生体認証システムの選択に関するガイドライン
～リスク評価からのアプローチ～
リスク工学グループ演習 3 班

茂木　友里加　　小岩　敬太　　小原　伸広
アドバイザー教員　　亀山　啓輔

1. はじめに
1. 1. 背景
生体認証とは、身体または行動の特徴を用いた個人の認証であり、身体特徴としては、指紋、顔、静脈、虹彩が、行動特徴としては、声紋、署名などが挙げられる。使用例としては、PC、携帯電話のロック解除、入退室管理、銀行の ATM などが挙げられる。生体認証のメリットとしては、パスワードの記憶や IC カードの管理が不要なため、記憶忘れや紛失によるトラブルがなく、利便性が高いことや、生体情報を使うため本人しか使用できず、偽造も難しいことが挙げられる。デメリットとしては、モダリティによっては経時的な特徴の変化に弱い、生体情報の秘匿性や識別性能の課題、一度登録した生体情報の変更の困難さ、使用に対する心理的抵抗があることなどが挙げられる。近年、こういった生体認証システムを不正に突破（攻撃）する犯罪が見られ、問題となっている。

生体認証の認証精度を表す指標としては FRR（False Rejection Rate）と FAR（False Acceptance Rate）があり、FRR は本人拒否率であり、本人を他人として拒否する割合を示している。FAR は他人受け入れ率であり、他人を本人として受け入れる割合を示していて、生体認証システムの安全性を考える場合、FAR の方を重要視する。どのセキュリティ方法にも脆弱性というものがあり、生体認証に対しても偽造などによる様々な攻撃が考えられる。攻撃事例としては、2005 年に使用者の指を切断することで、指紋認証付きの車両が盗まれる事件や、2008 年にシリコンで指紋認証を突破し、不法入国されるという事例が挙げられ、生体検知機能や他の認証システムとの併用利用の必要性が論じられている。

そこで、私たちは生体認証に関する文献調査を行い、セキュリティ機器の開発とサービス化を行っているセコム（株）の技術者にヒアリングを行い、生体認証技術に関すること、安全性評価に対する考えなどを聞いてきた。

1. 2. ヒアリング
調査概要

―日時：2012 年 6 月 20 日 10:30～
―調査対象：セコム株式会社セコム IS 研究所
・運営管理グループリーダー長谷川氏
・先端研究ディビジョンサブマネージャー兼画像センシンググループリーダー徳見氏
―目的：生体認証におけるリスクの定量評価（安全性評価）に対し、セコムの人たちはどのように考えているのか、そして、本調査研究のこれからの方針についてアドバイスをもらうこと。

ヒアリングの調査結果の一例

Q. 認証システムの安全性についてアドバイスをいただけますか？
A. 認証システムの安全性を評価についての考えは、開発目的や立場によって異なる。
（以下考察）
生体認証の種類、使用目的、使用者、評価を行う立場などによって、許容できるコスト、使用環境、求められる精度、問題となる脆弱性が異なる。したがって、生体認証全体に対するリスク評価をするのではなく、考える範囲を絞ってテーマに取り組むべきであることがいえる。

1. 3. 研究目的
文献調査、ヒアリングから様々な状況な状況により生体認証における脆弱性、許容できるリスクが異なり、生体認証全体に対して、リスクを定量的に評価することの難しさがわかった。そして、生体認証を導入する際に、どの認証システムを用いれば良いのか判断することも難しいと考えられた。そこから、生体認証におけるリスクを定量評価するとともに、使用環境に合わせた認証システム選択に関するガイドラインを作成し、生体認証導入の適切なコンサルティングを可能にすることを本のグループ演習の目的とした。

まず生体認証に関する文献調査を行い、現在の技術に対する偽造テストを行う。次に生体認証を種類ごとに比較することで、選択におけるガイドラインを作成し、ガイドラインを適用したケーススタディを行うことで、ガイドラインの流れを確認する。

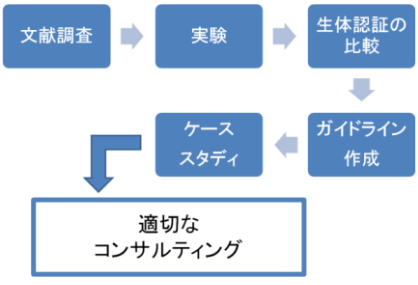

図1　研究の流れ

2. 主な認証システムの特徴

ここで、主な生体認証システムの特徴とその問題点を把握しておく。

2.1. 指紋認証

早くから実用化され、技術向上・普及が最も進んでいる生体認証システムである。指紋は万人が異なり、また成長などによる変化を伴わないとされる。[1)]

