連　載

都市小屋 集の ICカード研究会 202

虹彩を使った生体認証

企業では、従業員のノートパソコンやスマートフォン、タブレットなど私物のデバイスを業務に活用する「ブリング・ユア・オウン・デバイス（BYOD）」が広がりをみせている。会社の保有するデータへのアクセスが容易になるなど従業員の業務効率が向上する一方で、スマートフォンからの情報漏えいも起きているため、セキュリティリスクが懸念されている。こうした課題に対応する技術の1つが生体認証（バイオメトリクス）だ。今回は、目の虹彩（アイリス）を活用した認証システム「IrisKey（アイリスキー）」を手掛けるクリテックジャパンの對馬一彦氏に同製品の特徴や虹彩の生体認証の可能性などについて語ってもらった。

1．虹彩とは

虹彩とは、黒目と白目の間にあるこげ茶色などの色をおびたドーナツ状の部分を指す。色は人種により異なり青、緑、灰色など虹のように多様なため「虹彩」と呼ぶ。この模様は1人ひとり皆違う。DNAが同じ一卵性双生児でも異なり、同じ人物でも右左では異なる。2歳以降は一生パターンが変わらないとされている。

眼の水晶体の前にある筋肉組織でできているヒダの部分が虹彩だ。明るさによって瞳孔が大きくなったり小さくなったりするのは、虹彩が動いて起きる現象で、原理的にはカメラのレンズの絞りと同じ役割を果たしている。

2．虹彩認証の歴史

1986年、米国の特許庁に眼科医が「虹彩は人によってすべて違う」ということを出願して特許を取得。しかし、眼科医は特許を実用化できないため、英国ケンブリッジ大学のジョン・ドーグマン教授に虹彩認証システムの開発を依頼した。その後、ドーグマン教授が極座標を使った虹彩情報のコード化に成功し、虹彩アルゴリズムの特許を取得した。

その後、米国IRIDIAN社がこの特許を管理して市場を独占。IRIDIANからライセンス供与を受けた沖電気やパナソニック、韓国のLGなどが認証技術の開発に着手していった。

▲クリテック 代表取締役社長・對馬一彦氏

3．ドーグマン教授VSクリテック

現在、虹彩認証技術の99％でドーグマン教授のアルゴリズムが採用されており、これがデファクト･スタンダードになっている。このアルゴリズムは虹彩部分に8つの同心円を描いて、その同心円上の濃淡情報をフィルタリングしたり、ノイズを取るなどして、1と0の信号にしたもの。

ただし、このアルゴリズムと活用技術には2つの問題点がある。1つは、虹彩の同心円上からデータを抽出しているため、目が細い東洋人は上まぶたが下がって認証しにくいこと。2つ目は、初回登録時と認証時でモジュールを設置した周囲の明るさが変化すると瞳孔の大きさが変わってしまい、上手く認証できないことである。

クリテックではこの問題を数年かけて研究・改良し、全く新しいアルゴリズムを作成した。まず、瞳孔の上部と

図1　従来の虹彩認証

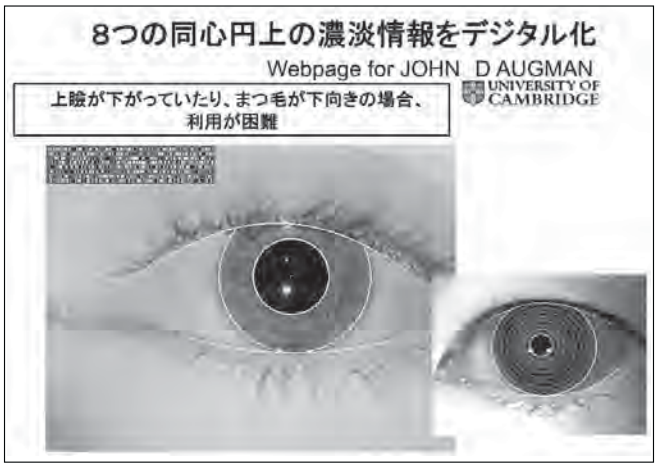
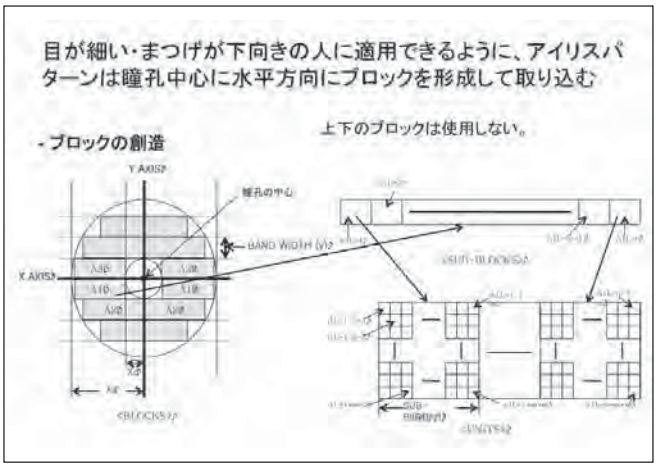


