金融取引における生体認証について

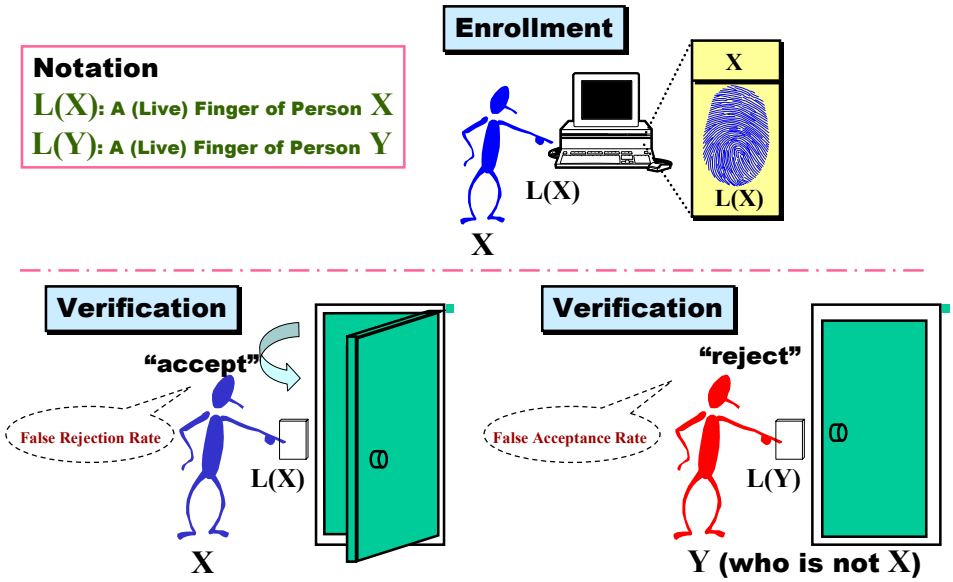
松本　勉
横浜国立大学　大学院　環境情報研究院

生体認証技術＝バイオメトリクス

- 「生体認証技術」は、
  - 身体的特徴や行動的特徴等、各個人に固有の特徴を用いて個人の認証を行う技術であり、「バイオメトリクス（biometrics）」、あるいは、
  「バイオメトリック個人認証技術」と呼ばれることも多い。
- ここでは、機械を用いた自動処理を行う生体認証技術について議論する。
- 「バイオメトリクス」という用語は、指紋や虹彩等、認証に利用される身体的あるいは行動的特徴そのものを指す場合もある。

生体認証システム

Notation
L(X): A (Live) Finger of Person X
L(Y): A (Live) Finger of Person Y



そもそも個人認証とは？

個人認証の問題 相手は本物か？
操作者は権利者か？

手段

- 記憶している情報
  （暗証番号、パスワード、・・・）
- 所持しているモノ
  （身分証明証、旅券、鍵、磁気カード、ＩＣカード、携帯電話、・・・）
- バイオメトリクス（"生体認証"）
  （身体的特徴＜顔・指・手・目・・・＞、
  行動的特徴＜声・筆跡・・・＞、・・・）
- 組合せ

各種個人認証技術の特徴一覧

方式	具体例	特徴	
		利点（一般の認識）	注意点
記憶	暗証番号、パスワード、 質問応答	簡単・経済性 広く普及	忘却・盗み見・推測
所持物	身分証明証、パスポート、 磁気カード、ＩＣカード、 ＵＳＢトークン、携帯電話機	操作が容易 広く普及 暗号技術の併用	要リーダライタ・コスト 紛失・盗難・スキミング 耐タンパー性 耐クローン性 暗号方式・実装の強度
生体認証 （バイオメトリクス）	指紋、掌形、虹彩、網膜、血管パターン（網膜、指、手の甲、手のひら）、顔、耳形状、 声紋、筆跡、歩き方、 キーストローク、匂い （ＤＮＡパターン）	利便性 万人不同 生涯不変（？） 偽造は困難（？）	読取装置が必要・コスト 本人拒否率・登録失敗 生涯不変（無効化が困難） 心理的抵抗感 機微な個人情報

