# 3. 虹彩による本人認証

沖電気工業（株）システムソリューショングループ
塚田 光芳

## ❑ 虹彩の特徴 ❑

個人識別のためのバイオメトリクスとして，掌形，網膜，指紋，声紋，手で書く署名等が長年に渡って研究されてきた．このようなバイオメトリクスの重要な特性は，そのバイオメトリクスに個人のユニーク性の存在，時間や環境による不変性と他からの無干渉性，パターンの効果的なコード化と信頼性ある同一パターンの認識性である．眼の虹彩が，個人を識別するために一種の指紋のように使える可能性があるということは，元々は眼科医によって提唱されたものであると伝えられている．眼科医は診療経験から，すべての虹彩が非常に精細かつユニークな組織を持っており，診療写真を見るとそれが何十年もの間変化しないでそのままの状態に保たれることに注目したようだ．

このような特徴を持つ虹彩と指紋の共通の特性から，J. G. Daugmanは，個人間の虹彩におけるバリエーションの形成の数学的証明を行い，虹彩画像から詳細な特徴を引き出すためのイメージ解析アルゴリズムを開発した[1]．このアルゴリズムは，人物の顔のライブビデオイメージの中の虹彩を取得し，その画像をエンコードして虹彩コードを得る．コード間における判定は，統計的な決定理論と信号処理法を使い，任意の２つの虹彩コードの排他的論理和（XOR）から計算されるハミング距離（HD: Hamming Distance）に基づいて行われる．

虹彩は高度にランダムかつ複雑でユニークな組織であり，人間の一生に渡って不変であることが知られている．同じ遺伝子を持つ一卵性双生児のみならず，同じ人でさえ両眼の虹彩のパターンはまったく異なる．虹彩は眼の透明な角膜と房水の後方にある内部器官であり，外部環境から隔離・防御されているが，1m程度離れた位置からでも容易に観察できる．虹彩は外光に反応して瞳孔の大きさを調節するために伸長および収縮するが，そのパターンは伸長および収縮してもほとんど変わらず，虹彩認識が潜在的に持つバイオメトリクスとしての優れた特徴の１つになっている．

## ❑ 虹彩認識プロセス ❑

虹彩自動認識の大きな特徴は，利用者に押し付けがましくない方法で，高品質な虹彩画像を取得し，高速で認証できることであり，その過程が**図-1**に示されている．システムはカメラの前に立つ利用者の頭／顔を広角カメラにより自動撮影し，利用者とカメラ間の距離zと同時に，この広角カメラ画像から眼の位置（x, y）を計算する．狭角カメラは計算した眼の位置（x, y）を目標に位置決めされ，さらにz方向の距離合わせのズーム機能を使って虹彩画像を取得する．このように広角カメラと狭角カメラとの連動により，カメラの前に立つ利用者を制約することなく適切にフレーミングすることができ，虹彩の自動取得が可能となる．一方，この広角カメラを省略したシステムでは，利用者が狭角カメラのモニタに映る本人の眼を確認しながら虹彩画像を取得する．これによりシステムの簡素化，小型化，低価格化が実現できる．

さて，図-1のステップ１において，システムは取得された虹彩とそのまわりの画像から，イメージ輝度の変化を利用して虹彩の強膜側境界，瞳孔側境界，上下瞼側境界を決定し，虹彩領域を特定化し虹彩画像のみを切り出す．**図-2**に示すように，システムは切り出された虹彩領域に８つの環状解析ゾーンを割り当てる．特に，虹彩の上下部が上下瞼により頻繁に閉じられデータを曖昧にするため，これらの領域は解析および虹彩コード化から除外される．このようにして解析のためのイメージ領域が正確に決定された後，虹彩コードを生成するためにそれぞ