図2　クリテックのアルゴリズム（ブロックパターン方式）



下部を除いた中心部を横軸に切って特徴点を抽出し、上まぶたやまつ毛の影響を受けにくいように改良した。

登録時と認証時の明るさの違いで虹彩の模様が変わって認証できない問題には、虹彩データ登録時にさまざまな明るさの光をあてた画像を複数枚登録することで回避している。また、システムを運用していく段階で、さらに大小さまざまな虹彩映像を追加学習して、8枚程度のテンプレートを使うように設定している。どうしても認証できない場合には、登録時と同じ光をあてて環境を整え、認証している。

4. クリテック社製品の特徴

2011年12月にリリースした主力商品の「アイリスキー」は、非常に小型の基盤とカメラで構成されている。カメラで撮影した虹彩画像から特徴点を抽出してテンプレートを作成し、データを保存することまでが可能だ。認証時はモジュール内で処理しているため、PCがなくても運用できる。

従来の虹彩認証機器では、データをモジュールからPCなどへ送って処理しなければならなかったため、なかなか製品コストが下がらなかった。当初は1扉で100 ～ 150万円程度、最終的には30万円程度まで値下げされた製品もあったが、太陽光のあたる屋外では使い勝手が悪いこともあり、あまり売れなかったようだ。国内の大手メーカーは、この事業から撤退してしまった。

クリテックの製品は虹彩を識別するモジュールが格納されているだけのシンプルなものだが、Windowsのログオンにも使える。PCにアカウントを設ければそのまま認証に使えて、人数分の虹彩を登録するだけで10人でも20人

