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

永井 慧[†1] 菊池浩明[†2]
尾形わかは[†3] 西垣正勝[†4]

生体情報を検証者に漏らさずにリモート認証を行う暗号プロトコルを提案する．提案方式は，ニューラルネットワークを用いて生体情報特有の曖昧さを処理し，ゼロ知識証明を用いて正規ユーザの認証を実現する．本論文では，試験実装に基づいて提案方式の性能と精度を評価する．偽拒否率と偽受入率の観点から，いくつかの特徴量抽出手法について定量的な評価を行った．

ZeroBio — Evaluation and Development of Asymmetric Fingerprint Authentication System Using Oblivious Neural Network Evaluation Protocol

Kei Nagai,[†1] Hiroaki Kikuchi,[†2] Wakaha Ogata[†3]
and Masakatsu Nishigaki[†4]

We propose a cryptographical protocol for remote biometrics authentication without revealing private biometrics data to verifier. Our protocol uses a neural network for dealing with uncertainty of biometric data, and a zero-knowledge interactive proof for valid user. In this paper, we evaluate the performance and the accuracy of the proposed protocol based on sample implementation system. Several algorithms for features extraction of fingerprint data are examined in terms of false acceptance and rejection ratios.

1. はじめに

パスワードに代わる安全な認証技術として，生体情報を用いた認証が注目されている．生体認証は自分自身の生まれつき保持している特徴を用いて認証を行うため，パスワードを記憶しておくデバイスを保持しておく必要もなく，秘密情報の忘却や紛失の危険性がない．それゆえに，利便性の高い次世代の認証方式として様々な分野で導入が進んでいる．しかし，リモートな環境から認証を行う場合，通信時における生体情報の盗聴や，検証者の不正による生体情報の漏洩が危惧される．特に，生体情報はひとたび漏洩してしまった場合，パスワードと違って変更することができないため，その取扱いに細心の注意を払う必要がある．

この問題に対して，Ratha らはキャンセラブルバイオメトリクス[1)]という概念を導入し，画像ブロック変換，マニューシャ非線形変換などの方式を提案した．また，太田らは虹彩情報に対して回転や歪曲などの変換を施し，変換に使用した乱数を変更することで登録した生体情報の更新を可能としている[2)]．高橋らも指紋情報に対して，生体情報の更新を可能としたキャンセラブル照合方式を提案している[3)]．しかし，彼らのシステムでは，いずれもサーバが類似度を保存する性質があるがゆえに，内部犯の犯行に対してロバストではない．

一方，伊藤らは，認証時にマルチパーティプロトコルを用いて生体情報を秘匿し，虹彩コードのハミング距離から認証を行うプロトコルを提案している[4)]．しかしながら，文献 2)，4) の方式は，認証時にハミング距離を利用しているため，取得する特徴量の変動が大きい指紋や静脈などの生体情報に対しては対応でき

†1 東海大学大学院工学研究科
Graduate School of Engineering, Tokai University
†2 東海大学情報理工学部情報メディア学科
School of Information Technology and Electronics, Tokai University
†3 東京工業大学大学院イノベーションマネジメント研究科
Graduate School of Innovation Managment, Tokyo Institute of Technology
†4 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

ない可能性がある．柴田らは，生体情報そのものではなく，生体情報から公開鍵暗号の秘密鍵を動的に生成し，ディジタル署名により利用者認証を行うメカニズムベース PKI を提案している[5]．実際に，指紋認証で提案方式を実行するシステムを実装し，さらに Fuzzy Commitment Scheme[9] を利用することで精度向上を試みている．また，これら以外にも，多項式復元問題を利用した符号化技術である Fuzzy Vault Scheme[8] を生体認証に適用した研究[6),7)] や，Dodis らによる，生体情報のような変動の大きい情報から一意な鍵を抽出する技術も研究されている[10),11)]．

以上のことより，リモートからセキュアに生体認証を行うためには，生体情報を所持する証明者と本人の確認を行う検証者の間で，管理する情報がそれぞれ異なる，すなわち，**非対称**である生体認証を行う必要がある．ここでいう非対称とは，公開鍵暗号と同様に，証明者が持つ生体情報を検証者は必要としないことを意味する．ディジタル署名の技術でよく知られているように，そのような非対称性を持つ認証方式は難しくはない．しかし，バイオメトリクスに関しては，人体特有のあいまいさから生じる生体情報の変動や読み取り誤差などの外乱が避けられないので，それらの変動に対処する認証方式を実現しなくてはならない．

そこで，これらの非対称性と不確定さという 2 つの要求条件に対して，我々は次の 2 つの技術を組み合わせることを提案する．

(1) ニューラルネットワーク
階層型のニューラルネットワーク[17] を用いて，登録に用いる複数の生体情報を学習し，本人だけを識別する関数を構成する．これにより，生体情報特有の曖昧さを克服する．

(2) ゼロ知識証明
秘密の入力である生体情報を検証者に漏らさずに，その入力が与えられた性質を満たしていることを検証者に示す．

ここで，ニューラルネットワークの出力が入力ベクトルと学習係数の線形和で定義されていることに着目する．ゼロ知識証明の要素技術として用いられているアルゴリズムには準同型性を満たすものがあり，線形和の演算ならば，入力値を秘匿した評価が可能である．これらを利用し，我々は次の新しい認証技術を提案する．

秘匿ニューラルネットワーク評価 ニューラルネットワークの重み（登録情報）に対して，出力層を満足する入力ベクトル（生体情報）を持っていることを，入力ベクトルを秘匿したままで証明する．

本研究では，この技術を用いて，入力する生体情報が登録したニューラルネットワークの正しい出力を得ることを，生体情報を秘匿した状態で証明するプロトコルを構成する．本論文では，提案方式が実現可能であることを示すために，提案プロトコルを用いた指紋認証システムを実装し，その精度や処理性能を報告する．提案方式の性能は，その入力となる特徴量の性質に依存するところが大きいため，いくつかの特徴量抽出方式についてその性質を調べ，提案方式に最適な実現方式を検討する．

本論文の構成は次のとおりである．2 章では，いくつかの既存方式とそれらの課題を示す．3 章では，まず要素技術を定義し，提案プロトコルに適した特徴量の要求条件を明らかにする．次に，提案方式の登録と認証のプロトコルを示す．提案方式の実現可能性を検証するために行った実装とその評価について 4 章で述べる．ここでは，(1) 特徴量抽出方式，(2) ニューラルネットワークの精度，(3) 総合処理の精度，(4) 処理時間について行った評価結果を報告するとともに，提案方式の安全性について考察する．最後に，5 章で本論文の結論を示す．

