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

上繁 義史† 櫻井 幸一‡

†長崎大学
852-8521 長崎県長崎市文教町 1-14
yueshige@nagasaki-u.ac.jp

‡九州大学
819-0395 福岡県福岡市西区元岡 744
sakurai@csce.kyushu-u.ac.jp

あらまし 近年，生体認証プロトコルの研究が活発に行われているが，これらの研究においてはプロトコル上通信される認証情報からプライバシ情報が漏えいしないことを安全性の根拠としている．一方，著者らは，認証サーバ上の認証情報などから，変換されたものを含めたプライバシ情報の過剰収集のリスクを指摘し，生体認証プロトコルにおいて無証拠性の概念を導入した．本研究では，これを進めて，生体認証プロトコルの耐強制性について検討を行った．本論文では，耐強制性の定義及び無証拠性との関係性，既存プロトコルの耐強制性に関する検討結果について報告する．

Receipt-freeness and coercion-resistance in biometric authentication protocols

Yoshifumi Ueshige† Kouichi Sakurai‡

†Nagasaki University.
1-14 Bunkyo-machi, Nagasaki, 852-8521, JAPAN
yueshige@nagasaki-u.ac.jp
‡Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN
sakurai@csce.kyushu-u.ac.jp

Abstract Recently, biometric authentication protocols are developed. Security of these protocols originates in compromising no privacy information in the authentication processes. On the other hand, the authors pointed out the risk of excess collection of privacy information caused by remaining biometric authentication data on authentication servers. In relation to this risk, the authors introduced receipt-freeness of biometric authentication protocols. In this research, the authors develop the above research by investigating coercion-resistance on biometric authentication protocols. This paper

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：25330155）の支援を受けて行われた．

describes definition of coercion-resistance, relevance to receipt-freeness, and analysis of coercion-resistance in some related protocols.

1 はじめに

生体認証は様々な場面で本人認証の手段として活用されている．例えば，金融機関の ATM，e Passport を用いた入出国管理，途上国での健康調査における個人識別[1]が知られている．その多くはクローズな環境での利用となっている．

その一方で，インターネットなどのオープンなネットワーク環境への応用が進んでいる．Identity Management （IdM）の分野で SSO の機能を実現するために SAML や OpenID といった仕様が開発されているが，これに生体認証を利用できるようにするために，ISO における国際標準化や開発[2]が進んできている．

生体認証において，指紋や虹彩，静脈パターンから取得された生体情報から認証情報を生成するため，特徴情報やテンプレートなど，プライバシ情報の保護が問題となっている．この観点に基づいて様々な技術が研究されている．オープンなネットワークでの認証への応用において，テンプレート保護技術を伴う手法[3]やゼロ知識証明を応用した手法[4]，PKI のフレームワークを用いる手法[5]などが提案されている．

1.1 本研究の位置づけ

上述のテンプレート保護技術を含む認証技術において，生体情報（変換された情報を含む）についてのプライバシ情報が漏えいしないことを根拠として安全性を議論している．

これらの技術を実装するにあたっては，

- 不適切な設定による情報の蓄積や公開
- 第三者による過度な情報収集

によって新たなプライバシ上の問題が考えられることから，著者らは文献[6]，[7]，[8]にてこの問題を指摘した．併せて生体認証プロトコルの認証サーバにおけるプライバシ情報収集の注目し，その可能性を議論するために，無証拠性（receipt-freeness）を定義した．この定義に基づいて，既提案の生体認証プロトコルが無証拠性の性質を有するかについて分析を行った．

本研究はこの視点を更に進めるものである．無証拠性と並んで電子投票の分野で重要な性質として耐強制性（coercion-resistance）がある．これは，第三者が特定候補者に投票するように投票者を脅迫しても，投票者はこの第三者に対して，自身の投票内容を証明することができない性質[9]である．これを生体認証プロトコルに応用ことにより，特にオープンなネットワーク上の認証において，プライバシ上の影響を明らかにできるものと期待できる．このことは今後の生体認証プロトコルを検討する上で，プライバシ要件を考える基礎となると思われる．

