本人認証技術検討ＷＧ報告書
－評価基準（第１版）－

平成 10 年 3 月

電子商取引実証推進協議会（ECOM）

本人認証技術検討WG報告書－評価基準（第１版）－

目次

本報告書の概要－Executive Summary－

＜本人認証とは＞

本人認証とは、個人の識別を行って、事前に登録されている本人であることを確認する技術であり、電子商取引のみならず、今後のデジタル社会のさまざまな分野での応用が期待されている。事前の登録とは、何らかのサービスを受けるための資格の申請手続きをいい、銀行口座の開設、クレジットカード会員への加入、入退室許可申請、特定ファイル閲覧申請、出生届・転出入届・婚姻届・印鑑登録等の行政サービスの申請などをその例として挙げることができる。銀行口座の利用、クレジットカードによる支払い、入退室、ファイル閲覧、印鑑証明などの上記申請に対応したサービスを受ける際には、申請した本人であることの確認が行われる。これが本人認証である。

＜本人認証の実現方式＞

ＥＣＯＭでは本人認証の実現方式を本人であることを立証するのに利用する情報に着眼して、次の５つに分類している。

(1)バイオメトリクスⅠ：指紋、網膜、虹彩、顔貌など

(2)バイオメトリクスⅡ：声紋、筆跡など

(3)所有物（所持品）：身分証明書、クレジットカード、運転免許証など

(4)秘密情報Ⅰ：パスワード、暗証番号など

(5)秘密情報Ⅱ：デジタル署名など

バイオメトリクスⅠは身体的特徴であって意図的に変えることが出来ないものであって、他人を真似ることができない物であるのに対して、バイオメトリクスⅡは同様に身体的特徴に準ずる生物学的な特徴であるが、ある程度意図的に変えることが可能で、他人を真似る事が出来るものをいう。

秘密情報は本人だけが知っている情報を示せるのは本人だけであるのを利用した方式であるが、それを確認する側にその秘密情報を登録しておかないと確認できない。ところが確認する側が本人に成りすます動機が有り得る状況ではこの方式は安全とは言えない。このような従来からの方式を秘密情報Ⅰと分類し、上記のような確認側の成りすましの可能性を無くした方式を秘密情報Ⅱと分類した。秘密情報Ⅱでは確認側に登録するのは秘密情報そのものではなく、それから一方向的操作で変換して得られる情報である。従って登

録した情報から元の秘密情報を得ることはできないので、確認側による成りすましは起こり得ない。

＜本人認証の評価基準＞

上述したように、本人認証技術には色んな方式があり、さまざまな製品が提供されている。本人認証が必要とされる場面に応じた最適な本人認証製品を利用者（構築者）が適切に選択できることが最も重要であるとＥＣＯＭでは考えており、製品間の比較検討を共通の尺度で行えるようにすることが必要であると考えている。この目的のために本人認証技術の評価基準を開発した。

評価基準は、本人認証技術・製品・システムの特性を客観的に把握して、各種製品間での比較を可能にするための共通基盤である。これを利用することにより、多様な製品群の中から自己の目的に最も適合するものを選択することが可能になる。

評価基準は、①社会的認知性、②利用者受容性、③脅威対抗性、④認証精度、⑤利便性、⑥保守･更新性の各観点から、本人認証技術･製品･システムの特性を把握･表現する尺度の集合であり、現在約５０個の詳細評価項目からなっている。各詳細評価項目は本人認証技術・製品・システムのあるべき姿を要件として記述したものであり、到達レベルを幾つかに分けて示したものもある。

＜評価基準開発の経緯＞

本人認証技術検討ＷＧでは付録６に示す各社からの委員の参加を得て、1996 年 4 月から約 2 ヶ年にわたり、本人認証の評価基準の開発を目標として活動してきた。

評価基準の開発にあたり、本人認証技術検討ＷＧでは、意識の統一と円滑な議論のために本人認証の参照モデルを作成した。このモデルは本人認証を議論するための共通基盤として内外で有効に利用されている。

次のステップとして、本人認証技術の評価の観点を洗い出す作業を行い、その中での具体的評価項目を抽出した。その結果を評価基準 v0.5 として 1997 年 5 月に公表した。これは完成度は低いものであったが、評価基準の具体的イメージの提示、ＥＣＯＭ会員によるレビュー、公開レビューを目的として、あえて公開したものである。

これらのレビューで得られた意見を反映し、更に各評価項目毎に客観的な評価可能性の観点から見直し作業を行って、今回の評価基準（第１版）として公表した。今後、第１版

に対するレビューを予定している。

＜評価基準の意義＞

本人認証の評価基準は参照モデルと合わせて、本人認証に関する共通認識として有用であり、本人認証に関する議論を行う上での共通基盤となる。

開発者にとっては、自社製品の特性をアピールするための表示尺度ならびに開発強化のロードマップとしての意味を持ち、利用者（構築者）にとっては開発者に対する要求条件を決めるためのスーパーセットならびに自システムの整備強化のためのロードマップとしての意味を持つものである。

別の視点から言うと、評価基準とは、本人認証の特性を表わす要因とその表現方法とを標準化したものと考えることができ、これによって本人認証の利用者（構築者）は各種の方式を同じ基準で比較検討して、最も自分の目的に適合するものを選ぶことが可能になり、その結果、開発者間の公平な競争が促進され、本人認証市場の健全な発展が期待される。

本人認証の評価基準

（第１版）

平成 10 年 3 月

１　はじめに

１．１　背景

コンピュータの利用が行われる以前から、社会の色々な局面で本人の確認が行われてきた。それは戸籍・住民登録のような行政上の制度に基づく身許の確認であったり、運転免許のような資格の確認であったり、会員制による何らかのサービスを享受する権利の確認であったりする。

つまり『本人』とは何らかの「制度」に基づいて、あらかじめ「登録」してある人を意味している。ここでいう「制度」とは公的なものに限らず、民間で作られる会員制のような仕組みをも含めた意味で使っている。また同様に「登録」も銀行口座の開設、カード会員への加入、運転免許の取得のような行為をも含む意味で使っている。『本人認証』とは当人があらかじめ登録してある人に間違いないことを確認する行為を言う。

コンピュータの普及によって、本人認証は情報技術の一環として実現されてきた。とりわけネットワークの発展によって非対面環境における本人認証の重要性が大きくクローズアップされてきた。この社会的ニーズにこたえる形として、色々な方式原理に基づく本人認証機能が開発されて、製品として市場に出されている。

このような中で、どのような適用領域に対して、どのような本人認証製品を使うのが最も適しているかの判断が求められるようになってきた。この基準はそのような判断に資するために、本人認証技術・製品・システムの特性をさまざまな観点から抽出し、共通な土俵上で比較対照するための枠組みを与えるものである。

１．２　本人認証技術の評価の目的

前節で述べたように、本人認証技術には利用する本人情報に関して以下のような様々な方式が存在する。

- バイオメトリクスⅠ（指紋、網膜、虹彩など）
  人間の身体的特徴であって意図的に変えることが出来ないものをいう。
- バイオメトリクスⅡ（署名／筆跡、声紋など）
  身体的特徴に準ずる人間の行動上の特性である。ある程度、他人の真似をすることが可能である。
- 所有物（身分証明書、パスポートなど）

物理的なものであって、それを持っていることが本人であることの証明になるものをいう。

- 秘密情報Ⅰ（パスワードなど）
  本人だけが知っている秘密情報で、事前にそれ自身を確認する側（認証者／検証者）に登録しておく必要があるものをいう。認証者／検証者による成りすましの可能性がある。
- 秘密情報Ⅱ（デジタル署名など）
  秘密情報を知っていることの確認に用いるために確認側に登録する情報と秘密情報自体が異なるものをいう。認証者／検証者による成りすましの可能性がない。

さらにそれらの実装トポロジーに関しても参照モデル（付録１参照）に挙げた以下のような多様性がある。

- 基本モデル
- 登録情報付き所有物認証モデル
- 証明書添付モデル
- 証明書取り寄せモデル
- 認証サーバモデル

現実に世の中に存在する製品はこれらの組み合わせであり、更に上記要因以外にも脅威対抗策の実施状況などの製品差別化ないし多様性の要因が種々あり、実に多くの製品ないしシステムが存在する。市場原理に基づいて本人認証技術の健全な発展を促進するには、本人認証技術の利用者が自分の利用目的に適合した本人認証製品ないし技術を適切に選択できる環境の整備が必要である。（ここでいう利用者とは、直接的には本人認証をサブシステムとして含んだシステム構築を行う構築者を指すが、間接的にはそのシステムで実際に本人認証機能を用いて自分の身元を証明するエンドユーザも含まれる。以下では、特に断らない限り、本人認証技術の利用者とは上記システム構築者とエンドユーザのことをいう。）

自分の利用目的に適合した本人認証製品ないし技術を適切に選択するには、どの本人認証技術ないし製品がどのようなものかを示す特性を明確に認識することが第一歩の作業として必要であり、幾つもの製品ないし技術に関するそれらの特性を比較することで、もっ

とも適切な製品ないし技術を選択することが出来る。本人認証技術ないし製品の特性を認識･把握することを本人認証技術の評価（Evaluation）という。

１．３　本人認証の評価と評価基準

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。この検証は通常様々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時に、プライバシー面、身障者／高齢者等社会的弱者への配慮、法的側面、保険等の実務的側面などの点で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。

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・生理的な面で受け容れられるかの観点からの評価である。

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。

④認証精度

本人を他人と間違えて排除する誤り、他人を本人と間違えて受け容れる誤りの２面から、認証の精度を評価する。

⑤利便性

利用者が使い易いかの観点での評価である。

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・更新のし易さの観点からの評価である。

評価基準とは対象の特性を表わす物差しであるが､上記の評価要因はそれぞれ独立な要因であり、単一の物差しに投影することはできない。すなわち、評価基準とは評価要因毎に作られた物差しの集合と考えることができる。たとえば立方体に対しては、幅、高さ、奥行きの３つの尺度が常識的に考えられる。これらは独立な評価要因であるが、立方体の場合にはこれらの３つの尺度を１つに投影する体積という量が存在する。これは立方体を単にその外面的寸法だけで評価する場合には可能であるが、更に重さ、表面の滑らかさ、

硬さなどの評価要因を考える場合には、投影できる１つの量（尺度）はもはや存在しない。結局、それぞれの尺度でどうであるかを表のように羅列する以外には評価結果を示し得ない。

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。特に上記のような本人認証技術の評価要因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、この基準は各評価要因毎に本人認証技術・製品・システムに対する要求条件の形で記述したものである。

この基準に従って行われた評価結果は、評価要因毎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、各評価要因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。

これによって、幾つもの本人認証技術・製品・システム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本人認証技術・製品・システム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要因毎の尺度の集合であり、そこには本人認証技術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・目的から派生す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要因毎に選ばれた具体的要件の集合である。

ある使用目的に適合する本人認証技術・製品・システムを選ぶための評価は、まずその使用目的をあらわすプロファイルを記述することから始まる。幾つかの候補技術・製品・システムについて、既に評価結果が得られていれば、それらとプロファイルとを比較対照することで、使用目的に適合するものを選ぶための情報を得ることができる。評価結果がなければ評価を行ってから上記のプロファイルとの比較照合を行うことになる。

システム構築者またはシステム購入者が本人認証技術･製品･システムの供給者に示すＲＦＰ（Request For Proposal）としてこの基準を用いる場合にも、同様に利用目的に応じた特殊化（サブセッティング）を行ってプロファイルを作ることになる。

１．４　評価基準の意味

評価基準は次のような意味を持っている。まず第一に、評価対象である技術分野に関す

る共通認識を与える点である。次に技術ないし製品の開発者にとっては、開発のためのロードマップとしての意味を持っている。また技術ないし製品の利用者にとっては、選択の際の考察要因の集合として、換言すればプロファイルを作成するためのスーパーセットとしての意味を持っている。このプロファイルは製品・システム発注に際しての発注仕様書（ＲＦＰ：Request For Proposal）として利用する事ができる。さらに実際に評価をする評価者にとっては、評価実施の際の尺度としての意味を持っている。

以上は評価基準の一般論としての意味であるが、本人認証技術に関する評価基準においても全く同様のことが成り立つ。すなわち、

- 本人認証技術に関する共通認識としての評価基準
- 本人認証技術の開発者に対するロードマップとしての評価基準
- 本人認証技術の利用者に対するシステム環境整備のロードマップとしての評価基準
- 本人認証製品・システムの発注仕様書としてのプロファイルを作成するためのスーパーセットとしての評価基準
- 評価実施者に対する具体的評価尺度としての評価基準

１．５　想定する読者

まず第一に、本人認証に関する各種特性を語る際の共通認識として、この基準が使われることを期待している。さらにこの基準は以下の読者層を想定しており、それぞれに以下に述べるような意義を持っている。

１．５．１　システム構築者

本人認証機能はさまざまなシステムのさまざまな局面において必要とされる。システム構築にあたっては、そこでの利用目的と環境とに最大限適合した本人認証機能を選んで実装しなければならない。本人認証機能の選択にあたっては利用可能な各種の本人認証技術・製品・システムを比較評価することが必要であり、この基準はその際の物差しとして重要な役割を果たす。

またシステム構築者が本人認証技術・製品・システムに関して、機器（技術）供給者に示す要求条件（ＲＦＰ：Request For Proposal）として、この基準を用いることができる。

さらに稼動後のバージョンアップ等のシステム整備に際しても、この基準はシステム構

築者／運用者に対するロードマップとして有用である。

１．５．２　開発者

この基準は本人認証技術・製品・システムに対する要求条件の集合という側面を持っており、技術・製品・システムの開発者にとってはこの基準は達成すべき要求仕様と考えることができる。

さらに技術･製品･システムの利用者であるシステム構築者に、自社製品の特性を伝えるための枠組みとして、この基準を利用することができる。

また技術・製品・システムの強化の際のロードマップとしての性格も備えている。

１．５．３　評価者

第三者的立場で本人認証技術・製品・システムを評価する人にとって、この基準は評価の対象がどのような特質を備えているかを判断する物差しとして利用するものであり、どのような適用領域に向いているかを判断するのに有用である。

2　評価要因毎の要件

この評価基準の構成を以下に示す。

【凡例】
２．１．１ バリアフリーに関する要件（ＳＡ１）
(1)高齢者・身障者、若年者への配慮（ＳＡ１１）
ＳＡ１１－１：バリアフリー（共用品、共用サービス）としての配慮は特に行なっていない。
ＳＡ１１－２：バリアフリー（共用品、共用サービス）としての工夫をしている。
（機能　：　　）

要件には上例に示すとおり、ＸＸｎｍ－ｐの形式の項番を付与してある。

ここに　ＸＸ＝ＳＡ｜ＵＡ｜ＴＣ｜ＡＡ｜ＥＵ｜ＭＡ　で評価要因を示す記号である。

ただし、ＳＡ：社会的認知性
ＵＡ：利用者受容性
ＴＣ：脅威対抗性
ＡＡ：認証精度
ＥＵ：利便性
ＭＡ：保守･更新性

ｎは各評価要因内の大分類を示す。
ｍは大分類内の要因の通番を示す。
ｐはＸＸｎｍの要件にレベルがある場合のレベルを示す。ｐ＝１は最も低いレベルを示し、ｐが大きくなるほど達成レベルが高くなる。

プロファイル作成時には本人認証機能の利用目的に照らして、
①必要な要件群を選択し、
②各要件毎にレベルがあるものについては必要なレベルを一つ選び、
③更に、その要件中に（　　）がある場合には、そこに具体的な要求値、要求条件等を設定する。

２．１ 社会的認知性（ＳＡ：Social Acceptability）

［解説］
本節の要件は本人認証技術･製品･システムを社会的なインフラストラクチャとして定着させる際のスムーズさの観点から評価するための要件である。バリアフリー、プライバシー保護、法的ないし制度的裏付け、標準化、認許可の必要性の各観点からなっている。

