■11 群（社会情報システム）－ 7 編（金融情報システム）

6 章 バイオメトリクス認証の実用における脆弱性と対策

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

■概要■

身体的・行動的特徴を利用して個人の認証を行う生体認証システムは，近年，指や掌の静脈パターンを用いた生体認証を ATM における顧客の本人確認に利用する動きがみられるなど，金融分野をはじめとする幅広い分野において利用されつつある．生体認証システムを活用していく際には，生体認証システム特有の脆弱性を把握し，適切な対策を講じていくことが重要である．特に，生きている人間の身体部分でない物体を誤って一致と判定してしまうという脆弱性（人工物などの受理）が一部の市販のシステムにおいて存在する可能性が学会などにおいて指摘されており，こうしたなりすましを目的とした攻撃法への対応が必要といわれている．

これまで，生体認証システム特有の脆弱性については，多くの検討が行われており，例えば，国際標準案 ISO/IEC FDIS 19792（生体認証のセキュリティ評価）では，ほかの検討と比べて相対的に多くの脆弱性について抽象的な記述レベルでまとめられている．これらの脆弱性のうち，人工物などの受理については，評価用の人工物（テスト物体）や被験者を用いて評価対象の生体認証システムを評価する手法である「テスト物体アプローチ」が提案されている．また，複数のデータと高い確率で誤一致するようなデータの存在が指摘されたことを受け，こうした脆弱性を評価するための新たな評価尺度「ウルフ攻撃確率」が提案され，評価手法の検討が進められている．

脆弱性の評価だけでなく，生体認証システムにおけるなりすましへの対策の評価も行われている．例えば，システムに提示されたものが生体部位か否かを識別する「生体検知技術」や，システムに登録されているデータを盗取したとしても，なりすましに利用可能な情報を入手できないようにする「テンプレート保護技術」について，実験などによる評価が行われるようになってきている．このほか，脆弱性や対策の評価だけでなく，運用されている生体認証システムに脆弱性が発見された場合の対応についても，近年検討が始まっている．

本章では，これらの概要や研究動向などについて説明する．

【本章の構成】

本章では，6-1 節で，生体認証システムにおけるセキュリティ評価の必要性について述べ，6-2 節では，生体認証システムに特有の脆弱性を紹介する．6-3 節では，こうした特有の脆弱性の評価手法であるテスト物体アプローチとウルフ攻撃アプローチについて説明する．更に，6-4 節では，なりすましへの対策として生体検知技術とテンプレート保護技術に焦点を当てて，評価の考え方などを説明し，6-5 節において，生体認証システムを適切に利用していくうえでの課題と，脆弱性情報の取扱いに関する検討状況について説明する．

■11 群 － 7 編 － 6 章

6-1 セキュリティ評価の必要性

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

生体認証システムは，PC へのログインや建物への入館の際の本人確認手段として広く利用されているほか，最近では，空港での入国審査における本人確認などに利用されるようになってきている．金融分野においても，従業員の本人確認のほか，指や掌の静脈パターンを用いた生体認証を ATM における顧客の本人確認に利用する動きがみられる．生体認証システムを適切に選択し利用するためには，セキュリティ評価の実施が求められるほか，生体認証システムの脆弱性や攻撃の洗い出し，攻撃への対策の整理などが必要である．国際標準策定の場においても，生体認証システムのセキュリティ評価・認証に関する標準（ISO/IEC 19792）の審議が進められている．こうしたなか，実際に運用されている一部の生体認証システムに対して分離された生体部位や人工物を提示するといった事例[1]が近年発生しており，従来理論上のものとみられてきた生体認証システム特有の脆弱性を現実のものとして認識することの重要性が改めて示されている．また，ウルフ攻撃 [2] などの新たな攻撃法も提案されてきている．生体認証システムは，ほかのセキュリティ・システムと同様に，時間の経過とともに新しい脆弱性や攻撃法が提案され，そのセキュリティは徐々に低下していくという性格をもつ．上記の事例やウルフ攻撃の提案からも読み取れるように，今後生体認証システムを利用していくうえで，新たな脆弱性を考慮しつつ，漏れのない対策を講じていくことが求められる．