2. 既存方式

本章では，文献 2)〜5) の各方式について説明するとともに，リモート環境下での生体認証が要求する条件について述べる．

2.1 正規化ハミング距離保存変換[2)]

ユーザは秘密情報としてランダムに選択した 2 値ベクトル $\boldsymbol{r}$ とランダムに選択した置換係数 π，および特定の条件を与えることで選択される行列 A を用意する．登録時には，ユーザは登録時生体情報ベクトル $\boldsymbol{x}$ に対し，$\boldsymbol{e} = A\pi(\boldsymbol{r}||\boldsymbol{x})$ をサーバへ登録する．

認証時には，ユーザは認証時生体情報ベクトル $\boldsymbol{x}'$ に対して $\boldsymbol{e}' = A\pi(\boldsymbol{x}'||\boldsymbol{r})$ をサーバへ送信する．サーバは $\boldsymbol{e}$，$\boldsymbol{e}'$ 間のハミング距離 $H(\boldsymbol{e}, \boldsymbol{e}')$ を計算し，これが閾値 τ 以下となった場合に認証許可として処理を終了する．登録情報の更新には再度 $\boldsymbol{e}$ を計算して登録を行えばよい．

本方式が正当なユーザを正しく認証できるのは $\boldsymbol{e}$ の演算によってハミング距離が計算されるところにある．しかしながら，ハミング距離を保存する制約があるゆえに，通常の公開鍵暗号や共通鍵暗号ほどの強度は達成されない[2)]．

2.2 キャンセラブル[3)]

ユーザは登録時に抽出する特徴量 $\boldsymbol{x}$ に対し，生体情報への復元困難性と精度保存性の条件を満たすよう

表 1 各認証方式の特徴
Table 1 The characteristics of each authentication method.

	生体情報	使用技術	ヒルクライミング	課題
太田ら[2]	虹彩	正規化ハミング距離保存変換（拡大，並べ替え，回転）	×	ハミング距離を保存する制約がある
高橋ら[3]	指紋	マニューシャ等長変換	×	$\boldsymbol{x}$ と $\boldsymbol{x}'$ の類似度がサーバに漏れる
伊藤ら[4]	虹彩	Oblivious Transfer	×	サーバとユーザ間の信頼関係を仮定
柴田ら[5]	指紋	統計的 AD 変換	○	公開鍵暗号の鍵として十分なエントロピが得られない（4.6 節参照）
提案方式	指紋	秘匿ニューラルネット評価	○	

なパラメータ θ を持つ変換関数 F_θ をランダムに作成する．これを用いて，$F_\theta(\boldsymbol{x})$ をサーバへ登録する．なお，パラメータ θ はクライアントが保管し，サーバに対してはこれを秘匿する．

認証時には登録時と同様に特徴量 $\boldsymbol{x}'$ を抽出し，F_θ により変換された特徴量 $F_\theta(\boldsymbol{x}')$ を送信する．サーバはテンプレートである $F_\theta(\boldsymbol{x})$ と $F_\theta(\boldsymbol{x}')$ を照合し，類似度を計算する．更新時には新規にパラメータ θ を設定し，それにより得られる $F_\theta(\boldsymbol{x})$ を再度サーバに登録しなおせばよい．

文献 2)，3) の各方式はともにサーバが $\boldsymbol{x}$ と $\boldsymbol{x}'$ 間の類似度計算が可能であることから，照合結果（類似度や距離）に漸近するように生体情報を徐々に変化させ，生体情報を取得する，いわゆる**ヒルクライミング攻撃**[15] を受ける．

2.3 マルチパーティプロトコル[4]

伊藤らの方式では，生体情報の類似度判定にハミング距離を用い，生体情報の秘匿には Oblivious Transfer を用いる．登録時には生体情報の 2 値ベクトル $\boldsymbol{x}$ に対して，あらかじめランダムに生成された 2 値ベクトル $\boldsymbol{r}$ をもとに，$\boldsymbol{x} \oplus \boldsymbol{r}$ をサーバに送信する．認証時には認証時に取得した生体情報ベクトルを $\boldsymbol{x}'$ として，ハミング距離 $H(\boldsymbol{x} \oplus \boldsymbol{r}, \boldsymbol{x}' \oplus \boldsymbol{r}) = H(\boldsymbol{x}, \boldsymbol{x}')$ を満たしているかどうかを判定する．

2.4 メカニズムベース PKI[5]

柴田らは，指紋から動的に秘密鍵を生成して PKI 認証を行っている．登録時には指紋を複数枚撮影し，各画像をメッシュに区切り，各メッシュについて指紋画像から得られる隆線ベクトルの平均と分散を算出する．隆線ベクトルの分散を考慮して量子化し，対応する乱数をもとにして秘密鍵を生成する．この処理を統計的 AD 変換と呼ぶ．

認証時には同様にメッシュごとの隆線ベクトルを得た後，動的に秘密鍵を作成し，ディジタル署名を用いた PKI 認証を行う．

本方式は生体情報が漏洩する可能性はきわめて低く，高い精度で一意な ID が生成されるため，安定した認証率が実証されている．しかしながら，鍵の不十分な長さや，個々の生体情報の分布を利用した鍵解析の危険性がある．

2.5 各方式の特徴

本節では，2.1〜2.4 節で述べられた各生体認証方式を**表 1** で整理する．ここで，ヒルクライミングの列は，類似度計算結果を利用したヒルクライミング攻撃に対するロバスト性を示している．

3. 提 案 方 式

3.1 要 素 技 術

本システムは，生体情報を秘匿した状態で類似度の計算を行うために，次の技術を用いる．

3.1.1 ニューラルネットワーク

入力層は，n 個のユニット $x_1, \ldots, x_n$ と，バイアス項と呼ばれるつねに 1 をとるユニット $x_{n+1} = 1$ からなる．同様に，中間層は $y_1, \ldots, y_\ell$ とバイアス項 $y_{n+1} = 1$，出力層は z の単一ユニットとする．入力層から中間層へは完全結合で，重み w_{ij} によって結び付けられており，中間層から出力層への重みは $\tilde{w}_j$ とする．各ユニットの出力は，閾値関数

$$s(x) = \frac{1}{1 + e^{-x}} \tag{1}$$

により定める．したがって，中間層は $j = 1, \ldots, \ell$ について，

$$\tilde{y}_j = s(y_j),$$
$$y_j = w_{1j}x_1 + w_{2j}x_2 + \cdots + w_{nj}x_n + w_{n+1,j} \tag{2}$$

