生体認証のネットワーク利用におけるリスク評価

リスク工学グループ演習9班

班員：　宮田孟

任旭輝

吉田太一

アドバイザー教員：　亀山啓輔

発表の流れ

背景・目的

セキュリティに関する情報漏洩事件について

ネットワーク利用の危険性について

ユーザーの安全性に対する意識調査

提言

背景・目的

研究背景

現在、「財」を保護するため、様々な認証方式が採用されている

パスワード ⇒ ・現在最も普及
・導入コストが低い
・ユーザーが扱い慣れている
・複数のパスワードを使い分けられる

しかし…

ネットワーク利用が盛んになり、
ネットワークの安全性要求も向上してきている

パスワードはユーザーの安全性要求を
満たせなくなりつつある

研究背景

一方で、生体認証が注目されている

生体認証⇒
- 指紋、静脈、顔、虹彩、腕振り、筆跡など人の体の一部、またはその人特有な行動を鍵として用いる
- 他者と同一であることがない
- 偽造されにくい
- 認証が煩わしくない

生体認証

人の体の一部を鍵として用いる認証システム

身体的特徴

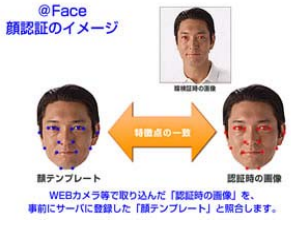
指紋認証

http://www.nec.co.jp/pid/product/h1usb.html

静脈認証

http://cloud.watch.impress.co.jp/epw/img/epw/docs/330/975/html/fu04.jpg.html

顔認証



http://www.sgis.co.jp/topics/html/whatsnew20060908151110-0000002496.html

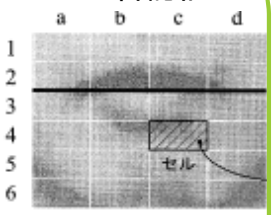
その他、
声や虹彩など

行動的特徴

瞬き認証

http://iris.sg-japan.com/iris_product/

口唇認証



腕の振り認証

http://iphonefan.seesaa.net/article/117309676.html

研究背景

生体認証⇒ ・指紋、静脈、顔、虹彩、腕振り、筆跡など人の体の一部、またはその人特有な行動を鍵として用いる
・他者と同一であることがない
・偽造されにくい
・認証が煩わしくない

様々な長所が挙げられるが、生体認証は
安全なネットワーク利用を行えるのだろうか？

潜んでいる危険を理解していない場合、
被害を受ける可能性がある

研究目的

生体認証は高い利便性と安全性から、
研究や実用化が今後進むことが予想される

ユーザーが生体認証の特性を十分に把握せずに
利用した場合、思わぬ被害を受ける可能性がある

- 生体認証のネットワークにおける安全な利用に関する提言
- より安全な生体認証の利用の一助となることを目的とする

セキュリティに関する情報漏洩事件について

セキュリティに関する漏洩事件

サーバーからの漏洩事件 - YAHOOの事例

- ネットワーク経由でサーバーが不正に侵入され、およそ50万のユーザーのIDとパスワードが漏洩するという事件が発生
- ユーザーのパスワードをプレーンテキストで保管し

一つのサイトの情報漏洩により、他のサイトも被害を受ける

- この事件をきっかけに、他社のユーザー情報も漏洩
- ネットワーク上で、情報がサイト間で共有されていたことが原因

セキュリティに関する漏洩事件

個人情報販売事件 –イギリスの調査(2003)

- 警察や政府機関スタッフは、国民の個人情報を違法に販売し、その情報はさらに新聞記者、探偵、保険会社等に販売されていたことが判明
- 個人の住所、電話番号、電話中の内容、電話する時の場所、友人と家族情報、運転履歴、違法行為記録等が販売される

