第1部

バイオメトリクスとは
（当協会による調査研究資料から）

1. 本人確認の手段

我々人間は、社会生活において常に他人と接する機会があり、必要があればその人が誰であるかを何らかの手段で確認している。同様に、自分が誰であるかを、何らかの手段で他人に証明する必要を迫られる。つまり、本人確認という作業は、監視やセキュリティに限ることなく、日常生活において当たり前のように行われている行為である。本人を確認する手段としては、次の三種類が存在する。

第一の手段は、本人の知識を用いるものである（What you KNOW）。パスワードや暗証番号、さらには母親の旧姓や過去の記憶など、本人しか知りえない情報をもとに本人を確認する方法である。例えばパスワードは、一般的な本人認証手段として最もよく使われているもので、システムへの実装も容易に行える。しかし、適切なセキュリティレベルを保持するためには、利用者にある程度の負荷を強いることになる。もともとパスワードは、キーボード入力を前提としたコンピュータシステム向けの本人確認手段であるため、キーボードに不慣れな人には使いにくい。無意味な文字列を覚えることは容易でなく、忘失の恐れがある。また、忘れないように記録した紙などを見られて盗用される恐れもある。さらに言えば、高いセキュリティレベルを保持するために、定期的にパスワードを更新させるという運用は、利用者にとってはより一層使いにくいものとなる。

第二の手段は、本人の所有物を用いるものである（What you HAVE）。IDを記録した磁気カードや運転免許証など、他人が持ち得ない物をもとに本人を確認する方法である。これらは、認証に用いられる媒体の偽造が難しければ難しいほどセキュリティレベルが高まるとされており、ホログラムやICチップの組み込みなどの工夫が施されている。しかし、物であるため盗用される危険性が高く、パスワードなど物以外の情報と併用しないと高いセキュリティレベルは保てない。また、媒体の低価格化が進んでも、破損や紛失によるメンテナンスコストが発生し、利用者には媒体の適切な管理が求められる。さらに、知識による認証手段も同様であるが、本人が協力した場合のなりすましに対しては、セキュリティ強度が保てないという弱点を有している。

第三の手段は、生体認証と呼ばれる本人の生体情報を用いるものである（What you ARE）。生体情報は、指紋や顔などの身体的特徴と、署名や音声などの行動的特徴に大別される。また、入力形態は、センサに身体の一部を直接触れる接触型と、何も触れる必要がない非接触型に分けられる。認証に用いる媒体が本人から切り離せないという特性から、紛失や盗難の危険がないという点で他の手段より優位である。認証に使われる媒体が常に本人の管理下にあり、しかも特別なメンテナンスは必要ないことから、利用者に対する負担は少ない。認証システムを管理する側からみれば、媒体の破損や紛失がないため再発行などの手間を必要とせず、ランニングコストを低く抑えられるメリットもある。

しかし、生体認証が持つセキュリティ上の脆弱性については注意すべき点がある。一つは、生体情報の複製の可能性である。例えば指紋を例にとると、指自体を奪われることは通常では考えられないものの、本人の残留指紋から指紋を複製される危険性が指摘されている。顔については、顔写真を使って本人に成りすますことが容易に考えられる。このような成りすましについては、運用に応じてそのセキュリティレベルに合った対策を講じる必要がある。もう一つは、生体情報は本質的にノイズを含むアナログ量である点である。つま

り、各試行によって得られる値が必ずしも一致するわけではなく、本人を拒否する誤りや、他人を受理する誤りが常に発生する。また、信号がノイズに埋もれてしまい、生体情報が取得できない場合もある。例えば、指先をよく使う職業の人は指紋が磨耗してしまい、きれいな指紋画像を得ることができない。生体認証では、このような未対応となる人が存在する点にも注意すべきである。

社会的受容性の点から言えば、取得された生体情報が2次利用される危険性やプライバシーの問題から、指紋や顔写真などの生体情報を取られることに抵抗を感じる人が少なくない。磁気カードなどが盗難された場合は再発行が可能だが、個人の身体的特徴や行動的特徴は変えることができないため、生体情報が悪用されてしまうと、その生体情報を使った本人認証は二度と行えなくなる危険性がある点にも注意すべきである。

このような運用上の課題は残されているものの、生体認証による利便性が周知されれば、第三の本人認証手段として市場は急速に広がると予想されている。ここでは、本人確認の手段としての生体認証の種類とその技術について概説する。（表1参照）

2. 顔認証技術

我々人間は、宗教的な例外を除いて、ほとんどの人が顔を見られることを前提に生活しており、顔によってその人が誰であるかを判断している。近年、工学的なアプローチで、顔を用いた本人認証を自動化する顔認証の研究が活発に進められている。遠くからでも、しかも本人に悟られずに計測できる顔は、他の生体情報にはない特性を有しており、顔認証システムは指紋に続く第二の市場に成長すると予測されている。

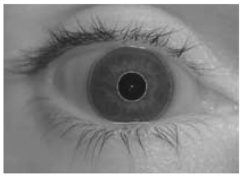
	符号化方式	ヘッダ情報	備考
顔画像データ  画像タイプ毎に撮影条件や顔向きなどの要件を規定	JPEG JPEG2000	必須：画像数、画像タイプ、画像サイズなど オプション：色空間、性別、顔向き、表情、顔特徴点、目の色・髪の色など	同一人物の複数の画像を一つのファイルフォーマットに収容可能
指紋画像データ 	RAW, WSQ, JPEG, JPEG2000, PNG	解像度、階調、画像サイズ、部位（親指-小指、左・右）など	複数の指の登録、一指あたり複数の画像を一つのファイルフォーマットに収容可能
虹彩画像データ  直交座標系と極座標系の画像表現形式	RAW, JPEG, ロスレス JPEG, JPEG2000	画像サイズ、画像向き、撮像波長、虹彩直径、傾きなど	一つのフォーマットに一つの虹彩画像を収容

表1　主要なバイオメトリクスデータ