と定める．同様に出力層は，

$$z = s(\tilde{w}_1\tilde{y}_1 + \cdots + \tilde{w}_\ell\tilde{y}_\ell + \tilde{w}_{\ell+1})$$

と書き表せる．入力ユニットと対応する出力層を学習データとして与えたとき，誤差を最小化する w_{ij} を求めるには，誤差逆伝搬法[17] と呼ばれる，以下の効率の良いアルゴリズムが知られている．

入力 $x_1, \ldots, x_n$ に対する出力の教師データを z'，ニューラルネットワークの出力を z とする．教師データ z' と出力 z の最小二乗誤差

$$\phi(z) = \frac{1}{2}||z' - z||^2$$

を計算し，$\phi(z)$ の値が小さくなる方向へ最急降下法[18]により重み $\tilde{w}_j$ を変化させる．このとき，$\tilde{w}_j$ の更新値 $\Delta\tilde{w}_j$ は，

$$\Delta\tilde{w}_j = -\eta\frac{\partial\phi(z)}{\partial\tilde{w}_j}$$

で定める．ここで，η は $[0,1]$ の値をとる学習係数である．重み $\tilde{w}_j$ を徐々に更新し，収束するまで繰り返す．中間層から入力層にかけての重み w_{ij} についても同様に行う．

3.1.2 コミットメント方式[14]

本方式の要素技術として，加法準同型性を満たすコミットメント方式を用いる．コミットメント $E(m,r)$ は，以下の性質を有する関数とする．

(1) $E(m,r)$ から m に関する情報が統計的に漏れない．

(2) 任意の m，m'（$\neq m$）に対して，$E(m,r) = E(m',r')$ を満たす m'，r' を求めることは困難である．

上記の条件を満たす具体的な構成として，以下に示す Fujisaki らのコミットメント方式[14] がある．

N を誰もその素因数を知らない大きな合成数とし，g，h を Z_N の要素とする．誰も h の離散対数 $\log_g h$ を知らないとする．このとき，

$$E(m,r) = g^m h^r \pmod N$$

を m のコミットメントとする．ただし，r は十分大きい乱数とする．このコミットメントは，明らかに加法準同型性

$$E(m,r) \times E(m',r') \stackrel{?}{=} E(m+m', r+r'),$$
$$E(m,r)^x \stackrel{?}{=} E(mx, rx)$$

を満たす．ただし，ここで，記法 $\stackrel{?}{=}$ は両辺が等しい関係にあることを明示した統合である．なお，Z_N の位数は誰も知ることができないため，$m+m'$ などは mod 演算ではないことに注意されたい．

加法準同型性を利用することにより，式 (2) のニューラルネットでの線形演算が m を伏せてコミットしたまま実現できる．

3.2 概　　要

本方式では証明者 P と検証者 V が存在し，登録と認証の 2 つのプロトコルからなる．登録時には，本人の複数の指紋データ $\boldsymbol{x}$ と他人のデータを合わせて教師データとし，ニューラルネットワークの重み w_{ij} を学習させる．このとき，w_{ij} のコミットメント $W_{ij} = E(w_{ij}, r_{ij})$ を V へ登録する．

認証時には新たに指紋データ $\boldsymbol{x}'$ を読み取り，$\boldsymbol{x}'$ が w_{ij} について，ニューラルネットワークの出力を満足する値であることを，V に $\boldsymbol{x}'$ を漏らすことなくゼロ知識証明で証明する．

3.3 登録プロトコル

登録時はリーダから本人の指紋と他人の指紋を複数枚読み取り，特徴量ベクトルの集合 A（本人），B（他人）を作る．

ここで得られた特徴量をニューラルネットワークの入力ユニット値 $\boldsymbol{x} = (x_1, \ldots, x_n)$ とする．次に，誤差逆伝播法を用いて 3 層のニューラルネットワークにかける．ここでは教師データを

$$z = \begin{cases} 1 & \text{if} \quad \boldsymbol{x} \in A \\ 0 & \text{if} \quad \boldsymbol{x} \in B \end{cases},$$

と定める．

登録プロトコルを次に示す．

Step 1. $A \cup B$ を教師データとし，ニューラルネットワークの重み w_{ij}，$\tilde{w}_j$ を学習する．この後，A，B は消去する．

Step 2. P は，中間層の重み w_{ij} のコミットメント $W_{ij} = E(w_{ij}, r_{ij})$ と，出力層の重み $\tilde{w}_j$ を検証者 V へ登録する．証明者 P は，コミットメントに用いた w_{ij}，r_{ij} を安全なデバイス☆に保持しておく．

3.4 認証プロトコル

プロトコルを**図 1** に示す．証明者 P は，デバイスから中間層の重み w_{ij} と登録時の乱数 r_{ij} を取り出し，新たに抽出した生体情報 $\boldsymbol{x}' = (x'_1, \ldots, x'_n)$ を用いて，検証者に登録されているコミットメント $W_{ij} = E(w_{ij}, r_{ij})$ と出力層の重み $\tilde{w}_j$ を満足することを証明する（ただし，$i = 1, \ldots, n$，$j = 1, \ldots, \ell$ とする）．

まず，P は $\boldsymbol{x}'$ についての中間層ユニット値

$$y'_j = \sum_{i=1}^{n} w_{ij} x'_i \tag{3}$$

を求め，V に送る．y'_j は登録時の値 y_i と必ずしも等しくないことに注意されたい．

次に，y'_j のコミットメント $E(y'_j, R_j)$ に等価な

$$Y_j = \prod_{i=1}^{n} W_{ij}^{x'_i} \tag{4}$$

を求めて，V に送る．ここで，R_j は

☆ このデバイスへ格納する情報に関しては，4.5 節で論じる．

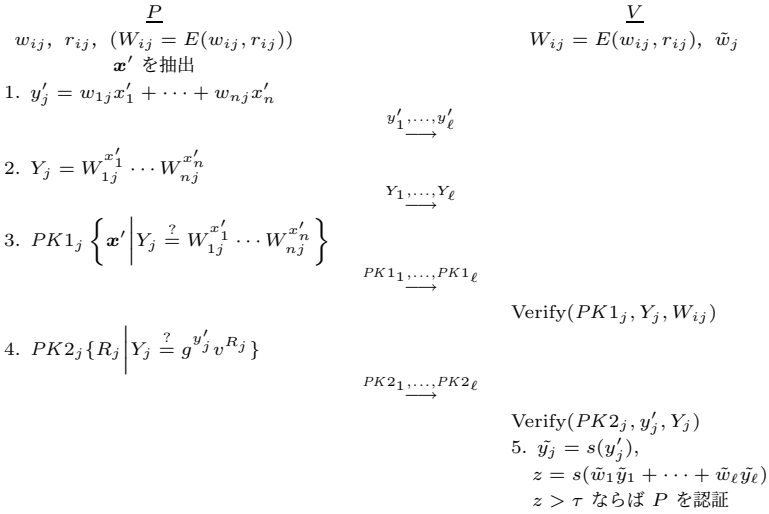

図 1 認証プロトコル
Fig. 1 Authentication protocol.

