1. 本人認証の全体像とバイオメトリクスの位置付け

電子商取引実証推進協議会
菅　知之

□ 本人認証とは □

社会生活はいろいろなサービスから成り立っているが，ほとんどの場合，これらのサービスを享受できる人は事前に登録または届出をすることが前提になっている．サービス提供者はサービスに先立って，相手が登録または届出をした本人であることを確認するのが普通である．これを本人認証という．

たとえば，クレジットカードで支払うときには，そのクレジットカードの会員であることをカードの提示によって示す必要があるし，銀行から預金を引き出す際には，その口座の持ち主であることを暗証番号によって示す必要がある．上でいうサービスとは広い意味でのサービスであり，特定施設への入場や会員制施設の利用，特定情報へのアクセス，印鑑証明等の行政サービスなども含まれる．

「本人認証」という時の「本人」には，単なる「人」ではなくて，「○○をしたその人」というニュアンスが含まれている．本人認証とはやみくもに人を確認するのではなく，相手が過去に○○した人（現在もその状態が続いている人）であることを確認することである．したがって正確には，○○についての本人認証というべきであって，修飾の付かない本人認証というのは有り得ない．換言すると，本人認証は何かの目的があって，その目的に即した観点で行うものであって，汎用の本人認証は有り得ないことを留意しておくべきである．

すなわち，本人認証は事前の登録／届出が前提になっていて，ある人がその登録／届出をした人に間違いないことを確認する行為である．当然，本人認証が必要とされる場面ごとに，確認の拠り所とする登録／届出は異なる．

□ 本人認証の原理と参照モデル □

本人認証を行うためには，登録した本人であることを何らかの形で証明させるプロセスが必要である．この証明にはいくつかの方法があるが，基本的には本人だけが示し得る情報または物を提示させることによる．この本人であることを証明するために用いられる情報を本人情報という．

すなわち，登録の一環として，本人情報も併せて登録しておき，それと本人認証時に提示された情報との照合で確認するのが一般的な原理である．物を用いる場合には，それは登録時に登録管理側から発行される必要があり，本人認証時には確かに本人に交付された実物であることの確認を行うのが一般的であるが，印鑑のように本人のものを登録して用いる場合もある．

ECOMでは各種の本人認証方式から，その共通的な原理を抽出して，参照モデルを作成した．参照モデルでは，本人認証に登場するプレーヤと用いる情報とを基本概念として以下のように定義している．

①認証請求者：自分が登録してある本人に間違いないことを主張する人．
②検証者：認証請求者の主張をその裏付けによって確認する人（またはシステム）．
③認証者：照合結果を最終的に判断して，認証請求者が本人であることを確信する人（それによって生じる利益／不利益を被る人）．
④登録情報：本人確認の裏付けとして登録し，検証者が利用する情報．
⑤提示情報：認証請求者が証拠として提示する情報（検証者により登録情報と比較検証される）．

これらの基本概念を用いると，本人認証の基本原理は次のように表現される．すなわち，まず事前の登録時に本人認証に用いる本人情報を登録する（これが登録情報である）．本人認証時に認証請求者によって提示された提示情報と登録情報とを認証者（検証者）が比較照合することで，認証請求者が登録された本人であることを確認する（**図-1** 参照）．

