ZeroBIO研究プロジェクトワークショップ

バイオメトリクスセキュリティの課題

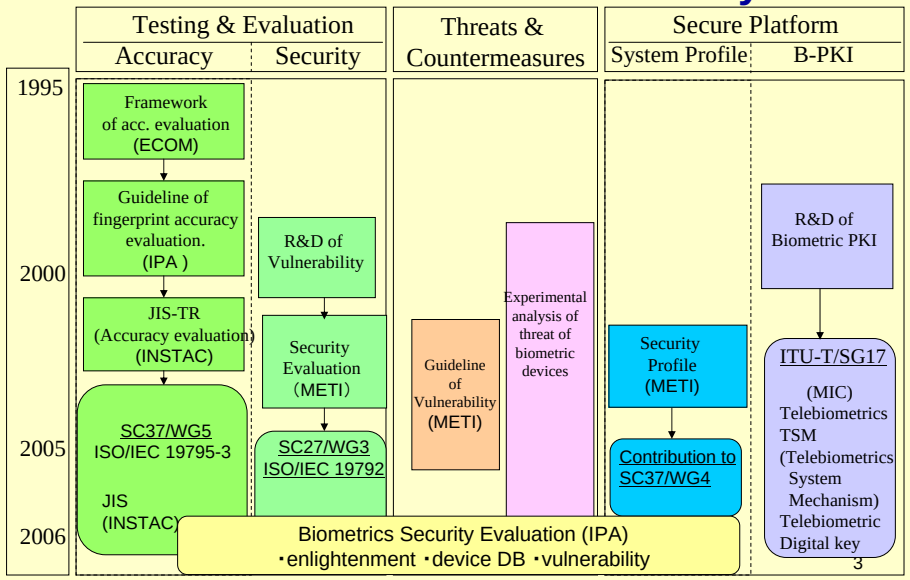
2007年3月9日

早稲田大学理工学術院
小松 尚久

目次

1. バイオメトリック認証の特徴
2. バイオメトリック認証の運用要件
3. バイオメトリクスの脆弱性
4. 諸外国の取り組み
   －韓国における研究開発－

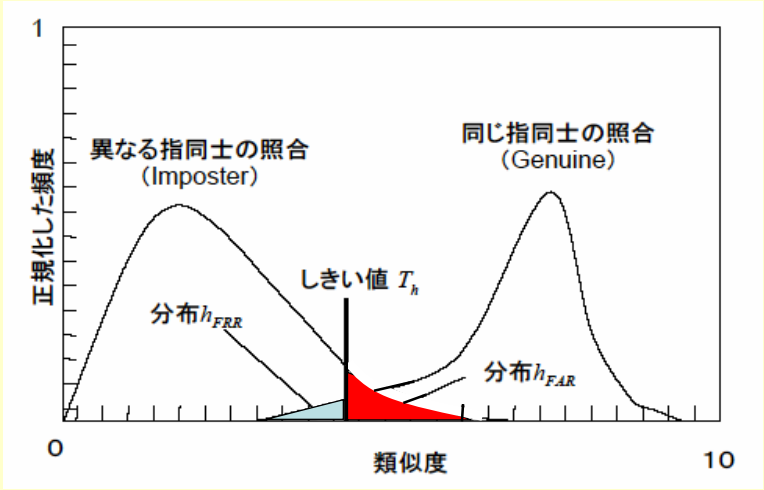
Japanese standardization activities related to biometrics Security



IPA : Information-technology Promotion Agency, Japan ECOM: Electronic Commerce Promotion Council of Japan MIC: Ministry of Internal Affairs and Communications METI: Ministry of Economy, Trade and Industry ISO: International Organization for Standardization ITU-T: ITU Telecommunication Standardization Sector INSTAC: International Study Center for Information Technology Standardization

