Biometric Signature Server

さまざまな技術との連携により、セキュリティ、ユーザビリティー向上に貢献。

■FIDO × PBI

生体認証と公開鍵を組み合わせる技術には、PBIの他にFIDO（Fast IDentity Online）というオンライン認証規格がある。FIDOとは、従来のパスワード認証に替わり、生体認証や多要素認証を活用する技術だ。スマートフォンを利用したネットバンキングなどで、徐々に普及が進んでいる。

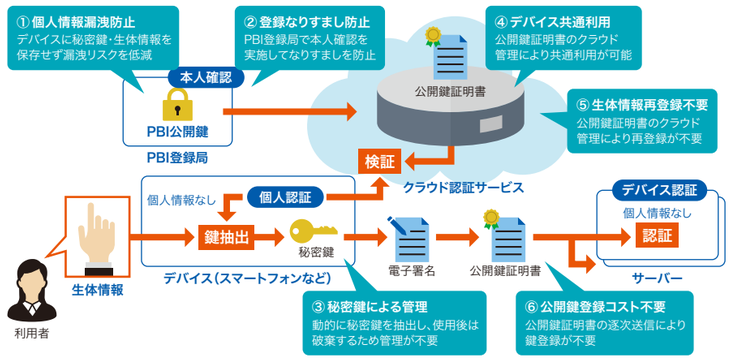
FIDOとPBIで大きく異なるのは、生体情報の管理だ。PBIでは生体情報そのものを保管しないが、FIDOでは利用者本人が所有するスマートフォンなどのデバイス内に、生体情報を登録・保管する必要がある。そのため、デバイスの取り扱いには細心の注意を払わなければならない。

PBIは、このFIDOの特性を生かしながら、さまざまな付加価値を提供すること、ウィークポイントを補強することが可能だ。

FIDOとPBIは、ともに端末と外部のユーザーやサーバーとの間のインタフェースが同じため、とても相性が良い。PBIの認証方式を、FIDOに準拠した認証器（Authenticator）として実装することで、セキュリティ、ユーザビリティーを向上し、FIDOだけではできない『完全な手ぶらでの認証』も可能にする。生体情報や秘密鍵を管理する必要がなくなり、ソフトウェア実装などでも漏洩リスクを低減することができる。また登録した認証情報を、サーバーや別の端末に安全に移行することができ、アカウントリカバリを、生体認証に基づいて簡単に実行することも可能となる。

FIDO × PBI 連携モデル　**サーバー認証モデル：公開鍵証明書をクラウド管理**

FIDO基盤へのPBI適用で、さまざまな付加価値を提供し、ウィークポイントを補強。



PBI（Public Biometric Infrastructure：公開型生体認証基盤）

■ブロックチェーン × PBI

近年、飛躍的に普及が進む仮想通貨のプラットフォームとして注目されるブロックチェーン。分散型の高信頼な取引記録技術であり、インターネットなどオープンなネットワークにおける非中央集権型システムを実現し、金融取引やサプライチェーンなど、広範な応用が期待されている。

一方、仮想通貨の多額な不正流出が起こっているのも事実。その多くは、電子署名に用いる秘密鍵の流出が原因と伝えられている。

このブロックチェーン基盤における鍵管理の問題も、PBIの適用で解決することができる。

PBIを用いることで、ユーザーの秘密鍵をサーバーや端末に保存することなく、またデバイスを持たせる必要もなくなる。より安全にブロックチェーンを利用できるだけでなく、ブロックチェーンを用いた取引などに対して、さらに厳密に本人の意思を確認できるようになるのだ。

PBI活用事例

PBIは、すでにさまざまな分野でPoC（概念実証）を成功させ、金融機関へも導入されるなど、着実に実績を増やし続けている。よりオープンなシステム・サービスに対応する生体認証として、今後ますます注目され、期待されることが予想される。

事例①　ブロックチェーン利用時の「本人確認」、「鍵管理」の問題を解決

- KDDI、ミスタードーナツと協力しPoCを実施（2018年7月）。
- ブロックチェーン利用時に課題となる「本人確認」、「鍵管理」の問題を、PBI技術で解決。
- クーポン発行時に本人認証を実施（発行したクーポンに本人の電子署名を付与）、クーポン利用時は「手ぶら」での決済を行い、ブロックチェーンを用いた管理を実施。

事例②　ATM・窓口における銀行取引を「手ぶら」で実現

- ATM・窓口で指静脈認証による手ぶらでの取引を、PBI適用の新システムで実現。

2017年4月～
山口銀行にてPBI「手ぶら」取引システム稼働開始

2017年5月～
北九州銀行にてPBI「手ぶら」取引システム稼働開始

2018年1月～
もみじ銀行にてPBI「手ぶら」取引システム稼働開始

事例③　学認システムへの適用実証実験を実施

- 京都産業大学で、学認システムへのPBI適用実証実験を実施。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/bss/

