1 安全性対策技術の動向

山崎　恭
北九州市立大学
国際環境工学部 情報メディア工学科
yamazaki@env.kitakyu-u.ac.jp

バイオメトリック認証システムの安全性対策が必要とされる背景について述べ，バイオメトリック認証システムにおける脆弱性と脅威に関するこれまでの分析結果を踏まえながら，脅威の発生個所ごとに必要となる対策技術の概要について説明する．また，安全性対策技術のうち，バイオメトリック認証特有の技術である生体検知技術やテンプレート保護技術の重要性について述べるとともに，特に，テンプレート保護技術に焦点を当て，技術の現状を紹介するとともに，今後解決すべき課題を明らかにする．

安全性対策の必要性

近年，情報システムの安全性に対する要求の高まりから，バイオメトリック認証技術の利用が急速に進みつつある．従来，バイオメトリック認証技術は，機密性の要求される施設への入退室管理など，限定的な場面での利用が多数を占めていたが，今日では，電子パスポートへの適用や金融機関での利用など安全性や公共性を重視した大規模なアプリケーションから，モバイル機器やアミューズメントへの適用といった利便性や個人性を重視したアプリケーションに至るまで，その適用分野は大きな広がりを見せている．

これまで，生体特徴を使用したバイオメトリック認証は，パスワードやカード等の本人の知識や所有に基づく認証と比較して，盗難，紛失，忘失の危険性がないことから安全性が高いとされてきた．しかしながら，近年の研究により，利用者の協力や不注意により提供された生体情報を利用してバイオメトリック認証装置を詐称する人工サンプルを製作できる可能性や，認証時に提示される生体情報と比較するためのデータとしてあらかじめシステムに登録される利用者の生体特徴を記録したテンプレート（template）から詐称可能な生体情報を復元できる可能性などが指摘されている．また，バイオメトリック認証の普及により，ネットワーク環境での利用が進展すると，生体情報や個人情報を取り扱う認証機関自身が不正を働き，テンプレートや個人情報を悪用する可能性も考慮する必要がある．このように，バイオメトリック認証に対する多くの潜在的危険性が指摘されるようになった現在，バイオメトリック認証の安全性対策の必要性が急速に高まっている．

バイオメトリック認証の安全性を確立するためには，バイオメトリック認証システムをセキュリティシステムとして捉え，リスク対策を講じる必要がある．すなわち，バイオメトリック認証システムに存在する脆弱性（弱点）を明確化し，それらの脆弱性を利用した脅威を分析し，脅威により引き起こされるリスクを評価することにより有効な対策を講じることが不可欠となる．そこで，本稿ではバイオメトリック認証システムの脆弱性，脅威，対策の関連性を踏まえながら，安全性対策技術の動向と今後の課題について述べる．

脆弱性・脅威の分析と対策

図-1は，一般的なバイオメトリック認証システムにおける脅威の発生個所（A ～ H）を示したものである．

また，**表-1**は認証時において，各脅威の発生個所における脅威の内容，脅威の分類，関連する脆弱性および対策手段の一例を示したものである．表-1の脆弱性の名称については，バイオメトリクスの脆弱性と脅威を分析した報告書[1)]を参照した．また，利用者を認証する際の