２．１．１ バリアフリーに関する要件（ＳＡ１）

(1)高齢者・身障者、若年者への配慮（ＳＡ１１）

ＳＡ１１－１：バリアフリー（共用品、共用サービス）としての配慮は特に行なっていない。

ＳＡ１１－２：バリアフリー（共用品、共用サービス）としての工夫をしている。

（機能 ：　　）

［解説］
共用品とは、社会的弱者（高齢者、身障者、若年者）のために特に配慮したものであって、かつそれ以外の人（青壮年、健常者）の利用を前提にしたものを言う。共用サービスも同様である。一例として、視覚障害者にテレホンカードの差込方向を示すためのカードの一辺上の切り込みを挙げておく。

２．１．２ プライバシー保護に関する要件（ＳＡ２）

(1)本人情報の装置及び認証パス上への残留（ＳＡ２１）

ＳＡ２１－１：利用した本人情報が本人認証装置及び認証パス上に残留する。

ＳＡ２１－２：利用した本人情報は本人認証装置及び認証パス上に残留しない、または残留している本人情報が容易に採取出来ない。

［解説］
プライバシー保護に関しては、本人認証に関連した個人情報（本人情報及び付帯情報）の保護を考えなくてはならないが、これらの要件の多くは本人認証技術･製品･システムの利用状況によって決まる。換言すると本人認証技術･製品･システムの選択とは独立な利用状況・環境に関する要件であるため、v0.5 にあったこれらの要件は第 1 版では削除し、技術･製品･システムで担保しなければ本人情報の保護がはかれない上記要件（ＳＡ２１）だけを残した。具体的に削除したのは、本人情報の管理体制、閲覧・修正・削除に関する手続き、個人情報の転用制限に関する要件である。本人認証技術・製品･システムの運用にあたっては、これらの今回削除した要件についても考慮しなくてはならないことは言うまでもない。

２．１．３ 法的ないし制度的裏付け（ＳＡ３）

(1)根拠性（ＳＡ３１）

ＳＡ３１－１：法律ないし制度で定められている方式ではない。

ＳＡ３１－２：法律ないし制度で定められている方式である。

（方式名 ：　　）

(2)保険引き受け条件（ＳＡ３２）

ＳＡ３２－１：保険料算定条件として考慮される方式ではない。

ＳＡ３２－２：保険料算定条件として考慮される方式である。

［解説］
本項の要件は、社会的インフラストラクチャとしての定着を助長する法的ないし制度的な裏付けの有無に関するものである。その観点では、v0.5 にあった使用する認証局の運用管理、トラブル保険は性質が異なるので第 1 版では削除した。

２．１．４ 標準化（ＳＡ４）

安全規格に関しては、利用者受容性の項を参照のこと。

(1)標準への準拠（ＳＡ４１）

ＳＡ４１－１：標準への準拠を特に考慮する必要はない。

ＳＡ４１－２：以下の標準規格（事実上の標準を含む）に準拠しなければならない。

（規格番号：　　）

２．１．５ 許認可の必要性（ＳＡ５）

(1)認証方式について（ＳＡ５１）

ＳＡ５１－１：認証方式の導入に関して、許認可・免許が必要である。

（許認可・免許 ：　　）

ＳＡ５１－２：認証方式の導入に関して、許認可・免許は不要である。

（許認可・免許 ：　　）

(2)機器について（ＳＡ５２）

ＳＡ５２－１：機器の導入に関して、許認可・免許が必要である。

（許認可・免許 ：　　）

ＳＡ５２－２：機器の導入に関して、許認可・免許は不要である。

（許認可・免許　：　　）

［解説］
認許可が必要な方式の方が一般利用者にとって安心感があるので定着し易いという考え方もあったが、ここでは認許可の手間のかからない方が普及定着し易いと見る立場を採った。

２．２ 利用者受容性（UA：End User Acceptability）

［解説］
本節の要件は、本人認証技術･製品･システムのエンドユーザが感じる心理的及び生理的な抵抗感に関するものである。

２．２．１ 心理的な抵抗感（UA１）

(1)本人排除された時の救済手段（ＵＡ１１）

ＵＡ１１－１：本人排除時の対応策を特に考えなくてよい。

ＵＡ１１－２：本人排除時の対応策が準備してなければならない。

［解説］
v0.5 では上記のほかに「利用者がコンプレックスや羞恥を感じる身体的特徴を使用してはならない」という要件があったが、コンプレックスや羞恥に関する客観的な評価が困難であるので、第 1 版では削除した。ただし、明らかにコンプレックスや羞恥を感じさせる身体的特徴を使用すべきでないのは言うまでもない。

２．２．２ 生理的な抵抗感（UA２）

(1)人体に対する安全性；安全規格への準拠（ＵＡ２１）

ＵＡ２１－１：安全規定／基準に関する要件は特にない。

ＵＡ２１－２：以下の安全規定／基準に準拠しなければならない。

（準拠すべき安全規定／基準：　　）

(注)電取法、ＩＥＣ、ＡＮＳＩ、ＵＬ、ＶＤＥ、ＦＤＡ、ＡＣＧＩＨ等の規定／基準を具体的番号で示す。（複数可）

［解説］
v0.5 では、安全規格のほかに清潔感、恐怖感に関する要件があったが、客観的に認め得るこれらの要件については安全規格に含まれているとの考えに立ち､第 1 版では削除した。

２．３ 脅威対抗性（ＴＣ：Threat Countering）

２．３．１ 認証用所有物に対する脅威対抗性（ＴＣ１）

(1)所有物の盗難（ＴＣ１１）

ＴＣ１１－１：認証用所有物の盗難に対抗するための特別な配慮は不要である。

ＴＣ１１－２：認証用所有物の盗難に対抗するため、盗難・紛失届による無効化処置がオフラインで行えなければならない。

ＴＣ１１－３：認証用所有物の盗難に対抗するため、盗難・紛失届による無効化処置がオンラインで行えなければならない。

ＴＣ１１－４：認証用所有物の盗難に対抗するための所有者認証を行わなければならない。

［解説］
「オンラインによる無効化処置」とは盗難･紛失届を受けて即座に発効させ得る処置をいい、「オフラインによる無効化処置」とは上記届を受けてから発効するまでに、電話連絡、郵送等による時間遅れがある処置をいう。認証用所有物に貼られた顔写真は所有者認証の手段の典型である。バイオメトリクスを用いる以外に、暗証番号等の秘密情報を用いる方法もある。

(2)所有物偽造（ＴＣ１２）

ＴＣ１２－１：認証用所有物の偽造を防止するための特別な配慮は不要である。

ＴＣ１２－２：認証用所有物の偽造を防止するための方策（ex.特殊印刷）を施さなければならない。

［解説］
特殊な印刷技術を用いることによりコピー機等による単純な偽造を防ぐ他に、貼付された顔写真の張り替えを防ぐための割印やエンボスも上記方策に該当する。

(3)情報の抽出・改竄（ＴＣ１３）

ＴＣ１３－１：認証用所有物中の情報の盗聴または改竄に対する特別な配慮は不要である。

ＴＣ１３－２：認証用所有物中の情報の盗聴または改竄ができてはならない。

［解説］
ここでいう情報とは認証用所有物に蓄積された電子的情報をいう。

２．３．２ 提示情報入力装置における脅威対抗性（ＴＣ２）

(1)提示情報の不法採取（盗聴）（ＴＣ２１）

ＴＣ２１－１：提示点における提示情報の第三者による不法採取について特別な配慮は不要である。

ＴＣ２１－２：提示情報が提示点において第三者に不法に採取されないような構造にしなければならない。

［解説］
提示点における第三者による提示情報の不法な採取の典型は暗証番号やパスワード等の秘密情報の入力を横から盗み見する行為である。

(2)提示情報の漏洩（ＴＣ２２）

ＴＣ２２－１：提示情報の漏洩について特別な配慮は不要である。

ＴＣ２２－２：提示情報が電気信号または電磁輻射信号として漏洩することがあってはならない。

［解説］
ＴＣ２１の一つとも考えられるが、電気信号または電磁輻射信号の傍受による情報の不正採取はそれが行われる時点で攻撃者が人目にさらされることを避け得るため、あえて別の要件として採り上げたものである。

(3)不正置換（ＴＣ２３）

ＴＣ２３－１：システムコンポーネントの不正な置き換えに対抗するための特別な配慮は不要である。

ＴＣ２３－２：システムコンポーネントの不正な置き換えに対抗するために相手機器（ソフトウエア）の認証ができなければならない。

［解説］
システムコンポーネントの一部を置換することで攻撃者の意図する動作を行わせる攻撃が想定し得る。特にネットワークをまたがるシステムではその可能性が大きくなる。

(4)生体情報確認機能（ＴＣ２４）

ＴＣ２４－１：バイオメトリクスを利用する場合、提示情報が生体から得られたものであることを確認する必要はない。

ＴＣ２４－２：バイオメトリクスを利用する場合、提示情報が生体から得られたものであることを確認して疑似データの提示を排除する機能を備えなければ

ならない。

［解説］
擬似データを排除する機能の動作原理は公表しない方が良い。例えば指紋を採取する際の生体情報確認に体温を用いていることが分かると容易にそれをくぐりぬけることが可能になるからである。

(5)攻撃・調査のチャンスの限定（ＴＣ２５）

ＴＣ２５－１：攻撃・調査のチャンスの限定について特別な配慮は不要である。

ＴＣ２５－２：攻撃・調査のチャンスを限定するために、ＧＵＩ，装置デザイン、物理的な対策も含め工夫がなされていなければならない。

［解説］
具体的には、不正行為の意図を検知し、不正行為からガードする機能を持たせることが必要。例えば、総当たりの攻撃（リジェクトが続く場合など）を検知し、その場合はそれ以上の攻撃を受けないようにガードするなどの対策を施する必要がある。

２．３．３ 認証パスにおける脅威対抗性（ＴＣ３）

(1) 暗号化（ＴＣ３１）

ＴＣ３１－１：本人情報（登録情報と提示情報）の盗聴・改竄に特別な配慮は不要である。

ＴＣ３１－２：本人情報（登録情報と提示情報）の伝送には暗号化を施さなければならない。

［解説］
認証パスにおける本人情報の盗聴はそれを再利用することによる攻撃につながる。また登録情報の改竄も考え得る攻撃方法である。

(2) 非反復性（ＴＣ３２）

ＴＣ３２－１：提示情報の非反復性について特別な配慮は不要である。

ＴＣ３２－２：認証パス上の提示情報に非反復性を持たせなければならない。

［解説］
非反復性とは同一の提示情報であっても毎回見かけが異なることをいう。ただし、そこから提示情報を抽出して次回に認証パス上に現れる情報の予測が簡単に行えるものであってはならない。チャレンジ／レスポンス方式、タイムスタンプ、シーケンス番号、乱数などを提示情報と連結して暗号化する方式等で実現される。
もともと非反復性を持つ本人情報（署名、声紋など）を用いる方式においては、履歴管理による反復性の検出を行って提示情報の盗聴・再利用を検出することも有効である。

２．３．４ 検証点における脅威対抗性（ＴＣ４）

(1)ファイアウォール（ＴＣ４１）

ＴＣ４１－１：ネットワークからのアクセスに対して特別な配慮は不要である。

ＴＣ４１－２：ネットワークから、認証用のトランザクション以外の不正アクセスを受付けてはならない。

［解説］
認証用のトランザクションによって起動されるのは検証用のロジックだけであるので、これ以外のトランザクションの受け付けを拒否する仕組を持っていれば、検証点の登録情報ファイルの読み出しや改竄、検証用ソフトウェアの書き換えなどがネットワークから不正に行われる可能性は極めて低くなる。

(2) 検証ソフトウェア・登録情報の漏洩・改竄（ＴＣ４２）

ＴＣ４２－１：検証ソフトウェア・登録情報の漏洩・改竄に対して特別な配慮は不要である。

ＴＣ４２－２：検証ソフトウェア、登録情報の漏洩・改竄防止のため、アクセス管理を行わなければならない。

(a)運用管理の権限を付与されたオペレータ以外が検証用システムに物理的にアクセスできないよう、パスワード入力などによりシステムを保護しなければならない。

(b)運用管理の権限を付与されたオペレータ以外が情報のバックアップを取れないように、パスワード入力などによりシステムを保護しなければならない。

(c)メンテナンスに伴う情報へのアクセスは、権限を付与されたオペレータないし保守者だけが、パスワード入力などによりアクセス可能とならなければならない。

［解説］
本人認証機能に対する攻撃の一つに検証点にある検証用ソフトウェアの書き換え、登録情報の読み出し、改竄がある。ネットワークからの攻撃に対してはある程度まではファイアウォールにより保護できるが、ローカルな攻撃に対してはそのコンピュータシステムにアクセスできる人を限定するアクセス管理が必要である。

２．３．５ トレーサビリティ（ＴＣ５）

［解説］
本項の要件は積極的に脅威に対抗するための要件ではないが、実際に本人認証機能に対する攻撃が行われた時に、その痕跡や記録を残すことで、さかのぼって調査を行うことを可能にするための要件である。これらは消極的な脅威対抗要件といってもよいが、不正を行う人に対する牽制効果もある。

(1) 攻撃の痕跡・証拠検出能力（ＴＣ５１）

ＴＣ５１－１：攻撃が行われた痕跡の検知について特別な配慮は不要である。

ＴＣ５１－２：攻撃が行われた痕跡を検知する能力を備えなければならない。

(a)物理的な攻撃があったことを検知できる仕組みを組込んでおかねばならない。

(b)不正アクセスを検出できなければならない。

ＴＣ５１－３：攻撃が行われた痕跡を検知し、通知する能力を備えなければならない。

(a)物理的な攻撃があったことを検知し、通知できる仕組みを組込んでおかねばならない。

(b)不正アクセスを検出時に管理者に通知する事ができなければならない。管理者が遠隔地にいる場合にはネットワークを利用して通知できなければならない。

(2) 攻撃者の記録保持（ＴＣ５２）

ＴＣ５２－１：攻撃に使われた提示情報の保存について特別な配慮は不要である。

ＴＣ５２－２：攻撃に使われた提示情報を保存できなければならない。

(3) 監査能力（ＴＣ５３）

ＴＣ５３－１：監査・ログ記録について特別な配慮は不要である。

ＴＣ５３－２：不正アクセスの追跡、監査人による監査のために、監査・ログ記録が残されていなければならない。

２．３．６ その他（ＴＣ６）

(1) システムに関する情報入手の可能性（ＴＣ６１）

ＴＣ６１－１：システムに関する情報の公開性について特別な配慮は不要である。

ＴＣ６１－２：システムに関する情報は公開性の低いものでなければならない。

［解説］

システムに関する情報、例えば認証パス上のプロトコルと情報形式に関する情報が公開されている場合に比べると公開されていない方が攻撃されにくい。ただし、公開性を低く抑える要求は標準化の要求と相反する性格を持っているので、適用領域によっていずれを重視するかの判断を行わなければならない。

２．４　認証精度（ＡＡ：Accuracy of Authentication）

バイオメトリクスを利用する方式では認証精度は実際の利用者集団毎に異なるのが普通であり、真の認証精度は特定の利用者集団毎に意味を持つものである。しかし本人認証技術・製品・システムの選択にあたって、認証精度が重要な考察要因の一つであることも確かであり、利用者集団を特定しない一般的な認証精度も目安としての意味を持つ。なお特定利用者集団における認証精度もサンプル者の選択がその利用者集団から行われる以外は全く同様に測定できる。

認証精度は、本人が登録した人物であると認識する同定精度と、本人を他人と区別して認識する識別精度の両面で表わすことが必要である。前者は本人拒否率（ＦＲＲ：False Rejection Rate）、後者は他人受入率（ＦＡＲ：False Acceptance Rate）によって評価する。ここに、本人拒否率は本人を本人と同定できない照合ミスの比率であり、他人受入率は他人を本人として誤って受け入れる誤識別の比率である。

本人拒否率と他人受入率とは独立ではなく、照合時の判別閾値によってそれぞれが決まり、一方を厳しくすれば他方はゆるくならざるを得ない性質を持っている。また後述の対応率とも密接な関係をもっている。従って、精度の要件は以下のような表示をする。

