

生体認証の現状と個人情報保護の 観点からの整理

2004年 10月 15日

早稲田大学理工学部

<http://www.kom.comm.waseda.ac.jp/>

小松 尚久

目次

- . 生体認証の現状
- . 国際標準化委員会及び欧米における取組み
- . 個人情報保護の観点からみた生体認証
- . 高度な管理が必要な生体認証情報の定義についての検討ポイント
- . 安全管理に係る上乘せ措置として考えられる内容

生体認証の現状

1. 銀行のキャッシュカードの暗証番号を何にしているのかの調査

分野	人数	うちわけ		分野	うちわけ	
誕生日	89人 (46%)	工夫のない誕生日	53人	その他	2001	映画のタイトル (1941も)
		誕生日をアレンジ	14人		1568	身長156.8 cmだから
		家族の誕生日	10人		4789	名前画数。4画7画8画9画
		他人の誕生日	12人		1425	カードを作った時刻 14時25分
電話番号	34人 (18%)	自宅	17人		3612	番地。3丁目6番12号
		実家	11人		1789	フランス革命
		彼、彼女	3人		1467	人の世むなし応仁の乱
		その他	3人		1134	文化放送
受験番号	7人 (4%)	大学受験と模試の受験			0101	丸井
出席番号	5人 (3%)	3419	3年4組19番		0480	民法480条 (受取証書の持参人への弁済)
語呂合わせ	13人 (7%)	4126	(4人) ヨイフロ		7777	気分で
		1168	ビビンバ			
		2180	ニイハオ			
		909	ワクワク			
		439	与作			
		3594	三国志			
		168	イロハ			
9602	苦勞人 など					

(のべ194人調査)

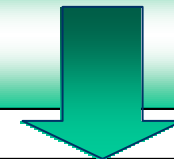
2. 個人認証のニーズ

社会環境変化	社会環境変化に応じた社会・個人・企業の動向	システム化が期待できる分野	個人認証のニーズ
高齢化	<ul style="list-style-type: none"> 医療相談ニーズの拡大 疾病者の在宅看護 	<ul style="list-style-type: none"> 遠隔医療, 遠隔健康管理 疾病者監視 (看護) 	<ul style="list-style-type: none"> 医療情報の広域管理
国際化	<ul style="list-style-type: none"> 海外とのコミュニケーション増大 (訪問・電話) 在日外国人の増加 外国人雇用の増大 (知識人・労働力) 海外事務所との遠隔会議 国際分業化進展、物流、情報の拡大 コンピュータシステム、オフィスの24時間利用 	<ul style="list-style-type: none"> テレビ会議 海外情報提供 自動翻訳 グローバルネットワーク エレクトリックコマース 24時間対応ビル入退管理 	<ul style="list-style-type: none"> 課金 (個人課金) 企業内データへのアクセス リモートアクセス利用者確認 利用資格証明
キャッシュレス化	<ul style="list-style-type: none"> 電子マネー カードの多様化・機能統合 	<ul style="list-style-type: none"> 電子取引、電子決裁 預金管理の統合 	<ul style="list-style-type: none"> カードの高機能化
コミュニティ化	<ul style="list-style-type: none"> 地域情報メディアの普及 	<ul style="list-style-type: none"> コミュニティ情報案内 生涯教育 	<ul style="list-style-type: none"> 個人情報のネットワーク管理 サービス提供に関する決済
企業の組織構造の変化	<ul style="list-style-type: none"> 企業活動に関する情報管理の進展 	<ul style="list-style-type: none"> 企業内情報伝達 マルチメディア分散DB 	<ul style="list-style-type: none"> 企業内データへのアクセス 利用資格証明
その他	<ul style="list-style-type: none"> 在宅選挙 教育機関の連携、地域との結びつき モバイルオフィスの普及 	<ul style="list-style-type: none"> 電子投票 遠隔教育 テレワーク 	<ul style="list-style-type: none"> 身分証明 個人情報の管理

3. ユーザ認証手段とパラメータ

知識	所有	個人の特徴	
		身体的特徴	身体的特性
暗証番号、パスワード	鍵 IDカード	指紋、顔、虹彩、網膜、掌形	筆跡、声、キーストローク
忘れる危険性	紛失する可能性	時間の経過等により特徴が変わる可能性	