次節以降で生体認証システムへの攻撃や対策を紹介するに当たり，まず，一般的な生体認証システムの構成を説明する（**図 6･1**）．登録時には，利用者が自身の身体的・行動的特徴（生体特徴）をセンサーに提示する．参照データ生成部は，センサーが読み取ったデータ（生体サンプル）から，認証時に利用者本人か否かを判定するために参照するデータ（参照データ）を生成し，ストレージに利用者の ID と紐付けして記録する．認証時には，ID と生体特徴を提示した利用者が ID の利用者本人か否かを確認する 1 対 1 認証と，生体特徴のみを提示した利用者が登録されている利用者のうち誰かを識別する 1 対 *n* 認証がある．1 対 1 認証を行う場合，利用者は ID をシステムに入力し，生体特徴をセンサーに提示する．判定部は，ID に対応する参照データをストレージから呼び出し，生体サンプルと照合したうえで，本人か否かを出力する．また，1 対 *n* 認証を行う場合，判定部は，ストレージから順次参照データを呼び出し，各参照データと生体サンプルの照合を行い，該当する利用者の ID を出力する．

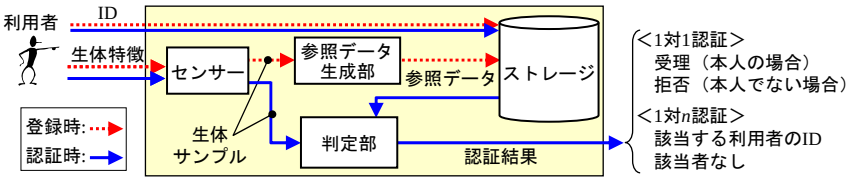


図 6・1　一般的な生体認証システムの構成（概念図）

[1] イモビライザーにおける本人確認に指紋を利用している自動車の運転手が，窃盗団に襲われ指を分離されたという事件が発生しているほか [1]，指紋のような模様が付いたテープを貼り付けた指を提示することで，国内地方空港の入国審査を通過したという事件が発生している（読売新聞 2009 年 1 月 1 日朝刊）．

■11 群 － 7 編 － 6 章

6-2 バイオメトリクス認証システム特有の攻撃と脆弱性

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

生体認証システムには，データの盗聴，改ざん，消去などの情報システムに一般的な脆弱性が存在しうるほか，生体特徴を模した人工物の提示などの生体認証システムに特有の脆弱性が存在しうる[3),4),5)]．ここでは，カバーしている生体認証システムに特有の脆弱性が相対的に多く，記述の抽象度が高い ISO/IEC FDIS 19792 に注目し，各脆弱性を紹介すると以下のとおりである．

- 「認証精度の限界（performance limitation）」は，他人の生体特徴がセンサーに提示された場合であっても誤って受理される可能性があるという脆弱性である．
- 「人工物などの受理（artefact of biometric characteristics）」は，ゼラチンで生成した指や顔の写真などの人工物によって生体特徴を偽造したものや，分離された生体部位の生体特徴をセンサーに提示した場合でも，誤って受理される可能性があるという脆弱性である．
- 「生体特徴の意図的な変更（modification of biometric characteristics）」は，整形手術，化粧，声色や筆跡の変更など，自分の身体的・行動的特徴を意図的に変更可能であり，それらがなりすましにつながる可能性があるという脆弱性である．
- 「生体特徴の秘匿困難性（difficulty of concealing biometric characteristics）」は，グラスやセンサー上の指紋の痕跡の記録，顔の撮影，音声の録音などのように，日常生活の中で秘匿が困難な生体特徴が存在するという脆弱性である．
- 「血縁関係による類似（similarity due to blood relationship）」は，双子の顔や声のように，血縁者の生体特徴が類似している可能性があるという脆弱性である．
- 「特殊な生体特徴の存在（special biometric characteristic）」は，多くの参照データと誤って「一致」と判定されるような生体特徴（ウルフと呼ばれる）が存在する可能性があるという脆弱性である．この脆弱性には，血縁関係により生体特徴が類似するケースは含まれない．
- 「合成された擬似生体サンプルの受理（synthesised wolf biometric samples）」は，多くの参照データと誤って「一致」と判定される（生体サンプルでない）データ（これらもウルフと呼ばれる）が存在する可能性があるという脆弱性である．
- 「環境変化による認証精度への影響（hostile environment）」は，センサー周辺の環境（気温，湿度，光量など）の変化が認証精度を低下させる可能性があるという脆弱性である．
- 「不適切な情報の登録（procedural vulnerabilities around the enrolment process）」は，不適切な情報（不鮮明な生体サンプル，合成された擬似生体サンプルなど）の登録により，なりすましが発生する可能性があるという脆弱性である．
- 「データの漏えい・改ざん（leakage and alteration of biometric data）」は，生体認証システム内のデータが漏えいする，または改ざんされる可能性があるという脆弱性である[2]．

