メディア・セキュリティ
レポート

濱崎 直紀
（学籍番号：28G19096）

令和２年１月14日

1 Chapter 7 : SECURITY OF BIOMETRIC SYSTEM

生体認証システムが満たす必要のある要件は主に 3 つ挙げられる．1 つは整合性である．これは否認防止認証を保証する能力によって決まる．否認防止とは，情報システムの利用や操作，データの送信などに対して，特定の人物が行ったことを後に証明できることを示す．2 つ目は可用性である．これは正規ユーザーが保護されたサービスへのタイムリーで信頼性の高いアクセスを持っているかどうかによって決まる．3 つ目は機密性である．これは保存された個人データが意図された目的のためだけに使用されるかということである．上記の 3 つの要件全てが満たされていない場合，生体認証システムは失敗していると見なされる．この失敗を引き起こす障害は種類に応じて Daniel-of-service(DoS)，Instruction，Repudiation，Function creep に分けられる．

生体認証の信頼はこれらの脅威から保護する能力にかかっているが，絶対に安全で確実なシステムはなく，確保されるセキュリティのレベルはアプリケーションに依存する．

生体認証システムのセキュリティを分析する最初のステップは，様々な脅威エージェントと攻撃する脅威モデルを定義することである．ここで脅威エージェントには 2 種類考えられる．1 つは他人受容，本人拒否やサンプル取得の失敗，登録の失敗などのようなシステムにおける障害である．これらの障害は意図的な攻撃ではなく，生体認証システムの様々なモジュールが原因で発生する（ゼロエフォート攻撃）．もう 1 つは詐称者，攻撃者によって引き起こされる障害である．詐称者は別の登録者になりすまそうとする個人を指し，攻撃者は生体認証システムの動作を妨害しようとする個人を指す．ここでは，攻撃者が実行できる攻撃に焦点を当てる．

そのような攻撃として，まずインサイダー攻撃が挙げられる．これは正規ユーザー自身がシステムを意図的に破壊する場合だけでなく，外部の敵がインサイダーの直接的または間接的な関与により生体認証システムを回避する場合も含む．生体認証システムでは多くの段階で人間の関与が必要であり，これが悪用される恐れがある．

もう 1 つの例としてインフラストラクチャ攻撃がある．これは攻撃者が生体認証インフラストラクチャを操作することでセキュリティを侵害するものである．

他の攻撃パターンとして，攻撃者が生体認証特性を提示して，システムに侵入しようとする試みがある．これはユーザーインターフェースレベルでの攻撃と見なすことができ，次のような攻撃と対策が存在する．

まずは「なりすまし（impersonation）」である．これは詐欺師自身が別の正規ユーザになりすましてシステムに侵入しようとする状況を指す．これには生体認証システムの誤一致率（FMR）をできる限り低くし，時間枠内で認証における失敗回数を制限することにより対策が可能である．

次に「難読化」である．これは生体認証システムによる検出を回避するために攻撃者が生体認証特性を変更しようとする状況を指す．つまり，難読化は攻撃者が自分の身元を隠したい場合に使用される．この攻撃の対策としては，ユーザ内変動に対してのシステムの堅牢性を改善することや，変更された部分を検出し，そのユーザーを二次検査にかけることなどが挙げられる．

最後に「なりすまし（spoofing）」である．これは他人から取得した生体認証特性から偽造した生体認証特性を用いて認証を試みる攻撃のことである．これを検出することは，本人の生体認証特性と他のソースを介した生体認証特性を区別することであり，そのようなシステムの開発が必要である．

また，攻撃者が生体認証システムのモジュールを直接弱体化したり，モジュール間の通信を操作することによる攻撃も存在する．これは，攻撃者が不正な変更を行うか，実装における障害を悪用することによって実現される．

不正な変更の例として「トロイの木馬」がある．トロイの木馬は自身をモジュールの 1 つとして偽装するこ

とでモジュール間の通信に侵入し，攻撃者が希望する値を後続のモジュールへ渡すことが可能となる．この攻撃の対策は，モジュール間の相互認証を使用して通信の双方向における信頼性が確立している生体認証システムを用いることである．加えて，ソフトウェアの安全な実行を強制できるコード実行プラクティスまたは改ざん防止ハードウェアを使用することも有用である．

また，実際には無視できる例外入力などを用いた攻撃など，システムの抜け穴を悪用される恐れもある．攻撃者はこれを実行するために少なくとも 1 つ以上のモジュールを経由する必要があるため，十分にテストされた生体認証アルゴリズムを使用することで，この悪用を防ぐことができる．

モジュール間の通信における攻撃には「中間者攻撃」「リプレイ攻撃」「ヒルクライミング攻撃」がある．中間者攻撃はすでに通信中の 2 つの接続間に独立した接続を確立し，それらの間でメッセージを中継し盗聴を行う．この対策としては，生体認証モジュール間の相互認証が挙げられる．リプレイ攻撃は保護されていない転送中のデータを傍受し，不正に利用する攻撃である．この対策として，その時限りのキーを生成するワンタイムセッションキーなどがある．ヒルクライミング攻撃は，一致スコア情報を利用し，人工的に生成された特徴ベクトルからその応答の一致スコアを記録していき，より高いスコアがでた場合はその特徴ベクトルを保持するという反復を行うことで，設定された閾値を越えることを目的とした攻撃である．時間枠内における失敗回数の制限などが主な対策となる．

