

# 1

## バイオメトリック認証の脆弱性 —身体的特徴の偽造問題—

松本 勉

横浜国立大学大学院環境情報研究院  
tsutomu@mlab.jks.ynu.ac.jp

### バイオメトリック認証システム＝ 生体認証システムの活用に向けて

バイオメトリック認証システム (Biometric System, 以下本稿では生体認証システムと記す) とは、個人に固有の身体的な特徴 (指紋、掌形、顔、虹彩、網膜、静脈 (血管) パターン、耳形状など) や行動的な特徴 (声紋、手書き署名 (筆跡)、キー・ストローク、歩行パターンなど) を用いて機械が個人の認証を行うバイオメトリック認証技術 (Biometrics, 以下本稿では生体認証技術と記す) を具現化した個々のシステムのことである。生体認証システムは生体情報の取得と処理とそれらに基づく個人認証管理を行う機器とソフトウェアなどから構成される。本稿では、身体的あるいは行動的特徴とその利用の方法を総合した様式 (modality) として M (たとえば「指紋」「顔」「虹彩」「静脈」「音声」「手書き署名」など) を用いる生体認証システムを、M 認証システムということにする。

生体認証システムの適用の歴史は長く、限定された利用者を対象とする組織において、重要な情報システムでの利用を中心として、一定の利用が古くからなされてきた。たとえば、厳重な警備が必要な建物や部屋への入退室管理や、サーバ計算機や監視カメラの使用に関するアクセス管理などで利用されてきた。近年の特徴は、生体認証の適用分野が多岐にわたり適用事例も爆発的に増加の傾向にあることである。具体的には、携帯電話や銀行カードの利用者認証、ノート PC へのログインやアプリケーションの利用者認証、ネットワーク上の取引での個人認証、集合住宅における入室管理、さらには空港等における入出国管理の本人確認手段としての利用など、多くの事例を挙げることができる。

生体認証システムをより良く活用していくためには、利用者、情報システム構築者、運用者、そして技術の提供者が、生体認証技術の利点や注意点・脆弱性をよく理解することが重要であることは言うまでもない。その上で利用者、情報システム構築者、および運用者は、そのセキュリティポリシーに見合った生体認証システムを採用することが望ましく、また、生体認証技術の提供者はそれらのニーズに合致した生体認証システムを提供することが望ましいといえよう。ただし、セキュリティ技術として達成できるセキュリティレベルの可能性と、実装された個別のシステムにおける実際のセキュリティを混同しないように注意する必要がある。つまり、同じ様式の生体認証システムでも、高いセキュリティのものから低いセキュリティのものまでの多様なものが存在し得るため (図-1 参照)、個別のシステムに対してセキュリティを評価 (計測) することの重要性が見てとれるであろう。

本稿では、生体認証システムが持つセキュリティ上の脆弱性、とりわけ生体を模擬したニセモノを受け入れる可能性を示し、その本質的なメカニズムの考察を行う。それを踏まえ、生体認証システムのセキュリティを評価する方法の開発とその活用が大切であることを述べる。

### 個人認証の方法としての生体認証の特徴

個人認証の基本的方法には大別して、本人だけが知っている情報を用いた暗証番号・パスワード・質問応答などの技術、本人だけが所持している身分証明書、パスポート、ICカード、携帯電話機などの物による技術、それから生体認証技術がある (表-1 参照)。これらは組み合わせられて利用することも多い。

