バイオメトリクス Ⅱ

目次

1. バイオメトリクス技術と本人認証
2. バイオメトリクス技術
3. 認証モデル
4. データおよびプログラムインターフェイス
5. 認証精度とその測定方法
6. 認証システムにおける脅威
7. バイオメトリクス技術の標準化動向
8. プライバシーとバイオメトリクス
9. 新しい技術の開発（マルチモーダル認証）
10. 応用事例
11. 市場動向

バイオメトリクス技術の標準化動向

ISO/IEC JTC1 SC37

空港でのバイオメトリクス技術利用の経緯

2001.9.11以前　利便性重視

米国同時多発テロ事件が発生する前は、世界の航空需要は順調に伸びていた。この需要増加に答えるだけの空港建設の余地が無いヨーロッパを中心に空港の混雑が深刻な問題となった。そこで空港関係者（IATA,空港、航空会社、税関など）は一人の旅客にかける処理を単純化しスピードをあげようと考え、STPIG（Simplifying Passenger Travel Interest Group)を結成した。そのためのキー・テクノロジーとしてバイオメトリクスに着目し、幾つかの実証実験を行っていた。そして、バイオメトリックスの有効性が確認され、実用化直前であった。

2001.9.11以降　セキュリティ重視

2001.09.11の米国同時多発テロが発生し、旅客処理の単純化の緊急性が薄らいだ
空港でのセキュリティの強化⇒米国国内空港で各種バイオメトリックス技術の利用が活発化
バイオメトリクス認証⇒「究極の高い安全性を実現する」バイオメトリックスならば、唯一無二の自分の生体情報を鍵にするので、自分が脅されでもしない限り、他人が勝手に自分に代わって認証をパスすることはできない。

利用できるかの議論→なぜ利用しないかの議論
補足的な技術→メインストリームの技術
プライバシーの保護主体→セキュリティ確保主体

米国国土安全保障省の創設

2001.9.11 米国同時多発テロ

2001.10～ 国土安全保障局の創設
ブッシュ米大統領はいち早く「国土安全保障局」を創設。本土防衛のために必要とされる政策調整機能をもつ。

2002.06.06 国土安全保障省の創設提唱
ブッシュ米大統領は、米国本土をテロ攻撃から守るため国土安全保障省を創設すると発表。テロ対策に関連した8省庁の約20部局を統合する包括的なテロ対策が狙い。

2002.11.19 国土安全保障省の創設法案可決
同法案は下院で可決しており、ブッシュ大統領の署名を経て発効。法的には同法発効と同時に国土安全保障省が誕生。 実際には膨大な人員の移動や省庁間の調整が必要になり、全面的に稼動するのは2003年秋以降とみられる。同省は8省庁の22部局を束ねる巨大省庁で国防総省を発足させた1947年以降、最大規模の機構改革となる。ブッシュ政権は国土防衛の強化に向け、同省を軸に包括的なテロ対策に取り組む。同省は国境・交通の安全確保や大量破壊兵器への対策、テロ情報の収集・分析、非常事態への対応を担当する四部門で構成。異なる省庁に分散しているテロ関連部門を統合し、テロ対策の「司令塔」の機能を担う。

2003.10～ 国土安全保障省の全面的稼動

国際標準化委員会設置の背景

米国同時多発テロ(2001.09.11)で、入出国管理、
空港管理の 重要性の増大
→IDカードにバイオメトリクス認証機能
ユビキタス機器の普及により、個人利用市場の
立ち上がり
→モバイル、トークン認証にバイオメトリクス認証機能

国際標準化組織
ISO/IEC JTC1/SC37
(2002.12)
Biometrics (バイオメトリクス)

タイトル/スコープ

Title Biometrics (バイオメトリクス)

Scope

Standardization of generic biometric technologies pertaining to human being to support interoperability and data interchange among applications and systems. Generic biometric standards include common file formats: biometric application programming interfaces : biometric interchange formats: and relate profiles, application of evaluation criteria to biometric to biometric technologies, and methodologies for performance testing and reporting and cross jurisdictional and social aspects.
Excluded is the work in ISO/IEC JTC1/SC17 to apply biometric technologies to cards, and personal identification
Excluded in the work in ISO/IEC JTC1/SC27 for biometric data protection techniques, biometric security testing, and evaluations methodologies

応用とシステムにおける、相互運用とデータ交換を行うための一般的なバイオメトリクス技術の標準化を行う。一般的なバイオメトリクス技術としては、API、データ交換フォーマット、運用仕様プロファイル、性能試験などの技術項目と、相互裁判や社会事象などを含む。
ISOSC17,SC27において作業中の案件は除外する

参加国

P(Participation) Member-20

Australia, Canada, Finland, France, Germany, Ireland, Italy, Japan, Rep. Of Korea, Malaysia, Netherlands, New Zealand, Norway, Russian Federation, Singapore, Rep. Of South Africa, Sweden, Switzerland, UK, USA, China(2004-）

O(Observer) Member-5

Czech Republic, Denmark, Hungary, Rep. Of Poland, Israel

リエゾン

Internal Liaisons

SC17: Card and Personal Identification
SC27: Information Technology Security Techniques
SC29: Coding of Audio, Picture & Multimedia & Hypermedia Information
SC32: Data Management and Interchange
SC36: Information Technology for Learning, Education and Training
ISO/TC68: Banking and Related Financial Service

International Liaisons

MasterCard International (A)
ITU-T SG17 (A) Data Networks and Telecommunications Software
Travel Scope (A)
International Biometric Industry Association
The Association for the Automatic Identification & Data Capture Technologies
BioAPI Consortium

ワーキンググループ構成

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

	WGタイトル	内容
WG1	Harmonized Biometric Vocabulary and Definitions	技術用語 言語翻訳の統一
WG2	Biometric Technical Interfaces	データ、 プログラムインターフェイス
WG3	Biometric Data Interchange Formats	データ交換形式
WG4	Biometric Functional Architecture and Related Profiles	導入、運用仕様
WG5	Biometric Testing and Reporting	性能試験
WG6	Cross-Jurisdictional and Societal Aspects	相互裁判権

