安全・安心・便利な社会を実現する生体認証基盤

—Public Biometric Infrastructure—

加賀 陽介 Kaga Yosuke　松田 友輔 Matsuda Yusuke　高橋 健太 Takahashi Kenta　長坂 晃朗 Nagasaka Akio

社会のIT（情報技術）化に伴うサイバー犯罪やテロ脅威の増加に伴い，安全を確保する個人認証手段として，生体認証が注目されている。しかし，生体認証は個人や組織単位での利用が多く，社会インフラとして広範に利用できる状況には至っていない。本稿では，生体認証を社会インフラにおける個人認証基盤として普及させるにあたっての課題を洗い出し，それらを解決するテンプレート公開型生体認証基盤（PBI）技術およびウォークスルー型指静脈認証技術を紹介する。これらの技術を適用することで，「手ぶら」で安全・安心な社会を実現することが可能となる。

1. はじめに

クラウドコンピューティングをはじめとする企業のICT（Information and Communication Technology）活用，各国における行政サービスの電子化や国民ID制度の導入などが進むにつれ，サイバー犯罪による被害が増加している。また，各国ではテロの脅威が増大し，都市における物理セキュリティの重要性が高まっている。このようなサイバー，フィジカルシステムを含む社会インフラにおけるセキュリティ対策において中核に位置する技術が，不正アクセスやなりすましを防止するための個人認証である。この個人認証技術の中でも高い安全性と利便性を両立可能な手法として，生体認証が注目されている。生体認証は，本人から静脈や指紋などの身体的・行動的特徴を読み取り，登録してある情報と照合することで本人確認を行う手法である。生体認証はパスワードやIC（Integrated Circuit）カードなどの従来の個人認証手法と比べ，紛失・盗難・忘却のリスクが低く，利便性が高い認証手法である。この生体認証を社会インフラにおけるさまざまなサービスの個人認証基盤として整備することで，カードもパスワードも不要な「手ぶら」で安全・安心な社会を実現することが可能となる。

しかし，生体認証を社会インフラとして普及させるためには，さまざまなサービスからの共通利用，生体情報のプライバシー・セキュリティの確保，認証時の利便性の向上という3つの課題がある。

(1) さまざまなサービスからの共通利用

現在使われている生体認証システムは，生体情報を単一のシステム内で管理することで安全性を確保している。しかし，このモデルでは複数のサービスシステムで生体認証を使う際に，システムごとの生体情報登録が必須となる。この登録の手間が生体認証普及の阻害要因の一つとなっており，生体認証を多種多様なサービスの個人認証手段として普及させるためには，さまざまなサービスから共通利用可能な認証基盤を開発する必要がある。

(2) 生体情報のプライバシー・セキュリティの確保

生体情報は人種，民族，健康状態などを特定できる可能性があるセンシティブ情報であり，プライバシーの観点から安全に保管することが求められる。また，生体情報は生涯不変で破棄・更新できない情報であり，一度漏えいすると，生体偽造やリプレイアタック※1）などによるなりすましの脅威が発生し，安全性の回復が非常に難しい。このようなセキュリティに対する脅威から利用者を守るため，生体情報の漏えいを防ぐ必要がある。

(3) 認証時の利便性の向上

社会インフラとして生体認証を浸透させていくためには，生体認証を使うことが不便を強いられるものであってはならない。そのため，誰もが迷わずに使いこなすことができる，直感的で分かりやすい，簡単な操作性が求められる。また，駅やビルといった大型施設や巨大なイベント会

※1）ネットワークを盗聴してIDやパスワードなどの認証情報を盗み，それを再利用してなりすましを試みる攻撃。

場など，たくさんの人々が一斉に集まる公共の場においても，待たされずスムーズに認証ができるスループットの高さと，確実な本人確認を実現する精度の高さの両立が不可欠である。

日立は，これらの課題 (1), (2) を解決する「テンプレート公開型生体認証基盤 (PBI：Public Biometric Infrastructure)」のコンセプトを提案し，その実現技術として生体署名技術を開発した[1), 2)]。さらに，課題 (3) を解決する「ウォークスルー型指静脈認証技術」の研究開発を進めている[3)]。