対応率≧（　　）％ の時、《以下の a、b、c いずれかの形式で示す》

a.本人拒否率(FRR)≦（　　）％

b.他人受入率(FAR)≦（　　）％

c.本人拒否率(FRR)≦（　　）％ かつ 他人受入率(FAR)≦（　　）％

［解説］
本人認証技術・製品・システムの供給者が製品特性としてカタログ等に認証精度を表示する場合、上記ｃの形式で次のケースを併記してもよい。
(1)本人拒否率を最良（最小）にした場合
(2)他人受入率を最良（最小）にした場合
(3)本人拒否率＝他人受入率 にした場合（これを等価エラー率という）

バイオメトリクスを利用する方式の場合、人によって、センサで本人情報を読み取りにくい、読み取った情報が安定でない、照合しにくいなどの状況が起こり得る。例えば指紋を利用する場合だと、生まれつき指紋が薄い（浅い）人や、職業上の理由で指の表面が摩滅して指紋が薄い人や皮膚表面の分泌状況の得意な人で上記のような状況が起こり得る。また事故等で指を失った人も考える必要がある。このような状況を「未対応」といい、そ

のような人を「未対応者」と呼ぶ。本人拒否率および他人受入率の算出にあたっては、測定サンプル群の中の未対応者のデータを除いて算出する事ができる。未対応状況の定義は装置メーカに任されるが、その割合は対応率として示されることが必要である。

対応率＝（全サンプル数－未対応サンプル数）×１００／全サンプル数

［解説］
どのサンプルを未対応サンプルとして、本人拒否率／他人受入率の算出から除外するかは、装置メーカ（提供者）が決める事ができるが、対応率だけを恣意的に高い値にできるのではなく、次に述べるようなトレードオフ条件が存在する。一般的には、対応率と本人拒否率／他人受入率とは独立ではなく、対応率を大きくすると本人拒否率、他人受入率は悪くなり、逆に対応率を小さくすると本人拒否率、他人受入率は良くなる傾向にある。この状況を勘案しながら、対応率をどれくらいに設定するかは、装置提供者のポリシーである。

２．４．１　本人拒否率の測定方法の水準（ＡＡ１）

(1)サンプルの選択

認証精度は実際の利用者集合毎に異なる。即ち、男性だけ、女性だけ、高齢者だけ、年少者だけ、その他色々な偏りのある利用者集合が有り得るが、認証精度はそれぞれ異なる値になることが予想される。むしろ認証精度は実際の利用者集団毎に異なるのが一般的と考えるべきである。

従って、精度の測定は実際の利用者を対象に行うのがベストであるが、それができない場合にはできるだけ実際の利用者集団の構成に近い形でサンプル者を選ぶことが重要である。実際の利用者集団を想定できない場合には一般的な社会の構成に近い形で選ぶべきである。

サンプル者の数は多いほど望ましく、可能な限り多数のサンプル者を選ぶべきである。現実世界の変化の影響を収集するため、人的条件や環境条件が偏らないように被験者をサンプル収集に参加させることが必要である。

バイオメトリクスの性質によっては、一人のサンプル者から複数のサンプルを収集することが可能である。例えば、指紋の場合でいうと、同一人の親指、人差し指、中指をそれぞれ別のサンプルとして収集することも可能である。この場合に、更に左右も考えれば、一人のサンプル者から６個のサンプルが収集可能である。

(2)登録情報サンプルの収集

登録情報サンプルの収集は実際の登録時と同じ手順で行わねばならない。各サンプル者は決められた装置毎に、決められた回数の登録を行う。

(3)提示情報サンプルの収集

提示情報サンプルの収集は実際の提示時と同じ手順で行わねばならない。

また提示毎に認証結果をサンプル者に知らせないやり方では良好な提示情報が得られないことがあるので、なるべく実際の利用時と同様に提示毎に認証結果を知らせる方が望ましい。

(4)本人拒否率の測定

本人拒否率＝本人拒否数×１００／全照合数（%）で定義される。ここで全照合数とはサンプル毎に提示情報と登録情報との照合の数を全サンプルについて合計したものである。ただしセンサ機能の限界等により正しい照合が得難いサンプル者（未対応者）の結果は除いて集計してもよい。

(5)本人拒否率測定におけるサンプル数（ＡＡ１１）

ＡＡ１１－１：サンプル数に関する要件はない。

ＡＡ１１－２：適用対象を（　　）人の母集団として、
１σの信頼度で精度をあらわすサンプル数である。

ＡＡ１１－３：適用対象を（　　）人の母集団として、
３σの信頼度で精度をあらわすサンプル数である。

(6)本人拒否率測定における登録および提示（ＡＡ１２）

ＡＡ１２－１：学習・非学習に関する要件はない。

ＡＡ１２－２：登録者および提示者は使用方法に関して学習していない。

ＡＡ１２－３：登録者および提示者は使用方法に関して学習している。

２．４．２　他人受入率の測定方法の水準（ＡＡ２）

(1)サンプルの選択

本人拒否率の項参照。

(2)登録情報サンプルの収集

本人拒否率の項参照。

(3)提示情報サンプルの収集

本人拒否率の項参照。

(4)他人受入率の測定

他人受入率＝他人受入数×１００／全照合数（%）で定義される。本人拒否率の場合の照合はサンプル毎の登録情報と提示情報との照合であったのに対して、他人受入率の場合の照合は、提示サンプル毎にその提示情報を全登録サンプルの登録情報と照合するものである。ただしセンサ機能の限界等により正しい照合が得難いサンプル者（未対応者）の結果は除いて集計してもよい。

(5)他人受入率測定における登録サンプル数（ＡＡ２１）

ＡＡ２１－１：サンプル数に関する要件はない。

ＡＡ２１－２：適用対象を（　　）人の母集団として、
１σの信頼度で精度をあらわすサンプル数である。

ＡＡ２１－３：適用対象を（　　）人の母集団として、
３σの信頼度で精度をあらわすサンプル数である。

(6)他人受入率測定における登録および提示（ＡＡ２２）

ＡＡ２２－１：学習・非学習に関する要件はない。

ＡＡ２２－２：登録者および提示者は使用方法に関して学習していない。

ＡＡ２２－３：登録者および提示者は使用方法に関して学習している。

２．４．３　認証精度（ＡＡ３）

(1)認証精度および対応率（ＡＡ３１）

ＡＡ３１－１：基本認証精度及び対応率に関しての要件はない。

ＡＡ３１－２:基本認証精度および対応率は以下に示す値をクリアしなければならない。

条件：　対応率≧（　　）％ の時、（以下 a、b、c のいづれかを示す）

a.本人拒否率(FRR)≦（　　）％

b.他人受入率(FAR)≦（　　）％

c.本人拒否率(FRR)≦（　　）％ かつ 他人受入率(FAR)≦（　　）％

２．４．４　認証精度に関連する機能（ＡＡ４）

(1)精度バランス調整機能（ＡＡ４１）

ＡＡ４１－１：固定されており、精度バランスを調整できない。

ＡＡ４１－２：全ての照合に対して、一括して精度バランスを変えることができる。

ＡＡ４１－３：個々の認証請求時に、認証の目的に応じて精度バランスを変えることができる。

［解説］
システム管理者の認証時は通常の利用者の認証時よりも、他人受入率を低く抑えたいような場合が想定される。

(2)登録情報の個別精度バランス調整(ＡＡ４２)

ＡＡ４２－１：情報登録時に、個別に精度バランスを変えることはできない。

ＡＡ４２－２：登録情報一件毎に、精度バランスを変えることができる。

［解説］
読み取りにくいバイオメトリクスを救済して、対応率を上げる目的で精度バランスを変える運用も考えられる。この場合には登録情報毎に精度バランスを変える必要があり、登録情報には、そのデータが照合に用いられる時の精度バランスを併せて蓄積しておく必要がある。

(1)学習機能（ＡＡ４３）

ＡＡ４３－１：認証機能には学習機能は特に要求しない。

ＡＡ４３－２：認証機能には、毎回の認証時に得られる提示情報を元にして登録情報の

質を向上させる等の学習機能を備えなければならない。

［解説］
本人情報の登録時には、複数回繰り返して読み取る等の良質のバイオメトリクス・データを取り込む工夫がなされているのが普通であるが、登録時と認証請求時との環境条件の変化などによって、認証請求時に得られた本人情報を登録情報に補って、登録情報をより良質にする工夫をする方が、認証精度の点で良好な結果が得られる場合がある。

２．４．５　バイオメトリクスⅡにおける認証精度の扱い

バイオメトリクスⅡは本人の意思である程度変えることが出来る、人間の動作上の特徴を分類付けたもので、署名／筆跡、声紋などが該当する。意図的に変え得るということは、登録する本人情報を本人の意思で選択できることを意味すると共に、程度の差はあろうが他人の特徴を真似る事ができることを意味する。このため、ここで述べた認証精度の測定方法の考え方はバイオメトリクスⅠについては適用可能であるが、バイオメトリクスⅡに適用する場合には、その意味を十分に吟味することが必要である。

(1)登録情報の自由度の問題

バイオメトリクスⅠでは登録時／認証請求時に読み取るバイオメトリクスの範囲や利用する特徴は装置･システムの方式と性能とによって決まり、それは認証請求者毎に異なることはなく同じ基準で扱われる。しかも人間はどの装置･システムに対する時でも、自分のバイオメトリクスを意図的に変えることはできず、どの装置・システムにも同じ情報が入力される。（勿論、読み取って扱う部分は装置･システムによって異なり得る。）この事は認証精度の測定に用いる本人情報の質と量とにある種の正規化を行う効果を持つ。従って、測定時の本人情報に関する条件を決めておかなくても、認証精度の装置間での比較はある程度可能である。。

しかし、バイオメトリクスⅡにおいては、登録する本人情報を各被験者の選択に任せたのでは、その情報量にばらつきが生じて、意味のある比較が可能な認証精度測定ができない。換言すると、利用する本人情報をある程度規定しておかないと認証精度としての表示は意味がない。書いたり、発声したりするものを決めておいて、情報量にある種の正規化を行うのが一つの方法である。具体例を挙げると、フルネームを書く／発声すると規定する方法がある。こうしておけば、ある程度比較可能なデータが得られる可能性はあるが、フルネームに限定しない運用も考えられるので、現実にその本人認証装置･

システムが用いられる環境とは乖離した精度であるという問題がある。また、名前の複雑さの違いも影響すると思われる。登録する本人情報を選べるのはバイオメトリクスⅡの特質の一つである。更に言語の差、文化の差をうまく吸収して比較できるかという問題もある。

バイオメトリクスⅡを用いた本人認証技術･製品･システムにも秘密情報で用いられるのと同様なチャレンジ／レスポンス型を採用して提示情報に非再現性を持たせる方式が最近見られるようになった。この方式では装置･システム側が提示する情報を指示できるので、ここで問題にした本人情報の自由度の問題はある程度解決できる可能性がある。

(2)他人を真似る可能性

更に、他人を真似る事ができるという特性は他人受入率の測定の考え方に大きく影響する。上で述べた他人受入率の測定方法は他人の提示情報がその装置･システムの識別能力では偶然に本人の登録情報と一致するとみなされてしまう場合を測定し、他人受入率と算出する。

これはバイオメトリクスⅠでは現実の運用環境で起こり得る状況とほぼ同様と考えられるが、バイオメトリクスⅡでは意図的に他人の真似をしたものをどれだけ排除できるかを測定しなければ意味がない。この時に問題になるのは他人の筆跡／署名や声を真似る技術のばらつきである。このような技術を正規化する方法は見付かっていない。従って、積極的に真似をさせて測定した他人受入率であっても、被験者の真似をする技術の水準を合わせることができないので、比較可能なデータは得られない。

(3)バイオメトリクスⅡにおける測定方法（ＡＡ５３）

意味のある比較の可能な測定を行う一つの考え方として、サンプルとして用いる本人情報（登録情報、提示情報）を蓄積したデータベースを構築して、誰にでも利用できる様にしておき、どの認証装置の精度測定にもこのデータを共通に使用する考え方がある。この考え方に基づく指紋データのデータベースは米国には例がある。

この方法だと装置間の精度測定結果の比較は可能であるが、蓄積される本人情報はセンサで読み取った結果であって、センサに入力する生体情報そのものでない点に問題が残る。即ち、センサの読み取り性能については比較できなくて、識別・照合アルゴリズムだけの比較に成ることである。アルゴリズムとしての優劣は判定できても、本当に問

題にすべき装置としての優劣は結論づけられない。

具体的な導入環境と運用環境とが決められた状況では、バイオメトリクスⅡを利用した装置でも、認証精度の実測を行うことは可能である。この場合でも、本人情報の自由度については、その運用環境に合わせることが可能であるが、バイオメトリクスⅡのもう一つの特徴である真似の問題については完全な解決にはならず、どこまで信頼のおける他人受入率が得られるかは疑問である。

結局、現時点ではバイオメトリクスⅡを利用する本人認証技術・製品・システムの本人拒否率は運用環境を仮定すれば、製品選択上の一つの目安として考えることもできるが、他人受入率はあくまで一例としての位置づけで扱うべきである。

２．５ 利便性（ＥＵ：Ease of Use）

［解説］
本節の要件は、本人認証技術・製品･システムの利用に際する手間に関するものであり、操作性、事前準備、認証時間、提示情報の記憶に関する各要件からなっている。v0.5 ではこの他に場所、時間に関する要件があったが、これらは利用状況に依存する要件であるため、第 1 版では削除した。また同じく v0.5 にあった代理人可否に関する要件については、代理人という考え方自体が運用面における便宜的な取り扱いであって、本人認証の持つべき本来的な性質ではないと考えて、第 1 版では削除した。

２．５．１ 操作性（ＥＵ１）

特殊なオペレーションの必要性に関するものである。

(1)本人情報登録・更新の容易性（ＥＵ１１）

ＥＵ１１－１：複雑な操作及び操作の習熟が必要である。

ＥＵ１１－２：操作は平易である。

ＥＵ１１－３：特別な／意識した操作を必要としない。

(2)認証請求の容易性（ＥＵ１２）

ＥＵ１２－１：複雑な操作が必要である。

ＥＵ１２－２：操作は平易である。

ＥＵ１２－３：特別な／意識した操作を必要としない。

(3)衣服／眼鏡等に関する要件（ＥＵ１３）

ＥＵ１３－１：認証請求時に眼鏡、コンタクトレンズ、指輪等の通常の室内環境において着用するものを外す必要がある。

ＥＵ１３－２：眼鏡、コンタクトレンズ、指輪等の通常の室内環境において着用するものをつけたままで認証請求できる。

ＥＵ１３－３：手袋等の防寒具、雨具等の室外環境で着用するものをつけたままで認証請求できる。

［解説］
本人認証技術･製品･システムの利用には、本人情報の事前登録と認証請求の両面を考えなくてはならない。本項の要件はこの両面でのエンドユーザの操作の簡単さを評価するためのものである。

２．５．２　事前準備（ＥＵ２）

［解説］
本項の要件は、必要なハードウェア、ソフトウェアの入手方法、セットアップ等に関するものであり、より一般的なものほど利便性が高いと位置づけた。

(1)ハードウエア　（ＥＵ２１）

ＥＵ２１－１：専用のハードウエアの購入を必要とする。

ＥＵ２１－２：ハードウエア(認定された一部の市販品)の購入を必要とする。

ＥＵ２１－３：専用のハードウエアが配布される。

ＥＵ２１－４：専用のハードウエアを必要としない。

(2) ソフトウエア　（ＥＵ２２）

ＥＵ２２－１：専用のソフトウエアの購入を必要とする。

ＥＵ２２－２：ソフトウエア(認定された一部の市販品)の購入を必要とする。

ＥＵ２２－３：専用のソフトウエアが配布（ダウンロードも可）される。

ＥＵ２２－４：専用のソフトウエアを必要としない。

(3) セットアップの必要性　（ＥＵ２３）

ＥＵ２３－１：専門家によるセットアップを必要とする。

ＥＵ２３－２：セットアップソフトの画面でユーザがセットアップ可能。

ＥＵ２３－３：マニュアル等によりユーザーがセットアップ可能。

ＥＵ２３－４：セットアップを必要としない。

(4)ソフトウエアの配付形態　（ＥＵ２４）

ＥＵ２４－１：（ファイルサイズが大きすぎて）可搬媒体（CD-ROM 等）から取得が必要である。

ＥＵ２４－２：ネットワークでも可搬媒体（CD-ROM 等）でも取得できる。

ＥＵ２４－３：（ファイルサイズが小さいので）ネットワークから取得できる。

［解説］
CD-ROM 等の可搬媒体による配布よりもネットワークによる配布の方が利便性が高いと考えた。ただし、これはネットワークによる配布に要する時間が実用的なオーダーであることを前提にしたものであり、ファイルサイズに関する要件と考えてもよい。

