情報セキュリティトピックセミナー

高度情報化社会を支える本人確認技術

才所　敏明
(株)IT企画　代表取締役社長
中央大学研究開発機構　客員研究員
toshiaki.saisho@advanced-it.co.jp

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
＊法政大学、日本大学で情報セキュリティに関する講義担当

2013年5月～　中央大学研究開発機構

＊国立研究開発法人情報通信研究機構（NICT）より受託した「組織間機密通信のための公開鍵システムの研究開発」PJより研究員として参加

本日のお話

（1）本人確認方法の分類・特徴

（2）記憶による本人確認方式
　　固定パスワード、ワンタイムパスワード

（3）持物による本人確認方式
　　ワンタイムパスワードトークンの保有を確認
　　レスポンス生成機能の所有を確認
　　コミュニケーションチャネルの所有を確認

（4）生体特徴による本人確認方式
　　主要な生体特徴による本人確認方法
　　　指紋認証、顔認証、虹彩認証、静脈認証

　　インターネット越しの生体特徴による本人確認の課題
　　　ACBIOによる克服のアプローチ
　　　FIDOによる克服のアプローチ

（5）終りに
　　NAF（National Authentication Framework）の必要性について
　　本人確認技術・サービスとの付き合い方について

（1）本人確認方法の分類・特徴

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）

5

（2）記憶による本人確認方式

記憶による本人確認方式の例

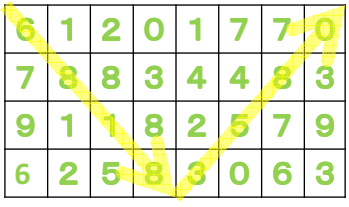
＊固定パスワード
　本人しか知らないはずの文字列（固定）による本人確認
　あらかじめ登録した質問に対する回答による本人確認

＊ワンタイムパスワード（記憶によるチャレンジレスポンス方式）
　本人しか知らないはずの情報（固定）
　をもとに生成された文字列による本人確認

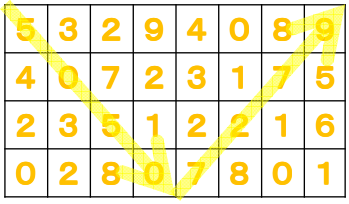
　マトリクス認証　（九州大学や青山学院大学等）
　イメージングマトリクス認証　（東北大学等）

マトリクス認証の例

①あらかじめパターン（パスワード）を登録　＝＞ V
②受け取ったマトリクスの、パターン上の
　　数字の列が（ワンタイム）パスワード



左図のマトリクスの場合
68183580



左図のマトリクスの場合
50507279

イメージングマトリクス認証の例

①あらかじめ動物の列（パスワード）を登録 ＝＞ 
②受け取ったマトリクスの、動物の位置の
　　数字の列が（ワンタイム）パスワード

	25	90	32
42			
66			
80			

左図のマトリクスの場合
802566324290

	67	04	21
33			
29			
45			

左図のマトリクスの場合
332129044521

記憶による本人確認の特徴・課題・対策

特徴
- パスワード記憶方式であり簡便
- 日常使い慣れた方式

課題
- 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、メモ作成➔盗用の危険
- 持物、生体特徴による本人確認に比べ、
  盗用され、悪用されても、気づきにくい

対策
- 複数のパスワード、秘密の質問により再確認すること
  （リスクベース認証）
- サービスへのログオン時には、
  必ず前回のログオン日時を確認すること
- 推測されにくいパスワードの設定、
  定期的な更新、使い回しをしない

10

（3）持物による本人確認方式

持物による本人確認方式の例

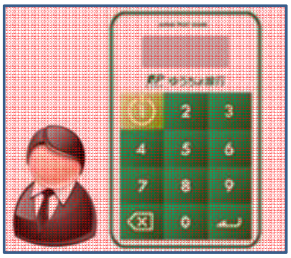
＊ワンタイムパスワードトークンの保有を確認
　専用のハード、ソフトの保有を確認
　ゆうちょ銀行（HS）、みずほ銀行（H）、
　　三菱東京UFJ銀行（HS）等で導入

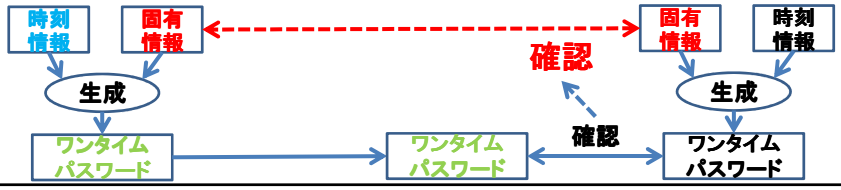
＊レスポンス生成機能の所有を確認
　固有の秘密情報、レスポンス生成機能の所有を確認
　みずほ銀行で導入

＊コミュニケーションチャネルの所有を確認
　専用のコミュニケーションチャネル・機器の所有を確認
　ゆうちょ銀行（メール）、みずほ銀行（メール）等で導入

ワンタイムパスワードトークン保有確認の例（時刻同期方式のハードウェアトークン）

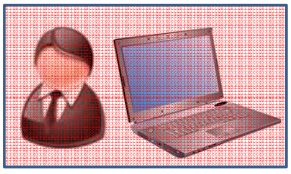
①固有の情報を保有し時刻を同期させたトークンを配布
②固有の情報＋時刻情報から生成した
ワンタイムパスワードにより当該トークン保有を確認