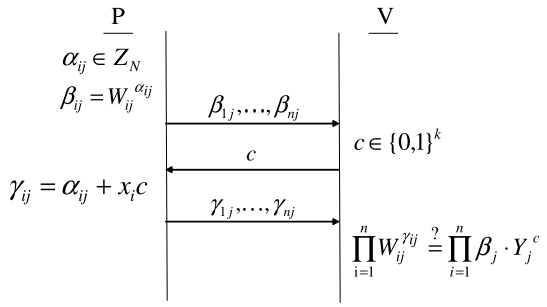

図 2 正しい生体情報 $\boldsymbol{x}'$ を持つことのゼロ知識証明 $PK1_j$
Fig. 2 $PK1_j$ – Zero-knowledge interactive proof of $\boldsymbol{x}'$ to be valid.

$$R_j = \sum_{i=1}^{n} r_{ij} x'_i$$

と定める．

P は，式 (4) を満たす生体情報 $\boldsymbol{x}'$ を持っていることを**図 2** のゼロ知識証明

$$PK1_j \left\{ x'_1, \ldots, x'_n \middle| Y_j \stackrel{?}{=} \prod_{i=1}^{n} W_{ij}^{x'_i} \right\}$$

により V に証明する．V は，式 (4) の Y_j と登録済みの W_{ij} について，$PK1_j$ を検証する．

Y_j は中間層ユニット値 y'_j のコミットメントであるが，登録時の y_j とは異なり，認証の度ごとに変わる．そこで，P が登録したユーザと同じであることを証明するために，重みのコミットメントに用いた乱数 R_j を知っていることを利用して，式 (4) の Y_j が式 (3) の中間層ユニット値 y'_j の正しいコミットメント $Y_j \stackrel{?}{=} E(y'_j, R_j)$ になっていることを，ゼロ知識証明

$$PK2_j\{R_j \mid Y_j \stackrel{?}{=} g^{y'_j} v^{R_j}\}$$

により，V に示す．これには，よく知られた離散対数のゼロ知識証明[13] を利用する．

2 つのゼロ知識証明を満足した後，V は登録された出力層の重み $\tilde{w}_j$ と式 (3) の中間層ユニット値 y'_j，式 (1) の閾値関数を用いて $\tilde{y}_j = s(y'_j)$ とし，出力値 z を

$$z = s\left(\sum_{j=1}^{\ell} \tilde{w}_j y'_j\right)$$

と求め，あらかじめ決められた閾値 τ について，

$$z > \tau \qquad (5)$$

を満たすことを確認する．以上の $PK1_j$，$PK2_j$，式 (5) をすべて満たすならば P を認証する．

3.5 特徴点抽出

提案方式を実現するためには，特徴点抽出アルゴリズムにいくつかの制約条件がある．本節では，その条件を整理し，いくつかの妥当な方式を示す．なお，対象とする生体情報は指紋データとする．一般には，マニューシャと呼ばれる指紋の隆線の端点や分岐点を特徴点とすることが多い．

3.5.1 抽出法の要求条件

まず，従来の生体認証に求められる条件を以下に示す．

(1) 特徴の変動が小さいこと
読み取り誤差や生体情報そのものの曖昧さに起

因する特徴の変動は避けられない．たとえば，指紋では読み取り時に生じる傾きや平行移動による変動があげられる．これが FAR の主な原因となる．

(2) 他人との差が十分に大きいこと
本人と他人を識別するためには，他者との特徴の差異が十分に大きいことが条件となる．この差異が FRR を決定する．

上記の条件に加え，ニューラルネットワークとゼロ知識証明を利用した提案方式を適用するためには，次の条件が要求される．

(3) 入力値の次元が一定であること
マニューシャは追加，消失が生じるため，入力次元が固定しているニューラルネットワークの入力には適さない．

(4) 入力値の順序が一定であることニューラルネットワークは，入力値の変動にはロバストであるが，値の置換には対処できない．たとえば，座標 (x, y) が (y, x) に変わるようなもので，正しい学習結果は期待できない．

3.5.2 特徴量抽出法式

3.5.1 項で触れた条件を満たすような入力値とし，以下のような手法を用いて，マニューシャよりニューラルネットワーク入力値の抽出を行った．ここで，特徴点にある処理を加えて抽出したニューラルネットワーク入力値を特徴量と定義する．

(1) メッシュ分布
指紋画像を $L \times L$ のメッシュに区切り，各メッシュに存在するマニューシャの数をカウントして L^2 次元の特徴量ベクトル $\boldsymbol{a} = (a_1, \ldots, a_{L^2})$ とする．$L = 5$ としたときの分布例を**図 3** に示す．この方式は位置合わせなどの前処理により，マニューシャ座標を正規化することで，ある程度指紋撮影時の回転や座標のずれによる誤差を吸収することが可能である．位置合わせのアルゴリズムとして，指紋の中心核を原点とした正規化の手法があるが，指紋の形状によっては中心核が存在しない可能性がある．

(2) 隆線角度分布
マニューシャの隆線角度について D 値に量子化し，各量子化角度に対応したマニューシャの数により，$\boldsymbol{a} = (a_1, \ldots, a_D)$ の特徴量ベクトルを定める．8 分割を行ったときの分布例を**図 4** に示す．(1) のメッシュを利用した方式と比べ，位置合わせなどの正規化を行う必要がないため，高速処理が可能である．

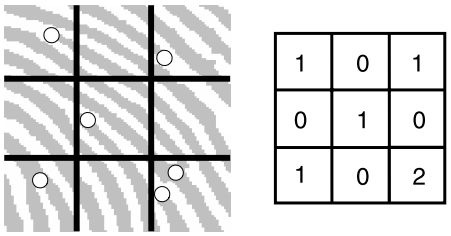

図 3 メッシュ分布方式
Fig. 3 Biometrics features method using a minutiae distribution over mesh map.