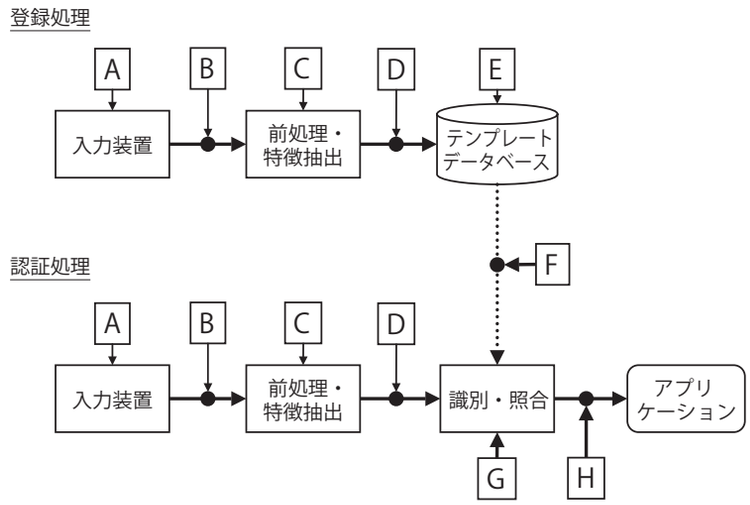

図-1　バイオメトリック認証システムにおける脅威

発生個所	内容	分類	関連する脆弱性	対策
A	・偽生体情報の提示 ・入力環境の変化	なりすまし， 可用性阻害	入力環境，認証パラメータ，習熟，抵抗感，複製，秘匿困難，遺留，類似性，変化，特異性，他人受入，本人拒否，推定，不定データなど	生体検知，マルチモーダル，監視，耐環境性対策
B	・不正に取得した生体情報の再入力 ・生体情報の漏洩	なりすまし， プライバシ漏洩	複製，類似性，特異性，プライバシ情報，他人受入，推定，不定データ，データ改竄，データ漏洩など	暗号化，チャレンジ・レスポンス認証，リトライ制限
C	・前処理・特徴抽出処理の置き換え	なりすまし	認証パラメータなど	耐タンパ対策
D	・生体特徴情報の不正変換 ・生体特徴情報の漏洩	なりすまし， プライバシ漏洩	複製，類似性，特異性，プライバシ情報，他人受入，推定，不定データ，データ改竄，データ漏洩など	暗号化，電子透かし，リトライ制限
E	・テンプレートの改竄	なりすまし	データ改竄など	テンプレート保護
F	・テンプレート情報の不正変換 ・テンプレート情報の漏洩	なりすまし， プライバシ漏洩	プライバシ情報，データ改竄，データ漏洩など	暗号化
G	・識別・照合処理の置き換え	なりすまし， 可用性阻害	認証パラメータ，データ改竄など	耐タンパ対策
H	・識別・照合結果の改竄	なりすまし	データ改竄など	暗号化

表-1　認証時の脅威

脅威については，第三者が正当な利用者になりすます「なりすまし」，認証時の可用性を阻害する「可用性阻害」，利用者のプライバシの漏洩につながる「プライバシ漏洩」に分類した．なお，利用者を登録する際の脅威についても，第三者が容易になりすましを行うことを可能とする「バックドア生成」，「可用性阻害」，「プライバシ漏洩」に分類できるが[1)]，本稿では紙面の都合上割愛した．

図-1の各点（A ～ H）における脅威と対策の概要は以下のとおりである．

点A：入力装置（センサ）に対する脅威であり，複製の脆弱性等を利用して作成した人工指を提示するなど，偽の生体情報の入力によるなりすましが代表的な脅威となる．また，入力環境の変化による本人拒否の発生など，バイオメトリクス特有の脆弱性による可用性阻害の脅威が存在する．なりすましに対する対策としては，提示された情報が生きている人間から提示された

ものか否かを確認する生体検知技術が最も重要である．また，複数の異なる生体情報を組み合わせるマルチモーダル認証や人間による認証プロセスの監視も有効な対策手段である．一方，可用性阻害に対する対策としては，たとえば音声認証や顔認証ではそれぞれ雑音や照明変動による影響を軽減する登録・認証アルゴリズムを採用するなど，入力環境の変化に頑健な耐環境性の高い前処理や特徴抽出処理の適用が挙げられる．

点B：入力装置と前処理・特徴抽出装置を接続する通信路における脅威であり，不正に取得した生体情報の再入力（リプレイ・アタック：replay attack）によるなりすましが代表的な脅威となる．また，推定の脆弱性等を利用し，認証結果を参照して正当な利用者の生体情報に漸近するように入力情報を変化させながら繰り返し入力を試みることによりなりすましを図るヒルクライミング・アタック（hill-climbing attack）も本個所の脅威である．さらに，生体情報の漏洩によるプライバシ漏洩の脅威も挙げられる．対策としては，データの暗号化が一般的である．また，リプレイ・アタックに対しては，チャレンジ・レスポンス認証（challenge-response authentication）の適用が，ヒルクライミング・アタックに対しては，リトライ回数の制限が有効と考えられる．

点C：前処理・特徴抽出における脅威であり，ハードウェアやソフトウェアの不正な置き換えによるなりすましが主な脅威として挙げられる．対策としては，ハードウェアやソフトウェアの耐タンパ対策が有効である．

