ICカードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題

田村裕子（たむらゆうこ）／宇根正志（うねまさし）

要　旨

金融分野では、キャッシュカードの偽造によるなりすまし防止を目的とするセキュリティ対策の1つとして、ICカードを利用した本人認証システムの導入を進めている。現時点では、CD・ATM取引への導入が中心であるが、今後はデビットカード取引、インターネット・バンキングなど、さまざまな場面での利用も想定されるであろう。

こうしたICカードを利用した本人認証システムをセキュリティの観点から有効に活用するためには、個々のアプリケーションに応じた適切なセキュリティ対策技術の採用が重要である。そうした方法の1つとして、想定される脅威を明確にしたうえで、セキュリティ要件を導出し、要件を充足する対策技術を採用することが考えられる。

個々のアプリケーションに応じた要件の抽出と、それを満足する対策技術の選択には、さまざまな方法が考えられる。まず、最初に挙げられる方法としては、対策技術に関する最新動向を把握しつつ、「目安の1つ」となる各種の国際標準や技術仕様を参照し、望ましい対策技術を探るという方法がある。

本稿では、こうしたアプローチに基づき、ICカードを利用した本人認証システムを対象に、関連する既存の国際・業界標準や技術仕様の記述を整理しつつ、セキュリティ要件とそれらを満足する対策技術について考察を行う。また、本考察に基づき、金融機関がこれらの文献を参照して対策技術の検討を行う際の留意点を示す。

キーワード：技術仕様、国際標準、セキュリティ要件、本人認証、ICカード

本稿は、2007年3月6日に日本銀行で開催された「第9回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいは独立行政法人産業技術総合研究所の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

田村裕子　日本銀行金融研究所（E-mail: 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
（現 日本銀行金融研究所企画役、E-mail: masashi.une@boj.or.jp）

１．はじめに

預金取引においては、取引を実行するユーザが預金者本人であることを確認する必要があり、一般に、こうした確認は本人認証と呼ばれる。金融業界では、CD・ATM等の端末を利用した預金取引における本人認証を、主に磁気ストライプによるキャッシュカードと4桁の暗証番号（PIN: personal identification number）を利用して行ってきた。しかし、キャッシュカードについては、磁気ストライプに記録される情報の読取りや書込みが可能なリーダ・ライタが比較的容易に入手できるようになり、端末に「金融機関が発行したキャッシュカード」と誤認させるカードの偽造が容易となったことから、本人認証の安全性が低下する結果となった。こうしたキャッシュカードの偽造によるなりすましを防止する技術、および、運用の見直しが金融機関に対して求められ（金融庁［2005］）、金融機関は対策の1つとして、キャッシュカードのICカード化や生体認証の導入を急速に進めている（金融庁［2006］）。ICカードを本人認証システムの一端を担うものとして十分に活用することができれば、より高度なセキュリティ機構を付与することができると期待できる。

一般に、情報システムにセキュリティ対策を講じる際にその対策の内容や実装方法が適切でない場合、導入した対策技術が期待されたレベルの効果を発揮しないことがある。セキュリティ対策を講じるうえでは、通り一遍の対策ではなく、個々のアプリケーションに応じたセキュリティ対策のあり方を考え、対策技術の内容や実装方法を適切に選択することが重要である。そのためのアプローチの1つとして、対策技術に求められるセキュリティ要件を導出するという方法が挙げられる。セキュリティ要件とは、自らで設定した安全性を確保するために必要な条件を指すものであり、導出したセキュリティ要件を満足するように当該システムを構築することができれば、要求したレベルの安全性を持つシステムを構築できることとなる。

金融分野の情報システムに関するセキュリティ要件を導出するうえで参考になると考えられる資料としては、まず、金融情報システムセンター（FISC）によって作成されている「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」（以下、FISC安全対策基準。金融情報システムセンター［2006］）が挙げられる。本基準は、わが国の各金融機関が提供する金融サービスに関連するコンピュータ・システムに安全対策を実施するための共通基準として策定されたものであり、各金融機関がコンピュータ・システムの適切な安全対策を実施するうえで参考にすることが期待されている。また、金融庁の金融検査マニュアル（金融庁［2007］）にも引用されており、FISC安全対策基準は、金融機関が情報システムの安全対策を講じる際に依拠する基準になっている。FISC安全対策基準では、アプリケーションに依存して金融機関が自らその対策技術を決定できるように、ある程度自由度が残されている項目がある。こうした項目については、想定するアプリケーションにおいてどのような対策技術を採用することが適切かを判断することによって、

セキュリティ要件を導出することが求められる。

そこで、本稿では、ICカードを利用した本人認証システムのセキュリティ要件を、FISC安全対策基準を参考にしながら導出するうえで検討が必要となる事項の整理・考察を試みる。特に、対策技術の自由度が比較的大きい項目として、生体認証方式とICカード等のハードウエアに焦点を当てる。検討の方法としては、生体認証方式やICカードに関する既存の国際・業界標準や技術仕様を参考にするという方法を採用する。これらの文献は、比較的具体的なアプリケーションを想定する場合に対策技術に求められるセキュリティ要件を記述しており、金融分野において適用される対策技術のレベルに関して1つの目安を提供するものと考えることができる。さらに、これらのセキュリティ要件を活用して具体的な対策を検討する際の留意点を示す。

本稿の構成は以下のとおりである。まず、2節において、本人認証を実行するためのツールとしてICカードを利用した場合の認証形態について説明する。3節では、FISC安全対策基準から、ICカードを利用した本人認証システムへの対策基準となる項目を抽出し、セキュリティ対策技術を選択するうえで検討が必要と考えられる主な課題を整理する。4、5節では、3節において整理した課題について、既存の国際・業界標準や技術仕様に記述されているセキュリティ要件や対策技術を参照しつつ検討する。特に、4節では生体認証について、5節ではICカード等のハードウエアの耐タンパー性について検討を行う。6節では、本稿における検討の結果をどのように活用できるかについて説明し、本稿を締めくくる。

2．金融取引における本人認証

(1) 本人認証の手段

本人認証とは、被認証者が本人（被認証者によって主張された身元）であることを確認することであり、本人のみが提示可能な情報を利用して実現される。「本人のみが提示可能な情報」とは、登録時において被認証者が届け出た身元と対応付けられる情報であり、その身元に対応するユーザのみが有する情報を指す。本人認証を行う手段としては、知識、所持物、生体情報を利用した以下の認証方式が代表的である。

- 知識認証（something you know）：認証者に登録された情報を知っているか否かによって本人であることを確認する方式。当該情報が本人によって適切に管理されていることが条件であり、第三者による推測が困難である場合等に有効である。金融取引での知識認証に利用される情報としては、PINやパスワードが代表的である。
- 所持認証（something you own）：認証者が配付した媒体を所持しているか否か

によって本人であることを確認する方式。認証者は、被認証者が所持する媒体に関する情報をあらかじめ入手・登録しておき、認証時に提示された当該媒体から対応する情報を読み出して照合する。所持認証では、当該媒体が本人によって適切に管理されていることが条件であり、第三者による偽造が困難である場合等に有効である。金融取引での所持認証に利用される媒体としては、キャッシュカードやクレジットカードが代表的である。そのほか、インターネット・バンキングにおける本人認証では、乱数表[1]やワンタイム・パスワード生成器[2]も所持認証のツールとして利用されている。

・生体認証（something you are）：認証者に登録された情報と提示された生体特徴に関する情報（以下、生体情報と呼ぶ）の対応関係によって本人であることを確認する方式。生体特徴が個人を識別できること、人工物等による偽造が困難であること等の条件が満足される場合に有効である。わが国の金融分野では、銀行ATMにおいて、手のひらや指の静脈パターンを生体特徴として利用するものが普及している。

上記いずれの認証方式も、認証者側にあらかじめ登録された情報と被認証者によって提示された情報とを比較・照合することで本人であることを確認する。例えば、1対1照合による認証形態では、登録と認証は次の要領で実行される。

・登録フェーズ：登録受付者は、身元証明書等によって提示された身元を示す情報（ユーザID）とともに、登録申請者が提出した「認証に利用する情報」をデータベースに登録する。この「認証に利用する情報」には、①登録申請者が秘密に記憶しておく情報、②所持物に固有の情報、③生体情報のいずれか、あるいは、④上記①～③の情報そのものではなく、それらと対応付けられた情報が利用される。知識認証や所持認証では、認証に利用する情報を登録受付者が生成し、当該情報、あるいは、当該情報を付与した媒体を安全な方法で登録申請者に渡すこともある。
・認証フェーズ：被認証者は、ユーザIDとともに認証に利用する情報を認証者に提示する。認証者は、提示された情報がデータベースに登録されたものと一致するか（あるいは、対応するものであるか）否かを確認し、確認できた場合、被認証者をユーザIDに対応するユーザであると判断する。

1 金融機関によって、数字、アルファベット、ひらがな等を要素とする行列が記載された媒体。乱数表は預金者ごとに異なる。認証では、金融機関から要求された位置（チャレンジ）に対応する行列の要素の入力が被認証者に求められ、金融機関は、その結果が預金者に対応付けられた乱数表と整合的であるか否かを確認する。金融機関によって、1回の認証に利用されるチャレンジの数や行列のサイズはさまざまである。

2 ある一定の時間ごとに自動的に変更されるパスワード（ワンタイム・パスワード）を表示する媒体。認証では、その時点で表示されているワンタイム・パスワードの入力が被認証者に求められる。ワンタイム・パスワードは、将来のパスワードを過去のものから推測困難な形態で生成する仕組みとなっており、ある時点におけるワンタイム・パスワードが漏洩した場合でもなりすましを困難にできるといわれている。

(2) ICカードを利用した本人認証

イ．ICカードを利用した本人認証とは

金融取引を行ううえでは、まず、金融機関は利用者の本人確認を行う必要があり、キャッシュカード取引やクレジットカード取引をはじめとする金融取引においては、本人認証のツールとしてICカードを利用するケースが多くみられる。そこで、本稿では、ICカードを利用して行う本人認証を以下のように定義し、その安全性に関する検討を進める。

・ICカードを利用した本人認証：ICカードを提示した被認証者が、当該被認証者によって主張された、金融機関にあらかじめ登録されているユーザであることを、ICカードおよびその他の情報（被認証者が秘密に記憶しておく情報、当該ICカード以外の所持物から得られる情報、生体情報）を利用して、機械で自動的に確認すること。

わが国の金融分野におけるICカードを利用した本人認証では、秘密に記憶しておく情報（PIN等）や生体情報（手のひらや指の静脈パターン等）を併用するケースが一般的である。これは、本節(1)で紹介したICカードによる所持認証に加えて、PINによる知識認証や静脈パターンによる生体認証を併用して実現する本人認証であるといえる。

ロ．想定するエンティティ

ICカードを利用した本人認証システムを構成するエンティティは、想定されるアプリケーションによって異なるが、本稿では、以下のエンティティで構成されるものとする。

・カード所持者：金融機関によってICカードと対応付けられているユーザ。
・ICカード：専用のカード・リーダで読み取る、CPU内蔵型の所持認証用デバイス。
・PINパッド：被認証者によってPINが入力されるデバイス。
・カード・リーダ：ICカードとのインターフェースであり、ICカード内データの読取り、書込みを行うデバイス。
・ホスト：金融機関内に設置され、ネットワークを介して、各アプリケーションを提供するコンピュータ。
・端末：ICカード・ホスト間の通信を媒介するデバイス。PINパッド、カード・リーダ、生体情報取得用センサ等が一体化して端末を構成している場合や、各デバイスが独立して存在する等、さまざまなケースがある。

ハ．本人認証の具体的手段

ICカードを利用した本人認証は、ICカードおよびその他の情報を利用して実行される。そのため、認証者は、提示されたICカードが真正なものであるか否かを確認するとともに、知識認証や生体認証を実行することとなる。以下では、こうした認証方式の形態の例を紹介する。

（イ）ICカード認証

ICカードによる所持認証では、被認証者によって提示されたICカードが金融機関によって配付されたものであるか否かを確認する必要がある。こうした確認処理をICカード認証と呼ぶとき、ICカード認証は、通常ICカード内に格納されているデータ[3]の一貫性を確認することによって行われる。

また、認証者（ICカードの真正性確認の処理を実行するエンティティ）が端末である場合にはオフライン認証、認証者がホストである場合にはオンライン認証と呼ばれる。そのほか、暗号技術として共通鍵暗号と公開鍵暗号のいずれの方式を利用するかによってもICカード認証を分類することができる。金融向けのICカードを利用したシステムに関する業界標準であるEMV（EMVCo［2004a, b, c］）では、公開鍵暗号（デジタル署名）を利用したオフラインでの認証方式が記述されている。

（ロ）PIN認証

PINによる知識認証[4]では、被認証者によって提示されたPINが、あらかじめ金融機関に登録されているデータ（参照PINデータ）に対応するか否かを確認する必要がある。こうした確認処理をPIN認証と呼ぶとき、PIN認証は、参照PINデータを格納するエンティティと認証処理を実行するエンティティの違いによって分類することができる。例えば、金融取引におけるPINの取り扱いに関する国際標準であるISO 9564（ISO［2002, 2003b］）では、認証処理を、ICカード、端末、ホスト、それ以外で実行することを想定しているほか、参照PINデータの格納先についてもICカード、端末、ホストを想定している。また、ホストを利用せず、ICカードや端末のみを利用して実行される形態はオフラインPIN認証、ホストを利用して実行される形態はオンラインPIN認証と呼ばれる。

（ハ）生体認証

生体認証では、被認証者が生体特徴を提示して行われる。具体的手順は以下のとおりである。

3 ICカード認証の形態としては、カード内部のメモリーに格納されるデジタル・データのみを利用するもののほかに、複製困難なカードの物理的情報を利用するもの（例えば、松本・青柳［2005］で検討されている人工物メトリクスの利用）も考えられる。ここでは、現時点ではわが国の金融分野で主に採用されている「メモリーに格納されるデジタル・データのみを利用する形態」に絞って議論する。

4 知識認証にPINとパスワードのどちらを利用するかによって、認証処理手順や認証形態の分類に差異が生じないことから、本節では、被認証者が秘密に記憶しておく情報としてPINを利用するケースを取り上げる。

(A)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。
(B)生体情報から被認証者に固有のパターン（以下、特徴データ）を抽出する。
(C)あらかじめ登録されている特徴データ（以下、テンプレート）と、認証時に得た生体情報から生成した特徴データを照合し、両者の類似度を算出する。
(D)上記(C)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。

