先端技術キーワード解説

知っておきたい最新の動き

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

IT システムの普及が進むにつれて、本人なりすましなどの犯罪が後を絶ちません。パスワードによる本人確認だけでは、容易に破られてしまいます。

そこで、最近、本人確認として取り入れられ始めているのが、本人固有の情報であり、一生変わらないとされる指紋や顔認証による生体認証です。ところが、その生体認証にも課題が浮上してきました。

１．生体認証で浮上してきた課題

現在、ノートパソコン、スマホなどで一般的になってきたのが顔認証、指紋認証などの「生体認証」です。本人固有の情報による認証であり、しかも、本人の身体のみで認証できます。

ところが、利用が拡大する中では、危惧や不安が起き始めています。認証のための生体情報そのものがどこかに保存されていることです。

もし、漏洩などが起きれば、その人は一生、全ての生体認証ができなくなります。（パスワードのように、変更することはできません。）関連するシステム全体が利用停止に追い込まれます。

２．公開型生体認証基盤（PBI：Public Biometric Infrastructure）の仕組み

（１）PKI（Public Key Infrastructure）とは

生体認証の仕組みを知るためには、PKI を知る必要があります。PKI は公開鍵と秘密鍵というキーペアで構成される公開鍵暗号方式です。秘密鍵で暗号化したデータは公開鍵で復号し、逆に公開鍵で暗号化したデータは秘密鍵で復号します。

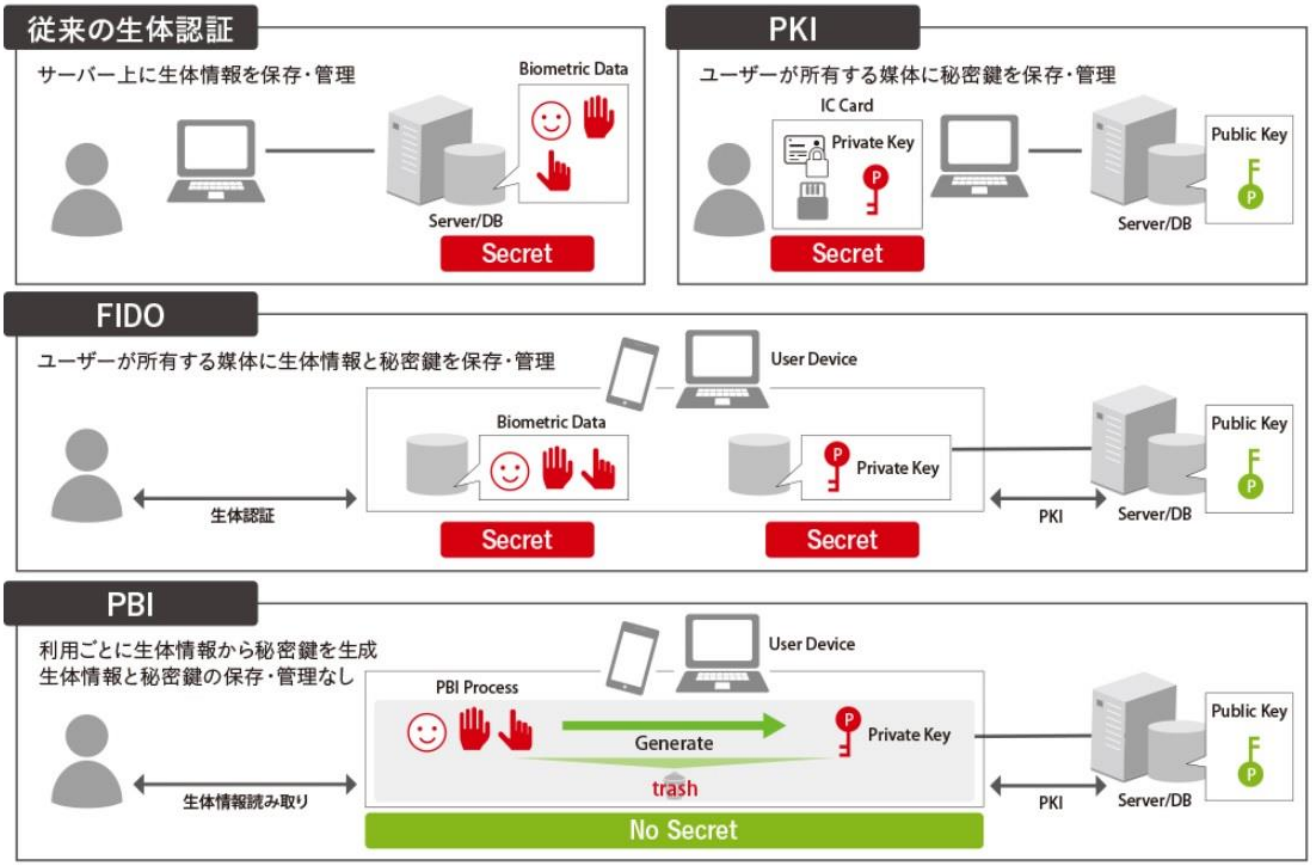
（２）FIDO（Fast IDentity Online）技術

現在、ノートパソコン、スマホなどで使われている技術です。端末内に、自身の生体情報と連携するシステムから発行された秘密鍵を保管します。ユーザーと端末間は生体情報を用いた認証、端末とシステム間は PKI を用いた認証を行うことで全体としての認証が完了します。

端末での情報は、機密情報として扱われていますが、もし、端末が盗難にあった場合には、生体情報を抜き取られる可能性があります。

（３）PBI の仕組み

PBI では、下図のように、生態情報から秘密鍵を生成します。このとき、生態情報そのものは、システム上のどこにも保存しません。このため、安全に管理することができます。



3．公開型生体認証基盤（PBI：Public Biometric Infrastructure）のメリットと期待

PBI では、秘密（Secret）の情報をどこにも保存しないため、漏えいや紛失のリスクが原理的に存在しません。今後、社会的にニーズが高まる確実な本人確認として、期待の高い技術です。

［参考文献］

1) 日経クロステック：生態情報を預けないので安心　より安全に使える生体認証とは
https://special.nikkeibp.co.jp/atclh/NXT/20/hitachi_solutions0924/

（注）

本解説は、執筆当時の状況に基づいて解説をしております。ご覧になる時には、状況が変わっている可能性がありますので、ご注意をお願いします。

技術・経営の戦略研究・トータルサポータ
ティー・エム研究所
工学博士
中小企業診断士
社会保険労務士（登録予定）
代表　芳賀　知
E-Mail：info_tm-lab@mbn.nifty.com　URL：http://tm-lab@a.la9.jp/