バイオメトリクス認証による
情報アクセスの現状と課題

法　雲　俊　邑

１．はじめに

2005年４月に、個人情報保護法が施行されたが、各界の組織におけるその対応は遅く、今尚、アメリカ大手クレジットカード会社VISA の 4000万件に及ぶ情報漏洩、わが国では、みずほ銀行のローン等を含む顧客情報27万件と４万件の漏洩など、後を絶たない。

また、情報漏洩を悪用したクレジットカードの偽造による現金引き出し事件、振込め詐欺、脅迫などが発覚している。これらの情報漏洩と事件を未然に防ぐには、社内の漏洩対策としてシステム面のガードと社員の倫理観の高揚が重要であるとともに、アクセス者の個人を特定する固体識別（生体認証）の導入が不可欠である。

各界の組織において情報が漏洩する事件が相次ぎ、被害者が告訴すれば多額の賠償責任を負う事例の現状と実態について、「オフィスの情報漏洩に関する一考察第１報」(OA 学会 2004 年全国大会) で紹介した。漏洩する情報量は、数十万件・数百万件の膨大な量にのぼり、その事件の８割程度は内部関係者に起因するものであることを指摘した。(1)

さらに、情報システムを確実に運用し本来の業務を適正に遂行する視点から、不正アクセス者の発見や情報漏洩対策の方法について、「オフィスの情報漏洩に関する一考察第２報」(OA 学会 2005 年全国大会) で発表し、特に生体認証に関する重要性について論及した。(2)

生体認証とはバイオメトリクス認証とも呼ばれ、本人しか持ち得ない身体の

一部（生体器官）や動作の特徴といった生体情報を利用して本人確認を行う個人認証技術である。人体に備わる特徴を利用して本人認証を行うため、忘失、盗難、偽造のリスクが少ない、安全性の高い認証方法である。この技術分野では近年、バイオメトリクス技術が注目を集めており、大手銀行などで採用を試みている所もある。本人確認の厳密さを象徴する例としては、９.11 同時多発テロの後、米国が入出国管理にバイオメトリクス認証を採用しており、世界各国でも導入検討を進めている段階にある。

本稿では、前記の研究をさらに進展させて情報漏洩の対策方法について探究するとともに、特に情報システムへアクセスする時点でバイオメトリクス技術を用いた場合の本人認証についてそれぞれの方法を比較検討する。今日、情報漏洩とそれにともなう事件に対する関心は高まりつつあり、バイオメトリクス認証に関する各種の技術が日新月歩の速さで開発されている。しかしながら、これらを情報システムへどのような場面で組み込んだら良いか、また、どのような用途に用いたら良いかという応用面からの研究は十分になされていない。これは、バイオメトリクス技術の開発者は情報処理技術者や情報システム開発者と専門を異にするもので、当然のことである。

つまり本稿での研究目的は、情報技術者の立場からシステムへの「なりすまし」や偽造による不正侵入や盗用や情報漏洩を防止するために、アクセス時の本人認証にバイオメトリクス認証をどのように適用すればシステムが安全に運用できるかを検討することである。

２．情報漏洩の被害の実態と管理システムの隘路

2002年に全国で、盗難通帳･カードによる不正引き出し被害額が42億円になったとの報告が報じられた。2003年には、クレジットカードの不正利用による被害額は272億円にのぼっている。

個人情報の主な流出･紛失例は、2004 年２月にプロバイダーから452 万件、

３月に通販会社から 30万件、４月に石油会社から 220万件、５月に信販会社から 116 万件、2005 年１月にテーマパークから 12 万件、３月に金融機関から 27 万件、４月に金融機関から 131万件、６月にクレジット会社から 4000万件、など枚挙に暇がない。2006年１月には銀行員が暴力団に顧客情報を手渡したことが報じられた。

被害の実態を再確認するために、以下では新聞などで報道されたデータから直接被害額・間接被害額をまとめてみよう。(3) なお、直接被害とはお詫びの金券（その配布費用を含む）や記者会見費用など一次的に発生する損失である。一方、間接被害とは損害賠償請求が確定し、被害者全員にそれを支払った場合に発生する損失である。

表1　主な情報漏洩事故

企業名	発生時期	件　数	内　　容	流出経路
TBC	2003年5月	3万7000件	氏名、住所、電話番号、メールアドレス、職業、スリーサイズ、エステに関する相談ほか	Web 上で実施したアンケートなどを集計した CSV ファイルを、Web 上に閲覧可能な状態で置いていた
ローソン	2003年8月	56万件	氏名、住所、性別、生年月日、電話番号ほか	社外開発委託先のコンピュータから抜き取られた可能性が高い
アプラス	2003年8月	7万9000件	氏名、住所、電話番号、性別、職業、年収ほか	社外開発委託先から流出
ファミリーマート	2003年11月	18万件	氏名、住所、メールアドレスほか	社外メール配信事業委託先から流出
ソフトバンクBB	2004年1月	451万件	氏名、住所、電話番号、メールアドレスほか	内部関係者による持ち出し

これらの事件について漏洩情報の悪用が無かった場合は、被害者へのお詫びに 500円から 1000円程度の金券を発行することが多い。そして謝罪のための放送や新聞広告費用など数十万円程度が計上されると考えられる。この結果、直

接被害額は、被害者100万人以下の情報漏洩で約10億円未満が必要と想定される。

また、漏洩情報の悪用があった場合は、上記の直接被害額とともに、被害者への被害額の弁済と裁判費用等が加算され、膨大な額になり企業の存続も危うくなるほどである。

表２　直接被害額と間接被害額の内訳

企業名	売上高	直接補償額（億円）	売り上げ比率	直接補償額の備考
	（億円）	間接補償額（億円）	売り上げ比率	間接補償額の備考
TBC	411	0.1	0.03%	10人が損害賠償訴訟を起こす
		425.5	103.50%	115万円を全員に適用と仮定
ローソン	2500	2.8	0.11%	全員に金券500円
		56	2.20%	全員に損害賠償額1万円と仮定
アプラス	1063	0.8	0.07%	全員に金券1000円
		7.9	0.70%	全員に損害賠償額1万円と仮定
ファミリーマート	9544	1.8	0.02%	全員に QUO カード1000円
		18.3	0.20%	全員に損害賠償額1万円と仮定
ソフトバンクBB	4069	23	0.56%	全員に金券500円
		40	1.00%	新聞報道による