生体認証の形態は、テンプレートを格納するエンティティ、認証時に特徴データを生体情報から抽出するエンティティ、照合処理を実行するエンティティによって分類することができる。ISO/IEC 7816-11（ISO and IEC［2004］）では、テンプレートをICカード内に格納し、端末で特徴データを抽出したうえで、①ICカード内で照合処理を実行する形態（on card matching）と②ICカード外（端末）で実行する形態（off card matching）が記述されている。

(3) デバイスのライフ・サイクル

本人認証システムのセキュリティ要件を検討する際には、システムを構成するエンティティのライフ・サイクルまでも包含したシステム全体をカバーしたかたちでの検討が求められる。例えば、金融向けの暗号処理を実行するデバイス（以下、暗号デバイス）の安全性に関する国際標準であるISO 13491-1(ISO［2006a］)では、暗号デバイスのライフ・サイクルを以下の5つのフェーズに分類している。

・製造・修理（manufacturing/repair）：暗号デバイスが意図する機能や物理的特性を有するよう、設計・構築・修理・改良・テストを行うフェーズ。
・製造後（post-manufacturing）：暗号デバイスの輸送・保管のフェーズであり、初期鍵の書込みを含む。
・使用前（pre-use）：サービス提供前のフェーズ。本フェーズでは暗号デバイス内に鍵は格納されているが、起動していない。
・使用中（use）：サービスを提供中のフェーズ。
・使用後（post-use）：サービスを提供後のフェーズ。本フェーズには修理のための移送等に伴う一時的なものや、廃棄のための移送も含む。

製造・修理、製造後、使用前、使用後のフェーズでは、金融機関、印刷メーカー、端末メーカー、流通業者等が関与し、これらのエンティティの内部者が関与するかたちでの不正が発生する可能性がある。使用中のフェーズでは、ICカードや端末が金融機関の顧客をはじめとする幅広い層に利用される。本稿では、金融機関等の内部者が不正に関与するケースではなく、外部者による不正の実行の可能性に焦点を当てる。このとき、使用中のフェーズが、攻撃が行われる可能性が相対的に高くな

るタイミングとして考えられるため、以下では使用中のフェーズに絞って検討することとする。

3．FISC安全対策基準におけるセキュリティ要件

(1) FISC安全対策基準について

各金融機関は、ICカードを利用した本人認証システムにセキュリティ対策を講じるに当たって、FISC安全対策基準に依拠している。FISC安全対策基準は、わが国の各金融機関が提供する金融サービスに関連するコンピュータ・システムに安全対策を実施するための共通基準として策定されたものである。ただし、基準項目には、対策技術の例示にとどまっているものが多く、セキュリティ要件を自ら導出することが求められるものも少なくない。

そこで、本節では、ICカードを利用した本人認証システムのセキュリティ要件をFISC安全対策基準に基づいて導出する際、金融機関にどのような検討を行うことが求められるかについて整理する。

イ．想定するアプリケーション

本基準は、金融機関によって提供される金融サービスに関連するコンピュータ・システム一般を対象としている。具体的には、CD・ATMのシステムやインターネット・バンキング等、顧客にオンラインサービスを提供するシステム、他の金融機関等との決済業務に使用するシステム、顧客データを扱うシステム、金融機関等が顧客に提供するハードウエアやソフトウエアを含んでいる。

本基準の対象となる「コンピュータシステム」は、「コンピュータ、端末機器、周辺機器、通信系装置、回線およびプログラム等の全部または一部により構成されるデータを処理するためのシステム」と定義されている。ここでのコンピュータは、「ホストコンピュータ、サーバ、ワークステーション、パソコンの総称」を表すものであると記述されており、金融機関によって管理されるものを示していると想定されることから、2節(2)ロ．におけるホストに相当するものであるほか、ここでの端末機器には、2節(2)ロ．におけるPINパッド、カード・リーダ、端末が含まれると考えられる。

ロ．記述されているセキュリティ要件

FISC安全対策基準は、設備基準、運用基準、技術基準で構成されており、これらの中に、ICカードを利用した本人認証システムに関連するセキュリティ要件が含まれている。各基準の内容は以下のとおりである。

・設備基準：コンピュータ・システムが収容される建物、設備を自然災害、不正

行為等から守るための設備面の対策であり、138の項目から構成される。以下では、設備基準項目X（Xは1～138）を【設 X】と記述する。

・運用基準：コンピュータ・システムの信頼性および安全性の向上を図るための、開発・運用管理体制等についての対策であり、113の項目で構成される。以下では、運用基準項目X（Xは1～113）を【運 X】と記述する。

・技術基準：コンピュータ・システムにおける信頼性および安全性の向上に関するハードウエア、ソフトウエア等技術面の対策であり、53の項目から構成される。以下では、技術基準項目X（Xは1～53）を【技 X】と記述する。

（2）本人認証に関するセキュリティ要件

以下では、FISC安全対策基準の中から、本人認証システムに関連する基準項目について、本人認証全般、PIN認証、ICカード認証、生体認証のそれぞれに関連する項目を整理する。

イ．本人認証全般に関するセキュリティ要件

本人認証全般に関するセキュリティ要件としては、まず、【技 35】「本人確認機能を設けること」が挙げられる。本項目では、「コンピュータシステムの不正使用およびネットワーク拡大による種々の端末を使用した不特定多数の者からの不正アクセスを防止するため、正当な権限を保有した本人であるか、もしくは正しい端末に接続されているかなど、接続相手先の正当性を確認することが重要である」と記述されている。

こうした本人確認に利用する情報については、①広義のパスワード、②暗号利用、③バイオメトリクス、④所有物、⑤これらの併用の5つのタイプに分類したうえで、各タイプに属する具体例が挙げられている（表1参照）。④の「所有物」は、2節で整理した所持認証において被認証者が提示する媒体、③の「バイオメトリクス」は、生体認証において被認証者が提示する生体情報にそれぞれ対応する。このように、ICカードによる所持認証、生体認証は、ともに本人確認を実行するための代表的な

表1　本人確認の方法の例（【技 35】）

本人確認の方法	例
①広義のパスワード	暗証番号、ID・パスワード、ワンタイムパスワード、チャレンジ・レスポンス方式等
②暗号利用	共通鍵暗号、公開鍵暗号、電子署名、認証機関が発行する電子的な証明書（認証書）等
③バイオメトリクス	指紋、声紋、掌紋、網膜パターン、虹彩、筆跡等
④所有物	磁気カード（キャッシュカード、オペレータカード、役席カード）、ICカード、アクセストークン等

表2　不正な預貯金払戻し等への対策の例（【運 44-1】）

対策	対策のための導入技術の例
認証技術の開発	ICカード、生体認証技術の導入等
情報漏洩の防止	自動機器室等における覗き見防止設備の設置、ICカードの導入、CD・ATMの伝送データの暗号化
異常な取引状況の早期の把握のための措置	異常取引検知技術の導入等
その他不正払戻し防止の措置	カードの偽造防止対策や携帯電話によるCD・ATMの取引ロック機能の導入等

方法として挙げられている。また、①の「広義のパスワード」の中には、被認証者が秘密に記憶しておく情報に加えて、ワンタイム・パスワード生成器等によって提示されるパスワードが含まれているほか、②の「暗号利用」については、所持認証に利用する媒体が暗号処理を実行可能である場合に、当該媒体の真正性を確認する手段として利用されることが想定される。

そのほか、FISC安全対策基準では、【運 44-1】「CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること」を設けており、本項目では、「不正払戻し防止のための措置を講ずることにより機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保すること」と記述されている。こうした不正払戻しに対する対策と導入技術として挙げられている例をまとめると以下の表2のとおりであり、ICカードによる所持認証、および、生体認証技術は、不正払戻しへの対策例としても示されている。

ロ．PIN認証に関するセキュリティ要件

PIN認証に関するセキュリティ要件としては、【運 17】「パスワードが他人に知られないための措置を講じておくこと」、【運 100】「口座番号、暗証番号等の安全性を確保すること」、【技 26】「暗証番号・パスワードは他人に知られないための対策を講ずること」が挙げられる。いずれも、第三者による暗証番号・パスワードの盗取を脅威として想定したものであり、漏洩を未然に防止する、あるいは、漏洩した場合においてもその使用を防止するといった対策が記述されている。これらの3つの項目における記述から、PINの漏洩を未然に防止するための対策として記述されている内容をまとめると表3のとおりである。

表3をみると、カード所持者からのPINの盗取、および、端末へのPIN入力時における盗取については、比較的多くの対策例が記述されている。また、端末に入力された後のPINについては、端末の耐タンパー性、あるいは、暗号化によって漏洩を防止する例が記述されている。デバイスの耐タンパー性、あるいは、暗号化によるデータの漏洩防止については、PIN認証のほか、ICカード認証や生体認証においても考慮すべき事項であることから、別途、本節(2)ホ. において整理する。

PINの漏洩については、真正なエンティティ、あるいは、真正なエンティティ間

表3　PINの漏洩に関する攻撃と対策についての記述（【運 17】、【運 100】、【技 26】）

想定する脅威	攻撃と対策に関連する記述	対策例
カード所持者からの盗取	以下の事項を使用者に注意喚起する等の対策が必要である。 ・類推されやすいパスワードを設定しないこと。 ・パスワード等を他人に知られないようにすること。 ・他人のパスワードを使用しないこと。	・使用者への注意喚起
PIN入力時における盗取	・端末機における漏洩防止として、暗証番号・パスワード等は、他人に知られないように、非表示、非印字、重ね打ち、覗き見防止等の対策を講ずることが必要である。 ・媒体上に暗証番号・パスワード等をそのまま記憶させない等の対策を講ずることが必要である。 ・ソフトウエアキーボードを使用し、キーロガーによる暗証番号・パスワードの盗取を防止する。	・PINの非表示、非印字、重ね打ち、覗き見防止（画面の表示［画面の視野角制限、文字の大きさ、文字の色合い、表示内容］、端末機の画面上におけるテンキーの利用者に応じた配列方式の採用） ・ソフトウエアキーボードの利用
PIN入力時における盗取（デビットカード・サービス）	――	・暗証番号入力用のキーパッドへのかざしの設置 ・暗証番号を入力する場所のパーティション等の設置 ・加盟店に防犯カメラ等を設置する場合は、暗証番号を入力する際の顧客の手元が写らないような配置の工夫
デビットカード端末からの盗取	――	・端末の耐タンパー性による保護 ・カード情報[5]の暗号化による保護
伝送データ時における盗取	・データ伝送について暗号化等の必要な対策の検討を行う必要がある。	・暗号化

からの漏洩のみを脅威として想定しており、偽端末等によるPINの盗取は想定していないようである。また、ICカード内に参照PINデータを格納する形態のPIN認証を採用する場合には、参照PINデータの盗取・改ざんを防止することが必要となるが、こうしたデータの盗取・改ざんへの対策についても、本節(2) ホ. にまとめて述べる。

5 カード情報にどういったデータが含まれるかについては明記されていないが、【運 100】では、口座番号等および暗証番号の安全性確保の手段として、それぞれ「カード情報の暗号化」が挙げられていることから、口座番号および暗証番号はこれに含まれると考えられる。

ハ．ICカード認証に関するセキュリティ要件

キャッシュカードのICカード化に当たっては、【技 35】「本人認証機能を設けること」において、「全銀協ICキャッシュカード標準仕様に要求される要件を満たすこと（セキュリティや互換性など）」と記述されているほか、ICカードの運用・技術面について、①ICカードの有効期限、②電子証明書の認証機関の信頼性（運用規定等）、③使用される暗号の強度、④耐タンパー性等に注意することが必要であると記述されている。同様の内容は、【技 40】「カードの偽造防止対策のための技術的措置を講ずること」にも記述されている。ただし、これらの事項①～④については、詳細な対策基準が設定されているわけではないため、金融機関は自らセキュリティ要件を設定する必要がある。

まず、上記①については、例えば、わが国の銀行が提供するICキャッシュカードのシステムの業界標準である全銀協ICキャッシュカード標準仕様（第2版）（以下、全銀協仕様。全国銀行協会［2006］）別冊1に記述されている、「具体的なカード利用の終了（有効期限）の考え方」を参照することができる。本仕様では、ICカードの有効期限の考え方について、(a)ICカードのチップの物理的寿命に起因するもの、(b)ICチップの樹脂モールドの物理寿命に起因するもの、(c)セキュリティ（カード所持者の信頼保証度）による有効期限の考え方、(d)その他の有効期限の考え方の4項目が記述されている。ICカード内に電子証明書（公開鍵証明書）を格納する場合、その有効期限との関係にも注意が必要である。

上記②の認証機関の信頼性については、一般に、認証業務の基本方針を規定した証明書ポリシー（CP: certificate policy）および、CPに基づいて決定される認証業務の具体的な施策を規定した認証実施規定（CPS: certification practice statement）を基に評価することができると考えられる。ISO 15782（ISO［2001, 2003a］）では、金融業務で利用されるPKIにおいて、認証機関が果たすべき役割や責任、公開鍵証明書の管理者拡張方法について規定しているほか、ISO 21188（ISO［2006c］）ではCP、CPSの作成方法が規定されている。そのため、こうした国際標準に準拠して認証業務を運用することによって信頼性を確保するといったことが考えられる。そのほか、「電子署名及び認証業務に関する法律」に基づく特定認証業務の認定制度等といった第三者によるセキュリティ監査の結果を利用することも可能である（宇根［2002］）。

上記③の暗号の強度、および、④の耐タンパー性については、PIN認証や生体認証にも関連する項目であり、本節(2)ホ．において整理することとする。

また、【運 100】「口座番号、暗証番号等の安全性を確保すること」では、デビットカード・サービスにおける口座番号等の安全性に関連して、想定する脅威とその対策が記述されている。それらをまとめると表4のとおりである。

デビットカード・サービスにおいては、キャッシュカードから出力される口座番号等を端末から盗取する攻撃を想定しており、端末への耐タンパー性の付与、カード情報の暗号化が技術的な対策として挙げられている。これらについては、別途、本節(2)ホ．において整理する。また、デビットカードの偽造防止策については、

表4　口座番号等の漏洩に関連する脅威・対策についての記述（【運 100】）

想定する脅威	対策例
デビットカード端末からの盗取	・端末の耐タンパー性による保護 ・カード情報の暗号化による保護
伝送データからの盗取	・伝送データからの漏洩防止策
利用明細書等からの盗取	・利用明細書への口座番号等のカード情報を一部あるいはすべて非印字 ・端末への口座番号等のカード情報を一部あるいはすべて非表示
デビットカードの偽造	・デビットカードの偽造防止策（【技 40】を参照）

