生体データの保護や管理を容易にできる生体認証技術

Biometric Authentication Technology Facilitating Protection and Management of Biometric Data

山田　茂史　　青木　隆浩　　下山　武司　　森　樹久

あらまし

近年，国内における改正個人情報保護法（2017年5月施行）やEU一般データ保護規則（2018年5月施行）などの法律の改正によって，個人データを安全に管理するニーズが高まっており，生体認証に利用する生体データもその対象となっている。生体データの活用に当たっては，生体データの保護を強化しながら容易にデータを取り扱えるようにする生体データ保護技術が注目されている。しかし，本技術は生体データの漏えいに対するセキュリティと生体認証としての認証精度の両立が難しいといった課題がある。これに対して，富士通研究所では強みである手のひら静脈認証技術を用いて，静脈パターンの変形にロバストな生体データ保護技術を開発した。本技術は，生体データの保護や管理を容易にできるため，システム側での生体データの集中管理が必要な手ぶら認証を利用した本人認証サービスの拡大への貢献が期待できる。

本稿では，手のひら静脈認証技術とIDを入力せずに生体データのみで認証を行う手ぶら認証などの活用事例について述べる。

Abstract

Recently, amendments to laws such as the Amended Act on the Protection of Personal Information (implemented in May 2017) in Japan and the General Data Protection Regulation in the EU (implemented in May 2018) have been increasing the need for safe management of personal data, with biometric data used for biometric authentication also falling under this scope. In utilizing biometric data, biometric data protection technology that allows for the easy handling of data while strengthening biometric data protections is attracting attention. However, there is a problem with this technology, with it difficult to achieve both security against biometric data leaks and accuracy in the provided biometric authentication. To deal with this issue, Fujitsu Laboratories has taken advantage of its palm vein authentication technology, one of its strength, to develop a biometric data protection technology that is robust against vein deformation. This technology facilitates the protection and management of biometric data and is expected to contribute to the expansion of personal authentication services that make use of empty-handed authentication, which requires centralized management of biometric data in the system. This paper presents examples of use of palm vein authentication technology and empty-handed authentication, which only requires biometric data for authentication without the need to enter IDs.

1. まえがき

近年，生体認証の利用が社会に浸透し，各種決済，ATM，入出国管理，PCへのログイン，SSO（シングルサインオン）など，様々な分野で利用されている。このような生体認証に用いる特徴データ（登録・照合データ）は，2017年5月に施行された改正個人情報保護法のもとで個人情報（個人識別符号）として明確化されており，データの取り扱いについて配慮が必要である。また，欧州では2018年5月に施行されたEU一般データ保護規則（GDPR：General Data Protection Regulation）[(1)]は，生体データを含む個人データの保護を目的としている。これらの法令の施行を受けて，生体データの保護を強化しながら活用する生体データ保護技術が注目されている。[(2)] 生体認証技術の国際標準化を行うISO/IEC JTC1 SC37（生体認証）においても，ISO/IEC 30136として生体データ保護技術をテストするための規格が新たに作成された。[(3)]

こうした背景から，富士通研究所では生体データの保護を強化する手のひら静脈認証技術を開発した。本技術は，生体データの保護や管理が容易になるため，システム側での生体データの集中管理にかかる負担やリスクが軽減できる。これによって，スマートフォンやカードがなくても利用できる手ぶら認証を利用した本人認証サービスの拡大への貢献が期待できる。

本稿では，まず生体データの保護を容易にするための富士通研究所独自の生体データ保護技術を述べる。そして技術の応用として，カードレス・キャッシュレス社会が進む中で利便性の高さから広がる手ぶら認証など，手のひら静脈認証を利用した本人認証ソリューションの活用事例を紹介する。

2. 生体データ保護のニーズ

生体認証の利用が拡大するにつれて，認証システムの中で生体データをより安心・安全に取り扱いたいというニーズが高まっている。システム提供者は，通常暗号化などによって生体データを安全に管理している。その一方で，生体認証アルゴリズムの普及が進み，同じ生体認証アルゴリズムを利用したほかのシステムで万が一登録データが漏えいした場合に自社のシステムへの影響が心配となる。