登録データ $\stackrel{?}{=}$ 入力データ



登録データ	個人の特徴 " ?
入力データ	個人の特徴

登録データ $\stackrel{?}{=}$ 入力データ

4 .生体認証 = バイオメトリクスによる個人認証 (biometrics=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

(参考)"Automatically recognizing a person using distinguishing traits
(a narrow definition)"

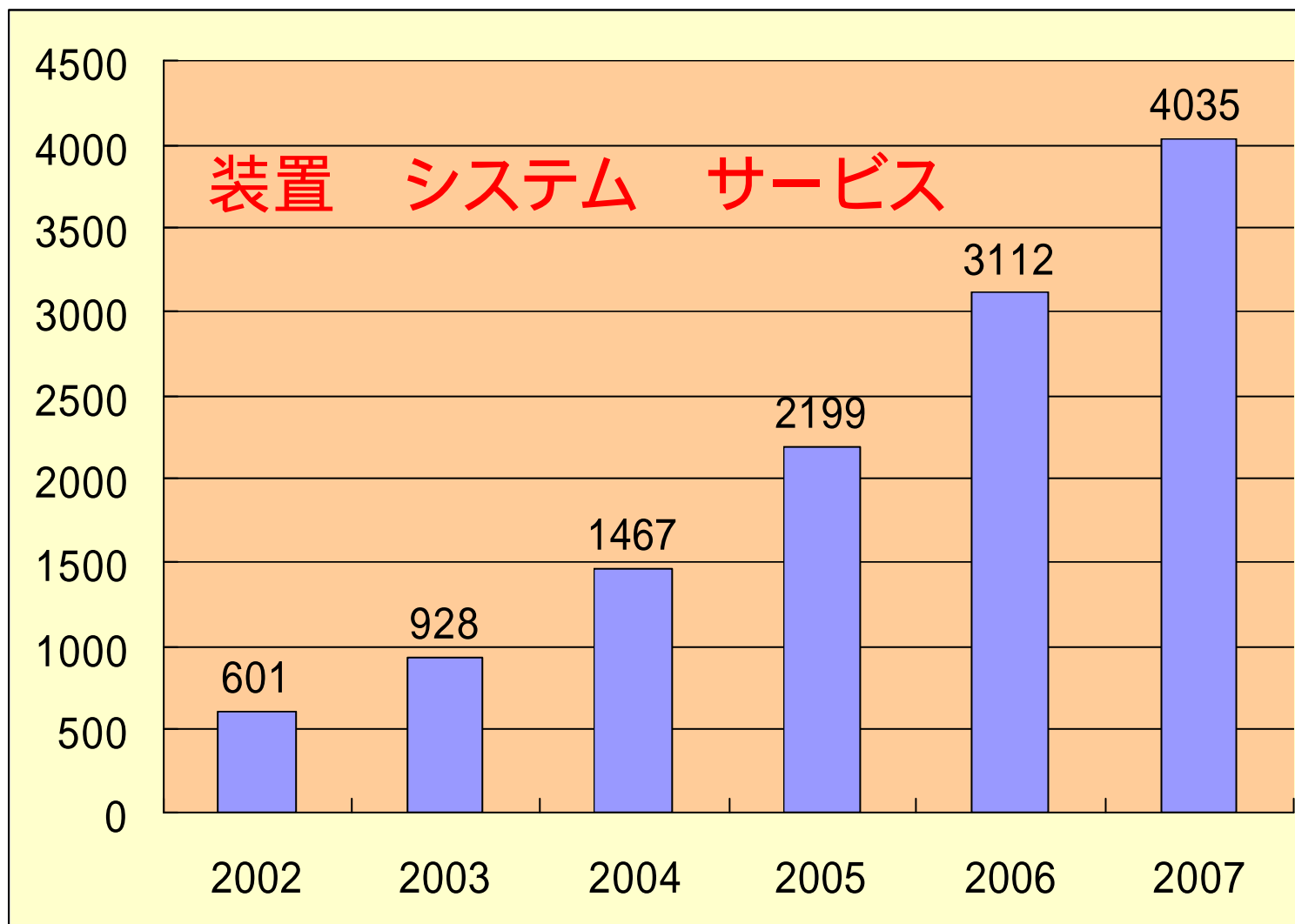
(The Biometric Consortium (<http://www.biometrics.org/>))

