第１回バイオメトリックスと認識・認証シンポジウム

世界最小の虹彩認証エンジンモジュールと組込商品の例

The Smallest Iris Recognition Engine Module in The World and Embedded Products

對馬　一彦　　上田　繁
クリテックジャパン株式会社
Kazuhiko TSUSHIMA　　Shigeru　UEDA
Qritek　Japan　Co.,Ltd.

アブストラクト

本報告は、従来の虹彩認証アルゴリズムの課題を解決し、精度向上、高速化、小型化、低コスト化を実現した新しい虹彩認証アルゴリズムと、それを実際に組み込んだ新商品を紹介する。開発に成功した「虹彩認証エンジンモジュール」は、虹彩イメージ取得・コード化・登録・認証等、全ての機能を小型一体化し、サーバー認証に加えて、端末認証を可能にした。また、写真、ビデオ映像、模様付コンタクト等による「なりすまし」を防止する機能を搭載。モジュール組込商品として①PC 接続で使用する認証デバイス IrisKey②Windows PC 用 虹彩認証 Logon プログラム③虹彩データによるファイル暗号･復号化プログラム④虹彩認証・入退室管理システム Iris Pass 2020 を紹介する。

１．　はじめに

米国の眼科医 Leonard Flom と Aran Safir が 1986 年に出願した特許（失効済）に基づき、ケンブリッジ大学の John Daugman 教授が 1992 年に出願した特許が、現在世界で一般的に使われている虹彩認識技術である。

この特許を応用した商品は、重要施設のアクセスコントロールや一部の空港でゴーダーコントロール等に適用されている。しかし、これらのシステムはアルゴリズムの関係で、大型、高価、本人拒否率が高いなどの問題があり、指紋認証などに比較して、一般市場にはまだ十分普及していない。

Qritek は、従来のシステムの問題を解決した新しいアルゴリズムによる「虹彩認証エンジンモジュール」の開発に成功した（日本を含む主要国で特許取得済）。今後、モバイル機器のセキュリティ、公的認証、サイバーセキュリティ等の幅広い分野への普及を目指す。

２．虹彩認証アルゴリズムの比較

２．１　従来の虹彩認証

（１）John Daugman の IrisCode アルゴリズム

瞳孔を中心に描いた８つの同心円上の円周方向に２５６分割し、ガボールフィルタを利用して画像の濃淡変化を、イメージの輝度を基準に 2,048bit の虹彩コー

ドを生成、ハミング距離により統計的に本人認証を決定する。

（2）従来システムの問題点

－大型･高価:これまでは、米国 Iridian 社の技術がデファクトスタンダードとなっているが、アルゴリズムの計算量が大きいため、小型化が難しく、高価であった。

－東洋人に多い、目が細く、まつ毛が下向きの人や欧米人の色が青、グリーン系の虹彩や、コントラストが弱い虹彩の人の登録・認証が困難であった。

－登録時と認証時に明るさが変わると、虹彩パターンの変化により本人拒否率が増大する（図２参照）

２．２　Qritek IRIBIO 虹彩認証

Qritek 社は、2000 年に生体認証の中で原理的に最も精度の高い虹彩認証の開発に着手し、従来方式の欠点を解消する、新しいアルゴリズムの開発に成功した。

（1）Qritek IRIBIO の虹彩認証アルゴリズム

従来の極座標方式と全く異なるブロックパターン方式（図１）を採用し、上まぶたや睫毛の影響を受け難いブロック情報を採用した(アルゴリズムを日、米、英、独、中、韓で特許取得済み)。

図２は、同一人物の同一の目であるが明るさによって拡大した瞳孔と、縮小した瞳孔とで虹彩パターンは大きく異なる。このため、従来システムでは、登録時と認証時とで照度が異なると本人が認証されないという問題が起こっていた。

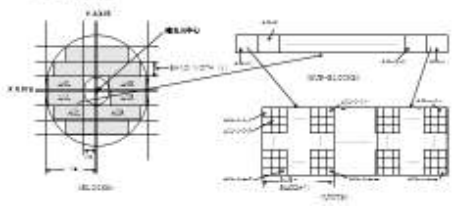

図１Qritek 方式のブロックパターン

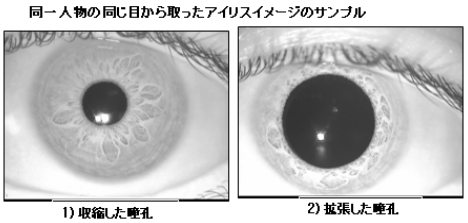

図２　同一人物の、明るさの変化による虹彩模様の変化

瞳孔の変化による虹彩パターンの変化は、変化が少ないときは、ある程度計算でシミュレーション可能であるが、変化が大きいと難しい。(生体であるため理論通りには変形しない)。