【技 40】を参照するよう記述されており、【技 40】では、カードの偽造防止対策の例の1つとして、「ICカード化等の高セキュリティ技術の導入」を挙げている。

【運 47】「防犯体制を明確にすること」においては、「巡回時にCD・ATM機、その周辺および出入口付近に隠しカメラやカード情報の不正な読取装置等の不審な装置がないか確認することが必要である」と記述されていることから、不正なカード・リーダの設置を攻撃として想定していると考えられる。この基準項目は、キャッシュカードとして磁気ストライプ・カードを利用する場合を想定しているものと考えられるが、キャッシュカードとしてICカードを利用する場合においても、不正なカード・リーダの設置が攻撃として想定されるケースがあることに注意が必要である。

ニ．生体認証に関するセキュリティ要件

生体認証に関しては、【運 53-1】「生体認証における生体認証情報の安全管理措置を講ずること」、【技 35-1】「生体認証の特性を考慮し、必要な安全対策を検討すること」の2つの対策基準が置かれている。

まず、【運 53-1】では、「生体認証情報を取り扱う各段階について、安全に管理するための手順を定めること」とあり、攻撃と対策に関する記述を整理すると、表5のとおりである。

表5のように、伝送データの盗取・改ざん、データベースやトークンにおける蓄積データの盗取・改ざんが想定されている。データの盗取に対しては、暗号化やデータを保管する装置への耐タンパー性の付与が技術的な対策として挙げられているほか、データの改ざんに対しては電子署名やメッセージ認証コードの適用が挙げられている。

次に、【技 35-1】には、「生体認証の導入と運用にあたって、考慮すべき特性」として、認証精度、代替措置手続き、否認防止、不正認証（なりすまし）等防止、テンプレート保護技術の5項目が記述されている。これらのうち、生体認証に特有の検討が必要となるのは、認証精度、不正認証（なりすまし）等防止、テンプレート保護技術の3つである。

認証精度に関しては、「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」とある。この項目を充足させるためには、各金融機関が、①どの程度の認証精度で

表5　生体認証に関する攻撃と対策についての記述（【運 53-1】）

生体認証情報の取扱段階	攻撃と対策に関連する記述	対策例
利用	・生体認証情報（テンプレート、サンプル・データ等）の不正利用等を防止するため、生体認証情報を移送・伝送する場合は暗号化が必要である。 ・テンプレートの改ざん検知策の実施が望ましい。 ・日常取引において、顧客から取得したサンプル・データについては、安全な管理のもとに速やかに消去することが必要である。	・伝送データの漏洩防止 ・伝送データの改ざん検知策
保存	・テンプレートを検索可能なデータベースに保存する場合は、氏名等の個人情報と生体認証情報を分別管理することが望ましい。 ・登録された生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送、保管する場合は暗号化が必要である。	・データの分別管理 ・伝送データの漏洩防止 ・蓄積データの漏洩防止 ・データ保護、破壊・改ざん防止 ・外部ネットワークからのアクセス制限
トークンの取扱管理	・顧客が保持する記憶媒体（トークン）にテンプレートを保存する場合、トークンを安全に発行するための、手順を明確にすることが必要である。 ・不正アクセス技術の向上等に対応するために、トークンの使用期限を考慮することが望ましい。	・顧客がトークンを保有する際の生体認証情報の漏洩防止対策 ・使用期限の設定

あれば適切であると考えられるか、②認証精度が適切であることをどのようにして確認すればよいかの2点に関して独自に検討する必要がある。

不正認証（なりすまし）等防止とテンプレート保護技術に関する記述を整理すると、サンプル・データ（すなわち、生体情報）に関するものとテンプレートに関するものに大別することができる（表6参照）。

サンプル・データに関する記述に着目すると、その盗取・偽造・不正使用が脅威として示されている。具体的には、既存のATMに偽センサを取り付けてサンプル・データを盗取するという攻撃と、人工物によってサンプル・データを提示するという攻撃が挙げられており、それらの対策例も示されている。テンプレートに関しては、テンプレートの不正利用が脅威として挙げられており、具体例としてテンプレートのサンプル・データへの流用が示されている。対策例としては、サンプル・データへの流用を困難とするテンプレートの設計と、高い類似度を生じるサンプル・データの拒否が挙げられている。また、注目される技術としてキャンセラブル・バイオメトリクスが紹介されている。

以上の整理から、金融機関は、認証精度の設定と確認をどのように行うかを、各アプリケーションに応じて検討する必要があるといえる。さらに、【技 35-1】における不正認証（なりすまし）等の防止を達成するうえで、例示されている攻撃を想定した対策をどのように講じるかを検討する必要もあるといえる。

また、【技 35-1】には、「生体認証の導入と運用にあたっては、技術の最新動向

表6　不正認証（なりすまし）等防止とテンプレート保護技術に関する記述（【技 35-1】）

セキュリティ対策の必要性		攻撃の例	対策例
サンプル・データに関するもの	生体認証情報の登録時や認証時に、センサ等を介して取得する「真正な顧客」のサンプル・データに関して、本人でない者による、その不正入手、偽造、不正使用等を防ぐ手段、運用上の措置を講ずることが必要である。	・偽ATM（偽センサ機器等）の設置による、生体認証情報の盗取	・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
		・人工的に合成してつくった偽造生体を使ったなりすまし	・生体検知装置での確認 ・職員による対面確認
テンプレートに関するもの	テンプレートの不正利用を防ぐ手段、運用上の措置を講ずることが必要である。	・悪意を持った内部者や、ネットワークを経由等した外部者が、「真正な顧客」のテンプレートを不正に入手・使用し、それをサンプル・データ等に不正流用して認証をパスする。	・テンプレートはサンプル・データに流用できない設計とする。 ・テンプレートとサンプル・データの類似度が極端に高い場合は、認証をパスさせない。 ・テンプレートのデータ保護について、キャンセラブル・バイオメトリクスなど技術動向を考慮することが望ましい。

等に留意し、その特性を十分考慮し、必要な安全対策を検討すること」と記述されている。この記述の趣旨を踏まえると、【技 35-1】に具体的に記述されてはいないものの、最新の研究成果によって示されている攻撃や対策技術についてもフォローし、それらに基づいた対策の検討も求められるといえる。

ホ．データの盗取・改ざんに関するセキュリティ要件

これまでに整理したように、ICカード認証、PIN認証、生体認証においては、データの盗取・改ざんが脅威として想定されている。データの漏洩防止については、【技 28】「蓄積データの漏洩防止策を講ずること」、および、【技 29】「伝送データの漏洩防止策を講ずること」から、その対策として記述されている内容を整理すると、表7、表8のとおりである。

また、データの改ざんについては、【技 33】「伝送データの改ざん検知策を講ずること」が準備されており、暗号技術を活用した認証機能、改ざん検知機能の例として、メッセージ認証コードと電子署名が挙げられている。そのほか、ソフトウエアの改ざんについては、【技 49】「コンピュータウイルス等不正プログラムへの防御対策を講ずること」が準備されており、「不正プログラムからシステムを守るため、コンピュータウイルスの侵入や、不正アクセスによるプログラムの改ざんを防止する対策を講ずることが必要である」と記述されている。具体的な防御策としては、コンピュータウイルスの侵入に対しては、①抗ウイルスソフト（ワクチンソフト）の導入、②ファイル管理の実施が挙げられている。また、不正アクセスによるプログラムの改ざんに対しては、①アクセス管理の実施、②不正侵入防止機能の導入、③不正アクセスの要因除去が挙げられているほか、不正プログラムの組込みに

表7　蓄積データの漏洩に関する攻撃と対策についての記述（【技 28】）

想定する脅威	攻撃と対策に関連する記述	対策例
ファイルの不正コピーや盗難	・重要なデータについては暗号化することが望ましい。 ・特に個人データを蓄積する場合には、暗号化・パスワード設定等の対策を講ずることが必要である。 ・電子的取引において蓄積されるデータについても暗号化・パスワード設定等の対策を講ずることが必要である。	・暗号化 ・パスワード設定
外部持ち出しや他の媒体へのコピーが物理的に不可能なコンピュータ機器内の個人データの盗取	・上記対策（暗号化・パスワード設定）のほか、本人確認機能を設けることにより、許可された者以外の者が当該データを判別できないようにする仕組みも有効である。	・本人確認機能
ICカードからの盗取	・耐タンパー性が考えられる。	・ICカードへの耐タンパー性の付与
その他（ICカード以外）蓄積媒体上からの盗取	・暗号化が考えられる。	・暗号化
渉外端末の盗難・紛失	・重要なデータを蓄積する場合には、暗号化することが望ましい。	・暗号化
コンピュータ端末および周辺機器から漏れる電磁波が盗聴され再現される（テンペスト）	・電磁遮蔽カバーの採用 ・電磁波防止フィルターの採用 ・保護対象機器の設置場所から一定範囲内の侵入制限	・電磁遮蔽カバー、電磁波防止フィルターの採用 ・侵入制限

表8　伝送データの漏洩に関する攻撃と対策についての記述（【技 29】）

想定する脅威	攻撃と対策に関連する記述	対策例
データの伝送時における盗聴	・重要なデータについては、暗号化することが望ましい。 ・個人データを伝送する場合には、暗号化・パスワード設定等の対策を講ずることが必要である。上記以外の対策として、以下の条件を満たしセキュアな環境とすることで、光ファイバーの専用線を用いることも有効である。 －建物内に不正な機器が接続されていないことの確認 －切断検知時の報告の徴求およびその分析	・暗号化 ・パスワード設定 ・光ファイバーの専用線の利用
オープンネットワークや無線を利用した重要なデータの伝送時における盗聴	・通信事業者と協力するなど暗号化対策をはかり、十分な漏洩防止対策を講じておくことが必要である。 ・開発時のドキュメント、ソースコード等もその重要性に配慮した伝送方式を考えること。	・暗号化
無線LANにおける盗聴	・ネットワーク構成機器への未承認機器の論理的・物理的な接続を不可能とする仕組みも有効である。	

対しては、開発の各段階において十分な検証を行うことが必要であると記述されている。

このように、【技 28】、【技 29】では、蓄積データの漏洩および伝送データの漏洩への主な対策としてデータの暗号化を挙げているほか、【技 33】では、伝送データの改ざん検知策として暗号技術の利用を挙げている。こうした暗号技術の安全性に関する記述としては、【技 29】において、「暗号・パスワードの使用にあたっては、信頼のおける適切な技術を選択することが必要である」とあるほか、【技 28】、【技 29】において、「なお、適用する技術は、情報処理の発展とともにその強度が変化することに留意するとともに、その使用にあたっては、複数の方式を適切に組み合わせて使用することが望ましい」とある。これらは、伝送データの改ざん検知策としてメッセージ認証コードや電子署名を利用するうえでも注意すべき事項であると考えられる。電子署名については、【技 35】の参考欄において、「鍵長等による暗号強度（暗号解読の困難性）が変わるなどに留意することが必要である」と記述されている。

暗号アルゴリズムを選択するうえでの参考情報として、【技 28】と【技 29】では、CRYPTRECによる「電子政府推奨暗号リスト」（総務省・経済産業省［2003］）を挙げている。CRYPTRECは、継続的に電子政府推奨暗号リストに掲載されている暗号アルゴリズムの安全性を監視・調査している。暗号技術の安全性評価には高度な専門知識が必要となることから、こうした信頼できる機関による評価結果を参照することが有益であると考えられる。

暗号処理に利用する秘密鍵の運用管理については、【運 43】「暗号鍵[6]の利用において運用管理方法を明確にすること」が準備されており、金融機関には秘密鍵の生成、配付、使用および保管等にかかわる手続きを定めておくことが求められている。また、【技 42】「電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること」では、秘密鍵の保護機能の例として、「ICカードにおける耐タンパー性のような保護機能、ID・パスワード等によるアクセス制限、暗号を用いた蓄積」を挙げており、これらの手段を組み合わせて総合的に対応する必要があると記述している。

データの盗取に対しては、これまでに整理した暗号化のほか、ICカードや端末への耐タンパー性の付与も対策の1つとして挙げられている。「耐タンパー性」については、【技 41】「電子的価値の保護機能、または不正検知の仕組みを設けること」の中で、「こじ開けや不正アクセスなどで情報を無理に取り出そうとした場合に、その情報を消去する等で不正を防止する技術」と説明されている。ここでは、デバイスに対して想定される攻撃の一例として「こじ開けや不正アクセス」が挙げられているが、デバイス内部に格納されているデータを盗取するための手段にはさまざまな方法が存在する。例えば、暗号処理を実行しているデバイスから漏洩する物理

6 「暗号鍵」については「共通鍵暗号方式あるいは公開鍵暗号方式の秘密鍵」と記述されている。

量（消費電力や電磁波等）を測定・解析することによって、暗号処理に利用された秘密鍵を特定するサイドチャネル攻撃もその1つであり、近年その対策技術に関する研究が盛んに行われている。また、FISC安全対策基準では、攻撃への対策の一例として、「その情報を消去する」ことを挙げているが、こうした能動的な対策方法のほかにも、攻撃の証拠を残す、あるいは、攻撃を受動的に防御するといった対策技術も考えられる。耐タンパー性を、「攻撃に対して秘密情報を守秘できる秘密情報守秘性と機能の改変を困難にする機能改変困難性」と定義する場合（日本規格協会［2004］）、その具体的内容は、FISC安全対策基準において例として記述されているように、攻撃と対策方法の組合せで表現されることとなる。したがって、金融機関は、デバイスが利用される環境においてどういった攻撃が想定されるか、また、そうした攻撃に対してどの程度の対策を講じるのが望ましいかを、自らの提供するアプリケーションやデバイスの種類に応じて検討する必要がある。

（3）検討が求められる項目

本節における検討結果から、金融機関がアプリケーションに応じて自ら検討を行うことが求められる項目の一部として次の事項が挙げられる。

・生体認証に関するセキュリティ要件について
  ―「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」（【技 35-1】）との記述から、認証精度の設定と確認をどのように行うかを検討する必要がある。
  ―「不正認証（なりすまし）等の防止」（【技 35-1】）を達成するうえで、例示されている攻撃への具体的な対応を検討する必要がある。また、「最新の技術動向等」を踏まえ、新しい攻撃や対策技術にどのように配慮するかについても検討する必要がある。
・暗号デバイス（ICカード、端末等）の耐タンパー性について
  ― データの盗取への対策の1つとして挙げられている、ICカードへの耐タンパー性の付与（【技 28】、【技 40】等）、および、端末への耐タンパー性の付与（【運 100】）を実現するうえで、アプリケーションに応じてどのような対策技術が有効かについて検討する必要がある。
  ― PIN認証やICカード認証においても、生体認証における「偽ATM（偽センサ機器等）の設置による、生体認証情報の盗取」（【技 35-1】）と同様の攻撃を想定し、どのような対策技術が有効かについて検討する必要がある。

そこで、4節および5節では、これらの検討課題について、既存の標準や技術文書を参考にしながら検討を行う。

4．生体認証における認証精度となりすましへの対策技術

本節では、別途検討が必要となる項目として前節において挙げた「生体認証における認証精度」と「生体認証におけるなりすましへの対策技術」について、既存の国際標準や業界仕様のセキュリティ要件を参照しながら検討を行う。

(1) 認証精度の設定と確認

認証精度の指標としては、誤受入率（FAR: false acceptance rate)、誤拒否率（FRR: false rejection rate)、誤合致率（FMR: false match rate)、誤非合致率（FNMR: false non match rate）が一般的である。こうした認証精度が適切か否かを確認するためには、認証精度の適切なレベルの設定、および、実現されている認証精度の確認を行う必要がある。

イ．適切な認証精度設定

認証精度の設定はアプリケーションに依存するものであり、さまざまな方法が考えられる。それらの1つとして、「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」（以下、運用要件指針。日本工業標準調査会［2004］）に記述されている方法が挙げられる。対象のアプリケーションにおいて許容できるリスクを算出可能な場合に、許容できる誤受入率（permissible false acceptance rate）の算出方法の例が以下のとおり示されている。

許容できる誤受入率＝(許容できるリスク)／(保護対象の価値×不正アクセス頻度
×不正認証阻止失敗率×ID既知率×認証可能回数).

