技術動向レポート

バイオメトリクス認証とセキュリティ評価

情報通信研究部　情報セキュリティ評価室
マネジャー　**大堀　雅勝**

IoT(1)やFinTech(2)という言葉に代表されるようにIT技術の活用が進む中、本人認証を行う技術として、生体的特徴を利用するバイオメトリクス認証への関心が高まっている。

本稿では、日本におけるバイオメトリクス認証製品のCC(3)による評価・認証に関する取り組みについて紹介する。

はじめに

IT技術の活用が進む中、他人のなりすまし対策の重要性が増している。他人のなりすましを防止するための本人認証技術として、バイオメトリクス認証への関心が高まり、銀行のATM等でも使われ始めている。一方、バイオメトリクス認証においては、生体の状態に起因する判定結果のばらつきや、偽造生体を利用した攻撃に対する対抗など、セキュリティ面での課題もある。

本稿では、パスワード認証とバイオメトリクス認証の比較を行い、バイオメトリクス認証の特徴を紹介した後、バイオメトリクス認証製品のCCによる評価・認証に向けた取り組み、ならびに、国際標準化に向けた展望について紹介する。

1. パスワード認証とバイオメトリクス認証

IT製品を利用するうえで最も身近な認証技術はパスワードによる認証であろう。これはパスワードを認証情報として用い、登録されているパスワードとの一致により本人を認証する技術であり、様々な場面で用いられている。一方、バイオメトリクス認証は、生体的特徴を認証情報とする技術であり、以下のような生体的特徴が利用されている。

・指紋
・手などの中に流れている静脈の血管
・顔
・手の形
・目の中の虹彩
・声

パスワード認証とバイオメトリクス認証の間には様々な違いがあるが、図表1はその一例である。

バイオメトリクス認証は、パスワードのように記憶するものが無く、また、身体部位を提示するなどすれば良いといったユーザにとってのメリットに加え、入力データと登録データの類似度に基づく判定値（しきい値）(4)を調節することで安全性を調節することが可能であり、運用者にとっても優れた特長を持つ技術である。このような特長からその利用が拡大してきているが、バイオメトリクス認証の性能の表し方や評価の方法にはバラつきがあり、導入を予定している運用者や利用するユーザが安全性を客観的に比較・評価することが難しい。このような

図表1　パスワード認証とバイオメトリクス認証の違い

	パスワード認証	バイオメトリクス認証
入力	キーボードなど一般的な入力装置から入力可能であるが、ユーザ自身が入力装置を操作して入力を行う必要がある場合が多い	専用のセンサーやカメラなどの入力装置が必要であるが、ユーザは入力装置に生体の部位を提示するだけでよい
強度	長さや使用する文字や数字の組み合わせに依存する	生体的特徴の盗難や偽造物生体作成の困難さに依存する
変更	変更は容易	生体的特徴そのものの変更は困難
その他	本人の責任で忘れないようにするとともに機密性を維持する必要がある	忘れる心配がない

（資料）各種資料よりみずほ情報総研作成

背景により、バイオメトリクス認証製品の安全性を客観的に評価するための統一された方法の確立が期待されている。

2. バイオメトリクス認証の特徴

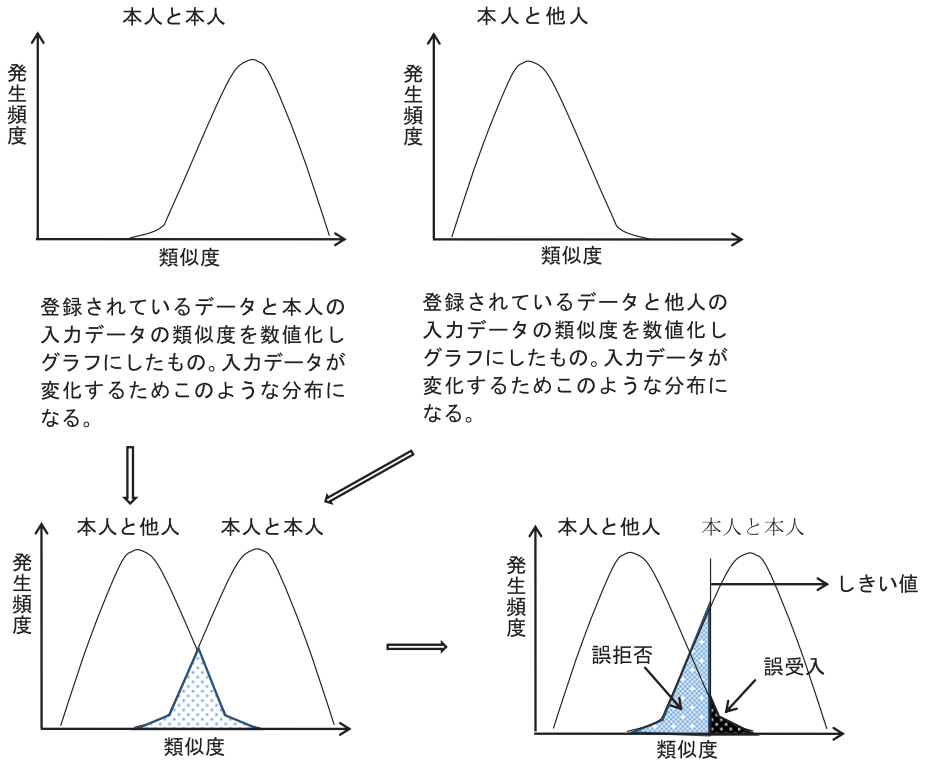
図表1においてパスワード認証とバイオメトリクス認証の比較を行ったが、バイオメトリクス認証にはさらに以下のような特徴がある。