提示情報は原理的に本人（認証請求者）が保持する以

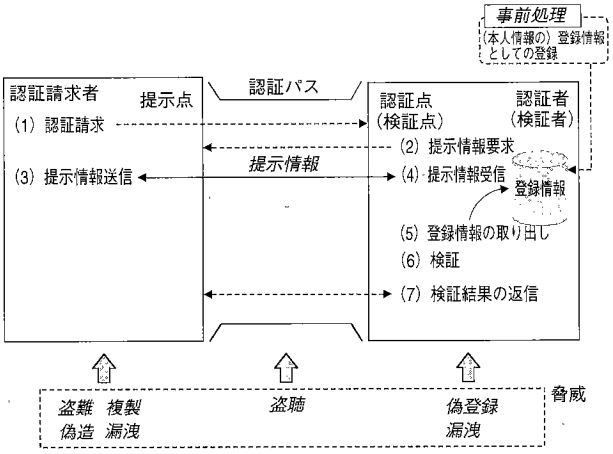

図-1　本人認証の参照モデル：基本モデル

- バイオメトリクスI
  （指紋，網膜，掌紋，虹彩，顔貌，etc）
- バイオメトリクスII
  （署名・筆跡，音声，etc）
- 所有物（身分証明書，パスポート，etc）
- 秘密情報I（暗証・パスワード）
- 秘密情報II（ディジタル署名）

表-1　本人認証の方式

外には有り得ないが，登録情報をどこにおくかに関してはいくつかの実現方式が有り得る．この登録情報の保持場所と情報の流れのトポロジに着目して，参照モデルはさらに複数のタイプに分類される．参照モデルの詳細については文献1）を参照されたい．

本人情報としてバイオメトリクスを使う場合には万人不同かつ終生不変であることが要求される．万人不同性については，個人の識別に用いるのであるから，当然の要求条件と理解されようが，終生不変性については補足が必要であろう．すなわち，生体は日々，極論すれば，刻々変化するものである．したがって，終生不変とはまったく変化しないという意味ではなく，万人不同を示す特徴の面で変わらないという意味である．

また，登録や提示がしやすいものであって，かつその際に痛み，恐怖感，羞恥などを伴わないものであることが必要である．

バイオメトリクスを利用する方式では，生体から直接得られた情報であることを確認して，写真，模造品，録音された声などを排除する機能を必ず備えていなければならない．この確認方法の詳細については，通常企業秘密になっていることが多い．

❑ 本人認証の方式 □

本人認証を行うには，本人情報として何を用いるかによって**表-1**に示す各種の方式に分類できる．

バイオメトリクスI

人体の生物学的特徴を利用するもののうちで外見的特徴に属するものをこの範疇に分類した．指紋，網膜における血管パターン，虹彩の模様などがこれに該当する．

(1) 顔貌

人間の顔には個人差があり，それによって各個人を識別することで人間の社会行動が成り立っているといっても過言ではないであろう．このように顔自体の特徴を利用する認証技術は，一番古くから用いられてきた本人認証と考えられるが，コンピュータで行う場合には顔の画像（写真）の照合技術に帰結される．ただし登録された登録情報としての顔画像と，認証時に撮影される提示情報としての顔画像とは撮影条件が異なるため，単純な画像マッチングではなく，さまざまな特徴を抽出して照合する必要がある．

顔の特徴としては，顔の外形（輪郭），眼の形，鼻の形，口の形などの2次元情報，顔の起伏などの3次元情報を用いる研究例が報告されている．顔による個人識別は照合アルゴリズムを含めて，なお盛んに研究が進められているが，すでに発表されている製品もある．ただし，一卵性双生児の識別可能性，眼鏡，髪型等の認証精度への影響の観点で，本当の実用化には今一歩と考えられる．

(2) 網膜

成人病検診で行われる眼底撮影は網膜上に現れた血管を撮影するものである．この網膜上に血管が形成するパターンは万人不同で個人識別に使えるといわれている．

網膜上の血管パターンを見るには眼底撮影と同様に専用器具に被験者の眼を近づけ，外から光を当てる必要がある．網膜による本人認証技術はある程度確立した技術ということができ，実用製品が発売されて久しく，かなりの利用実績がある．ただし特殊な機器を必要とするので適用領域は入退室管理もしくはそれに類するところに限られているのが現状である．

(3) 虹彩

網膜と同様に眼の一部である虹彩の模様も個人ごとに異なるといわれている．網膜が眼の奥に位置していて，眼底撮影のように眼を器具に近づけて外から光を当てないと見えないのに比べて，虹彩は普通に外部の離れた位置から見ることができるのが利点である．このため網膜に用いられるような特殊な装置ではなく，通常のビデオカメラやディジタルカメラのような汎用の撮像装置の使用でよいため，導入しやすい利点もある．虹彩利用の本人認証機能は実用製品が発売されていて，利用の緒に就いたところである．長野オリンピックでバイアスロンの銃保管室の管理に使われたのはまだ記憶に新しい．