2. テンプレート公開型生体認証基盤 (PBI)

本章では，さまざまなサービスからの共通利用と，生体情報のプライバシー・セキュリティの確保を両立するテンプレート公開型生体認証基盤 (PBI)[1)] のコンセプトおよび実現技術 (生体署名技術[2)]) について説明する。

2.1 既存の生体認証の課題

既存の生体認証では，登録時に利用者から取得した生体情報を保管しておき，認証時に利用者から取得する生体情報と照合することで利用者当人であることの認証を行う。生体認証システムは，生体情報の保管・照合を行う場所に応じていくつかのモデルに分けられる (図1参照)。本節では，各モデルの概要とそれぞれの課題について述べる。

(1) ICカード内認証

銀行のATM (Automated Teller Machine) で用いるキャッシュカードのように，ICカード内に生体情報を保管する方式である。ICカード内の安全な領域に生体情報を置くことで，強固なセキュリティを実現できるが，ICカードを発行して認証時に持参する必要があるため，他のモデルに比べて利用者に応じたICカード発行・運用コストが発生する。

(2) 端末内認証

生体情報を取得するセンサー，あるいはセンサーと接続されたPC (Personal Computer) やモバイルデバイス内に生体情報を保管する方式である。端末のセキュリティは利用者に依存するため，常に安全な状態に保つのは困難であり，マルウェア感染などのリスクがある。このような安全性が低い端末に生体情報を保管した場合，漏えいの危険性が高まる。

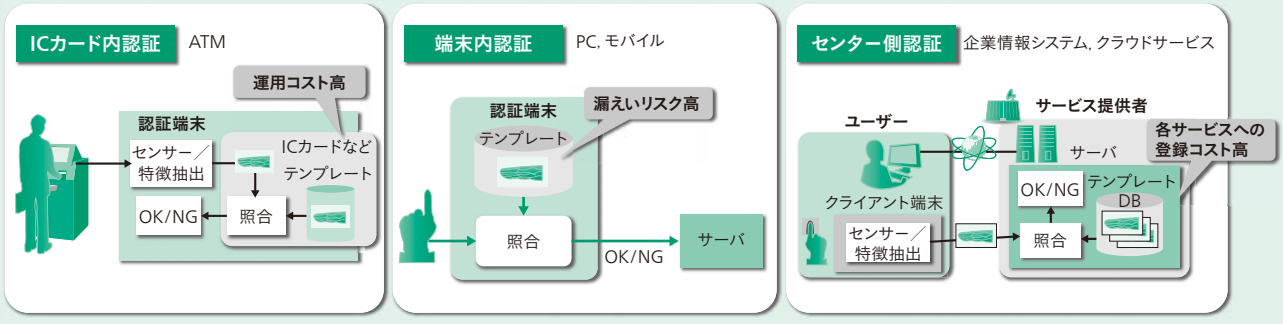
(3) センター側認証

端末とネットワークで接続されたセンター側に生体情報を保管する方式である。生体情報を各サービスのセンターへ登録するため，登録はサービスごとに行う必要があり，利用者の手間がかかる。また，多数の利用者の生体情報を一括管理することになるため，万が一生体情報が漏えいした場合には被害規模が大きい。

このように，既存の生体認証ではサービスごとに登録時に取得した生体情報を安全に保管する必要があるため，生体情報登録のコストや生体情報の漏えいリスクが課題となる。以降では，課題 (1) を解決することで生体情報登録コストを低減する生体認証基盤，および課題 (2) を解決することで生体情報漏えいリスクを低減する生体署名技術について説明する。

2.2 共通利用可能な生体認証基盤

本節では，複数のサービスからの共通利用が可能な生体認証基盤について説明する。テンプレート公開型生体認証基盤の概要を図2に示す。



注：略語説明　IC (Integrated Circuit)，ATM (Automated Teller Machine)，PC (Personal Computer)，DB (Database)

図1｜生体認証のシステムモデル

既存の生体認証には，ICカード内認証，端末内認証，センター側認証の3つのシステムモデルがあり，それぞれに運用コスト，漏えいリスク，登録コストなどの課題が存在する。