間接被害額の例については、宇治市住民基本台帳データ大量漏洩事件の判例などを基準にすると、訴訟を起こした人に対し損害賠償金額が１人当たり１万円程度である。この場合、訴訟は数人の人に留まったものの住民の多くが訴訟を起こせば、前代未聞の自治体破産になる。

TBC の情報漏洩事件では被害者の一部だけではあるが１人当たり 115万円の損害賠償を請求している。情報漏洩が一般的な項目のであれば、損害賠償額は１～４万円が中心となっており、総額は数十億円である。また、重要な項目の情報漏洩の場合、損害賠償額は 500 億円程度に達する。ここでいう重要な情報とは、与信情報など金融機関が保有する情報を指す。

これらの数例を取り上げただけでもその代償は膨大な被害額に登り、一時しのぎの曖昧な対策だけでは済まされない実態が理解できるであろう。そして情報漏洩を防止するためのセキュリティ投資として必要と思われる金額は、一般

的な項目の情報漏洩については、直接被害だけを考慮に入れた場合10億円未満、間接被害も考慮に入れれば 100 億円未満になる。また、重要な情報の漏洩の場合は、損害賠償金額がさらに大きくなる。このことを考慮に入れると金融機関など重要な情報を多く保有する企業の場合、上記の５～10倍のセキュリティ投資が必要と考えられる。過失が無ければ何でもないことであるが、一つ違えば上記のような多額の賠償問題になることを認識しておきたい。

ところで、情報システムや通信ネットワークが今日ほど普及していなかった時代は、機密情報（重要書類やマル秘文書など）を鍵のかかるロッカーや金庫に保管し、必要な時には権限のある人だけが鍵を開けて、それを読むことができた。あるいは管理人が存在する部署に預け、その文書を見たい場合は、管理人に対面して許可を得る、ないしは「許可された本人かどうか」が確認できれば、該当文書が利用できるという仕組みをとっていた。現在でも、契約書や登記書などの重要な書類や、裁判などで使用する証拠品に類するモノは前記のように保管し、外部に漏れないようにしている。

しかしながら、今日のように高度情報化が進展して様々な情報が電子化され、社会の様々な組織や個人がネットワークに結ばれ、ネットワークを利用した業務処理が多くなると、情報管理のあり方が変化してくる。ネットワークの発達により 2000 年以降には、セキュリティ管理の対象が、書類や入退出管理といった物理的な管理から、ネットワークを考慮した情報システム中心のセキュリティ管理へと変化してきた企業が多い。

株式会社 ITR が調査した「国内 IT 投資動向調査報告書 2004」によると、組織の情報管理者の役務が情報システム戦略の立案･執行や情報システムの開発･運用・管理、業務プロセスの改善・再構築だけでなく、ネットワークセキュリティの管理業務も含むようになった企業が多いという。(4)

これらの情報セキュリティ管理は、過去には未経験の新開拓の分野であり、事件や障害は予期しない環境を生み出している故に、事前に万全の対策を用意

することは困難である。様々な組織や個人がネットワークを経由してマルチメディアのデータを簡単に送受信できるようになると、対面して本人を確認することが不可能な環境になるのもその隘路の一つである。

例えば、座席予約やネット取引、銀行の ATM(現金自動預払機) を操作する場合である。銀行ではキャッシュカードを ATM に挿入し、ID およびパスワード (通常、４桁の数字) を端末の画面から入力して正しければ、ATM は「操作している人は本人である」と認識して、現金を引き出したり、残高照会などの操作を許可する。これは対面でチェックするのではなく、キャッシュカード、ID、パスワードという３つの要素のみを用いて「非対面」で本人確認をしていることになる。

これらの仕組みは、本人だけがアクセスできる方法として採用されたのであるが、キャッシュカードを盗まれたり紛失して複製され、ID とパスワードが判明すれば、誰でもお金を引き出したり、取引が成立する危険性を持っている。先にも紹介したが、こうした事件がテレビニュースや新聞などで日常茶飯事のように報道され、他人の出来事ではない問題になっている。なお、2006年２月に預金者保護の法律が施行され偽造・盗難カード被害に対する金融機関の保証割合が発表された。(添付資料を参照のこと)

インターネットのように極めてオープンな環境下におけるアクセスで、本人確認に ID とパスワードのような数字と文字列だけを用いる現状では、全く顔の見えない「非対面交渉」が加速化し、不正にそれを入手するだけで、本人に「なりすまし」て入り込む犯罪行為も容易である。さらにネットワークの発達によって、ID やパスワードを入力せずに、プリペードカードや携帯電話からの現金支払い、また、現金を使わずに大量のお金をネット上で移動する電子商取引などは、あまりにもリスクが大きい。

便利さの追求が先行して、その陰に潜む膨大なリスクを忘れたシステムがあちこちに蔓延し、莫大な被害を受けて初めて目が覚める状況にある。情報ネッ

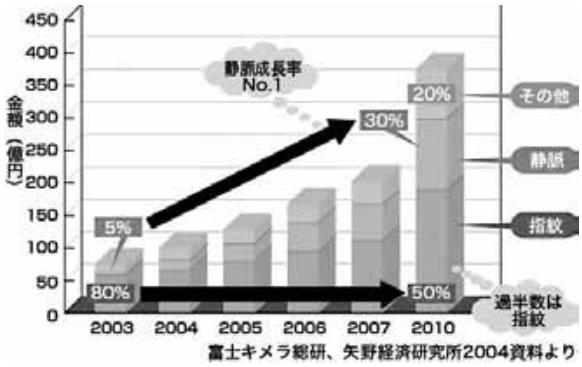
トワークが発達したことで、今やすべての人が個人情報の漏洩や預金の盗難など、さまざまな事件に巻き込まれる危険性にさらされており、情報セキュリティはすべての人々が意識をせざるを得ない重要な問題であり、本人認証の重要性がますます高まってきたといえよう。

３．バイオメトリクス認証

企業や公共団体などのオフィスの情報漏洩の８割程度が内部関係者に起因するものであるという調査結果は、社内の従事者の倫理的自覚を促すことが不可欠である。また、社会へ視野を広げた場合も ATM やクレジットカード、各種のカードによる決済、様々な場所への入退室なども本人認証の機会を増やすとともに、システム的にも安全対策を講じることが不可欠である。いずれにしても組織の内外を問わずに、様々な方法で毅然としたセキュリティ対策を講じることが重要である。

