バイオメトリクスによる本人認証技術
Biometric Identification Technology

山田　貢己　YAMADA Miki
出口　豊　DEGUCHI Yutaka
河村　聡典　KAWAMURA Akinori

パスワードや磁気カードなどの代わりとなる，指紋認証などのバイオメトリクス(生体測定法) による本人認証技術が使われ始めている。パスワードを忘れたり，カードを拾われて他人に利用されたりする危険性のないことがバイオメトリクスのメリットである。当社では，すでに指照合技術と顔認識技術を開発しているが，新たに音声および手書きサインによる本人認証技術と，バイオメトリクスのシステム技術を開発した。

かつてセキュリティを高めるために使われたバイオメトリクスは，現在ではその多くがパスワードよりも簡単に利用できるまでに使い勝手が向上してきており，今後パーソナルな用途も増えていくことが期待される。

Utilization of biometric identification (for example, fingerprint identification) has been increasing. Biometrics is superior to a password or an ID card, which may be forgotten, stolen, or illegally used by others.

Toshiba has already developed finger feature verification and face recognition technologies. Recently, we have also developed speaker recognition, dynamic signature identification, and biometric system technologies.

Personal usage of biometrics will continue to increase because many biometric system technologies are becoming easier to use than previous systems or the use of passwords.

1 まえがき

指紋認証，音声，サイン(筆跡) などのバイオメトリクス(biometrics：生体測定法) を用いて本人認証を行う方式が最近注目されている。従来の，パスワードやID(IDentification) カードを用いる方法と比べて，忘却，紛失，盗用による不正アクセスの危険性が低いことが特長である。

バイオメトリクスによる本人認証が有望視されている背景には，ネットワーク上での電子商取引など，取引き相手の“顔が見えない”状況における本人認証処理が重要視されるようになったことや電子化された機密情報の管理を厳しくしたいという要求が出てきたことがまず挙げられる。それらに加えて，パソコン(PC) のユーザー確認をバイオメトリクスで簡単に行わせるという用途も増えていることが注目される。

当社は，すでに指関節表面のしわ特徴に基づいた指照合技術と，顔画像による本人認証技術を開発している[(1),(2)]。ここでは，これらの本人認証技術に加えて，新たに開発を進めている，音声およびサイン(筆跡) による本人認証技術と，それらの応用システム技術を紹介する。

2 バイオメトリクス技術

いくつかの有望な本人認証技術があり，状況に応じて使い分けることが行われている。表1は主な本人認証技術の特徴を比較したものである。

表1．主な本人認証技術
Major biometric identification technologies

方式	技術	特徴	
		長所	短所
記憶	パスワード	費用も掛からずシステム構築が容易。	忘却，盗難の危険性がある。
所有物	磁気カード ICカード	使い勝手がよく，高機能。	紛失や，他人に使用されるおそれがある。
バイオメトリクス	指紋	高精度で，技術の認知度が高く，高普及率。	抵抗感をもつ人がいる。乾燥や手荒れで登録しにくいことがある。
	指照合	小型，薄型，軽量。	指全体をセンサに接触させる必要がある。
	手形	使用環境の変化に頑健。実績がある。	手全体が入る大きさの装置が必要。
	顔	汎用のカメラが利用可能。リアルタイムで認証可能。	認証精度が照明の変化の影響を受けやすい。
	網膜	高精度。実績が豊富。	目を接近させる抵抗感をもつ人がいる。
	虹彩	高精度。非接触。	虹彩画像を拡大する光学系が必要となる。
	声	電話のマイクで利用可能。暗やみでも利用可能。	騒音のある場所では使いにくい。
	サイン	抵抗感がない。個人情報端末機器に適合。	ペンが必要。

指や手の部分を用いた本人認証技術が多く利用されているが，なかでも指紋認証は普及が進んでいるバイオメトリクス技術である。一般的な光学式指紋認証装置は，指先をガラスに置いて内側から光を照射して指紋画像を取得し，特徴点が一致するかどうかで認証を行う。

指照合技術は，一次元的に配列された電極センサに指の

手のひら側を押し当てて指表面のしわ形状(通常の指紋照合とは異なる)を計測し認証を行う方式である[1]。指紋の薄い指でも認証できることや，光学系を用いないことによる小型・軽量・薄型化を実現していることが特長である。

