Vol.2020-DPS-182 No.42
Vol.2020-CSEC-88 No.42
2020/3/13

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

上繁義史*

概要：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あり，様々な Web サービス等の利用状況などのプライバシ情報の保護が重要となってきた．そのための端緒として，認証プロトコルに関する情報（View など）から，利用者について（類推可能なレベルのものも含めて）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．従前著者らは生体認証の認証プロトコルにおいて，利用者の生体情報に関連する情報の収集可能性を議論する土台として，無証拠性及び耐強制性について定義し，その特性を検討してきた．本研究ではこれを認証プロトコル一般に拡張すべく，その定義について提案する．

キーワード：認証プロトコル，無証拠性，耐強制性

Receipt-freeness and coercion-resistance of authentication protocols

YOSHIFUMI UESHIGE*

Abstract: Remote authentication protocols have risk of collecting intermediate data of authentication process in executing parallel. Since various web applications use the authentication protocols, privacy protection like the utilization situation becomes significant. Even though risk of directly compromising the content of the data is low, it is not clear what data can be collected and used as an evidence of some user's authentication process. This situation causes novel privacy issue. In order to discuss this issue, the author proposes receipt-freeness and coercion-resistance based on the discussion of biometric protocols which is the authors' previous work.

Keywords: Authentication protocol, Receipt-freeness, Coercion-resistance

1. はじめに

正規のエンティティ（利用者や機器）の認証，識別はネット上のサービス提供において基本的かつ不可欠な要素である．利用者認証の視点からは，記憶に基づく方式，所有物に基づく方式，身体的・行動的特徴に基づく方式に分類される．これをより一般化して考えると，記憶に基づく方式はあらかじめ相互に取り交わした秘密情報に基づく方式，所有物に基づく方式は正規エンティティがあらかじめ登録した特定機器を用いる方式，身体的・行動的特徴に基づく方式は正規エンティティが予め登録した測定可能な特徴情報によるマッチングを用いた方式である．これらの認証方式は単独，または組み合わせで用いられ，システムで扱われる情報の機密性の程度，システム上要求されるセキュリティの強度，利用可能なコストなどの要因で決定される．

近年，インターネットを介した遠隔の認証が一般的に行われるようになり，様々な認証プロトコルが利用されている。2014 年，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[1]され，近年，Windows Hello や Android OS が生体認証の機能を含めて FIDO の認証を受けるなど，この動向は加速の傾向を見せている。

1.1 本研究の位置づけ

本研究のスタンスを図 1 に基づいて説明する．一般的な認証技術においては，認証側において，利用者のアクセスの日時，クライアントに関する情報，アクセスした利用者に関する情報など,様々な情報をログの形で保持している．これにより，必要があれば，これらの情報を証拠として利用することができる．他方，ログなどにより長期に情報が保存されることになれば，プライバシ上の問題を生じることが予想されることから,証拠となる情報は保存期間など，考慮が必要であると考える．他にも，ログ以外から取得される周辺の情報(本研究で取り上げる認証の中間情報など)が証拠性を持つことでも同様と考えられる．そこで，本研究では，これらのプライバシ上の問題を考慮して，図 1 の「証拠収集を限定的にしたい立場」を重視している．

ログ以外から情報が取得されうる例としては，2014 年 4 月に公開された，暗号通信プロトコルのソフトウェア OpenSSL における Heartbleed の攻撃が挙げられる．この攻撃によってメモリに展開された情報（秘密鍵など）が漏洩する脆弱性が公開され，第三者がサーバ上で処理中の秘密情報を入手できる可能性が示された[2]．また，Web カメラ

長崎大学
Nagasaki University

Vol.2020-DPS-182 No.42
Vol.2020-CSEC-88 No.42
2020/3/13

の映像や身体に関する計測情報のようなプライバシ情報を扱う IoT 機器において，計算資源やセキュリティに関する機能の制約により，不正アクセスされる情報を窃取されるケースが考えられる[3].

また，近年データマイニングへの応用として，加法準同型暗号により暗号化されたデータを直接分析する手法の研究が進んでいる[4].