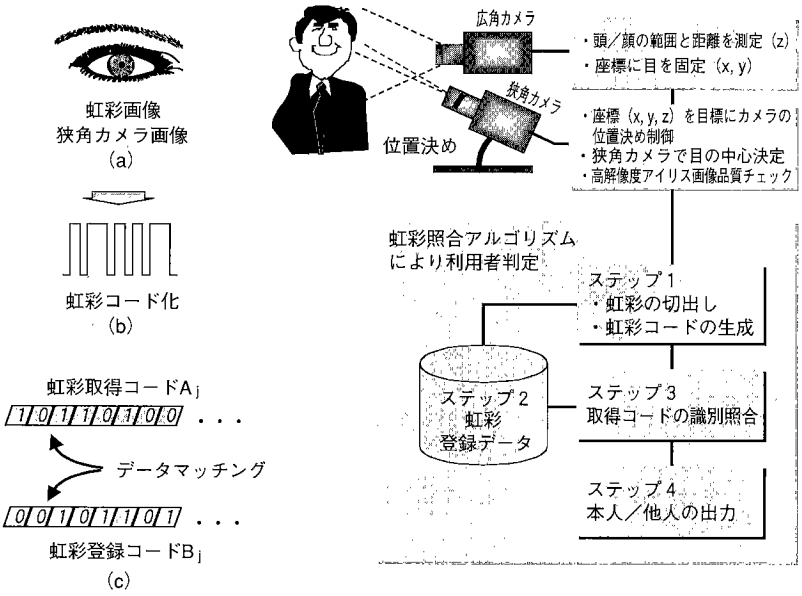



図-1　虹彩認識プロセス

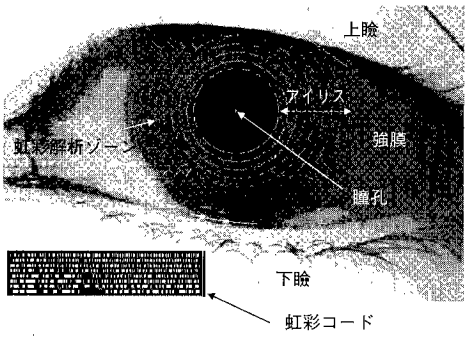



図-2　虹彩画像の解析

れの環状解析ゾーンを走査して，極座標の関数としてイメージ輝度（濃淡変化）抽出を行い，当該ゾーンの虹彩データをコード化する．このようにして得られた8つの環状解析ゾーンをコード化した2,048ビットの虹彩コードデータの一例が図-2に示されている．これはそれぞれ同心解析ゾーンに渡って計算された8ビットを有する256個の角度列として表示したものである．以上の工程でコード化された虹彩データは，システムのデータ登録制御により登録部に利用者の属性データとともに登録される（ステップ2）．次に，ステップ3において，上記の工程と同様な方法で取得された虹彩の取得データと，登録データが照合される．照合は2つのコード$A_j$，$B_j$間の類似度を，ハミング距離HDと呼ばれる式（1）で定義された尺度で評価される[2]．

$$HD = \frac{1}{2{,}048}\sum_{j=1}^{2{,}048} A_j \left(XOR\right) B_j \qquad (1)$$

このHDは2つのコード$A_j$，$B_j$のビットが完全に一致した場合はHD＝0，すべてのビットが不一致の場合はHD＝1になる．そして，HDがある一定の値より小さい時に両コードは同一のコードと見なされ，ステップ4においてシステムは利用者を本人であると出力する．

本人同士の場合，理想的には，イメージが真に同一ならば，これらのハミング距離はゼロでなければならない．しかしながら，凝視角度の差，部分的な瞼の閉鎖状態，角膜からの鏡面反射，および瞳孔の相対的な収縮によってコード化された構造における若干の差が生成される．

**図-3**に異なる時間に得られた同じ虹彩の異なるイメージの1,208対において計算されたハミング距離の分布（“本人”）と，異なる虹彩イメージの2,064個の計算されたハミング距離の分布（“他人”）のエラー率を共に示した．等価エラー率（Cross-over Error Rate）が131,000分の1の値で[2]，これは虹彩の個人識別特性が高いことを示している．