C19K-03-01　2019.09

HITACHI
Inspire the Next

公開型生体認証基盤

Biometric Signature Server
ホワイトペーパー

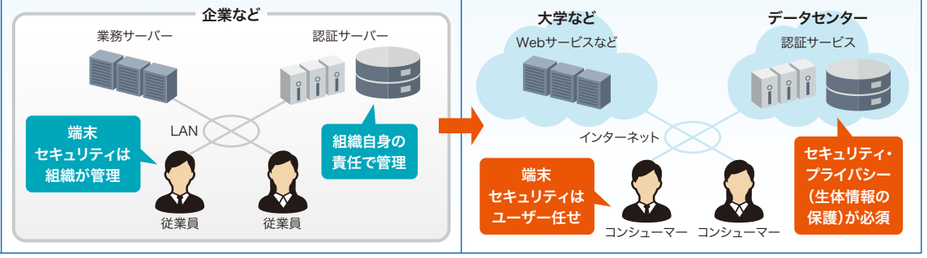
**よりオープンなシステム・サービスモデルへと変化するIT市場で
生体認証システムはどのように進化し、何を実現すべきか?
その答えを導くPBI（Public Biometric Infrastructure：公開型生体認証基盤）**

生体認証は、パスワードのように覚えておく必要がなく、ICカードのように携行する必要がない、利便性の高い認証手段だ。
一方、生体情報そのものはきわめてセンシティブで、徹底した安全管理が求められるため、
クローズドな単一システムに、利用を制限していたのも事実。
では、よりオープンなシステム・サービスモデルへと変化が進むIT市場において、
この先、生体認証システムはどのように進化し、何を実現すべきか。
その答えを導くのが、株式会社日立製作所のシステム研究所が特許を持つ
PBI（Public Biometric Infrastructure：公開型生体認証基盤）だ。
これまで指静脈認証システム「静紋シリーズ」を提供してきた日立ソリューションズの新製品、
公開型生体認証基盤 Biometric Signature Serverが適用した注目の技術。その仕組みや、もたらす効果を紹介する。

さまざまな認証技術が登場し、成熟が進む生体認証。
一方、よりオープンに変化するIT市場。

生体認証は、PC・スマートフォンへのログイン、施設への入退出管理、ATM、ネットバンキングなど、幅広い分野で、パスワード（記憶認証）やICカード（所有物認証）に替わる、あるいは併用される認証手段として導入・利用が着実に増えている。
また、指紋認証、静脈認証、顔認証、虹彩認証など、さまざまな認証技術が登場し、センサー技術・パターン認識の成熟などもあり、着実な進化を見せている。
一方、これと並行して進んでいるのが、IT市場の変化だ。

■IT市場で求められるシステム・サービスモデルの変化

	クローズド		オープン
システムモデル	オンプレミス型	→	クラウド型
利用範囲	単一システム/サービス	→	複数システム/サービス
利用者	従業員など	→	コンシューマー
競争軸	コスト	→	セキュリティ・プライバシー・信頼性
事業モデル・市場	B2B（既存市場）	→	B2B2C（新規市場）
システムイメージ			

株式会社 日立ソリューションズ

Biometric Signature Server

前ページの図に示したとおり、よりオープンなシステム・サービスモデルへと変化が求められている。
そんな中、システムの開発・構築企業が考えなければならないのは、生体認証システムはどのように進化し、何を実現すべきか。
大命題となるのは、【さまざまなサービスからの共通利用が可能な基盤】としての構築。そのために重要なのは、【生体情報のプライバシー保護・セキュリティ維持を徹底】すること、そして【コスト、利便性の面で、低負担での導入・利用】を実現することだろう。
生体情報は生涯変わることがなく、破棄・更新できない情報であり、いったん漏洩してしまうと、取り返しがつかない。データの改ざん・挿入などによるなりすましの脅威も発生させてしまう。これまでの生体認証システムは、生体情報をクローズドな単一システム内で管理し、利用を制限することで安全性を確保してきた。しかし、これからのオープンな環境では、これにふさわしいセキュリティレベルの確保が必須となる。
また、既存の資産をできるだけ有効に活用し、短期間・低コストでの導入と、運用の負担・コストを低減させなければならない。そして利用者にとっては、生体認証を使うことが負担になってはならない。たとえば高齢者などにとっても、直感的な分かりやすさ、容易な操作性が求められる。
こうした命題・課題に取り組んだのが、株式会社日立製作所のシステム研究所が特許を持つPBI(Public Biometric Infrastructure:公開型生体認証基盤)だ。