図3　クリテックの虹彩認証製品

図4　OEM　虹彩認証エンジンモジュール

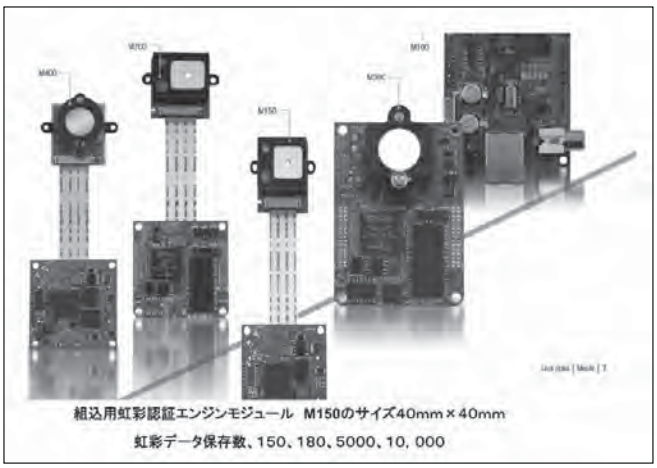


図5　虹彩のパターン変化

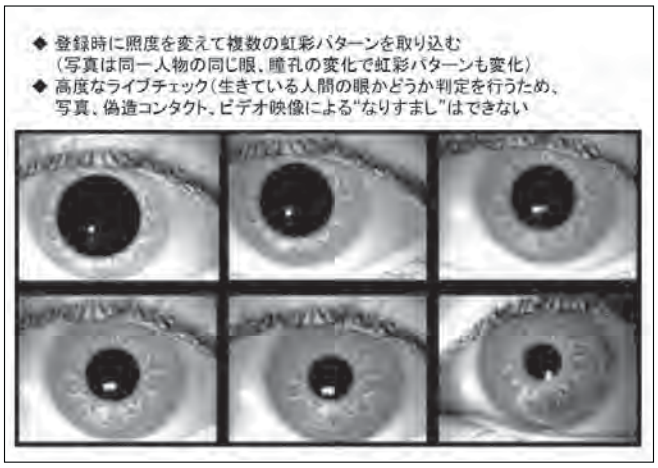


図6　各種生体認証方式の比較

認証方式	不変性	安定性	耐偽造性	精　度	コスト	特徴の情報量
指紋認証	△	△	△	○	◎	○（10の12乗）
静脈認証	○	△	△	○	○	○
掌形認証	○	○	△	△	△	△
顔認証	△	△	△	△	△	△
虹彩認証	◎	◎	○	○	△	◎（10の78乗）
クリテックの虹彩認証	◎	◎	◎	◎	◎	◎（10の78乗）

でも1台のPCを共用できる。虹彩認証の方法は、モジュールを顔から10㎝程度離してカメラレンズ（凹面鏡）を見るだけ。ピントが合うと「ピピッ」という音がして、0.3 ～ 0.5秒で認証することができる。

このように認証速度が非常に早いというのも特徴だ。1対1というのは、認証する人と登録データがそれぞれ1人しかいないもので、これは約0.3秒で認証する。1対nというのは、不特定多数の虹彩データと比較するものだが、認証時間は約0.5秒。虹彩が生きている人間のものかどうかのチェック機能を組み込んでいるため、なりすましの防止にも対応している。

虹彩データのセキュリティ面では、ハッキングに対抗するためのオプションとして、AESによる暗号化も可能だ。また、虹彩情報の自動学習機能を搭載しており、認証作業で使い続けていく過程では、常に画像を更新していくため、認証の精度向上と認証時間の短縮を実現している。

登録時や認証時の周囲の明るさの調整のため、製品は50 ～ 1万ルクスまでの照度に対応しており、一般的な環境ではほぼ問題なく運用が可能だ。さらに、この登録方法は、虹彩は明るさに応じて常に動くという特徴をとらえたものであるため、赤外線写真やコンタクトレンズなどには反応せず、なりすましを防ぐ効果もある。つまり、光が当たっても動かない虹彩はもともと登録できない仕組みで、生きている人間の虹彩でなければ認識しない点も大きな特徴だ。

ただ、静脈認証と同様に近赤外線照明を使用するため、認証機器を設置する環境面で太陽光の影響を受けやすく屋外で使いにくいという問題と、カメラが固定焦点のためピントを合わせにくいという問題があり、今後の課題となっている。

5. 生体認証の必要性と課題

そもそもなぜ、生体認証は必要なのか。世の中で個人を認証することは社会の基本的な要件となっている。

クレジットカード、パスポート、自動車運転免許証など本人を証明するものが世の中にはたくさんある。従来の本人認証はカードや鍵、ID・パスワードなどが主流だったが、偽造や詐取でセキュリティが破られるなど問題が出てきているため、本人の身体で確認する必要性が出てきた。

それぞれの認証方式の特徴を比較してみると、パスワードは低コストで正確な認証が可能だが、登録した本人が忘れしたり、ハッキングされたりしてしまう短所がある。印鑑やIDカードでも正確な認証が可能だが、偽造される恐れがあるのが弱点だ。バイオメトリクスで最も普及している指紋や、顔・手の形、静脈などは、忘れない、盗まれない、偽造が難しいという長所が挙げられるが、人体は千差万別で認証できない人もいることが課題となっている。

生体認証の脆弱性ということでは、数年前に横浜国立大学大学院環境情報研究院の松本 勉教授が発表した、指紋や虹彩、静脈を中心とした生体認証のセキュリティ評価実験の結果が物議をかもした。

