

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

班員：小岩 敬太

小原 伸広

茂木 友里加

アドバイザー教員：亀山 啓輔

1

目次

- ▶ 1. 背景・目的
- ▶ 2. 文献調査からわかったこと
- ▶ 3. なりすまし攻撃に関する実験
- ▶ 4. モダリティの比較
- ▶ 5. ガイドライン
- ▶ 6. ケーススタディ
- ▶ 7. まとめ

▶ 2

背景

セキュリティ

- ▶ キャッシュカード偽造による預金盗難事件、不法入国者のテロ……

様々な問題

時代はセキュリティ強化

➡ 生体認証の使用が注目を浴びている

▶ 3

背景

生体 (バイオメトリクス) 認証とは

- ▶ **身体または行動の特徴を用いた個人の認証。**

指紋、顔、静脈、虹彩

声紋、署名など様々なモダリティ

- ▶ 使用例

- ▶ 個人のPCや携帯電話のロック解除
- ▶ 企業などの顧客管理
- ▶ 施設のセキュリティ管理
- ▶ 銀行のATM
- ▶ 入国管理
- ▶ etc.



<http://sp.newsclip.be/sp/hitachi/009706.php>

▶ 4

背景

生体認証のメリット・デメリット

▶ メリット

- ▶ パスワードの記憶やICカードの管理が不要
- ▶ 記憶忘れ・紛失によるトラブル無し
- ▶ 利便性が高い
- ▶ 本人しか使用できない
- ▶ 偽造が難しい

▶ デメリット

- ▶ 共通
 - ▶ 識別性能の課題
 - ▶ 認証情報が変更困難
- ▶ モダリティによっては…
 - ▶ 成長や格好の変化など安定性の課題
 - ▶ 生体特徴の秘匿性の課題
 - ▶ 使用に対する心理的抵抗

背景

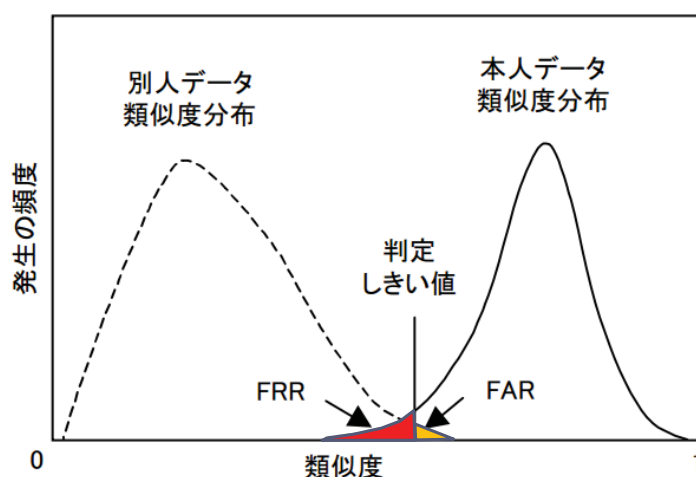
FRRとFAR

▶ 本人拒否率 (FRR)

- ▶ 生体特徴の一時的な変化などにより、本人を他人として拒否する割合

▶ 他人受け入れ率 (FAR)

- ▶ 生体特徴の類似などにより、他人を本人として受け入れる割合



<http://img.jp.fujitsu.com/download/jp/jmag/vol54-4/paper04.pdf>

背景

脆弱性について

▶ 生体認証の脆弱性

- ▶ 偽造
- ▶ 模倣
- ▶ 不正な利用
- ▶ etc.



- ▶ 生体認証に対する様々な攻撃
- ▶ それに対する脆弱性

背景

攻撃事例

- ▶ シリコンで指紋認証を突破、入国(2008)
 - ▶ コストがかかっても
偽造困難な認証を搭載すべきではないか
- ▶ 主人の指を切断することで、指紋認証付きのベンツ盗難(2005)
 - ▶ 生体検知機能または
他の認証システムとの併用利用が必要ではないか

想定される攻撃に対する防御も重要



ヒアリング調査

目的

- ▶ 研究をはじめた頃は、漠然と生体認証全体のリスク評価をしようと考えていた
- ▶ これからの研究方針を決めるためヒアリングを行うことを決めた
- ▶ ヒアリング先には、セキュリティー機器の開発とサービス化を行なっていて、指紋・顔認証機器も扱っているセコム(株)を選んだ

