平成１７年度経済産業省　産業技術研究開発委託事業－１
生体情報による個人識別技術（バイオメトリクス）を
利用した社会基盤構築に関する標準化

第７部　共同研究（早稲田大学）

平成１８年３月

財団法人ニューメディア開発協会

７　共同研究について

７．１　共同研究報告書（早稲田大学小松尚久）

－バイオメトリクスセキュリティ評価基準に関する研究－
－バイオメトリクスの安全性（脆弱性、対策技術）に関する研究動向－

（１） はじめに

昨今，バイオメトリクスの安全性に対する関心が高まっているが，現在，国内では主として以下の組織や研究プロジェクトによる活動を通じて，バイオメトリクスの安全性に関する検討が行われている．

(a) 経済産業省 基準認証研究開発事業「生体情報による個人識別技術を利用した社会基盤構築に関する標準化」（本事業）
(b) 電子情報通信学会（通信ソサイエティ）第二種研究会「ユビキタス社会におけるバイオメトリクスセキュリティ研究会」
(c) BSC（バイオメトリクスセキュリティコンソーシアム）「バイオメトリクスの安全性検討 WG（ワーキンググループ）」
(d) SSR（産学戦略的研究フォーラム）「バイオメトリクス個人認証の安全性に関する調査研究」

これらの組織やプロジェクトは相互に関連性をもち，一部では連携を図りながら活動を展開しているが，本節では，特に BSC「バイオメトリクスの安全性検討 WG」（以下，BSC 安全性検討 WG）および SSR「バイオメトリクス個人認証の安全性に関する調査研究」（以下，SSR 調査研究）における活動を取り上げ，バイオメトリクスの安全性に関する現在の検討状況について報告する．ここで，BSC 安全性検討 WG および SSR 調査研究の位置付けであるが，BSC 安全性検討 WG では，バイオメトリクスの安全性に関する情報の収集，バイオメトリクスの脆弱性情報に関する公開ガイドラインの策定，バイオメトリクスの安全性（脆弱性，攻撃，対策技術）に関するフレームワークの構築を活動の主旨とし，一方，SSR 調査研究では，海外におけるバイオメトリクスの安全性に関する情報の収集および海外の研究機関との共同研究体制の確立を活動の主旨としている．両者は 2005 年 8 月の検討組織設置以来，緊密に連携を取りながら活動を展開しており，特に，毎月開催される研究会（一部は BSC 安全性検討 WG と SSR 調査研究の共同開催）では，バイオメトリクスの安全性に関する最新動向を調査すべく，当該分野の代表的な研究者を講師として招聘し，最新の研究成果や技術動向の紹介を行った．そこで，本節ではこれまでの活動を通して得られた情報を整理し，バイオメトリクスの安全性に関する技術の現状と今後の動向について，セキュリティ評価，生体検知技術，テンプレート保護技術の三つの観点から解説を加

えることを目的とする．

（２） セキュリティ評価 [1]

バイオメトリクスを情報セキュリティ技術として利用するためには，バイオメトリクスのセキュリティ評価を行うためのフレームワークが不可欠となる．そこで，本節ではバイオメトリクスのセキュリティ評価に関する国際標準案 ISO/IEC 19792（”A framework for security evaluation and testing of biometric technology”）について取り上げ，その概要について解説する（図１参照）．