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

5. 生体認証の市場規模

2002-2007 (10⁶\$)



6. 生体認証の研究事例と特徴

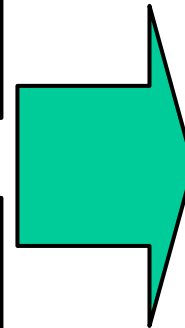
	パラメータ	特徴	課題
指紋	<ul style="list-style-type: none"> 特徴点 (マニューシャ) の位置 リレーション 	<ul style="list-style-type: none"> 万人不同, 終生不変 犯罪捜査での利用 	<ul style="list-style-type: none"> 指紋画像の品質 衛生面の確保 社会的な受容
網膜	<ul style="list-style-type: none"> 毛細血管パターン 	<ul style="list-style-type: none"> 万人不同, 終生不変 コピーが困難 	<ul style="list-style-type: none"> 眼底撮影と同様の専用装置が必要
虹彩	<ul style="list-style-type: none"> 瞳孔の開きを調節する筋肉のパターン 	<ul style="list-style-type: none"> 万人不同, 終生不変 眼球内部の疾病等の影響がない 	<ul style="list-style-type: none"> 睫毛の影響
血管パターン	<ul style="list-style-type: none"> 静脈パターンの直接照合 静脈の分岐点, 方向 	<ul style="list-style-type: none"> 非接触で認証可能 心理的抵抗が少ない 	<ul style="list-style-type: none"> 体毛, 脂肪層の影響
掌形	<ul style="list-style-type: none"> 掌の幅, 厚さ 指の長さ等 	<ul style="list-style-type: none"> 操作が容易 	<ul style="list-style-type: none"> 信頼性の確保 衛生面の確保
顔	<ul style="list-style-type: none"> 主成分分析を用いた固有顔 目, 口, 鼻の位置や形状等 	<ul style="list-style-type: none"> 非接触で認証可能 心理的抵抗が少ない 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> スペクトル包絡 ピッチ, 発音レベル, 発声, 速度等 	<ul style="list-style-type: none"> 非接触で認証可能 心理的抵抗が少ない テキスト依存型 	<ul style="list-style-type: none"> テキスト独立, テキスト提示型の実用化 時間的な変化 体調の影響
筆跡	<ul style="list-style-type: none"> 筆順, 筆速, 筆圧等 	<ul style="list-style-type: none"> 心理的抵抗が少ない 操作が容易 (小型タブレット) テキスト依存型 	<ul style="list-style-type: none"> テキスト独立, テキスト提示型の実用化 時間的な変化 偽筆対策

