情報処理学会論文誌　Vol. 49　No. 9　3016–3027 (Sep. 2008)

セキュアなリモート生体認証プロトコルの提案

高橋 健太[†1]　比良田 真史[†1]
三村 昌弘[†2]　手塚 悟[†1]

銀行 ATM や入退管理などへ生体認証技術の導入が進み，今後はインターネット決済などにおけるリモート認証への適用が期待される．しかし指紋や静脈などの生体情報は，プライバシ情報であると同時に一生涯変更できない情報であり，厳密な保護が要求される．本稿ではリモート生体認証における脅威を分析してセキュリティ要件を明確化するとともに，これを満たすリモート生体認証プロトコルを提案する．提案プロトコルは，キャンセラブルバイオメトリクスとゼロ知識証明を組み合わせることで，生体情報の漏洩やなりすましといった脅威に対抗する．提案プロトコルにより，ネットワークを介したセキュアな生体認証システムが実現可能となる．

A Protocol for Secure Remote Authentication Using Biometrics

Kenta Takahashi,[†1] Shinji Hirata,[†1]
Masahiro Mimura[†2] and Satoru Tezuka[†1]

Due to the high security and convenience, biometric authentication is used for access control, ATM and many kinds of identity verification. However, biometric data such as fingerprint and vein pattern is permanent feature which cannot be changed like passwords, and so must be protected securely. In this paper we analyze the threats to remote biometric authentication systems such as impersonation and compromise of biometric data, and specify security requirements. Then we propose a novel protocol scheme based on "cancelable biometrics" and zero knowledge interactive proof. The proposed protocol satisfies all the specified requirements and enables secure online biometric authentication.

†1 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†2 株式会社日立製作所セキュリティ・トレーサビリティ事業部
Security & Smart ID Solutions Devision, Hitachi, Ltd.

1. はじめに

近年，静脈や指紋などの生体情報に基づいて個人を認証する生体認証技術の導入が，銀行 ATM や保護区域への入退管理などを中心に進んでいる．今後はインターネット決済分野など，オープンネットワークを介した本人確認への普及が期待される．生体認証システムは，あらかじめシステムに登録してある正規利用者の生体情報（テンプレート）と，認証時に取得した利用者の生体情報を照合することで，本人（OK）/他人（NG）を判定する．しかし生体情報は個人のプライバシ情報であるうえに，漏洩してもパスワードのように任意に変更できないという問題があり，厳密な保護が要求される．

ネットワークを介してサーバがクライアント利用者の本人確認を行う生体認証システムのモデルとしては，(1) クライアント側で生体認証を実行し，結果（OK/NG）をサーバに通知するモデル（以下，ローカル生体認証モデル）と，(2) サーバ側で生体認証を実行するモデル（以下，リモート生体認証モデル）がある．

ローカル生体認証モデルでは，一般にテンプレートをクライアント内に保持するか，利用者が所持する媒体（カードなど）に保持する．しかしサーバ側でテンプレートを保持する場合と比較して運用管理による漏洩対策が困難であり，クライアントへの攻撃やカードの盗難による漏洩リスクが高い．これに対し，IC カードなどの耐タンパ性を持つ装置にテンプレートを格納し，カード内で照合したうえで，生体情報が一致した場合にカード内の秘密鍵を活性化し，サーバとの間で PKI 認証を行う方法（IC カード内照合方式）が提案されている[1)]．しかし生体認証機能を持つ特殊な IC カードが利用者の数だけ必要となるため，システム導入コストが高くなるという問題がある．またサーバ側から見ると単なる PKI 認証と区別がつかず，クライアント側で正しく生体認証が行われていることを確認することができない．なおクライアント側の生体認証結果の正当性をサーバが判断可能とするために，生体認証機器のセキュリティ強度情報などを証明書として発行し，認証時にサーバが証明書を用いて機器認証を行うスキームが提案されている[2)]．しかし機器内で秘密鍵とテンプレートを安全に保持するためには耐タンパ性が必要になるうえ，そのセキュリティ強度を客観的に評価・認証するスキームが必要となり，開発・導入コストの増大や評価・認証制度の確立など，多くの課題が残されている．

一方リモート生体認証モデルではテンプレートをサーバで保持するため，プライバシの観点から利用者の心理的抵抗が大きいという問題がある．またサーバ管理者（サーバ内のテンプレートにアクセスする権限を持つユーザ）のミスや不正によって情報漏洩が発生した場

合，全利用者のテンプレートが危険に曝される可能性がある．テンプレートを暗号化して保護する対策も考えられるが，照合時に復号する必要があるため，そのタイミングを狙った高度な攻撃や，サーバ管理者による内部不正に対して，十分に安全であるとはいえない．

リモート生体認証モデルにおけるこれらの問題に対し，生体情報に変換を施して元の情報を秘匿した状態のまま照合するキャンセラブルバイオメトリクス[3]や，生体情報の歪みやノイズを，特殊な量子化と誤り訂正により補正して一意のデータを生成し，これを秘密鍵として暗号技術に基づく認証を行うバイオメトリック暗号[4]，認証時の生体情報がテンプレートに十分近いことを，クライアントがサーバにゼロ知識証明する非対称生体認証[5]といった技術が提案されている．これらを総称してテンプレート保護型生体認証技術と呼ぶことにする．

このうちキャンセラブルバイオメトリクスは，虹彩認証，指紋認証，静脈認証などで従来用いられてきた特徴量や照合アルゴリズムを，大きく変更することなく適用可能な方式が提案されており[6)–9)]，このため従来技術の認証精度を保ったまま実現可能であるという特長を持つ．またこれらの方式は簡単なビット演算や，画像の高速フーリエ変換といった処理で構成可能であり，計算量が比較的小さいという特長を持つ．このため，バイオメトリック暗号や非対称生体認証と比較して実用的なアプローチといえる．しかしキャンセラブルバイオメトリクスを用いてリモート生体認証システムを構築した場合，変換生体情報が漏洩して攻撃者の手に渡ると，元の生体情報は復元できなくても，本人になりすます攻撃が可能であるという脅威が残されている．

本研究の目的は，リモート生体認証システムにおける脅威を分析して要件を明確化するとともに，それを満たす安全なリモート生体認証プロトコルを実現することにある．

本稿では，2 章でリモート生体認証システムにおける脅威分析を行い，セキュリティ要件を明確化する．次に 3 章でキャンセラブルバイオメトリクスについて述べ，問題点を指摘する．これに対し 4 章では，キャンセラブルバイオメトリクスとゼロ知識証明を組み合わせたリモート生体認証プロトコルを提案する．5 章において提案プロトコルのセキュリティを評価し，すべての要件を満たすことを示すとともに，バイオメトリック暗号や非対称生体認証といった他のプロトコルとの比較を行う．6 章では，提案方式の拡張について考察する．

2. リモート生体認証の脅威分析と要件検討

本章では，まず本稿が検討対象とするリモート生体認証のシステムモデルを定義し，前提条件を設定して脅威分析を行う．そしてその結果に基づき，リモート生体認証プロトコルが満たすべき要件を明確化する．

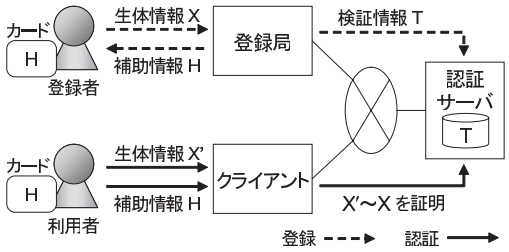

図 1　リモート生体認証モデル
Fig. 1　System model of remote biometric authentication.