[2] 本脆弱性は情報システムに共通であるものの，対象となるデータは生体認証システムに特有であることから，本国際標準案で取り上げられている．

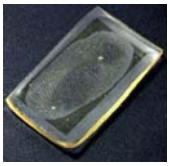
■11 群 － 7 編 － 6 章

6-3 なりすましにつながる脆弱性の評価手法

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

6-3-1 テスト物体アプローチ

一部の市販の生体認証システムを対象に,「人工物などの受理」の脆弱性が存在することが 2000 年頃から学会などで報告され，本脆弱性が広く認識されるようになっている [6), 7), 8)]．例えば，指紋認証システムについては，本人の指から形成した型を用いて媒体（ゼラチン，シリコーン・ゴムなど）上に指紋パターンを形成する方法や，本人の残留指紋から形成した型を用いて媒体上に指紋パターンを形成する方法によって作製された人工物（人工指）が，一部の市販のシステムにおいて誤って「一致」と判定されてしまうことが報告されている（**図 6･2**-(1)）[8)]．虹彩認証システムや指静脈パターン認証システムについては，赤外線カメラで撮影した虹彩画像や指静脈パターン画像を印刷した紙が，一部の市販のシステムにおいて誤って「一致」と判定されてしまうことが報告されている（**図 6･2**-(2)）[9), 10)]．



(1) 残留指紋からグミを用いて作製した人工指 [7)]

(2) 虹彩画像を印刷した紙 [9)]

図 6・2　人工物の例

人工物などの受理に対する安全性を評価するために,「テスト物体アプローチ」と呼ばれる評価手法が提案されている [11)]．テスト物体アプローチでは，まず，被験者の生体特徴を利用して様々なバリエーションの人工物（テスト物体）を作製する．これらのテスト物体や被験者の協力のもと，①テスト物体をシステムに登録できるか否か，②登録できた場合，同一のテスト物体を再度提示することで照合できるか否か，③テスト物体を登録し，被験者が生体情報を提示することで照合できるか否か，④被験者の生体情報を登録し，テスト物体を提示することで照合できるか否かという 4 種類の実験を行う．実験結果から，評価対象システムが受け入れやすいタイプのテスト物体を把握できるほか，同一のテスト物体と被験者を用いて別の生体認証システムを評価することで，評価結果の比較が可能となる．こうした評価を客観的に実施可能とするために，テスト物体の作製方法が公表されており，例えば，人工指については TS X0101（指紋読取装置の品質評価方法）に，静脈パターンに関する人工物については松本ら [12)] に示されている．ただし，評価に用いるテスト物体の妥当性を示すという課題が残されており，テスト物体の作製方法を検討するとともに，より多くの生体認証システムを用いた実験を行っていく必要がある．

なお，米国では，複数の金融機関によって，指紋認証システムと音声認証システムを対象とした評価プロジェクトが 2006 年に開始されており（実施主体は米国民間コンサルティング会社の IBG），本プロジェクトにおいてもテスト物体アプローチが採用されている [13)]．