利用者の観点では，生体認証の普及によって様々な場所での認証で生体認証が利用できるようになって利便性が向上する。反面，様々なシステムに自身の生体データを登録するのは不安という思いもある。このように，システム提供者と利用者のいずれも，生体認証をより安心・安全に利用できることを期待している。

このような状況の中，生体データをより安心・安全に取り扱うことを目的とした生体認証技術として，生体データ保護技術が提案されている。[(4)] 生体データ保護の安全性および性能の要件としては，以下の四つが挙げられる。

(1) Irreversibility

生成された登録・照合用の特徴データから，元の生体データの類推ができないこと。

(2) Un-linkability

利用者のプライバシーを保護するために，システムで用いられている特徴データを用いて，ほかの生体認証システムの特徴データと照合ができないこと。

(3) Diversity（Renewability）

同じ生体データから異なる特徴データを生成可能であること。また，漏えいした特徴データを利用不可にして，新しい特徴データを登録し直すことができること。

(4) Performance

上記の条件を満たすに当たり，生体認証としての認証精度や処理性能を劣化させないこと。

生体データ保護技術の研究開発では，2001年に米IBMのRathaらによる，一つの生体データから複数種類の登録・照合用の特徴データを生成可能にする「キャンセラブルな生体認証」が知られている。[(5)] 欧州においては，生体データ保護技術の研究開発のためのTURBINE（TrUsted Revocable Biometric IdeNtitiEs）Research Projectが，欧州プロジェクトFP7の枠組みで2007年から2010年まで進められていた。

生体データ保護技術は多数提案されているものの，実用化された技術は指紋や指静脈を用いたもの

にとどまっている。[6], [7] 開発された多くの技術が，保護する対象の特徴データとして0と1からなるバイナリコードを前提としている。生体データのパターンそのものは終生不変であるが，センサーを通じて取得された生体データには，変形やノイズの混入などによって揺らぎが生じる。そのため，生体データから抽出したバイナリコードは完全に一致することはない。画像パターンの比較により一致度合を評価するパターン照合をベースとした既存の認証アルゴリズムと比べて，バイナリコードを用いた認証アルゴリズムでは，生体データの揺らぎによる認証精度への影響が大きく，認証精度の向上が実用化に向けた課題となっている。

3. 富士通研究所独自の生体データ保護技術

富士通研究所では，つながる社会を支えるための認証技術として，生体データの保護をより簡便にする生体データ保護技術の研究開発を進めてきた。今般，富士通の強みである手のひら静脈認証を暗号化技術と融合することによって，静脈データを暗号化したまま登録・照合でき｛前章（1）の要件｝，かつ一つの手のひらから異なる登録・照合用の特徴データを生成でき｛前章（2）（3）の要件｝，従来の製品技術相当の認証精度と処理性能を有する｛前章（4）の要件｝，新しい手のひら静脈認証技術を実現した。

筆者らは，既存の暗号化技術で生体データのパターンを照合できるようにするために，手のひら静脈画像から0と1で表されるバイナリコードとして特徴データを抽出する技術と，既存の暗号技術を利用した生体データ保護機能を開発した。

以下に本技術の特長を示す。

3.1 揺らぎのある手のひら静脈のパターンから安定したコードを生成

筆者らは，静脈センサーを用いて取得した手のひら静脈画像の揺らぎを吸収するバイナリ特徴データ生成技術を開発した。これは，世界トップレベルの高い認証精度｛本人拒否率0.01％（リトライ1回含む），他人受入率0.00001％以下｝を実現している手のひら静脈認証技術をベースにしている。

手のひら静脈画像からバイナリ特徴データを生成する手順を**図-1**に示す。まず，手のひらの丸まり（3次元的な変形）を二次曲面でフィッティングし，それを平面に広げて画像を正規化するために補正する。これによって，手のひらの傾きや丸まりを補正できる。次に正規化後の手のひら静脈画像に対して静脈抽出を行う。これは現行の製品技術を利用して，手のひら静脈の特徴的な領域を複数検出する。そして，それぞれの領域から特徴成分を抽出し，バイナリコードに変換する。