ただし、保護対象の価値は生体認証装置による保護の対象となっているもの（あるいは情報）の価値、不正アクセス頻度は一定期間における不正アクセスの頻度、不正認証阻止失敗率は不正アクセスの阻止に失敗する確率、ID既知率は攻撃対象のユーザのIDが攻撃者によって知られている確率、認証可能回数は攻撃者が一定時間内に実行可能な認証回数と定義される。運用要件指針には、こうした算出方法を銀行ATMにおける生体認証装置に適用する際の例も以下のとおり記述されている（日本工業標準調査会［2004］21頁)。

（例）ある銀行のATMにおいて、毎日平均1,000件のアクセスがあり、1回の不正が成功したとして最大100万円の損害が出るとする。1回の不正に関して10分ほどの不正認証の時間がとれると仮定する。さらに1回の認証（ID入力、生体情報入力、システムの応答）に10秒かかるとする。また、1年間の許容できる損害額を300万円とする。

・最初のゲートにおける不正アクセス頻度の見積り：当該ATMが設置されている場所での犯罪発生確率が1/10,000であったとして、これを採用すると、1年間の不正アクセス頻度は1,000×365／10,000＝36.5となる。
・不正認証阻止失敗率の見積り：誰でも認証装置にアクセスできる設置環境なので1に設定する。
・ID既知率の見積り：IDの入力を盗み見ることができる環境と仮定すると1に設定する。
・認証可能回数の見積り：10分間に何回認証ができるかを計算すると、600／10＝60と見積れる。

以上から、許容できる誤受入率は300万円／（100万円×36.5×1×1×60）＝0.0014＝0.14%となる。

また、運用要件指針では、生体認証におけるリスクの3つのレベル（S、T、U）を設定し、表9のとおり各レベルに応じて許容できる誤受入率の範囲を示している。こうした情報も認証精度設定の際に参考にすることができる。

ロ．認証精度の確認

「適切」とみられる認証精度のレベルを決定したとして、次に、そのレベルが達成されていることを確認する必要がある。生体認証装置を提供するベンダーが実施した精度評価の結果を参照するケースが多いが、評価結果はサンプルや環境条件等によって変動することが知られており、想定されているアプリケーションと整合的な条件のもとで評価が実施されたことを確認することが重要である。そうした確認を行う際の留意事項として、金融向けの生体認証技術に関する国際標準ISO 19092-1（ISO［2006b］）には次の項目が規定されている。

表9　生体認証におけるリスクの3つのレベル

レベル分類	S	T	U
基準	本人認証によるリスクは天文学的に大きい。社会的安全に寄与する。	本人認証によるリスクが大きい。社会的信用にかかわる。	本人認証によるリスクが小さい。利便性が重視され、セキュリティへの要求がない。
許容できる誤受入率の範囲	0.00001～0.0001%	0.0001～0.01%	0.01～1%
アプリケーション例	・造幣局、ICカード発行施設、電子認証局、原子力施設、防衛・警察施設の入退室管理での本人確認	・金庫室、ホームバンキング、ATM、クレジットカードによる取引における本人確認 ・電子カルテ等のデータベースへのアクセス管理における本人確認	・PCログイン、勤怠管理における本人確認 ・不正監視、利用端末管理に用いられる本人確認

備考：日本工業標準調査会［2004］の表4-2を参考に作成したもの。

・評価テストに用いられたサンプルの提供者に関連する項目：
　― 提供者はどのようにして選抜されたか（実際のアプリケーションでの利用者の集団を反映しているか）。
　― 提供者は事前にどのようなトレーニングを受けたか（トレーニングによる習熟度が高いほど結果が良好となる可能性が高くなる）。
　― 生体情報が登録困難である等の問題を有する提供者をどのように排除したか（そうした問題を有する提供者が少ないほど結果が良好となる可能性が高くなる）。
・評価テストに用いられたパラメータに関連する項目：
　― テスト時の判定しきい値がどのような値に設定されていたか。
　― 最終的な認証結果を出力する際に何度生体情報が提示されるように設定されていたか（提示される回数が多いほど結果が良好となる可能性がある）。
　― 他者へのなりすましに関してどのような誘因が付与されていたか（誘因が弱いほど誤受入率の測定結果が良好となる可能性がある）。
・環境条件に関連する項目：
　― テスト時の環境条件は実際のアプリケーションで想定されているものとどのように異なるか。
　― テストは複数の組織によって別々に行われたか（複数の組織によって行われた場合、環境条件がそれぞれ異なっていた可能性がある）。
　― テスト時と意思決定時で当該製品・システムに変更があったか。

また、全銀協仕様では、附属書18において、ICキャッシュカード搭載用生体認証アプリケーションのIDの付与（全銀協による認定）に求められる情報として精度評価結果に関する情報を記述している。ベンダーには、精度測定方法を規定する日本工業標準に準拠するとともに、当該アプリケーションの仕様、照合精度特性（ROC曲線）、精度評価レポートを認定時に提出することが求められている。精度評価レポートには、被験者の構成、習熟度、限界精度（テストによって測定可能な精度の上限）、未対応率を含めなければならないとされており、これらは、ISO 19092-1に記述されている留意事項とほぼ同一となっている。

ベンダーによる認証精度評価のほかに、第三者機関が精度評価のテストを実施するプロジェクトも近年盛んに行われている（情報処理推進機構［2006］、新崎［2006］）。代表的なものとしては、NISTによる指紋認証装置の評価、米国とイタリアの研究機関による指紋認証装置の評価（FVC: Fingerprint Verification Competition）、米国のコンサルティング会社IBG（International Biometric Group）による虹彩や血管パターンの認証装置の評価が挙げられる（表10参照）。これらの評価結果を参照する際にも、上記のISO 19092-1に示されている留意点に配慮することが有用である。

表10　第三者機関による代表的な認証精度評価プロジェクト

推進主体／プロジェクト名	評価実施時期	評価対象のモダリティ	評価対象製品	サンプル数
米NIST（IR 7123）	2003年	指紋	34種類	約400,000
FVC2004	2004年	指紋	67種類	約3,500
IBG（CBT round 6）	2006年	虹彩・血管パターン	3種類	約650（人）

備考：新崎［2006］を参考に作成したもの。関連する情報のURLは以下のとおり。

・NIST: http://fingerprint.nist.gov/

・FVC2004: http://bias.csr.unibo.it/fvc2004/

・IBG: http://www.biometricgroup.com/reports/public/comparative_biometric_testing.html

（2）なりすましへのセキュリティ対策技術

なりすましを目的とする攻撃への対策を整理する方法の1つとして、各種の対策技術が攻撃のどの部分に影響を与えるかを明らかにすることが考えられる。ここでは、1つの攻撃を、攻撃者[7]による複数の行為の時系列的な流れによって完結するシナリオとして捉える。そのうえで、参考文献に記述されているセキュリティ要件や対策技術がシナリオのどの部分に影響を与えるかを考察する。

イ．攻撃シナリオ

（イ）準備フェーズと実行フェーズ

攻撃のシナリオは、攻撃の対象となるシステムにおいて実際に何らかの行為を行ってなりすましを実行するフェーズ（実行フェーズ）と、実行フェーズの準備のフェーズ（準備フェーズ）に分けることができる。現時点で生体認証システムの攻撃シナリオをすべて列挙することは困難であるため、既知の攻撃を包含することに主眼を置くと、準備フェーズと実行フェーズにおける攻撃者の行為として次の7つを挙げることができる（図1参照）。

・準備フェーズ：

― 準備A：センサに提示する情報を得る。

― 準備B：情報を提示する媒体を準備する。

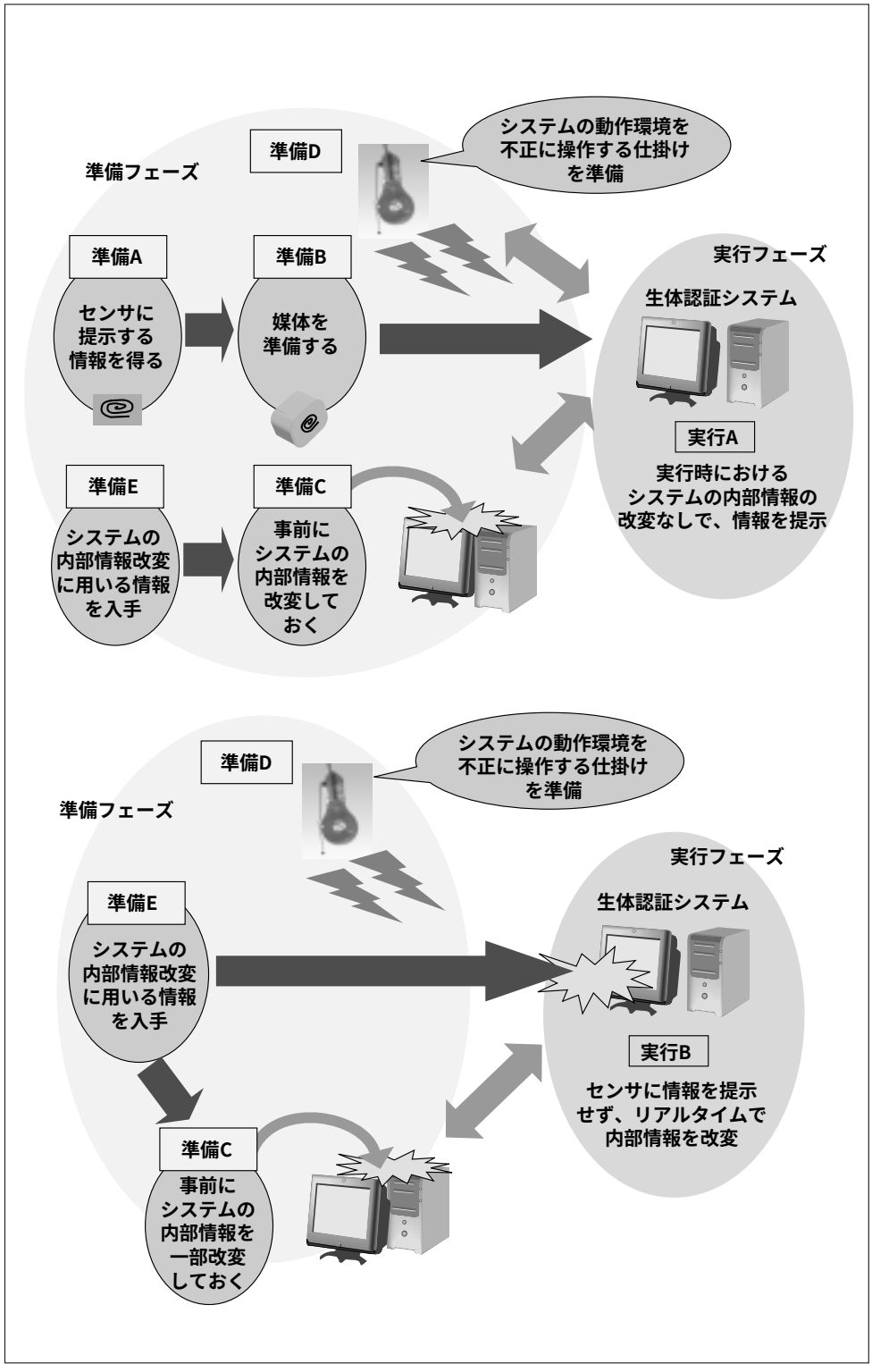
― 準備C：システムの内部情報を事前に改変する。

― 準備D：実行フェーズにおいてシステムの誤受入を誘発するために動作環境を変化させる仕掛けを準備する。

― 準備E：システムの内部情報を改変するために用いるデータを準備する。

7 セキュリティ評価の文脈で「攻撃者」という用語を使用する場合、攻撃首謀者だけでなくその結託者も含めた攻撃者集団を意味するケースが一般的である。本稿でも同様の意味で用いることとする。

図1　なりすましを目的とした主な攻撃のシナリオ



・実行フェーズ：
　― 実行A：システムの内部情報を改変せず、センサに情報を提示する。
　― 実行B：システムの内部情報を改変する。

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、それ以外の情報を入手する場合が想定される。

攻撃対象者の生体特徴を推定する手段としては、システムの内部情報（攻撃対象者の生体情報、テンプレート、判定しきい値、照合・判定処理アルゴリズム等）や外部に出力される情報（判定結果等）からの推定や、攻撃対象者本人からの採取等が考えられる。例えば、「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」という方法（ヒル・クライミング攻撃）が含まれる。

攻撃対象者の生体特徴以外の情報としては、例えば、既存の攻撃例を参考にすると、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（ウルフ[8]）が挙げられる。前者は、「攻撃者が自分の生体特徴を提示してなりすましを試みる」というゼロ・エフォート攻撃（zero-effort attack）に、後者はウルフ攻撃（宇根・大塚・今井［2007］、Une, Otsuka, and Imai［2007］）にそれぞれ用いられることになる。