(1) 類似度による判定

一般にバイオメトリクス認証は、入力データから特徴データを抽出し、登録されている特徴データと比較することで、本人か否かの判定を行う。入力データは身体の部位を入力装置[(5)]に提示することで得られるが、提示の仕方に加え、提示者の体調、気温、湿度といった環境の影響を受けるため、通常完全には一致しない。指紋の場合には、湿度の異なる夏と冬で入力データに差異が生じ、静脈の場合には、気温の影響による血管の拡張・収縮により入力データに差異が生じることがある。このようなことから、バイオメトリクス認証においては、パスワード認証における完全一致での本人判定とは異なり、入力データと登録データの類似度による判定が行われる。

図表2は類似度による判定の概要を表したものである。類似度はスコアと呼ばれる数値で表されるが、類似度の個人差や入力データの変化から、その値は単一とならずある範囲に分布する。この分布は、本人と本人の比較によるものと、本人と他人の比較によるものがあるが、通常、両者は重なりを持つ。本人か否かの判定は、スコアにしきい値を設定して、その値より高い場合には本人と、そうでない場合には他人と判断するが、前述の重なりにより、登録されている本人が他人と誤判定される、あるいは、他人が登録されている本人と誤判定されるケースが発生する。前者の割合をFRR（False Reject Rate 誤拒否率）、後者の割合をFAR（False Accept Rate 誤受入率）と呼ぶ。図表2で明らかなようにFRRとFARはトレードオフの関係にあり、安全性を重視してしきい値を高く設定すると、FARが低下するが、FRRが高くなり利便性が低下する。逆に、しきい値を低く設定すると、利便性が高まるが安全性が低下する。このように、FRR、FARはバイオメトリクス認証製品の性能を表す重要な指標である。また、認証を行うためには前もってデータを登録しておく必要があるが、入力データのばらつきと不正なデータの登録を防止するための機能等が原

図表2　バイオメトリクス認証における類似度の判定[6]



（資料）国立研究開発法人産業技術総合研究所「バイオメトリック照合製品プロテクションプロファイル第1.2版」よりみずほ情報総研作成

因で登録に失敗することが起こりえる。この登録に失敗する割合をFTE（Failure To Enrol 生体情報登録失敗率）と呼び、適用性にかかわる指標である。

これら3つの値はバイオメトリクス認証製品の性能を表す値としても利用される。

（2）偽造生体を使用した攻撃への対抗

他人の生体を入力装置に提示して他人になりすますことは困難であることから、バイオメトリクス認証においては、生体的特徴を偽造した人工物等を入力装置に提示して他人になりすますといった攻撃が想定される。バイオメトリクス認証製品は、このような攻撃に対抗することが求められ、認証に使用する生体的特徴に加えて、体温や湿度、動きといった生体の特徴を入力装置で検知して、偽造した人工物等による攻撃かどうかを判断する製品もある。

3. バイオメトリクス認証製品のCCによる評価・認証に向けた取組み

社会的に認知されたセキュリティ評価基準がないことにより、バイオメトリクス認証製品のセキュリティ性を客観的に評価できない状況を改善することを目的として、CCによるバイオメトリクス認証製品の評価・認証に向けた取組み[7]が行われている。これは、平成26年度か