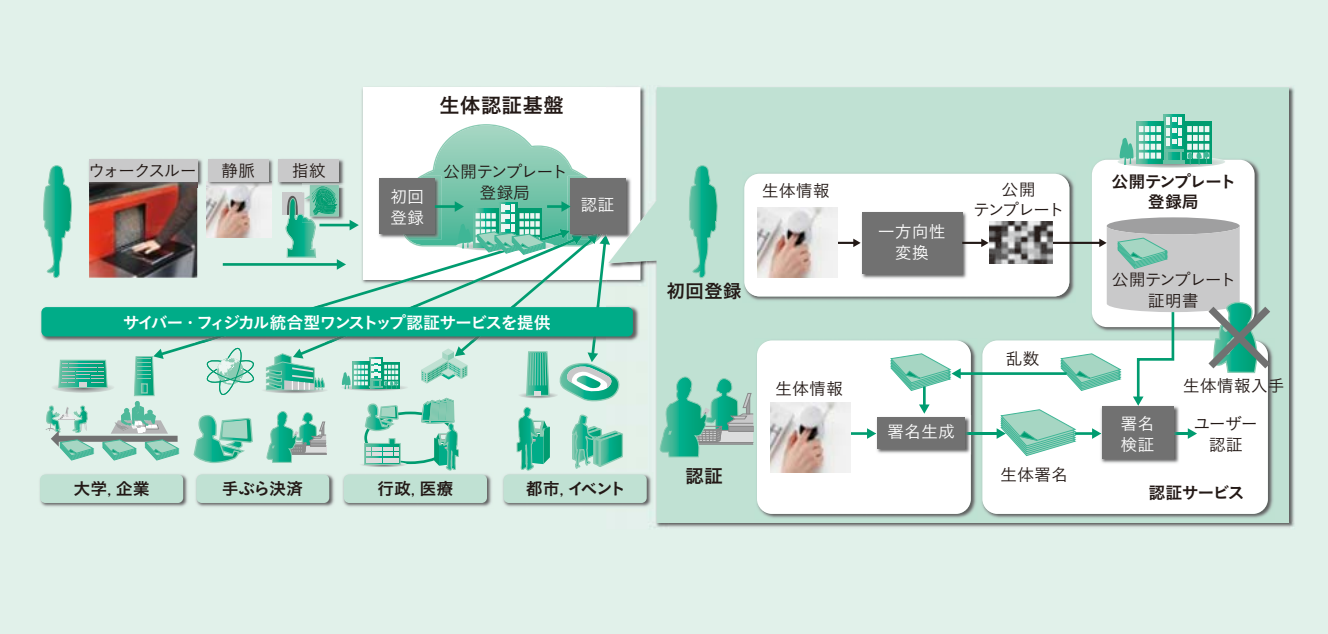


図2｜テンプレート公開型生体認証基盤の概要

利用者は1回だけ初回登録を実施し，公開テンプレート証明書を登録局へ登録する。登録された公開テンプレート証明書は，さまざまなサービスで共通利用可能であるため，登録の手間をかけずに複数のサービスを利用できる。

テンプレート公開型生体認証基盤では，公開テンプレート証明書の発行・管理を行う公開テンプレート登録局を新たに設置し，社会インフラとしての個人認証基盤を構築する。この個人認証基盤を共通的に利用することで，国民ID基盤，「手ぶら」の決済サービス，パスワードレスのクラウド認証，都市におけるフィジカルセキュリティなどにおける生体認証を個々のサービスへの登録なしで使うことができる。

利用者は，公開テンプレート登録局で身分確認を行ったうえで，初回登録を実施する。公開テンプレート登録局としては，例えば国民ID基盤では市役所，決済サービスでは銀行窓口，クラウド認証では各組織の情報部門などを想定する。この初回登録時では，利用者は生体情報に対して一方向性変換※2)を施して公開テンプレートを作成したうえで，公開テンプレート登録局へ提供する。得られた公開テンプレートに対して，登録主体である公開テンプレート登録局が署名を付与し，公開テンプレート証明書を発行する。この公開テンプレートは，一方向性変換によって元の生体情報の復元が不可能な形で保管されるため，公開しても生体情報を入手されるおそれはない。このため，さまざまなサービスから公開テンプレートを共通利用することが可能となる。