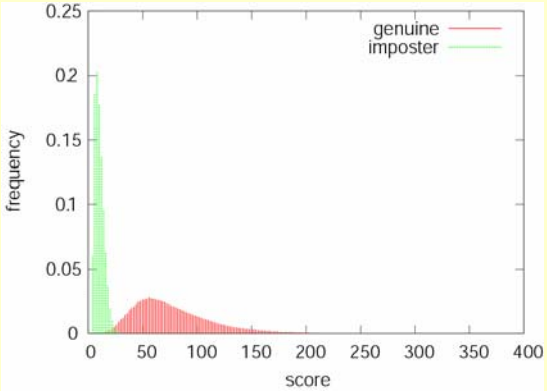
（SSR(産学戦略的研究フォーラム)講演資料「瀬戸教授資料」を参照）

1. バイオメトリック認証の特徴



類似度の分布

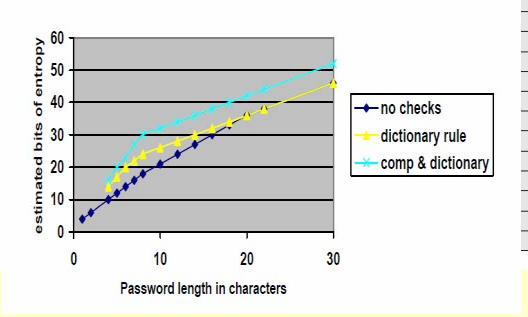
指紋照合スコアの分布



指紋データ	300枚×4指 （登録1指，照合3指で4通り）
照合アルゴリズム	NFIS2 (NIST Fingerprint Image Software)

Estimated Password Guessing Entropy in bits vs. Password Length

Length Char.	User Chosen 94 Character Alphabet: No Checks	Dictionary Rule	Dict. & Comp. Rule	User Chosen 10 char. alphabet	Randomly Chosen alphabet	Randomly Chosen 94 char alphabet
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
					20.0	39.5
					23.3	46.1
					26.6	52.7
					33.3	65.9
					40.0	79.0
					46.6	92.2
					53.3	105.4
					59.9	118.5
					66.6	131.7
					73.3	144.7
					79.9	158.0
					99.9	197.2
					133.2	263.4



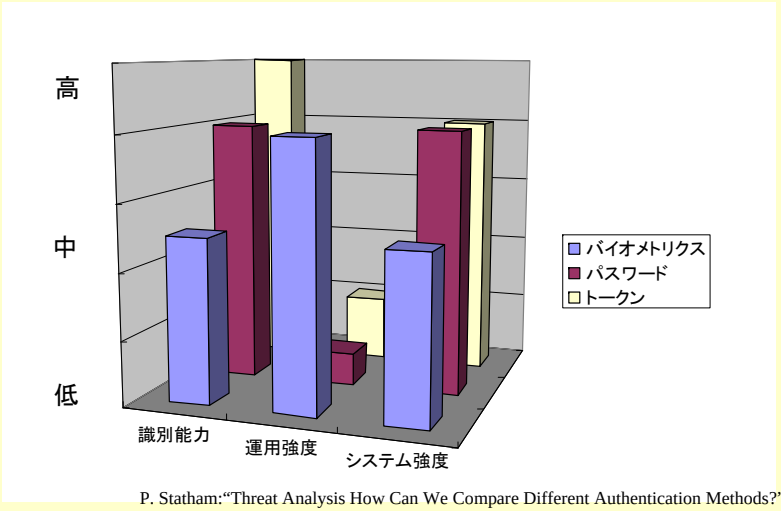
NIST Special Publication 800-63 Version 1.0.1

認証手段の比較

評価項目	パスワード	トークン	バイオメトリクス
識別能力	高 ●PWD空間が大 ⇒高いエントロピー	極めて高 ●PWDを保存	中～高 ●モダリティに依存 ●エントロピーはFARで制限
運用上の強度 ヒューマンエラー	弱 ●短いPWD ●推定容易なPWD ●メモ書き ●漏洩 ●社会工学的攻撃	弱 ●紛失 ●盗難 ●いつ紛失、盗難したかは分かる	強 ●本人の意識に影響しない ●管理の依存度が低い
システムの強度	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	極めて高 ●コピーが困難 （物理的条件） ●改ざんが困難 （物理的条件、暗号の適用） ●攻撃には高度な専門知識、技術が必要	中 ●なりすまし ●テンプレートの解析 ●登録データの取得

