

# 静脈認証技術

矢嶋 秀敏, 田辺 竜也

Hidetoshi YAJIMA, Tatyua TANABE

## 1 はじめに

コンピュータの普及とともに以前はアナログで処理されていた膨大な情報も現在ではすべてデジタル処理がなされるように社会が変化してきた。デジタル化によりデータ管理の効率化や情報を高品質のまま維持することができるようになった。一方で個人または企業の情報漏えいになりすましや不正アクセスによって頻繁に発生している。この問題に対して IT 技術を駆使した情報漏えいの防止が試みられている。しかし、これまでに開発され実用化された手法ではセキュリティ面で完全に情報漏えいを防ぐことができていないのが現状である。そこで、この問題を改善するために開発され現在実用化され始めている技術が静脈認証技術である。この静脈認証技術を使用すればセキュリティレベルを向上させることができ、情報漏えいの危険性を低下させることができると期待されている。本報告では静脈認証技術について述べ今後の展望について述べる。

## 2 静脈認証技術

### 2.1 静脈認証とは

静脈認証技術とはバイオメトリクス認証(生体認証)の1つであり、認証方法としてユーザの静脈パターンがあらかじめ登録している本人のものと一致するかどうかを確認するものである。また使用される静脈の体の部位としては手の指先の静脈を用いて識別する。他にも手の甲の静脈を用いて識別する手法や手のひらの静脈で識別する手法などが現在開発されている。静脈認証の仕組みを Fig. 1 に示す<sup>1) 3)</sup>。

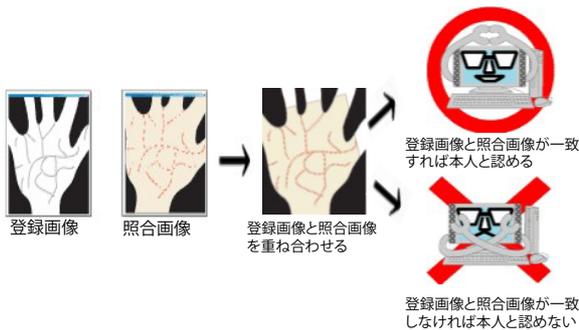


Fig.1 静脈認証<sup>(5)</sup>より参照)

### 2.2 静脈読み取りの原理について

静脈認証では近赤外線を用いて静脈の血管パターンを読み取る。血管パターンとは静脈の血管が網目のように広がった模様のことである。血液中のヘモグロビンは、肺

で酸素と結合すると酸化ヘモグロビンとなり動脈を通過して体の各組織に酸素を運ぶ働きをしている。そして、手のような酸素の乏しい末端で酸素を失うと、還元ヘモグロビンとなる。2種類のヘモグロビンは近赤外線の吸収率が異なり、還元ヘモグロビンの方がより多くの近赤外線を吸収する。この性質を利用して認証部位に近赤外線を照射し CCD カメラ等で撮影すると静脈の部分の暗く写る。これにより静脈の血管パターンを得られ静脈認証を行うことができる。しかし、体温の低下によって、認証に影響がでる場合がある。体温が下がると血流が緩やかになり血管が細くなる。そのため、近赤外線が静脈を透過しにくくなり、正しい静脈パターンの所得が困難となる。以下に静脈認証に用いられる代表的な手法を示す<sup>2)</sup>。

#### 2.2.1 透過型撮影方式

静脈の血管パターンを撮影する代表的な照明方式に透過型撮影方式がある。透過型撮影方式は認証部位以外に近赤外線を照射し、反射した光を CCD カメラ等で撮影するものである。具体例として以下に、認証部位が指の腹の場合について説明する。透過型撮影方式のイメージ図を Fig. 2 に示す。

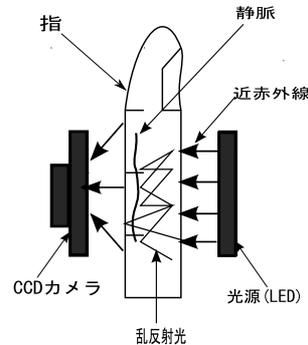


Fig.2 透過型撮影方式<sup>(8)</sup>より参照)

透過型撮影方式の装置の配置は、Fig. 2 のようになり、光源とカメラの位置は指をはさむ配置になる。この方式は静脈パターンを抽出するために、指の甲に近赤外線を照射する。静脈の光の吸収が他の組織と比べ相対的に大きいいため、CCD カメラに静脈が映し出される。これにより認証部位の静脈パターンを抽出することができる<sup>8)</sup>。