2.1　リモート生体認証モデル

リモート生体認証システムは，以下の 4 つのエンティティから構成されるものとする（**図 1**）．

・登録局：登録者の生体情報 X を取得してその登録情報 T を作成し，認証サーバに対して発行する．本稿では「生体情報」の意味として，センサが読み取った画像などの生データと，そこから抽出した特徴量の，両方を含むものとする．従来の生体認証システムでは登録情報 T は X そのものを含み，テンプレート（登録生体情報）と呼ばれるのに対し，テンプレート保護型生体認証技術を用いる場合，T は X そのものを含まない．そこでテンプレートを含むより広い概念として T を以下，検証情報と呼ぶことにする．テンプレート保護型生体認証技術を用いる場合，登録局はさらに補助情報 H を作成し，カードなどの媒体に記録して登録者に発行する．H には生体情報を秘匿するための乱数情報などが含まれる．一般に T，H が揃うと X が復元または推定可能となるため，認証サーバが保持する T と，登録者が保持する H が，同時に漏洩することがないよう管理する必要がある（2.2 節参照）．登録処理が終了したら X を消去する．

・クライアント：認証時に利用者のカードから補助情報 H を読み込み，また生体情報 X' を取得して，認証サーバに対し X' が X に十分近い（$X' \sim X$ と表す）ことを示す．このとき補助情報 H を用いる．認証処理が終了したらメモリから H，X' を消去する．

・認証サーバ：認証時に $X' \sim X$ であることを T を用いて検証する．検証に成功すれば，クライアントの利用者が登録者本人であると判定し，認証成功とする．$X' \sim X$ を判定するための尺度（距離）は，生体認証の種別（指紋，静脈，顔など）や生体情報の表現形式（画像，特徴量ベクトル，特徴点集合など）などによって異なる．

・カード（媒体）：登録時に登録局が作成した補助情報 H を格納し，利用者に発行される．カード自体は単なる媒体であり，生体認証や暗号などの計算能力は持たない．

2.2 前提条件

上述のリモート生体認証モデルにおいて，以下の前提条件を仮定する．

(A1) 登録局は安全に運用され，信頼できるとする．

(A2) クライアントの利用環境は必ずしも安全に管理されておらず，攻撃者が不正に利用する可能性があるとする．たとえば社外に持ち出すノート PC を使って社内ネットワークにアクセスするシステムでは，ノート PC が盗用され不正利用される可能性がある．またネットバンキングなどにおける利用者認証では，不正な利用者が自分の PC を利用して他人になりすます攻撃も考えられる．

(A3) クライアントのプログラムやデータを記録，実行する，CPU やメモリ，ハードディスクなどは，攻撃を検知して内部情報をゼロクリアするといった耐タンパ性（tamper resistant）を持たないとする．このため，攻撃者がクライアントを不正利用し，データやプログラムを実行時に盗聴，改ざんする攻撃を考慮する必要がある．

(A4) クライアントは，攻撃を受けたときにその証跡を残すタンパ証拠性（tamper evident [10]）を持ち，ハードウェアが不正に改造されたり，プログラムが改ざんされたりしている場合，利用者が認証時にそれを確認できるものとする．したがって，不正に改造，改ざんされたクライアントを正規の利用者が知らずに使って認証を行い，X' や H が攻撃者に送信されたり，不正に記録され後で回収されたりするといったリスクは，十分低いものとする．タンパ証拠性は，物理的な攻撃（装置をこじ開けるなど）の証拠を残すシールや，ソフトウェアの改ざんを検知する電子署名などによって実現することができ，前述の耐タンパ性と比較して低コストで実現可能である．

(A5) 認証サーバが管理する T と，利用者が管理する H が，両方漏洩して同一攻撃者の手に渡るリスクは十分低いとする．なお，キャンセラブルバイオメトリクスなどのテンプレート保護型生体認証技術は，T や H が漏洩しても，更新することで漏洩情報を無効化することができる（3.1 節参照）．したがってテンプレート保護型生体認証技術を用いることで，この前提条件は，「T と H が一定期間（更新期間）において同時に漏洩するリスクは十分低い」と緩めることができる．また認証サーバ管理者自身が，正規利用者のカードを盗用し（したがって T，H の両方を入手し），不正利用するリスクは低いものとする．

(A6) 認証サーバとクライアントの間の通信は暗号化されており，通信路の盗聴による情報漏洩のリスクは十分低いものとする．

2.3 脅威分析

前節の前提条件のもとで，脅威を分析する．生体認証システムにおける脅威は，生体情報の漏洩（機密性の損失），登録者以外の利用者によるなりすまし（真正性の損失），登録者本人が拒否されること（可用性の損失）がある．

生体情報漏洩の脅威は，たとえば顔写真を盗撮される，指紋センサに付着した指紋を採取されるなど，利用者が気づかない間に採取される脅威（生体スキミング）と，システムから X，X' が漏洩する脅威に分類できる．前者に対する対策には，静脈など読み取られにくく遺留しない生体情報を用いるといった対策が考えられるが，本研究の対象外とする．

なりすましの脅威は，攻撃者が自分もしくは共犯者の生体を入力して認証を試みる攻撃（消極的ななりすまし攻撃）と，システムからの漏洩情報（T，H，X など）を用いて偽造データを作成し，電子的にシステムに入力する攻撃（電子的偽造），漏洩生体情報をもとに物理的に偽造した生体を用いる攻撃（物理的偽造）が考えられる．このうち物理的偽造は，生体情報の漏洩を前提としているため，生体情報漏洩の脅威に含める．

本人拒否の脅威は，利用者が登録者本人であるにもかかわらず，生体情報が一致しない場合に発生する．原因としては，生体の経年変化や環境変動，ノイズの混入などが考えられる．

以下，消極的ななりすまし攻撃の脅威を (T1)，本人拒否による可用性に対する脅威を (T2) と識別する．(T1) の攻撃成功確率，(T2) の発生確率は，それぞれ FAR（False Acceptance Rate），FRR（False Rejection Rate）と呼ばれる．これらをまとめて認証精度と呼ぶ．

以下では (T1)，(T2) 以外の脅威である，システムからの生体情報漏洩と，電子的偽造によるなりすましの脅威を分析する．いずれの脅威も，システムからの情報漏洩を前提としているため，まずリモート生体認証システムにおいて考えうる情報漏洩をリストアップする（**図 2**）．

(1) 登録者のカード盗用などによる H の漏洩．

(2) 認証サーバ管理者の内部不正や外部からの攻撃による T の漏洩．

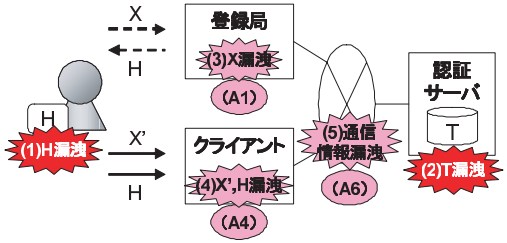

図 2　リモート生体認証における情報漏洩
Fig. 2　Information compromise of the remote biometric system.