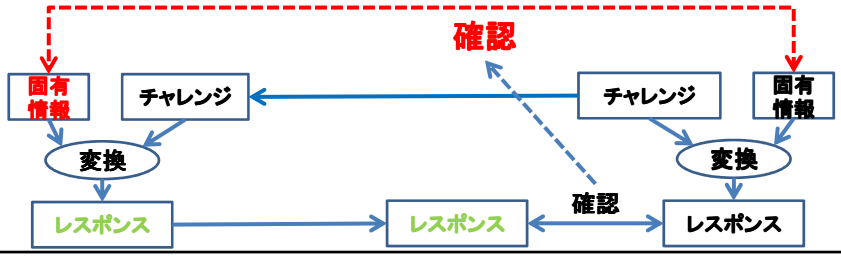




レスポンス生成機能所有確認の例

①あらかじめ固有の情報、レスポンス生成機能を配布
②送付したチャレンジに応じ生成したレスポンスにより
あらかじめ配布した固有情報、レスポンス生成機能の保有を確認

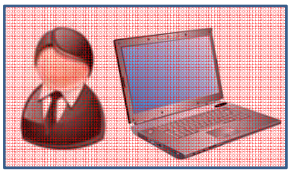


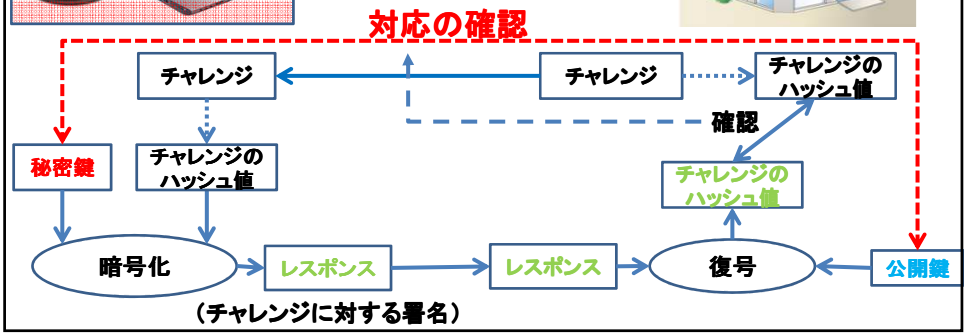


暗号技術を利用した
レスポンス生成機能（秘密鍵）所有確認の例

①公開鍵暗号の秘密鍵（固有の情報）、署名機能の保有が前提

②送付したチャレンジに対し、秘密鍵で付与した署名により
秘密鍵（固有の情報）、レスポンス生成（署名）機能の保有を確認

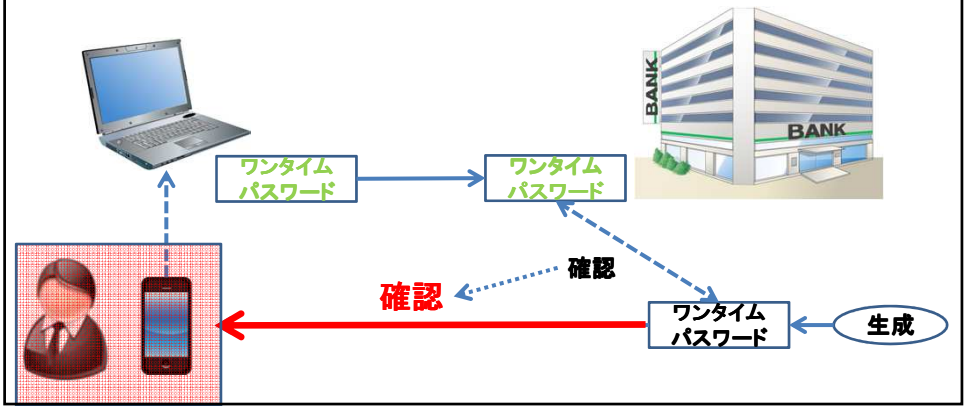




コミュニケーションチャネル所有確認の例
（スマホ向け電子メール）

①あらかじめ使用するメールアドレスを指定する

②メールアドレスに届いたワンタイムパスワード
により指定メールアドレス、スマホの所有を確認



持物による本人確認の特徴・課題・対策

特徴

* カード、スマホなどによる認証方式
* 日常的に使われ始めてきた

課題

* 常時携行が必要
* 生体特徴による本人確認に比べ、
  紛失・破損・盗難の危険大

対策

* 持物の所有者が正当な所有者かどうかの確認
  （PIN、パスワード、生体特徴の利用）

17

（4）生体特徴による本人確認方式

生体特徴による本人確認方式とは

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、その人と判断している。

生体特徴による本人確認（システム）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、あらかじめ登録した人である、
と判断する方式。

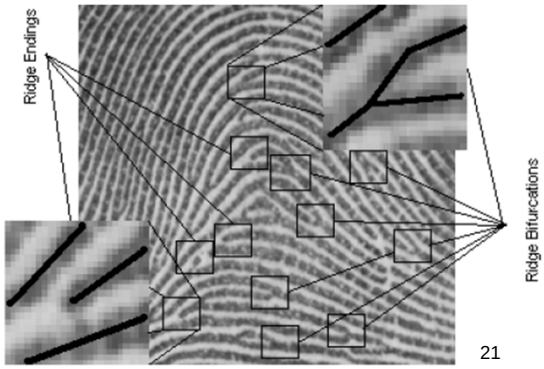
19

主要な生体特徴による本人確認方法

＊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



21

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

22

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

23

入退室時の本人確認への応用例

サーバ室

個人住宅

24

指紋認証による決済　Liquid Pay

Liquidが2015年2月9日に開始した、**指紋認証式のデポジット決済サービス「Liquid Pay（リキッド・ペイ）」は、指紋を決済IDとし、導入した店舗の登録専用の端末で指紋を登録、スマホなどのアプリ経由でクレジットカード情報の登録を行い準備が完了**するシンプルなもの。**商品決済時は指紋だけで決済が完了**。

このサービスの**実用例として、昨年10月31日に始まったハウステンボス園内での決済サービス**がある。これほど大規模な導入例は世界でも例を見ない。数百万人規模が来場するハウステンボスでは、園内で使用できる「テンボス通貨」という決済システムがあり、Liquidが提供する生体認証決算システムLiquid Payを使って園内で決済。

入園時に指紋を登録し、金額をデポジットすることで、園内の端末で指をタッチするだけで支払いが完了。

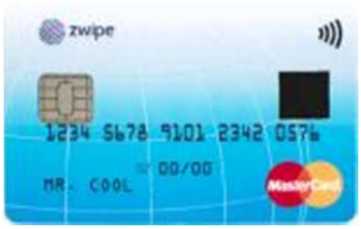
25

http://ecclab.empowershop.co.jp/archives/5242

指紋認証による決済　Zwipe

Zwipeは、2014年10月にMasterCardと提携し、非接触型のカード発行を目指した取り組みを推進。

この非接触型のカードは指紋センサーを搭載したもので、指紋データは直接カードに記載。外部データベースに登録をしないことで手軽さとセキュアさを実現しようとしている。また、**指紋をスキャンするだけで非接触決済を行うことができるので、PINコード（暗証番号）入力なしの支払いが可能**となった。



26

http://ecclab.empowershop.co.jp/archives/5242

外国人客、指紋認証で日本観光 政府実証実験へ

政府は今夏、**外国人観光客が指紋認証だけで買い物や本人確認ができるシステム**の実証実験を始める。

現金やクレジットカードを持ち歩かずに済む利便性や防犯効果をアピールし、訪日外国人の増加につなげたい考えだ。**2020年東京五輪・パラリンピックまでの実用化**を目指している。