指紋については、ゼラチンで偽造してほとんどのメーカーの認証技術が破れることが分かった。また、指静脈は大根を指の形にしてサランラップを巻

図7　各種生体認証方式の精度比較

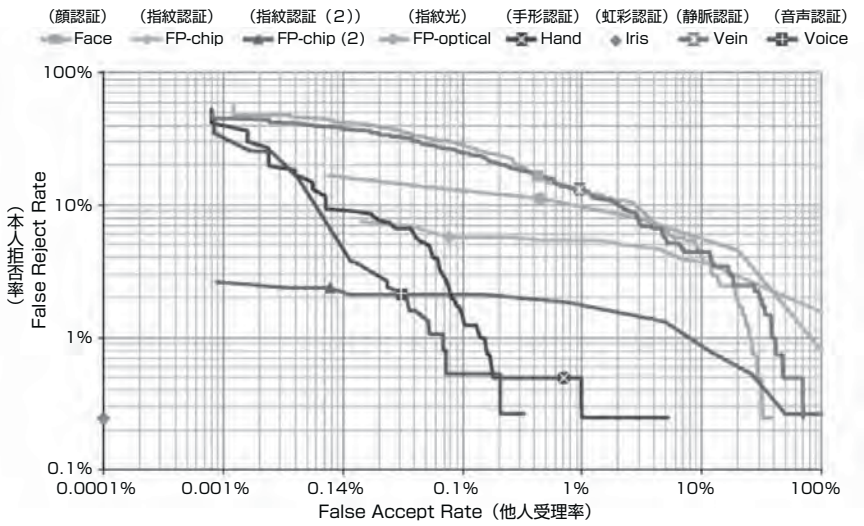


Figure 6. Detection error trade-off: Best of 3 attempts

出典：National Physical Laboratory　Biometric Product Testing Final Report issue 1.0 19 March 2001

いたもので登録できてしまい、認証もできるという結果が出た。手のひら(掌形）についてはプラスチックに模様を書くと登録・認証ができることが分かった。これらの結果は、画像認識できちんとした生体検知ができていないため偽物に騙される、ということを証明してしまったのだ。

6．虹彩認証と各種生体認証方式の精度比較

ここに英国National Physical Laboratory（国立物理学研究所）が発表した各種生体認証方式の精度比の比較データ（**図7**）がある。試験は、顔､指紋(チップ式2種と光学式)､手形、虹彩、静脈と音声の生体を活用したベストプラクティスという方法で行った。そのテスト結果をグラフにまとめたものだ。

グラフでは、他人を誤って受け入れた率「他人受理率（横軸）」が、虹彩認証技術の場合、100万分の1以下であり、他の生体認証技術の精度を圧倒していることが分かる。本人が誤って否認された率を表す「本人拒否率（縦軸)」との間に相関関係が示される。一般的に本人拒否率を下げようとすると他人受理率が上がってしまう傾向を持ち、その逆に他人受理率を下げようとすれば本人拒否率が上がってしまう。

具体例で見ていくと、他人受理率が同じ0.0001％でも、米IRIDIAN社の虹彩認証では、本人拒否率が0.25％。クリテックがサンプルとして集めた4万3000人分の実験データでは、本人拒否率は0.1％とさらに高い精度が示された。

クリテックの実験では、登録した虹彩データとどのぐらい一致したら本人と認められるかの「しきい値」を70にすると、他人受理率は0％で、本人拒否率は0.003％になる。実際に使用する環境での安全性を考慮し、しきい値を78や80まで上げると本人拒否率がそれぞれ0.05％、0.2％に上昇して実用化しやすくなるという結果が出た。クリテックの製品では、この数値の設定は規定値となっているが、一部の機種では求めるセキュリティレベルなどに応じて任意に設定が可能だ。

また、認証する上で虹彩が指紋や顔など他の生体に比較して優れているかは、データ量の多さなどからも分かる。虹彩のデータ量は10の78乗に及ぶ。参考までに、指紋・静脈は10の12乗程度である。さらに、虹彩は経年変化がなく、温度や湿度の影響も受けないため安定性が高い。

