GMO トラスト・ログイン

指静脈認証　第１回

SHIELD PBI 指静脈認証サービス

前回は身近な例から多要素認証について説明しました。普段使っている銀行の ATM やクレジットカードなどで多要素認証が身近に使われているということが理解いただけたかと思います。今回は多要素認証の種類や認証方式について説明します。

生体認証について

生体認証はバイオメトリクス認証とも呼ばれ人の生体的特徴や行動的特徴を使用して認証を行う認証要素です。ユーザの生体的特徴を使うことで本人であることを証明できるため、ほかの認証要素である「ユーザが知っていること（知識情報）」や「ユーザが持っていること（所持情報）」と比べて使用するユーザに負担が少ないのが特徴です。記憶に頼らないためパスワードを忘れるリスクや体の一部であることから認証デバイスを紛失するリスクがありません。生体認証には指紋、顔、網膜、虹彩、静脈や声紋、筆跡などの認証メソッドが利用されています。

生体認証の主なメソッド

認証メソッド	特 徴
指紋認証	指紋情報を使用して認証する。センサーデバイスは様々なタイプがあり指をガラス面に乗せて下部よりセンサーで読み取る、指をボタンにタッチするだけ、指をスワイプして読み取る方法などがある。怪我などで認証できなくなる場合がある。
網膜認証	目の網膜の毛細血管のパターンを認識して認証する。目をセンサーに近接させて網膜情報を撮影する。
虹彩認証	目の虹彩パターンを認識して認証する。網膜と比べて虹彩は目の表面にあるため網膜認証と比べると比較的撮影が容易に行えるためセンサーが小型化できる。
静脈認証	指や手のひらの静脈のパターンを認識して認証する。静脈は加齢による経年変化があっても不変と言われている。
顔認証	顔を識別して認証する。カメラが主なセンサーとなるため容易に実装することができる。加齢や眼鏡の有無によって認識率が低下することがある。
声紋認証	声を識別して認証する。マイクがセンサーとなる。健康状態によって認識率が低下することがある。
掌形認証	手のひらの幅や、指の長さなどを用いて認証する方法。
筆跡認証	サインをする時の軌跡・速度・筆圧の変化などの癖を利用する方法。

指静脈認証とは

静脈認証は生体認証の一つのメソッドで人間の身体を流れる静脈のパターンを光学センサーにてスキャンしそのパターン画像にて個人を識別します。静脈は指紋や虹彩のように非常に複雑で同じパターンを持つ人間は双子であっても存在しないといわれており、生体認証の中でも誤認率の低いメソッドとされています。また、身体の表面ではなく内部にある静脈を使用しているため、静脈の細部の形状を盗み出すことが難しく偽造やなりすましが非常に困難です。さらに、老齢化による変化や体調による変化、皮膚表面の荒れや発疹、摩耗や乾燥などによってもパターンの大きな変化がないのも特徴です。また、顔や指紋とくらべて静脈の場合、認証データとして登録するのに使用者が自分の身体的な特徴データを提供する心理的な抵抗が少ないとされています。現在製品化されている静脈認証デバイスは主に手のひらや指の静脈が利用されています。

指静脈認証とは静脈の中の人の指を流れる静脈パターンを使用し認証するものを言います。指静脈認証では手のひらの静脈と比べ静脈を読み取るリーダー部分が小型で安価であるため PC のログインや Web サイトの認証などにも利用することができるのが特徴です。

日立指静脈認証

日立が開発した指静脈認証技術は近赤外線を指に透過させて得られる指の静脈パターンの画像によって個人認証を行う世界最高レベル・最先端の認証技術です。指画像から静脈の存在する部分を人工知能手法で鮮明な構造パターンとして検出し、あらかじめ登録した静脈の構造パターンとマッチングさせて個人認識を行います。

透過光撮影方式の採用で、より安定した認証精度を実現しています。鮮明な静脈画像の取得が可能で、皮膚の表面（しわ、手相、肌荒れなど）が写りにくく、高コントラストな画像静脈パターン抽出を行うため、小容量の認証データで高精度、高速認証を実現します。

特徴として、認証スピードが速く、登録が簡単で操作性に優れています。非常に小型で USB にて PC と接続が可能なため簡単・低コストで運用開始することが可能です。