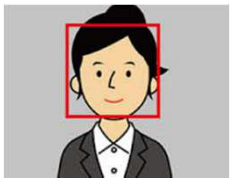
計画では、**外国人旅行者は空港などで指紋やクレジットカード情報などを登録**。店頭に置かれた専用端末で、**指2本の認証を行うだけで支払いや免税手続きが可能**になる。また、旅館業法に基づき、外国人旅行者にはホテルや旅館に泊まる際にパスポート提示を求めているが、指紋認証での代用を認める方針だ。

実証実験には、外国人に人気が高い神奈川県の**箱根と鎌倉、湯河原、静岡県の熱海にある約300の土産物店や飲食店、ホテルなどが参加**。来年春までに**東北の観光地や名古屋の市街地などにも順次広げ、20年には東京など全国で実用化する計画**だ。

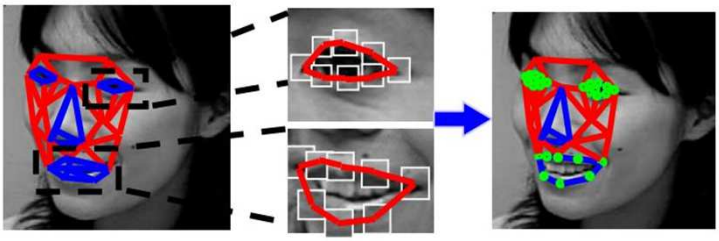
27

2016年4月8日　読売新聞から

顔（1）

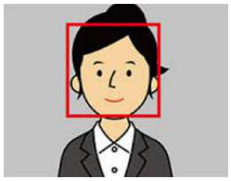


- **照合方法**
  - 目や口等の代表的な顔の部品の位置を原点にして、その他の部品の位置を位置データとして2次元的に照合する方法と、何らかの計測法を用いて鼻の高さや頬の形のような3次元構造を抽出し照合する方法がある



28

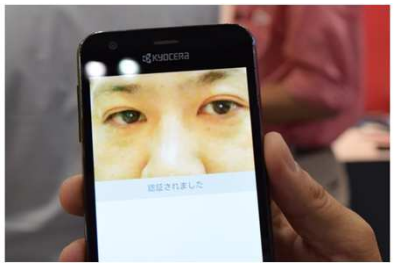
顔（2）



- 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

29

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

30

入退出時の本人確認への応用例

執務室入室時

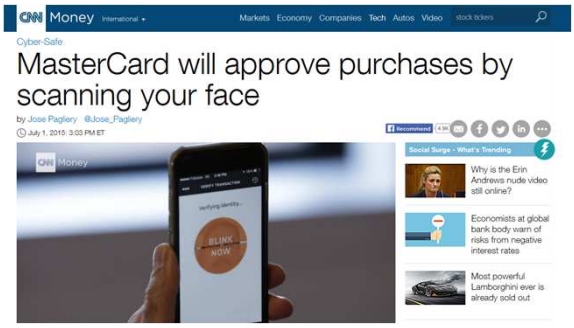
自社ビルへの入館時

31

顔認証による決済　Master Card

米国Master Cardは、パスワードの代わりに顔の情報を使って本人確認を行う決済認証システムの実験を予定。

規模としては500人程度の買い物客が参加する限定的なものとなるが、結果を検証した上で、外部への提供も検討していく方針だ。



32

http://ecclab.empowershop.co.jp/archives/5242

財布のいらない社会に？
企業が続々と「顔認証決済」を実証実験

三井住友が2017年にも実証実験？

読売新聞は22日、三井住友フィナンシャルグループが「顔パス」決済の実用化に向けた検討を進めていると報じた。

顔の情報を事前登録して画像データから本人を認証する実証実験を2017年にも小売店で始め、数年以内の実用化を目指すという。

既に実証実験を始めている企業も！

「顔認証」決済の実現に向けては、複数の企業が取り組みを始めている。

NECは現在、自社ビルの売店で「顔認証決済サービス」の実証実験を実施。

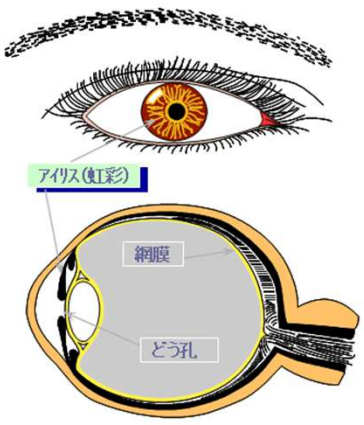
広島銀行も今年2月から、本店の食堂で「顔認証」による決済の試行をスタート。技術の特徴を確認した上で、地域電子マネーへの導入など、より利便性の高い決済環境を提供していきたいとしている。

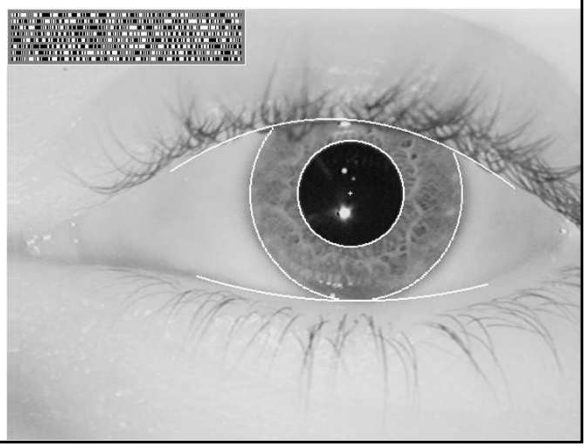
33

2016年8月23日　livedoorNewsより

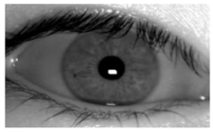
虹彩（1）

- 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
  - 個人性が高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。

35

個人用機器の本人確認への応用例

スマートフォン

日テレ・虹彩認証TV放送（4分4秒）

36

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

37

虹彩（Iris）認証による 将来の認証・決済基盤のイメージ：Okko

（1）利用登録
　　FaceToFaceの本人確認　個人IDと虹彩の登録
（2）Okkoシステムの説明
（3）レストランでンの支払い
　　テーブルで個人IDと虹彩で支払い　メールによるレシート送付
（4）、（5）医者との面談
（6）薬局での薬の受け取り
（7）空港でのボーディングパス無しのチェックイン