表 1　生体情報漏洩と電子的偽造の脅威
Table 1　Threats of biometric compromise and electronic forgery.

攻撃者の条件＼攻撃の目的	生体情報入手	なりすまし（電子的偽造）
認証サーバ管理者	(T3)	—
Tを入手した攻撃者	[(T3)に含まれる]	(T5)
Hを入手した攻撃者	(T4)	(T6)

(3) 登録局管理者・オペレータの内部不正や外部からの攻撃による X の漏洩.
(4) 不正改造されたクライアントを利用者が知らずに使用することによる，X'，H の漏洩.
(5) 通信路の盗聴による通信情報の漏洩.

このうち，前提条件 (A1) より (3) の漏洩リスクは低く，同様に (A4) より (4)，(A6) より (5) のリスクも低い．そこで以下では，(1)，(2)（T，H の漏洩）のみを考慮して，生体情報漏洩と電子的偽造によるなりすましの脅威を分析する．

攻撃者の目的は，生体情報の入手または（電子的偽造による）なりすましである．攻撃者の条件として，認証サーバ管理者，T または H を入手した認証サーバ管理者以外の攻撃者を考慮する．目的と条件の組合せによる脅威の分類を**表 1** に示す．なお，なりすましは，攻撃者が認証サーバを騙して登録者本人であると思わせることなので，認証サーバ管理者自身によるなりすましは脅威として識別しない．

(T3) 認証サーバ管理者が X または X' を入手する．管理者は T を知っているので，T を入手した攻撃者による生体情報入手は，本脅威に含まれる．
(T4) H を入手した攻撃者が X を入手する．
(T5) T を入手した攻撃者が電子的偽造によるなりすましを行う．
(T6) H を入手した攻撃者が電子的偽造によるなりすましを行う．

以上の脅威分析結果を**表 2** にまとめる．次節ではこの脅威分析結果に基づいて，リモート生体認証プロトコルが満たすべきセキュリティ要件を明確化する．

2.4　要　　件

前節で述べた脅威に対抗するためには，リモート生体認証プロトコルが以下の要件を満たす必要がある．

(R1) FAR，FRR が十分に小さいこと．ただし要求される認証精度はアプリケーションにより異なるため，絶対的な基準を示すことが難しい．そこでここでは，リモート生体認証プロトコルを適用することで，従来の照合方式（特徴量抽出・照合アルゴリズム）から認証精度が大きく劣化しないことを要件とする．

表 2　脅威分析結果
Table 2　Identified threats.

脅威の種類	攻撃方法		識別子	要件
生体情報漏洩（機密性の損失）	生体スキミング		—	—
	システム内の生体情報入手（及び物理的偽造）	認証サーバ管理者による不正	(T3)	(R2)
		Hを利用	(T4)	(R3)
なりすまし（真正性の損失）	電子的偽造	Tを利用	(T5)	(R2)(R4)
		Hを利用	(T6)	(R3)(R4)
	消極的な攻撃（攻撃者の生体を入力）		(T1)	(R1)
本人拒否（可用性の損失）	登録者本人の生体が一致しない		(T2)	

(R2) 認証サーバが T やクライアントとの通信データから X または X'（$\sim X$）を復元できないこと．
(R3) クライアントが H や認証サーバとの通信データから X または X'（$\sim X$）を復元できないこと．
(R4) 認証時にクライアントが $X' \sim X$ なる X' を知っていることを，（補助的に H を用いて）認証サーバに証明できること．具体的には以下の要件を満たすこと．
　(完全性) クライアントが $X' \sim X$ なる X'（および H）を知っているなら，認証サーバは十分高い確率でその主張を受理すること．
　(健全性) クライアントが $X' \sim X$ なる X' を知らないなら，認証サーバがこれを受理する確率が十分低いこと．

各要件が前節のどの脅威に対応するかを，表 2 に示す．たとえば T から $X' \sim X$ なる X' を復元することができず (R2)，そのような X' を知らなくては認証に成功できない (R4) ならば，T のみを用いて認証に成功することはできない（(T5) に対抗できる）．

以下，これらの要件をすべて満たす生体認証プロトコルを，キャンセラブルバイオメトリクスとゼロ知識証明プロトコルを用いて構築する．

3.　キャンセラブルバイオメトリクス

本章ではキャンセラブルバイオメトリクスの概要を述べ，これをナイーブに用いてリモート生体認証プロトコルを構築した場合の問題点を指摘する．

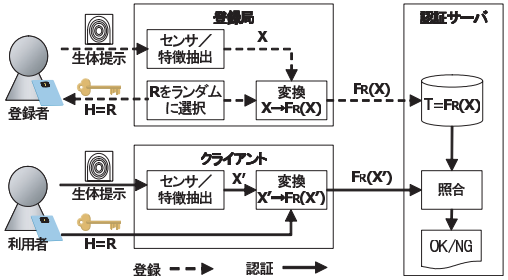

図 3　キャンセラブルバイオメトリクス
Fig. 3　Cancelable biometrics.

3.1 概　　要

キャンセラブルバイオメトリクスは，2001 年に Ratha らによって提案された，セキュリティ・プライバシ強化型生体認証の枠組みである．生体情報に変換（一種の暗号化）を施して元の情報を秘匿し，元に戻すことなく照合する．変換を決定するパラメータ（暗号鍵に相当）を，利用者またはクライアントが管理し，認証サーバに対して秘密にすることで，サーバ管理者に対して生体情報を秘匿したまま認証を受けることができる．キャンセラブルバイオメトリクスを用いたリモート生体認証プロトコルを，**図 3** を用いて説明する．

任意の 2 つの生体情報間の距離を保存する変換関数 $F_R : \mathbf{X} \to \mathbf{X}$（$\mathbf{X}$ は生体情報の空間）を考え，その集合を $\mathbf{F} = \{F_R\}$ とする．R は変換関数 F_R を決定するパラメータとする．

登録時，まず登録局は登録者の生体情報 X を取得する．次に変換パラメータ R をランダムに決定し，関数 $F_R \in \mathbf{F}$ により X を変換する．変換した $F_R(X)$ を検証情報 T として認証サーバに発行する．また R を補助情報 H としてカードなどに格納し，登録者に対して発行する．