非接触で本人認証する技術として，顔画像，網膜の血管パターン，虹彩(アイリス)などを利用したものがある。なかでも，顔画像による認証技術はPCに接続した汎(はん)用の小型ビデオカメラで手軽に利用でき，普及しつつある[1]。動画像からリアルタイムで顔領域を検出するとともに，相互部分空間法と呼ばれる複数枚画像を利用した認証技術によって，顔の向きの変化や表情変化に対しても高い認証精度を得ることができるようになっている[2]。顔画像による本人認証は，手に荷物を持ったまま，あるいは歩きながら認証できるという特長があり，また，顔を撮られて記録されることが不正侵入に対する抑止効果を生むと考えられる。

生体の動き(発声，動作)を用いた識別方式として，音声，サイン(筆跡)による本人認証技術がある。音声による認証技術は，マイクが小型・安価であることや，電話で利用できることなどのメリットが大きい。サイン認証は，ペン入力の個人情報端末のユーザー確認などに適している。

3 音声を用いた本人認証

3.1 音声を用いた本人認証の特徴

音声を用いた本人認証手法は，発声する内容を限定する発声内容依存手法と，発声内容として任意の発声を許す発声内容独立手法に大別される。定められたキーワードを発声した際の認証精度は発声内容依存手法の方が優れているが，発声内容依存手法では発声内容を事前に予測することができない音声，例えば電話対話中の音声などを扱うことができない。

当社では，幅広い分野に応用することができる発声内容独立手法の開発を行なっている。処理の流れを以下に示し，各処理に関して説明する(図1)。

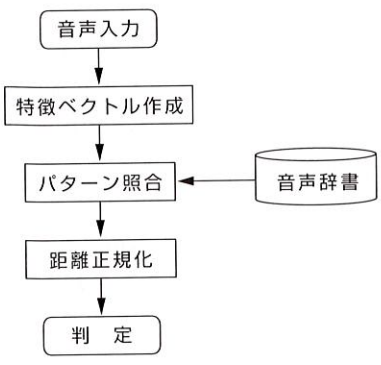

図1．音声による本人認証処理の流れ　音声から特徴ベクトルを作成後パターン照合し，距離正規化処理で距離値の補正を行う。
Flow of speaker recognition process

3.2 特徴ベクトル作成

音声を短い時間に分割し，LPCケプストラムと呼ばれる特徴量に変換する(LPCケプストラムは音声認識技術で一般的に用いられているものである)。

3.3 パターン照合

作成された各特徴ベクトルに対して音声辞書との距離を算出する。辞書の構造として，少ない音声データからも比較的良好な音声辞書が作成できるという特徴をもつ，VQ(Vector Quantization)符号帳を採用している。符号帳サイズをMとし，M個のベクトルの符号帳をy_m $(1 \leqq m \leqq M)$とする。入力音声の特徴ベクトル数をNとし，i番目の特徴ベクトルをv_i $(1 \leqq i \leqq N)$とすると，音声と符号帳の距離xは以下の式で算出される。なお，式中の距離関数dにはユークリッド距離(v_iとy_mの各ベクトル成分の差の二乗和)を採用している。

$$x = \sum_{i=1}^{N} \min_{1 \leqq m \leqq M} d(v_i, y_m)$$

3.4 距離正規化

音声による本人認証において，閾(いき)値を適切な値に設定することは簡単ではない。周囲の環境雑音や発声内容の違いにより，音声辞書との距離値が異なってくるので，一定の閾値では，さまざまな環境で高い認識精度を維持するのは難しい。ここでは，本人の辞書以外に他人の辞書との距離を算出し，それらの距離を用いることで距離値の正規化を行なっている。正規化の効果で，認識精度は5%以上向上することが実験で確認されている。

3.5 評価実験

50人の男性話者を対象として評価実験を行なった。音声辞書作成には約15秒程度の音声データを用いた。評価時には1秒弱および5秒程度の音声データに対して本人であるかどうかの判定を行なった。なお，音声はすべて同時期のものを用いており，時期差は存在していない。