(4) 指紋

個人を識別するバイオメトリクスの特徴としては精度面で一番信頼感があるものである．指紋による個人同定の方法については古くから法科学の分野で確立されており，コンピュータによる処理方法だけが問題になる領域であった．コンピュータによる認証技術としては研究の歴史が

古く，現在では技術的にほぼ確立されたと考えてよい段階にきている．すでにいろいろなメーカで製品化が行われ，実用化されている．方式的には特徴点を抽出して比較するマニューシャマッチング方式と画像マッチング方式とに大別できるが，マニューシャマッチング方式による製品が多いようである．

(5) その他のバイオメトリクスI

耳の形の個人差に関しては欧米でも日本でも研究報告がなされており，形態学的にも解剖学的にも万人不同であることが示されている．耳の大きさは長さ，幅ともに16～17歳以降は安定期に入り，その後も若干の成長がみられるが終生不変とみなし得る範囲内と考えることができる．しかし親子，兄弟，姉妹，双子等の遺伝的側面からの万人不同性の検証についてはなお研究が必要といわれている．

万人不同性を前提として識別・同定実験が重ねられており，識別・同定のアルゴリズムも研究途上にある．このように耳の形による本人認証については，まだ可能性も含めて研究段階にあり，現段階では実用に至っていない．

掌紋（手のひらのしわの形状）を利用する方式も研究されている．しかし指紋ほどの特徴点が多くないため，個人識別の精度は指紋に及ばない．また一般に指紋ほどの万人不同な特徴と信じられてもいない面があり，本人認証として利用できる場面は限定されざるを得ないのが現状である．開発中を含めていくつかの製品が出ており，入退室管理など比較的要求条件の緩いところでは使われるのではないかと考えられる．

掌紋が俗にいう手相の特徴を使うのに対して，掌形はいわゆる手形であって，手のひらの幅，長さ，指の長さ，形の特徴を捉えて利用するものである．個人識別能力が指紋に匹敵するほど高いとは考えられていなかったが，使用実績が増えるにつれて，実用的にはかなりの識別能力があることが分かってきた．方式が簡単な点と指紋に比べて利用者の抵抗感が少ない点とが利点で，使用実績も着実に増えつつある．有名なところでは，アトランタオリンピックでプレスセンターの入退室管理に使われた．

掌紋または掌形の一種と考えることもできるが，指の関節で区切られた部分の長さが個人的なばらつきを持つ点に着目した方式もある．これも掌紋，掌形と同様に，指紋に匹敵するほどの個人識別特性が実証されていなくて，本人認証としては利用できる範囲が限られるものであるが，入退室管理システムとして実用化された例がある．

手の甲に浮き出した血管の模様に着眼する方式もあるが，その個人識別精度は掌紋，掌形，指形以上に，信頼に足る検証がなされているとは言い難く，製品としても英国の数社が開発中と伝えられるが，掌紋，掌形，指形に比べて，特に優れた点は見当たらない．

バイオメトリクスII

人間の行動特性の個人差に着目したもので，広い意味での生物学的特徴といえるものであるが，恣意的に変化させることのできる特徴であり，それを利用した他人への成りすましを排除する必要があるものを特に上述のバイオメトリクスIと区別した．バイオダイナミックスと呼ばれることもある．署名（筆跡）や音声などがこれに該当する．

バイオメトリクスIIを用いた本人認証技術は，本人の署名や声を真似て作られた提示情報を排除できなければならない．この点においてバイオメトリクスIの場合とは，試験の方法が大きく異なることに留意しておかなければならない．