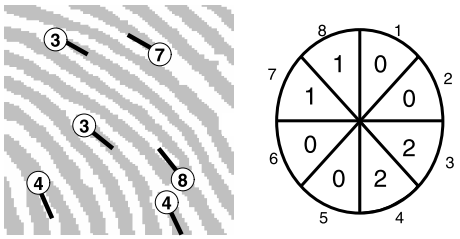

図 4 隆線角度分布方式
Fig. 4 Biometrics features method classifing minutiae for ridge angle.

(3) クラスタリング
特徴が似通ったマニューシャを指定した数にクラスタリングし，その代表元を特徴量とする．たとえば，最短距離アルゴリズム[16] を用いれば，A の中で最も距離の近い組 $\boldsymbol{a}_i$ と $\boldsymbol{a}_j$ を求め，それらを統合し，マニューシャ $\boldsymbol{a}_{ij} = (\boldsymbol{a}_i + \boldsymbol{a}_j)/2$ に置換する．ただし，$\boldsymbol{a}_i = (x_i, y_i)$ と $\boldsymbol{a}_j = (x_j, y_j)$ 間の距離 $d = (\boldsymbol{a}_i, \boldsymbol{a}_j)$ は，マニューシャ間のユークリッド距離であり，

$$d(\boldsymbol{a}_i, \boldsymbol{a}_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

と定義する．こうして，$|A|$ が希望クラスタ数になるまで上記の統合を繰り返す．

(4) 隆線ベクトル
メッシュ分布方式と同様に画像を $L \times L$ のメッシュに区切り，各メッシュにおける隆線の傾き，すなわち 0〜π までの角度を要素とするベクトル $\boldsymbol{a} = (a_1, \ldots, a_{L^2})$ を特徴量とする方式[5] である．メッシュによっては，隆線の方向が定まらない箇所が生じるという問題がある．

4. 実装評価

提案方式の実現可能性を検討するために，指紋を対象としたシステムを実装し，各特徴量の性質や認証精度を明らかにする．提案方式には，(1) 特徴量抽出，(2) ニューラルネットワーク，(3) ゼロ知識証明の 3 つ

表 2 NFIS2 が提供する各機能
Table 2 The functions of NFIS2.

機能	プログラム
指紋形状の分類	pcasys
特徴点抽出	mindtct
マッチング	bozorth3
画像処理	NFIQ

表 3 システム仕様
Table 3 System specification.

ソフトウェア	Java SE 1.5.0_06
指紋読み取り装置	Digital Persona U.are.U4000
特徴点抽出	NIST NFIS2

の不確定要素があるので，これらの関係も明らかにしなくてはならない．

4.1 実装システム

特徴量を抽出するための前処理である特徴点抽出には，米国標準技術研究所 National Institute of Standards and Technology（NIST）が提供する指紋認証ソフトウェア，Nist Fingerprint Image Software 2 [19]（以下 NFIS2 とする）を用いた．NFIS2 は主に**表 2** のような機能を提供している．

まず，mindtct を用いてマニューシャ情報を取得する．マニューシャは $(x_{NFIS}, y_{NFIS}, \theta_{NFIS}, r_{NFIS}, t_{NFIS})$ の形式をとる．x_{NFIS}，y_{NFIS} は座標，θ_{NFIS} は 90° を表す 0 から時計回りに 31 までの 32 値をとる．r_{NFIS} は $[0,1]$ の値をとるマニューシャ検出の信頼度を表し，かすれに起因する偽マニューシャを識別する．t_{NFIS} は分岐点（BIF: bifurcation）か端点（RIG: ridge ending）のどちらかをとる．**表 3** に試験システムの開発仕様を示す．

4.2 評価方法

本節では，各処理における評価方法について述べる．

(1) 特徴量抽出
3.5.1 項で述べた各手法について，ある 2 人の被験者について，同じ指を各々30 回ずつ読み取り，この画像の集合を A，B とおく．すなわち，$|A| = |B| = 30$ 本のデータを用いて各々の分布を調べる．また，各次元の量子特徴量を公平に評価するために，基準指 $\boldsymbol{a}^* \in A$ を定め，$A - \{\boldsymbol{a}^*\}$ と他人の指 $\boldsymbol{b}^* \in B$ の各要素 $\boldsymbol{a}^* = (a_1, \ldots, a_D)$，$\boldsymbol{b}^* = (b_1, \ldots, b_D) \in B$ についてのユークリッド距離の分布を求めた．

$$d(\boldsymbol{b}) = \sqrt{\sum_{i=1}^{m}(a_i - b_i)^2} \qquad (6)$$

各手法から抽出される特徴量が持つ情報量より，生体情報の解析困難性を検証する．

(2) ニューラルネットワーク
学習済みのニューラルネットワークの識別誤差を検証する．実際の指の代わりに，ランダムな擬似入力を作成し，それらを用いて他人受入率（FAR）を算出する．なお，学習はメッシュ分布での学習時と同数の $|A| = 80$ 本，$|B| = 40 \times 18 = 720$ 本のデータを使用した．

(3) 総合処理での精度
前述した 2 つの処理に加え，ゼロ知識証明までの処理を一連の動作として行い，認証精度を算出する．

(4) 処理時間
認証にかかる一連の処理時間を測定する．また，ニューラルネットワークの中間層の数について，評価を繰り返した．なお，ゼロ知識証明で用いるセキュリティパラメータ k については一般的に安全とされている 160 [bit] に設定している．

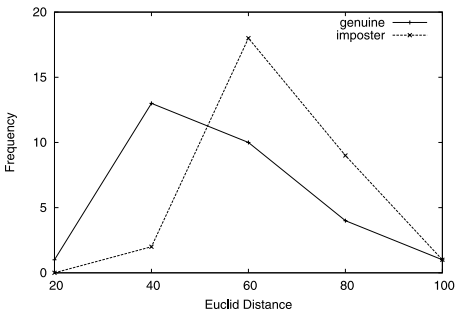

図 5 メッシュ分布におけるユークリッド距離分布
Fig. 5 The Euclid distance distribution in the mesh division method.

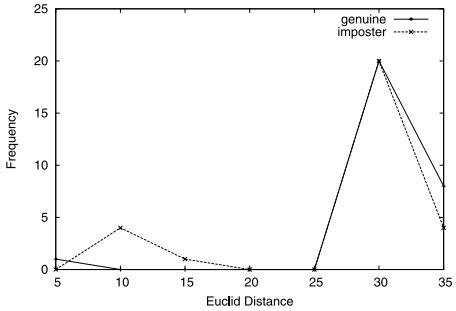

図 6 隆線角度分布におけるユークリッド距離分布
Fig. 6 The Euclid distance distribution in the ridge angle division method.