認証時，クライアントは利用者の生体情報 X' と，利用者のカードに格納された H（$= R$）を読み取る．次に X' を関数 F_R で変換し，$F_R(X')$ を認証サーバに送信する．認証サーバは $F_R(X)$，$F_R(X')$ 間の距離（X，X' 間の距離に等しい）を計算し，X' が X に十分近いか否かを判定する．

仮に T，H のいずれかが漏洩した場合，R を再度ランダムに生成して T（$= F_R(X)$），H（$= R$）を再発行し，古い T，H を破棄する．これによって，T と H を入手して X を復元する攻撃を困難にすることができる（前提条件 (A5) 参照）．

3.2 要件の評価と問題点

キャンセラブルバイオメトリクスを用いたリモート生体認証プロトコルを，2.4 節の要件に従って評価する．

要件 (R1) を満たすためには，変換関数 $F_R \in \mathbf{F}$ が，従来の照合方式で使われてきた生体情報（特徴量）間の距離を，大きく変化させなければよい．つまり距離関数を $d(\cdot,\cdot)$ としたとき，任意のパラメータ R と任意の生体情報 X，Y に対し，

$$d(X,Y) \simeq d(F_R(X), F_R(Y)) \tag{1}$$

を満たせばよい（正確には，距離の順序構造を保存すればよい）．これを満たす変換関数の具体例として，虹彩認証のように距離関数がハミング距離で定義される場合に $F_R(X) = X \oplus R$（X と R の排他的論理和）とする方法[6] や，さらにビット置換などを組み合わせる方法[7] が提案されている．また静脈のように画像の相互相関に基づいて距離が定義される場合，画像 X を数論変換（有限体 Z_p 上の離散フーリエ変換）してから Z_p 上の乱数列 R との乗算（登録時）または除算（認証時）を行う方式[9] が提案されている．文献 9) では実際に指静脈認証へ適用した結果，従来の照合方式とほぼ同程度の認証精度であったことが報告されている．

要件 (R2) を満たすためには，変換後の情報 $F_R(X)$，$F_R(X')$ から H（$= R$）を知らずに X（または X に十分近い生体情報）を復元できないことが要求される．これは暗号解読における暗号文単独攻撃への耐性を持つことに相当する．文献 6)，7) は一様乱数列との排他的論理和やランダムな置換を行うことで，文献 9) は有限体上で一様乱数との乗算を行うことで，変換後の情報を乱数列と区別すること自体を困難としており，本要件を満たしていると考えられる．ただしこれらの方法は，認証サーバに対して X，X' 間の距離以外の情報をまったく漏らさない，といったゼロ知識性を有するものではない．たとえば文献 6) の方法では，サーバは $X' \oplus X$ を知ることができる．このような部分情報によってただちに X，X' が復元されることはないが，詳細な安全性評価は今後の課題である．

要件 (R3) については，R を X と無関係にランダムに選択することで，これを満たすことができる．

キャンセラブルバイオメトリクスを用いたプロトコルの問題点は，要件 (R4) を満たさないことである．実際，$T = F_R(X)$ を入手した攻撃者は，認証時に $T \sim V$ を満たす V を作成し認証サーバに送信することで，X'（$\sim X$）を知らなくても認証成功できてしまう（健全性を満たさない）．このため認証サーバは，クライアントが本当に X' を知っているのか，上述のように V（$\sim T$）を知っているだけなのかを判別できない．

4. 提案プロトコル

本章では，キャンセラブルバイオメトリクスとゼロ知識証明プロトコルを組み合わせるこ

とで，2.4 節であげた要件をすべて満たすリモート生体認証プロトコルを提案する．

4.1　アプローチ

キャンセラブルバイオメトリクスでは，攻撃者が $T = F_R(X)$ に十分近い V を知っていれば，X に十分近い X' を知らなくても認証成功することができ，このため (R4) を満たしていなかった．

この問題は，クライアントが認証サーバに対し，登録局から発行された正しいパラメータ R の知識を証明することで，解決可能である．以下具体例として，虹彩のようにハミング距離を用いた生体認証方式に対して，アプローチを説明する．

生体情報が n ビットデータ（虹彩の場合 $n = 2{,}048$ または 4,096）で表現され，生体情報間の距離がハミング距離で定義されているとする．このとき，変換関数 $F_R(X) = X \oplus R$（X と R の排他的論理和）を用いてキャンセラブルバイオメトリクスを実現できる．具体的には認証サーバが，クライアントから受け取った V（$= X' \oplus R$）と，検証情報 T（$= X \oplus R$）のハミング距離を計算し，十分近い（$V \sim T$）ときに認証成功とする．これによって認証サーバは，F_R に関する V の逆像 $X' = V \oplus R$ が X に十分近いこと（$X' \sim X$）を確認できる．しかしこれだけでは，クライアントが X' を知っていることを認証サーバが確認したことにはならない．実際，サーバが受信した V に対して $V = x \oplus r$ となる (x, r) の組は 2^n 通り存在する．その中でクライアントが正しい (X', R) の組を知っているのか，それとも T を入手した攻撃者が (T, δ)（δ はハミング重みが十分小さい適当な n ビットデータ）なる組で $V = T \oplus \delta$ としているのか，サーバには判別できない．

ところで V を固定したとき，r を決めれば $V = x \oplus r$ なる x は一意に決まる（$x = V \oplus r$）．したがって R を知っているクライアントは，$V = x \oplus R$ なる x，つまり X' を知っていることになる．したがって X' の知識を示すためには，R の知識を証明すればよい．サーバはすでに $X' \sim X$ を確認しているため，これによってクライアントが X に十分近い生体情報を知っていることを確認することができる．

このことをベン図を用いて模式的に表したのが**図 4** である．V（$\sim X \oplus R$）を知っていて，かつ R を知っているクライアントは，$X' = V \oplus R$（$\sim X$）を知っている．

以上のアプローチを一般化する．任意の R に対して F_R が式 (1) を満たし，かつ逆関数 F_R^{-1} を持つものとする（文献 6)，7)，9) の方式はすべてこの条件を満たす）．逆関数の存在から，V を固定したとき r に対して $V = F_r(x)$ なる x が一意に決まるため，x の知識を示すためには r の知識を証明すれば十分である．

認証時，クライアントは認証サーバに対し，$V = F_R(X')$ を送信するとともに，R の知識を証明する．認証サーバは V，T を照合し $V \sim T$ を確認することで，F_R に関する V の逆像 $X' = F_R^{-1}(V)$ が，X に十分近いことを知ることができる．さらに R の知識証明により，認証サーバは，クライアントが V（$\sim F_R(X)$）と R を知っており，したがって X'（$= F_R^{-1}(V) \sim X$）の知識を持つことを検証できる．なお知識証明が満たすべき要件（完全性，健全性）の評価は，5.1 節で詳細に述べる．

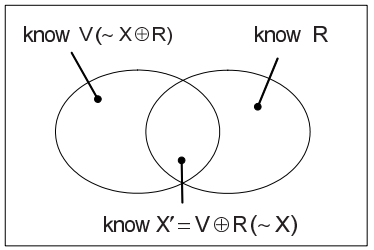

図 4　X'（$\sim X$）の知識証明
Fig. 4　Knowledge proof of $X'(\sim X)$.