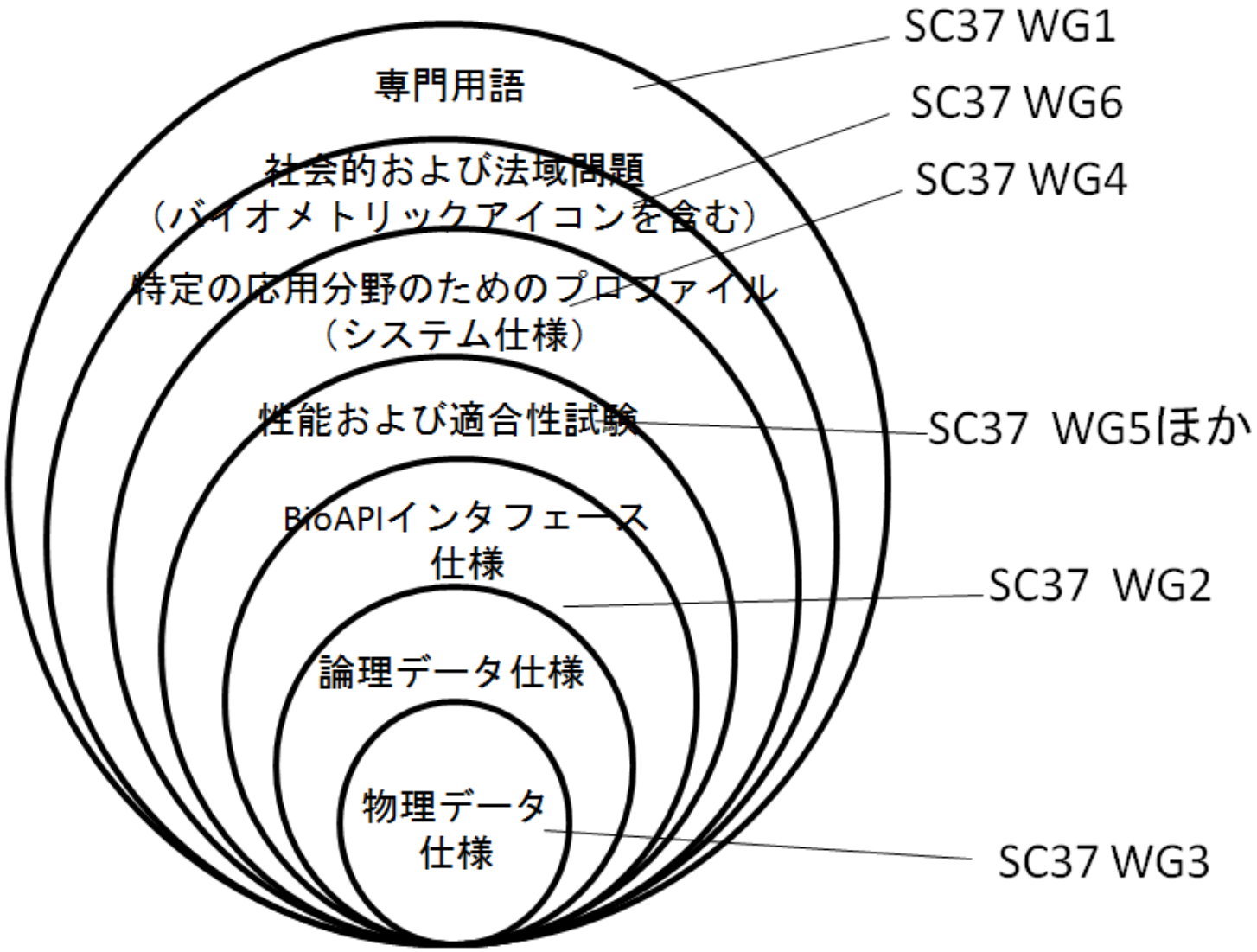
開発規格

WG2	ISO/IEC 19784	アプリケーションプログラムインターフェイス（API）
	ISO/IEC 19789	データ変換構造
	ISO/IEC 24708	バイオメトリクス機器とデータベースシステムとの相互作用プロトコル
	ISO/IEC 24709	API適合試験
	ISO/IEC 24722	マルチモード バイオメトリクス融合
WG3	ISO/IEC 19794	データ変換フォーマット（指紋、顔型、虹彩、静脈、動的署名）
WG4	ISO/IEC 24713	データ交換の操作性要件
WG5	ISO/IEC 19795	試験及び報告
WG6	ISO/IEC 26714	社会事業

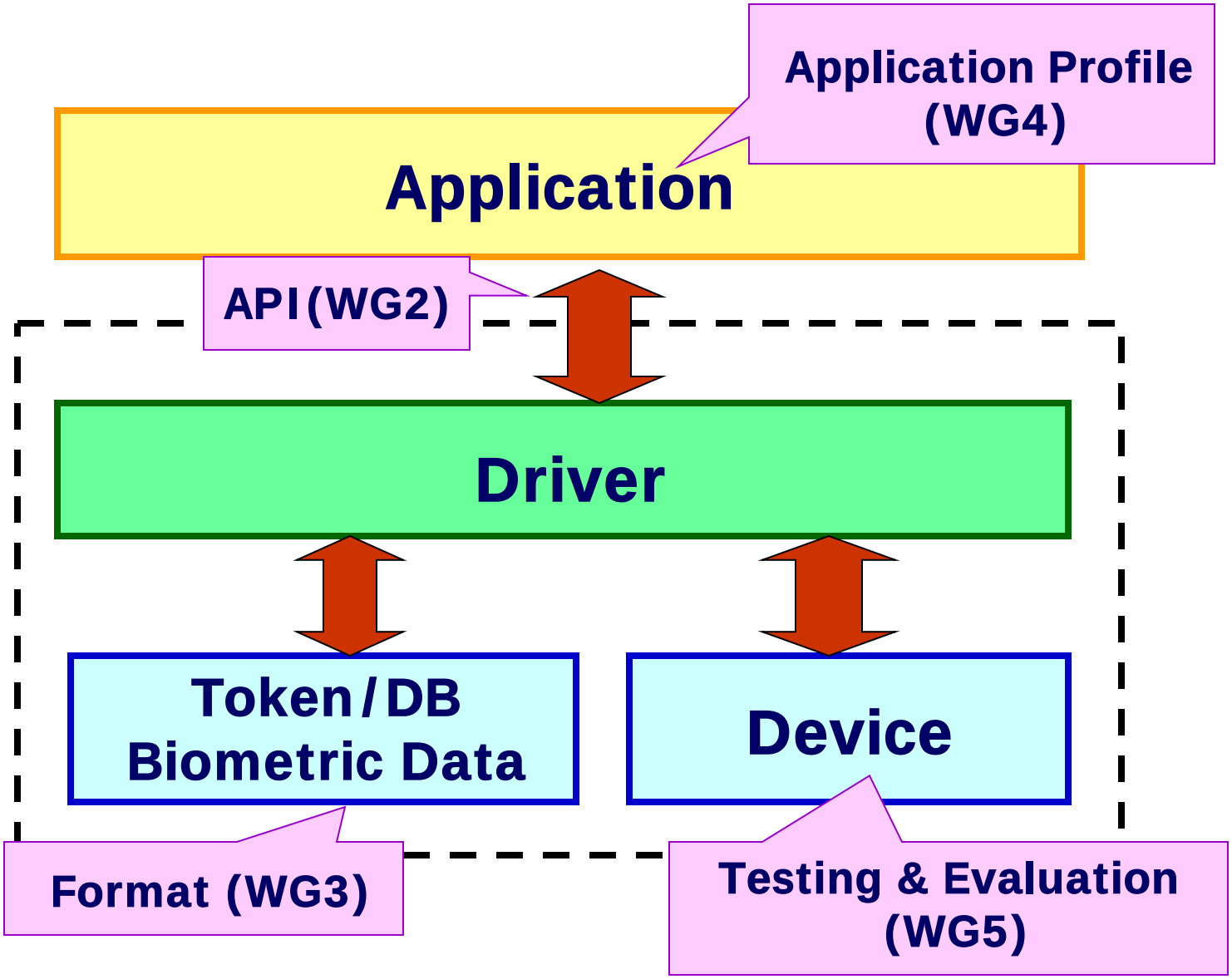
標準化の階層とワーキンググループ

階層	内容		番号
6	専門用語	Vocabulary	WG1
5	社会的および法域問題	Social and Jurisdictional	WG6
4	特定の応用分野のための プロファイル	Application Profiles	WG4
3	性能および適合性試験	Testing and Reporting	WG5
2	API仕様	BioAPI	WG2
1	論理データ仕様	Logical Data Structure	WG2
0	物理データ仕様	Data Interchange Formats	WG3

バイオメトリクスの標準化体制



ワーキンググループの関係



まとめ

1. 2001年の米国テロ以後、急速に普及
2. 市場の安全・安心を求めるニーズが後押し
3. 究極の個人認証はバイオメトリクス
4. 指紋、静脈認証が一歩リード
5. DNAは犯罪捜査で威力を発揮

プライバシーとバイオメトリクス

バイオメトリクスとプライバシー

プライバシー「自己情報を自分でコントロール可能な権利」

●プライバシーをバイオメトリクスで保護する。
●バイオメトリクス情報自体のプライバシー保護。

プライバシー問題	内　　容
取　替　不　能	●登録している個人情報が漏洩した場合、その情報を消し去ることができない。 ●偽造の可能性が否定できない。
同意なき情報取得	●身体情報が露出しているため、本人の同意なしに自然に採取可能。
強力な識別能力	●個人の身体情報であるため、そのテンプレート情報から個人を特定できる。 ●気づかれずに漏洩し、なりすましが行われた場合、否認が困難。
副次的情報抽出が可能	●人種、病歴、健康状態といった個人情報が抽出される可能性がある。（網膜認証→糖尿病）

プライバシーに関する歴史

国際	北米	欧州	その他
1980:OECDプライバシーガイドライン			
	1997:IPC(カナダオンタリオ州) 社会福祉改正法への関与	1997:Tele Trust/WG6(ドイツ)	
		1998～2002:Bio Trust(ドイツ)	
1999:IBIAプライバシー原則		バイオメトリックデータの悪用/誤用防止に関する勧告	
	2000～:IBG: Bio Privacy		
	2001:フロリダ州スーパーボウル顔認証試行に対する論議		
	2001:テキサス州法		
	2001～:DoD/BMO(アメリカ)		
	2001～:DHS(アメリカ)		
	2002:ニュージャージー州法	2002～ 2003:BIOVISION(EC/FP5)	
		Privacy Best Practice	
2003～:ISO/IEC JTC1 SC37/WG6		2003/8:EUデータ保護指令のバイオメトリック情報への適用方法に関する提言書	2003～:Biometric Institute(オーストラリア)
ISO/IEC TR24714(策定中)		イギリス:国民IDカード	Privacy Code for Biometric Industry.
2004:OECD WP on Information Security and Privacy Biometric-based Technologies.			