認証方法は、まず指紋のパターンを読み取り、分岐点や端となっている点の位置や 方向を数値化し、予め登録した数値と照合することで認証を行う。[2)] 広く普及したシステムであり、PC のログインなどから出入国審査まで、幅広く使用されている。

問題として、以下の点が挙げられる。

- 指の損傷などにより使用できなくなる可能性がある。
- もともと指紋を持たない個人に対しては別の認証が必要になる。
- 情報が漏えいしても、登録情報（指紋）の変更が困難である。
- 指紋の押印と捉えることもできるため、心理的抵抗を持つ人もいる。
- 鍵となる生体情報の秘匿性が低い。
- 比較的安価に装置を購入することができるため、偽の機会を設置し指紋情報を読み取られる可能性がある。
- 偽造が可能である。

2.2. 静脈認証

指紋認証などと比べてなりすましが難しい認証の方法として関心が高まっているシステム。静脈も万人が不同といわれており、大きさ以外の経年変化は見られない。認証として、手のひら、手の甲、指を用いるものがある。近赤外光により静脈パターンを読み取り、パターンの特徴に基づきマッチングを行う。[1)]

問題として、以下の点が挙げられる。

- もともとこの生体情報を持たない個人へは別の認証が必要になる。
- 情報が漏えいしても、登録情報（静脈パターン）の変更が困難である。
- 偽の認証装置を設置し静脈パターンを読み取り、悪用することが可能である。

2.3. 顔認証

他の生体認証に比べて、離れた場所からの認証が可能であり、手をかざすなど特別な動作を必要としない。歩いている状態からも認証可能なシステムが開発されたことでも注目されている。また自分の顔を用いるということから、不正利用者が発覚した場合、記録された顔画像から個人を特定することが容易であるといったメリットがある。同様の理由から、犯罪抑止効果も期待される。

照合方法は、まず撮影した画像から傾きや位置を検出して補正し、特徴点（眼の中心や唇の端など）の位置や点同士の距離などを計測、予め登録しておいた特徴データと照合する。

問題として、以下の点が挙げられる。

- 顔の角度や髪型・表情・成長、サングラスやマスクなどで、認識率が低くなる可能性がある。
- 比較的装置自体が高価である。
- 鍵となる生体情報の秘匿性の問題。

3. 生体認証の安全性に関する既往研究

3.1. 文献調査

生体認証の偽造に関するリスクについて、文献調査を行った。

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が、認証精度に関しては、日本国内では、日本規格協会情報技術標準化センター（IN-STAC）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制度の評価方法について検討が行われ、関連する TR(テクニカルレポート)が作られており、それらにおいては認証精度評価を行う際の留意点や評価結果報告方法等を規定している。しかし偽造に関する詳細なリスクについては、各々研究者による研究報告に留まっている。

米澤ら[3)]によると、FAR によってなりすましの確率を評価することができるが、悪意のあるユーザーによる故意の攻撃は含まれていない。なりすまし攻撃の種類としては、攻撃者がなりすまし対象の生体情報を取得してその模造物を作成し認証システムに提示するテスト物体攻撃と、攻撃者が認証アルゴリズムの情報を基にして、多くの登録ユーザーになりすますことのできるサンプルを作成し認証システムに提示するウルフ攻撃が提案されている。後者は、アルゴリズムの入出力及び動作が分かっているシステム（ホワイトボックスシステム）でのみ実行可能であり、それらの不明なブラックボックスシステムに対しては行うことのできない攻撃である。前者はどちらのシステムにも実行可能な攻撃である。しかし、ブラックボックスシステムの内部動作を分析し、ホワイトボックスシステムに帰着させるような攻撃も考えられるとしている。

また、松本[4)]は、ウルフ攻撃よりもテスト物体攻撃に着目し、認証システムのセキュリティについて論じている。これによると、システムの利便性上、FRR が適度に低く抑えられるように設計するのが普通であるため、FAR をゼロにすることは難しいという。身体部分と同じように観測される対象物であれば、受け入れられる可能性があるが、生体検知機能がうまくはたらいていれ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、利便性を優先して FRR を小さく設定することによって、この機能がうまくはたらかない場合があるとしている。