国際標準化委員会及び欧米における取組み

1 - 1 . 国際標準化委員会設置の背景

➤ 9月11日米国同時多発テロ
ホームセキュリティの観点から
生体認証技術の見直し

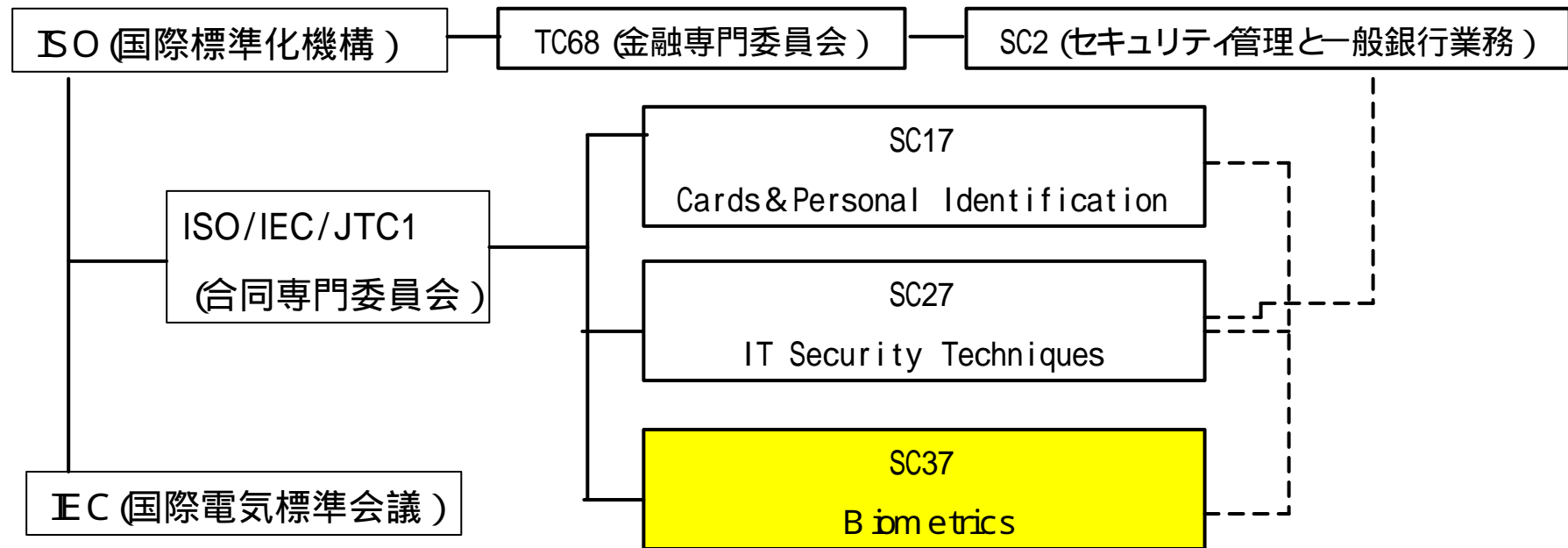
➤ 生体認証装置の低価格化と普及
個人利用市場への普及



国際標準化組織
ISO / IEC JTC1 /
SC37
“Biometrics”
生体認証」

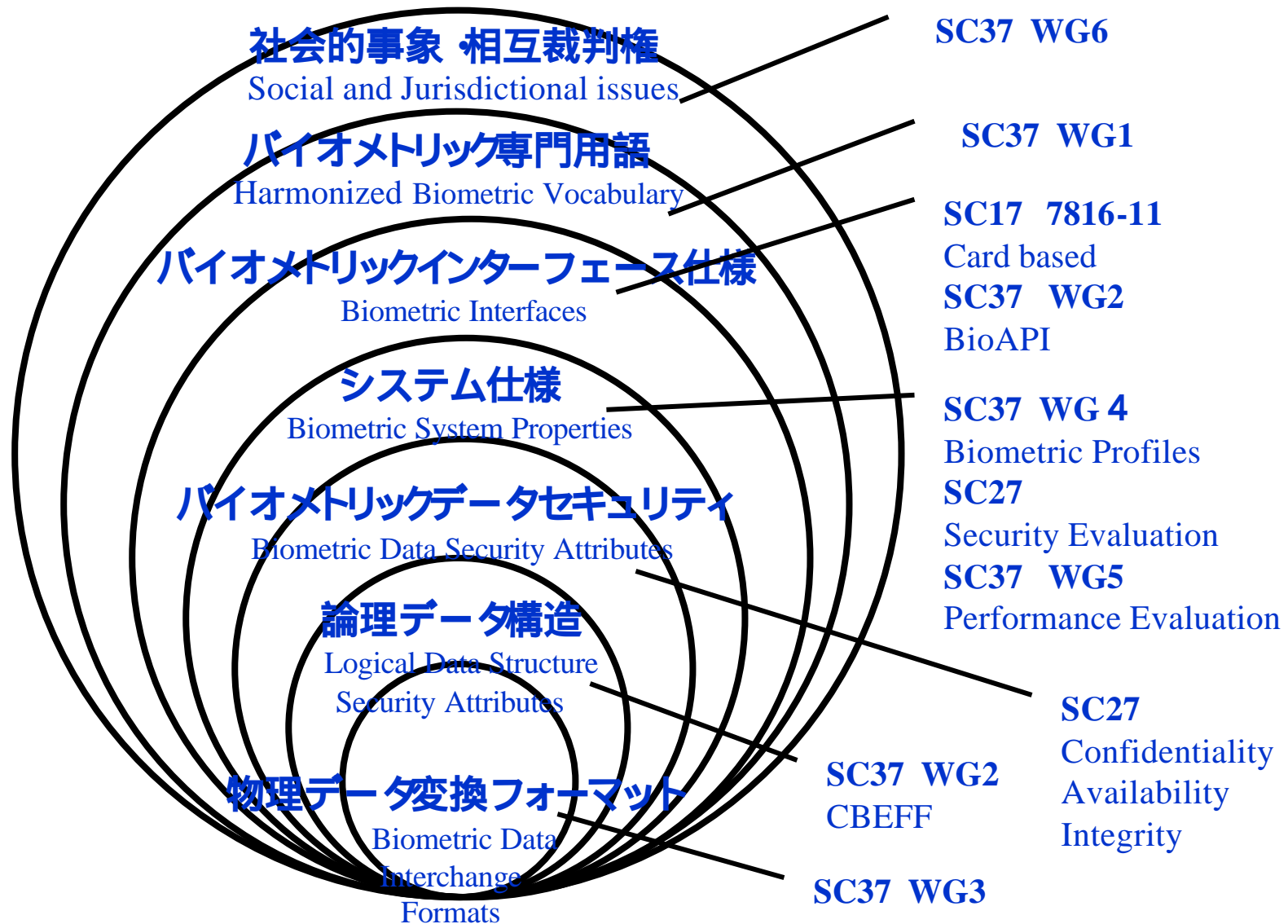
1 - 2 . 生体認証関係の標準化

・ 国際標準化の議論は、国際標準化機構 (ISO)と国際電気標準会議 (IEC) 第1合同専門委員 (ISO/IEC/JTC1)内に 設置された第37分科委員会 (SC37) が中心。



----- 生体認証関係の標準化
に関するリエゾン関係

1 - 3 .対象となる標準化項目と検討組織の関係



1 - 4 . 国際的な体制 (ISO/IEC JTC1 SC37)

議長 (Fernando Podio、米) セクレタリ (Lisa Rajchel、米)

WGタイトル	内容	主査
WG1 Harmonised Biometric Vocabulary and Definitions	技術用語 言語翻訳の統一	Rebe McIver (Canada)
WG2 Biometric Technical Interfaces	データ、プログラム インタフェース	Young-Bin Kwon (Korea)
WG3 Biometric Data Interchange Formats	データ交換形式	Axel Munde (Germany)
WG4 Biometric Functional Architecture and Related Profiles	導入、運用仕様	D.Hogan (USA)