(5) プラットホーム&OS

ＥＵ２５－１：専用の OS を必要とする。

ＥＵ２５－２：１つの市販 OS で動作可能である。

ＥＵ２５－３：複数の市販 OS で動作可能である。

２．５．３　認証時間（ＥＵ３）

(1)認証時間（注１～４）

ＥＵ３－１：認証時間は（　　）秒以下である。

（注１）認証時間とは，利用者が提示情報を提示する動作を開始してから，結果が通知されるまでの時間である。

ただし、認証時間を評価する条件(OS:　,CPU:　,メモリ:　MB)を明示すること。

（注２）認証時間は、1:1 照合の場合のみであり、ID 入力の時間は認証時間に入らない。

（注３）「利用者が提示情報を提示する動作の開始」の定義は，利用者が陽にその動作をする場合には、その動作開始時間からであり、そうでない場合は、その装置の保証するエリア内に入った瞬間とする。

（注４）上記の測定については，平均的な習熟度を持つ複数の被験者による平均値によること。

［解説］
v0.5 では認証時間に関する要件の他に本人情報の事前登録のための申請手続き、登録時間に関する要件があったが、申請手続きに関しては、その運用状況に依存する時間であること、登録時間に関しては本人情報以外の付帯情報の入力時間が占める割合が多くて利用目的･環境に依存する時間であることから、第 1 版では削除した。

２．５．４　提示情報の記憶（ＥＵ４）

(1)記憶の必要性（ＥＵ４１）

ＥＵ４１－１： 秘密情報の記憶は困難で別に記録保管することが必要である。

ＥＵ４１－２： 秘密情報が必要な場合、その記憶は容易である。

ＥＵ４１－３： 記憶すべき秘密情報がない。

２．６ 保守・更新性（MA：Maintenance and Administration）

［解説］
基本的には v0.5 で示した要件と同じであるが、表現を変更した。また保守作業が必要になる時期の見極めを行うための機能に関する要件を第 1 版で追加した（ＭＡ－３１）。

前提：保守作業は、装置設置時における性能を維持するために必要な作業と定義する。
また、更新作業とは、登録データの更新を意味し原則的には必要なしとする。ここでは、なんらかの理由により（指紋の場合を例にとると、指先を怪我したなど）発生した場合を想定する。

２．６．１ 保守に関して（MA１）

(1)保守が必要かどうか（ＭＡ１１）

ＭＡ１１－１：定期保守の必要有り。

ＭＡ１１－２：必要なし（問題が起こったときのみ）。

(2)メーカが行う１回当たりの保守の手間（時間換算）（ＭＡ１２）

ＭＡ１２－１：１回の保守時間は１日を超える。

ＭＡ１２－２：１回の保守時間は１日以内。

ＭＡ１２－３：１回の保守時間は半日以内。

ＭＡ１２－４：１回の保守時間は１時間以内。

(3)ユーザが行う１回当たりの保守の手間（時間換算）（ＭＡ１３）

ＭＡ１３－１：１回の保守時間は１日を超える。

ＭＡ１３－２：１回の保守時間は１日以内。

ＭＡ１３－３：１回の保守時間は半日以内。

ＭＡ１３－４：１回の保守時間は１時間以内。

(注)ここでいうユーザとは、エンドユーザではなく、実際の運用を行う組織または個人をいう。

(4)メーカの保守作業頻度（ＭＡ１４）

ＭＡ１４－１：保守作業頻度は毎日。

ＭＡ１４－２：保守作業頻度は毎週。

ＭＡ１４－３：保守作業頻度は毎月。

ＭＡ１４－４：保守作業頻度は毎年。

ＭＡ１４－５：保守作業頻度の間隔は１年を超える。

(5)**ユーザの保守作業頻度（ＭＡ１５）**

ＭＡ１５－１：保守作業頻度は毎日。

ＭＡ１５－２：保守作業頻度は毎週。

ＭＡ１５－３：保守作業頻度は毎月。

ＭＡ１５－４：保守作業頻度は毎年。

ＭＡ１５－５：保守作業頻度の間隔は１年を超える。

(6)**保守作業コスト（費用換算）（ＭＡ１６）**

作業コストは、人件費、計測器等の償却費、交換部品費（クリーナ等の）消耗品、出張費などの合計とする。

ＭＡ１６－１：保守作業コストに関する特別な要件はない。

ＭＡ１６－２：保守作業コストは（　　）円以下とする。

２．６．２ 更新に関して（ＭＡ２）

(1)**更新作業をするのは誰か（ＭＡ２１）**

ＭＡ２１－１：メーカ。

ＭＡ２１ー２：ユーザ（メーカより購入して設置した組織、または個人）。

(2)**１回当たりの更新の手間（時間換算）（ＭＡ２２）**

ＭＡ２２－１：１回の更新時間は１日を超える。

ＭＡ２２－２：１回の更新時間は１日以内。

ＭＡ２２－３：１回の更新時間は半日以内。

ＭＡ２２－４：１回の更新時間は１時間以内。

(3)**更新作業コスト（費用換算）（ＭＡ２３）**

更新コストは、人件費、計測器等の償却費、交換部品費、出張費などの合計とする。

ＭＡ２３－１：更新作業コストに関する特別な要件はない。

ＭＡ２３－２：更新作業コストは（　　）円以下とする。

２．６．３ その他（ＭＡ３）

(1)診断作業の自動化の程度（ＭＡ３１）

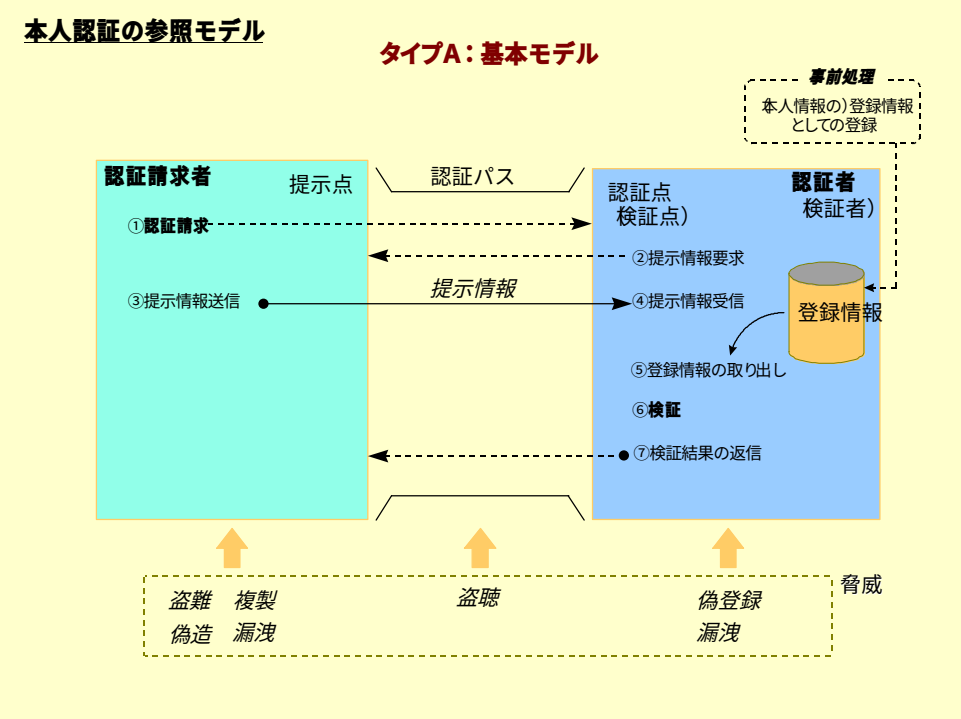
ＭＡ３１－１：キャリブレーションとか標準サンプルでの評価テストなどをしないとできない。

ＭＡ３１－２：自己診断がある程度可能。

ＭＡ３１－３：故障／照合性能低下に関する完全な自己診断が可能。

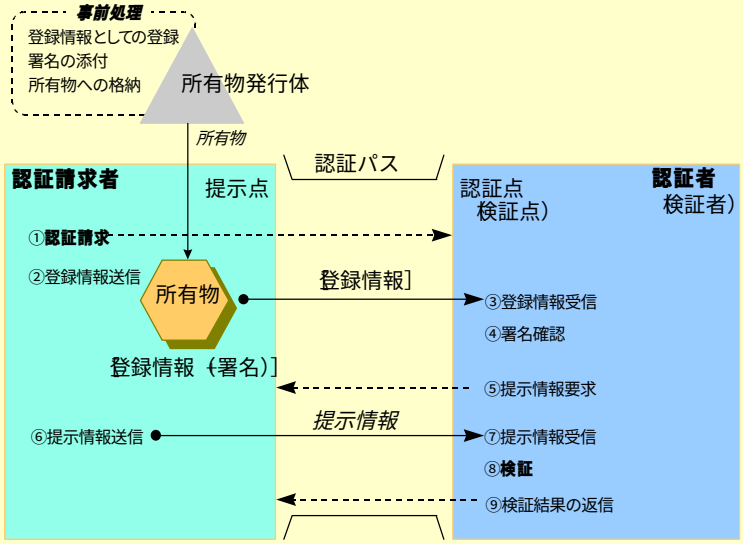
［解説］
装置としての性能が設置当初の性能からどの程度低下したかを判定するための機能に関する要件である。別の観点からいうと、部品交換等の時期の判定の自動化の度合いを示す要件でもある。

付録１ 本人認証の参照モデル



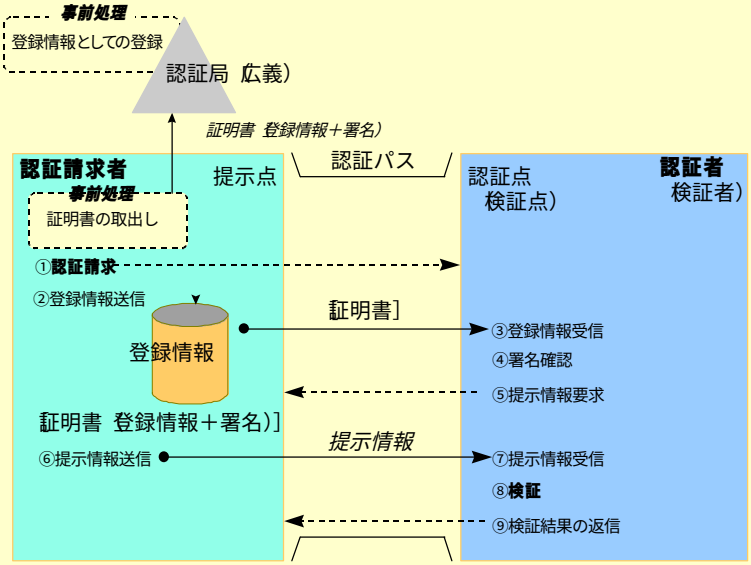
本人認証の参照モデル

タイプB：登録情報付き所有物認証モデル



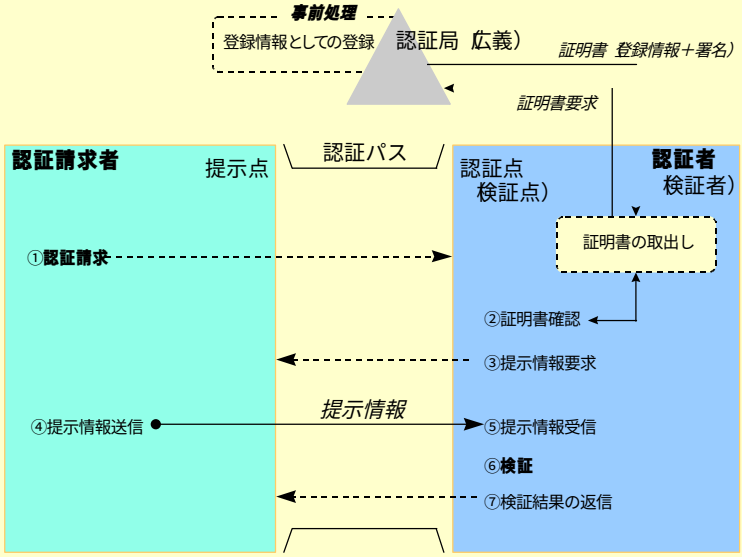
本人認証の参照モデル

タイプB'：証明書添付モデル



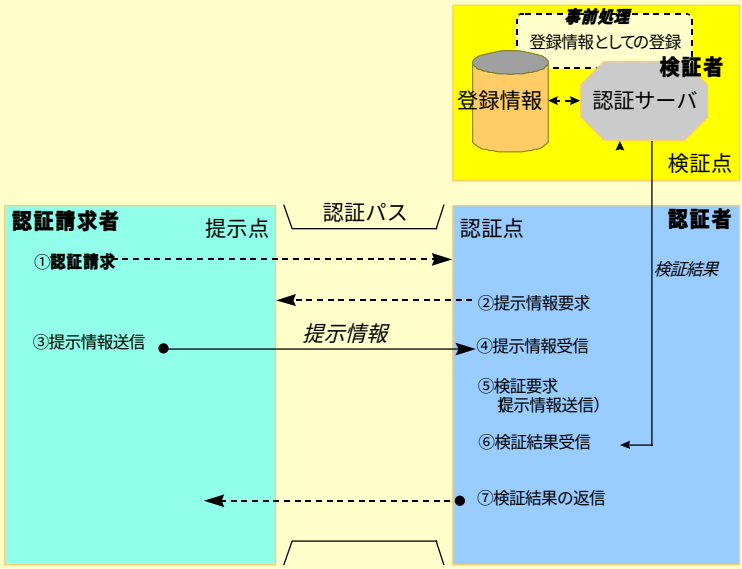
本人認証の参照モデル

タイプB”: 検証者による)証明書取寄せモデル



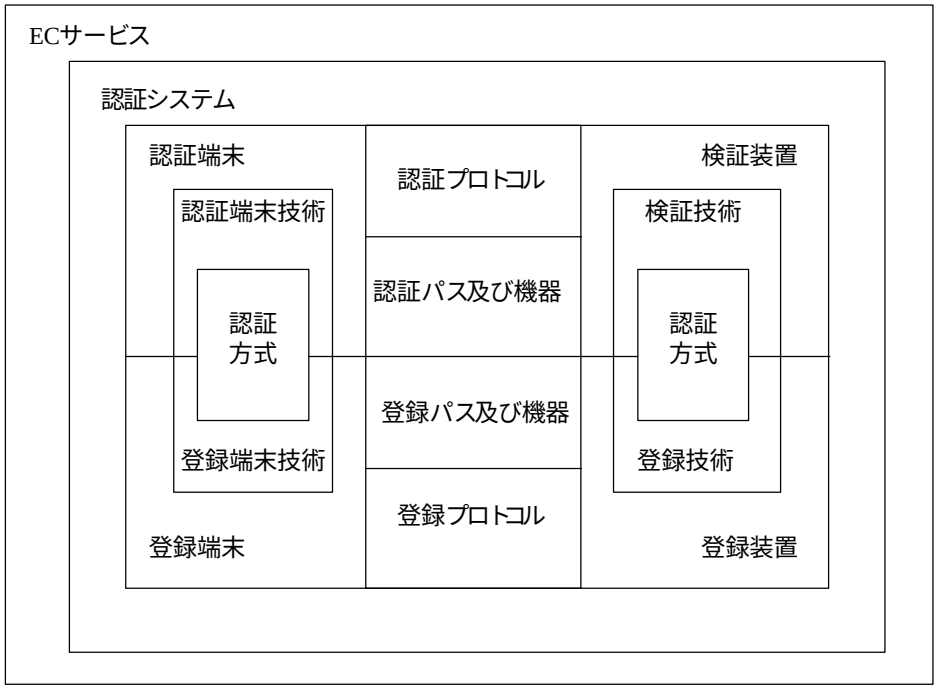
本人認証の参照モデル

タイプC :認証サーバモデル



付録２ 本人認証の実装モデル

実装モデルとは本人認証を実現する際に必要な技術（ハード、ソフト）、それらの技術を実装した装置・機器、プロトコル等の実装要素間の関連を示すものである。



＜用語定義＞

認証方式　　：本人認証の方式　　バイオメトリクスⅠ
バイオメトリクスⅡ
所有物
秘密情報Ⅰ
秘密情報Ⅱ

認証端末技術　　：提示点用技術　本人情報提示用端末用技術
認証端末　　：提示点　　本人認証提示の為の端末
認証パス及び機器　　：認証パス用通信回線及び機器
認証プロトコル　：認証パス用プロトコル
検証技術　　：検証点用技術　検証用技術
検証装置　　：検証に用いるハードあるいはソフト

