様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １６ 日現在

機関番号：１７３０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１２９７

研究課題名（和文）無証拠性・耐強制性・否認可能性を保証するプライバシ保護が可能な認証プロトコル

研究課題名（英文）Authentication protocol with privacy protection ensuring receipt-freeness, coersion-resistance and deniability

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）　　3,200,000円

研究成果の概要（和文）：無証拠性，耐強制性，否認可能性を持つ認証プロトコルの構築を目的として研究を行った。主要な成果は次の通りである。(1)匿名性と無効化を同時に実現する暗号を用いた認証の仕組みとして，失効機能を備えた匿名否認が可能な述語認証スキームを提案した。(2)ブロックチェーンを用いた電子投票における無証拠性と耐強制性の研究（11件）の評価を行った。その多くの方式において，無証拠性の議論はあるが，耐強制性の保証が難しいことが判明した。(3)認証の無証拠性と耐強制性について，証拠情報に基づき定義を行った。さらに定義を適切に行うため，生体認証について，正当な利用者に認証行為を強制しうるシナリオを提示した。

研究成果の学術的意義や社会的意義
本研究成果の成果は，（1）無証拠性及び耐強制性の議論の基礎となった，電子投票の分野における最新技術動向について精査し，耐強制性確保の難しさを確認した点，（2）認証における無証拠性及び耐強制性を定義する上で，証拠情報に関する考察だけでは不足であることを明らかにした点，（3）暗号学のアプローチによる匿名での否認可能な述語認証スキームを提案した点にある。特に（3）はプライバシリスクを低減した認証方法が構成できるようになったという意味で学術的意味は大きい。（1）と（2）については，当初の研究計画では想定できなかった事象であり，今後の研究展開の基礎的知見となった。

研究成果の概要（英文）：The purpose of this study is to construct an authentication protocol with receipt-freeness, coercion-resistance, and deniability. The main achievements are as follows. (1) As an authentication mechanism using encryption that simultaneously realizes anonymity and invalidation, we proposed a predicate authentication scheme that ensures anonymity and deniability with a revocation function. (2) We evaluated 11 studies on the receipt-freeness and coercion-resistance of electronic voting using blockchain techniques. In many of them, although there is an argument for receipt-freeness, it has been found that it is difficult to guarantee the coercion resistance. (3) The receipt-freeness and coercion-resistance of authentication were defined based on evidentiary information in authentication protocols. Furthermore, to define it appropriately, we proposed scenarios in which legitimate users can be forced to perform authentication acts for biometric authentication.

研究分野：情報セキュリティ，教育工学

キーワード：無証拠性　耐強制性　否認可能性　認証プロトコル　暗号

１．研究開始当初の背景

(1)　研究の背景

認証技術は様々な Web 等のサービスやパソコン，スマートデバイスなどのログオンなどに多用されており必要不可欠な技術である。2014 年には，国内外の多くの企業が参加する FIDO（Fast IDentity Online）アライアンスによる認証プロトコルが標準化[3]され，2017 年 10 月開催の CEATEC JAPAN2017 において，その実装が展示されるなど，セキュアかつプライバシに配慮した Web 認証の要求は高まる一方である。それ以降も，FIDO に準拠した製品は数多く発表されている。

研究代表者は，これまで生体認証が「証拠」を収集するフォレンジック的視点で研究されてきたのに対して，「無証拠」につながるアンチフォレンジック的視点で研究を展開してきた[1, 2]。そのポイントは認証プロセスの通信データの収集により，ユーザが Web 等サービスを利用した証拠を（過剰に）確保できる可能性を生じ，当該ユーザへのプライバシ侵害につながることを指摘した点にある。さらに証拠を悪用した，ユーザに対する認証の強制や，認証後のクライアント及びサーバに残った認証プロセスの中間情報の窃取の可能性により，このプライバシリスクはより深刻になることは自明である。本研究のポイントを下図に示す。