(1) 音声

音声は周波数成分に分解した周波数スペクトラムの時系列データとして捉えることができる．このデータをそのまま，またはそこから抽出した特徴パラメータを登録しておき，提示された音声とのマッチングによって本人認証を行う．発声という行為は随意的な要素があるため，必ずしも完全な再現性があるとはいえず，このマッチングは単純な重ね合わせではなく，話者の特徴を認識・抽出した上で，そのレベルでマッチングを行う必要がある．

また同時に登録時と認証時との差を小さくするような配慮が必要である．たとえば登録すべき言葉によっても再現の度合いは異なり，普段発声し慣れた言葉の方が高い再現性を持つといわれている．この理由で本人の名前などを言わせる実現例がある．

音声による本人認証はすでにいくつかの実用製品があり，利用実績もある．音声の研究は音声認識を目的として長い歴史があるが，本人認証のための個人同定・識別に関しては，アルゴリズムを含めてなお発展段階にあると考えられる．

(2) 署名

署名を用いる本人認証技術は筆者認識技術のうちの筆者照合技術を利用したものである．ちなみに筆者認識には筆者識別と筆者照合とがある．筆者識別とは筆跡から筆者が特定の複数の人物のうちの誰であるかを特定する技術であり，筆者照合とは筆者が特定のある人物であることを確認する技術である．筆者照合は対象となる人物の筆跡（今の場合，署名）をあらかじめ登録しておき，問題の筆跡と登録された筆跡との類似度を判定するものである．

筆跡の形だけを問題にする静的署名と，筆順，筆圧，運筆速度などをも問題にする動的署名とがあるが，当然ながら動的署名の方が利用できる情報が多い．動的署名の場合にはタブレット等の専用機器の上で書く必要がある．現在実用化されているものには動的署名を用いる方式が多い．

署名・筆跡による本人認証は動的署名方式の出現で実用化段階に入っていて，多くの実用製品が存在する．

所有物（所持品）

所有物による本人認証はコンピュータ以前から広く利用されてきた方法である．具体的にはパスポート，身分証

明書，運転免許証，会員証，クレジットカード等である．所有物認証は本人であることを証明するものを発行し，それを所持する者を本人と認める考え方に立つものであるが，純粋な所有物認証には，盗難や遺失によって他人が成りすますリスクが内在しており，それを軽減するために所有者認証を併用している場合が多い．パスポート，身分証明書，運転免許証における顔写真は所有者認証のための情報である．またクレジットカードでは署名（Signature）を，銀行のキャッシュカードでは暗証番号を用いた所有者認証が使われている．

ネットワークを介しての本人認証では，純粋な所有物認証は現時点では意味を持たない．すなわちネットワーク上で相手に提示するのは電子情報以外に有り得ず，コピー自在の電子情報では所有物認証が原理的に成り立たないのは明らかである．したがってネットワークを介した所有物認証は，電子情報のコピー／オリジナルを判別する技術が開発されない限り，ネットワークを介しての所有者認証を併用して，間接的にその所有物を持った人を特定する方式にならざるを得ない．

秘密情報Ⅰ

秘密情報を利用する方法も所有物認証と並んで古くから使われてきた本人認証の手段である．いわゆる「合い言葉」がそれであり，コンピュータの世界ではパスワードや暗証番号・PIN（Personal Identification Number）と呼ばれる方式である．パスワード等の秘密情報による本人認証は確立された技術といってよい．登録情報から提示情報を生成できるものを秘密情報Ⅰと分類して，後述する秘密情報Ⅱと区別する．

利用されるネットワークが従来のクローズ環境からオープン環境に移行するにつれて，単純なパスワード方式は盗聴＋再利用の手法で簡単に成りすましが可能になることから，見かけ上毎回異なるパスワードを用いる方法が研究開発され，実用化された．これはワンタイムパスワード（One Time Password）と呼ばれ，電卓に似た形のハンドヘルドデバイスにその都度表示される使い捨てパスワードを入力するものである．

