社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (62)
2007－CSEC－ 36 (62)
2007／3／2

金融分野における生体認証システムのセキュリティ要件に関する一考察※

田村 裕子*

*日本銀行金融研究所
情報技術研究センター
103-8660 東京都中央区日本橋本石町 2-1-1
yuuko.tamura@boj.or.jp

宇根 正志†

†独立行政法人 産業技術総合研究所
情報セキュリティ研究センター
101-0021 東京都千代田区外神田 1-18-13
masashi-une@aist.go.jp

あらまし わが国では，CD/ATM 端末における金融取引等において、顧客の本人確認手段の 1 つとして生体認証技術を利用する動きが広がっている．ただし，現時点では生体認証システムのセキュリティ評価手法が確立しておらず，生体認証システムを利用する際には，関連する標準規格の審議動向や研究開発動向を十分にフォローしておく必要がある．本稿では，金融分野で用いられる生体認証システムに関連する 4 つの文献を参照し，それらに記述されているセキュリティ要件を整理する．また，研究開発の現状を踏まえ，各要件をどのように満足させるかについて考察する．

A Study on Security Requirements of Biometric Authentication Systems in the Financial Sector#

Yuko TAMURA*

*Center for Information Technology Studies
Institute for Monetary and Economical Studies
Bank of Japan
2-1-1 Nihonbashi-Hongokucho Chuo Tokyo 103-8660
yuuko.tamura@boj.or.jp

Masashi UNE†

†Research Center for Information Security
National Institute of Advanced Industrial
Science and Technology
1-18-13 Sotokanda Chiyoda Tokyo 101-0021
masashi-une@aist.go.jp

Abstract In Japan, the use of biometric authentication techniques has spread as one of measures for customers authentication in financial transactions such as those at CD/ATM terminals. However, security evaluation methods for biometric authentication systems have not been established yet. In making use of such systems, financial institutions have to follow international standardization activities and recent R&D trends regarding the security of the biometric authentication techniques. In this paper, we will refer to four documents relating to the security of biometric authentication systems used for financial services and summarize the security requirements for such systems. Then, we will discuss how to meet the security requirements by taking into account the recent R&D trends of the biometric authentication techniques.

※ 本稿に示されている意見は，筆者たち個人に属し，日本銀行あるいは産業技術総合研究所の公式見解を示すものではない．

Views expressed in this paper are those of the authors and do not necessarily reflect the official views of Bank of Japan or National Institute of Advanced Industrial Science and Technology.

1 はじめに

機械によって個人を自動的に認証する手段として，生体認証技術が注目を集めている．金融分野においても，偽造キャッシュカードによる不正な預金引出しへの対策技術の1つとして注目され，CD/ATM 端末における本人確認手段として採用されている．

生体認証技術は，単独での利用を想定した場合，暗証番号やカードを装置に提示する手法と比べ，個人が情報を憶えておく，あるいは，物体を所持しておく手間が不要であり，使い勝手がよいとの評価が多い．認証精度評価については，その方法に関する国内標準が存在するほか，生体認証技術の国際標準化を担当する ISO/IEC JTC1/SC37 で精度評価方法の標準化が審議されている．また，生体情報のデータベースを構築し，生体認証システムやアルゴリズムを比較・評価するプロジェクトも欧米を中心に盛んに行われている[1].

一方，悪意をもったユーザを想定する場合のセキュリティ評価に関しては，主な脆弱性や脅威についての研究成果は少なくないものの（例えば[2]），評価手法の開発に関する研究発表が少なく，まだ評価手法が確立されていない．なりすましの脅威に対する評価尺度として誤受入率（FAR: false acceptance rate）が参照されるケースが多いが，本尺度は攻撃者が自分の生体情報を提示してなりすましを試みる“zero-effort attack”への耐性を評価するものであり，攻撃者に有利な状況を想定した場合の評価に用いることは適切とはいえない[3].