P. Statham:"Threat Analysis How Can We Compare Different Authentication Methods?", BC Conference (2005.9).

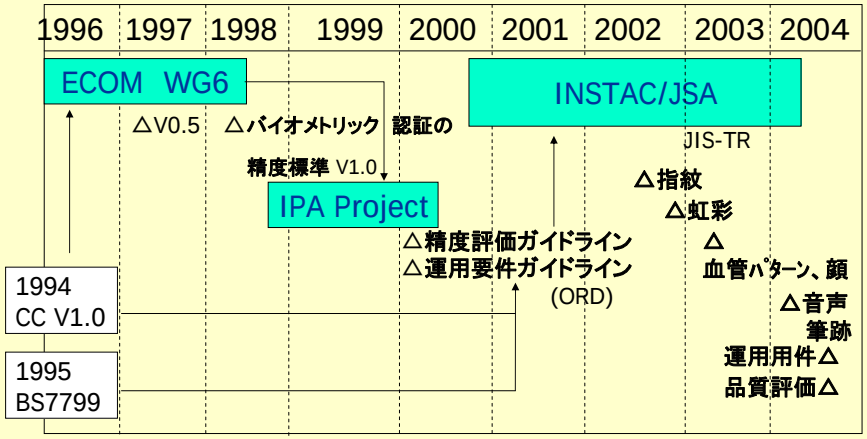
個人認証手段の比較



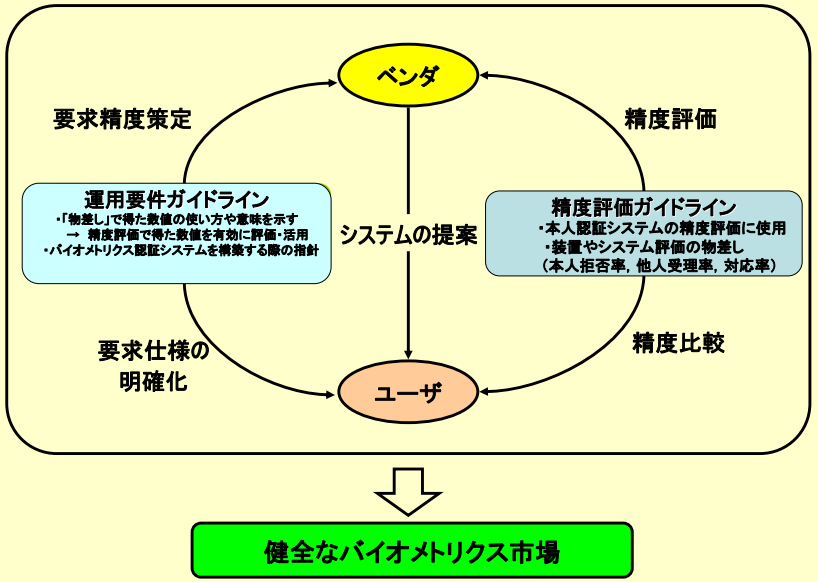
P. Statham:“Threat Analysis How Can We Compare Different Authentication Methods?”, BC Conference (2005.9).

2. バイオメトリック認証の運用要件

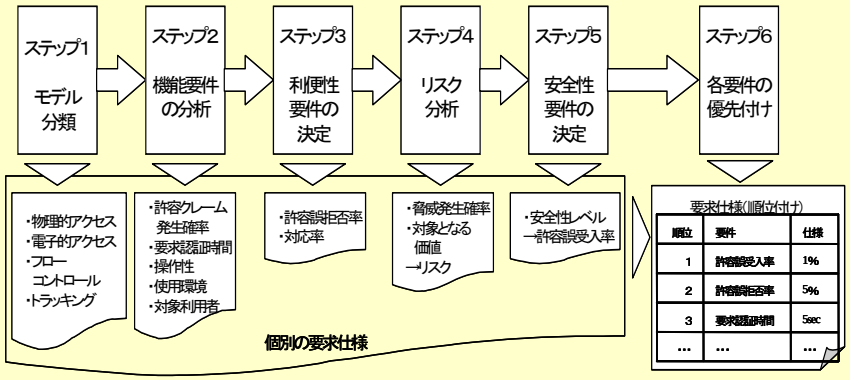
日本における標準化活動



ECOM：Electronic Commerce Promotion Council of Japan
IPA：Information-technology Promotion Agency,Japan
INSTAC：Information Technology Research and Standardization Center
CC：Common Criteria
BS7799：British Standard7799
ORD: Operating Requirements Decision



運用要件の決定フロー



機能要件分析

モデル	Example	考慮すべき機能要件
アクセスコントロール	[Physical] ・入退室管理 ・入国管理 ・Security box	・スピード(認証時間) ・対応率 ・使用環境 ・許容クレーム発生確率 ・操作性
	[Electronic] ・ネットアクセス ・DBアクセス	・操作性 ・対応率 ・スピード ・許容クレーム発生確率
フローコントロール	・ワークフロー ・リモートバンキング	・操作性 ・対応率 ・スピード(認証時間) ・許容クレーム発生確率
トラッキング	・勤怠管理	・操作性 ・対応率 ・使い勝手

