本人認証技術検討 WG 中間報告書

平成 9 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 中間報告書

1 はじめに（本人認証技術WG活動の概要）.....1
1.1 WG６の目標と作業スコープ.....1
1.2 本人認証の方式.....1
1.3 参照モデル.....1
1.4 評価基準.....1
1.5 まとめ.....3
2 本人認証とは.....4
2.1 本人認証の利用される場面の例.....4
2.1.1 銀行における本人認証.....4
2.1.2 クレジットカードにおける本人認証.....4
2.1.3 アクセス管理における本人認証.....4
2.1.4 入場時の本人認証.....4
2.2 本人認証の原理.....5
2.3 本人認証の方式.....6
2.3.1 バイオメトリクスⅠ.....6
2.3.2 バイオメトリクスⅡ（署名／筆跡、声紋など）.....8
2.3.3 所有物.....9
2.3.4 秘密情報Ⅰ.....9
2.3.5 秘密情報Ⅱ.....10
2.4 本人認証と認証局.....11
3 評価基準.....13
3.1 本人認証技術の評価の目的.....13
3.2 本人認証技術の評価基準.....13
3.3 プロファイル.....14
3.4 評価主体.....15
3.5 評価基準の意味.....15
3.6 まとめ.....16
付録A　参照モデル.....17
付録B　評価基準 v0.5.....24
付録C　本人認証に関する技術情報（文献リスト＆ＵＲＬ）.....55
付録D　本人認証技術検討WG名簿.....78

1 はじめに（本人認証技術WG活動の概要）

1.1 WG６の目標と作業スコープ

ＥＣユーザ（事業者、消費者）がその目的に合わせて、適切な本人認証技術を選択するのに必要な情報を作成・整理して提示する。具体的には各種の本人認証技術ないし、それを実装した製品を客観的に評価するための評価要因・評価観点を収集整理して、評価項目と尺度にまとめて、本人認証技術の市場原理に基づく健全な発展を図る。

そのためには、各技術の特性を明らかにして、ＥＣシステム構築時にその選択を容易にするための情報を整理・提示することが必要である。システム毎に勝手な特性を勝手に主張したのでは比較しようがないので、主張すべき特性を主張の形式を含めて標準化することと理解しても良い。別の表現をすると、本WGのミッションは各種本人認証技術の特性を計るメジャーを作ることと考えられる。技術の特徴には色々な側面があり、単一の scale で計ることはできず、いくつもの評価観点に対応した軸で考える必要がある。

本WGでは、本人認証を実現する個々の技術に関する具体的検討や開発は行わない。これらの作業は各開発メーカにおいて実施されるべきものであり、上述のような情報を提示することにより、市場原理の働くのを促進して本人認証技術の健全な発達に資するのが、本WGのミッションであると信じる。

1.2 本人認証の方式

本人認証には以下に示す各種実現方式があるが、WG６ではこれら全てを同列に扱ってゆく。

① バイオメトリクスⅠ（指紋、網膜、虹彩、指型、掌紋、掌形、顔貌、耳形など）
② バイオメトリクスⅡ（署名・筆跡、声紋など）
③ 所有物
④ 秘密情報Ⅰ（パスワードなど）
⑤ 秘密情報Ⅱ（デジタル署名、零知識証明など）

1.3 参照モデル

本WG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、参照モデルを作るところから始めた。ＯＳＩ等の他の領域においてもそうであったように、参照モデルはいろんなバックグラウンドを持つ委員で構成される作業形態において、議論の共通ベースを作る意味があり、作る過程そのものも意識合わせとしての効果を持つ。更に参照モデルは本人認証のフレームワークとして、今後のWGにおける作業展開上の活用のみならず、広く産業界／学界における共通認識としての利用が期待されるものである。この参照モデルについては、１月に福岡で開かれた“暗号と情報セキュリティ・シンポジウム（SCIS'97）”（電子情報通信学会）で発表した。またWWW上にも公開しており、３月には８００件を超えるアクセスがあった。

1.4 評価基準

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。

WG６の目的は、本人認証技術ないし製品の特性を明確にする各種評価要因について検討し、本人認証技術ないし製品の評価を行うための評価基準（Evaluation Criteria）を作成して、本人認証技術の市場原理に基づく健全な発展に資することである。

評価とは技術ないし製品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。

- 社会的認知性
- 脅威対抗性
- 利用者受容性
- 認証精度
- 利便性
- 実現性（その後の検討で、本要因はその他の要因を総合したものと結論された）
- 保守･更新性

評価基準とは評価のための物差しであるが、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。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。

この評価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。

以上に述べてきた評価基準は次のような意味を持つ。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

なお評価の実施主体についてはメーカが行う第一者評価、ユーザが行う第二者評価、中立機関が行う第三者評価の三つの考え方がある。コストや時間の観点からいえば、評価は本人認証技術ないし製品の開発メーカが行う方が現実的であると思うが、利用者がより信頼のおける評価結果を望むのであれば第三者評価も考えておく必要がある。この観点から、評価基準自体は評価主体とは切り離して設定すべきである。第三者評価機関のあり方や、評価・認証制度に関わる事項については、本WGの作業スコープの外と考えている。

1.5 まとめ

このような観点から、WG６では各種の評価要因を本人認証の評価基準(v0.5)としてまとめた。これはあくまで叩き台としての中間バージョンであり、９年度に予定している各種レビューから得られたコメントのフィードバックを通じて洗練してゆくべきものである。

2 本人認証とは

本人認証とは、あらかじめ本人であることを登録しておき、その証拠を示すことによって、本人であることを確認することをいう。上で言う登録という行為は、何らかの目的を持って行われるものであり、本人認証もまた何らかの（登録の目的と通常同じ）目的を持って行われるもので、漠然とした汎用的な本人認証という概念は存在しない。

何らかのサービス（これはかなり広い意味でのサービスであるが）を考える際に、そのサービスを受け得る人が限定されていて、確かにそのサービスを享受できる人であることを確認して始めてサービスを供与する仕組みにおいて必要になるものである。

2.1 本人認証の利用される場面の例

ここでは本人認証の利用される幾つかの例を具体的に挙げて本人認証の理解の一助とする。

2.1.1 銀行における本人認証

まず銀行の預金システムを考える。利用者は銀行に自分の口座開設を依頼する。この時にこれは上で言うところの登録に該当する。その時に本人認証のための証拠として後日用いるものを合わせて登録しておく。いわゆる届け出印がそうであるが、ＡＴＭ機での預け入れ／引き出しの時に用いる暗証番号も全く同じ効果を持つ。引き出しを行う際に間違いなく本人の口座から払い出すために本人の確認を行う必要があり、そのために届け出印または暗証番号が使用される。

2.1.2 クレジットカードにおける本人認証

クレジットカードを利用して買い物をする場合には、買い手は商店に対して、自分はその商店が加盟しているクレジットカードの会員であることを示す必要がある。各カード会員が所持するカードの提示がこれにあたる。（この場合、そのカードシステムへの加入手続きが事前登録にあたる。）この意味でクレジットカードで用いられる本人認証は所有物による認証であるが、カードの盗難や遺失に対応するために所有者認証を併用している。これにはカード裏面の署名が用いられる。商店主はカード伝票に署名される署名とカード裏面の署名とを比較検証することで、カードの正しい持ち主であることが確認できる。

2.1.3 アクセス管理における本人認証

コンピュータシステムへのアクセスにおいては、その利用者がアクセスしてよい情報だけにアクセスを許すようにアクセス制御を行うのが普通である。アクセス制御は誰がどのファイルへのアクセス許可を持っているかに従った制御であり、利用者が誰であるかをシステム運用側が確認するのが必須の前提になっている。この確認はログイン時に提示されたパスワードとあらかじめ利用者登録時に登録されたパスワードとの比較照合で行われている。

2.1.4 入場時の本人認証

コンピュータシステムでなく、物理的な施設への入場／入室管理も全く同じ原理で行われる。入場が可能なのは、あらかじめ施設管理者に登録した人に限定される。入場時にはその人が登録されている本人であることの確認を行っている。確認には身分証明書（入場証）の目視確認、指紋認証システム、パスワードなどが用いられている。

2.2 本人認証の原理

前述したように、本人認証とは事前に登録した本人であることを確認する行為である。そのためには、登録した本人であることを何等かの形で証明させるプロセスを経る必要がある。この証明の方法には２．３節で述べるような幾つかの方法があるが、基本的には本人だけが持つ情報又は物を提示させることによる。これを本人情報という。即ち、登録の一環として、ここでいう証明のための情報も併せて登録しておき、それと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側から発行される必要があり、確認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ことになる。

本WG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、参照モデルを作るところから始めた。ＯＳＩ等の他の領域においてもそうであったように、参照モデルはいろんなバックグラウンドを持つ委員で構成される作業形態において、議論の共通ベースを作る意味があり、作る過程そのものが意識合わせとしての効果を持ち、その成果である参照モデルは本人認証のフレームワークとして、今後の作業展開上の活用が期待されるものである。（付録A参照）

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を基本概念として定義している。

［基本概念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。

［基本概念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）。

［基本概念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事を確信する人（それによって生じる利益／不利益を被る人）。

［基本概念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。

［基本概念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。

更に以下の補助概念をも定義している。

［補助概念１］提示点：認証請求者が提示情報を提示する点をいう。

［補助概念２］認証点：認証請求者が本人であることを確信する点。

［補助概念３］検証点：登録情報と提示情報の照合を行う点。

［補助概念４］認証パス：提示点と認証点との間にあり、提示情報やその他の本人認証に必要な情報が伝送される経路を一般化した論理的な伝送路をいう。あくまで論理的なものである。

提示情報は原理的に本人（認証請求者）が保持する以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幾つかの variation 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ーに着目して、参照モデルは以下のような variation で構成されている。

すなわち、

① 基本モデル：基本原理を表わしたモデル。
② 登録情報付き所有物認証モデル：所有者認証のための登録情報を持つ所有物による所有物認証のモデル。
③ 証明書添付モデル：主としてデジタル署名の利用を意識したモデル。
④ 証明書取り寄せモデル：③の変形。
⑤ 認証サーバモデル：認証機能をサーバ化したモデル。

2.3 本人認証の方式

本人認証を行うには、本人であることを示す情報（これを本人情報と呼ぶ。）として何を用いるかによって以下に示す各種の方式に分類できる。

2.3.1 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であるが、恣意的に変化させ得ないものをこの範疇に分類した。指紋や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、顔の起伏などを用いる研究例が報告されている。顔による個人識別はアルゴリズムをふくめて、なお研究段階にあり、現時点で利用可能な製品は発表されていない。

(2) 網膜

人間の血管の中で目の奥の網膜上に現れているいるものだけが直接見ることの出来るものである。成人病検診で眼底撮影をする所以である。この網膜上の血管が形成するパターンは各人各様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を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出来、米国の Eyedentify 社から製品が発売され、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毎に異なるといわれている。網膜は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。このため網膜のような特殊な装置でなく、通常のビデオカメラやデジタルカメラのような汎用的な撮像装置の使用で良く、導入しやすい利点もある。虹彩利用の本人認証機能は沖電気で試作開発中である。

(4) 耳

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才以降は安定期に入り、その後も若干の成長が見られるが終生不変とみなし得る範囲内と考えることが出来る。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・同定実験が解剖学的および形態学的の両側面から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。こうしたことから耳の形による本人認証については、可能性はあるものの未だ feasibility も含めて研究段階であり、現段階では実用に至っていない。

(5) 指紋

いわゆる指紋が万人不同といわれることに着目した方式であり、個人を識別するバイオメトリクスの特徴としては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来ている。既に色々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。

富士通、三菱、ＮＥＣ、ＳＯＮＹ、日商岩井、日本ＬＳＩカード、浜松ホトニクス、松村エレクトロニクス、山武ハネウェル、翼システム、セコムなどから製品が発表されている。

(6) 掌紋

手のひらのしわの形状の特徴を利用するものであるが、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およばない。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。開発中を含めて幾つかの製品がでており、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。

KFKI Computer Systems Corporation、Biometrics Inc.、PIDEAC、Talos Technology Inc.が製品化ないし開発中と伝えられている。

(7) 掌形

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。これも掌紋と同じく、指紋ほどの個人識別能力があるとは考えられていないが、方式が簡単な点でやはり入退室管理などの限定された局面での利用が考えられる。内外の数社で製品化しており、アトランタオリンピックで入退室管理に使われた実績がある。

Recognition System、BioMet partners、Bio-metric Security Sys、三菱電機から製品が発表されている。

(8) 指形

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もので

ある。同じアイデアは平安時代に画指（かくし）と呼ばれ、字の書けない人の署名代わりに利用できることが令に定められていた。これも掌紋、掌形と同様に、指紋のような個人識別能力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ろう。現在東芝がこの技術を入退室管理システムとして組み込んで製品化しているだけである。

(9) 手の甲の血管模様

手の甲に浮き出した血管の模様に着眼するものであるが、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。

British Technology Group、Edith Cowan University、Veincheck Systems の各社が製品開発中と伝えられる。

2.3.2 バイオメトリクスII（署名／筆跡、声紋など）

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出来る特徴で、それを利用して他人に成りすます可能性を秘めているものを特に区別した。署名（筆跡）や声紋などがこれに該当する。

(1) 声紋

発声という行為は随意的な要素があるため、必ずしも再現性があるとは言えず、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。音声信号は音圧の時系列データであるが、これを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が声紋グラフである。声紋の照合は登録したのと同じ言葉の声紋データを採取し、両者のマッチングを行うものである。前述したように完全な再現性はないので、このマッチングは単純な重ねあわせではなく、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ものである。

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再現性が高いといわれている。この理由で本人の名前などを言わせる実現例がある。

声紋認識の実用例としては米国のスプリント社の公衆電話用クレジットカードシステム“Voice Phone Card”がある。これはＴＩ社の技術を用いて実現されたものでユーザはガイドメッセージに従って１０桁の社会保障番号を発声するやり方を採っている。日本では最近富士通からテレホンバンキングという名前で発表された。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研究の余地があると考えられる。

(2) 署名

署名を用いる本人認証技術は筆者認識技術の内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。こ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。

実用製品の例としてCADIX社のCybersignを挙げておく。

(3) バイオメトリクスIIの特質

バイオメトリクスIは本人に意志で変える事ができない特徴であるのに対して、バイオメトリクスIIは恣意的に変える事ができる。これは指紋等は他人に似せることはできないが、筆跡、声は他人の特徴を真似る事ができる事を意味する。

従って、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。

2.3.3 所有物

所有物認証はコンピュータ以前から本人認証の手段として広く利用されてきた技術である。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、純粋な所有物認証では、盗難や遺失によって他人が成りすますリスクを内在しており、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登録情報である。またクレジットカードでは署名（Signature）を用いた所有者認証が使われている。銀行のキャッシュカードも所有物認証に分類されるが、所有者認証には暗証番号が用いられている。

またコンピュータの世界では、パスワードや暗号鍵などを格納するために磁気カードやＩＣカードを利用するケースが良くあり、操作上からは所有者認証を伴わない純粋の所有物認証に該当するが、人の頭に記憶しきれない情報を格納するための補助記憶として上記のカードを使っているに過ぎず、本人認証技術の分類の観点からは秘密情報による本人認証に分類すべきものである。

更に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意味を持たない。即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なり立たないのは明らかである。従ってネットワークを介した所有物認証は所有者認証を併用し、所有者認証をネットワークを介して行うことで、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えない。従って、この場合は所有者認証を行う方式によって分類されることになる。

このように考えてくると、今後ＥＣの世界で利用される本人認証技術には所有物認証に分類されるものはなく、系統的に認証技術を調査するにはそれ以外の分類の技術（即ち、バイオメトリクス、秘密情報を利用する技術）を調べれば充分であると考えられなくはないが、製品としての見えかたが異なる可能性もあり、重複よりも欠落を恐れて、所有物認証という分類でも技術調査を行うことにした。上述したように利用されている個別の技術は他の分類と重複していることが多い。

2.3.4 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来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言ってよく、それ自体には今更調べるほどのものはない。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＋replay の手法で簡単に成りすましが可能になることから、ネットワーク上を裸のパスワードを流さない方法が研究開発され、実用化された。

これらのなかで最初に考案されたのは、ワンタイムパスワード（One Time Password）と呼ばれる方式で、更に以下の方式がある。いずれも実用化されて製品が市販されている。

