IMES DISCUSSION PAPER SERIES

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

田村 裕子（たむら ゆうこ）・宇根 正志（うね まさし）

Discussion Paper No. 2006-J-4

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

IMES Discussion Paper Series 2006-J-4
2006 年 4 月

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

田村 裕子[*]・**宇根 正志**[**]

要　　旨

わが国では、偽造キャッシュカードを用いたなりすましによる不正な預金引出しが深刻な問題となっている。こうした問題への対応として、金融機関は、従来の磁気ストライプによるキャッシュカードの IC カード化を進めている。IC カードを利用したシステムを構築する際には、IC カードはもとより、システム全体に存在する脆弱性を明確にしたうえでセキュリティ要件を導出し、当該システムがそうした要件を満足しているか否かを適宜評価していくことが、安全な金融取引を実現するために必要となる。

本稿では、金融取引において今後普及すると見込まれる IC カードを利用した本人認証のシステムにおけるセキュリティ要件の導出を行う。IC カードを利用した本人認証には、暗証番号（PIN）による認証と併用するもの、生体情報を利用する認証と併用するものなど、さまざまな方式が考えられるが、本稿では、IC カードを利用した本人認証のなかでも、現在広く利用されている PIN による認証と併用する方式を対象とする。想定する脅威として、第三者によるなりすましに焦点を当てるとともに、動的／静的認証、オフライン／オンライン認証等、認証形態のバリエーションを考慮して検討を行う。また、こうした検討の枠組みや結果をどのように活用することができるかについて説明するとともに、今後の検討課題を整理する。

キーワード：本人認証、IC カード、PIN、セキュリティ要件
JEL classification: L86、L96、Z00

[*] 日本銀行金融研究所情報技術研究センター（E-mail: yuuko.tamura@boj.or.jp）
[**] 日本銀行金融研究所情報技術研究センター（E-mail: masashi.une@boj.or.jp）

本論文は、2006 年 3 月 28 日に日本銀行で開催された「第 8 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。

目 次

1 はじめに **1**

2 金融取引における本人認証 **3**
2.1 本人認証とは 3
2.2 金融取引における本人認証手段の事例 4
2.3 IC カードを利用した本人認証 6
2.4 本稿における検討の内容 8

3 IC カードによる所持認証におけるセキュリティ要件 **10**
3.1 IC カード認証の機能と定義 10
3.2 IC カード認証の形態 11
3.3 IC カード認証に対する脅威 12
3.4 動的認証を利用した IC カード認証 16
3.5 静的認証を利用した IC カード認証 25
3.6 IC カード認証のセキュリティ要件に関する考察 32

4 PIN による知識認証におけるセキュリティ要件 **35**
4.1 PIN 認証の機能と定義 35
4.2 PIN 認証の形態 35
4.3 PIN 認証に対する脅威 38
4.4 想定する攻撃に対する対策法 46
4.5 セキュリティ要件 50
4.6 PIN 認証のセキュリティ要件に関する考察 52

5 考察と今後の課題 **54**
5.1 本稿における検討結果の活用 54
5.2 今後の検討の方向性 55

6 おわりに **58**

補論 本人認証後からサービス提供までのフローにおけるセキュリティ要件 **61**

1　はじめに

CD/ATM を利用した預金取引においては、機械で自動的に預金者本人であることを確認する手段が必要となる。金融機関では、機械による本人確認を主に 4 桁の暗証番号（PIN：personal identification number）と磁気ストライプ・カードを利用して行ってきた。このタイプのキャッシュカードは、銀行番号、支店番号、口座番号といった預金取引に必要な情報を記録させた磁気ストライプをプラスチック・カードに貼付したものである。これまでは、このようなキャッシュカードを偽造することは困難であろうと想定され、キャッシュカードが本人の手元にある限り、CD/ATM が読み取ることのできるキャッシュカードを提示できるのは本人のみであるとして本人確認を行ってきた。しかし、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カード・リーダ／ライタが比較的容易に入手できるようになり、CD/ATM といった端末に「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、キャッシュカードを利用した本人認証の安全性が低下する結果となった[1]。

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業界に対して求められ（金融庁［2005］）、金融機関はその手段の 1 つとしてキャッシュカードの IC カード化を進めている（金融庁［2006］）。現在、金融機関で導入が進められている IC カードは、中央処理装置（CPU：central processing unit）が搭載されているタイプである。こうした IC カードは、演算機能や判断機能を有するほか、CPU がアクセス制御することでメモリ内データの不正な読出しや改ざんを困難とする「耐タンパー性」を実現する媒体であると言われており、磁気ストライプ・カードに代わって、安全な本人確認を実現するためのツールとして注目を集めている。

しかし、IC カード等の暗号モジュールのメモリ内に格納される秘密情報を盗取する故障利用攻撃やサイドチャネル攻撃といった新たな攻撃法が提案されており、無条件にすべての CPU 搭載型 IC カードが安全であるとは言えない。また、IC カードが期待どおりの安全性を有する暗号モジュールであったとしても、安全性の低い認証方式の採用が IC カードの偽造に繋がるおそれがあるほか、攻撃者は本人認証システムを構成する IC カード以外のエンティティや通信路からなりすましに必要な情報の入手を試みることも考えられる。IC カードを利用したシステムを構築する際には、IC カードの安全性（耐タンパー性）のみに着目するのではなく、シ

[1] 金融情報システムセンター［2005a］によれば、キャッシュカードの真偽チェックとして、磁気ストライプの特定のフィールドに CD/ATM 取引の利用明細書等には表示していない秘密のコードを設定し、磁気ストライプに書き込むべきデータを容易に推定できないようにしている金融機関もあるようである。しかし、秘密のコードの値や計算方法が既知である場合や、スキミングによって読み取った磁気ストライプの情報を転写して偽造カードを作製する攻撃に対しては、こうした秘密コードのチェックは有効に機能しないこととなる。

ステム全体に存在する脆弱性を明確にしたうえでセキュリティ要件を導出し、当該システムが同セキュリティ要件を満足しているか否かを適宜評価していくことが、安全な金融取引を実現するために必要である。

IC カードを用いた本人認証システムのセキュリティ要件に関する研究成果は、これまでにいくつか発表されている。例えば、ECOM［1997, 1998］においては、金融分野における IC カードを用いる本人認証システム一般に適用可能なセキュリティ要件について検討されている。ただし、こうした検討は、IC カードや端末の物理的な安全性に主として焦点を当てたものであり、本人認証の有効性を左右する要素である認証方式の形態のバリエーションを考慮したものとはなっていない。

そこで、本稿では、こうした認証方式の形態を考慮して、IC カードと PIN を組み合わせて用いる本人認証システムにおける、なりすましに対するセキュリティ要件を検討する。IC カード認証においては、動的／静的認証、オフライン／オンライン認証、共通鍵暗号／公開鍵暗号を用いた認証の差異に着目して場合分けを行ったうえで分析を行う。PIN 認証においては、PIN の照合を実行するエンティティ、および、PIN の正当性の確認に利用するデータの格納先の差異による場合分けを行い分析を行う。

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、真正な IC カードを所持するユーザを本人であるとする認証方式について、偽造カードによるなりすましを脅威とした場合に想定される攻撃、および、そうした攻撃に対する対策法を列挙したうえで、セキュリティ要件を導出する。4 節では、正しい PIN を提示するユーザを本人であるとする認証方式について、そのセキュリティ要件を 3 節と同様の過程で導出する。5 節では、IC カードと PIN を併用する本人認証システムの安全性について検討するうえで、本稿における検討の枠組みや結果をどのように活用することができるかについて説明するとともに、今後の検討課題を整理する。

2　金融取引における本人認証

2.1　本人認証とは

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（図 1 参照）。

- **知識認証（something you know）：** 認証者に登録された情報（PIN、パスワード等）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。
- **所持認証（something you own）：** 認証者が配付（指定）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。
- **生体認証（something you are）：** 認証者に登録された情報と提示された身体的あるいは行動的特徴に関する情報（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。生体情報が個人を識別できる性質をもつことが条件であり、人工物による偽造が困難である場合等に有効である。

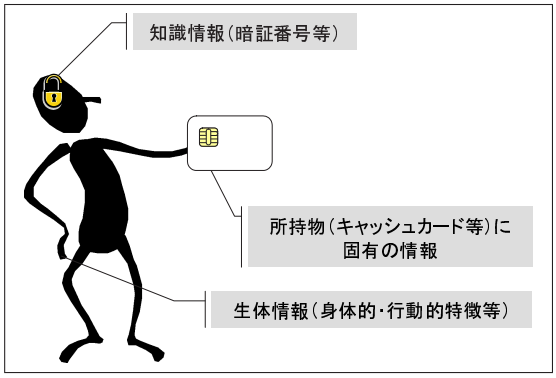

図 1: 本人認証に利用される 3 種類の情報

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[2]による認証形態においては、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[3]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（登録申請者が秘密に記憶しておく情報、所持物に固有の情報、生体情報）」（あるいは、その情報に対応づけられた情報）をデータベースに登録する。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。

2.2 金融取引における本人認証手段の事例

金融取引は、金融機関の窓口において職員を介して行われることもあるが、利便性の観点から機械で自動的に実行するケースが圧倒的に多い。この場合、金融取引に伴う顧客の本人認証についても機械で実施することとなる。

ここで、わが国における機械を介した各種金融取引の際に実施されている本人認証の事例を紹介する。

− CD/ATM を利用したキャッシュカード取引： 4 桁の PIN と磁気ストライプ・カードによる本人認証のほか、4 桁の PIN と IC カード、あるいは、手のひらや指の静脈パターンを利用した生体認証を併用した本人認証の手法も採用されている。

− オンライン・バンキング： インターネット経由でパソコンから金融機関のサービスを利用するオンライン・バンキングでは、パスワード[4]、あるいは、パ

[2]被認証者を識別するためのデータ（ユーザ ID 等）をインデックスとして、被認証者によって提示された情報と、ユーザ ID と対応づけされてデータベースに管理される情報が一致するか否かを判断する方法。これに対して、提示された情報がデータベース内の n (≥ 2) 個の情報のうちのいずれかと一致するか否かを順に照合していく方法は 1 対 n 照合と呼ばれる。

[3]登録フェーズで要求される身元の確かさは、本人認証を利用するアプリケーションによって異なる。

[4]一般には、PIN は数字列、パスワードは英数字やカナ文字で表現されるものを指す。

スワードと乱数表[5]を利用して本人認証を行うケースが多い（パスワードは複数利用されるケースもある）。そのほか、通常のパスワードとワンタイム・パスワード[6]の組合せやパスワードとICカードの組合せによって認証を行う金融機関もある。また、オンライン・バンキングに利用するパソコンのドメイン名やIPアドレスを事前に登録することで、登録者以外からのアクセスを制限するサービスもある。この場合、当該パソコンが利用可能なユーザのみがサービスを利用可能であるという観点から、パソコンを所持認証のツールとして利用しているとみることもできる。

― モバイル・バンキング： インターネット経由で携帯電話等のモバイル端末から金融機関のサービスを利用するモバイル・バンキングでは、パスワードによって本人認証を行う方式や、登録されたモバイル端末以外からのログインを制限する機能を導入した方式が導入されている。後者の方式については、モバイル端末を所持認証のツールとしてみることができる。

― 店頭やCD/ATMにおけるクレジットカード取引： クレジットカードの加盟店の店頭に設置されるPOS端末で磁気ストライプ・カードのデータを読み出すとともに、サイン（手書き署名）を用いて本人認証を行うケースが多い。クレジットカードとしてICカード[7]を利用するとともに、4桁のPINを用いて本人認証を行うケースもある。また、提携CD/ATMにおいて、4桁のPINとクレジットカード（磁気ストライプ・カードあるいはICカード）を用いて本人認証を行うケースもある。

― オンライン・クレジットカード取引： パソコン等のキーパッドからのカード番号とカードの有効期限等の提示により本人であると判断するケースが多いが、これらの情報に加え4桁のPINを利用して本人認証を行うケースもある。そのほか、ICカード・リーダ／ライタを利用してICカードが提示する情報で本人認証を行うケースもある。

[5]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である。乱数表は各預金者ごとに異なるものであり、乱数表と預金者は対応づけられている。認証では、サーバ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求められる。各金融機関によって、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。

[6]金融機関によって配付されるパスワード生成器が表示するパスワードであり、ある一定の時間ごとに自動的に変更され、被認証者は認証を実行する時点で表示されているワンタイム・パスワードを利用する。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定困難な形態で生成される仕組みとなっており、ある時点におけるワンタイム・パスワードが盗取された場合でも、なりすましを困難にできるといわれている。

[7]ICチップを搭載した携帯電話を所持認証のツールとして利用するケースもある。

2.3 IC カードを利用した本人認証

2.2 節で紹介した本人認証手段の中でも、キャッシュカードの偽造への対応として注目されている IC カードを本人認証のツールとして利用するケースに焦点を当てる。ここで、IC カードを利用した本人認証を以下のように定義する。

> **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。

また、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を次のように定義する（図 2 参照）。

- カード所持者： 当該 IC カードと対応付けされているユーザ。
- IC カード： 専用のリーダで読み取る（接触、非接触の）CPU 内蔵型の所持認証用デバイス。磁気ストライプを併用したものは含まない、あるいは、併用している場合においても磁気ストライプ・データは利用しないことを想定する[8]。
- 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。金融機関の責任により、設備・運用面の種々のセキュリティ対策が施されていることで安全に管理される状況を想定する。
- 端末： IC カードと直接通信を行い、IC カード・ホスト間の通信を媒介するデバイス。キーパッド（あるいは、PIN パッド）、IC カード・リーダ／ライタ等が一体化[9]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場合等、さまざまなケースがある。本稿では、各デバイスが一体化し、端末として 1 つの装置を形成しているケースを想定する。なお、3、4 節での議論を、各デバイスが独立して存在するケースに拡張することも可能である。

[8] 現在、金融機関が発行する IC キャッシュカードは互換性確保の観点から磁気ストライプも併用されているケースが多い。ATM が IC キャッシュカードに対応していない場合、あるいは、他の金融機関の ATM を利用する場合には、磁気ストライプに書き込まれたデータを利用して金融取引を行っている。これらの場合、IC カードであっても、偽造に対するリスクは磁気ストライプ・カードと同様である。

[9] ここで、「一体化」とは、端末を構成するコンポーネント間の通信の傍受が極めて困難な状況を指すものとする。

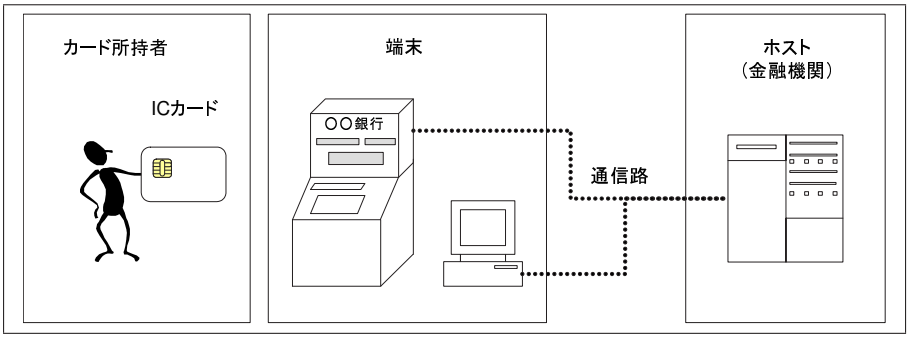

図 2: IC カードを利用した本人認証におけるエンティティ

2.2 節で紹介した各種金融取引に関係するエンティティのうち、端末に関しては、アプリケーションによってその形態や管理環境等が異なる。そこで、各アプリケーションにおける端末の形態、および、その管理環境について整理する。

・CD/ATM を利用するキャッシュカード、クレジットカード取引： 端末（CD / ATM）が設置される環境としては、(1) 営業時間内の銀行店舗内、(2) 銀行店舗外の有人エリア、(3) 無人エリアの 3 つのケースが考えられる。いずれの場合においても、端末が設置される環境は監視カメラによって管理されることが想定される。また、上記 (1) に関しては、監視カメラに加え、金融機関（職員または警備員）によって端末が管理され、上記 (2) については当該エリアの管理者によって端末が管理される。CD/ATM は、一般に、PIN パッドやカード・リーダ／ライタが一体化して形成されている。

・店舗等の POS 端末を利用するクレジットカード取引： 端末（POS 端末）は、一般に当該店舗の店員によって管理されることが想定されるほか、監視カメラが設置される場合もある。POS 端末は、PIN パッドやカード・リーダ／ライタが一体化しているケースやそうでないケースがあるほか、PIN パッドとカード・リーダ／ライタのみが一体化しているケースもある。

・パソコン、モバイル端末を接続して利用するオンライン・バンキング： オンライン・バンキングを利用する際に使用する端末（パソコン、モバイル端末）については、自宅のパソコンやインターネット・カフェにあるパソコンといったように、カード所持者が管理するケース、あるいは、第三者が管理するケースが考えられる。オンライン・バンキングにおいて IC カードを利用する場合では、一般に、カード・リーダ／ライタはパソコン等と一体化していないことが多い。ただし、モバイル端末を利用する場合においては、モバイル端末に IC チップが組み込まれ、カード・リーダ／ライタが一体化していると

位置付けられる場合があるほか、モバイル端末にカード・リーダ／ライタを接続して利用することもある。

2.4 本稿における検討の内容

本稿では、2.3 節において定義した「IC カードを利用した本人認証」のシステムを安全に運用していくうえで、どのようなセキュリティ要件を満足させることが求められるかについて検討する。本人認証の手法としては、2.1 節で説明したように、生体情報を利用する方法やワンタイム・パスワードを利用する方式をはじめとしてさまざまものが実際に利用されているが、ここでは、検討の手始めとして、今後普及すると見込まれる IC カードによる所持認証と、現在広く利用されている PIN による知識認証に焦点を当てることとする。また、これらの認証手法の単独での効果を明らかにするために、各認証手法を別々に検討することとする。

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検討する際には、システムを構成するエンティティ（ここでは、IC カードや端末が該当する）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。実際に、ECOM［1997, 1998］では、IC カードや端末のライフ・サイクルを設計・製造、発行・設置、使用、廃棄のフェーズに分けたうえで、各フェーズにおいて想定される脅威・脆弱性とその対策について検討されている。例えば、ECOM［1997］を参照して IC カード等のライフ・サイクルとその脅威についてまとめると、表 1 のとおりである。

表 1 のうち、「使用」のフェーズが、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ことから、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。もちろん、設計・製造、発行・設置、廃棄のフェーズにおいても、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もある。ただし、本稿ではこれらのエンティティは不正を行わない（運用によって不正の発生を予防することが可能）と仮定し、IC カードや端末の使用のフェーズに焦点を当てて検討することとする。