安全性要件の決定

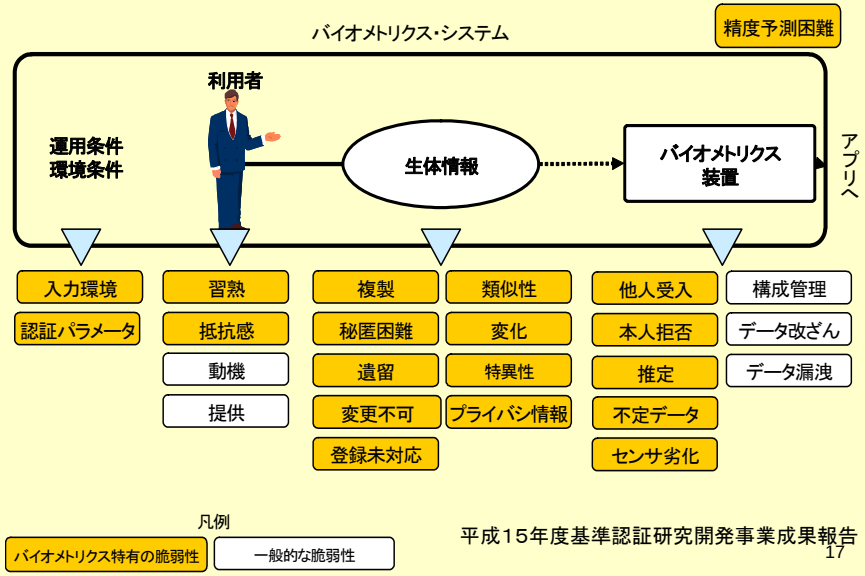
$$0.14\% = \frac{\text{許容損害額 300万円}}{\text{損害 100万円} \times 36.5\text{回/年} \times (\text{誰でもアクセス可能:1} \times \text{IDの盗み見可能:1} \times 60\text{回/10分}}$$

ATM:アクセス1,000件/日
認証可能時間10分
所要認証時間10秒/回
犯罪発生率 1/10,000

PFAR:許容他人受入率
PR:許容できるリスク
PV: 保護されている価値
IGIAF: 最初のゲートにおける不正アクセス頻度
IABMR: 不正認証阻止失敗率
IDR: ID既知率
NPAA: 認証可能回数

3. バイオメトリクスの脆弱性

バイオメトリクスの脆弱性分類



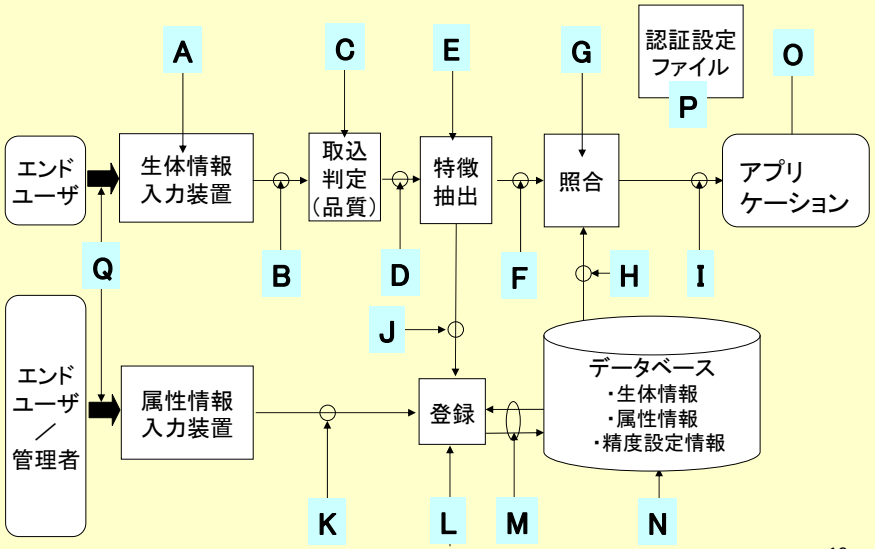
平成15年度基準認証研究開発事業成果報告

バイオメトリクス特有の脆弱性

- バイオメトリクス特有の性質に起因する脆弱性
  - 生体情報は意識的な秘匿が困難
    - パスワードやICカードは意識的に秘匿できる
  - 生体情報を無限に作り出すことはできない
    - パスワードや秘密鍵は作り変えが可能
  - 生体情報は入力の度に変化する
  - 生体情報は個人情報のひとつである
- 脆弱性の程度がバイオメトリクス特有の脆弱性
  - 生体情報の複製の難易度
    - パスワードはコスト0，ICカードはコスト大
  - 利用者の習熟による精度の変化
  - センサ（入力装置）の劣化による精度の変化
    - 汚れなどにより比較的短期間に精度劣化を引き起こす