ここでは、各種のセキュリティ対策の中からバイオメトリクス認証に焦点をあてて、その現状と有効性を検討してみる。先にも述べたようにこの認証方法は、人間の一部の生体器官の情報を用いて行う個人認証技術で、近年、セキュリティ対策として注目を集め、ここ数年で１兆円の産業規模に成長する可能性がある。

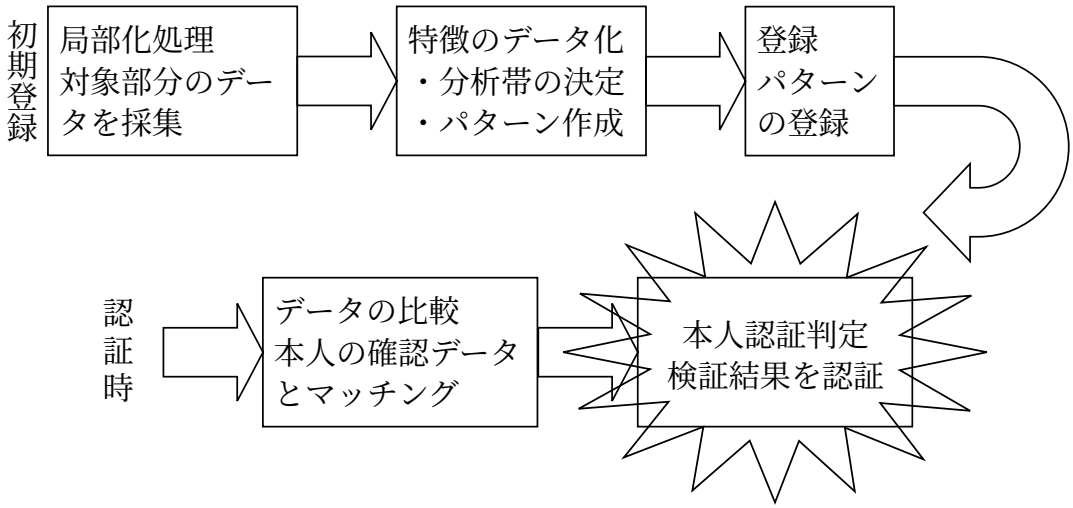
図１　バイオメトリクス産業の成長率



バイオメトリクスの要素技術には様々なものがある。まず、指紋や声紋、顔

貌、掌形、署名（サイン）、虹彩などの利用であり、従来から、犯罪の捜査などにも利用されてきた経緯がある。その実績もあるが近年は飛躍的に技術が進歩して、認識精度の向上、機器操作の容易さ、機器の小型化も進んでいる。また、最近の研究成果から、指や手のひらの静脈（血管）パターンや網膜、そしてDNA(遺伝情報)を採用する技術が実用化され始めている。いずれの方法も、生体の形状をスキャンしてパターンをコンピュータにテンプレートとして登録し、認証時にスキャンしたパターンとテンプレートを照合することによって本人を識別する方法である。

図２　バイオメトリクス認識のステップ



これらは認証時の利用者意識や使い勝手の容易さ、機器への接触・非接触性、機器の大きさや設置場所、精度や価格などの点で異なり、認証現場の用途に合わせて使い分けることが賢明である。

なお、認証の精度を本人拒否率（本人を本人と正しく認識しない率、反対は本人受理率)、他人許容率(他人を本人と誤って認識する率、反対は他人棄却率)、等価エラー率（他人を本人と認識するエラー率と本人を他人と認識するエラー率が等しくなるように調整したときのエラー率)などで現している。

以下では、それぞれの特徴について列挙してみよう。

第３表　バイオメトリクス認証の特徴

認証対象	認　証　方　法
指　紋	指紋の分岐・端点などの特徴点で判別
署　名	筆跡、筆圧、輪郭、形状などで判別
顔　貌	目・鼻・眉毛の配置、顔の輪郭などで判別
掌　形	掌(てのひら) の大きさ、長さ、形状などで判別
声　紋	音声の波形、発声速度などで判別
虹　彩	瞳孔より外側の部分の紋様(紅彩) で判別
網　膜	眼底の網膜の形状で判別
静　脈	手の甲や指などの静脈血管の形状で判別
DNA	遺伝子の塩基配列部分を用いて数値化して判別

指紋　バイオメトリクス技術の中で指紋認証は、情報システム分野でも近年、最もよく普及しており、小生の研究室でも指紋をパソコンに記憶させて起動時に認証して利用するシステムを導入している。古くから犯罪捜査にも使われてきたが、1970年頃からコンピュータを使った指紋解析作業が一般化されるようになり、ここ数年で一気にパソコンでも取り扱える分野の製品が登場するようになった。

指紋認証は、指紋模様をスキャナーでコンピュータに取り込み、その模様を数十点の位置から読み取り、模様の特徴をパターンとして登録する。認証時に、読み取った模様と記憶されているパターンを照合して認証する。

第１図　指紋の模様の種類

ループ型　うず巻型　アーチ型

認証時に、指の一部分しか使わないので装置を小型化でき、作業が容易であることが大きなメリットである。この理由から多くのメーカーが参入して競争が激しく、安価なシステム構築も可能である。製品としての熟成度が高く、本人拒否率、他人許容率なども良い結果を残している。(5)

しかし、実用化の面からは、従来まで犯罪捜査に使われてきたという理由で、指紋の登録を不快に感じる人もあったり、数百人に１人の割合で指紋が取れない人や取りにくい人もいる。利用する部位が指であるため、外的要因ですり減ったり、傷が付くことで認識率が下がるという欠点もある。

また、指紋認証の偽造は、残留指紋をゼラチンに写し取って人工指を作り、その人工指で認証を通過させる事に成功した事例もあり、安全性には疑問が残る。最近、米国でシリコンラバーを使って指紋を偽造して、犯罪に悪用するケースなども出てきている。この予防に一部のメーカーの指紋認証装置は、指の温度なども確認して正確に認証できる高機能製品も開発されているが高価である。