そこで，本研究は次のことを目的とする．まず本研究が対象とする無証拠性を定義し，それに基づいて耐強制性を定義する．続いて，これらの定義に基づいて，既提案の生体認証プロトコル[11]，[12]が耐強制性及び無証拠性の性質を有するかについて検証を行う．

1.2 本論文の構成

本論文は以下のように構成される．2 で生体認証プロトコルにおける耐強制性及び無証拠性の定義などについて議論する．3 で既提案の生体認証プロトコル[11]，[12]について耐強制性及び無証拠性の評価を行い，4 でまとめとする．

2 生体認証プロトコルにおける無証拠性及び耐強制性

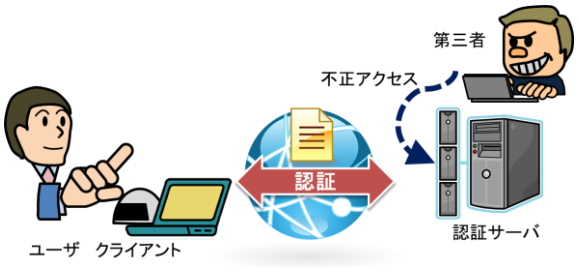
本章では，電子投票における無証拠性と耐強制性の定義より類推して，生体認証プロトコルにおけるこれらの性質を定義する．続いて無証拠性及び耐強制性の関係について議論する．

2.1　無証拠性の再検討

著者らは文献[6]，[7]，[8]において，無証拠性の定義を「サービス提供中・停止中の区別を問わず，蓄積されたログ等のデータから，登録者と結びつけられる生体情報，もしくは生体情報から一意に計算された情報（暗号やハッシュ値など）を得られないこと」と定義した．

この定義は，図 1 (a) に示すように，サーバ上における第三者（攻撃者）による不正な情報収集を想定したものである．第三者がサーバを不正に操作するためには，操作可能な権限を持ったユーザアカウントを乗っ取るなどの攻撃が成功することが前提条件となる．その結果，第三者は認証プロセスにおける通信データや処理中のデータなど，多種のプライバシ情報を収集できることを想定している．

本研究では，図 1 (b) に示すように，（セキュアではない）オープンネットワーク上のクライアントと認証サーバ間の通信を盗聴により収集が可能な第三者を想定し，盗聴における無証



(a) 認証サーバのログから収集できる場合

(b) 認証時の通信を盗聴できる場合

図 1　本研究が想定する生体認証プロトコルにおける第三者による証拠（プライバシ情報など）の収集

拠性として以下のように定義する．

「ネットワーク上で観測可能な認証に関する情報を収集しても，登録者と結びつけられる生体情報，もしくは生体情報から一意に計算された情報（暗号やハッシュ値など）を得られないこと．」

2.2　耐強制性の定義

耐強制性に関連する研究としては Gupta と Gao の皮膚のコンダクタンスの変化による暗号鍵生成方式[10]がある．これは鍵生成のパスワードを音声により入力し，皮膚のコンダクタンスが平常時と判定される場合に正しい暗号鍵を生成し，脅迫などの脅威が発生したと判断される場合にこれを検知して，正しくない暗号鍵を生成する手法である．この手法においては，強制された状況を平常時からの生物的な変化により検出して，耐強制性を確保している．

一方，電子投票の分野において，耐強制性がプロトコルの備えるべき要件と考えられており，複数の定義が知られている[9]．電子投票における無証拠性の特徴は，強制する第三者 (coercer) が，投票者が投票を行っている間に，誰に投票するか指示するなど，投票者に影響を与える点にある．

本研究では，無証拠性の議論と関連して，生体認証プロトコルの性質を検討する観点から，電子投票のアプローチに基づいて耐強制性を定義する．本研究では，第三者を図 1 (b) の能力をもち，遠隔によりユーザに対して強制する者と仮定し，以下のように定義する．

「認証プロセス中に遠隔で強制（指示）する第三者に対して，ユーザが証拠（自身と結びつけられる生体情報，もしくは生体情報から一意に計算された情報（暗号やハッシュ値など））を提示できないこと．」