使用のフェーズにおいてどのような切り口でシステムのセキュリティ要件を導出するかについては、認証方式の形態に着目したセキュリティ要件の検討を行うこととする。IC カードを用いた本人認証の形態としては、3.2 節で紹介する動的認証や静的認証、オフライン認証やオンライン認証、暗号を利用する場合には共通鍵暗号を利用する方式や公開鍵暗号を利用する方式といったように、さまざまなバリエーションが存在する。金融取引にこうした認証方式を適用することを想定した場合、求められるセキュリティ要件や、認証方式の形態の差異とセキュリ

フェーズ	IC カード	端末
設計・製造	印刷メーカーによる IC カードの設計・製造（$\Longrightarrow$ 主な脅威：機密情報の漏洩、IC カードの盗難・変造）	端末メーカーによる設計・製造（$\Longrightarrow$ 主な脅威：IC カードと同様）
発行・設置	(1) 印刷メーカーによる IC カードの個別化（personalization）、(2) 金融機関による IC カードの顧客への発送、(3)（場合によっては）認証機関による公開鍵証明書の発行（$\Longrightarrow$ 主な脅威：機密情報の漏洩、不正な公開鍵証明書の組込み、IC カードの盗難）	(1) 金融機関等による端末の設置、(2)（場合によっては）認証機関による公開鍵証明書の発行（$\Longrightarrow$ 主な脅威：機密情報の漏洩、不正な公開鍵証明書の組込み、各種攻撃を実行するための不正な仕掛けの組込み、端末の盗難）
使用	IC カード所持者による IC カードの使用（$\Longrightarrow$ 主な脅威：IC カードの盗難、カードの偽造・変造、カードの情報の改ざん・コピー、通信データの盗聴）	IC カード所持者による端末の使用、端末保守作業員等による端末のメンテナンス（$\Longrightarrow$ 主な脅威：端末の盗難、端末への不正アクセス、内部のデータの改ざん、通信データの盗聴）
廃棄	IC カード所持者や金融機関による IC カードの廃棄（$\Longrightarrow$ 主な脅威：破棄された IC カードの不正な再利用）	金融機関による端末の廃棄（$\Longrightarrow$ 主な脅威：廃棄された端末の不正な再利用）

備考：ECOM［1997］表 2-10 を参照して作成。

表 1: IC カードと端末のライフ・サイクルと主な脅威

ティ要件との間の関係等について検討することは、IC カードを積極的に活用していこうとしているわが国の金融機関にとって有用な情報を提供すると考えられる。

IC カードによる所持認証と PIN による知識認証を検討対象とするにあたって、想定すべき脅威や具体的な攻撃手法等に関しては、3 節および 4 節においてそれぞれ説明することとする。

3　IC カードによる所持認証におけるセキュリティ要件

3.1　IC カード認証の機能と定義

認証者である金融機関が配付した IC カードを携帯するユーザを本人（カード所持者）であるとする所持認証によって本人認証を行う場合、被認証者によって提示された IC カードが盗難されたり偽造されたりしたものでないこと、および、当該 IC カードがどの個人の所持物かを確認する必要がある。そのため、IC カードによる所持認証が本人認証を行う手段として有効に機能するためには、以下の条件が満足されることが求められる。

条件 1　カード所持者以外による真正な IC カードの不正利用を防止可能であること。

条件 2　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が確認可能であること。

条件 3　IC カードに対応するカード所持者のユーザ ID を特定可能であること。

IC カードによる所持認証とは、IC カードに対応するカード所持者のユーザ ID を確認することであり、被認証者が IC カードに対応するカード所持者であるか否かまでは確認できない。そのため、所持認証によって本人確認を実現する場合には、被認証者はカード所持者であることが条件であり、それ以外のユーザによって IC カードが提示される場合には、その利用を防止することのできる機構が別途必要となる（条件 1）。そのような機構としては、被認証者とカード所持者のユーザ ID との対応を確認可能とする別の認証手段等を利用するのが一般的である[10]。

条件 1 が満足される状況においても、金融機関によってカード所持者に配付された IC カードであると誤って認識される IC カードを入手することができれば、カード所持者へのなりすましが可能である。このため、認証者は、被認証者の提示した IC カードが金融機関によって配付されたものであること、すなわち、偽造されたものでないことを確認する（条件 2）とともに、カード所持者のユーザ ID を特定する（条件 3）必要がある。これらは、ユーザ登録の時点でデータベースに登録した IC カードに固有の情報と、IC カードが提示する情報が対応するものであるか否かを確認することで行われる。IC カードに固有の情報として利用可能なものとしては以下の 2 つが考えられる。

[10]仮に、IC カードが盗取され、条件 1 を満たすために準備した他の認証手段が有効に機能しない場合には、IC カードによる所持認証も本人認証の手段として有効に機能しないこととなる。

(1) IC チップ内に格納されるデジタル・データ

(2) IC チップ外（プラスチック・カード部分等）に含まれる情報

上記 (1) におけるデジタル・データ（以下、データと呼ぶときはデジタル・データを指すものとする）を利用した認証は、当該データが金融機関に登録されているデータに対応するものであるか否かを確認することで実現される。

上記 (2) における IC チップ外の情報を利用した認証の手段としては、ホログラムやマイクロ文字等の偽造防止技術の適用が挙げられる。その中でも、人工物メトリクス（松本ほか［2004］）は、人工物に固有の物理的特性（光学特性、磁気特性等）を利用して自動的に人工物を認証する技術であり、偽造防止対策に有効な手段の 1 つである。人工物メトリクスを利用することで IC カード認証の安全性を高める方法については、松本＝青柳によって検討結果が示されており（松本・青柳［2005］）、他の偽造防止技術についても、機械による読取りが可能なものであれば、同様の議論によってその有効性を検討できると考えられる。そのため、本稿では、IC チップ内のデータのみを利用した所持認証のシステムについて検討を行うこととする。

ここで、条件 1 は他の認証手段等によって満足されることを想定するとともに、条件 2 および条件 3 を満足させるための手段を「IC カード認証」と呼び、以下のように定義する。

> **IC カード認証**： IC カードが提示するデータを利用して、当該 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とともに、当該 IC カードに対応するカード所持者のユーザ ID を特定すること。

3.2 IC カード認証の形態

IC カード認証は、認証時における IC カードの動作の違いによって以下の 2 つに分類される。

- **動的認証**（dynamic authentication）： 認証の都度、新たに IC チップ内で生成されるデータを認証者に提示することにより実行される認証方式。認証時に IC カードが提示するデータが毎回異なることから、動的データ認証（dynamic data authentication）とも呼ばれる。
- **静的認証**（static authentication）： IC チップ内にあらかじめ格納されているデータを認証者に提示することにより実行される認証方式。認証時に IC カードが提示するデータが常に同じであることから、静的データ認証（static data authentication）とも呼ばれる。

また、認証者の違いによってICカード認証は以下の2つに分類される（図3参照）。

- **オフライン認証**： 端末がICカードを認証する方式。
- **オンライン認証**： ホストが端末を介してICカードを認証する方式。

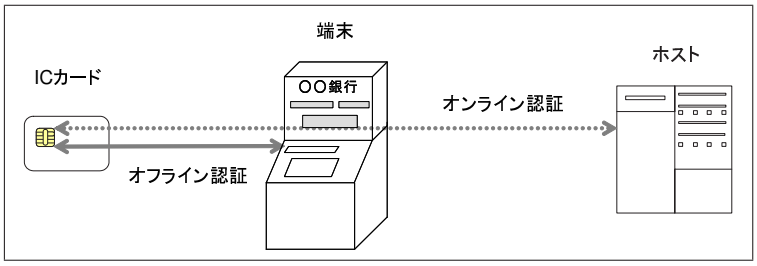

図 3: オフライン認証とオンライン認証

この結果、ICカード認証の形態は4種類に分類されることとなる（図4参照）が、以下では、3.4節において動的認証、3.5節において静的認証に関するセキュリティ要件について考察を行い、各節において、それぞれオフラインとオンラインの認証形態について取り扱うこととする。

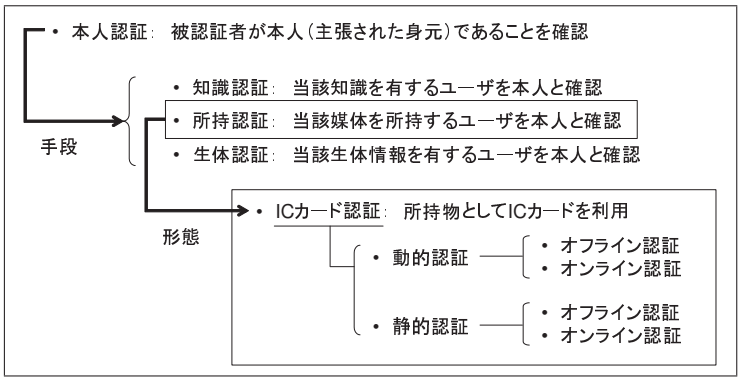

図 4: 本人認証を実現する手段

3.3 ICカード認証に対する脅威

キャッシュカード・クレジットカード取引におけるICカード認証のセキュリティ要件を導出するには、ICカード認証における脅威、および、攻撃者の能力を想定したうえで、考えられる攻撃、また、それへの対策について考察を行う必要がある。本節では、まず、ICカード認証における脅威、および、攻撃者の能力に関する想定環境を述べることとする。

3.3.1 想定する脅威と対策方針

金融取引を行うユーザに対する攻撃としては、まず、キャッシュカードのICカード化の契機ともなった、偽造カード作製によるカード所持者へのなりすましが挙げられる。3.1節のICカード認証の定義より、認証方式におけるなりすましは、(1)金融機関によって配付されたものでないICカードが金融機関によって配付されたものであると判断され、かつ、(2)ICカードに対応するユーザIDが別のユーザのIDとして認識される場合に成功する。

ここで、なりすましに対する安全性を考察するうえで利用する用語を定義しておく。

- 真正なICカード： 金融機関が正規の手続に沿って配付したICカード。
- 偽造カード： なりすましの対象であるユーザの真正なICカード（以下、偽造対象カードと呼ぶ）以外のICカードのうち、攻撃者がなりすましを行うために作製したもの。
- 偽ホスト： ICカードあるいは端末に対してホストになりすましを試みるコンピュータ。
- 真正な端末： 攻撃者によって不正な細工が加えられていない端末。真正なCD/ATMやPOS端末は、金融機関によって設置される。
- 攻撃モジュール： ICカードや端末内部のデータを盗取・改ざんすることを目的としたモジュール。例えば、スパイウエアやウイルスといったソフトウエアや、秘密情報の盗取に利用されるハードウエアがこれに含まれる。
- 不正端末： 攻撃モジュールが組み込まれた真正な端末。
- 偽端末： カード所持者、ICカード、ホストに対して真正な端末になりすましを試みるハードウエア。

なお、ホストに関しては、金融機関において安全に管理されると想定していることから、金融機関が管理するホストに対して攻撃モジュールが組み込まれることはないと考える。このため、上記の不正端末に対応する「不正ホスト（攻撃モジュールが組み込まれたホスト）」は想定しない。上記の偽ホストは、金融機関の管理が及ばないところで、攻撃者が独自に準備して設置するものを想定する。

ICカード認証をオフラインで実行するケースにおいてなりすましを行う具体的な手段としては、(1) 真正な端末に対してなりすましが成功する偽造カードを作製する、(2) 攻撃者が作製した偽造カードと整合性を持つように端末を不正に操作するという2つが考えられる。上記 (2) の具体的手段としては、端末における処理で

用いられるパラメータ（秘密鍵等）を攻撃者にとって都合のよいものに改ざんするものが考えられる[11]。

一方、オンライン認証においては、ホストは安全に管理されることを想定しているため、(3) ホストに対してなりすましが成功する偽造カードを作製する、もしくは、(4) ホストに対して、偽造対象カードと通信しているかのように、不正端末あるいは偽端末（以下、不正・偽端末と呼ぶ）を操作するという方法が考えられる。これらのうち、上記 (4) を実行するためには、偽造対象カードが認証の際に用いるデータを入手することが求められるが、これは上記 (3) における偽造カード作製の際にも必要となる事項であり、上記 (3) への対策は同時に上記 (4) への対策にもなると考えられる。

そこで、以下では、上記 (1)、(2)、(3) の手段で別のカード所持者になりすますことを脅威として想定し、検討を進める。

偽造カードを利用したなりすましに対する対策としては、(A) 偽造カードの作製を防ぐ、(B) 偽造カードの使用を防ぐ、(C) 偽造カードの使用を追跡するといった 3 段階の対策が考えられる。上記 (A)、(B) といった事前的な対策は被害の発生を抑えるために利用され、上記 (C) のような事後的な対策は、その補助的な役割を担うものと思われる。一般には、両者の対策方法を併用することで、なりすましに対する安全性の向上を図ることが多いが、本稿では、まず、偽造カードによるなりすましに対する事前的な対策に焦点を当てて検討を行うこととする。

3.3.2 真正な端末への攻撃モジュールの組込みや偽端末の設置

不正端末や偽端末を用いた攻撃の実現可能性については、2.2 節において整理したアプリケーションによってその困難さが異なると考えられる。そこで、真正な端末への攻撃モジュールの組込みや偽端末の設置の手段について整理する。

・CD/ATM を利用するキャッシュカード、クレジットカード取引： 真正な端末への攻撃モジュールの組込みを行うためには、銀行店舗内や銀行店舗外の有人エリアの環境では、攻撃者は端末の管理者やメンテナンス作業員と結託するといったことが必要となる。無人エリアの端末に関しては、メンテナンス作業員と結託するといった方法のほか、結託せずとも監視カメラの細工を行ったうえで攻撃者単独で攻撃モジュールの組込みを行うといったことが考えら

[11] 端末を不正に操作する攻撃については、端末による処理フロー（認証処理を実行するプログラム）を改変して、攻撃者に都合のよい結果を出力させるということも考えられる。この場合には、偽造カードを作製せずとも端末単独で不正行為を実行可能である。本節では、IC カードを偽造することによるなりすましを検討対象としていることから、こうした攻撃については補論において議論することとする。

れる。そのほか、端末がそもそも設置されていない環境に偽端末を設置するといったことも考えられる。

・店舗等の POS 端末を利用するクレジットカード取引： POS 端末は、CD/ATM に比べて持運びが容易であることから、偽端末の設置が相対的に容易となる可能性が高い。真正な端末への攻撃モジュールの組込みについては、当該店舗の店員と結託する、あるいは、当該店舗に単独で侵入するといったことが考えられる。監視カメラが設置されている場合には、監視カメラを欺く細工も必要となる。そのほか、真正な端末が置かれていない店舗に偽端末を設置するといったことも考えられる。

・パソコン、モバイル端末に接続して利用するオンライン・バンキング： カード所持者に検知されないようにパソコンやモバイル端末に攻撃モジュールを組み込む方法としては、主に、これらのハードウエアを直接不正に操作する方法と、ネットワーク経由で攻撃用のソフトウエアを不正に組み込む方法が考えられる。直接不正に操作するためには、カード所持者がパソコンやモバイル端末を管理している環境に侵入する必要があるほか、インターネット・カフェ等の端末においては、当該施設の管理者と結託する、あるいは、そうした管理者に気づかれないように単独で攻撃モジュールを組み込むこととなる。監視カメラが設置されている場合については、カメラを欺く細工も必要である。ネットワーク経由で実行する方法に関しては、パソコンやモバイル端末にインターネットを通じてスパイウエアやウイルス等を不正にインストールさせる方法が考えられる。こうした方法のほかに、金融機関からの指示と偽って不正なソフトウエアをカード所持者に配付してパソコン等にインストールさせるとか、管理者に気づかれないようにインターネット・カフェ等に偽端末を設置することも考えられる。

以上の整理から、端末の管理環境の違いによって攻撃モジュールの組込みや偽端末の設置の実現可能性は異なってくるものの、いずれの場合においてもそうした攻撃の可能性は否定できないと言える。そのため、以下では特定のアプリケーションを想定することなく、金融取引において IC カード認証を実現するシステム一般を対象として考察を行うこととする。

3.3.3 攻撃者の能力

IC カードの開発を手掛けるセキュリティ技術の専門家と同等の知識・技術を有していなければ現時点では実行が困難とされている攻撃であっても、IC カードや端末等の解析手法が進歩すれば、将来そうした専門家でなくとも実行可能な攻撃

となる可能性がある。IC カードを利用した本人認証システムを今後中・長期間にわたって使用していくことを想定した場合、こうした可能性に留意することが必要であることから、本節では、IC カードの開発を手掛けるセキュリティ技術の専門家と同レベルの知識・技術を有する攻撃者を想定して検討を行う。具体的には以下の能力を持つものとする。

- IC チップ内部に格納すべき情報が入手できれば、当該IC カードと同じ機能を実現する IC カードを作製可能である。
- IC カード、および、端末内で秘密に管理されている情報以外の情報（例えば、IC カード認証方式の実行手順および利用される暗号アルゴリズムに関する情報）を有する。
- IC カードと端末、および、端末とホスト間の通信路上のデータの盗聴を試行する。
- 真正な端末への攻撃モジュールの組込みや偽端末の設置を試行する。
- 偽ホストの設置を試行する。
- IC カードや端末に対して、内部信号を直接観測する等の手段によって内部データの不正入手・改ざんを試行する（以下では、こうした攻撃を侵入型攻撃[12]と呼ぶ）。
- IC カードや端末に対して、故障利用攻撃[13]やサイドチャネル攻撃[14]といった手法を利用して、暗号処理中のモジュールから秘密鍵の不正入手を試行する（以下では、こうした攻撃を非侵入型攻撃[15]と呼ぶ）。

3.4 動的認証を利用した IC カード認証

3.4.1 動的認証の種類

動的認証は、IC カード内部でリアルタイムに生成されたデータを利用する認証方式であり、IC カード内に格納される秘密鍵を認証者に提示することなく、当該秘密鍵が金融機関によって設定されたものか否かの検証を可能とする。

[12]侵入型攻撃の詳細については、情報処理振興事業協会［2000］、日本規格協会［2003］を参照。
[13]故障利用攻撃（fault attack または fault based attack）は、暗号処理中のモジュールに、放射線の照射、電圧の変化、クロック周波数の変化等の物理的影響を故意に与えることによって誤作動を生じさせ、誤動作による出力と正しい出力からモジュール内に格納される秘密鍵を不正に入手する攻撃である。
[14]サイドチャネル攻撃（side-channel attack）は、暗号処理の際に生じる消費電力、電磁波、処理時間といった暗号モジュールの正規の入出力データ以外の情報を利用して、秘密鍵を不正に入手する攻撃である。
[15]非侵入型攻撃の詳細についても、侵入型攻撃と同様に、情報処理振興事業協会［2000］や日本規格協会［2003］を参照。

