

バイOMETRICS認証

2019年12月20日

才所 敏明 (株)IT企画

toshiaki.saisho@advanced-it.co.jp

<http://advanced-it.co.jp/>

<https://www.facebook.com/toshiaki.saisho>

自己紹介

1970年4月～1994年12月 東京芝浦電気(東芝)・情報システム部門
本社情報システム部門に所属、東芝Gの技術部門・研究部門の
研究開発活動環境の整備・高度化を推進

1995年1月～2007年9月 東芝・セキュリティ技術研究開発部門
東芝のセキュリティ技術センター発足と同時にセンター長就任
その後、東芝Gのセキュリティ技術開発・事業支援活動を推進

2007年10月 (株)IT企画を設立
情報技術および情報セキュリティ技術分野の研究開発や
その応用事業に対するプロフェッショナルサービスを開始

[現職]

(株)IT企画 代表取締役社長

事業支援活動(顧問・相談役): 2社(日、米)

大学教育活動(情報セキュリティ): 九大、慶応、目白大

研究開発活動(研究員): 中央大学研究開発機構、九州大学大学院

暗号・認証、秘密分散、バイOMETRICS、電子メールセキュリティ、

IoTシステムセキュリティ、FinTech(仮想通貨、ブロックチェーン)

ビッグデータ、AI

< 本日の内容 > バイオメトリクス認証

- (1) バイオメトリクス認証とは
- (2) 本人確認方法における
バイオメトリクス認証の位置づけ・特徴
- (3) 主要なバイオメトリクス認証方式概要
- (4) バイオメトリクス認証のプロセス
- (5) バイオメトリクス認証応用の現状・動向
 - 5. 1 ナショナルセキュリティ
 - 5. 2 ネット経由の本人確認
 - 5. 3 店頭での支払い

(1)

バイオメトリクス認証とは

人が持つ生体特徴により、 本人確認を行う認証方式

人は

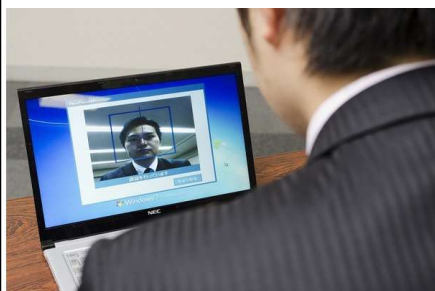
- * 顔を見て、その人だとわかるように
- * 電話で声を聞いて、その人だとわかるように

あらかじめ知っている人の生体特徴(顔、声など)と
どの程度似ているかにより、その人と判断

コンピュータで実施するバイオメトリクス認証も

あらかじめその人の生体特徴を登録しておき、
その場に居る人の生体特徴と突きあわせ、
その似ている度合いにより、その人である、と判断

(例) 顔認証によるPCログイン



<http://www.gsd-inc.com/event/index.html>

- (1) PC所有者はあらかじめ
PCへ顔画像(特徴)を登録しておく
- (2) PCの前に座った人の
顔画像(特徴)をカメラで入手する
- (3) 入手した顔画像(特徴)と
登録画像(特徴)を比較する
- (4) 比較の結果(類似のレベル)に応じ
PCの前に座っている人が
PCの所有者かどうかを判断する

PCの所有者は、パスワード等を入力せず、PCの利用が可能となる

■ 13:07

(2)

本人確認方法における バイオメトリクス認証の位置付け・特徴

システム利用時の本人確認方法は 大きく次の三つの方式に分類される

- (1) その人しか知りえない情報を知っていること
を確認することによる本人確認
→ 記憶による本人確認
- (2) その人しか持っていない筈の物を持っていること
を確認することによる本人確認
→ 持物による本人確認
- (3) その人しか持ちえない生体特徴を持っていること
を確認することによる本人確認
→ 生体特徴による本人確認(バイオメトリクス認証)

記憶による本人確認の特徴

- * 事前に登録している、その人しか知らない秘密の情報を、
知っているかどうか
提供する側の費用負担が少ない
日常使い慣れた方式
- * 人が記憶できる長さ(情報量)に限界
→ 推測されやすいものになりがち
- * 多数のパスワード記憶が必要 → 忘失の危険大
- * 忘失対策としてのメモ → 盗用の危険
- * 盗用され、悪用されても、気がつかないことが多い

持物による本人確認の特徴

- * 事前に登録している、その人しか持っていない物を、
持っているかどうか
学生証、社員証、マイナンバーカード、
クレジットカード、スマホなど
- * 常時携行が必要 → 紛失・破損・盗難の危険
- * 偽造の危険性も
ICカードになると偽造の危険性は少ない

生体特徴による本人確認の特徴

- * 事前に登録している、その人しか持っていない生体特徴を、
持っているかどうか
- * 偽造は他の方式に比べ困難
- * 実装方法によっては、記憶も所持物も不要
- * 一度で照合できない場合もある

■ 13:15

(3)