今日ではパソコンや携帯電話に組み込まれた製品もあるが、１万円前後の安価な製品から数十万円のシステムまであり、採用する場合には偽造の対策にも注意を払うべきである。

署名（サイン）純粋な意味では生体認証ではなく動作認証になるが、本人の署名時の動作や筆跡をパターン化するという意味ではバイオメトリクスのカテゴリーに入れて考えられている。単に筆跡だけではなく、署名時の筆跡、筆圧、筆順、筆記に要した時間などの具体的事象を登録し、それをデータとして保持することで同一人物が書いたものかどうかを判断する。

実用的には筆記具さえあれば、どこででも利用できる手軽さがある半面、手が負傷している場合や、登録時と違った書き方をすれば認識率が下がるというデメリットがある。また、認識ソフトのアルゴリズムや設定方法などによって認識率を上げたり、認識までの時間を短くすることができるが、これらのデー

タは精度に比例し、また、メーカーの製品によって署名認識のノウハウの違いがあり、現状では互換性はない。

認識率を上げるために厳密なチェックを行うと、本人拒否率も上がるが、日本のようにサインに慣れていない国柄では拒否反応もあり、バランスが難しい。また、一部の PDA(携帯情報端末) の OS には署名を認識する機能が組み込まれているものもあるが、本格的な普及はこれからの段階である。

顔貌　人が相手を識別する時、顔を見てその人を判別するのは本能的な行為である。この視覚を用いた識別をコンピュータで画像処理して行うのが顔貌認証である。システムの仕組みは、人間の顔をカメラで撮影し、あらかじめ登録した顔の画像の特徴点 (目、口、鼻、眉、頬の輪郭など) を比較照合することで認証を行う。(6)

顔貌認証のメリットは人と人とが出会った時の無意識な行為を機械で代用するだけなので、指紋などに比べて心理的な抵抗が少なく、認証時は特別な操作も不要で、カメラの前に数秒間立つだけであり、利便性も高い。

しかしながら実用的には、顔の正面の映像と側面の映像の違いによる誤認証、双子の厳密な識別の困難さ、暗い場所では利用できないなどの問題がある。また、事前に登録したテンプレートの画像と認証時の顔が変化していると認証されにくいというデメリットもある。たとえば、病気でやせたり、髪型を変えたり、装飾品を付けたり、美容整形をしたような場合である。これらには再登録の作業が必要になる。他のバイオメトリクス認証方法と比較すると、本人拒否率や他人許容率の値が悪く、今後に開発の余地を残している。

掌形　人の手のひらは、形、指の長さ、太さ、しわなどが微妙に違うという特徴を認証に応用した技術である。これらは生前に胎内で定まったあと、大きさが変化する以外、生涯不変であり、一人ひとりに固有のもので、右左の手でも異なる。また、身体の一部の情報であることから、他人に知られにくい。他の認証方法と比較すると、認証時間が速く、１秒前後で認証を行えるというメ

リットがある。待ち行列になる所や出入りの激しいオフィスの入退室などに使うと効果的である。

実用的には、認証処理が高速というメリットはあるが、認証時に手のひらをかざす装置の設置場所の面積が大きくなり、狭いオフィスには向いていない。非接触という点では衛生面に問題はないが、製造メーカーが少なく価格が高い。また、精度を上げたい場合には、観測点を多くすることも可能であるが、認証処理が遅くなることにもなり、20から 40の点で識別するのが通常のようである。

掌形の照合時に点灯したガイド用 LED のガイドピンを、指で挟んで消す必要があるが、この時の行為を生体反応としてチェックする機能もある。そのため、「なりすまし」を行うことを防げるのも特徴の一つである。(7)

声紋　音声を登録しておき、その波形に認証時の入力音声を照合して認識するものである。登録する音声の処理は一般的なパソコン、音声認識用のソフト、マイクを用いるため、汎用性が高く、他のバイオメトリクス認証と比べると低コストでシステム構築ができる。認証には、普通に話している感覚で利用でき、指紋や顔のデータを取られるのに抵抗がある人でも心理的な抵抗感は少ない。

しかしながら、実用的には本人拒否率、他人許容率が高めに出たり、音声を録音するにはある程度静かな場所が必要なので、使う場所が限られるという問題がある。したがって声紋による認証は単体で使うよりも、他の認証技術や IC カードなどと組み合わせて使われることが多い。

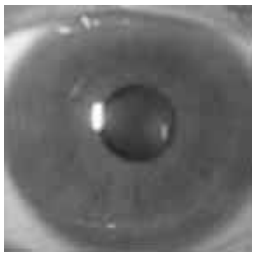
耳介　人間の耳介は、集音と増幅機能を果たすために複雑に入り組んだ鞍骨の凹凸によって形づくられているが、その形状にはきわめて著しい個人差がある。耳介の長さ、軟骨の長さ、耳介の幅などの成長は、耳長は 16 〜 17 才、耳幅 は 10 歳前後で男女とも成長が止まり安定期に入り、40 歳前後で少しずつ成長することが報告されている。

生涯にわたって大きく変化することがなく、固体ごとの特徴点を多く持つバイオメトリクス認証技術である。ただし、現在は実験段階で、今のところこの

技術を活かした製品は登場していない。

虹彩（アイリス）　紅彩とは黒目の内側で瞳孔より外側のドーナツ状にヒダヒダになっている部分のことで、外界から眼球内部へ入射される光の量を調整する機能をもつており、瞳孔の開き具合を調節する筋肉から構成されている。言い換えれば、紅彩はカメラの絞りに相当する。(第3図)。

図３　紅彩と網膜



虹彩 iris

網膜 retina

図４　目の構造

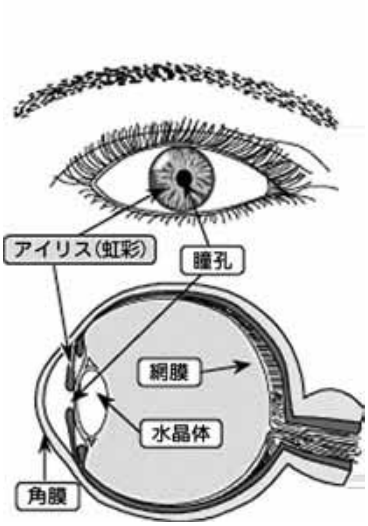


図３の出典：http://homepage2.nifty.com/medamacafe/J/iris_idntfctn.html
図４の出典：http://www.jaisa.or.jp/action/group/bio/Technologies/Iris/Irs-f.htm