WG5 Biometric Testing and Reporting	性能試験	Bob Carter (UK)
WG6 Cross-Jurisdictional Societal Aspects	相互裁判権	Mario Savastano (Italy)

1 - 5 .日本の体制 (情報処理学会 規格調査会 SC37専門委員会)

- 委員長 : 瀬戸洋一@日立、幹事 : 向井幹雄@ソニー
- リエゾン : SC 1 7、SC27、TC 6 8、ITU-T、JAISA
- 暫定的な委員会を2002年10月に立ち上げ、2003年11月より正式体制で運営

WGタイトル	国内主査
WG1 専門用語 Harmonized Biometric Vocabulary and Definitions	溝口 (NEC)
WG2 バイOMETリック テクニカル インターフェース Biometric Technical Interfaces	中野 (沖電気)
WG3 バイOMETリックデータ変換フォーマット Biometric Data Interchange Format	森 (富士通研究所)
WG4 バイOMETリック機能アーキテクチャと関係する運用仕様 Biometric Functional Architecture and Related Profiles	道坂 (NTTデータ)
WG5 バイOMETリック技術の試験および報告 Biometric Testing and Reporting	鷲見 (京都大学)
WG6 相互裁判権および社会的事象 Cross-Jurisdictional and Societal Aspects	池野 (セコムIS研究所)

2. 米国における取組み (X9.84 ・ISO CD19092比較表)