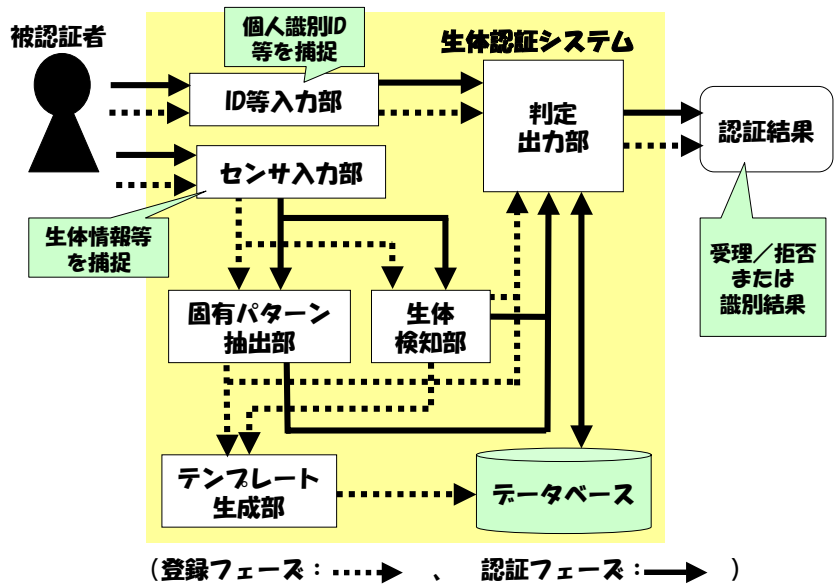
生体認証技術のわが国の金融分野における動向

- 従来から、一部の銀行において事務センター等における職員の入退室管理等の手段として指紋認証技術等が採用されていたが、最近では、銀行の窓口やATMにおける顧客の本人確認の手段とし生体認証技術が活用される場面が増えてきている。
- 金融分野での動向は、金融情報システムセンターによるアンケート調査や調査報告において具体例を交えつつ紹介されている（FISC［2004, 2005］）。
- 顧客向けサービスへの適用をスタートしているものとして、手のひらの静脈パターンを用いた生体認証技術を採用しているスルガ銀行（スルガ銀行［2004］）と東京三菱銀行（東京三菱銀行[2004］）の事例がある。
- このほか、三井住友銀行、みずほ銀行、日本郵政公社が、指の静脈パターンを利用した本人確認方式の採用を予定している（三井住友銀行［2005］、みずほ銀行［2005］、日本郵政公社［2005］）ほか、広島銀行、池田銀行、北海道信金共同事務センター加盟の19の信用金庫が、手のひらの静脈パターンを利用した本人確認方式の導入を予定している（広島銀行［2005］、池田銀行［2005］、北海民友新聞社［2005］）。

金融庁のガイドライン・実務指針

- 「個人情報保護に関する法律」に対応し、金融庁が、「金融分野における個人情報の保護に関するガイドライン」を2004年末に公表したほか、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」（以下、単に実務指針と呼ぶ）を2005年はじめに公表しており、金融サービスにおける顧客の本人確認等に用いられる生体情報の管理方法について規定している。
- 一般的に規定されている個人情報の安全管理措置に加えて、生体認証情報に関しては、追加的に次の措置について規定に盛り込まなければならない旨が実施指針の別添2に規定されている。
  - 生体認証情報を登録する際における、なりすましによる登録の防止策、本人確認に必要な最小限の生体認証情報のみの取得、生体認証情報の取得後に基となった生体情報の速やかな消去に関する事項
  - 認証時における、偽造された生体認証情報による不正認証の防止措置、登録された生体認証情報の不正利用の防止措置、残存する生体認証情報の消去、認証精度設定等の適切性の確認に関する事項
  - 生体認証情報の保存時における、生体認証情報の暗号化、氏名等の個人情報との分別管理に関する事項
  - 生体認証情報を本人確認に用いる必要がなくなった場合における、生体認証情報の速やかな消去に関する事項
- なお、金融情報システムセンターでは、「生体認証情報の管理」に関する「金融機関等コンピュータシステムの安全対策基準・解説書」改訂を2005年春に行っている。

生体認証システムの構成（概念図）



生体認証システムにおけるなりすましに関する脆弱性と対策のポイント

脆弱性の名称	対策を検討する際に考慮すべき主なポイント
他人受入	・誤受入率や誤合致率等の認証精度指標とその評価
狼（wolf）	・誤受入率や誤合致率等の認証精度指標とその評価 ・脆弱性を引き起こす可能性がある生体情報を有する個人が存在する割合、および、その影響度
子羊（lamb）	
類似性	
偽生体情報	生体情報の物理的な偽造の難易度の評価（クローン受理率やクローン一致率に類似の指標に関する検討等） ・生体検知機能の採用
公開	・生体情報捕捉の難易度
推定	・生体情報とその照合結果を外部に漏洩させない手段
利用者状態	・品質の低い固有パターンの登録を回避する手段
入力環境	
認証パラメータ	・パラメータの適切な選択とその設定に関する管理・運用方法
登録	・登録時における本人確認方法
データ漏洩	・システム内部で処理・保管されるデータの機密性、一貫性を確保するとともに、後日再度の検証を可能にする手段
データ改ざん	
単独	・生体認証システムおよびその代替認証手段に求められるセキュリティ要件と、適切なセキュリティ評価
代替手段	
提供	・脅迫等による脅威への対策
サイド・チャネル	・想定されるサイド・チャネル攻撃への対策
センサ露出	・センサに生体情報が残留しない手段　・生体検知機能の採用
構成管理	・生体認証システムの設計・テスト・評価