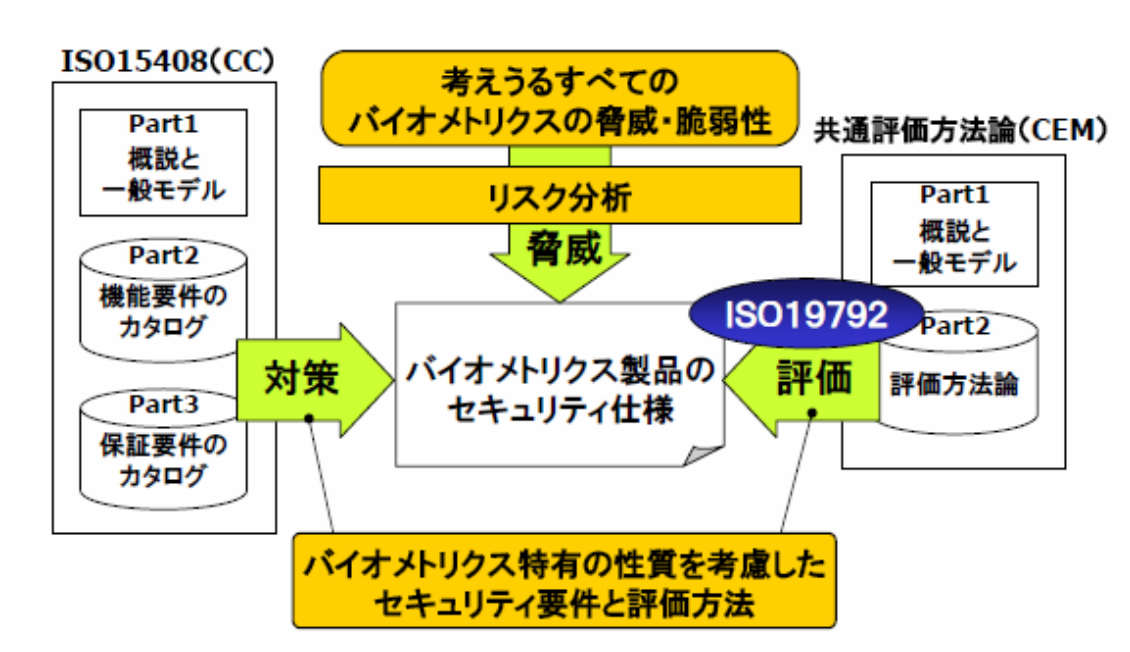

図１：バイオメトリクスの安全性評価における ISO/IEC 19792 の位置付け[1]

ISO/IEC 19792 は，バイオメトリクスのセキュリティ評価における要件を提示しており，基本コンセプト（Basic Concept）として，評価の対象・目的に合わせた３つのセキュリティ評価レベル（Component level, System level, Application level）を導入している点が特徴として挙げられる．ここで，Component level は認証アルゴリズムの評価，System level は制御可能な環境下におけるシステムの評価，Application level は実運用システムの評価に関するレベルをそれぞれ表す．精度評価の実施にあたっては，①セキュリティに関係する精度（FAR：他人受入率）を評価すること，②FAR の原因を分析すること，③異なる評価レベル間での精度評価結果に矛盾がないこと，④精度の信頼区間は要求される保証レベルを満足すること，⑤ベンダによる精度評価の方法および結果の妥当性を検証すること等が要求される．本標準案では，バイオメトリクス認証システムは代替手段を持つことを想定しているため，FRR（本人拒否率）は精度評価の対象外となっている．また，脆弱性評価（Vulnerability Assessment）については，①生体情報の性質に起因する脆弱性（生体情報の複製，秘匿の困難性，経年変化等）の評価，②バイオメトリクス装置に特有の脆弱性

（しきい値の設定等）の評価，③一般的な IT に共通する脆弱性（生体情報の漏洩，改ざん等）の評価等が要求される．さらに，プライバシ保護の観点から評価すべきシステムの仕様についても規定されており，①生体情報やテンプレートへの不正アクセスを防止すること，②Application level では評価者がプライバシ保護を不要と判断した場合にはその根拠を示し，判断がつかない場合にはプライバシ保護を必要とすることを推奨すること，③利用者の認識なしにテンプレートが使用されることを防止する機能を確認すること，④利用者に関する情報をシステムから削除する機能を確認すること，⑤利用者へバイオメトリクスの利用を告知する機能を確認すること等が要求される．本標準案は，2005 年 8 月に 4th Working Draft が発行され，同年 10 月末に Working Draft へのコメントが締め切られた．今後，アルゴリズム，装置，システム等の開発者は，設計段階での自己評価用に，また，評価標準や評価方法の策定者は，最上位の要件集として本標準案を利用することが期待される．

（３）生体検知技術 [2]