点D：前処理・特徴抽出処理後の生体特徴情報が伝送される通信路における脅威であり，生体特徴情報の不正な変換やヒルクライミング・アタックによるなりすましが代表的な脅威となる．また，生体特徴情報の漏洩によるプライバシ漏洩の脅威も存在する．対策としては，データの暗号化が一般的である．また，電子透かし技術を適用し，抽出された生体特徴情報に透かしを埋め込み，識別・照合時に透かしを検出することにより生体特徴情報の正当性を確認する手法も有効である．さらに，ヒルクライミング・アタックに対しては，リトライ回数の制限が有効である．

点E：テンプレートデータベースにおける脅威であり，利用者のテンプレートの改竄によるなりすましが代表的な脅威となる．対策としては，後述するようにテンプレートの保護が最も重要である．

点F：テンプレートデータベースと識別・照合装置を接続する通信路における脅威であり，テンプレート情報の不正変換によるなりすましが代表的な脅威となる．また，テンプレート情報の漏洩によるプライバシ漏洩の脅威も存在する．対策としては，データの暗号化が一般的である．

点G：識別・照合装置における脅威であり，ソフトウェアの不正な置き換えによるなりすましが主な脅威として挙げられる．また，可用性阻害の脅威も存在する．対策としては，ハードウェアやソフトウェアの耐タンパ対策が有効である．

点H：識別・照合結果を外部のアプリケーションに伝送する通信路における脅威であり，識別・照合結果の改竄によるなりすましが主な脅威となる．対策としては，データの暗号化が一般的である．

上述のように，バイオメトリック認証の脅威に対抗し，バイオメトリック認証の安全性を確立するためには，生体検知やテンプレートの保護といったバイオメトリック認証特有の対策技術と，従来の暗号に基づく対策技術とを効果的に組み合わせる必要がある．特に，前者のバイオメトリック認証特有の対策技術についてはまだ十分に確立されておらず，今後，バイオメトリック認証の安全性を確立する上で最も重要な検討課題の1つとして位置付けられる．そこで，以下ではバイオメトリック認証の安全性に関する技術のうち，バイオメトリック認証特有の対策技術の1つであるテンプレート保護技術に焦点を絞り，現状と問題点について整理する．

テンプレート保護技術

テンプレート保護技術の確立が重要とされる背景には，生体情報は一度漏洩すると取り替えることができないというバイオメトリクス特有の性質がある点に注意する必要がある．テンプレートの保護を実現するためには，生体情報を管理する管理者であってもテンプレートの取り出しや改竄を困難にする技術や漏洩したテンプレートを無効化する技術，テンプレートから元の生体情報を復元できなくする技術などが必要となる．そこで，本稿ではこのような条件を考慮して提案された代表的なテンプレート保護技術[2), 3)]について紹介し，その特徴と課題について述べる．

(a) Cancelable Biometrics方式[4)]

図-2(a)に示すように，入力データに対して一方向性ハッシュ関数を適用し，アプリケーションごとに異なるテンプレートを生成する方式である．多対一の対応を持つ一方向性ハッシュ関数を使用するため，元のデータを一意に復元することができないという特徴を持つ．また，使用中のテンプレートが漏洩した場合には，異なるハッシュ関数を適用することにより，使用中のテンプレートを無効化し，新しいテンプレートを生成することが可能