信頼性が実証されている「PKI」と、「生体認証」を組み合わせたPBI。

PBIは、「生体認証」と「PKI(Public Key Infrastructure:公開鍵基盤)認証」を組み合わせた技術。
PKIは、ネットワーク上で、サービス提供者と利用者との間でお互いが本人であることを認証し合うためのセキュリティ基盤。公開鍵暗号技術や電子署名技術に基づいている。電子政府における電子署名や、SSL、電子商取引に使われ、今や社会のネットワーク基盤のほとんどに何らかのかたちでかかわり、信頼性が実証されている技術だ。
この分散型でオープンな認証へと進化したPKIと、生体認証を組み合わせて開発したのがPBIだ。
PBIでは、生体情報から「秘密鍵」「公開鍵」を生成する。生体情報から作成した公開鍵をあらかじめサーバーに登録しておき、認証時に生体情報から秘密鍵を抽出する。生体情報を直接利用せず、公開鍵や電子署名に「一方向性変換」して利用するのだ。
PBIは、システム上は“PKI認証と同じように”生体認証を利用することができる。PKIと同等のセキュリティ機能と、確実な本人確認、高利便性の特長を併せ持っている。
PBI実現に向け、技術的課題となったのは、生体情報特有の「揺らぎ」「曖昧さ」への対応だ。PKIにおける電子署名の秘密鍵は、デジタルな情報であるため、データとして一致すれば正しい、一致しなければ誤り、あるいは偽造だという判断ができる。これに対して、生体情報は生身の身体から収集するアナログな情報だ。指の置き方やセンサーノイズなどのわずかな影響が、データに誤差を生じさせてしまう。これを的確に判断し、電子署名の秘密鍵に使えるよう精度を向上したのがPBIだ。