Okkoid.com.flv （Okkoidビデオ：6分33秒）

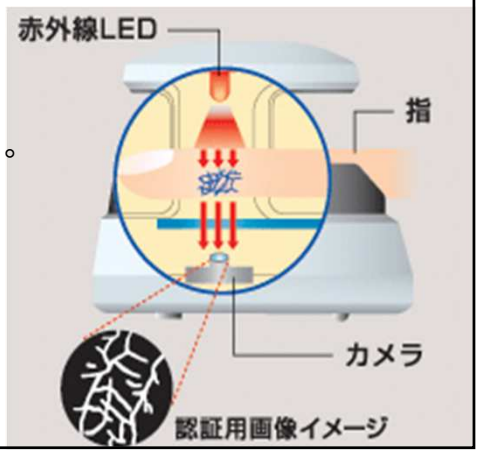
38

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。

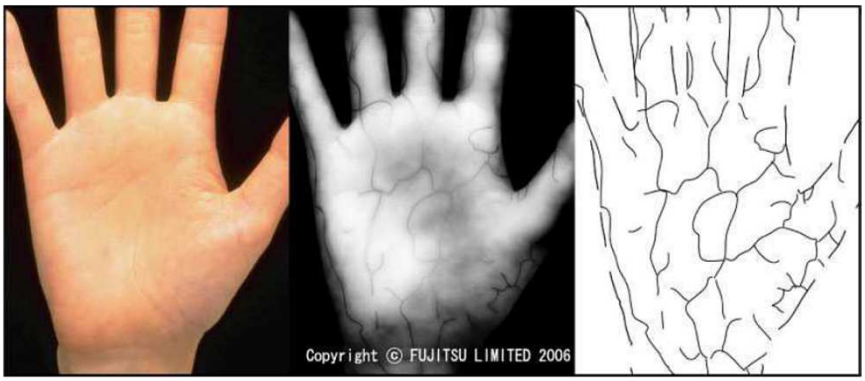


静脈（2）

- 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

40

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

41

生体認証導入・運用のためのガイドライン（IPA)より

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

42

ATMへの応用

指静脈認証

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

手のひら静脈認証

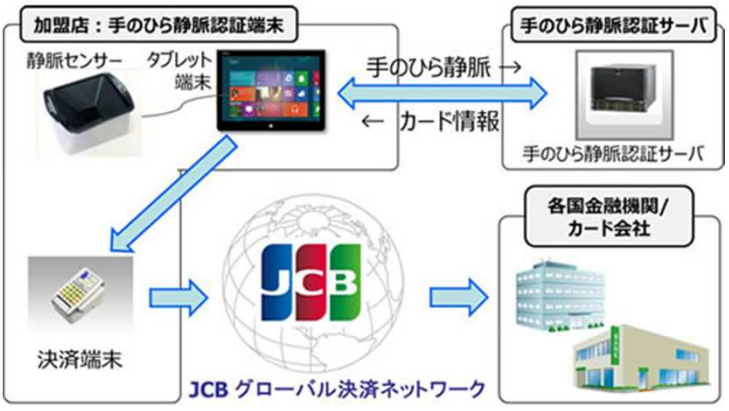
出典:http://jbpress.ismedia.jp/articles/-/42629

43

静脈認証による決済　富士通/JCB

富士通と富士通フロンテックは、JCBのグローバル決済ネットワークに富士通の**手のひら静脈認証技術を取り入れ、カードレス決済システムを構築**。

まず**手のひら静脈情報を、カード情報と共に富士通のデータセンター内の手のひら静脈認証サーバに登録**しておく。そして買い物の際に、**手のひらを静脈センサーにかざし、手のひら静脈認証サーバから合致するカード情報が読み出され、決済**が行われるという仕組みだ。



http://ecclab.empowershop.co.jp/archives/5242　http://pr.fujitsu.com/jp/news/2015/10/7.html