新アルゴリズムでは、虹彩イメージ取得時に付属の LED の輝度を変化させ、複数の虹彩イメージを取得し、テンプレートを作成している。
このことにより、50 ルックスから 10,000 ルックスの範囲で認証を可能にした。

（2）Qritek IRIBIO 認証の特長

－アルゴリズムの改良により、小型DSPでの処理が可能になり、モジュールの小型化、端末認証を可能にした。
－写真やビデオ映像、カラーコンタクトによる「なりすまし」を防止している。
－ISO の BioAPI 2.0 に適合
－韓国政府機関のアルゴリズム評価試験に合格し、Certificate 取得

３．各種生体認証の精度比較

３．１　英国物理学研究所の評価

図３は、英国物理学研究所が 2001 年に発表した、生体認証の相対的認証精度比較である。これによると、虹彩認証は、あらゆる生体認証の中で最も正確で、速く、従って、最もスケール拡大が容易と結論づけている。
図３の左下◆が虹彩認証の精度。他人受理率（FAR）100 万分の１の時の本人拒否率（FRR）は 0.25%。

３．２　クリテックの虹彩認証の精度評価試験

Qritek 社の社内試験では、学生、教会などのボランティアから 43,000 虹彩サンプを収集して評価試験を行った。
表１に評価試験結果を示す。他人受理率（FAR）100 万分の１の時の本人拒否率（FRR）0.１%以下を得ている（閾値７６の場合）。
図３にも追記（クリテックと表記）。

表１　評価試験結果

Threshold	66	68	70	72	76	78	80	82	84	86
FAR(%)	0.0089	0.0044	0	0	0	0	0	0	0	0
FRR (%)	0.0001	0.0005	0.003	0.004	0.01	0.05	0.2	1.2	2.65	4.95

Certified by Eunik Kim

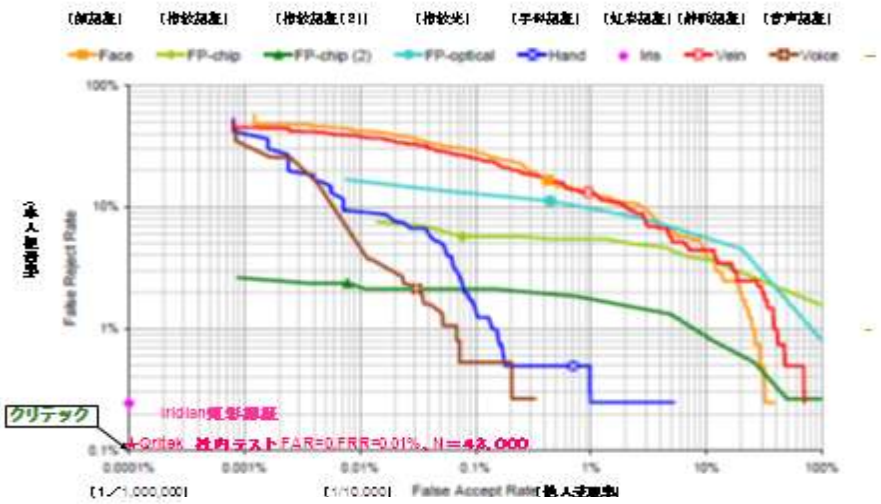

図３　各種生体認証方式の精度比較

４．Qritek IRIBIO 虹彩認証の商品化

４．１　虹彩認証エンジンモジュール

虹彩認証エンジンモジュール M150_USB と、カメラモジュールを図４、図５に示す。

他に M150_UART,　N300_UART（カメラ一体型）がある。

図４ 虹彩認証エンジンモジュール（40mm×40mm 世界最小）

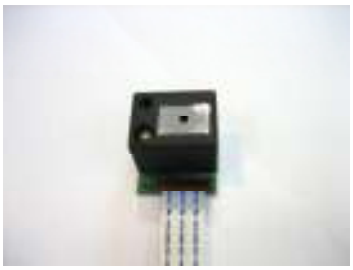

図５　虹彩撮影カメラモジュール（18mm×23mm×21mm）

認証処理 DSP、虹彩保存メモリ、照明回路等を搭載

４．２　虹彩認証端末（IrisKey）

M150_USB を組み込んだ虹彩認証端末を図６に示す。この単体の中に 150 人分のテンプレートが保存可能。

PC に USB 接続して、広い応用が可能である。Windows XP, VISTA, ７のログオンを虹彩認証により行う「Iris LogOn Program」を同梱してある。

