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

2006－CSEC－34 (39)
2006／7／21

# 金融取引におけるPIN認証のセキュリティ要件について[1]

田村 裕子† 宇根 正志†‡

†日本銀行金融研究所 〒103-8660 東京都中央区日本橋本石町 2-1-1
‡ 産業技術総合研究所 〒101-0021 東京都千代田区外神田 1-18-13 秋葉原ダイビル 11F
E-mail: †yuuko.tamura@boj.or.jp, ‡masashi-une@aist.go.jp

**あらまし** 金融機関では，CD/ATMによる本人認証を主にキャッシュカードと4桁の暗証番号(PIN)を利用して行っている．キャッシュカードに関しては，わが国の多くの金融機関は，カードの偽造対策の 1 つとして，従来の磁気ストライプ・カードに代えてICカードの導入を現在進めている．こうした実態を踏まえ，我々はICカードとPINを組み合わせて利用する認証システムにおけるセキュリティ要件について検討を進めている．検討にあたっては，まず，組み合わせて利用する 2 つの認証方式について別々に分析を行い，それらの分析結果を組み合わせるというアプローチを採用する．我々は，既に[2]において，被認証者が正当なICカードを所持しているか否かを確認する認証システムに焦点を当て，偽造カード作製によるなりすましに対抗するための必要条件を導出した．そこで，本稿では，次の検討の対象として，PIN を利用した認証システムに焦点を当てる．まず，ISO 9564-1に基づいて同システムを5つのタイプに分類するとともに，なりすましを目的とする具体的な攻撃方法を明らかにする．そのうえで，なりすましに対抗するための必要条件を各タイプに応じて導出する．本稿および[2]の検討結果を同時に参照することによって，なりすましを想定した場合にICカードとPINを組み合わせて利用する認証システムのセキュリティ要件を容易に得ることができる．

**キーワード** 本人認証，なりすまし，PIN，セキュリティ要件

# Security Requirements for PIN Authentication in Financial Transactions[2]

Yuko TAMURA† and Masashi UNE†‡

†Institute for Monetary and Economic Studies, Bank of Japan, 2-1-1 Nihonbashi-Hongokucho, Chuo-ku, Tokyo 103-8660 Japan
‡National Institute of Advanced Industrial Science and Technology, 11F Akihabara Dai Bldg., 1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021 Japan
E-mail: †yuuko.tamura@boj.or.jp, ‡masashi-une@aist.go.jp

**Abstract** Financial institutions authenticate their customers at CD/ATM terminals mainly by using an ATM card and a four-digit personal identification number (PIN). With regard to ATM cards, many Japanese financial institutions are now replacing conventional magnetic stripe cards with IC cards as one of countermeasures against counterfeit of ATM cards. Thus, we have been discussing security requirements for authentication systems using the combination of an IC card and a PIN. We adopt the following approach: we first analyze IC card based authentication systems and PIN based authentication systems separately, and then combine results of these analyses. So far, in [2], we focused on the IC card based authentication systems which confirmed whether the customer to be authenticated had a genuine IC card or not, and clarified necessary conditions required to be secure against an impersonation attack by counterfeiting an IC card. In this paper, we will focus on the PIN based authentication systems as a next target to be discussed. At first, we classify the systems into five types by referring to ISO 9564-1, and describe concrete methods of the impersonation attack. Then, we clarify necessary conditions to be secure against the impersonation attack in each type of the authentication systems. By referring to the results of this paper and [2] simultaneously, we can easily obtain security requirements for the authentication systems using the combination of an IC card and a PIN when assuming the impersonation attack.

**Keyword** entity authentication, impersonation, PIN, security requirement

[1] 本稿に示されている意見は，著者たち個人に属し，日本銀行あるいは産業技術総合研究所の公式見解を示すものではない．
[2] Views expressed in this paper are those of the authors and do not necessarily reflect the official views of the Bank of Japan or National Institute of Advanced Industrial Science and Technology.