動的認証では、時間情報や認証者が生成した乱数、および、カード所持者を特定するための情報（ユーザ ID）等に対して、IC カードが秘密鍵を用いた演算を実行し、演算結果を認証者に送信する[16]。認証者は、演算結果を検証し、金融機関が設定した正しい秘密鍵が当該 IC カードに格納されていることを確認することによって、当該 IC カードの真正性を確認するとともに、カード所持者の特定を行う。

動的認証はさまざまな観点から分類することができるが、まず、1 つの IC カード内の秘密鍵が漏洩した場合に他の IC カードにどのような影響が及ぶかを明確にするという目的から、次の 2 つの形態を検討対象とする。

個別鍵利用タイプ： IC カード内に格納される秘密鍵が IC カードごとに異なるという形態。

統一鍵利用タイプ： IC カード内に格納される秘密鍵がすべての IC カードにおいて同一であるという形態。

なお、上記の形態のほか、すべての IC カードではないが、一定のグループに属する IC カードの秘密鍵が同一に設定されるという形態も想定される。そうした形態において、例えば同一グループに属する IC カードが多く、1 つの IC カード内の秘密鍵漏洩によって無効化する必要が出てくる IC カードも多くなるといったケースは、上記の統一鍵利用タイプに対応するとみなすことができる。

動的認証の形態を分類する別の観点として、動的認証に採用する暗号技術に着目する。具体的には、共通鍵暗号を利用した動的認証と公開鍵暗号を利用した動的認証に分ける。各認証方式の持つ性質は以下のとおりである。

－ 共通鍵暗号を利用した動的認証　認証者（端末あるいはホスト）と IC カード間で共有される秘密鍵を利用し、通信相手が秘密鍵の共有者であることの確認によって認証を行う。IC カードは、時間情報や認証者から受信した乱数、および、ユーザ ID に対する暗号文を生成し、認証者はそれを復号して得た平文を検証することで相手を認証することができる。この場合、IC カードおよび認証者のいずれにおいても秘密鍵を用いた演算が実行される。また、MAC を利用して認証を行うケースもある。

認証者が、被認証者となり得るすべてのユーザの IC カードと秘密鍵を共有する手段としては、それらすべての秘密鍵を内部に格納しておくケースと、1 種類の秘密鍵（マスター鍵）を保持し、認証時において IC カードから送られるデータをもとに適宜 IC カードと共有する秘密鍵を生成するケースが考

[16] ユーザ ID を演算を行う関数への入力とせず、演算結果とは独立にユーザ ID を送信するといった方法もある。ただし、本節では、まず、動的認証によって IC カード認証を行うケースに焦点を当てて検討を行うこととする。

えられる。検証に利用するすべての秘密鍵を認証者が管理するケースでは、秘密鍵を一意に特定するための情報を別途送信する必要がある。

- **公開鍵暗号を利用した動的認証**　公開鍵暗号を利用する方式には、デジタル署名を利用するケースとゼロ知識証明を利用するケースがある。IC カードは、時間情報や認証者（端末あるいはホスト）から受信した乱数、および、ユーザ ID に対して秘密鍵を利用した演算を実行する。認証者は公開鍵を用いて IC カードによる演算結果を検証することで、当該公開鍵に対応する秘密鍵の保持を確認する。この場合、秘密鍵を用いた演算を実行するエンティティは IC カードのみである。

  IC カード内の秘密鍵に対応する公開鍵は、認証者が保持するケースと IC カード内に格納されるケースがある。後者のケースでは、当該公開鍵は公開鍵証明書の一部として格納され、公開鍵証明書が金融機関によって発行されたものであることを確認する必要がある。ルート認証局の公開鍵証明書は認証者が保持することとするほか、PKI については正しく構築されているとして議論を進める。また、検証に利用する複数の公開鍵を認証者が管理するケースでは、公開鍵を一意に特定するための情報を別途送信する必要がある。

例えば、EMV（EMVCo［2004a, b］）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動的認証が想定されている。

3.4.2　想定する攻撃

なりすましを行う手段として、3.3.1 節で整理したように、(1) 真正な端末やホストに対してなりすましを成功させるような偽造カードのみを作製する、(2) オフライン認証において、攻撃者が作製した偽造カードと整合性を持つように端末内に格納されるパラメータ（秘密鍵等）を改ざんするという 2 つを想定する。以下では、これらの攻撃についてそれぞれ検討を行う（図 5 参照）。

(1) 偽造カードのみを作製する攻撃

動的認証における偽造カードとしては、(A) 偽造対象カードと同一の秘密鍵を格納する IC カードと、(B) 秘密鍵を持たずとも真正な IC カードと同じふるまいが実行可能な IC カードがある。こうした偽造カードを作製するための具体的な攻撃手段としては、上記 (A) については、偽造対象カードおよび同じ秘密鍵を有するエンティティ（表 2 参照）から秘密鍵を盗取することが考えられるほか、上記 (B) については、動的認証方式の脆弱性を利用して、偽造カードの作製に必要となる

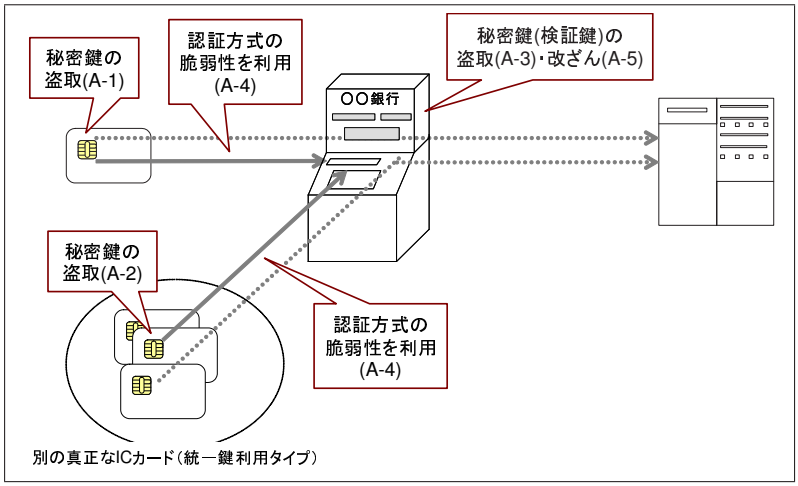

図 5: 動的認証において想定される攻撃（概念図）

認証形態			エンティティ		
			端末	ホスト	別の IC カード
個別鍵利用タイプ	オフライン	共通鍵暗号	秘密鍵		
		公開鍵暗号			
	オンライン	共通鍵暗号		秘密鍵	
		公開鍵暗号			
統一鍵利用タイプ	オフライン	共通鍵暗号	秘密鍵		秘密鍵
		公開鍵暗号			秘密鍵
	オンライン	共通鍵暗号		秘密鍵	秘密鍵
		公開鍵暗号			秘密鍵

表 2: 秘密鍵の保管場所

データを収集することとなる。ここで、偽造カードの作製に必要となるユーザ ID といった IC カードに固有の秘密鍵以外のデータについては、攻撃者は既に入手しているものと仮定する。

偽造カードの作製に必要となる情報の収集先としては、(1)IC カード、(2) 端末、(3)IC カード・端末間、あるいは、端末・ホスト間の通信路が挙げられる。ホストは安全に管理されることを仮定しているため、ホストに対する攻撃については想定しない。以下に、これらエンティティに対して想定される攻撃を列挙する。

- **IC カード内のデータを利用した攻撃：** 個別鍵利用タイプと統一鍵利用タイプのいずれにおいても、攻撃者が偽造対象カードに接触することができるのは、カード所持者に気付かれずに当該 IC カードを不正操作[17]している時間、お

[17]IC カードが端末と無線通信を行うケースでは、カード所持者が気付かないうちに、攻撃モジュールによって IC カード内部のデータが盗取される可能性もある。こうした状況も、ここでの「不正操作」に含めることとする。

よび、カード所持者が金融取引を実行している時間（IC カードが端末と通信を行っている時間）のみである。統一鍵利用タイプにおいては、攻撃者が何らかの手段で偽造対象カードと同じ秘密鍵を有する別の真正な IC カードを入手することができれば、そのカードを攻撃に利用することができる。そのため、個別鍵利用タイプと比べて、相対的に長い時間をかけて攻撃を実行可能であることが想定される。

IC カードに対して想定される具体的な攻撃は以下のとおりである。

- 攻撃 A-1： 個別鍵利用タイプにおいて、不正・偽端末や攻撃モジュールの利用により、偽造対象カードから動的認証に利用する秘密鍵を盗取することで偽造カードを作製する。
- 攻撃 A-2： 統一鍵利用タイプにおいて、不正・偽端末や攻撃モジュールの利用により、偽造対象カード、あるいは、それ以外の真正な IC カードから盗取した動的認証に利用する秘密鍵を利用して偽造カードを作製する。あるいは、偽造対象カード以外の真正な IC カードのユーザ ID を書き換えることで偽造カードを作製する。

・端末内のデータを利用した攻撃： 表 2 に示したように、共通鍵暗号を利用したオフライン認証では、端末に偽造対象カードが認証に利用するものと同じ秘密鍵が格納されるため、以下の攻撃が想定される。

- 攻撃 A-3： 共通鍵暗号を利用したオフライン認証において、攻撃モジュールの利用により端末から偽造対象カードと共有する秘密鍵を盗取することで偽造カードを作製する。

・通信路上のデータを利用した攻撃： 攻撃 A-1〜3 は、各エンティティから直接秘密鍵を盗取すること、あるいは、ユーザ ID を改ざんすることで偽造カードを作製する攻撃であるが、動的認証方式の脆弱性を利用して偽造カードの作製が可能になるおそれもある。動的認証方式の脆弱性とは、真正な端末、不正端末、ホストと IC カードの間での認証プロトコルの実行中に送受信されるデータを利用してなりすましが可能となることを指す。こうした脆弱性を利用した攻撃として、例えば、通信データから IC カードの秘密鍵を効率的に推定するといった攻撃や、送受信されるデータそのものを利用する攻撃

（リプレイ攻撃[18]、インターリービング攻撃[19]、マフィア・フロード[20]等）が挙げられる。こうした攻撃を動的認証方式への攻撃として以下に挙げる。

― 攻撃 A-4： IC カード認証に利用される動的認証方式の脆弱性を利用することにより、偽造対象カードの秘密鍵を推定して偽造カードを作製する、あるいは、秘密鍵を盗取せずともなりすましを可能とする偽造カードを作製する。

(2) 偽造カードの作製と端末内部のデータ改ざんによる攻撃

オフライン認証では、IC カードが提示するデータと、端末内部にあらかじめ格納されているデータとの整合性を確認する。つまり、共通鍵暗号を利用した方式では IC カードと共有される秘密鍵、公開鍵暗号を利用した方式では少なくともルート認証局の公開鍵証明書が端末内に格納されており、これらのデータ（以下、検証鍵と呼ぶ）を利用して検証が行われる。したがって、攻撃者が適当に設定したデータを秘密鍵として格納する IC カードを偽造するとともに、侵入型攻撃等によって当該秘密鍵と整合性を持つように端末内部の検証鍵を改ざんすることでなりすましを行うことが可能である。以下に、これを攻撃 A-5 として挙げる。

― 攻撃 A-5： オフライン認証において、偽造カードを作製するとともに、端末内部に格納されている検証鍵を偽造カードと整合性を持つように改ざんする。

各動的認証方式において適用可能であると想定される上記攻撃については、表 3 にまとめた。

3.4.3 想定する攻撃に対する対策

想定した攻撃への対策には、以下が挙げられる。

[18] リプレイ攻撃（replay attack）は、過去に実行された 1 回の認証プロトコルで送受信されたデータをそのまま利用してなりすましを試みる攻撃である。

[19] インターリービング攻撃（interleaving attack）は、実行中、あるいは、過去に実行された複数の認証プロトコルで送受信されたデータを利用してなりすましを試みる攻撃である。入手するデータは、攻撃者自身が実行したプロトコルから得られる情報も含まれる。

[20] マフィア・フロード（mafia fraud、Beth and Desmedt［1991］）は、不正・偽端末の設置や攻撃モジュールを利用して、偽造対象カードからの通信データを偽造カードに転送させることにより、真正な端末に対してなりすましを試みる攻撃である。マフィア・フロードに対しては、認証者・被認証者間でのデータの送受信に係る遅延時間を利用して、IC カード・端末間の距離を測定することで当該攻撃を回避する対策法が提案されている（Brands and Chaum［1994］、Lemke, Sadeghi and Stuble［2005］）。そのほか、人工物メトリクスを利用する（松本・青柳［2005］）ことによって偽造カードを排除するといった対策も有効であると考えられる。

動的認証方式の形態			想定される攻撃				
			A-1	A-2	A-3	A-4	A-5
個別鍵利用タイプ	オフライン	共通鍵暗号	○		○	○	○
		公開鍵暗号	○			○	○
	オンライン	共通鍵暗号	○			○	
		公開鍵暗号	○			○	
統一鍵利用タイプ	オフライン	共通鍵暗号		○	○	○	○
		公開鍵暗号		○		○	○
	オンライン	共通鍵暗号		○		○	
		公開鍵暗号		○		○	

表 3: 各動的認証方式において想定される攻撃

— 攻撃 A-1、A-2 に対する対策 (I)： IC カードに当該攻撃に対する防御技術を組み込むことで、秘密鍵の漏洩および内部データの改ざんを防ぐ。

— 攻撃 A-1、A-2 に対する対策 (II)： 当該攻撃を検知し、金融機関に異常を知らせる機構を IC カードに組み込むことで、偽造カードの不正利用を防ぐ。

— 攻撃 A-1、A-2 に対する対策 (III)： 当該攻撃を検知し、内部に格納される秘密鍵を自動的に消去する機構等を IC カードに組み込むことで、秘密鍵の漏洩を防ぐ。

— 攻撃 A-3 に対する対策 (I)： 端末に当該攻撃に対する防御技術を組み込むことで、秘密鍵が漏洩するのを防ぐ。

— 攻撃 A-3 に対する対策 (II)： 当該攻撃を検知し、金融機関に異常を知らせる機構を端末に組み込むことで、偽造カードの不正利用を防ぐ。

— 攻撃 A-3 に対する対策 (III)： 当該攻撃を検知し、内部に格納される秘密鍵を自動的に消去する機構等を端末に組み込むことで、秘密鍵の漏洩を防ぐ。

— 攻撃 A-4 に対する対策： 既存の攻撃法に対して安全と評価されている動的認証方式を利用することで、エンティティ間で通信されるデータを利用して偽造カードの作製が可能となることを防ぐ。

— 攻撃 A-5 に対する対策 (I)： 端末に当該攻撃に対する防御技術を組み込むことで、検証鍵が改ざんされるのを防ぐ。

— 攻撃 A-5 に対する対策 (II)： 当該攻撃を検知し、金融機関に異常を知らせる機構を端末に組み込むことで、偽造カードの不正利用を防ぐ。

— 攻撃 A-5 に対する対策 (III)： 当該攻撃を検知し、内部に格納されるデータを自動的に消去する機構等を端末に組み込むことで、検証鍵が改ざんされるのを防ぐ。

攻撃 A-1〜3 に対する対策としては、(1) 秘密鍵の漏洩を防ぐことで偽造カードの作製を防止する方法と、(2) 作製された偽造カードの利用を防止する方法が考えられる。上記 (1) については、当該攻撃を防御する受動的対策（攻撃 A-1、A-2 に対する対策 (I)、攻撃 A-3 に対する対策 (I)）と、攻撃を検知し秘密鍵を自動的に消去するといった能動的対策（攻撃 A-1、A-2 に対する対策 (III)、攻撃 A-3 に対する対策 (III)）が考えられる[21]。上記 (2) については、たとえ侵入型攻撃や非侵入型攻撃によって内部の秘密鍵が漏洩してしまったとしても、金融機関によってその事実が把握され、速やかに当該秘密鍵に対応する IC カードを無効化することができれば、当該秘密鍵を格納した偽造カードを利用して金融取引を実行することを困難にする対策が考えられる（攻撃 A-1、A-2 に対する対策 (II)、攻撃 A-3 に対する対策 (II)）。

攻撃 A-5 に対しては、端末内の検証鍵の改ざんを防止する、あるいは、検知するという方法が考えられ、攻撃 A-1〜3 と同様の対策が適用できる。

ただし、統一鍵利用タイプの攻撃 A-2、および、A-3、A-5 に対して、攻撃の検知を金融機関に知らせるといった対策を採用した場合において、実際に攻撃が検知された際には、すべての IC カードを無効化することが必要となる。本対策を採用するか否かは、無効化によって損なわれるユーザの利便性、および、すべての IC カードの無効化・再発行を含めた一連の処理に必要となるコストを、他の対策（攻撃の防御技術や鍵の自動消去機能の採用）に必要なコストと比較したうえで決定することになる。

3.4.4 セキュリティ要件

以上の考察により、動的認証を利用した IC カード認証におけるセキュリティ要件として以下の 7 項目を挙げることができる。各認証方式に対応するセキュリティ要件については表 4 にまとめている。

D-1. IC カードは、侵入型攻撃および非侵入型攻撃に対してタンパー・レジスタンス[22]であること。

D-2. IC カードは、侵入型攻撃および非侵入型攻撃を検知して金融機関に異常を速やかに知らせること。

---

[21] 攻撃 A-1、A-2 に対しては、IC カード認証の前にまず動的認証等によって端末の真正性を認証することで攻撃を防御するといった対策も考えられる。この場合、端末認証によって偽端末や攻撃モジュールを排除することは可能であるが、真正な端末に細工が加えられた不正端末をも排除することは困難であると考えられる。

[22] タンパー・レジスタンス（tamper resistance）は、デバイスを特殊なシールドによってコーティングする等、外部からの攻撃に対して秘密情報を漏らさないようにするための受動的な対抗策を有するというデバイスの特性を指す（ISO［1998］）。

D-3. IC カードは、侵入型攻撃および非侵入型攻撃に対してタンパー・レスポンス[23]であること。

D-4. 端末は、侵入型攻撃および非侵入型攻撃に対してタンパー・レジスタンスであること。

D-5. 端末は、侵入型攻撃および非侵入型攻撃を検知して金融機関に異常を知らせること。

D-6. 端末は、侵入型攻撃および非侵入型攻撃に対してタンパー・レスポンスであること。

D-7. 当該システムにおいて採用される動的認証方式は、想定される攻撃に対して安全であると評価されていること。

端末内部のデータを改ざんする攻撃 A-5 は侵入型攻撃であるが、セキュリティ要件を整理するにあたり、侵入型攻撃と非侵入型攻撃の両方に対して対策を講じることを内容とする要件 D-4〜6 に集約する扱いとした。また、セキュリティ要件 D-1〜3、および、D-4〜6 に関しては、それぞれの対策のいずれかを適用すれば攻撃を防ぐことができるが、それぞれを完全に実現することが困難である場合には、複数の対策法を施すことが望ましい。