主要なバイOMETRICS認証方式概要

主要なバイオメトリクス認証方式

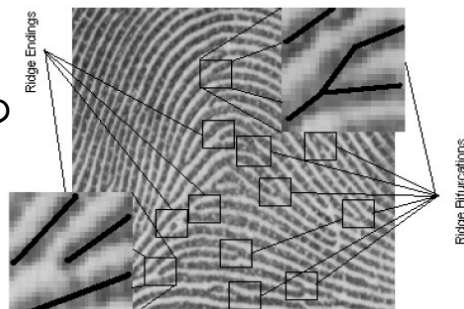
- * 指紋認証
指紋画像や特徴点の存在・位置関係等が
個人別に異なることを利用
- * 顔認証
顔画像や顔の部品の位置関係・形状等が
個人別に異なることを利用
- * 虹彩認証
目の虹彩のパターンが個人別に異なることを利用
- * 静脈認証
静脈血管のルート(血流のパターン)が
個人別に異なることを利用

指紋(1)

・ 照合方法

- 指紋紋様には特徴点(マニューシャ)と呼ばれる固有の特徴があり、この特徴点から座標と角度を取り出してデータとして使用するのが代表的な方法である

- 指紋画像を使って、画素毎のマッチングを行う方法もある



指紋(2)



- ・ 精度
 - 高精度な照合方式が確立している
- ・ 実装上の特徴
 - 入力センサが接触型で小型化できる
 - 皮膚の乾燥、発汗、傷、摩耗等により必要な品質のデータが得られない場合がある
 - 「指紋を取られる」ことに対する抵抗感がある

個人用機器の本人確認への応用例



スマートフォン



パソコン

入退室時の本人確認への応用例

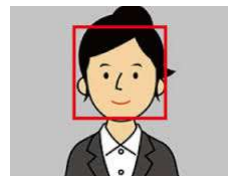


サーバ室

個人住宅

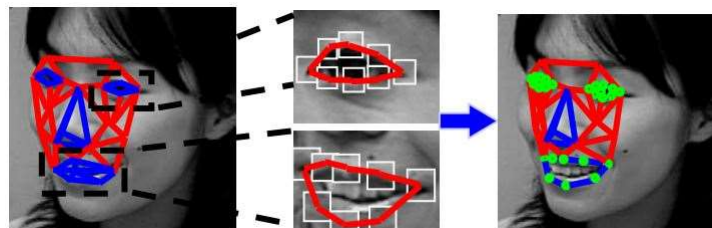


顔(1)

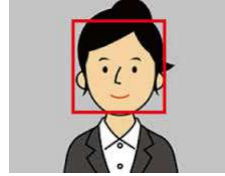


・ 照合方法

- 目や口等の代表的な顔の部品の位置を原点にして、その他の部品の位置を位置データとして2次元的に照合する方法と、何らかの計測法を用いて鼻の高さや頬の形のような3次元構造を抽出し照合する方法がある

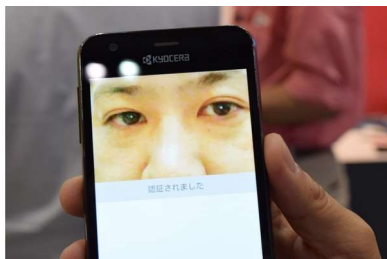


顔(2)

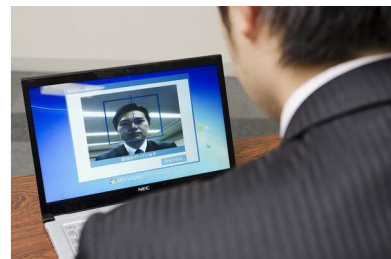


- ・ 精度
 - － 向き、照明、髪型、サングラス、マスク等によって照合精度に影響がでやすい
- ・ 実装上の特徴
 - － 顔を見て誰であるかを判断することは普段から人同士で行われており、利用者の抵抗感が少ない
 - － 顔は常時露出しているので、本人が意識しなくても入力、照合可能である

個人用機器の本人確認への応用例



スマートフォン



パソコン

入退出時の本人確認への応用例



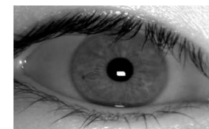
執務室入室時



自社ビルへの入館時

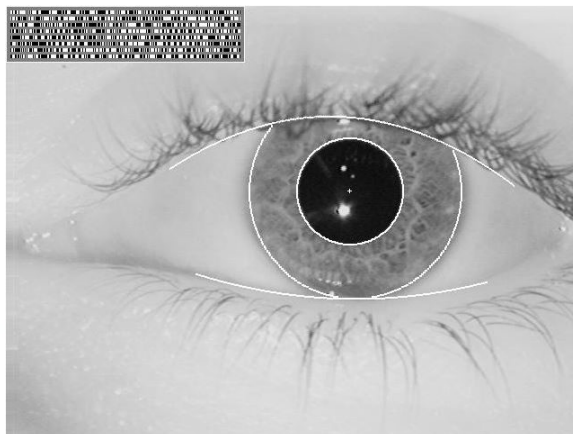
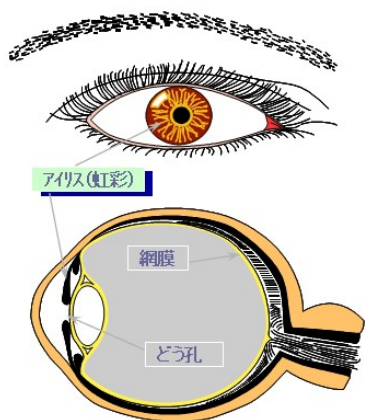
■ 13:22

虹彩(1)

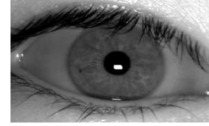


・ 照合方法

- 虹彩(アイリス: 黒目のうち瞳孔を囲む放射状の筋肉の表面にある模様)のパターンによって照合



虹彩(2)



