



## 個人認証技術 - 指紋認証とその他のバイOMETRICS技術の応用 -

株式会社ディー・ディー・エス  
東日本営業課長 中野 慎二

### 個人認証技術の必要性

2005年4月1日より「個人情報保護法」が完全施行された。以前より情報漏洩対策に取り組んできた企業や、これをきっかけに対策に取り組んでいる企業を見ていると、何をどこまで対策すればよいのか戸惑いがある中で、試行錯誤している様子がうかがえる。

「個人情報保護法」に対して公表されている各種ガイドラインを読み解いてみると「アクセス制御・ログの保存・暗号化・入退室」という4つの共通するキーワードが浮かんでくる。但し、この4つの中でも「アクセス制御」というキーワードは、とかく解釈が分かれる部分である。外部または内部からの不正アクセス、人的またはシステム的な管理問題、と大変広範囲にわたり「これをすれば万全」という答えがないのである。

アクセス制御という部分でいえば、昨今、発生している情報漏洩事故の約80%は、外部からの不正アクセスではなく、内部からの不正アクセス（成りすまし）によるデータの持ち出しであるとされている。ここでいう内部からの不正アクセスを防ぐ方法として、最近注目を浴びているのがバイOMETRICSを利用した個人認証技術である。

### バイOMETRICSの適用例

従来から見受けられた入退管理用の装置のみならず、空港での出入国時における個人認証や、銀行でのATMにおける個人認証用として、様々なバイOMETRICS認証技術が実用化されてきている。“バイOMETRICS”と一括りに

されることが多いが、実は用途により市場における棲み分けが進みつつある。

これは大きく分別すると「防犯セキュリティ分野」と「情報セキュリティ分野」の違いであると捉えられる。「防犯セキュリティ分野」とは即ち現金に直結するような犯罪防止、例えば、カード盗難やピッキングが話題になっているATMやマンションの入退室といった用途などである。これに対して「情報セキュリティ分野」とは、PC内に保存されているような、まさに個人情報漏洩の類が該当する。

「防犯セキュリティ分野」において現在採用されている代表的なバイOMETRICSは、虹彩認証、指静脈認証、手のひら静脈認証、顔認証などである。一方「情報セキュリティ分野」において最も採用が進んでいるのは指紋認証である。この理由は「非接触方式か、接触式か」というセンシング方式によるところが大きく、前者がATMのような1つの装置を多数で利用する機器が中心であるのに対して、後者はPCなど1対1で利用されることが多いためである。また、後者において指紋認証が採用されている理由としては「コスト・大きさ・耐久性」などがあげられる。PC全てに設置することを考えると1クライアントあたり2万円前後が相場になってくるため、他の方式はまだ採用できないというのが現状である。

### バイOMETRICSの優位性

ここで少し「情報セキュリティ分野」に絞って、バイOMETRICSとその他の方式による個人認証の技術比較を行ってみる。

従来の個人認証といえば、パスワードによる認証がほと

んどであった。但し、このパスワード認証は、運用管理を誤るとセキュリティ上の脆弱性が露呈する。例えば、複数のパスワードを定期的に更新し、かつ使いまわしを禁止して常に新しいパスワードを設定するなど、全てを個人で管理させるためには相当な人的運用管理が必要になるであろう。管理を怠れば、安易なパスワードの組み合わせや、はたまたデスクトップに貼り付けるといった人まで現れる。それを防ぐために、これまでワンタイムパスワードトークン、USBキー、ICカードといったシステムで管理できるものが利用されてきた。但し、物理的なキーを利用する場合、紛失した時を想定し、予備キーを各部署に配備して貸し出しのログを報告するなど、厳密な運用方法を構築しなければ高いセキュリティを保つことができないという問題が常につきまとう。この運用面のコストは意外なほど大きい。バイオメトリクスがこれらの認証方式に代わるものとして注目を浴びているのは、単純に他人への貸し借りや、成りすましができないといった確実な本人確認手段ということだけではない。登録作業さえしっかりと行うことができれば、他方式に比べ運用面でのランニングコストが大幅に低く抑えられるというメリットを享受できるのである。

### 指紋認証システムの選択

「情報セキュリティ分野」において、最も採用されているバイオメトリクスである指紋認証のシステム導入要件を以下にあげる。

- クライアントPCに接続でき、小型で高い耐久性があること
- 1クライアントの導入コストが安価であること
- 各企業のセキュリティポリシーに応じた運用が可能であること
- 万人が利用できる指紋認証システムであること