生体認証システムを利用する際には，アプリケーションで要求されるセキュリティ・レベルをどのように達成するかが課題となる．関連する標準・ガイドライン・技術仕様等のセキュリティ要件や，最新の研究開発動向をフォローし，既知の脆弱性を回避しているか，また，既存のセキュリティ評価尺度からみて適切なセキュリティ・レベルを確保しているかを継続的に確認することが求められる．

本稿では，4 つの代表的な文献を参照し，金融用途の生体認証システムのセキュリティ要件を整理するほか，各要件を満足させるための方策について考察する．

2 生体認証システムと主な脅威

2.1 生体認証システムの構成

生体認証システムは，個人の身体的・行動的特徴（以下，生体特徴と呼ぶ）を用いて自動的に本人確認を行うシステムであり，一般に次の 4 つの処理から構成される．

(1) センサによって，被認証者の生体特徴を反映する生体情報（アナログ）を取得する．
(2) 生体情報から被認証者に固有のパターン（特徴データと呼ぶ）を抽出する．
(3) 予め登録されている特徴データ（テンプレートと呼ぶ）と，認証時に得た生体情報（サンプルと呼ぶ）から生成した特徴データを照合し，類似度を算出する．
(4) 上記(3)で得た類似度を判定しきい値と比較し，被認証者が本人か否かの判定結果を出力する．

2.2 主な脅威と攻撃シナリオ

生体認証システムの代表的な脅威として，認証時のなりすましや登録時のバックドアの作成（登録者以外でも認証をパスできるテンプレートを登録する）が挙げられる（例えば[4]）．認証時のなりすましに焦点を当てて，これまでに明確化されている脅威から攻撃のシナリオを考えると，以下の 5 つが挙げられる（図参照）．

- **攻撃シナリオ 1**：センサに提示する情報を得る（準備 A）→準備 A で得た情報を提示する媒体を得る（準備 B）→認証時にシステム内部の情報の改変は行わず，センサに生体特徴等を提示する（実行 A）
- **攻撃シナリオ 2**：準備 A→準備 B→誤受入を誘発するために動作環境を変化させる（準備 D）→実行 A
- **攻撃シナリオ 3**：準備 A→準備 B→システム内部の情報を改変する（準備 C）→実行 A
- **攻撃シナリオ 4**：準備 A→準備 B→準備 C→準備 D→実行 A
- **攻撃シナリオ 5**：システム内部の情報の改変に利用するデータを準備する（準備 E）→認証時にシステム内部の情報を改変する（実行 B）

準備 A は，攻撃対象のユーザ（攻撃対象者という）の生体特徴を推定する場合と，攻撃対象者の生体特徴以外の情報を入手する場合が考えられる．攻撃対象者の生体特徴を推定する手段としては，(1)システム内部の情報（攻撃対象者の生体情報やテンプレート）や外部に出力される情報（判定結果等）から推定する，(2)攻撃対象者本人から採取する，(3)その他の場所（残留した生体情報，血縁者）から採取した情報から推定するというものが考えられる．「システムから出力される判定結果を観察しつつシステムに提示する情報を変化させ，攻撃対象者のテンプレートと誤一致させる生体特徴を探索する」という攻撃（hill-climbing attack）は上記(1)に含まれる．また，攻撃対象者が気づかないうちに生体特徴に関する情報を得るという方法は上記(2)に含まれる．

攻撃対象者の生体特徴以外の情報としては，例えば，攻撃者自身の生体特徴や，複数のテンプレートと誤一致を引き起こす情報（wolf と呼ばれる）が挙げられる．前者は zero-effort attack に，後者は wolf attack [3]にそれぞれ用いら

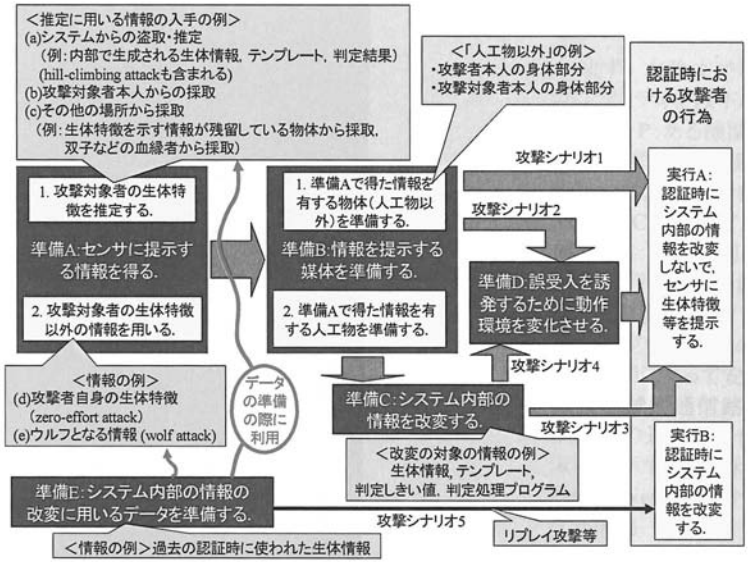

図: 認証時におけるなりすましを目的とする攻撃シナリオ

れることになる.