(1) チャレンジレスポンス方式

認証側からチャレンジと呼ぶ乱数列を提示し、認証請求者はこの乱数列に一定の操作・変換を加えたもの（これをレスポンスと呼ぶ）を生成して送り返す。上記の一定の操作・変換は利用者毎に異なり、認証者側に登録されている。すなわちこの操作・変換手順が登録情報に他ならない。

提示される乱数列は毎回異なるので、ネットワーク上を監視してこれらを盗聴しても replay には利用できない。この操作・変換手順は複雑で記憶するには情報量が大きすぎ、毎回手動操作するには運用性が悪くなる問題があるので、電卓用のハンドヘルドデバイスにチャレンジをレスポンスに変換する機能を内蔵させる実現方法を採る事が多い。

この方式自体は新しいものではなく、日本では昭和３０年代に試作されたＥＴＳＳで既に採用されている。

この操作･変換手順として、暗号化機能を用いることもできる。この場合、登録情報は（アルゴリズムと）暗号鍵となる。

(2) 同期方式

チャレンジレスポンス方式と似たハンドヘルドデバイスを利用するが、チャレンジはなく、認証者側の内部クロックとハンドヘルドデバイスのクロックを同期させておき、時刻の関数として双方で生成された時限パスワードを利用するものである。つまり利用者はその時点でハンドヘルドデバイスに表示されるものをパスワード（提示情報）として入力し、認証者側ではその時の時刻と利用者のＩＤを元にしてパスワード（登録情報）を生成して照合確認する方式である。

2.3.5 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、１対１ないし１対ｎの関係では安全であるが、ＥＣのようなｎ対ｎの関係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。

本質的には上の秘密情報Ｉと同じであるが、例えばデジタル署名を用いる方式では、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って、登録してある公開鍵を入手しても、提示する情報を作成できないので、ここでは区別して別のカテゴリーに分類しておく。零知識証明を用いるものもこれに属する。

このほかにクライアント／サーバシステムにおいてサーバ毎にパスワードを持つ煩雑

さと裸のパスワードがネットワーク上を流れる危険性とを解決する目的で米国ＭＩＴで開発されたＫｅｒｂｅｒｏｓがある。個別の機能サーバとは別に認証サーバを設けて、クライアントはこの認証サーバから目的とする機能サーバへの電子的身許保証状（ticket と呼ぶ）をもらい、目的サーバにこれを提示する考え方をベースとしている。第三者認証方式とも分類される。

この ticket は共通鍵暗号による所有者認証を併用した一種の所有物認証とも考えることが出来る。なお ticket には有効期限が設定される。これはＵＮＩＸをベースとしたクライアント／サーバシステムで実用化されているが、ＥＣ環境では主流にはなっていない。

2.4 本人認証と認証局

本人認証を行うのが認証局であると誤解されているケースに時々遭遇するので、ここで両者の関係について触れておきたい。本人認証の「認証」は英語では“Authentication”であり、真正性を確認することである。従って本人認証とは人の真正性を確認することである。一方、認証局の「認証」は“Certification”であり、認証書（Certificate）を発行することである。（ちなみに認証局は“Certification Authority”であって、認証書を発行する主体のことである。）それでは全く無縁のものかというとそうではなく、以下に述べるような深い関連がある。

ＰＫＩ（Public Key Infrastructure）における認証局はＸ．５０９に準拠する認証書を発行する主体として位置づけられている。この認証書は公開鍵の持ち主を証明するものであって、印鑑証明と類似の機能を果たすものである。デジタル署名を用いる本人認証においては、登録情報は本人の公開鍵であり、提示情報は本人の秘密鍵による署名である。認証者（検証者）は署名を検証することで本人であることを確認するが、公開鍵が正しく本人のものであることが保証されていないと正しい本人認証は行えない。したがってデジタル署名を用いる本人認証では、本人認証の確かさは公開鍵の持ち主を証明する認証書に拠っていると言ってよく、更にはそれを発行する認証局に拠っていると言ってよい。この意味において認証局は本人認証上に重要な位置づけを占めている訳で、認証局が本人認証を行っているという表現もあながち間違いとは言えない。

認証局は本人認証の前提条件である登録を行うところが認証者と異なる場合に出てくるものである。認証局とは本人認証における登録を行う主体に他ならない。（登録主体と認証者とが同じ場合には必要がない。）異なる存在である認証者に正当な（登録してある）本人であることを伝える手段が認証書であり、世の中で広く使われてきた身分証明書を電子化したものと考える事ができる。

このように認証局は登録主体である以上、そこで発行される認証書の真正性は登録時における本人確認手続きの厳密さに依存する。そのために別の方式による本人認証を行うことになり、そこで用いる本人情報の確かさによって発行される認証書の確かさが決まる。逆に言えば、認証書を用いる本人認証の用途（目的）によって、本人登録時の本人確認手続きに要求される厳密さが決まってくる。

蛇足になるが、認証局はＴＴＰ（Trusted Third Party）のひとつであるといわれるので、認証局は第三者でなければならないという誤解が散見される。ここでいうＴＴＰとは当事者（本人認証の場合、認証請求者と認証者）以外の第三者という意味であって、世間

一般で言われる第三者とは若干異なることに注意が必要である。認証局は登録主体であるので、純粋な第三者では有り得ないことを認識しておかなければならない。身分証明書を発行できるのはその人が所属する団体・組織以外には有り得ないし、クレジットカード会員であることの証明書を発行できるのはカード発行会社以外では有り得ないことを考えると、これが自明であることが分かるであろう。蛇足ついでに言えば、上記の登録主体以外が認証局となって単独に発行できる認証書が使える用途はあまり深い信頼性を要求されないものに限定される。

本WGではデジタル署名以外の本人情報を用いる方式も含めて総合的に扱うため、ＰＫＩにおける認証局と区別して、広義の認証局という表現を用いている。また公開鍵だけでなく本人情報一般の真正性を保証するものとして、認証書ではなく証明書という表現を用いている。

3 評価基準

ここでは、本人認証技術の評価に関わる項目、即ち評価の目的、評価に用いる評価基準、評価基準の意味、評価の実施形態などについて概説する。

3.1 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）
- バイオメトリクスⅡ（署名／筆跡、声紋など）
- 所有物
- 秘密情報Ⅰ（パスワードなど）
- 秘密情報Ⅱ（デジタル署名）

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

- 基本モデル
- 所有者認証モデル
- 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･把握することを本稿では本人認証技術の評価（Evaluation）という。

本研究の目的は、本人認証技術ないし製品の特性を明確にする各種評価要因について検討し、本人認証技術ないし製品の評価を行うための評価基準（Evaluation Criteria）を作成して、本人認証技術の市場原理に基づく健全な発展に資することである。

3.2 本人認証技術の評価基準

評価とは技術ないし製品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。

- 社会的認知性
- 脅威対抗性
- 利用者受容性
- 認証精度
- 利便性
- 実現性（その後の検討で、本要因はその他の要因を総合したものと結論された）
- 保守･更新性

評価基準とは評価のための物差しであるが、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。

このように考えると、評価基準とは各評価要因毎に本人認証技術ないし製品に対する要求条件、ないしはその本人認証技術ないし製品の要求条件の満足度の形で記述したものと考えることができる。この評価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。非常に端的な喩えをすれば、評価基準とは本人認証技術ないし製品の特性表の記述項目と記述内容を標準化したものと考えても良い。これによって、幾つもの本人認証技術ないし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本人認証技術ないし製品を選択することが可能になる。

3.3 プロファイル

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尺度（必ずしも定量的尺度とは限らない）の集合である。

ある使用目的に適合する本人認証技術ないし製品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。幾つかの候補技術ないし製品について、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技術ないし製品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えば良い。

3.4 評価主体

なお評価の実施主体についてはメーカが行う第一者評価、ユーザが行う第二者評価、中立機関が行う第三者評価の三つの考え方がある。評価にかかる費用・期間の観点では第一者評価が最も効率的であり、評価結果の信頼度の観点では第三者評価が最も安心である。第二者評価を自身で行うだけの技術がないユーザは第三者に委託することになる。

先行するコンピュータセキュリティ評価の例では、欧米では第三者評価に関する仕組みが整備されていて、政府調達などで利用されているが、第三者評価に要する期間は年オーダーであり、費用は億円オーダーだと言われている。この観点でいえば、評価は本人認証技術ないし製品の開発メーカが行う方が現実的であると思うが、利用者がより信頼のおける評価結果を望むのであれば第三者評価も考えておく必要がある。換言すれば、評価基準自体は評価主体とは切り離して設定すべきである。

コンピュータセキュリティ評価においては、評価結果の認証の考え方がある。これについては、評価機関自体を認定する考え方と組み合わせて、認定された機関の評価結果に基づいて認証する考え方が欧州では一般的である。即ち、欧州ではコマーシャルベースの民間企業が国から認定を受けることで評価機関としてのビジネスを行うことが出来る。一方米国では、評価の実施、評価結果の認証共に国家機関であるＮＣＳＣ（National Computer Security Center）が行い、民間の評価機関は存在しない。これは評価結果の利用が政府調達条件になっていることとも関係があると思われる。

第三者評価機関のあり方や、評価・認証制度に関わる事項については、本WGの作業スコープの外と考えている。

3.5 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

3.6 まとめ

このような観点から、本WGでは各種の評価要因を本人認証の評価基準(v0.5)としてまとめた。これはあくまで叩き台としての中間バージョンであり、来年度に予定している各種レビューから得られたコメントのフィードバックを通じて洗練してゆくべきものである（付録B参照）。

付録A　参照モデル

１　はじめに

本人認証に関する議論を行う上で、異なった業界の人間が円滑な議論を行うためには、用語や概念に対する解釈を合わせておく必要がある。そこで検討に先立ち、本人認証に関する参照モデルを定義することにした。

本人認証とは、事前の登録行為を前提にした本人確認行為であり、単なる個体識別ではない。換言すれば、事前に登録した本人であることを同定する行為である。ここでいう登録行為の意味は、その用いられる局面によって様々で、運転免許やデータアクセス権のような資格の保有状況、クレジットカードのような会員加入、更には出生届や住民登録のような社会の一員としての登録までも考え得る。本人認証は登録してある本人であると主張する人が、本当に登録している本人であることを確認する行為である（通常、登録が意味するところの権限の行使に際して行われる）。

登録してある本人であると主張する人は、その証拠を示して相手に納得させなければならない。これが本人認証の基本原理である。証拠の示し方として以下の方法が使われてきた。

①生物学的特徴によるもの（バイオメトリクス）

顔写真等各人の生物学的特徴を予め登録しておき、それとの比較照合によるもの。指紋、網膜、虹彩、声紋等が該当する。

②サイン・署名

欧米では古くからある。日本でも花押（書き判）が昔使われた。

③所有物を示すことによるもの

証明書のような登録時に発行される物を提示するのが一般的である。日本で古来使われてきた印鑑も間接的にこの範疇に入る。

④あらかじめ登録しておいた秘密情報を提示するもの

古来利用されてきた合言葉。銀行端末利用時の暗証番号やコンピュータのログイン時のパスワードが該当。最近脚光を浴びているデジタル署名を使う方法もこのvariationの一つであり、各人の持つ秘密鍵（Private Key）が秘密情報であるが、この場合には登録されるのは秘密鍵そのものではなく対応する公開鍵（Public Key）である。

２　基本モデル

前述の本人認証方式の内で一番自然で原理的な方式は、登録してあるものと同じ物または等価な情報を提示させるものである。そこで、この方式を参照モデルのタイプA：基本モデルとして、モデル化する。このモデルには５つの基本概念と４つの補助概念が定義されている。

［基本概念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。

［基本概念２］検証者：認証請求者の主張をその裏付けによって確認して納得する人（またはシステム）。

［基本概念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事を確信する人（それによって生じる利益／不利益を被る人）。

［基本概念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。
［基本概念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）。
［補助概念１］提示点：認証請求者が提示情報を提示する点をいう。
［補助概念２］認証点：認証請求者が本人であることを確信する点。
［補助概念３］検証点：登録情報と提示情報の照合を行う点。
［補助概念４］認証パス：提示点と認証点との間にあり、提示情報やその他の本人認証に必要な情報が伝送される経路を一般化した論理的な伝送路をいう。あくまで論理的なものである。

３　登録情報付き所有物認証モデル

従来から使われてきたものでは、身分証明書、会員証、クレジットカード等が該当する。その所有物の提示により真正な本人であることの裏付けとするのが、所有物による認証の基本原理であるが、多くの所有物認証では提示する人がその所有物の正当な所有者であることの本人認証（所有者認証）を併用している。身分証明書や会員証の顔写真、クレジットカードの署名等がそのための情報である。

このような所有者認証のための登録情報を所有物中に持つ所有物認証を、タイプＢ：登録情報付き所有物認証モデルとする。このモデルでは登録情報の保持される場所が基本モデルとは異なる。即ち、登録情報は所有物発行体によって所有物自体に書き込まれ、さらに改竄を防ぐための対策が発行体によってなされている必要がある。従来の証明書類の顔写真ではエンボスないし割印がこれにあたり、電子情報の世界ではデジタル署名技術による。

［特記事項］このモデルは所有物による本人認証全てをカバーするものではない。ここでは認証のための登録情報を所有物中に保持する方式だけをモデル化している。　該当しない例として、銀行のキャッシュカードがある。この場合カード所有者認証は、暗証番号を入力することで行っている。利用者が入力する暗証番号はそのための提示情報であり、比較照合される登録情報は銀行システム中に保持されているため、この場合のカード所有者認証方式はむしろモデルＡ：基本モデルに該当する。

４　証明書添付モデル

タイプBの変形として、タイプＢ’：証明書添付モデルを定義しておく。これはネットワークを隔てての非対面状況での本人認証を意識したもので、登録情報の保持場所としてカード等の携帯する所有物ではなく、認証請求者のコンピュータのファイルを考える。（ここで考えるファイルはＰＣの固定ディスクのような内蔵媒体だけでなく、フロッピーディスクやＩＣカードのような可搬媒体をも含めてよい。）ここにおかれる登録情報は、登録をつかさどる組織によって生成され、内容の完全性（integrity）を保証されたものでなくてはならない。この情報は電子的な証明書と考えることができ、この証明書を発行する組織は広義の認証局（Certification Authority）に他ならない。

広義というのは、一般的には公開鍵とその持ち主の名前とを登録情報とする証明書(X.509 準拠)を発行するものが認証局と呼ばれているのに対し、ここではデジタル署名用

の公開鍵 (public key)以外の登録情報を用いる所有者認証（たとえば指紋等のバイオメトリクス）をも考えているので、敢えて広義の認証局と呼んでいる。

電子的証明書の所有者認証にデジタル署名を用いている場合にはこれは（いわゆる狭義の）認証局である。クレジットカード決済をネットワーク上で安全に行うためのＳＥＴプロトコルで使われている方式はまさにこのタイプＢ’モデルにあたる。

５ （検証者による）証明書取寄せモデル

タイプBのもう一つの変形として、タイプＢ”：（検証者による）証明書取寄せモデルを定義する。タイプＢ’においては認証請求者から提示情報に添えて証明書が送られるのに対し、ここでは、検証者の側において証明書の取得を行う。これは、登録情報を含む証明書を認証請求者側に置いて認証パス上を流すと盗聴と replay とによるなりすましの危険性が予測される場合の対応として考えられるものである。ＳＥＴで使われているデジタル署名を用いる方式では登録情報は公開鍵であり、提示情報は秘密鍵によるデジタル署名文なので上記の危険性はないが、登録情報と提示情報とが同種の情報であって比較的単純な照合による方式ではこのような配慮が必要である。