本人確認方法の比較の例

	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になる

45

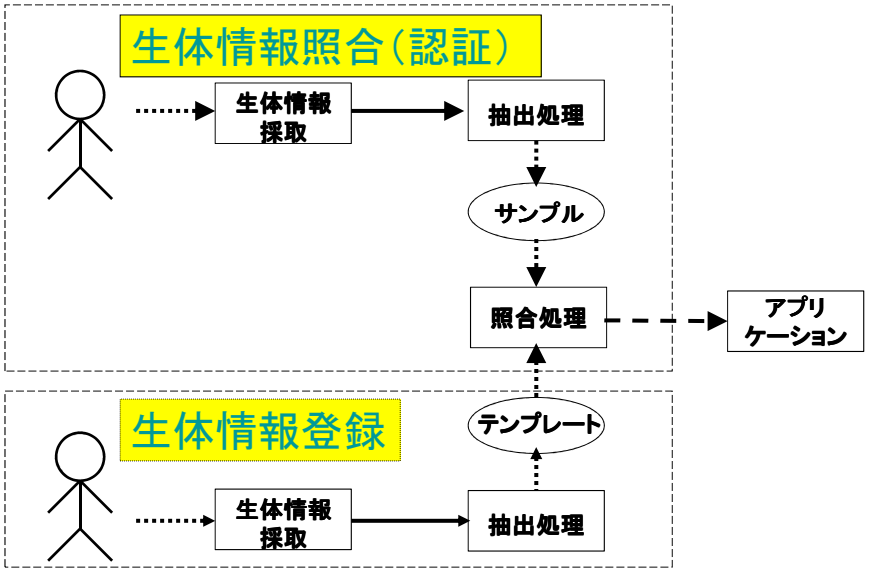
生体特徴による本人確認の基本

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

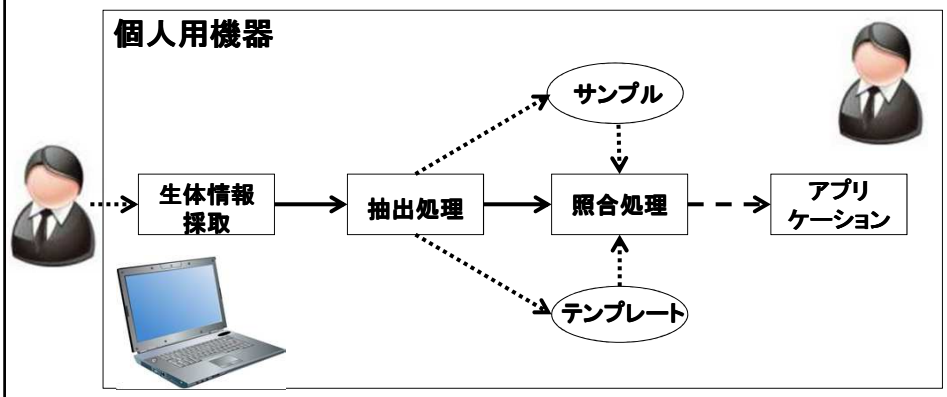
46

生体特徴による本人確認プロセス
（使用する生体特徴によらず、ほぼ同一）



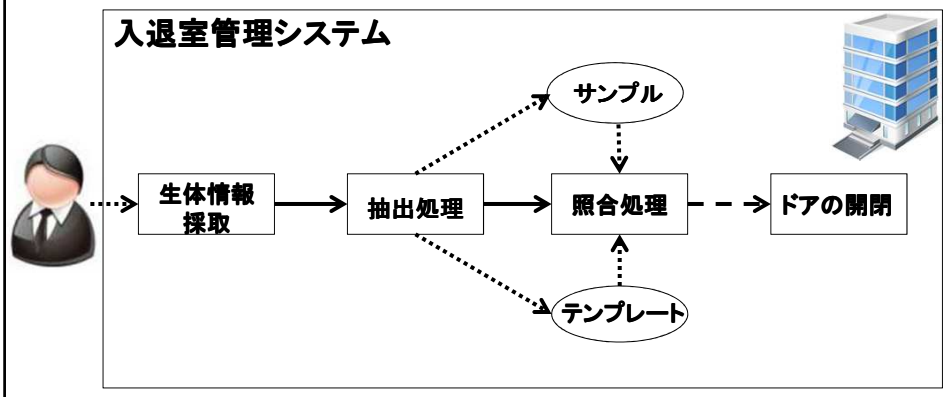
47

個人用機器利用時の
生体特徴を利用した本人確認の場合



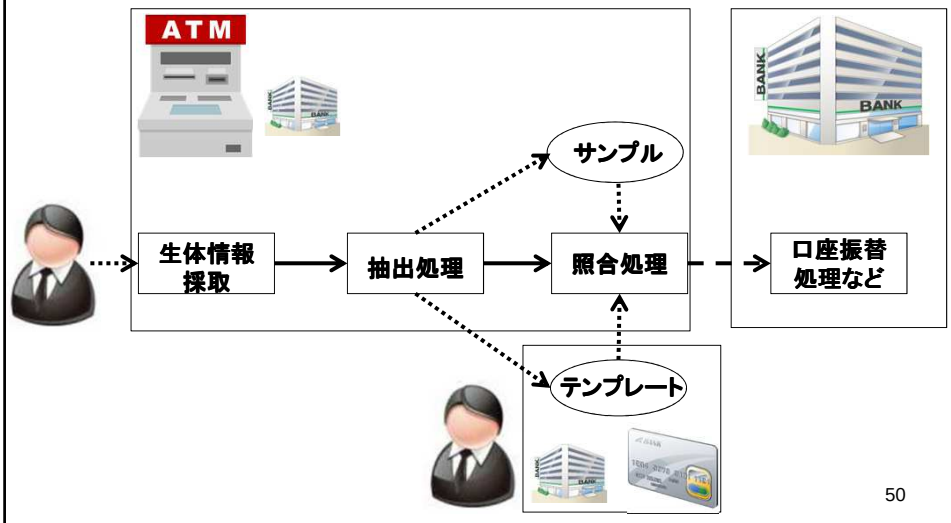
48

入退室時の
生体特徴を利用した本人確認の場合



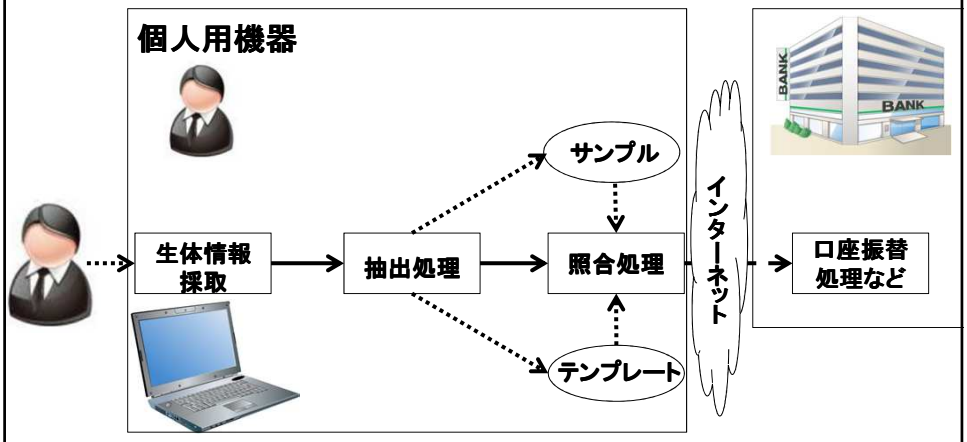
49

ATM利用時の
生体特徴を利用した本人確認の場合



50

では、自宅のPCを使用した 生体特徴による本人確認の利用は？



本人確認結果を受け取る組織が、
その結果を信じて良いのかどうか？

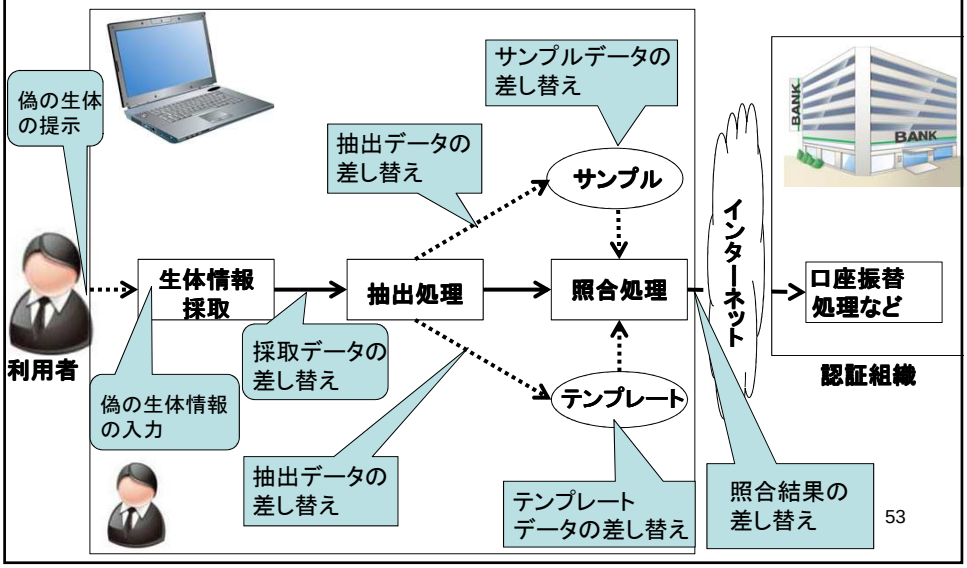
＝＞ No!