<p>標準化組織</p>	<p>ISO TC68 SC2 TC68は、銀行業界、証券業界、およびその他金融サービス」を対象とする専門委員会 SC2は、金融分野に利用される情報通信技術、情報セキュリティ技術を担当するサブ委員会</p>	<p>ANSI X9F American National Standards Institute 米国規格協会 X9Fは、銀行サービスにおけるセキュリティを担当するサブ委員会</p>
<p>標準の名称</p>	<p>ISO CD19092 ANSI X9.84を基に、米国より提案された規格 ISO/CD 19092 1 'Financial Service Biometrics Part1 ,Security Framework ” ISO/CD 19092 2 'Financial Service Biometrics Part2 ,Cryptographic Requirement ”</p>	<p>ANSI X9.84 金融機関における生体認証情報の管理と運営のためのセキュリティ要件を明確化した米国国内基準</p>
<p>成立時期</p>	<p>未成立 (国際標準化の作業中) (PWI NP WD CD DIS FDIS IS)の内、CDの段階</p>	<p>1998年1月X9F 銀行サービスにおけるセキュリティに関するサブ委員会より提案 1999年末 X9F (本標準を開発したWG)がドラフト版を完成させレビュー 2001年3月 ANS 認可 事務局は American Bankers Association</p>
<p>内容</p>	<p>Part1:Security Framework (セキュリティフレームワーク) 金融アプリケーションの検討 管理とセキュリティ要件 金融機関のセキュリティ基盤 生体認証の妥当性検証のための管理基準 Part2:Cryptographic Requirements (暗号の要件) 暗号技術と構文 生体照合の判定制御 Webサービス</p>	<p>目的 金融機関による生体認証情報の管理と運用のためのセキュリティ要件を明確化すること (主な内容) 管理要件とセキュリティ要件 (第8章) 実装技術 (第9章) セキュリティ検討事項 (Annex E) 生体認証についての管理・運用要件 (Annex F)</p>

3. 欧州における取組み (B D V I D N)

— 欧州における生体認証普及に向けたロードマップの検討を主目的として2002年6月から2003年5月までの12か月にわたり、欧州委員会 (EC) が統括する第5期研修開発プログラムの情報社会技術プロジェクトの一環として、実施されたプロジェクト。

- 2003年8月 プライバシーの観点からの検討結果として、「バイオメトリクスシステムのシステム展開におけるプライバシーに関するベストプラクティス」を公表。
- 2003年7月設立されたヨーロッパ・バイオメトリクス・フォーラムではプライバシー問題検討の内部グループを設立。

本ベストプラクティスは、EUにおけるデータ保護とプライバシーに関する諮問機関であるArticle29ワーキングパーティーが検討を行い、2003年8月に、生体認証情報を考慮した作業文書を公表。

個人情報保護の観点からみた生体認証

1. 生体認証情報の持つ二面性

プライバシー保護手段としての有用性だけでなく、プライバシーに対する潜在的な脅威を検討することも重要。
適切な防止策を講じることが技術の発展につながる。

プライバシー保護手段としての有用性

- ◆ パスワードなどのような伝統的方法よりも、個人データへのアクセス権のより良いリンクを提供し得る。
- ◆ ID窃盗への保護 :個人データが真正な者のみに用いられることを確保できる。

プライバシーに対する潜在的な脅威

- ◆ 他の情報と異なり、取り替え不能な究極の情報のため、漏えい時の影響が甚大。
- ◆ 認証の非常に強力な手段として認められる場合、詐称者が誤用したときの証明は不可能又は極めて困難かつ高価。

2. 生体認証と個人情報保護

生体認証情報

個人情報の中でも、特に重要な究極の個人情報である。

取り替え不能な情報である

指紋等身体的な情報が盗まれた場合には、暗証番号等と異なり、再発行が不可能である。

同意なしに情報が取得される可能性がある

カメラ等の非接触入力可能なシステムでは、本人の同意なく顔画像等のデータがとられる危険性がある。

副次的情報が抽出される可能性がある

生体認証情報については、副次的に健康・人種などの情報を取得することが可能。例えば、網膜の血管パターンなどから糖尿病などの病歴を知ることができる。

(参考) BIOVISION 「Privacy Best Practice in Deployment of Biometric Systems

情報処理推進機構, 各国バイオメトリクスセキュリティ動向の調査」

高度な管理が必要な生体認証情報の定義 についての検討ポイント

1. 「身体的な情報」と「行動的な情報」は同等であるべきか？

プライバシーの観点では、「身体的な情報」がより重要との指摘もみられる。

情報盗難時に情報を代替することが不可能

静脈情報を盗まれた場合、代わりの静脈を用意することは不可能。

本人の意志で変えることが不可能

行動的な情報は、本人が意図的に同定を回避することが可能。

- (例) ・ 声色を変えること
・ サインを崩すこと
・ 意図的に動作速度・様式を変えること

身体的	行動的
<ul style="list-style-type: none">指紋顔虹彩網膜静脈 (手のひら、手の甲、指)耳介匂い	<ul style="list-style-type: none">声紋署名キーストローク手指動作歩き方
等	等