#### 2.2.2 反射型撮影方式

反射型撮影方式は 2.2.1 節の透過型撮影方式とは異なり、認証部位の表面に光を照射し透過した光を CCD カメラ等で撮影するものである。この方式も透過型撮影方式と同様に、認証部位は指の腹として以下に説明する。Fig. 3 に反射型撮影方式のイメージ図を示す。

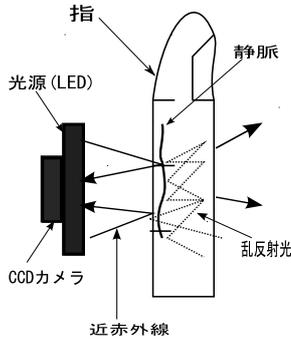


Fig.3 反射型撮影方式<sup>(5)</sup>より参照)

透過型撮影方式の装置の配置は、Fig. 3のような配置になる。反射型撮影方式は透過型撮影方式とは異なり、近赤外線を指先の腹に当てる。この方式では CCD カメラと光源の位置が同一方向にあるため、静脈で吸収されなかった光は CCD カメラには入らない。そのため、透過型撮影方式よりもよい静脈パターンが得られるので、反射型撮影方式のほうが認証精度が高い。また、CCD カメラと光源の位置が同一方向であることから、透過型撮影方式と比べ、装置のサイズは小さくすることが可能となる<sup>8)</sup>。

### 2.3 アルゴリズム

静脈認証装置を用いてユーザが認証を行うまでの流れを以下の Fig. 4 に示す。

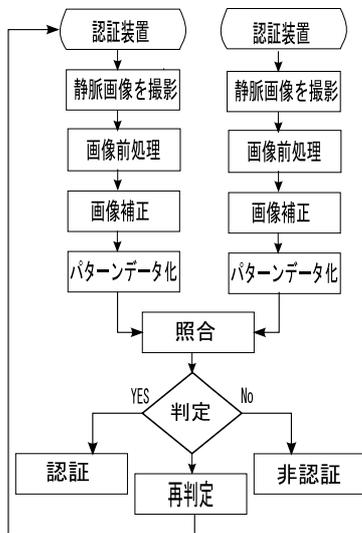


Fig.4 静脈認証のフロー<sup>(9)</sup>より参照)

1. 事前登録画像撮影  
データベースに格納する手の画像を撮影する。
2. 画像のデータ化  
1 で撮影した画像をデータベースに格納するために撮影画像をデータ化する。
3. データ格納  
2 でデータ化した画像をデータベースに格納する。

4. 認証装置  
認証させる手の部位を認証装置にセットする。
5. 静脈画像を撮影  
認証させる部位の静脈パターンを撮影する。
6. 画像前処理  
撮影した画像をデータ化する。
7. 画像補正  
データ化された画像はカメラとの距離、角度、位置により毎回異なるので画像を補正する。
8. パターンデータ化  
画像補正された画像データから静脈パターンを抽出する。
9. 照合  
データベースに格納された画像データとパターンデータ化された画像を重ね合わせる。
10. 判定  
照合を行い画像が一致すれば認証され、不一致の場合は非認証になる。判定が上手く行われなければ、4 のプロセスに戻り再び判定までの処理を行う。

ここで、7 の画像補正に着目する。CCD カメラ等で撮影された画像は、解像度が悪く血管の形状が鮮明ではない。よって、画像補正を行い、血管の形状をより鮮明し、照合を行う必要がある。もし画像の解像度が悪い画像で認証を行った場合、血管の形状が正しく得られず、認証精度が下がり適切な判定が行われなくなるからである。また、認証画像を撮影するとき、カメラに対して左右上下にずれたり、斜めの状態で撮影された場合なども画像補正する必要がある。これは、あらかじめ撮影され、登録してある画像が、カメラに対して正しい位置、角度で撮影されたものであるためである。この場合も画像補正を行わなければ認証精度が下がる。Fig. 4 の画像補正を行う流れを以下に Fig. 5 で示す。

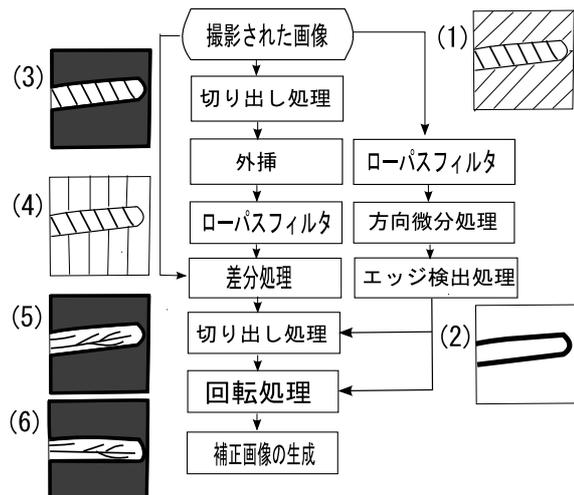


Fig.5 補正処理の流れ<sup>(11)</sup>より参照)