使用イメージ

透過パターン取得イメージ

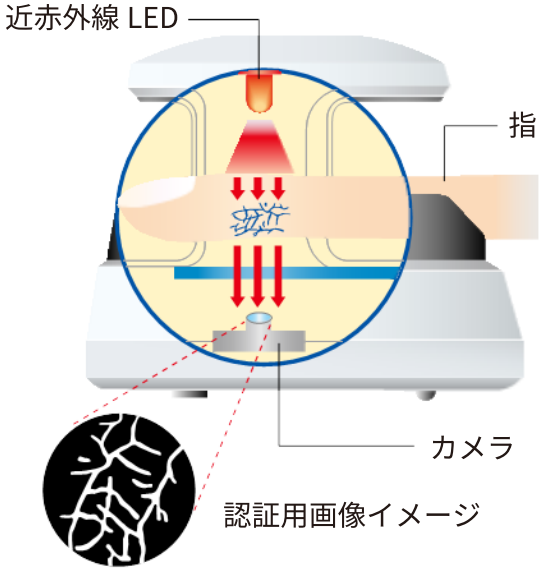
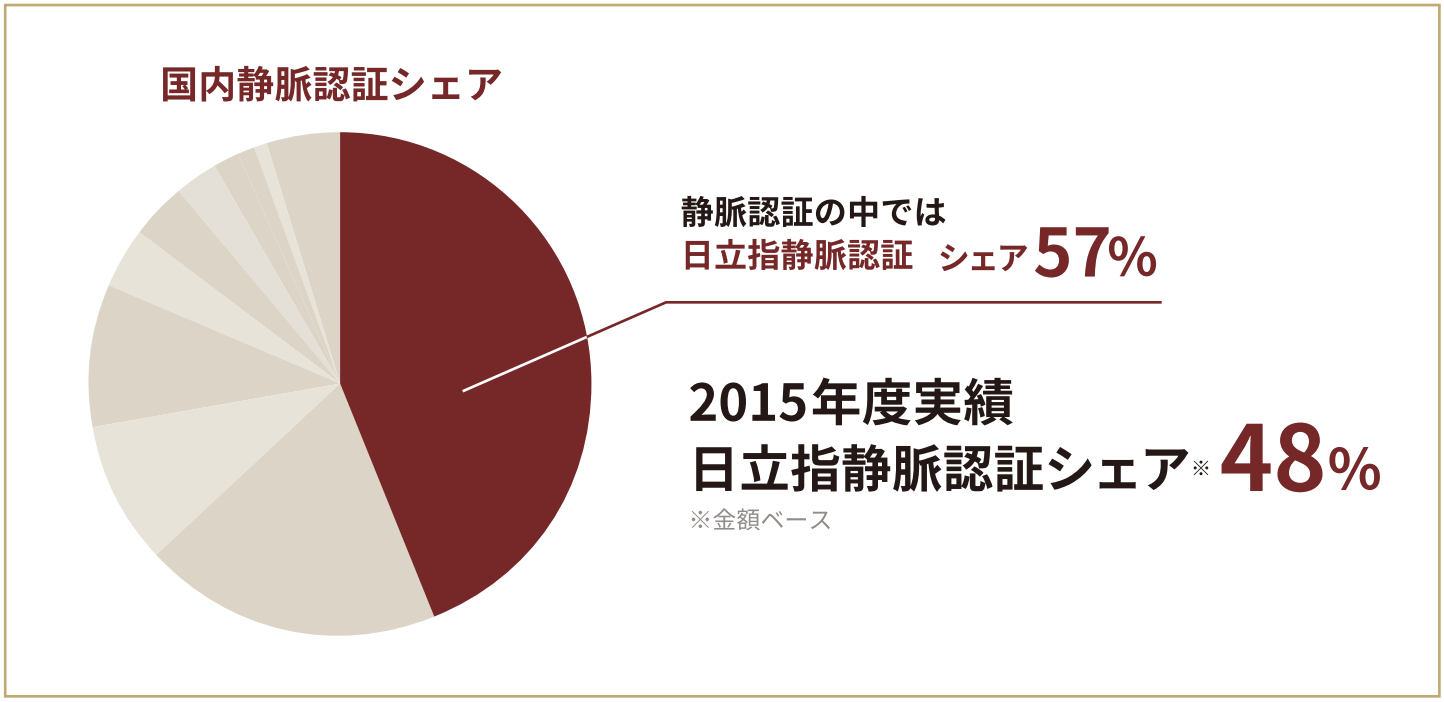