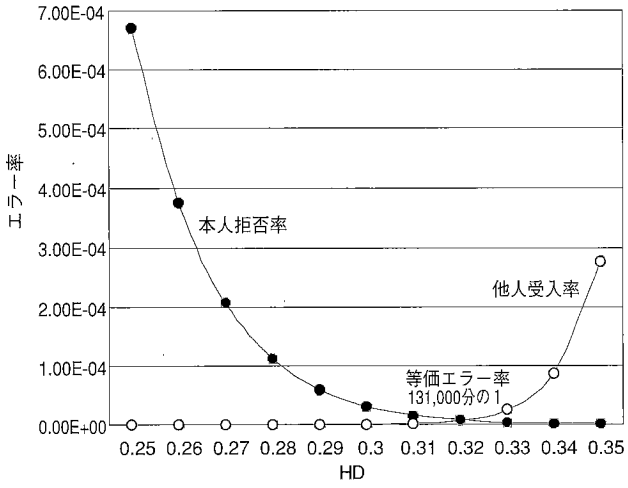



図-3　HDでみた虹彩の個人認識特性

| 市場セグメント | 錠／鍵 | コンピュータアクセス | 身分証明 | 資格／ライセンス |
|---|---|---|---|---|
| 金融市場 | 営業店鍵管理，貸し金庫，ATM後扉，他 | コンピュータN/W，RBT，HB/FB，ATM，電子商取引，口座アクセス，他 | 出退勤管理，他 | |
| 企業 官公庁 市場 | 施設ゲート／入退室管理，防犯／防盗／防事故管理，貸し金庫，研究施設，原子力施設，電力施設，病院，防衛施設，他 | コンピュータN/W，自動契約機，ATM，POS，KIOSK端末，クレジットカード決済，無人局，基地局，危険物倉庫，他 | 自治体住民情報，出入国管理，学生証，社員証，パスポート，搭乗券，受験票，投票権，他 | 医師／弁護士登録，外国人登録，運転免許証，犯罪者登録，他 |
| その他市場 | 自動車キーレスシステム，他 | コンピュータN/W，電子承認（稟議，各種承認），他 | レジャー施設／テーマパーク，他 | |

N/W：ネットワーク，RBT：リモートブランチターミナル
HB/FB：ホームバンキング／ファームバンキング

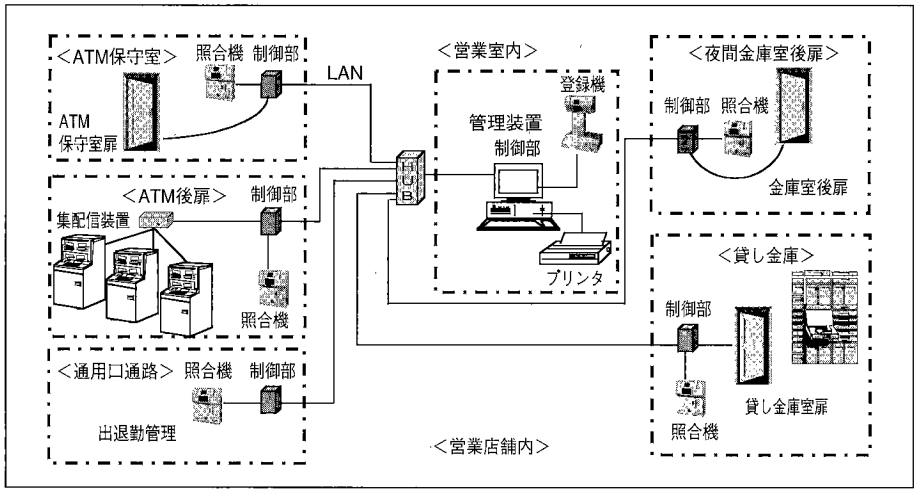
図-4　バイオメトリクス認証システムの応用市場

## □ バイオメトリクス認証の利用法 □

本人認証手段として圧倒的に多く利用されているものがIDカードまたはパスワードである．しかし，システムとして，不正アクセスを絶対に許さず，厳重性を優先させたハイセキュリティ指向のアプリケーションに対しては，現行の方式による本人認証は機能不十分で，きわめて高精度に本人認証を行うことのできるバイオメトリクス認証システムが必要である．**図-4**は本人認証の社会的要請を踏まえ，想定されるバイオメトリクス認証システムの応用市場を図解したものである．アプリケーションとして錠／鍵，コンピュータアクセス，身分証明，資格／ライセンスの4つの分野に大別される．それぞれの分野に対して対象となる現行の仕組み，システムを市場ごとに示した．この中で市場は小さいが最も導入の容易なシステムは，物理的鍵の代替となる入退室管理システムである．しかし，現行では一部のシステムに指紋照合等のバイオメトリクスが利用されているに過ぎない．一方，これから大きく発展する市場はコンピュータアクセス市場である．世の中のあらゆる仕組みがコンピュータネットワークを介したシステムとして構築されると，企業内，企業間のコミュニケーションを脅威から守る手段として，イントラネット，エクストラネットへのバイオメトリクス認証の適用が進んでいくものと考えられる．