### 1. エッジ強調画像の抽出

撮影画像 (1) は指部, エッジ部, 周辺部に分割される. 画像 (1) はノイズが含まれているのでローパスフィルタによりノイズの細かい構造を除去し, 指輪郭等の大きな構造の強調を行う. その後方向微分処理を行い, エッジ強調画像 (2) を得る<sup>11)</sup>.

### 2. バックグラウンド画像の抽出

エッジ強調画像はエッジ部が大きな画素値を持ち, 検出したエッジの位置情報をもとに撮影画像 (1) から指部分のみを切り出し, 指の周辺部分に画素値 0 を挿入した図 (3) を作成する. さらに, 指のエッジ部の画素値がローパスフィルタ処理によって不必要に強調されることを防ぐために, この画像の指の周辺部分の値をエッジ部の値で上下方向に外挿し画像 (4) を作成する. そしてローパスフィルタ処理を行いバックグラウンド画像のみを抽出する<sup>11)</sup>.

### 3. 血管構造画像の抽出

撮影画像 (1) とバックグラウンド画像の差分処理を行い, 筋肉や骨等の透過光や散乱光によって発生するノイズに相当するバックグラウンド構造が除去できる. そして, 血管構造のみが強調された画像 (5) を得る<sup>11)</sup>.

### 4. 補正画像の作成

エッジ部の位置から指の傾きに応じて, その傾きが 0 となるように画像を回転させた画像 (6) を作成し補正画像を得る<sup>11)</sup>.

## 3 静脈認証のメリット

### 3.1 偽造が困難

現在用いられている認証方法としては暗唱番号と IC カードの組み合わせが主である. しかし暗唱番号は, 生年月日や身周りに関することで暗唱番号を設定するケースが多く, 類推される危険性がある. また, IC カードは盗難, 紛失の可能性がある. しかし, 体内情報を用いた静脈認証を駆使すれば, 撮影, 録音, 接触による手段から他人に盗まれる心配がない. 静脈の形状は人それぞれ独立しており決して同一の形状のものがないため, 現段階では偽造は不可能とされている. また認証を行う際に, 生体検知も同時に行っているため血流のない死亡者や人工の手のひらでは反応しない仕組みになっている<sup>3)</sup>.

### 3.2 コスト削減

IC カードを用いて出入管理を行った場合, IC カードの発行・印刷にコストがかかる. 静脈認証の場合は IC カードを携帯する必要がないので, IC カードの紛失・再発行の必要もなくなるためコスト削減につながる.

また, IC カードが不携帯の場合の使用するだけであるのでカードの発行・再発行・印刷の紛失の恐れもなくコスト削減ができる<sup>3)</sup>.

### 3.3 認識率と信頼性の高さ

静脈認証と他の生体認証の認証精度を比較するため, 被験者数 10 万人を対象とした各認証技術の本人拒否率と

他人受率を Table 1 に示す. 本人拒否率とは本人が静脈認証装置を使用した場合に本人と照合されなかった割合である. また他人受率とは第三者が静脈認証装置を使用した場合に登録者とは異なると照合した割合を示す.

Table1 本人拒否率と他人受率 (出典: 自作)

生体認証名	本人拒否率 (%)	他人受率 (%)
静脈認証	0.01 以下	0.00008 以下
指紋認証	0.1 以下	0.0001 以下
声紋認証	0.5 以下	5.0 以下
顔認証	1.0 以下	1.0 以下

Table 1 より静脈認証は他の生体認証と比べて本人拒否率, 他人受率とも一番良い結果である. よって静脈認証は認識率と信頼性が高いと言える<sup>10)</sup>.

## 4 静脈認証の実用例

### 4.1 銀行の ATM への設置

現在銀行の ATM で多く用いられている認証システムは IC カードと暗証番号の組み合わせが主である. しかし, 静脈認証技術を搭載した ATM が 2005 年 12 月に三井住友銀行に設置するに至った. そして, この ATM を使用する際にはあらかじめ IC カードに登録されている生体情報と使用者の生体情報の照合を行う. これによって, 暗証番号の管理や使用する必要もなくなる. また, カードを紛失した場合でも不正利用されることが無い<sup>7)</sup>.