2.3　無証拠性と耐強制性の関係

本研究における無証拠性と無証拠性の定義において，異なる点は第三者の能力である．2.1 では「クライアントと認証サーバ間の通信内容

を収集可能」という能力を仮定している．2.2 においては 2.1 の能力に加えて，「遠隔により認証プロセス中のユーザに影響を与える」ことを挙げている．両方の定義において，ユーザが証拠（自身と結びつけられる生体情報，もしくは生体情報から一意に計算された情報（暗号やハッシュ値など））を得ることができない点が共通している．このことから，集合として考えると，無証拠性⊃耐強制性となっており，定義の強さとしては，耐強制性が無証拠性よりも強いことが分かる．

また無証拠性及び耐強制性を有するプロトコルにおいては否認可能性（deniability）の性質を有することが考えられる．理由としては，上述の定義により，提示した生体情報もしくはそれを変換した情報が得られないことから，「自分の ID を使って，他者が生体認証を行った」との主張が可能となるためである．

3　無証拠性及び耐強制性の評価

本研究では，生体認証プロトコルとして，図 2 に示すフレームワークをもつ手法[11]，[12]について無証拠性及び耐強制性の性質を評価する．本稿で採り上げる手法においては，認証サーバが複数あることが仮定されている．

本稿で用いる記号の定義を表 1 に示す．

3.1　Khan らの方法

この手法[11]は Khan と Kumari が提案したもので，ユーザの匿名性を確保することができる．本手法は以下の 4 つのステップから構成される．

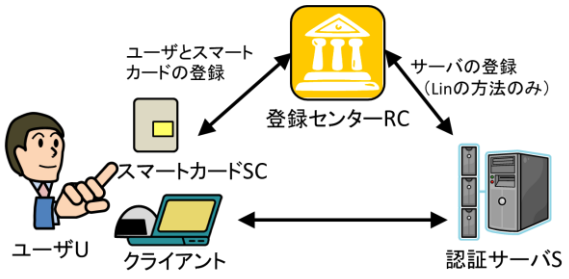


図 2　本研究で仮定する生体認証のフレームワーク

表 1　記号の定義

記 号	定　義
U_i	ユーザ
S_i	認証サーバ
RC	登録センター
ID_i	ユーザ U_i の ID
PW_i	ユーザ U_i のパスワード
BIO_i	ユーザ U_i の生体情報（テンプレート，特徴情報など）
SC_i	ユーザ U_i のスマートカード
$h(\cdot)$	ハッシュ関数
$\oplus$	ビット単位での XOR 演算
$\|$	結合演算

(1)　登録フェーズ：ユーザ情報を登録し，ユーザが所有するスマートカードに必要な情報を書き込むフェーズである．この通信はセキュアな通信路を用いている．

(2)　ログインフェーズ：ユーザが認証サーバにログインするフェーズである．このフェーズはオープンネットワークにて行われる．

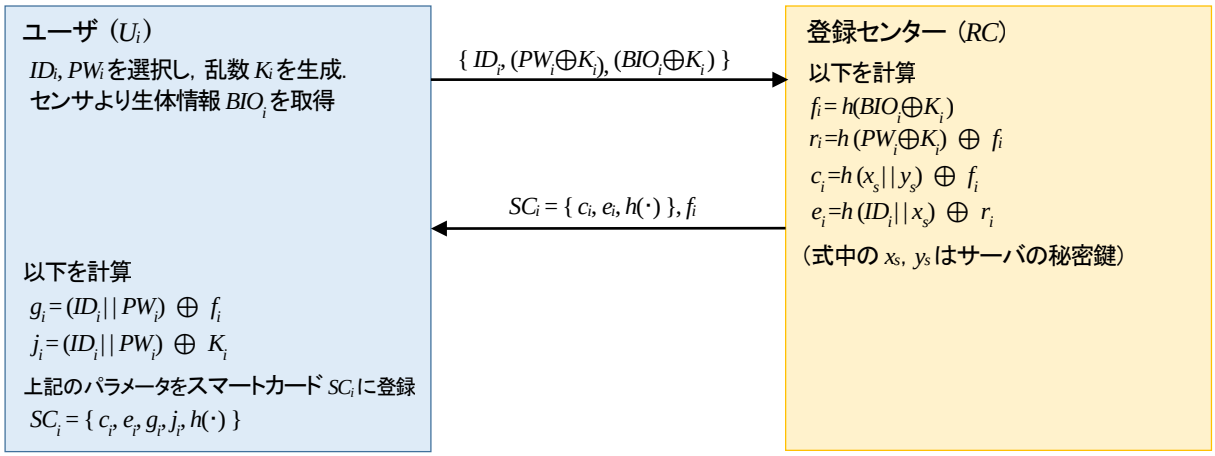
(3)　認証フェーズ：ログイン成功後に続いて行われるもので，ユーザ（クライアント）とサーバの相互認証を行うフェーズである．

