

指静脈認証技術を活用した 非接触型認証ソリューション

デジタル化の進展に伴い、生活の利便性が向上する一方、なりすましなどによる情報漏洩、業務妨害といった脅威も増加している。こうした中、本人認証手段としての生体認証が注目されて久しい。中でも、日立の指静脈認証技術は高い認証精度を持ち、金融機関や小売店舗での決済、各種業務での本人認証など、多くの導入実績がある。

日立は、これらの生体認証技術をより安心・安全に活用できるよう、生体情報を保護するテンプレート公開型生体認証基盤（PBI）を発明した。さらに、PBIを中核にニューノーマルの働き方や生活様式に対応する、非接触型認証ソリューションを新たに提供開始した。今後、さまざまなパートナーと連携して幅広い分野のニーズに合わせて提供し、一層の普及をめざしていく。

高谷 学 | Takatani Manabu

鈴木 彦太郎 | Suzuki Hikotaro

椿 直樹 | Tsubaki Naoki

松木 譲介 | Matsuki Josuke

山口 光博 | Yamaguchi Mitsuhiro

1. はじめに

2019年に発生したCOVID-19が一つの契機となり、テレワークやキャッシュレス決済など、ニューノーマルと称される、デジタル技術に支えられた生活様式の浸透が加速している。この環境下では、なりすましなどによる情報漏洩、業務妨害といった脅威から組織や個人を守るべく、離れた環境でも確実に本人認証を行うことが高レベルで求められる。

こうした中、確実な本人認証を実現する技術として生体認証が着目され、適用が広がっている。日立は、これまで多方面に導入実績を持ち、高い精度で本人認証が可能な指静脈認証技術を活用した、非接触で大規模認証が可能な指静脈認証装置と、PCカメラ向け生体認証ソフトウェア開発キットを開発し、提供を開始した。

本稿では、これらの製品と、テンプレート公開型生体認証基盤（PBI：Public Biometric Infrastructure）技術を活用したニューノーマル対応ソリューションと今後の展開について述べる。

2. PBIで広がる安心で便利な生体認証

2.1

指静脈認証技術

生体認証には指紋や顔、静脈、虹彩などを用いる方式がある。特に静脈は他の生体情報と比較して経年変化が小さく、十分な複雑性があり認証精度が高い。

日立は、1997年から指静脈認証技術の基礎研究を開始し、2002年に入退室管理分野の製品の販売を開始した。その後も、金融分野、行政サービスなど国内外の幅広い分野へ市場を広げている¹⁾。

2.2

生体認証技術の課題

個人情報保護法やGDPR（General Data Protection Regulation：EU一般データ保護規則）²⁾によって、生体情報を安全に管理することがベンダーやサービス提供者に義務付けられている。

特に電子決済やインターネットバンキングなどでは、公開鍵暗号基盤（PKI：Public Key Infrastructure）の秘密鍵によって電子署名を発行するが、秘密鍵と利用者の生体情報の組を安全に管理するために、IC（Integrated Circuit）カードなどのHSM（Hardware Security Module）に保管する形態が広く普及している³⁾。しかし、これらの形態では、物理媒体の発行コストがかかるだけでなく、紛失時に郵送などの手段で再発行手続きをする必要があり、サービス提供者・利用者ともに金銭的、時間的コストが負担となっている。

2.3

生体情報を鍵とする電子署名技術

前節で述べた課題に対して、日立では、「テンプレート公開型生体認証基盤」⁴⁾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。以下では、図1に基づきPBIの特徴を説明する。

(1) 登録処理

PBIでは登録時に利用者の生体情報を撮影し、ファジー鍵抽出アルゴリズムによってファジー鍵と呼ばれる情報を生成する。一般的に、生体情報には撮影のたびに变化する位置や姿勢、外光などの揺らぎが含まれるが、このファジー鍵抽出アルゴリズムにより安定した情報に変換できる。