バイオメトリクスシステムの脆弱性を利用したなりすましの脅威が指摘されている．このようななりすましの脅威に対する対策技術の一つとして，現在，生体検知機能を組み込んだバイオメトリクスシステムの有効性に関する検討が盛んに行われている．そこで，本節ではバイオメトリクスシステムの脆弱性に対する対策技術の一つである生体検知技術に着目し，生体検知機能に必要とされるセキュリティ要件およびそれに基づくバイオメトリクスシステムの分類法について解説する．生体検知機能は，バイオメトリクスシステムにおいて，登録・照合時に読み取られた生体特徴情報（人間の身体的・行動的特徴のアナログ情報）が，生きている人間から読み取られたものか否かを自動的に確認する機能と定義することができる．また，被認証者が生きている人間か否かを確認する目的で読み取られるアナログ情報を生体検知情報と定義すると，攻撃者が生体特徴情報を偽造して提示するとともに，自分の生体検知情報を提示するか，または生体検知情報を偽造して提示することにより第三者へのなりすましを試みる脅威が想定される．このようななりすましに対抗するためには，次の二つのセキュリティ要件を満足する必要がある．①生体検知情報と生体特徴情報がそれぞれ読み取られた被認証物が同一か否かを確認可能であること，②生体検知情報が生きている人間から読み取られたか否かを確認可能であること．ここで，①は攻撃者自身の生体検知情報の提示による脅威に対応し，②は偽造した生体検知情報の提示による脅威に対応したセキュリティ要件となっている．①の要件を満足するためには，生体検知情報の読取形態に着目し，②の要件を満足するためには，読取時に付与する刺激の形態に着目する方法が考えられる．生体検知情報の読取形態については，二つの情報の読取タイミングが同一であるか否かという観点と，二つの情報の読取部位が同一であるか否かという観点に基づく分類が可能であり，これらを組合せることにより，以下の四種類の分類が可能となる．1．完全同一型：読取タイミングおよび読取部位が同じである．2．同時

読取型：読取タイミングは同じであるが読取部位は異なる．3．同位読取型：読取タイミングは異なるが読取部位は同じである．4．独立読取型：読取タイミングおよび読取部位が異なる．一方，読取時に付与する刺激の形態については，以下の三種類の分類が可能である．a．変化非誘発型：読取部位の状態変化の誘発を意図しない刺激を付与する．b．固定パターン刺激型：読取部位の状態変化の誘発を意図し，一定のパターンで変化する刺激を付与する．c．ランダム刺激型：読取部位の状態変化の誘発を意図し，ランダムに変化する刺激を付与する．以上の点を考慮すると，生体検知情報の読取形態（1～4）と読取時に付与する刺激の形態（a～c）の組合せに基づき，バイオメトリクスシステムは 12 種類に分類することができる．図２は，生体検知機能を組み込んだ指紋認証装置（左）と虹彩認証装置（右）の例を示したものである．同図左の指紋認証装置では，指の静電容量に基づき生体検知を行うが，当該装置による生体検知は，生体検知情報の読取形態の観点からは完全同一型，読取時に付与する刺激の形態の観点からは変化非誘発型に分類される．一方，同図右の虹彩認証装置では，瞳孔の拡張・収縮といった目の特性に基づき生体検知を行うが，当該装置による生体検知は，生体検知情報の読取形態の観点からは同時読取型，読取時に付与する刺激の形態の観点からは固定パターン刺激型あるいはランダム刺激型に分類される．当該分野における今後の課題として，バイオメトリクスシステムの分類法の精緻化，生体検知情報の再現困難性の評価等が挙げられる．

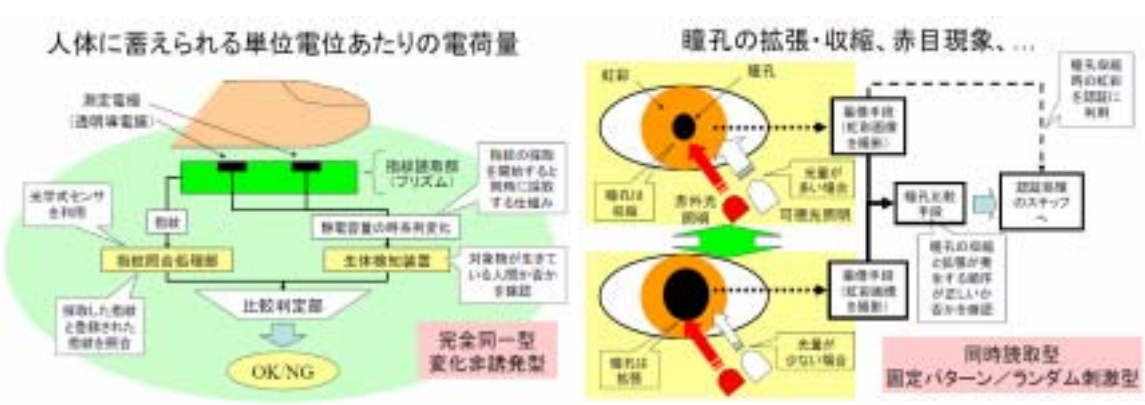

図２：生体検知機能を組み込んだ指紋認証装置（左）と虹彩認証装置（右）[2]

（４）テンプレート保護技術 [3]