ただしクライアントは R を開示してはならない．なぜなら認証サーバに R が知られると，$F_R(X)$ と R から X が復元可能となり，要件 (R2) を満たさなくなるためである．そこでゼロ知識証明を用いて R の知識を証明する．R は（X' と異なり）あいまいさを含まない値なので，たとえば Schnorr 認証[11] や Integer commitment scheme[12] などの方法を用いてゼロ知識証明プロトコルを実現することができる．

4.2　登録・認証プロトコル

キャンセラブルバイオメトリクスにおける変換関数の集合 $\mathbf{F} = \{F_R : \mathbf{X} \to \mathbf{X}\}$ が以下の条件を満たすものとし，これを用いてリモート生体認証の登録・認証プロトコルを構築する．

1. F_R は生体情報間の距離（の順序構造）を大きく変化させない．
2. $F_R(X)$，$F_R(X')$ から R を知らずに X，X' を復元することはできない．
3. $Y = F_R(X)$ の逆関数 $X = F_R^{-1}(Y)$ が存在．

すでに述べたように，文献 6)，7)，9) の変換関数はこれらの条件を満たしている．

登録プロトコル

Step 1. 登録局はパラメータ R をランダムに選択して $F_R \in \mathbf{F}$ を決定し，また R の知識をゼロ知識証明プロトコルを用いて証明するための乱数情報 s，および検証するための情報 $C(R)$ を作成する．

Step 2. 登録局は登録者の生体情報 X を取得し，上記変換関数を用いて $F_R(X)$ を作成

する．

Step 3. 登録局は $T = (C(R), F_R(X))$ を検証情報として認証サーバに発行する．また $H = (R, s)$ を補助情報として利用者に対して発行する．

認証プロトコル

Step 1. クライアントは R を知っていることを，認証サーバに対してゼロ知識証明する．証明に失敗したら認証失敗としてプロトコルを終了する．

Step 2. クライアントは利用者の生体情報 X' を取得し，$F_R(X')$ を作成して認証サーバに送信する．

Step 3. 認証サーバは $F_R(X)$ と $F_R(X')$ を照合し，十分近いならば本人と判定し，認証成功とする．そうでないなら他人と判定し，認証失敗とする．

4.3 プロトコルの具体例

上記提案プロトコルの具体例として，生体情報が n ビット列 X で表現され，生体情報間の距離がハミング距離で定義される場合を考える．文献 9) のようにハミング距離以外の場合でも同様にプロトコルを構築することができる．

登録プロトコル

Step 1. 登録局は n ビット列 R をランダムに選択する．次に R の知識のゼロ知識証明に必要となる情報 s，$C(R)$ を作成する．ここでは整数の知識のゼロ知識証明が可能な Integer commitment scheme [12] を用いる．

まず n ビット以上の十分大きな合成数 $N = pq$（RSA モジュラス）を用意し，位数の十分大きな $h \in Z_N^*$ をランダムに選択する．また α，$s \in [0, 2^k N]$（k はセキュリティパラメータ）をランダムに選択し，

$$g = h^{\alpha} \bmod N, \tag{2}$$

$$C(R) = g^{int(R)} h^{s} \bmod N \tag{3}$$

とする．ここで $int(R)$ は R を 2 進表現された整数と見なした値を表す．

Step 2. 登録局は登録者の生体情報 X を取得し，R を用いて以下のように変換する．

$$F_R(X) = X \oplus R$$

変換関数 F_R は前節で述べた 3 つの条件を満たしている．

Step 3. 登録局は $T = (C(R), F_R(X))$ を検証情報として認証サーバに発行し，$H = (R, s)$ を補助情報として登録者に発行する．また (N, g, h) を公開する．

認証プロトコル

Step 1. クライアントは以下のように R，s の知識を認証サーバに証明する．

表 3　認証プロトコルの計算量・通信量
Table 3　Calculation and communication complexity.

プロトコル	計算量（べき乗回数）		通信量（ビット）
	登録局/クライアント	サーバ	
登録	3	0	2n
認証	2	3	3(n+k+l)

(1) クライアントは $x \in [0, 2^{k+l+n}]$，$y \in [0, 2^{2k+l} N]$（l はセキュリティパラメータ）をランダムに選択し，$b = g^x h^y \bmod N$ を計算して認証サーバに送る．

(2) 認証サーバは $e \in [0, 2^l]$ をランダムに選び，クライアントに送る．

(3) クライアントは $u = x + e \cdot int(R)$，$v = y + es$ を計算し，認証サーバに送る．

(4) 認証サーバは $g^u h^v \equiv bc^e \pmod N$ の成立をチェックし，成立しなければ認証失敗としてプロトコルを終了する．

Step 2. クライアントは利用者の生体情報 X' を取得して $F_R(X') = X' \oplus R$ を作成し，認証サーバへ送信する．

Step 3. 認証サーバは $F_R(X)$ と $F_R(X')$ のハミング距離を計算し，十分近いならば本人と判定して認証成功とする．そうでないなら認証失敗とする．

適切なセキュリティパラメータ k，l の定め方については文献 12) を参照のこと．N を n ビットとした場合，本プロトコルの計算量・通信量は**表 3** のとおりとなる．ただし計算量は，最も計算時間のかかる，N を法としたべき乗計算の回数で評価した．なお登録・認証プロトコルの **Step 2**（排他的論理和）の計算量は，べき乗計算と比較して無視できる．本プロトコルをたとえば虹彩認証（$n = 2{,}048$）に適用した場合，十分実用的な計算量・通信量であるといえる．

5. 評　　価

5.1 提案方式のセキュリティ評価

提案プロトコルが 2.4 節で述べたリモート生体認証のセキュリティ要件を満たしているか評価する．

(R1) 4.2 節で述べた変換関数の条件 1 より，F_R の適用によって X，X' 間の距離と認証しきい値との大小関係は大きく変化しないため，認証精度が大きく劣化することはない．したがって提案プロトコルは要件 (R1) を満たす．

(R2) 変換関数の条件 2 より，認証サーバは $F_R(X)$，$F_R(X')$ から X，X' を復元することはできない．また R の知識証明において，4.3 節のように適切なゼロ知識証明を用いることで，認証サーバは $C(R)$ や通信データから R に関するいかなる情報も得られない．したがって提案プロトコルは要件 (R2) を満たす．

(R3) $H = (R, s)$ は X と独立にランダムに選択されるため，H から X を推定することはできない．また同じ理由から，H のみを入手しても $F_R(X)$ に十分近い $F_R(X')$ が分からないため，認証成功することはできない．したがって提案プロトコルは要件 (R3) を満たす．

