TOSHIBA
Leading Innovation

リモート生体認証のための システム的アプローチ

～ACBio (Authentication Context for Biometrics) ～

東芝ソリューション株式会社
IT技術研究所
岡田 光司

2007年3月9日

TOSHIBA
Leading Innovation

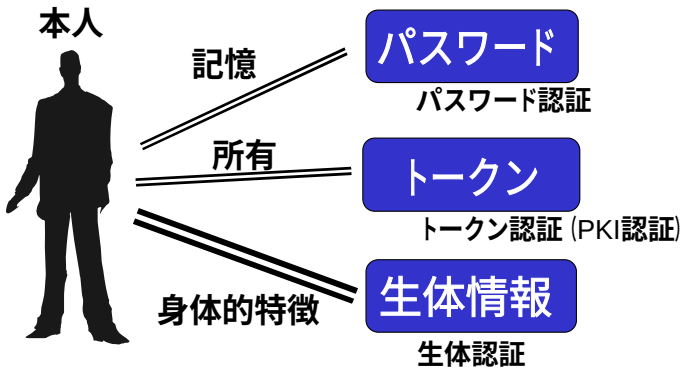
本人認証技術の比較

目次

ACBio (Authentication Context for Biometrics)
東芝ソリューションからの提案でISO/IEC JTC 1/SC 27/WG 5 において国際標準化を進めているリモート生体認証に関する情報セキュリティ技術

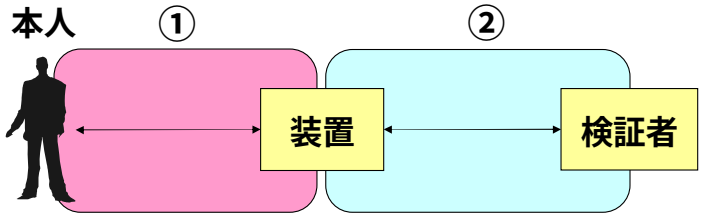
- リモート環境における生体認証の問題点
  - 本人認証技術の比較
  - リモート環境における生体認証の問題点
- リモート生体認証のためのシステム的アプローチ
  - ACBioとは
  - 標準化動向，技術動向

本人認証の種類



いずれも「本人」であることを認証したい

本人認証システム

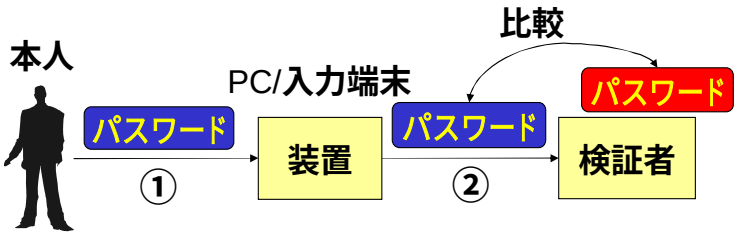


2つの視点で各認証方式を比較

- **利便性**
  生体情報 ＞ パスワード ＞ トークン
- **真正性** (Authenticity)
  - ① **本人 - 装置間の完全性** (Integrity)
  - ② **装置 - 検証者間の完全性** (Integrity)

※ 認証アルゴリズムの強度は一定と仮定.

パスワード認証

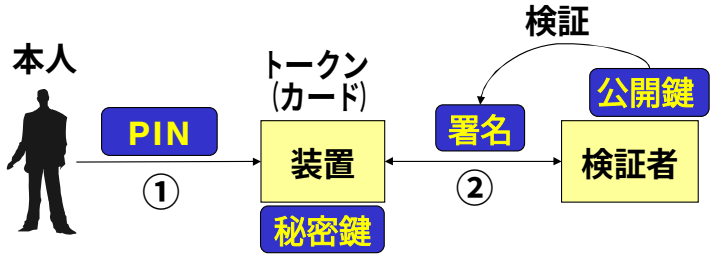


①の完全性: **低**
パスワードの保護は本人任せ. 複製が容易.

②の完全性: **インフラに依存**
装置・通信路の完全性. プロトコルの完全・健全性.