三村氏（日立製作所）講演資料

バイオメトリクス認証のモデル例



IPA研究会資料

各プロセスで考えられる攻撃例

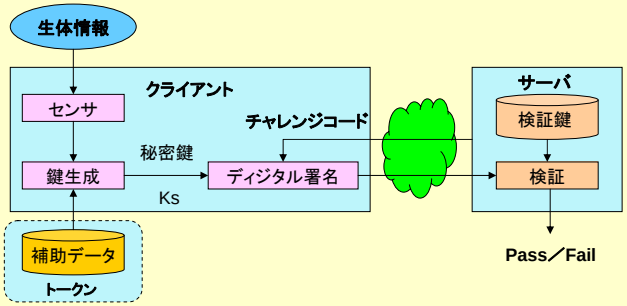
	脅威	事例
A	・偽の情報提示	・偽造物による照合
	・デバイスレベルでの再生	・遺留物利用，素子への直接入力
B	・生体情報の再生	・電子的な再利用
	・センサ情報の改竄	・電子的な改竄
C	・取込判定部の改竄	・偽造物の入力 ・低品質データの入力（誤一致しやすい） ・部分的なデータのみの入力（小面積）
D	・取込後の生体情報の再生・改竄	・電子的な再利用
E	・特徴抽出部の改竄	・特定条件で特定特徴データを出力するモジュール
		・他人と一致しやすいデータの出力
	・特徴抽出アルゴリズムの脆弱性	・特定条件で他人受入/本人拒否を起こす
F	・特徴データの不正変換・改竄	・特徴データの差し替え
		・特徴データの再利用
		・他人と一致しやすいデータとの差し替え

IPA研究会資料

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。

バイオメトリクス暗号のシステム構成要素と安全性評価のポイント



1. 補助データからの生体情報の再構築の困難さ
2. 補助データからのKsの推定の困難さ
   アルゴリズムによっては、ダミーデータの選択・決定方法に依存し、ダミーデータの量とのトレードオフとなる（例えば、Fuzzy vault）。
3. 補助データが他人に使われた場合にKsが生成される確率と、本人が生成できない確率
   FARとFRRのトレードオフと同様の関係。アルゴリズムによっては、Ksの鍵長にも依存。

磯部氏（日立製作所）講演資料を参照

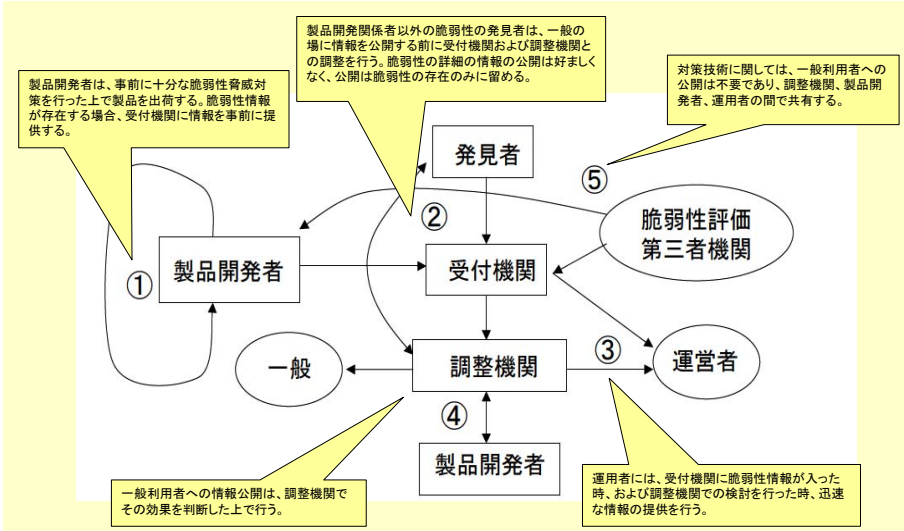
IPA バイオメトリクス・セキュリティ評価に関する研究会 (2006.3~)