このような生体認証基盤を用いる場合のメリットについて考察する。生体認証基盤は，公開テンプレート登録局で証明書を保管して任意のサービスへ配信するモデルであり，一度の登録で得られた情報を複数のサービスから共通利用することが可能となっている。よって，課題（1）は解決されている。

2.3　生体情報を鍵とする電子署名技術（生体署名技術）

課題（2）で述べたリプレイアタックによるなりすましを防ぐ技術として，チャレンジレスポンス認証※3)がある。この技術で認証を行うことによって安全性を確保することが可能となるが，通常の電子署名ではICカードなどに秘密鍵を安全に保管する必要があり，ICカードの紛失・盗難，運用コストなどが課題となる。

日立は，生体情報を秘密鍵として用いることで，ICカードに代わって利用者自身の身体に秘密鍵を安全に保管できる生体署名技術を開発した。生体情報を鍵として用いるにあたって最も大きな問題は，生体情報に含まれる誤差である。従来のPKI（Public Key Infrastructure：公開鍵認証基盤）では，秘密鍵が1ビットでも異なると正しく認証・署名が行えない。しかし，生体情報はアナログ情報であり，読み取り時の誤差を許容する必要がある。そこで，生体署名技術を開発し，この問題を解決した（**図3**参照）。

生体署名技術では，まず初回登録において，生体情報から誤差が少なく安定的な特徴ベクトルであるファジー鍵を抽出し，ファジー鍵に対してファジー署名を用いて公開テンプレートを生成する。

