2 バイオメトリック認証システムのセキュリティ評価

三村 昌弘
(株)日立製作所 システム開発研究所
mmimura@sdl.hitachi.co.jp

昨今，バイオメトリック認証システムの安全性を議論するにあたり，他人受入率といった精度や，生体情報の偽造耐性が注目されている．しかし，実用的な観点からバイオメトリック認証システムの安全性を保証するには，認証装置の精度やセキュリティ対策（偽造耐性など）だけに注目するのではなく，実利用時の認証システムや運用要件による対策まで含めて評価しなければならない．現在，この考えに基づいたバイオメトリック認証システムのセキュリティ評価基準（ISO/IEC 19792）が，国際標準として策定されつつある．本稿では，国際標準案における評価の基本的なポリシー，評価参照モデル，評価すべき脆弱性などについて解説し，バイオメトリクスの安全性に関する正しい理解を促すことを狙いとしている．

はじめに：バイオメトリクスのセキュリティ評価と国際標準規格

近年，バイオメトリクスは，電子パスポートや銀行ATMにおける本人確認や，企業情報システムにおけるアクセスコントロールなど，情報セキュリティ技術の1つとして急速に普及しつつある．特に電子パスポートや銀行ATMなどの公共性の高い分野においては，バイオメトリック認証システムの安全性を保証することが重要な課題である[1)]．

当然ながら，安全性を保証するには何らかの評価の基準が必要であるし，その基準は広く共通化されていることが望ましい．バイオメトリック認証システムもIT製品の一種なので，ITセキュリティの国際評価基準であるISO/IEC 15408[2)] を適用することが可能である．しかし，ISO/IEC 15408は一般的なITシステムを対象としており，バイオメトリクス特有の問題には言及していない．そのため，ISO/IEC 15408をバイオメトリクスに適用するには，開発者・評価者が独自にバイオメトリクス特有の性質に対応したセキュリティ要件や評価方法を詳細化しなければならず，評価コストが大きいことが課題であった(図-1)．

この背景から，現在，ISO/IEC JTC1 SC27では，バイオメトリクスの安全性を評価するための国際標準規格であるISO/IEC 19792 "Security Evaluation of Biometrics"が策定中である（2006/4現在）．同標準規格では，バイオメトリック認証システムの安全性を評価するための評価項目や基本的な評価の考え方といった，最上位の要件が記載されている．本稿では，国際標準案における評価の基本的なポリシー，評価参照モデル，評価すべき脆弱性などについて解説する．

セキュリティ評価のフレームワーク

図-2はバイオメトリック認証システムのセキュリティ評価における基本的なフレームワークを示している．評価の対象となるバイオメトリック認証システムを中心に，開発者，評価者，評価結果の利用者の関係が示されている．バイオメトリック認証システムの評価には，高度に専門的な知識（たとえば生体情報の照合に用いられる画像処理技術など）が要求される場合があるため，評価者が単独で認証システムを評価することは困難と予想される．そのため，開発者が評価を実施するために必要な情報を評価者に提供し，評価者はその妥当性を検証する方が適している．