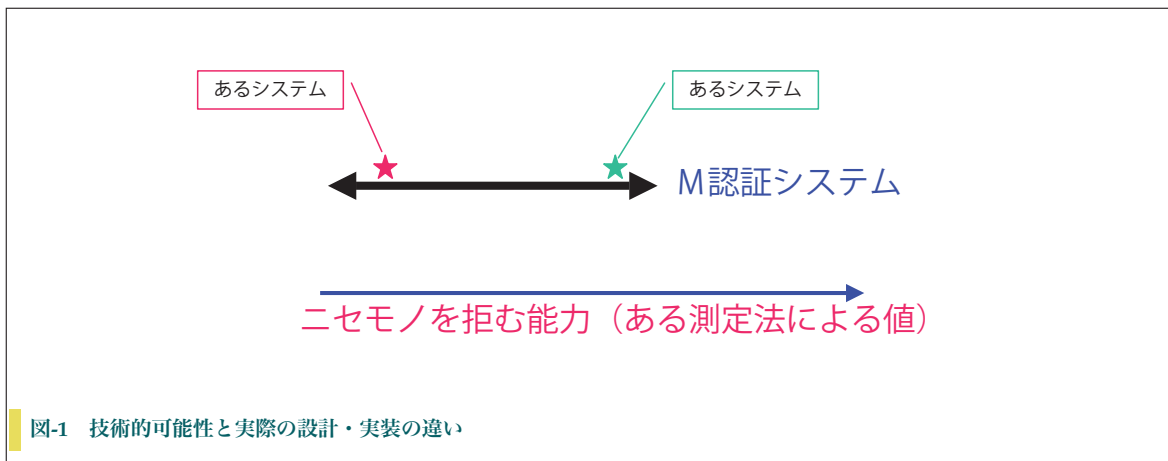


図-1 技術的可能性と実際の設計・実装の違い

| 方式               | 具体例(モード)                                                                                        | 特徴                                                       |                                                                                                            |
|------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
|                  |                                                                                                 | 利点(一般の認識)                                                | 注意点                                                                                                        |
| 記憶<br>ピンからキリまで   | 暗証番号, パスワード,<br>質問応答                                                                            | 簡単・経済性<br>広く普及                                           | 忘却・盗み見・推測・<br>フィッシング・<br>横流し・脅迫／強制対策                                                                       |
| 生体認証<br>ピンからキリまで | 指紋, 掌形, 虹彩, 血管パター<br>ン(網膜, 指, 手の甲, 手の<br>ひら), 顔, 耳形状, 声紋, 筆<br>跡, 歩き方, キー・ストローク,<br>匂い(DNAパターン) | 簡単・忘れない<br>万人不同といわれる<br>生涯不変といわれる<br>横流しできない<br>偽造は困難だろう | 読取装置が必要・コスト<br>装置の耐タンパー性<br>フィッシング<br>本人拒否・登録失敗<br>生涯不変(無効化困難)<br>心理的抵抗感・機微な個人情報<br>偽造・偽装に対する強度<br>脅迫／強制対策 |
| 所持物<br>ピンからキリまで  | 身分証明書, パスポート,<br>磁気カード, ICカード,<br>USBトークン, 携帯電話機                                                | 操作が容易<br>広く普及<br>暗号技術が併用可<br>偽造は困難にできるだ<br>ろう            | 要リーダライタ・コスト<br>紛失・盗難・スキミング<br>横流し・脅迫／強制対策<br>耐タンパー／耐クローン性<br>暗号方式・実装の強度                                    |

表-1 個人認証技術の特徴

生体情報は、パスワードのように記憶する必要がなく、ICカードのように紛失の危険が少ないが、本人が確実に本人と認められないことや、一定割合で特定の生体情報を利用できない人々がいることなど、他の技術との違いがある。また、生体認証においては、生体情報の偽造が困難であることが求められるが、現実には、利用者および管理者の利便性を追及すると、生体認証システムにとって本物の生体部分のように見えるものが提示された場合に完璧に受入を拒否するような生体認証システムを、許容できるコストで作ることが、必ずしもうまくできるとは限らない。パスワードやICカードは無効化し再発行することができるが、たとえば顔が人工物によって偽造されたことが分かって、顔を新しいものに変更することはできないことは、特筆すべき生体認証システムの注意点である。

## 生体認証システムの構成と働き

生体認証システムの働きには登録(enrollment)と認証(authentication)の2つの段階がある。生体認証システムは一般に、生体情報取得部、固有パターン抽出部、生体検知部、テンプレート生成部、生体情報記録部、照合部、登録総合判断部、照合総合判断部から構成されると考えられる。

生体認証には、1対1照合(verification)と1対n照合(identification)の区別がある。1対1照合とは、生体認証システムに提示された特徴の持ち主があらかじめ識別された個人であるかどうかを確認する方式である。この場合、利用者の固有パターンは、利用者のIDと結び付けられて、テンプレートとして保管される。認証時には、被認証者となる利用者は、自分の生体情報とIDを生体

認証システムに提示する。生体認証システム側は、提示された生体情報から固有パターンを抽出し、対応するIDのテンプレートと照合する。

一方、1対n照合では、生体認証システムには利用者のIDなしで生体情報だけが提示される。この方式では、生体認証システム側は固有パターンを抽出し、登録されている(n人の候補のうちの)いずれかのIDの利用者に対応するものであればそのIDを出力し、誰にも対応しない場合はそうだという結果を返す。この方式は、被認証者がブラック・リスト等に登録されている個人でないことを示す目的で使うこともある。