そこで、偽造や他人受け入れ問題に関して

は、①テスト物体がそのシステムに登録できるか②登録できたら再び提示した同じテスト物体で照合されるか③人間の身体部分に対してそれを模擬してつくられたテスト物体は照合できるか④そのテスト物体を登録して対応する人間の身体部分で照合できるか。といった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が有用であり、このような目的に用いることのできるテスト物体が満たすべき条件の整備や作成の方法を確立することが必要であるとしている。[5)]

さらに、指紋認証について、実際に指紋を偽造しテストを行い、容易性を研究したものがある[6)]。これによれば、指紋認証システムに対する攻撃として考えられるものは

① 登録された人物の指（本人意思に反する利用）
② 登録されていない人物の指（出入国の際など）
③ 切断された登録者の指
④ 登録者の遺伝子クローンの指
⑤ 登録者の人工的模造物の指

などであり、その中でも⑤が最も簡易であると推測される。そこで、実際に指から直接指紋を取り偽造する方法と、残留指紋から指紋パターンを採取し偽造する方法の 2 パターンについて実験を行っている。その結果、どちらも 1 時間～2 時間程度の労力で偽造可能であり、指から直接偽造する方法に至っては 600 円程度で作成することができ、それら偽造指紋は 11 タイプの指紋認証に照合されている。

また、松本らによる、指静脈認証システムについて偽造を試みた研究もある。[7) 8) 9)] 予め用意した静脈画像をプリントし、光の散乱や透過を制御するためビニールテープ等を用い、試験管などパイプ状の物に静脈をプリントした紙を貼り付けることで再現している。紙の種類や画像の処理方法、パイプの種類等の条件を変化させて実験を繰り返し行った結果、いくつかの条件の組み合わせを除いて、登録・照合可能なテスト人工指が作成できることがわかっている。

3.2. 考察

既往研究から、攻撃者によっては、登録者の多くに照合するようなウルフ物体をつくることが可能であるということ、またテスト物体においては、指紋・指静脈については偽造が可能であるということがかわった。それぞれの性質から、ウルフ攻撃よりもテスト攻撃の方が多くの攻撃者に可能な手段であり、また容易であると考えられる。そのため、本研究ではブラックボックスシステムを前提とし、テスト物体攻撃の可能性を攻撃リスクとする。

また、顔認証、手のひら静脈認証については偽造攻撃に対する安全性に関する研究はなされていない。

さらに、これらの研究が行われた時から数年が経過しており、偽造に対する対策を含め認証システムの技術は格段に上がっている可能性がある。そのため現在主流となっている認証システムにおいてもこれらの偽造方法が有効であるという保証はない。

4. 実験

現在の認証システムに、既往研究でなされた偽造が有効であるかどうかを検証するため、実際に指紋認証装置を用いて偽造攻撃実験を行った。実験手順は松本[6)]の実験報告を参考にしている。

使用認証装置

（1）USB 指紋認証システムセット・スワイプ式 SREX-FSU2（ラトックシステム株式会社）
（2）FMV-BIBLO　MG75Y（FUJITSU）

使用材料

・ゼラチンリーフ（186 円／1.5g×20 枚）
・自由樹脂 JJ-35（367 円／35g）

手順

① 指紋認証システムに自分の指紋情報を登録
② 自由樹脂 35g をお湯で柔らかくし、指を押し付けて指紋の型を作成
③ 自由樹脂が固まったら、その型に、水に溶かしたゼラチン（水：ゼラチン＝1：1）を流し入れ、冷蔵庫で固める
④ 固まったら取り出し、指紋センサーでの認証を試みる

本実験では、現在の認証技術に対する偽造突破を試みるため、松本らの実験[6)]とは異なり、現在主流となっているスワイプ式の指紋認証を用いている。その結果、ゼラチンで作られた偽造物体は読み取り装置の上を上手く滑らず、つっかえてしまうため指紋が途切れ途切れに認識され、認証されない。また、スライドさせることでゼラチンが傷ついていく上に、熱で表面が溶けてくるため、同物体で 10 回も試すと、表面が削れ、さらにベタベタとするためますます滑らなくなった。ゼラチンの濃度を高くしたり、冷凍庫で冷やしたりしても、僅かにつっかえにくくなるが結果は同じであった。（1）（2）で別々の人間の指紋を用いて試したが、両者とも結果は同様であった。