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。後者の例としては、攻撃対象者から分離された身体部分や、攻撃者本人の身体部分が想定される[9]。

準備Cにおけるシステムの内部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ものが想定される。判定処理を行うプログラムを改変しておき、どのような生体情報に対しても「一致」との判定結果を出力するようにしておくものも準備Cに含まれる。また、実行Bを実行しやすくするために、事前に準備Cによって攻撃対象のシステムの内部情報を一部改変しておくというケースも考えられる。

準備Dは、生体認証システム、とりわけ、生体情報を取得するセンサが環境条件の変化に敏感であり、誤受入率が高くなってしまう可能性を有してい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波長の光と類似の光を照射することによって生体情報の品質を変化させ、誤一致を引き起こしやすくさせるといったことが想定される。

8 ウルフに対する脆弱性は、生体認証システムのセキュリティ評価の枠組みを規定する国際標準案ISO/IEC CD 19792においても規定されている（ISO and IEC［2006］）。ISO/IEC CD 19792において、ウルフは、多くのテンプレートと誤一致を引き起こす生体情報と定義されている。

9 準備Aと準備Bは、それぞれ個別に実現可能性を評価する試み（例：準備Aはウルフ攻撃確率、準備B：テスト物体アプローチ）が行われており、各種対策の有効性を検討することを考えると、独立に位置付ける方がよいと考えられる。

準備Eは、準備Cや実行Bの前処理となる。例えば、過去の認証時に使われた生体情報やテンプレートを入手する、ウルフとなる生体情報やテンプレートを準備するといったものが想定される。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、システムの内部構造に関する情報を入手するという行為も本準備に含まれる。

次に、攻撃を実行する際の攻撃者の行為であるが、認証時にシステムの内部情報を改変するという実行Bと、そうした改変は行わず、生体特徴等の情報をセンサに提示するという実行Aが考えられる。このうち、攻撃シナリオ5における実行Bは、認証処理中にシステム内部の情報を改変するという行為を意味し、その手段は形式的には準備Cと同一となると考えられる。

（ロ）各準備・実行の組合せ

準備A～Eと実行A、Bの関係を整理する。攻撃者が実行Aを選択する場合、センサに何らかの情報を提示するために準備Aと準備Bは必須となる。また、これらと準備Cや準備Dを組み合わせるケースも考えられる。準備Cを実行する場合には準備Eも行う必要がある。すなわち、まず攻撃シナリオとして次の4つが挙げられる。

・攻撃シナリオ1：準備A、B→実行A
・攻撃シナリオ2：準備A、B、C、E→実行A
・攻撃シナリオ3：準備A、B、D→実行A
・攻撃シナリオ4：準備A、B、C、D、E→実行A

次に、実行Bを選択する場合、攻撃者は準備Eを実行することが必須となる。そのうえで、準備C、Dを併用するケースも考えられるため、次の4つの攻撃シナリオを挙げることができる。

・攻撃シナリオ5：準備E→実行B
・攻撃シナリオ6：準備C、E→実行B
・攻撃シナリオ7：準備D、E→実行B
・攻撃シナリオ8：準備C、D、E→実行B

これらの攻撃シナリオを銀行店舗内ATMのように比較的管理の行き届いたケースに適用してみると、システムの改変（準備C、実行B）を行ったり、運用環境を変化させるような仕掛けを準備したり（準備D）することは相対的に困難であると考えられる。すなわち、管理・運用に適切な対策が講じられていれば、攻撃シナリオ1以外のものは実行が容易でなく、準備A、Bや実行Aにどのように対応するかという点に検討の重点を置くことになる。一方、直接的な管理がより困難なアプリケーションにおいては、考慮すべき攻撃シナリオが増えてくることになる。

また、実行Aと実行Bを組み合わせる攻撃シナリオも考えられる。そうした攻撃

シナリオは、上記の攻撃シナリオを組み合わせることによって表現することができる。セキュリティ対策としては、攻撃シナリオ1～8への対策を実施することによって対応することができると考えられるため、ここでは触れない。

ロ．3つの文献

FISC安全対策基準以外の金融向け生体認証システムのセキュリティ要件に関する代表的な文献として次の3つを取り上げる。

- ISO 19092-1, “Financial services - Biometrics - Security framework”（ISO［2006b］）
- 全銀協仕様
- 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」（以下、NMDA報告書。ニューメディア開発協会［2005］）

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基本的な構成、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、ICカードとATM間の通信方式、および、ATM内部での処理方法を規定しており、ICカード内にテンプレートを保管したうえで、銀行店舗のATM等において、同ICカード内部でテンプレートと入力された生体情報から得られる特徴データの照合・判定を行い、その結果をサーバに送信するというタイプを想定している。さらに、こうした処理に関連するセキュリティ要件の一部が記述されている[10]。

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セキュリティや相互運用性等に関する要件の導出を主な内容としている。本報告書では、全銀協仕様と同様に生体情報をICカード（トークン）内部に格納してATM内で照合・判定を行うケースと、生体情報の保管・照合・判定をすべて銀行のサーバで行うケースの2通りが想定されている。

このように、全銀協仕様とNMDA報告書は具体的な認証形態を想定している。これらは、いずれもATMや銀行窓口での認証実行を想定しており、金融機関の管理が行き届いているという状況を前提としているといえる。一方、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。ただし、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。

10 全銀協仕様の記述は、わが国の金融機関がICキャッシュカードの互換性を確保するうえで準拠することが求められており、他の文献のセキュリティ要件に比べて充足させることが実質的に必要とされているという点で意味合いが異なっている。ただし、生体認証用のデータ・フォーマットに関してISO/IEC 7816-11を参照しつつも、その他の部分については基本的には金融機関に検討を委ねる形となっており、金融機関が自ら決定可能な部分も少なくない。

ハ．3つの文献のセキュリティ要件

上記の文献に記述されているセキュリティ要件のうち、主として技術的対策に関するものを整理すると表11のとおりである。これらの要件について、FISC安全対策基準のセキュリティ要件とも比較しながら考察を行う。

①準備Aについて

システム内部の情報の盗取に対しては、暗号化、耐タンパー性の付与、インターフェース等の物理的保護、生体情報のシステム内での残留防止、データベースやサーバへの適切なアクセス制御の実施をセキュリティ要件として挙げている。偽の装置による攻撃者本人からの生体情報の盗取に対しては、警備員やカメラによる監視を要件としている。また、テンプレートからの生体情報の推定に対しては、キャンセラブル・バイオメトリクスの適用の検討が推奨されている。これらの他に、ヒル・クライミング攻撃への対策手段として、離散値による類似度の表示が挙げられている。

これらのうち、次節で詳しく検討する耐タンパー性に関しては、ISO 19092-1において、物理的な改変を伴う攻撃の痕跡を残すとともに、内部情報を消去する機能を実装することが要件となっている。

類似した生体情報を有する個人やウルフ攻撃に関しては、最近詳しい研究成果が発表されたという事情もあり、FISC安全対策基準と同様に触れられていない。

②準備Bについて

いずれの文献においても準備Bに対するセキュリティ要件が記述されていない。これは、準備Aで得られた情報を提示する媒体の準備を防止することが原理的に困難であるという事情によるものと考えられる。

③準備Cについて

テンプレート、判定しきい値、判定処理プログラム等の改変が想定されており、セキュリティ要件として、各種データの一貫性確認（電子署名等の暗号技術の採用）、システムへの耐タンパー性の付与、インターフェース等の物理的保護、モジュール間の相互認証機能の付与が挙げられている。また、不正なキャリブレーションへの運用面での対応として、適切に設定されたFAR等の実現に必要なポリシーの設定、誤り率を検証するためのログの管理が挙げられている。

④準備Dについて

要件として、FARの変動の検知、一定範囲の環境変化を想定した動作確認のテストの実施といった項目が含まれている。FISC安全対策基準の「防犯カメラによる監視」がいずれの文献にも含まれていないが、ATM等の運用環境ではこうした監視は通常行われており、その意味であえて要件として記述していないとも考えられる。ただし、リモートでの生体認証システムの使用を想定した場合、FARの変動検知等の対応が求められる。

表11　3つの文献に記述されているセキュリティ要件

準備／実行	ISO 19092-1	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盗取に対する要件】 ・テンプレートや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が漏れる可能性がある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、痕跡が装置に残るとともに、攻撃を検知し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】 ・偽の装置での生体情報盗取を防ぐために警備員やビデオカメラで監視する。 【ヒル・クライミング攻撃に対する要件】 ・テンプレートと入力された情報の類似度の表示が必要な場合は離散値で行う。	【システム内部の情報盗取に対する要件】 ・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し、格納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は、十分に安全な管理のもとで運用するか、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C	【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暗号技術で確認する。 ・インターフェース、ケーブルを物理的に保護する。 ・装置の物理的改変を伴う攻撃に対し、その痕跡が装置に残るとともに、攻撃を検知し、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で確認する。 ・不適切なキャリブレーションに対して、適切に設定されたFARとFRRの実現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。	（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	・環境条件の変化でFARが許容レベルを超える事象を検知する。 ・一定範囲の環境変化における安定動作の確認のために、適切なテストを行う。	・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。	・準備Aに対する要件が該当する。
実行A	【ゼロ・エフォート攻撃に対する要件】 ・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。	【ゼロ・エフォート攻撃に対する要件】 ・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、不一致となった回数をカウントし、上限値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、身体的特報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。	・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】 ・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・データ等）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セキュリティ機能の保証などがある。

⑤準備Eについて

本準備に対する要件は準備Aに対する要件が該当すると考えられる。

⑥実行Aについて

FISC安全対策基準と同様に、ゼロ・エフォート攻撃と人工物によって生体特徴を提示する攻撃が想定されている。ゼロ・エフォート攻撃への要件としては、認証精度の適切な設定、一定回数の認証失敗に対する認証機能提供停止が挙げられている。認証機能提供停止については、一般の生体認証システムで既に実現されているケースが多い。人工物によって情報を提示する攻撃に対する要件としては、生体検知機能の利用、人間やカメラによる監視が挙げられている。

⑦実行Bについて

本実行に対する要件は準備Cに対する要件が該当すると考えられる。NMDA報告書では、リプレイ攻撃を想定した対策の要件が記述されているが、その内容をみると基本的には耐タンパー性の付与となっており、耐タンパー性の付与を含む準備Cに対する要件によってカバーされると考えられる。

ニ．小括

本節では、既知の攻撃を前提に8つの攻撃シナリオを整理し、シナリオを構成する各要素に対してどのようなセキュリティ要件や対策技術が挙げられているかを、3つの文献を参照しながら検討した。各攻撃シナリオへの対策技術としては、生体検知手法やキャンセラブル・バイオメトリクス等、さまざまな技術が挙げられていることがわかった。しかし、それらの中にはセキュリティ対策としての効果を定量的に評価することが困難なものも少なくない。

例えば、生体検知手法のセキュリティ評価の方法が確立していない（宇根・田村[2005]）ほか、キャンセラブル・バイオメトリクスについては、現時点での実用化は困難との見方が一般的となっている。ウルフ攻撃への対策技術については、ウルフ攻撃がごく最近提案されたということもあって、どのような対策が効果的かについての研究がこれから本格化するという段階にある。また、FARの変動の検知といった対策については、環境条件の変化が認証精度にどのような影響を及ぼすかに関してセキュリティの観点からほとんど議論されていないのが実情であり、そうした対策の効果を評価するまでには至っていない。

もちろん、技術的な対策手段でカバーできない部分は運用でカバーするという考え方もある。実際に、本節で整理したセキュリティ要件に付随して記述されている対策手段にも運用的な手法（防犯カメラによる監視等）が取り入れられている。しかし、金融機関による直接的な管理が比較的困難なアプリケーションの場合、そうした運用による対応は困難なケースも考えられる。

このように現時点では課題が山積しているのが実情であるものの、生体認証システムのセキュリティに関する研究・開発は今後一層進展していくことが見込まれ

る。生体認証システムの今後の活用を検討する際には、生体認証システムのセキュリティ評価の現状をフォローし、どこまで評価が可能になっているのかをベンダーやSI事業者に確認しながら慎重に見極めることが必要である。

ただし、評価が困難な対策技術を採用せざるを得ない状況のもとで生体認証システムを利用しなければならないケースにおいては、各攻撃シナリオにおいてどれか1つの要素に着目して1つの対策技術のみを採用するのではなく、少なくとも、複数の対策技術を組み合わせて対応することが求められると考えられる。また、安心して利用できる金融サービスの提供を目指すという観点からは、生体検知機能等、対策技術の評価手法を早期に確立することが求められる。こうした問題意識を踏まえ、生体認証システムのユーザとして、ベンダーやSI事業者に対して評価手法の確立に向けた取組みを一段と加速させるように働きかけることが必要ではないかと考えられる。

5．暗号デバイスの耐タンパー性

本節では、別途検討が必要となる項目として3節において挙げた「暗号デバイスの耐タンパー性」について、既存の国際標準や業界仕様に記述されているセキュリティ要件を参照しながら検討を行う。

(1) 暗号デバイスに対して想定する攻撃

ICカードや端末といった暗号デバイスの攻撃に対する耐性については、まず、暗号デバイスに対して想定される攻撃を明確にしたうえで、各攻撃に対してどの程度の耐性を付与させるかということを決定する必要がある。

そこで、暗号デバイスに対して想定される攻撃を、ISO 13491-1を参照して整理すると、以下の攻撃①～⑦にまとめることができる。ただし、ISO 13491-1で「改ざん」として記述されているものを攻撃⑤と⑥の2つに分けたほか、ISO 13491-1には記述されていないが後述する他の標準等で想定されている攻撃として攻撃④を加えた。

- 攻撃①［デバイスへの侵入］：物理的な改変を加えてデバイス内部に侵入し、秘密情報を盗取する。
- 攻撃②［サイドチャネル攻撃］：デバイスから漏洩する物理量や当該デバイスへの入力情報を観測し、秘密情報を推測する。
- 攻撃③［デバイスの不正操作］：デバイスに不正な入力を与えることによって秘密情報を推定するための手掛かりを得る。
- 攻撃④［規格外環境での操作］：デバイスが動作する環境を変化させることによって秘密情報を推測するための手掛かりを得る。

