様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　　６　日現在

機関番号：　１７３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３３０１５５

研究課題名（和文）生体認証におけるデジタル証拠性・無証拠性に基づく分類と強制・悪用への耐性評価

研究課題名（英文）Categorization of biometric authentication based on digital receipt-freeness and evaluation of coercion-resistance

研究代表者

上繁　義史（UESHIGE, Yoshifumi）

長崎大学・ICT基盤センター・准教授

研究者番号：００３００６６６

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：遠隔で行われる生体認証の処理過程で生じる中間情報（通信情報など）を収集しても，生体認証の証拠となる情報が得られないことを無証拠性と定義した。また，無証拠性の議論を基に，第三者からの脅迫があったとしても，証拠を提示できないことを耐強制性と定義した。
この定義に基づいて，これまでに提案されてきた遠隔の生体認証の方法について，無証拠性と耐強制性を有するか検証を行った。そのほとんどのケースで，その性質を満たさないことが分かった。これらの成果を情報セキュリティに関する国内学会（4件），国際会議（4件（2件は審査を受け採択，2件は招待講演））で報告した。

研究成果の概要（英文）：We defined third person cannot obtain evidence of remote biometric authentication transaction as "receipt-freeness", if the third person could not collects intermediate information of biometric authentication process such as communicating data. Depending upon the discussion of "receipt-freeness", we also defined no user could obtain the evidence such that coercer who constrained the user to execute biometric authentication is convinced as "coercion-resistance."
From the above definition, we investigated whether "receipt-freeness" and "coercion-resistance" are satisfied or not in conventional remote biometric authentication protocols. As a result, most of them did not satisfy. We read the papers of the results at domestic conference (4 papers) and international conference (2 regular papers and 2 invited lectures) of information security.

研究分野：　情報セキュリティ，教育工学，画像工学

キーワード：　生体認証　プロトコル　無証拠性　耐強制性

１．研究開始当初の背景

生体認証技術は本人認証技術として，重要施設への入退室，パソコンやスマートフォンなどの情報端末へのログオン，マンションなどの出入口開閉，入出国管理といった場面で利用されている。最近では Facebook や Google といったソーシャルメディアにおける，顔認証技術を用いた写真の自動タグ付与機能のように，本人認証とは異なるアプリケーションも出てきている。

生体認証については，従来本人認証の機能に関するセキュリティ維持に主眼を置いて，様々な脆弱性の検討がなされてきた。この検討は，「本人認証の機能を提供する側」の視点に立ったものであり，本人認証の精度，照合テンプレートの保護，認証システムの可用性の維持などについての分析であった。近年生体認証を遠隔で行うためのプロトコル（生体認証プロトコル）の研究が行われており，研究代表者も研究分担者と共同研究により，利用者のプライバシに配慮した生体認証プロトコルを発表している。

生体認証技術は証拠性確保（フォレンジック）の視点で研究がなされてきた（図 1）が，証拠性確保と反対の視点，すなわち電子データを認証システム内部に残さない「無証拠性」の視点（アンチフォレンジック）にたった研究が体系的になされてはいない。暗号プロトコルの分野では，Sakurai と Itoh のゼロ知識証明による本人認証における無証拠性確保をはじめとする数多くの研究事例あり，図 3(b)のような強制された状況への耐性について研究が行われている。生体情報を使った研究として，音声の特徴による暗号化鍵生成，皮膚の電気抵抗の変化による暗号鍵生成方式があるものの，これらは脅威が発生した際の生体の変化を捉えることを主眼に置いたもので，必ずしも生体認証に関する研究ではない。日本においては，このような研究事例もほとんど見られない。

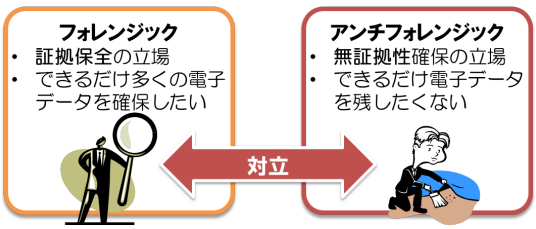


図 1　証拠性(フォレンジック) VS 無証拠性(アンチフォレンジック)