図 日立の指静脈認証

また、日立は静脈認証装置の中で国内シェア No.1 の 48% を獲得しています。実績のある指静脈認証装置ということがよくわかります。



出典：富士経済「2016 セキュリティ関連市場の将来展望」より

PKIとは

PKI(公開鍵暗号基盤Public Key Infrastructure)は、公開鍵と秘密鍵のキーペアからなる「公開鍵暗号方式」という技術を利用し、インターネット上で安全に情報のやり取りを行うセキュリティ基盤です。暗号化するときと復号するときに「公開鍵」と「秘密鍵」というペアの別々の鍵を使うのが特徴です。「公開鍵」は誰でも入手可能で「秘密鍵」は受信者だけが持っている鍵です。暗号化には一般的に「公開鍵」を使用します。この暗号化されてデータの復号にはこの公開鍵とペアとなっている「秘密鍵」を使用します。

電子署名とはデータが正しいものであると証明する「公開鍵」と送信者がデータに署名するのに「秘密鍵」を使用します。送信者は相手にデータを送付する前に、そのデータのハッシュ値を作成し自分の「秘密鍵」で暗号化します。送信者は受信者に「元のデータ」と「ハッシュ値の暗号文」と自分の公開鍵を含んだ「電子証明書」を送付します。受信者は電子証明書が信頼できるか認証局に問い合わせ、電子証明書から公開鍵を取得しハッシュ値を復号します。受信者は受信した「元のデータ」からハッシュ値を生成し、この復号したハッシュ値と同一かどうか確認します。同一であった場合このデータは送信者本人が作成したデータであることを立証することができます。この一連の流れで電子署名がデータの正当性、改ざんされていないことを保証することができます。

PBIとは

PBI(公開型生体認証基盤 Public Biometric Infrastructure) とは電子署名の秘密鍵として生体情報そのものを利用するセキュリティ技術です。これまで IC カードなどを併用して電子署名の秘密鍵の管理に生体認証を用いる方式はありましたが、PBI は生体情報自体を秘密鍵として利用することで証明書の管理を不要にします。
一般的な生体認証システムは生体の特徴データを数値化してから暗号化しシステム内に登録します。認証時は暗号化されたデータを復号し生体特徴データと照合して認証します。
PBI では生体情報の特徴データを暗号学的に安全な「一方向性変換」により、復号できない形（PBI 公開鍵）で登録・認証します。そのためシステム内のデータが漏洩した場合でも、そこから生体情報や特徴データを復元することができません。また、生体情報からの変換時に乱数パラメータを用いることで、同じ生体情報から無数の異なる PBI 公開鍵を生成することが可能なため、登録データを破棄・更新することができます。

PBI の特徴

1

機微情報にあたる生体情報の管理が不要

- 生体情報を直接利用せず、公開鍵や署名に「一方向性変換」を利用
- プライバシを高速に保護。破棄更新も可能

2

IC カードや暗証番号を使わず便利で安全な PKI を実現

- 「忘れない」「無くさない」「手ぶら」で認証・署名が可能
- 生体情報に基づく確実な本人確認と PKI の高セキュリティを両立

PBI を使った認証処理は次のプロセスで実現されています。

（1）認証データの登録

センサーから読み取ったユーザの生体情報に対して一方向性変換を施し、PBI 公開鍵を生成。PBI 公開鍵は公開鍵証明書の形でリポジトリに登録します。

（2）認証時

認証時には再びセンターから生体情報を読み取り秘密鍵を生成します。認証サーバーから送信されるチャレンジコード（乱数）に対する電子署名データを生成します。この電子署名データを認証サーバーに送信し、認証サーバーは署名検証することで本人認証を実施します。このとき登録時に入力した生体情報と署名時に入力した生体情報が一致していれば成功します。