秘密情報Ⅱ

秘密情報Ⅰに分類したものは，登録情報が知られるとそれを元に提示情報を作ることが可能であり，ECのような認証者が認証請求者に成りすます可能性がある環境においては必ずしも安全とはいえない．登録してある情報が漏れても，提示する情報につながらない方式を秘密情報Ⅱと分類する．秘密を共有するという本質においては秘密情報Ⅰと同様であるが，共有の形を工夫することでこの方式が可能になる．

上記の性質を実現する方法の１つに一方向性関数を利用するものがある．提示する秘密情報を一方向性関数で変換したものを登録することにして，照合時には提示情報をこの一方向性関数を通してから登録情報と比較する方式である．ディジタル署名を用いる方式はこれを具体的に実現した例である．登録してあるのは公開鍵であり，提示するのはそれに対応した秘密鍵で署名した情報であるので，登録してある公開鍵を入手しても，提示する情報は作成できないので，安全性が高い．

□ 本人認証の評価基準 □

本号で取り上げたバイオメトリクスを含めて，さまざまな本人認証方式があり，それぞれ異なった持ち味がある．自分の利用目的に適合した本人認証製品を適切に選択するには，各製品の特性を明確に認識することがまず必要であり，いくつもの製品に関するそれらの特性を比較することで，最も適切な製品を選択することができる．本人認証製品の特性を認識・把握して利用目的に対する満足度を検討することを本人認証製品の評価という．

評価基準

評価基準とは対象の特性を表す物差しであるが，いろいろな側面からの独立な観点での評価が必要であり，単一の物差しで評価することはできない．すなわち，評価基準とは評価の観点ごとに作られた物差しの集合と考えることができる．

この基準に従って行われた評価結果は，評価の観点ごとの評価内容を記述した特性表のような形で表現される．もちろん，各観点を軸としたレーダーチャートのような表現を考えても等価である．

評価は必ずしも物理量のような尺度で定量的に行えるとは限らない．観点の多くは定量的な評価は困難で，定性的な評価しか行えないものである．そのため，この基準は各評価観点ごとに本人認証製品に対する要件（要求条件）の形で達成レベルを記述したものである．これによって，いくつもの本人認証製品の特性を横並びに比較することが可能になり，使用目的に適合した製品を選択することが可能になる．

前述したように評価基準は評価の観点ごとの尺度の集合であり，そこには本人認証の使用環境や目的に関する観点は入っていない．使用目的に即した現実の評価に際しては，その特定の使用環境・目的における要求条件を明確にする必要がある．これは汎用に作られた評価基準を特定用途に特殊化したものと考えてよく，汎用の評価基準から作られるサブセットと考えてもよい．これをプロファイル（Profile）と呼ぶ．プロファイルは評価観点ごとに選ばれた具体的要件の集合である．本人認証の評価イメージを**図-2**に示す．

評価の観点

評価とは技術・製品・システムの使用目的に対する適合性を検証することと考えてもよい．この検証は通常さまざまな観点から行われる．この観点のことを評価要因という．本人認証技術の評価要因としては以下のものを

考える必要がある.

①社会的認知性

本人認証を社会システムの一環として位置付けるときに，社会的コンセンサスが得られるかの観点からの評価である.

高齢者・身障者，若年者への配慮等のバリアフリーに関する項目，本人情報の装置への残留等のプライバシー保護に関する項目，法的ないし制度的裏付けの有無，標準への準拠，認証方式・機器について許認可の必要性など7件の評価項目からなる.

②利用者受容性

本人認証システムを利用して本人であることを主張するエンドユーザに心理的・生理的な面で受け入れられるかの観点からの評価である.

本人排除されたときの救済手段と人体に対する安全性の観点に立つ安全規格への準拠性との2件の評価項目がある.

③脅威対抗性

さまざまな脅威に対抗する能力を備えているかの観点からの評価である.

所有物の盗難・偽造，所有物からの情報の抽出・改竄等の認証用所有物に対する脅威対抗性に関して3件の評価項目がある.

提示情報入力装置関連では，提示情報の不法採取（盗聴），提示情報の漏洩や不正置換，生体情報確認機能，攻撃・調査のチャンス限定など5件の評価項目がある.