次に，公開テンプレートを活用した認証を行う。認証時

※2) 元の情報を復元することが不可能であることが，数学的に証明されている変換。

※3) 公開鍵暗号による電子署名を用いて構成することができる，リプレイアタックなどに耐性を持つ認証方式。

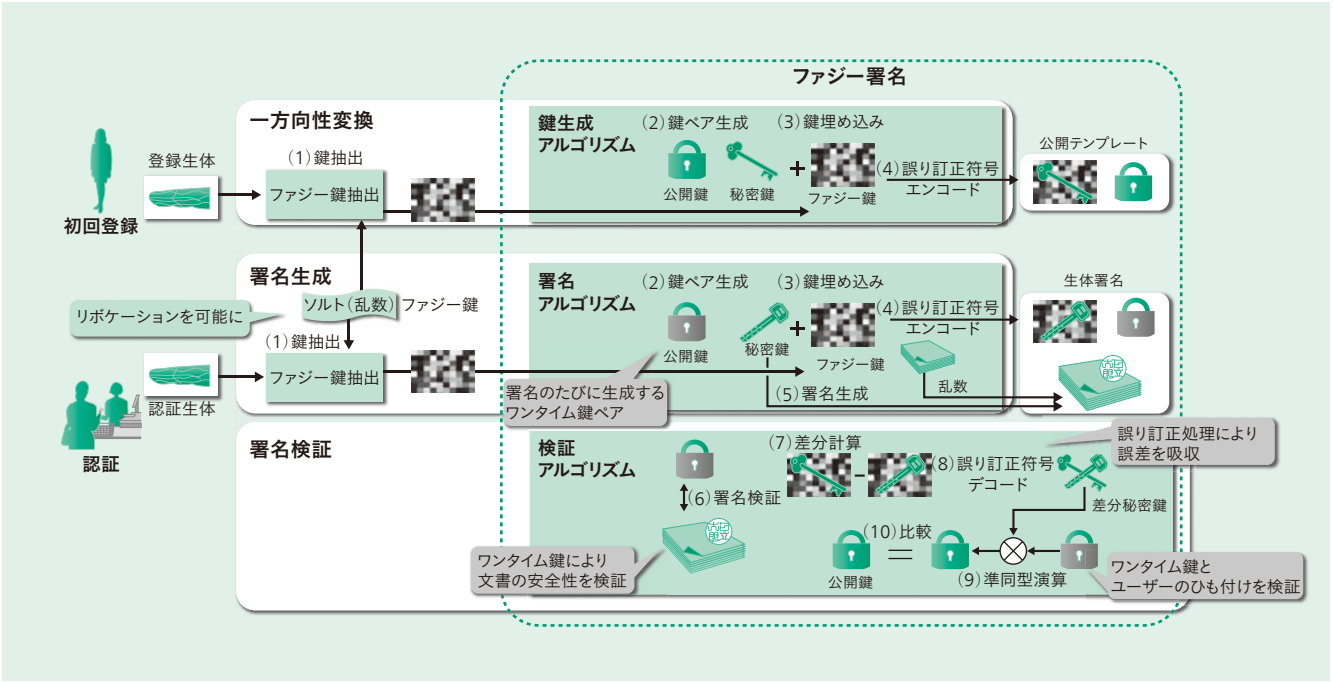


図3｜生体署名技術の概要

登録時には，登録生体からファジー鍵抽出を行い，ファジー署名における鍵生成を行うことで公開テンプレートを作成する。認証時には，認証生体からファジー鍵抽出を行い，ファジー署名における署名と検証を用いてチャレンジレスポンス認証を実施する。

には，登録時と同様に生体情報からファジー鍵を抽出した後，ファジー鍵を用いて乱数に対する生体署名を生成する。その後，公開テンプレートを用いて生体署名を検証することで，利用者の認証を行う。

以降で，初回登録時および認証時の具体的な処理について述べる。

2.3.1　初回登録時

まず，ファジー鍵抽出アルゴリズムによって生体情報から特徴抽出を行い，特徴ベクトルを生成する。一般に生体情報には多くの誤差が含まれるが，この特徴抽出によって誤差が少ないデータが得られる。次に，得られた特徴ベクトルに対してソルト（乱数）を付加し，秘密鍵データ（ファジー鍵）へと変換する［手順 (1)］。

次に，ファジー鍵を入力として，ファジー署名方式における鍵生成アルゴリズムによって公開テンプレートを生成する。鍵生成では，公開鍵と秘密鍵のペアを生成し［手順 (2)］，秘密鍵をファジー鍵の中に埋め込む［手順 (3)］。このとき，鍵ペア生成には，鍵の準同型性※4) を満たす既存の電子署名方式S(例えば，Waters署名[4])が用いられる。さらに，秘密鍵とファジー鍵が復元不可能な形に加工したうえで，誤り訂正符号※5) を付加し，公開鍵と合わせて公開テンプレートとする［手順 (4)］。

2.3.2　認証時

まず，初回登録時と同様の手順で，ファジー鍵抽出アルゴリズムによって利用者の生体情報からファジー鍵を生成する［手順 (1)］。

次に，ファジー署名方式における署名アルゴリズムと検証アルゴリズムを用いてチャレンジレスポンス認証を行う。

署名アルゴリズムでは，サーバ側から送信された乱数に対する生体署名を生成する。まず，電子署名方式Sに基づき，秘密鍵と公開鍵の鍵ペア（ワンタイム鍵ペア）を生成する［手順 (2)］。このワンタイム鍵ペアはランダムに生成されるため，毎回異なるデータが得られる。次に，ワンタイム秘密鍵をファジー鍵に埋め込む処理を行う［手順 (3)］。このワンタイム秘密鍵とファジー鍵を復元不可能な形に加工したうえで，誤り訂正符号を付加する［手順 (4)］。さらに，乱数に対して電子署名方式Sのワンタイム秘密鍵で署名を作成し［手順 (5)］，ワンタイム秘密鍵が埋め込まれたファジー鍵とワンタイム公開鍵を合わせて生体署名とする。