真正性: **低**
本当に本人が入力したパスワードかを検証できない.

PKI認証 (トークン認証)

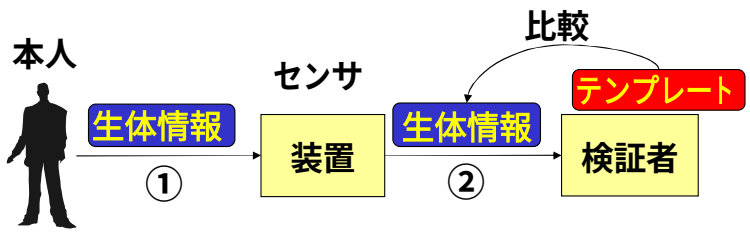


①の完全性: **中**
複製は困難. PIN等のパスワード認証で活性化.
しかし, トークン/PINの管理は本人任せ.

②の完全性: **高**
トークンの耐タンパ性. 安全な暗号プロトコル.

真正性: **中**
本当に本人がトークンを提示したかを検証できない.

生体認証



①の完全性: **高**
生体情報の複製は困難.
本人が生体情報を管理する必要がない.

②の完全性: **インフラに依存**
装置・通信路の完全性. プロトコルの完全・健全性.

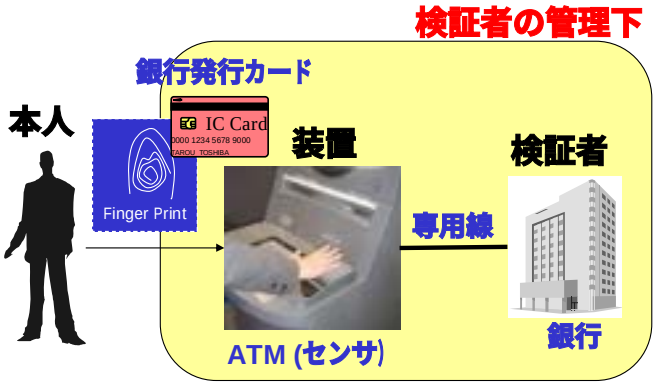
真正性: **高** (インフラが整っていることが条件)

認証技術の比較

	利便性		① 本人-装置	② 装置-検証者	真正性
パスワード認証	中		低	インフラ依存	低
PKI認証(トークン)	低		中	高	中
生体認証	高		高	インフラ依存	高 (条件付)

■ 生体認証のためのインフラ整備が重要

現状の生体認証システム



■ 全てのインフラは検証者の管理下にある
■ インフラが完全であることは検証者が事前確認済み

TOSHIBA
Leading Innovation

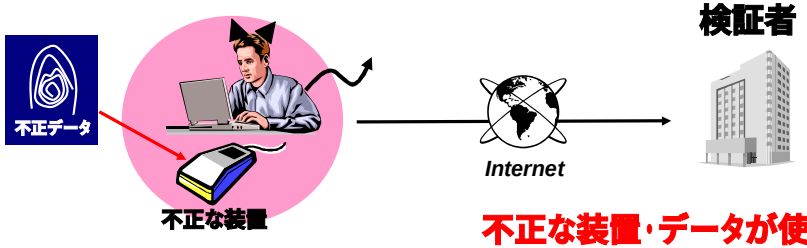
リモート環境における生体認証の問題点

リモート環境における生体認証の問題点

■ 3つの問題点
– インフラの完全性
ユーザ側で用意された装置により，オープンネットワーク上で認証が実行される．
– 相互運用性
様々な装置 (センサ，PC，携帯など) や方式が使用される．
– プライバシ
検証者毎にテンプレートが登録される．
オープンネットワーク上に生体情報が流れる．