4.3 実験結果

4.3.1 特徴量抽出法の評価

各抽出アルゴリズムにおける式 (6) のユークリッド距離の分布を**図 5**，**図 6**，**図 7**，**図 8** に示す．また，

表 4 各手法の基本統計量
Table 4 Statistics for division methods.

	平均 μ_A	標準偏差 σ_A	$\Delta\mu$	$\Delta\mu/\sigma_A$	$\sigma_A/\Delta\mu$
メッシュ分布	43.93	16.01	11.76	0.73	1.36
隆線角度分布	28.35	5.48	3.46	0.63	1.58
クラスタリング	571.49	109.09	9.77	0.08	11.15
隆線ベクトル	141.75	47.24	51.01	1.07	0.92

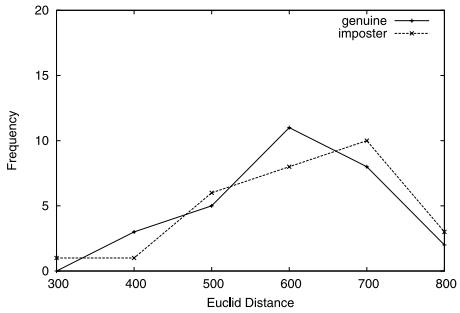

図 7 クラスタリングにおけるユークリッド距離分布
Fig. 7 The Euclid distance distribution in the clustering method.

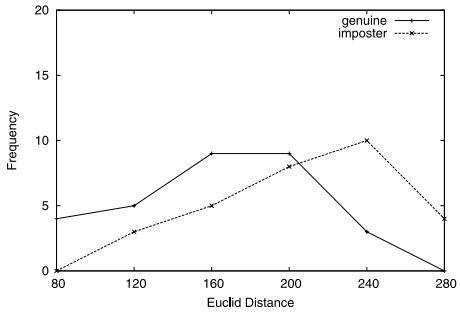

図 8 隆線ベクトルにおけるユークリッド距離分布
Fig. 8 The Euclid distance distribution in the ridge slope vector method.

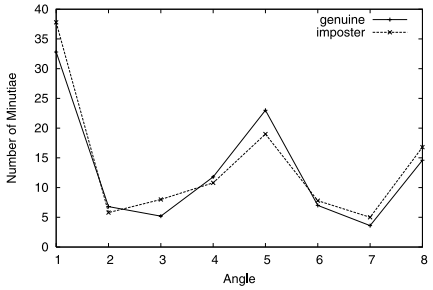

図 9 隆線角度分布の個人差
Fig. 9 Variance of ridge angle.

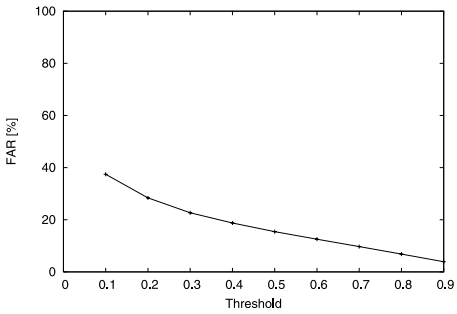

図 10 ニューラルネットワークにおける誤差率
Fig. 10 False acceptance rate (FAR) with respects to threshold.

ここでは他人との特徴量の差を表す A と B の平均の差を $\Delta\mu = |\mu_A - \mu_B|$，本人の特徴量の変動を σ_A で表し，各々を σ_A，$\Delta\mu$ により正規化した．これらの結果を**表 4** に整理する．

以上より，最も他人との差異が大きい方式と，本人の特徴量の変動が最小である方式は両方共隆線ベクトルであった．また，隆線角度分布により抽出される特徴量は**図 9** からも明らかなように，指紋は縦長であるため，図 9 における 1 と 5 の要素は万人に共通して多いことが分かった．

4.3.2 ニューラルネットワークの精度

ニューラルネットワークは任意の連続関数を近似できることが知られているが，学習データに偏りや不足があった場合はその限りではない．そこで，この学習精度を評価するため，ランダムに定めた特徴量を入力値とし，それにより得られる出力値を観察する．**図 10** に，出力値の閾値 τ を変動させた場合の誤差率を示す．

メッシュ分布による分割手法での最適な閾値は，4.3.3 項で述べる FAR-FRR の関係から，FRR=10% を与える $\tau = 0.6$ であり，FAR = 8%である．これはすなわち，ランダムに作成した特徴量でも 10 回に 1 回は受理してしまうことを表している．

4.3.3 総合処理の精度

ここでは一連の動作における FAR と FRR を算出し，その認証精度を示す．ニューラルネットワークの入力数が冗長なため，隆線ベクトルを除く 3 つの特徴量抽出手法について検証した．ニューラルネットワークの閾値 τ を変動させて求めた FAR-FRR の比較結果を**図 11** に示す．

クラスタリングや隆線角度分布方式では，マニューシャの消失や座標軸のずれなどにより，認証精度に多

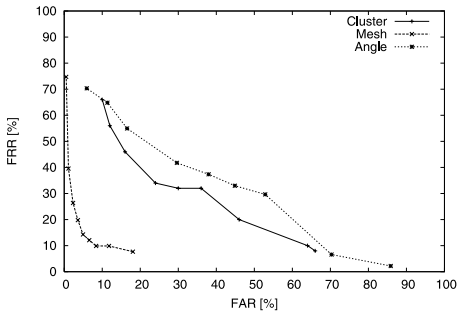

図 11 各手法の精度評価
Fig. 11 Evaluation on accuracy in several methods.

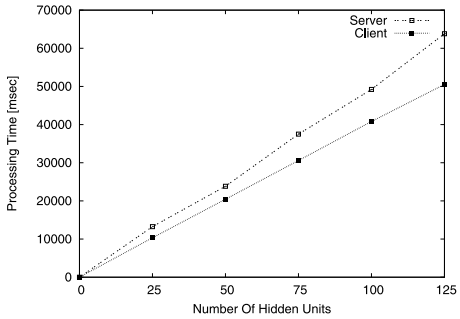

図 12 中間層数による処理時間実測
Fig. 12 Processing time with respects to the number of hidden units.