・攻撃⑤［デバイスの物理的改ざん］：デバイスに物理的な変更を加え、当該デバイスを不正に動作させる。不正なハードウエアのインストールもこれに含まれる。
・攻撃⑥［デバイスの論理的改ざん］：デバイスに論理的な改変を加え、当該デバイスを不正に動作させる。不正なソフトウエアのインストールもこれに含まれる。
・攻撃⑦［デバイスの置換］：デバイスを別のデバイス（偽造したものを含む）に置き換える。攻撃①～⑥の実行のため、真正なデバイスを移動させることを目的とするものであり、その間、真正なデバイスが存在した位置に別のデバイスを配置するものを含む。

（2）暗号デバイスのセキュリティ特性

暗号デバイスのセキュリティ特性についても、ISO 13491-1を参照することができる。本標準が対象とする暗号デバイスについては、PINパッド等が例として挙げられているほか、ATMやPOS端末等に一体化されるものと記述されている。

ISO 13491-1では、暗号デバイスに対する攻撃に対抗するには、デバイス特性、デバイス管理、環境の3つの観点からの対策が必要であり、特にデバイス特性については、物理的および論理的なセキュリティ特性の付与が必要であると記述されている。その中でも、暗号デバイスの物理的なセキュリティ特性については、タンパー・エビデンス特性、タンパー・レジスタンス特性、タンパー・レスポンス特性の3つのクラスに分類し、各特性を以下のように整理している。

イ．タンパー・エビデンス特性

タンパー・エビデンス特性とは、攻撃が試行されたことを物理的に証拠として残すことを目的とする性質であり、以下の必要条件を満たすものである。

・暗号デバイスの偽造等による置換を防御するため、入手が容易な部品を利用してデバイスの複製を作製することが現実的でないこと。
・暗号デバイスの改ざんには、物理的なダメージや、長い時間が必要となること。

ロ．タンパー・レジスタンス特性

タンパー・レジスタンス特性とは、攻撃を受動的に防御することを目的とする性質であり、以下の必要条件を満たすものである。

・暗号デバイスは侵入に対する受動的耐性を有すること。
・暗号デバイス内部に格納される機密データの改ざんや盗聴装置の設置が不可能であること。
・暗号デバイスから漏洩する電磁波の観察によって、内部に格納される機密デー

タが漏洩しないよう、電磁波が放射することを物理的に防ぐこと。
・観察を防御することのできない暗号デバイスの部品内に機密データの格納や転送をしないこと。
・暗号デバイスに入力された機密データを他人に覗き見されないよう、物理的に遮蔽すること。
・暗号デバイスの不正な移動が困難であること。

ハ．タンパー・レスポンス特性

タンパー・レスポンス特性は、攻撃を能動的に防御することを目的とする性質であり、以下の必要条件を満たすものである。

・暗号デバイス内部への侵入や不正な改ざんに対しては、内部の機密データを速やかにかつ自動的に消去すること。
・暗号デバイスの安全性が動作環境に依存する場合、当該デバイスの不正な移動を検知して、内部の機密データを速やかにかつ自動的に消去すること。

FISC安全対策基準では、耐タンパー性を「こじ開けや不正アクセスなどで情報を無理に取り出そうとした場合に、その情報を消去する等で不正を防止する技術」と記述している。ここでの「こじ開けや不正アクセス」は攻撃①～⑦のいずれによっても実行されうると考えられる。したがって、FISC安全対策基準における耐タンパー性は、主に攻撃①～⑦に対してタンパー・レスポンス特性を示すものと考えられる。

(3) 暗号デバイスのセキュリティ要件

以下では、既存の国際・業界標準や技術仕様を参照して、ICカードおよび端末に関するセキュリティ要件を整理する。FISC安全対策基準では、PINパッドやカード・リーダが端末と一体化しているケースが想定されているようであり、セキュリティ要件についてもそうした形態の端末を対象としたもののみが準備されている。ただし、デビットカード端末やPOS端末を利用した取引、あるいは、インターネット・バンキングを想定した場合には、PINパッドやカード・リーダが端末と独立したデバイスとして存在することが想定されることから、これらのデバイスに関するセキュリティ要件についても別途整理することとする。

イ．ICカードに関するセキュリティ要件

ICカードに関するセキュリティ要件については、ICカードに関する代表的なセキュリティ要求仕様書（PP: protection profile）である、SCSUG-SCPP（SCSUG［2001］）やBSI-PP-0002（EUROSMART［2001］）を参照することができる。いずれのPPにおいても、その機能強度（strength of function）は高位に設定されて

いる[11]。SCSUG-SCPPは、VISA等のクレジットカード会社が中心となって作成されたものであり、クレジットカード取引をはじめとする金融用途を意識したPPとなっている。一方、BSI-PP-0002は、欧州のカード・メーカが中心となって作成されたPPであり、必ずしも金融用途に限定したものとはなっていない。

ICカードに対して想定される攻撃は、本節(1)で定義した攻撃①～⑥であり、各仕様で想定されている攻撃、および、それらに対する主なセキュリティ要件については、表12のように整理できる。

SCSUG-SCPPでは、攻撃①、②、④、⑤に対して、ICカードが攻撃を検知して自動的に反応することで攻撃を防御すること（以下、自動的反応）が記述されているが、具体的な動作については明記されていない。コモン・クライテリアでは、こうした自動的反応の例として、保護された情報が読み出せないようデバイスの処理を停止させることが挙げられており、SCSUG-SCPPにおいてもこうしたタンパー・レスポンス特性が想定されているものと考えられる。

また、BSI-PP-0002も、攻撃①、⑤に対して自動的に反応することをセキュリティ要件としているが、SCSUG-SCPPにおける自動的反応とは意味合いが異なっている。すなわち、ICカードに電源が供給されていない状況で攻撃が行われたとしても、攻撃への防御を可能とする機能を有するものを自動的反応と呼んでいる。こうした特性は、タンパー・レジスタンス特性を示すと考えられる。

これらのPPでは、想定する攻撃への直接的な対抗策となるセキュリティ要件がコモン・クライテリアにないこと等から、攻撃に対してどのような機能で対抗するかといった具体的な要件を設定していないものもある。対抗するための機能をデバイス特性によって実現しようとする場合には、どういった対策技術の適用が可能か、別途検討が必要である。

また、これらのPPでは、攻撃⑦が想定されていないが、攻撃者がカード所持者のICカードを偽のICカードに置き換えた後、攻撃①～⑥を実行することを想定すれば、攻撃⑦に対するタンパー・エビデンス特性の付与によって、攻撃①～⑥を防止することが考えられる。例えば、ICカードのタンパー・エビデンス特性によってICカードが偽のカードに置き換えられたことをカード所持者が検知し、金融機関によってその事実が把握され、当該カードを速やかに無効化するといった方法も考えられる。

もっとも、本人認証システムで利用されるICカードは、当該カード所持者によって管理されることから、金融機関自らでICカードへの攻撃を検知することは困難である。そのため、ICカードに対しては、運用面での対策に限界があることから技術面での対策がより重要となる。こうした金融機関の管理外での利用が想定される場

11 機能強度は、PPにおける評価対象のセキュリティ機能が、どの程度の攻撃に対して耐性を持つかをレベル付けしたものであり、基本（SOF-basic）、中位（SOF-midium）、高位（SOF-high）に分類される。なお、高位については、高い攻撃能力を有する攻撃者を想定した場合においても、そのセキュリティ機能が十分な抵抗力を備えていると認められるレベルを示す。

表12　攻撃①～⑥に対応する攻撃手段とそれらに対する主なセキュリティ要件

攻撃手段	標準・仕様名	
	SCSUG-SCPP	BSI-PP-0002
攻撃① デバイスへの侵入	・プロービング：ICカードへのプロービングによって、設計情報（機密データ等を含む）や処理内容を露呈させる。 ・自動的反応により防御すること。	・プロービング：ICカードへのプロービングによって、機密データ等を盗取する。 ・常に攻撃の存在を仮定するとともに、対策手法を提供することによって防御すること。
攻撃② サイドチャネル攻撃	・情報の漏洩：ICカードから漏洩する電磁波の放射、消費電力の変化量、入出力特性、クロック数、処理時間の変化量を利用して、機密データを露呈させる。 ・自動的反応により防御すること。	・情報の漏洩：電力、クロック、入出力ライン等の信号の形状や振幅を計測・分析する、あるいは、計測した信号から割り出したイベント間の時間を計測・分析することで、機密データを露呈させる。 ・アクセス制御や情報フロー制御によって、物理的に分離されたパーツ間で通信されるデータの漏洩を防止すること。
攻撃③ デバイスの不正操作	・強制リセット：処理を不適切に終了させることによって、ICカードの処理内容を変更させる。 ・リプレイ攻撃：過去に認証に利用されたデータを繰り返し利用することによって、ICカードの処理内容を変更させる。 ・以前に利用したいかなる情報も利用させないこと。 ・ユーザ認証を行うこと。 ・認証の間は､ユーザに何もフィードバックしないこと。 ・リプレイ攻撃を検知すること。	・機能の悪用：ICカードの出荷後には使用しない機能を利用することによって、機密データの盗取・操作等を行う。 ・機密データの盗取・操作ができないこと。
攻撃④ 規格外環境での操作	・規格外環境での操作：温度、電圧、クロック数等を変化させる等の規格外の環境状態にさらすことにより、エラーを引き起こす。 ・自動的反応により防御すること。	・規格外環境での操作：温度、電圧、クロック数等を変化させる等の規格外の環境状態にさらすことにより、セキュリティ機能を非活性化・改ざんする。 ・故障が発生するような環境にさらされた場合においても、セキュアな状態を維持すること。
攻撃⑤ デバイスの物理的改ざん	・物理的改変：設計情報（機密データ等を含む）や処理内容を露呈させる、あるいは、機密データやセキュリティ機能を改変させる。 ・自動的反応により防御すること。	・物理的操作：ICカードを物理的に改ざんする。 ・常に攻撃の存在を仮定するとともに、対策手法を提供することによって防御すること。
攻撃⑥ デバイスの論理的改ざん	・不正プログラムの読込み：不正プログラムを利用することによって、ICカードの処理内容を変更させる。 ・ユーザ認証およびユーザ識別を実行すること。	・プロービング：ICカードへのプロービングによって、ソフトウエアを改ざんする。 ・機能の悪用：ICカードの出荷後には使用しない機能を利用することによって、セキュリティ機能やソフトウエアの操作等を行う。 ・常に攻撃の存在を仮定するとともに、対策手法を提供することによって防御すること。 ・ソフトウエアの再インストール、セキュリティ機能に関する重要性の低い情報の収集ができないこと。

備考：各攻撃に関する記述欄において、実線上部は具体的な攻撃手法を示し、同下部はそれに対する主なセキュリティ要件を示す。

合においては、多くのタイプの攻撃を想定したうえで比較的高いセキュリティ・レベルを確保する必要があると考えられることから、本節で調査対象とした機能強度が高位に設定されているPPを参考にすることが適切であると考えられる。

ロ．端末に関するセキュリティ要件

端末に関するセキュリティ要件を導出するうえで参照することのできる国際標準・業界仕様としては、まず、ISO 13491、EMV、ISO 9564[12]が挙げられる。そのほか、セキュリティ要件仕様書としては、金融向けPIN認証装置を対象とするAPACSによるPP（APACS［2003］）とCD・ATMを対象とするPP 9907（BULL *et al.*［1999］）が挙げられるほか、全銀協仕様を参照することができる。これらの標準・仕様において想定されている端末の形態をまとめると表13のとおりである。なお、ISO 13491は、単体の暗号デバイス一般に関するセキュリティ要件を記述するものであることから、表13には加えていない。

まず、各標準・仕様から端末に対する攻撃として想定されているものを整理すると表14のとおりである。ISO 13491では攻撃①～⑦、EMVでは攻撃①、⑤～⑦、ISO 9564では攻撃①、③、⑤、⑥、APACSによるPPでは攻撃①～⑥、PP 9907では攻撃①、⑤、⑥、全銀協仕様では攻撃①、③、⑤、⑥に対応するとみられる攻撃が想定されている。さらに攻撃①～⑦に対して、各標準・仕様が記述しているセキュリティ要件を整理すると、表15のとおりとなる。

表13　想定されているアプリケーションの形態とICカード、PIN認証の形態

標準・仕様名	端末の形態
EMV	カード・リーダは端末と一体化
ISO 9564	端末の形態としては以下の4つが挙げられる。 1. PINパッドは端末と一体化 2. PINパッドは端末と分離 3. PINパッドはカード・リーダと一体化 4. PINパッドはカード・リーダと分離
APACSによるPP	PIN認証装置（PINパッド、カード・リーダ、端末で構成されるデバイス）としては以下の5つが挙げられる。 1. PINパッドはカード・リーダと一体化 2. カード・リーダは端末と一体化 3. PINパッドは端末と一体化 4. すべてが一体化 5. 上記1～4以外
PP 9907	端末（CD・ATM）は、PINパッド、カード・リーダが1つのハードウエアに格納された形態。
全銀協仕様	——

12 ISO 9564での端末に対するセキュリティ要件は、PINパッドと一体化して端末が構成される場合に求められるものである。

表14　端末に対して想定されている攻撃

攻撃手段	ISO 13491	EMV	ISO 9564	APACSによるPP	PP 9907	全銀協仕様
攻撃① デバイスへの侵入	・侵入：物理的な改変を加えて暗号デバイス内に侵入し、秘密情報を盗取する。	・測定：機密データを測定する。	・侵入（ISO 13491に準拠）	・侵入：動的な働きかけ（例えば、デバイスに穴をあける、デバイスを開放する）によって、その処理内容を露呈させる。 ・観察：受動的な手段（例えば、デバイス内部を直接観察する）によって、内部構造や処理内容を露呈させる。	・物理的攻撃：CD・ATM内に格納されている鍵を盗取する。	・筐体の開放
攻撃② サイドチャネル攻撃	・観測：暗号デバイスから漏洩する物理量（消費電力、電磁波等）や当該デバイスへの入力情報を観測し、秘密情報を推定する。	——	——	・観察：受動的な手段（例えば、デバイス内部を直接観察する）によって、内部構造や処理内容を露呈させる。	——	——
攻撃③ デバイスの不正操作	・操作：暗号デバイスに任意の入力を与える、あるいは、当該デバイスが動作する環境を変化させることによって秘密情報を推定するための手掛かりを得る。	——	・操作(ISO 13491に準拠)	・操作：サービスやデバイス内に保護されている情報に不正にアクセスする。	——	・筐体の開放 ・アプリケーションへの侵入
攻撃④ 規格外環境での操作		——	——	・規格外環境での操作：環境上のストレスにさらす（例えば、温度や電圧や放射する電磁波を変化させる）ことによって、保護されている情報の盗取や改ざんを行う。	——	——
攻撃⑤ デバイスの物理的改ざん	・改ざん：暗号デバイスに物理的あるいは論理的な変更を加え、当該デバイスを不正に動作させる。	・ハードウエアを追加・置換・改ざんする。	・盗聴装置の設置	・PIN盗聴装置の設置 ・動的な働きかけ（例えば、デバイスに穴をあける、デバイスを開放する）によって、想定外の動作をさせる。	・ハードウエアのインストール：ICカードやPINを盗取するための装置を設置する。	・筐体の開放
攻撃⑥ デバイスの論理的改ざん		・ソフトウエアを追加・置換・改ざんする。機密データを改ざんする。	・内部オペレーションを改ざんする。	・改ざん：デバイス内部に格納される情報を不正に改ざんする、あるいは、サービス内容を不正に変更する。	・ソフトウエアのインストール：不正なソフトウエアをインストールすることで、PINの盗取、周辺機器との通信データの改ざん等を行う。	・筐体の開放 ・セキュリティ関連情報の不正操作（登録・変更・削除）
攻撃⑦ デバイスの置換	・置換：暗号デバイスを別のデバイス（偽造したものも含む）に置き換える。	・類似デバイスを作製する。	——	——	——	——