- ・ 精度
 - － 精度は非常に高い
 - － 個人性が強く一生を通じて変化しない
- ・ 実装上の特徴
 - － 外部から見えやすく非接触で撮像できる
- ・ 最近の動向
 - － 虹彩認証の基本特許が切れ、安価でコンパクトな実装が可能な、そして精度も良い新たな虹彩認証アルゴリズムが開発された。

入退室時の本人確認への応用例



執務室入室時



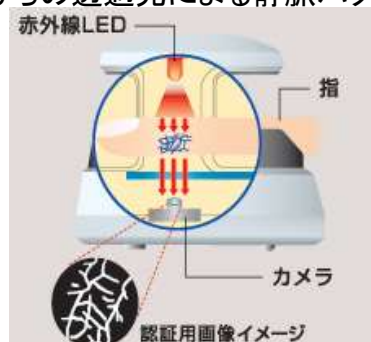
マンションエントランス入館時

静脈(1)



・ 照合方法

- 動脈は、酸化ヘモグロビンを体の各組織へ送り込み、酸素を供給する。静脈は、酸素を失った還元ヘモグロビンを心臓へ戻す。その血流のパターンは、個人個人によって異なる。
- 近赤外光領域の約760nmの波長の光は、還元ヘモグロビンが吸収するため、近赤外光を当てると、静脈の血管パターンだけが暗く映る。指/手のひらの透過光による静脈パターンによって照合する。



静脈(2)



・ 精度

- 指紋、虹彩と同程度の、高い精度が期待できる
- 経年変化がほとんど無い

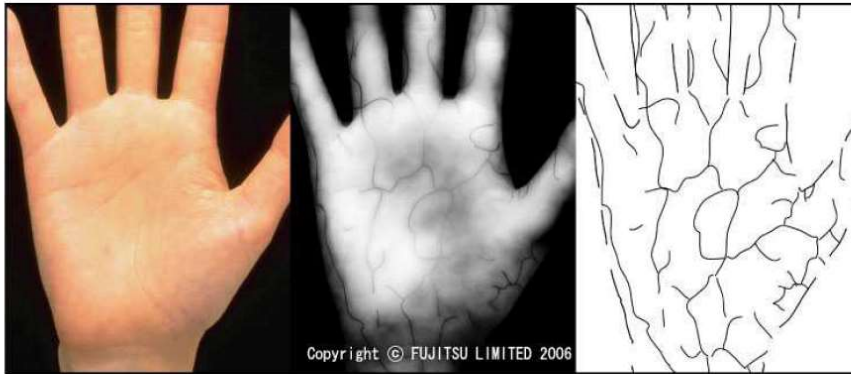
・ 実装上の特徴

- 接触部分が少なく、利用者の抵抗感はほとんど無い

・ 技術の特徴

- 対応率が良い
- 他のバイオメトリクスに比べ偽造が困難

手のひら静脈のパターン



(a) 一般のカメラで撮影した画像 (b) 赤外線カメラで撮影した画像 (c) 手のひらの輪郭および抽出した静脈パターン

生体認証導入・運用のためのガイドライン(IPA)より

ATMへの応用



指静脈認証



手のひら静脈認証

出典: <http://www.itmedia.co.jp/mobile/articles/0410/01/news076.html>

出典: <http://jbpress.ismedia.jp/articles/-/42629>

入退室時の本人確認への応用例



マンションエントランス入館時

出典: <http://www.kaji-gl.com/security/index.html>



執務室入室時

出典: <http://pr.fujitsu.com/jp/news/2005/08/18.html>

まとめ

- ① バイオメトリクス認証には様々な方式がある
- ② 全てにおいて優れたタイプは無く、
 可用性、利便性や価格性能比など、
 実際の利用環境、システム要件などを鑑みて
 最適な方式を選択する必要がある

バイオメトリクス認証の比較の例

	指紋	顔	虹彩	静脈
認証精度	◎	○	◎	○
使いやすさ	◎	◎	○	◎
小型化	◎	○	○	△
低価格化	◎	○	○	△
清潔感	△	◎	◎	◎
データ漏洩	△	△	△	△
偽造のしにくさ	○	○	◎	○
環境変化	△	△	◎	◎
経年変化	◎	○	◎	○

可用性、利便性や価格性能比など、
実際の利用環境、システム要件等を鑑みて
最適な方式を選択することが必要

■ 13:35

(4)

バイオメトリクス認証のプロセス

バイオメトリクス認証の 基本的な考え方

あらかじめ本人であることを確認した上で
採取した生体情報(テンプレート)