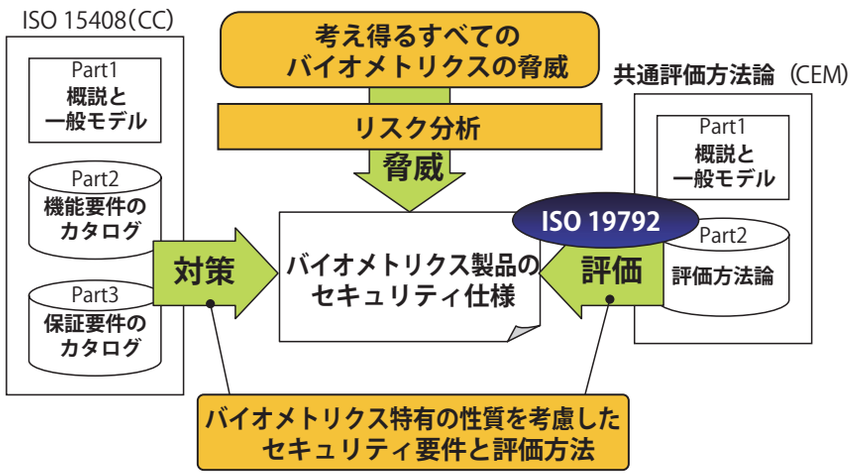

図-1 ISO/IEC 15408によるバイオメトリック認証システムの評価

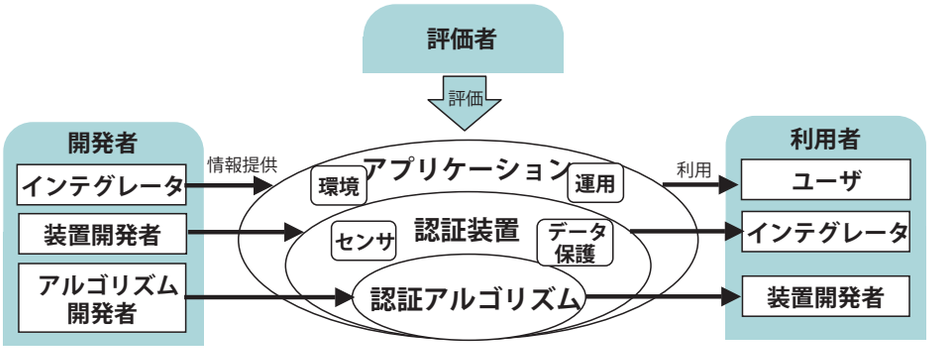

図-2 セキュリティ評価のフレームワーク

評価対象となるバイオメトリック認証システムは，3つのレベル（認証アルゴリズム，認証装置，アプリケーション）に分かれている．認証装置には，認証アルゴリズムに加え，センサや生体情報などのデータを保護する機能が含まれる．またアプリケーションは認証装置に加えて，装置の運用条件や物理的な環境条件が含まれる．各レベルに含まれる機能に応じて評価の観点も異なるため，対象に合わせて3つの評価レベルが存在する．評価レベルは独立しているわけではなく，アプリケーションの評価は認証装置の評価を，認証装置の評価は認証アルゴリズムの評価を含む階層構造をとっている．これは，認証アルゴリズムや認証装置のレベルにおいて必ずしも安全性が保たれていなくてもよいことを意味する．たとえば，認証装置において脆弱性が存在したとしても，アプリケーションのレベルで運用や環境条件によってその対策が実施できればよい．そのためには，認証装置に存在する脆弱性を利用者であるインテグレータが認識し，アプリケーションのレベルで対策を施し，最終的にアプリケーションレベルでの評価結果をユーザが利用する，図-2に示すような評価フレームワークが必要となる．

バイオメトリック認証システムの参照モデルと評価レベル

図-3はセキュリティ評価におけるバイオメトリック認証システムの参照モデルを示している．バイオメトリック認証システムにおける各機能グループは認証アルゴリズム，認証装置，アプリケーションの3つのレベルにまとめられている．認証アルゴリズムは主に照合を行うための画像処理・信号処理にかかわる機能群を指す．認証装置はコンポーネントを含み，さらに生体情報を取得するためのセンサ，生体情報の特徴量と利用者IDなどをまとめた登録データを生成する機能，登録データを保管

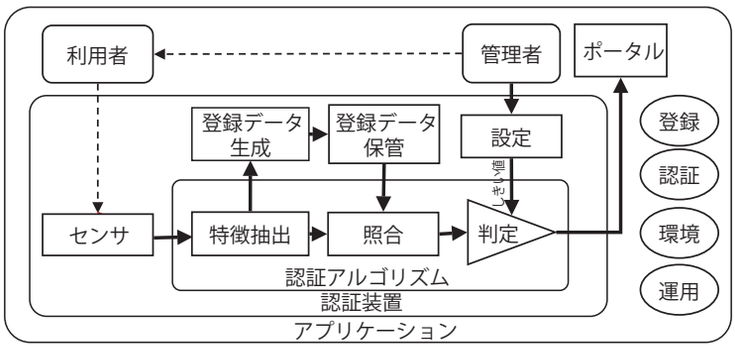

図-3　評価の参照モデル

する機能，コンポーネントやセンサに対してしきい値などのパラメータを設定する機能を含む．設定機能や登録データ保管機能は管理者が操作することを想定しており，管理者の権限確認機能（アクセスコントロール）を含んでいる．アプリケーションは認証装置を含み，さらに認証装置を利用するシステムと連携するためのポータル機能，利用者の性質（振る舞いや生体情報の質），利用者あるいは管理者に課される運用条件，システムが利用される物理的な環境（温度・湿度・照明環境など）を含む．

それぞれの機能グループで評価の観点は異なってくる．認証アルゴリズムにおいては，特徴抽出や照合，判定を行う画像処理・信号処理機能の精度や，想定しないデータの入力に対して誤動作を生じないような実装上の頑強さを確認することが評価の目的になる．認証装置では，さらにセンサの性能を含めた精度や，生体情報・認証結果を保護する機能の有無が重要になる．また，アプリケーションとしては，認証装置を利用する上での，登録・認証作業の運用方法やセンサの周囲の環境を含めた上で，バイオメトリック認証システムの精度，生体情報・認証結果の保護，バイオメトリクス特有の問題への対策状況を総合的に評価する必要がある．