図8　虹彩認証の特徴

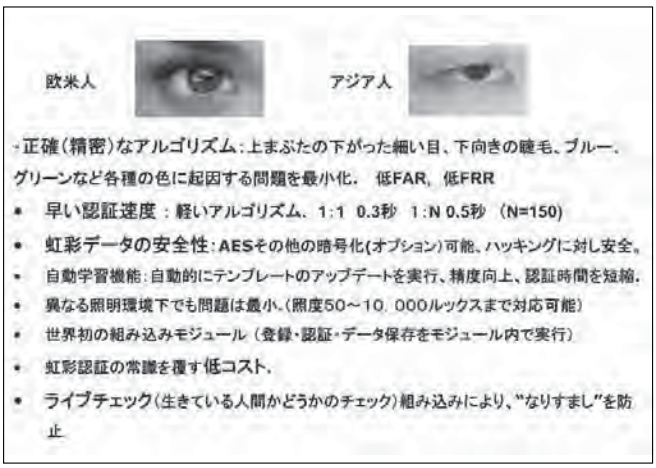


図9　虹彩認証の導入事例①

図10　虹彩認証の導入事例②

7．虹彩認証の適用マーケット

全体的に高精度とされる生体認証の中でも、最も精度が高い虹彩の生体認証のマーケットとしては、重要施設の出入り管理には最適だ。価格が下がってくれば戸建住宅などにも導入できる。

勤怠管理などにも需要があるだろう。飲食店などでアルバイトの勤務時間を管理するため、よく指紋認証を採用しているが、調理場など水仕事する人などは指紋が薄くなってしまい、使えないことも多い。こうした分野では静脈認証が使われていることが多いが、より認証精度の高い虹彩も有効だ。

大きなマーケットでは、情報セキュリティ分野が上げられる。

今はID・パスワードが主流だが、盗難やハッキング、ウイルス感染で機器がのっとられたりするため、パスワードに代わるシステムを検討しないと今後の情報社会では安全確保が難しい。ネットバンクやネット証券など、高額取引をするビジネスにも虹彩認証のニーズがあるだろう。

最近はスマートフォンが爆発的に普及しているが、セキュリティ対策を施さないと、落とした時に社内の情報が漏洩のリスクにさらされる。すでにアップル社が指紋認証の会社を買収しているのは、次に指紋認証つきのiPhoneをリリースする前触れではないかと思う。

公共サービスでは、電子パスポートに需要がありそうだ。国連の下部機関の国際民間航空機関（ICAO）がバイオメトリクス・パスポートの国際的な導入を推進しており、その仕様として生体の顔認証を必須事項とし、虹彩と指紋の認証をオプションとして採用している。

実際に日本でも出入国管理にバイオメトリクスを使おうと、法務省がテストを始めたところだ。生体認証が実用化すれば、将来的には交通ゲートのように、出入国ゲートを無人にできる。

観光立国を目指している日本は、現在年間の訪日外国人旅行者数が800万人程度だが、観光庁では平成32年までに2,500万人を目指している。そうなると、空港設備も職員も足りなくなってしまう。日本人は基本的に出国するときに生体情報を登録して、帰国の際は無人ゲートで認証されれば入国できるようにしようとしているようだ。

このほか、社会保障サービスの提供や徴税を適切に行うため、国民全員に番号を割り振る「共通番号（マイナンバー）制度」が始まるが、カードを持っている人が本人だということを証明するために顔写真と指紋や虹彩情報を入れておけば、身分証明になるのでここにも市場があるとみている。このカードと虹彩認証を組み合わせると、ほとんどの行政サービスを自宅に居ながらにして受けられる。インターネットでの選挙投票も将来は可能になるかもしれない。

8．世界で進む虹彩認証の導入例

先進的な取り組みとしては、米国で歩行者の虹彩認証が開発されている。ゲートの中を通るだけで、虹彩認証をしてしまうというものだ。米国企業がFBIやCIAに認証システムを納入していて、空港への採用も計画されているようだ。

映画「マイノリティ・リポート」では殺人事件ゼロの未来社会が実現し

ているが、虹彩で誰がどこを歩いているか分かってしまうという恐ろしい世界が描かれていた。しかし、実社会の話になるのもそう遠くないといえる状況になっている。

アラブ首長国連邦の17の国際空港では、外国人の入国は虹彩認証を必須としている。労働者の大半は外国人で、犯罪者などを入国させないための仕組みだ。導入から10年が経過しているが、のべ2,000万人を認証しており、今まで誤認証は起きていないという。