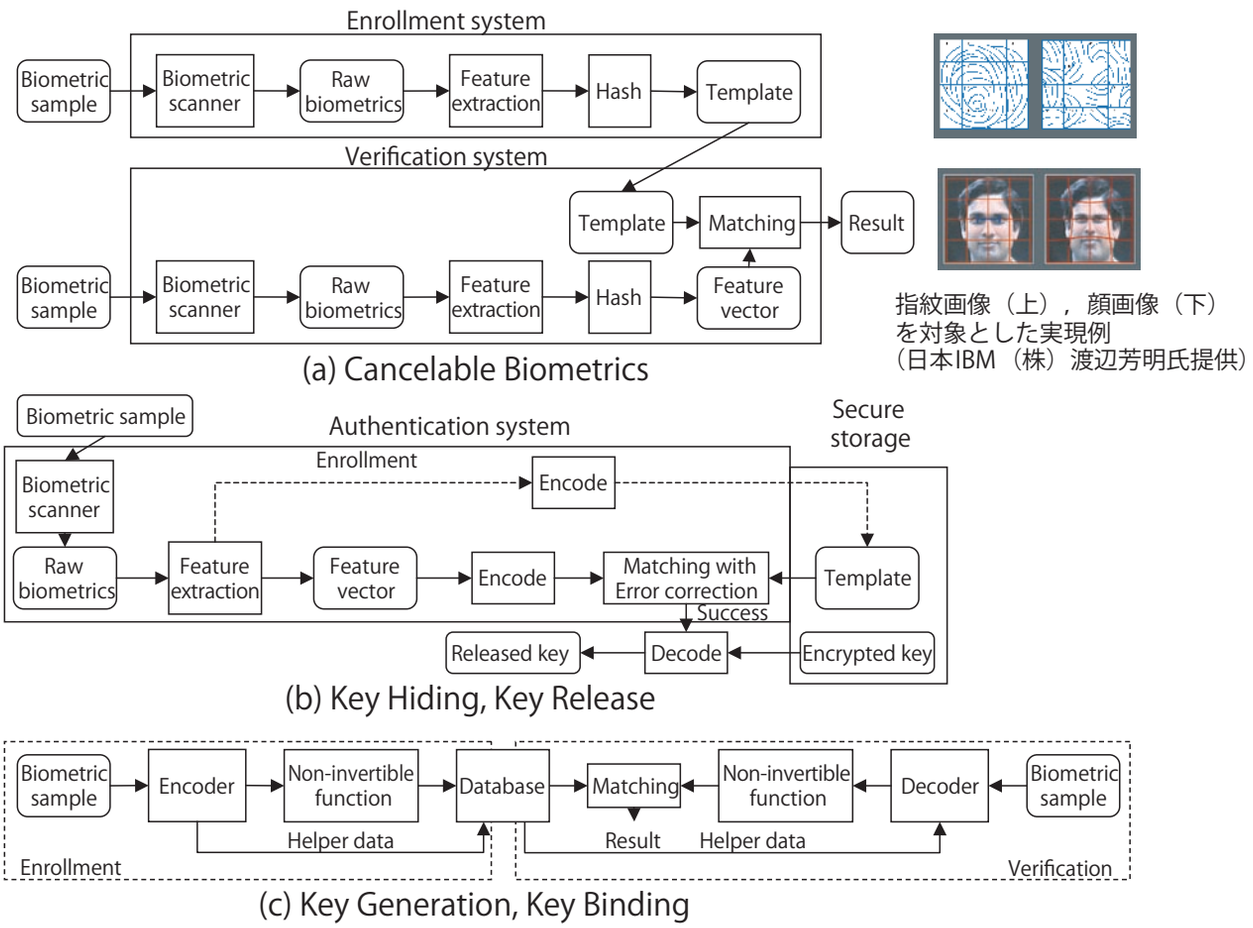

図-2　テンプレート保護方式の例

である．ただし，照合のたびに変化する入力データに対し，同じハッシュ値が得られるような実装上の工夫が必要となる．本方式の具体的な実現方法として，ブロックに分割した指紋画像や顔画像に対してブロック単位の位置の入れ替えやブロックの形状の幾何学的な歪みにより，元のテンプレートの予測を困難にする方法が提案されている．本方式の利点は，従来のテンプレートと互換性が高く，特徴抽出や照合のアルゴリズムをそのまま利用することができる点にある．一方，照合時において，入力データとテンプレートの類似度を表す照合スコアが連続値で与えられるシステムでは，直接元のテンプレートが復元できずとも，適切に設定した初期値からヒルクライミング・アタックを行うことにより，詐称可能なテンプレートを推定できるという問題点が残されている．

（b）Key Hiding, Key Release方式

図-2(b)に示すように，テンプレートを暗号化して保存し，照合時に復号して使用する方式である．暗号化されたテンプレートと入力データから生成されたテンプレートが一致したときにのみ，保存された秘密鍵を取り出すことができる．本方式は，入力データの揺らぎを補正する機能を持つ点に特徴がある．また，照合スコアが表出しないため，ヒルクライミング・アタックによる攻撃を防止することが可能である．本方式に基づく具体的な実装方法[5]が提案されており，提案手法では，フーリエ変換した入力データの位相項と乱数を畳み込んで生成されるフィルタ，フィルタと秘密鍵から生成される参照テーブル，一方向性ハッシュ関数により暗号化された秘密鍵をそれぞれテンプレートに保存する．テンプレートに登録された情報から元の生体情報を復元することは困難であり，使用中のテンプレートが漏洩した場合にはテンプレートを無効化し，パラメータを変更することで新しいテンプレートを生成することが可能である．提案手法の利点としては，フーリエ変換の使用により入力データの位置ずれの許容度が大きい点が，欠点としては，多くの入力データを使用することにより，秘密鍵が推定され