(R4) 適切なゼロ知識証明を用いれば，クライアントが正しい H を知っているとき，認証サーバは十分高い確率でその証明を受理し，認証プロトコルの **Step 1** をパスする．また $X' \sim X$ ならば条件 1 より $F_R(X') \sim F_R(X)$ となり，**Step 3** をパスする．したがって，クライアントが X'（$\sim X$）および H を知っていれば，十分高い確率で認証に成功する（完全性を満たす）．

健全性を評価するため，以下ではクライアントが $X' \sim X$ なる X' を知らないとき，攻撃者が認証（なりすまし）に成功する確率 P を見積もる．P が FAR 以下であれば健全性を満たすものとする．なぜなら，どのようなリモート生体認証プロトコルでも，攻撃者が H さえ知っていれば，攻撃者自身あるいは適当な他人の生体情報を X' とすることで，確率 FAR でなりすましに成功する（X' と X が偶然一致する）ためである．

なりすましに成功するためには，R の知識のゼロ知識証明をパスし，さらに $V \sim F_R(X)$ なる V を認証サーバに送信しなくてはならない．以下，攻撃者が (1) H を知っている場合，(2) T を知っている場合，(3) いずれも知らない場合に分けて P を評価する．

(1) 攻撃者が H を知っていたとする．このとき $V \sim F_R(X)$ なる V を推定できれば，なりすましに成功する．その方法としては，生体情報空間 $\mathbf{X}$ から V をランダムに選択する（成功確率 $P_{V \sim F_R(X)}$ とする）か，$X' \sim X$ なる X' を生体情報データベースなどからランダムに選択し（成功確率 $P_{X' \sim X}$ とする），$V = F_R(X')$ とすることが考えられる．一般に生体情報は空間 $\mathbf{X}$ に一様に分布してはおらず，偏った分布を持つと考えられるため，$P_{X' \sim X} > P_{V \sim F_R(X)}$ と考えられる．$P_{X' \sim X}$ は異なる生体情報が偶然一致する確率であり，FAR と等しい．つまりなりすまし成功確率は FAR で評価できる．

(2) 攻撃者が T を知っていたとする．H を推定できれば，なりすましに成功する．$H = (R, s)$ をランダムに選択する以上に有効な推定方法として，まず T に含まれる $C(R)$ から計算する方法が考えられるが，これは適切なゼロ知識証明プロトコルを用いることで十分困難とすることができる．これ以外の推定方法としては，生体情報データベースなどから X' をランダムに選択して $T = F_R(X')$ なる R を計算し，s はランダムに選択する方法が考えられる．しかし正しい R が計算されるためには，選択した生体情報 X' が X に完全一致してなくてはならず，その確率は FAR 以下である．さらに，ランダムに選択した s が正しい値である確率は十分小さくすることができる．たとえば 4.3 節の例では $1/(2^k N)$ なので N や k を十分大きくとればよい．したがって攻撃者が T を知っている場合のなりすまし成功確率 P は FAR 以下である．

(3) 攻撃者が H，T のいずれも知らない場合，いずれかを知っている (1)，(2) の場合よりなりすまし成功確率は低く，FAR 以下である．

以上 (1)〜(3) の評価より，$X' \sim X$ なる X' を知らないクライアント（攻撃者）による認証成功確率は FAR 以下であり，健全性を満たしている．つまり提案プロトコルは完全性，健全性を満たし，要件 (R4) を満たす．

5.2　既存プロトコルとの比較

提案方式を，既存のリモート生体認証プロトコルと比較する．既存プロトコルとしては，生体情報を直接登録，照合する従来方式と，テンプレートを秘匿したまま認証するテンプレート保護型生体認証方式を考慮する．後者には様々な方式が提案されているが，それらをキャンセラブルバイオメトリクス，バイオメトリック暗号，非対称生体認証の 3 つに分類して評価し，提案プロトコルと比較する．

5.2.1　従 来 方 式

従来のリモート生体認証方式として，生体情報を直接登録，照合するプロトコルを考える．つまり $T = X$ とし，認証時には X' を直接送信して認証サーバが X' と T（$= X$）を照合する．R は用いない．以下，この従来方式がリモート生体認証の要件を満たしているか評価する．

(R1) 従来の照合方式（特徴量抽出・照合アルゴリズム）が利用できるため，要件を満たす．

(R2) 認証サーバ側で X，X' を知ることができ，要件を満たさない．

(R3) H は用いないため，本要件は評価対象外．

(R4) クライアントは認証サーバに対して X' を提示し，認証サーバは認証時に X，X' を直接照合して $X' \sim X$ を判定するため，完全性，健全性を満たす．

なお AES などの一般的な暗号アルゴリズムを用いて X を暗号化したものを T とし，照合時に復号する方式も，まったく同じ評価となる．

5.2.2　キャンセラブルバイオメトリクス

3.2 節で述べたように，キャンセラブルバイオメトリクスは要件 (R1)，(R2)，(R3) を満

たすものの，(R4) は満たさない．

5.2.3　バイオメトリック暗号

バイオメトリック暗号は，生体情報の歪みやノイズを特殊な量子化と誤り訂正によって補正して，一意のデータ（秘密鍵）を生成する技術（動的鍵生成技術）と，公開鍵暗号などの暗号技術を組み合わせて，リモート認証を行う方式である．登録時には秘密鍵 SK と公開鍵 PK のペアを生成し，PK を検証情報 T とする．また SK を生体情報 X に埋め込み，補助情報 H を作成する．認証時にはクライアントが X' を用いて H から SK を復元し，認証サーバとの間でチャレンジレスポンスを行い SK の知識を示す．

動的鍵生成技術の具体例として，たとえば生体情報間の距離がハミング距離で定義される場合，X と同じビット長の誤り訂正符号語 w をランダムに選択して $SK = w$，$H = X \oplus w$ とし，認証時には $H \oplus X' = w \oplus (X \oplus X')$ を誤り訂正することで w（$= SK$）を復元する方式（Fuzzy Commitment [13]）が提案されている．ほかにも指紋認証に適用可能な特殊な誤り訂正方式を用いた Fuzzy Vault [14] や，生体情報のゆらぎを統計的に学習して量子化を行う統計的 AD 変換[15] といった方式が提案されている．これらの動的鍵生成技術を用いたバイオメトリック暗号について以下，リモート生体認証の要件を満たしているか評価する．