最後に，生体認証テンプレートのデータベースへの攻撃が 2 種類考えられる．1 つは，テンプレートデータベースのハッキングまたは変更である．これにより，不正なアクセスや正規ユーザーのアクセス拒否が可能になる．このような脅威を軽減するためには，データベースアクセスを厳密に制御する必要がある．もう 1 つは生体認証テンプレートの漏洩である．生体認証はパスワードとは異なり再発行などができないため，漏洩は非常に深刻な問題である．よって，対策を練ることが大事であるが，生体認証ではユーザー内変動が存在するため，パスワードにおけるセキュリティシステムを用いることはできない．そこで，生体認証テンプレートを保護する最も簡単な方法として，RSA や AES などの標準的な暗号化技術を用いてテンプレートを暗号化する手法がある．しかし生体認証においては，暗号化されたドメインで直接マッチングを行うことができないため，認証試行中には復号化する必要があり，テンプレートを保護する手法としては不十分である．その問題を克服するための手法として，特徴変換アプローチと生体認証暗号システムが提案されている．

特徴変換アプローチでは，生体認証テンプレートに対して変換関数を適用し，それによって変換されたテンプレートのみがデータベースに保存される．クエリ特徴にも同じ変換関数が適用され，変換されたテンプレートと直接照合が行われる．変換関数が可逆的である場合は，攻撃者によって復元される恐れがあるが，ユーザー固有のキーを用いることから，特徴空間でのユーザー間の分離性が向上し，誤一致率が低下するというメリットがある，変換関数が非可逆的である場合は，攻撃者がテンプレートを復元することが困難であるという明確なメリットがある．変換のパラメーターが危険にさらされた場合でも，元の生体認証テンプレートを回復するのは難しいため，可逆変換アプローチよりも優れたセキュリティを提供する．しかし，高い認識パフォーマンスを保持しながら，非可逆的である変換関数を設計することが困難であるというデメリットがある．

生体認証暗号システムは，生体特徴から暗号キーを直接生成する手法であり，例としてキーバインドシステムが挙げられる．これは，キーと生体認証テンプレートをバインドして，両方の情報を持つ 1 つの存在をデータベースに保存するシステムである．ユーザーの生体認証データがなければ，キーまたはテンプレートをデコードすることは困難であり，秘匿性に優れている．

このように生体認証は多くのセキュリティ脅威に対して脆弱であり，その対策が非常に重要となっている．しかし，すべての要件に対しての完璧な手法はなく，それぞれの脅威に対して適切な手法を用いることが大切であると言える．

2　最新のバイオメトリクス認証

一言でバイオメトリクス認証と言っても，様々な種類がある．それらは大きく分けて身体的生体認証と行動的生体認証に分けられる．

まず，最新の身体的生体認証に注目する．これは個人の持つ身体的特徴を利用して認証するものである．最近では，スマートフォンの認証に指紋や顔認証が使われるなど，非常に一般的な認証方法になっている．日常でよく目にするのは指紋，顔による認証であるが，最新の研究では虹彩を利用した技術も開発されている．これは歩きながらでも，虹彩を高精度かつ迅速に認証するというものである．これを実現する技術は「歩行者の虹彩を鮮明かつ高解像度に撮影する技術」と「撮影後の画像処理を高速化する画像解析技術」である．まず，歩行者の目の周辺領域の位置を正確に推定する技術を開発することで，画像データ量を削減し，高解像度に撮影することを実現している．これにより，利用者がカメラの正面に静止したり，目の位置をカメラに合わせたりするなどの手間を省くことが可能となっている．また，撮影画像から虹彩認証に適した画質の画像のみを高速に抽出する技術の開発により，瞬時に虹彩認証を行うことを可能としている．認証の手間を大幅に削減できることから，空港や改札などでの活用が見込まれている．

しかし，こうした身体的生体認証の問題点として，「突破される可能性が比較的高い」ということが挙げられる．例えば指紋認証においては，画像解析などで指紋を取られる恐れがあり，取られた場合は他人による認証の突破が容易となってしまう．それだけでなく，指紋や虹彩ではパターンの偽造による攻撃手法も考案されており，安全性の低さが問題視されている側面もある．さらに身体的生体認証にはプライバシーの問題もある．身体的生体認証では生体情報を登録する必要があるため，これらの情報が盗まれた場合に，プライバシーが侵害される恐れがある．このように日常的に使われている身体的生体認証であるが，問題が幾つか存在する．

次に，最新の行動的生体認証に注目する．行動的生体認証は，デバイス側がユーザーの行動を直接集め，その癖やパターンから認証を行う方法であり，身体的生体認証に比べて「突破されにくく，プライバシー性の高い認証」とされている．先ほど述べた通り，身体的生体認証では生体情報が盗まれることにより突破される危険がある．しかし，行動的生体認証における「行動の癖」は非常に複雑なデータから成るため，それらが盗まれたとしても，他人による突破は難しいとされている．また，行動の癖のデータは盗まれたとしても，個人を特定することは非常に難しく，プライバシーの問題も解決できる．実際に，歩圧と歩き方のモデルから行動生体認証を可能にする研究などが進められており，非常に高精度であるという結果も得られている．しかし，行動的生体認証にも「環境や外的要因に大きく作用される」という問題点がある．つまりその人の置かれている状況（酩酊状態や急いでいる時など）によって行動が変化してしまい，現状の技術ではそのような変化に対応することが難しいということである．この問題が致命的なこともあり，行動的生体認証は身体的生体認証に比べて普及が進んでいない．

このように，生体認証は日々研究されており，問題点が指摘されつつも，現状のセキュリティシステムとして幅広く使用されている．2020 年の東京オリンピック・パラリンピックでは NEC の顔認証システムが採用されることが決定されており，生体情報による認証は今後も使用されていくことが予想される．