動的認証方式の形態			セキュリティ要件		
			D-1 ∨ 2 ∨ 3	D-4 ∨ 5 ∨ 6	D-7
個別鍵利用タイプ	オフライン	共通鍵暗号	○	○	○
		公開鍵暗号	○	○	○
	オンライン	共通鍵暗号	○		○
		公開鍵暗号	○		○
統一鍵利用タイプ	オフライン	共通鍵暗号	○	○	○
		公開鍵暗号	○	○	○
	オンライン	共通鍵暗号	○		○
		公開鍵暗号	○		○

備考：“ ∨ ”は、“ または ”を表すこととする。例えば、“ D-1∨2∨3 ”は、“ D-1 または D-2 または D-3 ”を表す。また、各認証方式については、“ ○ ”が付いている要件をすべて満足することが求められる。

表 4: 各動的認証方式におけるセキュリティ要件

[23]タンパー・レスポンス（tamper response）は、デバイスへの侵入、変更が行われようとした場合、あるいは、操作環境からデバイスが取り外された場合等に、内部の秘密情報等を即座に自動的に消去する等、外部からの物理的手段による攻撃に対して能動的に対抗する機能を有するというデバイスの特性を指す（ISO［1998］）。

3.5 静的認証を利用したICカード認証

3.5.1 静的認証の種類

静的認証では、ICチップ内に格納されるデータそのものを認証者に提示することで、当該データが金融機関に生成されたものか否かを検証する。動的認証と大きく異なる点は、ICカードは演算を実行せず、毎回同じデータを認証に利用することである。以下では、静的認証の際にICカードが送信するデータを静的認証データと呼ぶ。

ICカードが提示する静的認証データが金融機関によって生成されたものであり、その一貫性が保たれていることを確認する手段としては、(1) 認証者が静的認証データそのものをデータベースに保管する必要のないものと (2) 保管する必要があるものの2つが考えられる。上記 (1) は、MACやデジタル署名を利用して実現可能であり、秘密鍵をパラメータとする関数（以下、認証子生成関数と呼ぶ）にユーザID等を入力して得た値を静的認証データとして利用する[24]。一方、上記 (2) は、認証子生成関数を利用せず、静的認証データがデータベースに登録されているものと一致するか否かを確認する方法である。ただし、静的認証データの生成には、公開されている情報から出力値の推測が困難となる変換アルゴリズムを利用する形態を想定する[25]。

ICカード内に格納される静的認証データの形態は、認証子生成関数を利用して生成されたものか否か、また、利用する関数（パラメータとなる秘密鍵）がICカードごとに異なるか否かによって以下の3つのケースに分類できる。

個別関数利用タイプ： 静的認証データの生成に利用する認証子生成関数がICカードごとに異なるという形態。

統一関数利用タイプ： 静的認証データの生成に利用する認証子生成関数がすべて同じであるという形態。

データベース利用タイプ： 静的認証データの生成に認証子生成関数を利用しないという形態。

個別関数利用タイプと統一関数利用タイプにおける静的認証データの生成方法としては、以下に挙げるMACやデジタル署名を利用することが考えられる。

---

[24] ユーザIDを認証子生成関数への入力とせず、MACやデジタル署名とは独立にユーザIDを送信するといった方法もある。ただし、本節では、まず、MACやデジタル署名を静的認証データとして扱う場合に焦点を当てて検討を行うこととする。

[25] 出力値の推測が容易である場合には偽造カードの作製が容易であるため、ここではそうした構造とはなっていないものとする。

- **MAC を利用した静的認証**　IC カード内には、金融機関がユーザ ID 等のデータに対して生成した MAC があらかじめ格納されている。認証者（端末あるいはホスト）は、MAC 生成に利用したものと同一の秘密鍵を用いて IC カードが提示する MAC を検証することで、IC カードが金融機関によって発行されたものであるか否かを判断するとともに、カード所持者を特定する。

  認証者が、被認証者となり得るすべてのユーザの IC カードに対応する秘密鍵を利用する手段としては、それらすべての秘密鍵を内部に格納しておくケースと、1 種類の秘密鍵（マスター鍵）を保持し、認証時において IC カードから送られるデータをもとに検証鍵となる秘密鍵を生成するケースが考えられる。検証に利用するすべての秘密鍵を認証者が管理するケースでは、秘密鍵を一意に特定するための情報を別途送信する必要がある。

- **デジタル署名を利用した静的認証**　IC カード内には、金融機関がユーザ ID 等のデータに対して生成したデジタル署名があらかじめ格納されている。認証者は、金融機関の公開鍵を用いてデジタル署名を検証することで、当該 IC カードが金融機関によって発行されたものであるか否かを確認する。デジタル署名を利用した静的認証の場合、いずれのエンティティも認証時に秘密鍵を用いた演算を実行することはない。

  本認証方式では、デジタル署名検証のほか、金融機関の公開鍵証明書を検証することも必要である。特に、個別関数利用タイプの場合、各 IC カードに対応する秘密鍵および公開鍵が準備されることから、各 IC カードに対応する公開鍵証明書の検証も認証者側で必要となる。署名検証の際に必要となる公開鍵証明書の格納先については、認証者あるいは IC カード内が考えられる。ただし、ルート認証局の公開鍵証明書は認証者が保持することとするほか、以下では、PKI については正しく構築されているとして議論を進める。また、検証に利用するすべての公開鍵証明書を認証者が管理するケースでは、公開鍵証明書を一意に特定するための情報を別途送信する必要がある。

例えば、EMV（EMVCo［2004a, b］）では、静的認証の形態として、デジタル署名を利用したオフラインでの静的認証を想定している。

3.5.2　想定する攻撃

静的認証においてなりすましを行う手段としては、動的認証の場合と同様、3.3.1 節で整理したように、(1) 真正な端末やホストに対してなりすましを成功させるような偽造カードのみを作製する方法と、(2) オフライン認証において、攻撃者が適当に設定した静的認証データを格納する偽造カードと整合性を持つように端末内

に格納されるパラメータ（検証鍵等）を改ざんする方法が挙げられる。上記 (1) の具体的な手法としては、偽造対象カード内の静的認証データを入手し偽造カードを作製する、あるいは、偽造対象カード内の静的認証データを生成するための秘密鍵を入手し偽造カードを作製することが考えられる。

以下では、これらの攻撃についてそれぞれ検討を行う（図 6 参照）。

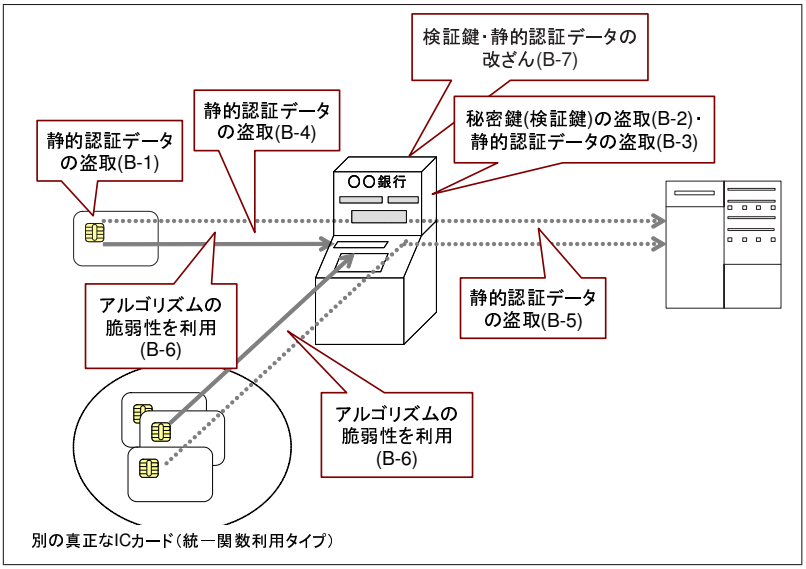

図 6: 静的認証において想定される攻撃（概念図）

(1) 偽造カードのみを作製する攻撃

静的認証では、偽造対象カード内に格納される静的認証データが入手できれば偽造カードを作製可能である。そのほか、MAC を利用した静的認証では、MAC の検証鍵が秘密鍵に対応するため、認証者から秘密鍵を盗取したうえで MAC を偽造することも考えられる。この場合、ユーザ ID を含む MAC の対象となるメッセージも入手する必要があるが、攻撃者はこれらの情報をすでに入手していることを仮定して議論を進める。

静的認証データ、あるいは、それを生成するための情報を格納するエンティティとそのデータの種類は表 5 のとおりである。

以下に、静的認証データ、あるいは、MAC を生成するための秘密鍵を入手する方法として考えられる攻撃を列挙する。また、前節と同様、将来において実行可能となりうる攻撃についても想定される脅威として挙げている。

- **IC カード内のデータを利用した攻撃：** 偽造対象カードから静的認証データの盗取を試みることができるのは、カード所持者に気付かれずに当該 IC カー

認証形態			エンティティ	
			端末	ホスト
個別関数利用タイプ	オフライン	MAC	秘密鍵	
		デジタル署名		
	オンライン	MAC		秘密鍵
		デジタル署名		
統一関数利用タイプ	オフライン	MAC	秘密鍵	
		デジタル署名		
	オンライン	MAC		秘密鍵
		デジタル署名		
データベース利用タイプ	オフライン		静的認証データ	
	オンライン			静的認証データ

表 5: 秘密鍵または静的認証データの保管場所

ドを不正操作する時間、および、カード所持者が金融取引を実行している時間のみである。静的認証データは、カード・リーダからの正しいリード・コマンドに対して出力されるため、動的認証における秘密鍵のように侵入型攻撃や非侵入型攻撃を実行せずとも、比較的容易に盗取が可能であることが想定される。想定される具体的な攻撃は以下のとおりである。

— 攻撃 B-1： 不正・偽端末や攻撃モジュールが真正な端末になりすまして、偽造対象カードから静的認証データを不正に出力させて盗取することで偽造カードを作製する。

・端末内のデータを利用した攻撃： 表 5 に示したように、端末は、MAC を利用した場合のオフライン認証において検証鍵を格納するほか、データベース利用タイプのオフライン認証では静的認証データそのものを格納する。そこで、攻撃者は以下の手段によって端末からそれらを不正入手しようと試みることが可能である。なお、ホストは安全に管理されることを想定しているため、ホストに格納されるデータを盗取するといった攻撃については想定しない。

— 攻撃 B-2： MAC を利用したオフライン静的認証において、攻撃モジュールの利用により、偽造対象カード内に格納される静的認証データの検証鍵を端末から盗取することで偽造カードを作製する。

— 攻撃 B-3： データベース利用タイプのオフライン静的認証において、攻撃モジュールの利用により、偽造対象カード内に格納される静的認証データを端末から盗取することで偽造カードを作製する。

・通信路上のデータを利用した攻撃： 静的認証データを入手する方法としては、攻撃 B-1〜3 のように、エンティティ内からデータを盗取するほか、通信路

の盗聴により不正入手することも考えられる。また、MAC やデジタル署名方式を利用した静的認証において、静的認証データを生成するアルゴリズムが脆弱[26]であった場合、別の IC カード内に格納される静的認証データ等から意図するデータの生成が可能となるおそれがある。これらを静的認証方式に対する攻撃として以下に挙げる。

- 攻撃 B-4： 偽造対象カード・端末間の通信路の盗聴により静的認証データを入手することで偽造カードを作製する。
- 攻撃 B-5： オンライン静的認証において、偽ホストの設置、あるいは、端末・ホスト間の通信路の盗聴により IC カードから送信される静的認証データを入手することで偽造カードを作製する。
- 攻撃 B-6： 静的認証データを生成するアルゴリズムの脆弱性を利用して偽造カードを作製する。

攻撃 B-4、B-5 への対策としては、データの送信先となるエンティティの真正性を確認するとともに、IC カード・端末間、および、端末・ホスト間の通信路の盗聴によるデータの漏洩を防止するための機構を採用することが考えられる[27]。

(2) 偽造カードの作製と端末内部のデータ改ざんによる攻撃

オフライン認証では、攻撃者が生成した偽造カードと整合性を持つように端末を不正操作することでなりすましを実行する攻撃が可能である。MAC あるいはデジタル署名を利用した方式では、攻撃者が適当に生成したデータを秘密鍵として静的認証データを生成し、それと整合性を持つように端末内の検証鍵を改ざんすることでなりすましが成功する。一方、認証子生成関数を利用しない方式では、端末の静的認証データを、攻撃者が適当に生成したものに改ざんできればよい。これらを攻撃 B-7 として以下に挙げる。

- 攻撃 B-7： オフライン認証において、偽造カードを作製するとともに、端末内部に格納されている検証鍵あるいは静的認証データを、偽造カードと整合性を持つように改ざんする。

各静的認証方式において適用可能であると想定される攻撃を表 6 にまとめた。

[26]データベース利用タイプにおいては、静的認証データの推測が容易となるアルゴリズムを脆弱であると呼ぶ。

[27]そうした機構として静的認証データを暗号化するという方法も考えられるが、リプレイ攻撃等を回避するためには、暗号化された静的認証データが認証の都度ランダムに変化するようにしておくことが必要となり、結局は動的認証となってしまうこととなる。

静的認証方式の形態			想定される攻撃						
			B-1	B-2	B-3	B-4	B-5	B-6	B-7
個別関数利用タイプ	オフライン	MAC	○	○		○		○	○
		デジタル署名	○			○		○	○
	オンライン	MAC	○			○	○	○	
		デジタル署名	○			○	○	○	
統一関数利用タイプ	オフライン	MAC	○	○		○		○	○
		デジタル署名	○			○		○	○
	オンライン	MAC	○			○	○	○	
		デジタル署名	○			○	○	○	
データベース利用タイプ	オフライン		○		○	○		○	○
	オンライン		○			○	○	○	

表 6: 各静的認証方式において想定される攻撃

3.5.3 想定する攻撃に対する対策

以上で想定した攻撃への対策には、以下が挙げられる。

- 攻撃 B-1 に対する対策： 被認証者および IC カードによって、端末が真正なものであることを確認できるようにすることで、静的認証データの漏洩を防止する。
- 攻撃 B-2、B-3 に対する対策 (I)： 端末に当該攻撃に対する防御技術を組み込むことで、検証鍵、あるいは、静的認証データが漏洩するのを防ぐ。
- 攻撃 B-2、B-3 に対する対策 (II)： 当該攻撃を検知し、金融機関に異常を知らせる機構を端末に組み込むことで、偽造カードの不正利用を防ぐ。
- 攻撃 B-2、B-3 に対する対策 (III)： 当該攻撃を検知し、内部に格納されるデータを自動的に消去する機構を端末に組み込むことで、検証鍵、あるいは、静的認証データの漏洩を防ぐ。
- 攻撃 B-4 に対する対策： IC カード・端末間の通信路の盗聴を防止するための機構を採用することで、静的認証データの漏洩を防ぐ。
- 攻撃 B-5 に対する対策 (I)： 端末・ホスト間の通信路の盗聴を防止するための機構を採用することで、静的認証データの漏洩を防ぐ。
- 攻撃 B-5 に対する対策 (II)： 偽ホストへのデータ漏洩を防止するための機構を採用することで、静的認証データの漏洩を防ぐ。
- 攻撃 B-6 に対する対策： 既存の攻撃法に対して安全な静的認証データ生成アルゴリズムを利用することで、偽造カードの作製が可能となることを防ぐ。
- 攻撃 B-7 に対する対策 (I)： 端末に当該攻撃に対する防御技術を組み込むことで、検証鍵、あるいは、静的認証データが改ざんされるのを防ぐ。

— 攻撃 B-7 に対する対策 (II)： 当該攻撃を検知し、金融機関に異常を知らせる機構を端末に組み込むことで、偽造カードの不正利用を防ぐ。

— 攻撃 B-7 に対する対策 (III)： 当該攻撃を検知し、内部に格納されるデータを自動的に消去する機構を端末に組み込むことで、検証鍵、あるいは、静的認証データが改ざんされるのを防ぐ。

攻撃 B-1 については、静的認証データの提示前に端末の真正性を確認できれば当該攻撃を防ぐことができる。IC カードによる端末認証を採用した場合[28]、偽端末や攻撃モジュールへの静的認証データの漏洩は防止可能であるが、真正な端末に攻撃モジュールが組み込まれた不正端末の検知は困難であることから、IC カードによる端末認証等の手法の適用には限界がある。また、IC カードの提示前に、カード所持者によって不正端末を検知することが考えられるが、カード所持者による端末の真正性確認が困難なケース（攻撃モジュールを利用して、カード所持者に気付かれずに攻撃 B-1 を実行するケース）では、攻撃 B-1 を防止・検知することは困難である。よって、カード所持者による端末の真正性を確認可能とする仕組みに加えて、そうした真正性確認が困難な場合の備えとして、偽端末や攻撃モジュールの検知を可能とする機構を IC カードに付与することも必要となる。

攻撃 B-2、B-3 については、端末内部のデータ漏洩を防ぐことで偽造カードの作製を防止する対策（攻撃 B-2、B-3 への対策 (I、III)）と、攻撃を検知し当該データを格納する IC カードを無効化することによって、作製された偽造カードの利用を防止するといった対策（攻撃 B-2、B-3 への対策 (II)）が考えられる。また、攻撃 B-7 に対しても同様の対策によって端末の内部データの改ざん等を防ぐことができると考えられる。

ただし、攻撃 B-2、B-3、B-7 に対して、攻撃の検知を金融機関に知らせるといった対策を採用した場合において、実際に攻撃が検知された際には、すべての IC カードを無効化することが必要となる[29]。したがって、こうした対策を採用するか否かは、IC カードの無効化によって損なわれるユーザの利便性、および、IC カードの無効化・再発行を含めた一連の処理に必要となるコストを、他の対策（攻撃の防御あるいは検知を行う技術の採用）に必要なコストと比較して決定することとなる。

[28]静的認証が実装される IC カードは、計算能力が限られている状況が想定されるため、端末認証等の高度な計算処理を必要とする対策が適当でないことが多い。

[29]MAC を利用する方式、および、データベース利用タイプでは、被認証者となりうる複数の IC カードの検証鍵や静的認証データがリストとして格納されることが想定されるため、攻撃 B-2 や B-3 が実行された場合にはリスト内のすべての検証鍵や静的認証データが同時に漏洩した可能性が考えられる。そのほか、攻撃 B-7 が実行された場合にはすべての検証鍵や静的認証データが改ざんされた可能性も考えられる。

3.5.4　セキュリティ要件

以上の考察により、静的認証を利用したICカード認証におけるセキュリティ要件として、以下の7項目を挙げることができる。各認証方式に対応するセキュリティ要件については表7にまとめている。