人間の皺状の虹彩は極めて複雑なパターンで形成されており、妊娠６、７カ月頃までに形作られ、その時点で瞳の部分に孔が開き、その開口部、すなわち瞳孔から外側に 向かってカオス状の皺が発生することが知られている。生後２～３歳でその成長が止まり、それ以降、形が変化することがないと言われている。

この皺の形状（模様）は遺伝子の作用と発育時の環境により外部に現れるもので、遺伝的影響度が少ないことが 知られている。そのため、紅彩の模様は指紋などと同様にその人固有のパターンとなり、同一人の左右の目でも異なり、一卵性双生児でも異なるパターンになる。[8]

目の内部の場所であるため傷も付きにくく、紅彩 が目の表面（角膜の下）に存在することから眼球内部の疾病などの影響を受けることはほとんどなく、目の充血にも影響を受けることがない。また、目の不自由な方の多くは、視神経の障害であり、ほとんどの場合紅彩は正常に存在し、生体としては最高レベルの「同一性」を保つと言われている。

紅彩を使って認証を行う場合、利用者はカメラの前に立って内部を覗くだけでよい。カメラは非接触型で、指紋のように多くの利用者が次々に触ることがなく、衛生面でもメリットが大きい。

また、本人拒否率や他人許容率なども、最高レベルであり、事実上、バイオメトリクスの決定版と見られている。しかしながら、あまり普及していない原因は、装置が非常に高価格であり、指紋認証装置と比べると、約 1.5 倍～２倍の価格差である。

また、最近の研究では紅彩でその人の病歴がわかるといった学説も出てきた。それが事実だとすると、必要な認証情報以外の個人情報が登録されることに対して、不快感を感じる人が出てくる可能性もある。

網膜　目の奥にある網膜内の血管パターンを、円柱状にした近赤外線で測定するバイオメトリクス認証技術で虹彩とは異なる。網膜は、表面からは見えないが、生後３か月ぐらいで血管パターンが完成し、以後、成人になっても変化しない。また、生まれた時から盲目の人でも網膜内の血管パターンはあり、生後、外傷によって失明しても残っている人が多いという特徴がある。

測定データは個人の一生において安定性を持つことも重要で、この点、網膜上の血管パターンによる識別は非常にすぐれた独自性と安定性を持ち正確である。網膜は脳の感覚プロセス機能の必要性から安定性が必然であり、一生涯のなかで変化することはなく同一人物でも左右の目で異なる。また、眼は高い反射的特徴を持っているために、非接触で簡単に測定することができる。これらの特徴を生かし 1985 年に米国の Eyedentify 社で開発され、米国を中心に普及

している。

現在では、本人拒否率、他人許容率が極めて低く、正確な認証によりセキュリティのレベルは高いクラスである。米国では銀行 (City-Money: 指紋認証と併せて 2002年５月から) や軍などのハイセキュリティ施設へ設置される例が多く、既に一部の銀行で網膜認証を使った ATM が稼働し始めている。高額であり、一般企業で容易に利用できる製品は少ない。[9]

静脈　手の甲に現れる静脈が個人によってパターン差があることに着目し、1995年に発見された、新しいバイオメトリクス認証技術である。掌形と同様に手のひらを装置の上でかざし、非接触でスキャーンしてテンプレートを登録する。

この静脈パターン認証は、本人拒否率、他人許容率の値とも最高レベルであり、虹彩と同じ高レベルのセキュリティが可能である。装置の価格が下がれば虹彩による認証を脅かす可能性もある。

第３図　富士通のマウスに静脈パターンを組み込んだ認証装置

新しい技術であるため、製品の絶対数は少ないが、既に富士通がマウスに静脈パターンの認証装置を組み込んだ製品の開発を発表している。等価エラー率は 0.5% 以下である。これは、およそ 200 回に１回の割合でエラーが起こる確率に相当する [10] 。

日立の指静脈認証技術は、指に光を透過させて静脈画像を撮影する透過光方式を採用しており、一人ひとり異なる指静脈のパターンを高いコントラストで照合できる、高精度 (本人拒否率：0.3% 以下、他人受入率：0.001% 以下：日立実測値) を実現している。装置もコンパクトで、ATM の本人認証、入退室管理、

ノートPC や携帯端末などへの内蔵が可能な世界最小の超小型指静脈認証装置(容積19ml、サイズ39mm ×34mm ×15mm) である。また、自動車のエンジンキーへの応用など、オフィスはもとより暮らしのあらゆる場面への指静脈認証技術の活用が期待できる。(11)

DNA　人間の DNA(遺伝子情報) をバイオメトリクス認証に応用する技術で、犯罪捜査などにも使われている。人間の DNA は、約30億個の塩基配列から成っておりその配列の仕方が、人体の設計図ともいわれるように人体の構造などを決定し、人間の一生で決して変わることのない固有情報である。一人ひとりの容貌や性格が少しずつ違うように、DNA の塩基配列も人によって異なる。この部分の情報を抽出して使えば、他の生体情報と同じように個人認証を行うことができる 。

個人識別用の DNA 情報は、病気や人体の構造には無関係な領域の情報で、短い塩基配列の繰り返し回数が、個人によって異なることから、新技術では、この繰り返し回数を認証データとして利用する。

DNA 以外のアナログ情報に基づくバイオメトリクス認証方式では、50 万～100 万分の１の認証精度（他人受入率）となっているが、DNA 情報を ID とした場合、現状の抽出技術による同値確率を 10^{-21}程度とすることができ、識別精度が高い 。(12)

具体的には、DNA の情報を基に、鍵となる「DNA － ID 」を作成し、IC カードなどに 2 次元バーコードなどで埋め込む。DNA － ID を基に公開鍵と秘密鍵を作成し、公開鍵を「実印」のように利用すれば、生体情報を組み込んだ法的効力のある署名が行える。ただし、現在は DNA － ID を生成するため多くの時間やコストがかかるので、一般的に普及するには今後数年かかかると思われる。認証方法がほかのバイオメトリクス認証技術と違うため、IC カードと併用される可能性も高い。