## 1. はじめに

金融機関では，CD/ATM 等による本人認証を主にキャッシュカードと 4 桁の PIN を利用して行っている．近年，偽造キャッシュカード問題を回避することを目的としてキャッシュカードの IC カード化が進められているが，キャッシュカードが耐タンパー性を有していたとしても，本人認証システムが適切に構築されていなければ，その脆弱性によりなりすましが容易となる可能性がある．安全な金融取引を実現するためには，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必要である．

そこで，金融分野におい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，各認証方式の単独での効果を明らかにするため，[2]では，まず IC カードによる所持認証システムのセキュリティ要件の導出を行った．

本稿では，PIN による知識認証において，なりすましを目的とする攻撃方法を明確にしたうえで，そのセキュリティ要件を導出することとする．具体的には，PIN の照合を実行するエンティティ，および，PIN の正当性確認の際に参照するデータを格納するエンティティの差異による認証形態を考慮した分析を行う．

## 2. PIN 認証について

### 2.1. 想定するアプリケーションとエンティティ

機械を介した主な金融取引には，CD/ATM や POS 端末を利用したキャッシュカード・クレジットカード取引，パソコンやモバイル端末を利用したオンライン・バンキング等が挙げられる．本稿では，こうしたアプリケーションにおいて，PIN を利用する本人認証システムを想定し，当該システムを構成するエンティティを以下のように定義する．

- PIN 登録者：PIN に対応するエンティティとして金融機関に登録されているユーザ．
- IC カード：端末と通信を行うとともに，PIN の照合等の処理が実行可能なデバイス．こうした機能を実現するデバイスの形態としてはさまざまなものが考えられるが，現在金融分野では IC カードが採用されつつあることから，本稿では上記デバイスを「IC カード」と呼ぶこととする．また，金融機関が正規の手続に沿って配付したものは「真正な IC カード」と呼ぶ．

| 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 1：PIN 認証の 5 つの形態

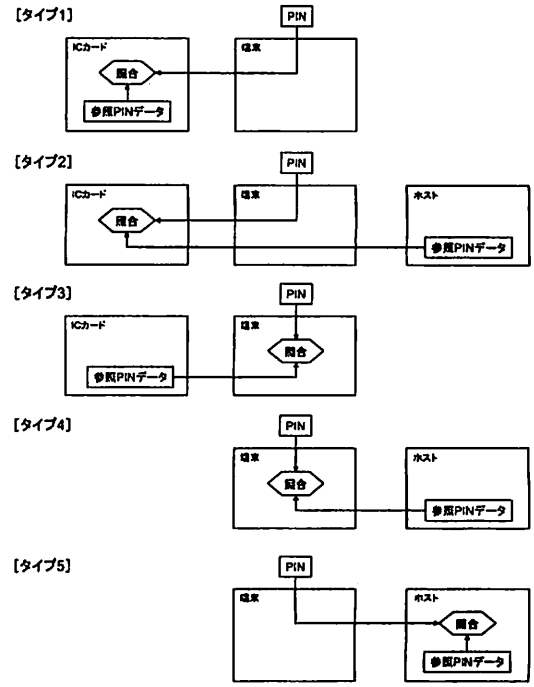



図 1：各 PIN 認証におけるデータの流れ

- ホスト：金融機関内に設置され，ネットワークを介して，本節で想定しているアプリケーションを提供するコンピュータ．金融機関により，設備・運用面の種々のセキュリティ対策が施され安全に管理されていると仮定する．
- 端末：被認証者や IC カードと直接通信を行い，被認証者・IC カード・ホスト間の通信を媒介するデバイス．端末は，PIN パッドおよびカード・リーダ／ライタが一体化して形成されるものとする．攻撃者によって PIN を盗取することを目的とした細工が加えられていないものは「真正な端末」と呼ぶ．

### 2.2. PIN 認証の形態

本稿では,「被認証者によって端末に入力されたPINが,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」をPIN認証と呼ぶ.また,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)を指すこととする.PIN 認証では,被認証者が身元を示す情報(ユーザ ID)と PIN を提示し,認証者はユーザ IDと対応付けられた参照PINデータと当該PINの照合を行う.