る可能性のある点がそれぞれ挙げられる．

(c) Key Generation, Key Binding方式

図-2(c)に示すように，符号化された入力データに対して一方向性ハッシュ関数を適用して生成したテンプレートと入力データの揺らぎを補正するhelper dataと呼ばれるデータをデータベースに保存し，認証が成功した場合に毎回同一の鍵を生成する方式である．本方式に基づく具体的な実装方法[6]が提案されており，指紋照合を対象としたFingerprint Vaultと呼ばれる手法では，真の特徴点と偽の特徴点，および秘密情報に基づき生成した多項式の値をテンプレートに登録し，認証時に得られた入力データの特徴点と真の特徴点の多くが一致した場合に元の多項式が得られる．あらかじめ定められた近傍内に特徴点が発生した場合には特徴点が一致したと判定することにより，微小な位置変動を吸収することが可能である．提案手法の利点としては，他の方式と比較してテンプレートの安全性が高い点が挙げられる．一方，欠点としては，認証時に入力データとテンプレートの位置合わせが必要であり，その際，暗号化されていないテンプレートの使用により，テンプレートから生体情報の一部を推定できる可能性のある点が挙げられる．

主なテンプレート保護技術には，(a)のように特徴空間において近傍での距離を保存し遠方での距離を大きく変化させる幾何的な変形を与える方式と，(b)，(c)のように，生体情報の微小な変動を吸収する機能を導入した上で一方向性ハッシュ関数を適用する方式がある．いずれの方式にも一長一短があり，前者は従来の特徴抽出や照合処理との互換性が高いため，比較的規模の小さいバイオメトリック認証システムにおける安全性向上の用途には適しているが，テンプレートの秘匿性能の点では必ずしも十分とは言えず，不特定多数の認証機関を対象とするような用途には適さない．一方，後者は入力データの揺らぎを補正する範囲と識別可能距離に関するパラメータを調整して識別性能を作り込むことが可能であり，広範囲の用途に適用できると考えられるが，現実の運用に当たっては，入力雑音モデルの推定，雑音モデルと識別性能，マルチモーダル認証への拡張などの課題を解決する必要がある[3]．テンプレート保護技術は，現在，最も研究開発の盛んな分野の1つであり，今後，上記の問題点を解決する多くの提案が行われるものと期待される．テンプレート保護技術の詳細に関心のある読者は文献3)を参照されたい．

安全性の確立に向けて

バイオメトリック認証システムの安全性を確立するためには，本稿で述べたテンプレート保護技術をはじめとするバイオメトリック認証特有の対策技術の確立を急ぐとともに，既存の情報セキュリティ技術との整合性をどのように図るかという問題にも取り組む必要がある．また，技術的な側面のみならず，人的要因や制度の整備まで視野に入れた総合的な視点から，バイオメトリック認証システムの安全性を議論することが重要である．

謝辞　本稿の一部は，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」の成果によるものである．

参考文献

1)（社）日本自動認識システム協会：平成15年度基準認証研究開発事業 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(2004)．
2)（社）日本自動認識システム協会：平成16年度基準認証研究開発委託事業-2 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(2005)．
3) 鷲見和彦，松山隆司，中嶋晴久：バイオメトリクス認証テンプレート保護に関する検討，2005年暗号と情報セキュリティシンポジウム(SCIS2005), pp.535-540 (2005).
4) Ratha, N. K., Connell, J. H., and Bolle, R. M.：Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, 40, 3, pp.614-634 (2001).
5) Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, V.：Biometric Encryption, http://www.bioscrypt.com/assets/Biometric_Encryption.pdf
6) Clancy, T. C., Kiyavash, N. and Lin, D. J.：Secure Smartcard-Based Fingerprint Authentication, Proc. of 2003 ACM SIGMM Workshop on Biometrics Methods and Applications, pp.45-52 (2003).

（平成18年4月28日受付）