表15　端末におけるセキュリティ要件

攻撃手段	ISO 13491	EMV	ISO 9564	APACSによるPP	PP 9907	全銀協仕様
攻撃① デバイスへの侵入	・受動的耐性を有すること。 ・内部の機密データを速やかにかつ自動的に消去すること。	・攻撃に対して内部の機密データを速やかに消去すること。	・速やかにかつ自動的に内部に格納される機密データが消去されること。	・物理的攻撃の実行の有無を判断可能であること。 ・自動的反応で機密データに関する情報を消去すること。 ・データの漏洩や改ざんを防御すること。	・自動的反応によって、攻撃を防御すること。	・筐体の一体化、施錠を行うこと。 ・筐体の開放部をシール等により封印すること。 ・筐体の開放時に、可視または可聴で警告を促す、および、内部の機密情報やプログラムを消去すること。
攻撃② サイドチャネル攻撃	・電磁波の放射を物理的に防ぐこと。 ・観察を防御困難な暗号デバイスの部品内に機密データの格納や転送をしないこと。	——	——	・漏洩電磁波の解析によって鍵が推測されないこと。	——	——
攻撃③ デバイスの不正操作	（対応するセキュリティ要件の記述なし）	——	・機密データが漏洩しないこと。	（情報フローの制御を行うこと）	——	・筐体の開放については、攻撃①に対するセキュリティ要件と同様。 ・アルゴリズムおよび鍵／証明書等のセキュリティ情報を格納する物理的・論理的に安全なモジュールとしてSAMを端末内に組み込む。（例：SAMとしてICチップを利用）
攻撃④ 規格外環境での操作		——	——	・攻撃を検知可能であること。 ・自動的反応によって攻撃や許容範囲外の物理的操作を防御すること。	——	——
攻撃⑤ デバイスの物理的改ざん	・物理的なダメージや、長い時間が必要となること。 ・内部の機密データの改ざんや盗聴装置の設置が不可能であること。 ・内部の機密データを速やかにかつ自動的に消去すること。	・特別な技術や一般に入手困難な機器が必要となるほか、デバイスに攻撃の検知を可能とする痕跡が残ること。	・盗聴装置が設置されていないことを保証すること。	・物理的攻撃の実行の有無を判断可能であること。 ・自動的反応で機密データに関する情報を消去すること。 ・PIN盗聴装置の設置を検知や自動的反応で防御すること。	——	——
攻撃⑥ デバイスの論理的改ざん			・内部での処理内容の一貫性を保証すること。	・認証されたユーザはセキュリティ機能の一貫性を検証可能であること。	・ダウンロードしたソフトウエアの一貫性を確認できること。	・筐体の開放については、攻撃①に対するセキュリティ要件と同様。 ・暗証番号の入力、認証カード等により操作者の本人確認を実行する。
攻撃⑦ デバイスの置換	・入手容易な部品によるデバイスの複製が困難であること。 ・不正な移動が困難であること。 ・移動を検知し、内部の機密データを速やかに自動消去すること。	・一般に入手可能な部品から類似のデバイスを作製困難であること。	——	——	——	——

まず、攻撃①に対しては、攻撃を検知したうえで、内部の機密データを自動的に消去するといった、端末にタンパー・レスポンス特性を付与することをセキュリティ要件としているものが多い。

一方、攻撃②のサイドチャネルを攻撃手段として設定しているのは、ISO 13491とAPACSによるPPのみであり、物理的に電磁波の放射を防ぐこと、あるいは、放射した電磁波の解析によって鍵が推測されないことといった、タンパー・レジスタンス特性をセキュリティ要件として記述している。

攻撃③のデバイスの不正操作については、ISO 9564、APACSによるPP、全銀協仕様にセキュリティ要件が記述されている。APACSによるPPでは、不正操作を防止するためユーザ認証を実行することをセキュリティ要件としているのに対し、ISO 9564では不正操作による機密データの漏洩を防止するための具体的技術については記述されていない。また、全銀協仕様においては、物理的・論理的に安全なモジュールとしてSAM（secure application module）を端末内に組み込むことをセキュリティ要件の例として挙げている。

攻撃④の規格外環境での操作に対するセキュリティ要件はAPACSによるPPに記述されており、タンパー・レスポンス特性を端末に付与することが要件とされている。

攻撃⑤のデバイスの物理的改ざんについては、タンパー・エビデンス特性を付与することをセキュリティ要件としている標準・仕様が多い。そのほか、ISO 13491においては、タンパー・レスポンス特性による対策が記述されているほか、APACSによるPPにおいても、PIN盗聴装置の設置を検知あるいは自動的反応によって防御することがセキュリティ要件として記述されている。ただし、自動的反応としてどのような動作を想定しているかについては明記されていない。また、FISC安全対策基準で想定されている脅威のうち、偽センサ機器等の設置や不正なカード・リーダの設置は、ここでの攻撃⑤に相当すると考えられる。

攻撃⑥のデバイスの論理的改ざんに対するセキュリティ要件としては、ISO 13491とEMVにおいてタンパー・エビデンス特性の付与が挙げられている。APACSによるPPやPP 9907においても、ソフトウエアが改ざんされていないことの確認手段を提供することをセキュリティ要件として挙げていることから、タンパー・エビデンス特性を示すものと考えられる。ISO 9564におけるセキュリティ要件である、内部での処理内容が改ざんされていないことを保証することについても、タンパー・エビデンス特性を示すものと読み取ることができる。一方、ISO 13491では、タンパー・レスポンス特性の付与がセキュリティ要件となっているが、デバイスの物理的改ざん（攻撃⑤）と論理的改ざん（攻撃⑥）を1種類の攻撃として扱っていることから、タンパー・レスポンス特性の付与がデバイスの論理的改ざんへの対策として記述されているか否かは明確ではない。FISC安全対策基準において想定されている、コンピュータウイルスの侵入や不正アクセスによるプログラムの改ざんは、攻撃⑥に相当すると考えられる。

攻撃⑦のデバイスの置換については、ISO 13491とEMVのいずれも、偽端末の作

製が困難となるようなタンパー・エビデンス特性の付与をセキュリティ要件としているが、ISO 13491では、さらに端末の移動に対してタンパー・レスポンス特性を付与することを記述している。EMVでは、ATM、POS端末、PC等を端末として想定していることから、すべての端末に付与することが可能な特性をセキュリティ要件として挙げているものと考えられる。ISO 13491においてもATMやPOS端末と一体化される暗号デバイスを想定しているが、POS端末等の比較的軽量で移動させやすいものに対してはタンパー・エビデンス特性の付与、ATM等の重量の端末に対してはタンパー・エビデンス特性に加えタンパー・レスポンス特性の付与をセキュリティ要件として準備しているものと考えられる。FISC安全対策基準では、攻撃⑦に相当すると考えられる偽ATMの設置に対する対応策として、「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等」を挙げており、運用面から対策することとしている。そのほか、【運 113】「防犯措置を講ずること」では、「温度の異常、本体の傾き、振動等を管理して発報し、警備会社、金融機関等の管理センター等に知らせるセンターを設置し、非常ベルと連動させる」等と記述されている。これは、端末の現金収納部に対する防犯措置として準備されているものと考えられるが、同時に攻撃⑦への対策技術として利用することも考えられる。

金融機関店舗外のATM、POS端末、個人用パソコンといった端末を利用したサービスの拡大に伴い、金融機関の直接の管理下にない端末も増えてきている。こうした端末についてもアプリケーションに応じたセキュリティ対策が必要であり、相対的に強力な攻撃者を想定することが求められるケースにおいては、上記攻撃①～⑦のすべてに対する対策技術を適用することが必要であると考えられる。さらに、端末に対して付与される「耐タンパー性」に関して、FISC安全対策基準の【技 41】に記述されているタンパー・レスポンス特性を付与する際には、具体的にどのような技術を採用してタンパー・レスポンス特性を充足させるかを想定される攻撃を踏まえたうえで検討することが必要である。

ハ．PINパッドに関するセキュリティ要件

PINパッドを利用するアプリケーションを想定する標準・仕様としては、EMV、ISO 9564、APACSによるPP、FINREAD（CEN［2003a, b］）が挙げられる。

APACSによるPPでは、PINパッドやカード・リーダを含むPIN認証装置の形態が想定されているが（表13参照）、PINパッドに特化したセキュリティ要件は準備されていない。ただし、PINパッドとカード・リーダが一体化していないケース（表13における2、3、5の形態）では、PINパッドとカード・リーダ間の通信に関するセキュリティ要件が、PIN認証装置のセキュリティ要件に追加される形で記述されている。PIN認証装置のセキュリティ要件については、本節（ロ）の端末のセキュリティ要件において整理したため、以下では取り扱わない。また、金融向けICカード・リーダの欧州仕様であるFINREADは、PINパッドを備えたカード・リーダに関するセキュリティ要件を記述しているが、これについては、カード・リーダに関するセキュリティ要件として整理することとする。

EMVやISO 9564では、PINパッドに特化したセキュリティ要件が記述されている。EMVおよびISO 9564では、PINパッドとPINの照合を行うエンティティ間の通信路からPINが漏洩することを防止するため、一体化していないデバイスにPINを送信する場合には、PINをPINパッド内で暗号化することが想定されている。いずれの標準・仕様においても、基本的には、本節(ロ)で整理した端末に対するものと同一の要件をPINパッドに対して求めることとしている。ただし、ISO 9564では、端末に対するものと同一のセキュリティ要件の代替となるセキュリティ要件が用意されており、PINパッドが端末と一体化していない場合、あるいは、一体化している場合でも端末が本節(ロ)におけるセキュリティ要件を充足していない場合に、PINパッドに端末と同一のセキュリティ要件を充足するか、あるいは、以下に整理する代替のセキュリティ要件を充足することを求めている。

EMVでは、PINパッドに対して攻撃①、⑤～⑦が想定されており、ISO 9564では攻撃①と⑤が想定されている。これら攻撃の内容とPINパッドのセキュリティ要件を整理すると、表16のとおりである。

EMVでは、取引終了後、あるいは、一定時間ごとに内部データを自動的に消去することを別途要件としている。また、ISO 9564においても、取引終了の時点でPINパッド内にPINに関する情報を一切残さないこととしているほか、PINの暗号化に利用する鍵は取引後に変更し、過去に利用した鍵に関する情報をPINパッド内に残さないことを求めている。そのため、本節(2)ハ.(ロ)で整理した、端末に対して想定されている攻撃やセキュリティ要件とは差異がある。ただし、こうしたケースにおいても、デバイスの論理的改ざん（攻撃⑥）や偽PINパッドの設置（攻撃⑦）

表16　PINパッドへの攻撃に対するセキュリティ要件

攻撃手段	標準・仕様名	
	EMV	ISO 9564
攻撃① デバイスへの侵入	・攻撃に対して内部の機密データを消去すること。	・過去に利用されたPINが漏洩しないこと。 ・攻撃には専門的な技術が要求されることに加え、本来設置されている場所からPINパッドを長時間移動させておくことが必要であること、あるいは、PINパッドが正常に機能しなくなること。
攻撃⑤ デバイスの物理的改ざん	・特別な技術や一般に入手困難な機器が必要となるほか、デバイスに攻撃の検知を可能とする痕跡が残ること。	・盗聴装置の設置には、専門的な技術が要求されることに加え、本来設置されている場所からPINパッドを長時間移動させておくことが必要であること、あるいは、PINパッドが正常に機能しなくなること。
攻撃⑥ デバイスの論理的改ざん		——
攻撃⑦ デバイスの置換	・一般に入手可能なコンポーネントから類似のデバイスを作製できないこと。	——

を脅威として想定し、その対抗策に関して検討する必要があると考えられる。

セキュリティ特性をみると、EMVでは、攻撃①に対してタンパー・レスポンス特性を付与することをセキュリティ要件としているのに対し、攻撃⑤〜⑦に対しては、タンパー・エビデンス特性の付与を挙げている。攻撃⑤〜⑦については、攻撃の実行後、カード所持者にPINパッドを利用させることによってPINの盗取等の不正行為が成立するものである。したがって、カード所持者あるいはPINパッドの管理者（アクワイアラ）によって攻撃⑤〜⑦の実行を検知することができれば、攻撃者による不正行為を阻止することができるため、タンパー・エビデンス特性が選択されたものと考えられる。一方、ISO 9564では、攻撃①、⑤に対してタンパー・エビデンス特性、あるいは、タンパー・レスポンス特性のいずれかを選択できるようなセキュリティ要件が設定されている。

ニ．カード・リーダに関するセキュリティ要件

ISO 9564、FINREADではカード・リーダに特化したセキュリティ要件が記述されている。カード・リーダに対して想定されている攻撃、および、攻撃に対抗するためのセキュリティ要件を整理すると、表17のとおりである。

ISO 9564において、カード・リーダを利用するPIN認証は、参照PINデータの格納先とPINの照合先がともにICカードである形態のみである。この形態では、PINパッドでPINが暗号化されるが[13]、ICカードに直接PINの暗号文が送信されるケースと、カード・リーダで復号したPINがICカードに送信されるケースが想定されている。そのため、カード・リーダからICカードに平文のPINが送信される際には、それを盗聴するための装置の設置が攻撃として想定されているほか、カード・リーダが暗号処理を行うため、侵入による内部の機密データの漏洩（すなわち攻撃①）の防止がセキュリティ要件となっている。