インフラの完全性の問題

装置・通信路は検証者の管理外



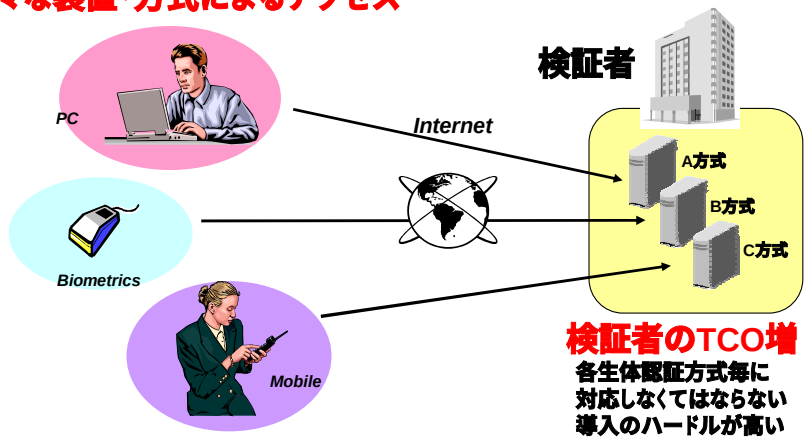
不正な装置・データが使用されても確認できない

問題1．各装置の完全性，通信路の完全性を検証できる仕組みが必要

機器認証とセキュア通信で十分か？

相互運用性の問題

様々な装置・方式によるアクセス

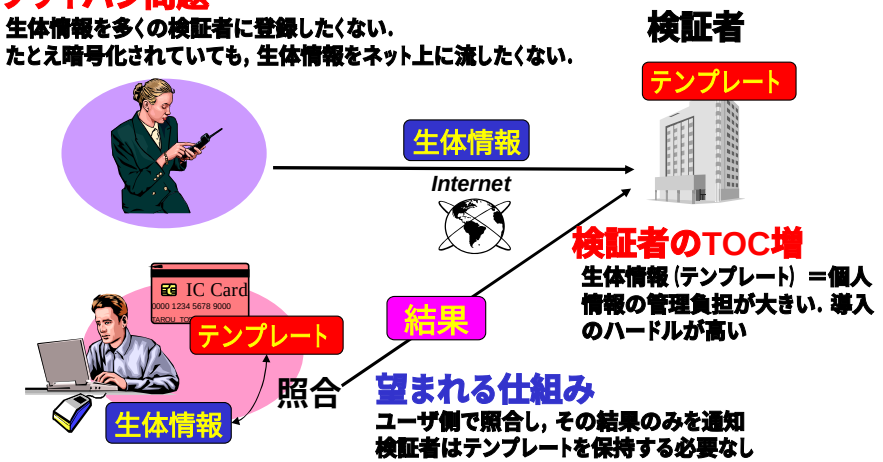


検証者のTCO増
各生体認証方式毎に
対応しなくてはならない
導入のハードルが高い

問題2．全ての装置・方式に対応できる統一の仕組みが必要

プライバシの問題

プライバシ問題
生体情報を多くの検証者に登録したくない．
たとえ暗号化されていても，生体情報をネット上に流したくない．



問題3．ユーザ側での照合（結果のみの送信）にも対応できることが望ましい

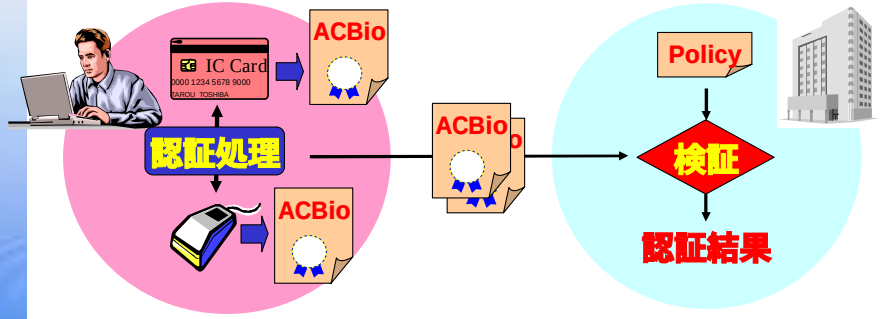
TOSHIBA
Leading Innovation >>>

リモート生体認証のための システム的アプローチ