表４　バイオメトリクス認証の特徴

認証方法	本人拒否率 (%)	他人許容率 (%)	長　所	短　所	代表的なメーカー	利用用途
指紋	0.5 製品により差異あり	0.001	・技術が成熟、認証精度が高い・操作性良・装置が小型・安価である・各種アプリケーションとうまく統合・成熟した認証技術・様々な形態方式の装置	・心理的抵抗・指紋状態が悪い場合認識できないことがある	20 数社１～数十万円程度	全般・業務用入退出全般 ・PC セキュリティ全般 ・集合住宅・戸建住宅用へ普及
署名	0.2 文字の複雑さに依存	0.6	・耐環境性が高い・周囲の影響を受けにくい・利用者の抵抗感が比較少ない・変更が可能	・慣れが必要・本人拒否率が高い・筆跡変動に対応した判断ロジックが必要 ・怪我をした場合に認証できない・精度は書く文字に依存	日本サイバーサインシステム構成による価格	ＰＣ認証・書類ほか
顔貌	1	1	・遠隔からの認証が可能・衛生的（非接触認証）・利用者の抵抗感が低い・歩行しながら認証可能	・認証精度が低い・環境が影響・厳密な識別はできない（双子の方など）・表情変化・着用物・化粧で左右される・光や体調、飲酒にも左右される・老化など経年変化耐性が弱い	米e-True、 米Vision ネクサス、 東芝、 オムロン ５万円程度～	空港入出国管理などで採用され始める・ドア・指名手配
声紋	1	0.1	・衛生的（非接触認証）・特別な装置の購入が不要	・ノイズに弱い・盗用・真似の恐れがある・他人の受け入り率が高い・経年変化耐性が弱い・体調に影響される・認証精度が低い	アニモ 米 T-NetrICs ２～100万円程度	CTI・電話での認証・ＰＣ認証

掌	0.2	0.2	・認証が高速・技術が成熟・操作性良い・各種アプリケーションとうまく統合・偽造の可能性が低い	・機器が大きい・利用者の心理的抵抗感がややある	米 RecognitionSystems エエム・エー・ジェー 50万円程度～	ドア・出国管理・業務用入退出全般
虹彩	0.0001	0.0001	・認証精度が高い・衛生的（非接触認証）・経年変化しない・偽造が困難・離れていても認証できる	・慣れが必要・プライバシー保護問題（虹彩から人の病歴が分かるなど）・利用者の抵抗感がある（目に認証のための光が入る）・装置が高価・大型になる	Iridian(認証) 沖電気(カメラ) 松下通信工業(カメラ) 200万円程度～	ドア・ハイセキュリティ業務用入退出全般・金融取引本人確認
網膜	0.0001	0.0001	・認証精度が高い・偽造が困難・離れていても認証できる	・慣れが必要・目を押し付けリアルタイムにスキャンすることで、目の健康を損害することがある・装置が高価・大型になる	同上	ドア・ハイセキュリティ業務用・刑務所
静脈	0.01	0.00002	・環境条件に左右されにくいために認証精度が高い・非接触認証・汚れにも対応	・非接触で偽造や複製もシャットアウトできる・利用者に認知度が低い・装置がやや大型になる	東西電機産業、ロックシステム、アイ・ディ・テクニカ、富士通 日立　40万円程度～	入退出管理ほか多用途
DNA	10^{-21}	10^{-21}	・識別精度が圧倒的に高い・配列の比較なので照合自体は非常に簡単・不変である	・認証精度が高い・細胞から抽出し分析するのにコスト・時間がかかる	アニモ 米 T-NetrICs 2～100万円程度	・ID タグコード・電子認証・犯罪者特定・血縁者特定

出典：ネットマークス http://www.netmarks.co.jp/ および
日 経 http://premium.nikkeibp.co.jp/security/special/biometrix_02_05.shtml の資料を加筆修正。

４．セキュリティ対策とバイオメトリクス認証の課題

前記では、さまざまなイオメトリクス認証に関するそれぞれの特徴について

述べてきた。ここではセキュリティ対策にその認証を採用する場合の課題について検討する。現在、バイオメトリクス認証は開発された初期の時期で各メーカーが単独で用途開発に専念しているが、実用化にあたっては他種の認証方法と組み合わせて用いることが賢明である。

たとえば、パソコンからのログイン時にパスワードとともに指紋認証を行う。あるいは、銀行の ATM で暗証番号とともに手のひらの静脈の形を読み取って本人確認を行うなどである。

また、安全性の面から検証した場合、本人のその日の状態に依存する音声や署名などよりも、指紋、静脈、虹彩などのように本人の体の状態に依存しない認証方法の方が精度が高いと言われている。しかしながら、これらの認証方法を使ったシステムもセキュリティ上に疑問が残るシステムもある。

たとえば、指紋認証の場合は、先に述べたように残留指紋をゼラチンに写し取って人工指を作り、その人工指で認証を通過させる事に成功しているし、紙で作った人工虹彩で虹彩認証システムを通過できる可能性がある事すら指摘されている。静脈認証システムでも、生体以外(大根で作った人工指) を登録でき、2005年時点では、それをデータ登録して人工指を認証に通過させるという実験に成功した例もある。(13)

直ちに危険があるとは言えないが、内部犯の場合やシステム管理者が犯人の場合は人工指を容易にデータ登録できる。これを使えば以後は人工指で認証を繰り返してシステムが通過でき、追跡されること無く悪事を行う事ができ、安全性に疑問が残る。

また、生体認証には次のような安全性上の問題点が指摘されている。

〇ケガや病気などによって、認証を受けられなくなる可能性がある。

〇生体情報は生涯不変であるが故に、一度盗まれて複製によって破られた場合、暗証番号と違い、情報自体の変更ができず一生安全性を回復できない。

〇生体情報は生涯不変であるが故に、解約や脱退等の時に無効化できない。

○全てのシステムで同じ認証情報を使うことになる。これによって他システムとの情報セキュリティの照合・統合性、発展性が容易になる。
○逆に指紋認証等のプライバシー情報を知ることのできる立場のシステム管理者であれば、それを悪用することによって登録された情報を使って別のシステムの認証も通過することが可能になる。

このようにしてシステム管理者から生体認証データの漏洩を防ぐために、IC チップにデータを書き込んだカードを使用する方法も採用されている。つまり、登録情報の保管をサーバーのデータベースではなく、本人所持の IC に保管する方法である。

指紋や手のひらの静脈認証の情報を、キャッシュカードの IC チップに登録すれば、カードが他人の手に渡らない限り、他人がなりすまして使うことがなく安全度は、暗証番号よりも高くなる。カードの中にある本人確認用のテンプレート情報と持参した本人の生体を照合して確認すれば、個人の認証データを金融機関に保管しないため、情報が金融機関から流出することもなくなり、個人情報保護法対策にも有効な手段となる。