S-1. カード所持者とICカードによって端末の真正性を確認可能であること。

S-2. 端末は、侵入型攻撃および非侵入型攻撃に対してタンパー・レジスタンスであること。

S-3. 端末は、侵入型攻撃および非侵入型攻撃を検知して金融機関に異常を速やかに知らせること。

S-4. 端末は、侵入型攻撃および非侵入型攻撃に対してタンパー・レスポンスであること。

S-5. ICカード・端末間の通信路上のデータが漏洩しないこと。

S-6. 端末・ホスト間の通信路上のデータが漏洩しないこと、および、偽ホストへデータが漏洩しないこと。

S-7. 当該システムにおいて採用されている静的認証データの生成アルゴリズムは、想定される攻撃に対して安全であると評価されていること。

端末内部のデータを改ざんする攻撃B-7は侵入型攻撃であるが、セキュリティ要件を整理するにあたり、侵入型攻撃と非侵入型攻撃の両方に対して対策を講じることを内容とする要件S-2〜4に集約する扱いとした。

動的認証の場合と同様、セキュリティ要件S-2〜4に関しては、それぞれの対策のいずれかを適用することで当該攻撃を防御できると考えられるが、一般には、複数の対策法を適用することが望ましい。

3.6　ICカード認証のセキュリティ要件に関する考察

3.6.1　動的認証における各認証方式の違い

3.4節では、動的認証の形態を8つに分類したうえで、それぞれに求められるセキュリティ要件を導出した。

その結果、まず、秘密鍵がICカードごとに異なる個別鍵利用タイプと、秘密鍵がすべてのICカードで同一である統一鍵利用タイプの間でセキュリティ要件の比較を行うと、例えば攻撃A-1とA-2のように攻撃の対象となるエンティティや攻撃の手段は異なるものの、求められるセキュリティ要件は同一となることがわかる。

静的認証方式の形態			セキュリティ要件				
			S-1	S-2 ∨ 3 ∨ 4	S-5	S-6	S-7
個別関数利用タイプ	オフライン	MAC	○	○	○		○
		デジタル署名	○	○	○		○
	オンライン	MAC	○		○	○	○
		デジタル署名	○		○	○	○
統一関数利用タイプ	オフライン	MAC	○	○	○		○
		デジタル署名	○	○	○		○
	オンライン	MAC	○		○	○	○
		デジタル署名	○		○	○	○
データベース利用タイプ	オフライン		○	○	○		○
	オンライン		○		○	○	○

備考：“ ∨ ”は、“ または ”を表すこととする。また、各認証方式については、“ ○ ”が付いている要件をすべて満足することが求められる。

表 7: 各静的認証方式におけるセキュリティ要件

ただし、セキュリティ要件 D-1〜3 のうち、D-2 によって IC カード内に格納される秘密鍵の漏洩を防止する場合において、実際に攻撃が検知された際には、統一鍵利用タイプでは当該秘密鍵を格納するすべての IC カードを無効化する必要がある。したがって、無効化によって損なわれるユーザの利便性や IC カードの無効化・再発行を含めた一連の処理にかかるコストは、個別鍵利用タイプより大きくなるという点に注意が必要である。

また、オフライン認証とオンライン認証におけるセキュリティ要件を比較すると、オフライン認証においては、共通鍵暗号、公開鍵暗号のいずれを採用した場合でも、端末内に格納される検証鍵が改ざんされると偽造カードの利用が可能となってしまうため、端末に関するセキュリティ要件 D-4〜6 の少なくとも 1 つを満たすことがオンライン認証の場合と比べて追加的に必要となることがわかる。また、オフライン認証において公開鍵暗号を利用する場合には、少なくともルート認証局の公開鍵証明書の改ざん（攻撃 A-5）を防御する必要があるのに対し、共通鍵暗号を利用した場合には、秘密鍵の漏洩（攻撃 A-3）と改ざん（攻撃 A-5）の両方を防御する必要があることもわかる。

3.6.2 静的認証における各認証方式の違い

3.5 節では、静的認証の形態を、認証子生成関数が IC カードごとに異なる個別関数利用タイプ、認証子生成関数がすべての IC カードで同じとなる統一関数利用タイプ、認証子生成関数を利用しないデータベース利用タイプの 3 つに分けるとともに、認証子生成関数の種類とオフライン／オンライン認証の差異も考慮し、全体で 10 種類に分類してセキュリティ要件を導出した。

まず、個別関数利用タイプと統一関数利用タイプとの間でセキュリティ要件の

比較を行うと、いずれもセキュリティ要件が同一となるほか、認証子生成関数として MAC を利用する方式とデジタル署名を利用する方式との間においても、セキュリティ要件が同一となることがわかる。

オフライン認証あるいはオンライン認証という軸を固定すると、個別関数利用タイプと統一関数利用タイプのセキュリティ要件は、いずれも、データベース利用タイプのセキュリティ要件と同一となることがわかる。

また、オフライン認証とオンライン認証のセキュリティ要件を比較すると、オフライン認証においては、端末内に格納される検証鍵あるいは静的認証データが改ざんされると偽造カードの作製が可能となるため、端末に関するセキュリティ要件 S-2〜4 の少なくとも 1 つを満たすことが、オンライン認証に比べて追加的に必要となることがわかる。さらに、オフライン認証における端末に対するセキュリティ要件については、デジタル署名を利用する場合にはルート認証局の公開鍵証明書の改ざん（攻撃 B-7）のみを防御する必要があるのに対し、その他の形態では、内部データ（検証鍵、静的認証データ）の漏洩（攻撃 B-2、B-3）と改ざん（攻撃 B-7）の両方を防御する必要があることがわかる。一方、オンライン認証においては、偽ホストへの静的認証データの漏洩、および、端末・ホスト間の通信路上でのデータ漏洩を防ぐためのセキュリティ要件 S-6 が、オフライン認証に比べて追加的に必要となることもわかる。

3.6.3 動的認証と静的認証におけるセキュリティ要件の違い

動的認証では秘密鍵を認証者に送信することなくその保持を証明するのに対し、静的認証では静的認証データそのものを認証者に送る。そのため、偽造カードの作製を可能とする情報を入手するための攻撃対象やその手法が異なることとなる。

動的認証には、IC カードや端末から秘密鍵を盗取するための侵入型攻撃や非侵入型攻撃に対するセキュリティ要件（セキュリティ要件 D-1〜6）が求められる。これに対し、静的認証では、端末に求められるセキュリティ要件は同一であるものの、IC カードに求められるセキュリティ要件が異なる。静的認証では、静的認証データを当該 IC カードからリード・コマンドによって正規の出力チャネルから比較的容易に入手可能であると考えられるほか、端末や通信路からも盗取を試みることが可能であることから、侵入型攻撃や非侵入型攻撃への対策ではなく、IC カードとカード所持者による端末の真正性の確認（セキュリティ要件 S-1）、および、通信路上のデータ保護（セキュリティ要件 S-5、6）が必要であるためである。

4　PINによる知識認証におけるセキュリティ要件

4.1　PIN認証の機能と定義

被認証者によって主張された身元と対応付けされ、金融機関に登録されるPINを提示できるユーザを本人であるとする知識認証が本人認証を行う手段として有効に機能するためには、以下の条件が満足されることが求められる[30]。

> **条件1** PINに対応付けされて金融機関に登録されるユーザ以外による、当該PINの不正使用を防止可能であること。
>
> **条件2** 被認証者によって提示されたPINが、金融機関に登録されたデータに対応するものであるか否かを確認可能であること。

PINによる知識認証は、PINが第三者に漏洩した場合には本人認証の手段として有効に機能しない。そのため、PINに対応するユーザ以外によって当該PINが提示される場合には、その利用を防止できる機構が別途必要となる（条件1)。そのような機構としては、別の認証手段等を組み合わせるケースが一般的である。しかし、条件1が満たされていたとしても、被認証者によって入力されたPINとの照合に利用されるデータが第三者によって改ざんされてしまうケースでは本人認証を行うことができない。そのため、被認証者によって提示されたPINが、主張された身元に対応するPINとして金融機関に登録されたものであるか否かを確認可能であることが求められる（条件2)。本節では、上記条件2を満足させるための手段をPIN認証と呼び、以下のとおり定義する。

> **PIN認証**： 被認証者によって入力されたPINが、被認証者によって主張された身元に対応して金融機関に登録されているデータに対応するものであるか否かを確認すること。

4.2　PIN認証の形態

PIN認証では、被認証者がPINを提示し、あらかじめ金融機関に登録されているデータと照合する。この登録されているデータを参照PINデータと呼び、以下では平文の状態で管理されるPIN（のリスト）を指す。

[30]認証者に登録された情報としてPINを利用する場合について考察を行うが、英数字やカナ文字を用いたパスワード等のその他の情報についても同様の議論が可能であり、本節の「PIN」をその他の情報として読み替えることができる。

PIN 認証のシステムを構成するエンティティとしては、3 節の IC カード認証における検討と同様に、カード所持者、IC カード、端末、ホストを想定するほか、カード所持者は主張された身元に対応するエンティティであり、その身元はユーザ ID として示されるものとする。IC カードは、端末と通信を行うとともに、PIN の照合等の処理等についても実行可能なデバイスとして用いられる状況を想定する。ただし、IC カード認証は実行されないものとする。

PIN 認証の形態を考えるうえで、PIN をどこで照合するか、また、照合に用いられる参照 PIN データをどこに格納先しておくかがポイントとなる。PIN の照合先、参照 PIN データの格納先としては、IC カード、端末、ホストのいずれかが想定されるが、本節では、金融分野における PIN の管理に関する国際標準 ISO 9564-1（ISO［2002］）を参照し、どのような形態を検討対象とするかを考える。

ISO 9564-1 は、オンラインで実行される PIN 認証における PIN の照合先として、端末（at a terminal）、カード発行者（by an issuer）、カード発行者以外の機関（by an institution other than an issuer）を想定している。このうち、カード発行者とカード発行者以外の機関については、いずれも本稿におけるホストに対応すると考えられる。端末における PIN 照合については、実際の照合の処理が、端末に挿入された IC カード内で行われる場合と端末で行われる場合の 2 通りが考えられる。こうしたことから、本節では、PIN の照合先として、IC カード、端末、ホストの 3 通りを想定することとする。

参照 PIN データの格納先については、ISO 9564-1 は、(a) 端末において PIN 照合を実行する場合、参照 PIN データが顧客カード（customer's card）またはカード発行者に格納される状況を想定しているほか、(b) カード発行者において PIN 照合を実行する場合にはカード発行者に格納される状況を想定している。そこで、本稿では、顧客カードとして IC カードを想定したうえで、まず上記 (a) から、IC カードあるいは端末において PIN 照合を実行する場合、参照 PIN データが IC カードまたはホストに格納される状況を想定することとする。また、上記 (b) から、ホストにおいて PIN 照合を実行する場合には、参照 PIN データがホストに格納される状況を想定することとする。

以上を整理すると、表 8 のとおりとなり、これら 5 つの PIN 認証の形態（タイプ 1〜5、図 7）について検討を行う[31]。ちなみに、EMV（EMVCo［2004a, b］）では、表 8 におけるタイプ 1、5 が想定されている。

PIN 認証では、PIN と参照 PIN データの照合を行うエンティティが認証者となる。一般に、ホストを利用せず実行されるタイプ 1、3 はオフライン PIN 認証、ホ

[31]IC カードを用いてオフラインで実行される PIN 認証に関する国際標準 ISO 9564-3（ISO［2003］）においては、PIN 認証の形態として、PIN 照合先と参照 PIN データ格納先をともに IC カードとする形態（表 8 のタイプ 1 に対応）が想定されている。

PIN 認証の形態	PIN の照合先	参照 PIN データの格納先
タイプ 1	IC カード	IC カード
タイプ 2		ホスト
タイプ 3	端末	IC カード
タイプ 4		ホスト
タイプ 5	ホスト	ホスト

表 8: PIN 認証の形態

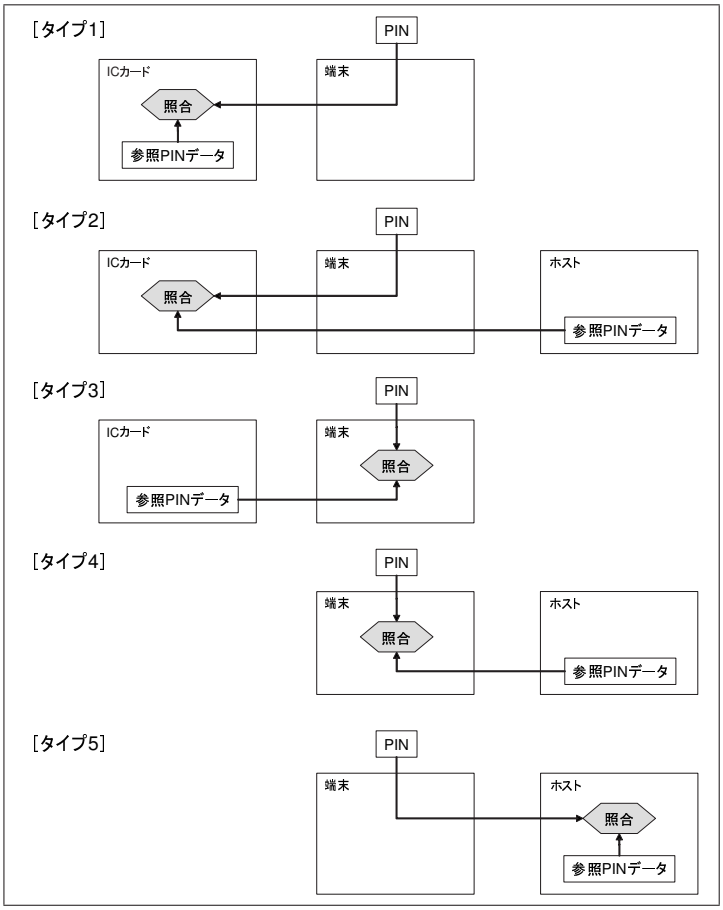

図 7: PIN 認証におけるデータの流れ

ストを利用して実行されるタイプ 2、4、5 はオンライン PIN 認証と呼ばれる。また、タイプ 1〜3 では、PIN の照合先、あるいは、参照 PIN データの格納先として IC カードを利用するため、被認証者によって主張される身元の情報（ユーザ ID）についても IC カードによって提示するケースが自然であると考えられる。これに対して、タイプ 4、5 では、PIN の照合先あるいは参照 PIN データの格納先として IC カードを使用しないため、ユーザ ID を IC カード以外の媒体（磁気ストライプ・カード等）によって提示するケースも考えられる。

4.3 PIN 認証に対する脅威

4.3.1 想定する攻撃

3 節と同様、PIN 認証における脅威として第三者によるなりすましを想定する。4.1 節の PIN 認証の定義より、PIN 認証におけるなりすましは、カード所持者以外の第三者によって入力された PIN が、カード所持者に対応して金融機関に登録されている参照 PIN データに対応するものであると判断されるときに成功する。このとき、カード所持者になりすます手段としては、(1) カード所持者の PIN を盗取する、(2) 攻撃者が適当に設定した PIN と整合性を持つように、システム側にあらかじめ設定されているカード所持者の参照 PIN データを改ざん・偽造することが考えられる[32]。以下では、攻撃者はユーザ ID といった秘密情報以外のデータを既に入手しているものとするほか、参照 PIN データが IC カード内に格納されている PIN 認証の形態（タイプ 1、3）において上記 (1) によりなりすましを行う際には、カード所持者の IC カードを既に入手しているものとして議論を進める。

以下では、上記 (1) の具体的手段を、PIN を直接入手する攻撃と、参照 PIN データを入手したうえで PIN を入手する攻撃に分類し、上記 (2) については、真正なエンティティ内に格納される参照 PIN データを改ざんする攻撃と、通信路上の参照 PIN データを改ざん・偽造する攻撃に分類して検討を行う。以下で取り上げる攻撃をまず整理しておくと、次の図 8 のとおりである。

(1)PIN を盗取する攻撃

攻撃者が PIN を盗取する方法には、PIN を直接盗取するケースと、盗取した参照 PIN データから PIN を入手するケースが考えられる。PIN や参照 PIN データを盗取する先としては、(1) 当該システムのハードウエア（端末と IC カード）、(2) ハードウエア間を結ぶ通信路、(3) カード所持者・端末間の通信路、(4) カード所持者自身の 4 つが考えられる。このうち、上記 (4) のカード所持者自身から盗取する方法として、ソーシャル・エンジニアリング（social engineering）やカード所持者による PIN の不適切な管理を巧みに利用する方法が挙げられる。ここでのソーシャル・エンジニアリングとは、金融機関の職員になりすまして PIN を不正に聞き出すといった攻撃を指す（Anderson［2001］）ほか、コンピュータを不正操作するためのプログラムを不正にインストールさせることや、フィッシング攻撃（phishing attack）にみられるような、偽サイトへ誘導したうえで PIN の入力を求めるといったテクニックも含まれる。一方、PIN の不適切な管理とは、第三者によって容易

[32]PIN 照合を実行するエンティティにおける処理フロー自体を改変し、攻撃者の都合のよい認証結果を出力させるという手段も考えられる。こうした攻撃については、3.3.1 節で説明した IC カード認証における端末への攻撃と同じ議論ができるため、補論において取り扱うこととする。

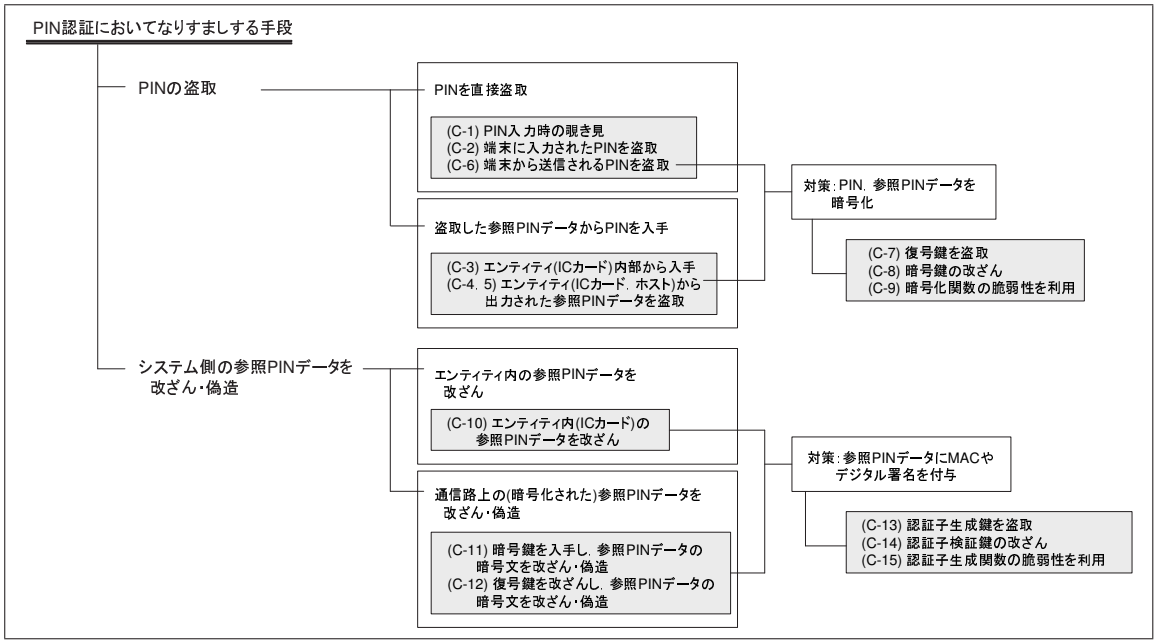

図 8: 本節で検討する具体的な攻撃手段

に推測可能な PIN を利用していたことで PIN が漏洩する、あるいは、自らの記憶を補完するために書き込んだ何らかの媒体（IC カード以外）から PIN が漏洩する等の状況を指す。