ヒアリング調査

調査概要

- ▶ 日時: 6/20(水) 10:30~
- ▶ ヒアリング対象: 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 徳見様
 グループリーダー
- ▶ ヒアリング内容:
生体認証技術の最先端と、その安全性評価について

ヒアリング調査

調査結果（一部）

Q.顔の状態変化にはどのように対応していますか？

A.顔認証では老化や化粧、怪我といった微妙な変化にも対応できるが、マスクやサングラス等顔がある程度隠れてしまうものに関しては、認証できないようになっている。

Q.認証システムの実験はどのような人を用いて行われたか？

A.認証システムの精度に関する実験は、外国人も含めた様々な特徴の人に対して行われている。また、同一人物の表情や顔の向きの変化に対する実験も行った。

Q.偽造による不正に関して、どのような対策が考えられますか？

A.偽造による不正に関しては、判明・発表され次第対策を行なっている。

Q.認証システムの安全性の評価について、アドバイスをいただけますか？

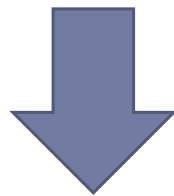
A.認証システムの安全性評価についての考えは、開発目的や立場によって異なる。

▶ 11

ヒアリング調査

考察

- ▶ 生体認証の種類、使用目的、使用者、評価を行う立場によって、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。



- ▶ 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だと感じた。
- ▶ 顧客の要望に合わせたシステムの提供が必要ではないかと考えた。