しかしながら、不正の方法としては、次のようにカード側か本人側かのいずれかを変造して行うことが考えられる。例えば、① IC チップのデータを改ざんして、カードを持参した他人を本人と誤認させる方法、②人造物で指紋や手のひら静脈と同じ反応をするものをつくる方法である。

また、技術的課題としても次のことが指摘できる。認証をする際に主として、指紋、音声、顔、虹彩、網膜などのような身体的特徴（アナログ情報）をデジタルデータ化して照合し、「人」を認識する手法が使われていたが、指紋や虹彩による認証方法は、判断の基準となる情報がアナログであり、あいまいさが残り、精度上に問題があった。たとえば指紋などの特徴のパターンを統計的に処理するため、システムを開発した企業ごとに異なった方式(アルゴリズム)が使用され、それぞれの企業の独自技術として、公開されることがない。この

ような理由から、本当に「その人」の固有データかどうかの判定に、あいまいな部分が出る可能性も否定できない。

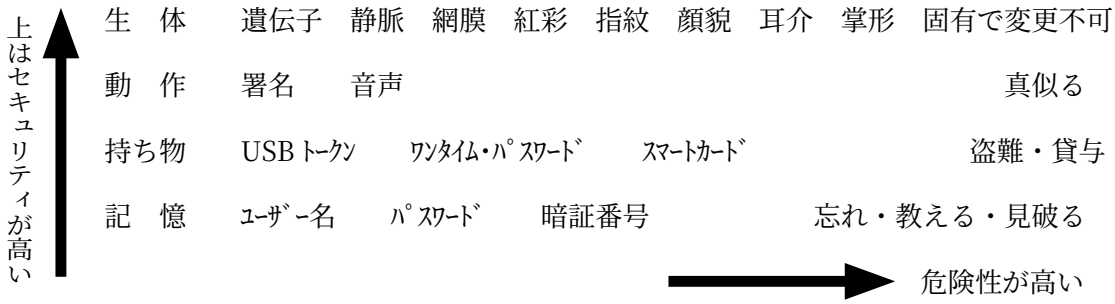
以上のような不正や誤認を防御するには、忘れない、失くさない、盗まれない、複製されないセキュリティシステムのリスクに対応できる個人の生体的特性・習慣的特性を利用した個人認証の技術が必要になる。この視点から、DNA による認証が最有効であると思われる。

2001 年に NTT データと NTT データテクノロジは、DNA 情報を利用して認証する技術で「なりすまし」を防ぐ「DNA 実印IC カード」と「物品認証システム」を開発した。(14) 両社の DNA 認証システムは、辻井重男中央大学教授らの研究グループによって開発された新技術を用い、人それぞれのプライバシーには関わらない部分の DNA 情報を扱い、倫理上から数値化したデータも DNA 情報に復元できない配慮がされ問題もない。

この技術を応用すると個人の固有データとして「DNA-ID」を生成し、これを暗号鍵(秘密鍵および公開鍵)として IC カードに記録させ、「DNA 実印 IC カード」を作って個人認証に用いる。「物品認証システム」では、これをバーコード化するなどの方法で、認証マークをつくり、商品に貼付または直接商品に印刷すれば、ブランド商品、あるいは重要証書などの真贋判定に利用する。これらの認証システムは、技術的には実現可能であるが、実用化には電子署名法など、法律や制度の整備が不可欠であり、現段階では、製品化の時期は未定のようである。

ところで、現在開発されつつあるバイオメトリクス認証技術は精度の表現や測定方法について、統一された基準がなく、それぞれのメーカーが独自の測定基準によって性能を発表している。したがってカタログベースだけでは単純に製品比較ができず、採用にあたっては実物を試用することによって導入を決めることが大切である。

認証の種類と危険性



また、バイオメトリクス認証は、装置を導入しドライバーを情報システムに組み込めば終了というわけではない。導入にあたってはその前後にやるべき準備作業が山積している。具体的には、①バイオメトリクス・パターンデータの採取とデータベース化、②企業が保有しているパソコンやサーバーなどシステムノードの総点検とソフトのインストール、③ Windows などのパッチ適用・管理システムの構築および運用、④ウイルス対策のためのパターンデータ配信・管理システムの構築および運用などを実施しなければ、システムは構築できない。これらの準備は、利用者が何万人にもなれば膨大な作業になり、導入には疎外要因の一つにもなる。

ところで、セキュリティ対策や本人認証の方法などには、組織全体の総合的な観点からアプローチすることができる。一側面だけからの対策では不十分であり、複合的で且つ組織全体の対策が講じられなければならない。以下にそのアプローチ方法を列挙してみよう。

a. アクセス者の検証

本稿で述べてきた情報システムへのアクセスに対するアプローチである。複数手法による認証や複合的な識別方法の採用など、セキュアな認証基盤の構築が重要である。上記したようにバイオメトリクスの先端技術によって高精度の識別を実現し、高速の認証エンジン(1秒で 300～500人を認証の程度) が開発されることも期待される。これらと ID/ パスワードを組み合わせ、容易で精度の高い安全な認証による本人確認が必要である。

また、情報システムへのアクセスとともに、本人確認が必要な建物・部屋・保管庫等の設備に関する入退出の安全管理規定の整備と運用も重要である。

b. データの保護対策

サーバーに蓄積されたデータの保護対策である。データの更新・維持の容易さ、リカバリソリューション、遠隔ファイル共有やバックアップ、不正バックアップの拒否などを、レスポンスの高いアプリケーション利用環境で構築する必要がある。

c. 組織内部の情報システムによるガード

情報システム面からの全体的な安全対策である。TCP/IP ネットワークによるユーザの権限の一元管理とシステマテックで確実な運用を可能にするとともに、強度のファイヤーウオール設置、ウイルス対策、システム管理全体のハード・ソフトの両面から安全対策を講じた構成などが必要である。本人認証の証の紛失・複製・濫用によるセキュリティ上の問題を解決するとともに、アクセス権限管理が容易且つ確実に行えるシステムが必要。

d. 社員教育による意識の高揚

個人情報保護法にもとづく規定の作成、マニュアル、訓練等による、人為的側面からの意識の高揚である。情報セキュリティとシステム運用の容易さや PC 周辺装置等の取り扱い基準が徹底した環境での業務の遂行が重要である。また、入退室・出退勤管理とも連動した全組織的な取り組みの統合管理など。たとえば、バイオメトリクス認証・ID/ パスワード・RF カードの利用とともにセキュリティ対策に対する意識の高揚を図ることである。

e. 追跡調査(監査証跡) による漏洩の抑止。

定められた規定の適切な運用と監査証跡 (入退室履歴) の保持が必要である。このため安全対策の啓蒙、漏洩発生時の早急な証跡追求などから、クライアント PC 管理やログデータ管理により抑止と追跡調査を可能にする必要がある。確実で且つ容易な履歴情報の管理、ネットワークでのログ一元管理、Excel 等