上記 (4) のうち、カード所持者が PIN を不適切に管理したことに起因する PIN の漏洩等、技術的な手法だけでは十分な対策とはなりえないものについては、他の認証手段によって対応するといったケースが一般的であることから、以下では検討の対象外とする。

各エンティティが格納するデータ、および、通信路上のデータは、PIN の照合を実行するエンティティおよび参照 PIN データの格納先によって異なるため、以下ではそれぞれの場合に分けて想定される攻撃を列挙する。本節において利用する用語は、前節で定義したものと同様の意味を持つものとするほか、攻撃者の能力に関しても前節において想定した攻撃者と同様であるとする。

- **すべてのタイプ：** カード所持者が端末（PIN パッド）に PIN を入力する際（カード所持者・端末間の通信路に相当する）に想定される攻撃は以下のとおりである。

  — 攻撃 C-1： カード所持者による PIN 入力時の様子を覗き見ることによって PIN を盗取する。

  — 攻撃 C-2： 不正・偽端末や攻撃モジュールの利用により、カード所持者によって入力された PIN を盗取する。

- **参照 PIN データの格納先が IC カードとなるタイプ：** IC カード内に参照 PIN データが格納されるタイプ 1、3 では、なりすましの対象であるカード所持者の真正な IC カードから参照 PIN データを盗取することを試みることができる。PIN 照合を IC カード内で実行するタイプ 1 では、参照 PIN データが IC カードの外部へ出力しないように管理されることから、IC カードの正規の出力チャネルから参照 PIN データを盗取することができず、侵入型攻撃を実行して PIN を盗取する必要がある。これに対して、IC カード以外の他のエンティティにおいて PIN 照合が実行されるタイプ 3 では、端末からのリード・コマンドに対して正規の出力チャネルから参照 PIN データが出力されることから、真正な端末になりすまして IC カードから参照 PIN データを不正に出力させる、あるいは、IC カードから送信された参照 PIN データを通信路から盗取することが考えられる。

  — 攻撃 C-3： 不正・偽端末や攻撃モジュールを利用して侵入型攻撃を実行し、IC カード内部に格納される参照 PIN データを正規の出力チャネル以外から盗取する。（タイプ 1 の場合）

  — 攻撃 C-4： 不正・偽端末や攻撃モジュールが、IC カードに対して真正な端末になりすまし、参照 PIN データを IC カードの正規のチャネルから不正に出力させて盗取する、あるいは、通信路の盗聴によって、IC カードから出力された参照 PIN データを盗取する。（タイプ 3 の場合）

- **参照 PIN データの格納先がホストとなるタイプ：** 参照 PIN データの格納先がホストであり、かつ、PIN 照合がホスト以外のエンティティ内で実行されるタイプ 2、4 では、以下の攻撃によってホストから送信される参照 PIN データの盗取を試みることが可能である。

  — 攻撃 C-5： 参照 PIN データを盗取するための IC カードや不正・偽端末の利用、あるいは、通信路の盗聴によって、ホストが送信する参照 PIN データを盗取する。（タイプ 2、4 の場合）

- **PIN の照合先が IC カードあるいはホストとなるタイプ：** IC カードあるいはホストで PIN の照合が実行される場合、カード所持者によって端末に入力された PIN は照合先となるエンティティに送信される。そのため、攻撃者は以下の手段によってハードウエア間の通信路から PIN を盗取しようと試みることが可能である。

  — 攻撃 C-6： PIN を盗取するための IC カードの利用や偽ホストの設置、あるいは、通信路の盗聴によって端末から送信される PIN を盗取する。

（タイプ 1、2、5 の場合）

これまでに整理した、各 PIN 認証において想定される攻撃については表 9 にまとめた。

PIN 認証の形態	想定される攻撃
タイプ 1	C-1, C-2, C-3, C-6
タイプ 2	C-1, C-2, C-5, C-6
タイプ 3	C-1, C-2, C-4
タイプ 4	C-1, C-2, C-5
タイプ 5	C-1, C-2, C-6

表 9: 各 PIN 認証において想定される攻撃

攻撃 C-4〜6 への対策としては、まず、データの送信先となるエンティティ以外への PIN の漏洩を防止するための機構を採用することが考えられる。このような機構として各エンティティが送信するデータ（PIN あるいは参照 PIN データ）を暗号化するという手段を採用し[33]、PIN の照合は復号して得た平文を利用して行うことが考えられる。その場合[34]、(1) 暗号文を復号するための秘密鍵を盗取して、PIN や参照 PIN データの暗号文を不正に復号する、(2) 暗号化を行うための鍵を改ざんすることで、攻撃者が PIN や参照 PIN データを復号可能となる暗号文を生成させる、(3) 暗号化に利用するアルゴリズム（以下、暗号化関数と呼ぶ）の脆弱性を利用して、PIN や参照 PIN データの暗号文を不正に復号するといった方法によって PIN を盗取することが考えられる。

上記 (1) については、暗号化に公開鍵暗号を利用する場合には、復号を行うエンティティのみが攻撃対象となるのに対し、共通鍵暗号を利用する場合には、暗号化を行うエンティティと復号を行うエンティティのいずれも攻撃対象となる（表 10 参照）。また、共通鍵暗号を利用する場合には、真正な IC カード・真正な端末間であらかじめ鍵共有は行われており、公開鍵暗号を利用する場合には、暗号化前に公開鍵証明書の検証によって暗号文の送信先を確認することとする。このとき、上記 (2) の暗号鍵（共通鍵暗号における秘密鍵、公開鍵暗号における公開鍵証明書）を改ざんする攻撃は、暗号化を行うエンティティが IC カードや端末であ

[33]共通鍵暗号や公開鍵暗号のほかに、ハッシュ関数を利用して PIN の漏洩を防止するという対策も考えられるが、PIN のサイズが小さく、ハッシュ関数およびそのメッセージ・フォーマットが公開である場合には、通信路上のデータ（ハッシュ値）から総当り攻撃によって PIN が容易に求められてしまう可能性がある。

[34]PIN の照合は、侵入型攻撃に対する対策が施されているモジュール内で実行されることを想定する。また、平文から一意に暗号文が生成される暗号化アルゴリズムを利用する場合には、暗号文同士の照合によって PIN 照合を実行することも可能であるが、本節では平文同士の照合による PIN 認証について検討を行う。

PIN 認証の形態	データの流れ		秘密鍵を持つエンティティ	
	PIN	参照 PIN データ	共通鍵暗号を利用	公開鍵暗号を利用
タイプ 1	端末→ IC カード	—	IC カード、端末	IC カード
タイプ 2	端末→ IC カード	ホスト→ IC カード	IC カード、端末、ホスト	IC カード
タイプ 3	—	IC カード→端末	IC カード、端末	端末
タイプ 4	—	ホスト→端末	端末、ホスト	端末
タイプ 5	端末→ホスト	—	端末、ホスト	ホスト

表 10: エンティティ間のデータの流れ

るタイプ 1〜3、5 において想定され、PIN や参照 PIN データを送信するエンティティが当該攻撃の対象となる。

また、参照 PIN データを送信する際に暗号化を実行する場合には、タイプ 3 においても平文の参照 PIN データそのものを外部へ出力しないデータとして格納することができる。この場合には、タイプ 1 と同様に攻撃 C-3 が想定されることとなる。

本節では、攻撃 C-4〜6 への対策としてデータを暗号化するという手段を採用することとし、こうした対策に伴う以下の攻撃についても検討対象とする[35]（図 9 参照）。

・攻撃 C-4〜6 への対策に対する攻撃：

— 攻撃 C-7： 暗号化された PIN あるいは参照 PIN データの復号鍵を盗取し、通信路上を盗聴して得た暗号文を復号して PIN または参照 PIN データを入手する。

— 攻撃 C-8： 暗号化を行うエンティティ内に格納される暗号鍵を改ざんし、通信路上を盗聴して得た暗号文を復号して PIN または参照 PIN データを入手する[36]。

— 攻撃 C-9： 暗号化関数の脆弱性を利用して、通信路を盗聴して得た暗号文を復号して PIN または参照 PIN データを入手する。

PIN や参照 PIN データの暗号化に共通鍵暗号あるいは公開鍵暗号を利用する場合、攻撃 C-7、C-8 の対象となるエンティティは表 11 のとおりである。

[35] 3.4 節での静的認証において、端末・ホスト間のデータ漏洩を防止するための機構として暗号化を採用する場合には、以下と同様の議論が必要である。

[36] 暗号通信の前に、データ受信者が公開鍵証明書をデータ送信者（暗号文作成者）に送信するようなケースでは、そうした通信路上の公開鍵証明書についても改ざんする必要がある。

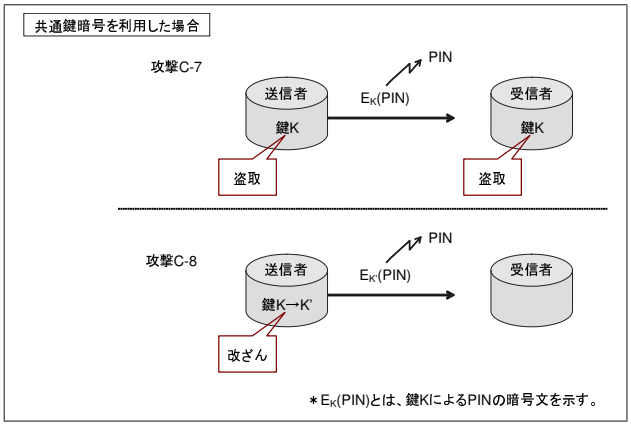

図 9: PIN を盗取する攻撃（攻撃 C-7、C-8）の概念図

PIN 認証の形態	復号鍵を盗取 (C-7)		暗号鍵を改ざん (C-8)	
	共通鍵暗号	公開鍵暗号	共通鍵暗号	公開鍵暗号
タイプ 1	IC カード、端末	IC カード	端末	
タイプ 2	IC カード、端末	IC カード	端末	
タイプ 3	IC カード、端末	端末	IC カード	
タイプ 4	端末	端末	—	
タイプ 5	端末	—	端末	

表 11: 攻撃 C-7、C-8 の対象となるエンティティ

(2) 参照 PIN データを改ざん・偽造する攻撃

なりすましを行う手段には、4.3.1 節で述べたように、攻撃者が適当に設定した PIN と整合性を持つように、システム側にあらかじめ設定されているカード所持者の参照 PIN データを改ざん・偽造するという手段が考えられる。具体的には、(1) 真正なエンティティ内に格納されている参照 PIN データの改ざんと、(2) 通信路上の参照 PIN データの改ざん[37]・偽造が考えられる。

上記 (1) については、参照 PIN データは IC カードとホストのいずれかに格納されており、ホストは安全に管理されていることから、こうした攻撃は参照 PIN データが IC カードに格納されるタイプ 1、3 において想定される。

上記 (2) は、参照 PIN データが通信されるタイプ 2〜4 において想定される攻撃である。しかし、攻撃 C-4〜6 への対策が講じられ、エンティティ間で送受信されるデータが暗号化されることを前提とすれば、改ざん後のデータは正しい暗号文である必要がある。ここで、正しい暗号文とは、データの受信者（PIN の照合を行うエンティティ）の復号鍵に対応する暗号鍵で生成された暗号文をいう。したがって、上記 (2) を実行する際には、攻撃者は、正しい暗号鍵を盗取する、あるい

[37]攻撃者が適当に設定した PIN に対応する参照 PIN データを格納するエンティティの偽造を含む。

は、データ受信者が格納する復号鍵を適当に設定したものに改ざんする必要がある。暗号鍵の盗取においては、暗号化に公開鍵暗号を利用するケースでは、公開鍵証明書は通信路から比較的容易に入手可能であると想定されるが、共通鍵暗号を利用するケースでは、暗号文の送信者あるいは受信者となるエンティティから侵入型攻撃や非侵入型攻撃を利用して暗号鍵を盗取することになる。

具体的な攻撃手段は以下のとおりであり（図 10 参照）、参照 PIN データの暗号化に共通鍵暗号または公開鍵暗号を利用する場合の暗号鍵の入手や復号鍵の改ざんに関する攻撃対象となるエンティティについては表 12 にまとめた。

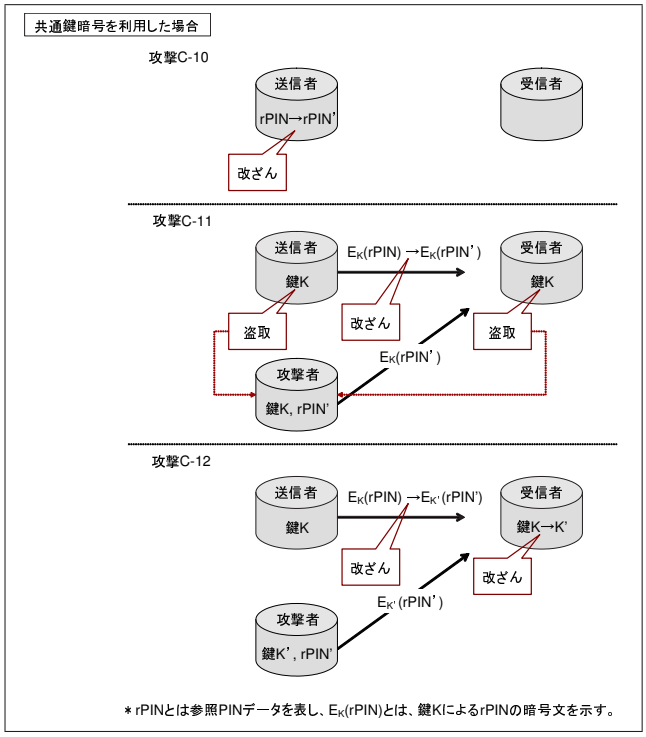

図 10: 参照 PIN データを改ざんする攻撃（攻撃 C-10〜12）の概念図

— 攻撃 C-10： 参照 PIN データを格納しているエンティティ内の参照 PIN データを改ざんする。

— 攻撃 C-11： (a) 暗号鍵を入手したうえで、攻撃者が適当に設定した PIN に対応する参照 PIN データの暗号文を生成し、PIN の照合を行うエンティティに送信する、あるいは、(b) 通信路上のデータをそのように改ざんする。

— 攻撃 C-12： (a) 攻撃者が適当に設定した暗号鍵と PIN に対応する参照 PIN データを用いて生成した暗号文を、PIN の照合を行うエンティティに送信する、あるいは、(b) 通信路上のデータをそのように改ざんするとともに、当該暗号鍵と整合性を持つようにデータ受信者内に格納される復号鍵を改ざんする。

PIN 認証の形態	参照 PIN データの改ざん (C-10)	暗号鍵の盗取 (C-11)		復号鍵の改ざん (C-12)	
		共通鍵暗号	公開鍵暗号	共通鍵暗号	公開鍵暗号
タイプ 1	IC カード	—	—	—	
タイプ 2	—	IC カード	○	IC カード	
タイプ 3	IC カード	IC カード・端末	○	端末	
タイプ 4	—	端末	○	端末	
タイプ 5	—	—	—	—	

備考：“ ○ ”は、受信者の公開鍵証明書を入手することによって容易に攻撃を実行可能であることを表す。

表 12: 攻撃 C-10〜12 の対象となるエンティティ

攻撃 C-10〜C-12 への対策について検討する。まず、攻撃対象となるエンティティに当該攻撃を防御・検知する機構を組み込むことで防止することができると考えられる。そのほか、参照 PIN データを格納するエンティティと PIN の照合を行うエンティティが異なる認証形態（タイプ 2〜4）における攻撃（攻撃 C-11、C-12、タイプ 3 に対する攻撃 C-10）では、参照 PIN データが改ざんされたものでないこと、すなわち、参照 PIN データがカード所持者によって金融機関に届け出られたものであることを確認することで攻撃を防止することが可能である。こうしたデータの一貫性、および、データの作成者を確認する方法としては、金融機関が生成した MAC やデジタル署名（以下、これらをまとめて認証子と呼ぶ）を利用することができる。しかし、そうした対策が施された場合においても、(1)MAC やデジタル署名の生成鍵（以下、これらをまとめて認証子生成鍵と呼ぶ）を盗取する、(2)MAC やデジタル署名を検証する鍵（以下、これらをまとめて認証子検証鍵と呼ぶ）を改ざんする、(3)MAC やデジタル署名を生成するアルゴリズム（以下、これらをまとめて認証子生成関数と呼ぶ）の脆弱性を利用するといった手段によって認証子を偽造することが考えられる。これらの攻撃を攻撃 C-13〜15 として以下に挙げる。

— 攻撃 C-13： 認証子生成鍵を盗取したうえで、攻撃者が適当に設定した PIN に対応する参照 PIN データに付与する認証子を偽造する。

— 攻撃 C-14： 攻撃者が適当に設定した PIN に対応する参照 PIN データと認証子生成鍵を用いて認証子を生成するとともに、当該認証子生成鍵と整合性を持つようにデータ受信者に格納される認証子検証鍵を改ざんする。

— 攻撃 C-15： 認証子生成関数の脆弱性を利用して、攻撃者が適当に設定した PIN に対応する参照 PIN データに付与する認証子を偽造する。

攻撃 C-13 については、認証子生成鍵はホストに格納されることが想定されるが、MAC を利用した場合には認証子生成鍵と認証子検証鍵が同一であることから、受

信者内部に格納される認証子検証鍵を盗取することが考えられる。攻撃 C-14 については、MAC とデジタル署名のいずれを利用した場合においても想定される攻撃であり、その対象となるエンティティは参照 PIN データの受信者である。攻撃 C-13、14 の攻撃対象となるエンティティについては表 13 にまとめた。

PIN 認証の形態	認証子生成鍵の盗取 (C-13)		認証子検証鍵の改ざん (C-14)	
	MAC	デジタル署名	MAC	デジタル署名
タイプ 2	IC カード	—	IC カード	
タイプ 3	端末	—	端末	
タイプ 4	端末	—	端末	

表 13: 攻撃 C-13、14 において攻撃対象となるエンティティ

以上の考察より、エンティティ間で送受信されるデータを暗号化した場合において想定される攻撃を表 14 にまとめる。

PIN 認証の形態	想定される攻撃
タイプ 1	C-1, C-2, C-3, C-7, C-8, C-9, C-10
タイプ 2	C-1, C-2, C-7, C-8, C-9, C-11, C-12, C-13, C-14, C-15
タイプ 3	C-1, C-2, C-3, C-7, C-8, C-9, C-10, C-11, C-12, C-13, C-14, C-15
タイプ 4	C-1, C-2, C-7, C-9, C-11, C-12, C-13, C-14, C-15
タイプ 5	C-1, C-2, C-7, C-8, C-9