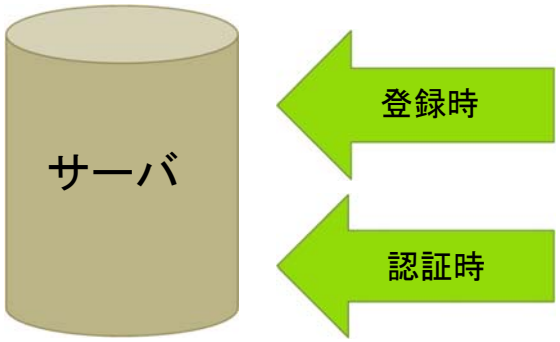
生体情報も個人情報として
売買される危険性がある

生体認証のネットワーク上利用の危険性

モダリティ機器

- 指紋、虹彩などの生体特徴をモダリティという
- 生体認証を行う機器をモダリティ機器と定義する

- ネットワークで使う時は、
  登録及び認証時にサーバにアクセスする



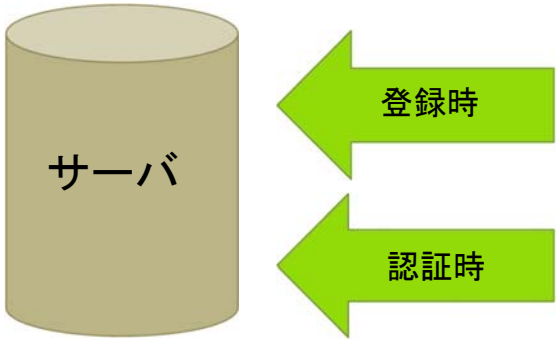
指紋認証モダリティ機器

モダリティ機器

暗号化などをしなければ、パスワードの事例のように情報が漏洩してしまう

- ネット
  登録及び アクセスする

不正アクセス
情報漏洩



指紋認証モダリティ機器

モダリティ機器

生体情報はモダリティ機器内で
暗号化することができる

- ネットワ
登録及び認 スする

漏れる情報は
暗号化されている

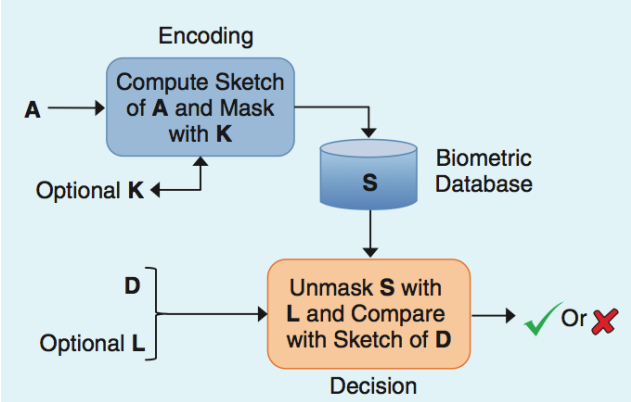
指紋認証モダリティ機器

近年の研究状況

- Secure sketches
  - 生体情報に別の情報を加え、暗号化してサーバに保存。ユーザーはトークン等で認証を行う
- Biometrics as secure multiparty computation
  - 生体情報を関数を使い暗号化する。認証段階では、ユーザー側が持っている秘密鍵をサーバー側が確認
- Cancelable biometrics
  - 生体情報の画像を関数で暗号化、認証する際も同じ関数で変換する

近年の研究状況
—Secure Sketches—

- 生体情報にランダムなベクトル等の情報を加え、暗号化してサーバに保存
- トークンを持って、暗号化された情報の暗号を解き、認証を実行する

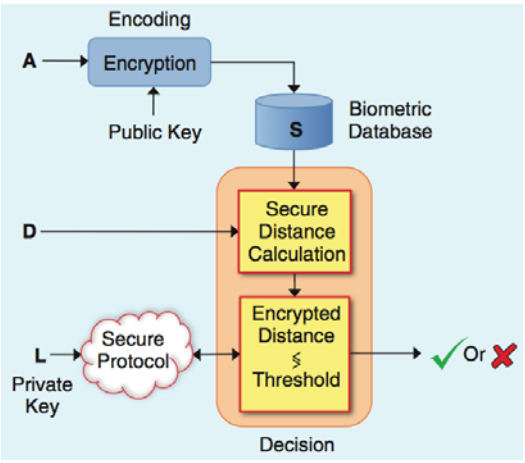


Secure Sketch

S. Rane, Y. Wang, S. C. Draper and P. Ishwar, "Secure Biometrics - Concepts, authentication architectures and challenges -," IEEE Signal Processing Magazine, Vol. 30, No. 5, pp. 51-64, 2013