これらの処理を行う際に，特徴成分の信頼性が低い領域を除外することで，生成されるバイナリコードの再現性を向上できる。最終的に，複数領域から生成したバイナリコードをまとめてバイナリ特徴データとする。これらのバイナリコードに対して，後述する暗号化処理を適用する。照合処理では，登録側と照合側の複数のバイナリコードをそれぞれ対応づけて比較することで，部分的な変形を吸収できる。

以上の技術によって，手のひらの変形の影響を低減するとともに高い認証精度を実現できる。

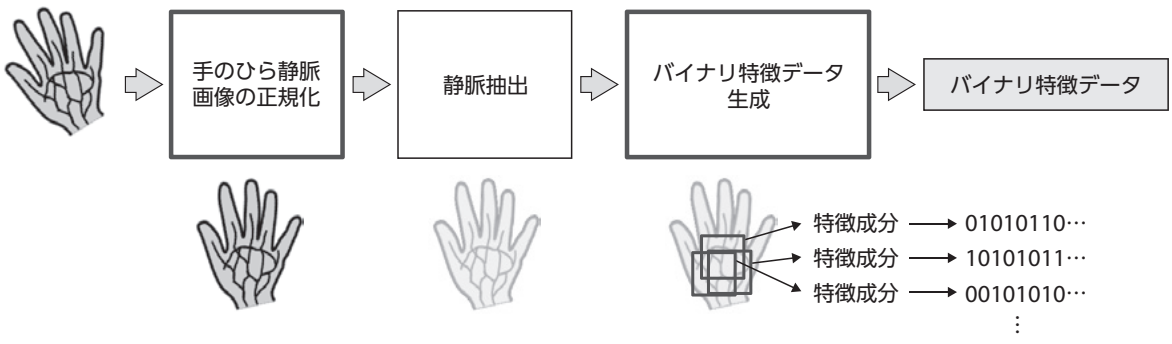


図-1　バイナリ特徴データ生成

3. 2 生体データ保護の実現

登録・照合用データの生成時に補助情報（暗号鍵のシードに相当）に基づいて暗号化する処理と，暗号化したままコードの比較演算（ハミング距離）による照合処理を，既存の暗号化技術を利用して実現した（図-2）。暗号鍵のシードとして入力する補助情報を認証システムごとに切り替えることで，同じ生体データから複数の異なる暗号化特徴データの生成を可能にした｛図-3（a)｝。

同じ人の暗号化特徴データであったとしても，異なる補助情報で暗号化されているため，これらを照合したとしても認証に成功しない。更に，万一のデータ漏えい時にも，認証システムに格納された全ての登録データについて，一括して補助情報を切り替えて変換する｛図-3（b)｝。漏えいしたデータを利用してなり済ましを行ったとしても，認証されることはない。こうして，利用者による再登録を不要にすることで，手ぶら認証などの利用が多い大規模な認証システムにおいても，シームレスに運用を継続できる。

4. 手のひら静脈認証を利用した本人認証ソリューションの事例

本章では，手のひら静脈認証 FUJITSU 生体認証 PalmSecureを利用した手ぶら決済など，IDレス認証の事例を紹介する。

（1）カードレスATM：大垣共立銀行様[8]

手のひら静脈認証を利用したカードレスATMを国内で初めて実現した事例である（2012年9月稼働）。2011年に発生した東日本大震災の際には，多くの被災者の方が通帳やキャッシュカードを紛失されたため，必要な資金を即座に引き出せなかった。大垣共立銀行様は，これを業界の課題と捉え，通帳・カードなどの本人と口座とをひも付けるモノがなくても利用できる金融サービスが必要と考えられた。

従来のATMで利用される生体認証は，ICカードのセキュリティ強化としての役割が強く，ICチップ内に生体データを保存していた。カードレスATMでは，静脈データをシステムに保存して管理するため，通帳やカードがなくても本人の口座を特定し，ATMで取引ができるようになった。物理的