準備 B における生体特徴を提示する媒体としては, 人工物の場合とそれ以外の場合が考えられる. 後者には, 攻撃対象者や攻撃者自身の身体の一部が想定される.

準備 C におけるシステム内部の情報の改変については, なりすまし試行前に判定しきい値やテンプレートを都合のよいものに改変するという手段が想定される.

準備 D は, 一般にセンサが環境の変化に敏感である点に着目するものである. 例えば, 光学センサの場合, 当該センサが感知する光の波長と近い光の光源を装置近くに配置し照射することで生体情報の品質を変化させ, 誤一致を引き起こしやすくしておくといった手段が考えられる.

準備 E では, 例えば, 過去の認証時に使われた生体情報を入手するといった準備を行うことが想定される. wolf となる生体情報やテンプレートを準備することも想定される. このように, 準備 E を実行する際には, 準備 A で用いられる情報と同種の情報も用いられると考えられる. また, 実行 B において判定結果のデータを改変するという攻撃を行う場合, 準備 E では特段データを準備する必要がなくなる.

また, 攻撃シナリオ 5 における実行 B はシステム内部の情報の改変に相当し, その手段は形式的には準備 C と同一となる.

3 標準・ガイドライン等のセキュリティ要件

3.1 参照する文献

金融向け生体認証システムのセキュリティ要件を検討する際の参考文献として, 以下を取り上げる.

- 金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」(安全対策基準と呼ぶ) [5]
- ISO 19092-1, "Financial services – Biometrics – Security framework" [6]
- 全国銀行協会「全銀協 IC キャッシュカード標準仕様」(全銀協仕様と呼ぶ) [7]
- ニューメディア開発協会「金融分野におけるバイオメトリック認証の適用研究」(NMDA 報告書と呼ぶ) [8]

安全対策基準は, わが国の金融機関の情報システムに安全対策を実施する際の共通基準であり, 金融庁の金融検査マニュアルにも参考文献として規定されている.

ISO 19092-1 は, 金融機関が生体認証システムを利用する際の留意点を規定した国際標準であり, 生体認証システムのモデル, 脅威, セキュリティ要件, 認証精度等について解説的な記述を含んでいる.

全銀協仕様は, わが国の銀行が提供するキャッシュカード・サービスの情報システムの技術仕様を規定する業界標準であり, 全国銀行協会によって策定されたものである. IC キャッシュカード取引で利用される生体認証のセキュリティ要件の一部が記述されている. 特に, IC カード内でテンプレートとサンプルから生成する特徴データの照合を行うケースが想定されている.

NMDA 報告書は, ATM や銀行窓口での金融取引時の本人確認に生体認証を利用する際のモデルの構築, 生体認証システムの各種要件の導出等を内容としている.

全銀協仕様と NMDA 報告書は比較的具体的なアプリケーションを想定している．安全対策基準と ISO 19092-1 は，金融向けの生体認証システム一般を対象としている．いずれの文献も想定されるセキュリティ要件を網羅したものではない点に留意する必要がある．

3.2 セキュリティ要件

4 つの文献におけるセキュリティ要件は，2.2 節の準備 A ～E，実行 A，B を困難にするための要件として解釈・整理できる．その結果は表 1，2 のとおりである．

4 考察：どのようにセキュリティ要件を満足させるか？

4.1 準備 A と実行 A に対する要件

(1)攻撃対象者の生体情報の推定

攻撃対象者の生体特徴の推定を困難にするための要件として，テンプレート等の暗号化，データベースのアクセス管理，キャンセラブル・バイオメトリクスの利用，装置の耐タンパー化が主に挙げられている．暗号化については，例えば CRYPTREC の評価結果を参照することで一定のセキュリティを有する方式を選択できる．