次に、別途生成したPKIの鍵ペアのうち秘密鍵をファジー鍵により秘匿し、公開テンプレートと呼ばれる情報を生成する。秘密鍵の秘匿には特殊な誤り訂正符号が使われる。この処理は一方方向性変換の特性があり、公開テンプレートからファジー鍵を復元することは困難である。

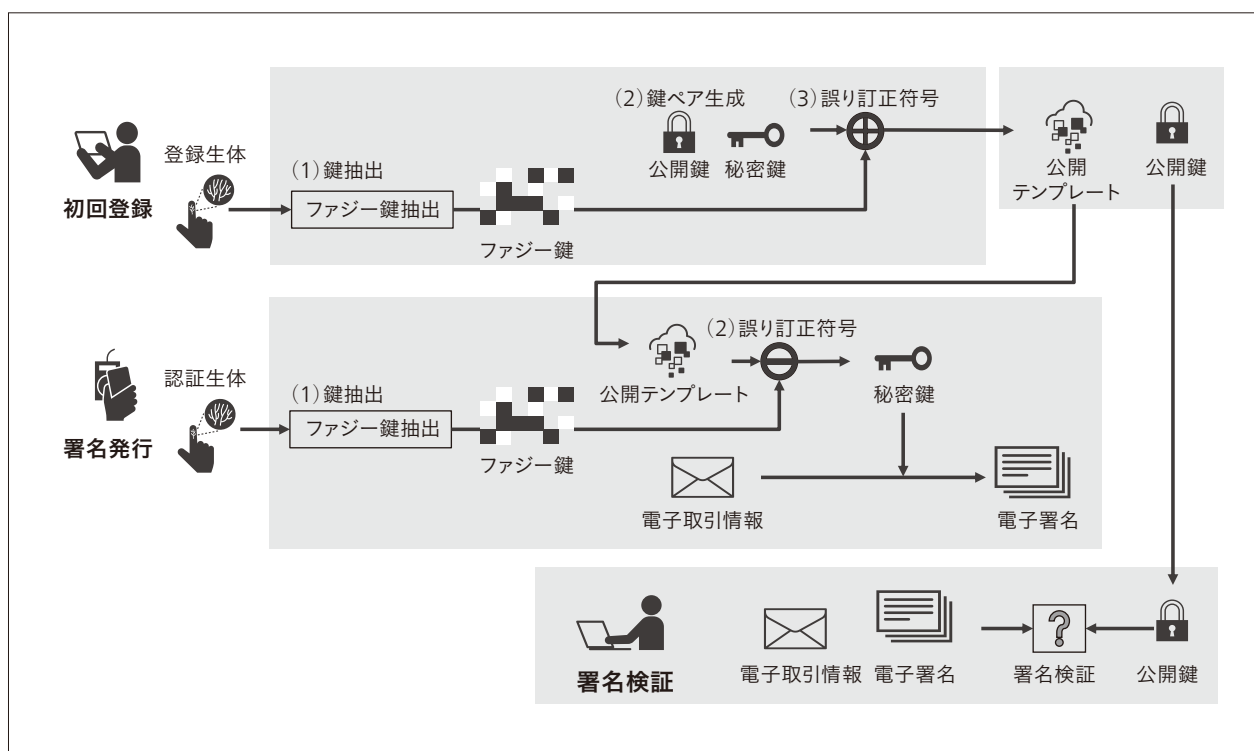
(2) 署名処理

電子取引情報にPBIで電子署名を発行するには、登録時と同様、利用者の生体情報からファジー鍵を抽出する。このファジー鍵を公開テンプレートと組み合わせて誤り訂正符号処理をすることでPKIの秘密鍵を一時的に復元する。

生体認証基盤に登録した公開鍵と復元した秘密鍵が対になっていれば、PKIの電子署名と同様に秘密鍵で電子取引情報に電子署名を発行できる。このとき、登録時と認証時のファジー鍵の誤差が十分小さくなければ秘密鍵の復元に失敗するため、利用者本人以外がPKI秘密鍵を