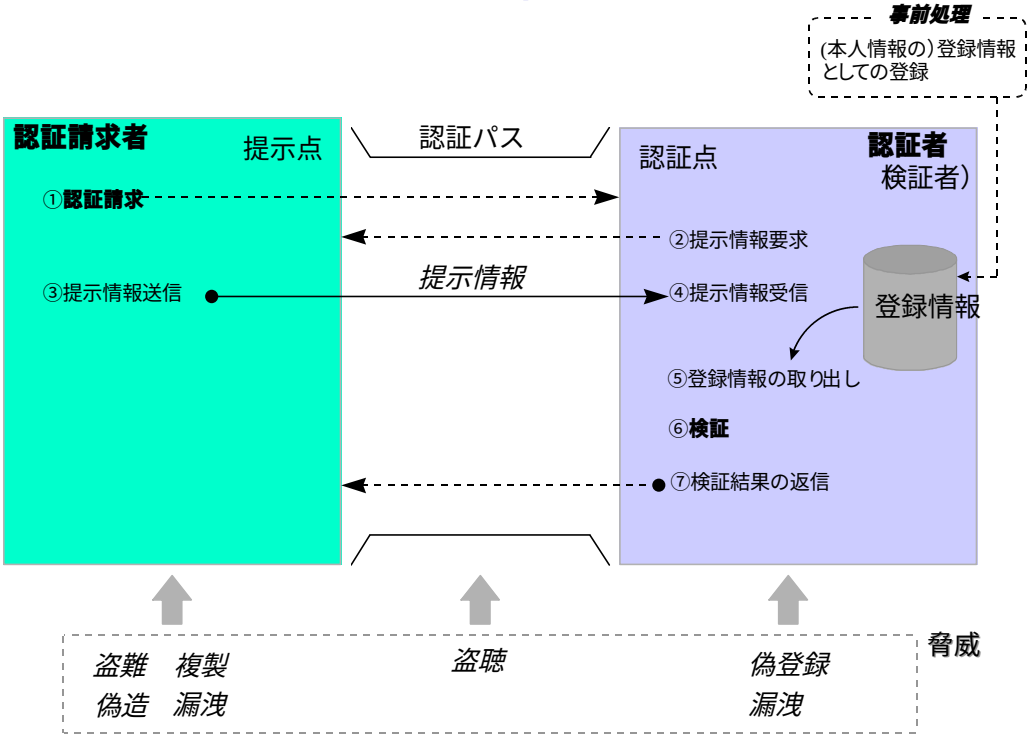
（注）電子的証明書を考える場合、証明書の有効性をチェックするプロセスが必要である。これは認証局が保持する Revocation List を参照することで行うが、上の説明では煩雑さを避けるためにこれを省略した。このためタイプＢ”はタイプＢ’に比べて検証時の認証局へのアクセスが余分に必要なように見えるが、いずれのタイプでも検証時には Revocation List 参照のための認証局へのアクセスが必要なので、タイプＢ’とタイプＢ”とは認証局へのアクセスに関して同じ条件である。

６ 認証サーバモデル

これはタイプＡ：基本モデルの発展形と考えてよい。タイプAにおいて登録情報を認証者（検証者）が保持することからくる運用上の窮屈さを解決するために、登録情報を認証者とは別に設けた認証サーバに持たせ、認証者はそこに認証請求者からの提示情報を送り、検証結果のみを取出す。認証サーバへのなりすましを防ぐために、認証サーバは検証結果にデジタル署名を施して認証者に送る方が良い。

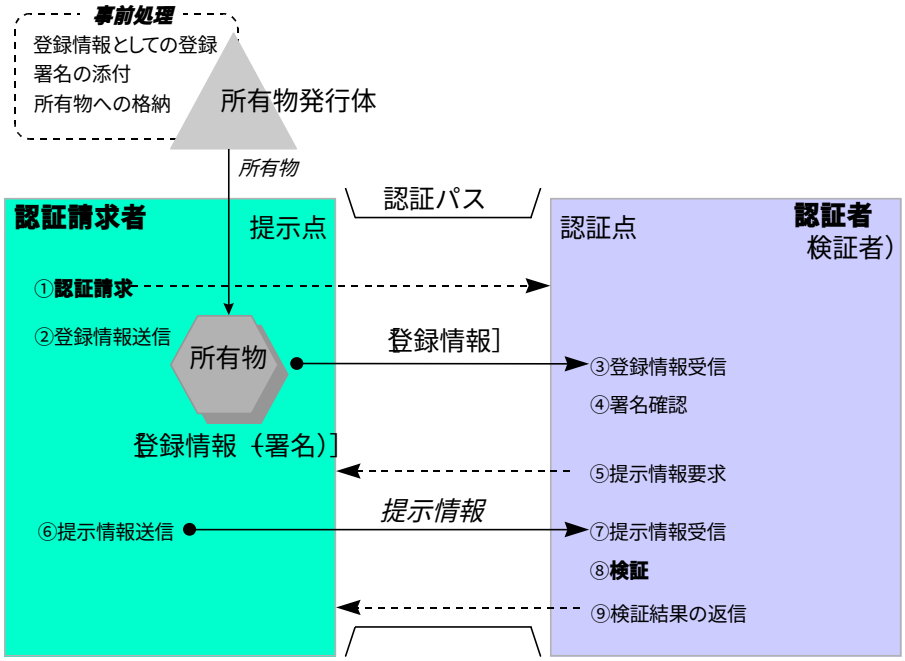
本人認証の参照モデル

タイプA：基本モデル



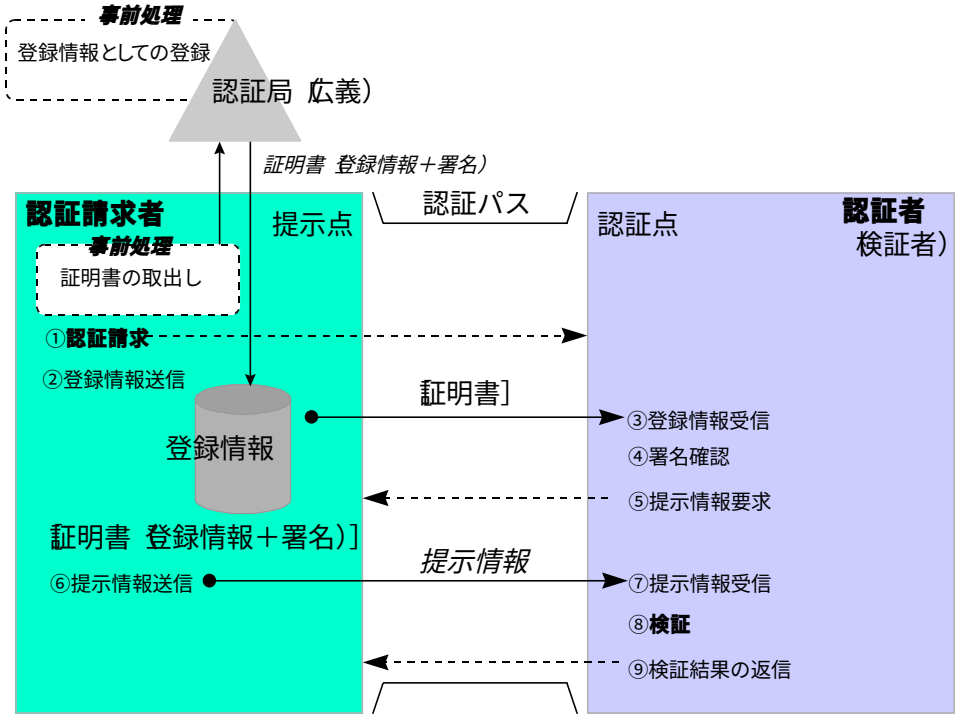
本人認証の参照モデル

タイプB：登録情報付き所有物認証モデル



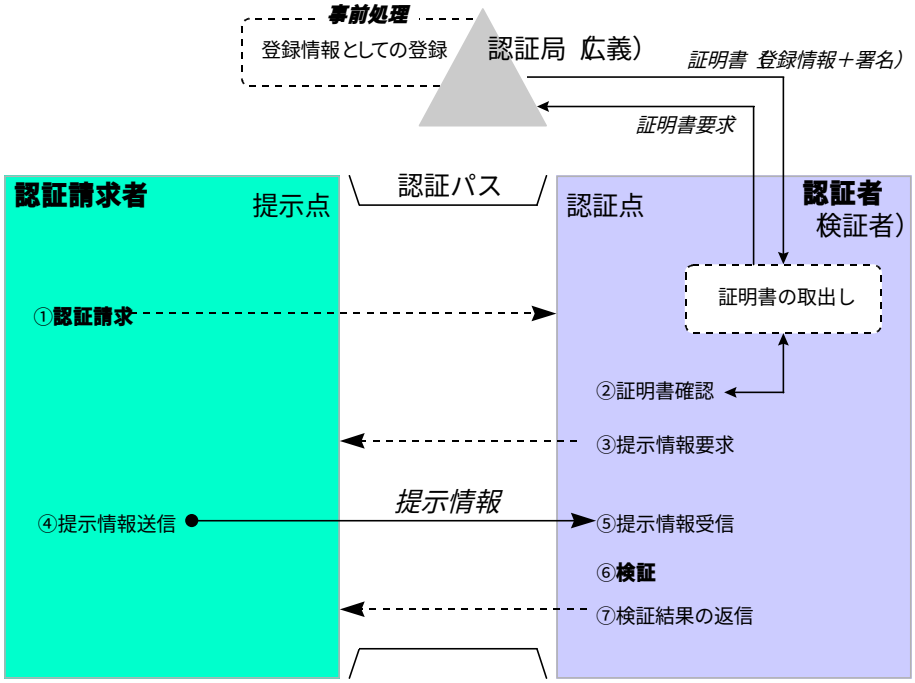
本人認証の参照モデル

タイプB’：証明書添付モデル



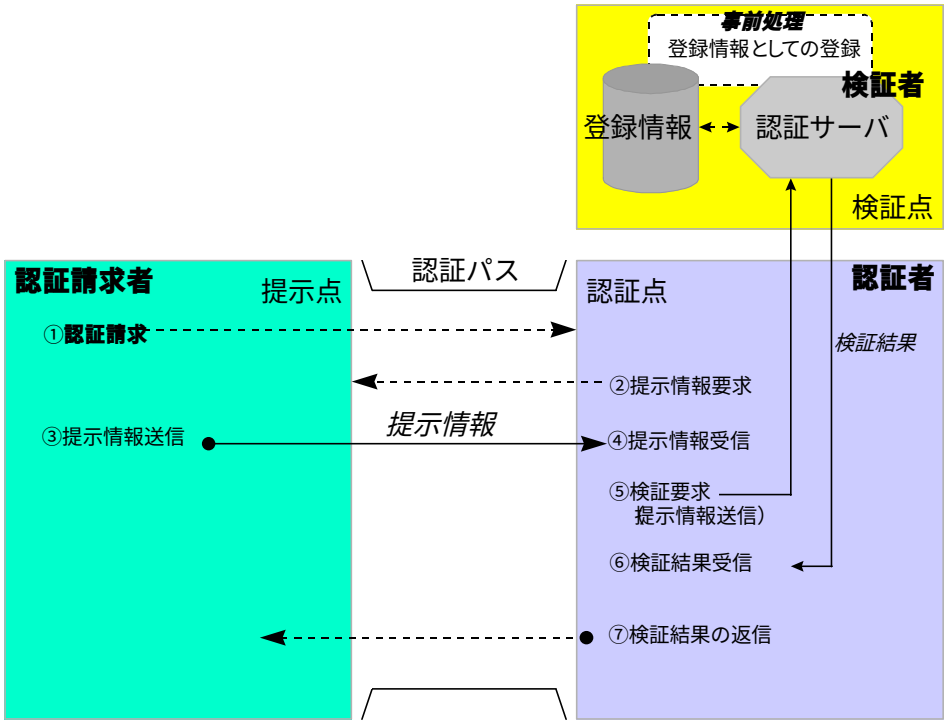
本人認証の参照モデル

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Ｂ　評価基準v0.5

本人認証の評価基準

目次

１　はじめに
　１．１　背景
　１．２　想定する読者
　　１．２．１　システム構築者
　　１．２．２　開発者
　　１．２．３　評価者
　１．３　本人認証の評価と評価基準
２　評価要因毎の要件
　２．１　社会的認知性
　２．２　利用者受容性
　２．３　脅威対抗性
　２．４　認証精度
　２．５　利便性
　２．６　保守･更新性
付録Ⅰ　本人認証の参照モデル(規定)
付録Ⅱ　認証精度の測定方法(規定)
付録Ⅲ　脅威対抗性の評価（参考）

Version 0.5　1997年３月

電子商取引実証推進協議会（ＥＣＯＭ）

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　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。

１．２．１　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。

１．２．２　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。

１．２．３　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。

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利用者に心理的・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。

２　評価要因毎の要件

この評価基準の構成を以下に示す。

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）

(1)高齢者・身障者への配慮（ＳＡ１１）

ＳＡ１１－１：高齢者、身障者には利用出来ない場合がある。

ＳＡ１１－２：高齢者、身障者等にも間違いなくかつ簡単に使えなければならない。

(2)共用品（Universal Design）について（ＳＡ１２）

（以下略）

２．２　利用者受容性（ＵＡ：End User Acceptability）

２．３　脅威対抗性（ＴＣ：Threat Countering）

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

２．５　利便性（ＥＵ：Ease of Use）

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

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　で上記の評価要因を示す。

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しめし、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利用目的に照らして適切なレベルを一つ選ぶ。

なお、本評価基準の付録Ⅰ～Ⅲの内で、ⅠとⅡとは規定であり、評価基準の一部であるが、Ⅲは参考である。

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）

(1)高齢者・身障者への配慮（ＳＡ１１）

ＳＡ１１－１：誰にでも使えることが望ましいが、高齢者、身障者等の一部に使えない又は使い難い場合があってもやむを得ない。

ＳＡ１１－２：高齢者、身障者等にも間違いなくかつ簡単に使えなければならない。

(2)共用品（Universal Design）について（ＳＡ１２）

ＳＡ１２－１：共用品としての配慮は特に不要である。

ＳＡ１２－２：共用品としての工夫をしていなければならない。

２．１．２ 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）

ＳＡ２１－１：個人情報（本人情報及び付帯情報）の管理に関しては特別な体制をとる必要はない。

ＳＡ２１－２：個人情報（本人情報及び付帯情報）の管理に関しては規定を設け十分な運用管理が行われていなければならない。

ＳＡ２１－３：個人情報（本人情報及び付帯情報）の管理に関しては規定を設け十分な運用管理に加えて、技術的な保護対策が施されていなければならない。

(2)個人情報の閲覧・修正（ＳＡ２２）

ＳＡ２２－１：本人に対しても個人情報の閲覧を許す必要はない。

ＳＡ２２－２：本人に対しては個人情報の閲覧を許すことができなければならない。

ＳＡ２２－３：本人に対しては個人情報の閲覧を許し、誤りがあった場合には本人からの申告で修正することができなければならない。

(3)個人情報が他の用途に使用されない保証（ＳＡ２３）

ＳＡ２３－１：公権力の要請等であれば、個人情報が本人認証以外の目的の為に開示されることもやむを得ない。

ＳＡ２３－２：公権力の要請等がある場合、本人の同意がある場合に限り、個人情報を本人認証以外の目的の為に開示する事ができる。

ＳＡ２３－３：公権力の要請等であっても、個人情報は本人認証以外の目的の為に開示されてはならない

(4)個人情報の削除（ＳＡ２４）

ＳＡ２４－１：本人がこの本人認証システムの利用を止めた後も、登録された個人情報に対して特別な考慮を払う必要はない。

ＳＡ２４－２：本人がこの本人認証システムの利用を止めた場合、登録された個人情報は速やかに削除されなければならない。

(5)本人情報の装置上への残留（ＳＡ２５）

ＳＡ２５－１：利用した本人情報が本人認証装置上に残留してもやむを得ない。

ＳＡ２５－２：利用した本人情報は本人認証装置上に残留してはならない、または残留している本人情報が容易に採取できてはならない。

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ある必要はない。

ＳＡ３１－２：法律ないし制度で定められている方式でなければならない。

(2)認証局（ＳＡ３２）

ＳＡ３２－１：利用する認証局は特にガイドラインにそった運用管理を行う必要はない。

ＳＡ３２－２：利用する認証局はガイドラインにそった運用管理が行われていなければならない。

(注)ここでいう認証局とは、ＰＫＩ（Public Key Infrastructure）における認証局だけでなく、参照モデルでいう広義の認証局を指す。

(3)トラブル保険（ＳＡ３３）

ＳＡ３３－１：事故／トラブルをカバーする(目的とする)保険は特に必要ない。

ＳＡ３３－２：事故／トラブルは保険でカバーされていなければならない。（事故／トラブルを目的とする保険がなければならない。）

(4)保険引き受け条件（ＳＡ３４）

ＳＡ３４－１：保険料算定条件として考慮される方式である必要はない。

ＳＡ３４－２：保険料算定条件として考慮される方式でなければならない。

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)認証方式及び、機器自体について（ＳＡ５１）

ＳＡ５１－１：許認可が必要であってもよい。

ＳＡ５１－２：方式及び機器の使用に関して、特別な許認可は不要でなければならない。

(2)サービス提供者について（ＳＡ５２）

ＳＡ５２－１：サービスの提供者が許認可・免許を受ける必要があってもよい。

ＳＡ５２－２：サービスの提供者が許認可・免許を受ける必要のないものでなければならない。

２．１．６　その他（ＳＡ６）

(1)宗教、因習、慣習によるタブー（ＳＡ６１）

ＳＡ６１－１：利用できない国や地域、集団があってもやむを得ない。

ＳＡ６１－２：宗教、因習、慣習によるタブーによって利用できない国や地域、集団があってはならない。

２．２　利用者受容性（UA：End User Acceptability）

２．２．１　心理的な抵抗感（UA１）

(1)誰でもが使用することができる（UA１１）

UA１１－１：本人情報として用いる情報は何でもよい。

UA１１－２：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。

(2)本人排除された時の救済手段（UA１２）

UA１２－１：本人排除時の対応策を特に考えなくてよい。

UA１２－２：本人排除時の対応策が準備してなければならない。

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）

(2)清潔感（UA２２）

UA２２－１：登録・提示における本人情報の採取時に、多少不潔と感じる人がいてもやむをえない。

UA２２－２：登録・提示における本人情報の採取において、通常の衛生観念上、不潔と感じる手段を用いてはならない。

(3)恐怖感（UA２３）

UA２３－１：登録・提示における本人情報の採取時に、体にショック・苦痛を感じてもやむを得ない。

UA２３－２：登録・提示における本人情報の採取は侵入的な（intrusive）な手段に拠ってはならない。

２．３　脅威対抗性（ＴＣ：Threat Countering）

脅威には、故意・悪意によるもの以外に、地震・水害用の災害によるもの、運用上の操作ミスによるもの、機器の障害によるものがあるが、本節では主として故意・悪意によるものについて記述してある。また本人認証機能に対する故意・悪意による脅威は本人認証機能を欺瞞して他人に成りすますことを目的とするもの以外に、本人認証およびそれを含む業務を妨害することを目的とするものがある。