生体部分でない対象物の受入可能性に関する考察

- 生体認証システムでは対象とする
  生体部分（指、手の甲、手のひら、目、顔など）を、
  光などの手段を用いて計測している。
  従って，
  - 光などで見て生体部分と同じように見える対象物であれば、
    生体認証システムに受け入れられる可能性があるが、
  - バイオメトリクス入力装置に提示される対象物が生体であるかどうかを検知する何らかの“生体検知”機能がうまく組み込まれ、
    うまく働いているならば、
    そのような対象物は登録も照合もできないことになる。
- しかし、生体認証においては、利用者・管理者の利便性を重視し、登録失敗(Failure to Enroll)や誤拒否(False Rejection) ができるだけ少なくなるような設定がなされることが多い。
- このため、バイオメトリクス入力装置に、人間の生体とは限らない何らかの対象物が提示された場合でも、生体検知のメカニズムがうまく働かず、これを拒否することに失敗することがある。

生体検知＝Liveness Detection

- 生体認証システムにおいては、身体的あるいは行動的特徴の照合だけでなく、
  - 生体情報が生きた人間の身体から直接提示されているか否かを確認する機能（以下、生体検知機能と呼ぶ）

  を利用して認証を行う場合がある。

- 生体検知機能の実現方法は、認証時に用いられる生体情報に依存し、多種多様な手法が提案されている。具体的な手法に関しては、各種の特許資料や、Schuckers [2002]、Valencia and Horn [2003]、Sandström [2004]、Daugman [2004b]といった文献において紹介されている。

- ただし、市販されている生体認証システムにおいて実際にどのような手法が採用されているかについては、あまり公開されていない。

生体検知機能の実現方法の分類例

- (1)生体に固有の性質を利用する方法、(2)生体から自然に発せられる情報を利用する方法、(3)外部からの刺激に応じて生体から発せられる情報を利用する方法に分類して議論されることがある（Valencia and Horn [2003]ほか）。

  (1)生体に固有の性質の例
  　皮膚における光の吸収・反射、色の変化
  (2)生体から自然に発せられる情報の例
  　脈拍、体温
  (3)外部からの刺激に応じて生体から発せられる情報の例
  　光に対する瞳孔の変化

実験において評価者に与える知識

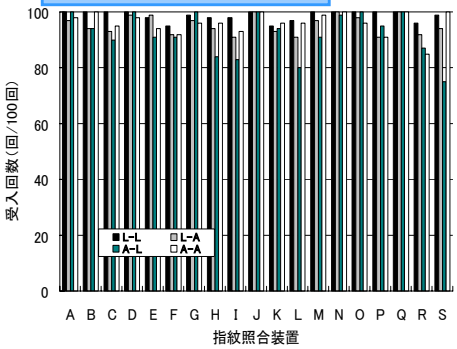
- 評価対象である生体認証システムについて、
  どのような知見を得ることを目的とするかで、評価の方法は変わりうる。
  すなわち、評価対象である生体認証システムにおける、
  バイオメトリクス入力装置や照合・認証の方式に関する知識が評価者に
  全て与えられている場合、
  全く与えられていない場合、そして
  その中間的な場合
  がありえる。
- 以下でご紹介する研究では、評価対象システムを
  ほぼブラックボックスとして扱う場合
  で検討した。すなわち、装置の分解やソフトウェアの解析は行わず、システムについてカタログ等で公表されている情報は参考にするという場合である。
- ただし、最強の攻撃者による攻撃に関して評価する際には、
  攻撃者は開発者と同等の知識を有しているとして扱うことが妥当である。
  特に、ユーザの手元に渡るシステムである場合にはそのような厳しい条件
  における評価が必要な場合があろう。