備考：攻撃 C-13〜15 については、攻撃 C-10〜12 の対策として参照 PIN データに MAC やデジタル署名を付与した場合に追加される攻撃を示す。

表 14: 送受信されるデータを暗号化する対策を講じた場合において想定される攻撃

4.4 想定する攻撃に対する対策法

4.3 節で列挙した攻撃の対策には、以下が挙げられる。

(1) PIN を盗取する攻撃への対策

— 攻撃 C-1 に対する対策 (I)： 被認証者が PIN 入力時の様子が覗き見されていないことを確認可能にするとともに、確認できたときに限り PIN パッドに PIN を入力することで PIN の漏洩を防止する。

— 攻撃 C-1 に対する対策 (II)： 被認証者による PIN 入力時の様子が覗き見されたとしても、その様子から PIN を推定困難とする手法を採用することで PIN の漏洩を防止する。

— 攻撃 C-2 に対する対策： 被認証者が端末が真正であることを確認可能にするとともに、確認できたときに限り PIN パッドに PIN を入力することを可能にする機構を端末に組み込むことで、PIN の漏洩を防止する。

— 攻撃 C-3 に対する対策 (I)： IC カードに当該攻撃（侵入型攻撃）に対する防御技術を組み込むことで、参照 PIN データの漏洩を防ぐ。

— 攻撃 C-3 に対する対策 (II)： 当該攻撃を検知し、金融機関に異常を知らせる機構を IC カードに組み込むことで、漏洩した参照 PIN データから得た PIN の不正利用を防ぐ。

— 攻撃 C-3 に対する対策 (III)： 当該攻撃を検知し、内部に格納される参照 PIN データを自動的に消去する機構を IC カードに組み込むことで、参照 PIN データの漏洩を防ぐ。

— 攻撃 C-3 に対する対策 (IV)： IC カード内の参照 PIN データから元の PIN を復元困難な状態で格納しておくことで、参照 PIN データからの PIN の漏洩を防ぐ。

— 攻撃 C-4 に対する対策： IC カードは、端末あるいはホストに送信する参照 PIN データを暗号化することで、他のエンティティへのデータ漏洩を回避するとともに、通信路上の盗聴によるデータの漏洩を防ぐ。

— 攻撃 C-5 に対する対策： ホストは、IC カードあるいは端末に送信する参照 PIN データを暗号化することで、他のエンティティへのデータ漏洩を回避するとともに、通信路上の盗聴によるデータの漏洩を防ぐ。

— 攻撃 C-6 に対する対策： 端末は、IC カードあるいはホストに送信するデータ（PIN あるいは参照 PIN データ）を暗号化することで、他のエンティティへのデータ漏洩を回避するとともに、通信路上の盗聴によるデータの漏洩を防ぐ。

— 攻撃 C-7、C-8 に対する対策 (I)： IC カードが攻撃対象となるケースにおいて、IC カードに当該攻撃（侵入型攻撃と非侵入型攻撃）に対する防御技術を組み込むことで、復号鍵の漏洩、および、暗号鍵の改ざんを防ぐ。

— 攻撃 C-7、C-8 に対する対策 (II)： IC カードが攻撃対象となるケースにおいて、当該攻撃を検知し、金融機関に異常を知らせる機構を IC カードに組み込むことによって、漏洩した復号鍵、および、改ざんされた暗号鍵の不正使用を防ぐ。

— 攻撃 C-7、C-8 に対する対策 (III)： IC カードが攻撃対象となるケースにおいて、当該攻撃を検知し、内部に格納されるデータを自動的に消去する機構等を IC カードに組み込むことで、復号鍵の漏洩、および、暗号鍵の改ざんを防ぐ。

— 攻撃 C-7、C-8 に対する対策 (IV)： 端末が攻撃対象となるケースにおいて、端末に当該攻撃（侵入型攻撃と非侵入型攻撃）に対する防御技術を組み込むことで、復号鍵の漏洩、および、暗号鍵の改ざんを防ぐ。

— 攻撃 C-7、C-8 に対する対策 (V)： 端末が攻撃対象となるケースにおいて、当該攻撃を検知し、金融機関に異常を知らせる機構を端末に組み込むことで、漏洩した復号鍵、および、改ざんされた暗号鍵の不正使用を防ぐ。

— 攻撃 C-7、C-8 に対する対策 (VI)： 端末が攻撃対象となるケースにおいて、当該攻撃を検知し、内部に格納されるデータを自動的に消去する機構等を端末に組み込むことで、復号鍵の漏洩、および、暗号鍵の改ざんを防ぐ。

— 攻撃 C-9 に対する対策： 既存の攻撃に対して安全な暗号化関数を利用することで、PIN および参照 PIN データの漏洩を防ぐ。

外部へ出力しないように管理される参照 PIN データを IC カードや端末から盗取しようとする攻撃 C-3 への対策としては、データの漏洩を防止する対策（攻撃 C-3 に対する対策 (I、III)）と、漏洩したデータの利用を防止する対策（C-3 に対する対策 (II)）がまず挙げられる。これらに加えて、参照 PIN データが侵入型攻撃によって漏洩した場合においても、参照 PIN データから PIN を復元困難であれば PIN の漏洩を防ぐことができると考えられるため、攻撃 C-3 に対する対策 (IV) も挙げられる。こうした対策の例として、PIN を含むメッセージのハッシュ値として参照 PIN データを用いるという方法も考えられるが、PIN のサイズが小さく、ハッシュ関数およびそのメッセージ・フォーマットが公開されている場合には、総当り攻撃によって PIN が容易に求められてしまう可能性もある点には留意が必要である。そのほか、PIN の暗号文を参照 PIN データとする方法も考えられるが、PIN の照合時には復号する必要があることから、復号鍵も参照 PIN データと同じエンティティ内に格納されることとなる。よって、復号鍵の盗取を試みる侵入型攻撃や非侵入型攻撃に対する対策が別途必要となるため、PIN の暗号文を参照 PIN データとする方法は攻撃 C-3 に対する対策とはならないと考えられる。

IC カードや端末に格納される復号鍵を盗取する、および、暗号鍵を改ざんする攻撃 C-7、C-8 に対しても、データの漏洩・改ざんを防止する対策（攻撃 C-7、C-8 に対する対策 (I、III)）と漏洩・改ざんされたデータの利用を防止する対策（攻撃 C-7、C-8 に対する対策 (II)）が挙げられる。復号鍵の盗取については、復号鍵そのものを復元困難な形態で格納することで復号鍵の漏洩を防止するという方法も考えられるものの、暗号文の復号処理の実行中に当該復号鍵が利用されるため、非侵入型攻撃による復号鍵の漏洩の可能性が依然として残ることとなる。そのほか、復号鍵を暗号化して格納したとしても、さらにその復号鍵も同じエンティティ内に格納されることから、侵入型攻撃あるいは非侵入型攻撃によって当該復号鍵が

漏洩する可能性があると考えられる。このため、復号鍵を復元困難な形態で格納するという対策は有効とならない。

(2) 参照 PIN データを改ざん・偽造する攻撃への対策

4.3 節で列挙した、参照 PIN データの改ざん・偽造に対する対策には、以下が挙げられる。

- 攻撃 C-10〜14 に対する対策 (I)： IC カードが攻撃対象となるケースにおいて、IC カードに当該攻撃に対する防御技術を組み込むことで、参照 PIN データの改ざん、暗号鍵・認証子生成鍵の漏洩、復号鍵・認証子検証鍵の改ざんを防ぐ。
- 攻撃 C-10〜14 に対する対策 (II)： IC カードが攻撃対象となるケースにおいて、当該攻撃を検知し、金融機関に異常を知らせる機構を IC カードに組み込むことで、改ざんされた参照 PIN データ、漏洩した暗号鍵・認証子生成鍵、改ざんされた復号鍵・認証子検証鍵の不正利用を防ぐ。
- 攻撃 C-10〜14 に対する対策 (III)： IC カードが攻撃対象となるケースにおいて、当該攻撃を検知し、内部に格納される鍵を自動的に消去する機構等を IC カードに組み込むことで、参照 PIN データの改ざん、暗号鍵・認証子生成鍵の漏洩、復号鍵・認証子検証鍵の改ざんを防ぐ。
- 攻撃 C-11〜14 に対する対策 (I)： 端末が攻撃対象となるケースにおいて、端末に当該攻撃に対する防御技術を組み込むことで、暗号鍵・認証子生成鍵の漏洩、復号鍵・認証子検証鍵の改ざんを防ぐ。
- 攻撃 C-11〜14 に対する対策 (II)： 端末が攻撃対象となるケースにおいて、当該攻撃を検知し、金融機関に異常を知らせる機構を端末に組み込むことで、漏洩した暗号鍵・認証子生成鍵、改ざんされた復号鍵・認証子検証鍵の不正利用を防ぐ。
- 攻撃 C-11〜14 に対する対策 (III)： 端末が攻撃対象となるケースにおいて、当該攻撃を検知し、内部に格納される鍵を自動的に消去する機構等を端末に組み込むことで、暗号鍵・認証子生成鍵の漏洩、復号鍵・認証子検証鍵の改ざんを防ぐ。
- 攻撃 C-15 に対する対策： 既存の攻撃法に対して安全な認証子生成関数を利用することで、参照 PIN データの偽造が可能となることを防ぐ。

参照 PIN データの格納先と PIN の照合先が異なる認証形態における参照 PIN データの改ざん・偽造については、攻撃 C-10〜12 をエンティティの耐タンパー性

によって直接防止する、あるいは、参照 PIN データに MAC やデジタル署名を付与したうえで攻撃 C-13〜15 への対策を講じることとなる。すなわち、攻撃 C-10〜12 への対策としては、「表 12 に示した攻撃対象となるエンティティへの耐タンパー性の付与」、または、「表 13 に示した攻撃対象となるエンティティへの耐タンパー性の付与、および、攻撃 C-15 に対する対策」が必要となる。

4.5 セキュリティ要件

以上で列挙した対策に対応するセキュリティ要件を以下の 13 項目にまとめた。

P-1. カード所持者による PIN の入力時の様子を覗き見されないこと。

P-2. カード所持者による PIN の入力時の様子から PIN の推定を困難とすること。

P-3. カード所持者が端末の真正性を確認可能であること。

P-4. 他のエンティティに送信するデータは暗号化すること[38]。

P-5. IC カードは、侵入型攻撃および非侵入型攻撃に対してタンパー・レジスタンスであること。

P-6. IC カードは、侵入型攻撃および非侵入型攻撃を検知して金融機関に速やかに異常を知らせること。

P-7. IC カードは、侵入型攻撃および非侵入型攻撃に対してタンパー・レスポンスであること。

P-8. 端末は、侵入型攻撃および非侵入型攻撃に対してタンパー・レジスタンスであること。

P-9. 端末は、侵入型攻撃および非侵入型攻撃を検知して金融機関に速やかに異常を知らせること。

P-10. 端末は、侵入型攻撃および非侵入型攻撃に対してタンパー・レスポンスであること。

P-11. IC カードに対する侵入型攻撃によって漏洩したデータから PIN の復元が困難であること。

P-12. 当該システムにおいて採用されている暗号化関数は、想定される攻撃に対して安全であると評価されていること。

P-13. 当該システムにおいて採用されている認証子生成関数は、想定される攻撃に対して安全であると評価されていること。

セキュリティ要件	各セキュリティ要件に対応する対策
P-1	C-1(I)
P-2	C-1(II)
P-3	C-2
P-4	C-4〜6
P-5	C-3(I)、C-7,8(I)、C-10〜14(I)
P-6	C-3(II)、C-7,8(II)、C-10〜14(II)
P-7	C-3(III)、C-7,8(III)、C-10〜14(III)
P-8	C-7,8(IV)、C-11〜14(I)
P-9	C-7,8(V)、C-11〜14(II)
P-10	C-7,8(VI)、C-11〜14(III)
P-11	C-3(IV)
P-12	C-9
P-13	C-15

備考：“ C-1(I) ”は、“ 攻撃 C-1 に対する対策 (I) ”を表す。

表 15: 各セキュリティ要件に対応する対策手法

上記のセキュリティ要件と各要件に対応する対策の関係を整理する（表 15 参照）。まず、データの暗号化に関する対策（攻撃 C-4〜6 に対する対策）は要件 P-4 に対応する。IC カード内部から参照 PIN データを盗取する攻撃 C-3 に対する対策の中でも、侵入型攻撃への対策（攻撃 C-3 に対する対策 (I〜III)）は、侵入型攻撃と非侵入型攻撃の両方に対して対策を講じることを内容とする要件 P-5〜7 に対応する。また、暗号化された PIN や参照 PIN データを復号するための秘密鍵の盗取（攻撃 C-7）、および、暗号鍵の改ざん（攻撃 C-8）への対策については、IC カードや端末への侵入型攻撃と非侵入型攻撃の両方に対して対策を講じることを内容とする要件 P-5〜7、P-8〜10 にそれぞれ対応する。そのほか、IC カードが攻撃対象となる場合において、エンティティ内に格納される参照 PIN データの改ざん（攻撃 C-10）、暗号鍵の盗取（攻撃 C-11）、復号鍵の改ざん（攻撃 C-12）、認証子生成鍵の盗取（攻撃 C-13）、認証子検証鍵の改ざん（攻撃 C-14）への対策は、要件 P-5〜7 に対応する。一方、端末が攻撃対象となる場合の攻撃 C-11〜14 への対策は、要件 P-8〜10 に対応する。

こうしたセキュリティ要件と対策の対応関係と、表 9、14 に示されている各 PIN 認証の形態において想定される攻撃とを組み合わせると、各認証形態におけるセキュリティ要件を導出することができる（表 16 参照）。例えば、表 9、14 をみると、タイプ 1 において想定される攻撃は、C-1、C-2、C-3、C-6、C-7、C-8、C-9、C-10 であり、表 15 によって、攻撃 C-1 に対する対策から導出されるセキュリティ要件は「P-1 または P-2」であることがわかる。同様に、攻撃 C-2 に対する対策か

[38]本節における検討では、IC カードにおいて暗号化を実行可能であることを想定し、暗号化による対策を前提として検討していることから、暗号化によるデータ漏洩の防止をセキュリティ要件として記述した。

らP-3、攻撃C-3に対する対策から「P-5またはP-6またはP-7またはP-11」、攻撃C-6に対する対策からP-4が導出される。また、暗号化に公開鍵暗号を利用するケースに注目すると、攻撃C-7とC-9の対象はICカードであることから「P-5またはP-6またはP-7」、攻撃C-8に対する対策から「P-8またはP-9またはP-10」、攻撃C-9に対する対策からP-12、攻撃C-10に対する対策から「P-5またはP-6またはP-7」がセキュリティ要件として導出される。

その結果、この形態のPIN認証にはセキュリティ要件として、表16の[(P-1 ∨ 2) ∧ P-3 ∧ P-4 ∧ (P-5 ∨ 6 ∨ 7) ∧ (P-8 ∨ 9 ∨ 10) ∧ P-12]（ただし、“ ∨ ”は“ または ”を、“ ∧ ”は“ かつ ”を表す）が求められることとなる。なお、P-11は、攻撃C-3への対策に関する要件「P-5またはP-6またはP-7またはP-11」の要素として登場していたが、同時に、攻撃C-7、9、10への対策に関する要件「P-5またはP-6またはP-7」も満足する必要があり、セキュリティ要件としては「P-5またはP-6またはP-7」が残るため、P-11は最終的なセキュリティ要件に含まれないこととなる。

PIN認証の形態	セキュリティ要件
タイプ1	(P-1 ∨ 2), P-3, P-4, (P-5 ∨ 6 ∨ 7), (P-8 ∨ 9 ∨ 10), P-12
タイプ2	(P-1 ∨ 2), P-3, P-4, (P-5 ∨ 6 ∨ 7), (P-8 ∨ 9 ∨ 10), P-12, P-13*
タイプ3	(P-1 ∨ 2), P-3, P-4, (P-5 ∨ 6 ∨ 7), (P-8 ∨ 9 ∨ 10), P-12, P-13*
タイプ4	(P-1 ∨ 2), P-3, P-4, (P-8 ∨ 9 ∨ 10), P-12, P-13*
タイプ5	(P-1 ∨ 2), P-3, P-4, (P-8 ∨ 9 ∨ 10), P-12

備考：各認証形態については、列挙されたすべての要件を満足することが求められる。
また、“ ∗ ”は、参照PINデータの暗号化に公開鍵暗号を利用した場合に求められる要件である。

表16: 各PIN認証におけるセキュリティ要件

4.6 PIN認証のセキュリティ要件に関する考察

表16をみると、まず、セキュリティ要件（P-1 ∨ P-2)、P-3、P-4、P-12は、いずれのPIN認証の形態においても求められる要件となっている。これは、すべてのPIN認証において、被認証者が端末にPINを入力するほか、エンティティ間でPINや参照PINデータの送受信が行われることによるものであり、PIN入力時の覗き見防止、偽端末によるPINの盗取防止、PINや参照PINデータの暗号化等による機密性確保を実現することが必要であるといえる。

また、ICカードに関するセキュリティ要件（P-5 ∨ 6 ∨ 7）がタイプ1〜3において求められるほか、端末に関するセキュリティ要件（P-8 ∨ 9 ∨ 10）がすべてのPIN認証の形態において求められる。これらのセキュリティ要件によって防御す

べき攻撃は、表 17 に示すように、PIN 認証の形態によって異なる。このため、本要件に基づいて具体的にセキュリティ要件を検討する際には、想定される各攻撃の内容に留意して、適切な対策手法を選択することが求められる。

PIN 認証の形態	IC カードを対象とするセキュリティ要件 (P-5 ∨ 6 ∨ 7) によって防御される攻撃	端末を対象とするセキュリティ要件 (P-8 ∨ 9 ∨ 10) によって防御される攻撃
タイプ 1	・参照 PIN データの改ざん ・PIN の復号鍵の盗取	・PIN の暗号鍵の盗取（共） ・PIN の暗号鍵の改ざん
タイプ 2	・PIN の復号鍵の盗取 ・参照 PIN データの復号鍵の盗取 ・参照 PIN データの復号鍵の改ざん ・認証子生成鍵の盗取（MAC） ・認証子検証鍵の改ざん	・PIN の暗号鍵の盗取（共） ・PIN の暗号鍵の改ざん
タイプ 3	・参照 PIN データの改ざん ・参照 PIN データの暗号鍵の盗取 ・参照 PIN データの暗号鍵の改ざん	・参照 PIN データの復号鍵の盗取 ・参照 PIN データの復号鍵の改ざん ・認証子生成鍵の盗取（MAC） ・認証子検証鍵の改ざん
タイプ 4		・参照 PIN データの復号鍵の盗取 ・参照 PIN データの復号鍵の改ざん ・認証子生成鍵の盗取（MAC） ・認証子検証鍵の改ざん
タイプ 5		・PIN の暗号鍵の盗取（共） ・PIN の暗号鍵の改ざん