図1 | PBIの仕組みと特徴

PBI（Public Biometric Infrastructure）において、誤り訂正符号処理は一方方向性変換の性質を持つため、公開テンプレートから認証生体やファジー鍵の復元は困難である。また、認証時において、登録時と異なる生体から抽出したファジー鍵では秘密鍵の復元に失敗する。この性質により、秘密鍵は本人以外使用不可である。



入手することは困難である。

(3) 署名検証時

(2) で発行した電子署名は生体認証基盤のPKI公開鍵を使うことで、PKIの署名検証と同様の処理によって電子取引情報の完全性を確認することができる。

このように、これまでの生体認証製品にPBIを組み合わせて、ICカードなどのHSMを用いることなく、生体情報と秘密鍵の安全な管理が可能となる。

2.4

PBIによって広がる日立の生体認証

前節で解説したように、日立の生体認証製品にPBIを組み合わせることで、HSMを用いることなく生体情報と秘密鍵の安全な管理が可能となる。

PBIの持つ「生体情報保護」と「生体による電子署名」の二つの特徴はFinTech分野と特に相性がよく、金融機関の窓口やATM（Automated Teller Machine）で採用実績がある。

3. ニューノーマルの生活様式に応じた非接触でセキュアな認証ソリューション

PBIの登場により、ATMや銀行窓口業務、店舗での電子決済など、生体認証が提供できる価値や適用分野は劇的に拡大した。さらに、2019年に発生したCOVID-19の影響によって進展したニューノーマルの生活様式においては、不特定多数の利用者が想定される分野に対応可能な非接触かつ大規模な認証製品が求められている。

日立は、これらの市場動向を踏まえて、「日立指静脈認証装置C-1」、「日立カメラ生体認証SDK（Software Development Kit） for Windows^{※1)} フロントカメラ」を開発し、幅広いニーズに対応しようとしている。本章で

はこれらの製品について解説する。

3.1

日立指静脈認証装置C-1

日立は、これまでに複数の指静脈認証製品を開発しているが、いずれも1:N認証^{※2)}を用いた1人～数百人までの認証精度の小規模認証向け製品であり、手ぶらキャッシュレス決済やイベント会場の入退管理などの大規模認証に対応するにはさらなる高精度化が必要であった。また、既存の小規模認証では、限られた利用者が同一装置を利用するため問題とならなかったが、大規模認証では不特定多数の利用者が同一の装置を利用するので、COVID-19などの感染症を拡大させないために非接触で利用できるようにする必要があった。このような背景から、高精度かつ非接触で利用可能な大規模認証装置として指静脈認証装置C-1を開発した。

指静脈認証装置C-1では、高い認証精度を実現するために、従来は指1本で行っていた指静脈認証を指3本で行うこととした。指を3本使用することで、認証に利用できる情報量が大幅に増加し、高い認証精度を実現することができた（図2参照）。

また、非接触でも指3本をスムーズに読み取ることができるように、従来のように指の上から赤外LED（Light-emitting Diode）光を照射する構造ではなく、指の下側からLED光を照射する開放型の構造とした。非接触の開放型装置としたことで、従来機種よりも周囲の環境や指のかざし方の影響を受けるようになったが、新しく開発した高感度撮影方式とロバスト性に優れた認証アルゴリズムによって、これらの問題を解決した。

※1) Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標および商標である。

※2) 生体情報だけを用いて個人を識別する生体認証方式。

図2| 従来製品とC-1の外観比較

従来製品では天蓋付きの筐体を使用し、天井に配置したLED（Light-emitting Diode）の透過光で静脈パターンを撮影していた。C-1では不特定の利用者が共通の装置を使用することを想定し、天蓋なしの開放型筐体で内部からLED光を照射する反射光方式を採用することで非接触での指静脈認証に対応した。



