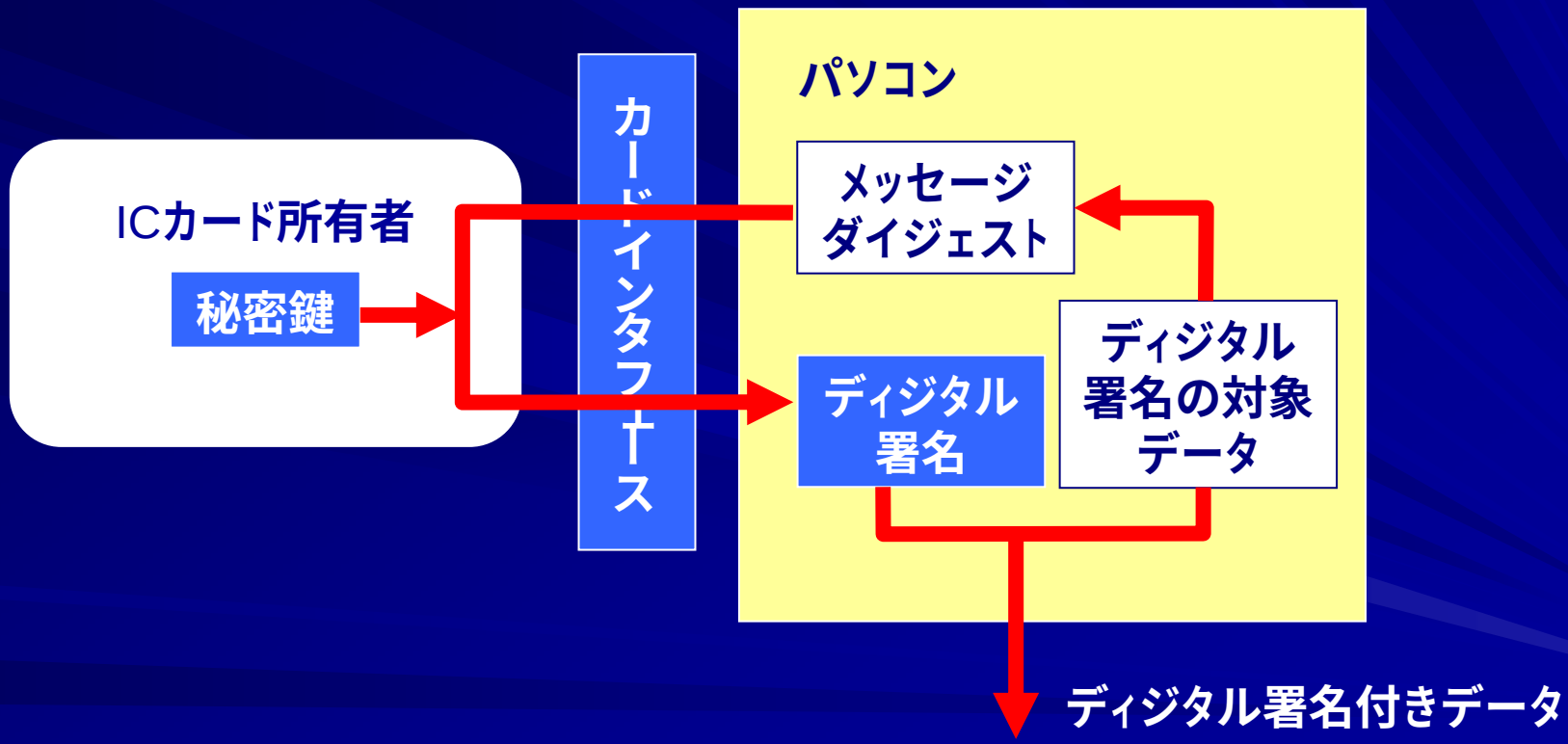
ICカードを用いた本人認証技術

- ICカードは携帯性と内蔵ICチップにより、カード自身により内部データの改ざんに対する防御が可能
- ICカードと生体認証技術はセキュリティを補完する関係
- 施設管理などの箱物管理、PKIなどにおける個人情報管理、e-コマースにおける本人認証などに展開
- ICカードに備わるセキュリティ機能
  - 暗号化のための鍵補完機能
  - ディジタル署名生成機能