OECDプライバシーガイドライン

原　則	ポ　イ　ン　ト
収集制限の原則	適法かつ公正な手段で収集。妥当な場合には、データ主体の同意を得る。
データ内容の原則	利用目的に沿った内容で、利用目的に必要な範囲内で 正確、完全、最新に維持。
目的明確化の原則	収集目的を、収集時以前に明確化。 収集後のデータ利用は、該当目的に限定。
利用制限の原則	前項で明確化された目的以外の開示・使用の制限。 ただし、データ主体の同意/法律規定がある場合を除く。
安全保護の原則	不正アクセス・破棄・使用・修正・開示などの危険に対し、 合理的な安全保護措置により保護。
公開の原則	開発・運用・方針の一般公開。 データの存在とデータ管理者連絡先へのアクセス手段。
個人参加の原則	データ主体(個人)に次の権利: (1)データ管理者が該当個人データを有しているかの確認。 (2)自己に関するデータを延滞なく明瞭に通知してもらう。 (3)前2項が拒否された場合の理由確認および異議申立。 (4)自己に関するデータへの異議申立およびその異議が認められた 場合のデータ消去、修正、完全化、補正。
責任の原則	データ管理者には、上記諸原則実施のための措置に従う責任。

●OECD: Organization for Economic Cooperation and Development.

BIOVISIONの提言

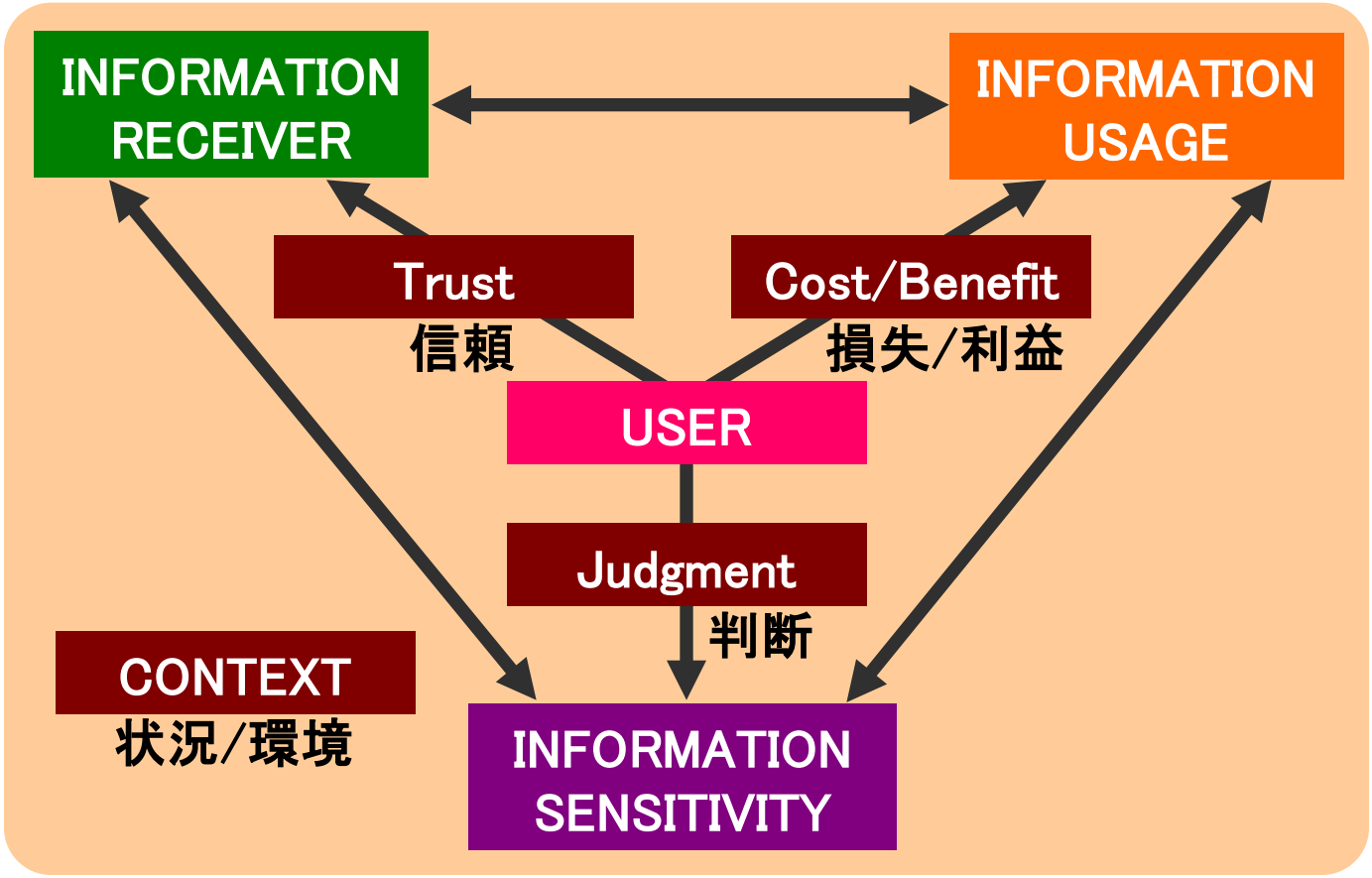
(1)データ提供者の同意のみに基づくデータ処理。
(2)センシティブなデータ使用時の明示的同意。
(3)事前説明に基づく目的特化したデータ収集/使用。
(4)データ提供者の同意の範囲内での第三者へのデータ提供。
(5)司法判断による場合に限定した法執行機関へのデータ提供。
(6)取り扱いデータに関するプライバシーポリシーの告知
　(セキュリティレベル、システムへのアクセス制限、
　バイオメトリックデータと他の個人情報との分離保存など)。
(7)精度維持のためのバイオメトリックデータの更新。
(8)バイオメトリックデータ取り扱いに関する監査当局への通知。
(9)監査当局による事前監査。

BIOVISION

2002～2003年に欧州委員会予算で実施されたバイオメトリクスに関する包括的な課題検討プロジェクト。

プライバシーモデル

マルチメディアコミュニケーションを対象



情報の機微度合

出典：Anne Adams, "Users' Perception of Privacy in Multimedia Communication", Proceeding of CHI'99, ACM Press, pp.53～54(1999).