ACBio（Authentication Context for Biometrics）とは

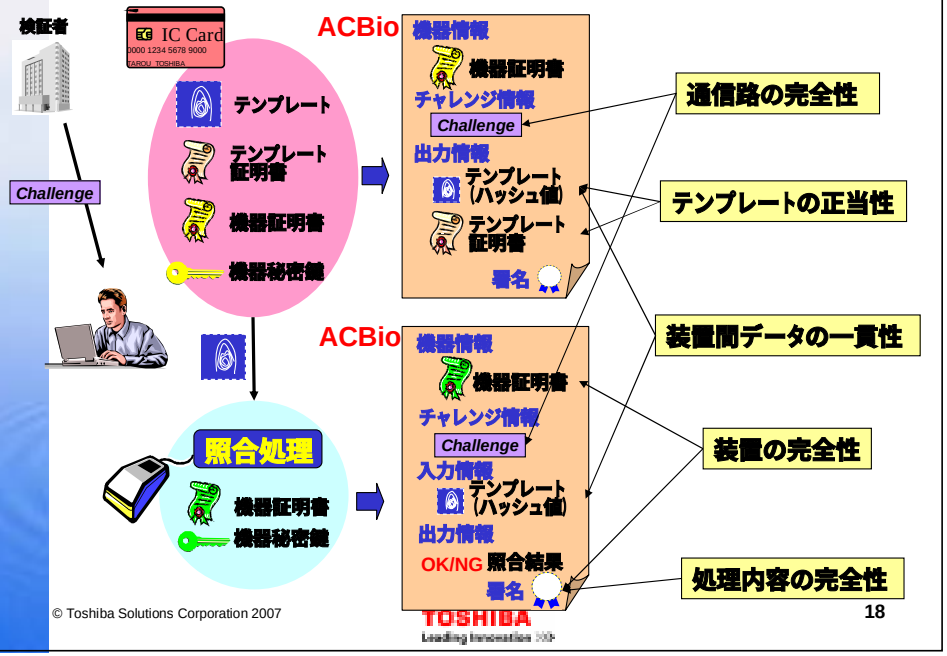
ACBioとは

■ 各装置が，実行した生体認証処理の結果を通知するための統一的なデータフォーマット（Authentication Context）を規定



装置・方式に非依存なデータフォーマットにより，検証者は全ての装置・方式に対応可能（問題2解決）

ACBioの解決策 STOC（STore on Card）モデルの例

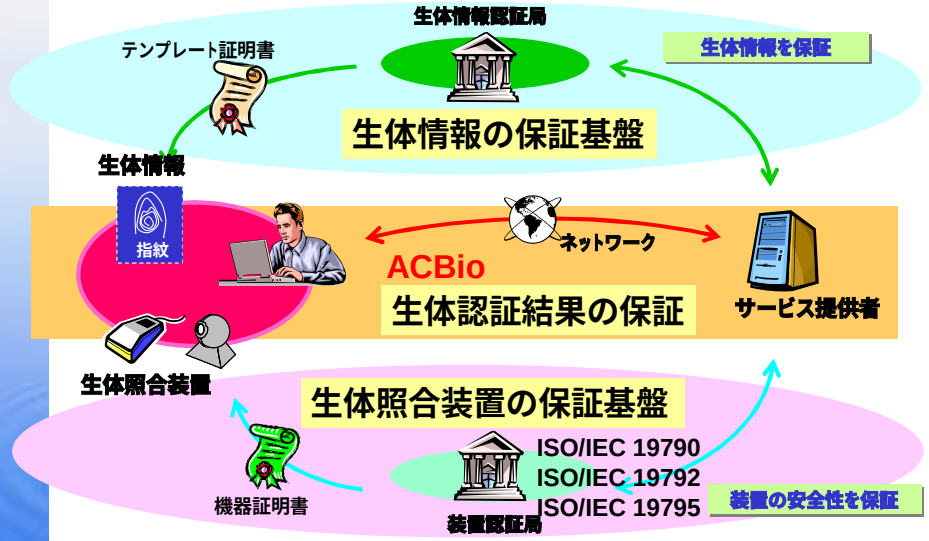


ACBioに望まれる要件と解決策

■ 装置・通信路の完全性が検証可能（問題1解決）
- 正しい精度・品質の装置が使用されたか？
  - 第三者機関の発行する，装置の精度・品質（耐タンパ性を含む）を保証した証明書である「機器証明書」を使用
  - 各装置の署名により機器認証
- 生体認証処理が完全に実行されたか？
  - 各装置が入出力データに対して署名生成（処理内容の完全性保証．装置間のデーター貫性保証）
  - チャレンジ・レスポンス方式の認証（通信路の完全性保証）