生体部分でない対象物の受入可能性に関する検証方法

- 与えられた生体認証システムの生体検知機能がどの程度であるかを実験的に把握する必要が生じた場合に考えられる評価の方法には、次の２段階が考えられる：
  第１段階
  生体認証システムに生体でない対象物を提示し、
  （A）登録できるかどうか、
  （A-A）登録できた場合，再度提示して照合できるかどうか
  について調べる。
  第２段階
  生体認証システムに
  （L-A）生体部分を登録し、生体でない対象物で照合できるかどうか、
  （A-L）生体でない対象物を登録し，生体部分で照合できるかどうか
  について調べる。
- ここに示した第１段階はいわば対象物の**素材に関する検討**であり、第２段階は、第１段階の実験に成功した素材を用いて生体部分を模擬した対象物を作成し、実施することが妥当だと考えられる。
- ただし、第１段階の（A）が成功しない、すなわち、システムに登録ができない対象物であっても、第２段階の（L-A）が成功する可能性があることには注意を要する。

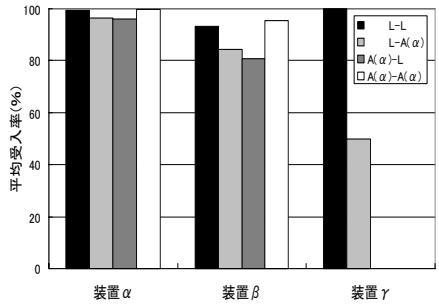
指紋・虹彩認証システムの脆弱性評価の現状

指紋照合における脆弱性



ゼラチン等を材料として，
・ 生体指から直接かたどった人工指
・ 遺留指紋から作製した人工指
が，一般に入手できる19機種以上の指紋照合装置に，高い割合で受け入れられた．

虹彩照合における脆弱性



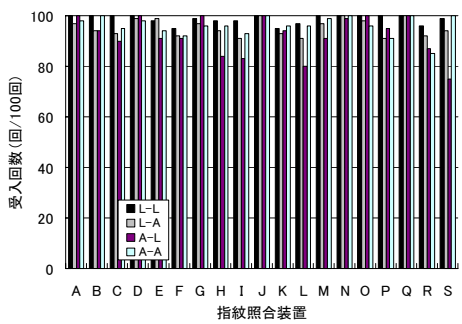
・ 装置の使用時に入手出来る虹彩画像
・ ディジタルマイクロスコープでの撮影で入手出来る虹彩画像
を紙に印刷し作製した人工虹彩が，一般に入手できる3機種の虹彩照合装置に，高い割合で受け入れられた．

なお、日経バイト２００５年４月号（３月２２日発行）の
BYTE LABにおいても最新の１８機種の照合装置に対する実験結果が紹介されている。

指紋照合における生体部分でない対象物の受入可能性に関する検証

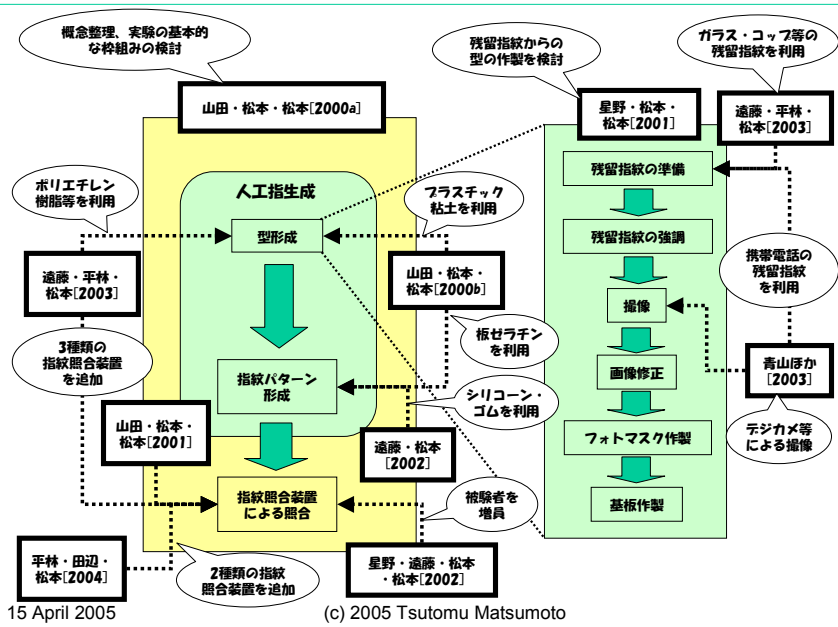
これまでの研究により、指紋照合については、第１段階においては、ゼラチンや導電性シリコーンゴムなどを材料として作製した対象物（人工指）が、光学式、静電容量式、電界式、指内散乱光直接読取り方式、感圧式の、実験した１９機種以上の全ての指紋照合システムに登録（A）・照合（A-A）できることを確認し、かつ、第２段階の（L-A）、（A-L）の照合もすべてのシステムにおいて行えることを示している。