新しい技術の開発
マルチモーダル認証

マルチモーダル認証技術とは

マルチモーダル認証技術

●複数の身体情報を用いて行う本人認証技術。

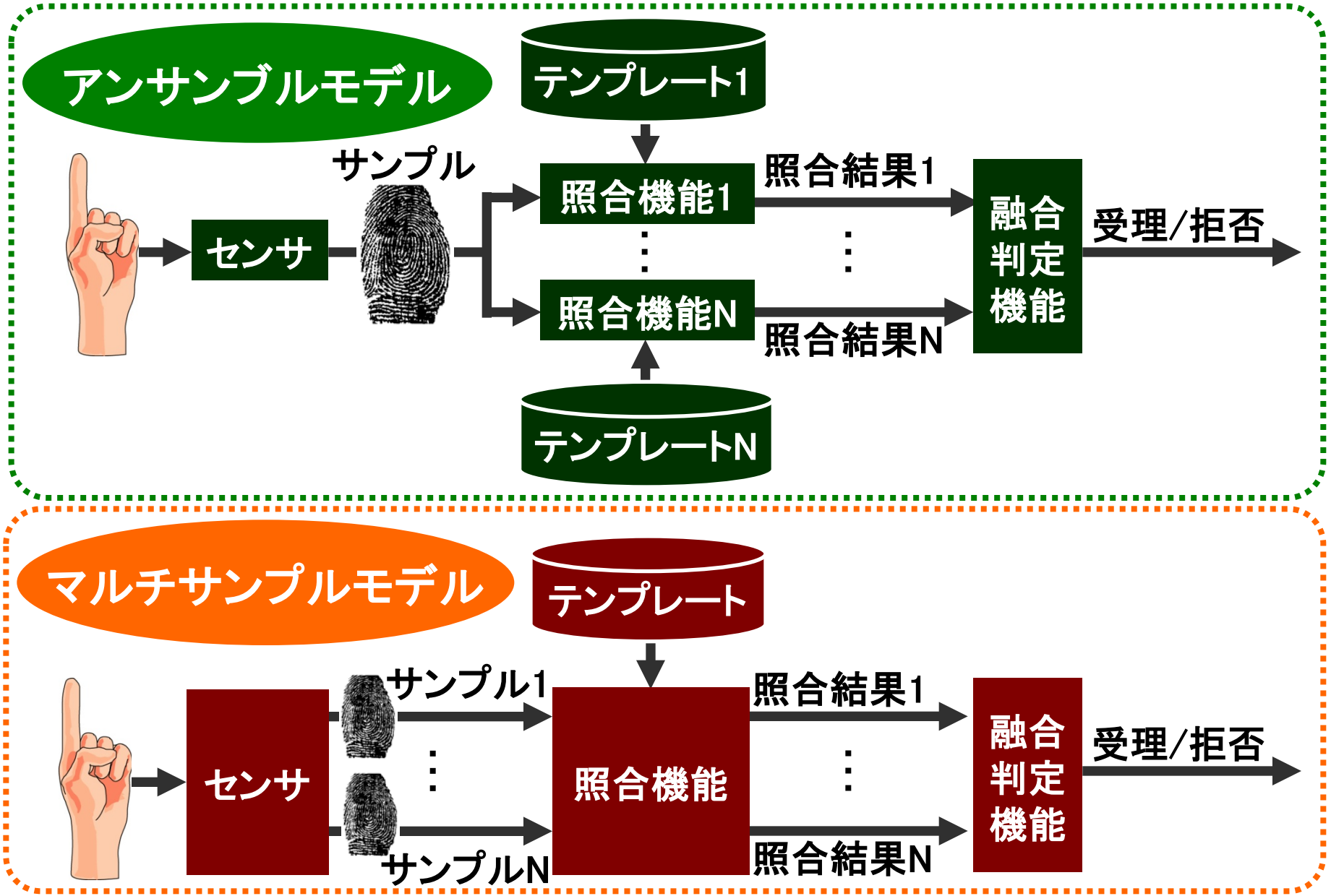
マルチモーダル認証技術のメリット

●本人拒否率や他人受入れ率などの精度改善。
●識別を目的とした場合の処理時間改善。
●身体情報の偽造防止対策。
●最適な身体情報を選択することによる利便性改善。

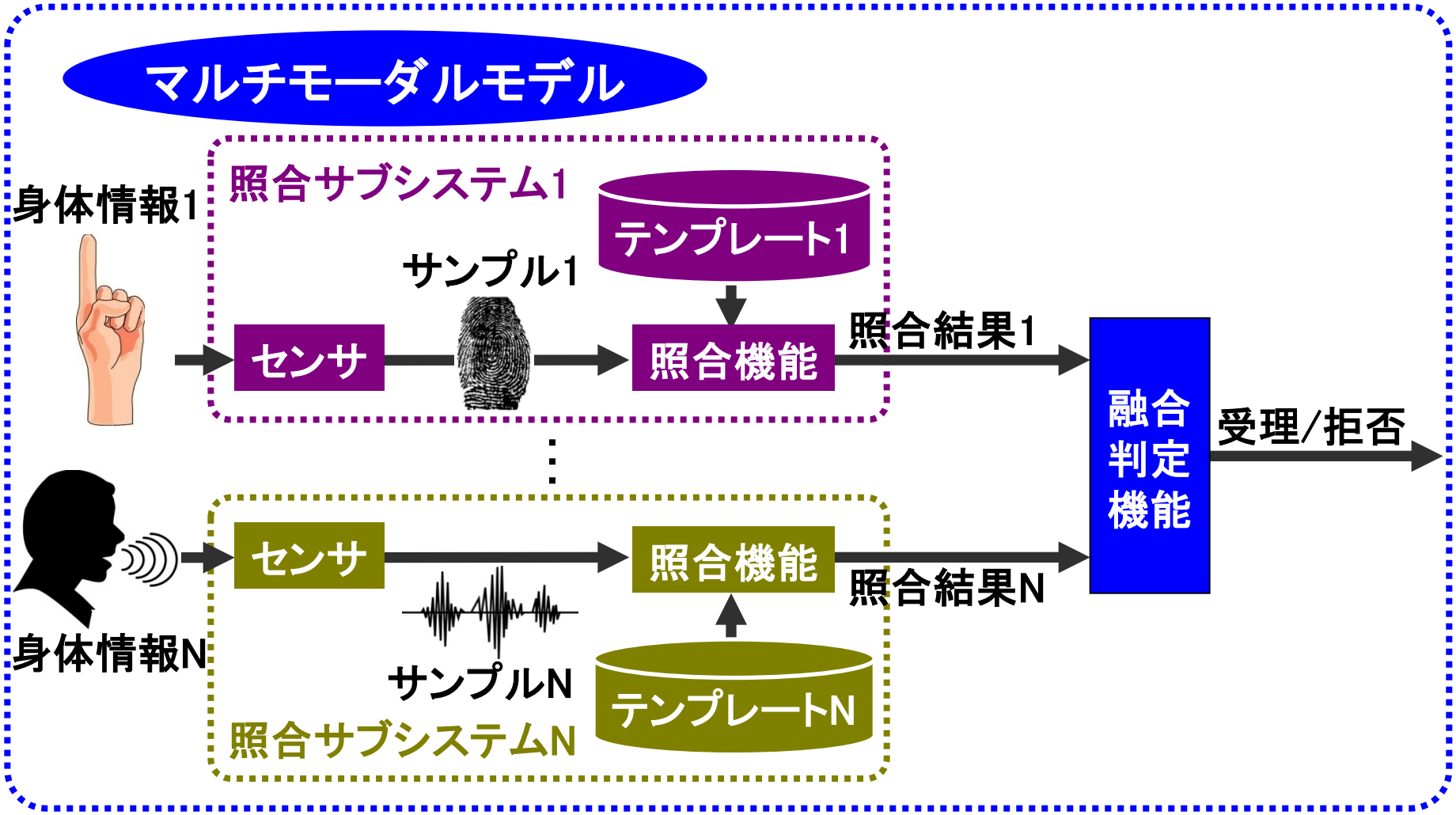
■融合モデルの分類

モデル分類	融合する情報	精度向上	利便性･可用性･受容性向上効果	特　長
アンサンブル	複数の照合アルゴリズムによる、1つの身体情報の照合結果	中	一般的な身体認証システムと同じ	ユーザインターフェースを変更せず適用可能
マルチサンプル	1種類の身体情報を複数回繰り返しサンプリングし、照合した結果	低	利便性低下	システム構成を変更せず適用可能
マルチモーダル	複数種類の身体情報の照合結果	高	可用性･受容性向上	高精度化が可能。可用性、受容性を向上可能