PIN 認証は,PIN の照合先や参照PIN データの格納先の違いによって,いくつかのタイプに分類することができる.こうしたエンティティとしては,IC カード,端末,ホストのいずれかが想定されるが,本稿では,金融分野における PIN の管理に関する国際標準 ISO 9564-1[5]を参照し,表1の5つのPIN認証の形態(タイプ1〜5,図1参照)について検討を行うこととする[3].

## 3. PIN 認証に対する攻撃

### 3.1. 想定する脅威

IC カードを利用した本人認証システムに対する脅威の中でも最も代表的なものとして,なりすましが挙げられる.こうした脅威に対抗するためには,技術面および運用面での対策の有効性に関する検討が必要となるが,本稿では,PIN 認証のみに依拠したシステムを想定し,PIN 登録者へのなりすましに対する技術的な対策に焦点を当てることとする.なお,こうしたシステムについては,金融機関や端末メーカー等の内部者が関与する形で不正が発生する可能性もあるが,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)と仮定する.

PIN 認証におけるなりすましの手段としては,以下の2つが考えられる.

① なりすまし対象であるユーザの 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ユーザの参照 PIN データを改ざん・偽造する.

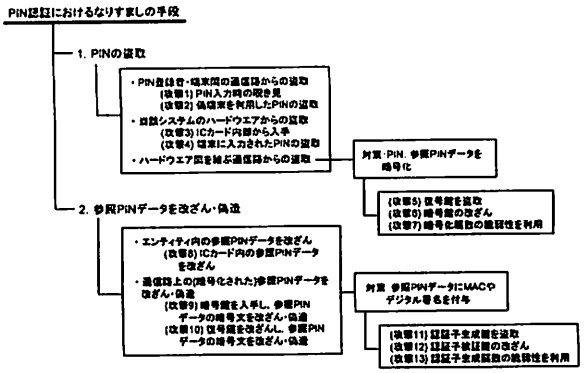



図 2:本稿で検討する具体的な攻撃手段

| PIN 認証の形態 | 想定される攻撃 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1, 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9~13 |
| タイプ 1 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| タイプ 2 | ○ | | ○ | ○ | ○ | ○ | | ○ |
| タイプ 3 | ○ | | ○ | ○ | ○ | ○ | ○ | ○ |
| タイプ 4 | ○ | | ○ | ○ | | ○ | | ○ |
| タイプ 5 | ○ | | ○ | ○ | ○ | ○ | | |

表 2:各 PIN 認証の形態において想定される攻撃

上記①,②については,それぞれ 3.3 節,3.4 節において検討を行うこととする.3.3 節,3.4 節で取り上げる攻撃を整理すると図2となり,各認証形態において想定される攻撃は表2のとおりである.

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,PIN 登録者の IC カードを既に入手しているものとして議論を進める.

まず,PIN 認証の安全性を考察するうえで利用する用語を定義する.

- 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
- 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[4].
- 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:PIN 登録者,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.

[3] IC カードを利用しないタイプ 4, 5 では,ユーザ ID の提示を IC カード以外の媒体(磁気ストライプ・カード等)によって行うことも考えられる.

[4] 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.