ゼラチン製人工指

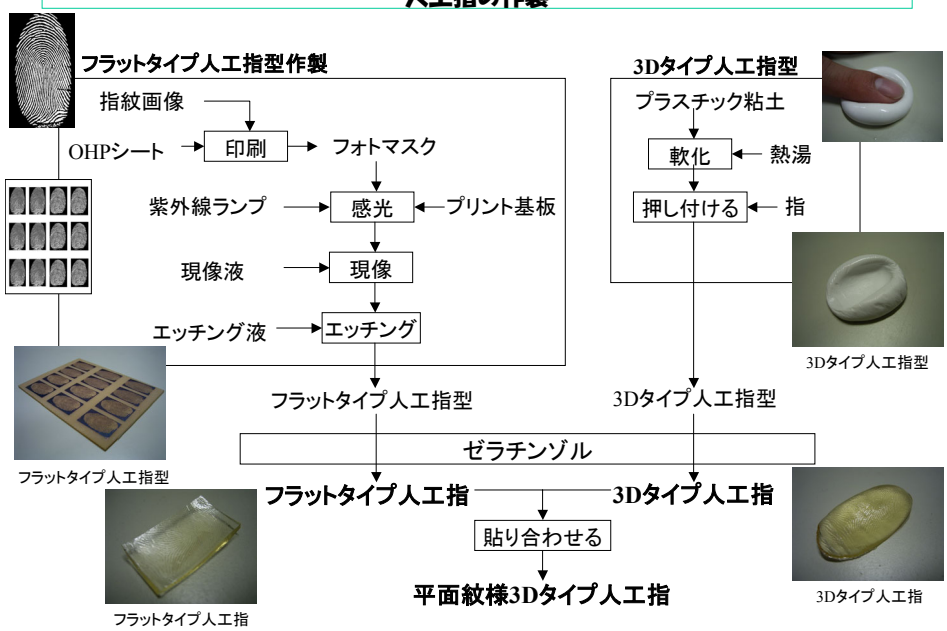


ゼラチン等を材料として，
・ 生体指から直接かたどった人工指（3Dタイプ人工指）
・ 遺留指紋から作製した人工指（フラットタイプ人工指）
が，一般に入手できる
19機種の指紋照合装置に，
高い割合で受け入れられた．
装置A～E，J，K　光学式
装置F～I　静電容量式
装置O　指内散乱光直接読取式
装置P　感圧式
装置Q　感熱式
装置R，S　電界式

指紋照合（認証）装置の脆弱性評価の研究の流れ

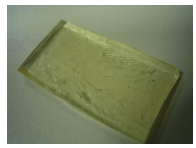


人工指の作製



指紋照合における生体部分でない対象物の受入可能性に関する検証

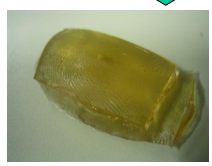
- また最近、携帯電話やＰＫＩトークン用の指紋照合システムについても評価を行い、全く同様の結果を得ている。なお、その際に、スイープ型の指紋入力装置を有する指紋照合システムの評価に用いる人工指として、指紋画像でエッチングしてできたプリント基板を型として作製したフラットタイプのゼラチン製人工指を指状のゼラチン製の棒にゼラチンで接着したもの（平面紋様３Ｄタイプ人工指）の作製プロセスを新たに開発した。

①薄めのフラットタイプ人工指を作製


②紋様を持たない3Dタイプ人工指を作製

ゼラチンゾルを接着剤として②の曲面に沿って
①をきれいに貼り合わせる



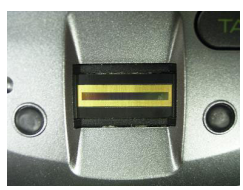

完成した平面紋様3Dタイプ人工指

田辺・森下・松本
電子情報通信学会
暗号と情報セキュリティ
シンポジウムSCIS 2005
2005年1月

最近の研究対象の例----携帯電話搭載指紋照合装置---

		装置S	装置T	装置U
指紋読取装置	製造者	Authentec	Authentec	STマイクロエレクトロニクス（UPEK）
	名称	EntrePad	EntrePad	TouchStrip™ Solution
	型番	AES3400	AES2501 もしくは AES2510と推測	TCS3-TCD41
	製造番号	0AF00555	AAF09161	NFJFC209441
	読取方式	エレクトリック フィールド式（電界式）	エレクトリック フィールド式（電界式）	CMOS active capacitive pixel-sensing