認証パスにおける脅威対抗性に関しては，暗号化および本人情報の非反復性の2件の評価項目がある.

検証点における脅威対抗性としては，ファイアウォール，検証ソフトウェアおよび登録情報の漏洩・改竄防止など2件の評価項目がある.

その他に攻撃の痕跡・証拠検出能力，攻撃者の記録保持，監査能力等のトレーサビリティ，システムに関する情報の入手可能性限定などの4件の評価項目がある.

④認証精度

本人を他人と間違えて排除する誤りと他人を本人と間違えて受け入れる誤りとの2面から，認証の精度を評価する.

本人拒否率／他人受入率測定におけるサンプルの選択およびサンプル数等の測定方法の水準に関する項目と本人拒否率／他人受入率／対応率に関する項目の他に，精度バランス調整機能，学習機能等の認証精度に関連する付帯的な項目があり，全部で9件の評価項目がある.

⑤利便性

利用者が使いやすいかの観点での評価である．本人情報登録・更新の容易性，認証請求の容易性，衣服／眼鏡等に関する要件，認証時間，提示情報の記憶の必要性などの操作性に関する項目の他に，専用ハードウェア・専用ソフトウェアの必要性，セットアップ作業の必要性，ソフトウェアの配付形態，プラットホーム&OSの汎用性等のシステム環境の事前準備に関する項目があり，全部で10件の評価項目がある.

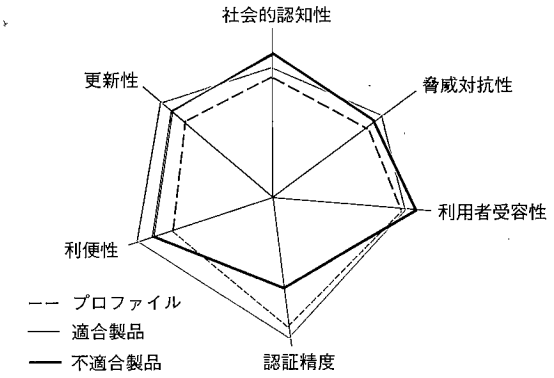

図-2　本人認証の評価イメージ

⑥保守・更新性

認証用機器の保守，認証に用いる情報の保守・更新のしやすさの観点からの評価である.

保守技術の専門性，頻度，時間に関する項目，保守コスト要件，登録情報の更新に関する項目，診断作業の自動化に関する項目など10件の評価項目からなる.

ここで述べた評価基準の詳細については文献2）を参照されたい.

□ 今後の展望 □

バイオメトリクス認証は他の認証方式に比べて，何も覚えなくてよい，何も携行しなくてよい，分かりやすい，本人情報の偽造が難しいなどの強みがある.

一方，弱みと思われるものには，特殊入力装置が必要，対応率が100％ではないこと，認証誤りが0％ではないこと，社会的受容性に問題がある場合がある，オープンネットワークとの相性が必ずしも良くない，性能が環境条件に依存する等の点が挙げられる.

このようにバイオメトリクス認証は万能ではないが，反面優れた特性を持っており，適用領域によっては，現在，すでに実用期にあると考える.

今後の課題としては，技術的には認証精度，対応率の一層の向上が求められるのはいうまでもない．認証精度に対する懸念が導入阻害要因になっている場合もあると思われるが，2回提示させるなどの工夫をすれば，バイオメトリクス認証でも，4桁の暗証番号認証よりも高い精度を実現できる可能性がある.

むしろ適性の高い領域に積極的に使って，その利便性をアピールするとともに，バイオメトリクスに対する信頼感を得ることの方が普及への鍵ではないかと考える.

参考文献

1）本人認証の参照モデル: ECOM報告書, H8-WG06,
http://www.ecom.or.jp/about_wg/wg06/model/index.htm

2）本人認証の評価基準: ECOM報告書, H9-WG06,
http://www.ecom.or.jp/about_wg/wg06/h9doc/wg06-list.htm

（平成11年6月26日受付）