### 3.2. 攻撃者の能力

本稿で想定する攻撃者は，システム設計者と同レベルの知識・技術を有し，以下の能力を持つものとする．

- IC チップ内に格納すべき情報を入手すれば，同じ機能を実現する IC カードを作製可能である．
- IC カードや端末内で秘密に格納されている情報以外の情報（例えば，認証方式の実行手順や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・端末間，および，端末・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，内部信号を直接観察する等の手段によって内部データの不正入手・改ざんする攻撃（以下，侵入型攻撃[1,3]と呼ぶ）を試行する．
- IC カードや端末に対して，故障利用攻撃やサイドチャネル攻撃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情報を不正に入手する攻撃（以下，非侵入型攻撃[1,3]と呼ぶ）を試行する．

### 3.3. PIN を盗取する攻撃

3.1 節で述べたなりすまし手段のうち，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 データの盗取先としては，①PIN 登録者・端末間の通信路，②当該システムのハードウエア（IC カード，端末），③ハードウエア間を結ぶ通信路，④PIN 登録者自身の 4 つが考えられる．このうち，上記④の PIN 登録者自身から盗取する方法としては，ソーシャル・エンジニアリング[5]や，PIN 登録者による PIN の不適切な管理を巧みに利用する方法が挙げられる．上記④のような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，他の認証手段等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，本稿では検討の対象外とする．

以下では，上記①~③から PIN あるいは参照 PIN データを盗取する攻撃として想定される手段を列挙する．

#### ① PIN 登録者・端末間の通信路からの盗取

PIN 認証では，PIN 登録者は端末に PIN を入力する必要があることから，PIN 認証のすべてのタイプにおいて以下の攻撃が想定される．

- 攻撃 1：PIN 登録者による 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 2：偽端末の利用により，PIN 登録者によって入力された PIN を盗取する．

#### ② 当該システムのハードウエアからの盗取

IC カード内に，外部に出力されないデータとして参照 PIN データが格納されるタイプ 1 では，以下の攻撃 3 が想定される[6]ほか，すべてのタイプにおいて端末に入力された PIN を盗取する攻撃 4 が想定される．

- 攻撃 3：不正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．
- 攻撃 4：不正端末や攻撃モジュールの利用により，PIN 登録者によって入力された PIN を端末から盗取する．

#### ③ ハードウエア間を結ぶ通信路からの盗取

PIN の照合を端末以外で実行するタイプ 1，2，5 と，参照 PIN データの格納先と PIN の照合先が異なるタイプ 2~4 では，それぞれ PIN や参照 PIN データがハードウエア間を通信されるため，データを盗取するための IC カード，不正・偽端末や偽ホストの利用，あるいは，通信路の盗聴によってデータを盗取する攻撃が想定される．

本稿では，ハードウエア間を結ぶ通信路からのデータ漏洩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[7]こととし，PIN の照合は復号し

---

[5] 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[6]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．

[6] タイプ 3 においても，IC カード内に参照 PIN データが格納されるが，タイプ 3 では IC カードの正規出力チャンネルから参照 PIN データを盗取する攻撃が想定されるため，こうした攻撃については，「③ハードウエア間を結ぶ通信路からの盗取」で取り扱う．

[7] 暗号化に共通鍵暗号を利用する場合には，真正なハードウエア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．

て得た平文を利用して行うこととする．その場合に想定される攻撃を以下に挙げる(図 3 参照)．

- 攻撃 5:復号鍵を盗取し，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．
- 攻撃 6:暗号鍵を改ざんし，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．
- 攻撃 7: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．

暗号鍵や復号鍵が格納されるエンティティについては，PIN 認証の形態，および，利用する暗号アルゴリズムによって異なるため，表 3 にまとめることとした．そのほか，参照 PIN データを暗号化して送信する場合には，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 3 が想定されることとなる．

### 3.4. 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，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 PIN 登録者の参照 PIN データを改ざん・偽造するという手段もある．具体的な方法としては，①真正なエンティティ内に格納されている参照 PIN データを改ざんするケースと，②通信路上の参照 PIN データを改ざん・偽造するケース[8]が考えられる．