## 生体認証システムの認証精度

生体認証システムでは、本人であるが本人であると照合されない場合(False Rejection)が存在する。これは、登録時と認証時で状況が異なるためである。登録時と認証時の装置の違い、生体情報の変化、生体情報の提示方法のばらつき、環境の変化などが原因である。このため、照合を厳密にしすぎず、誤拒否率(FRR: False Rejection Rate)が適度に低く抑えられるようにシステムのパラメータを調整して用いることが普通である。このため、異なる人間の生体情報で厳密には異なっているものが提示された場合に、それを誤って正しい本人の生体情報であると認証されることが避けられない。つまり、誤受率(FAR: False Accept Rate)をゼロにすることは困難である。FRRやFARを生体認証システムの認証精度という。

生体認証技術を対象とする標準やガイドライン等の策定は世界中で活発に行われている。認証精度に関して日本国内では、日本規格協会情報技術標準化センター(INSTAC)のバイオメトリクス標準化調査研究委員会によって、指紋、虹彩、血管パターン、顔、音声、手書き署名を用いた認証精度の評価方法について検討が行われ、関連するJIS-TR(テクニカルレポート)が作られている(日本工業標準調査会 JIS TR X 0053, JIS TR X 0072, JIS TR X 0079, JIS TR X 0086, JIS TR X 0098, JIS TR X 0099)。これらのJIS-TRでは認証精度評価を行う際の留意点や評価結果の報告方法等を規定している。

## 生体認証システムのセキュリティ上の脆弱性

認証精度の問題は、生体認証システムの各構成要素において、そのアルゴリズムや取得データの品質に起因するものといえる。認証精度の問題以外には、第1に、生体認証システムの各構成要素あるいはそれらの間(通信

回線を含む)において、各種データの不正な読み出しと書き換え、各種機能の不正な変更などの攻撃が行われる可能性がある。これは、暗号アルゴリズムを実装した暗号モジュールへの各種実装攻撃に対処しなければならないという問題と同様である。対応としては、実装上のセキュリティ要件を整備することにより、この意味でのセキュリティの高い生体認証システムを得ることが可能であろう。

第2に、生体認証システムの入力がニセモノであったときにそれを確実に見破れるか、という問題がある。生体認証システムでは対象とする身体部分を、光などの手段を用いて計測している。したがって、光などで見て身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。生体認証システム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”(Liveness Detection)機能が組み込まれ、期待通りに働いているならば、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、生体認証システムに本来提示される人間の身体部分の代わりに人間の身体部分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。この関係を詳しく見てみよう。

すべての対象物(3次元的な形を有するもの、身体部分を含む)の集合を $\Omega$ とする。様式Mの身体部分(指、手の甲、手のひら、眼、顔、など)を対象とする生体認証システムのすべてからなる集合を $B[M]$ と書く。システム $S \in B[M]$ への提示の仕方や環境が適切であれば $S$ に登録できる対象物の全体を、 $\Omega$ の部分集合 $\text{Enroll}[S]$ で表すことにする。さらに、様式Mの身体部分のすべての個人にわたる集合を、 $\Omega$ の部分集合 $\text{Human}[M]$ で表すことにする。