本実験により、スワイプ式の指紋認証を松本ら[6)]によるゼラチン偽造物体で突破することは困難であることがわかった。

5. モダリティの比較

本章では、モダリティ（選択肢としての生体認証システムの種類）の各性能における比較を行い、ガイドラインを作成する際の指針となる表を作成する。なお、モダリティのひとつとして、暗証番号を用いた認証について

も考えていく。

5.1. セキュリティ機器選択肢

セキュリティ機器の選択肢については以下のようになる。値段・FAR については、実際の製品を参考に、平均的な値を示している。

- 暗証番号(4 桁)：10 万円・FAR 無し
- 指紋認証：40 万円・FAR0.00001%
- 静脈認証
  - ✓ 指：60 万円・FAR0.0001%
  - ✓ 手のひら：70 万円・FAR0.00008% 以下
- 顔認証
  - ✓ 静止時での認証：100 万円・FAR0.0001%
  - ✓ ウォークスルー：FAR0.0001%（価格はインターネット上で確認できないが、静止時のものよりも高度な技術であるため高価格であることが推測される）

5.2. 生体認証機器の評価項目

生体認証の各評価項目を挙げ、比較を行う。

① 認証精度

生体認証特有の誤検知率(FAR・FRR)の低さを表す。暗証番号には FAR・FRR といった概念は存在しないため、認証精度は最も良いとする。また、各 FAR の値から、指紋認証、静脈認証、顔認証の順に認証精度は高いとする。

② なりすまし耐性

不正者がなりすましを行なった際に突破される可能性から評価を行う。これについては、後になりすまし耐性の節で議論する。

③ コスト

各生体認証の購入にかかる費用を評価する。費用が安いほど評価は高い。

④ 経年変化耐性

利用する生体特徴に経年変化があった際に、認証を問題なく行なえるかどうかを評価する。顔は年月による変化が大きいため、顔認証は経年変化耐性が低いと言える。

⑤ 使いやすさ

認証を行うために必要な動作から使いやすさの性能を評価する。暗証番号は指で番号の入力を行う必要があり、番号も記憶していなければならないため、評価は最も低い。指紋・静脈認証は、指をスライドする・かざすといった動作が必要だが、番号を覚える必要は無い。顔認証は顔を近づけるだけで認証が行えるので、評価は最も高い。

⑥ 清潔感

認証を行う時の清潔感を評価する。認証機器に触れる必要がある暗証番号や指紋認証は評価が低い。静脈認証は手を触れるもの・触れないものの両方が存在し、顔認証は認証機器に触れる必要が無いので、評価は最も高い。

5.3. なりすまし耐性

ここでは、各セキュリティ機器のなりすまし耐性を評価する。

まず、偽造を用いずに正攻法で 1000 回認証を試みる場合の成功確率を求める。暗証番号の場合、4 桁の数字の組み合わせ 10000 通りに対し、1000 通りのパターンを試行できるので、突破確率は(1000/10000) = 0.1 となる。生体認証の場合、不正を行わない他人が少なくとも 1 回認証を突破できる確率は、FAR = a とすると、$(1-(1-a)^{1000})$で求めることができる。指紋認証の場合、$(1-(1-10^{-7})^{1000}) \fallingdotseq 0.1\times10^{-3}$ となる。静脈認証(手のひら)の場合、$(1-(1-0.8\times10^{-6})^{1000}) \fallingdotseq 0.8\times10^{-3}$以下となる。静脈認証(指)・顔認証の場合、$(1-(1-10^{-6})^{1000}) \fallingdotseq 0.1\times10^{-2}$ となる。

次に、偽造など不正行為を行う場合の成功確率を考える。暗証番号の場合、4 桁の数字が判明してしまうと誰でも認証を突破することができてしまう。指紋認証の場合、現在の主流であるスライド式をゼラチンで突破することは難しいが、指紋自体は用意に採取することができてしまうため、使用材料次第では突破できる可能性がある。静脈認証の場合、1000 円強と比較的安価な金額で偽造を行うことができるが、偽造に必要な静脈の情報を得ることが難しい。顔認証の場合、近年では 3 次元顔認証が増えているため写真で突破することは難しく、判定に使うポイントが骨格の作りに関係する場所が多いため、骨格まで変える大幅な整形や特殊メイクといったものが必要となる。しかし、これで認証を突破できる保障はない。