上記①は IC カード内に参照 PIN データが格納されるタイプ 1，3 に想定される攻撃であり，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．いま，ハードウエア間を結ぶ通信路から PIN を盗取する攻撃への対策としてハードウエア間で送受信されるデータを暗号化することとすれば，上記②における改ざん後のデータは正しい暗号文(データの受信者の復号鍵に対応する暗号鍵で生成された暗号文)である必要がある．したがって，上記②を実行する際には，攻撃者は，暗号鍵を盗取する，あるいは，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ことが必要になる．

具体的な攻撃手段は以下のとおりであり(図 4 参照)，攻撃対象となるエンティティについては表 3 にまとめている．なお，攻撃 9，10 の攻撃対象はそれぞれ暗号鍵の入手先および復号鍵の改ざん先であり，暗号化関数として公開鍵暗号を利用する場合については，公開鍵証明書が容易に入手可能であることから，攻撃対象となるエンティティは特段存在しないこととなる．

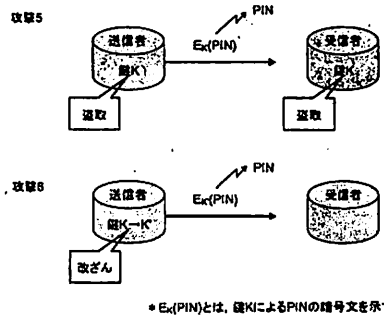



図 3:PIN を盗取する攻撃(攻撃 5，6)の概念図
(通信データの暗号化に共通鍵暗号を利用する場合)

- 攻撃 8:IC カード内に格納されている参照 PIN データを改ざんする．
- 攻撃 9:(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 10:(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．

攻撃 8～10 は，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 データの格納先と PIN の照合先が異なる認証形態(タイプ 2～4)における攻撃(攻撃 9，10，タイプ 3 に対する攻撃 8)では，別の対策方法として，参照 PIN データが改ざんされていないことを確認可能とする機構を採用することが考えられる．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，金融機関による 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認証子生成鍵を盗取する，②認証子検証鍵を改ざんする，③認証子生成

[8] 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．

関数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．そこで，これらの攻撃を攻撃 11～13 として以下に挙げるとともに，攻撃対象となるエンティティを表 3 にまとめる．

- 攻撃 11: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 12: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 13: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．

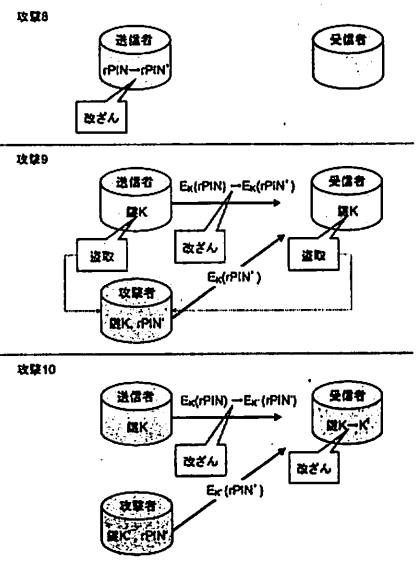
## 4. PIN 認証のセキュリティ要件

### 4.1. 想定する攻撃に対する対策法

まず，攻撃 1 については，PIN の入力時における覗き見を防止する対策と，たとえ覗き見された場合にも，その様子から PIN の推測が困難となるような機構を採用するという対策が考えられる．

攻撃 2 への対策としては，PIN 登録者が端末の真正性を確認可能であるような機構を採用することが考えられる．

攻撃 3~6 と攻撃 8~12 は，ハードウエア(IC カード，端末)内に格納されるデータ(PIN，参照 PIN データ，暗号鍵，復号鍵，認証子生成鍵，認証子検証鍵)を改ざん・盗取する攻撃である．こうした攻撃への対策としては，データの改ざん・盗取を防止する方法と，改ざん・盗取されたデータの利用を防止する方法が挙げられる．データの改ざん・盗取を防止する方法としては，①攻撃に対する防御技術