このように，バイオメトリック認証システムの機能グループによって評価の観点が異なるため，評価は機能グループごとに実施するのが妥当である．ISO/IEC 19792 "Security Evaluation of Biometrics"ではこれを評価レベルと呼んでいる．ただし，それぞれの評価レベルは完全に独立しているわけではない．認証装置を評価するためには，当然その下位の認証アルゴリズムの評価も行わなければならない．したがって評価レベルは，図-2に示すように，アプリケーションの評価は認証装置の評価を，認証装置の評価は認証アルゴリズムの評価を含む階層構造をとる．

■評価項目

バイオメトリクスの安全性を示す指標としては，誤って他人を受け入れてしまうエラーの発生率，すなわち他人受入率（FAR：False Accept Rate）がよく知られている．他人受入率は認証システムの性能の1つであるが，他人受入率が十分に低ければ安全性は高いといえるため，安全性を示す指標でもある．また，バイオメトリック認証システムをIT製品として捉えた場合は，指紋画像や顔画像といった生体情報や，生体情報から個人を識別するための特徴を抽出したテンプレート，およびシステムが出力する最終的な認証結果などの漏洩や改ざんに対する対策状況が安全性の指標となる．さらに指紋や虹彩の偽造といった問題も指摘されている[3]．このようなバイオメトリクス特有の弱点（脆弱性）は偽造だけではない[4]．そのため，バイオメトリック認証システムの安全性を示すには，バイオメトリクス特有のあらゆる脆弱性に対する対策状況を把握する必要がある．

このように，バイオメトリック認証システムの安全性を評価するには，性能，ITシステム，バイオメトリクス特有の脆弱性，の3つの観点からアプローチしなければならない．各指標に沿った評価の基準として，性能面やITシステムの面からは，それぞれバイオメトリック認証システムの精度評価基準[5] やITセキュリティの評価基準（ISO/IEC 15408）が策定されている．現在策定が進められているISO/IEC 19792 "Security Evaluation of Biometrics"はすべての評価項目を含むが，おもにバイオメトリクス特有の脆弱性に関する評価を中心に扱っている．

バイオメトリクスに特有の脆弱性としては，指紋や虹彩の偽造が知られている．正確に言えば，「生体情報としてバイオメトリック認証システムに受け入れられる人工物が作成され得る性質」が脆弱性になる．この種の脆

評価レベル		認証アルゴリズム	認証装置	アプリケーション	関連評価基準
評価結果の利用者		装置開発者	インテグレータ	ユーザ	—
評価項目	精度	生体情報DBに基づく精度評価	センサの性能を含めた精度評価	運用における環境を含めた精度評価	ISO/IEC 19795
	データ保護	—	装置の機能によるデータ保護対策状況の評価	運用を含めたデータ保護対策状況の評価	ISO/IEC 15408
	脆弱性	アルゴリズムに存在する脆弱性の評価	装置の機能による脆弱性対策の評価	運用を含めた脆弱性対策の評価	ISO/IEC 19792（策定中）

表-1　評価レベルと評価項目の関係

弱性はほかにもあり，大きくはバイオメトリクス特有の性質に起因する脆弱性と，脆弱性の程度（攻撃のしやすさ）がバイオメトリクス特有の脆弱性の2つに分類できる．

バイオメトリクス特有の性質に起因する脆弱性としては，たとえば「生体情報は意識的に秘匿することが困難な性質」があり得る．パスワードやICカードなどの本人確認手段は，それらが秘匿される，すなわち他人に教えたり貸したりしないことを前提に運用される．一方，生体情報は個人の身体情報や行動情報であるため，必ずしも秘匿できるとは限らない．指紋は遺留するし，顔はいつも他人にさらしている．つまり自分の意思で秘匿することが困難な性質を持つことがあるといえる．

脆弱性の程度がバイオメトリクスに特有のものとしては，先に挙げた偽造がある．これをパスワードにあてはめて考えてみると，パスワードは入手さえできれば誰でも入力できるので，偽造そのものが必要ない．一方，ICカードの偽造には相当のコストがかかることが知られている．生体情報の偽造コストは，おそらくこれらの中間（幅はあるが）に位置するだろう．

このようにバイオメトリクスには，他の本人確認手段にはない特有の性質があり，この性質を攻撃される可能性がある．そのため，バイオメトリック認証システムの安全性を考える際には，これらの性質がどの程度脆弱なのか，つまりどの程度簡単に攻撃者に利用されてしまうのか，について評価しなければならない．