(R1) 動的鍵生成を実際の生体情報に適用し，精度評価を行った研究例として，指紋認証に対する Fuzzy Vault および統計的 AD 変換の適用が報告されており[16),17)]，たとえば文献 17) では FAR 0.73%，FRR 0.45%（指紋画像の位置ずれ補正は手作業）と報告されている．しかしいずれも従来の指紋認証技術との精度比較は行っていない．精度評価結果は，生体情報のサンプルを取得する際の実験条件（被験者の習熟度，体調，環境，登録/認証の時間間隔など）により大きく影響を受けるため，これらの方式が要件 (R1) を満たしているか否かは不明である．なお一般に生体認証における照合アルゴリズムは，2 つの生体情報 X，X' を比較して，同一の生体から取得されたものかを判定すればよいのに対し，動的鍵生成は X' がある生体 A から取得されたものであるとき，X' から A に紐付いた一意のデータ（鍵）SK_A を生成する（その際，基準となる A の生体情報 X や，生成すべきデータ SK_A を知ることなく生成する），という問題を対象とする．動的鍵生成をある精度で実現するアルゴリズムが存在するなら，単純に生成した鍵を比較することで同じ精度の照合アルゴリズムを実現できるが，逆にある精度の照合アルゴリズムが存在しても，それと同じ精度を持つ動的鍵生成アルゴリズムを構築する方法は知られていない．このため一般に動的鍵生成の方が，高精度化が困難であると考えられる．

(R2) PK，SK は X と無関係に選択されるため，認証サーバは T やクライアントとのチャレンジレスポンスから X，X' に関する情報を得られず，要件を満たす．

(R3) Fuzzy Commitment では，ランダムに選択した誤り訂正符号語 w（$= SK$）と X の排他的論理和を H とすることで，H から X，SK を復元困難としている．また Fuzzy Vault や統計的 AD 変換では，X に SK を埋め込む際にダミー情報を混入させることで，H から X，SK を復元することを困難にしている．このように H のみを用いて X の推定やなりすましを行うことは困難であり，要件 (R3) を満たしていると考えられる．ただしその困難性は証明可能なものではなく，たとえば Fuzzy Vault は，実装によっては H から X を推定可能であることが指摘されている[18]．

(R4) クライアントは SK を知っていることを証明するが，SK は X と無関係な（登録時にランダムに選択された）値であるため，SK の知識証明によって X'（$\sim X$）の知識証明をしたことにはならない．実際 SK を知っていれば X'（$\sim X$）を知らなくても認証成功できるため，健全性を満たさない．このため要件 (R4) を満たしていない．

5.2.4　非対称生体認証

非対称生体認証は，クライアントが認証時に取得した生体情報 X' が，登録時の生体情報 X に十分近い（$X' \sim X$）ことを，認証サーバに対してゼロ知識証明する方式である．ここでのゼロ知識性は，$X' \sim X$ であるか否かの 2 値の情報のみを開示し，それ以外の情報はいっさい漏らさないことを意味する．実現方式としては，準同型暗号を用いてニューラルネットワーク（NN）の秘密計算を行う方式[19] や，コミットされた秘密の整数が特定の区間に入っていることを示す暗号プロトコルを利用する方式[20] が提案されている．ただし後述するように，文献 19) の方式は，厳密には前述のゼロ知識性を満たしていない．

以下具体例として文献 19) のプロトコルを説明し，各要件について評価する．登録時，登録者の生体情報 $X = (x_1, \cdots, x_n)$ に十分近い生体情報 X' を受理するようにニューラルネットワーク（NN）の学習を行い，その中間層ノードの重みを $W = \{w_{ij}\}$，出力層ノードの重みを $W' = \{w'_i\}$ とする．W を暗号化した $E(W) = \{E(w_{ij}, r_{ij})\}$ と W' の組を検証情報 $T = (E(W), W')$ とし，暗号化に用いた乱数 r_{ij} と W の組を補助情報 $H = (\{r_{ij}\}, W)$ とする．認証時にはクライアントが $X' = (x'_1, \cdots, x'_n)$ を入力として NN を計算し，中間層の出力 $Y = \{y_i\}$ を認証サーバに送信するとともに，X' の知識と計算過程の正しさをゼロ知識証明する．認証サーバは Y と W' を用いて NN の出力値（受理/拒否）を計算する．以下，非対称生体認証がリモート生体認証の要件を満たしているか評価する．

(R1) 非対称生体認証を実際の指紋情報に適用した研究例が報告されている[5] が，FAR 8.3%，FRR 9.8%と報告されており，現状では要件を満たしているとはいえない．NN の入力次元

表 4　プロトコルの比較
Table 4　Comparison of the protocols.

プロトコル	(R1)	(R2)	(R3)	(R4)
従来方式	○	×	–	○
キャンセラブル	○	○	◎	×
バイオメトリック暗号	△	◎	○	×
非対称生体認証	×	○	◎	○
提案プロトコル	○	○	◎	○

数やノード数を増やすことで，従来の生体認証で用いられている様々な距離関数を近似できる可能性を持っているものの，これに比例して秘密計算やゼロ知識証明の計算量・通信量が増加する．計算量・通信量の削減と精度向上の両立が課題である．

(R2) $T = (E(W), W')$ のうち $E(W)$ は暗号文，W' は出力層ノードの重みであり，これらの情報から X を復元することは困難であると考えられる．また認証サーバは，クライアントが計算した中間層の出力 $Y = \{y_i\}$ を得るが，中間層の重み W を知らないため，ここから X を復元することは困難であり[5]，要件 (R2) を満たすと考えられる．ただしその困難性は証明可能なものではない．実際 Y は X の線形結合で表せるため，認証サーバに対して X の部分情報を開示していることになる．

(R3) $H = (\{r_{ij}\}, W)$ において $\{r_{ij}\}$ は X と無関係に選択される乱数であり，また W のみから X を復元することもできない[5] ため，要件を満たす．

(R4) クライアントは，X' が中間層出力 Y を与える NN の入力であることを，認証サーバに対してゼロ知識証明する．この証明プロトコルは完全性，健全性を満たす．さらに認証サーバは Y を入力として NN の出力層を直接計算し，$X' \sim X$ であることを確認するため，全体として完全性，健全性を満たし，要件を満たす[5]．

5.2.5　各方式の比較

上記の各方式と，提案プロトコルの比較結果を**表 4** に示す．既存プロトコルが，それぞれいずれかの要件に関して問題があったのに対し，提案プロトコルはすべての要件を満たしている．

なお 5.2.3 項で述べたように，バイオメトリック暗号を指紋に適用した研究例の中には，比較的高い精度（FAR，FRR ともに 1%以下）を報告しているものもあるが，同じ指紋サンプルを用いた従来の指紋認証技術との精度比較を行っていないため，(R1) に関しては不明（△）とした．また (R2)，(R3) については，要件を満たすことが証明可能な場合に◎とした．たとえば H を X と無関係な乱数として選択できるキャンセラブルバイオメトリクスや提案方式は，H から X の情報がまったく得られないため，(R3) に関して◎とした．

6. 考　　察

3.2 節で述べたように，文献 6)，7)，9) などのキャンセラブルバイオメトリクス方式では，認証サーバが $F_R(X)$，$F_R(X')$ から X，X' を復元することが困難であると考えられるものの，その困難性は証明可能なものではない．

そこで提案プロトコルを拡張し，認証サーバに対して $X \sim X'$ であるか否かの情報以外を漏らさないようにする方法を考察する．具体的には以下の条件を満たすゼロ知識証明プロトコルを構築できればよい．