＊rPINとは参照PINデータを表し，$E_K(rPIN)$とは，鍵KによるrPINの暗号文を示す．

図 4:参照 PIN データを改ざん・偽造する攻撃
(攻撃 8～10)の概念図
(通信データの暗号化に共通鍵暗号を利用する場合)

を当該デバイスに組み込むといった受動的対策と，②攻撃を検知し，内部データを自動的に消去する機構等を当該デバイスに組み込むといった能動的対策が挙げられる．また，改ざん・盗取されたデータの利用を防止する方法としては，たとえ内部データが改ざん・盗取されてしまった場合でも，金融機関によってその事実が把握され，速やかに当該データに対応する PIN を無効化することで，攻撃者による不正を困難にするという対策が考えられる．こうした対策は次節のセキュリティ要件 SR4～6，7～9 に対応する．そのほか，参照 PIN データについては，仮に漏洩した場合においても，参照 PIN

| PIN 認証の形態 | 攻撃 5 | | 攻撃 6 | 攻撃 8 | 攻撃 9 | 攻撃 10 | 攻撃 11 | 攻撃 12 |
|---|---|---|---|---|---|---|---|---|
| | 利用する暗号技術 | | | | | | | |
| | 共通鍵暗号 | 公開鍵暗号 | 共通鍵・公開鍵暗号 | | 共通鍵暗号 | 共通鍵・公開鍵暗号 | MAC | MAC・デジタル署名 |
| タイプ 1 | IC カード 端末 | IC カード | 端末 | IC カード | —— | —— | —— | —— |
| タイプ 2 | IC カード 端末 | IC カード | 端末 | —— | IC カード | IC カード | IC カード | IC カード |
| タイプ 3 | IC カード 端末 | 端末 | IC カード | IC カード | IC カード 端末 | 端末 | 端末 | 端末 |
| タイプ 4 | 端末 | 端末 | —— | —— | 端末 | 端末 | 端末 | 端末 |
| タイプ 5 | 端末 | —— | 端末 | —— | —— | —— | —— | —— |

表 3:各攻撃の対象となるエンティティ

データからPINの復元が困難であればPINの漏洩を防止することができると考えられる.

攻撃 8～10 については，上記の対策のほか，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 11～13 への対策を講じることが考えられる. すなわち，攻撃 8～10 への対策としては，「攻撃 8～10 の対象となるハードウエアへの耐タンパー性の付与」，または，「攻撃 11，12 の対象となるハードウエアへの耐タンパー性の付与，および，攻撃 13 に対する対策」が必要となる. なお，暗号化に公開鍵暗号を利用するケースにおける攻撃 9 については，暗号鍵が公開されるケースを想定していることから，暗号鍵を格納するハードウエアの耐タンパー性によって対策することができないため，後者の対策によって攻撃を防ぐことが必要となる.

そのほか，採用する暗号化関数や認証子生成関数の脆弱性を利用する攻撃 7 と攻撃 13 については，そうした攻撃に対して安全であると評価されたものを利用することが求められる.

### 4.2. セキュリティ要件

前節における対策方針から，PIN 認証のセキュリティ要件を以下の 12 項目にまとめることができる.

[SR1] PIN 登録者による PIN の入力時の様子を覗き見されないこと.

[SR2] PIN 登録者による PIN の入力時の様子から PIN の推定を困難とすること.

[SR3] PIN 登録者が端末の真正性を確認可能であること.

[SR4] 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[9]であること.

[SR5] 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.

[SR6] 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[10]であること.

[SR7] 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.

[SR8] 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.

[SR9] 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.

[SR10] 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.

[SR11] データの送受信に利用する暗号化関数は，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.