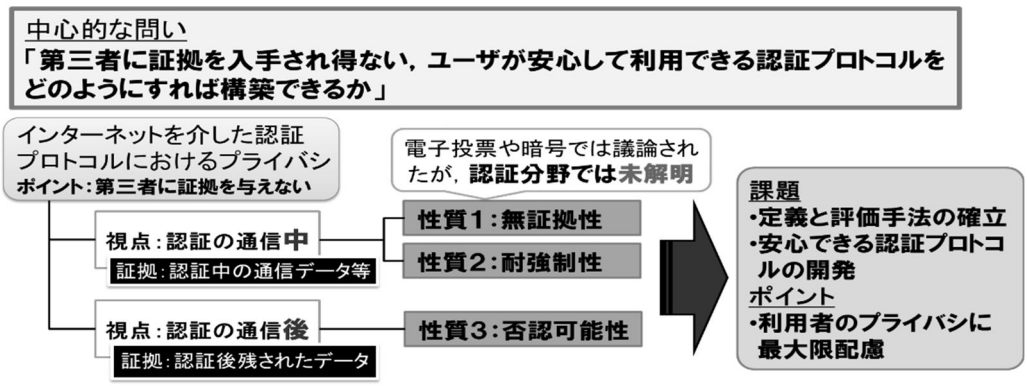

図 1　中心的な問いと主な研究課題

(2)　本研究の着想に至った経緯

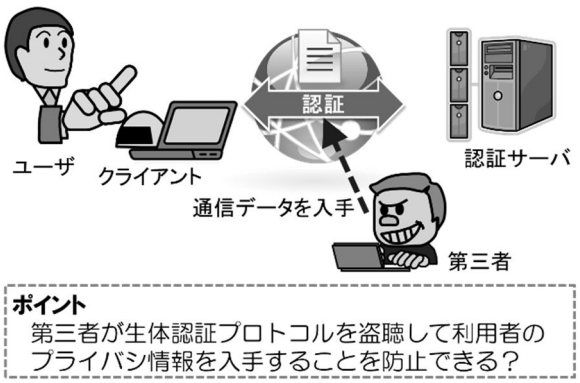

図 2　生体認証におけるプライバシリスク

認証技術のセキュリティはこれまで「本人認証のサービス提供者」の視点に立ったものであった。一方，インターネットを介した遠隔での認証サービスが一般的になった昨今，左図のような状況が発生し，ユーザの「忘れられる権利の行使」を含めた，将来のプライバシリスクを招くと考えられる。

従前，研究代表者が生体認証に特化して検討してきた概念を認証プロトコル全般に拡張することにより，保証すべきプライバシを特定し，「ユーザが真に安心できる認証プロトコル」に昇華させることができると考えた。

２．研究の目的

研究代表者は従前，上述の視点に基づき，生体認証プロトコル利用のプライバシについて，電子投票 [6]での議論を応用した。すなわち，実行中における，認証に関する証拠取得の不可能性（無証拠性）及び，第三者からの強制に対する，ユーザによる証拠提示の不可能性（耐強制性）について提案し，既存の認証プロトコルがその性質を満たすか評価を行ってきた[1, 2]。本来この議論は生体認証に限定されないので，本研究の目的を以下の通りとした。

我々の生体認証における成果を，インターネットを介した認証プロトコル一般の議論に拡張して，プライバシに関する厳密な定義や評価手法を確立するとともに，評価の高くなる認証プロトコルを理論的に明らかにし，そのプロトタイプ実装を開発すること

暗号通信プロトコルのソフトウェア OpenSSL において Heartbleed の攻撃により秘密鍵をはじめとしたメモリ情報が漏えいする脆弱性が発見され [4]，第三者が処理中の秘密のデータを入手できる可能性が示された。Google が公開した TensorFlow といったディープラーニングのソフトウェアを入手し[5]，これらの秘密データを整形して入力することにより，個人がユーザのプライバシを分析できる基盤を容易に入手できるようになった。特に 2020 年代より，生成系 AI が複数登場し，一般にも開放されていることから，脅威は増大する一方と考えられる。