検証アルゴリズムでは，生体署名の正当性を検証する。まずワンタイム公開鍵によって乱数に対する署名を検証する［手順 (6)］。次に，公開テンプレート中の秘密鍵が埋め込まれたファジー鍵と，生体署名に含まれているワンタイム秘密鍵が埋め込まれたファジー鍵との差分を計算する［手順 (7)］。このとき，誤り訂正によって登録時と署名時の生体情報の誤差が吸収され，差分秘密鍵が生成される［手順 (8)］。この差分秘密鍵に基づく準同型演算によってワンタイム公開鍵を変換し［手順 (9)］，得られた結果と，公開テンプレート内の公開鍵とが一致すれば，生体署名が

※4) 暗号化したままで加算や乗算などの演算ができる性質。
※5) データの誤りを訂正するために付加する冗長なデータ。

正当なものであると判定する［手順（10）］。

以上のファジー鍵抽出，ファジー署名により，生体情報を鍵とする生体署名技術が実現する。

なお，生体署名技術の安全性に関しては，この方式を破って偽造や改ざんを行うことが十分に困難であることが数学的に証明されている。具体的には，生体署名の偽造困難性を，偽造困難性がすでに数学的に証明されているWaters署名[4]に帰着させることで安全性を示している[2]。よって，生体認証基盤の一方向性変換に生体署名技術を適用することで，課題（2）を解決することが可能となる。この生体署名技術を用いることで，電子決済や電子行政サービスで広く用いられているPKIと同等の認証や署名が，ICカードやパスワードを使わず生体認証に基づいて実現可能となる。

3. スムーズで正確な本人確認を実現する生体認証技術

本章では，たくさんの人々が一斉に集まる場所においてもスムーズで正確な認証ができる生体認証技術について述べる。

3.1 生体認証における利便性

日立は，これまでにも指の静脈パターンに着目した生体認証技術を開発し，金融向けや入退管理・情報セキュリティ用途に製品化している。この指静脈認証技術は，所定の位置に生体を提示すれば，高い認証精度を得ることができる。そのうえ，静脈は生体内部に存在する特徴であるため偽造が困難であるというメリットがある。

しかし，認証するためにユーザーは立ち止まって所定の位置に指を提示する必要があり，認証動作をスムーズに行うことが難しかった。高い認証精度と利便性の両立のためには，短時間の簡単な操作で正確な本人確認を行う必要がある。

そこで，高精度であり，かつ耐偽造の面で優れている指静脈認証を基本としつつ，歩きながらスムーズな動作で本人確認が可能な新しい生体認証技術を開発した。

3.2 ウォークスルー型指静脈認証技術

指静脈認証技術は，近赤外光を指に照射して生体内を透過した光を撮像して得られる静脈特徴を用いる。この技術をさらに進化させ，歩きながら指をかざすという直感的かつ簡単な操作でスムーズに本人確認ができるウォークスルー型指静脈認証技術を開発した（**図4**参照）。

今回，試作した認証装置の構成を**図5**に示す。提案手法の概要は，まず，距離センサー［3D（Three-dimensional）センサー］を利用して指の位置および姿勢を検知する。次に，指の位置や姿勢に応じて光源を制御し，静脈を撮影する。最後に，静脈画像から抽出した複数の指の静脈パターンとあらかじめデータベースに登録されている静脈パターンを照合し，認証判定を行う。提案手法の要点は以下のとおりである。

（1）歩行を妨げない開放的なインタフェース
（2）指の位置・姿勢に応じた光源制御による静脈撮影
（3）複数の指静脈パターンを用いた高精度化

まず，歩きながらスムーズに手をかざして認証できるようにするため，装置の上方，およびユーザーの進行方向（側方）を開放的にした装置形状とした。

歩きながらかざす指の位置・姿勢は変動しやすく，その下でも安定に静脈パターンを撮影するため，複数の光源（光源アレイ）を用いる。指の位置および姿勢の変動が大きいと単一光源からの光は指に届かない場合があり，鮮明