[SR12] 参照 PIN データの一貫性確保に利用す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.

| 想定する攻撃 | 各攻撃に対応するセキュリティ要件 |
|---|---|
| 攻撃 1 | SR1, SR2 |
| 攻撃 2 | SR3 |
| 攻撃 3 | SR4~6, SR10 |
| 攻撃 4 | SR7~9 |
| 攻撃 5 | SR4~6, SR7~9 |
| 攻撃 6 | SR4~6, SR7~9 |
| 攻撃 7 | SR11 |
| 攻撃 8 | SR4~6 |
| 攻撃 9 | SR4~6, SR7~9 |
| 攻撃 10 | SR4~6, SR7~9 |
| 攻撃 11 | SR4~6, SR7~9 |
| 攻撃 12 | SR4~6, SR7~9 |
| 攻撃 13 | SR12 |

表 4: 各攻撃と対応するセキュリティ要件

| PIN 認証の形態 | セキュリティ要件 (SR) | | | | | |
|---|---|---|---|---|---|---|
| | 1∨2 | 3 | 4∨5∨6 | 7∨8∨9 | 11 | 12 |
| タイプ 1 | ○ | ○ | ○ | ○ | ○ | |
| タイプ 2 | ○ | ○ | ○ | ○ | ○ | ○ |
| タイプ 3 | ○ | ○ | ○ | ○ | ○ | ○ |
| タイプ 4 | ○ | ○ | | ○ | ○ | ○ |
| タイプ 5 | ○ | ○ | | ○ | ○ | |

(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. 例えば，タイプ 1 の PIN 認証のセキュリティ要件は，「(SR1∨2)∧SR3∧(SR4∨5∨6)∧(SR7∨8∨9)∧SR11」となる.

表 5: 各認証方式のセキュリティ要件

3 節で列挙した各攻撃とそれに対応するセキュリティ要件の関係を表 4 に整理する. その際，侵入型攻撃への対策は，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に対応させることとした. また，攻撃 5，6，9～12 については，PIN 認証の形態によりその攻撃対象が異なるため，IC カードおよび端末に関するセキュリ

[9] 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[4].

[10] 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対して能動的に対抗する機能を有するデバイスの特性を指す[4].

ティ要件に対応する形となっている.

こうしたセキュリティ要件と想定する攻撃の対応関係と, 表 2 に示した各 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 5 参照). 1 つの攻撃に対して複数のセキュリティ要件が対応するセキュリティ要件 SR1, 2, および, SR4～6, および, SR7～9 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攻撃を防ぐことができると考えられる. ただし, 各要件を完全に実現することが困難である場合には, 複数のセキュリティ要件を満足させるよう対策を施すことが望ましい.

## 5. 考察とまとめ

IC カードを利用した本人認証のセキュリティ要件について検討を進めるにあたって, [2]では IC カード認証について分析を行い, 本稿では PIN 認証について分析を行った. 両者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を想定した場合, IC カードの偽造および PIN の盗取や参照 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, それぞれの認証方式におけるセキュリティ要件の和によって示されることとなる. 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のみならず, 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.

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, [2]および本稿で導出したセキュリティ要件の和を参照し, それが達成されているかを検証する方法が考えられる. 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は, どの形態の認証方式を組み合わせるかを検討するうえで, [2]および本稿で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, ある事象が発生したときに, 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たうえで, 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方法が考えられる. ただし, 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と考えられる.

[2]および本稿では, なりすましを脅威として想定した場合のセキュリティ要件を, 各認証方式の形態を考慮して導出した. 安全な金融取引を実現するためには, 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, そうした検討については今後の課題である.

## 文　献


[1] 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.

[2] 田村裕子, 宇根正志, "金融取引における IC カード認証のセキュリティ要件について, "SCIS2006 予稿集, 2006 年.

[3] 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.

[4] International Organization for Standardization, ISO 13491-1, Banking − Secure cryptographic devices (retail) − Part 1: Concepts, requirements and evaluation methods, 1998.

[5] International Organization for Standardization, 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.

[6] Ross J. Anderson, A guide to Building Dependable Distributed Systems, Wiley Computer Publishing, 2001.