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の所有者認証を行わなければならない。

(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：認証用所有物には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。

(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･

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。

(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事があってはならない。

(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

（ソフトウェア）の認証ができなければならない

(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特に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。

(5)設置環境と設置場所（ＴＣ２５）

ＴＣ２５－１：装置の設置に関して特別な条件はない。

ＴＣ２５－２：装置の設置に際しては、不正利用や妨害工作に対する牽制効果を持つ場所を選定しなければならない。

(6)違法性の表示（ＴＣ２６）

ＴＣ２６－１：不正利用や不正アクセス、妨害工作の違法性の表示について特別な配慮は不要である。

ＴＣ２６－２：不正利用や不正アクセス、妨害工作の違法性が提示点に表示されていなければならない。

(7)攻撃・調査のチャンスの限定（ＴＣ２７）

ＴＣ２７－１：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。

ＴＣ２７－２：攻撃・調査のチャンスを限定できるように物理的な対策も含むユーザインターフェイス上の工夫がなされていなければならない。

(8)プレゼンテーション・装置デザイン（ＴＣ２８）

ＴＣ２８－１：ＧＵＩ、装置のデザインなどに特別な条件はない。

ＴＣ２８－２：ＧＵＩ、装置のデザインなどに攻略困難のイメージがなければならない。

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。

(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：タイムスタンプ、シーケンス番号、乱数、チャレンジ／レスポンス方式等を用いて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。または、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もよい。（非反復性とは同一人の提示情報であっても毎回見かけが異なることをいう。）

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け付けてはならない。

(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へ物理的にアクセスできてはならない

(b)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てはならない。

(c)バックアップ媒体は運用管理規定に沿って管理されなければならない。

(d)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行えるようにしなければならない。

２．３．５　トレーサビリティ（ＴＣ５）

(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)筐体が開かれたことを検出できる仕組みを組み込んでおかねばならない。

(b)提示点に監視カメラの設置または監視人の配置を行わなければならない。

(c)不正アクセス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)攻略メリットの限界・ユーザインターフェイス（ＴＣ６１）

ＴＣ６１－１：ユーザインターフェイスやシステムデザインに、不正利用の限界特に考慮する必要はない。

ＴＣ６１－２：ユーザインターフェイスやシステムデザイン上、不正利用の限界が考慮されていなければならない。

(2)事前教育・宣伝・啓蒙（ＴＣ６２）

ＴＣ６２－１：不正利用防止についての事前啓蒙策について特別な配慮は不要である。

ＴＣ６２－２：ユーザが利用する時点で不正利用防止について認識しているように、啓蒙策を講じなければならない。

(3)不正アクセスに関する情報入手の可能性。（ＴＣ６３）

ＴＣ６３－１：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。

ＴＣ６３－２：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。。

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

認証精度の測定に関する考え方は付録Ⅱを参照されたい。

本節の要件の内で他人受入率に関するものはバイオメトリクスⅠ（指紋、虹彩等の恣意的に変化させ得ないバイオメトリクス）を利用する方式に対するものである。[1]

２．４．１　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）

ＡＡ１１－１：サンプル者数に関する要件はない。

ＡＡ１１－２：サンプル者は１００人以上でなければならない。

ＡＡ１１－３：サンプル者は１，０００人以上でなければならない。

ＡＡ１１－４：サンプル者は１０，０００人以上でなければならない。

(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）

ＡＡ１２－１：登録情報サンプル数／サンプル者・登録装置に関する要件はない。

ＡＡ１２－２：登録情報サンプル数／サンプル者・登録装置は２以上でなければならない。

ＡＡ１２－３：登録情報サンプル数／サンプル者・登録装置は５以上でなければならない。

ＡＡ１２－４：登録情報サンプル数／サンプル者・登録装置は１０以上でなければならない。

(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）

ＡＡ１３－１：提示情報サンプル数／サンプル者・提示装置に関する要件はない。

ＡＡ１３－２：提示情報サンプル数／サンプル者・提示装置は１０以上でなければならない。

ＡＡ１３－３：提示情報サンプル数／サンプル者・提示装置は１００以上でなければならない。

(4)本人拒否率測定における登録装置サンプル台数（ＡＡ１４）

ＡＡ１４－１：測定時に使用する本人情報登録装置の台数に関する要件はない。

ＡＡ１４－２：測定時に使用する本人情報登録装置は２台以上でなければならない。

ＡＡ１４－３：測定時に使用する本人情報登録装置は５台以上でなければならない。

(5)本人拒否率測定における提示装置サンプル台数（ＡＡ１５）

ＡＡ１５－１：測定時に使用する本人情報提示装置の台数に関する要件はない。

ＡＡ１５－２：測定時に使用する本人情報提示装置は２台以上でなければならない。

ＡＡ１５－３：測定時に使用する本人情報提示装置は５台以上でなければならない。

---

[1] バイオメトリクスⅡ（署名、声紋等の恣意的に変化させ得るもの）を利用する方式における他人受入率の考え方については、なお検討中である。

(6)登録装置とサンプル者との組み合わせ（ＡＡ１６）

ＡＡ１６－１：組み合わせに関する要件はない。

ＡＡ１６－２：各サンプル者はそれぞれに決められた登録装置群の各装置で決められた回数の登録を行わなければならない。

ＡＡ１６－３：各サンプル者は全ての登録装置で決められた回数の登録を行わなければならない。

(7)提示装置とサンプル者との組み合わせ（ＡＡ１７）

ＡＡ１７－１：組み合わせに関する要件はない。

ＡＡ１７－２：各サンプル者はそれぞれに決められた提示装置群の各装置で決められた回数の提示を行わなければならない。

ＡＡ１７－３：各サンプル者は全ての提示装置で決められた回数の提示を行わなければならない。

(8)登録装置と提示装置との組み合わせ（ＡＡ１８）

ＡＡ１８－１：組み合わせに関する要件はない。

ＡＡ１８－２：測定時の照合は、登録装置と提示装置との全ての有意な組み合わせについて行わなければならない。

２．４．２　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）

ＡＡ２１－１：登録サンプル者数に関する要件はない。

ＡＡ２１－２：登録サンプル者は１００人以上でなければならない。

ＡＡ２１－３：登録サンプル者は１，０００人以上でなければならない。

ＡＡ２１－４：登録サンプル者は１０，０００人以上でなければならない。

(2)他人受入率測定における提示サンプル者数（ＡＡ２２）

ＡＡ２２－１：提示サンプル者数に関する要件はない。

ＡＡ２２－２：提示サンプル者は１０人以上でなければならない。

ＡＡ２２－３：提示サンプル者は１００人以上でなければならない。

ＡＡ２２－４：提示サンプル者は１，０００人以上でなければならない。

(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）

ＡＡ２３－１：登録情報サンプル数／登録サンプル者･登録装置に関する要件はない。

ＡＡ２３－２：登録情報サンプル数／登録サンプル者･登録装置は２以上でなければならない。

ＡＡ２３－３：登録情報サンプル数／登録サンプル者･登録装置は５以上でなければならない。

ＡＡ２３－４：登録情報サンプル数／登録サンプル者･登録装置は１０以上でなければならない。

(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）

ＡＡ２４－１：提示情報サンプル数／提示サンプル者･提示装置に関する要件はない。

ＡＡ２４－２：提示情報サンプル数／提示サンプル者･提示装置は１０以上でなければならない。

ＡＡ２４－３：提示情報サンプル数／提示サンプル者･提示装置は１００以上でなければならない。

(5)登録装置サンプル台数（ＡＡ２５）

ＡＡ２５－１：測定時に使用する本人情報登録装置の台数に関する要件はない。

ＡＡ２５－２：測定時に使用する本人情報登録装置は２台以上でなければならない。

ＡＡ２５－３：測定時に使用する本人情報登録装置は５台以上でなければならない。

(6)提示装置サンプル台数（ＡＡ２６）

ＡＡ２６－１：測定時に使用する本人情報提示装置の台数に関する要件はない。

ＡＡ２６－２：測定時に使用する本人情報提示装置は２台以上でなければならない。

ＡＡ２６－３：測定時に使用する本人情報提示装置は５台以上でなければならない。

(7)登録装置とサンプル者との組み合わせ（ＡＡ２７）

ＡＡ２７－１：組み合わせに関する要件はない。

ＡＡ２７－２：各サンプル者はそれぞれに決められた登録装置群の各装置で決められた回数の登録を行わなければならない。

ＡＡ２７－３：各サンプル者は全ての登録装置で決められた回数の登録を行わなければならない。

(8)提示装置とサンプル者との組み合わせ（ＡＡ２８）

ＡＡ２８－１：組み合わせに関する要件はない。

ＡＡ２８－２：各サンプル者はそれぞれに決められた提示装置群の各装置で決められた回数の提示を行わなければならない。

ＡＡ２８－３：各サンプル者は全ての提示装置で決められた回数の提示を行わなければならない。

(9)登録装置と提示装置の組み合わせ（ＡＡ２９）

ＡＡ２９－１：組み合わせに関する要件はない。

ＡＡ２９－２：測定時の照合は、登録装置と提示装置との全ての有意な組み合わせについて行わなければならない。

２．４．３　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）

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。

精度設定	条件A	条件B	条件C
本人拒否率	_____%	_____%	_____%
他人受入率	_____%	_____%	_____%
対応率	_____%	_____%	_____%

条件Ａ：本人拒否率を重視して閾値を設定した場合
条件Ｂ：本人拒否率と他人受入率が同一になるような設定の場合
条件Ｃ：他人受入率を重視して閾値を設定した場合

２．４．４　限界基本精度（ＡＡ４）

(1)標準環境における限界基本精度（ＡＡ４１）

ＡＡ４１－１：標準環境における限界基本精度に関する要件はない。

ＡＡ４１－２：付録Ⅱに規定する精度影響要因の標準環境の範囲における限界基本精度は以下の通りでなければならない。

精度設定	条件A	条件B	条件C
本人拒否率	_____%	_____%	_____%
他人受入率	_____%	_____%	_____%
対応率	_____%	_____%	_____%

条件Ａ：本人拒否率を重視して閾値を設定した場合
条件Ｂ：本人拒否率と他人受入率が同一になるような設定の場合
条件Ｃ：他人受入率を重視して閾値を設定した場合

(2)仕様条件限界基本精度（ＡＡ４２）

ＡＡ４２－１：仕様条件限界基本精度に関する要件はない。

ＡＡ４２－２：精度影響要因について別途に示す仕様で規定する許容範囲における限界基本精度は以下の通りでなければならない。

精度設定	条件A	条件B	条件C
本人拒否率	_____%	_____%	_____%
他人受入率	_____%	_____%	_____%
対応率	_____%	_____%	_____%

条件Ａ：本人拒否率を重視して閾値を設定した場合
条件Ｂ：本人拒否率と他人受入率が同一になるような設定の場合
条件Ｃ：他人受入率を重視して閾値を設定した場合

２．４．５　認証精度に関連する機能（ＡＡ５）

(1)精度バランス調整機能（ＡＡ５１）

ＡＡ５１－１：固定されており、精度バランスを調整できない。

ＡＡ５１－２：事前の設定で少なくとも段階的に、精度バランスの調整ができなければならない。

ＡＡ５１－３：事前の設定で連続的に、精度バランスを自由に調整ができなければならない。

ＡＡ５１－４：個々の照合ごとに少なくとも段階的に、精度バランスの調整ができなければならない。

ＡＡ５１－５：個々の照合ごとに連続的に、精度バランスを自由に調整できなければならない。

(2)学習機能（ＡＡ５２）

ＡＡ５２－１：認証機能には学習機能は特に要求しない。

ＡＡ５２－２：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。

２．４．６　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）

ＡＡ６１－１：実用認証精度及び対応率に関しての要件はない。

ＡＡ６１－２：実用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。

精度設定	条件Ａ	条件Ｂ	条件Ｃ
実用本人拒否率	_____%	_____%	_____%
実用他人受入率	_____%	_____%	_____%
対応率	_____%	_____%	_____%

条件Ａ：実用本人拒否率を重視して閾値を設定した場合

条件Ｂ：実用本人拒否率と実用他人受入率が同一になるような設定の場合

条件Ｃ：実用他人受入率を重視して閾値を設定した場合

２．４．７　限界実用精度（ＡＡ７）

(1)標準環境における限界実用精度（ＡＡ７１）

ＡＡ７１－１：標準環境における限界実用精度に関する要件はない。

ＡＡ７１－２：付録Ⅱに規定する精度影響要因の標準環境の範囲における限界実用精度は以下の通りでなければならない。

精度設定	条件Ａ	条件Ｂ	条件Ｃ
実用本人拒否率	_____%	_____%	_____%
実用他人受入率	_____%	_____%	_____%
対応率	_____%	_____%	_____%

条件Ａ：実用本人拒否率を重視して閾値を設定した場合

条件Ｂ：実用本人拒否率と実用他人受入率が同一になるような設定の場合

条件Ｃ：実用他人受入率を重視して閾値を設定した場合

(2)仕様条件限界実用精度（ＡＡ７２）

ＡＡ７２－１：仕様条件限界実用精度に関する要件はない。

ＡＡ７２－２：精度影響要因について別途に示す仕様で規定する許容範囲における限界実用精度は以下の通りでなければならない。

精度設定	条件Ａ	条件Ｂ	条件Ｃ
実用本人拒否率	_____%	_____%	_____%
実用他人受入率	_____%	_____%	_____%
対応率	_____%	_____%	_____%

条件Ａ：実用本人拒否率を重視して閾値を設定した場合

条件Ｂ：実用本人拒否率と実用他人受入率が同一になるような設定の場合

条件Ｃ：実用他人受入率を重視して閾値を設定した場合

２．５　利便性（ＥＵ：Ease of Use）

２．５．１　操作性（ＥＵ－１）

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：複雑な操作が必要であってもやむを得ない、または操作の習熟が必要であってもやむを得ない。