融合モデル

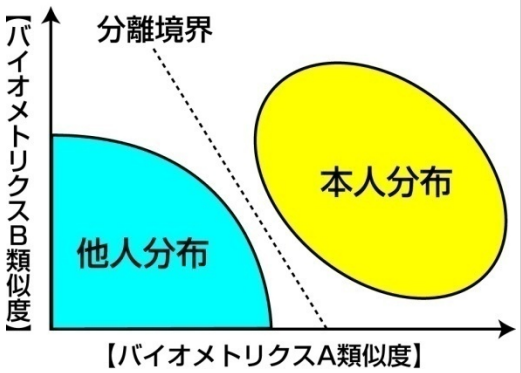


マルチモーダルモデル



●マルチモーダルバイオメトリクス認証システムの精度は、
個々の照合機能の性能と融合判定の方法に依存する。

マルチモーダルモデルの融合判定の方法

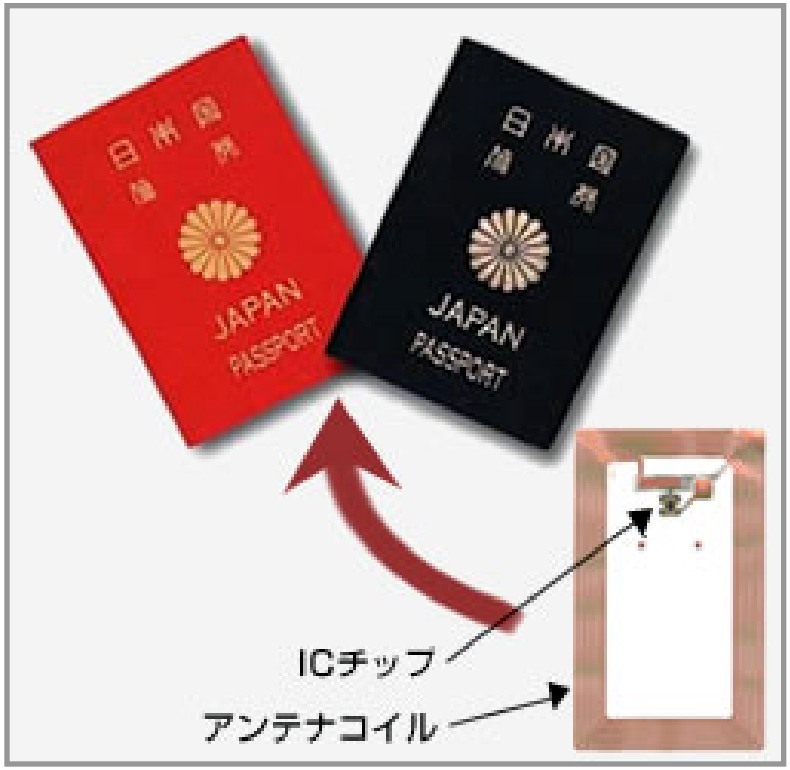
種　別		構　成	備　考	特　徴
OK/NG（アブストラクトレベル）	直列	身体認証A　身体認証B	他に、 ●重みつき結合 ●多数決 ●ルールベース などの応用あり	●単純で制御容易 ●各身体認証の精度からシステム精度を推定可能 ●FRRとFARのどちらかを選択的に向上
	並列	身体認証A 身体認証B		
類似度の相対リスト（ランクレベル）		類似度の相対的なリスト(B_1,B_2)から幾何平均により順位を決定。 $g = \sqrt{B_1^2 + B_2^2}$	高速化を目的とした類似度法との組合せもあり (Retrieval + Verification Biometrics)	●高速な個人識別が可能
類似度（メジャメントレベル）			分布の推定方法は確立していない	●FRRおよびFARを同時に改善可能 ●精度を統計的に計測可能 ●分布の計測には大規模なサンプルが必要 ●分布をモデル化により推定する手法が研究中

応用事例

バイオメトリクスの応用分野

身分証明証	企業等の身分証明から出勤管理・大学出席管理。 社会ID　・パスポート・運転免許証・船員手帳 ・国民ID他。
入退室管理	個人住宅・オフィス・マンション・企業・研修所等の 出入及び入退室状況の確認。
金融サービス	ATM・電子商取引や口座などの本人確認・ 渉外取引時における本人確認。
医療福祉サービス	介護を受ける本人の確認、病院の患者の管理、 モバイル活用、 携帯電話・PDA携帯端末でのネット決済。
アクセス権限者の限定	企業などの機密情報取得権限・会員権の行使。 ゲームやホビーなどの個人認識、 ゲーム場などでの本人権限管理。
その他	自動車の鍵・エンジンキーの代替・運転者の限定、 家電製品などの所有者の特定

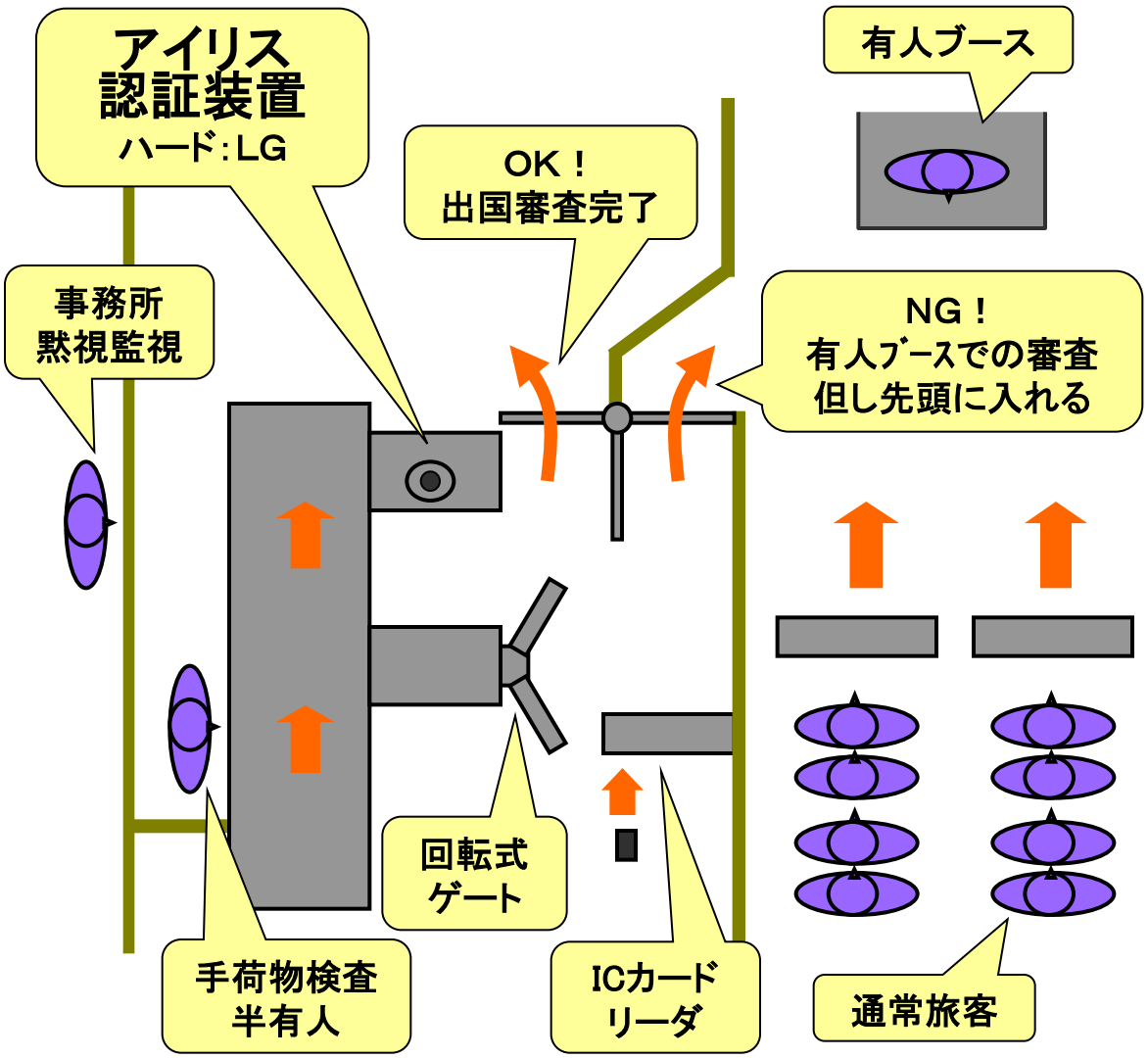
応用事例　電子パスポート



- 電子パスポートは、国際連合の下部組織である「ICAO(国際民間航空機関)」で標準仕様を開発。
  顔認証の採用は、心理的な抵抗感少。
- 世界規模で連携運用される技術で相互運用性を保証。
- 世界連携のため、セキュリティは弱い国に発現しないように。