大な影響を与えていたが，メッシュ方式では FAR と FRR をともに 10%未満に抑えている．

4.3.4 処 理 時 間

メッシュ分布によるプロトコルを例にして，認証時の処理時間を測定した．処理時間を**図 12** に示す．中間層ユニット数に比例して計算時間が増加するのは，ゼロ知識証明をユニット数に応じた回数行う必要があるためである．ただし，Pentium4 1.8 GHz の Linux, 1,000 Mbps の環境で計測した．

4.4 安 全 性

安全性の観点より，本システムを破る際には，

(1) 生体情報を推定する，
(2) ニューラルネットワークの重みを推定する，
(3) ゼロ知識証明を破る，

という 3 つが考えられる．(1) の困難さは，特徴量空間の大きさに依存している．そこで，各特徴量における情報量を算出する．

ここでは，仮に NFIS2 を用いて，256×256 の分解能 v を持つ $n = 200$ 個のマニューシャが得られたと仮定し，各々の持つ情報量を計算する．特徴量は T 値をとる D 次元のベクトル $\boldsymbol{a} = (a_1, \ldots, a_D)$ と考えることができる．たとえば，(1) のメッシュ分布では，メッシュの数 $L = 5$ とすると，次元 D は，$5 \times 5 = 25$ で与えられる．このとき，n 個のマニューシャが各メッシュに均等に分布したとすると，平均 $n/D = 200/25 = 8$ 個のマニューシャが分布する．したがって，特徴量空間は，

$$v^D = 8^{25} = 2^{75} = 3.7 \times 10^{22}$$

すなわち，75 [bit] となる．同様にして，他の方式について算出した結果を**表 5** に示す．この結果より，特徴量が一様に分布しているならば，隆線ベクトルが最も推測困難であるといえる．

表 5 特徴量空間の情報量
Table 5 Entropy of biometrics features.

	次元 D	分解能 v	情報量 v^D [bit]
メッシュ分布	25	$8 = 2^3$	75
隆線角度分布	8	25	37
クラスタリング	10	$256^2 = 2^{16}$	160
隆線ベクトル	324	$32 = 2^5$	1,620
マニューシャ	200	$256^2 \times 32 = 2^{21}$	4,200

表 6 特徴量抽出方式の精度
Table 6 Accuracy for several features division methods.

抽出法	FRR	FAR	閾値 Θ
メッシュ分布	0.51	0.06	50
クラスタリング	0.55	0.33	210
隆線ベクトル	0.10	0.50	660

しかし実際には，生体情報は一様には分布していない．攻撃者は統計的な予測が可能である．そこで，4.3 節の結果に基づいて，この偏りについての精度と期待値を求める．2 者間の分布における交差点を閾値として与え，式 (6) のユークリッド距離のみで認証を行うことを考える．メッシュ分布の場合で，図 5 より本人と他人とを識別する閾値 $\Theta = 50$ であることが分かる．したがって，

$$FRR = \frac{|\{\boldsymbol{a} \in A | d(\boldsymbol{a}) > 50\}|}{|A - \boldsymbol{a}^*|} = \frac{15}{29} = 0.51$$

$$FAR = \frac{|\{\boldsymbol{b} \in B | d(\boldsymbol{b}) < 50\}|}{|B|} = \frac{2}{30} = 0.06$$

が求められた．同様に，他の方式についても評価すると**表 6** のようになる．ただし，図 4 のように，交差点が得られない方式については計測を行っていない．

次に，(2) の困難さについて考察する．V は，y'_j を知っているが，式 (2) の線形式を満たす $\boldsymbol{x}'$ は一意には決まらない．加えて，式 (2) における w_{ij} はコミットメントの性質 (1) より，W_{ij} から w_{ij} を推定することは困難である．したがって，(2) のリスクは少ないといえる．

次に，(3) の困難さについて考察する．この安全性は，ゼロ知識証明 $PK1_j$，$PK2_j$ のセキュリティパラ

表 7 各フェーズにおける誤認証率
Table 7 The FAR and FRR at each phase.

	特徴量（メッシュ分布）	ニューラルネットワーク	ゼロ知識証明	統合（メッシュ分布）
FAR	0.06	0.13	2^{-k}	0.083
FRR	0.51	-	0	0.098

メータ k に依存するため，k を十分に大きくすることで安全性の向上が期待できる．このとき，正しい R_j を知っている利用者ならば必ず $PK1_j$，$PK2_j$ を合格できるので，FRR は 0，一方，不正者が V の作成するチャレンジ c を予測できる確率は 2^{-k} なので，FAR は 2^{-k} である．

また，4.3.2 項で述べたようにニューラルネットワークの識別誤差も考慮する必要がある．この影響を考察する．図 5〜図 8 の分布に基づいて，ニューラルネットワークで学習を実行して A と B を識別するが，2 つの群の差は十分でないことが明らかになった．原因として，特徴量抽出の前処理の段階での不整合，メッシュや角度における分割数の不整合が考えられる．

これまで論じてきた安全性と精度の関係を**表 7** に整理する．ただし，特徴量はメッシュ分布，ニューラルネットワークの閾値は $\tau = 0.6$ を用いている．これらのバランスを考えて，適切なセキュリティパラメータ k を選ぶ必要がある．

4.5 デバイスへ格納する情報

提案方式では，登録プロトコルにおける中間層の重み w_{ij} と，コミットメントの乱数 r_{ij} をデバイスへ格納する必要がある．したがって，利便性を損ない，従来のデバイスに生体情報を保持する認証方式（たとえば，文献 12) のようなアプローチがある）と同等に見える．しかしながら，デバイスを盗まれたら即座に認証を許してしまう従来方式に比べ，本方式は対応する生体情報なしでは認証できない（$PK1_j$ で失敗するため）．

加えて，従来方式では生体情報そのものを格納しているので，耐タンパ性といった高い安全性を担保する必要があった．一方，本方式では，記録されているのは乱数と中間層の重みのみであり，たとえ漏洩しても更新を行えばよい．

したがって，提案するデバイスと生体情報を組み合わせた認証方式の有用性は高い．

4.6 統計的 AD 変換[5] との比較

提案方式と同様に，生体情報の空間と公開鍵暗号理論の鍵空間を結び付ける試みに，2.4 節で述べた統計的 AD 変換[5] がある．この方式は，生体情報の量子化された特徴量と公開鍵対が，1 対 1 に対応しているので，可能な鍵の個数は特徴量空間に制約される．したがって，公開された鍵から全特徴量について総あたりされる攻撃のリスクがある．