ＥＵ１１－２：必要な操作は平易でなければならない。

ＥＵ１１－３：特別な／意識した操作を必要としてはならない。

(2)認証請求の容易性（ＥＵ１２）

ＥＵ１２－１：複雑な操作が必要であってもやむを得ない。。

ＥＵ１２－２：必要な操作は平易でなければならない。

ＥＵ１２－３：特別な／意識した操作を必要としてはならない。

(3)衣服等に関する要件（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ってもやむを得ない。

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なければならない。

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なければならない

２．５．２　事前準備（ＥＵ2）

(1)ハードウェア（ＥＵ２１）

ＥＵ２１－１：専用のハードウェアを必要としてもやむを得ない。

ＥＵ２１－２：必要なハードウェアは市販されていて容易に入手可能なものでなければならない。

(2)ソフトウェア（ＥＵ２２）

ＥＵ２２－１：専用のソフトウェアを必要としてもやむを得ない。

ＥＵ２２－２：必要なソフトウェアは市販されていて容易に入手可能なものでなければならない。

(3)事前学習の必要性（ＥＵ２３）

ＥＵ２３－１：マニュアル等による事前学習と理解とが必要であってもやむを得ない。

ＥＵ２３－２：特別な前提知識を必要としてはならない。

２．５．３　処理時間（ＥＵ3）

(1)本人情報登録・更新の処理時間（注１）（ＥＵ３１）

ＥＵ３１－１：本人情報登録・更新の処理時間は２日を超えてもよい。

ＥＵ３１－２：本人情報登録・更新の処理時間は１日以内でなければならない。
ＥＵ３１－３：本人情報登録・更新の処理時間は半日以内でなければならない。
ＥＵ３１－４：本人情報登録・更新の処理時間は１時間以内でなければならない。
ＥＵ３１－５：本人情報登録・更新の処理時間は１分以内でなければならない。

(2)登録申請から手続き完了まで（注２）（ＥＵ３２）
ＥＵ３２－１：登録申請から手続き完了までは１ケ月を超えてもよい。
ＥＵ３２－２：登録申請から手続き完了までは１ケ月以内でなければならない。
ＥＵ３２－３：登録申請から手続き完了までは１週間以内でなければならない。
ＥＵ３２－４：登録申請から手続き完了までは１日以内でなければならない。

(3)認証時の処理時間（注３）（ＥＵ３３）
ＥＵ３３－１：認証時の処理時間は１分を超えてもよい。
ＥＵ３３－２：認証時の処理時間は１分以内でなければならない。
ＥＵ３３－３：認証時の処理時間は 30 秒以内でなければならない。
ＥＵ３３－４：認証時の処理時間は 10 秒以内でなければならない。
ＥＵ３３－５：認証時の処理時間は５秒以内でなければならない。
ＥＵ３３－６：認証時の処理時間は１秒以内でなければならない。

（注１）本人情報の登録・更新における認証請求者の操作に要する時間
（注２）認証請求者が検証者／所有物発行体／認証局に対して本人情報の登録・更
新の申請を行ってから、登録・更新の完了の通知を受けるまでの手続き全体に要する時間。
（注３）認証請求者が提示点で認証請求操作を開始してから、検証結果の返信を受けるまでの時間。

２．５．４　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）
ＥＵ４１－１：本人情報の登録は指定の場所で行えなければならない。
ＥＵ４１－２：本人情報の登録は任意の場所で行えなければならない。

(2)認証請求可能な場所の制約（提示点の制約）（ＥＵ４２）
ＥＵ４２－１：認証請求は指定の場所で行えなければならない。
ＥＵ４２－２：認証請求は任意の場所で行えなければならない。

２．５．５．　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）
ＥＵ５１－１：本人情報の登録は定められた時間帯に可能でなければならない。
ＥＵ５１－２：本人情報の登録は休日以外の 9 時から 17 時の間に可能でなければなら

ない。

ＥＵ５１－３：本人情報の登録は毎日 9 時から 17 時の間に可能でなければならない。

ＥＵ５１－４：本人情報の登録は 24 時間 365 日可能でなければならない。

(2)認証請求可能な時間的制約（ＥＵ５２）

ＥＵ５２－１：認証請求は定められた時間帯に可能でなければならない。

ＥＵ５２－２：認証請求は休日以外の 9 時から 17 時の間に可能でなければならない。

ＥＵ５２－３：認証請求は毎日 9 時から 17 時の間に可能でなければならない。

ＥＵ５２－４：認証請求は 24 時間 365 日可能でなければならない。

２．５．６　提示情報の保管（EU6）

(1)所有物に関する条件（ＥＵ６１）

ＥＵ６１－１：携帯が困難または特別な保管が必要な所有物を必要としてもやむを得ない。

ＥＵ６１－２：所有物を利用する場合に、携帯／保管に関しては特別な問題があるものであってはならない。

ＥＵ６１－３：特別な所有物を必要としてはならない。

(2)記憶の必要性（ＥＵ６２）

ＥＵ６２－１：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ってもやむを得ない。

ＥＵ６２－２：秘密情報が必要な場合、その記憶は容易でなければならない。

ＥＵ６２－３：記憶すべき秘密情報があってはならない。

２．５．７　その他（EU7）

(1)代理人可否（ＥＵ７１）

ＥＵ７１－１：代理人による認証請求はできなくてもよい。

ＥＵ７１－２：代理人による認証請求はそれが本人の意思による場合には可能でなければならない。

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

２．６．１　初期設置コスト（MA１）

(1)初期設置コスト（ＭＡ１１）

初期設置コストは設置すべき機器および所要付属品の価格、運送費、据え付け･調整費（、必要なら、設置場所に要する費用）の合計とする。

ＭＡ１１－１：初期設置コストに関する特別な要件はない。

ＭＡ１１－２：初期設置コストは（　　）円以下とする。

２．６．２．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）

ＭＡ２１－１：専門家による１回の保守作業時間は１日以上かかってもよい。

ＭＡ２１－２：専門家による１回の保守作業時間は１日以内でなければならない。

ＭＡ２１－３：専門家による１回の保守作業時間は半日以内でなければならない。

ＭＡ２１－４：専門家による１回の保守作業時間１時間以内でなければならない。

ＭＡ２１－５：専門家による１回の保守作業時間１０分以内でなければならない。

(2)保守作業頻度（ＭＡ２２）

ＭＡ２２－１：専門家による保守作業頻度は毎日１回以下でなければならない。

ＭＡ２２－２：専門家による保守作業頻度は毎週１回以下でなければならない。

ＭＡ２２－３：専門家による保守作業頻度毎月１回以下でなければならない。

ＭＡ２２－４：専門家による保守作業頻度毎年１回以下でなければならない。

ＭＡ２２－５：専門家による保守作業は不要でなければならない。

(3)作業コスト（ＭＡ２３）

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)消耗品費、出張費の合計とする。

ＭＡ２２－１：保守作業コストに関する特別な要件はない。

ＭＡ２２－２：保守作業コストは（　　）円以下とする。

２．６．３　ユーザによる保守作業（MA３）

(1)1 回の作業時間（ＭＡ３１）

ＭＡ３１－１：ユーザによる１回の保守作業時間は１時間以内でなければならない。

ＭＡ３１－２：ユーザによる１回の保守作業時間は１０分以内でなければならない。

(2)作業頻度（ＭＡ３２）

ＭＡ３２－１：ユーザによる保守作業頻度は毎日１回以下でなければならない。

ＭＡ３２－２：ユーザによる保守作業頻度は毎週１回以下でなければならない。

ＭＡ３２－３：ユーザによる保守作業頻度は毎月１回以下でなければならない。

ＭＡ３２－４：ユーザによる保守作業頻度は毎年１回以下でなければならない。

ＭＡ３２－５：ユーザによる保守作業は不要でなければならない。

(3)ユーザ保守作業コスト（MA３３）

ユーザ保守作業コストは交換部品費、（クリーナ等の）消耗品費の合計とする。

MA３３－１：ユーザ保守作業コストに関する特別な要件はない。

MA３３－２：保守作業コストは（　　）円以下とする。

２．６．４　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）

MA４１－１：登録情報の更新（再登録）作業は月１回以下でなければならない。

MA４１－２：登録情報の更新（再登録）作業は年１回以下でなければならない。

MA４１－３：登録情報の更新（再登録）作業は１０年程度に１回以下でなければならない。

MA４１－４：登録情報の更新（再登録）作業は不要でなければならない。

(2)登録情報ファイルの保守作業（再編成等）（MA４２）

MA４２－１：登録情報ファイルの保守作業（再編成等）は日に１回以下でなければならない。

MA４２－２：登録情報ファイルの保守作業（再編成等）は月に１回以下でなければならない。

MA４２－３：登録情報ファイルの保守作業（再編成等）は年に１回以下でなければならない。

MA４２－４：登録情報ファイルの保守作業（再編成等）は不要でなければならない。

２．６．５　（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）

MA５１－１：所有物等の）提示情報の保守作業の必要な周期は月１回以下でなければならない。

MA５１－２：所有物等の）提示情報の保守作業の必要な周期は年１回以下でなければならない。

MA５１－３：所有物等の）提示情報の保守作業の必要な周期は１０年程度に１回以下でなければならない。

MA５１－４：所有物等の）提示情報の保守作業は不要でなければならない。

(2)提示情報保守作業の専門性（MA５２）

MA５２－１：発行体等の専門家でないとできなくともやむを得ない。

MA５２－２：提示情報の保守作業は本人が簡単にできるものでなければならない。

付録Ⅰ　本人認証の参照モデル(規定)

（省略）

付録Ⅱ　認証精度の測定方法(規定)

A　精度の評価指標

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。

A－1　精度水準の評価指標とその表示

精度は標準的な環境と、決められた手順に基づき、偏りがなく十分な数のサンプル者によるテストの結果得られた精度を表示する。

1）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）によって評価し、対にして表示する。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。

2）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。従って、精度は、判別閾値調整の可能なものは、３つの判別閾値設定による３組の精度対で表示する。閾値調整により精度バランス調整の出来ないものは、１組の精度対で表す。

精度設定	A	B	C
本人拒否率	_____%	_____%	_____%
他人受入率	_____%	_____%	_____%

A：本人拒否率を重視して閾値を設定した場合の精度
B：本人拒否率と他人受入率が同一になるような設定の場合の精度
C：他人受入率を重視して閾値を設定した場合の精度

A－2　対応率の表示

1）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＝（全サンプル者数－未対応者数）×１００／全サンプル者数

Ａ－３　基本認証精度と実用認証精度

上で述べた本人拒否率／他人受入率は利用するバイオメトリクスの性質およびセンサの性能を表わすものである。これを基本認証精度または基本精度という。特に断らない限り、認証精度とは基本認証精度を意味する。

一方、方式の実装にあたっては、より安全を期するために、２回の（一般的にはｎ回の）提示・照合により本人認証を行う実装方式を採る場合がある。この時の精度を実用認証精度または実用精度と総称し、それぞれ実用本人拒否率（または本人拒否率(n)）、実用他人受入率（または他人受入率(n)）という。実用認証精度の測定に関する考え方は基本認証精度の場合と同じである。

Ｂ　測定の方法

Ｂ－１　本人拒否率

１）サンプル者の選択

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。

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環境で行わねばならない。登録装置にばらつきが有り得るので複数の装置を使うのが望ましい。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環境で行わねばならない。提示装置にばらつきが有り得るので複数の装置を使うのが望ましい。各サンプル者は決められた装置毎に、決められた回数の提示を行う。提示装置が登録装置と兼用である場合も多いが、この測定では同じ機器であっても論理的に別とみなす。

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者毎の登録情報サンプル群と提示情報サンプル群とのあらゆる組み合わ

せの照合の数を全サンプル者について合計したものである。
ただしセンサ機能の限界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。
照合はほとんどの場合ソフトウェアで行われていると考えられ、実環境と著しく状況が異ならない限り、実際に使われるプロセッサとは別のプロセッサで行ってもよい。

5）まとめ

本人拒否率の測定の十分さの水準は、サンプル者数、登録装置数、提示装置数、提示回数／サンプル者・提示装置、登録回数／サンプル者・登録装置、登録装置とサンプル者の組み合わせ状況、提示装置とサンプル者との組み合わせ状況、登録装置と提示装置との組み合わせ状況で決まる。

B－2　他人受入率

1）サンプル者の選択

本人拒否率の項参照。登録サンプル者と提示サンプル者とは全く別であってもよいし、重複していてもよい。

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＝他人受け容れ数×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者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、提示サンプル者毎にその提示情報を全登録サンプル者の登録情報と照合するものである。

5）まとめ

他人受入率の測定の十分さの水準は、登録サンプル者数、提示サンプル者数、登録装置数、提示装置数、提示回数／サンプル者・提示装置、登録回数／サンプル者・登録装置、登録装置とサンプル者の組み合わせ状況、提示装置とサンプル者との組み合わせ状況、登録装置と提示装置との組み合わせ状況で決まる。

C　限界精度

精度に影響する要因を変化させた場合に標準環境限界域や、仕様でうたっている使用条件の限界域での精度をいう。

C－1　標準環境での限界精度

精度影響要因の標準環境限界における限界精度である。

温度：１０℃から３０℃における精度
湿度：３０%もしくは７０%における精度
その他

C－2　仕様条件下での限界精度

精度影響要因について仕様が示す許容範囲における限界精度である。

温度：仕様に指定した温度範囲における精度

湿度：仕様に指定した湿度範囲における精度

その他

D　標準試験条件

D－１　標準環境

場所：屋内

温度：１０℃（±１０℃）

湿度：５０％（±２０％）

明るさ：ＴＢＤ

バックグラウンドノイズ：ＴＢＤ

D－２　サンプル者の選択

人選：偏らない集団からランダムに人選すること

人数：全体的な照合確率分布が出来るだけ忠実に表現される程度に多くサンプル者を用いて試験する

D－３　操作の指示、習熟

指示：サンプル者に簡単な操作マニュアルを読んでもらい指示に替える。操作は出来るだけ実際の使用方法に即した方法を指定する。適度な注意を払って正しく操作していることを確認する、

習熟：カタログに習熟を要求しない場合は、訓練してははならない。

付録Ⅲ　脅威対抗性の評価（参考）

脅威対抗性に関する評価手法に関する検討は現時点では未だ充分深まったとはいえず、Version 0.5 においては脅威対抗性の要件レベルは未分化である。検討の過程で以下のような考察要因があることが分かっており、今後どのように基準に取り込んでゆくかが課題と考えている。

A　知識水準、技術水準などの分類

A-1．単一の知識しか持たない一般ユーザ:
　　アプリケーションプログラムのユーザ等で最低必要な操作しか知らない。

A-2．周辺知識を有する熟練ユーザ:
　　ファイル管理、OS のインストール、システムのセットアップの技術水準を有する。

A-3．アクセス特権を有する管理者:
　　システム管理者、ネットワーク管理者、データベース管理者等で特殊な知識を有し、かつアクセス特権を有している。

A-4．特殊技能者:
　　特定分野の開発研究者、ハードウェア技術者、システム開発者、特殊な技術および知識を有している。

B　ツールなどの必要条件

B-1．通常のシステム環境で特に何も必要としない。

B-2．一般市販品:
　　量産品として一般の人が容易に入手できるもの、インターネットなどから得られるプログラムなどが必要。

B-3．専門家用特殊機器:
　　研究所などにあるような一般に特殊で高価な測定機器や分析用機器。

B-4．非市販品:
　　専門知識や技術を必要とする製作可能な機器が必要。

C　時間的コストの必要条件

C-1．特別な時間を必要としない。--- 分のオーダ。

C-2．あまり労を要しない。--- 時間のオーダ。

C-3．相当の時間を要する。--- 月のオーダ。

C-4．長期間を要する。 --- 年のオーダ。

D　金額的コストの必要条件。

D-1．コスト不要。

D-2．個人で容易に支払が可能。

D-3．高額。
D-4．通常個人では対応できない価格。

E　対策の導入。
E-1．考慮されていない。
E-2．一部考慮されている。
E-3．十分考慮されている。

F 存在する標準への適合性。
F-1．適合していない。
F-2．一部適合（標準名）
F-3．完全に適合（標準名）

以上

付録C　本人認証に関する技術情報（文献リスト＆ＵＲＬ）

C.1　バイオメトリクスＩ（指紋、顔貌、虹彩、網膜、耳等）

C.1.1　指紋関連

（１）河嶋、木地,“指紋と掌紋による個人識別技術”,情報処理,Vol.25,No.6,pp.599-605,1984

（２）浅井　他、“マニューシャネットワーク特徴による自動指数照合－特徴抽出過程－”、信額論、J72-D-II、５、pp. 724-732 (1989).