応用事例 アムステルダム スキポール空港の実証実験

空港出国審査ゲート 平面図



応用事例　入退室管理

●入退室が許可される方の登録

あらかじめ 指静脈パターン画像をICカードに登録する。

●入退室時の動作

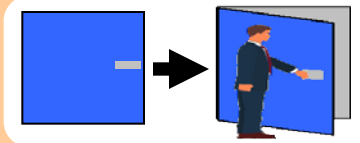
① 入退室の際にカードをかざす。

② 入退者の指静脈画像を入力する。

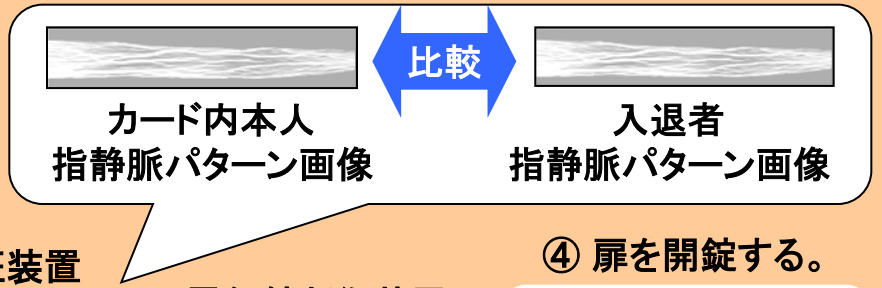
認証装置

電気錠制御装置

④ 扉を開錠する。



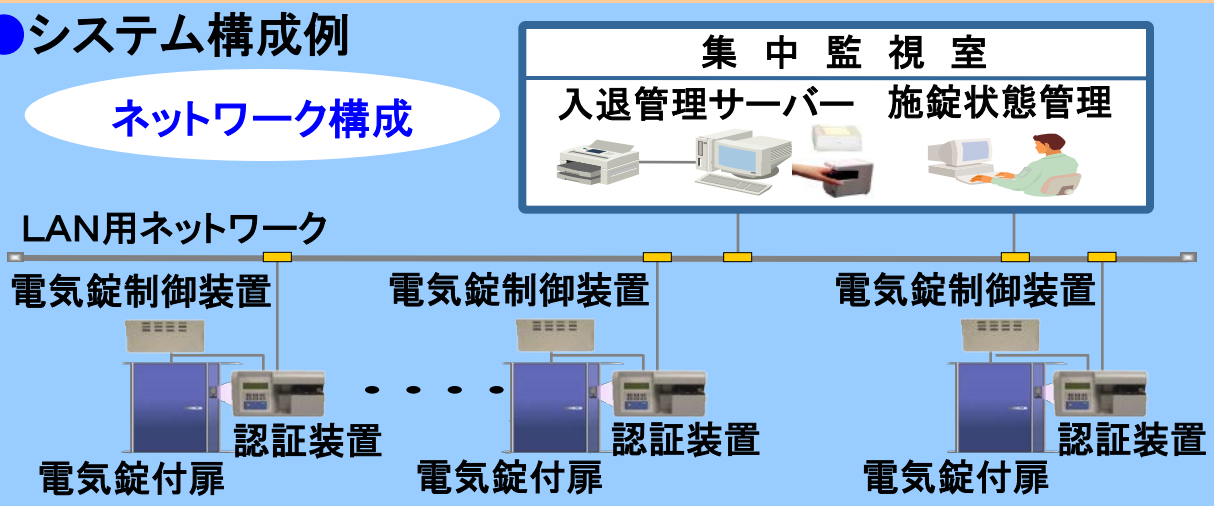
③ 指静脈パターン画像を照合する。



① IC カードより 登録済 指静脈パターン画像を取得する。
② 指静脈パターン画像を認証装置で取得する。
③ ①と②を認証装置内で照合し、結果を電気錠制御装置へ送信する。
④ 扉を開錠する。