と

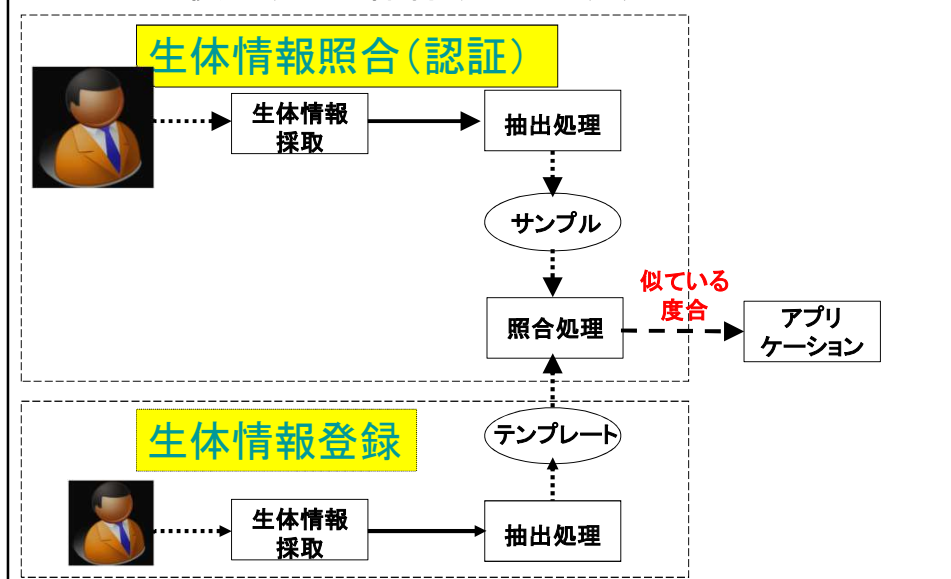
その場で採取した生体情報(サンプル)

を

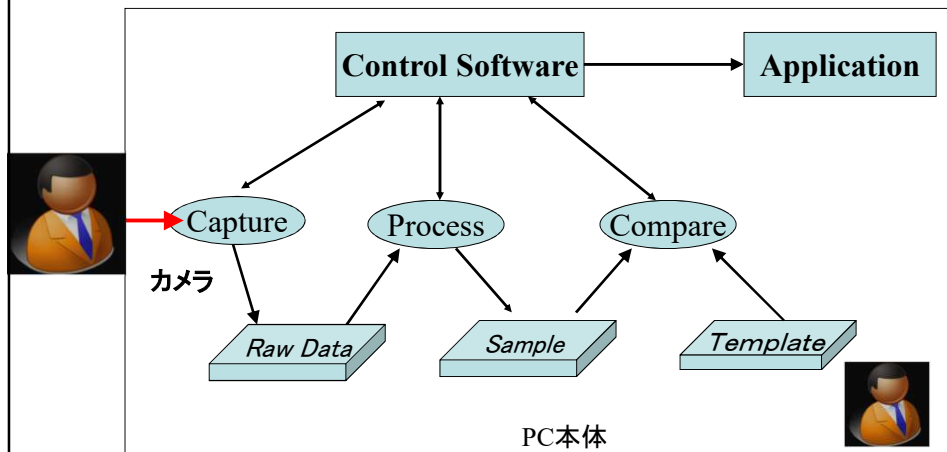
照合することにより

その場に居る人が、あらかじめ本人であることを確
認したその人と、同一人かどうかを判定する

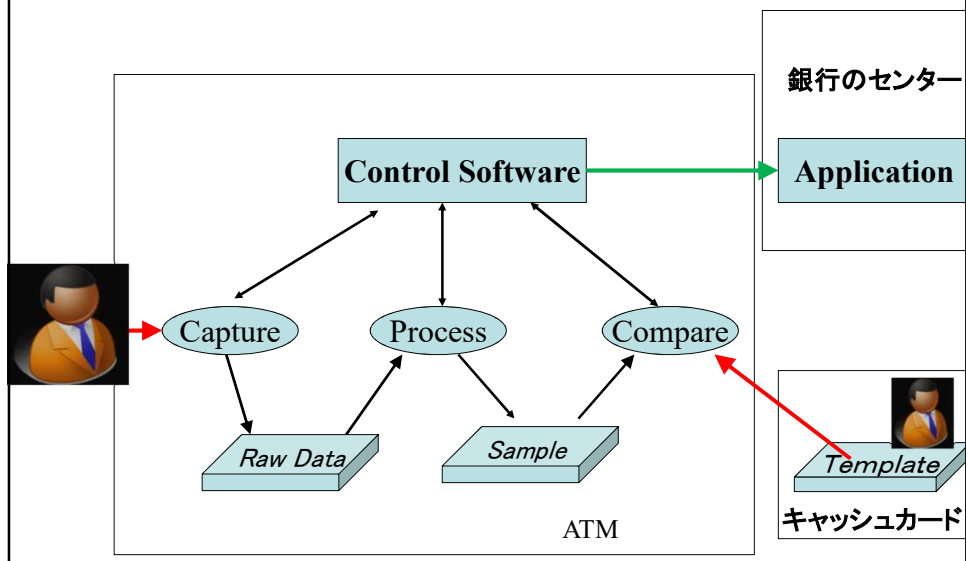
一般的なバイオメトリクス認証プロセス (使用する生体特徴によらず、ほぼ同一)