6-3-2 ウルフ攻撃アプローチ

ウルフ攻撃とは，生体認証システムに登録されている多くの参照データと一致すると誤判定されるような特殊な入力情報（ウルフ）を探索し，それを生体認証システムに提示することでなりすましを行うという攻撃である．この攻撃は 6-2 節に示した脆弱性のうち，「特殊な生体特徴の存在」と「合成された擬似生体サンプルの受理」を利用している[3]．ウルフ攻撃の研究は，2006 年に一部の指静脈パターン照合アルゴリズムにおいて任意の参照データと誤一致するウルフ（ユニバーサル・ウルフ）が存在することが指摘されたことが契機となっており [14]，その後，一部の指紋照合アルゴリズムや虹彩照合アルゴリズムに関しても研究成果が報告されている [15), 16)]．虹彩は目の瞳孔（黒目の部分）の周辺の筋繊維のパターンであり，特定の虹彩照合アルゴリズムにおいては，照合に利用される筋繊維の数が減るように加工した入力情報を与えると，誤って一致と判定される確率が高まることが指摘されている．

ウルフ攻撃に対する安全性を評価する手法はこれまで確立されていなかった．例えば，従来，生体認証システムの性能評価に用いられてきた他人受入率 FAR（False Acceptance Rate）が，ウルフ攻撃への評価尺度になりうるかについて考えてみる．一般に，FAR の測定に用いる被験者や生体サンプルの集合（データセット）は，対象システムが取り得るすべての入力の集合に対する部分集合に過ぎない．このため，このデータセット以外のデータがウルフである場合には，ウルフ攻撃に対する安全性を適切に評価することができない．また，仮に，データセットにウルフが含まれていたとしても，各入力情報の FAR を測定し，それらの平均値を対象システムの FAR とするため，ウルフの存在を検知することが難しくなってしまう．こうしたなか，宇根ら [2)] は，評価対象の生体認証システムが取り得るあらゆる入力情報のなかからウルフを探索し，ウルフを用いたなりすましの成功確率の上限値（ウルフ攻撃確率）によりウルフ攻撃に対する安全性を評価するという手法を提案している．ウルフ攻撃確率が低いほどウルフ攻撃に対する安全性が高いといえる．

こうしたウルフ攻撃確率を自動的に見積る方法についての研究も進められている [17)]．初期画像を生成し，その一部をランダムに変更することで複数のバリエーションの画像を生成したうえで，これらの画像を照合アルゴリズムに入力し，なりすましの成功確率が最大となった画像を選択する．この画像の一部をランダムに変更して複数の画像を生成し，各画像についてなりすましの成功確率を求め最も確率が高くなる画像を探索するという処理を繰り返すことで，この照合アルゴリズムにおけるウルフ攻撃確率を見積ることができる．すべての入力画像について探索することは現実には困難であるため，評価対象の照合アルゴリズムに関する知識を踏まえ，探索範囲を限定したシミュレーション実験が行われている．

また，ウルフ攻撃確率が一定の確率以下となる照合アルゴリズムの構成方法が理論的に示されているほか [18)]，ある参照データと一致すると判断された入力について残りの参照データとも照合し，一定数以上の参照データと一致と判断された場合には，ウルフとみなして拒否するという認証方法も検討されている [19)]．

[3] ウルフから作製した人工物を用いる場合は「人工物などの受理」を，ウルフを生体認証システムに電気的に挿入する場合は「データの漏えい・改ざん」をそれぞれ利用することになる．

■11 群 － 7 編 － 6 章

6-4 対策技術とその効果に関する評価

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

6-4-1 生体検知技術

6-3-1 節で触れたように「人工物などの受理」の脆弱性が広く認識されるようになり，その対策として生体検知技術が 1990 年代から特許を中心に提案されはじめ [20]，2000 年以降は学会でも発表されるようになってきている [21]．例えば，指紋認証システムに提示された物体の脈拍の有無を調べるという方法が提案されているほか，虹彩，静脈パターン，顔などについても多数の方法が提案されており，人間に関する電気特性（電気抵抗，静電容量など），光学特性（光の反射・透過光など），生理的特性（脈拍，発汗など）などが利用されている [22]．