表 1：安全対策基準および ISO 19092-1 に記述されている主なセキュリティ要件

攻撃シナリオの一部	セキュリティ要件	
	安全対策基準	ISO 19092-1
準備 A	【システム内部の情報の盗取に対する要件】 <運 53-1>生体認証情報（テンプレート，サンプル等）の不正利用等の防止のため，生体認証情報を移送・伝送・保管する場合は暗号化が必要．（例：暗号化や耐タンパー性の付与，外部ネットワークからのアクセス制限） 【テンプレートからの推定に対する要件】 <技 35-1>テンプレートはサンプルに流用できない設計とする．（キャンセラブル・バイオメトリクスなど技術動向を考慮） 【攻撃対象者本人からの盗取に対する要件】 <技 35-1>偽 ATM（偽センサ機器等）の設置による，生体認証情報の盗取を想定した場合の対策例：防犯カメラでの監視，職員による巡回点検，利用者への注意喚起	【システム内部の情報の盗取に対する要件】 ・テンプレートや入力される生体情報等を暗号化する． ・類似のテンプレートの探索を防止するために，テンプレートのデータベースへのアクセスを適切に管理する． ・テンプレートや生体情報等が漏れる可能性があるインターフェースやケーブル等を物理的に保護する． ・装置の物理的な改変を伴う攻撃に対しては，その痕跡が装置に残るとともに，攻撃を検知して内部のテンプレート等を直ちに消去する機構を有している． 【攻撃対象者本人からの盗取に対する要件】 偽の装置による生体情報の盗取を防ぐために，警備員やビデオカメラによる監視を行う． 【hill-climbing attack に対する要件】 テンプレートと入力情報の類似度を表示する場合，類似度を連続値で示すのではなく，hill-climbing attack を困難にするように離散値で示す．
準備 B	記述なし	記述なし
準備 C	【テンプレートや生体情報の改変に対する要件】 <運 53-1>テンプレートの改ざん検知策の実施が望ましい．（対策例：伝送データの改ざん検知策→電子署名やメッセージ認証コード） <技 35-1>判定における類似度が極端に高い場合は，認証をパスさせない． 【判定しきい値や判定処理プログラムの改変に対する要件】 <技 33>伝送データの改ざん検知策を講ずること．（対策例：電子署名，メッセージ認証コード）	【テンプレートや生体情報の改変に対する要件】 ・伝送・保管中のテンプレートの一貫性をデジタル署名等の暗号技術を用いて確認する． ・外部インターフェースやケーブルを物理的に保護する． ・装置の物理的な改変を伴う攻撃に対しては，その痕跡が装置に残るとともに，攻撃を検知して，内部のテンプレート等を直ちに消去する機構を有している． 【判定しきい値や判定処理プログラムの改変に対する要件】 ・判定結果の一貫性を暗号技術によって確認可能にする． ・不適切なキャリブレーションに対しては，適切に設定された FAR と FRR を実現するために必要なポリシーを定め，誤り率を検証するログを生成・管理する．
準備 D	<設 113>防犯カメラにより，出入口，自動機器室の状況を撮影，監視する．	・環境条件の変化によって FAR が許容レベルを超えるという事象が発生していないか検知する． ・（一定範囲の環境変化において安定して動作することを確認するために，）システムの適切なテストを実施する．
準備 E	準備 A に対する要件が該当する．	準備 A に対する要件が該当する．
実行 A	【zero-effort attack に対する要件】 <技 35-1>認証精度設定等の適切性の確認を行うことが必要である． 【人工物等の提示に対する要件】 <技 35-1>生体検知装置での確認，職員による対面確認	【zero-effort attack に対する要件】 適切に設定された FAR と FRR を実現するために必要なポリシーを定め，誤り率を検証するログを生成・管理する． 【人工物等の提示に対する要件】 ・生体情報取得時に，被認証物の生体検知を行う． ・生体認証装置を人間やカメラ等によって監視する．
実行 B	準備 C，D に対する要件が該当する．	準備 C に対する要件が該当する．