※上記の仕様表はウェブページなどを元に筆者が独自に作成。




装置S　装置T　装置U

- これらの結果は、現状で実装されている指紋照合技術の脆弱性を示しており、指紋照合によるセキュリティ向上を目指すアプリケーションに導入される指紋照合システムにおいては、利便性の低下をできる限り抑えた上での生体検知機能の充実を工夫していく必要があることが明らかである。
- なお、たとえば、*Biometrics Consortium Conference 2004* にて米国のLumidigm 社により複数波長で指を計測する技術が発表されるなど、ゼラチン製人工指を受け入れないようにできるとする技術はいくつか発表されている。ただし、製品化されたものを筆者らが実機にて実験をする機会には恵まれていないので、未検証である。
- また、もはや、指紋照合技術というよりは、指照合技術ないし指認証技術にシフトしているので、どこまでを指紋照合技術と呼ぶかの検討が必要な時代が到来しつつある。
- いずれにしても、シリコーンゴム、導電性シリコーンゴム、ゼラチンなどの材料で作製した対象物（人工指）を指紋照合システムに提示して第１段階（Ａ）、（ＡＡ）、第２段階（ＬＡ）、（ＡＬ）の実験を行い、どの程度の割合で受け入れられるかを測定することは、生体部分でない対象物の受入可能性に関する指紋照合システムの脆弱性評価方法として意味がある。このために、対象物の材料や作製方法や実験方法について標準的プロセスを定めることが有用であり、具体的な検討が必要であると考えられる。

静脈認証における生体部分でない対象物の受入可能性に関する検証

松本-鉢嶺-森下-佐藤、「バイオメトリクスにおける生体検知と登録失敗---静脈認証に関する速報---」電子情報通信学会技術研究報告 ISEC2004-141, 情報セキュリティ研究会、京都大学、2005年3月18日から紹介。

- 静脈認証技術は金融分野へのアプリケーションを中心として最近急速に注目を浴びている技術であり、指の静脈、手の甲の静脈、手のひらの静脈を用いるものが存在している。静脈照合ないし静脈認証と称しているが、対象とする生体の何を観測しているかなど、技術の詳細はあまり開示されていない。
- 指紋照合や虹彩照合のように、まず、生体でない対象物が受け入れられる可能性があるかどうかについて、第１段階の実験を試してみることが有用であろう。すなわち

  （Ａ）静脈認証システムに生体でない対象物を提示し、登録できるかどうか調べる

  （Ａ－Ａ）登録できた場合、再度提示して照合できるかどうかについて調べる

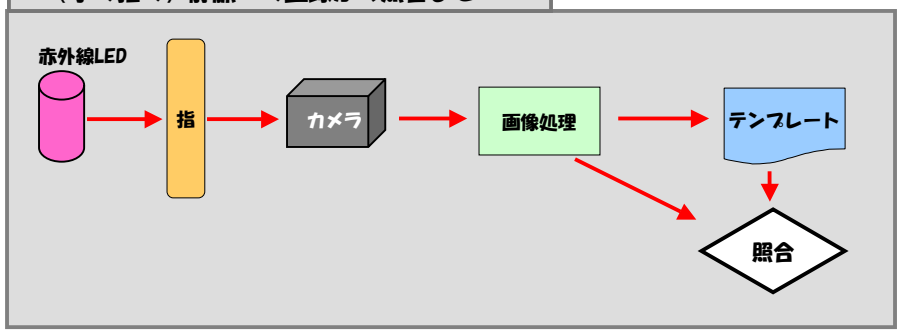
  の２つの実験を行うことが必要であろう。
- 静脈認証システムは、光などにより指や手を計測していると考えられる。従って、光などで見て指や手と同じように見える対象物であれば，静脈認証システムに受け入れられる可能性がある。

静脈認証技術の概要

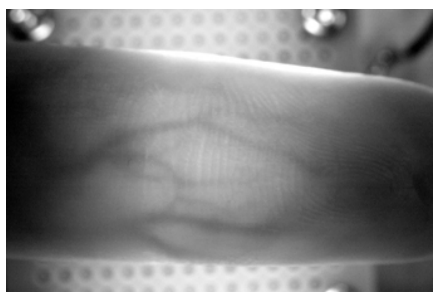
静脈の取得方法

静脈には還元ヘモグロビンが流れている．この還元ヘモグロビンが，近赤外光領域（約760nm）の波長の光を吸収する性質を静脈認証に利用している．そのため，手のひらや手の指に近赤外光をあてると静脈が存在する部分だけ光が多く吸収され，画像上暗く映しだされる．これを画像処理により抽出し，静脈パターンとして登録・照合を行う．

“（手の指の）静脈” の登録から照合まで



指静脈の撮影例



撮影：松本研究室

- 光の分散の具合が人間の指や手と類似の対象物の候補としては、
  - 植物（野菜）などを生体部分に類似の形状にしたものなど、
  - 適当なポリマーと硬化性樹脂を混ぜて作製した物体など
  - その他