▶ 12

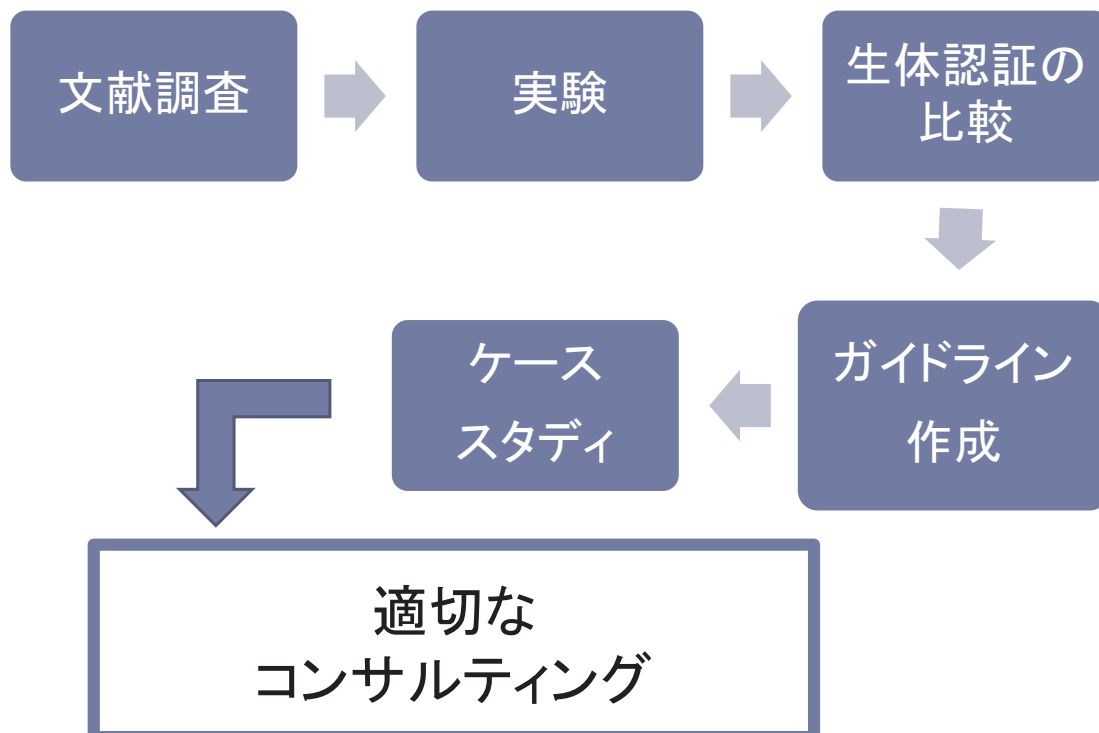
目的

- ▶ 各モダリティにおけるリスクを評価
- ▶ 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



生体認証導入の
適切なコンサルティングを可能にする

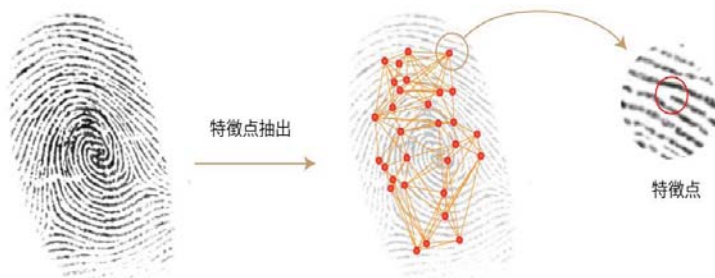
研究の流れ



各モダリティの特徴と問題点

指紋認証システム

- ①技術・普及が最も進んでいるシステム
- ②指紋は万人が不同
- ③指紋は成長などによる変化を伴わない



http://www.daishinsha.co.jp/technology/column/design/design_655.html

▶ 15

- ▶ 怪我など損傷で使用不可
- ▶ 生体情報の秘匿性
- ▶ 偽の機械の危険性
- ▶ 偽造(なりすまし)の容易性
- ▶ 生体情報の変更困難
- ▶ 心理的な抵抗

各モダリティの特徴と問題点

静脈認証システム

- ①静脈は万人が不同
- ②静脈は成長などによる変化を伴わない
- ③種類として、手のひら・指を用いるものがある



- ▶ 生体情報の変更困難
- ▶ 偽の機械の危険性

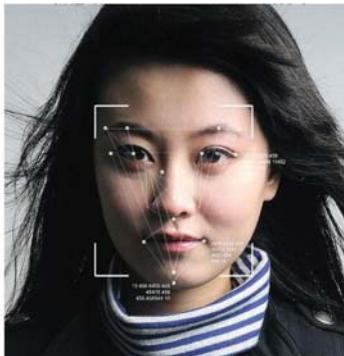
<http://www.ja-kamiina.ijjan.or.jp/kurashi/bank/iccashcard.pl>

▶ 16

各モダリティの特徴と問題点

顔認証システム

- ①離れた場所からの認証
- ②特別な動作を必要としない
- ③ウォークスルー
- ④不正利用者の特定が容易
- ⑤犯罪抑止効果



<http://chc-oim.com/old/>

17

- ▶ 顔の角度、サングラスやマスク
- ▶ 経年変化への対応
- ▶ 装置自体が高価
- ▶ 生体情報の秘匿性
- ▶ 生体情報の変更困難

なりすまし攻撃に関する文献調査

調査結果

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

FARで、なりすまし攻撃の確率評価をする方法もあるが、FARのみでは悪意のあるユーザーによる故意の攻撃リスクは測れない。

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

松本: Impact of Artificial "Gummy Fingers" on Fingerprint Systems

- ・利便性からFRRを低く設定することが多く、偽造を排除するための生体検知機能がうまくはたらかない場合がある。
- ・指紋・静脈の偽造テストを、数種類の認証装置で行ったところ、90%程度の確率で登録・認証に成功。

18

なりすまし攻撃に関する文献調査

考察

- ▶ 松本らが、指紋・静脈認証システムにおいて、偽造物体の登録・認証に容易に成功している
 - 指紋や静脈システムはなりすまし攻撃に対するリスクが非常に高い？

しかし、、、

実験から7年程経った現在、技術は進歩し、認証装置も変化している

松本らのやり方で、現在主流の生体認証システムを偽造突破することができるか？

文献から安易に「なりすましリスクが高い」と断定する危険

▶ 19

実験

方法

▶ 使用装置 **New**

(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)
- ・木工用ボンド(189円/50ml) **New**
- ・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自由樹脂に指を押し付けて指紋の型を作成
- ③その型に、水に溶かしたゼラチンまたはボンドを流し入れ、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



実験

結果・考察

- ▶ ゼラチン
 - ・滑らない(スワイプできない)
 - ・削れていく(10回も試すとボロボロ)
 - ・登録不可・認証不可
- ▶ 木工用ボンド
 - ・滑るけれど認識されない
 - ・登録不可・認証不可