近年の研究状況
—Biometrics as Secure Multiparty Computation—

- 生体情報を関数を使い暗号化する
- 秘密鍵で本人を確認して認証を実行する
- スキャンされた情報も関数で暗号化される

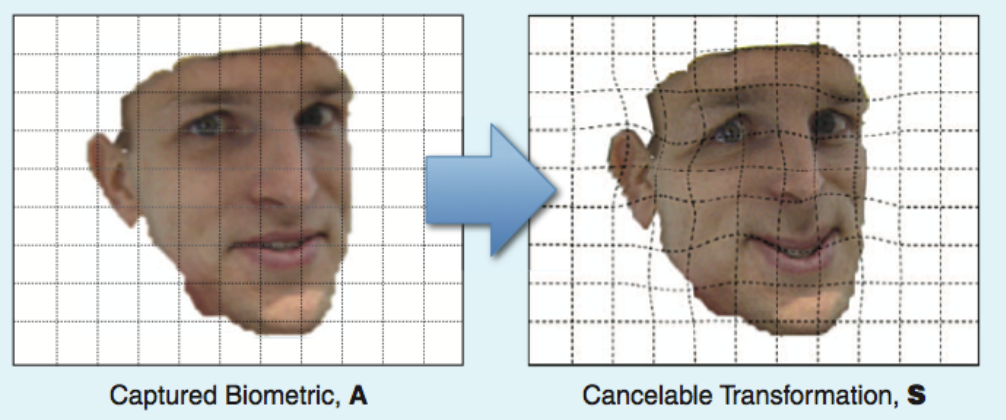


Biometrics as Secure Multiparty Computation

S. Rane, Y. Wang, S. C. Draper and P. Ishwar, "Secure Biometrics - Concepts, authentication architectures and challenges -," IEEE Signal Processing Magazine, Vol. 30, No. 5, pp. 51-64, 2013

近年の研究状況
—Cancelable biometrics—

- 生体情報の画像そのものを保管する
- 画像を関数で変形する
- 認証はスキャンされた情報を同じ関数で変形する



Cancelable Biometrics

S. Rane, Y. Wang, S. C. Draper and P. Ishwar, "Secure Biometrics - Concepts, authentication architectures and challenges -," IEEE Signal Processing Magazine, Vol. 30, No. 5, pp. 51-64, 2013

近年の研究状況

- Secure sketches
  - 生体情報に別の情報を加え、暗号化してサーバに保存。ユーザーはトークン等で認証を行う
- Biometrics as secure multiparty computation
  - 生体情報を関数を使い暗号化する。認証段階では、ユーザー側が持っている秘密鍵をサーバー側が確認
- Cancelable biometrics
  - 生体情報の画像を関数で暗号化、認証する際も同じ関数で変換する

暗号化された状態ならば漏洩しても被害は最小限で抑えることができる

生体認証固有のリスク

- パスワードは暗号化は情報を管理する運営者に委ねられる
- 生体認証はモダリティ機器内で暗号化が完結する
- 不正アクセスにより暗号化されていない情報が漏洩するということが将来的には減っていくと考えられる

しかし…

パスワードでは起こらなかった形で第三者が情報を盗むことが考えられる

想定できるリスク

- 街中での採取
  - カメラ、モダリティ観測技術の向上により、街中を歩く通行人から顔や虹彩などを読み取る
  - SNSなどで公開されている情報で、個人を特定する
- 訪問販売、宅配便を装って採取
  - 静脈・指紋認証などが宅配便の受取などで普及する場合、業者を装った第三者が盗む可能性がある
- 有害なアプリ
  - スマートフォン、PCなどにウィルスを感染させ、暗号化機能を使用不能にし、情報を抜き取る