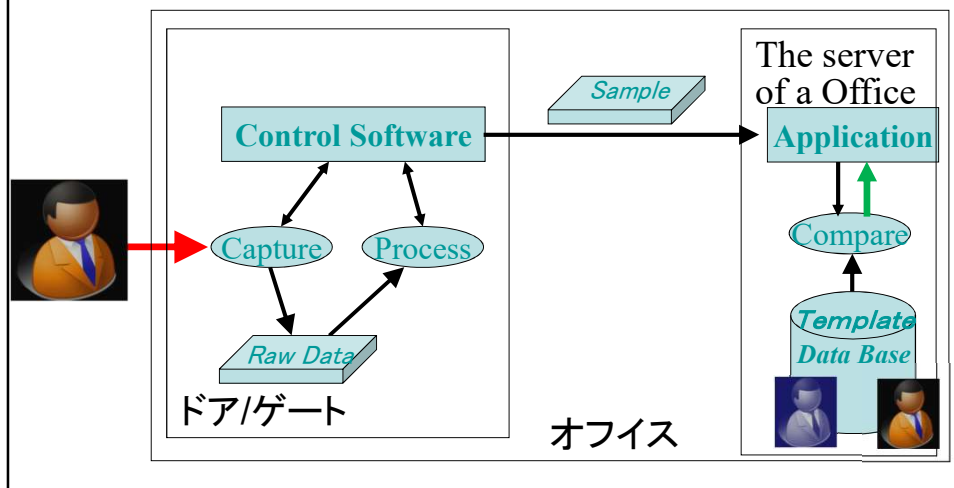
PCへの顔認証適用例



銀行ATMへの顔認証適用例



オフィスの入室管理への顔認証適用例

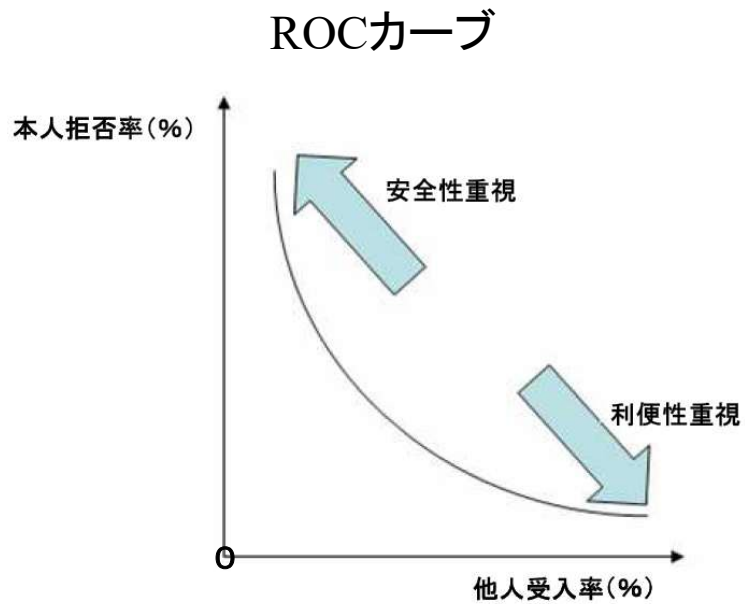


(4) バイオメトリクス認証プロセス

©Advanced IT Corporation 38

FARとFRR

- ① 本人かどうかの判定は、Compare (照合) プロセスの結果
(似ている度合) に基づき行われる
- ② 緩い判定基準にすると、
他人を本人だと間違って判定することもある
この確率を、FAR (他人受入率: False Acceptance Rate)
- ③ 厳しい判定基準にすると、
本人さえも他人だと間違って判定することもある
この確率を、FRR (本人拒否率: False Rejection Rate)



■ 13:45

(5)

バイオメトリクス認証応用の現状・動向

- 5.1 ナショナルセキュリティ
- 5.2 ネット経由の本人確認
- 5.3 店頭での支払い

米国入出国審査におけるバイOMETRICS認証 (US-VISIT)

2001年9月11日の同時多発テロ対応施策の一環

2004年9月30日: 入国審査時に両手の人差し指2本の指紋採取と
顔写真撮影開始(2008年末には、各地の入国審査時に実施)

2006年: ICAO(International Civil Aviation Organization)が、
顔画像必須、指紋と虹彩をオプションとする
MRP(Machine Readable Passport)の仕様を発表

2007年11月29日: ワシントン・ダレス空港にて、
10本の指紋採取が開始(現在は全ての空港で採取)

＜米国の入出国手続紹介動画(10本の指紋+顔画像)＞

① [DHS US-VISIT What to Expect When Visiting the United States\(2:51\)](#)

② [Automated Passport Kiosk\(1:36\)](#) (入国時の自動パスポート検査端末)

2009年7月2日: アトランタ、デトロイトの空港で、
出国審査時のバイOMETRICS利用のトライアルに着手

2015年3月: 出国審査時の顔写真撮影のテスト開始(Biometric Exit)
トランプ大統領の指示により、予定より早く2017年より配備開始

英国の入国審査におけるバイOMETRICS認証 (ePassport gate)

2006年: ICAOがバイOMETRICデータを含むMRPの仕様を発表

2006年: 最初のバイOMETRICパスポートを発行
チップに所有者の情報を格納

2008年: 最初のePassport gateを導入
現在では240以上の

ePassport gateが稼働中
(年間利用登録料: £70~£50)

＜英国の入国時の

自動パスポート検査端末

の紹介(顔画像)＞

[ePassport gate\(2:21\)](#)



アラブ首長国連邦(UAE)の入国審査 におけるバイOMETRICS認証(Smart Gate)