遠隔での認証プロトコルにおいて，その通信内容が窃取されるリスクが現実のものとなっており，様々な Web サービス等の利用状況に関するプライバシ保護が困難になってきた。そのようなことから，本申請のように，認証プロトコルのプライバシ保護について新たな視点を提起し，その実装を可能とする研究は，今後のユーザフレンドリーなインターネットビジネスを展開する上で必要不可欠であると考えられる。

【参考文献】

[1] Kouichi Sakurai, “Forensic vs. Anti-forensic in Biometric Authentication Protocols: Towards Receipt-freeness and Coercion-Resistance in biometrics”, Cyber Security Workshop, （2016 年，招待講演）

[2] Yoshifumi Ueshige, Kouichi Sakurai, “Analysis of “Receipt-freeness” and “Coercion-resistance” in Biometric Authentication Protocols”, The 30th IEEE International Conference on Advanced Information Networking and Applications (AINA 2016), pp. 769-775, （2016 年，査読あり）

[3] FIDO Alliance, “FIDO Alliance”, 更新 2017-09-14, https://fidoalliance.org/,（参照 2017-09-30）

[4] 情報処理推進機構,“ 更新：OpenSSL の脆弱性対策について(CVE-2014-0160) ”, 更新 2014-04-15，https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html，(参照 2016-09-25)

[5] “TensorFlow”, 更新 2017-09-08, https://www.tensorflow.org/, （参照 2017-09-30）

[6] J. Heather, S. Schneider, “A formal framework for modelling coercion resistance and receipt freeness”, FM 2012: Formal Methods, LNCS Vol. 7436, pp 217-231, 2012.

３．研究の方法

本研究ではこの目的を達成するために，以下のサブテーマを設け，理論的検討を中心に進めた。

- 一般の認証に拡張された無証拠性及び耐強制性の強度指標に基づく認証プロトコルの評価手法
- プロトコル上，認証後にクライアント及び認証サーバに残されるデータを収集しても，第三者に対して認証の証拠を提示できず，ユーザが否認可能となる性質（否認可能性）の定義及び強度の評価手法
- 高い無証拠性・耐強制性・否認可能性の性質を有する遠隔の認証プロトコル
- 上記認証プロトコルの実装と評価・改良

研究体制としては，研究代表者 上繁が研究全般を担当し，無証拠性及び耐強制性の検討を主に研究分担者 櫻井，否認可能性の検討を主に研究分担者 穴田が担当する。その体制は右図の通りである。

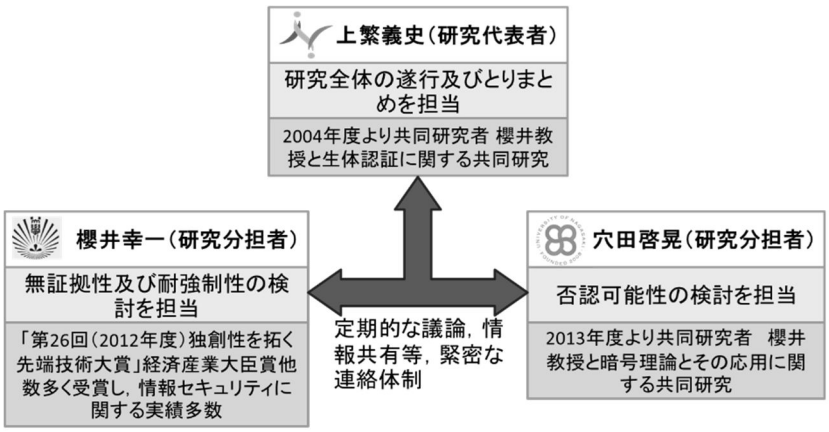

図 3 本研究の研究体制

４．研究成果

上述の 2 にて述べた目的に向けて研究を推進した。各年度での研究成果について，概要を述べ

る。

(1) 2018 年度の研究成果

2018 年度は，否認可能性に関連する成果が 2 つ得られ，2 件の国内学会での発表を行っている。

① サービスに登録された利用者を廃止することができて，なおかつ否認可能性をもつ認証プロトコルを提案した。これは属性（所属など）を利用して，個人のプライバシ性を担保することができる暗号化法を用いて，秘密情報を知っていることを対話的に示す認証を行うものである。（国内学会 1 件）