また、ISO 9564では、本節（ハ）において説明したように、取引終了の時点でPINパッド内やカード・リーダ内にPINや暗号処理に利用する鍵に関する情報を格納しないケースを想定している。このため、上記の攻撃①のほかには、カード・リーダに対する脅威として攻撃⑤のみが想定されている。

FINREADでは、デバイスへの侵入（攻撃①）、および、デバイスの置換（攻撃⑦）に対して、カード・リーダがタンパー・エビデンス特性を有することをセキュリティ要件としている。また、秘密鍵が格納されるパーツには、攻撃①、②、⑤〜⑦を想定したうえでタンパー・レジスタンス特性を有することが記述されている。このように、FINREADでは、主にタンパー・エビデンス特性、タンパー・レジスタンス特性がセキュリティ要件として選択されている。その理由としては、攻撃による被害の範囲と、対策に必要な費用が考えられる。タンパー・レスポンス特性は、攻撃

13 PINパッドが端末と一体化し、端末が「物理的に安全なデバイスである」場合には、端末がPINの暗号化を行う。

表17　カード・リーダに対して想定されている攻撃手段とそれらに対するセキュリティ要件

攻撃手段	標準・仕様名	
	ISO 9564	FINREAD
攻撃① デバイスへの侵入	侵入 ・過去に利用されたPINが漏洩しないこと。 ・内部に格納されるPINや鍵の盗取には、専門的な技術が要求されることに加え、本来設置されている場所からPINパッドを長時間移動させておくことが必要であること、あるいは、PINパッドが正常に機能しなくなること。	侵入（ISO 13491に準拠） ・タンパー・エビデンス特性を有すること。 ・受動的耐性を有すること（ISO 13491）。
攻撃② サイドチャネル攻撃	——	観測（ISO 13491に準拠） ・電磁波の放射を物理的に防ぐこと（ISO 13491）。 ・観察を防御困難な部品内に機密データの格納や転送をしないこと。
攻撃⑤ デバイスの物理的改ざん	PIN盗聴装置や内部データの盗聴装置の設置 ・盗聴装置の設置には、専門的な技術が要求されることに加え、本来設置されている場所からカード・リーダを長時間移動させておくことが必要であること、あるいは、カード・リーダが正常に機能しなくなること。 ・PIN盗聴装置を設置するスペースがないこと。 ・PIN盗聴装置の設置をユーザが検知できること。 ・内部データの盗聴装置の設置を防止すること。	改ざん（ISO 13491に準拠） ・盗聴装置の設置が不可能であること（ISO13491）。
攻撃⑥ デバイスの論理的改ざん	——	改ざん（ISO 13491に準拠） ・内部の機密データの改ざんが困難であること（ISO 13491）。 ・ソフトウエアや公開鍵の改ざんを検知可能であること。
攻撃⑦ デバイスの置換	——	置換（ISO 13491に準拠） ・識別を可能とする特性を有すること。 ・不正な移動が困難であること（ISO 13491）。

備考：1. 各攻撃に関する記述欄において、実線上部は具体的な攻撃手法を示し、同下部はそれに対する主なセキュリティ要件を示す。
2. FINREADにおいて想定される攻撃については、それらが明記されているわけではないが、セキュリティ要件からISO 13491-1で記述されている攻撃が想定されているものと考えられる。

を検知した場合に内部データを自動的に消去する性質であり、同特性の実現には他の特性の場合に比べて相対的に多くの費用が必要になることが想定される。また、FINREADにおけるカード・リーダは、ユーザのプライベートな環境で利用されることが想定されている。仮にカード・リーダに対して攻撃が実行された場合においても、その被害は当該ユーザの範囲にとどめることができる。こうした点を考慮するとともに、プライベート環境での利用を想定した結果、タンパー・レスポンス特性ではなく、タンパー・レジスタンス特性が選択されたものと考えられる。

一方、ISO 9564では、ユーザのプライベート環境に加え、公共の場における利用を想定した結果、タンパー・エビデンス特性とタンパー・レスポンス特性のいずれかを選択できるようセキュリティ要件が設定されたものと考えられる。

(4) 小括

ICカードについては、その管理は当該カード所持者が行うため、金融機関の運用による対策では不十分であり、技術的な対策技術の導入が重要となる。そのため、ICカードに付与する耐タンパー性については、機能強度が高位に設定されている本節(2)ハ.(イ)で整理したPP等が参考になると考えられる。これらのPPでは、ICカードのセキュリティ要件として、主に、タンパー・レスポンス特性を付与することを挙げている。そのほか、EMVCoによる認定制度を参考にすることも考えられる。EMVCoによる認定は、ICカードを利用したクレジット決済取引の総合的な安全性を確保するために、どのようにICとOS（operating system）を利用するかという観点で行われるのが特徴である。

デビットカード端末の耐タンパー性を考えるうえでは、まず、その形態を整理する必要がある。デビットカード端末は、一般に、PINパッド、カード・リーダ、端末の3つのデバイスで構成されるが、3つのデバイスが一体化しているケース、PINパッドとカード・リーダのみが一体化しているケース、端末とカード・リーダのみが一体化しているケース等、さまざまな形態がある。そのため、デビットカード端末に関するセキュリティ要件を導出するうえでは、こうした端末の形態を考慮し、同様のアプリケーションを想定している標準や業界仕様を参考にすることができる。注意すべき点は、PIN認証、ICカード認証、生体認証を行ううえで、各デバイスにどのようなデータが格納されるか、また、各デバイス間をどのようなデータが通信されるかということであり、それらが保護すべきデータであるか否かを検討することが重要となる。

また、インターネット・バンキングの本人認証にICカードを利用するために、金融機関がPINパッドやカード・リーダを各ユーザに配付することを想定する場合においても、本節で整理したセキュリティ要件を参考にすることができる。耐タンパー性が付与されたPINパッド、カード・リーダの利用によって、PINやICカードに格納されているデータの漏洩等を防止することはできると考えられる。ただし、本人認証後の処理は各ユーザが管理するPCやモバイル端末を利用するため、それらが

安全に管理されていない場合には不正な処理が実行される惧れがあることに注意が必要である。

例えば、EMVやISO 9564では、端末の安全性が確保できないケースにおいても、PINパッドによってPINを保護できるようにセキュリティ要件を準備している。また、FINREADでは、攻撃に対する主なセキュリティ用件としてタンパー・レジスタンス特性の付与を挙げている。一般に、デバイスに求めるセキュリティ要件が多ければ、その分コストが高まることが想定されることから、自らのビジネス環境に応じたセキュリティ要件を導出することが重要である。

本稿では、FISC安全対策基準に記述されている「耐タンパー性」について、具体的にどのような機能をデバイスに付与することが必要であるかを、既存の国際・業界標準、技術文書を参考に整理した。今回は技術的な対策にのみ着目したが、デバイスの安全性は、環境面、運用面での対策も踏まえた総合的な対策によって確保されることから、環境面や運用面からの検討も必要である。ただし、自行の管理下にないデバイスを利用したサービスが拡大していることからも、技術面でのセキュリティ対策が今後より重要になってくると考えられる。

6．おわりに

本稿では、ICカードを利用した本人認証システムを対象として、個々のアプリケーションに応じたセキュリティ要件の明確化と、それらの要件を満足する対策技術の検討を行う際に、どのような事項に留意する必要があるかについて考察を行った。特に、同システムを対象とする国際標準や業界仕様に規定・記述されているセキュリティ要件を整理し、それらの要件をベースとして望ましい対策技術について考察するというアプローチを採用した。具体的には、生体認証方式を実装した場合における生体認証特有の問題点、および、ICカード等の暗号デバイスの耐タンパー性を実現するための物理的セキュリティ特性を論点とした。

生体認証に関しては、各種の既知の攻撃に対抗するセキュリティ要件が準備されているものの、要件を満足させる対策技術の効果を評価することが現時点では困難なケースが多いという点に留意する必要があるとの考察を得た。生体認証を金融サービスの中で活用する際には、今後の研究開発の動向をフォローし、生体認証システムをどこまで評価できるかについて慎重に見極める必要があるといえる。

また、暗号デバイスの耐タンパー性に関しては、カード・リーダ等の端末を金融機関が直接管理することが困難な環境下では運用による対策が十分に機能しないことから、端末に付与する耐タンパー性としてはより高いレベルの物理的セキュリティ特性が求められる可能性があることを示した。ICカードを利用した本人認証システムは、現在はCD・ATMでの利用が中心であるが、今後はインターネット・バンキング等のオープンなネットワークを利用した金融サービスでの利用へと、その裾野が拡大していく可能性もある。そうした場合に、本稿において取り上げた国際標準

や業界仕様を参考にしながらセキュリティ対策の検討を進めることが対応の1つとして考えられる。

本稿では、各標準・仕様が想定する脅威に対する技術的な対策に焦点を当てた。ただし、運用面や環境面における対策についても同様な検討が必要である。これらの多面的な対策を考慮し、ICカードを利用した本人認証システム全体としてのセキュリティ対策のあり方について今後検討していく必要があろう。

参考文献

宇根正志、「金融分野におけるPKI：技術的課題と研究・標準化動向」、『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年、227～283頁

――――・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」、『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

――――・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』第24巻別冊第2号、日本銀行金融研究所、2005年、1～56頁

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

金融庁、『金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）』、2007年

――――、『偽造キャッシュカード問題に関するスタディグループ最終報告書～偽造・盗難キャッシュカード被害発生の予防策・被害拡大の抑止策を中心として～』、2005年

――――、『偽造キャッシュカード問題に対する金融機関の取組み状況（平成17年12月末）』、2006年

情報処理推進機構、『バイオメトリクス評価に関する調査』、2005年

――――、『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

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

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

総務省・経済産業省、『電子政府推奨暗号リスト』、総務省・経済産業省、2003年（http://www.cryptrec.jp/images/cryptrec_01.pdf）

田村裕子・宇根正志、「金融取引におけるICカードを利用した本人認証について」、『金融研究』第25巻別冊第1号、日本銀行金融研究所、2006年、73～131頁

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

日立製作所、「バイオメトリクスセキュリティ評価基準の研究開発」、『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』、日本自動認識システム協会、2004年

日本規格協会、『耐タンパー性に関する標準化調査研究開発 報告書 第一部』、2004年

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

松本 勉・青柳真紀子、「人工物メトリクスによってICカードのセキュリティを高める方法」、『情報処理学会論文誌』、Vol. 46、No. 8、2005年、2098～2106頁

Association for Payment Clearing Services (APACS), *PIN Entry Device Protection Profile, version1.37,* APACS, 2003.

Biometrics Management Office (BMO) and National Security Agency (NSA), *U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments*, Version 1.0, Jan. 2006.

BULL, DASSAULT A.T., DIEBOLD, NCR, SIEMENS NIXDORF, and WANG GLOBAL, *Protection Profile version 1.00: Automatic cash dispensers / teller Machines*, 1999.

EMVCo, *EMV Integrated Circuit Card Specifications for Payment Systems– Book 1 Application Independent ICC to Terminal Interface Requirements, Version 4.1*, EMVCo, 2004a.

————, *EMV Integrated Circuit Card Specifications for Payment Systems– Book 2 Security and Key Management, Version 4.1*, EMVCo, 2004b.

————, *EMV Integrated Circuit Card Specifications for Payment Systems– Book 3 Application Specification, Version 4.1*, EMVCo, 2004c.

EUROSMART, *Smartcard IC Platform Protection Profile*, Version 1.0, 2001.

European Committee for Standardization (CEN), *pr CWA 14174-2: Financial Transactional IC card reader (FINREAD)– Part 2: Functional requirements*, 2003a.

————, *pr CWA 14174-3: Financial Transactional IC card reader (FINREAD)– Part 3: Security requirements*, 2003b.

International Organization for Standardization, (ISO) *ISO/DIS 13491-1, Banking– Secure cryptographic devices (retail)– Part 1: Concepts, requirements and evaluation methods*, ISO, 2006a.

————, *ISO 13491-2, Banking– Secure cryptographic devices (retail)– Part 2: Security compliance checklists for devices used in financial transactions*, ISO, 2005a.

————, *ISO 15782-1, Financial services– Public Key Infrastructure Management for Financial Services Certificate Management for Financial Services– Part 1: Public Key Certificates*, ISO, 2003a.

————, *ISO 15782-2, Financial services– Public Key Infrastructure Management for Financial Services Certificate Management for Financial Services– Part 2: Certificate Extensions*, ISO, 2001.

———— *ISO 19092-1, Financial services– Biometrics– Part 1: Security framework*, ISO, 2006b.

————, *ISO 21188, Financial services– Public Key Infrastructure Management for Financial Services Certificate Management for Financial Services– Public Key Infrastructure for Financial Services– Practices and Policy Framework*, ISO, 2006c.

————, *ISO 9564-1, Banking– Personal Identification Number (PIN) management and security– Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*, ISO, 2002.

————, *ISO 9564-2, Banking– Personal Identification Number (PIN) management and security– Part 2: Approved algorithms for PIN encipherment*, ISO, 2005b.

————, *ISO 9564-3, Banking– Personal Identification Number (PIN) management and security– Part 3: Requirements for offline PIN handling in ATM and POS systems*, ISO, 2003b.

————, *ISO/TR 9564-4, Banking– Personal Identification Number (PIN) management and security– Part 4: Guidelines for PIN handling in open networks*, ISO, 2004.

———, and International Electrotechnical Commission (IEC), *ISO/IEC 15408-1, Information technology– Security techniques– Evaluation criteria for IT security– Part 1: Introduction and general model*, ISO, 1999.

———, and———, *ISO/IEC 15408-2, Information technology– Security techniques– Evaluation criteria for IT security– Part 2: Security functional requirements*, ISO, 2005.

———, and ———, *ISO/IEC 7816-11, Identification cards– Integrated circuit cards– Part 11: Personal verification through biometric methods*, ISO, 2004.

———, and ———, *ISO/IEC 2nd CD 19792: Information technology– Security techniques– Security evaluation of biometrics*, 2006.

Smart Card Security User Group (SCSUG), *Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP), Version 3.0*, 2001.

Une Masashi, Akira Otsuka, and Hideki Imai, "Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems," *forthcoming to Advances in Biometrics, Proceedings of International Conference on Biometrics 2007*, LNCS 4642, Springer-Verlag, 2007, pp. 396-406.

VISA International Service Association (VISA), *PIN Management Requirement: PIN Entry Device Security Requirements Manual*, Version 3.0a, 2004.