想定できるリスク

- 街中での採取
- 訪問販売、宅配便を装って採取
- 有害なアプリ

- 一度の漏洩により、同じ部位で登録している別のサービスも次々と破られてしまう
- パスワードと違い情報を変えることができない

漏洩した場合の被害はパスワードよりも深刻

ユーザーの安全性に対する意識調査

ユーザーの安全性に対する意識調査

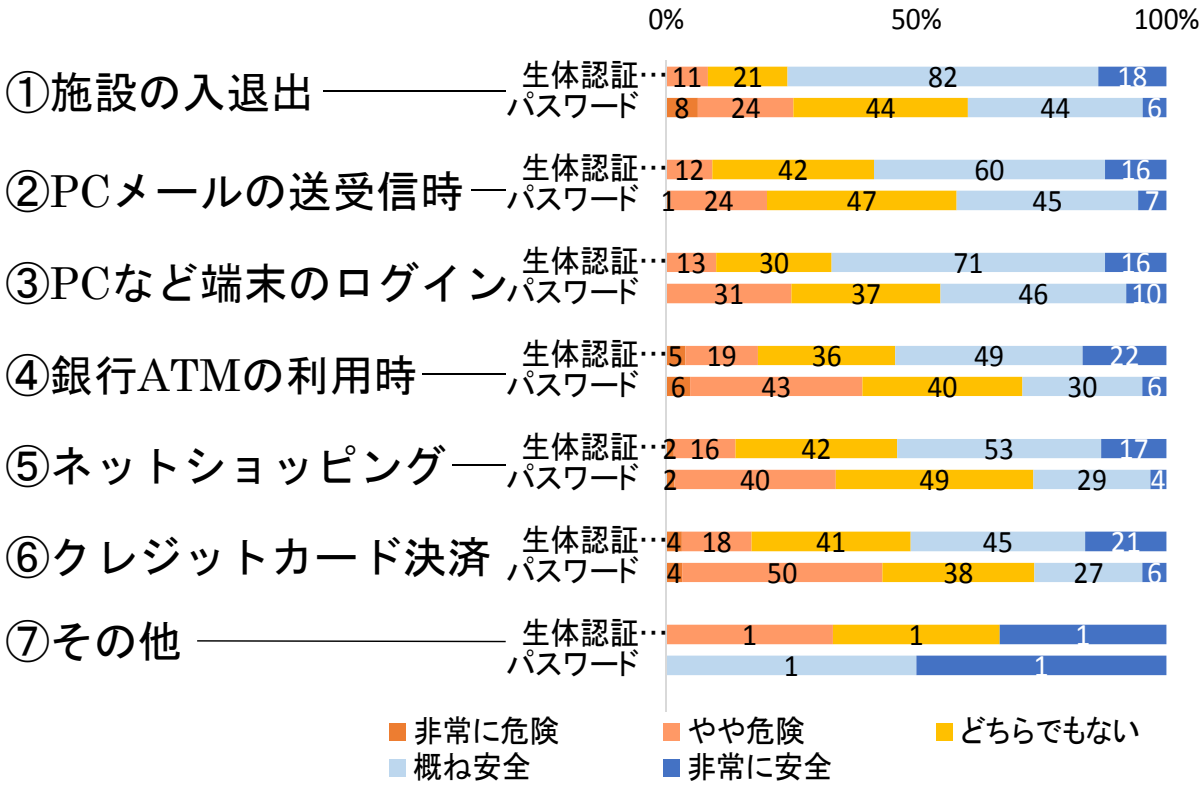
ユーザーは生体認証とパスワードの利用に関し、
安全性に差があると認識していることが懸念される

筑波大学の学生を対象に、生体認証とパスワードの
利用と安全性に関する意識調査を実施

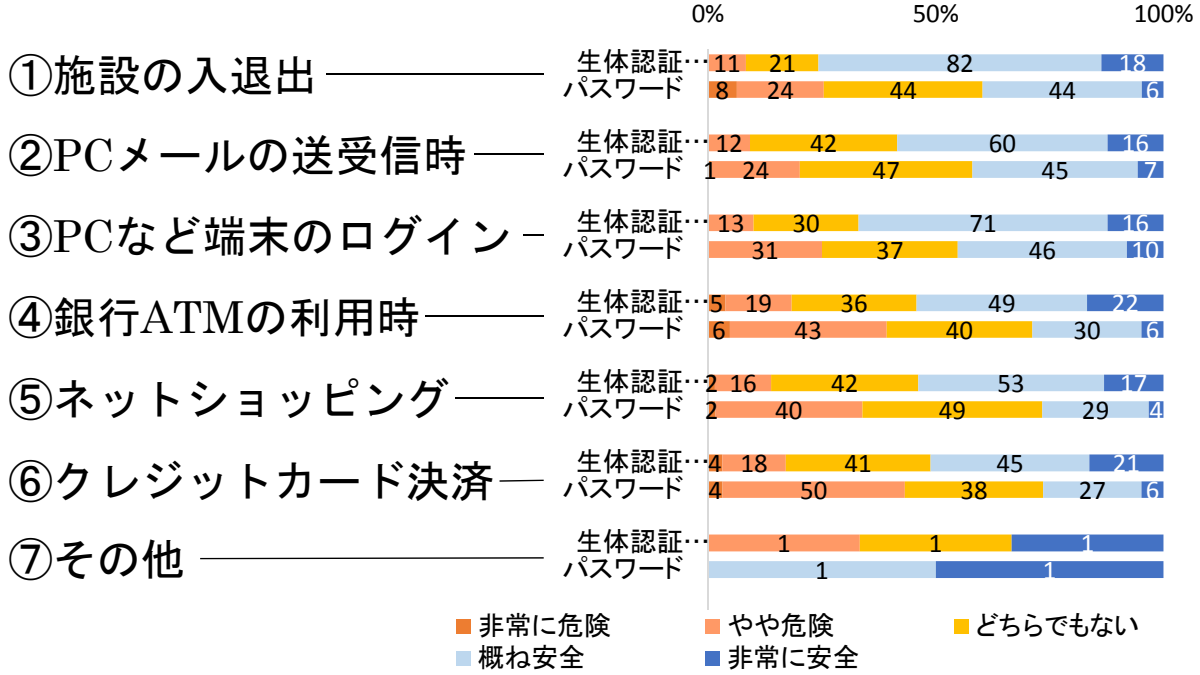
実施日程	7月24日、25日、26日
調査対象	筑波大学の学群生
回収方法	授業の履修者を対象にアンケート調査
サンプル数	134