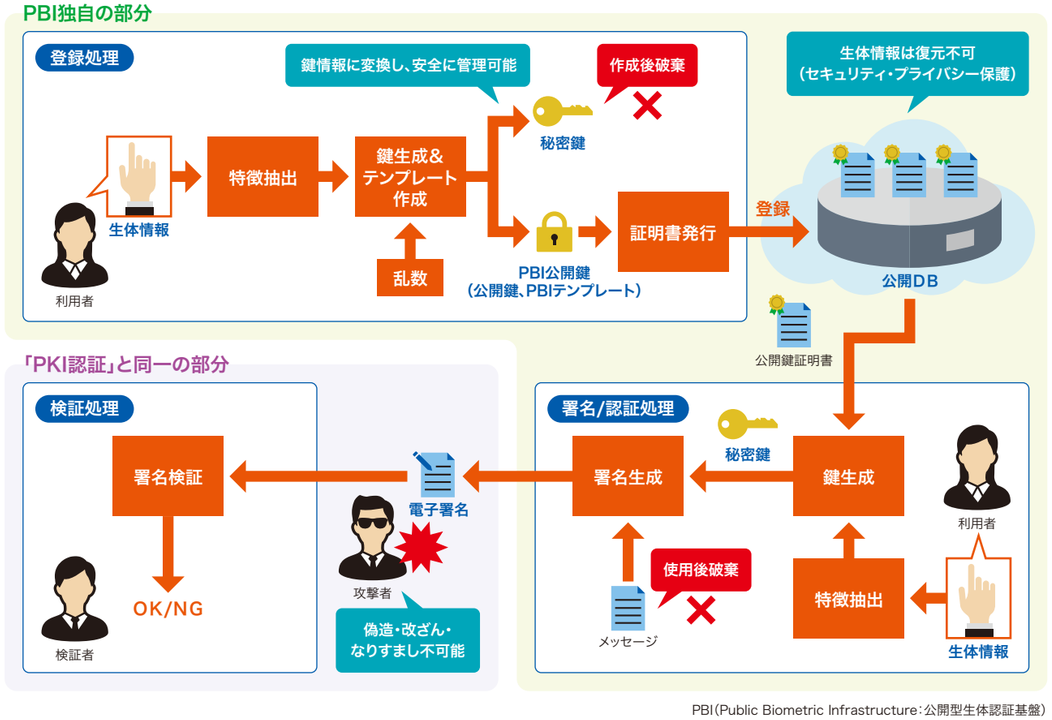
オンプレミス、オンライン上を問わずさまざまなサービスからの共通利用が可能。

このPBIを適用する、日立ソリューションズの公開型生体認証基盤 Biometric Signature Serverは、生体認証システムの進化を体現。PBI開発時に、重要視していた【生体情報のプライバシー保護・セキュリティ維持を徹底】すること、【コスト、利便性の面で、低負担での導入・利用】を実現すること、そして大命題であった【さまざまなサービスからの共通利用が可能な基盤】を可能にした。
Biometric Signature Serverの認証精度は他人受入率(FAR)0.000016%未満*を実現。セキュリティを、より高いレベルへと向上させた。
利用者にとっては…
生体認証ならではの利便性が、さらにアップ。暗証番号やICカードを必要としない「手ぶら」での認証・電子署名が可能になった。「忘れる」「紛失する」といった心配のない、自分の身体さえあれば誰にでも、オンプレミス、オンライン上を問わずさまざまなサービスを使える環境だ。
システムの運用管理面では…
生体情報に基づく確実な本人確認の「認証」と「電子署名」、そしてPKIの高セキュリティを両立した。生体情報そのものを利用しないため、個人情報にあたる生体情報の管理が不要。事業者は、生体情報の漏洩リスクを回避でき、オンプレミスに加え、クラウド上でもサービスを提供できるようになる。異なるサービス間で、生体認証の共同利用も可能になる。
また、既存のPKI認証基盤に大幅な変更を加えることなく導入できるのも大きなメリットだろう。ICカードなど、従来利用していた認証媒体の用意、配布、更新、回収、廃棄などにかかっていた運用コストも劇的に低減される。
利用者に、企業に、そして社会インフラに…これまでとは異なる価値を提供することが期待される。

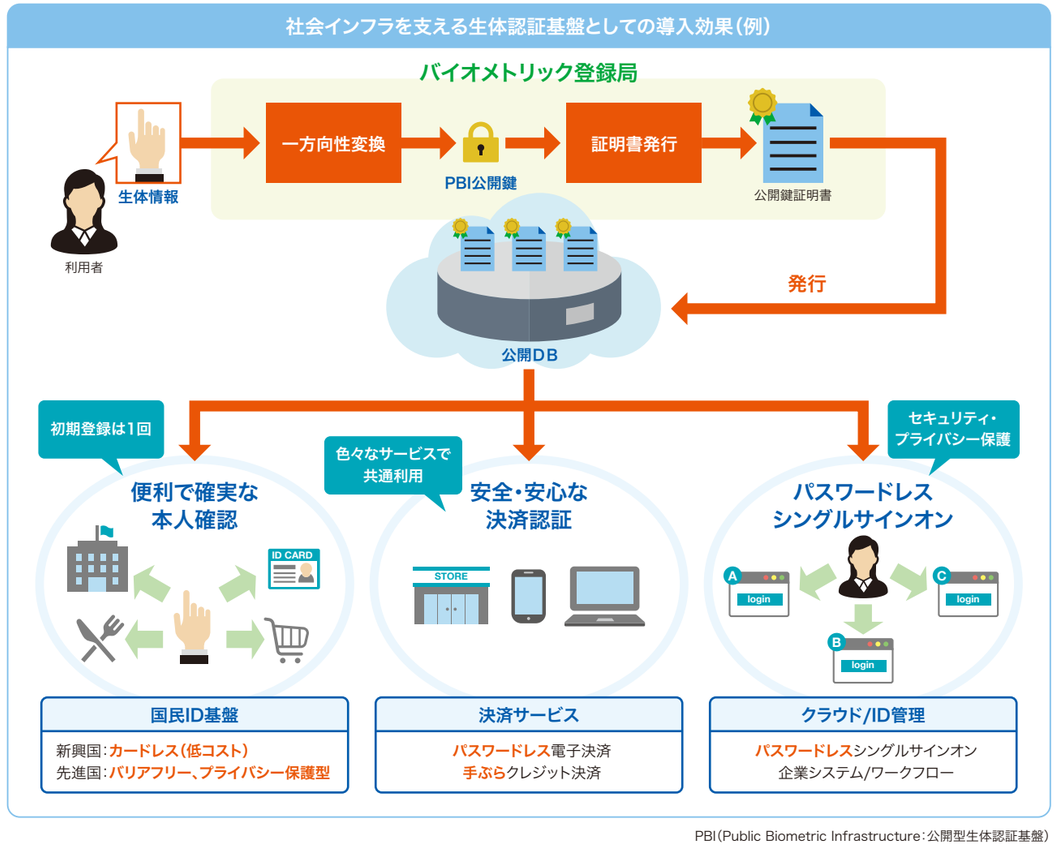
＊:バイオメトリクスの精度評価に関する国際規格 ISO/IEC 19795-1 に基づいた測定数値。
数値が低いほど認証精度が高いことを示す。
公開型生体認証基盤 Biometric Signature Serverの数値は、以下のとおり。
FAR(False Acceptance Rate:他人受入率):0.000016%未満
FRR(False Rejection Rate:本人拒否率):0.1%

■PBI技術の概要

「生体認証」と「PKI認証」を組み合わせた技術。“PKI認証と同じように”生体認証を利用できる。



PBI(Public Biometric Infrastructure:公開型生体認証基盤)



PBI(Public Biometric Infrastructure:公開型生体認証基盤)