（３）浅井　他、“マニューシャネットワーク特徴による自動指紋照合－照合過程－”、信学論、J72-D-II、５、pp. 733-740 (1989).

（４）渋谷　他、“隆線方向特徴を用いた指数画像自動分類方法、”第 41 回情処全国大会（1990）.

（５）伊藤　他、“方向分布パターンによる指数画像の分類、”、信学論、J73-D-II、10、pp. 1733-1741 (1990).

（６）中村　他、“方向分布パターンによる指数画像の分類、”信学論、J65-D、10、pp.1286-1293 (1982).

（７）Kawagoe et. al. “Fingerprint Pattern Classification,” Pattern Recognition, 17,3 pp.295-303 (1984).

（８）上条　他“ニューラルネットワークによる指紋画像の分類、”信学論、J74-D-II、２、pp. 199-208 (1991).

（９）T. Candela et. al., “ PCASYS-A Pattern- Level Classification Automation System for Fingerprints National Institute of Standards and Technology, NISTIR 5647 (1995).

（１０）内田　他、“大規模指数データベース照合のための照合候補選択”、信学技報、PRU (1996 年１月研究会）（1996).

（１１）I. Watson “NIST Spacial Database 14: Mated Fingerprint Card Paris 2,"National Institute of Standards and Technology (1993).

（１２）尾崎、松本、今井 “指紋ブロック照合の依頼計算における安全性に関する一考察” 信学技報 ISEC93-28

（１３）鹿井、仲嶋、他 “ファイバオプティックプレートを用いた指紋センサ” 第 54 回応用物理学会学術講演会予稿集

（１４）大和一晴 “指紋照合技術と入出管理セキュリティシステムの動向” 映像情報 1992 年 2 月

（１５）笹川、磯貝、池端 “低品質画像への対応能力を高めた個人確認用指紋照合装置” 信学会論文誌 vol. J72-D-II No.5

（１６）中島 他“位相限定相関法の原理と指紋照合への応用”第

２回画像センシングシンポジウム講演論文集
（１７）幸田、木村、酒井 “指走査形指紋撮像方法と指紋画像取り込み位置の規格化処理”１９９６年信学会総合大会 D-346
（１８）http://www.dermalog.de/ Identification Systems DERMALOG GmbH(DE)
（１９）http://www.identix.com/TLock.htm Identix(US)
（２０）http://143.101.112.12/afis/ NEC(US)
（２１）http://www.nrid.com/personal_id.html Personal Identification-NRI(US)
（２２）http://www.recogsys.com/ Recognition Systems(US)
（２３）http://www.nrid.com/ National Registry Inc.(US)
（２４）http://www.melco.co.jp/news/1996/0109.htm 三菱電機
（２５）http://www.infoweb.or.jp/f-denso/products/finger.htm 富士通電装

C.1.2 顔貌関連

（1）P. J. Neufeld and N. Colman, When science takes the witness stand, Sceint. Am. 262 46-53 (May 1990).
（2）K. Mase, Y. Suenaga and T. Akimoto ead reader－a head motion understanding system for better manmachine interaction Proc. 1987 IEEE Int. Conf. Syst. Man Cybern. pp. 970-974 (1987).
（3）D. E. Pearson and J. A. Robinson Visual communication at very low dats rates, Proc. IEEE 73 pp. 795-812 (April 1985).
（4）H. D. Ellis, Processes underlying face recignition The Neuropsychology of Face Perception and Facial Expression R. Bruyer, ed. Chapter 1, pp. 1-27. Lawrence Erlbaum Associates New Jersey (1986).
（5）D. C. Hay and A. W. Young, The human face, Normality and Pathology in Cognitive Functions, A. W. Ellis ed., Chapter6 pp. 173-203. Academic Press, New York (1982).
（6）L. D. Harmon The recognition of faces Scient. Am. 229, 71-82 (October 1973).
（7）A, Samal Minimum resolution for human face detection and identification Proc. SPIE/SPSE Symp. Electronic Imaging (January 1991).
（8）J. C. Bartlett S. Hurry and W. Thorley, Typicality and familiarity of faces Memory Cognition 12 219-228 (1984).
（9）W. W. Bledsoe, Man machine facial recognition Technical Report PRI 22, Panoramic Research Inc. (August 1960).

(10) M. D. Kelley Visual identification of people by computer, Ph. D. thesis Department of Computer Science Stanford University (1970).

(11) R. J. Baron, Mechanisms of human facial recognition, Int. J. Man-Mach. Stud. 15, 137-178 (1981).

(12) R. Buhr, Analyse und klassifikation von gesichtsbildern, ntz Archiv 8, 245-256 (1986).

(13) I. Craw, H. Ellis and J. R. Lishman, Automatic extraction of face-features. Pattern Recognition Lett.5 183-187 (1987).

(14) A. J. Goldstein, L. D.Harmon and A. B. Lesk, Identification of human faces Proc. IEEE 59, pp. 748-760 (May 1971).

(15) L. D. Harmon S. C. Kuo, P. F. Raming and U. Raudkivi dentification of human face profiles by copmputer, Pattern Recognition 10, 301-312 (1978).

(16) L. D. Harmon M. K.Khan, R. Lasch and P. F. Raming Machine idertification of human faces, Pattern Recognition 13, 97-110 (1981).

(17) G. J. Kaufman Jr and K. J. Breeding, The automatic recognition of human faces from profile silhouettes IEEE Trans. Syst. Man Cybern. 6, 113-121 (1976).

(18) Nixon, Eye spacing measurements for recognition, SPIE Proc. 575, Applications of Digital Image processing VIII pp. 279-285 (1995).

(19) G. Della Riccia and A. Iserles Automaticidentification of pictures of human faces Proc. 1977 Carnahan Conf. Crime Countermeasures, pp. 145-148 (1977).

(20) K. H. Wong H. H. M.Law and P. W. Tsang, A system for recognizing human faces, Proc. ICASSP 89 pp. 1638-1642 (May 1989).

(21) C. J. Wu and J. S. Huang Human face profile recognition by computer Pattern Recognition 23 255-260 (1990).

(22) R. A. Campbell S. Cannon, G. Jones and N. Morgan, Individual face classification by computer vision Proc. Conf. Modeling Simulation Microcompute. pp. 62-63 (1987).

(23) . T. Sakai M. Nagano and T. Kanada, Computer anaklysis and classfication of photographs of human faces, Proc, 1st USA-Japan Comput. Conf. pp 55-62 (1972).

(24) Sir. F. Galton Numeralized profiles for classification and recognition, Nature 83 127-130 (31 March 1910).

(25) K.Pearson, Photographic Researches and Portrature,

Volume II Chapter XII, pp. 283-333. Cambridge University Press Cambridge (1924).

(26) Sir Francis Galton, Personal identification and description-I Nature 173-177(21 June 1888).

(27) V. Govindaraju S. N. Srihari and D. B. Sher A computartional model for face location Proc. 3rd Int. Conf. Comput. Vision, pp. 718-721 (1990).

(28) V. Govindaraju D. B. Sher R. K. Srihari and S. N. Srihari, Locating human faces in newspaper photographs Proc. CVPR pp. 549-554 (1989).

(29) J. L. Perry and J. M. Carney Human face recognition using a multilayer perceptron Proc. Int. Conf. Naural Networks II, pp. 413 (Janusry 1990).

(30) M. Propp and A. Samal, Human face recognition nsing neural networks. (In preparation.)

(31) A. L. Yulie, D. S. Cohen and P. W. Hallinan, Feature extraction from faces using deformable templates, Proc. CVPR, pp. 104-109(1989).

(32) Sir Francis Galton. Personal identification and description-II Nature 201-203 (28 June 1888).

(33) L. D. Harmon Automatic recognition of human face profiles Proc. 3rd Int. Joinr Conf. Pattern Recognition pp. 183-188 (1976).

(34) P. Baylou, E. H. Bouyakhf, G. Bousseau and A. Mora Identification d'individus par analyse analyse automatique du profil du visage Proc. 3rd Int. Conf.:Security Through Sci. Engng, pp. 145-149 (September 1980).

(35) J. T. Lapreste J. Y. Cartouc and M. Richetin, Face recognition from range data by structural analysis Syntactic and Structural and Pattern Recgnition, G. Ferrate, T. Pavlidis A. Sanfeliu and H. Bunke eds, pp. 303-314. NATO ASI Series (1988).

(36) J. C. Lee and E. Milions Matching range images to human faces Proc. 3rd Int. Conf. Comput. Vision, pp 722-726 (1990).

(37) Y. Kaya and K. Kobayashi A basic study on human face recognition, Frontiers of Pattern Recobnition, pp. 265-289. Academic Press New York (1971).

(38) K. Preston Jr, Computing at the speed of light Electronics 38 72-83 (1965).

(39) W. K. Taylor Machine learning and recognotion of faces,

Electronic Lett. 3,436-437 (1967).
（４０）H. Schlosberg, Three dimensions of emotion Psychol. Rev. 61 81-88 (1954).
（４１）P. Ekman and W. V. Friesen Manual for the Facial Action Coding System. Cousuluting Psychologists Press, Palo Alto (1977).
（４２）S. M. Platt and N. I. Badler Animating facial expressions Comput. Graphics 15, 245-252 (August 1981).
（４３）K. Waters, A muscle model for animating three-dimensional facial expression, Comout. Craphics 22 17-24 (1987).
（４４）M. Suwa, N. Sugie and K. Fujimora, A preliminary note on pattern recognition of human emotional expression Proc. 4th Int. Joint Conf. Pattern Recognition pp. 408-410 (1978).
（４５）D. Terzopoulos and K. Waters Analysis of facial images using physical and anatomical models Proc. 3rd Int. Conf. Comput. Vision, pp. 727-732 (1990).
（４６）小杉“個人識別のための多重ピラミッドを用いたシーン中の顔の探索・位置決め” 信学会論文誌 Vol.J77-D-II No.4 (1994)
（４７）小杉“モザイクとニューラルネットを用いた顔画像の認識”信学会論文誌 J76-D-II No.4 (1993)
（４８）http://www.cs.rug.nl:80/~peterkr/FACE/face.html
Face Recognition Home Page(NL)

C.1.3 虹彩関連

（１）J.G.Daugman “High confidence visible recognition of persons by a test of statistical independence” IEEE Trans. Pattern Analysis and Machine Intelligence 15 pp.1148-1161 (1993)
（２）J.G.Daugman “High confidence Personal Identification by Iris Analysis” 14th meting of Internatinal associatin of Forensic Science(IAFS), Aug 26 1996 Tokyo (1996)
（３）J.G.Daugman US Patent No. 5,291,560:Biometric Personal Identification System Based on Iris Analysis: March 1(1994)

C.1.4 網膜関連

（１）F. W. Campbell How much of the information Falling on the retina reaches the visual cortex and how much is stored in the visual memory? Seminar at the Pontificae Academiae Scoentiarim Scripta Varia (1983).

（２） 砂川 他“網膜個人識別システム”映像情報, Vol.22 No.3 (1990)
（３） 砂川、柴田 “網膜血管パターンによる個人識別システム” 日本原子力学会誌 Vol.29 No.6 (1987)

C.1.5 耳関連

（１）結城、大宮、他 “モルフォロジー演算に基づく耳介の特徴抽出及び個人識別への応用” テレビ学技報, Vol.18 No.27（1994）
（２）大宮、篠原、結城 “耳介画像における個人性の分析” テレビ学技報 Vol.18, No.60（1994）

C.1.6 その他

（１）竹田、内田、平松 “指の特徴による個人認証方式” 東芝レビュー 1991 Vol.46 No.8
（２）佐々木、田崎、前田 “指照合付き入退室管理システム” 東芝レビュー 1992 Vol.47 No.6
（３）塩野、石川、島田,“手形を用いたゲート管理のための個人同定実験”,信学論(D-II),J74-D-II,No.6,pp.688-697,1991

C.2 バイオメトリクスII（署名・筆跡、声紋等）

C.2.1 筆跡・署名関連

（１）情報セキュリティ 研究所でハイセキュリティＯＡを運用開始 ハイセキュリティＯＡプラットホームの構築 AU 浅沼 透 (ＮＴＴ) JN F0050B (0915-2318) ＮＴＴ技術ジャーナル VN VOL.7,NO.10 PAGE.57－59 1995
（２）ＰＣＳにおける個人の移動性 (英題)Personal Mobility in PCS. AU ZAID M (BNR, OTTAWA, CAN) JN W0577A (1070-9916) ＩＥＥＥ Ｐｅｒｓ Ｃｏｍｍｕｎ VN VOL.1,NO.4 PAGE.12－16 1994
（３）電子決裁及び意思決定支援によるＯＡシステムの高度化 研究開発部門のマネジメント支援システムから AU 寺島信義, 笹島義弘, 大村清 (ＮＴＴ) JN F0050B (0915-2318) ＮＴＴ技術ジャーナル VN VOL.3,NO.5 PAGE.74－75 1991
（４）適応的ファジィクラスタリングニューラルネットワークを用いた筆者照合の一手法 (英題)A Method of Person Recognition System Based on Handwritten Characters using Adaptive Fuzzy Clustering Neural Network. AU 多田彰, 志水英二 (大阪市大 工) JN S0532B 電子情報通信学会技術研究報告 VN VOL.94,NO.509(PRU94 118-129) PAGE.15－22 1995

（５）携帯情報機器とヒューマンインタフェース論文特集　筆跡情報に重み付けを施した筆者照合方式 (英題)Special issue on Portable Information System and Human Interface Invited Papers. Writer Verification Method using Weighted Feature Parameters. AU 山崎恭, 小松尚久 (早稲田大 理工) JN S0815A (0285-9831) 画像電子学会誌 VN VOL.23,NO.5 PAGE.438－444 1994

（６）書写技能に基づく特性値を用いた筆者照合 (英題)Automatic writer verification using parameters derived from calligraphic Skills. AU 中村善一 (奈良工高専) JN S0573A (0387-1150) 奈良工業高等専門学校研究紀要 VN NO.29(1993) PAGE.27－31 1994

（７）手書き文字によるオンライン筆者照合 (英題)On－line writer verification based on handwritten characters. AU 横井仁史 (聖徳学園女短大); 吉村ミツ (中部大 経営情報); 吉村功 (名古屋大工) JN G0508A 電子情報通信学会全国大会講演論文 VN VOL.1991,NO.Spring Pt 7 PAGE.7.255 1991

（８）ファジィテンプレートを用いた筆者照合アルゴリズム ファジィテンプレートによる照合率の向上について (英題)Writer verification algorism using a fuzzy template. improvement of error rate with the fuzzy template. AU 森健一郎 (オムロン) JN S0266A (OMTKA) (0474-1315) Omron Tech VN VOL.30,NO.4 PAGE.303－308 1990

（９）握り圧力センサを埋め込んだ電子ペンの開発 (英題)Development of electric pen with grip pressure sensor. AU 渡辺正晴, 青木由直 (北大) JN G0508A 電子情報通信学会全国大会講演 VN VOL.1990,NO.Spring Pt.6 PAGE.6.235 1990

（１０）ファジィテンプレートによるオンライン筆者照合 (英題)Online writer verification using a fuzzy template. AU 森健一郎 (オムロン) JN S0532B 電子情報通信学会技術研究報告 VN VOL.89,NO.436(PRU89 118-125) PAGE.9－14 1990

（１１）スペクトル分解による手書き文字個人性の分析と筆跡認証 (英題)Analysis of personal information in handwritten characters and automatic writer recognition using a spectral resolution technique. AU 尺長健 (電電公社); 金子博, 淀川英司 (電電公社武蔵野電通研) JN F0137A (DTKKA) (0415-3200) 電気通信研究所. 研究実用化報告 VN VOL.34,NO.1 PAGE.35－46 1985

（１２） 筆跡認証と文字認識の異同について AU 吉村ミツ，木村文隆，吉村功（名古屋大工） JN S0532B 電子通信学会技術研究報告 VN VOL.82,NO.31 PAGE.49－56(PRL82－7) 1982

（１３）書写技能に基づく筆跡に現れる個人性の抽出 (英題)An Extraction of Individual Handwriting Characteristics Based on calligraphic skills. AU 中村善一 (奈良工高専); 豊田順一 (大阪大 産科研) JN L0197A (0915-1923) 電子情報通信学会論文誌 Ｄ－２ VN VOL.77,NO.3 PAGE.510－518 1994