各認証方式の安全性に関する質問

Q:次のような状況で生体認証及びパスワードを利用するとしたら、
どの程度安全だと思いますか？



各認証方式の安全性に関する質問

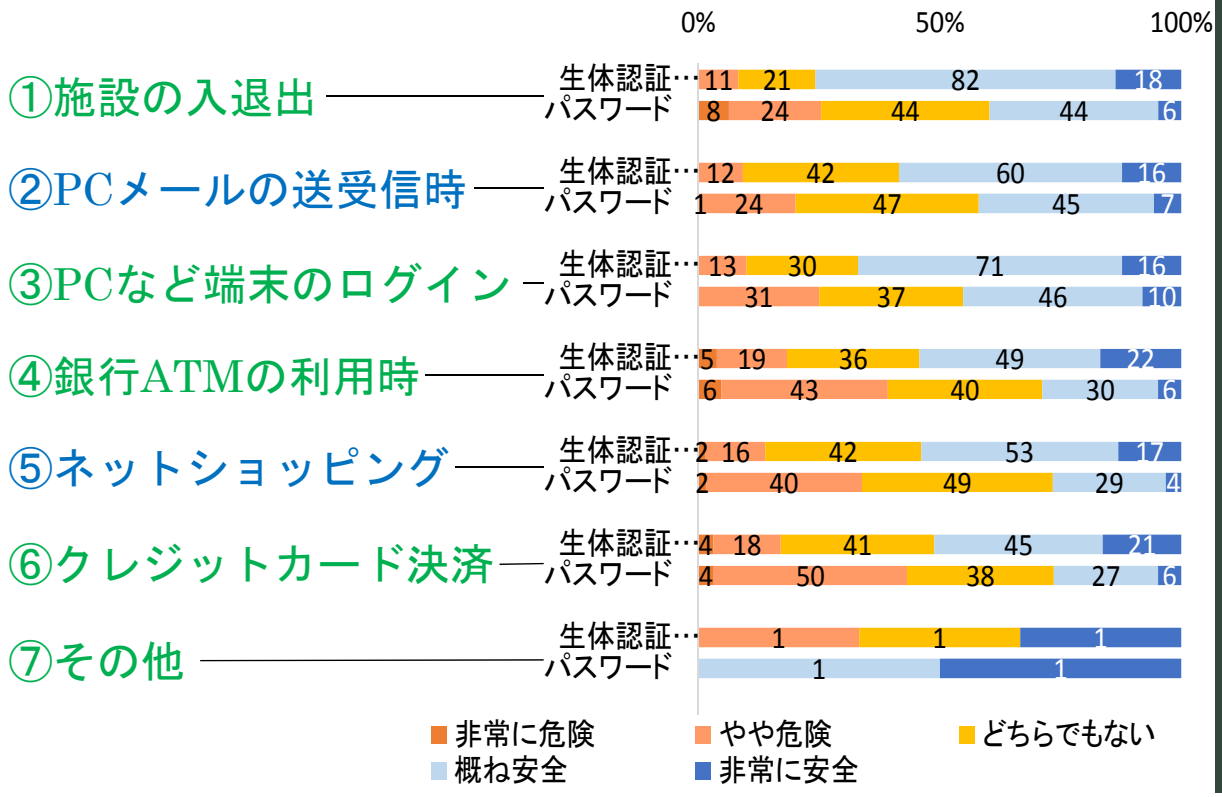


ユーザーは生体認証の安全性を過大評価している可能性あり

情報漏洩などの危機意識が
低下してしまう恐れがある

ネットワーク利用の安全性に関する意識

ネットワークを利用する状況とは…？



ネットワーク利用の安全性に関する意識

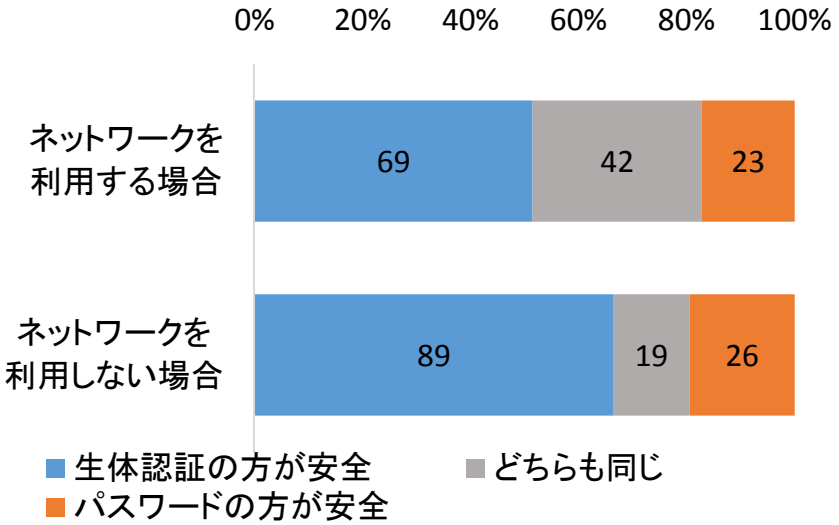
例えば…Q「施設の入退出」について

⇒「施設の入退出」は生体認証の方が安全と判断

ネットワークを利用する場合としない場合で分類

各状況で生体認証とパスワードのどちらが安全かを判断するかを導く

ネットワーク利用の安全性に関する意識



過半数はネットワーク上でも生体認証が安全であると判断

生体認証のネットワーク利用の安全性を過大評価しているのではないか

生体認証のネットワーク利用に関する提言

社会に対する提言

生体認証を運用する際には…

- サーバとアクセスするタイプのモダリティ機器は個人が持つものとする

  ↳ 第三者から提示されたモダリティ機器から真の生体情報を読み取られるのを防ぐ

- モダリティ機器を製造する側の企業は、暗号化技術を取り入れたモダリティ機器を作る
- 不正アクセス行為の監視の強化
- 生体情報の漏洩が発覚した場合は、すぐにその生体情報で登録したサービスすべてを凍結できるようなシステム

  ↳ 安全性の更なる補強を行う

ユーザーに対する提言

- 生体情報が換えの効かないものということの認識
- 自分のモダリティ機器をしっかり管理し、安易に他の人から提示されたモダリティ機器を使わない

  ↳ 詐欺や情報漏洩の防止

- マスメディアや教育機関での告知

  ↳ 大衆やこれから生体認証を利用する若い世代に対する注意喚起

参考文献

- [1] 古川宏, 佐藤美佳[他]：リスク工学の視点とアプローチ: 現代生活に潜むリスクにどう取り組むか，コロナ社，2009