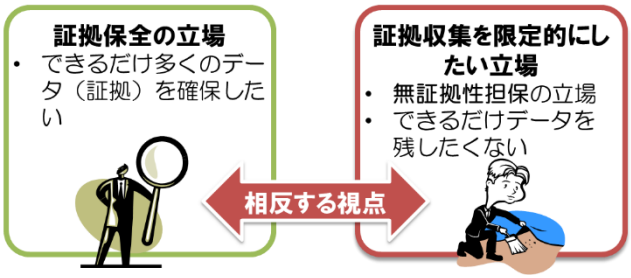

図 1　証拠情報の収集についての異なる立場

Figure 1 Standing positions of collecting evidence

このようなことから，認証プロトコルに関する第三者による過度な情報収集とその利用が可能になることが予想され，証拠収集を限定的にすることが難しくなるものと考えられる．また，大量の証拠情報を収集できた場合，利用者の動向や認証プロトコルの特徴を学習可能になることも予想される．これまで認証プロトコルは機密性の観点から安全性について検証されてきたが，上述のリスクを理解するには十分ではないと考えられる．そこで，本研究では，証拠情報の収集に関するリスク要因を記述する認証プロトコルの性質の検討を目的とする．

本研究のアプローチとして証拠情報の収集と取扱いに注目して，電子投票プロトコルの要件と生体認証における同様の議論[7-9]を参考に，認証プロバイダにおける無証拠性と耐強制性の考え方について検討を行ったので報告する．

2. 認証における証拠性の議論

2.1 なぜ証拠性を考えるか

認証においては，図 2 のように，利用者がその手続きに従って認証者が要求するクレデンシャル等の情報を送信し，認証者側で検証されればその結果（認証結果）を利用者に返す．認証者の機能によっては，トークンを発行するなどして，他のサービスに移行するものもある．

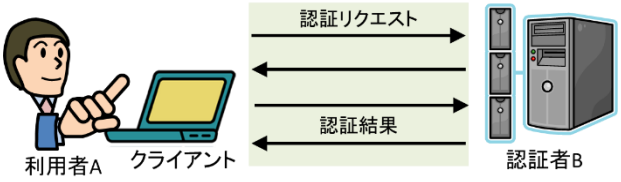

図 2　基本的な認証の流れ

Figure 2 Basic flow of authentication

図 2 では単独の認証セッションを示しているが，昨今の Web サービスのように，利用者とサービス提供者が遠隔となっている状況においては，若干のタイミングのずれはあるものの，多数の認証セッションが並行して実行される．そこでは，個々の認証セッションの中間情報がインターネットをはじめとする通信回線上でやりとりされることになる．それぞれの中間情報は，種々の暗号プリミティブを利用するなどして，第三者に直接的に内容（平文）が知られないことにより機密性を維持している．その安全性については暗号プリミティブの安全性に負う部分が大きいと考えられる．暗号分野においては識別不可能性に基づく，攻撃者の計算能力を仮定した安全性解析が行われる[6].

図 2 の認証者 *B* の行う通信（正確には View）を観測する第三者を仮定すると，この第三者は複数のセッションに関する中間情報を観測することで，膨大な情報を入手できることになる．個別の中間情報の内容それ自体が漏洩するリスクが低いとしても，他の付随する中間情報や認証プロトコルに関する知識を利用することができれば，個々の利用者の利用状況やプロトコルの実装等に関連付けられる情報を入手されるリスクを生じると考えられる．そのような情報のうち，第三者を納得させられるものについては，これを「証拠」と捉えることで，プライバシ情報の収集リスクと考えることができる．第三者が証拠を求める動機づけとしては，利用者のプライバシ情報の収集，不正利用を目的とした調査などが考えられる．

これまでの認証プロトコルに関する議論では，上述したように，単独の認証セッションを想定し，送信した個別の情報の機密性を重視していると考えられ，必ずしも並行して実行される場合の大量の情報の入手までは考慮されていないと考えられる．

2.2 何が証拠になり得るか

まず利用者に関する情報について考えると．認証プロトコルでは，ユーザ ID や秘密情報（パスワード，センサから取得した特徴情報，テンプレート情報など）といったクレデンシャル情報をはじめ，様々な情報が結合され暗号プリミティブを用いて変換されて通信される．これらの情報は利用者に特有の発生の仕方をする場合，証拠となりうる．認証プロトコルについては，ネゴシエーション段階で暗号プリミティブの選択，認証結果，電子証明書，認証後利用されるサービスに関する情報が考えられる．