システム $S \in B[M]$ で身体部分の登録にほぼ問題がないことは、

$$\text{Human}[M] - \text{Enroll}[S] \quad (1)$$

が十分に小さいこと(理想的には空集合 $\Phi$ )と表せる。

同時に、システム $S \in B[M]$ が様式Mの身体部分以外を排除することも望まれるが、それは

$$\text{Enroll}[S] - \text{Human}[M] \quad (2)$$

が十分に小さいこと(理想的には空集合 $\Phi$ )と表せる



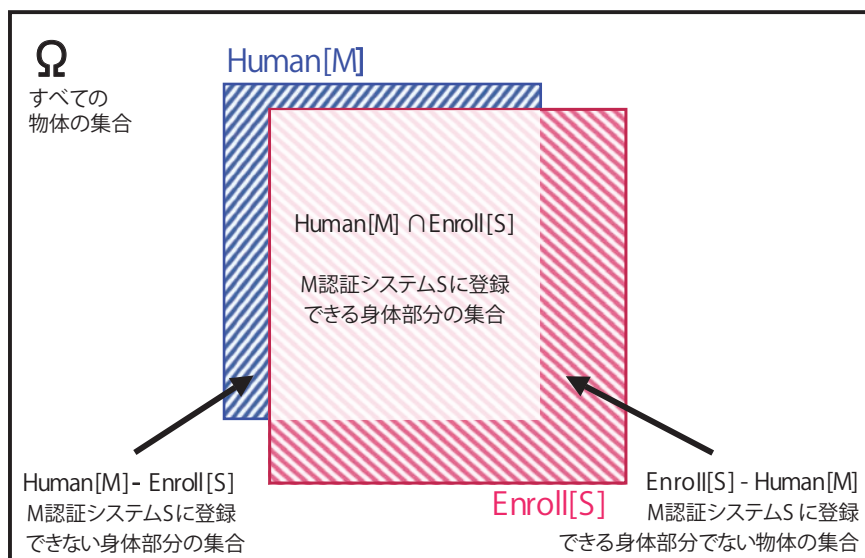


図-2 生体認証システムSの脆弱性

(図-2参照)。考察すべきポイントは、(2)の集合をΦにするようにEnroll[S]を作ると(1)の集合が大きくなる傾向があることである。

## 生体認証システムのセキュリティ評価

生体認証においては、本人を間違えることなく認めると同時に、本人でない者が本人になりすますことをいかに排除するかがセキュリティ上の焦点となる。なりすましに関する脆弱性にはさまざまな項目があり、その多くはシステム設計・運用で対処できるが、前項で述べたように最大の懸念事項は、特定の具体的な生体情報の代わりをする対象の提示である。以下では身体的特徴を用いる生体認証システムに限定して考察する。

指の指紋、眼の虹彩、指や手のひらや手の甲の静脈などの身体的特徴を用いた生体認証システムのセキュリティを評価する際には、当該身体部分の偽造や偽装の困難性（あるいは容易性）について検討することが必須である<sup>1)</sup>。筆者らは2000年7月から指紋認証システムに関して<sup>2)</sup>、また2003年7月から虹彩認証システムに関して<sup>3)</sup>、さらに2005年3月から静脈認証システムに関して<sup>4)</sup>、身体的特徴の偽造に関するセキュリティ研究報告を行った。一連の研究から、ある生体認証システムの開発・製造・試験などの各段階で必要となるセキュリティ評価の方法として、人工的に作成しておいたテスト物体(Biometric Test Object)を用いた次のような方法が有用であることを見出した。すなわち、以下のような事項について実

験を行い、その結果を分析するセキュリティ評価方法である(図-3参照)。

- ・テスト物体がそのシステムに登録できるか
- ・登録できたら再び提示した同じテスト物体が照合されるか
- ・ある人間の身体部分を模擬して作ったテスト物体を登録し、対応する人間の身体部分が照合されるか
- ・登録した人間の身体部分に対して、それを模擬して作ったテスト物体が照合されるか

こうした方法の有効性は内外の研究者により追試され妥当であることが確認されている。たとえば2005年3月時点での各種指紋認

証システムに対する調査結果については記事5)を参照されたい。

さらに、このようなセキュリティ評価用のテスト物体が満たすべき条件の整備や作製方法の確立が求められる。指紋認証システムに対しては、テスト物体(テスト人工指)に関する検討をまとめ、日本規格協会作成の標準仕様書(TS X 0101:2005)「指紋読取装置の品質評価方法」の一部分として2005年5月に公表した。この仕様書は、指紋読取装置の品質および読取装置が出力する画像の品質についての評価基準(セキュリティの評価基準ではなく、読取装置と出力画像の品質の基準である)について規定したものである。また、虹彩認証システムのセキュリティ評価については、テスト物体のセット(紙製人工虹彩などの組)を開発する際に必要な基本的検討事項を文献6)で考察した。図-4に各種テスト物体のサンプルを示す。

## テスト物体を用いるセキュリティ評価方法

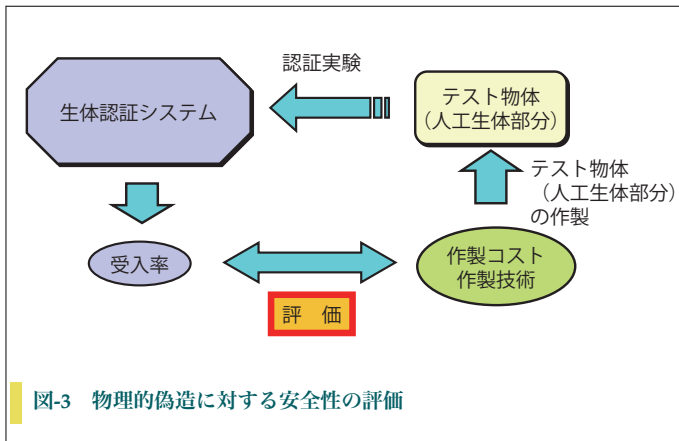
与えられた生体認証システムの身体部分の偽造に対するセキュリティを実験的に評価する方法には、次の2段階が考えられる：