  が考えられる。

- ある特定の静脈認証システムにおいて、もしこれらを用いた第１段階の実験が成功したとするとそのシステムの生体検知機能に脆弱性があることが判明する。

- この第１段階の実験で吟味された材質で個人性のある指や手のパタンを有する対象物を作り、第２段階の実験を実施するというプロセスが考えられる。

- 個別の静脈認証システムについて実験を進め、生体でない対象物の受入可能性についての評価の方法を、指紋照合技術と同様に整備していく必要がある。

実験に用いた静脈認証システム

本稿における名称		システムFV
製品名		指静脈認証システム　静紋
型名		K－Y100－10000
認証の方式		正規化指静脈マッチング方式 開発：（株）日立製作所 中央研究所
撮影方法		透過型
Interface		USB1.1
寸法(mm)		約80(W)×110(D)×120(H)
認証	証証精度	他人受け入れ率：0.0001% 本人拒否率　　：0.01%
	照合方式	1対N照合
機能		Windowsログオンおよびスクリーンセーバロック解除時の指静脈による認証
製造者		日立ソフトウェアエンジニアリング（株）
参照URL		http://www.ms.hitachi-sk.co.jp/joumon/

実験の概要

- 実験で用いた静脈認証システムFVに提示するものとしては，
  L：人間の指と，

人間の指でない対象物として，
  A1およびA2：植物である大根
  A3およびA4：全くの人工物

を検討した．

（1）A1，A2：大根スティック：
  大根を人間の指の大きさになるようにスティック状にカットし，
  料理用のラップで包んだもの．
  A1とA2は異なる個体である．

（2）A3，A4：人工雪剤＋エポキシ樹脂：
  人工雪剤 30gとエポキシ樹脂の主剤15gをよく混ぜ，
  さらに硬化剤8gを加えよく混ぜて，
  透明ビニール管（A3は内径18mm，A4は内径15mm）に注ぎ，
  約18時間室温で放置し固め，
  硬化後ビニール管から取り出して作製．

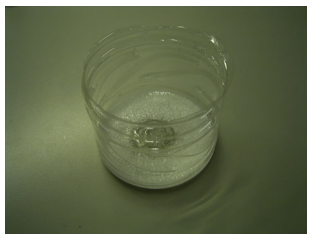
材料

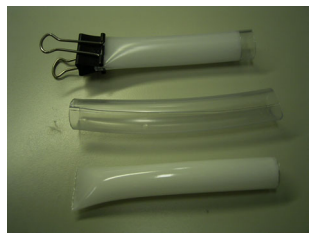
人工雪剤 “スノーパック”
製造元：株式会社スノーヴァ
主成分：ポリアクリル酸塩系特殊吸水性ポリマー

透明・低粘度エポキシ樹脂 “クリスタルレジン”
製造元：日新レジン株式会社
型番：N4L01N｛1，2｝

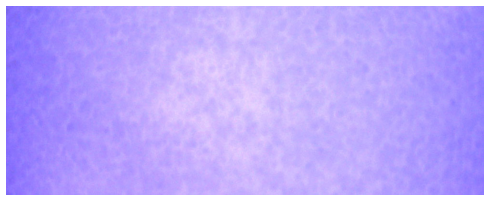
野菜（大根スティック）

対象物（人工物）の作製





人工物の赤外線撮影画像



システムＦＶに対する実験結果

照合パターン	受け入れ回数（回）	備　考
L－L	91/100	左手中指
A1－A1	100/100	大根スティック 実験日当日に登録
A2－A2	98/100	大根スティック 実験日1週間前に登録
A3－A3	100/100	人工雪剤＋エポキシ樹脂 （直径18mm）
A4－A4	100/100	人工雪剤＋エポキシ樹脂 （直径15mm）

- システムFVには当然であるが，人間の指Lが登録でき，照合もできる．表にはその受入回数の実験結果も示している．
- 第１段階の実験（A）におけるシステムFVへの対象物の登録については，A1，A2，A3，A4ともに行えた．
- そこで実験（Ａ－Ａ）に進んだ。その結果、表のように、どの対象物も高い割合で照合が行えた。
- 表において、照合パターンにα－βとあるのは、αを登録しβで照合を試みたことを示している。なお、対象物の提示は１人の実験者が行った。