登録端末技術　　：登録端末用技術
登録端末　　：登録用の端末
登録パス及び機器　　：登録パス用通信回線及び機器
登録プロトコル　：登録パス用プロトコル
登録技術　　：登録用技術
登録装置　　：登録に用いるハードあるいはソフト

認証システム　　：提示点 ～ 検証点までを含む
ＥＣサービス　　：認証システムを利用する

付録３ 評価基準の適用表（参考）

		認証方式	認証端末技術 登録端末技術）	認証端末 登録端末）	認証パス機器 登録パス機器）	認証プロトコル 登録プロトコル）	検 登
認証端末メーカー		○	◎	◎			
検証装置メーカー		○					
認証システム提供者		○	○	○	◎	◎	
ECサービス提供者							
ECサービス利用者		(○)	(○)	(○)	(○)	(○)	
評価者		○	○	○	○	○	
2．1社会的認知性（SA：Social Acceptability）							
2．1．1バリアフリーに関する要件	SA1						
⑴高齢者・身障者への配慮	SA11	＊		＊		＊	
2．1．2プライバシー保護に関する要件	SA2						
⑴本人情報の装置上及び認証パスへの残留	SA21			＊	＊		
2．1．3法的ないし制度的裏付け	SA3						
⑴根拠性	SA31		＊	＊			
⑵保険引き受け条件	SA32			＊			
2．1．4標準化	SA4						
⑴標準への準拠	SA41		＊		＊	＊	
2．1．5許認可の必要性	SA5						
⑴認証方式について	SA51	＊					
⑵機器について	SA52		＊	＊			

＊：該当　◎：提示　　○：参照

付録４ Version0.5からの変更点

社会的認知性（ＳＡ：Social Acceptability）

Version0.5	**第1版**
バリアフリーに関する要件（ＳＡ１） (1)高齢者・身障者への配慮（ＳＡ１１） (2)共用品（Universal Design）について（ＳＡ１２）	(1)高齢者・身障者・若年者への配慮（ＳＡ１１）
プライバシー保護に関する要件（ＳＡ２） (1)個人情報の管理体制（ＳＡ２１） (2)個人情報の閲覧・修正（ＳＡ２２） (3)個人情報が他の用途に使用されない保証（ＳＡ２３） (4)個人情報の削除（ＳＡ２４） (5)本人情報の装置上への残留（ＳＡ２５）	(1)本人情報の装置及び認証パス上への残留（ＳＡ２１）
法的ないし制度的裏付け（ＳＡ３） (1)根拠性（ＳＡ３１） (2)認証局（ＳＡ３２） (3)トラブル保険（ＳＡ３３） (4)保険引き受け条件（ＳＡ３４）	(1) 根拠性（ＳＡ３１） (2) 保険引き受け条件（ＳＡ３２）
標準化（ＳＡ４） (1)標準への準拠（ＳＡ４１）	(1) 標準への準拠（ＳＡ４１）
許認可の必要性（ＳＡ５） (1)認証方式及び、機器自体について（ＳＡ５１） (2)サービス提供者について（ＳＡ５２）	(1) 認証方式について（ＳＡ５１） (2) 機器について（ＳＡ５２）
その他（ＳＡ６） (1)宗教、因習、慣習によるタブー（ＳＡ６１）	

利用者受容性（ＵＡ：End User Acceptability）

Version0.5	**第1版**
心理的な抵抗感（ＵＡ１） (1)**誰でもが使用することができる（ＵＡ１１）** (2)**本人排除された時の救済手段（ＵＡ１２）**	(1) **本人排除された時の救済手段（ＵＡ１１）**
生理的な抵抗感（ＵＡ２） (1)**人体に対する安全性；安全規格への準拠（ＵＡ２１）** (2)**清潔感（ＵＡ２２）** (3)**恐怖感（ＵＡ２３）**	(1) **人体に対する安全性；安全規格への準拠（ＵＡ２１）**

脅威対抗性（ＴＣ：Threat Countering）

Version0.5	**第1版**
認証用所有物に対する脅威対抗性（ＴＣ１） (1)所有物の盗難（ＴＣ１１） (2)所有物偽造（ＴＣ１２） (3)情報の抽出・改竄（ＴＣ１３）	(1)所有物の盗難（ＴＣ１１） (2)所有物偽造（ＴＣ１２） (3)情報の抽出・改竄（ＴＣ１３）
提示情報入力装置における脅威対抗性（ＴＣ２） (1)提示情報の不法採取（盗聴）（ＴＣ２１） (2)提示情報の漏洩（ＴＣ２２） (3)不正置換（ＴＣ２３） (4)生体情報確認機能（ＴＣ２４） (5)設置環境と設置場所（ＴＣ２５） (6)違法性の表示（ＴＣ２６） (7)攻撃・調査のチャンスの限定（ＴＣ２７） (8)プレゼンテーション・装置デザイン（ＴＣ２８）	(1) 提示情報の不法採取（盗聴）（ＴＣ２１） (2)提示情報の漏洩（ＴＣ２２） (3)不正置換（ＴＣ２３） (4)生体情報確認機能（ＴＣ２４） (5)設置環境と設置場所（ＴＣ２５）
認証パスにおける脅威対抗性（ＴＣ３） (1)暗号化（ＴＣ３１） (2)非反復性（ＴＣ３２）	(1)暗号化（ＴＣ３１） (2)非反復性（ＴＣ３２）
検証点における脅威対抗性（ＴＣ４） (1)ファイアウォール（ＴＣ４１） (2)検証ソフトウェア・登録情報の漏洩・改竄（ＴＣ４２）	(1)ファイアウォール（ＴＣ４１） (2)検証ソフトウェア・登録情報の漏洩・改竄（ＴＣ４２）
トレーサビリティ（ＴＣ５） (1)攻撃の痕跡・証拠検出能力（ＴＣ５１） (2)攻撃者の記録保持（ＴＣ５２） (3)監査能力（ＴＣ５３）	(1)攻撃の痕跡・証拠検出能力（ＴＣ５１） (2)攻撃者の記録保持（ＴＣ５２） (3)監査能力（ＴＣ５３）
その他（ＴＣ６） (1)攻略メリットの限界・ユーザインターフェイス（ＴＣ６１） (2)事前教育・宣伝・啓蒙（ＴＣ６２） (3)不正アクセスに関する情報入手の可能性（ＴＣ６３）	(1)システムに関する情報入手の可能性（ＴＣ６１）

認証精度（ＡＡ：Accuracy of Authentication）

Version0.5	**第1版**
本人拒否率の測定方法の水準（ＡＡ１） (1)**本人拒否率測定におけるサンプル者数（ＡＡ１１）** (2)**本人拒否率測定における登録情報サンプル数／サンプル者・登録装置（ＡＡ１２）** (3)**本人拒否率測定における提示情報サンプル数／サンプル者・提示装置（ＡＡ１３）** (4)**本人拒否率測定における登録装置サンプル台数（ＡＡ１４）** (5)**本人拒否率測定における提示装置サンプル台数（ＡＡ１５）** (6)**登録装置とサンプル者との組み合わせ（ＡＡ１６）** (7)**提示装置とサンプル者との組み合わせ（ＡＡ１７）** (8)**登録装置と提示装置との組み合わせ（ＡＡ１８）**	(1)**サンプルの選択** (2)**登録情報サンプルの収集** (3)**提示情報サンプルの収集** (4)**本人拒否率の測定** (5)**本人拒否率におけるサンプル数（ＡＡ１１）** (6)**本人拒否率における登録および提示（ＡＡ１２）**

他人受入率の測定方法の水準（ＡＡ２） (1)**他人受入率測定における登録サンプル者数（ＡＡ２１）** (2)**他人受入率測定における提示サンプル者数（ＡＡ２２）** (3)**他人受入率測定における登録情報サンプル数／登録サンプル者･登録装置（ＡＡ２３）** (4)**他人受入率測定における提示情報サンプル数／提示サンプル者･提示装置（ＡＡ２４）** (5)**登録装置サンプル台数（ＡＡ２５）** (6)**提示装置サンプル台数（ＡＡ２６）** (7)**登録装置とサンプル者との組み合わせ（ＡＡ２７）** (8)**提示装置とサンプル者との組み合わせ（ＡＡ２８）** (9)**登録装置と提示装置の組み合わせ（ＡＡ２９）**	(1)**サンプルの選択** (2)**登録情報サンプルの収集** (3)**提示情報サンプルの収集** (4)**他人受入率の測定** (5)**他人受入率測定における登録サンプル数（ＡＡ２１）** (6)**他人受入率測定における登録および提示（ＡＡ２２）**
標準環境での基本認証精度（ＡＡ３） (1)**基本認証精度および対応率（ＡＡ３１）**	**認証精度（ＡＡ３）** (1)**認証精度および対応率（ＡＡ３１）**
限界基本精度（ＡＡ４） (1)**標準環境における限界基本精度（ＡＡ４１）** (2)**仕様条件限界基本精度（ＡＡ４２）**	**認証精度に関する機能（ＡＡ４）** (1)**精度バランス調整機能（ＡＡ４１）** (2)**登録情報の個別精度バランス調整（ＡＡ４２）** (3)**学習機能（ＡＡ４３）**
認証精度に関連する機能（ＡＡ５） (1)**精度バランス調整機能（ＡＡ５１）** (2)**学習機能（ＡＡ５２）**	**バイオメトリクスⅡにおける認証精度の扱い（ＡＡ５）** (1)**登録情報の自由度の問題** (2)**他人を真似る可能性** (3)**バイオメトリクスⅡにおける測定方法**
標準環境での実用認証精度（ＡＡ６） (1)**実用認証精度および対応率（ＡＡ６１）**	

限界実用精度（ＡＡ７） (1)**標準環境における限界実用精度** **（ＡＡ７１）** (2)**仕様条件限界実用精度（ＡＡ７２）**	

利便性（ＥＵ：Ease of Use）

Version0.5	**第1版**
操作性（ＥＵ－１） (1)本人情報登録・更新の容易性（ＥＵ１１） (2)認証請求の容易性（ＥＵ１２） (3)衣服等に関する要件（ＥＵ１３）	(1)本人情報登録・更新の容易性（ＥＵ１１） (2)認証請求の容易性（ＥＵ１２） (3)衣服等に関する要件（ＥＵ１３）
事前準備（ＥＵ２） (1)ハードウェア（ＥＵ２１） (2)ソフトウェア（ＥＵ２２） (3)事前学習の必要性（ＥＵ２３）	(1)ハードウェア（ＥＵ２１） (2)ソフトウェア（ＥＵ２２） (3)セットアップの必要性（ＥＵ２３） (4)ソフトウェアの配布形態（ＥＵ２４） (5)プラットフォーム＆ＯＳ（ＥＵ２５）
処理時間（ＥＵ３） (1)本人情報登録・更新の処理時間（ＥＵ３１） (2)登録申請から手続き完了まで（ＥＵ３２） (3)認証時の処理時間（ＥＵ３３）	**認証時間（ＥＵ３）** (1)認証時間
場所に関する条件（ＥＵ４） (1)本人情報登録可能な場所の制約（ＥＵ４１） (2)認証請求可能な場所の制約（提示点の制約）（ＥＵ４２）	
時間に関する条件（ＥＵ５） (1)本人情報登録可能な時間的制約（ＥＵ５１） (2)認証請求可能な時間的制約（ＥＵ５２）	
提示情報の保管（ＥＵ６） (1)所有物に関する条件（ＥＵ６１） (2)記憶の必要性（ＥＵ６２）	**提示情報の記憶（ＥＵ４）** (1)記憶の必要性（ＥＵ４１）
その他（ＥＵ７） (1)代理人可否（ＥＵ７１）	

保守･更新性（MA：Maintenance and Administration）

Version0.5	**第1版**
初期設置コスト（MA１） (1)**初期設置コスト（ＭＡ１１）**	**保守に関して（MA１）** (1)**保守が必要かどうか（ＭＡ１１）** (2)**メーカが行う１回当たりの保守の手間（時間換算）（ＭＡ１２）** (3)**ユーザが行う１回当たりの保守の手間（時間換算）（ＭＡ１３）** (4)**メーカの保守作業頻度（ＭＡ１４）** (5)**ユーザの保守作業頻度（ＭＡ１５）** (6)**保守作業コスト（費用換算）（ＭＡ１６）**
設置された機器の専門家による保守作業(MA２) (1)1 **回の保守作業時間（ＭＡ２１）** (2)**保守作業頻度（ＭＡ２２）** (3)**作業コスト（ＭＡ２３）**	**更新に関して（MA２）** (1)**更新作業をするのは誰か（ＭＡ２１）** (2)**１回当たりの更新の手間（時間換算）（ＭＡ２２）** (3)**更新作業コスト（費用換算）（ＭＡ２３）**
ユーザによる保守作業（MA３） (1)1 **回の作業時間（ＭＡ３１）** (2)**作業頻度（ＭＡ３２）** (3)**ユーザ保守作業コスト（ＭＡ３３）**	**その他（MA３）** (1)**診断作業の自動化の程度（ＭＡ３１）**
登録情報の保守作業（MA４） (1)**更新（再登録）作業の必要な周期（ＭＡ４１）** (2)**登録情報ファイルの保守作業（再編成等）（ＭＡ４２）**	
（所有物等の）提示情報の保守作業（MA５） (1)**提示情報保守作業の必要な周期（ＭＡ５１）** (2)**提示情報保守作業の専門性（ＭＡ５２）**	

以上

付録５：海外動向（論文等の紹介）

1.数学的手法を用いたバイオメトリクス装置の評価

2.バイオメトリクス製品認可試験の計画と提案

3.バイオメトリクス技術の検討と評価

4.IriScan 社製バイオメトリクス装置の研究評価

5.個人認証 API（HA-API)の仕様について

論文１：数学的手法を用いたバイオメトリクス評価への科学的アプローチ

（1997 年 10 月、CTST'97 における発表）

A Scientific approach to evaluating biometric systems using mathematical methodology

著者名：James L. Wayman ／San Jose State University**（米国）**

要約

バイオメトリック技術を利用したセキュリティシステムの性能評価には、精度、経済性、受容性などがあるが、本論文では精度評価の方法に関して論じている。

精度評価を行うため、バイオメトリクスの弁別性と再現性を知る必要がある。独自の判定方法（Decision Policy**）によって決まる他人受入率（**False Acceptance Rate**）と本人拒否率（**False Reject Rate**）は、判定方法およびバイオメトリクスの弁別性と再現性に依存しており、本質的な測度ではない。弁別性と再現性を決めるのはバイオメトリクスの特徴量間の距離である。**