２．研究の目的

本研究では，まず耐強制性や無証拠性について理論的に定義を行い，それに基づいて近年提案されている生体認証プロトコルについて，証拠性・無証拠性の視点から分類を行い，強制，悪用への耐性について強度評価を行い，アンチフォレンジックの視点から見た生体認証の体系化を目的とする。

３．研究の方法

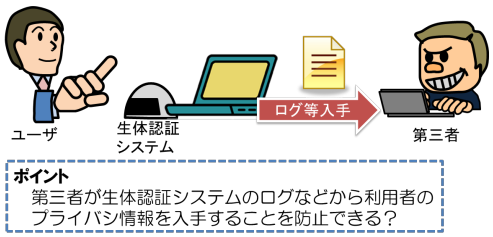
全体の研究目標としては，生体認証における無証拠性・耐強制性について理論的な定義を行い，多種に及ぶ生体認証プロトコルや生体認証を組み込んだデバイスについて，無証拠性・耐強制性の視点から理論的評価を行い，体系化することとする。これを実現するために申請期間（平成 25 年度～平成 27 年度）において，以下の小課題に関する研究を行った。

（1）　生体認証における無証拠性・耐強制性について理論的な定義と評価モデルの検討

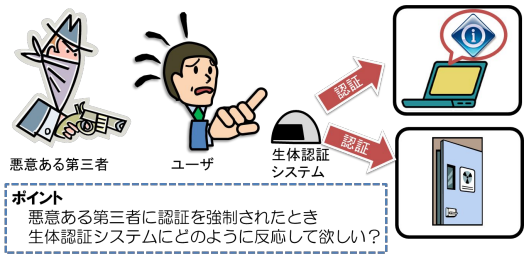
電子投票プロコトルにおける無証拠性，証拠性に関する議論を参考として，生体認証における無証拠性・耐強制性について理論的定義を行い，これらの性質に関して生体認証プロトコルを評価するにあたって適切なシナリオ，及び評価項目を明らかにする。

（2）　生体認証プロトコルの証拠性・無証拠性の分類，強制・悪用への耐性評価

生体認証プロトコルについて，用いられている基礎技術（暗号系など）や証拠性・無証拠性がどの程度確保できるか/できないかに基づいて分類を行う。分類結果を用いて，シナリオに基づく通信を行ったと仮定して，個々の生体認証プロトコルについて強制及び悪用への耐性に関する強度評価を行う。



(a) 第三者による過剰なプライバシ情報収集



(b) 悪意のある第三者による強制

図 2　生体認証において無証拠性の確保が必要な状況と検証のポイント

４．研究成果

無証拠性と耐強制性について，電子投票プロトコル（インターネットを用いた ICT による投票システムの通信方法）における要件を参考に，インターネットを介した遠隔の生体

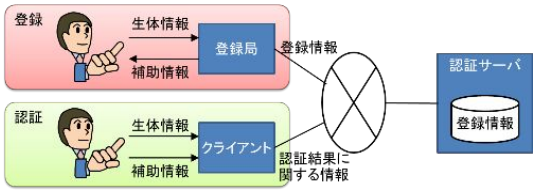


図 3　本研究が対象とするリモート生体認証のモデル

認証(図 3 を参照)を想定して定義を行った。無証拠性の定義のポイントは「ユーザの認証行為を第三者に証明できるような，生体情報（指紋，虹彩，静脈パターンなどの画像を変換したもの）に関する証拠が得られない」というものである。耐強制性については，無証拠性の議論を前提に，「第三者から強制されたとしても，強制したとおりの認証が行われたことを示すような，生体情報に関する証拠を提示できない」ものと定義した。

これに基づいて，既存のインターネットを介した遠隔の生体認証に関する研究について，無証拠性及び耐強制性の有無について検証を行った。その対象としたのは，以下の研究である。それぞれの研究について，認証の過程で通信される情報や認証サーバなどに蓄積される，認証の処理過程で生成される情報の中に，元の生体情報（指紋，虹彩，静脈パターンなどの画像）を変換したものが含まれるかどうかによって，評価を行った。変換した情報が逆変換によって元に戻るかどうかについては，本研究では問わないこととした。