■評価の進め方

表-1は前出の評価レベルと評価項目の関係を示している．

アルゴリズムを評価対象とした場合，評価結果を利用するのはアルゴリズムを利用する装置開発者が想定される．精度に関する評価としては，センサを含まないため，生体情報DBなどあらかじめ何らかの手段で収集された生体情報を利用した実験的な精度評価を実施する．データ保護に関しては，この段階で評価する必要はなく，上位の評価レベルでアルゴリズムを実装した場合に評価される．アルゴリズムに存在する脆弱性としては，主に生体情報自身の性質により他人受入を引き起こすケースや，想定外のデータの入力により他人受入を引き起こすケースがある．前者は，たとえば顔認証において一卵性の双子を識別することが困難な性質などを指している．後者としては，ノイズ画像の入力による誤動作などがあり得る．これらの脆弱性は，必ずしもアルゴリズムのレベルのみで対策される必要はない．重要なのは，アルゴリズムレベルで脆弱性が存在する場合，その事実を利用者である装置開発者が理解し，装置のレベルで必要な対策を施すことにある．

認証装置を対象とした場合，評価結果を利用するのは装置を利用するインテグレータである．精度に関する評価は，アルゴリズムレベルでの精度評価に加え，実際に使用するセンサで収集した生体情報に基づいた精度評価を実施する．この際，生体情報を収集する物理的な環境は装置開発者が制御するが，他人受入率に影響を及ぼす環境条件を報告しなければならない．インテグレータはこれらの環境条件を考慮して，アプリケーションで装置を利用する際の環境条件を決定する必要がある．装置レベルの評価では，生体情報・認証結果・他人受入にかかわるパラメータの設定などに関し，装置の機能により保護対策がとられているかを評価する．具体的には，暗号・署名による生体情報・認証結果の保護機能や，設定でき

るパラメータの範囲限定，パラメータ設定に要求するアクセス権限などである．また，脆弱性については，センサや生体情報の取得機能などに存在する脆弱性とその対策が評価される．具体的には，生体情報の複製や，生体情報の入手の容易性などがある．対策としては，偽造物の検知機能や生体の検知機能が考えられる．先の認証アルゴリズムレベルの評価と同様，データ保護や偽造などの脆弱性対策がすべて認証装置レベルで実施されている必要はない．認証装置レベルで対策されていない場合は，さらに上位のアプリケーションにおける運用などで対策することもできるからである．認証装置レベルでこれらの対策を実施するか否かは，費用対効果の観点から検討されるべきであり，同じ効果を持った対策をより安価にアプリケーションのレベルで実施することができるのであれば，必ずしも装置レベルでの対策は必要とされない．もちろん，評価結果を利用するインテグレータは，装置レベルに残る問題を認識し，装置の設置場所（環境条件），登録作業の運用要件，管理者の運用要件など，運用で解決しなければならない．

アプリケーションレベルを評価の対象とした場合，評価結果の利用者はバイオメトリック認証システムを導入するユーザとなる．アプリケーションレベルの評価は，認証装置レベルの評価を含み，さらに運用による対策を考慮した評価を実施する．最終的なバイオメトリック認証システムの安全性は，この運用による対策を含めて総合的に判断される．これは，ユーザにとってアルゴリズムや認証装置のレベルに脆弱性が存在することは大きな問題とはなり得ないことを意味する．ユーザにとって重要なのは，あくまでアプリケーションレベルによる運用まで含めた総合的な評価結果であり，運用まで含めたとしてもまだ残っている脆弱性に対して，そのリスクを評価し，どのように対応するかを決定することにある．

おわりに：安全なバイオメトリック認証システムの実現に向けて

本稿では，現在策定が進められているバイオメトリクスのセキュリティ評価標準における，評価の基本的な考え方を紹介した．安全なバイオメトリック認証システムの実現には，具体的な評価方法の検討，公的な評価機関の設立，評価結果の認定制度の整備など，まだ多くの課題が残る．その一方で，バイオメトリクスは電子パスポートをはじめとした公共性の高い分野に向けて急速に展開しつつあり，安全性保証のニーズはすぐにでも立ち上がると予想される．両者には大きなギャップがあると言わざるを得ない状況である．

バイオメトリクス技術は画像処理・信号処理から発達した技術であるため，バイオメトリクスの専門家は必ずしもITセキュリティの専門家ではない．今後は，バイオメトリクス技術とITセキュリティを融合した分野の技術者を育成することも，上記のギャップを埋めるために必要である．本稿が，研究者・技術者のバイオメトリクスとITセキュリティの融合分野への参画を促す一助となれば幸いである．

参考文献

1）瀬戸編著：ユビキタス時代のバイオメトリクスセキュリティ，日本工業出版（2003）．
2）ISO/IEC 15408：Information Technology - Security Techniques - Evaluation Criteria for IT Security.
3）松本：Impact of Artificial Gummy Fingers on Fingerprint Systems, proc. SPIE Optical Security and Counterfeit Deterrence Techniques IV（2002）.
4）三村：バイオメトリクス技術の脆弱性とその対策：セキュリティ評価，電子情報通信学会 バイオメトリクスセキュリティ研究会（2005）.
5）ISO/IEC 19795:2006：Biometric Performance Testing and Reporting - Part 1, Principles and Framework, International Organization for Standardization.

（平成18年4月28日受付）