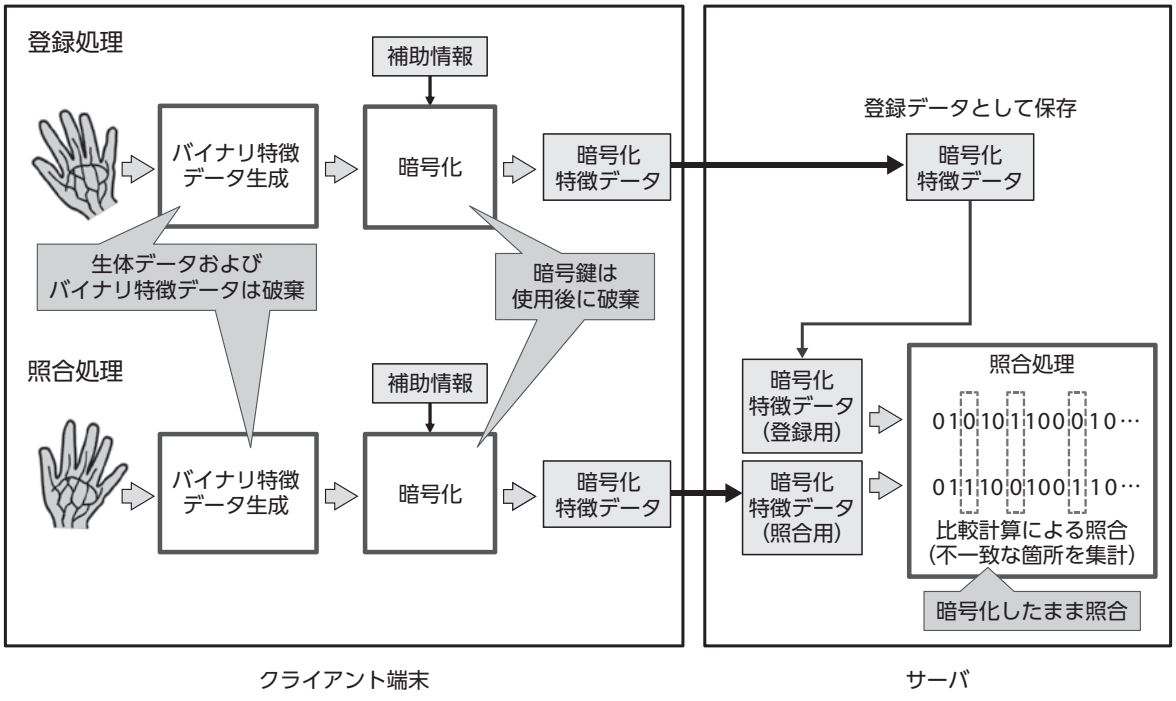
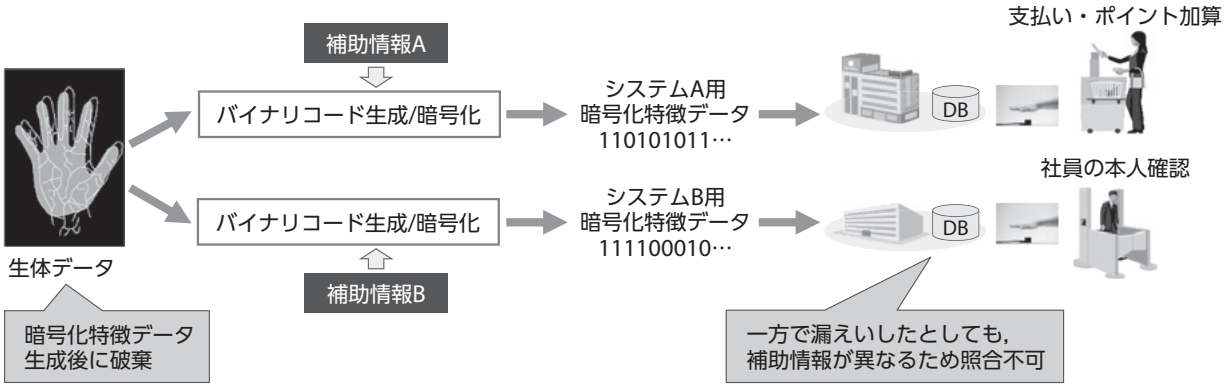
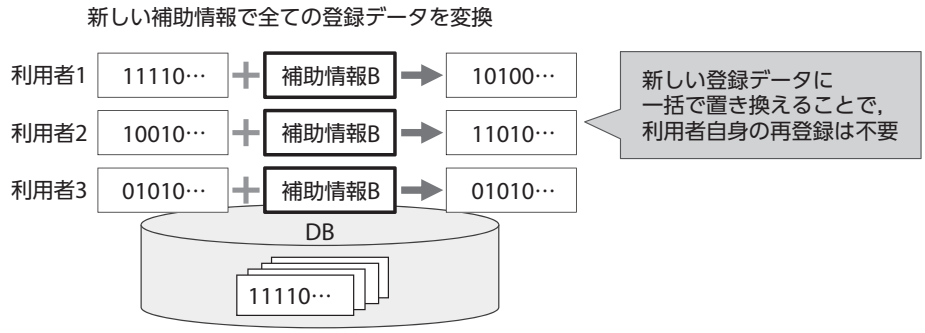