、 については、近年の技術革新により小型・低価格化が進み、実用レベルまでできている。 については、サーバの管理機能により様々な運用が可能な製品も一部存在す

る。しかし、これら3つの要件よりも、最終的には を満たしているかどうか重要視されることが多い。従来の指紋認証システムのほとんどは、乾燥肌・指の磨耗・手荒れなどの要因により、登録および認証できない人が発生する。指紋認証システムの導入にあたっては、これらの要件を満たすことができる製品であるか、例外発生時にもセキュリティレベルを落とさない運用が可能な製品であるかをよく吟味する必要がある。

### 指紋認証システムの比較

登録拒否、認証拒否といった指紋認証システムの基本性能は、指紋照合アルゴリズムとセンサ方式の組み合わせにより左右される。

現在、製品化されている指紋認証システムの照合アルゴリズムを分類すると、次の3種類に大別される。

#### (1) パターンマッチング法

登録してある指紋の画像データとスキャンした指紋の画像データを比較するもの。精度が比較的低いほか、認証システムに指紋画像そのものを登録しておく必要があるという欠点がある。



図1 パターンマッチング法

#### (2) 特徴点抽出法(マニューシャ法)

指紋の端点、分岐点の属性や相対的な位置関係の特徴としてとらえ照合するもの。複雑な画像処理が必要であるた

め照合前処理に時間がかかる、登録拒否が比較的多いという欠点がある。

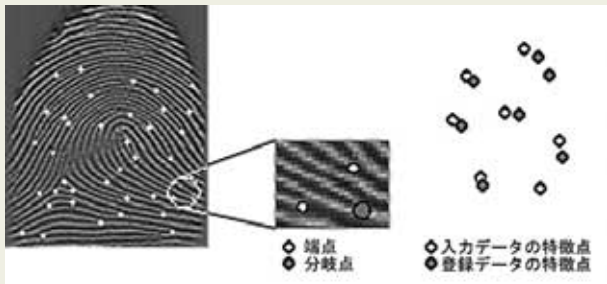


図2 特徴点抽出法（マニューシャ法）

### （3）周波数解析法\*

指紋をスライスしたときの断面を信号波形とみなし、周波数解析したものを特徴量として照合するもの。登録拒否が無く、処理時間が短い、指紋画像そのものを登録しないのでプライバシー侵害の可能性が無い、という特徴がある。

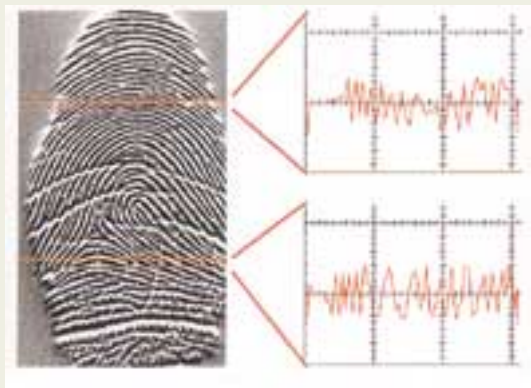


図3 周波数解析法

各アルゴリズムの特徴を表1に示す。

表1 アルゴリズム比較

	登録拒否	プライバシー保護	照合精度	かすれ影響
パターンマッチング法	原則無し			
特徴点抽出法	1~3%			
周波数解析法	原則無し			

表1にある登録拒否とは、指紋紋様の特徴部位が取得できず、指紋認証システムへ指紋情報を記録できないため、

利用者の登録が拒否されることである。周波数解析法とパターンマッチング法は原則的に指紋の紋様がある限り登録拒否が起こらない。

しかし特徴点抽出法は、特徴点の少ない指や女性の小さな指、手荒れにより特徴点が消えている指など、登録できない指が存在する。また、周波数解析法と特徴点抽出法が指紋画像を特徴量へ変換してから保存するため、画像を破棄するのに対して、パターンマッチング法は指紋画像そのものを保存する。また特徴ではなく、登録時の指紋画像そのものをマッチングさせるため、微妙な指の状態変化により認証拒否が発生しやすい。これらの理由により周波数解析法は登録拒否および認証拒否が無く、かつ安全であり、多種多様な人物の使用が想定される大規模企業での運用に向いているといえる。

センサ方式には、代表的なものとして、次の5方式があげられる。

表2 センサ方式の違い

光学式	指の表面の凹凸に従った反射光の強弱をCCD等を用いて画像化するもの
静電容量式	微小電極と指の皮膚との間に生ずる電位差を取り出して画像化するもの
電界式	指先とシリコンチップセンサ間に発生する電界の強弱を検出するもの
感熱式	指先と温度検知素子の間に生じる温度差を検知して画像化するもの
感圧式	指の凹凸に従って生じる圧力の違いを電位差として取り出して画像化するもの