51

インターネット越しの 生体特徴による本人確認の課題

認証組織にとってのリスク

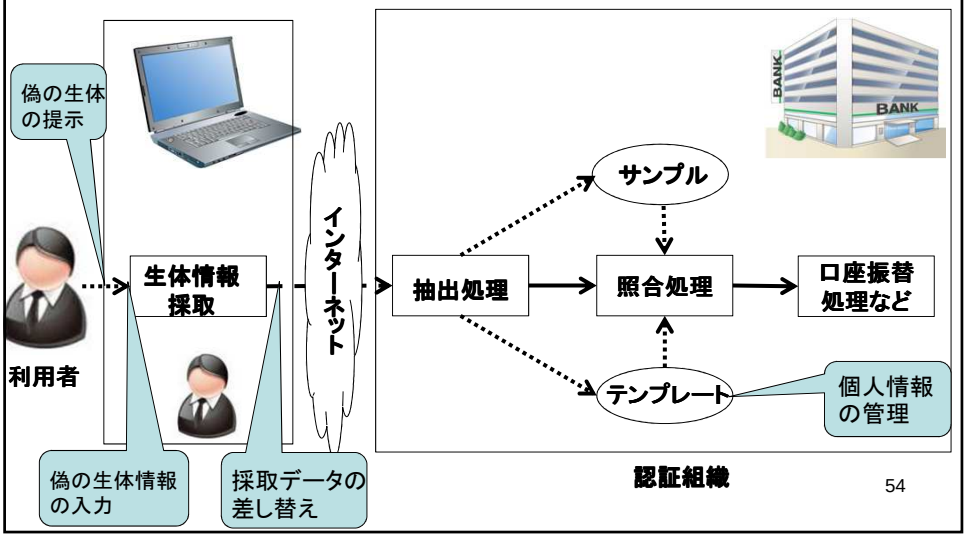
＜インターネット越しの生体特徴による本人確認モデル（1）＞



53

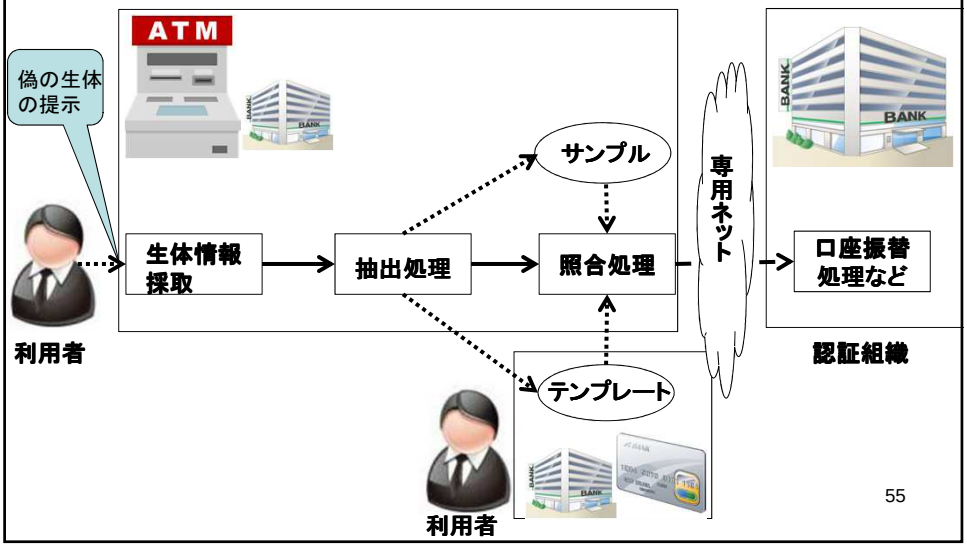
認証組織にとってのリスク

＜インターネット越しの生体特徴による本人確認モデル（2）＞



54

では、ATM利用時の生体特徴を利用した本人確認の場合は？



55

利用者の手元で実施する生体特徴による本人確認結果を認証組織が信頼できるためには

以下の条件を満たしている利用者システムで実施された本人確認結果であることを認証組織が確認できること

（1）高精度の本人確認が可能な技術に基づくシステムを使用

（2）システムが改ざんされることなく、正しい状態で実行

（3）システムが使用するデータの改ざんや差し替えが無い

（4）偽の生体提示に騙されない工夫が施されている

56

利用者の手元での生体特徴による本人確認の結果が認証組織として信頼できるためのアプローチ

[1]利用者システムは、「生体特徴による本人確認結果」のみでなく、使用した機器・装置群やパラメータ設定等の処理の情報を認証組織へ通知する

（認証組織は、装置の安全性、機能性についての評価結果を入手可能とする）

＝＞ACBIOが採用したアプローチ

（機器が未成熟な中で、認証組織で判断可能なように）

[2]安全性や機能性についてあらかじめ評価されている装置を利用することを前提とし、利用者システムは「生体特徴による本人確認結果」のみではなく、使用した装置の情報を認証組織へ通知する