サンプルの評価によって 2 つの分布を得ることができる。

第 1 の分布は、同一人物のサンプルと特徴量（template**）の距離から作成された「真の分布」であり、同じ人物の再現性を示す。**

第二の分布は、別人のサンプルと特徴量の距離から作成された「にせの分布」であり、別人の弁別性を示す。

バイオメトリクスの特徴量間の距離の分布を本人同士と他人同士に分離する場合、一般に両者の分布には重なり合った領域が存在するため、完全に分離できず誤差が生ずる。これらの曲線はバイオメトリクスの弁別性と再現性だけに依存するので、分布の分離度を表す無次元の測度を導入することにより、異なるバイオメトリクスを利用したシステムを共通の尺度で比較できる。

分布の分離度を表す測度としては、Transformed Receiver Operating Curve(TROC)、Equal Error Rate（EER）、D-prime **などがある。**TROC **はしきい値をパラメータにして、縦軸に偽一致率（**False Match Rate：FMR**）を横軸に偽不一致率（**False Non-Match Rate：FNMR**）をとったグラフである。信頼性が収集したデータとしきい値に依存するため、共通の評価にはならない。**

ERR **は** FMR **と** FNMR **を等しくとったときの値である。精度の評価基準としてとして**

扱われる場合があるが、収集したデータに依存する。

D-prime は正規分布やカイ二乗分布の分離度を表す。これらの測度はすべて母集団もしくはしきい値に依存している（つまり共通の尺度にはならない）。

バイオメトリクスの精度を測定するにあたり、まずバイオメトリクスの特徴量とサンプルを収集する必要がある。同一人物のサンプルと特徴量を比較して得られる距離は真の分布となり、別人の場合にせの分布となる。異なるテンプレート間の分布で、にせの分布を置き換えることも可能である。収集する特徴量とサンプルの数は、目的とする誤差（FMR や FNMR）と要求される統計的確度によって決まる。例えば、統計的確度 95%以上で誤差が 0.01 以下となることを示すためには、独立な 300 組の特徴量とサンプルが必要である。同一人物から得られるサンプルが互いに独立である保証はないため、統計的な独立性を失わないためには 300 人もの被験者が必要となる。

サンプルが M 個、特徴量がN個の M 対N認証の場合、他人受入率（False Acceptance Rate：FAR）と本人拒否率（False Reject Rate：FRR）の定義は判定方法によって異なる。以下に３つの例を示す。M 対１認証において、M 個のサンプルのうち 1 つ以上が特徴量と一致するとき受け入れられ、なにも一致しないとき拒否されるとする。このとき本人拒否率は偽不一致率の M 乗となり、他人受入率は近似的に偽一致率の M 倍となる。また 1 対 N 認証において、1 つ以上の特徴量と一致すると受け入れ、それ以外を拒否する場合には、他人受入率は近似的に偽一致率の N 倍となり、本人拒否率は近似的に偽不一致率に等しくなる。このとき他人受入率は N に従い大きくなるが、1 をこえることはなく、また現実の他人受入率は不正利用率との積になるため、さほど問題ではない。

もう一つの 1 対 N 認証の例として社会サービスを挙げる。ここでは、一致が見つかると申請者を拒否し、一致が見つからないと申請者を受け入れるものとする。このときの他人受入率の期待値は FMR の N 倍となり、N が大きくなると 1 をこえる。すなわち P 回の 1 対 N 認証において平均 P 回以上の他人受入が生じ、システムは破綻する。この問題を軽減するには、特徴量のデータベースを区分し、N を小さくすればよい。これにより本人拒否率が減少し、他人受入率が増加する。不正登録者の割合は、他人受入率と不正利用率の積であるため、不正の率が低い場合には、高い他人受入率でも問題ない。

以上の議論では収集したサンプルによって作成された分布を使用している。統計的信頼区間はサンプルが少ないことによる不確実性を考慮しているが、アプリケーションに対するサンプルの適合性を反映していない。精度評価の適切な目標は、精度限界を与えること

にあり、一般的なサンプルにおける精度の下限および特殊なサンプルにおける精度の上限を示すことである。

　しかし現在これらの限界はいずれの装置でも示されていない。精度はバイオメトリクス装置の最良の評価方法として扱われてきたが、実際にはユーザー受容性、価格、処理速度なども評価に含める必要がある。

論文２：NCSA のバイオメトリクス製品の認証試験／1997 年

Biometric Product Certification Test Plan & Proposal

著者名：米国・NCSA **社／** National Computer Security Association

要約

１ NCSA **による認証の概要**

NCSA（National Computer Security Association）**は現在は改称して** ICSA（International Computer Security Association）**を名乗る米国の民間団体である。（本稿では** NCSA **で統一した。）**NCSA **ではウイルス対策製品、ファイアウォール等の製品から** WWW**、インタネットのサイトのようなシステムにいたるさまざまなカテゴリーにおいて認証を行っている。**

認証のための試験は公開された基準に基づいて行われ、結果は合格／不合格のいずれかになる。合格した製品・システムに対して認証が与えられる。認証を受けた製品・システムは NCSA **が主催する会議やその他の有名な会議／展示会において** NCSA **が展開するキャンペーンに採り上げられる。さらに、**15,000 **部以上発行される** NCSA **ニュースの記事としても載せられるし、**NCSA **の** WWW **サイトの認証製品一覧に各社のコンタクト先とともに収録されて、広く公開される。また認証を受けた会社は** NCSA **認証のロゴを販促・宣伝媒体や** WWW **に使う事ができる。**

認証を受けるための価格体系は以下のとうりである。

最初に認証を受ける機種については＄22,500

（1 **年間の期限付きの認証と** NCSA **ロゴの使用権および** NCSA **キャンペーンへの参加権が含まれている。）**

２機種目の製品については＄19､000

３機種目以降は＄15,500 **の割引制度がある。**

２　バイオメトリクス製品のための評価基準

NCSA **では次の** 3 **つのフェーズに分けて評価を実施する。**

２．１　評価のフェーズ

(1)**フェーズ** 1**：スクリーニング・試験**

フェーズ 1 はフェーズ 2 以降を始めるための準備作業的なフェーズであり、以下のような作業からなっている。

(a)評価基準と評価計画の定義する。

(b)評価者に対してそのベンダーの技術・製品に関する教育を実施する。

(c)評価対象の装置を搬入する。

(d)対象がプロトタイプであれば、ベンダーの支援を得て準備評価を行う。

(e)フェース２以降の評価に耐えられる製品であることを確認する。

(2)フェーズ 2：Verification（1 対 1 照合）

フェーズ２では、本人拒否率および他人受入率を計測する。

(a)フェーズ 1 の結果を踏まえた評価基準・計画を立案する。

(b)評価中はベンダーは立ち会わないが、装置に問題が生じた場合、速やかな交換等の処置を行う。

(c)フェーズ１の評価結果に基づいて、より厳密な評価を行う。

(d)評価対象に関わる人的要因を記録する。

(e)評価結果に対して統計処理を行う。

(f)認証結果を WWW で公開する。（ただし、合格した場合のみ。）

(3)フェーズ３：Identification（1 対多照合）

フェーズ３では、False Positive Identification Rate（登録外の人が登録した人と見とめられる誤り）および False Negative Identification Rate（登録してあるにもかかわらず本人と認められない誤り）の計測を行う。

(a)生サンプルを 3,000 件用意する。指紋であれば、300 人からそれぞれ 10 指の情報を収集してもよい。

(b)フェーズ 2 の評価を踏まえて、フェーズ 3 の評価計画を立案する。

(c)更に、3,000 件のサンプルを追加する。

(d)3,000 件の生サンプルと 6,000 件のサンプルとの間で照合を行う。

(e)6,000 件に対して 3 秒以内の照合で、F+/F-が 1%以下であることを検証する。

(f)結果に対して統計処理を行う。

(g)結果を WWW 上に公開する。（認証に合格した場合のみ）

(h)サンプル数は将来的には 30,000 件に増やすつもりである。

２．２　サンプルの条件による評価のサブクラス

(1)生サンプリング

(a)サンプル者は NCSA 職員及び会員企業から選ばれる。

(b)サンプル者は１年間に少なくとも４回サンプリングに参加することが要請される。これは季節等の環境条件の変化を網羅するためである。

(c)将来的にはサンプル者は大学､病院､展示会、アミューズメントパーク等で選ぶ予定である。

(2)蓄積された生サンプル

(a)生サンプリングの過程で得られたデータを蓄積しておく。

(b)蓄積されたデータで、正しくサンプリングされたものは再現デバイスによって読み取りセンサに対して再現できなくてはならない

(c)再現デバイスは全ての信号を再現できなくてはならない。

２．３　１対１照合の評価

(1)本人拒否率（FRR）の測定

各サンプル者に対して以下の手順で評価を行う。

(a)バイオメトリクス装置でサンプル者毎に３回データを登録する。

(b)３回連続的に試行して、本人と認められなかった場合を本人拒否と定義する。

（本人拒否されたら､続けてもう２回の試行のうちに本人と認められればよい。）

(c)各人が５回、本人認証をトライする。

(d)さらに以上の手順を季節毎のスポットを選んで、３回繰り返す。

(2)他人受入率（FAR）の測定

各サンプル者に対して、以下の手順で測定する。

(a)その他の 5 人をランダムに選び､それらの選ばれたサンプル者が最初のサンプル者として誤認されるかを確認する。

(b)(a)のランダムな選択を３回行って他人受入が起こるかの検証を行う。

２．４　１対多照合の評価

(1)False Positive Identification rate の測定

(a)登録情報データベースの登録されていないサンプル者を選ぶ。

(b)登録情報データベース全体と照合して、正しく拒否されることを確認する。

(c)３回連続して、なりすましを試みる。

(2)False negative Identification rate の測定

(a)(1)のテストの後で、新たなサンプル者を登録データベースに登録する。これは一人当たり３回のトライを行い、良好な登録情報を得る。

(b)新しく登録したサンプルが正しく本人と認証されることを確認する。

(c)正しく認証されるまでに、３回のトライを許す。

(d)上記のテストを５回繰り返す。

(e)さらに以上の手順を季節毎のスポットを選んで、３回繰り返す。

２．５　人的要因の記録

サンプル者に関する以下のような属性が記録対象として挙げられるが、製品のベンダーからの申告によって必要の無い属性も有り得る。

(1)年令

(2)性別

(3)体重

(4)皮膚の色

(5)髪の色

(6)眼の色

(7)職業

(8)趣味

２．６　サンプル者数の統計的充分性について

エラー率が 1%以下であることを結論づけるために、必要なサンプル者数とその時の信頼度は以下の通りである。

80%の信頼度を得るためには、161 人、

85%であれば、189 人、

90%であれば、230 人、

95%であれば、300 人、

99%であれば、459 人のｻﾝﾌﾟﾙ者が必要となる。

従って、300 人のｻﾝﾌﾟﾙ者を用いるこの評価には 95%の信頼度がある。これらのサンプル者が一般的な人口構成を反映したものであるか否かが結果の信頼性に大きく影響する。そのため前記の人的要因に関して統計的アプローチを行って、これを検証しなければならない。

以上

論文３：バイオメトリクス技法／識別および認証用バイオメトリクス技法の検討と評価
（1994 年 4 月）

Biometric Techniques: Review And Evaluation Of Biometric Techniques For Identification And Authentication, Including An Appraisal Of The Areas Where They Are Most Applicable

著者名：Despina Polemi ／ **国立アテネ工業大学／通信コンピュータ・システム研究所**
Institute Of Communication And Computer Systems
National Technical University Of Athens

要約

この論文の主たる目的は、適用領域の評価を含めてバイオメトリック技術を検討・評価することである。また、この研究は、論文、技術報告書、評価用調査、メーカおよび設計者の主張など利用可能な文献に基づいている。

文献に基づいて、この研究ではバイオメトリクス方式と装置を評価するための「基準」を提案している。この基準は 2 組からなり、第 1 組はアルゴリズムやプロトコルの評価のため、第 2 組は操作、財務面などを評価するためのものである。

論文の主な構成は以下のとおりである。

1. **バイオメトリクスの包括的アプローチ**
2. **バイオメトリクス技法・システム・デバイス**
3. **アプリケーションの領域**
4. **結論・推奨事項**

付録：バイオメトリクス・テクノロジーに対する基準
（方式に対する基準、装置に対する基準）

(1) **バイオメトリクスの包括的アプローチ**

認証の手続きは次のようなアプローチによる。

- **知識によるもの**
  本人のみが知っているか、提出できる情報。
- **所有（物）によるもの**
  目標物の所有をしていること。

- **プロバティ（人的特徴）によるもの**
  本人の人的特徴を使用するもの。

＜精度測定＞

伝統的な認証手段であるパスワードは、入力の正誤により、受入れられるかまたは拒否されるかのいずれかのものであるのに対して、バイオメトリクスは人間の特徴や行動を測定するものであるから、本人拒否エラーや、他人受入エラーが発生する。この 2 つのエラーの許容差をどのように設定するのかが、システムの精度設定にとって非常に重要な要素である。

＜テンプレート＞

利用者のテンプレート記憶場所は、アプリケーションやそのサイズによる。

- **バイオメトリクス・デバイスのメモリ**
  メモリに格納すればテンプレートが伝送されないのでセキュリティが向上。
- **中央データベース**
  利用者が多い、あるいは遠隔検証が必要なときに用いられる。
  データベースへの侵入対策が重要である。
- **プラスチックカードまたはトークン**
  利用者自身がテンプレートを搬送できる。

＜脅威＞

脅威の根元には次のようなものがある。

- **自然：天災や環境条件**
- **技術：ハードやソフトにおける障害や、誤動作。**
- **人間：アクセス未許可の人間やハッカーなど。**
- **理論：アルゴリズムやプロトコルの脆弱さ。**

脅威の種類：

進入、サービス拒否、情報開示（漏洩）、情報破損、未許可資源の使用など。

(2) **バイオメトリクスの技法、システム、デバイス**

ここでは、さまざまなバイオメトリクスをその特徴により分類している。

1.生理学的バイオメトリクス技法

- **指紋照合、虹彩分析、顔分析、手の形状－血管パターン、について**

2.行動によるバイオメトリクス技法

- **音声（声紋）分析、手書署名検査、キーストローク分析、について**

3.新しいバイオメトリクス技法

- **DNA パターン、汗孔分析、耳の認識、臭気の探知、について**

（3）アプリケーションの領域

バイオメトリクスが最も適用可能な領域のアプリケーションをあげ、その特徴について述べている。

- **公共事業：入国審査等への応用。福祉における給付金支払いなど。**
- **法の執行：投票。犯罪者の識別。**
- **銀行業務：ATM、ホームバンキングへの応用。**
- **物理アクセス管理：特定の建物などへの入退。会員権使用者の確認。**
- **コンピュータとネットワーク：端末、ネットワークへのアクセス制限など。**

（4）結論・推奨事項

バイオメトリクス方式のセキュリティ上の強さを証明する必要がある。とくに、バイオメトリクス方式を任意の暗号解読攻撃に対してテストをする必要があるが、そのようなテストが専門の機関などによって実行されることが望ましい。

また、独立した（メーカが関与しない）評価センターによってシステムが評価されることが必要である。そこで、バイオメトリクス装置をブラックボックスとして扱い、どれだけうまく機能するかを調べる必要がある。

バイオメトリクス技術に対する自信の欠如は、「標準」と試験の欠如によるものである。「標準」の存在はバイオメトリクス技術がセキュリティを提供するための信頼できる選択であることを証明することになるだろう。

バイオメトリクス技術に対する基準

1．方式に関する基準

- **正しい（より良い）アルゴリズム**
  そのアルゴリズムによって実行された数学が正しい。
- **安全なアルゴリズム**
  解読困難なアルゴリズム。
- **安全なデータベース**
  データベース管理者が信頼できることが証明される必要がある。
- **安全なプロトコル**
  欠陥のないプロトコルなど。
- **安全なネットワークと分散システムであること**
  利用するネットワークの安全性を（専門機関よって）評価する必要がある。

2．装置に関する基準

- **操作面**
  便利であること、ユーザーフレンドリーであることなどが規定されている。
- **技術面**
  最低認証時間、測定・記憶時間、テンプレートのサイズなどがあげられている。
- **費用面**
  装置費用、更新費用、システム管理サポート費用などがあげられている。
- **製造面**
  サポートと交換データがあげられている。