表2のようなセンサ方式の違いは、指の状態により読み取り画像に大きな影響を与える。方式により一長一短があるが、指紋の状態に左右されずに認証に適した画像が取れるかどうかは重要な検討項目となる。乾燥湿潤に弱いものや、原理的に大きくならざるを得ないものなど、それぞれの特性を考慮して選択する必要がある。なぜならば、このセンサ方式と指紋認証アルゴリズムの組み合わせが、最終的にコスト、大きさ、認証精度といった指紋認証システムの仕様や性能差となって顕著に現れるからである。

その他にライン型のセンサを採用し、センサ上に残る残留指紋に対する問題や、指紋認証に対する従来の指紋押捺



図4 ライン型指紋センサを採用したユニット

イメージを払拭する製品も現れ始めている。

## ソリューションとしての指紋認証

弊社ではWindows PC 向けや機器組み込み向けなど、幅広く指紋認証ソリューションを提供している。

Windows PC向けにはソフトウェアライブラリとUSB接続の指紋センサユニット（図4参照）から構成されるシス

テムを提供している。クライアント・サーバ構成とすることができ、認証で使用する指紋情報やアクセスログなどの情報をサーバで一元管理することで、各企業のセキュリティポリシーに応じた運用を実現できる。

組み込み機器においても携帯電話、POSレジ、プリンタ複合機への搭載など様々な製品に指紋認証ライブラリを提供している。

今後は、認証精度の向上やユーザーインターフェースの改善を続け、指紋認証システム単体ではなく、様々なアプリケーションや組み込み機器と連携させたトータルセキュリティソリューションとして提供することにより、さらに利用分野を広げると共に、指紋認証が「情報セキュリティ分野」のメインストリームとなることを期待している。

\*周波数解析法：周波数解析法を用いた指紋認証アルゴリズムは、名古屋工業大学大学院梅崎太造教授が考案し、DDSと共同開発したものです。

本コラムは「ビジネスコミュニケーション2005年5月号」に掲載された記事を一部修正したものです。

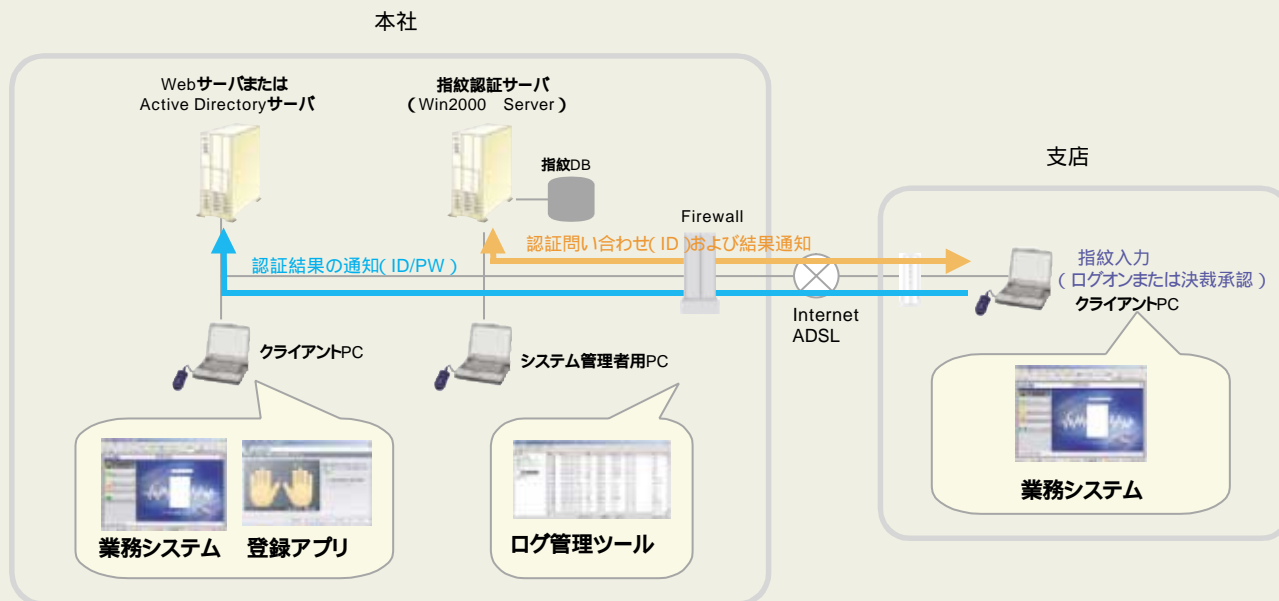


図5 Web業務システムへの指紋認証ログオンおよび決裁承認ボタンの指紋利用例