2001年より17箇所の全ての国境審査にて

外国人の入国審査に虹彩認証を採用

UAEは80%が海外の人の入国、1日7000人の海外からの入国
危険人物発見のためのブラックリスト(50万人のDB)利用

2017年: Dubai airportにSmart Gateの導入開始

現在は130台以上のSmart Gateが運用中

従来は入国審査に50分、Smart Gateにより22秒へ短縮

[Smart Gate\(1:58\)](#) <顔画像、指紋、虹彩による自動入国審査>

Emirates IDカード保有者以外は事前登録が必要

2018年: Biometric smart tunnelのトライアル開始

Walk-Throughタイプの入国審査、審査時間は15秒に短縮

日本入出国審査におけるバイOMETRICS認証

2006年3月20日: バイOMETRICSデータを含む

新しいパスポート(IC旅券)へ移行

顔写真を貼り替えたパスポート等を使用してもICチップに記録
されている情報と照合することにより偽造を見破ることが容易

今後、各国の出入国審査等でICチップに記録された顔画像と
その旅券を提示した人物の顔を照合する電子機器が段階的に
整備されていくことにより、他人の「なりすまし」によるパスポート
の不正使用防止の効果が期待

申請手続きは基本的に変わらず。

申請用顔写真の規格が変更

旅券発給手数料が1000円Up



バイオメトリクスを利用した自動化ゲート

指紋認証自動化ゲート: 2009年11月より

日本国籍で有効な日本国旅券を所持しているか、日本の外国人で有効な旅券(パスポート・在留カード・難民旅行証明書又は再入国許可書)を所持している場合に利用可
事前登録が必要なため、全出入国者の約8%にとどまっている

顔認証自動化ゲート: 2017年10月より

日本人の帰国手続きにおいて導入(約10秒で再入国可)

日本人の出国者数、2018年は1895万人

訪日外国人旅行者数の急増への対応

2011年の622万人から急増し、2018年には3119万人

2020年(オリパラ)目標4000万人、2030年目標6000万人

成田でも顔認証導入へ 出入国審査、新ゲート運用開始(2018年6月)

[紹介動画\(1分33秒\)](#)

2019年7月、羽田空港を皮切りに、外国人出国手続きでも運用開始
事前登録不要

ナショナルセキュリティへの応用

①主たる目的は二つ

セキュリティ:

テロリスト、犯罪者の拘束・入出国防止

利便性・効率性:

利用者の利便性(すみやかな入出国)

運用組織の効率性(入出国審査業務・費用負担軽減)

②使用されるバイオメトリクスはICAO標準に準じたもの

必須: 顔画像 オプション: 指紋、虹彩

ACBio (Authentication Context for Biometrics)

①ISO/IEC JTC1 SC27にて国際標準となったネット経由のバイオメトリクス認証に関する技術仕様

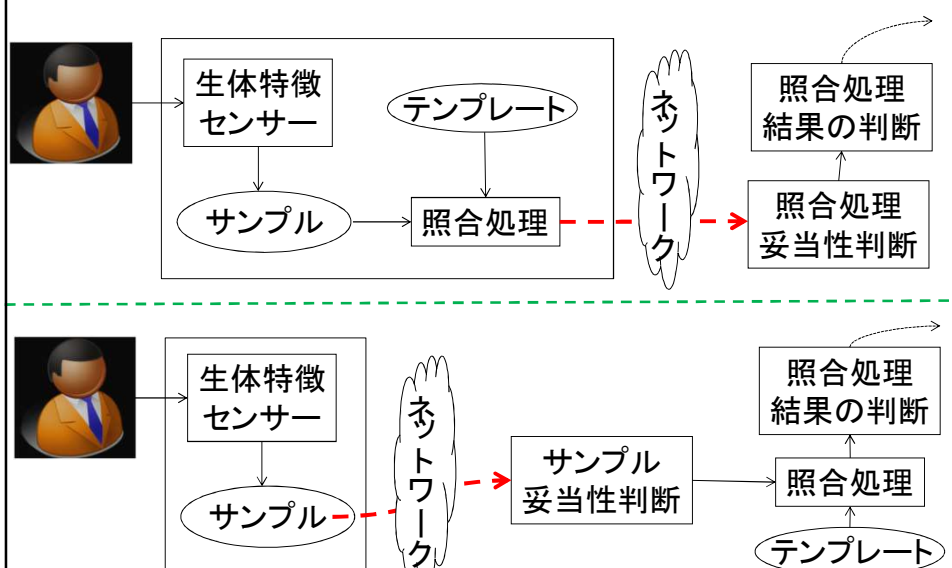
ISO/IEC 24761:2009 “Information technology -- Security techniques -- Authentication context for biometrics”

②認証する組織の管理下に無いバイオメトリクス認証装置によるバイオメトリクス認証結果が信頼できるかどうかを確認可能な仕組み

③2000年頃に、ネット経由のバイオメトリクスによる本人確認を研究テーマとして取り上げ、経済産業省の協力を得、プロトタイプを開発し、2004年にISO/IEC JTC1 SV27/WG2へ提案。2009年に国際標準へ。

■PASS

ACBioによる ネット経由のバイオメトリクス認証構成(例)



FIDO (Fast Identity Online)

①FIDOはその名の通り「高速なオンラインID認証」をめざし、パスワードに代わる新しい認証技術の開発・普及活動を実施する団体。以下の二つの技術仕様がITUにて国際標準へ。

ITU-T X-1277 2018年11月 (Universal authentication framework)