- 最近のバイオメトリクス認証技術の応用状況は、局所的な入退室管理などでの利用から、多国間でのセキュリティ確保のためパスポートへの指紋採用、日常生活でのIT化に伴い銀行のATMでも「静脈認証」が開始されるなど、更に拡大傾向にある。
- 現在、バイオメトリクス製品はモダリティ毎に多くの製品があるが、製品を導入するために参考となる資料は、ベンダが作成したカタログに頼らねばならない状況である。現状では、ユーザは簡単に製品比較が行えない状況にある。
- このため、本研究会では、
  - 現状でバイオメトリクス認証技術や、これを用いた製品の実態を調査し、ユー ザがバイオメトリクス認証技術の特性等について、比較分析を可能とするデータベースのコンテンツ作成及び継続した情報更新方法等についてとりまとめる。
  - バイオメトリクス認証技術は、パスワード、暗号等を用いた認証技術と異なり、認証精度や本人認証のためのアルゴリズム等において、独特のセキュリティ上の課題がある。このため、本研究会では、バイオメトリクス・セキュリティの観点から課題と今後取り組むべき方向性についても検討する。

IPA: Information-Technology Promotion Agency
（情報処理推進機構）
http://www.ipa.go.jp/security/fy18/reports/biometric/index.html

IPA研究会における検討課題

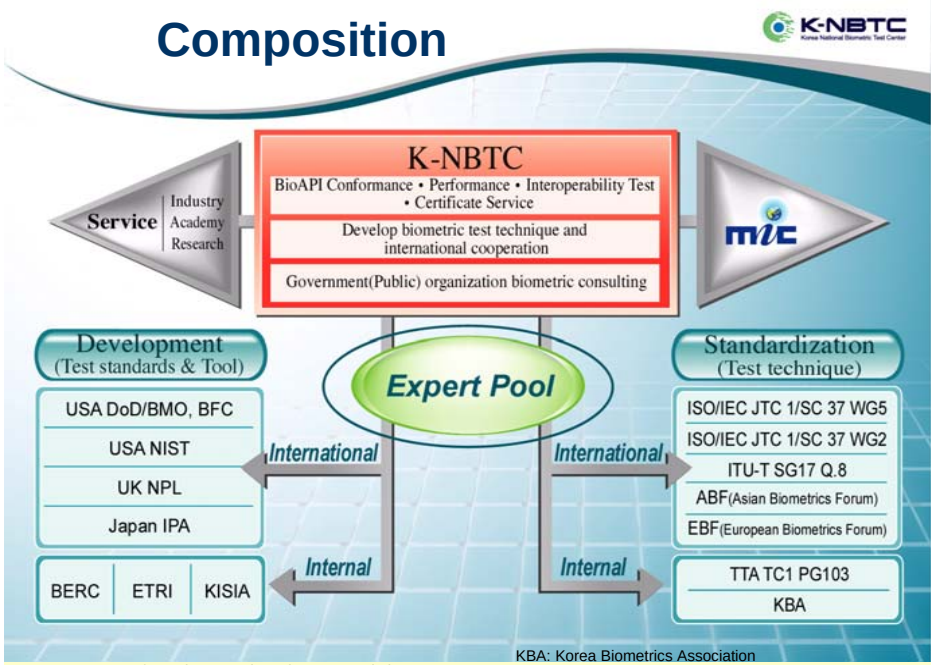
1. ユーザへのバイオメトリクス・セキュリティの普及に向けた取組み
2. バイオメトリクス製品データベースの構築・公開
3. ガイダンスや注意事項集などによるバイオメトリック情報の提供
4. 脆弱性情報の取り扱い
5. 第3者機関による精度評価



バイオメトリック製品に係る脆弱性関連情報取扱の概要

平成16年度経済産業省 産業技術研究開発委託事業報告書

4. 諸外国の取り組み
－韓国における研究開発－



KISIA: Korea Information Security Industry Association

KBA: Korea Biometrics Association
TTA: Telecommunication Technology Association of Korea

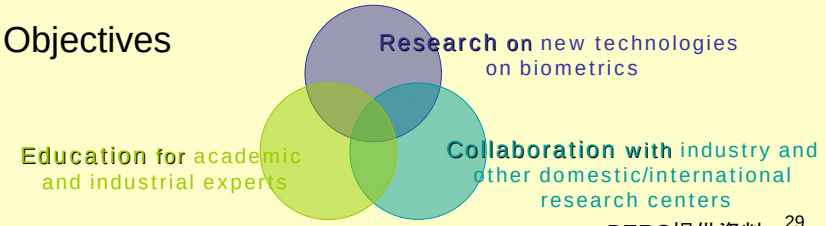
BERC Backgrounds

- History

  Established on July, 2002 as a government supported Engineering Research Center.