図4｜ウォークスルー型指静脈認証装置の外観
開放的なインタフェースによって歩きながらでも指をかざして認証が可能である。

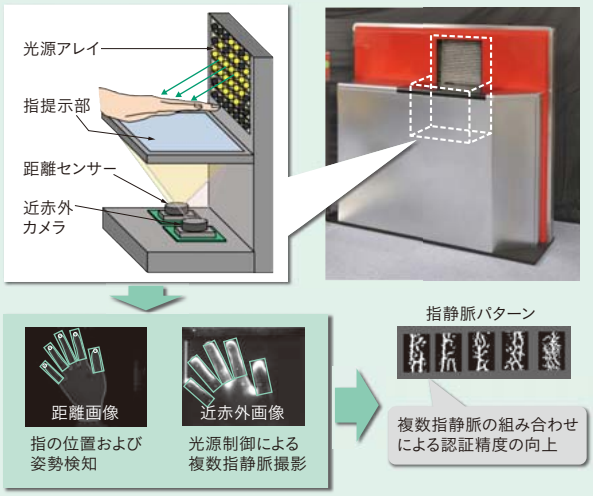


図5｜認証装置の構成および認証の概要
距離センサーを用いて指の位置および姿勢を検知し，光源アレイを適応的に制御して瞬時に取得した複数の指静脈パターンで認証を行う。

な静脈の撮影が難しい。そこで，指の位置・姿勢に応じて複数の光源を制御し，点灯する光源を決定することで，位置や姿勢変動にロバストな静脈撮影が可能となる。

認証精度の高精度化のため，複数の指を用いる。**図4**の認証装置は，指を1本のみ撮影する従来の認証装置と比べて指提示部が広く，同時に複数の指が撮影できる。したがって，複数指の静脈画像を利用して照合を行うことで認証精度が向上する。

開発した技術のスループットと認証精度を確認するため，同図に示した試作装置を用いて原理実験を行ったところ，最大で1分当たり70人が認証可能なことを確認した。また，まだ少数データによる精度評価ではあるが，上述のスループットを可能にしながら，現在，製品化されている認証装置と同程度の精度が得られた。今回開発したウォークスルー型指静脈認証技術は，従来にない高い利便性を提供するセキュリティ技術として，幅広い用途が期待できる。今後は，開発した技術をセキュリティソリューションの中核として，さらなる事業拡大をめざす。

4. おわりに

本稿では，生体認証を社会インフラの個人認証基盤として普及させていくために必要な技術として，テンプレート公開型生体認証基盤（PBI）とウォークスルー型指静脈認証について説明した。これらの技術を活用することにより，カードやパスワードを使わなくても「手ぶら」で安全・安心な社会を実現することが可能となる。

今後も日立は，生体認証をはじめとするサイバー／フィジカルセキュリティに関する研究開発を推進し，利便性が高く安全・安心な社会の実現に貢献していく。

参考文献など

1) 高橋，外：テンプレート公開型生体認証基盤，2012年 暗号と情報セキュリティシンポジウム（SCIS 2012）(2012)
2) 高橋，外：秘密鍵に曖昧さを許す証明可能安全な電子署名と，テンプレート公開型生体認証基盤への応用，2013年 暗号と情報セキュリティシンポジウム（SCIS 2013）(2013)
3) 日立ニュースリリース，スムーズで正確な本人確認を実現するウォークスルー型指静脈認証技術を開発 (2014.12)，http://www.hitachi.co.jp/New/cnews/month/2014/12/1208a.html
4) B. Waters: Efficient Identity-Based Encryption Without Random Oracles, In EUROCRYPT 2005, Vol. 3494 of LNCS, pp. 114–127 (2005)

執筆者紹介

加賀 陽介
日立製作所 研究開発グループ 基礎研究センタ I3プロジェクト 所属
現在，生体認証に関する研究開発に従事
電子情報通信学会会員

松田 友輔
日立製作所 研究開発グループ システムイノベーションセンタ セキュリティ研究部 所属
現在，画像認識，生体認証の研究開発に従事
電子情報通信学会会員

高橋 健太
日立製作所 研究開発グループ システムイノベーションセンタ セキュリティ研究部 所属
現在，生体認証の研究開発に従事
博士（情報理工学）
電子情報通信学会会員，情報処理学会会員

長坂 晃朗
日立製作所 研究開発グループ システムイノベーションセンタ 所属
現在，生体認証に関する研究開発に従事
博士（工学）
電子情報通信学会会員