(4)　パスワード更新フェーズ：パスワードから計算される，スマートカード上のパラメータを更新するフェーズである．この処理はクライアント上で行われる．

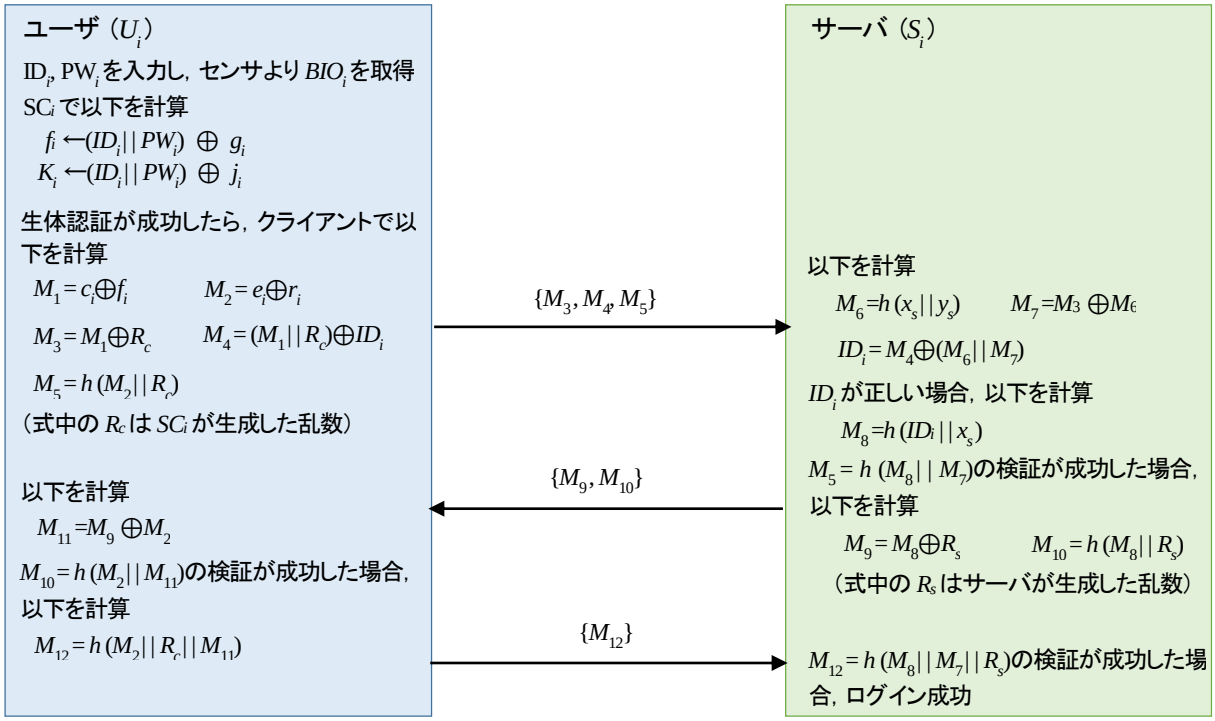
Khan らのプロトコルのうち，登録フェーズ，ログイン及び認証フェーズについて，詳細を図 3 に示す．