脆弱性評価実験からのインプリケーション

- 生体部分でない対象物の提示による脆弱性評価の方法に関する検討を行った。第１段階の実験、第２段階の実験というステップ構成で脆弱性評価を行うことが有益である。個々のバイオメトリック認証技術が対象とする生体部分について、評価のための（テストチャートないしリトマス試験紙に対応する）対象物の吟味と標準化を行うことにより、特定のバイオメトリック認証システムのセキュリティレベルを測ることができる可能性が明らかとなった。

- 特定の具体的生体部分の代わりをする対象物による不正の３ステップと対策としては
  - ①生体部分に関する情報入手　←　偽ＡＴＭ等の排除
  - ②対象物の作製　←　生体検知機能の充実
  - ③対象物の使用　←　監視・運用面での対応

  といったことがらがポイントとなるであろう。

おわりに（１）

- 生体認証技術は、個人を認証する有力な技術の1つとして現在注目を集めており、入国管理等の公共部門において今後活用される見通しであるほか、金融サービスにおいても顧客の本人確認手段として採用する動きがみられている。また、わが国では、こうした動きに先立って生体認証技術の精度評価に関する標準規格等が既に策定されたほか、ISOにおいては、関連する国際標準の審議が活発に進められているところである。

- 生体認証技術を採用する動きが広がる中で、それらを安全に活用していくために、生体認証システムに内在する脆弱性にこれまで以上に注意を払っていく必要がある。既に明らかになっている脆弱性の中でも、人工指や人工虹彩に代表されるように、物理的に偽造された生体情報を受け入れてしまうという脆弱性に今後注目していくことが求められる。
- こうした脆弱性に対抗する生体検知機能に関する研究についても、その動向を注視する必要があろう。

おわりに（２）

- 特に、幅広い層の顧客が利用する金融サービスにおいて生体認証技術の導入を検討する場合には、少なくとも既に明らかになっている脆弱性を考慮し、候補となっている生体認証システムにおいてそうした脆弱性が存在するか否かを厳格に確認することが必要であると考えられる。
- 本発表では、いくつかの生体認証技術の脆弱性について解説したが、こうした研究蓄積の存在は、これらの技術の安全性を客観的に評価することを可能とするものであり、研究蓄積が存在する技術は、研究蓄積がないものに比べて相対的に信頼できるとも言える。
- この点、まだ評価の対象となっておらず、脆弱性に関する報告があまり行われていない生体認証技術については、当該分野の専門家に評価を依頼し、その結果を慎重に検討したうえで、実際に採用するか否かを判断すべきである。

おわりに（３）

- また、既知の脆弱性だけでなく、未知の脆弱性についても将来顕現化することを想定し、新たな脆弱性への対応方針とそのための体制整備を進めておくことが必要である。具体的には、
  - 拡張性の高い生体認証システムの実現、
  - 脆弱性に関する情報の収集・分析や、
  - 発見された脆弱性の影響等に関する情報の迅速な提供を可能にするための体制整備

  等について検討することが考えられる。
- こうした点に留意して脆弱性に対して適切な措置を講じ、安全で信頼性の高い生体認証システムが継続的に利用可能になることが望まれる。今後も、生体認証技術とその脆弱性に関する動向に注目していく必要があろう。

著者連絡先：松本 勉 （横浜国立大学大学院環境情報研究院）
電子メイル tsutomu@mlab.jks.ynu.ac.jp

参考文献

- 「生体認証技術の最新動向と金融機関における活用」金融情報システム、No. 276、平成17年冬号、金融情報システムセンター、2005年1月1日
- 「「生体認証情報の管理」に関する「金融機関等コンピュータシステムの安全対策基準・解説書』改訂」金融情報システム、No. 277、平成17年春号、金融情報システムセンター、2005年4月1日
- 松本勉・鉢嶺拓二・森下朋樹・佐藤健二、「バイオメトリクスにおける生体検知と登録失敗---静脈認証に関する速報---」電子情報通信学会技術研究報告 ISEC2004-141, 情報セキュリティ研究会、2005年3月18日
- 堀内かほり、BYTE LAB 「濡れた指、乾燥した指----指紋認証の実際」NIKKEI BYTE、2005年4月号、pp. 60-67、日経ＢＰ社（2005年3月22日発行）
- 宇根正志・松本勉、「生体認証システムの脆弱性について―身体的特徴の偽造に関する脆弱性を中心に―」日本銀行金融研究所ディスカッション・ペーパー・シリーズ　2005-J-2、
  http://www.imes.boj.or.jp/japanese/jdps/jdps2005_index.html
  http://www.imes.boj.or.jp/japanese/jdps/2005/05-J-02.pdf
  （2005年3月24日掲載）
- 松本勉、「金融取引のセキュリティ問題と個体認証技術」週刊金融財政事情、第56巻第1号、pp. 36-42、2005年4月11日