図７は、USB 接続により、パソコンの Log オン用に使用している例を示す。

図６　IrisKey の外観（47mm×91mm×２５mm）

図７　IrisKey の適用例

４．３　虹彩暗号化プログラム（MyGuard IrisDoc）

IrisDoc がインストールされると、隠しドライブ“Z”が作られ、ディスクトップに「暗号化ドライブ」のショートカットが作成される。そこに保存されたファイルは、PC シャットダウン時に自動的に AES（米国標準暗号）で全文暗号化され、隠しドライブに保存される。復合化は、虹彩

認証を行うと、隠しドライブが現れ、「暗号化ドライブ」内部のファイルを一括復号化する。万一 PC を盗まれ、HDD を解析されても情報は解読されない。

４．４　虹彩アクセスコントロール（IrisPass）

虹彩認証モジュールを組み込んだ入退室管理システム。従来のドアホンや電子ロックと上位互換を取るため、インターフォン機能、テンキーによるパスワード認証、RFID による ID カード認証を一体化し、ユーザーの自由な組み合わせが選択可能。

４．５　虹彩認証システム開発キット

Qritek IRIBAIO 虹彩認証方式の広い応用をはかるため、カメラモジュールに加え、API・テストプログラムのソースプログラムを提供している。

４．６　認証技術のライセンス供与

顧客ニーズにより、スマートフォン、タブレット PC, ノート PC, 自動車などの分野向けにライセンス供与を行う。

４．７　応用商品

（１）自動車盗難防止システム

近年、盗難防止の決め手と言われた「イモビライザー」がイモビカッターにより簡単に破られ、盗難に合い解体されてアフリカなどに輸出する犯罪が増加している。（NHK,の追跡 A to Z,2011 年 11 月 17 日の読売新聞）。

アクシオヘリックス社は、虹彩認証モジュールを応用して、エンジンをかけられても虹彩認証をしないと、シフトレバーが動かず、アクセルも聞かない自動車盗難防止システムのプロトタイプを開発した（図８）。

図８　自動車盗難防止システム

（２） ID 管理システム

大手企業向けシングルサイン・システムとの統合を進めています。　セキュリティレベル、ユーザー権限により、カードや他の生体認証との使い分け・共用が可能となります。

５．おわりに

最近、政府機関や防衛産業などを標的としたサイバー攻撃により大規模な情報漏洩事件が多発している。これらは、ウイルス感染が原因の一つとみられる。特定の情報にアクセスできる人間や、システムの管理権限を有する人間の ID、パスワードが盗まれれば、情報漏洩は防げない。この対策としてワンタイムパスワードが推奨されているが、本人そのものを認証しているものではないので、モノを盗まれれば容易になり

すましが可能となる。

“ウイルス感染は基本的に防げない”(防御は常に後手になる)。“内部犯罪も無くならない”ことを前提にした、セキュリティシステムの再構築が重要と考える。

重要な情報は暗号化する。たとえ漏洩しても、復号化できないようにする。暗号キーの管理が重要であり、正当な権利を有する人間の生体で認証しなければ復号化できない仕組みが必要となる。パスワードを使わない新たな個人認証システム、新たなセキュリティシステムの構築に寄与して行きたい。

(参考文献)

１．How Iris Recognition Works, John Daugman,IEEE TRANSACTIO ON CIRCUTTS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL.14, NO.1, JANUARY 2004

２．松本　勉、金融取引における生体認証について、金融庁・第 9 回偽造キャッシュカード問題に関するスタイディグループ、2005 年 4 月 15 日

３．Biometrics Product Testing Final Report, UK National Physical Laboratory.
http://www.biometricscatalog.org/2003GBW/downloads/Biometric_Test_Report_pt1.pdf#search='CESG/BWG

{筆者紹介}

對馬　一彦

クリテックジャパン（株）代表取締役社長

〒105-0004　東京都港区新橋 6-14-4

和田ビル４階

Tel / Fax：03-3437-3190

email：info@qritek.co.jp

URL: http://www.qritek.co.jp

(略歴)

前、「日本原子力防護システム株式会社」常務取締役、(品質保証、情報システム、技術開発担当),元、「セコム株式会社」取締役システムエンジニアリングセンター長、(大規模・ハイグレードセキュリティ　システムの SI 担当), 元「日立造船株式会社」(神奈川工場 QC マネージャー、原子力・石油化学プラントのプロジェクトマネージャ).

上田　繁

クリテックジャパン（株）常務取締役

（略歴）電電公社・NTT 通信研究所で大型コンピュータ（DIPS）の周辺漢字プリンタ等開発。シャープ（株）技術本部で、携帯通信機器の開発（特許開発室長)。