  ＊ERC (Engineering Research Center):
  Korea Science Foundation establishes 3~5 ERCs/year after evaluating proposals from all areas in engineering.
  (100万ドル/年の資金援助)

- Objectives



BERC提供資料

Research Collaboration

BERC

- Core Technologies for Biometrics
- Technologies for Biometric Information Security
- Performance Evaluation Technologies for Multimodal Biometrics

International

Research Center	Association
WVU(U.S.A)	B.C(U.S.A)
★NTU(Singapore)	★BSC(Japan)
★12R(Singapore)	AfB(U.K)
★HPU(Hong Kong)	BioApi(U.S.A)
MSU(U.S.A)	★ABW(Asia)
★UCSB(U.S.A)	
MGIC(Canada)	

Domestic

Research Center	Industry Sponsor	Korean Biometrics Association
ETRI	★Samsung Electronics	Univ. : 23
KISA	★LG Electronics	Industry : 32
★NISI	★Hyundae Info. & Tech.	Research Center : 4
★KIST	etc.(23)	

★ Already in collaboration

2nd stage Research Members (2005. 3~2008. 2)

AREA - I
Core Technologies for Biometrics

- **Item I : Fingerprint** — Kim, Jaihie (Yonsei Univ.); Cho, Sung-Bae (Yonsei Univ.); Kim, Hakil (Inha Univ.)
- **Item II : Iris** — Kim, Jaihie (Yonsei Univ.); Kang, Moon Gi (Yonsei Univ.); Park, Kang Ryoung (Sangmyung Univ.)
- **Item III : Face** — Sohn, Kwang Hoon (Yonsei Univ.); Byun, Hye Ran (Yonsei Univ.); Lee, Sangyoun (Yonsei Univ.); Kim, Daejin (Postech)
- **Item IV : Speech** — Youn, Dae Hee (Yonsei Univ.); Kim, Weon-Goo (Kunsan Univ.)
- **Item V : Multi-modal** — Prof. Toh (Yonsei Univ.)

AREA - II
Technologies for Biometric Information Security

- **Item I : Fake Detection** — Kim, Jaihie (Yonsei Univ.); Yi June Ho (Sungkyunkwan Univ.)
- **Item II : Watermarking** — Lee, Sangyoun (Yonsei Univ.)
- **Item III : Biometric Key /Changeable biometrics** — Park, Kang Ryoung (Sangmyung Univ.)

AREA - III
Performance Evaluation Technologies for Multimodal Biometrics

- **Item I : Multi-modal DB** — Kim, Hakil (Inha Univ.)
- **Item II : Multi-modal Algorithm** — Prof. Toh (Yonsei Univ.)

From 6 Universities
21 Research Projects

Professors(12), Post-Doc.(2)
Ph.D(29), MS(37) candidates

BERC提供資料

Area II : Technologies for Biometric Information Security

- Fake Biometric Detection
- Biometric watermark
- Biometric Code

Current Method

Low performance fake biometric detection

Covert countermeasures which raise the uncertainty about the safeness of biometrics system

Problems

Cannot detect the fake Biometric attacks (e.g. gummy finger, contact lens iris, video replayed face, etc)

Objectives

Development of high performance and real-time fake biometric detection method, which can increase the safeness and credibility of biometric system

BERC提供資料

Area II ：Technologies for Biometric Information Security

Fake Biometric Detection

Biometric watermark

Biometric Code

Current Method

Watermark algorithm for conventional image contents

Problems

- The recognition performance may be degraded using the previous watermark algorithm
- The inserted watermark is easily corrupt by simple blurring attack

Objectives

- Development of watermark algorithm for biometric information authentication
- Development of watermark algorithm, which can maintain recognition performance
- Development of watermark algorithm robust to various attacks such as cropping and blurring

BERC提供資料

Area II ：Technologies for Biometric Information Security

Fake Biometric Detection

Biometric watermark

Biometric Code (Cancelable Biometrics)

Current Method

Biometric code generation based on identification with enrolled data

Problems

- The security problem of enrolled data (stolen and non-cancelable)
- Variant biometric code generation according to recognition environment such as illumination, focusing etc.