2.3 悪意ある証拠の利用

上では，第三者は認証プロトコルに基づく通信を外部から観測するケースを考えた．次に，第三者が攻撃者として関与するケースとして，自身が望む行動を利用者に対して強制する状況を考える．第三者が直接利用者を監視できる場合には，第三者が望む通りに利用者が行動した（認証した）ことを容易に確認することができる．他方，第三者が利用者に対して遠隔となるケースでは，利用者の行動につ

いて,何らかの方法で納得のできる情報を得る必要がある．そのような情報が利用者から提示され，第三者を納得させるものであるならば，この情報も証拠の一種と考えることができる．

以下では，認証プロトコルの性質として，この議論を踏まえて，無証拠性と耐強制性を定義して，より一般的な視点で議論を行うための土台について考察する．

3. 無証拠性

無証拠性（Receipt-freeness）は従来電子投票の分野で研究における，要求事項の 1 つとされており[5]，投票者が誰に投票したのかを示す証拠（Receipt）を生成することができないという性質であった．本研究では，これと生体認証における同様の議論[7-9]をヒントとして，認証一般において第三者が，平文レベルのクレデンシャル情報が直接得られなくても，通信の View として観測される暗号文やハッシュ値，その他の付随的な情報から利用者に関連付けられる情報を得られた場合に，第三者を納得させられる情報ととらえることができるため証拠になると考える．逆にこのような情報が得られない場合に無証拠であると考えることができる．

また，単独の認証実行時の View から上記の証拠が得られなくても，認証プロトコルの実装などの付随する情報が得られる場合，第三者が認証プロトコルについて学習することが考えられる．その知識の蓄積から，部分的であっても，複数の利用者に関するプロトコル利用の情報を入手するリスクを生じる．これについても第三者を納得させることが可能な情報であれば証拠として扱うことができる．

証拠となる情報の範囲が広いことや，検証に必要な情報を利用者から得る必要性から，証拠が完全に残らないことは,認証プロトコルにおいて,必須の要件とは言えないが，この性質を満たさない認証プロバイダを利用する場合には,サービスの内容や情報を必要とする期間などを考慮すべきものと考える．

3.1 認証プロトコルにおける無証拠性

本論文では，認証を行うのが利用者もしくは直接利用者が操作する端末に限定する．下図に示す状況を想定して，認証プロトコルの無証拠性を以下のように定義する．

定義 1（認証プロトコルの無証拠性）

認証プロトコル X を動作させて通信路上で観測される View に現れる情報を$I = \{I_1, I_2, \cdots, I_n\}$とする．semi-honest な利用者（認証クライアント）A と honest な認証者（認証サーバ）B の間で認証プロトコル X を使って認証が行われたことを,送信者 A の認証プロセスについて観測可能な View の情報 I を用いて，第三者 C を納得させられる情報$E = \{E_1, E_2, \cdots, E_m\}$を全く得られない性質

定義 1 で利用者 A を Semi-honest と仮定した理由は，認証プロトコル X に関する情報を得るために，自己の認証プロセス実行に関する I（可能であれば E）を第三者 C に売り渡すことで利益を得るなど，第三者と結託する可能性が考えられるためである．利用者 A の能力としては，正常に認証プロトコルを実行し I の部分集合（認証者 B から送られてきた情報や自身のクレデンシャルを用いて変換された情報など）を自力で計算できるものとする．また，認証セッションに関する何らかの情報を入手するために，本来認証プロトコルに含まれない情報を選択的に生成し，その情報を X の実行時に挿入する程度の計算能力を仮定する．ここでは暗号解析のような計算ではなく，認証プロトコル X を実行できれば十分と考えられるので，多項式時間程度の計算能力が妥当と考えられる．