(1) 取り消し可能な生体認証（センサから取得した生体情報もしくは特徴情報に対して，ランダムな摂動や座標変換などの非可逆な変換を施すことにより，元の情報を秘匿する認証方式）
(2) 非対称生体認証（認証サーバに対して，生体認証に必要な情報を直接提示することなく，両者が近いことを，ゼロ知識証明プロトコルを用いて証明することによって，認証を行う方式）
(3) 生体認証と公開鍵基盤を用いた拡張可能な本人認証基盤（インターネットにおいて生体認証の背景情報をやりとりする基盤における認証）
(4) IC カードを用いた利用者の匿名性を確保可能な生体認証ベースの認証（登録センターが発行するスマートカード上の生体認証の情報を用いてクライアント側で認証し，その結果をサーバにて相互認証する方式）

その結果，(3) のケースにおいて，テンプレートのハッシュ値を含まないなどの特定の利用法をした場合と，(4) のプロトコルの 1 つがこれらの性質を満たしうることが分かった。その他のケースにおいては，これらの性質を満たさないことが分かった。理由としては，インターネット上で行われる通信内容に，何らかの形で生体情報を変換したものを含んでいたことが上げられる。このことが直接生体情報の漏えいを意味するものではないが，多くの生体認証プロトコルにおいて，生体認証に関する何らかの情報収集が可能であることが分かった。

これらの成果は下記の国内学会 (4 件)，国際会議（4 件（2 件は審査を受け採択，2 件は招待講演））で発表した。

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 8 件）

下記発表のうち，(1) 及び (5) は査読有りの国際会議での講演，(4) 及び (6) は国際会議での招待講演である。

(1) Yoshifumi Ueshige, Kouichi Sakurai, Analysis of “Receipt-freeness” and “Coercion-resistance” in Biometric Authentication Protocols, 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA2016), 23-25 March 2016, Crans-Montana (Switzerland)
(2) 上繁義史，櫻井幸一，生体認証プロトコルにおける無証拠性に基づく否認可能性, 2016 年電子情報通信学会総合大会，2016 年 3 月 15 日～3 月 18 日，九州大学伊都キャンパス（福岡県福岡市）
(3) 上繁義史，櫻井幸一，生体認証プロトコルにおける無証拠性と耐強制性に関する考察，コンピュータセキュリティシンポジウム 2015 (CSS2015)，2015 年 10 月 21 日～10 月 23 日，ブリックホール（長崎県長崎市）
(4) Kouichi Sakurai, “Forensic vs. Anti-forensic in Biometrics: Towards Receipt-freeness and Coercion-Resistance in biometric authentication protocols”, The 3rd International Conference on Information and Communication Technology (ICoICT2015), 27-29 May 2015, Bali (Indonesia)
(5) Yoshifumi Ueshige, Kouichi Sakurai, “Towards "Receipt-freeness" in Remote Biometric Authentication”, Fifth International Conference on Emerging Security Technologies (EST2014), 10-12 Sep. 2014, Madrid (Spain)
(6) Kouichi Sakurai, Yoshifumi Ueshige, “Receipt-freeness of remote

biometric authentication protocols”, The First Collaboration under MoU between the Centre for Information Security, MMU and ISIT Security Laboratory: Attribute-Based Identification and Remote Biometric Authentication, 23 Jun. 2014, Melaka (Malaysia)

(7) 上繁義史，櫻井幸一，“生体認証プロトコルにおける無証拠性確保に関する考察”，電子情報通信学会 2014 年総合大会，2014 年 3 月 18 日～3 月 21 日，新潟大学（新潟県新潟市）

(8) 上繁義史，櫻井幸一，“生体認証プロトコルにおける証拠性・無証拠性に関する一検討”，2014 年暗号と情報セキュリティシンポジウム（SCIS2014），2014 年 1 月 21 日～1 月 24 日，城山観光ホテル（鹿児島県鹿児島市）

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
上繁　義史（UESHIGE, Yoshifumi）
長崎大学・ICT 基盤センター・准教授

研究者番号：00300666

(2)研究分担者
櫻井　幸一（SAKURAI, Kouichi）
九州大学・システム情報科学研究科・教授

研究者番号：60264066