●システム構成例

ネットワーク構成



スタンドアロン構成

応用事例　住宅のドア開錠

●2001年7月、個人住宅向けの玄関用指紋錠として、
　日本で初めて開発された。
●指が鍵の代わりに用いられた。

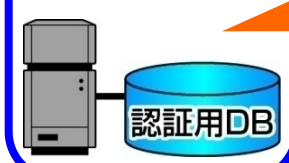



応用事例　金融機関での想定システム

システムイメージ

生体情報を活用した本人認証による、
預金者からの信頼性と預金口座の安全性向上

PKI



PKIによるカード
及び
生体情報の
偽造チェック

銀行ネットワーク

インターネット

銀行窓口

指静脈認証端末

ICキャッシュカード

窓口での本人認証

盗難通帳による払い出しの防止

ATM

指静脈認証ATM

ICキャッシュカード

ATMでの本人認証

カード、暗証番号盗難への対応

貸金庫

指静脈認証ゲート

受け取り口

ICキャッシュカード

貸金庫での本人認証

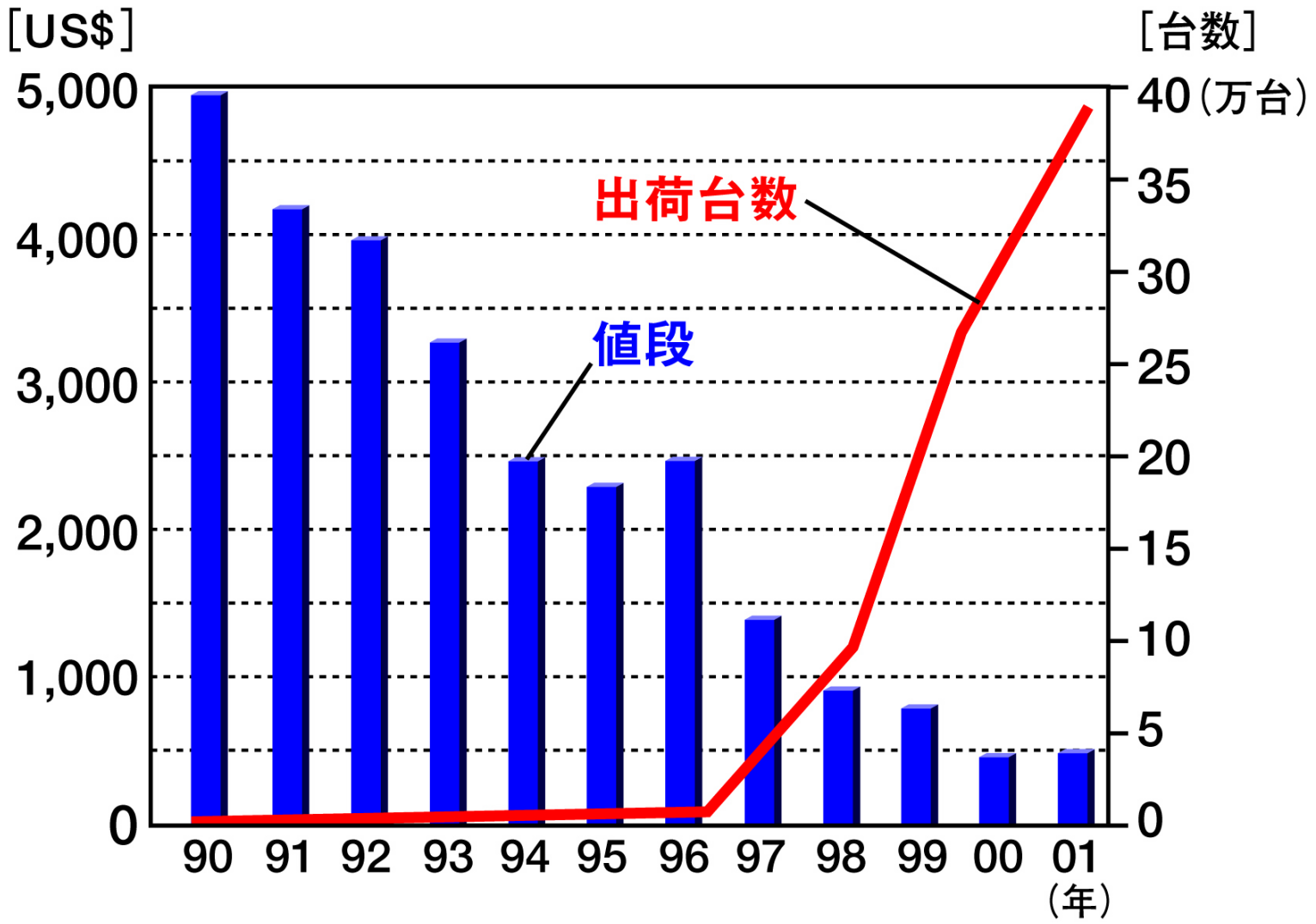
セキュリティ強化、省力化

家庭

家庭からの
ネット
バンキング

市場動向（統計）

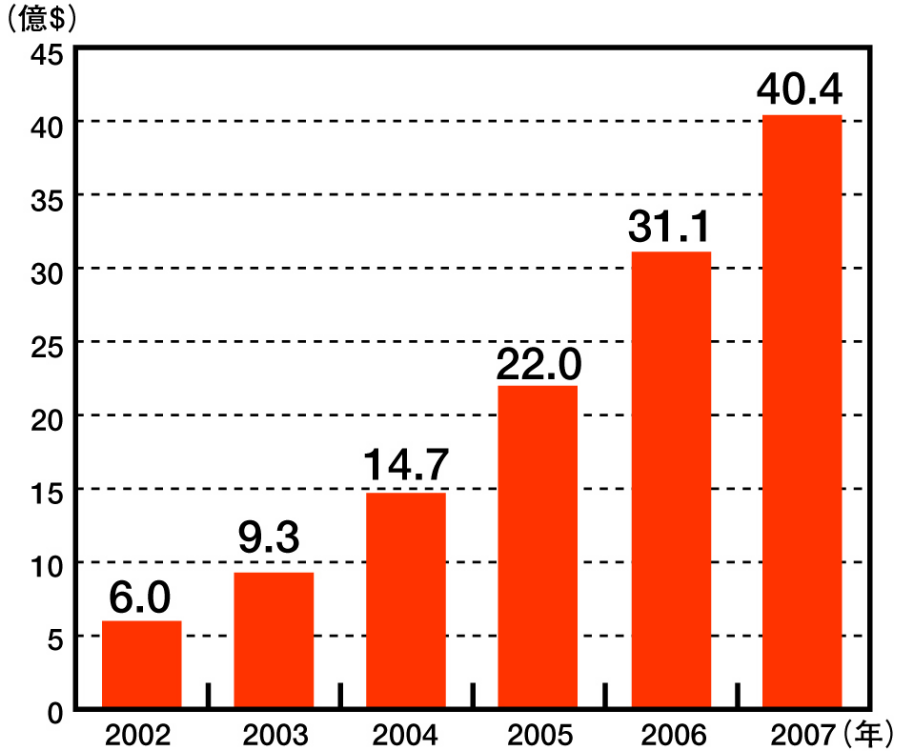
機器の市場規模 1990-2001



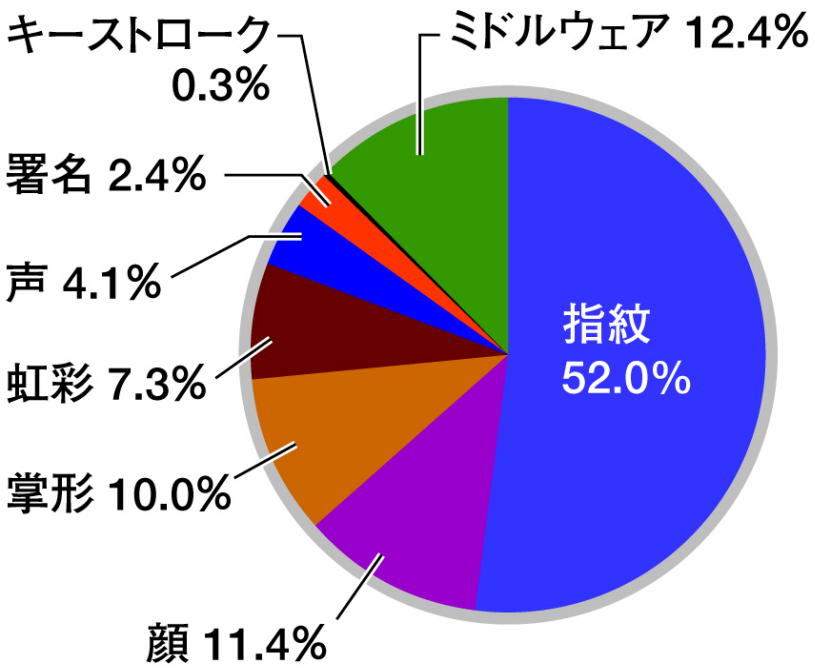
出典：The Biometric Industry Report "Market and Technology Forecasts to 2003" Elsevier Advanced Technology (2000).