（あらかじめ評価されている装置の情報は信頼できる機関から入手可能とする）

＝＞FIDOが採用したアプローチ（市販機器が成熟してきたため、可能に）

57

ACBIO

（Authentication Context for BIOmetrics）

＊インターネットなどのオープンなネットワーク上で「生体特徴による本人確認」を利用するための技術規格

＊利用者の手元で実施した「生体特徴による本人確認結果」と共に、本人確認プロセスの情報をサービス提供者に安全に提供するためのデータ内容・構造を定めたもの

＊この規格に準拠したデータを利用者がサービス提供者へ提供することで、サービス提供者は本人確認結果とその信頼性を検証できる

58

ACBIOの歴史

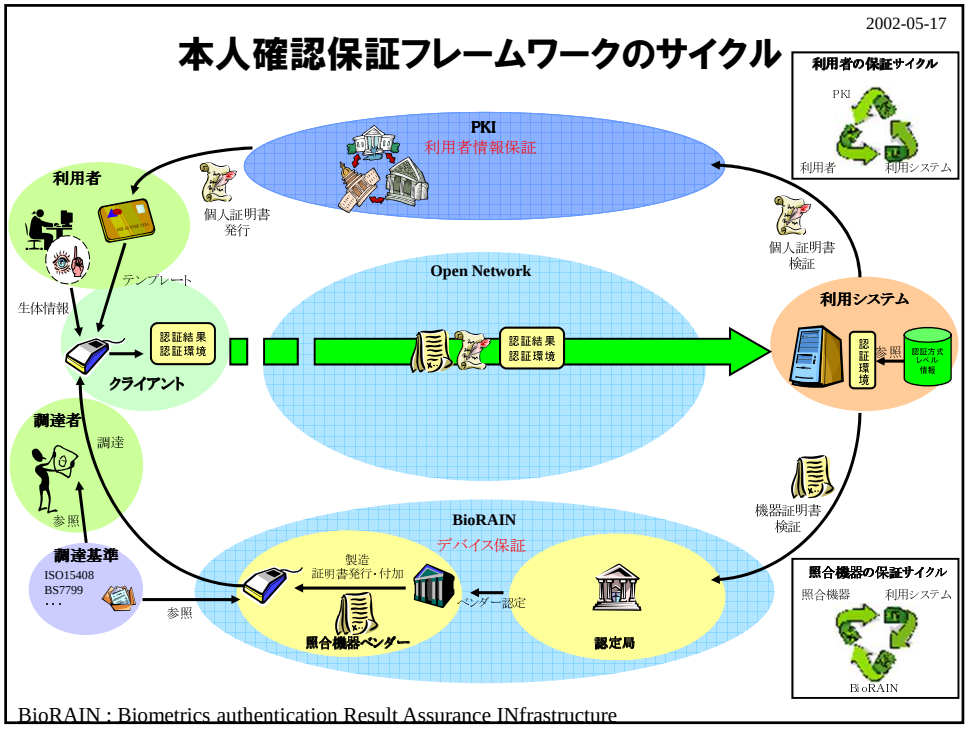
＊2000年頃より構想策定開始
　　経済産業省の支援を受け、詳細技術検討
＊2004年、ISO/IEC SC27 WG2へ提案実施
＊2005年、ISO/IEC SC27 WG2のPJとして承認される
　　連携先は以下の通り
　　ISO/IEC SC17（ICカード）
　　ISO/IEC SC37（バイオメトリクス）
　　ITU-T SG17（セキュリティ）
＊2007年、WD、1stCD、2ndCDを経て、FinalCDを提出
＊2009年、ISとして承認　ISO/IEC 24761
　　Information technology – Security techniques –
　　Authentication context for biometrics

59

ACBIOの目的

＊利用者の手元で実施された「生体特徴による本人確認」の結果の信頼性のレベルを評価できる情報をサービス提供者に提供すること
＊生体特徴による本人確認プロセスを構成する各デバイスごとに、
　デバイス証明書、デバイスの動作条件、
　デバイス間の情報の授受の妥当性を検証可能なデータ
　をまとめ、安全にサービス提供者側へ提供
＊デバイス証明書はインターネット上で入手可能で
　以下の情報などが記載されているものとする
　　ベンダーコード、モデル番号、機器番号、
　　機能性評価書へのポインター、安全性評価書へのポインター
＊機能性評価書もインターネット上で入手可能で、
　　精度に関する評価情報が記載されているものとする
＊安全性評価書もインターネット上で入手可能で、
　　耐タンパー性に関する評価情報が記載されているものとする

60



BioRAIN : Biometrics authentication Result Assurance INfrastructure

FIDO（First IDentity Online）

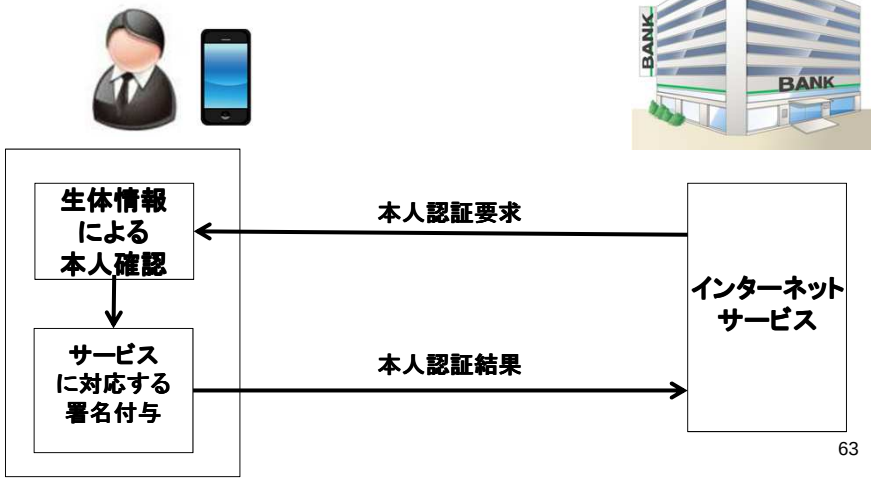
＊米国のFIDO Alliance（2012年発足）が策定を進めている生体情報を利用するオンライン認証の規格。