■ 生体情報を送信することなく検証可能（問題3解決）
- 使用されたテンプレートが正当なものか？
  - 登録機関の発行する，テンプレートのハッシュ値に対する証明書である「テンプレート証明書」を使用

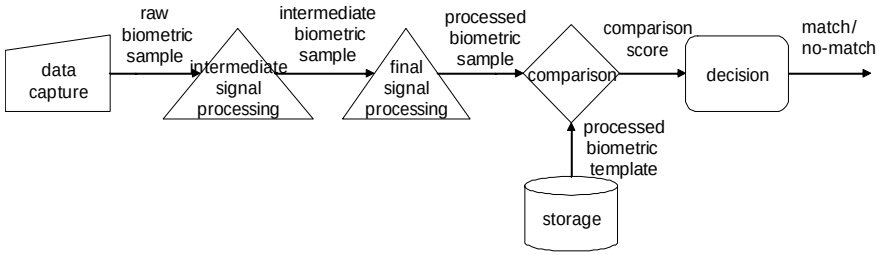
ACBioのフレームワーク



課題：他標準化との連携と，生体情報/装置認証局の設立が必要

ACBio詳細（1）生体認証のサブプロセス

生体認証は6つのサブプロセスから成ると定義



※storageに保持するデータが上図とは異なるプロセスレベルの場合もある（例：raw biometric template）

※複数のモダリティ（指紋，顔など）や複数のサンプル（複数の指の指紋）を扱うマルチモーダルフュージョンもある

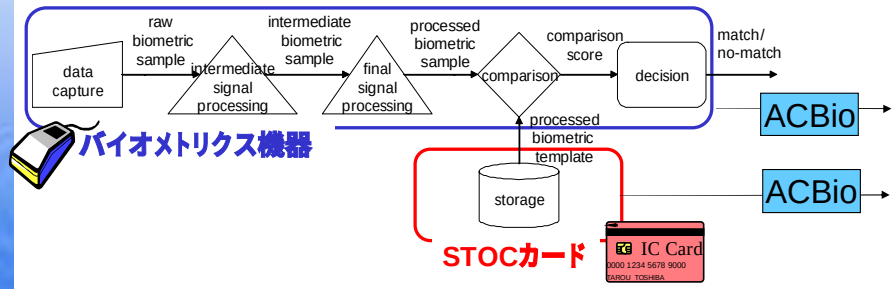
ACBio詳細（2）BPU

BPU (Biometric Process Unit)

生体認証の6つのサブプロセスのいくつかを含む独立した機器であって，連続するサブプロセス間のデータ授受がその中で行われる最大の単位

各BPU がその処理に対するACBioインスタンスを生成

下のSTOCモデルでは，2つのACBioインスタンスが生成される



ACBio詳細（3）構造

ACBioインスタンス：

- ACBioContentInformation型のSignedDataとして定義
- ACBioContentInformationはBPUの静的情報及び実行時の情報を含む

ACBioContentInformation		
	Version	
	BPU Information Block	
		BPU Certificate Referrer Information
		BPU Report Information
		BT Certificate Information
	Verifier Controlling Block	
		Control Value
	Biometric Process Block	
		Input Information[1]
		：
		Input Information[N]
		Output Information[1]
		：
		Output Information[N]