従来製品外観



C-1外観

開放型としたことで、従来機種からの追加機能として、バーコード読み取り機能が搭載可能となった。これにより、一つの装置で会員証などのバーコード読み取りと指静脈認証を行ったり、バーコードと指を併用した本人確認を行ったりすることが可能となっている。

指静脈データは日立独自の技術であり、高いセキュリティのテンプレート保護技術であるPBIで保護されており、インターネット経由での指静脈認証をセキュアに行うことが可能となっている。

指静脈認証装置C-1の高い認証精度、非接触による使い勝手のよさ、PBIによる高いセキュリティという特徴を生かし、コンビニエンスストアやスーパーマーケットなどでの手ぶらキャッシュレス決済や、各種会員管理、イベント会場の入退管理などへの適用を想定している（図3参照）。

3.2

日立カメラ生体認証SDK for Windows フロントカメラ

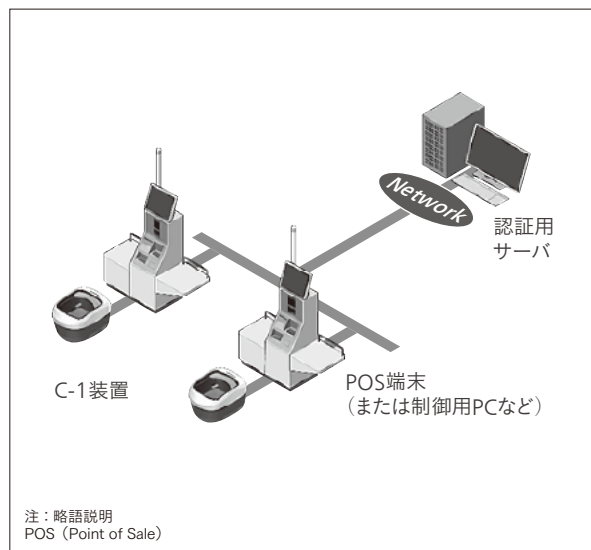
生体認証への注目が集まるにしたがって、生体認証の特徴である高いセキュリティをより低いコストで実現することが求められるようになった。このような状況の中、日立では、PCに内蔵された可視光カメラを用いる指静脈認証ソフトウェアを開発した⁵⁾。

本製品の特長は、完全非接触の指静脈認証を、専用装置不要で提供できることである。また、本製品はシンプルなAPI（Application Programming Interface）を持つSDK形式で提供しており、専用装置も不要なため、低コストかつ手早く指静脈認証ソリューションを開発できる。

本製品の開発にあたっては、(1) 可視光で撮影した画像から指静脈パターンを抽出しなければならないこと、

図3| C-1システム構成

C-1は装置内に生体情報を保持せず、ネットワーク内の認証用サーバにPBI公開鍵として保存し、窃取などによる流出リスクを回避する。認証システムはC-1装置以外に、C-1と接続して認証制御を行うPOS端末（または制御用PCなど）、認証用サーバにより構成する。



(2) 背景が乱雑かつ指の提示姿勢が不安定であることから、専用装置を用いた場合と比較して認証精度が劣化しやすいという課題があった（図4参照）。

そこで日立は、(1) 色情報を用いた静脈パターンの抽出技術、(2) 撮影画像からの背景除去（複数指検出）・指姿勢補正技術、(3) 複数指を同時に用いた認証判定技術を新たに開発し、課題を克服することで、可視光カメラによる指静脈認証実用化を達成した。本製品の処理概要を図5に示す。