生体検知技術の導入・利用を検討するうえで，セキュリティ，利便性，コスト，社会的受容性について評価することが重要と考えられる．

- セキュリティ：生体であることの検知をどの程度正しく実行できるか（検知精度）を評価することが考えられる．様々な材料・製法による人工物や特定の生体検知の手法を破る人工物が検討されていることから，極力多くの人工物などを用いて検知精度を評価することが望ましい．また，検知精度は，生体認証システムに提示する際の環境（温度，湿度など）の影響を受けると考えられることから，こうした条件を明確にすることも重要である．
- 利便性：生体検知の導入によって利便性が低下する可能性がある．例えば，生体検知に用いる情報（生体検知用サンプル）の読取りや処理が発生するほか，生体検知のために利用者に一定の動作を要求する方法も提案されている．こうした生体検知にかかる時間，利用者に要求する動作などについて明確にしたうえで評価することが望ましい．
- コスト：既存の生体認証システムに生体検知の手法を導入する際，ソフトウェアの変更が必要になるほか，既存のシステムのセンサーで生体検知用サンプルを取得できない場合にはハードウェアの追加・変更も必要になる．そのため，生体検知を行うために要求されるハードウェアの性能を明確にしたうえで評価することが望ましい．
- 社会的受容性：生体検知に用いる特徴から副次的情報が漏れるケース（脈拍を調べることで不整脈の有無が分かるなど）が考えられることから，社会的受容性の観点からの検討が行われることが望ましい．

セキュリティについては，検知精度や実験に用いた人工物の情報を明記している研究事例が徐々に増加している一方で，実験時の環境が明記されている研究事例はまだ少ない．また，同一のデータセットを用いて異なる手法を評価する試みが行われており，データセットの影響を排除することを意識した検討も行われている．利便性については，生体検知用サンプルの取得時間や生体検知全体にかかる時間などを明記している研究がまだ多くない．研究事例のなかには，提示した指を反時計回りに 15 度回転させる動作やセンサーに乗せた指を前後左右にずらす動作などを利用者に要求する手法があるが，こうした動作が利用者に与える負荷や認証精度の低下への影響については，あまり議論されていない．コストについては，実験

に用いた装置の仕様を明記している研究事例が多いが，装置の性能ごとに検知精度がどのように変化するかといった観点から議論している事例はほとんどない．社会的受容性については，議論している文献がほとんどないのが実情である．

6-4-2 テンプレート保護技術

近年，漏えいした参照データ（テンプレートと呼ばれることもある）を用いてなりすましを行うという攻撃が注目を集めている．例えば，参照データとして指紋画像を登録している場合には，漏えいした指紋画像から人工指を作製する攻撃が想定されるほか，指紋の特徴点の情報（座標，隆線の傾きなど）のみを登録している場合であっても，なりすましに利用可能な情報を復元できるケースがあることが報告されている [23]．対策としては，そもそも参照データが漏えいしないように厳格に管理することが重要であるが，参照データが漏えいした場合も想定し，なりすましを困難にするための対応を検討することも重要になってきている．そうした対策の一つとして「テンプレート保護技術」が検討されている [24]．

本技術のアイデアは，漏えいした参照データからなりすましに必要な情報を入手困難にすることに加えて，漏えいした参照データを無効化し，新たに参照データを登録することである．例えば，指紋認証システムにおいて，センサーで読み取った指紋画像を細かいブロックに分割し，各ブロックを入れ換えたものを参照データとして登録し，認証時に同様の処理を行ったデータを用いるという手法が提案されている．本手法では，別の入換方法で変換したデータの登録により参照データを更新できる．こうした画像処理を利用した手法のほかに，暗号や誤り訂正符号を利用した手法が提案されている．典型的なテンプレート保護技術では，サーバ・クライアントのモデルを想定しており，登録時においては，クライアントにおいて生体特徴を読み取ったうえで加工・変換を施し，サーバにおいてこのデータを参照データとして登録する．認証時においては，クライアントにおいて生体特徴の読取りと加工・変換を行い，サーバにおいてこのデータと参照データを用いて照合処理を行う[4]．