SignedData：
CMS（Cryptographic Message Syntax）で定義
署名はBPUの秘密鍵で生成

ACBio詳細（4）ACBioContentInformationのブロック概要

- BPU Information Block
  - BPUの静的情報
- Verifier Controlling Block
  - 検証者からのチャレンジ
    - 認証要求と返されるACBioインスタンスの対応を示し，再利用攻撃を防止する
- Biometric Process Block
  - BPUの実行時の情報
    - 特に，生体認証が複数のBPUによって実行される場合，入出力が正しく実行されているかを示す

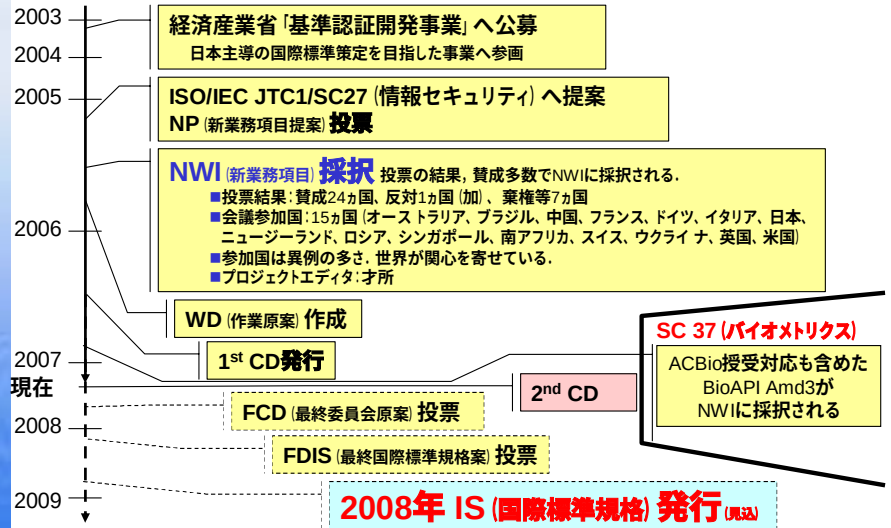
TOSHIBA
Leading Innovation

リモート生体認証のための システム的アプローチ

標準化・技術動向

ACBio国際標準化活動状況

ISO/IEC JTC 1/SC 27にて標準化中



TOSHIBA Leading Innovation

ACBioと他標準化活動の関係

- ISO/IEC JTC 1/SC 37（バイオメトリクス）
  - Special Group on ACBioが各ドラフトをレビュー
  - ACBioのBT certificateはCBEFFを利用
  - ACBioに関連し以下の3つのPJが成立
    - CBEFF part 4 (Security Block Format Specifications)
      - CBEFF Security BlockでACBioインスタンスを扱えるように
    - BioAPI Amendment 3（Security Amd.）
      - BioAPIにACBioインスタンスを授受するインタフェース追加
    - BioAPI Interworking Protocol (BIP) Amd.1
      - BIPをBioAPI Amd.3に対応
  - 精度評価の電子フォーマット作成で意見交換
- ISO/IEC JTC 1/SC 17（カードと個人識別）
  - ICカードでACBioインスタンスを生成できるかを共同検討
- ISO/IEC JTC 1/SC 27（情報セキュリティ）
  - 各種評価結果の電子フォーマット要求
    - ISO/IEC 19792（バイオメトリクスのセキュリティ評価）
    - ISO/IEC 19790（暗号モジュールのセキュリティ評価）
    - ISO/IEC 15408（製品・システムのセキュリティ評価）

TOSHIBA Leading Innovation

その他リモート生体認証標準化・技術

ITU-T SG 17

- X.tai（Telebiometrics Authentication Infrastructure）
  - Biometric template，Biometric algorithm certificate を定義
- X.tsm（Telebiometrics System Mechanism）
  - TLSのクライアント認証に生体認証を追加
  - データ授受にACBioをオプション利用

U.S. INCITS M1 – Biometrics

- OMB,NISTのe-Authentication Guidelineを受け，Ad Hoc Groupがリモート環境での生体認証に関するStudy Reportを公開．ACBioについても参照．

TOSHIBA Leading Innovation

TOSHIBA
Leading Innovation

Collaborative Innovation

東芝ソリューション株式会社