図 3 (a)は登録センターRC とスマートカード SC に保存されている情報の種別を明示するために示している．上述のようにセキュアな通信路を用いて行われており，盗聴が困難と考えられることから，評価の対象とはしない．

図 3 (b)がログイン及び認証フェーズに相当する．この通信はセキュアではないオープンネ



(a) 登録フェーズ



(b) ログイン及び認証フェーズ

図 3　Khan らのプロトコル

ットワーク上で行われることが仮定されている．このような通信路においては，様々な手法で通信データを盗聴することが可能と考えられるため，このフェーズを分析の対象とする．

このプロトコルにおいて，生体情報（もしくは変換された情報）を含みスマートカード SC_i に保存されている情報は c_i，e_i，f_i である．生体認証の処理はクライアント内で実行され，生体認証の成功後にサーバへのログインを行う．このプロセスにおいてクライアント内で計算されるパラメータのうち，生体情報（もしくは変換された情報）を含むかを検証する．M_1 及び M_2 において，以下の計算により，生体情報を含まないことが分かる．

$$M_1 = c_i \oplus f_i = \{h(x_s \parallel y_s) \oplus f_i\} \oplus f_i = h(x_s \parallel y_s)$$

$$M_2 = e_i \oplus r_i = \{h(ID_i \parallel x_s) \oplus r_i\} \oplus r_i = h(ID_i \parallel x_s)$$

また，M_3～M_{12} は M_1，M_2，ID_i，x_s，y_s，R_s，R_c を含み，生体情報 BIO_i を含まない．以上のことか

ら，2.1 の定義に照らして，本手法のログイン及び認証フェーズにおいて，無証拠性が成り立つ．

次に耐強制性について検討する．ユーザ U_i の認証プロセスにおいて，第三者が遠隔から U_i に指示を出す場合であっても，上述のように BIO_i を含む通信情報が観測されないので，U_i が第三者に対して生体情報（もしくは変換された情報）を提示することはできない．したがって，耐強制性の性質を有することがわかる．

3.2 Lin らの方法

この手法[12]は Lin，Wen，Du より提案されたプロコトルで，マルチサーバの環境において，ユーザの匿名性を確保できる鍵交換の手法として提案された．このプロトコルにおいて，以下の 5 つのステップから構成される．

(1) 初期設定フェーズ：これは登録サーバ RC 上で行われる．楕円曲線及びジェネレータを選定すると共に，各サーバの ID にあたる SID_j 及び RC のマスターパスワード x より計算された$r_j = h(SID_j \| x)$をプリシェアードキーとして各サーバに送付する．

(2) 登録フェーズ：Khan らの方法と同様に，ユーザ U_i の登録と U_i がもつスマートカード SC_i への登録情報の保存がセキュアな通信路を通じて行われる．

(3) ログインフェーズ：クライアント上で生体認証成功後にサーバにログインするフェーズである．このフェーズはセキュアではないオープンネットワーク上で行われる．

(4) 認証フェーズ：ログインフェーズ後に，ユーザ（クライアント）と認証サーバ間の相互認証を行うフェーズである．

(5) パスワード更新フェーズ：パスワードから計算されるスマートカード上のパラメータをクライアント上で変更するフェーズである．

上のフェーズの内，初期設定フェーズ，登録フェーズ，ログイン及び認証フェーズのプロトコルを図 4 に示す．

初期設定フェーズ（図 4(a)）は直接認証と関連しないため，分析の対象としない．登録フェーズ（図 4 (b)）について，3.1 と同様の理由により分析対象に含めない．ログイン及び認証フェーズ（図 4 (c)）は 3.1 と同様の条件下で実行されるため，分析の対象とする．

まず無証拠性について検討する．このプロトコルにおいて，生体情報 BIO_i を含む項は d_j, g_i, j_i, k_i, l_i である．クライアントでの生体認証成功後に，クライアントから認証サーバに送信される情報に g_i が含まれる．続いて認証サーバからクライアントに向けて k_i が，更にその後にクライアントから認証サーバに l_i が送信される．