### 第1段階

生体認証システムにテスト物体を提示し、

(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

(A-L) テスト物体を登録し、身体部分で照合できるかどうか、

(L-A) 身体部分を登録し、テスト物体で照合できるかどうか、

について調べる。

ここで、記号Aは「Artificial Object」の略であり人工のテスト物体を意味する。また記号Lは「Live Object」の略であり生体の身体部分を意味する。また、記号(L-L)で、身体部分を登録し身体部分で照合する普通の使い方を表現することにする。

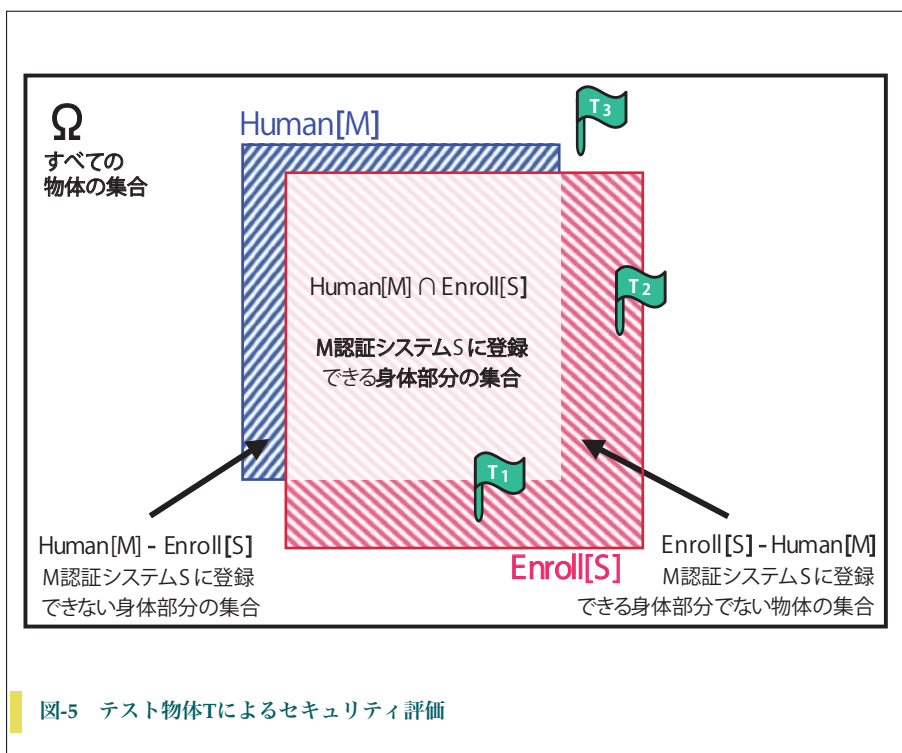
図-5に例示した状況はテスト物体 $T_1$ 、 $T_2$ について(A)および(A-A)に成功し、テスト物体 $T_3$ については(A)に(したがって(A-A)にも)失敗した場合である。つまり図-5では、生体認証システムSにテスト物体( $T_1$ 、 $T_2$ 、 $T_3$ )を提示する実験により集合 $Enroll[S]$ に関する情報が増えたことを示している。よって、適切なテスト物体の組(セット)を揃えることは有益である。

なお、第1段階の(A)が成功しないテスト物体、すなわち、システムに登録ができないテスト物体については自動的に(A-A)や(A-L)が成功しないが、第2段階の(L-A)は成功する可能性があることに注意が必要である。たとえば図-5のテスト物体 $T_3$ については(L-A)が成功する可能性がある。実際、ある虹彩認証システムをこの方法でテストした際にこのような事例があることを確認している<sup>3)</sup>、<sup>6)</sup>。

## 身体部分の情報入手に関する考察

生体認証システムに登録・照合できる身体部分を模擬したテスト物体を作製するには、身体部分の情報入手が必要である。しかし、第1段階の実験においては、必ずしもある特定個人の身体部分の特徴を模擬する必要はない。この身体部分の情報入手に際して、評価対象の生体認証システムそのものは必要ではなく、システムとは独立に、身体部分につき各種の測定を行えばよい。ただし、評価対象のシステムが特に“何を見ているのか”に関する情報が増えれば、省略可能な測定項目が増えることになる。