（１４）ストローク解析による筆跡認証 (英題)Writer Recognition with the Stroke Analysis. AU 井出正弘，山田新一，藤川英司（武蔵工大） JN S0731A 情報処理学会全国大会講演論文集 VN VOL.45th,NO.2 PAGE.2.289－2.290 1992

（１５）神経回路網のモデルを用いた手書き文字による筆跡認証 (英題)Writer Identification of Hand－Writing Character Using Neural Network Models. AU 佐藤邦夫，大友照彦 (山形大 工); 原健一 (石巻専修大 理工) JN S0532B 電子情報通信学会技術研究報告 VN VOL.93,NO.50(PRU93 5-16) PAGE.81－88 1993

（１６）筆跡認証に用いる特徴の比較―濃度，方向，円弧 AU 吉村ミツ (中部大 総合工研) JN L0278A (0915-3292) 中部大学総合工学研究所総合工学 VN VOL.4 PAGE.1－10 1992

（１７）木マッチングによる英字署名識別に関する研究 (英題)A Study on the English Signature Verification Using Tree Matching. AU 安居院猛，中嶋正之 (東京工大 工); LEE Y H, KIM T K (Chun gnam National Univ., Daejon, KOR) JN L0197A (0915-1923) 電子情報通信学会論文誌 Ｄ－２ VN VOL.75,NO.1 PAGE.31－38 1992

（１８）ファジィ理論による筆跡認証の検討 (英題)Study of Writer Recognition by means of fuzzy theory. AU 尾崎正弘 (岡崎女短大); 足達義則 (中部大) JN L0486A ファジィシステムシンポジウム講演論文集 VN VOL.7th PAGE.427－429 1991

（１９）ニューラルネットワークと空間スペクトルを用いたテキスト独立型筆跡認証の性能評価 (英題)Performance of text－independent writer recognition using neural network and space spectrum. AU 津田雄則，長谷川孝明 (埼玉大工) JN G0508A 電子情報通信学会大会講演論文集 VN VOL.1991,NO.Shuki Pt 6 PAGE.6.242 1991

（２０）オンライン文字による筆者識別に関する研究　第２報（英題）A study of signature verification　using on‐line information of　characters. part2. AU　安居院猛，衛藤郁雄，長橋宏（東京工大　工　像情報工研施設）JN G0508A 電子情報通信学会大会講演論文集 VN　VOL.1991,NO.Shuki Pt 6 PAGE.6.234 1991

（２１）Leave‐one‐out 法を用いた適応型筆者照合システム(英題)Adaptive writer verification system using the leave‐one‐out‐method.　AU　吉村ミツ（中部大)；吉村功（名古屋大　工）　JN　S0532B 電子情報通信学会技術研究報告 VN　VOL.90,NO.252(PRU90 58-67) PAGE.25‐30 1990

（２２）ファジィ理論を用いた筆跡認証の試み（英題)Writer recognition by means of fuzzy theory. AU　尾崎正弘（岡崎女短大)；足達義則（中部大)；ＭＵＪＩＮ　Ｐ，岩堀祐之，石井直宏（名古屋工大）JN　G0508A 電子情報通信学会全国大会講演論文集 VN　VOL.1991,NO.Spring Pt 7 PAGE.7.256 1991

（２３）２次元空間スペクトルとニューラルネットワークを用いた手書き文字の筆跡認証（英題）Writer recognition of handwriting characters using two‐dimensional space spectrum analysis and neural network. AU　長谷川孝明，津田雄則，羽倉幸雄（埼玉大　工）JN　L0197A (0915-1923) 電子情報通信学会論文誌　Ｄ－２　VN　VOL.73,NO.12 PAGE.2083‐2085 1990

（２４）２次元空間スペクトル分析による手書き文字の筆跡認証(英題)Writer recognition of handwriting characters by analysis of two‐dimensional space spectrum. AU　長谷川孝明，津田雄則，羽倉幸雄（埼玉大　工）JN　G0508A 電子情報通信学会全国大会講演論文集 VN VOL.1990,NO.Spring Pt.7 PAGE.7.250 1990

（２５）ニューラルネットワークと２次元空間スペクトルを用いたテキスト独立性のある筆跡認証システム（英題）Text‐independent‐writer recognition　using neural network and two‐dimensional space spectrum. AU 長谷川孝明，津田雄則，羽倉幸雄（埼玉大　工）JN G0508A 電子情報通信学会全国大会講演論文集 VN VOL.1990,NO.Autumn Pt 6 PAGE.6.348 1990

（２６）相似パターンの頻度による筆者識別　（英題）Writer identification based on Frequencies of similar patterns. AU 吉村ミツ（中部大　経営情報)；吉村功（名古屋大　工）

JN L0197A (0915-1923) 電子情報通信学会論文誌 D－２ VN VOL.72,NO.12 PAGE.2051－2060 1989

（２７）一般文によるオフライン筆跡認証 （英題）Off－line writer recognition using an Arbitrarily fixed text. AU 吉村ミツ (中部大); 吉村功 (名古屋大 工) JN S0532B 電子情報通信学会技術研究報告 VN VOL.89,NO.468(IE89 108-117)PAGE.1－8 1990

（２８）筆跡認証技術の最近の動向 （英題）Recent trends in the writer Recognition technology. AU 吉村ミツ (中部大 経営情報); 吉村功 (名古屋大 工) JN F0019A (0913-5693) 電子情報通信学会誌 VN VOL.72,NO.7 PAGE.788－791 1989

（２９）弧パターン変換に基づく著者同定 （英題）Mriter identification based on the arc pattern transformation. AU yoshimura i (nagoya univ., Nagoya, jpn); yoshimura m (shotoku－gakuen women's junior coll., Gifu, jpn) JN E0037C Proc Int Conf Pattern Recogn VN VOL.9th,NO.Vol.1 PAGE.35－37 1988

（３０）筆速と筆圧によるオンライン筆跡認証 （英題）On－line writer recognition based on handwriting speed and pressure. AU 岡田謙一, 横山光男, 北川節 (慶応大 理工) JN S0757A (0913-5731) 電子情報通信学会論文誌 D VN VOL.71,NO.10 PAGE.2214－2216 1988

（３１）加重方向指数ヒストグラム法による筆跡認証実験 ＩＩ （英題）Writer recognition experiments using weighited direction index histgrams.2. AU 吉村ミツ (聖徳学園女短大); 吉村功 (名古屋大 工) JN G0508A 電子情報通信学会春季全国大会講演論文集 VN VOL.1988,NO.Pt. D-1 PAGE.185 1988

（３２）筆圧と筆速による手書き文字の筆跡認証 (英題)Automatic writer recognition based on writing pressure and speed. AU 岡田謙一, 横山光男, 北川節 (慶応大 理工) JN F0370B 電子情報通信学会情報・システム部門全国大会講演論文集 VN VOL.1987,NO.1 PAGE.72 1987

（３３）ミニ特集；個人識別技術 筆者識別技術の現状 (英題) Special issue on biometric recognition technique. A review of automatic writer recognition. AU 吉村功 (名古屋大 工); 吉村ミツ (聖徳学園女短大) JN F0131A (KESEA) (0453-4662) 計測と制御 VN VOL.25,NO.8 PAGE.694－700 1986

（３４）平均値の差の検定による筆者識別の妥当性について （英

題）On the validity of writer identification by the statistical test of mean difference.AU 高沢則美，谷本益み（科学警察研）JN F0738A (KKHKA) (0285-7960) 科学警察研究所報告 法科学編 VN VOL.39,NO.1 PAGE.1－5 1986

（３５）スペクトル分解による手書き文字個人性の分析と筆跡認証（英題）Analysis of personal information in handwritten characters and automatic writer recognition using a spectral resolution technique. AU 尺長健（電電公社）; 金子博，淀川英司（電電公社武蔵野電通研）JN F0137A (DTKKA)(0415-3200)電気通信研究所. 研究実用化報告 VN VOL.34,NO.1 PAGE.35－46 1985

（３６）音声と筆跡による個人識別技術 AU 白井克彦(早稲田大理工)JN G0427A (0447-8053) 情報処理 VN VOL.25,NO.6 PAGE.592－598 1984

（３７）２次統計量の線分スペクトル分解 テクスチャ性からの手書き文字個人性情報の抽出 AU 尺長健，金子博，淀川英司（電電公社武蔵野電通研）JN S0757A (0374-468X) 電子通信学会論文誌 D VN VOL.67,NO.4 PAGE.488－495 1984

（３８）筆者情報を表す複雑な漢字の構造変数 AU 小川正太郎，吉村ミツ，鳥脇純一郎，福村晃夫（名古屋大工）JN S0731A 情報処理学会全国大会講演論文集 VN VOL.27th,NO.2 PAGE.897－898 1983

（３９）筆者識別に影響する要因の分析 AU 吉村ミツ，木村文隆，吉村功（名古屋大工）; 藤田宏昭（ヤマハ発動機）JN S0757A (0374-468X) 電子通信学会論文誌 D VN VOL.66,NO.1 PAGE.1－8 1983

（４０）弾性的マッチングによる筆記体認識（英題）Cursive script recognition by elastic matching. AU TAPPERT C C (IBM, NY) JN D0061B (IBMJA) (0018-8646) IBM J Res Dev VN VOL.26,NO.6 PAGE.765－771 1982

（４１）手書き漢字認識における筆記者の個人性学習 AU 内藤誠一郎，増田功（電電公社武蔵野電通研）JN S0532B 電子通信学会技術研究報告 VN VOL.82,NO.175 PAGE.55－62(PRL82－45) 1982

（４２）筆跡認証と文字認識の異同について AU 吉村ミツ，木村文隆，吉村功（名古屋大工）JN S0532B 電子通信学会技術研究報告 VN VOL.82,NO.31 PAGE.49－56(PRL82－7) 1982

（４３）スペクトル解析による筆跡認証（英題）Writer recognition by spectral analysis. AU KUCKUCK W (Bundeskriminalamt, W.Germany) JN K810312 (0-89779-

042-1) proc third int conf secur sci eng 1980 VN ｐａｇｅ．１－３ 1980
（４４）筆者および話者認識における加重最小二乗アルゴリズムの応用 （英題）Application of a weighted least squares algorithm to writer and speaker recognition. AU NASKE R D (Bundeskriminalamt, Germany) JN K810111 Proc 5th Int Conf Pattern Recogn1980 VN PAGE.27－30 1980
（４５）http://www.penware.com/ PenWare(US)
（４６）http://www.cadix.co.jp/ キャディックス

C.2.2 声紋関連

（１）E. D. Petajan,Antomatic lipeadsing to enhance speech recognition Proc. CVPR pp. 40-47 (1985).
（２）松井、古井“話者識別技術” NTT R&D Vol.43 No.10 (1994)
（３）古井“声の個人性の話” 日本音響学会誌 Vol.51 No.11 (1995)
（４）http://www.fujitsu.co.jp/hypertext/news/1996/Jul/3.html 富士通

C.3 所有物

（１）Smart Card Technology: New Methods for Computer Access Control, National Institute of Standards and Technology, NIST Special Publication 500-157, National Technical Information Service, Springfield, VA, September 1988.
（２）Dray, J. F., M. E. Smid and R. Warnar, A Token Based Access Control System for Computer Networks, Proceedings - The 12th National Computer Security Conference, October 1989.
（３）NIST SACS Reader/Writer Specification, Datakey, Inc., Report #065-0098-000, July 11, 1991.
（４）ASACS Portable Reader/Writer Specification, Datakey, Inc., Report #065-0131-000, April 24, 1992.
（５）Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 2: Dimensions and Location of the Contacts, International Organization for Standardization, International Standard 7816-2, 1988.
（６）Identification Cards - Contactless Integrated Circuit(s) Cards - Part 3: Electronic Signals and Transmission Protocols, International Organization for Standardization, International Standard 7816-3, 1989.
（７）Dodson, D. F., J. F. Dray, and R. Warnar, "Security

Features for an FMS Smart Card", National Institute of Standards and Technology Special Report, September 25, 1990.
(8) Dray, J. F., and D. M. Balenson, An Overview of the Advanced Smartcard Access Control System (ASACS), Proceedings of the PSRG Workshop on Network and Distributed System Security, pp. 125-133, February 1993.
(9) ASACS Smartcard Specification, Datakey, Inc., Report #065-0130-000, April 24, 1992.
(10) Smartcard Application Program Interface for the Advanced Smartcard Access Control System (ASACS), TISR #465D, Trusted Information Systems, Inc., Glenwood, MD, October 1992.
(11) Advanced Smartcard Access Control System (ASACS): Smartcard Command Set Interface, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, D.C., 1992.
(12) Advanced Smartcard Access Control System (ASACS): Reader/Writer Command Set Interface, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, D.C., 1992.
(13) Advanced Smartcard Access Control System (ASACS): The DSS Signature Utility Program Manual, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, D.C., 1992.
(14) Advanced Smartcard Access Control System (ASACS): UNIX Access Control Software Manual, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, D.C., 1992.
(15) NIST SACS Smartcard Specification, Datakey, Inc., Report #065-0097-000, July 11, 1991.
(16) Hitachi H8/310 Single-Chip Microcomputer, Hitachi, Ltd., Tokyo, Japan, 1989.
(17) Haykin, M. E., and R. Warnar, Smart Card Technology: New Methods for Computer Access Control, National Institute of Standards and Technology, NIST Special Publication 500-157, National Technical Information Service, Springfield, VA, , September 1988.
(18) International Standard 7816-1, Identification Cards - Integrated Circuit(s) Cards with Contacts -- Part 1:

Physical Characteristics, International Organization for Standardization, 1987.
（１９）Krajewski, M., Concept for a Smart Card Kerberos, Proceedings - The 15th National Computer Security Conference, Volume 1, October 1992.
（２０）Johnson, J.T.; Tolly, K. “Token authentication” Data Communications International vol.24, no.6 p.62-6,68-70, 72, 74, 76
（２１）Gaskell, G.; Looi, M. “Integrating smart cards into authentication systems” Cryptography: Policy and Algorithms. International Conference. Proceedings p.270-81
（２２）http://www.cryptocard.com/ CRYPTOCCard(US)
（２３）http://www.securid.com/ SecurID - Security Dynamics(US)
（２４）http://www.safeword.com/ SafeWord - Secure Computing(US)
（２５）http://www.gold.net/users/ct96/supplier.htm Card Europe Supplier Database
（２６）http://www.smart-card.com/smartcard.htm The Smart Card Resource Center

C.4 秘密情報Ｉ（パスワード等）

（１）Password Usage, National Institute of Standards and Technology, Federal Information Processing Standards Publication 112, National Technical Information Service, Springfield, VA, May 1985.
（２）Automated Password Generator (APG), National Institute of Standards and Technology, Federal Information Processing Standards Publication 181, National Technical Information Service, Springfield, VA, March 29, 1994.
（３）American National Standard X9.26-1990, Financial Institution Sign-on Authentication for Wholesale Financial Systems, American Bankers Association, Washington, D.C., 1990.
（４）Data Encryption Standard (DES), National Institute of Standards and Technology, Federal Information Processing Standards Publication 46-2, National Technical Information Service, Springfield, VA, Reaffirmed December 30, 1993 (Supersedes FIPS PUB 46, January 15,

1977).
(5) DES Modes of Operation, National Institute of Standards and Technology, Federal Information Processing Standards Publication 81, National Technical Information Service, Springfield, VA, December 2, 1980.
(6) Guidelines for Implementing and Using the NBS Data Encryption Standard, National Institute of Standards and Technology, Federal Information Processing Standards Publication 74, National Technical Information Service, Springfield, VA, April 1, 1981.
(7) Kohl, J. (Digital Equipment Corporation), and Neumann, C. (University of Southern California/Information Sciences Institute), The Kerberos Network Authentication Service (V5), Internet Request For Comments (RFC) 1510, September 1993.
(8) Steiner, J. G., C. Neuman, and J. I. Schiller, Kerberos: An Authentication Service for Open Network Systems, Proceedings of the Winter USENIX Conference, Dallas, Texas, March 30, 1988.
(9) American National Standard X9.17-1985, Financial Institution Key Management (Wholesale), American Bankers Association, Washingtion, D.C., reaffirmed 1991.
(10) Bellovin, S. M., and M. Merritt, Limitations of the Kerberos Authentication System, Computer Communications Review, October 1990.
(11) Chin-Chen Chang; Tzong-Chen Wu; Chi-Sung Laih "Cryptanalysis of a password authentication scheme using quadratic residues" Computer Communications vol.18, no.1 p.45-7
(12) Horng-Twu Liaw; Chin-Laung Lei "An efficient password authentication scheme based on a unit circle" Cryptologia vol.19, no.2 p.198-208
(13) Tran Van Trung "On the construction of authentication and secrecy codes" Designs, Codes and Cryptography vol.5, no.3 p.269-80
(14) Horng, G." Password authentication without using a password table" Information Processing Letters vol.55, no.5 p.247-50
(15) McDonald, D.L.; Atkinson, R.J.; Metz, C. "One time Passwords In Everything (OPIE): experiences with building

and using stronger authentication" Proceedings of the Fifth USENIX UNIX Security Symposium pp.177-86
（１６）Horng-Twu Liaw "Password authentications using triangles and straight lines" Computers & Mathematics with Applications vol.30, no.9 p.63-71