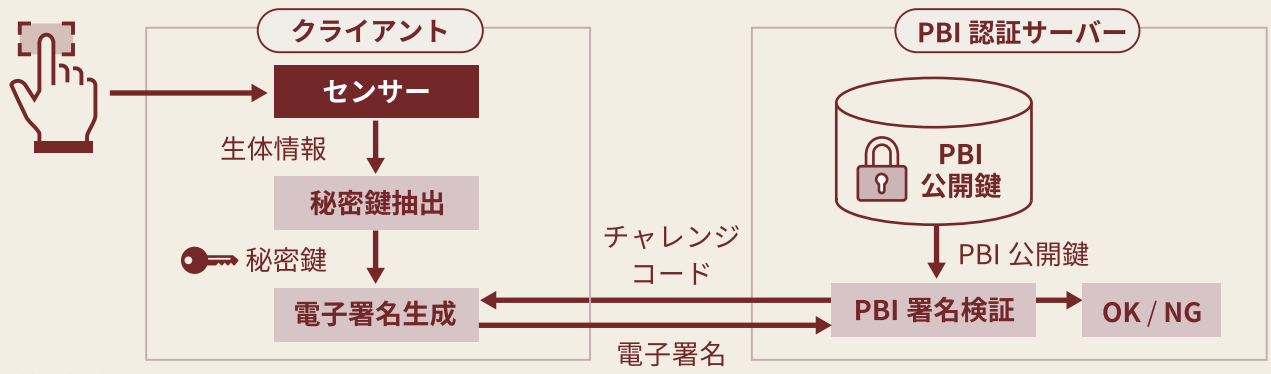


図 PBI 技術概念図

生体情報の誤差と電子署名

電子署名の秘密鍵はデジタルな情報として処理されます。これはデータとして誤差を許さないことを前提に仕組みが構築されています。すなわち秘密鍵が１ビットでも違っていればそれは電子署名が検証に失敗することになります。
一方、生体認証に使用する生体情報はセンサーで読み取るたびに誤差が発生するアナログな情報です。指の置き方やセンサーのノイズなど様々なところで誤差が発生します。したがってセンサーから検出した生体情報をそのままには電子署名の秘密鍵として使用することはできません。
PBI では誤り訂正技術を用いることで、署名時に入力した生体情報に含まれる誤差が一定未満であれば、生体情報をもとに秘密鍵を抽出し正しい電子署名データの生成に成功するようにしています。誤差を許容することで、生体情報を秘密鍵とする PKI が実現できるのです。

図 電子署名と生体認証

SHIELD PBI 指静脈認証サービス

PBI を構成する生体情報として指静脈認証を利用する仕組みを日立システムズが運営、管理しているのが SHIELD PBI 指静脈認証サービスです。
日立システムズが運営し公開鍵を安全に管理しているため PBI 指静脈認証を簡単に利用することが可能です。この SHIELD PBI 指静脈認証を利用することで利用者は公開鍵の管理をする必要がありません。また指静脈リーダーは小型で利用しやすく読み取り速度も速いため高速に認証を実現できます。