（備考）「安全対策基準」の欄の「<技-○>」「<運-○>」はそれぞれ当該要件が記述されている技術基準項目，運用基準項目を示す．

表2：全銀協仕様およびNMDA報告書に記述されているセキュリティ要件

攻撃シナリオの一部	セキュリティ要件	
	全銀協仕様（9節から引用・要約）	NMDA報告書（6.2.5，6.2.6節から引用・要約）
準備A	【システム内部の情報の盗取に対する要件】 ・センシティブ情報の漏洩を防止するため，ATM 端末～カード間の暗号化は必須とする． ・照合処理が終了した際には，装置内に残留する生体情報を消去することが望ましい．	【システム内部の情報の盗取に対する要件】 ・登録情報（テンプレートや当該ユーザの属性情報）をサーバで管理する場合，サーバのアクセス権限を設定するとともに，格納されたデータは適切な強度で暗号化し管理すべき． ・口座持ち主の生体情報を入力する装置や登録装置は，十分に安全な管理の下で運用するか，十分な耐タンパー性を備えるべき．また，生体情報を出力する場合は適切な強度で暗号化し出力すべき． ・トークンは適切な耐タンパー性を保持すべき． 【テンプレートからの推定に対する要件】 ・キャンセラブル・バイオメトリクスの適用を推奨．その成熟を見極め，適用を検討されたい．
準備B	記述なし	記述なし
準備C	（CD/ATM 端末と IC カード間での交信データのフォーマットは ISO/IEC 7816-11 を参照している．同標準は，デジタル署名やMACによって交信データの一貫性を確認可能なデータ形式を規定している．）	【判定しきい値の改変に対する要件】 認証パラメータの設定の不正変更への要件として，物理的セキュリティ機能の導入やセキュリティ機能の保証が挙げられる． 【判定処理プログラムの改変に対する要件】 認証結果の改ざんによる不正利用への対策として，例えば，照合機能と，その結果を判定してサービスを提供する機能までの間のそれぞれの実装モジュール間の相互認証機能の導入がある．
準備D	登録時と照合時に利用環境をできるだけ合わせることが望ましい．	記述なし
準備E	準備Aに対する要件が該当する．	準備Aに対する要件が該当する．
実行A	【zero-effort attack に対する要件】 無制限に生体認証のリトライを繰り返す攻撃に対応するために，生体認証不一致となった回数をカウントして上限値として設定した回数を超える場合に生体認証アプリケーションを閉塞する機能の実装は必須とする	【人工物等による提示に対する要件】 ATM など自動機によるバイオメトリック認証において，身体的特徴の複製物による生体情報の入力による不正利用への対策として，例えば生体検知機能の導入がある．
実行B	準備Cに対する要件が該当する．	・準備Cに対する要件が該当する． 【リプレイ攻撃に対する対策】 ATM など自動機によるバイオメトリック認証において，電子的な真正情報（過去に詐取したバイオメトリック・キャプチャ・データなどによるリプレイ攻撃）の入力による不正利用への対策として，例えば，自動機の物理的セキュリティ機能の導入やそのセキュリティ機能の保証などがある．

データベースのアクセス管理については，生体情報やテンプレートが個人情報であり，通常の個人認証で利用されるパスワードや秘密鍵とは異なる性格を有している点に留意して管理方法を検討することが求められる．

キャンセラブル・バイオメトリクスについては，実用の域に達していないという見方が一般的であり，現時点で本手法を採用するという要件の充足は困難である．こうした事情から，安全対策基準と NMDA 報告書では，本手法の採用を要件としているのではなく，今後の技術動向の見極めが重要である旨の記述をしている．

装置の耐タンパー化については，既存の耐タンパー化手法の中から各アプリケーションに応じてどれを選択するかという課題がある[9]．ISO 19092-1 では，攻撃に対する能動的な対応を可能とする機能（タンパー・レスポンスと呼ばれる）の実装が要求されている．

(2)攻撃対象者の生体特徴以外の情報の利用

攻撃対象者の生体特徴以外の情報（攻撃者自身の生体特徴やwolfとなる情報等）の利用については，それ自体を困難にすることは容易でなく，これらがセンサに提示される時点（実行Aのタイミング）でいかに検知・排除するかが重要となる．

実行 A を困難にするための要件をみると，zero-effort attack に対しては，FAR 等の認証精度の要件設定と実システムの精度評価値が適切であることを確認する必要がある．認証精度要件の設定については，既存の JIS TS X 0100[10]を参照可能である．実システムの認証精度については，当該システムの精度評価値が実際の動作環境を反映した条件下で測定されたものであることをベンダー等に確認することが有用である．

また，既存の攻撃の例として wolf attack が提案されているが，本攻撃の提案はごく最近であり，今回参照した文献には対応する要件となるものは見当たらない．現時点での wolf attack への対応として考えられるのは，ウルフ攻撃確率（wolfを提示した場合に誤一致が生じる確率）[3]が許容

レベル以下となることを確認可能なシステムやアルゴリズムを選択するというものである．また，ウルフを人工物によって提示する攻撃に限定する場合，生体検知機能等，人工物を検知・排除する手段の採用も一案であると考えられる．いずれにしても，ウルフ攻撃確率は当該照合アルゴリズムが公表されていないと算出困難であり，ベンダー等に対応を確認することが必要となる．