テンプレート保護技術においては，従来の生体認証システムに加工・変換の処理を追加することによる処理時間の増加や認証精度の低下などが想定されることから，こうした性能に関する評価項目があるほか，漏えいした情報からなりすましに利用可能な情報を入手可能か否かなどのセキュリティに関する評価項目が考えられる．セキュリティ評価については，最近，満たすべきセキュリティ要件や攻撃のモデル化について本格的に検討が始まっており [25), 26)]，暗号や誤り訂正符号を利用した手法については評価が試みられている．一方，画像処理を利用した方式については，加工・変換の処理が複雑なため評価が進んでいないのが実情である．

暗号や誤り訂正符号を利用した手法については，理論的な検討が先行しており，性能や実現可能性の評価が今後の課題である．また，画像処理を利用した方式については，どのようにセキュリティ評価を行うかを検討することが課題となっている．

[4] 手法によっては，登録時と認証時の加工・変換処理が異なるケースや，認証時にサーバが乱数をクライアントに送るケースなどがある．

■11 群 － 7 編 － 6 章

6-5 今後の課題と脆弱性情報の取扱いについて

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

生体認証システムを安全に利用するうえで，事前に生体認証システムの脆弱性評価を行い，問題がないか否かを確認しておくとともに，後になって新たな脆弱性が発見された場合においても適切に対処するための仕組みを準備しておくことが望ましい．脆弱性の評価については，ISO/IEC FDIS 19792 において，生体認証システム特有の脆弱性（6-2 節参照），候補となる対策，評価手続のあり方などが規定されており，評価実施のための枠組み整備に向けた検討が進展している．実際に運用されている生体認証システムにおける脆弱性情報の取扱いについても，近年検討が始まっている．情報処理推進機構のバイオメトリクス・セキュリティ評価に関する研究会においては，生体認証システムの脆弱性情報を取り扱う枠組みとして，「ソフトウェア製品やウェブアプリケーションに関する脆弱性情報の届出制度（情報セキュリティ早期警戒パートナーシップ）」を活用する方向で検討されている [27]．その中間報告書には，①届けられた情報が脆弱性であるとみなす際の基準を定めること，②脆弱性情報に関する事例の蓄積を行い，脆弱性とみなす際の判断基準や脆弱性の情報の取扱方法の検討に反映させること，③ソフトウェア製品などの場合と異なり，生体認証システムの場合はハードウェアに関する脆弱性が届出される可能性があり，こうした差異を整理すること，④システムの設置環境などによって脆弱性が顕現化する条件が異なることが想定され，こうした条件の捉え方を検討することなどの課題が示されている．

このほか，6-4-1 節において説明したように，生体検知技術などの技術的な対策についても評価の検討が学会において一部始まっているものの，評価手法が確立しているとはいえないのが実情である．そのため，生体認証システムへの攻撃に関する情報をフォローし，実行可能性が高い攻撃については，認証時にスタッフが立ち会う，あるいは，サービスを一部制限するなどの運用面からの対応も検討していくことが有用である．

■参考文献■

1) J. Kent, “Malaysia car thieves steal finger,” BBC News, 31 March, 2005. http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm
2) M. Une, A. Otsuka and H. Imai, “Wolf Attack Probability: A Theoretical Security Measure in Biometric Authentication Systems,” IEICE Trans. Inf. & Syst., vol.E91-D, no.5, pp.1380-1389, IEICE, 2008.
3) 日本バイオメトリクス認証協議会（JBAA），“JBAA 技術部会 2002 年度成果報告会配付資料 バイオメトリクスシステムの脆弱性に関する報告書 Ver. 0.6,”日本バイオメトリクス認証協議会，2003.
4) 宇根正志・松本勉，“生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に,”金融研究，vol.24, no.2, pp.35-83，日本銀行金融研究所，2005.
5) 情報処理推進機構，“バイオメトリクス・セキュリティ評価に関する研究会 平成 18 年度 研究会中間報告書,”情報処理推進機構，2006.
6) D. Wills and M. Lee, “Six biometric devices point the finger at security,” Network Computing, vol.9, no.10, pp.84-96, 1998.
7) T. van der Putte and J. Keuning, “Biometrical fingerprint recognition: Don’t get your fingers burned,” IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pp.289-303, 2000.
8) T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, “Impact of artificial ‘Gummy’ fingers on fingerprint systems,” Optical Security and Counterfeit Deterrence Techniques IV, Proc. SPIE, vol.4677, pp.275-289, 2002.