図-2　生体データ保護の仕組み



(a) 異なるシステムで照合できない（Un-linkability）



(b) データ漏えい時の補助情報の切り替え

図-3　生体データ保護の効果

なモノ（通帳，カード）を必要としないため，今まで不可能であった被災時・避難時においても，ATMサービスの継続が可能となった。

(2) LOTTE CARD様/韓国セブンイレブン様[9]

韓国セブンイレブン様における，LOTTE CARD会員様向けに手ぶらショッピング「Hand Pay」を開始した事例である（2017年5月稼働）。Hand Payは，現金・カード・スマートフォンなどを携帯していなくても，自身の身体と電話番号だけで本人認証・決済ができる利便性の高いサービスである。手のひら静脈認証は生体データを利用するため，改ざんやなり済ましが非常に困難である。静脈データはシステムに登録されるため，店舗をまたいだ決済が可能である。Hand Pay導入店舗の拡大によって，更なる利便性の向上につながる。

本技術は，生体データを容易に管理できるため，システム側での生体データの集中管理が必要な手ぶら認証に適している。本技術によって，手ぶら認証の更なる拡大に貢献する。

5. むすび

本稿では，生体データの保護を容易にするための富士通研究所独自の生体データ保護技術について述べた。また，カードレス・キャッシュレスなど利便性につながる手ぶら認証など，手のひら静脈認証を利用した本人認証ソリューションの活用事例を紹介した。

今後は，本技術を活用した様々なユースケースを検討して実証につなげていく。そして，実証を通じて認証精度・セキュリティ機能の改善，更にシステム適用する際に必要となる周辺技術の拡充を図る。

参考文献

(1) REGULATION（EU）2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE

COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC（General Data Protection Regulation）.
(2) ISO/IEC 24745:2011：Information technology -- Security techniques -- Biometric information protection.
https://www.iso.org/standard/52946.html
(3) ISO/IEC 30136:2018：Information technology -- Performance testing of biometric template protection schemes.
https://www.iso.org/standard/53256.html
(4) Anil K. Jain et al.：Biometric Template Security. EURASIP Journal on Advances in Signal Processing, 2008.
(5) Ratha N. et al.：Enhancing security and privacy in biometrics based authentication systems. IBM Systems Journal 40, p.61-634, 2001.
(6) Genkey：BioHASH.
https://www.genkey.com/privacy-by-design/
(7) 株式会社 日立システムズ：SHIELD PBI指静脈認証サービス.
https://www.hitachi-systems.com/solution/s0307/pbi/
(8) 富士通フロンテック：全国初！通帳・カードレスを実現 大垣共立銀行様、手のひら静脈認証によるATM運用を開始.
http://www.fujitsu.com/jp/group/frontech/resources/news/press-releases/2012/0926.html
(9) 手のひら静脈認証装置を韓国の決済市場へ提供～韓国富士通が生体認証決済市場へ本格参入～.
http://www.fujitsu.com/jp/group/frontech/resources/news/press-releases/2017/0529.html

著者紹介

山田　茂史（やまだ　しげふみ）
（株）富士通研究所
デジタル革新コア・ユニット
生体認証技術の研究開発に従事。

青木　隆浩（あおき　たかひろ）
（株）富士通研究所
デジタル革新コア・ユニット
生体認証技術の研究開発に従事。

下山　武司（しもやま　たけし）
（株）富士通研究所
セキュリティ研究所
暗号技術の研究開発に従事。

森　樹久（もり　しげひさ）
富士通（株）
共創ビジネスグループ
手のひら静脈認証PalmSecureの販売推進に従事。