＊汎用性・相互運用性に配慮された方式で、FIDOを採用したサービスシステムでは、端末機種や生体特徴の種別に依存せず、生体情報を利用するオンライン認証が可能。

＊「FIDO」を使うことで、IDやパスワードを入力することなく簡単にオンライン認証を行うことが可能。

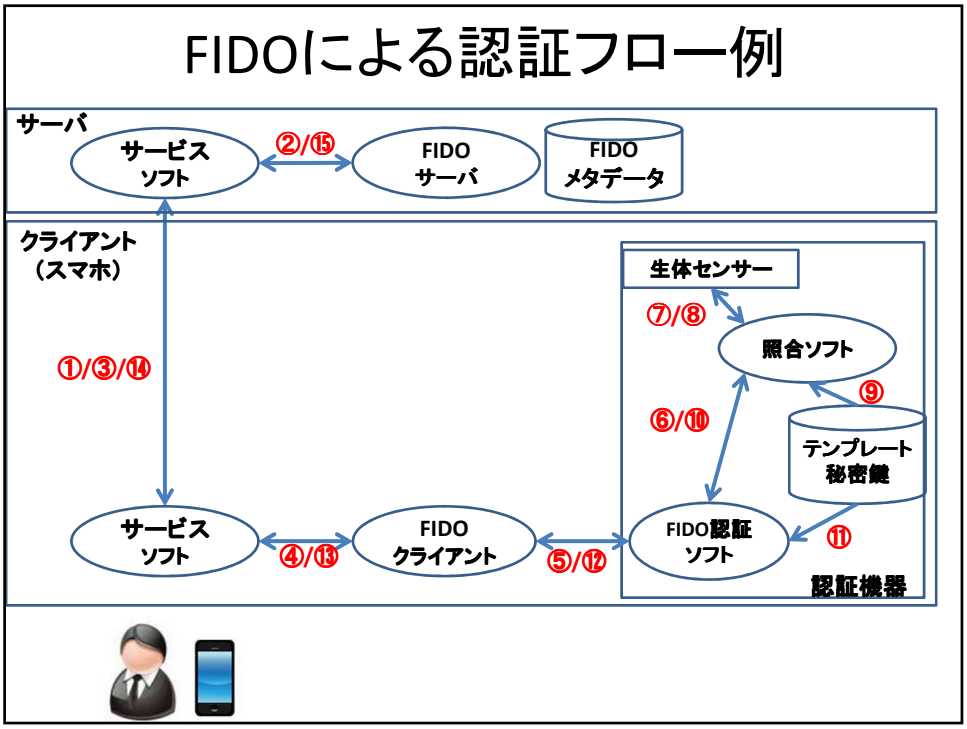
62

FIDO（First IDentity Online）



63

FIDOによる認証フロー例



FIDOの歴史

2012年　PayPal、Lenovo、Nok Nok Labsなどの6社によって
FIDO Alliance設立
2013年　FIDOが一般公開（public launch）
2014年　米Google、米PayPal、米Microsoft、米Amazon、
米Dell、中国Alibaba グループなど手企業が加盟
課名団体が150を突破
（日本：ISR、（株）ディー・ディー・エスが加盟）
2014年12月　FIDO1.0仕様を公開。
2015年　GoogleやYubicoなどの31製品がFIDO1.0認定
(株)NTTドコモがFIDOにボードメンバーとして加盟
米国立標準技術研究所（NIST）、
英U.K.'s Office of the CabinetがFIDO加盟
（Government Class Memberとして）
2016年9月21日のメンバ数：264
Board Level Member（$50,000）:30
Sponsor Level Member（$25,000）：81
Associate Level Member（$2,500～$15,000）：153

Board Level Members（30）

Sponsor Level Members（81）

日本企業一覧

DDS DIGITAL DEVELOPMENT SYSTEMS
FUJITSU
MUFG Bank of Tokyo-Mitsubishi UFJ
Rakuten
DNP
isr International Systems Research Co.
Yahoo! JAPAN

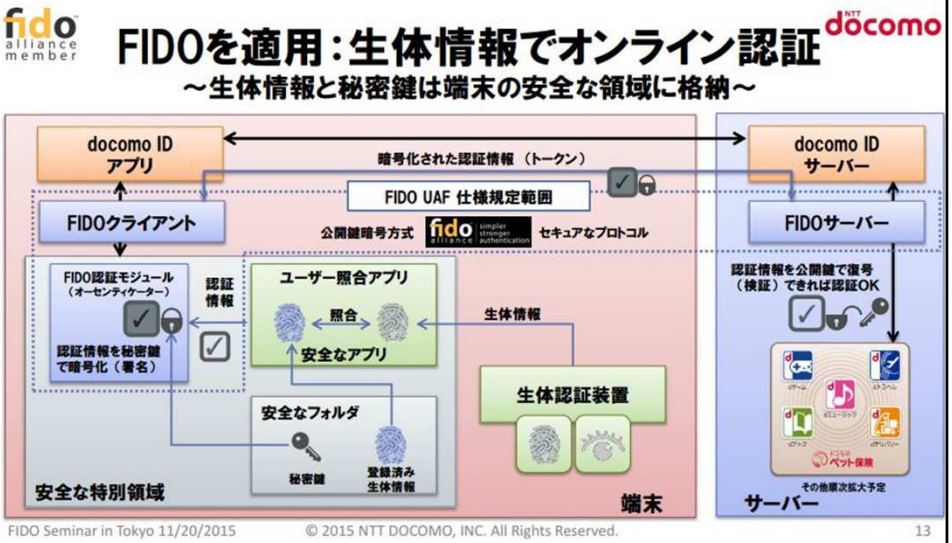
NTTドコモのUAF導入事例紹介（1/3）

第2回 FIDOアライアンス東京セミナー（2015年11月20日） NTTドコモ資料より

NTTドコモのUAF導入事例紹介（2/3）

第2回 FIDOアライアンス東京セミナー（2015年11月20日） NTTドコモ資料より

NTTドコモのUAF導入事例紹介（3/3）



第2回 FIDOアライアンス東京セミナー（2015年11月20日） NTTドコモ資料より

FIDOの可能性と課題

（1）ACBIO構想を策定した15年前と比べ、
技術も製品も大幅に改善された現状を活用した構想

（2）暗号技術を搭載した機器の保有の確認と、
その機器の所有者の確認を組み合わせた技術

（3）機器の所有者の確認には、生体特徴の代わりにパスワードの利用にも対応

（4）利用企業の導入負担の、大幅な軽減が期待できるビジネスフレームワーク

（5）多くの企業、製品開発企業、利用企業、クラウド企業が結集

（6）かなり複雑な仕様で、導入・実装負担は利用企業にはまだ荷が重いか

（7）製品の技術評価は現在は製品開発企業の自己評価、
第3者評価の仕組みを期待したいが
（第3者による評価ビジネス、保険ビジネスなどの可能性）

生体特徴による本人確認方式のまとめ

（1）記憶とか持物に寄らず、直接本人を確認する方式
（2）生体特徴固有の課題がある
　　環境により特徴取得が困難/リトライの必要性
　　年齢による変化、対応できない人の存在
（3）多様な方式が存在、用途ごとに選定要
（4）インターネット経由の利用上の課題が存在しているが、
　　近年、克服のための活動が本格化
　　＝＞ACBIO、FIDO（Fast IDentity Online）
（5）リアルな生活の場面での利用も
　　新たな局面に（カード、現金レス決済）
　　＝＞スマートシティ、観光客対応（東京オリンピック）
（6）各国のボーダーセキュリティへの応用が活発
　　＝＞日本（指紋、顔）、英国（指紋）、ドバイ？（虹彩）

（5）終りに

NAF（National Authentication Framework）の必要性

本人確認サービスの現状

＊本人確認を必要とするネット経由のサービスの急増、今後も継続

＊本人確認は各サービスごとに実施

＊そのため、利用者は各サービスごとの
本人確認機能に対応せざるを得ない

＝＞多数のパスワード、多数のワンタイムパスワードトークン、
多数の秘密鍵－公開鍵証明書

＊本人確認技術はまだまだ発展途上

＝＞各サービスベンダはそれぞれに
本人確認機能の改良・追加・高度化に対応が必要

将来像

＊公的または第3者機関による本人確認機能の集約が望ましい

本人確認技術・サービスとの付き合い方

利用者として:
本人確認方法のそれぞれの特質を良く理解し
なりすまし検知・防止能力を高め、
ICTを利用した機器やシステム、情報サービスの
安全な活用を！

技術者・研究者として:
要素技術およびシステム技術、共にまだまだ発展途上。
新たな技術開発・研究開発テーマは豊富！

ビジネスマンとして:
本人確認技術・機器・システムの進展は今後も期待される。
ビジネスチャンスは豊富！

終

ご清聴、ありがとうございました！