らの3年間で、バイオメトリクス認証製品のセキュリティ評価基盤を整備することを目指した取組みであり、その1つの成果として、平成28年に「バイオメトリック照合製品プロテクションプロファイル　第1.2版」[8]が日本で認証されている（以下、BVPPP）。プロテクションプロファイルとは、IT製品等のセキュリティ要件をISO/IEC 15408[9]に基づいて記述した要求仕様書であり、平成29年1月現在、バイオメトリクス認証製品の評価手法の研究と並行して、このBVPPPに適合したソフトウェアの評価[10]が行われている。BVPPPでは、バイオメトリクス認証製品におけるセキュリティ機能に関し、照合メカニズムの性能（FAR、FRRの値）、ならびに、照合のために参照するデータの登録メカニズムの性能（FTEの値）の宣言、品質の低い生体情報の使用[11]や、偽造生体の使用に対抗する機能の実装を求めている。BVPPPへの適合を主張する製品は、評価機関による評価を受け、宣言された機能および性能が実現されていることが確認される。この結果、認証された製品の性能値（FAR、FRR、FTE）は制度によって保証された値となり、従来の各製品ベンダーが自己評価した結果に基づくカタログ表示等とは、客観性の面で一線を画すことになる。

CCにおいては、異なる制度や異なる評価機関で評価がなされても、その評価結果が均質であることを求めるため、CEM（Common Methodology for Information Technology Security Evaluation：情報技術セキュリティ評価のための共通方法）[12]による評価が行われる。バイオメトリクス認証製品の評価にあたっては、2で述べたような特徴から、CEMに加えて、以下のような評価が求められる。これらはベンダーが行う社内試験、評価機関が行う独立試験、評価機関が行う脆弱性検査に関係する。

・分散の推定、信頼区間の推定を行い、性能値（FAR、FRR、FTE）が信頼区間の上限値を超える値で表されていることを確認する。
・ベンダーが行った社内試験のエビデンスから性能値（FAR、FRR、FTE）を検証するとともに、独立試験を実施し、社内試験エビデンスの適正さを確認する。
・バイオメトリクス認証製品の技術や特徴を踏まえて、脆弱性を検査するための試験を実施する。

CCによる評価・認証に向けた取り組みにおいては、上記の手法をサポート文書にまとめる作業も行われている。この作業は、EUが出資して結成されたバイオメトリクス評価検討組織であるBEAT（Biometric Evaluation and Testing）における脆弱性評価手法の最新動向、および、欧米の海外研究機関による脆弱性評価の最新動向をふまえており、国際標準化を意図したものとなっている。

4. 国際標準化に向けた展望

バイオメトリクス認証製品のCCによる評価・認証に向けた取り組みの成果は国際的に広く認知させるべきものであり、日本での活動もCCRAで世界共通の「国際標準に基づくセキュリティ要件」（cPP（Collaborative Protection Profiles））[13]化するという方針のもとに行われている。cPPは、国際標準として、共通のセキュリティ機能要件、達成可能な保証レベルのミニマムセットを定めるものであり、バイオメトリクス認証製品のcPPが作成されることで、販売先国ごとの評価が不要となって評価コストが低減され、セキュリティ性の客観評価が可能となる。この活動は、国際調達を後押しし、バイオメトリクス認証製品の普及の促進につながるものと思われる。日本は静脈認証製品分野での実績を踏まえ、国際標準化においてイニシアチブをとることが期待される。

注

(1) IoT: Internet of Things コンピュータなどの情報・通信機器だけでなく、様々な物体（モノ）に通信機能を持たせ、インターネットに接続したり通信したりすることにより、相互に制御する仕組み。

(2) financial technology 情報技術（IT）を活用して金融サービスを生み出したり、見直したりする動き。

(3) CC（Common Criteria）とは、情報技術に関連した製品及びシステムが、情報技術セキュリティの観点から適切に設計され、その設計が正しく実装されていることを評価・認証するための国際標準規格である。
http://www.ipa.go.jp/security/jisec/about_cc.html

(4) 「バイオメトリクス認証の特徴」を参照

(5) 指紋を読み取るセンサー、赤外線センサーなど専用のセンサーのほかスマートフォンのカメラなどを利用するケースがある。

(6) バイオメトリック照合製品プロテクションプロファイル1.2版（http://www.ipa.go.jp/security/jisec/certified_pps/c0501/c0501_pp.pdf）の「図3 バイオメトリック照合の類似度分布」を参考に作成。

(7) http://www.jaisa.jp/pdfs/160502/01.pdf

(8) http://www.ipa.go.jp/security/jisec/certified_pps/pp_list.html

(9) IT セキュリティ基準のための評価基準を示す名称としては CC と同じものを意味する。
http://www.ipa.go.jp/security/jisec/about_cc.html

(10) http://www.ipa.go.jp/security/jisec/certified_products/in_eval_list/UR_AndroidOS_software.html

(11) 生体の部位を提示するにあたり、一部を隠すなどによって特徴データの抽出を困難にして誤受入れを行わせることを目的とする。

(12) http://www.ipa.go.jp/security/jisec/cc/index.html

(13) 統一セキュリティ要件（cPP）と関連するサポート文書 http://www.ipa.go.jp/security/jisec/seminar/documents/CCRAReport_20131114.pdf