これらの点を考慮してなりすまし耐性の評価を行う。暗証番号は不正無しでも突破確率が高く、番号さえ入手できれば誰でも突破可能なため、なりすまし耐性は低いと言える。反対に、顔認証は偽造が難しくコストもかかることから、なりすまし耐性は高いと言える。指紋・静脈認証は不正無しでの突破確率はあまり変わらず、偽造の方法も存在するが、指紋と比較して静脈の情報を入手することは困難なため、指紋認証よりも静脈認証の方がなりすまし耐性は高いと言える。

5.4. 生体認証の比較

評価項目に基づいて各認証システムの評価を行い、表 1 にまとめた。各項目は 4 点満点で評価を行なっており、この点数がガイドラインに用いられる。

表1　生体認証の比較

		暗証番号	指紋認証	静脈認証	顔認証
前提条件	予算上限(万円)	10	40	60	100
	経年変化耐性	有	有	有	無
リスク耐性	認証精度	4	3	2	1
	なりすまし耐性	1	2	3	4
コスト		4	3	2	1
使いやすさ		1	2	2	4
清潔感		1	1	2	4

6. ガイドライン

以上の内容を踏まえ、実際の使用者の状況に合った適切なモダリティ選択を可能にする、生体認証システム選択ガイドラインを提案する。ガイドラインは、使用者がいくつかの質問に答えることでモダリティを選択する形をとる。以下が設問の内容である。

使用者への設問

① 予算上限額
② 使用予定年数

また、以下の項目について、重要視する度合いを、0，1，2 の三段階評価で示す。

③ コスト（購入価格）
④ 使いやすさ（手間、認証スピードなど）
⑤ なりすまし耐性（攻撃からの安全性）
⑥ 清潔感（接触型か非接触型か）

①の設問によって、予算上限額を超える価格の認証システムを排除する。②において、使用期間が長い場合は経年変化に対応しづらい認証システムを排除する。③～⑥では三段階評価で重み付けをしてもらう。

次に、①②で残ったモダリティについて、表の各項目の値に対応する③～⑥の数値をそれぞれかけ合わせることにより、使用者が考える各項目の優先順位を反映した値を算出する。続いて認証精度項目も加えてモダリティごとの各項目の数値を足し合わせ、最終的にはその合計値の大きいモダリティを選択する。

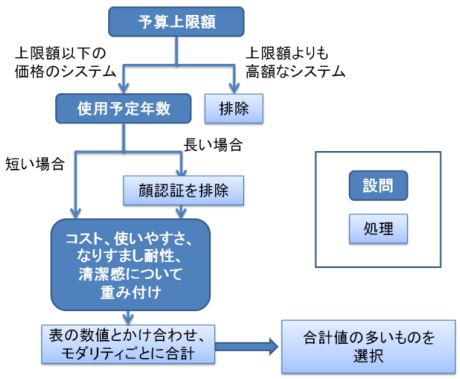

図 2　ガイドラインの流れ

7. ケーススタディ

本章では、前章のガイドラインに基づいて、ケース毎にどの認証システムが選択されるかのケーススタディを行う。

ケース Ⅰ

ここでは、予算が 200 万円で経年変化耐性が必要なく、なりすまし耐性を重視しコストについては問わない場合を想定する。この場合、重み付けによりなりすまし耐性のポイントを 2 倍、コストについてのポイントを 0 倍するため、各認証システムのポイントは以下の通りになる。

① 暗証番号
$4+1\times2+4\times0+1+1=8$
② 指紋認証
$3+2\times2+3\times0+2+1=10$
③ 静脈認証
$2+3\times2+2\times0+2+2=12$
④ 顔認証
$1+4\times2+1\times0+4+4=17$