② 否認可能性を担保した秘密ハンドシェークプロトコルにおける問題を指摘した。インターネットなどの通信において，ペアリング暗号を用いて当事者同士がお互いの ID などを秘密に保ってハンドシェークを行う秘密ハンドシェークのプロトコルにおいて，提案者が想定していた否認可能性が保たれず，通信の証拠となる情報を残すケースがあることを理論的に示した。（国内学会 1 件）

(2) 2019 年度の研究成果

2019 年度は，本研究の主要テーマである無証拠性・耐強制性について，研究の基礎となった電子投票の分野で検討を行うとともに，認証一般に適用すべく，定義を進めた。また，匿名性と否認可能性を有する認証プロトコルの構築方法について成果を得た。この年度では 5 件の学会発表を行った。

① ブロックチェーンを用いた電子投票における無証拠性と耐強制性の研究を評価し，耐強制性を保証することが困難なケースが多いことが分かった。電子投票の近年の研究事例のうち，ブロックチェーン（仮想通貨で用いられている）を利用した電子投票方式 11 件について比較検討を行い，その多くで無証拠性の議論はあるものの，耐強制性の保証が難しいことが判明している。（国際会議の招待講演 1 件，国内学会 1 件）

② 認証の無証拠性と耐強制性に関する定義を行った。遠隔での認証プロトコルにおいて，通信情報から，利用者についてどのような情報が収集可能かを明らかにする必要があると考えられる。そこで認証プロトコル一般において，何が証拠となり得るか，証拠が得られる場合にどのような悪用が考えられるかを理論的に検討し，無証拠性の定義について提案した。無証拠性の考え方から論理を展開して，耐強制性の定義を行った。（国内学会 1 件）

③ 匿名性と否認可能性がある匿名否認可能認証を構築する方法を提案した。匿名性と無効化を同時に実現する，暗号を用いた認証の仕組みについて，安全性の定義を行った上で，匿名否認可能述語認証スキームの発展形として提案している。（国際会議 1 件，国内学会 1 件）

(3) 2020 年度の研究成果

2020 年度は本来最終年度であったが，新型コロナウイルス（COVID19）の影響により，研究推進が十分に行えなかった。研究成果は以下のとおりである（国内学会 1 件）。

① 認証プロトコルのスキームの機能として失効（revocation）がある。失効は登録（registration）と対をなす処置でもあり，デジタルにおける登録情報を無効化する処置を意味する。失効機能を実現する方法としては，失効リストを用いる方法が一般的である。これは，失効リストにデジタルにおける登録情報が載っているか否かで，失効されているか否かを判定する方法である。ここで，認証プロトコルに匿名性を持たせようとすると，執行させるべき登録者を特定することが困難なことから，失効機能の実現が困難となる。本研究では，暗号学に基づいて，否認可能性をも実現する具体策として，失効機能を備えた匿名否認が可能な述語認証スキーム rADPA を提案して，その具体例を提示した。

(4) 2021 年度～2022 年度の研究成果

2021 年度及び 2022 年度は，COVID19 の影響による研究活動の遅延から，研究代表者が研究期間の延長を申請し，認められたものである。（国内学会 1 件）

無証拠性及び耐強制性について，2019 年度の研究成果において想定していた，証拠情報に基づくアプローチだけでは，認証における定義としては不足することが分かった。そのため，当初見込んでいた無証拠性及び耐強制性を有する認証プロトコルの提案が困難となった。