バイオメトリクスシステムは，生体情報が漏洩した場合に生体情報を取り替えることができないという問題点を有する．そこで，一旦登録したテンプレートを再登録により無効化する技術や，テンプレートから元の生体情報を復元したり他の装置用のテンプレートに作り変えたりする操作を不可能にする技術が必要となる．そこで，本節ではこのようなバイオメトリクスシステムにおけるテンプレート保護技術の現状について整理する．テンプレート保護技術に関しては，これまで多くの方式が提案されているが，主として以下のような手法を単独または組合せて用いることにより実現されることが多い．

（**A**）幾何学的変換（Geometric transformation）

【特徴】秘密関数に基づき画像やテンプレートを変形あるいはスクランブルする方式．照合時も同一の関数を使用．

【利点】関数のパラメータを変えることによりテンプレートの無効化が可能．従来のマッチングアルゴリズムをそのまま使用することが可能．

【課題】ヒルクライミング・アタックに対する脆弱性の問題．

【事例】Ratha, “Cancelable biometrics”, 2001.

（**B**）信号の部分的削除（Partial signal removal）

【特徴】原画像の位相情報のみ，または元のテンプレートの一部のビットのみを使用する方式．

【利点】元の信号を復元することが非常に困難．ヒルクライミング・アタックに対する耐性あり．

【課題】テンプレートの無効化に関する問題．生体情報の大きな変動に対する耐性の問題．

（**C**）ランダムパターンとの畳み込み（Convolution with random patterns）

【特徴】ランダムパターンとの畳み込みにより生成されたテンプレートを用いて照合を行う方式．

【利点】ランダムパターンのパラメータを変えることによりテンプレートの無効化が可能．元の信号を復元することが非常に困難．ヒルクライミング・アタックに対する耐性あり．

【課題】生体情報の変動に対する耐性の問題．

【事例】Soutar, “Bioscript”, 1998.

（**D**）統計モデル（Statistical model）

【特徴】生体情報の個人内変動の統計的な性質に基づき算出された量子化レベルを使用する方式．

【利点】生体情報の個人内変動に対する耐性あり．暗号技術への適合性あり．

【課題】テンプレートの無効化に関する問題．Pre-alignmentの必要性に関する問題．

【事例】柴田他，“メカニズムベースPKI－指紋からの秘密鍵動的生成”，2004．

（**E**）Anonymous Biometrics

【特徴】生体情報の微小な変動に対してhelper dataと呼ばれる誤り訂正機能を有するデータを使用し，さらに一方向性関数を適用する方式．

【利点】誤り訂正可能な範囲と識別可能な距離に関するパラメータを指定して識別性能を制御することが可能.
【課題】雑音モデルの推定に関する問題.
【事例】Linnartz, “Anonymous Biometrics”, 2003.

（**F**）Fuzzy vault scheme
【特徴】生体情報の組とダミーデータの併用による方式.
【利点】テンプレートの無効化が可能．秘密鍵はテンプレート中に存在しない.
【課題】ノイズの含まれる生体情報に対する耐性の問題．Pre-alignmentの必要性に関する問題.
【事例】Clancy, “Fingerprint Vault”, 2003.

（**G**）Secret key maintenance
【特徴】Secret key maintenance は，”key hiding and retrieval”と”key generation” の二つの方式に分類可能.
○key hiding and retrieval：ハッシュ化された秘密鍵をテンプレートに格納する方式．認証が成功したときのみ秘密鍵が復元．ハッシュ化された秘密鍵による攻撃の可能性あり.
○key generation：認証が成功したときのみ秘密鍵を生成する方式．Key hiding and retrievalより安全性は高いが，クライアント側での秘密鍵の管理の問題あり.

上述のように，テンプレート保護技術にはまだ多くの課題が残されており，より実用性の高いテンプレート保護技術の開発，ならびに安全性に関するより厳密な評価が必要と考えられる.

（参考文献）
[1] 三村昌弘,「バイオメトリクスセキュリティ評価基準の開発」，BSC バイオメトリクスの安全性検討 WG　第 3 回研究会講演資料，2005.10.25.
[2] 宇根正志，田村裕子,「生体認証における生体検知機能について」，BSC バイオメトリクスの安全性検討 WG　第 2 回研究会講演資料，2005.9.28.
[3] 鷲見和彦,「バイオメトリクス個人認証の脆弱性保護技術」，BSC バイオメトリクスの安全性検討 WG　第 2 回研究会講演資料，2005.9.28.