備考：“（共）”は、データの暗号化に共通鍵暗号を利用する場合に想定される攻撃を表す。“（MAC）”は、参照 PIN データに MAC を付与する場合に想定される攻撃を表す。参照 PIN データの暗号化に共通鍵暗号を利用する場合には、参照 PIN データの復号鍵の盗取（攻撃 C-7）と参照 PIN データの暗号鍵の盗取（攻撃 C-11）は、同じ攻撃を示すことになるが、それらについては、エンティティが暗号化を行う場合には暗号鍵、復号を行う場合には復号鍵という記述を用いた。

表 17: セキュリティ要件によって防御される攻撃

5　考察と今後の課題

5.1　本稿における検討結果の活用

本稿では、IC カードを利用した本人認証の中でも、IC カード認証と PIN 認証を別々に取り上げてセキュリティ要件の導出を行った。これらを併用し、両方の認証方式において本人であると判断されたときに限り認証が成功するタイプの本人認証システムにおいては、IC カードの偽造および PIN の盗取（ユーザによる不適切な管理に起因するものを除く）や参照 PIN データの改ざんによるなりすましに対抗するためのセキュリティ要件は、本稿の 3、4 節において導出したセキュリティ要件の和によって示されることとなる。ここで、セキュリティ要件の和となるのは、2 つの認証方式のいずれかが有効に機能すればなりすましを防止することができると考えられるためである。ただし、なりすましに対する安全性を向上させるために 2 つの認証方式を利用するのであれば、一方の認証方式のセキュリティ要件だけを満足させるのではなく、2 つの認証方式のセキュリティ要件を同時に満足させるよう対応することが重要である。このように、2 つの認証方式を組み合わせた本人認証システムの安全性について検討するうえで、そのセキュリティ要件の内容に着目して分析するという枠組みは有用である。

例えば、IC カード認証は共通鍵暗号を利用したオフラインの動的認証で実行し、PIN 認証にはタイプ 1 の形態を採用している場合、これら 2 つの認証方式を併用したシステムのセキュリティ要件は、[(D-1 ∨ 2 ∨ 3) ∧ (D-4 ∨ 5 ∨ 6) ∧ D-7] ∨ [(P-1 ∨ 2) ∧ P-3 ∧ P-4 ∧ (P-5 ∨ 6 ∨ 7) ∧ (P-8 ∨ 9 ∨ 10) ∧ P-12] となる。ただし、D-1〜3 と P-5〜7、および、D-4〜6 と P-8〜10 は、それぞれ同一内容のセキュリティ要件である。

既存のシステムにおけるなりすましへの耐性を評価する際には、こうしたセキュリティ要件の和を参照し、それが実際にどれだけ達成されているか（すなわち、セキュリティ要件を構成する条件がどれだけ満足されているか）を検証するという方法が考えられる。ただし、そうした検証を行う際には、本稿において導出したセキュリティ要件の内容を、適用するアプリケーションに応じて具体化したうえで要件が満たされているか否かの検証を行うことになる。

また、IC カードと PIN を併用したシステムを新たに導入する場合に、本稿において前提としたなりすましへの耐性に着目してどの形態の IC カード認証と PIN 認証を組み合わせるかを検討するうえで、本稿において導出したセキュリティ要件をベンチマークとして活用することもできる。例えば、IC カード認証と PIN 認証のセキュリティ要件の内容を調べ、アプリケーションにおいて想定されている事象が発生したときに、IC カード認証と PIN 認証の両方ともセキュリティ要件が満足

されず無効になってしまう状況が発生しないか否かを調べ、両方の認証方式がともに無効になることがない認証形態の組合せを選択するという方法が考えられる。

例えば、PIN 認証と併用する IC カード認証として静的認証を採用した場合、それぞれの認証形態におけるセキュリティ要件には、カード所持者による端末の真正性確認に関するセキュリティ要件である S-1 と P-1 が必ず含まれる。このため、仮にカード所持者によって端末の真正性が確認不可能である状況が発生し、IC カード認証と PIN 認証のどちらも有効に機能しなくなった場合には、第三者によるなりすましを防止することができなくなる。これに対して、動的認証にはカード所持者による端末の真正性確認に関するセキュリティ要件は必須ではないため、そうした状況においても IC カード認証の安全性を維持することが求められるアプリケーションにおいては、静的認証より動的認証が望ましく、PIN 認証と併用される方式の候補になると考えられる。

こうした考察は認証方式を 3 つ以上組み合わせて利用する場合においても同様に、本分析の枠組みが適用可能である。したがって、本稿において想定している形態のなりすましに対する安全性を高めることを目的として複数の認証方式を併用する場合には、各認証方式のセキュリティ要件に含まれる条件がなるべく重複しないものを選択することが望ましいと考えられる。ただし、IC カードと PIN を併用するシステムのセキュリティ要件を満足させやすいという観点からは、併用した認証方式に求められるセキュリティ要件がなるべく重複していた方が実装上望ましいという見方もありうる。このように、どのようなセキュリティ要件を有する認証方式を採用するかについては、認証方式を導入する目的の軸足をどこに置くかによって異なることとなる。

また、本人認証に加えて、サービスの提供の承認・通知の処理フローまでをスコープに入れる場合、補論において取り扱うセキュリティ要件にも考慮することが必要である。

5.2 今後の検討の方向性

5.2.1 技術面における課題

【セキュリティ要件を実現する手段の選択】

本稿では、IC カード認証については認証形態の差異、PIN 認証については参照 PIN データの格納先や PIN 照合先の差異によるセキュリティ要件の違いを明らかにすることを目的としたため、各攻撃の具体的な実現方法については明記しなかった。しかし、3、4 節で導出したセキュリティ要件に基づいてシステムを設計するためには、具体的な攻撃手法とそれへの対策手法を明確にすることが求められる。

例えば、IC カードや端末に対する侵入型攻撃、および、非侵入型攻撃としては、さまざまな攻撃手法が提案されており、それぞれ異なる対策手法が存在することとなる。そのため、各攻撃法に関する実現可能性や脅威の度合いに関してレベル付けを行うことができれば、優先的に対策すべき手法を適切に採用することが可能になると考えられる。

【検討スコープの拡張】

本稿では、第三者によるなりすましを脅威として想定し検討を行ったが、本人認証システムにおいては、なりすまし以外にも、カード所持者がカード所持者として認証されないといった脅威（本人拒否）等が存在するほか、金融取引システム全体をみれば、本人認証が正しく実行された後の金融取引に係る脅威も存在する。例えば、取引が正常に処理されないといったサービス妨害や、カード所持者による自己否認や不正請求といった攻撃等が想定されるため、こうした脅威に対するセキュリティ要件についても検討を行うことが望まれる。

また、金融業界においては本人認証を行う手段として生体認証を採用する動きや、ワンタイム・パスワードを利用する動きも見られることから、こうした認証方式に関する検討も必要である。

5.2.2 運用面における課題

【脅威に対する対策方針】

想定される対策については、本稿において検討の対象とした事前的な対策のほか、事後的な対策によって攻撃を検知するといったことが考えられる。第三者によるなりすましに対する事前的な対策によって防止困難な攻撃に対しても、当該攻撃を事後的に検知することができれば、なりすましによる被害の補填が可能となるほか、当該攻撃を事前に防止するための検討を行うことができる。したがって、事後的な対策としてどのような手法が有効であるか検討を行うことは有益である。

【拡張性のあるシステム設計】

IC カードを利用した本人認証システムを今後中・長期的に利用していくことを想定する場合には、システムに搭載した技術が危殆化する状況に備えて、当該技術を比較的容易に安全性の高いものに代替できるよう準備しておくことが必要である。例えば、IC カード認証や PIN 認証において採用する暗号技術については、暗号解読技術の進展、計算機のコスト・パフォーマンスの向上、分散コンピュー

ティング環境の整備等による安全性の低下に伴う問題に迅速かつ適切に対応できる体制の整備が求められている（宇根・神田［2005］）。システム設計者には、システムを構築する時点において、将来顕現化するおそれのある脆弱性についても考慮し、拡張性を意識したモジュールを設計することが求められる。

【国際標準・技術仕様における本人認証のセキュリティ要件】

本稿では、IC カード認証と PIN 認証において、なりすましを脅威として想定した場合に満たすべき性質をセキュリティ要件として導出することとし、セキュリティ要件を満たすための具体的な手段については明記しなかった。こうした具体的な手段については、IC カードを利用した金融取引に関連する国際標準や技術仕様を参考にすることができると考えられる。国際標準や技術仕様と本稿で導出したセキュリティ要件との対応関係を示すことは、IC カードを用いる金融向けアプリケーションのセキュリティ対策を講じる際に、国際標準・仕様に規定／記述されているセキュリティ要件のうち、どの要件を抽出・使用すればよいかを検討するうえで参考になると考えられる。

6　おわりに

IC カードは、メモリ内に秘密に格納するデータの読出しを困難とする耐タンパー性を実現する媒体であると言われており、金融分野をはじめとする幅広い分野において、本人認証を実行するためのツールとして利用され始めている。IC カードを利用したシステムを構築する際には、IC カードはもとより、システム全体に存在する脆弱性を明確にしたうえでセキュリティ要件を導出し、当該システムが同セキュリティ要件を満足しているか否かを適宜評価していくことが、安全な金融取引を実現するために必要である。

本稿では、IC カードによる所持認証（IC カード認証）と PIN による知識認証（PIN 認証）を組み合わせた本人認証システムにおいて、IC カードの開発を手掛けるセキュリティ技術の専門家と同レベルの知識・技術を有する攻撃者を想定し、第三者によるなりすましに対抗するセキュリティ要件を認証形態の差異を踏まえて導出した。まず、IC カード認証においては、動的認証と静的認証、および、オフライン認証とオンライン認証に分類したほか、利用される暗号技術のバリエーションも考慮して、偽造カードを利用したなりすましに対抗するためのセキュリティ要件の導出を行った。PIN 認証においては、PIN の照合を実行するエンティティ、および、PIN の正当性の確認に利用するデータ（参照 PIN データ）の格納先の差異による場合分けを行ったうえで、各 PIN 認証におけるセキュリティ要件を導出した。

安全な金融取引を実現するためには、本稿で導出したセキュリティ要件を満足させる具体的な手法に関する検討や、なりすまし以外の脅威に対する検討も重要であり、今後の課題としたい。

以　上

参考文献

宇根正志・神田雅透、「暗号アルゴリズムにおける 2010 年問題について」、IMES Discussion Paper Series 2005-J-22、日本銀行金融研究所、2005 年

金融情報システムセンター、「キャッシュカードシステムの課題と欧米金融機関の対応例」、『金融情報システム』No. 278、2005 夏号、2005 年 a、6〜46 頁

——、「第 10 回コンピュータシステムの安全対策状況調査報告書」、『金融情報システム』No. 281、増刊 60 号、2005 年 b、1〜178 頁

金融庁、『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〜』、http://www.fsa.go.jp/news/newsj/16/ginkou/f-20050624-4/01.pdf、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）』、http://www.fsa.go.jp/news/newsj/17/ginkou/f-20060223-3.pdf、2006 年

情報処理振興事業協会、『スマートカードの安全性に関する調査 調査報告書』、2000 年

——、『本人認証の現状に関する調査』、http://www.ipa.go.jp/security/fy14/reports/authentication/authentication2002.pdf、2003 年

総務省･経済産業省、『電子政府推奨暗号リスト』、http://www.soumu.go.jp/joho_tsusin/security/pdf/cryptrec_01.pdf、2003 年

電子商取引実証推進協議会（ECOM）、『IC カードの現状調査報告書－利用ガイドライン策定に向けた現状報告－』、1997 年

——、『IC カード利用ガイドライン（接触／非接触）』、1998 年

日本規格協会、『平成 14 年度 耐タンパー性調査研究委員会報告書』、2003 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

——・岩下直行、「インターネットを利用した金融サービスの安全性について」、『金融研究』第 21 巻別冊第 1 号、日本銀行金融研究所、2002 年、207〜226 頁

松本弘之・宇根正志・松本勉・岩下直行・菅原嗣高、「人工物メトリクスの評価における現状と課題」、『金融研究』第 23 巻別冊第 1 号、日本銀行金融研究所、2004 年、61〜140 頁

松本泰、『偽造キャッシュカード問題と認証システムの考察』、http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/03.pdf、2005 年

Anderson, Ross J., *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, 2001.

Beth, Thomas, and Yvo Desmedt, "Identification Tokens – Or: Solving the Chess Grandmaster Problem," *Proceedings of CRYPTO'90*, LNCS 537, Springer - Verlag, 1991, pp. 169–176.

Brands, Stefan, and David Chaum, "Distance-Bounding Protocols," *Proceedings of EUROCRYPT'93*, LNCS 765, Springer - Verlag, 1994, pp. 344–359.

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

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

International Organization for Standardization, *ISO 13491-1, Banking – Secure Cryptographic Devices (retail) – Part 1: Concepts, Requirements and Evaluation Methods*, 1998.

——, *ISO 13491-2, Banking – Secure Cryptographic Devices (retail) – Part 2: Security Compliance Checklists for Devices Used in Financial Transactions*, 2005a.

——, *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*, 2002.

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

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

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

Lemke, Kerstin, Ahmad–Reza Sadeghi, and Christian Stuble, "An Open Approach for Designing Secure Electronic Immobilizers," *Proceedings of IPSEC 2005*, LNCS 3439, Springer - Verlag, 2005, pp. 230–242.

補論　本人認証後からサービス提供までのフローにおけるセキュリティ要件

本人認証後における金融サービス提供時の処理のフローに着目すると、顧客の本人認証の結果は、認証者から当該サービスの提供を承諾・指示するエンティティ（以下、サービス承諾者と呼ぶ）に送信され、サービス承諾者はサービス提供の如何をメッセージとして当該サービスを実際に提供するエンティティ（以下、サービス提供者と呼ぶ）に送信する。そうした一連の手続によって、金融機関は被認証者に対してサービスを提供することになる。3、4 節では、IC カードや PIN を利用した顧客の本人認証におけるなりすましについて検討を行ったが、たとえ本人認証が失敗であろうと、エンティティ間で送受信されるデータを不正に操作する、あるいは、認証者による処理フローを改変することで攻撃者の都合のよいメッセージを認証者に出力させることができれば、攻撃者が不正にサービスを受けることが可能になるケースも考えられる。そこで、ここでは、本人認証の結果やサービス承諾のメッセージを不正に操作することで、攻撃者が真正なサービス提供者に対してカード所持者になりすますことを脅威として想定し、その脅威に対抗するためのセキュリティ要件を導出する。

例えば、CD/ATM を利用したキャッシュカード取引における預金引出しは、ホストによって本人認証が実行される場合、以下のフローで行われることが想定される。

1. ホストは CD/ATM に本人認証の結果を送信する。
2. 本人認証が成功した場合、CD/ATM は顧客に引出し金額を入力させ、本人認証が失敗した場合には取引を中止する。
3. CD/ATM は、顧客が入力した預金引出し金額をホストに送信する。
4. ホストは預金払戻しの可否のメッセージを CD/ATM に送信する。
5. CD/ATM は、ホストから預金払戻しの許可のメッセージを受け取った場合、当該金額分の現金を払戻す。

こうした一連の手続によって、顧客は預金を引き出すことができる。上記の例では、認証者とサービス承諾者はともにホスト、サービス提供者は端末（CD/ATM）となる。

本人認証、サービス承諾、サービス提供を行うエンティティとして、3、4 節と同様に、IC カード、端末、ホストを想定する。その組合せは想定するアプリケーションによってさまざまであることから、ここでは特定のアプリケーションを想定せず、2 つのエンティティ間でメッセージが送信されるというプロトコルに着目

して検討を行うこととする。以下では、本人認証の結果、あるいは、サービス承諾のメッセージをまとめてメッセージと呼び、メッセージの送受信を行うエンティティを、それぞれ送信者、受信者と呼ぶこととする。このとき、攻撃者がなりすましを行うための具体的攻撃は以下のとおりである。

― 攻撃： 真正な送信者になりすまして偽造したメッセージを送信する、あるいは、真正な送信者が生成したメッセージを改ざんする。

上記攻撃については、受信したメッセージが真正な送信者によって生成されたものであることを受信者が確認することで防ぐことが考えられる。この場合、MACやデジタル署名によってメッセージの一貫性および作成者を確認するだけでは、リプレイ攻撃等によってなりすましが可能となってしまうため、メッセージ送信者となるエンティティがそのセッションで生成したメッセージであることを受信者が確認する必要がある。こうした事項を確認する手段としては、3.1 節で紹介した動的認証が利用できる[39]。例えば、EMV（EMVCo［2004a, b］）では、MAC を利用した動的認証によりメッセージの一貫性および作成者を確認している。

動的認証を利用することで、メッセージの偽造や通信路上のメッセージの改ざんを防止できるが、攻撃モジュールが組込まれることによりプログラムが改ざんされたような IC カードや不正端末は、利用する秘密鍵が改ざんされていなければ動的認証で真正と判断される。しかし、こうした IC カードや不正端末は、正規の手順でカード所持者の本人確認を実行していない、あるいは、サービスが提供可能か否かの審査を正しく実行していないことも考えられる。そのため、メッセージの受信者はなんらかの手段でメッセージの送信者が真正なエンティティであることを確認する必要がある。

― 対策 1： メッセージの受信者は、動的認証を利用することでメッセージの一貫性および送信者を確認する。

― 対策 2： メッセージの受信者は、メッセージの送信者に攻撃モジュールが組み込まれておらず、送信者が正しく処理を実行していることを確認する。

以上の考察により、本人認証後からサービス提供までのフローにおけるセキュリティ要件として以下の 2 項目を挙げることができる。

F-1. メッセージの受信者は、動的認証によってメッセージの一貫性および送信者を確認すること。

[39]動的認証は、本来、エンティティ認証の手段であるが、被認証者による秘密鍵を用いた演算への入力としてメッセージを追加することも可能である。

F-2. 真正な IC カードや真正な端末に攻撃モジュールが組み込まれないこと。

セキュリティ要件 F-1 では、動的認証を実行することをセキュリティ要件として挙げたが、具体的には、3.1 節での IC カード・認証者間で実行される動的認証に求められるセキュリティ要件を、メッセージの送信者・受信者間に置き換えることができる。その場合、表 4 に示したように、採用する動的認証の形態に応じてセキュリティ要件の内容が決まってくることになる。また、セキュリティ要件 F-2 については、3、4 節と同様の方針での議論が可能である。

（補論おわり）