9) 松本勉・平林昌志・佐藤健二，“虹彩照合技術の脆弱性評価（その 3)，”2004 年暗号と情報セキュリティシンポジウム，vol.II，no.2B5-5，pp.701-706，電子情報通信学会，2004.
10) 松本勉・田中瑛一，“指静脈認証システムのテスト物体によるセキュリティ測定法の研究，”2007 年暗号と情報セキュリティシンポジウム, vol.3F3-4，電子情報通信学会, 2007.
11) 松本勉，“生体認証システムのセキュリティ設計とセキュリティ測定，”ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会 第 7 回研究発表会予稿集，pp.57-64，電子情報通信学会，2006.
12) 松本勉・田中瑛一，“透過光利用バイオメトリック認証システムのためのテスト物体作製方法，”2008 年暗号と情報セキュリティシンポジウム，vol.3B4-1，電子情報通信学会，2008.
13) Financial Services Technology Consortium: “Spoof 2007”, http://www.fstc.org/projects/index.php?id=15”
14) 渡邉直彦・繁富利恵・宇根正志・大塚玲・今井秀樹，“指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ”，コンピュータセキュリティシンポジウム 2006，vol.9B-1，pp.621-626，情報処理学会，2006.
15) 河上梨恵・繁富利恵・美添一樹・宇根正志・大塚玲・今井秀樹：“マニューシャマッチングのウルフに関する理論的考察”，2007 年暗号と情報セキュリティシンポジウム，vol.3F3-2，電子情報通信学会，2007.
16) 小島由大・繁富利恵・美添一樹・井沼学・大塚玲・今井秀樹，“虹彩認証におけるウルフ攻撃確率の理論的考察”，2008 年暗号と情報セキュリティシンポジウム，vol.3B4-3，電子情報通信学会，2008.
17) 田辺康宏・美添一樹・今井秀樹，“指静脈認証システムにおけるセキュリティ評価手法の提案，”2008 年暗号と情報セキュリティシンポジウム，vol.3B4-2，電子情報通信学会，2008.
18) M. Inuma, A. Otsuka and H. Imai, “Theoretical framework for constructing matching algorithms in biometric authentication systems,” in submission to International Conference on Biometrics (ICB) 2009, 2009.
19) 小島由大・繁富利恵・井沼学・大塚玲・今井秀樹，“ウルフ攻撃確率を考慮したマッチングアルゴリズムのフレームワークにおける安全で可用性の高い認証プロトコル，”2009 年暗号と情報セキュリティシンポジウム，vol.4E1-4，電子情報通信学会，2009.
20) 加藤雅之・新崎卓・井垣誠吾・山岸文雄・池田弘之，“生体検知装置および該装置を用いた指紋照合システム，”特公平 8-23885 (公告日 1996 年 3 月 6 日)
21) R. Derakhshani, S. Schuckers, L. Hornak and L. O’Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” Pattern Recognition, vol.36, no.2, pp.383-396, 2003.
22) 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，”金融研究，vol.24，no.s2，pp.1-55，日本銀行金融研究所，2005.
23) C. J. Hill, “Risk of masquerade arising from the storage of biometrics”, Bachelor thesis, ANU, 2002.
24) N. K. Ratha, J. H. Connell and R. M. Rolle, “Enhancing security and privacy in biometric-based authentication systems,” IBM System Journal, vol.40, no.3, 2001.
25) 高橋健太・比良田真史，“セキュアなリモート生体認証プロトコルの提案，”2007 年暗号と情報セキュリティシンポジウム，vol.3F4-3，電子情報通信学会，2007.
26) 尾形わかは，“リモート生体認証の安全性，”ZeroBIO 研究プロジェクト主催第 1 回ワークショップ 生体情報のプライバシー，pp.77-80，2007.
27) 情報処理推進機構，“バイオメトリクス・セキュリティ評価に関する研究会 - 調査報告書 - ，”情報処理推進機構，2008.