C.5 秘密情報II（デジタル署名等）

（１）Proposed Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S. Department of Commerce, Washington, D.C., August 30, 1991.
（２）Rivest, R. L., A. Shamir and L. M. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM, Volume 21, Number 2, February 1978, pp. 120-126.
（３）Linn, J., Privacy Enhancement for Internet Electronic Mail: Part I -- Message Encipherment and Authentication Procedures, Internet Request For Comments (RFC) 1421, July 23, 1992.
（４）Kent, S., Privacy Enhancement for Internet Electronic Mail: Part II -- Certificate-Based Key Management, Internet Request For Comments(RFC) 1422, BBN Communications, February 1993.
（５）Balenson, D. M., Privacy Enhancement for Internet Electronic Mail: Part III -- Algorithms, Modes, and Identifiers, Internet Request For Comments (RFC) 1423 , Trusted Information Systems, February 1993.
（６）Kaliski, B., Privacy Enhancement for Internet Electronic Mail: Part IV -- Key certification and Related Services, Internet Request For Comments (RFC) 1424, RSA Laboratories, February 1993.
（７）CCITT Recommendation X.509, The Directory - Authentication Framework, The International Telegraph and Telephone Consultative Committee, November 1988.
（８）Galvin, J., et al, Security Issues of a UNIX PEM Implementation, TISR #468D, Trusted Information Systems, February 11, 1993.
（９）X.500 Directory Services Recommendation
（１０）Public Key Cryptography, National Institute of Standards and Technology, NIST Special Publication 800-2, National Technical Information Service,

Springfield, VA, April 1991.
（１１）Mendes, S.; Huitema, C. “A new approach to the X.509 framework: allowing a global authentication infrastructure without a global trust model” Proceedings of the Symposium on Network and Distributed System Security p.172-89
（１２）English, E. “Use of Kerberos authentication (network security)” Computer Fraud & Security Bulletin p.16-18
（１３）I-Lung Kao; Chow, R. “An efficient and secure authentication protocol using uncertified keys” Operating Systems Review vol.29, no.3 p.14-21
（１４）Schiller, J.I.; Atkins, D. “Scaling the web of trust: combining Kerberos and PGP to provide large scale authentication” Proceedings of the 1995 USENIX Technical Conference p.83-94
（１５）Lowe, G. “An attack on the Needham-Schroeder public-key authentication protocol” Information Processing Letters vol.56, no.3 p.131-3
（１６）Wei-Bin Lee; Chin-Chen Chang “Integrating authentication in public key distribution system” Information Processing Letters vol.57, no.1 p.49-52
（１７）Johansson, T. “Constructions of asymmetric authentication systems” Proceedings 1995 IEEE International Symposium on Information Theory p.354

C.6 その他本人認証全般（複数カテゴリにまたがるものも含む）

（１）林,“個人識別技術とそのニーズおよび期待”,計測と制御,Vol.25,No.8,1986
（２）塩野、真田,“個人識別技術の最近の研究動向”信学技報,OFS92-17,IE92-49,pp.1-8,1992
（３）小畑,“個人識別技術の現状と展望”システム／制御／情報,Vol.35,No.7,pp.383-389,1991
（４）Woo, T. Y. C., and S. S. Lam, Authentication for Distributed Systems, IEEE CS Press, January 1992.
（５）Guideline on User Authentication Techniques for Computer Network Access Control, National Institute of Standards and Technology, Federal Information Processing Standards Publication 83, National Technical Information Service, Springfield, VA, September 1980.
（６）Secure Hash Standard (SHS), National Institute of

Standards and Technology, Federal Information Processing Standards Publication 180, National Technical Information Service, Springfield, VA, May 11, 1993.
(7) Kaliski, B., The MD2 Message-Digest Algorithm, Internet Request for Comments (RFC) 1319, RSA Laboratories, April 1992.
(8) Rivest, R., The MD5 Message-Digest Algorithm, Internet Request for Comments (RFC) 1321, MIT Laboratory for Computer Science and RSA Laboratories, April 1992.
(9) Biometric Access Control Device Evaluation Criteria (Draft Report), DCI Intelligence Information Handling Committee, February 1991.
(10) Linn, J., Common Authentication Technology Overview, Internet Request For Comments (RFC) 1511, Geer-Zolot Associates, September 1993.
(11) Kaufman, C., DASS: Distributed Authentication Security Service, Internet Request For Comments (RFC) 1507, Digital Equipment Corporation, September 1993.
(12) Linn, J., Generic Security Services Applications Program Interface, Internet Request For Comments (RFC) 1508, Geer-Zolot Associates, September 1993.
(13) Wray, J., Generic Security Service API: C-Bindings, Internet Request For Comments (RFC) 1509, Digital Equipment Corporation, September 1993.
(14) Gollmann, D. "What do we mean by entity authentication?" Proceedings 1996 IEEE Symposium on Security and Privacy p.46-54
(15) Stubblebine, S.G.; Wright, R.N. "An authentication logic supporting synchronization, revocation, and recency" 3rd ACM Conference on Computer and Communications Security p.95-105
(16) Samar, V. "Unified login with pluggable authentication modules (PAM)" 3rd ACM Conference on Computer and Communications Security p.1-10
(17) Zuquete, A.; Guedes, P. "Transparent authentication and confidentiality for stream sockets" IEEE Micro vol.16, no.3 p.34-41
(18) Petraglia, J. "Situated cognition and the technology of authentication" Proceedings of International Conference on Computers in Education 1995. p.340-7

(19) Maurer, U.M. "A unified and generalized treatment of authentication theory" STACS 96. 13th Annual Symposium on Theoretical Aspects of Computer Science. Proceedings p.387-98
(20) Gehrmann, C. "Information theoretical lower bounds for unconditionally secure group authentication" Proceedings 1995 IEEE International Symposium on Information Theory p.350
(21) Odaka, T.; Kato, T.; Takada, M.; Nishino, J.; Ogura, H. "An authentication method based on analysis of input strings from user to interactive computer system" Transactions of the Institute of Electronics, Information and Communication Engineers A vol.J79-A, no.4 p.1001-3
(22) Bolignano, D. "Format verification of cryptographic authentication protocols" Technique et Science Informatiques vol.15, no.4 p.451-81
(23) Fujii, H.; Kachen, W.; Kurosawa, K. "Combinatorial bounds and design of broadcast authentication" IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences vol.E79-A, no.4 p.502-6
(24) Maurer, U.M. "Information-theoretic bounds in authentication theory" Proceedings 1995 IEEE International Symposium on Information Theory p.12
(25) Yun Ding; Horster, P. "Why the Kuperee authentication system fails" Operating Systems Review vol.30, no.2 p.42-51
(26) Shiuh-Pyng Shieh; Wen-Her Yang "An authentication and key distribution system for open network systems" Operating Systems Review vol.30, no.2 p.32-41
(27) Sugiyama, H.; Obata, M.; Tanabe, K. "Design and implementation of user authentication system in distributed systems" NTT R & D vol.45, no.1 p.67-72
(28) Denning, D.E.; MacDoran, P.F. "Location-based authentication: grounding cyberspace for better security" Computer Fraud & Security p.12-16
(29) Menkus, B. "Various user authentication mechanisms" EDPACS vol.23, no.9 p.14-17
(30) Pierson, L.G. "Integrating end-to-end encryption

and authentication technology into broadband networks" Proceedings of the SPIE - The International Society for Optical Engineering vol.2615 p.260-9
(３１) Van Tilborg, H.C.A. "Authentication codes: An area where coding and cryptology meet" Cryptography and Coding. 5th IMA Conference. Proceedings pp.169-83
(３２) Hosny, W.; Kamel, T.; Shahin, S. "New design for network layer authentication model in TCP/IP suite" Egyptian Computer Journal vol.23, no.1 p.77-94
(３３) Rees, R.S.; Stinson, D.R. "Combinatorial characterizations of authentication codes II" Designs, Codes and Cryptography vol.7, no.3 p.239-59
(３４) Mitchell, C.J.; Piper, F.C.; Walker, M.; Wild, P. "Authentication schemes, perfect local randomizers, perfect secrecy and secret sharing schemes" Designs, Codes and Cryptography vol.7, no.1-2 p.101-10
(３５) Mohan, S. "Network impacts of privacy and authentication protocols for PCS" ICC `95 Seattle. Communications - Gateway to Globalization. 1995 IEEE International Conference on Communications Part vol.3 p.1557-61 vol.3
(３６) Murthy, V.K. "Probabilistic quorum protocols for biometrical user authentication in OLTP" SIGSAC Review vol.14, no.1 p.5-10
(３７) Tzong-Chen Wu "Remote login authentication scheme based on a geometric approach" Computer Communications vol.18, no.12 p.959-63
(３８) Kwok-Yan Lam "Replay tolerance of authentication protocols" Computer Communications vol.18, no.12 p.988-92
(３９) Chin-Chen Chang; Sun-Min Tsu; Chien-Yuan Chen "Remote scheme for password authentication based on theory of quadratic residues" Computer Communications vol.18, no.12 p.936-42
(４０) Song, Y.; Kurosawa, K.; Tsujii, S. "Authentication codes based on association schemes" IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences vol.E79-A, no.1 p.126-30
(４１) Hayashi, S.; Saito, T.; Murata, Y. "Encryption and authentication program module" NTT R & D vol.44, no.10 p.913-22
(４２) Oppliger, R. "Firewalls aren`t enough: authentication

and key distribution systems" Computer Security Journal vol.11, no.2 p.15-24
(43) Hung-Yu Lin; Harn, L. "Authentication protocols for personal communication systems" Computer Communication Review vol.25, no.4 p.256-61
(44) Touch, J.D. "Performance analysis of MD5 [authentication algorithm]" Computer Communication Review vol.25, no.4 p.77-86
(45) Li Gong " Efficient network authentication protocols: lower bounds and optimal implementations" Distributed Computing vol.9, no.3 p.131-45
(46) Kato, T.; Takada, M.; Odaka, T.; Ogura, H. "A modeling method for keyboard input series in an interactive computing environment and its application for user authentication" Transactions of the Institute of Electronics, Information and Communication Engineers A vol.J78-A, no.9 p.1251-4
(47) Kurosawa, K.; Kageyama, S. "Title: New bound for affine resolvable designs and its application to authentication codes" Computing and Combinatorics. First Annual International Conference, COCOON'95. Proceedings p.292-302
(48) Dingyi Pei "Information-theoretic bounds r authentication codes and block designs" Journal of Cryptology vol.8, no.4 p.177-88
(49) Leach, J. "Dynamic authentication for smartcards" Computers & Security vol.14, no.5 p.385-9
(50) Johansson, T." Authentication codes for nontrusting parties obtained from rank metric codes" Designs, Codes and Cryptography vol.6, no.3 p.205-18
(51) Castro, A. "Identification and authentication of users on IP networks" SECURICOM 95. 13th Worldwide Congress on Computer and Communications Security and Protection Proceedings p.131-49
(52) Taylor, R. "Near optimal unconditionally secure authentication" Advances in Cryptology - EUROCRYPT '94. Workshop on the Theory and Application of Cryptographic Techniques. Proceedings p.244-53
(53) Oppliger, R. "Authentication and key distribution in computer networks and distributed systems" Communications

and Multimedia Security. Proceedings of the IFIP TC6, TC11 and Austrian Computer Society Joint Working Conference on Communications and Multimedia Security, 1995 p.148-59
(54) Gehrmann, C "Secure multiround authentication protocols". Advances in Cryptology - EUROCRYPT '95. International Conference on the Theory and Application of Cryptographic Techniques. Proceedings p.158-67
(55) Hyun-Jung Kim "Biometrics, is it a viable proposition for identity authentication and access control?" Computers & Security vol.14, no.3 p.205-14
(56) Mao, W.; Boyd, C. "Methodical use of cryptographic transformations in authentication protocols" IEE Proceedings-Computers and Digital Techniques vol.142,no.4 p.272-8
(57) Wilkes, J.E. "Privacy and authentication needs of PCS" IEEE Personal Communications vol.2, no.4 p.11-15
(58) Brown, D. "Techniques for privacy and authentication in personal communication systems" IEEE Personal Communications vol.2, no.4 p.6-10
(59) Borcherding, M. "Efficient failure discovery with limited authentication" Proceedings of the 15th International Conference on Distributed Computing Systems p.78-82
(60) De Paoli, D.; Goscinski, A. "The ring based conference authentication service" Australian Computer Science Communications vol.17, no.1 p.120-9
(61) Rogers, J "Neural network user authentication" AI Expert vol.10, no.6 p.29-33
(62) Stubblebine, S.G. "Recent-secure authentication: enforcing revocation in distributed systems" Proceedings 1995 IEEE Symposium on Security and Privacy p.224-35
(63) Anderson, S.; Garvin, R. "Sessioneer: flexible session level authentication with off the shelf servers and clients" Computer Networks and ISDN Systems vol.27, no.6 p.1047-53
(64) Bird,R.; Gopal,I.; Herzberg,A.;Janson,P.; Kutten,S.; Molva,R.; Yung,M. "The KryptoKnight family of light-weight protocols for authentication and key distribution" IEEE/ACM Transactions on Networking vol.3, no.1 p.31-41
(65) Tzonelih Hwang; Narn-Yih Lee; Chuan-Ming Li;

Ming-Yung Ko; Yung-Hsiang Chen "Two attacks on Neuman-Stubblebine authentication protocols" Information Processing Letters vol.53, no.2 p.103-7
(66) Tzonelih Hwang; Yung-Hsiang Chen "On the security of SPLICE/AS -the authentication system in WIDE Internet" Information Processing Letters vol.53, no.2 p.97-101
(67) Chae Hoon Lim; Pil Joong Lee "Several practical protocols for authentication and key exchange" Information Processing Letters vol.53, no.2 p.91-6
(68) Wu Chuankun; Wang Xinmei "Authentication from linear codes" Chinese Journal of Electronics vol.4, no.1 p.96-8
(69) http://weber.ucsd.edu/~pagre/identification.html
(70) http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID
(71) http://www.vitro.bloomington.in.us:8080/~BC/ Biometric Consotium
(72) http://www.nist.gov/itl/lab/fips/ FIPS(Federal Information Processing Standards
(73) http://www.ncsa.com/ NCSA(National Computer Security Association)
(74) http://www.nist.gov/ NIST(National Institute of Standards and Technology)
(75) http://www.aiia.com.au/ AIIA(Australian Information Industry Association)
(76) http://www.auscert.org.au/ AUSCERT(Australian Computer Emergency Response Team)
(77) http://www.sjb.co.uk/btt.html BTT(Biometric Technology Today)
(78) http://www.w3.org/pub/Conferences/WWW4/Papers/330/ Smart Tokens and their Implementation - W3C(US)

付録D　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ー マルチメディアＳＩ担当 課長代理
	塚田光芳	沖電気工業（株） 情報通信システム事業部ＥＣ事業推進センター 金融・情報システム研究部 担当部長
	高橋　章	オムロン（株） ＥＦＴＳ統轄事業部開発センタ第３開発部（ＥＸ） 主幹
	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
	石原洋之	（株）システムズナカシマ 東京支店システム部　課長
	杉浦和彦	綜合警備保障（株） 技術業務本部技術部計画課
	辻　　健	ソニー（株） 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） 第一パーソナルＣ＆Ｃ事業本部 パーソナルワークステーション事業部第一商品部
	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
	中島雅人	（株）富士通 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
	福崎康弘	（株）ワコム 新事業室
	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　（財）情報処理振興事業協会 技術センター
コンピュータセキュリティ技術調査室　室長補佐