暗号化のための鍵補完機能

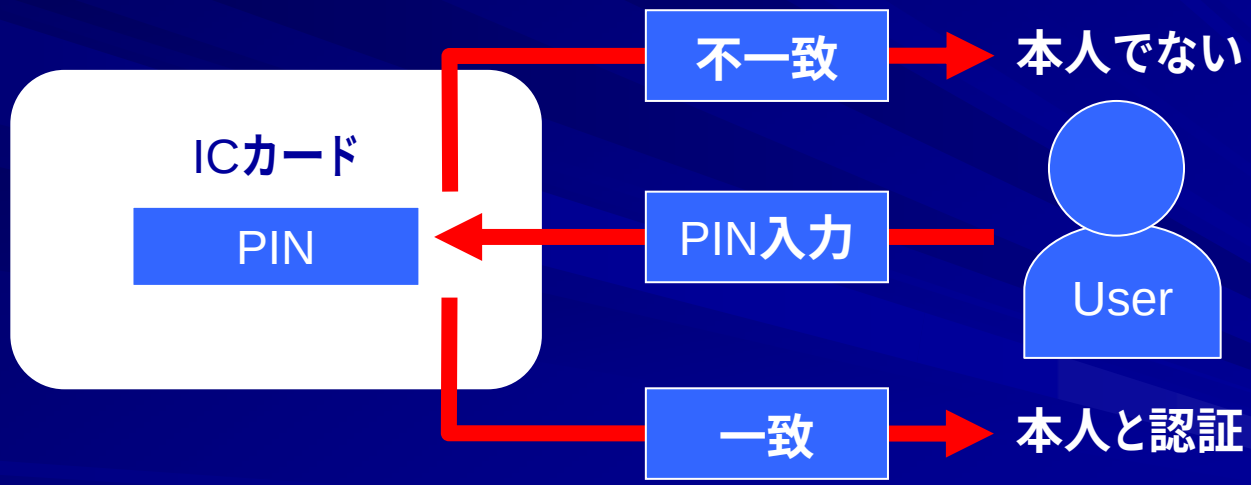


ディジタル署名生成機能



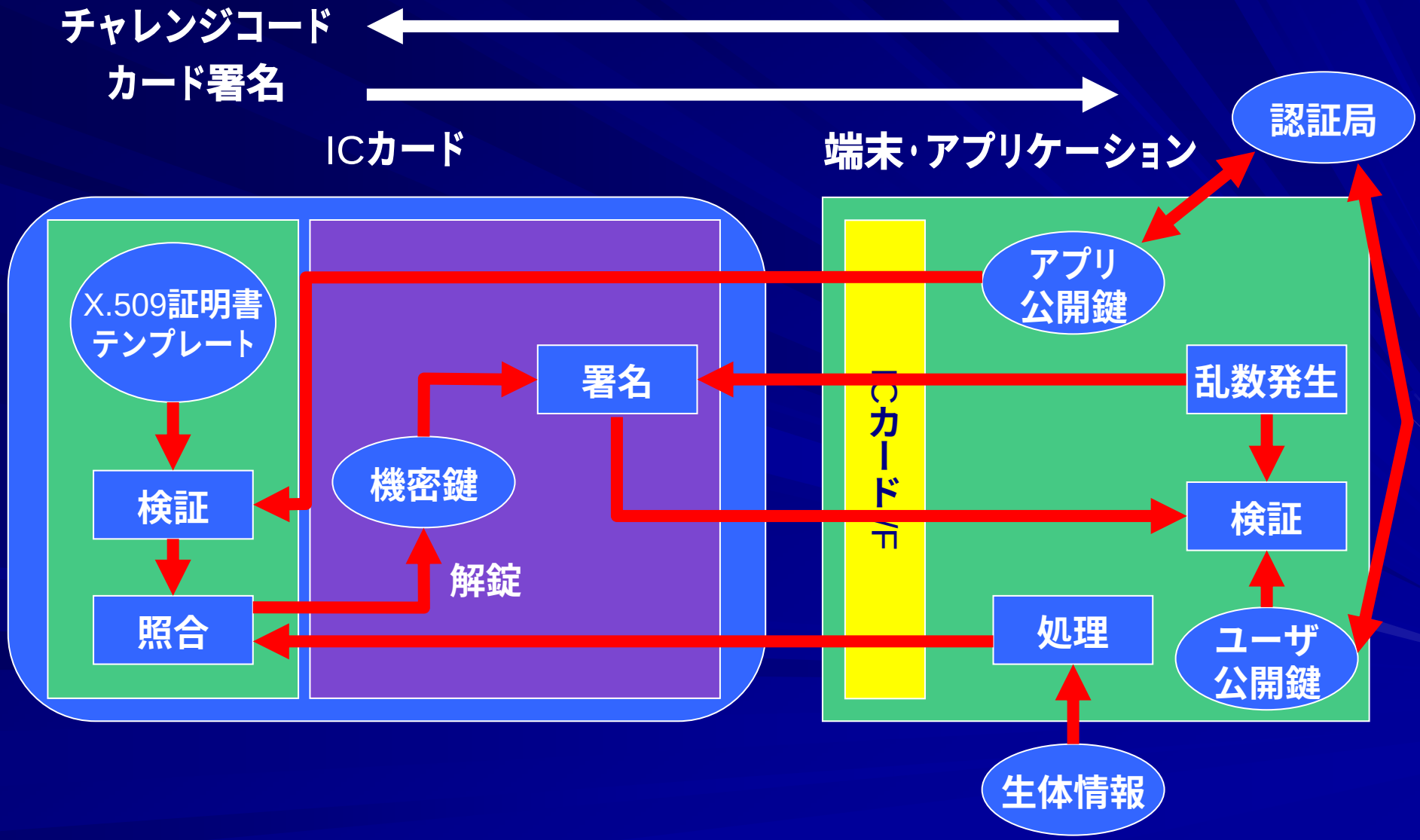
アクセス管理のための認証と内部データ保護機能

- ICカードにユーザが正当な所有者であるかどうかを認証する本人認証機能を持たせる。



  - カード所有者による不正防止機能
  - アクセス対象によるカード正当性の確認機能

ICカードを用いた生体認証モデル



社会基盤としての生体認証技術

- ヒューマンクリプト認証技術
  (Human Cryptography Authentication)
  生体認証を画像処理装置ではなく、セキュリティシステムとの位置付けで、暗号技術などとの組み合わせにより高い安全性と利便性を確保する生体認証技術
- ＰＫＩとの密接な関係
  - 実印に相当する秘密鍵や証明書の管理媒体の所有者認証
  - 管理された生体情報自身の真正性の証明
  - 生体認証自身を電子認証の基盤とする生体認証ＰＫＩの構築
- 次世代携帯電話における生体認証ＰＫＩシステム
- 法律との関係

おわり

本発表を網羅した詳細な情報をPDFでまとめてあるので、参考にしてください。

¥¥172.18.16.34¥documents