ITU-T X-1278 2018年11月

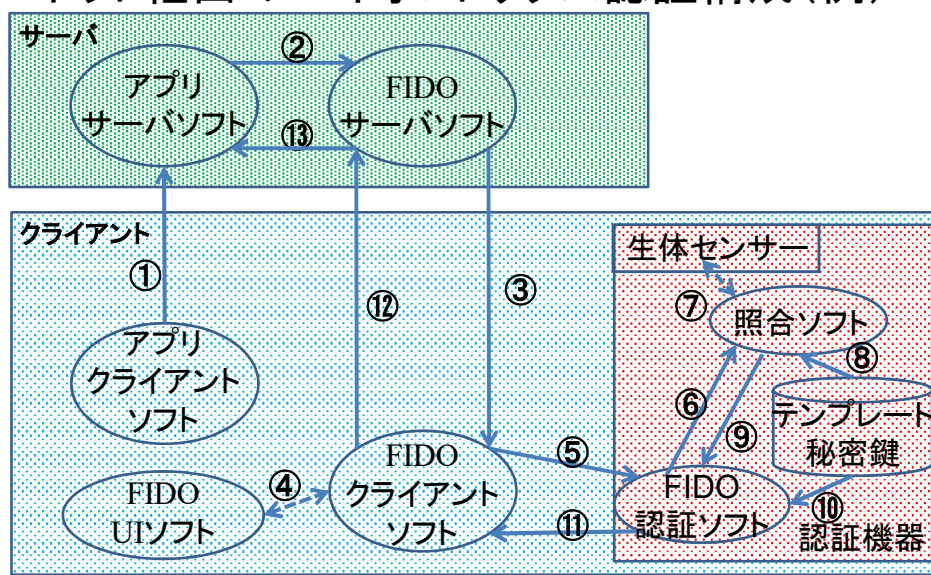
(Client to authenticator protocol/Universal 2-factor framework)

②バイOMETRICSによるパスワードに変わる本人確認方法であり、バイOMETRICSに限らず多様な本人確認方法が可能な仕組み、バイOMETRICSデータをサーバには格納しない仕組みを提案。

③2009年頃から、パスワードの代わりにバイOMETRICSを、という議論が米国で始まり、2012年に国際的な組織FIDO Allianceが発足。様々の技術仕様をまとめ、標準化を推進。日本のNTT DOCOMOも2015年にメンバへ。

もっと広がる生体認証～あんしんをもっと便利に～

FIDOによる ネット経由のバイOMETRICS認証構成(例)



ネット経由の本人確認 ACBioとFIDO 比較

	ACBio	FIDO
国際標準化	2009年 ISO/IEC	2018年 ITU
評価単位	構成デバイス	システム一式
生体認証(ローカル)	○ (サーバにて使用コンポーネント検証)	○ (サーバにて使用システム検証)
生体認証(サーバ)	○ (生体情報採取以外)	×
当人認証	照合処理結果の確認 (生体認証技術)	秘密鍵保有の確認 (公開鍵暗号技術)
	<暗号技術は 生体認証処理結果の確 実な送信に利用>	<生体認証技術は FIDOシステムの 保有者確認に利用>
推進体制	東芝およびパートナー	FIDOコンソーシアム

バイOMETRICS認証による二つの支払い方式

認証サーバ連携決済方式:

生体情報と関連付けられた

デポジット/クレジットカード/銀行口座等からの支払い

デポジット/クレジットカード/銀行口座等に対応付けられている

生体情報と、生体特徴センサーにてその場で採取した利用者の

生体情報の照合が成功すると、

登録されているデポジット/カード/銀行口座等からの決済が可能

オンカード認証決済方式:

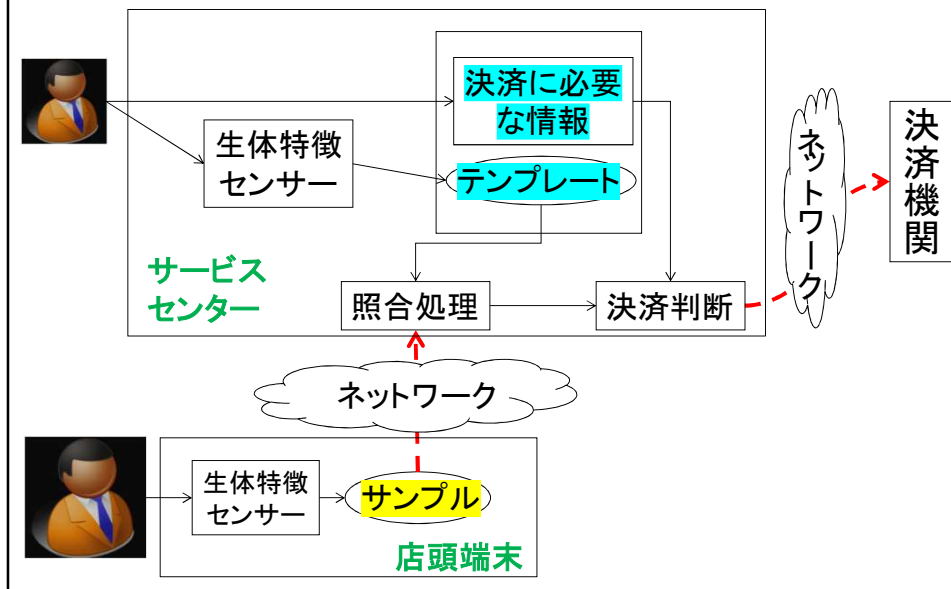
バイOMETRICS認証機能が実装されたカードによる決済

カード上で実施されるバイOMETRICS認証が成功すると、

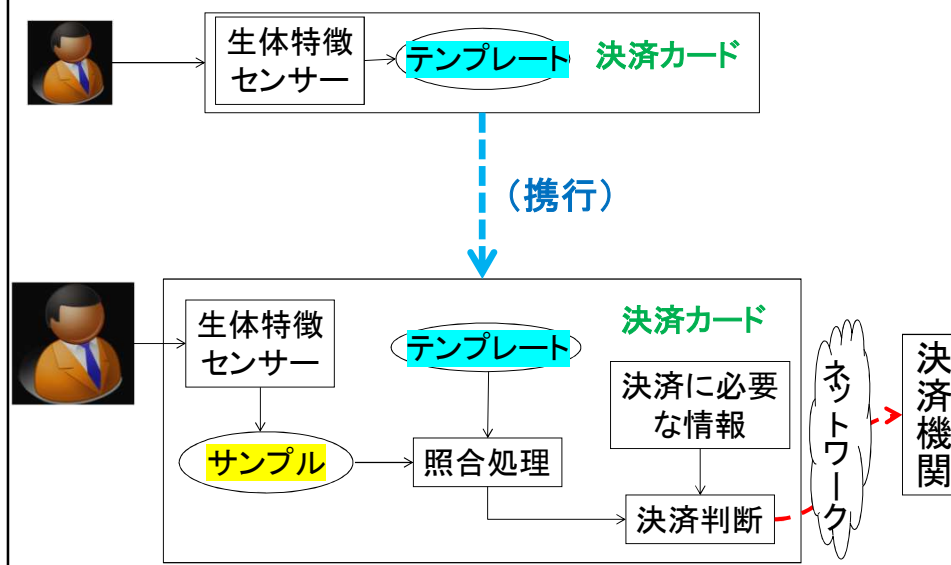
そのカードからの決済が可能

(PIN番号の代わりにバイOMETRICS認証)

認証サーバ連携決済方式の構成(例)



オンカード認証決済方式の構成(例)



認証サーバ連携決済方式 指紋認証の例

デポジット: ハウステンボスマネー(2015年10月31日サービス開始)

登録: ハウステンボスの会員窓口にて、

電話番号と指紋を指紋認証端末にて登録、その場でチャージ

利用: 利用可能店舗にて、会計の際に指(人差し指と親指)を

タッチするだけ(追加のチャージは各店舗で可能)

銀行口座: 「PASS」三菱地所にて2018年より実証実験

登録: 指紋、銀行口座、個人情報等を登録

利用: 社員食堂等における指紋による決済

クレジットカード: 「Touch&Pay」2017年10月より本格展開(全国へ拡大)

登録: 入国時に空港で

クレジットカード番号、指紋、パスポート情報等を登録

利用: 指紋により、クレジットカード決済、ホテルチェックイン

[Demonstration experiment of Kanto region \(3:37\)](#)

認証サーバ連携決済方式 顔・静脈認証の例

顔認証

2017年9月: アリババグループ・Ant Financialは顔認証決済サービス

‘SMILE TO PAY’を中国にてサービス開始

登録: 支払サービスALIPAYのアカウントと顔画像を紐づけ

利用: 顔認証後、携帯番号を入力

[“smile to pay” at KPRO\(KFC\) \(1:38\)](#)

2019年3月: 日本電気(NEC)は顔認証技術を使った

クレジットカード決済サービスの実証実験を開始

静脈認証

2018年9月: イオンクレジットサービスは

手のひら静脈認証を活用したカードレス決済の実証実験を開始

2019年3月: 東芝テック、日立等は、

指静脈認証による決済の実証実験を開始

オンカード認証決済方式 指紋認証の例

Mastercard: 指紋認証クレジットカード
南アフリカ、ブルガリア、メキシコにて
実証実験中

[MasterCard biometric card\(1:52\)](#)



VISA: コンタクトレス指紋認証クレジットカード(キプロスで実証実験中)
指紋認証銀行カードも実証実験中

[VISA biometric card\(0:34\)](#)

日本: 凸版印刷がフランスのIDEMIA
と連携し指紋認証クレジットカード開発
JCBが実証実験中



店頭での支払いへの応用

① バイオメトリクス認証応用は大きく2種に分類

認証サーバ連携決済方式

利用時の決済には、店舗以外のセンターのサポート要

オンカード認証決済方式

利用時の決済には、店舗端末のみで可能

② 実用化は未だこれから

特定のサービス組織内運用で、

認証サーバ連携決済方式の実用化が始まっているが

オンカード認証決済方式は未だ実証実験レベル

< 本日の内容 > バイオメトリクス認証

- (1) バイオメトリクス認証とは
- (2) 本人確認方法における
バイオメトリクス認証の位置づけ・特徴
- (3) 主要なバイオメトリクス認証方式概要
- (4) バイオメトリクス認証のプロセス
- (5) バイオメトリクス認証応用の現状・動向
 - 5. 1 ナショナルセキュリティ
 - 5. 2 ネット経由の本人確認
 - 5. 3 店頭での支払い

終りに

1. バイオメトリクスは確実に皆さんの生活の場へ浸透しつつある。
2. 一方、まだまだ解決すべき課題も多く、研究・技術開発の対象テーマの宝庫であり、
3. また、先駆的応用は始まりつつあるも、新たな応用、事業創出の宝庫でもある。
4. 本講義が、それぞれの立場で、バイオメトリクス分野へ関心を持っていただけるきっかけになれば幸いです。

終