偽造への対応も含めて、技術が進歩している

指紋・静脈認証の偽造は
以前よりも困難になっている可能性がある

モダリティの比較

セキュリティ機器の選択肢

		値段(万円)	FAR (%)
暗証番号(4桁)		10	
指紋認証		40	0.00001
静脈認証	指	60	0.0001
	手のひら	70	0.00008以下
顔認証		100	0.0001

モダリティの比較

生体認証機器の評価項目

① 認証精度

- ▶ 生体認証の誤検知率(FAR・FRR)から評価。
 - ✓ 暗証番号にはFAR・FRRがないため、認証精度は最も良いとする。
 - ✓ 指紋認証、静脈認証、顔認証の順に認証精度は高い。

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。
 - ❖ この項目は後で詳しく解説する。

③ コスト

- ▶ 認証機器の購入にかかる費用を評価。
- ▶ 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、認証に影響するかを評価。
 - ✓ 顔認証は経年変化耐性が低い。

モダリティの比較

生体認証機器の評価項目

⑤ 使いやすさ

- ▶ 認証を行うために必要な動作から評価。
 - ✓ 暗証番号：番号の記憶・入力が必要 → 評価は最も低い。
 - ✓ 指紋認証・静脈認証：指をスライドする・かざすという動作が必要。
 - ✓ 顔認証：顔を近づけるだけで認証可能 → 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。
 - ✓ 暗証番号・指紋認証：認証機器に触れる → 評価が低い。
 - ✓ 静脈認証：手を触れるもの・触れない(かざす)ものの両方が存在。
 - ✓ 顔認証：認証機器に触れない → 評価は最も高い。

モダリティの比較

なりすまし耐性

- ▶ 暗証番号
 - ▶ 番号が判明すると誰でも認証を突破できる → なりすまし耐性は低い。
- ▶ 指紋認証
 - ✓ 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。
 - ✓ 指紋は用意に採取できるため、使用材料次第では突破できる可能性がある。
- ▶ 静脈認証
 - ✓ 比較的安価な金額で偽造を行うことができる。
 - ✓ 偽造に必要な静脈の情報を得ることが難しい。
- ▶ 顔認証
 - ✓ 3次元顔認証が増えているため、写真で突破は難しい。
 - ✓ 骨格まで変える大幅な整形や特殊メイクなどが必要。
 - ▶ 認証を突破できる保障は無く、コストも高い → なりすまし耐性は高い。