これらの情報の内，g_i の一部$E_{b_{ij}}[h(PW_i \| BIO_i)]$において，パスワード PW_i と生体情報 BIO_i を連結してハッシュを求め，これを鍵 b_{ij} で暗号化している．第三者がこの値を用いて BIO_i を導出することは極めて困難と考えられる．一方．式中のいずれのパラメータもセッション単位で変化する数値を含んでいないことから，パスワードや生体情報を更新しない限りにおいて，セッション間で一定と考えられる．そこで，$E_{b_{ij}}[h(PW_i \| BIO_i)]$ は生体情報から一意に計算された情報と考えることができる．

k_i の一部 $E_{b_{ij}}[j_i] = E_{b_{ij}}[h(SID_j \oplus h(PW_i \| BIO_i))]$についても上と同様に議論することができ，セッション間において一定と考えられるため，生体情報から一意に計算された情報と考えられる．

l_{ij} については，セッションキーSK_{ij}を含んでおり，セッション毎に変化すると考えられるため，一意性はない．

以上のことから，本プロトコルにおいて，g_i 及び k_i の一部により無証拠性を満たさないことが分かる．

次に耐強制性について考察する．第三者が遠隔から U_i に指示を出す場合においても，上述のように BIO_i から一意に変換した情報が含まれるため，U_i は第三者に対してこの情報を提示す