### 4.2 患者の個人情報保護

個人情報保護法施行により 2005 年に東京大学医学部病院は情報部門を対象に富士通の静脈認証技術を採用し入室管理システムを構築し, 導入を行った. このシステムによりセキュリティレベルを事務室, 開発室, サーバールームに適用し各部屋の入室者の絞り込みを行っている. これにより, 患者情報を扱う人が制限され, 個人情報の不正流失を防ぐことができる<sup>6)</sup>.

### 4.3 ドア鍵の代替

近年ピッキングや車上荒らしの件数が増加している. 以前までそれらの防止策としてカードキー, 暗証番号などが使用されていた. しかし, カードキーの情報や暗証番号が流出, 偽造されることでロックを解除されてきた. この問題を改善するために, ドアノブに静脈認証装置を内蔵する. そうすることで鍵の携帯や暗証番号を覚える必要がなくなる. また, 静脈認証を使用しているため不正に侵入することが困難となりセキュリティを高めることにつながる<sup>6)</sup>.

### 4.4 自動車の鍵の代替

日立製作所は自動車のハンドルに指静脈認証装置を設置した. ハンドルに静脈認証装置を内蔵することでドライバーの照合を行う. このシステムはあらかじめドライバーの生体情報を登録しておく. ドライバーが照合を行い本人と一致した場合に自動でエンジンの起動やカーナ

ピの起動を行うことで利便性がよくなる。また、照合した時の静脈パターンでドライバーの識別を行う。それにより前もってユーザ毎に設定されているシートポジションのようなドライバーの使用に合わせた設定に自動的に設定を行うというシステムが開発された<sup>4)</sup>。

## 5 静脈認証の問題点

### 5.1 認証を譲渡できない

認証には本人の手が必要となるため他人に認証を譲渡することができない。そのため身体的な障害により腕が使えない場合や、外出できない場合など本人が認証を行えない場合は第三者が代理を行なうこともできない<sup>2)</sup>。

### 5.2 病気・怪我に起因する認証不可

怪我等をした状態で認証装置にかけると、事前登録した画像と一致せずに認証エラーが起こる場合がある。また貧血などの病気にかかりヘモグロビンの量が低下すると認証できなくなる場合がある<sup>8)</sup>。

## 6 今後の展望

現在、静脈認証装置の更なる小型化、軽量化や認証精度の向上させるために改良がなされている。今後、静脈認証装置を、ドアノブ、自動車、ケータイ電話のような私たちが日頃から使用しているものに取り入れることができれば、セキュリティの高い生活を送ることができるであろう。今後、静脈認証装置の普及率が上がれば、IDカード、ICカード、カギ等といった、私たちが常に手にしているものがこの社会から存在しなくなる日が実現するかもしれない。また、現段階では、静脈認証を破る偽証技術は開発されていない。

しかし、生体情報を偽証する技術が開発された場合、生体情報なので変更することができない。そのため万が一認証された場合に信頼性を回復することができないと思われる。そこで静脈認証と指紋認証を組み合わせるといったようなセキュリティレベルの高いものを複数組み合わせる技術を開発し完璧に近いセキュリティを実現することが望まれる。また、今まで認証に使用されていたカードや紙媒体も使用する必要が無くなるので環境問題の改善につながると期待される。

## 参考文献

- 1) 日立：指静脈認証の特徴  
<http://www.hitachi.co.jp/products/>
- 2) 日立：指静脈認証の仕組み  
<http://www.hitachi.co.jp/products/>
- 3) パイオオメトリクスについて  
<http://www.jaisa.jp/action/group/>
- 4) 日立：自動車ハンドル一体型静脈認証  
<http://www.blwisdom.com/word/key>
- 5) 富士通：手のひら認証  
<http://jp.fujitsu.com/group/labs/>
- 6) 東大病院：静脈認証の導入  
<http://www.keyman.or.jp/3w/prd/81/20010381/>

- 7) スキミング、偽造カード  
<http://allabout.co.jp/finance/creditcard/>
- 8) 反射型撮影方式、透過型撮影方式  
[http://www.jstage.jst.go.jp/article/jsmbe/44/1/27/\\_pdf/](http://www.jstage.jst.go.jp/article/jsmbe/44/1/27/_pdf/)
- 9) 静脈認証のアルゴリズム  
<http://www.veins.co.jp/whats.htm>
- 10) ソニー：指静脈認証技術  
<http://www.sony.co.jp/SonyInfo/technology/>
- 11) 画像補正  
[http://www.jstage.jst.go.jp/article/jsmbe/44/1/20/\\_pdf/](http://www.jstage.jst.go.jp/article/jsmbe/44/1/20/_pdf/)