モダリティの比較

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

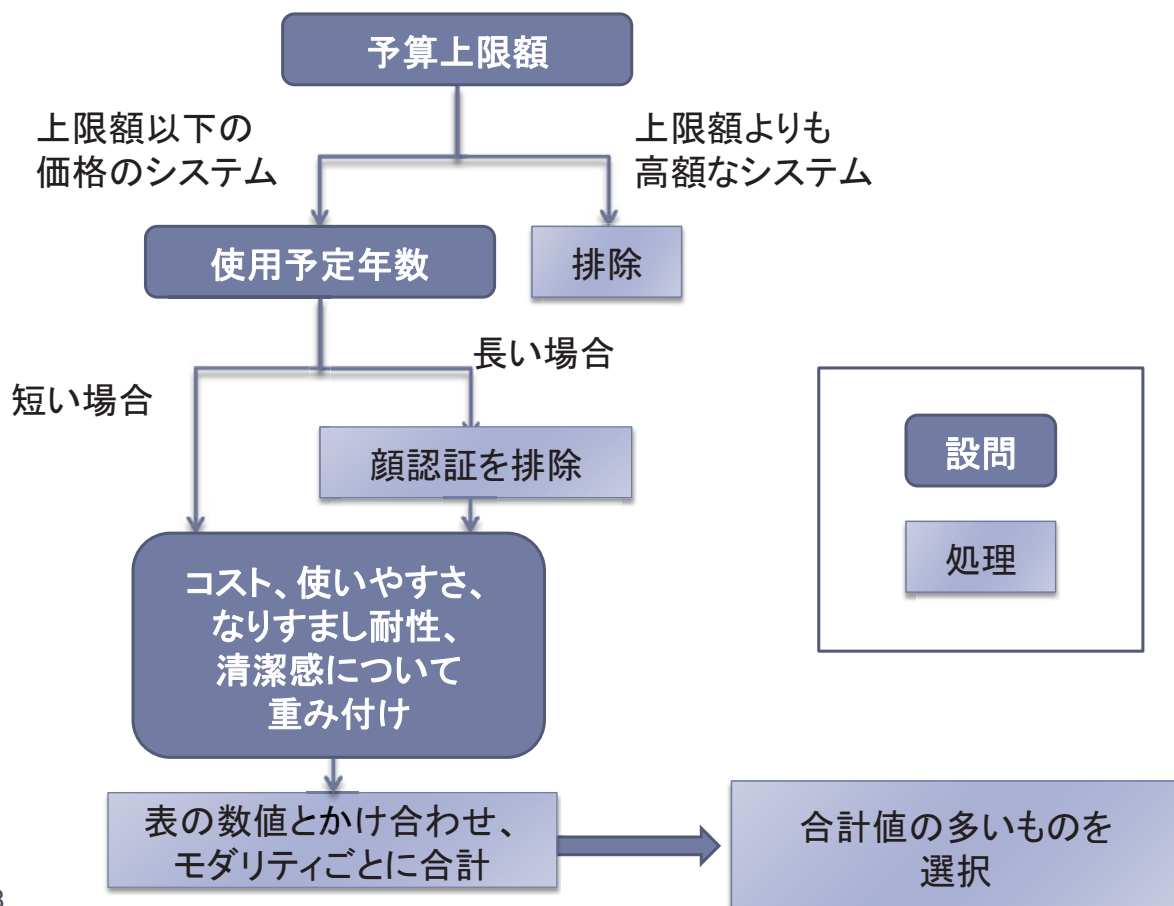
ガイドラインの提案

使用者の状況、優先したい機能・特徴に合わせた、生体認証システム選択のガイドラインを作成する

使用者への質問

- ▶ 予算上限額 （上限額より高いシステムを排除）
 - ▶ 使用予定年数 （多い場合は顔認証システムを排除）
 - ▶ 以下の項目に対し、優先度を0・1・2の三段階で評価
 - ① なりすまし耐性
 - ② コスト
 - ③ 使いやすさ
 - ④ 清潔感
- （表の数値とかけ合わせ、合計額の大きいシステムを選択）**

ガイドラインの流れ図



ケーススタディ

ケース I

- ▶ 予算：200万円、経年変化耐性：不必要
- ▶ なりすまし耐性を重視し、コストについては問わないとする。
 - ❖ なりすまし耐性のポイントを2倍、コストのポイントを0倍する。
- ▶ 各認証システムのポイントは以下の通りになる。

	認証精度	なりすまし耐性	コスト	使いやすさ	清潔感	合計
倍率	×1	×2	×0	×1	×1	
暗証番号	4	1×2	4×0	1	1	8
指紋認証	3	2×2	3×0	2	1	10
静脈認証	2	3×2	2×0	2	2	12
顔認証	1	4×2	1×0	4	4	17

❖ 最適な認証システム：顔認証

▶ 29

ケーススタディ

ケース II

- ▶ 予算：80万円、経年変化耐性：必要
 - ❖ このケースでは、顔認証は選択できない。
- ▶ 使いやすさを重視し、清潔感については問わないとする。
 - ❖ 使いやすさのポイントを2倍、清潔感のポイントを0倍する。
- ▶ 各認証システムのポイントは以下の通りになる。

	認証精度	なりすまし耐性	コスト	使いやすさ	清潔感	合計
倍率	×1	×1	×1	×2	×0	
暗証番号	4	1	4	1×2	1×0	11
指紋認証	3	2	3	2×2	1×0	12
静脈認証	2	3	2	2×2	2×0	11
顔認証	選択不可能					

❖ 最適な認証システム：指紋認証

▶ 30

まとめ

文献調査

- ▶ 各認証システムの特徴、な

実験

- ▶ 技術の進歩とともにになりすま

モダリティの比較

- ▶ なりすましの危険性も含めて

ガイドライン作成

- ▶ ガイドラインの作成

ケーススタディ

- ▶ ガイドラインによって、使用者の要望に合ったモダリティ選択ができることを確認

生体認証システム
選択における
ガイドラインを提案

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ス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)