本製品を用いることで、PCや業務アプリケーションへの指静脈認証によるログインを、専用装置不要で実現することが可能になる。

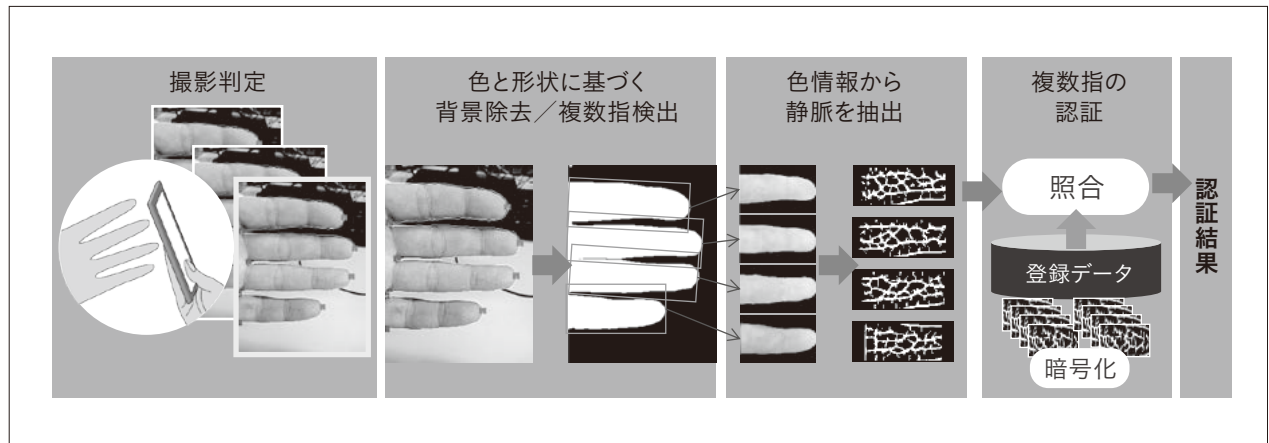


図4| 汎用カメラ生体認証SDKの開発における課題

可視光による指静脈認証SDK（Software Development Kit）の開発においては、専用装置と比較して認証精度が劣化しやすいという課題がある。

図5| 汎用カメラ生体認証SDKの処理概要

一連の処理において、さまざまな精度向上策を講じた。



4. 日立が提案する 指静脈認証技術の展望

日立では、3章で述べた指静脈認証製品群にとどまらず、これらの知見を生かし、対応モダリティの拡充と認証精度や実行速度をさらに高める研究・開発を推進している。また、2章で述べたPBI技術は、TPM (Trusted Platform Module) といった、耐タンパ性を備えたハードウェアが不要であることから、より多くのプラットフォームで、生体認証を実現可能とする。