条件：認証サーバは $U \in \mathbf{X}$ としきい値 t を保持し，クライアントは $V \in \mathbf{X}$ を知っている．二者間のプロトコルの実行の結果，認証サーバは $d(U, V) \leq t$ であるか否かの情報のみを得，クライアントは何も得ない．

このようなプロトコルの例として，$d(U, V)$ がハミング距離で定義される場合，Oblivious Transfer と Yao の財産比べプロトコルを用いたマルチパーティープロトコル[21] が提案されている．また，互いにベクトルを秘匿したまま内積の大小関係を比較する，秘匿内積比較プロトコル[22] を利用することで，ユークリッド距離に対しても所望のプロトコルを構築できる可能性がある．ただしこれらのプロトコルは，X のビット数または次元数に比例した回数のゼロ知識証明を行う必要があり，計算量，通信量の削減が課題である．

7. ま と め

本稿では，ネットワークを介した安全な生体認証を実現することを目的に，リモート生体認証システムにおける脅威分析とセキュリティ要件の明確化を行い，これを満たすリモート生体認証プロトコルとしてキャンセラブルバイオメトリクスとゼロ知識証明を組み合わせた方式を提案した．またセキュリティ要件に関して既存方式との比較を行い，提案方式の利点を明らかにした．

今後は，提案プロトコルが部品として用いるキャンセラブルバイオメトリクスの変換関数について，その安全性を詳細に評価するとともに，安全性を証明可能なゼロ知識証明プロトコルへの拡張について検討していくことが課題である．

参 考 文 献

1) Mimura, M., Ishida, S. and Seto, Y.: Development of personal authentication tech-

niques using fingerprint matching embedded in smart cards, *IEICE Trans. Information and Systems*, Vol.E84-D, No.7, pp.812–818 (2001).
2) 山田朝彦：バイオメトリクスのための認証コンテキスト（ACBio），東芝レビュー，Vol.62, No.9, pp.74–75 (2006).
3) Ratha, N.K., Connell, J.H. and Bolle, R.M.: Enhancing security and privacy in biometric-based authentication systems, *IBM System Journal*, Vol.40, No.3 (2001).
4) Uludag, U., Pankanti, S., Prabhakar, S. and Jain, A.: Biometric cryptosystems: Issues and challenges, *Proc. IEEE*, Vol.92, No.6, pp.948–960 (2004).
5) 永井　慧，菊池浩明，尾形わかは，西垣正勝：ZeroBIO — 秘匿ニューラルネットワーク評価を用いた非対称指紋認証システムの開発と評価，情報処理学会論文誌，Vol.48, No.7, pp.2307–2318 (2007).
6) Braithwaite, M., Cahn von Seelen, U., Cambier, J., Daugman, J., Glass, R., Moore, R. and Scott, I.: Application-specific biometric templates, *AutoID02*, pp.167–171 (2002).
7) 太田陽基，清本晋作，田中俊昭：虹彩コードを秘匿する虹彩認証方式の提案，情報処理学会論文誌，Vol.45, No.8, pp.1845–1855 (2004).
8) 高橋健太，三村昌弘：キャンセラブル指紋照合方式の提案，*CSS2005*, pp.379–384 (2005).
9) 比良田真史，高橋健太，三村昌弘：画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案，情報処理学会研究報告，2006-CSEC-34, pp.435–440 (2006).
10) ISO/TC68/SC6, ISO 13491-1: Banking – secure cryptographic devices (retail) – Part1: Concepts, requirements and evaluation methods (1996).
11) Schnorr, C.P.: Efficient identification and signatures for smart cards, *CRYPTO '89*, LNCS 435, pp.239–251, Springer-Verlag (1990).
12) Damgård, I.B. and Fujisaki, E.: A statistically-hiding integer commitment scheme based on groups with hidden order (2002).
13) Juels, A. and Wattenberg, M.: A fuzzy commitment scheme, *Proc. ACM CCS1999*, pp.28–36 (1999).
14) Uludag, U., Pankanti, S. and Jain, A.K.: Fuzzy vault for fingerprints, *AVBPA*, pp.310–319 (2005).
15) 柴田陽一，三村昌弘，高橋健太，中村逸一，曽我正和，西垣正勝：メカニズムベースPKI—指紋からの秘密鍵動的生成，情報処理学会論文誌，Vol.45, No.8, pp.1833–1844 (2004).
16) 星　勇輔, 大木哲史, 山崎　恭, 小松尚久, 笠原正雄：Fuzzy Fingerprint Vault Schemeにおけるダミーデータの生成手段に関する検討，*SCIS2007* (2007).
17) 柴田陽一，宮木　孝，三村昌弘，高橋健太，水野忠則，西垣正勝：Fuzzy Commitmentを用いた統計的 AD 変換の改良に関する考察（その 3）— 複数の特徴量からの生体鍵生成，*SCIS2007* (2007).
18) Mihailescu, P.: The fuzzy vault for fingerprints is vulnerable to brute force attack (2007). [Online] Available from http://arxiv.org/abs/0708.2974v1
19) 菊池浩明：非対称生体認証，*CSS2005*, pp.307–311 (2005).
20) 尾形わかは，菊池浩明，西垣正勝：リモートバイオメトリクス認証に有効な「近い」ことを示す零知識証明プロトコル，*SITA2006*, pp.319–322 (2006).
21) 伊藤　隆，鶴丸豊広，米田　健：マルチパーティプロトコルを用いた生体情報秘匿型生体認証方式，*SCIS2006* (2006).
22) 佐久間淳，小林重信：プライバシを保護した内積比較プロトコルの提案，情報処理学会研究報告，2006-CSEC-034, pp.257–264 (2006).

(平成 19 年 11 月 28 日受付)
(平成 20 年 3 月 4 日採録)

高橋　健太（正会員）

1998 年東京大学理学部情報科学科卒業．2000 年同大学院修士課程修了．同年（株）日立製作所入社．以来，同システム開発研究所にて生体認証技術の研究開発に従事．

比良田真史

2002 年東京大学大学院総合文化研究科修士課程修了．同年（株）日立製作所入社．以来，生体認証技術の研究開発に従事．

三村　昌弘（正会員）

1991 年東京工業大学工学部機械物理学科卒業．1997 年同大学院博士課程修了．同年（株）日立製作所入社．以来，生体認証技術の研究開発に従事．工学博士．

手塚　　悟（正会員）

1984 年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所に勤務し，パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LAN システム等の研究開発に従事．その後，システム開発研究所に勤務．以来，パーソナルコンピュータを中心とした LAN システムの構築・運用管理の研究開発，さらにセキュリティシステムの研究開発に従事，現在に至る．東京工科大学非常勤講師（2005 年）．2004 年度情報処理学会論文賞受賞．工学博士．著書に『Inside CORBA』アスキー出版（共訳）（1998 年），『インターネットコマース　新動向と技術』共立出版（共著）（2000 年），『インターネット時代の情報セキュリティ—暗号と電子透かし』共立出版（共著）（2000 年）．