インドでは、12億の全国民のバイオメトリクス（虹彩、指紋、顔）のデータベースを作ろうとしている、識字率の低いインドでは、食料の不正受給が多発しているため、これを防ぐ目的で構築をするという。米国、英国、オーストラリアでも大規模バイオメトリクスデータベース構築の動きがあるといい、世界的にバイオメトリクスのデータベース構築はトレンドのようだ。

9. クリテック社製品導入事例

われわれの虹彩認証システムは、総務省が沖縄県で自治体や琉球大学などと進めている情報通信技術（ICT）を活用した植物工場「中城デージファーム」（沖縄県中城村）で、無菌状態を保たなければならない工場内の入退室管理に3台導入されているほか、サーバー用のプログラムソフト制作会社「ステラクラフト」（東京都千代田区）の入退室管理にも使われている。

ステラクラフトの入居するビル全体は、三菱電機の防犯と綜合警備保障のシステムが入っており、会社の出入口にはセコムの入退室カードシステムを整備しているが、さらにわれわれのシステムを取り入れてもらっている。カードは酔って落とす危険などがあるためだ。紛失時にカード拾得者が防犯システムを解除したり、部屋に入ることができないようにするため、出入り口の電気錠に虹彩認証を導入した。最初の出勤者と最後の退勤者が虹彩認証で電気錠を開錠またはロックする仕組み。日中はカードのみで入退室管理のセキュリティ強度を場面に応じて変えた運用スタイルで運用されている。また、マスクや手袋を着用している食品工場の入退室管理にも利用されている。

10. スマートフォンの虹彩認証の必要性

2012年6月、政府が国家公務員の私物スマートフォンの業務使用を認める方針（BYOD）を発表した。早ければ2013年4月をめどに政府は解禁する方向だ。このBYODは民間企業でも少しずつ広がりを見せており、用途は個人利用から仕事の業務利用へと拡大しつつある。スマートフォンは管理が個人に任されているためセキュリティは甘く、パスワードロックすらかけていない人もいるなど、現状の安全対策は十分といえない。

報道では、「スマホで個人情報1000万件流出」などと情報漏洩の後もたたないようだ。スマートフォンが急速に普及しているということもあり、セキュリティ性向上の観点から、虹彩認証を役立てていきたいと考えている。

虹彩認証は、スマートフォンのセキュリティ性を高める役割を担う一方で、世間の既存のサービスの利便性を向上させることも可能だ。現在、虹彩認証モジュールの作業をスマートフォンのカメラやCPUを使って稼動させることができないかと検討している。これが実現すれば、買い物やレストランなどでの決済に虹彩認証のみで、デビットカードのように自分の口座から直接代金を精算することも可能になる。また、病院の病歴データの管理の鍵や薬局の処方箋も虹彩認証で代替するなど、さまざまな用途が考えられる。

虹彩認証技術の導入先としてスマートフォンの市場を非常に有力視しており、一部のメーカーと共同開発やライセンス契約の交渉を始めている。

11. 虹彩認証導入現場から見える今後の課題

医療情報での認証方法は、「私は○○です」といって認証する1対1が望ましいとされているが、実際には不特定多数と比較する1対nが導入されている。その中では20人に1人が本人否認されるという状況もでてきており、実験結果で出ている否認率どころではないという話もある。これが生体認証の泣き所でもある。

実験室・研究室では健康体で若い人が実験対象になるため、結果もそれなりに良い。しかし世の中で実用化するとなると、年齢、職業、人種、性別や環境など、利用者の属性などが多岐に渡るため実験ほどの成果が出にくい。特に指紋や静脈は寒さに弱い。だから、全国のATMにあれだけ静脈認証を採用しているにもかかわらず、実際に使っている人ほとんどいない。

自分の体で間違いなく自分を証明できればこんな便利なことはない。生体認証技術はまだまだ完璧とはいえないが、今抱えている課題に取り組みつつ、世の中の要請に応えていきたいと思う。