認識精度は，他人受入率と本人拒否率が等しくなるように事後に閾値を設定した条件では，1秒弱の発声に対して6.0%，5秒程度の発声に対して0.8%となった。この結果は，この手法の長い発声に対する有効性を示している。

なお，このシステムは現在PC上で動作している。CPUにPentium®(注1)プロセッサ(233MHz)を搭載したPC上で，認証はリアルタイムで，辞書作成は発声終了後数分で行うことができる。

4 サインによる本人認証

4.1 サイン認証の特徴

サイン(署名)は，クレジットカードやチェック使用時の

(注1)　Pentiumは，インテル社の商標。

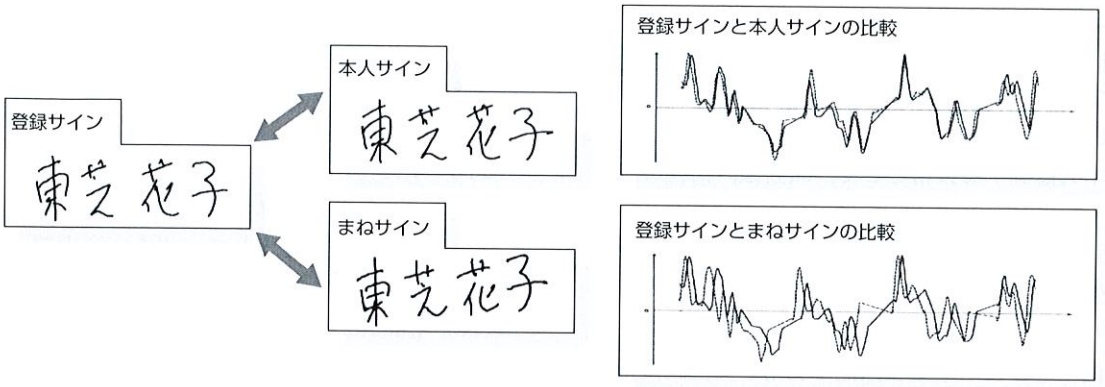

図2．オンラインサイン認証の基本的しくみ　運筆情報を考慮した判定をするため，サインの偽造は難しい。
Comparison of standard signature and input signatures

本人確認手段として，日常的に利用されている。また，欧米では公的書類の“承認印”としてサインが利用されている。計算機を利用した自動本人認証においても，このように社会的認知性の高いサインを利用したい，と考えるのは自然な発想である。

計算機によるオンラインサイン認証では，タブレットと呼ばれる座標入力装置を利用して，ペン先の二次元座標値の時間変化情報や，ペンの筆圧情報，傾き情報などを取得し，これを認証に使用する。サインの形状をまねすることはできても，これらのペンの動きまでまねをすることはきわめて困難なため，紙に書かれたサインを認証する場合と比較して，より高精度な認証が可能になる。

また，通常のいわゆる“署名”に限らず，本人しか知らないパターンを使うことで，パスワードのような秘密情報に基づく認証の性質をもたせることもできる。例えば，サインの一部の筆順を意図的に変えるだけでも，いっそうセキュリティを向上させることができる。

最近は，ペン入力インタフェースを標準搭載した情報機器も多い。これらの機器においては，サイン認証により安価に本人認証を実現することができる。

4.2　オンラインサイン認証方式

サインの認証は，入力サインデータと，登録サインデータを比較照合することにより行われる。

図2は，登録サインデータと，本人サインデータ／他人がまねをしたまねサインデータについて，x座標の時間変化を示したものである。横軸は時間で，縦軸は前処理により正規化された座標値である。

登録サインの波形が，入力サインの波形にもっともよく一致するように，登録サインの時間軸を非線形伸縮し，そのときの相違度があらかじめ定めた閾値よりも小さい場合には本人のサイン，大きい場合には他人のサインであると判定する。

実際には，y座標情報，ペンの筆圧や傾き情報などの時間変化波形も照合に利用することにより，高精度な認証が可能になる。

ただし，サイン認証精度は，サインそのものの複雑さ，筆順などの書き方のくふう，サインの秘密性に大きく影響されるため，認証アルゴリズムの高精度化はもちろん，運用時のくふうも非常に重要である。