第三者 C については，その目的を認証プロトコル X の View の観測値 I から証拠 E（サービスの利用傾向に関する情報や認証プロトコルについての情報）を入手することを想定している．すなわち，第三者 C は必要とする情報 E を得るために，$E = f(I)$のような n 対 m の写像 f を構成する必要がある．このことから，第三者 C の能力としては，認証セッションに直接的な攻撃（中間者攻撃やリプレイ攻撃など）を行うことは想定せずに,利用者 A に関する View の情報 I を取得して蓄積できる必要がある．また，取得した I から f を構成し，$E = f(I)$ を得るための分析が必要となると考えられるため，確率的多項式時間程度の計算能力を仮定すべきと考える．

定義 1 では無証拠性として，証拠 E が全く得られない性質を定義しているが，これは定義としての条件が強いと考えられるので，部分的な証拠を得られる場合について考慮できるように，以下の定義を置く．

定義 2（部分証拠性）

定義 1 における第三者 C が納得するのに必要十分な情報$E = \{E_1, E_2, \cdots, E_m\}$の全ては得られないが，その部分集合$E' = \{E_{m_1}, E_{m_1}, \cdots, E_{m_k}\}$ $(m > m_k)$を得られる性質

定義 2 においては，第三者 C が納得する要件として，証拠として，$E = \{E_1, E_2, \cdots, E_m\}$ を全ての要素を入手することを挙げている．部分証拠性の定義においては，証拠 E の部分集合 E'を得ることを想定しているため，C は納得すること（検証や推定すること）はできないが，疑いをもつことは可能になると考えられる．

3.2 本研究における無証拠性と機密性との違い

本研究における証拠に関する議論においては，攻撃者を含めた第三者がクレデンシャル情報それ自体を平文で入手することは必ずしも目的としていない．認証プロトコルの利用に関する直接的な情報，もしくは傍証を含めて入手可能な情報の集合 I に基づいて証拠 E を推定あるいは検証し

Vol.2020-DPS-182 No.42
Vol.2020-CSEC-88 No.42
2020/3/13

得るかに関心がある．この立場では，必ずしも機密性と無証拠性は等価ではないと考えられる．

4. 耐強制性

耐強制性（Coercion-resistance）も従来から電子投票のプロトコルが具備すべき要件と考えられており，複数の定義が知られている[5]．電子投票における耐強制性の特徴は，強制者（coercer）が，投票者が投票を行っている間（投票ブースにいる間）に，誰に投票するかを指示するなど，投票者の行動に影響を与える状況が仮定されている．投票者が第三者に指示に従ったことを納得させる情報が得られない性質が求められる．

本研究では，上記 3．無証拠性の議論に基づいて，認証プロトコルの性質としての耐強制性について考察する．

強制者に関する仮定として，被強制者（サービスの利用者）が利用可能であり，強制者には利用できないサービス（認証を含む）について，強制者は，指示や結託により被強制者に何らかの行為を強制することができるものとする．認証等のサービスの強制にあたって，強制者は被強制者に対して遠隔で指示するものとし，被強制者と直接会うことはないものとする．

強制者は被強制者から入手できる情報を用いて利益を得ることが考えられる．本研究では，強制者の関心を，サービス全体もしくは認証プロセスについて情報を得ることに限定して定義する．

定義 3（耐強制性）

semi-honest な利用者 A と（利用者 A に対する）強制者 Co が結託したことを前提に，利用者 A と honest な認証者 B が認証プロトコル X を使って認証したことを，A が観測可能な View $I=\{I_1, I_2, \cdots, I_n\}$及び取得可能な認証の中間情報$I'=\{I'_1, I'_2, \cdots, I'_l\}$を用いて，強制者 Co が納得できる証拠$E=\{E_1, E_2, \cdots, E_m\}$を得られない性質

この定義において，Semi-honest な利用者 A は，強制者 Co の意志に基づいて認証を行い，認証プロトコルXを実行したことを Co に納得させるための情報（View $I=\{I_1, I_2, \cdots, I_n\}$及び$A$が入手可能な中間情報$I'=\{I'_1, I'_2, \cdots, I'_l\}$）を収集できる必要がある．利用者 A の能力としては，定義 1 における利用者と同様と考えられる．

強制者 Co は直接認証セッションに参加することができないものとし，認証プロトコルの View を自身で観測することを必須の要件としない．その一方で，強制者 Co は利用者 A の提供する情報 I と I'が，自身を納得させられるか否かを判定する，すなわち定義 1 における第三者 C の証拠 E に関連付ける能力を有する．この計算にあたって，強制者 Co は確率的多項式時間で計算する能力が必要になるものと思われる．