論文４：IriScan 社のバイオメトリック識別装置 プロトタイプの研究評価

1996 年 4 月

Laboratory Evaluation of the IriScan Prototype Biometric Identifier

著者名：Frank Bouchier, Janet S. Ahrens, Grant Wells ／ 米国・サンディア国立研究所

Entry Control/System Engineering Department

Sandia National Laboratories

要約

これはサンディア国立研究所の入室管理／システム・エンジニアリング部門が作成したレポートであり、IriScan 社が開発したプロトタイプのバイオメトリック識別装置の 95 会計年度中に行った評価について述べている。この識別装置は、人間の目の虹彩に特有な視覚的特徴に基づいて個人を認識するために開発されたものである。評価の主な目的は、ボランティアを募った試験を通し、このシステムをアクセス管理装置としてエネルギー省（DOE）内で使用できる可能性があるかをどうかを決定することであり、主な評価項目は、他人受入率および本人拒否率の点でシステムの精度を評価することである。また、収集したスループット時間および利用者許容度を推測するデータに関しても言及している。

利用者インタフェース

利用者は可動式サブシャシーに装備されているバックライトの LCD モニターを見ることにより、システムとのインタフェースを取る。このモニターは、部分反射鏡の後ろに設置されている。反射画像はビデオ・カメラに送られ、ビデオ・カメラは瞳の入力画像を取り込み、プロセッサー・シャシーに装着された LCD モニターおよびフレーム・グラバーに入力する。このように、利用者は、自分の目の画像がモニターの中心におかれ、焦点が合うようになるまで、頭を動かすのと入力サブシャシーを傾けるのを組み合わせて行うことにより、画像の目の位置を調整し、焦点を合わせることができる。画像表示器から約 2 インチ下のところに置かれた小さなハロゲン・ライトは、赤いフィルターを通して照明を行う。

登録プロセス

利用者は、上述したように目の位置を調整する。オペレーターは、フレーム・グラバー

の出力を表示する外部モニター上で利用者の位置調整を監視する。利用者が適切に位置調整を完了したら、オペレーターは登録プロセスを開始する。システムは、フレーム・グラバーから 3 つの連続した画像を収集し、それぞれの画像に対して虹彩コードを生成する。3 つの虹彩コード中のハミング距離の平均が十分小さい場合、オペレーターは、その人の目の登録を選択する。

認識プロセス

利用者はメイン・シャシーのフロント・パネル上のボタンを押し、モニターに向かって目の位置調節を行うだけである。システムは、その人の目を認識するため、多くの試行を行う。それぞれの試行で、システムは、十分なコントラストが得られるまで画像を収集する。そして、その画像の虹彩コードを生成し、データベース内の虹彩コードと突き合わせる。新虹彩コードと登録された虹彩コードの中の 1 つとの間のハミング距離が十分小さい場合、システムはマッチするものが見つかったと判断し、受諾ビープ音を発して画像収集を終了する。試行後、マッチするものが見つからなかった場合、システムは拒否音を発する。

試験解説

システムはビルの屋根付き通路に設置されたが、この場所の難点は、多方向からの日光の照射を可能にする大きな窓である。それは、虹彩画像に反射光が入る原因となった。

約 400 の目が予めメーカーによるシステムに登録されており、更に 122 人のボランティアがこの試験のために登録された。両目を登録してもらう予定であったが、人によっては両目を登録するのが難しいことが確認された。難しい場合は片方の目のみを登録した。結果として、122 人から 199 の目が登録された。

登録者の虹彩認識の試行は、オペレーターによって観察され、試行結果も記録された。有効な利用者の拒否を、それぞれ本人拒否（FR）と呼び、これらのトランザクションを FR 試行と呼ぶ。次に全ての登録者はデータベースから削除され、メーカーによって提供された 403 人の登録者のデータが再び格納された。ボランティアは、その後もう一度、虹彩認識の試行を行った。有効でない人の認識を、それぞれ他人受入（FA）と呼び、これらのトランザクションを FA 試行と呼ぶ。

試験結果

登録

新規利用者の登録は、ほとんどの人が画像システムに順応するのに時間を要したが、利用者が一度順応してしまうと、ほとんどの登録は素早く行われた。登録は普通きき目であったが、もう一方の目を登録しようと試みて困難な場合は登録をあきらめた。平均登録時間は、2 分 15 秒である。これはシステムの概要を始めたときから最初の目の登録が完了するまでの時間である。

本人拒否試験

この試験の初期段階では、895 件のトランザクションに対し 106 件の拒否（11.8%の FR 率）が記録された。この本人拒否に関する理由は以下の３グループにまとめられる。

グループ１）利用者または環境エラー

利用者が登録されていない方の目を提示したり、その他数多くのエラーが含まれた。

グループ２）眼鏡からの反射

通常眼鏡をかけている利用者はすべて眼鏡をかけたままでシステムを使用した。ほとんどの利用者は問題なかったが、非常に厚い眼鏡や汚れた眼鏡をかけている何人かの利用者には困難であった。

グループ３）利用者の困難

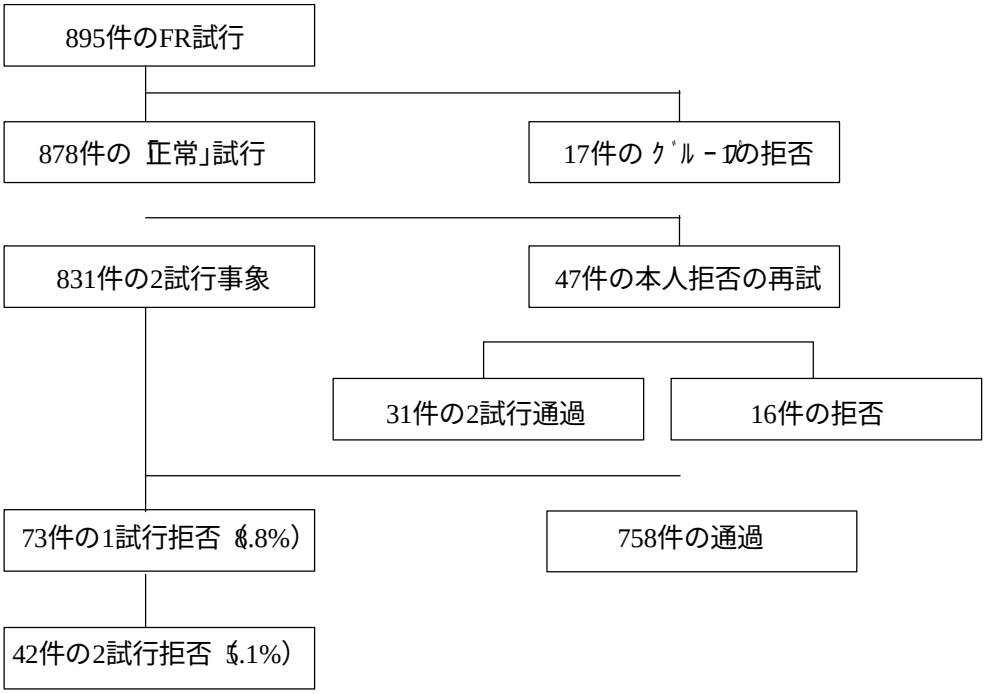
髪の毛による画像の不明瞭化、焦点を合わせる上での困難、もう一方の目でシステムを使用するのがより困難などを含めた利用者の困難。

次にエラー率を分析する。グループ 1 に属す 17 件のトランザクションを取り除くと、878 件の「正常な」トランザクション（89 件の FR）が残り、FR 率は 10.2%であった。しかし、本人拒否のいくつかは 1 つ以上のグループに起因するため、各グループにおけるエラー率がどの程度かを決定するのは困難である。

本人拒否された多くは再試行を行い 2 試行で通過した。このため、2 度目試行でのエラー率を判定した。この分析では、トランザクションは事象ごとにグループ分けされた。2 試行事象は、認識されようとする試行および拒否された場合に同じ目で繰り返し行われる試行からなる。878 件の「正常な」トランザクションの内、47 件が再試行によるものであり、831 件の 2 試行事象が残った。47 件の再試行を検証してみると、31 件が通過し 16 件

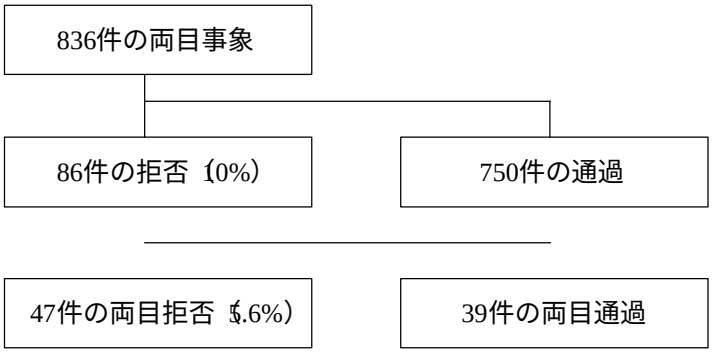
が拒否された。このことにより、最初の試行では 73 件の拒否が残り、42 件が 2 試行の機会を与えられた後に依然拒否されたことになる。これは、1 試行の FR 率が 8.8%、2 試行の FR 率が 5.1%ということを導き出す。

本人拒否試験（ＦＲ試行）



片方の目と両目によるＦＲ率を調査した結果では、836 件の両目事象のうち、最初の試行の後 86 件の本人拒否が発生し、内 47 件はもう一方の目で再試行後も依然として拒否された。これにより、片目 FR 率が 10%、および両目 FR 率が 5.6%という結果が得られた。

両目による本人拒否試験（ＦＲ試行）



トランザクション時間

平均トランザクション時間	最低トランザクション時間	最高トランザクション時間
14 秒	6 秒	23 秒

この時間は、利用者が最初にスタート・ボタンを押したときからシステムが認識または拒否を示すビープ音を発するまでの時間

以上の結果よりシステム性能に及ぼす影響として、試験を効き目でするか否かが影響を及ぼし、オペレーターのコメントとして、利用者の身長、眼鏡のレンズの厚さ、および体重が、本人拒否率に影響を及ぼすとして指摘された。

他人受入試験

他の確認装置と異なり、IriScan 社の装置は認識装置であり、データベース上のそれぞれの登録者と突き合わせてマッチングを試みる機械である。この試験では、データベースはメーカーが提供したオリジナルの 403 件のテンプレートに限られた。そして、各ボランティアによる１回の試行では、実際の他人受入が 1 件も発生せずに、96 件の FA トランザクションが記録された。

結論

本システムは、困難な条件下においてきわめて正常に実行された。試験設置場所の強い周囲の光からの反射が本人拒否のうちの何件かの原因となった可能性がある。これは、システムが屋外または窓の近くで使用される予定の場合、囲いまたは少なくとも側面に日除けを置く必要があるということを示す。それでも、システムの本人拒否率は良好であり、他人受入はまったく観測されず、高精度のセキュリティー・アプリケーション用に使用できる可能性が示された。

また、この試験は、本システムが高機密性バイオメトリック識別装置として使用される可能性が非常に高いということを示した。DOE コミュニティーにおいて十分関心が示されるなら、製品システムのより完全な調査を引き続き行うべきである。そのような調査では、本試験中発見された性能に影響を及ぼす変数について考慮に入れるべきである。また、追跡調査には、不防備性分析も含まれるべきである。

論文５：個人認証 API（HA-API)の仕様について／1997 年 11 月

Human Authentication - Application Program Interface Ver 1.02

著者名：米国・ナショナルレジストリ社／The National Registry Inc.

要約

本仕様書は、米国ナショナルレジストリが米国国防総省向けに作成、提唱したものであり、バイオメトリクスをベースにした個人認証用のアプリケーション・プログラム・インターフェース（API）を定義したものである。正式名称は Human Authentication - Application Program Interface **であり、略称を** HA-API **という。**1997 **年の** 8 **月** 27 **日に** Rev.1.0 **が作成され、**1997 **年** 12 **月** 30 **日現在で、**Rev.1.03 **である。全部で** 9 **章からなり、**

１章：全体解説、

2 **章：設計、**

3 **章：機能、**

4 **章：**API **定義、**

5 **章：アプリケーション連携、**

6 **章：構造、**

7 **章：メッセージフローサンプル、**

8 **章：リファレンス、**

9 **章：その他、**

で構成される。Rev.1.03 **では** A4 **版で** 61 **ページのドキュメントである。**

HA-API **の目的は、バイオメトリクスベースの個人認証において、**API **を共通化し、複数のバイオメトリクス認証方式の統合を可能にすることにある。下記にその目的の詳細である。**

１）インターオペラビリティの向上

- **同一のアプリケーションを使いながら､バイオメトリクス技術の更新あるいは変更を可能にする柔軟性**
- **同一のアプリケーションを使いつつ､バイオメトリクス装置や技術を提供しているベンダーの更新あるいは変更を可能とする柔軟性**

２）セキュリティーの向上／リスクの低減

- **複数のバイオメトリクス技術の組み合わせを行い、安全性の向上を実現する**

- 複数のバイオメトリクス技術の組み合わせにより、一般へのシステム対応性を高め、システム運用時の不正な認証／拒絶エラーの発生する可能性を減少させる

3）個人認証 API インターフェースの標準化

- 汎用性のあるインターフェースの導入により、個人認証における多様なバイオメトリクス技術の統合を可能にする
- 大幅なソフトウェアの再設計をともなわずに各種バイオメトリクス技術を増設・変更ないし組み合わせられる柔軟性を実現する

要するに、標準 API の導入により、システムやアプリケーションに対してバイオメトリクス技術もしくは装置の組み合わせを可能にし、装置変更時のアプリケーション開発への負荷を低減することが目的である。

HA-API で想定しているシステムは、ネットワーク用オペレーティング・システム上で動作するクライアント・サーバ型のユーザ認証システムである。HA-API の実装例として検討されているバイオメトリクス技術は、指紋、音声、顔による照合である。

2．仕様検討にあたって

HA-API はオープン・システム・アーキテクチャーと、可能な限り広範なバイオメトリクス製品とメーカー、ならびに広範なバイオメトリクス認証用途の両面において可能な限りオープンであるよう設計されている。プラットホームないし機器依存は想定されていない。HA-API を検証するためのターゲットには、指紋の画像処理、音声認証および容貌認識キャプチャー/エンジンをサポートした、TCP/IP LAN を介したクライアント／サーバー環境における Windows NT ログイン機能を選択している。HA-API を検証し実装するためのターゲットアプリケーションは、ナショナルレジストリ社の The Secure Authentication Facility for Windows NT（SAF/NT）に設定されている。Windows NT のセキュリティー・アーキテクチャー内で該当するものがあれば既存のサービスを利用しながら、既存の機構を考慮して作業を進めている。現状でのソフトウェア環境は「C」言語に基づく Win32 クライアント／サーバー環境用として定義されているが検証後に他のソフトウェア・プラットホームへの移植も可能となる。

３．HA-API の構造

HA-API の構造には、各バイオメトリクス技術固有の側面と、各メーカーの独自機能、製品および機器の相違をの影響を可能な限り抑えながら、複数のソフトウェア・アプリケーションでの利用に対応するために、バイオメトリクス機能からなる「ツールボックス」を提供するアプローチが取られた。ツールボックスへのアクセスは、一連の標準的なインターフェースによって行われる。メーカーから供給されるバイオメトリクスコンポーネントが、HA-API インターフェース仕様に準拠していれば、HA-API に則って開発された任意のアプリケーション上で使用可能となる。

HA-API はアプリケーション開発者とバイオメトリクス技術の開発者の双方の利用を意図して設計されている。また、バイオメトリクス技術に伴う繁雑さを可能な限り表に出さないように考慮されている。この方法は、多くのバイオメトリクス技術とアプリケーションに対応させ、インターフェースの汎用性を広げるのに役立っている。

HA-API の範囲は最上位にある「登録」および「確認」機能から、機器の動作を司る最下位のサブファンクションにまで及んでいる。もっとも有用で、かつ汎用性を保っているとの観点から、最上位機能から１階層下に位置する機能を選択している。