5　バイオメトリクス応用システム

音声やサインなどのバイオメトリクスのもっとも身近な応用は，PCのユーザー名とパスワードを入力する場面への適用であろう。ログオンや画面ロック解除をバイオメトリクスにより簡単に行うことができれば便利である。ほかに，ファイルの暗号化やアプリケーションソフトウェアの起動時のユーザー確認にも適用される。

バイオメトリクス技術の利用は，単純に，パスワードを高度化したいときに導入するものと考えればわかりやすい。しかし，見かたを変えて，本人認証の手段が同一システム上で複数存在し，それらの組合せを統一的に扱うフレームワークの策定に特徴があると考えることもできる。つまり，複数の本人認証技術の扱いかたを管理する必要が生ずるのである。例えば，パスワードと音声認証を併用する場合，それらを両方必須(す)とさせるか(AND)，どちらか一方でアクセスを許可させるか(OR)ということを決めたり，また，同一ユーザーがモバイルにおいてサイン認証を利用し，オフィスでは別の本人認証技術を用いるという使い分けを行うことにより，バイオメトリクスを有効活用できる。

ICカードにバイオメトリクスの登録データを記録してバイオメトリクス装置を利用する場合の認証システム構成の一例を図3に示す。バイオメトリクスにICカードを組み合わせる目的は，バイオメトリクス登録データの記録媒体と

してのICカードの利用，ICカードの所有者確認を目的としたバイオメトリクスの利用，さらには他のICカードアプリケーションシステムへのバイオメトリクスの導入などである。双方に証明書をもたせることにより，多数のICカードを発行したり，バイオメトリクス装置の入替えなどに柔軟に対応し得るシステム構築が可能となる。

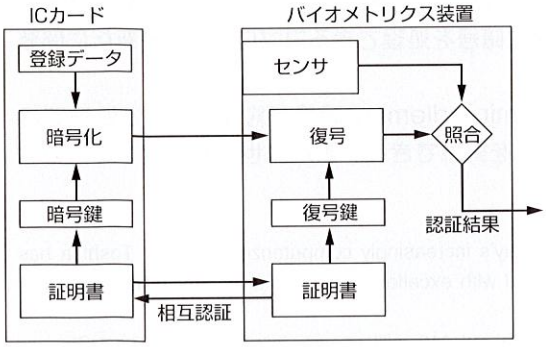

図3．ICカードとバイオメトリクスのシステム構成　通信経路上の暗号通信が登録データを盗聴から守る。
Configuration of smart card and biometric system

6 あとがき

音声およびサインによる本人認証技術が，新たなパターン認識アルゴリズムの開発により実用化の段階を迎えた。また，これらのバイオメトリクス技術を利用した応用システムの構築も進められている。

かつては指紋や網膜などのバイオメトリクスを利用するのは厳重な警備が必要な場所であったが，最近ではパスワードよりも簡単で便利であることが各種のバイオメトリクスのメリットと言えるようになってきた。バイオメトリクス技術に対して高精度であることはもちろん，ユーザー側から見た使い勝手の良さがますます求められている。

今後，電話には音声本人認証，ペン入力機器にサイン認証など，機器の特性に合わせた本人認証技術が適用される機会が増えていくであろう。

文　献

(1) 岡崎　彰夫，他．個人識別技術への取り組み．東芝レビュー．52，2，1997，p.8-13.
(2) Yamaguchi,O., et al. "Face Recognition using Temporal Image Sequence" IEEE 3rd International Conference on Automatic Face and Gesture Recognition, Nara, 1998, p.318－323.


山田　貢己　YAMADA Miki, D.Sc.
情報・社会システム社 SI技術開発センター SI技術担当主務，理博。情報セキュリティ技術の開発に従事。電子情報通信学会，日本神経回路学会会員。
System Integration Technology Center


出口　豊　DEGUCHI Yutaka
研究開発センター ヒューマンインターフェースラボラトリー。音声認識および話者認識技術の研究・開発に従事。情報処理学会，音響学会会員。
Human Interface Lab.


河村　聡典　KAWAMURA Akinori
デジタルメディア機器社 パーソナル＆マルチメディア開発センター 開発第四部主務。文字認識，ペン入力要素技術の研究・開発に従事。
Personal & Multimedia Development Center