一方，提案方式では特徴量 $\boldsymbol{x}$ からニューラルネットワークの重み w_{ij} を求め，w_{ij} をコミットして認証に用いている．コミットメントの性質 (1) により，$E(w_{ij}, r_{ij})$ と $E(w'_{ij}, r'_{ij})$ は識別不能である．ゆえに，特徴量空間と鍵空間（コミットメント）は独立であり，前述の攻撃には耐性がある．

4.7 内部犯行に対する耐性

不正なサーバの管理者による内部犯の犯行は，管理者が知りうる中間層ユニット値 y'_j とそのコミットメント Y_j，および重みのコミットメント W_{ij} が与えられたときに，それらを満たす生体情報 $\boldsymbol{x}$ をヒルクライミング攻撃により同定することである．

しかし，認証プロトコルにおける $PK1_j$ が対話的であるため，証明者 P の助けなしに $\boldsymbol{x}'$ が正しいかどうかのテストを実行できない．

5. ま と め

生体情報特有の曖昧さに対し，ニューラルネットワークを適用することでこれを解決し，ゼロ知識証明を用いることで生体情報を秘匿した非対称生体認証を実現した．また，ニューラルネットワークでは対応できないマニューシャの消失にともなう次元の変動や，入力順序の変動に対し，これらを包括した特徴量抽出手法を用いて，各々の精度比較を行った．

今回の実験では FAR = 0.083，FRR = 0.098 の精度を得ることが分かった．ニューラルネットワークやゼロ知識証明では，学習時間やセキュリティパラメータを上げることで誤認証率を下げることができるが，特徴量そのものの識別が十分でないことがあるので，その制約の中で最適化を行う必要がある．今後の課題として，生体情報に適したニューラルネットワークを探すこと，情報量の低減が少ない特徴量抽出方式について比較・検証を行うことがあげられる．

謝辞 本研究は文部科学省科学研究費補助金基盤研究（B）「ゼロ知識証明を用いた非対称なリモートバイオメトリクス利用者認証」の助成を受けている．

参 考 文 献

1) Ratha, N.K., Connell, J.H. and Bolle, R.M.: Enhancing Security and Privacy in Biometrics-based Authentication Systems, *IBM Systems Journal*, Vol.40, No.3 (2001).
2) 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).
3) 高橋健太，三村昌広：キャンセラブル指紋照合方式の提案，コンピュータセキュリティシンポジウム CSS2005，pp.379–384 (2005).
4) 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，暗号と情報セキュリティシンポジウム SCIS2006 (2006).
5) 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).
6) Uludag, U. and Jain, A.K.: Fuzzy Fingerprint Vault, *Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice*, pp.13–16 (2004).
7) 大木哲史，田島 賢，赤塚志郎，小松尚久，笠原正雄：Fuzzy Biometrics Vault Scheme を用いたテンプレートの安全性に関する一考察，暗号と情報セキュリティシンポジウム SCIS2005，pp.547–552 (2005).
8) Juels, A. and Sudan, M.: A Fuzzy Vault Scheme, *Proc. IEEE Int'l. Symp. Information Theory*, Lapidoth, A. and Teletar, E. (Eds.), p.408 (2002).
9) Juels, A. and Wattenberg, M.: A Fuzzy Commitment Scheme, *6th ACM Conf. Computer and Comm. Security*, Tsudik, G. (Ed.), pp.28–36 (1999).
10) Dodis, Y., Reyzin, L. and Smith, A.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, *Adv. EUROCRYPT 2004*, LNCS 3027, pp.523–540, Springer (2004).
11) Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R. and Smith, A.: Secure Remote Authentication Using Biometric Data, *EUROCRYPT 2005*, LNCS 3494, pp.147–163, Springer (2005).
12) 妹尾尚一郎，厚井裕司，貞包哲男，中谷直司，馬場義昌，鹿間敏弘：生体認証によるネットワーク個人認証システム，情報処理学会論文誌，Vol.44, No.4, pp.1111–1120 (2003).
13) Boudot, F.: Efficient Proofs that a Committed Number Lies in an Interval, *Proc. EUROCRYPT 2000*, LNCS 1807, pp.431–444, Springer (2000).
14) Fujisaki, E. and Okamoto, T.: Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations, *Proc. CRYPTO'97*, LNCS 1294, pp.16–30, Springer (1997).
15) Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S.: Handbook of Fingerprint Recognition, Springer Sccience + Buisiness Media (2003).
16) 福田剛志，森本康彦，徳山 豪：データサイエンスシリーズ 3 データマイニング，pp.131–150, 共立出版 (2001).
17) 麻生英樹：ニューラルネットワーク情報処理，pp.39–54, 産業図書 (1988).
18) Rumelhart, D.E., Hinton, G.E. and Williams, R.J.: Learning representations by backpropagating errors, *Nature*, Vol.323, pp.533–536 (1986).
19) NIST FINGERPRINT IMAGE SOFTWARE 2 (NFIS2). http://fingerprint.nist.gov/NFIS/

(平成 18 年 11 月 2 日受付)
(平成 19 年 4 月 6 日採録)

永井 慧

平成 18 年東海大学電子情報学部情報メディア学科卒業．現在，同大学大学院修士課程在学中．2006 年 CSS 論文賞受賞．情報セキュリティに関する研究に従事．

菊池 浩明（正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学大学院博士前期課程修了．1990 年（株）富士通研究所入社．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授，1997 年カーネギーメロン大学計算機科学学部客員研究員．2000 年東海大学電子情報学部情報メディア学科助教授，2006 年同大学情報理工学部教授，現在に至る．博士（工学）．ファジィ論理，多値論理，ネットワークセキュリティに興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞，2004 年情報処理学会研究開発奨励賞受賞．電子情報通信学会，日本ファジィ学会，IEEE，ACM 各会員．

尾形わかは（正会員）

1989年東京工業大学理学部物理学科卒業．1991年同大学大学院理工学研究科修士課程修了．1994年同大学院同研究科博士後期課程修了．1995年年姫路工業大学工学部助手．2000年東京工業大学理財工学研究センター助教授．2005年より同大学大学院イノベーションマネジメント研究科助教授．2007年4月より准教授．情報セキュリティおよび暗号プロトコルの研究に従事．博士（工学）．

西垣　正勝（正会員）

1990年静岡大学工学部光電機械工学科卒業．1992年同大学大学院修士課程修了．1995年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996年静岡大学情報学部助手．1999年同講師，2001年同助教授．2006年より同大学創造科学技術大学院助教授．2007年より准教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．