そこで，これ以降は，生体認証に特化して，耐強制性に関する定義について再考を進めることとした。この年度では，新たな定義を見出すため，2019 年度発表の議論の形態にこだわらず，認証行為を強制しうるシナリオをベースとしたアプローチにより研究を行った。

シナリオとしては，生体認証が用いられる，次の 2 つのケースに絞った。1 つ目は，施設の入退出のような，固定された装置による認証，2 つ目は Web サービスなどの移動端末を用いた認証である。

施設の入退出で固定式の端末で認証するケースでは，ID を有する正規の利用者に侵入させ，第三者の希望する操作や情報収集を行わせることが考えられる。このシナリオが実現する場合，入退出の生体認証システムは，強制する第三者が介在した場合，その行動の阻止は困難となる。

次に，移動端末における認証として，多要素認証での応用を想定したシナリオを検討した。多

要素認証の利用者が認証を経て重要情報にアクセスできるとする。この情報の窃取を目的とする第三者がソーシャルエンジニアリング等の方法により，当該利用者を誘導して多要素認証を実行させて重要情報にアクセスさせれば，この第三者は目的達成が可能となる。情報を外部に送信せずとも，画面を撮影すれば，持ち出しが可能となるためである。

以上のように，無証拠性に基づく議論では，認証における耐強制性について定義することは困難であり，シナリオを重視したアプローチが有効となる可能性があることが示唆された。

以上のことから，本研究は否認可能性を有する認証プロトコルについては，実現方法を見出したものの，無証拠性及び耐強制性について，その定義について十分検討が進まず，認証プロトコルの提案には至らなかった。本助成終了後，上記の成果を基に，改めて本研究で目的とした認証プロトコルの検討を進める予定である。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計8件（うち招待講演　1件／うち国際学会　2件）

１．発表者名 穴田 啓晃，上繁 義史
２．発表標題 失効可能な匿名否認可能述語認証スキームの具体化
３．学会等名 コンピュータセキュリティシンポジウム2020
４．発表年 2020年

１．発表者名 上繁義史
２．発表標題 認証プロトコルにおける無証拠性と耐強制性に関する一考察
３．学会等名 情報処理学会コンピュータセキュリティ研究会
４．発表年 2020年

１．発表者名 穴田啓晃，上繁義史
２．発表標題 リボーク機能を備えた匿名否認可能述語認証スキームについて
３．学会等名 2020年暗号と情報セキュリティシンポジウム（SCIS2020），3B2-3
４．発表年 2020年

１．発表者名 Misni Harjo Suwito, Sabyasachi Dutta, Kouchi SAKURAI
２．発表標題 ブロックチェーンを利用した電子投票システムの安全性
３．学会等名 2020年暗号と情報セキュリティシンポジウム（SCIS2020），2E1-3
４．発表年 2020年

１．発表者名
Kouchi SAKURAI

２．発表標題
Security of Anonymous E-voting Scheme after Blockchain: A challenge of achieving Receipt-freeness

３．学会等名
13th International Conference on Network and System Security（NSS2019）（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Hiroaki Anada, Yoshifumi Ueshige

２．発表標題
Generic Construction of Anonymous Deniable Predicate Authentication Scheme with Revocability

３．学会等名
International Conference on Information Technology and Communications （SecITC2019）（国際学会）

４．発表年
2019年

１．発表者名
穴田啓晃，上繁義史

２．発表標題
リボーク機能を備えた匿名否認可能述語認証スキームの一般的構成の検討

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2019年

１．発表者名
櫻井幸一，Somnath PANJA，Sabyasachi DUTTA

２．発表標題
How to make undeniable evidence on Secret handshakes

３．学会等名
情報処理学会 第81回全国大会

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	櫻井　幸一 (Sakurai Kouichi) (60264066)	九州大学・システム情報科学研究院・教授 (17102)	
研究分担者	穴田　啓晃 (Anada Hiroaki) (40727202)	長崎県立大学・情報システム学部・教授 (27301)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関