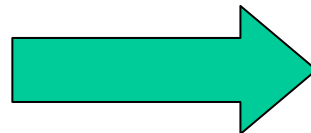
2. 「機械による自動認証に用いられる情報」と「機械による自動認証以外に用いられる情報」は同等であるべきか？

「機械による自動認証に用いられる情報」は、それによりアクセス等が可能となるため、より重要との指摘もみられる。

プライバシーを重視する欧州の議論でも、対象は「機械による自動認証」に限定。
「ここでの議論の対象となるバイオメトリクスは、情報セキュリティの手段である『機械による自動認証』とカテゴライズされたものを対象とする。」
(BIOVISION、“Privacy Best Practices in Deployment of Biometric Systems”)。

「機械による自動認証」に限定しない場合、管理方法の概念は一般社会通念等から大きく乖離。

- ◆ 顔写真入りの名刺の管理
- ◆ 守衛に顔の識別
- ◆ 卒業アルバムの管理



高度な管理が必要？

3 . 「公知の情報」と「非公知の情報」は同等であるべきか？

同じ情報形態であっても、公知・非公知により情報の価値は異なるとの指摘もみられる。

既に知られている情報に対し、高度な管理を求めるメリットは管理コストに見合うか。

デジカメで撮影した写真を厳重に管理しても、本人の顔はすれ違う人は皆見ることが可能。

同一の情報形態であっても、公知・非公知により漏えい時における本人への影響は大きく異なる。

顔情報でも、宗教上の理由等から常にベールで顔を覆っている人の顔情報は、一般的な日本人の顔情報とは重要性が異なる。

安全管理に係る上乗せ措置として考えられる内容

1. 安全管理に係る上乗せ措置検討に際してのポイント

最新の技術動向や日本独自の観点から欧米基準の内容を取捨選択し 参考とすべき

(参考となる基準)

米国

- ・ ANSI X9.84

「Biometric Information Management and Security for the Financial Services Industry」

欧州

- ・ BIOVISION

「Privacy Best Practices in Deployment of Biometric Systems」

(チェックすべき視点)

基準の内容の精査

- ・ 一般情報と重複したチェック項目
通常 of 安全管理措置にて対応
- ・ 最新の技術動向の観点からの
チェック

日本独自の観点からの精査

(商慣習 ・ 法制度 ・ 社会通念等)

2 .ANSI X9.84では、生体認証システムにおける脅威及びセキュリティの観点から考慮すべき事項が取りまとめられている。

- 1 .なりすましによる登録
- 2 .合成された生体情報 (写真を使った覆面、偽造の指紋、システム・データの再入力等)による不正認証
- 3 - 1 .生体情報の置き換え
- 3 - 2 & 3 - 3 .マッチング・データの検索による不正
 - 自らのデータとの適合者検索による不正取引の共謀
 - 任意の適合者検索による不正取引の共謀
- 4 .照合結果の修正
- 5 .不適切な認証精度設定、検定、システム能力
- 6 .ヒレクライミング・アタック及び登録生体認証情報の不正な更新
- 7 .過度に重層的な認証方式の導入によるセキュリティ・レベルの低下
- 8 .生体認証システムの精度評価に関する用語や手続きの不統一
- 9 .オープン・システムとクローズド・システムにおける相違点
- 10 .プライバシーの観点からの生体認証情報の漏えい・き損防止措置
- 11 .データ圧縮
- 12 .迂回装置の存在

ANSI X9.84 「Biometric Information Management and Security for the Financial Services Industry Annex E:(Informative) Security Considerations」

3. B D V I S D Nでは、プライバシーの観点から取組むべき事項 が取りまとめられている。

(B D V I S D N 「プライバシーベストプラクティス」骨子)

- データ提供者の同意に基づくデータ処理
- センシティブなデータ取り扱い時の明示的同意
- 事前説明に基づく目的に特化したデータの収集および使用
- データ提供者の同意の範囲内での第三者へのデータ提供
- 司法判断による場合に限定した法執行機関へのデータ提供
- 取り扱いデータやプライバシーポリシーの告知
- バイオメトリクスデータの更新と正確性
- バイオメトリクスデータを自動処理する場合における監督当局への通知
- 監督当局による点検・確認