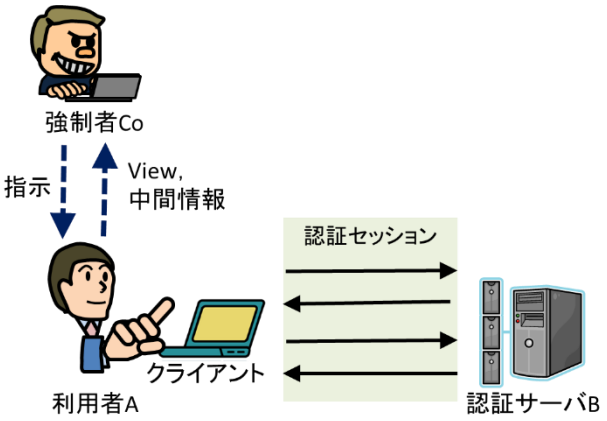

図 3　強制を伴う認証の実行

Figure 3　Execution of authentication process with coercion

4.1 無証拠性との関連

定義 3 においては，定義 1 に含まれていた，View を観測する第三者 C が存在しない．これは，View に関する情報の収集は利用者 A が直接行うことを想定しているためである．無証拠性の議論では，利用者 A と第三者 C の関係は特に明示されていなかったが，耐強制性の議論においては，強制者 Co は利用者 A に対して，認証された後のサービス参加を強制させるなど，直接の関係性を有している．

強制者 Co は利用者 A が生成もしくは入手可能な情報を入手することができるが，その範囲は，定義 1 における第三者 C と比較して，広範になることが考えられる．すなわち，I に加えて，I'として，利用者 A が受信，生成する乱数や検証に用いるハッシュ値などの情報を平文で入手できることが想定される．例えば，パスワード認証において，利用者が自身の手操作で ID・パスワードを入力する場合，I'にこれらの情報が含まれるので，強制者は特別な計算を行うことなしに証拠 E を得られることとなり，耐強制性は満たされないことになる．

以上のことから，耐強制性は無証拠性との共通部分を多く有する一方，強制者が利用者の中間情報を得られるなど，異なる部分もあることが分かる．

5. まとめ

本論文では，認証プロトコルに関する，第三者による過度な情報収集とその利用というプライバシ上のリスクについて指摘し，その要因を記述する認証プロトコルの性質として，無証拠性と耐強制性を提案して，その特徴に関する考察を行った．

今後の課題としては，既存の認証プロトコルにおける無証拠性及び耐強制性についての分析とこれらの性質を満たす認証プロトコルの設計が考えられる．

Vol.2020-DPS-182 No.42
Vol.2020-CSEC-88 No.42
2020/3/13

謝辞

本研究は，日本学術振興会科学研究費補助金（基盤研究(C)）（課題番号：18K11297，研究課題名「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」）の支援を受けて行われた．

本研究の遂行にあたり，助言をいただいた九州大学大学院　櫻井幸一教授，長崎県立大学　穴田啓晃准教授に感謝します．

参考文献

[1] FIDO Alliance, “FIDO Alliance”, 更新 2019-12-10, https://fidoalliance.org/, （参照 2019-12-11）
[2] 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 2019-12-08)
[3] 瀬戸洋一編著, 慎祥揆, 飛田博章, 難波康晴,湯田晋也 著, 「技術者のための IoT の技術と応用 -「モノ」のインターネットのすべて-」, 日本工業出版 （2016 年）
[4] 林卓也, “準同型暗号を用いた秘密計算とその応用”, システム/制御/情報, Vol. 63, No. 2, pp.64-70, （2019）
[5] 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).
[6] 岡本龍明, 「現代暗号の誕生と発展　ポスト量子暗号・仮想通貨・新しい暗号」, 近代科学社（2019 年）
[7] Yoshifumi Ueshige, Kouichi Sakurai, “Towards "Receipt-freeness" in Remote Biometric Authentication”, Fifth International Conference on Emerging Security Technologies (EST2014), pp. 8-12, (2014)
[8] 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 2015，3D2-3, pp.1050-1057，(2015).
[9] 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)