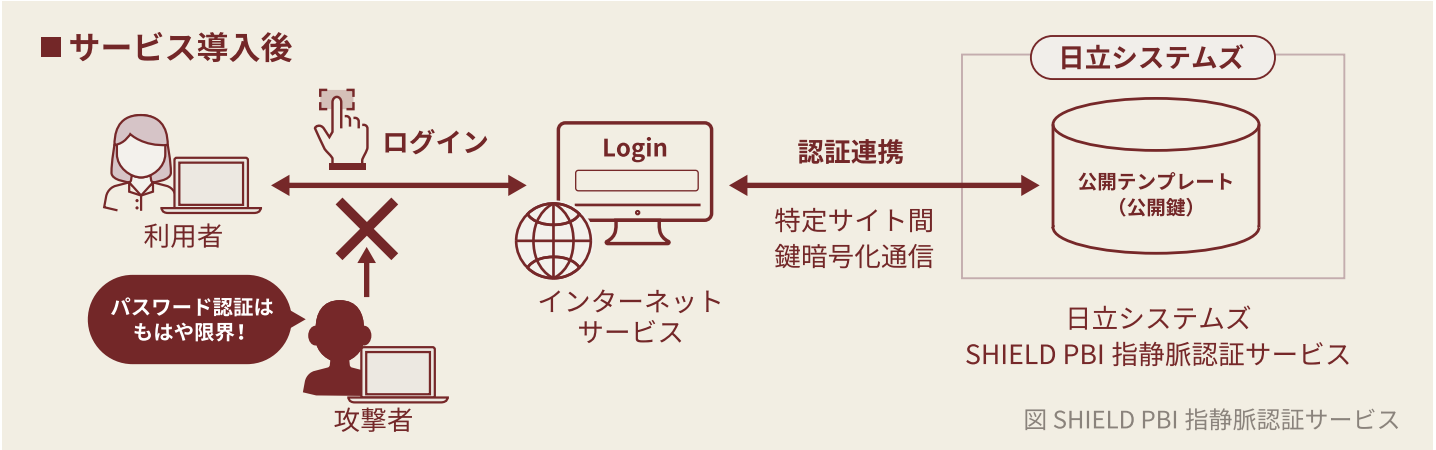


図 SHIELD PBI 指静脈認証サービス

高度な手法でも
サイバー攻撃は困難

- PASS の入力をしないので、ウィルス感染させても認証情報は盗めない。
- 偽 HP に誘導させても正式なアプリケーション HP 同様の認証要求・認証処理は困難。
- 偽 HP から日立システムズ指静脈認証と通信できないので認証できない。

トラスト・ログインと SHIELD PBI 指静脈認証サービスを組み合わせた高セキュリティ IDaaS サービス

SHIELD PBI指静脈認証サービスによるセキュアな生体認証を使用した電子署名と一度ログインしたら様々なサービスへシングルサインオン（SSO）が可能なトラスト・ログインを組み合わせることで高いセキュリティとSSOの利便性を両立することができます。

※SHIELD PBI 指静脈認証サービスはトラスト・ログインの有償オプションとしてサービス提供される予定です。

トラスト・ログインと SHIELD PBI 指静脈認証サービスの活用例

トラスト・ログインと SHIELD PBI 指静脈認証サービスの活用の例をいくつか紹介します。

■ 共有PCを使用するショップ

ショップでは数台のPCを複数の店員で共有して利用しています。共有 PC では必要な時にログインしシステムを使用し、終わったらすぐにログアウトしています。またシステムのタイムアウトを短く設定しログアウトし忘れたときに強制的にログアウトさせます。

このような利用シーンでは店員が PC にログインするときにできるだけ容易に入れるように簡単なパスワードを使用しがちです。それはセキュリティの低下につながります。セキュリティを高めようとパスワードに加えてワンタイムパスワードを組み合わせる場合、店員が常にトークンを身に着けておく必要があります。

ここでトラスト・ログインと SHIELD PBI 指静脈認証サービスを利用すると忙しいショップ店員は自分の指を使うだけで高いセキュリティと忙しい中で素早く PC を利用し複数のシステムへアクセスすることができるようになります。

■ 研究所の高セキュリティシステム

研究施設など高度に機密性の高い情報を取り扱う必要がある場合、高い認証セキュリティが必要となります。そのため多要素認証としてID/パスワードに加えてICカードやワンタイムパスワードを利用していました。ICカードは紛失や忘れたりするリスクがありました。

また、SaaSを利用する場合それぞれのSaaSで対応している認証方法が異なる場合、複数のトークンを持ち歩く必要がありました。トラスト・ログインとSHIELD PBI指静脈認証サービスを利用すると紛失や忘れたりすることがなくなり、さらに一度の高セキュリティな指静脈認証でさまざまなSaaSサービスへ同じセキュリティレベルを保ってアクセスすることが可能となります。

指静脈認証と電子署名を組み合わせた SHIELD PBI 指静脈認証サービスを使うことで自分の指を使用するだけで容易に非常に高いセキュリティを保った認証を実現することが可能となり、SHIELD PBI 指静脈認証サービスとトラスト・ログインの組み合わせで指静脈を利用した高いセキュリティと様々なシステムへの SSO によるアクセスを同時に利用することが可能となります。

お問い合わせ
（GMOグローバルサイン株式会社）
03-4545-2303
support-jp@globalsign.com