機器の市場規模 2002-2007

市 場 規 模

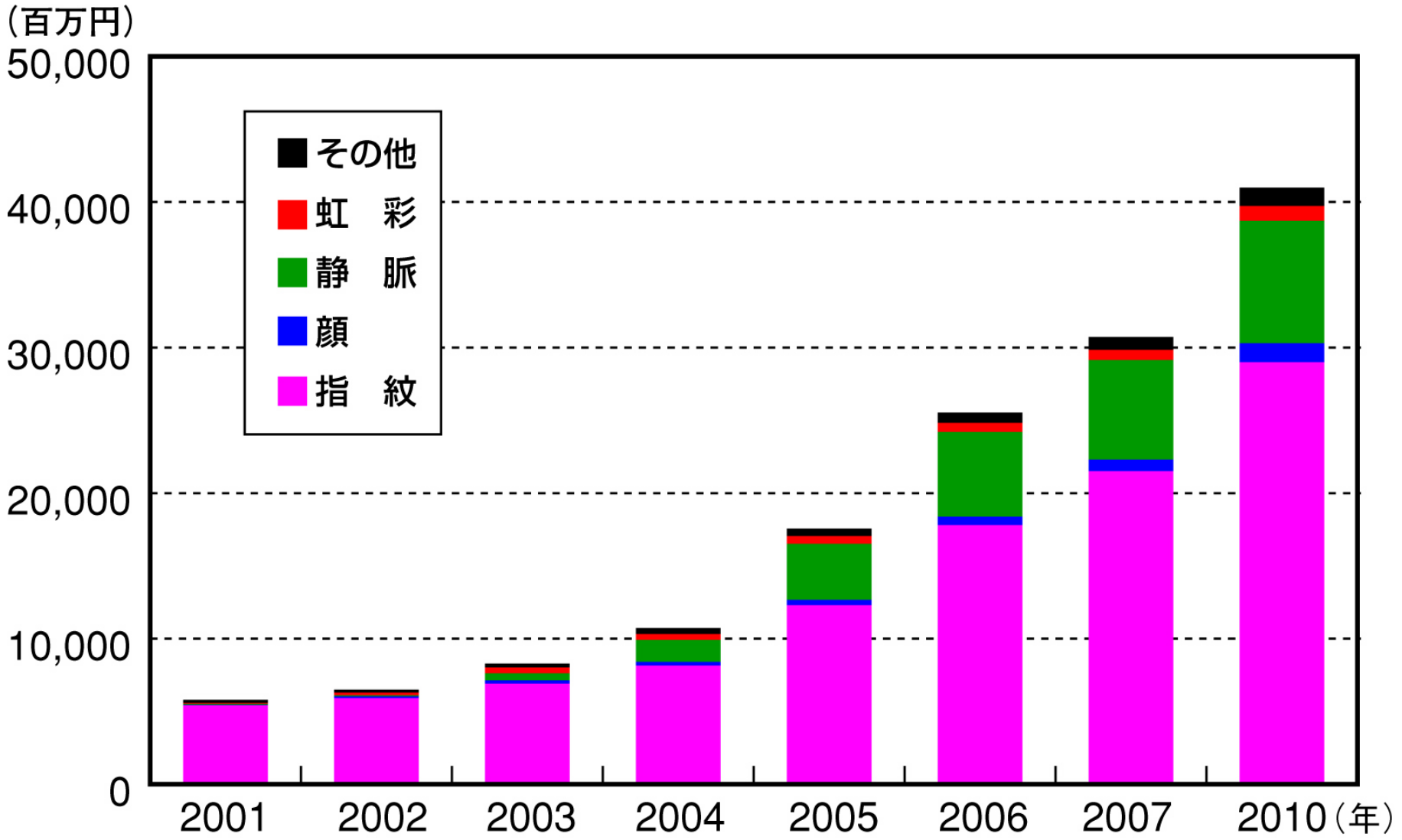


2003年の技術別のシェア



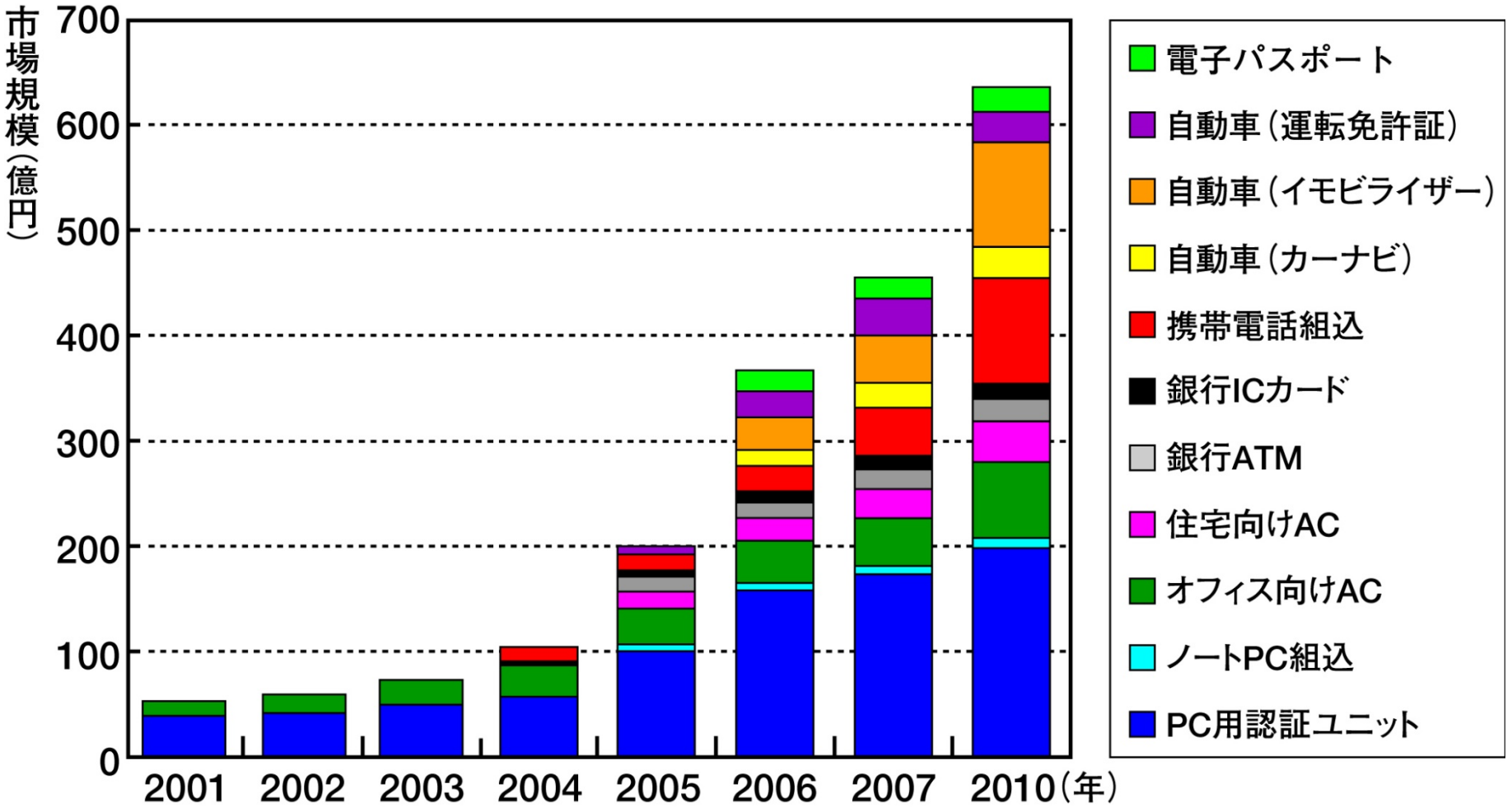
出典:"Biometric Market Report 2003-2007"(2002.9.30).
International Biometric Group.

技術の現状と将来予測 2001-2010



出典：バイオメトリクス セキュリティ コンソーシアム (2005.7)

バイオメトリクス用途規模　2001-2010

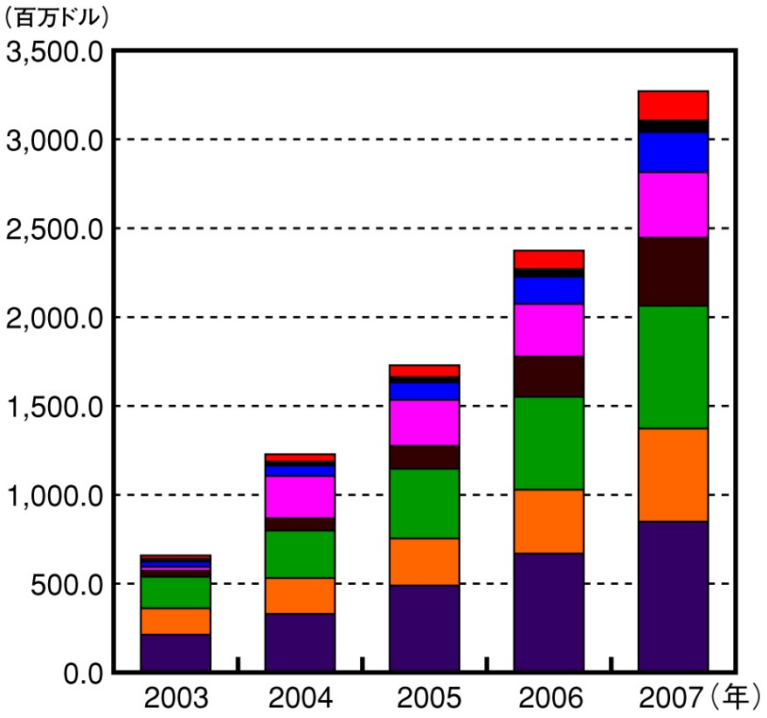


出典：バイオメトリクス　セキュリティ　コンソーシアム

バイオメトリクスの用途規模 2003-2007

（百万ドル）

用途	2003年	2004年	2005年	2006年	2007年
National ID	213.1	329.9	490.4	669.1	849.4
アクセスコントロール/勤怠管理	148.7	202.5	264.0	360.0	523.7
PC/ネットワークアクセス	176.9	266.2	382.2	522.4	690.3
eコマース/電話	34.5	69.4	128.9	226.0	383.1
犯罪関連	221.3	237.3	258.6	296.4	368.1
リテール/ATM/POS端末	29.0	58.7	97.5	152.7	255.6
デバイスアクセス	17.4	22.9	30.7	43.2	65.8
監視・モニタリング	18.1	41.3	66.8	104.0	164.7
合計	859.0	1228.2	1719.1	2373.8	3270.7



出典：Fuji Keizai USA.

ご清聴、ありがとうございました。