Objectives

Cancelable biometrics

-> Can revoke the stolen biometric data and reissue it

Invariant biometric code generation without enrolled data

-> Private key for PKI algorithm

-> Can be used directly as a "pointer" to an identity, rather than exhaustively searching through a large DB for best matching

-> Can be used as simple password in conventional authentication system

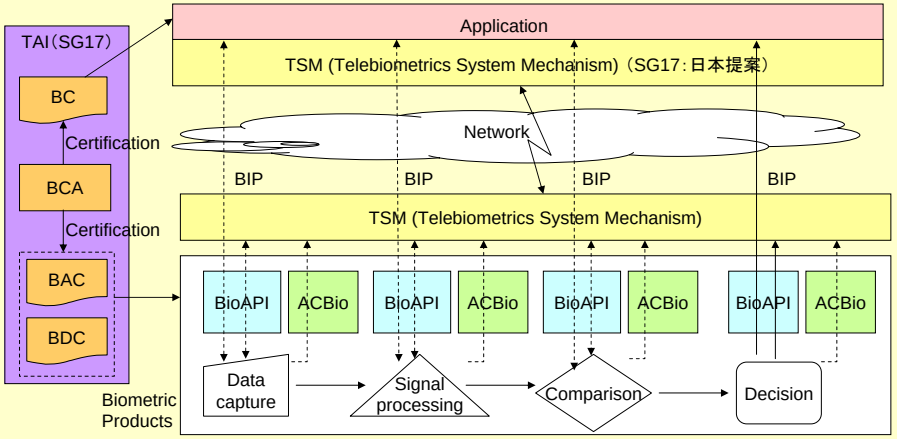
BERC提供資料

バイオメトリクスセキュリティに関する課題

- 脅威・攻撃分析と対策・評価
  生体検知、IT技術応用、運用
- テンプレートプロテクション
  キャンセラブルバイオメトリクス、バイオメトリック暗号、非対称バイオメトリック認証
- 認証精度評価
  評価用データベース、認証手段の相互評価
- バイオメトリクスセキュリティの啓発
  バイオメトリクスに対するユーザの正しい理解
- 公的ルール、民間ガイドライン
  プライバシー保護、脆弱性関連情報の管理と公開

Telebiometrics標準化課題の位置付け

- ISO/IEC JTC1 SC27、SC37では標準プロダクト向けの仕様策定が目的。
- オープンあるいはキャリアに跨った生体認証向けの標準策定はSG17課題8以外にない。
- 研究段階の生体認証技術を利用した通信環境向けの提案への対処が急務。



BioAPI: Biometrics Application Program Interface, BIP: BioAPI Interworking protocol, ACBio: Authentication Context for Biometrics, TAI: Telebiometrics Authentication Infrastructure, BCA: Biometric Certification Authority, BC: Biometric Certificate, BAC/BDC: Biometric Algorithm/Device Certificate

磯部氏（日立製作所）講演資料

人を対象とする研究等倫理規程

（２００６年８月１４日規約第０６－２０号）

《所管：研究支援課長》

人を対象とする研究等倫理規程（２００５年１月２８日規約第０４－４４号）の全部を改正する。

第１章　総則

（目的）

第１条　この規程は、1964年６月に開催された第18回世界医師会総会において採択されたヘルシンキ宣言の趣旨に鑑み、生存している人、胎児または死体から採取した臓器、組織、細胞、体液、血液、排泄物、タンパク質、ＤＮＡ、ＤＮＡ配列情報、動物性集合胚またはヒトＥＳ細胞その他ヒト（生物の種としての人をいう。以下同じ。）に由来する試料（以下「ヒト由来試料」という。）を利用した研究および実験（以下「研究等」という。）その他の人を対象とする研究等（以下「人を対象とする研究等」という。）について、研究等の対象となる者（以下「被験者」という。）の人としての尊厳および基本的人権を尊重し、人を対象とする研究等で取得される個人情報を保護し、ならびに人を対象とする研究等の被験者によるインフォームドコンセント（十分な説明に基づく自由な意思による同意をいう。以下同じ。）を得ることを徹底するとともに、本大学に隣接する地域住民の安全の確保のための措置および情報の積極的な開示を行うことを定め、人を対象とする研究等が倫理的、法的、社会的に適正に実施されることを確保することを目的とする。

（大学の責務）

第２条　大学および箇所長は、前条の目的を達成するために必要な措置を講じなければならない。

http://www.waseda.jp/rps/LOCAL/hito/hitotetu.htm