4.2 準備Bと実行Aに対する要件

準備Bを実行困難にするための要件はいずれの文献においても見当たらないが，実際に人工物の作製等を防止することは困難であると考えられるため，不自然なことではない．したがって，人工物等が提示される時点（実行A）で検知・排除することが重要となる．

実行Aを困難にするための要件としては，生体検知，人間あるいはカメラ等による監視が挙げられている．生体検知については，既存の各種手法に関する評価方法が確立されていないという問題がある．したがって，生体検知手法を利用する際には，ベンダー等に具体的な評価結果の提示を求め，十分に機能することを確認する必要がある．ただし，ATMでの利用等においてはカメラ等による監視も一定の効果を有しているといえる．こうした監視が困難なアプリケーションにおいては生体検知によらざるを得ない．

4.3 準備Cに対する要件

準備Cの実行を困難にするための主な要件として，デジタル署名等の暗号技術によるデータの一貫性確保と，装置の耐タンパー化が挙げられている．これらについては4.1節と同様の考察ができる．

4.4 準備Dに対する要件

準備Dの実行を困難にするための要件として，防犯カメラ等による監視，FARの変動の検知が含まれている．FARの変動検知については，装置の誤判定をリアルタイムで検知する必要があるが，そもそも誤判定か否かをどのように判別するかが問題となる．動作環境の変化の許容度を予め設定し，その変化をモニターして範囲内に収まっているか否かを確認するという対応も考えられるが，その場合，同機能を別途準備する必要がある．ATM等の管理された環境下での利用であれば，常時監視という対応も現実的と考えられる．

4.5 準備Eに対する要件

準備Eを実行困難にするための要件は準備Aと同様であり，4.1節の考察が当てはまる．

4.6 実行Bに対する要件

実行Bを困難にするための要件は準備Cに対する要件と同様となる．ただし，実行Bは認証時において実行されるため，ATM等の管理された環境下においては監視体制の充実といた対応も有効であると考えられる．一方，監視が困難なアプリケーションでは装置の耐タンパー性による対策が重要になる．

4.7 各要件と攻撃シナリオの関係

以上のように，各準備や各実行を困難にするための要件が既存の文献に記述されている．各攻撃シナリオを実行困難にするためには，攻撃シナリオを構成する要素（準備，実行）の1つに対する要件を満足するようにすればよいと考えられる．その際，各要件を実現する対策技術の効果について現時点で定量的に評価できないものも存在するという点に留意する必要がある．そうした場合，複数の要件を組み合わせて対応するという考え方が妥当であろう．

5 おわりに

本稿では，金融用途向けの生体認証システムのセキュリティ要件を既存の4つの文献から引用・整理し，各要件を充足させる方法について考察した．生体認証技術は，セキュリティ技術としてはまだ研究途上にある．生体認証技術の採用を新たに検討する，あるいは，現在使用している生体認証システムの評価を行う際には，本稿で行った考察のように，「どこまで要件を達成可能か」をベンダー等に確認しながら適切に対応していくことが求められる．

参考文献

[1] 新崎卓，“バイオメトリックデータ収集から見た国際標準の状況，”「バイオメトリック認証を支える光センシング技術セミナー講演資料」，オプトロニクス社，2006年

[2] 情報処理推進機構セキュリティセンター，「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」，2006年

[3] 宇根正志・大塚玲・今井秀樹，“生体認証システムにおける新しいセキュリティ評価尺度：ウルフ攻撃確率，”　「SCIS2007論文集」，電子情報通信学会，2007年

[4] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 2nd CD 19792: Information technology – Security techniques – Security evaluation of biometrics, 2006.

[5] 金融情報システムセンター，「金融機関等コンピュータシステムの安全対策基準・解説書 第7版」，2006年

[6] ISO, ISO 19092-1: Financial services – Biometrics – Part 1: Security framework, 2006.

[7] 全国銀行協会，「全銀協ICキャッシュカード標準仕様（第2版）」，2006年

[8] ニューメディア開発協会，“金融分野におけるバイオメトリック認証の適用研究，”「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年

[9] 田村裕子・宇根正志，“金融分野における国際標準・技術仕様等にみる暗号デバイスの物理的セキュリティ特性について，”「2007年暗号と情報セキュリティシンポジウム論文集」，電子情報通信学会，2007年

[10] 日本工業標準調査会，「JIS TS X 0100 バイオメトリクス認証システムにおける運用要件の導出指針」，日本規格協会，2004年