HA-API は、複数のバイオメトリクス方式を、各々単独で、組み合わせで、カスケード方式で、複数サポートできるよう設計されている。複合的なバイオメトリクス認証に対応するには、こうした構造が適しているという。

４．登録照合機能について

初期バージョン（当該 HA-API のバージョン 1.0x）では、バイオメトリクス API による一対一確認形式のマッチング処理がサポートされている。想定した認証環境下（クライアント・サーバ型のログイン等）では通常、一対多の検索マッチング処理は要求されておらず、また現在の作業方針からの逸脱を強いる（精度、応答時間、複数候補間の判定、およびデータベース同調問題をはじめとする）付加的な課題や考慮を要するため、この種の機能の導入は見送っている。ただし、使用の記述にあたっては一対多検索マッチング機能の導入を排除せぬよう配慮している。

照合時のマッチング・スコア、閾値設定および精度スコア／閾値に関する問題は、現時点では業者に依存すべきと捉えている。したがってこの種の値における絶対的な要求値は定められていない。しかし、任意のバイオメトリクス方式の応用について、各種の当該パ

ラメーターを取得および／あるいは設定するためのより洗練された開発者／アプリケーションの採用を許容する情報機能の定義がなされている。任意のメーカー／製品に関する情報機能の使用は、当該製品に関するプログラマーの記述によって定義されることを前提にしている。オペレーティング・システム上のアプリケーションへの対応に加え、API は（バイオメトリクス試験へのサポートなどの）非オペレーティング・システム環境下でも使用可能となっている。ただし、上記の情報機能は綿密な試験に通常求められる設定や詳細な結果を得るために利用される可能性が高いと考えている。メーカーは、別途もしくはオプション機能として試験モードないしツールボックスを供給するよう奨励されている。

５．データ形式とデータベース管理

本 API はクライアント（ローカル）とサーバー確認処理の双方をサポートしている。汎用性を最大限に高くしてクライアント／サーバー環境をサポートするため、バイオメトリクスデータベースは中央サーバー内に格納するよう推奨される。これが最も適当な使用法であり、ローカル端末とサーバーの双方における確認処理がサポート可能となる。バイオメトリクスデータの形式は 6 章で述べられている。

データベース機能に関しては、各々のシステムおよびアプリケーションでは異なったデータベース形式および設計を採用するため、（バイオメトリクスデータの追加、削除および検索をはじめとする）HA-API の仕様では省略されている。

以上

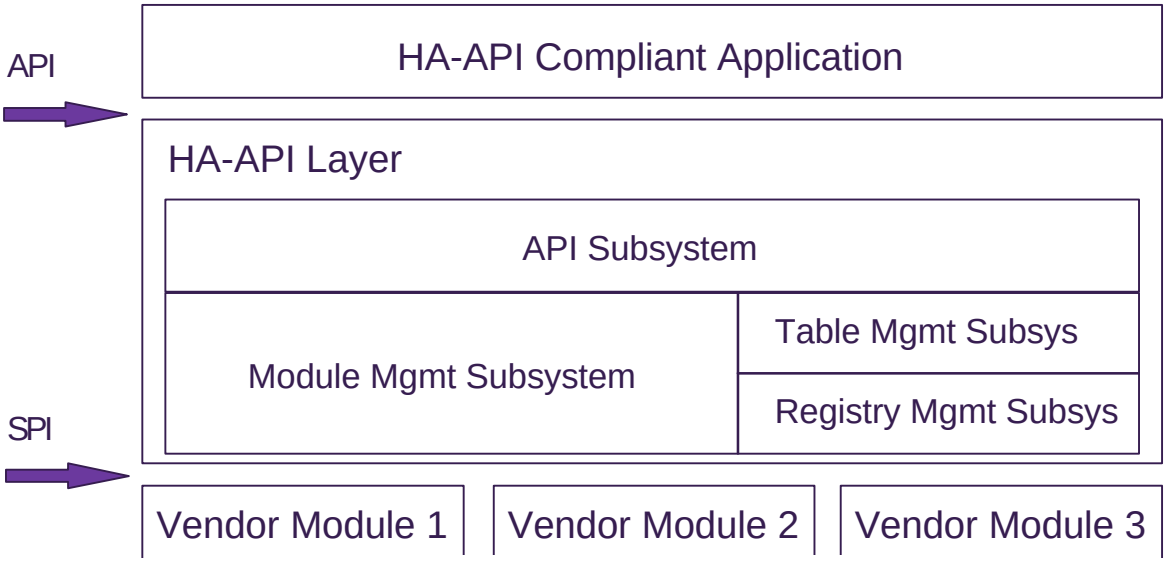


図 1 HA-API の構造

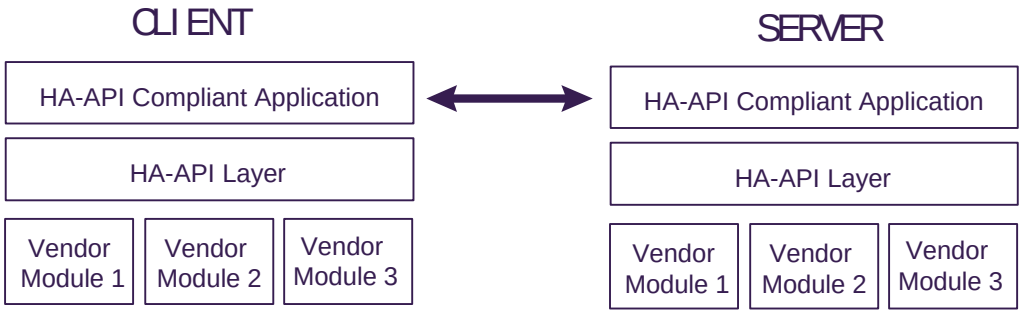
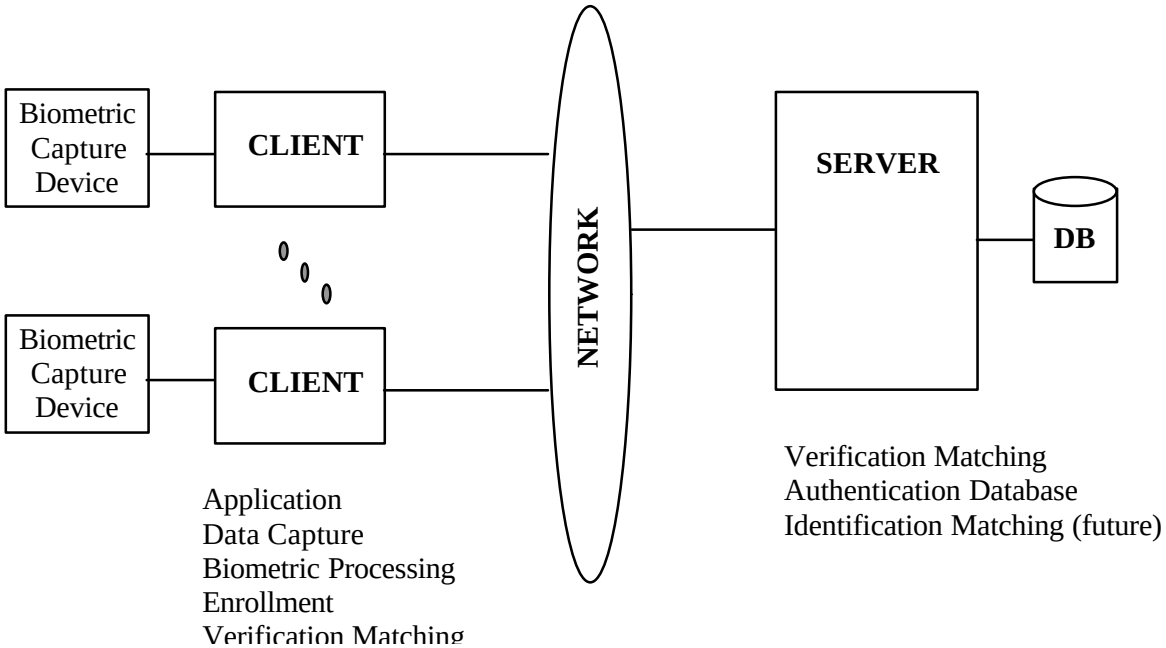


図 2 クライアントサーバ型での HA-API



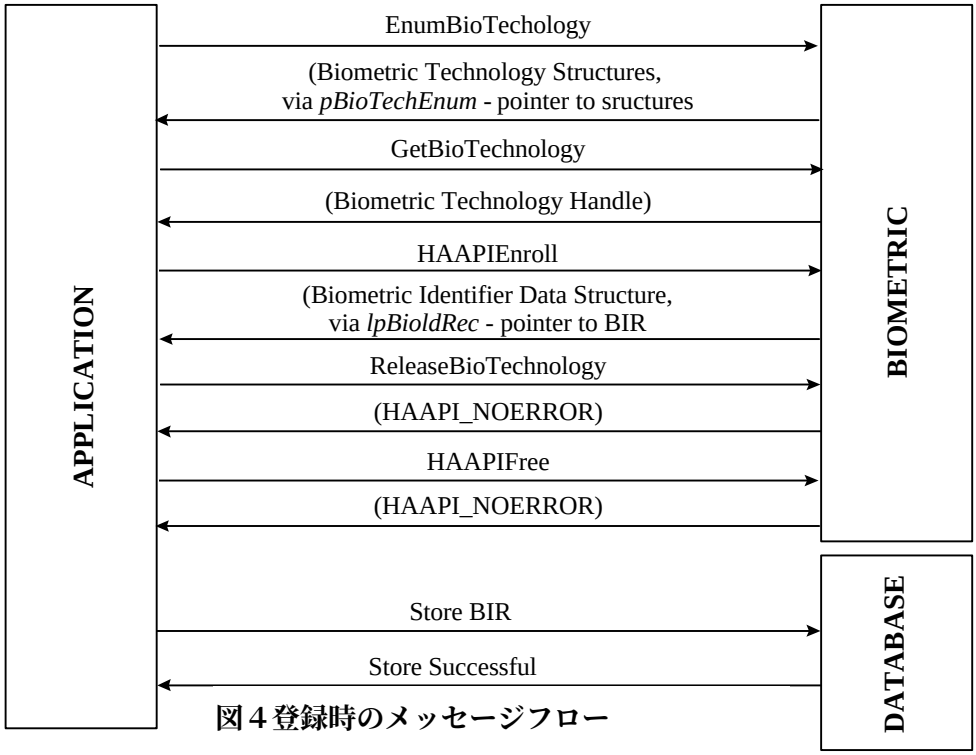


図４登録時のメッセージフロー

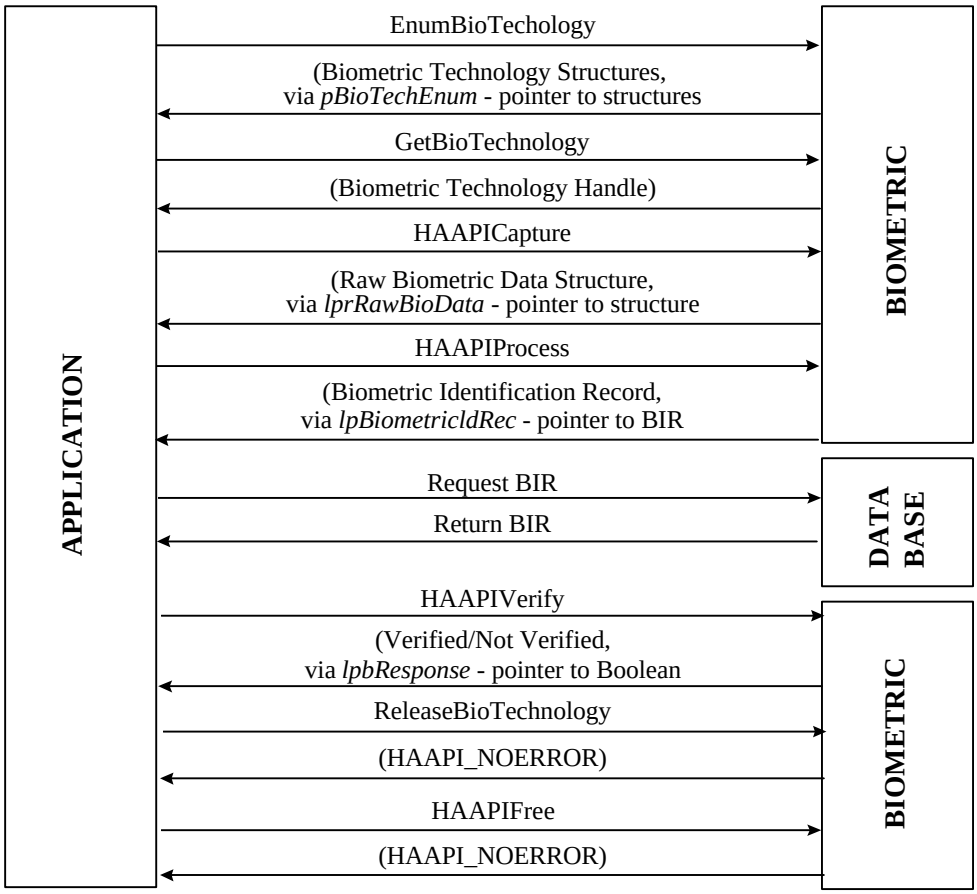


図５ 照合時のメッセージフロー

付録６ 本人認証技術検討ＷＧ名簿

主査　　菅　知之　ＥＣＯＭ 主席研究員

副主査　　東　昌弘　ＥＣＯＭ 主席研究員

副主査　　三沢　永　ＥＣＯＭ 主席研究員

委員　　横塚志行　ＮＴＴデータ通信（株）　技術開発本部マルチメディア技術センタ
マルチメディアＳＩ担当 課長代理

塚田光芳　沖電気工業（株）　システムビジネスグループ金融システム事業部
Ｅコマース企画推進部　部長

繁水秀幸　オムロン（株）
ソーシアル事業グループ 電子マネー事業開発プロジェクト

高橋　章　同上（平成9年10月迄）
ソーシャル事業グループ 電子マネー事業開発プロジェクト 部長

片岡　玲　川鉄情報システム（株）
ビジネスシステム事業部　システムデザインセンター　技術グループ

田吹隆明　（株）キャディックス
第二営業部　課長

山崎勝行　（株）さくら銀行
システム部システム企画グループ 調査役

植木康雄　(株)三和銀行
システム部 部長代理

石原洋之　(株)システムズナカシマ（平成9年３月迄）
技術部システム一課 課長

杉浦和彦　綜合警備保障（株）
技術本部技術部設備計画課

船橋　武　ソニー（株）
バイオニクス事業開発室テクニカルサポート担当 課長

中村　明　同上（平成９年６月迄）
コンピュータペリフェラル&コンポーネントカンパニー NB部一課 統括課長

	辻　　健	同上（平成９年３月迄）
		コンピュータペリフェラル&コンポーネントカンパニー NB部 部長補佐
	岡崎彰夫	（株）東芝
		マルチメディア技術研究所開発第六部 課長
	増尾剛彦	（株）土木情報サービス
		システム開発部 係長
	星野　聡	日本電気（株）
		ワークステーション・サーバ事業部 第一製品技術部
	岩田憲治	（株）ハイコム
		部長
	瀬戸洋一	（株）日立製作所 システム開発研究所
		第１部１０３研究ユニット ユニットリーダ・主任研究員
	新崎 卓	（株）富士通
		ペリフェラルシステム研究所入出力研究部
	中島雅人	同上
		ペリフェラルシステム研究所 主席部長
	吉澤正充	三菱商事（株）
		技術部 主事
	篠田誠一	三菱電機（株）
		情報システム製作所マルチメディアシステム部官公システム第一課 主幹
	佐藤裕明	ユーシーカード（株）
		マーケティング開発部 アシスタントマネージャー
	福崎康弘	(株)ワコム（平成9年3月迄）
		新事業室 係長
特別会員	大林正英	（財）日本情報処理開発協会
		セキュリティ対策室
オブザーバ	高橋基二	情報処理振興事業協会
		セキュリティセンター 暗号技術調査室　室長補佐