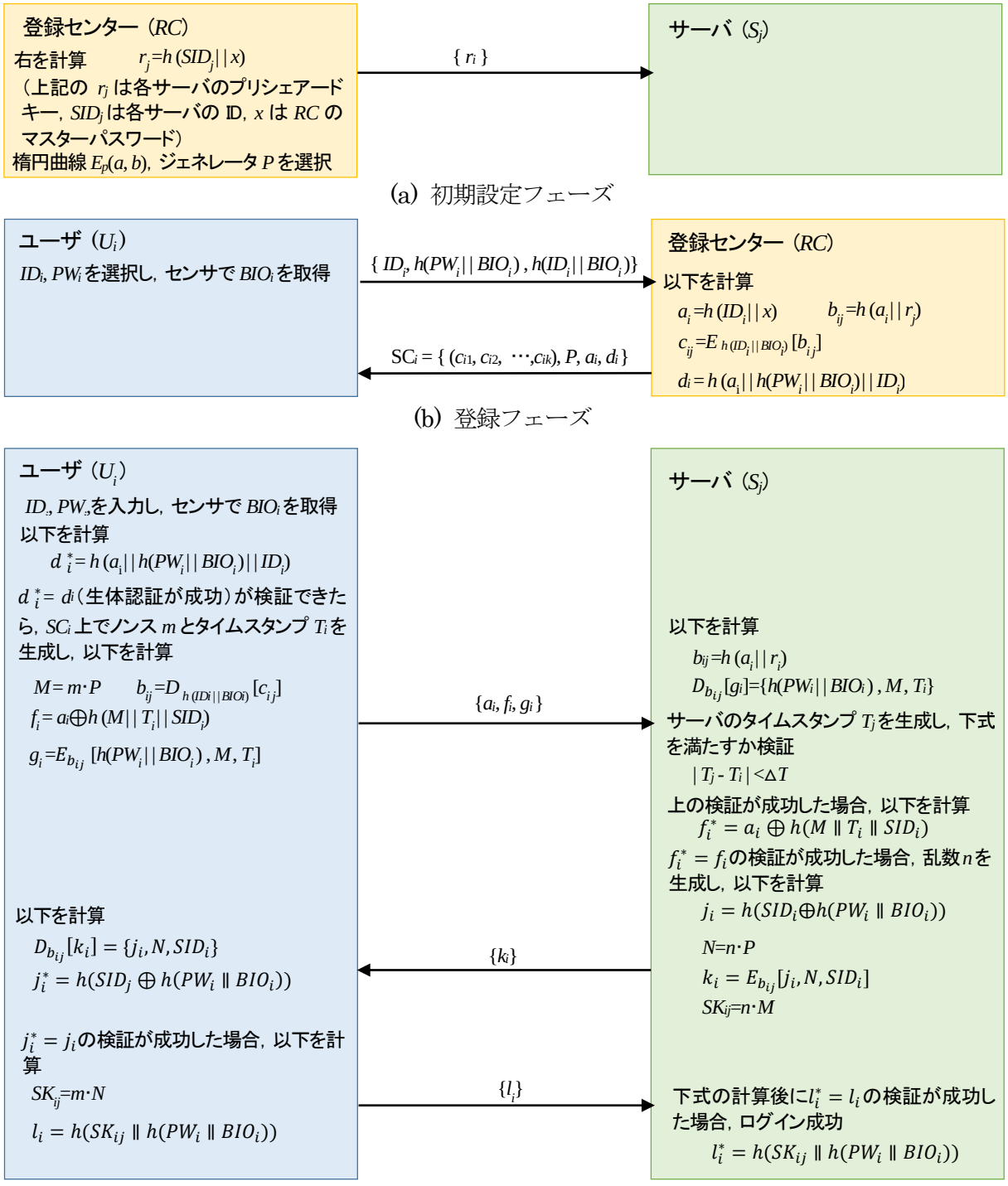


図 4　Lin らのプロトコル

ることが可能となる．したがって，耐強制性の性質を有さないがわかる．

4　まとめ

本研究では，生体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検討することを目的として，これらの性質について定義を行い，2 つの既提案のプロトコルに対して，考察を行った．その結果，Khan らの方法においては，無証拠性及び耐強制性を満たすことが分かっ

た．また，Lin らの方法においてはこれらの性質を満たさないことが分かった．

今後の課題として，他の生体認証プロトコルにおいて同様の検証を行うことや，本研究の対象に含めなかった，生物的反応を考慮した耐強制性について検討することなどが挙げられる．

参考文献

[1] 総合地球環境学研究所，長崎大学，日立製作所：総合地球環境学研究所と長崎大学が、日立の「指静脈認証」を活用しラオス人民民主共和国で肝吸虫症などの感染症撲滅に向けた健康調査を実施，長崎大学，http://www.nagasaki-ac.jp/ja/about/info/news/news1141.html，(2012)

[2] 日本自動認識システム協会：平成 24 年度 IdM における共通本人認証基盤の開発研究報告書，バイオメトリクスセキュリティコンソーシアム，http://www.bsc-japan.com/pdf/20130415/20130415-idm.pdf，(2013)

[3] N. K. Ratha, J. H. Connell, R. M. Bolle: Enhancing security and privacy in biometrics-based authentication system, IBM System Journal, Vol.40, No.3, pp. 614-634, (2001) など

[4] 高橋健太，比良田真史，三村昌弘，手塚悟：セキュアなリモート生体認証プロトコルの提案，情報処理学会論文誌，Vol. 49, No. 9, pp. 3010-3027，（2008）など

[5] Koji Okada, Tatsuro Ikeda, Hidehisa Takamizawa, Toshiaki Saisho: Extensible Personal Authentication Framework using Biometrics and PKI, IWAP2004, (2004) など

[6] 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，第 31 回暗号と情報セキュリティシンポジウム（SCIS2014），3E4-3，（2014）

[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，AS-3-12，（2014）

[8] Y. Ueshige, K. Sakurai: Towards “Receipt-freeness” in Remote Biometric Authentication, 2014 International Conference on Emerging Security Technologies (EST2014), pp. 8-12,(2014)

[9] James Heather, Steve Schneider: A formal framework for modelling coercion resistance and receipt freeness, FM 2012: Formal Methods, LNCS Vol. 7436, pp 217-231, (2012)

[10] P. Gupta, D. Gao: Fighting Coercion Attacks in Key Generation using Skin Conductance, USENIX Security Symposium 2010, pp. 469–484, (2010)

[11] Muhammad Khurram Khan, Saru Kumari: An Improved Biometrics-Based Remote User Authentication Scheme with User Anonymity, BioMed Research International, Vol. 2013, Article ID 491289, 9 pages, http://dx.doi.org/10.1155/2013/491289, (2013)

[12] Hao Lin; Fengtong Wen; Chunxia Du: An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics, Wireless Personal Communications, http://link.springer.com/journal/11277, (2015)