従って、Ⅰのケースでは顔認証が最適な認証システムとして選択される。

ケース Ⅱ

ここでは、予算が 80 万円かつ経年変化耐性が必要で、使いやすさを重視し清潔感については問わない場合を想定する。まず、予算が 80 万円かつ経年変化耐性が必要であるため、顔認証を選択することはできない。次に、重み付けにより使いやすさのポイントを 2 倍、清潔感についてのポイントを 0 倍するため、各認証システムのポイントは以下の通りになる。

① 暗証番号
$4+1+4+1\times2+1\times0=11$
② 指紋認証
$3+2+3+2\times2+1\times0=12$
③ 静脈認証
$2+3+2+2\times2+2\times0=11$
④ 顔認証
選択不可能

従って、Ⅱのケースでは指紋認証が最適な認証システムとして選択される。

8. 今後の課題

例えば、顔認証システムに対して 3D プリンターを用いた場合の攻撃リスク評価など、各認証システムに対する攻撃事例の拡大が必要であると考えられる。また、各認証システムを組み合わせる場合など、想定使用状況をさらに拡大することも、今後の課題といえる。

9. おわりに

本研究では、外部からの攻撃リスクを考慮した生体認証システムの選択におけるガイドラインを提案した。また、実験により、技術の進歩によって、指紋認証においては従来よりも偽造による突破がしにくくなっていることがわかった。課題としては、本研究で取り扱わなかったが、虹彩などの認証システムを取り入れてのガイドライン作成などが挙げられる。

謝辞

本調査・研究において、ヒアリングにご協力いただいた、セコム IS 研究所　運営管理グループグループリーダー 長谷川様、セコム IS 研究所　先端研究ディビジョンサブマネージャー兼画像センシンググループグループリーダー 徳見様、及びご指導いただいた筑波大学システム情報工学系亀山先生に、心より感謝申し上げます。

参考文献

1) 森ら(2003)：バイオメトリクス認証技術について，FUJITSU.54，4，p.272-279
2) SECOM:指紋認証 http://www.secomtrust.net/secword/fingerprintauth.html (最終閲覧日:2012,9,20)
3) 米澤ら(2010)：バイオメトリクス認証システムへの攻撃に関する分類，映像情報メディア学会技術報告　34(54)，37-40，2010-12-09
4) 松本(2006)：生体認証システムのニセモノ拒否能力をどう測るか，情報処理学会研究報告．DSM，2006(80)，1-6，2006-07-20
5) 松本(2006)：バイオメトリックのセキュリティ評価方法の開発に向けて，生体医工学 ： 日本エム・イー学会誌 44(1)，54-61，2006-03-10
6) 松本:Impact of Artificial "Gummy Fingers" on Fingerprint Systems，ITU-T，Workshop on Security，Seoul
7) 松本ら(2005)：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．ISEC，情報セキュリティ 104(732)，81-82，2005-03-11
8) 松本ら(2005)：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．ISEC，情報セキュリティ 105(51)，29-33，2005-05-11
9) 松本ら(2006)：バイオメトリクスにおける生体検知と登録失敗(3) ： 静脈認証システムに関する研究(その 2)，電子情報通信学会技術研究報告．ISEC，情報セキュリティ 106(51)，53-60，2006-05-12
10) 総務省:国民のための情報セキュリティサイト http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k01_bio.htm(最終閲覧日：2012,9,20)
11) 日立総合計画研究所 http://www.hitachi-hri.com/research/keyword/k11.html (最終閲覧日：2012,9,20)
12) 森雅博，新崎卓，佐々木繁：バイオメトリクス認証技術，FUjITSU.54,4,p272-279，2003
13) 松本勉:金融取引における生体認証について，金融庁・第９回偽造キャッシュカード問題に関するケーススタディグループ，2005 http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdf(最終閲覧日：2012,9,20)
14) 石橋雄一郎、山口修、助川寛：顔認証技術によるハンズフリーの次世代物理セキュリティシステム http://www.nec.co.jp/soft/neoface/(最終閲覧日：2012,9,20)
15) 顔認証システム：ソフトウェア｜NEC http://pachinkokouryaku.fc2web.com/kao1.html(最終閲覧日：2012,9,20)
16) e-words 顔認証 http://e-words.jp/w/E9A194E8AA8DE8A8BC.html (最終閲覧日：2012,9,20)
17) 顔認識システム http://ja.wikipedia.org/wiki/%E9%A1%94%E8%AA%8D%E8%AD%98%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0(最終閲覧日：2012,9,20)