- [2] YAHOOサーバの漏洩事件: http://www.csmonitor.com/Innovation/Horizons/2012/0712/Yahoo-hack-steals-400-000-passwords.-Is-yours-on-the-list
- [3] YAHOOサーバの漏洩事件の損害: http://money.cnn.com/2012/07/12/technology/yahoo-hack/
- [4] Operation Motorman: http://blogs.journalism.co.uk/2011/02/04/observer-seeks-to-distinguish-operation-motorman-from-the-phone-hacking-scandal/
- [5] ICO: What price privacy? – The unlawful trade in confidential personal information, Information, Commissioner to Parliament, 2006
- [6] NEC イグアス、暗号化／生体認証と管理ソフトを組み合わせた情報漏洩防止パッケージ
- http://www.nikkeibp.co.jp/article/news/2030521/351232/
- [7] S. Rane, Y. Wang, S. C. Draper and P. Ishwar, "Secure Biometrics - Concepts, authentication architectures and challenges -," IEEE Signal Processing Magazine, Vol. 30, No. 5, pp. 51-64, 2013.
- [8] 鈴木雅貴，井沼学，大塚玲：生体認証システムにおける情報漏洩対策技術の研究動向，日本銀行金融研究所，2010
- [9] EMC：正しい認証方式の選び方ハンドブック，RSAセキュリティ, 2008
- [10] 桝野隆平：タキヒラパスワードの脆弱性と対策-認知心理学の知見を生かして，ニーモニックセキュリティ，2010