特に金融機関は，国の経済活動はもとより国民生活全般に深く関与しており，高い公共性と社会的重要性を担っている．したがって，金融機関のコンピュータシステムの犯罪・トラブルが与える社会への影響は，他の産業にくらべひときわ重大である．このため，従来からコンピュータルーム等の重要施設への入館・入室には，テンキーによる暗証打鍵やIDカードが利用されてきた．しかし，

アイリスパスーSゲート管理装置による金融営業店向け鍵管理ネットワークシステム




HUB（ハブ）：LANの集線装置

**図-5　金融機関営業店での適用例**

出入りする関係者数および入室頻度の増大とともに，暗証打鍵の誤入力や，第三者への暗証番号の漏洩の対策が課題となっている．また，IDカードの発行枚数が増加するとともに，その維持・管理および安全対策のために多大な労力が必要となっている．一方，銀行の各営業店舗では，大金庫をはじめとして，約四十種に及ぶ業務用の物理的鍵が運用され，誰が，いつ，いかなる鍵を，何の目的で使用したかが管理されている．しかし，個々の鍵の管理や紛失などに対する安全性の面から，これらの物理的鍵の管理をなくし，それに費やす日常の人的負荷を削減したい要求がある．このような課題のソリューションとして，沖電気の金融営業店向け鍵管理ネットワークシステム（アイリスパスーSゲート管理装置）がある．**図-5**にそのシステム構成例を示すように，営業室に管理装置を配し，ATM後扉およびその保守室，貸し金庫，夜間金庫室，出退勤管理等をゲートアプリケーションとしてネットワーク構築している．営業室内の管理装置は，利用者の登録台帳管理，各錠の状態監視／制動部制御，履歴収集／管理等の機能を持ち，ATM後扉等のゲート装置は入室認証，履歴収集の機能を備えている．その他にこの鍵管理ネットワークシステムは，利用者の許可錠や許可曜日，許可時間等の設定，さらに解錠状況や警報機作動等の履歴収集の一元管理が可能で，各錠の状態監視を一括リアルタイムに行い，6カ月間保持できる収集ログを登録者や錠，日時ごとにまとめるなどさまざまなフォーマットで出力することが可能である．

さて，銀行業務そのものの信頼性と，組織全体の健全性を守ることを徹底原則とする営業店の中で，特にATMの現金詰替え業務は，銀行独自の方針のもとに，ATMへのアクセス権限を持つ複数人が共同で行い，安全かつ厳格で一貫した管理がなされている．このATM後扉の物理的鍵の代替として虹彩による認証を行うことで，現金詰替え業務を1人で済ませることが可能になる他に，営業室内の管理装置を通して，リアルタイムですべてのATMの運用状態（虹彩ログ，取引状態，現金金種残，媒体残，等）を常時確認できるため，今までにないセキュリティ上の厳格性を持たせたATMの運用管理が可能となる．

また，その他の特徴あるアプリケーションとして貸し金庫がある．貸し金庫サービスは営業店サービスと多少趣が異なり，顧客の自主的利用を目的としたプライバシーを尊重すべき性質のサービスであり，ほとんどの営業店に常設されている．しかしながら，多くの貸し金庫は，顧客が来行のたびに銀行鍵を持った行員が付き添い銀行錠を解錠し，顧客も契約錠で解錠するダブルチェック運用の貸し金庫システムである．この銀行錠および顧客の契約錠の解錠を顧客の虹彩照合に代替するシステムでは，顧客が単独で，誰にも拘束されることなく，自由な時間に自分の契約金庫にアクセスできるようになり，顧客のプライバシーを保護することが可能となる．

このように，虹彩による本人認証に代替することで，営業店業務の省力化やコスト低減等を達成し，営業店の業務プロセスの改善にも効果のあるセキュリティシステムとなる．

**参考文献**

1) Daugman, J. G.: High Confidence Visual Recognition of Persons by a Test of Statistical Independence, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.15, No.11 (Nov. 1993).
2) Daugman, J. G.: Oki Electric Industry Co. Ltd. Sensar Inc., High Confidence Personal Identification by Iris Analysis: 14th Meeting of the International Association of Forensic Sciences (IAFS), Tokyo (Aug. 26-30 1996).

(平成11年6月22日受付)