で加工が容易なファイルの生成などにより、すぐに役立つ追跡システムの構築である。

以上のようなアプローチで総合的な観点からセキュリティ対策に取り組む必要がある。本稿ではアクセス者の認証を中心に論じてきたが、他の課題の詳細については今後の研究テーマとして検討したい。

最後に、それぞれのバイオメトリクス認証の開発・実用化の現状と特徴を比較すれば、生体から特徴ある情報を抽出して数値化したDNA情報を用いる方法は、バイオメトリクスの中で最も有効であると思われる。しかしながら、開発や利用の仕方に余地を残しており、DNA認証はセキュリティとコストのバランスの面で、一般の実用化には若干遠いのが現状である。そして、複合使用によるバイオメトリクス認証は、単純なIDやパスワードの情報に比較して、安全度は飛躍的に高まるが正確で100%安全とは言い切れず、幾多の危険性を残すとともに紛失や盗難などの隘路を残している。

これらの問題を解決するには、現在では静脈認証が様々な面において優れており、この方法に他の認証方法を組み合わせるとともに、紛失や盗難で偽造を防ぐ手法が加えられることが肝要である。指の静脈認証は機械が小型・低コスト・高精度であることから今後、有効な認証手段として注目されるであろう。いずれにしても、プライバシー保護を十分に考えたシステムそして、セキュリティと使いやすさの共存する安全対策を早急に講じる必要がある。

注釈と引用文献

⑴ 法雲俊邑稿「オフィスの情報漏洩に関する一考察第1報」、OA学会2004年全国大会予稿集、pp.21-24、OA学会2004年11月。
⑵ 法雲俊邑稿「オフィスの情報漏洩に関する一考察第2報」、OA学会2005年全国大会予稿集、pp.67-70、OA学会2005年11月。
⑶ 情報漏洩に関するセキュリティ投資については、下記の文献を参考にした。「アッ

トマーク・アテイ情報セキュリティ投資講座」「情報漏えいに備えるセキュリティ投資の目安」、井上真一、2004/8/25、http://www.ATMarkit.co.jp/fsecurity/special/50invest/invest.html
(4) 経済産業省情報処理実態調査、http://www.meti.go.jp/polICy/it_polICy/statistICs/jyojitsu.htm
(5) 内田薫稿「指紋による個人認証の最前線」映像情報メディア学会、Vol.55 No.2 pp.176-179
および、バイオメトメトリクス全般の動向は (6) の URL を参照した。
(6) http://www.jaisa.or.jp/action/group/bio/Technologi
(7) 日経BP 社http://premium.nikkeibp.co.jp/ security/
(8) http://homepage2.nifty.com/medamacafe/J/iris_idntfctn.html
(9) 川崎雅也稿「「網膜」の識別でセキュリテイを守る」エレクトロニクス、オーム社、1998年。
http://www.jaisa.or.jp/action/group/bio/Technologies/Iris/Irs-f.htm
(10) http://journal.fujitsu.com/282/topstory2/
(11) http://www.hitachi-hec.co.jp/virsecur/shimonni/shimon01.htm
(12) 板倉征男，長嶋登志夫，辻井重男稿「個人識別用 DNA 情報の統計的検証」情報処理学会コ
ンピュータセキュリティ・シンポジウム2000、pp121-126 2000年10月。
(13) DNA 認証の動向は右記を参照。http://pcweb.mycom.co.jp/new
(14) 財団法人ニューメディァ開発協会では、平成 16 年度経済産業省業技術研究開発委託事業の成果として「生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化」を 2005年6月30日に下記URL に発表している。
http://www.nmda.or.jp/nmda/bio/
同様の成果を生体認証の脆弱性について、松本勉 (横浜国立大学)「金融取引における生体認証について」に詳しく報告している。http://www.fsa.go.jp/singi/
注. 本研究は星城大学高度ネットワーク社会研究所の 2005 年度の特別研究奨励費助成を受けて研究した成果の一部である。

補足資料

国会で成立した「偽造・盗難カード預貯金者保護法」の法律は 2006 年２月の施行で、それ以後の被害から補償が適用される。同法律は、偽造・盗難キャッシュカードによる不正な預金引き出しの被害について金融機関に幅広く補償を義務づけ、預金者保護の責任を問うものである。金融機関も偽造されにくいカードの導入など、「安全対策」の強化が求められる。ただ、この法律は ネット犯罪への対応が不十分で、残された課題も少

なくない。

全国銀行協会は今秋をめどに新法に沿った約款のひな型を作成する方針で、各金融機関がそれぞれ約款を改定した時点で、新しい補償制度が事実上スタートすることになりそうだ。

偽造・盗難カード被害に対する金融機関の保証割合

	偽造カード	盗難カード
預金者の過失程度	重過失　０％ 過失なし　１００％	重過失　０％ 軽過失　７５％ 過失なし　１００％

重過失　・他人に故意に暗証番号を教えた場合　・暗証番号を券面に書いた場合
軽過失　・誕生日などを暗証番号に使い、金融機関から何度も注意され変更しなかった
過失なし・上記以外のほとんどの場合

金融機関による補償は、ATM（現金自動預け払い機）からの預金引き出しと借り入れによる被害が対象になる。偽造カードと盗難カードに分け、被害者の過失の程度に応じて補償の割合が定められている。偽造カードは、暗証番号を他人に故意に教えるなど被害者に「重過失」があった場合以外は全額補償される。一方、盗難カードでは重過失のほか、誕生日など犯人に類推されやすい暗証番号を使い続けるなどの「軽過失」があった場合は補償額を被害の 75%にとどめるのが特徴になる。