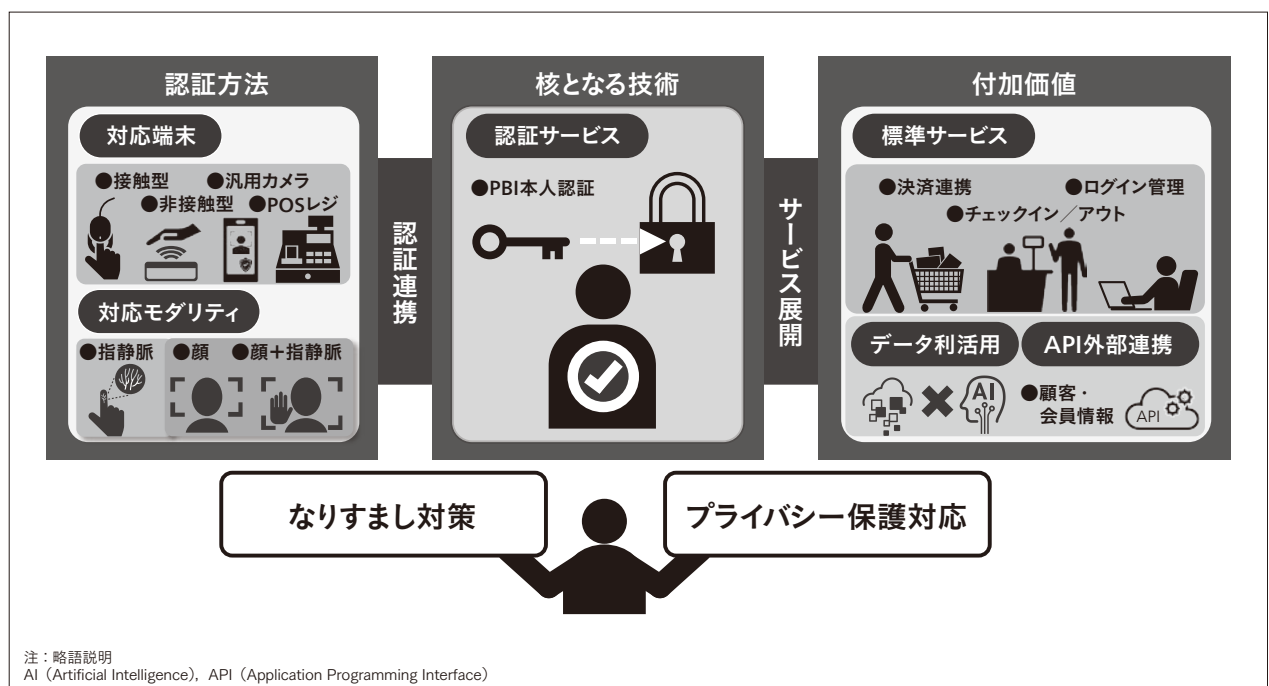
今後はこれらの認証方法と技術を連携させ、付加価値

のあるサービスを展開していく（図6参照）。決済との連携や、チェックイン／アウトといった、SECaaS (Security as a Service) を整え、さらに、AI (Artificial Intelligence) によるデータ活用や、APIを用いた他システムとの連携も視野に入れる。

この「連携」は従来の、一つの製品・サービスを構成するための縦方向の層 (Layer) 連携だけではない。顧客のシステムや、異なる分野の技術を結ぶ、横方向の層 (Tier) も含まれる。将来は、生体認証技術で電気・ガス・水道・通信といったインフラと同水準の社会貢献をめざしていく。

図6| 今後の展望

多様な認証方法の提供と、核となるPBI技術を用いた決済連携やログイン管理などの付加価値を提供し、さらにはデータ活用や外部システムとの連携で、生体認証にとどまらない社会貢献をめざす。



5. おわりに

本稿では、ニューノーマルに対応した指静脈認証ソリューションおよびPBIを活用したソリューションと、今後の展望について述べた。

デジタルとリアルをシームレスにつなぐ日立のPBI技術は、これからの時代の本人認証において、核となる技術であると考えている。これを普及するべく、高いセキュリティと利便性を両立させた指静脈認証技術を活用した認証ソリューションの拡充を推進し、さまざまな分野のパートナーとの協創を通じてグローバルに事業を展開していく。

参考文献など

- 1) 松井隆, 外: 指静脈認証のグローバル展開, 日立評論, 93, 4, 364~367 (2011.4)
- 2) EUR-Lex Access to European Union law, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 3) 日立ニュースリリース, 日立ヨーロッパ社が, 英国の金融機関として初めてパークレイズ社が運用開始する指静脈認証装置を提供 (2014.9), <https://www.hitachi.co.jp/New/cnews/month/2014/09/0905.html>
- 4) 高橋健太, 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) (2013.1)
- 5) 三浦直人, 外: 汎用カメラ指静脈認証技術とその将来展望, 日立評論, 100, 3, 294~301 (2018.6)

執筆者紹介



高谷 学

日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティイノベーション本部
認証ソリューション部 所属
現在, 指静脈認証製品の設計・開発に従事



鈴木 彦太郎

日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティイノベーション本部
認証ソリューション部 所属
現在, 指静脈認証製品の設計・開発に従事



椿 直樹

日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティイノベーション本部
認証ソリューション部 所属
現在, 指静脈認証製品の設計・開発に従事



松木 譲介

日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティイノベーション本部
認証ソリューション部 所属
現在, 生体認証製品におけるセキュリティ設計に従事
情報処理安全確保支援士(登録番号第011037号)



山口 光博

日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティイノベーション本部
認証ソリューション部 所属
現在, 指静脈認証製品の開発に従事