また、第2段階の実験においては、特定個人の身体部分の特徴を採取することが必要である。セキュリティ評価の実験では、実験に協力する個人の身体部分を計測すればよい。

実際の攻撃者が個人の身体部分に関する情報を入手しようとした場合の困難性を論じるには、撮影された顔画像やガラス等についた指紋のように本人の身体部分を直に計測しなくてもよい場合と、本人の身体部分を直に計測しなければならない場合とがあることに留意が必要である。目（虹彩）あるいは指や手の内部（静脈）を用いたバイオメトリクスは後者に分類されるといえる。しかし、後者であっても本人の身体部分を直に計測することが攻撃者にとって困難であるとは限らない。たとえば、生体認証システムの利用が普及するにつれ、バイオメトリクス入力装置に自らの身体部分を提示することが日常的になるであろう。そのような状況では、偽のバイオメトリクス入力装置に、それとは気づかず身体部分を提示して情報取得がなされてしまう、といった危険性も考慮しなければならないからである。偽夜間金庫や偽ATM、あるいはインターネットにおけるフィッシング詐欺事件の場合と類似の状況になるわけである。利用者に対する注意喚起も必要であろう。

## セキュリティ評価技術の開発と活用

生体認証システムをしっかりと利用していくためには、その潜在的な脆弱性を理解して、それを考慮したセキュリティ測定手段を整備し、できる限り客観的に個々の

システムのセキュリティを把握するよう、努力すべきである。また、セキュリティの基準、クラス分類を設定することも課題といえよう。本稿では生体認証システムの二セモノ排除能力に関するセキュリティを中心として概念的整理を行い、テスト物体を用いることにより生体認証システムのセキュリティを具体的に計測できる可能性があることを説明した。

このような方法論は洗練する価値があるのではないと思われる。というのは生体認証システムの形態に応じたセキュリティ測定・評価技術を開発できれば、適切なセキュリティのクラス分けや基準の設定が可能となり、生体認証システム利用者が求めるセキュリティ

上の要求と、生体認証システムが提供するセキュリティ上の性能をマッチングするための言語が用意できる可能性があるからである。すなわち、テスト物体の整備は重要課題の1つといえよう。

また、エンドユーザにとって、解りやすく、確かに信頼できると実感できる生体認証とはどのようなものであるか、それを育て、いかに適用していくか等につき、さらなる検討を進めるべきであろう。

### 参考文献

- 1) 宇根正志, 松本 勉: 生体認証システムの脆弱性について一身体の特徴の偽造に関する脆弱性を中心に, 金融研究, Vol.24, No.2, pp.35-83, 日本銀行金融研究所 (July 2005), <http://www.imes.boj.or.jp/japanese/kinyu/2005/kk24-2-2.pdf>
- 2) Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S.: Impact of Artificial "Gummy Fingers" on Fingerprint Systems, Optical Security and Counterfeit Deterrence Techniques IV, Rudolf L. van Renesse, Editor, Proceedings of SPIE Vol.4677, pp.275-289, SPIE - The International Society for Optical Engineering (2002), <http://www.spie.org/web/abstracts/4600/4677.html>, <http://spie.org/Conferences/Programs/02/pw/confs/4677.html>
- 3) 松本 勉, 平林昌志, 佐藤健二: 虹彩照合技術の脆弱性評価 (その3), 電子情報通信学会 2004年暗号と情報セキュリティシンポジウム, SCIS2004, Vol.1, pp.701-706 (Jan. 2004).
- 4) 松本 勉, 鉢嶺拓二, 田辺壮宏, 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 (2) - 静脈認証システムに関する研究 (その1) -, 電子情報通信学会技術研究報告, ISEC2005-5 (May 2005).
- 5) 堀内かほり, BYTE LAB: 濡れた指, 乾燥した指 - 指紋認証の実験, NIKKEI BYTE, 2005年4月号, pp.60-67, 日経BP社 (2005年3月22日発行).
- 6) 松本 勉, 佐藤健二: 虹彩認証システムのセキュリティ評価用テスト物体セットについて, 情報処理学会 コンピュータセキュリティ研究会, CSEC-31 (Dec. 9, 2005).

(平成18年5月6日受付)