生体認証システムにおける情報漏洩対策技術の研究動向

鈴木雅貴（すずき まさたか）／井沼　学（いぬま まなぶ）／大塚　玲（おおつか あきら）

要　旨

生体認証技術は、個人の身体的な特徴等を用いた認証技術であり、わが国では ATM における顧客の本人確認等に活用されている。生体認証には、認証に利用される身体的な特徴等を変更困難という特徴がある。仮に、生体情報が第三者に知られた場合には、なりすましの脅威から、当該情報を用いた認証をそれ以降利用不可能になる可能性がある。また、同一の生体情報がさまざまなアプリケーションで利用される場合、どこか 1 つのシステムから生体情報が漏洩すると、他のシステムへも影響が波及するおそれがある。

こうした問題に対して、登録される生体情報や認証時に取得される生体情報に特殊な変換を施し、それらが漏洩したとしても生体情報自体の推定や、なりすましを防止する技術（テンプレート保護型生体認証技術）が注目を集めている。ただし、本技術は現在研究途上にあり、IC カードに各ユーザーの生体情報を格納するという ATM での利用形態を想定した研究は少ない。また、テンプレート保護型生体認証技術の評価方法も確立されておらず、既存の提案方式が ATM のシステムにおいて有効か否かが明確になっていない。

本稿では、IC カードに生体情報を格納するタイプの生体認証システムに焦点を当ててなりすましへの耐性について分析を行う。その結果として、テンプレート保護型生体認証技術を適用したとしても、なりすましへの耐性が常に向上するとは限らないことを示す。そのうえで、テンプレート保護型生体認証技術を導入する際には、システムをどのように構成すればなりすましへの耐性が向上するかを検討することが重要であることを示す。

キーワード：生体認証システム、なりすまし、情報漏洩、テンプレート保護型生体認証技術、キャンセラブル・バイオメトリクス、IC カード、ATM

本稿の作成に当たっては、日立製作所の高橋健太氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行および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。

鈴木雅貴　日本銀行金融研究所（E-mail: masataka.suzuki@boj.or.jp）
井沼　学　独立行政法人産業技術総合研究所（E-mail: inuma.manabu@aist.go.jp）
大塚　玲　独立行政法人産業技術総合研究所（E-mail: a-otsuka@aist.go.jp）

1. はじめに

生体認証技術は、静脈パターンや指紋といった個人の身体的な特徴や、手書署名や声紋といった行動的な特徴（これらを以下では生体特徴と呼ぶ）を読み取ってデジタル・データに変換し、同データ（以下、生体情報と呼ぶ）を用いて認証を行う技術である。わが国の金融機関は、2004 年頃から、ATM における顧客の本人確認をはじめ、PC のログインや入館管理等のさまざまな用途にこうした生体認証を実現するシステム（以下、生体認証システムと呼ぶ）を利用している。

生体認証システムにおける代表的な脅威として、同システムに対して別の個人になりすますという脅威が知られており、学界をはじめとして盛んに研究が進められている。実際になりすましが成功してしまった場合には、例えば、ATM における不正な預金の引出しや建物への侵入につながる可能性があることから、この脅威にどのような対策を講じるかが重要となっている。わが国の金融機関が金融情報システムにおける情報セキュリティ対策を講じる際の指針としている金融情報システムセンター（FISC）の『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』（FISC [2009]）においては、なりすましについて技術や運用による対策を講じる必要があると記述している。また、本基準においては、生体認証システムに登録されたユーザーの生体情報（以下、参照データと呼ぶ）が漏洩した場合の問題についても記述されており、参照データがなりすましに流用されうると指摘したうえで、参照データが漏洩した場合の対策の研究動向にも留意することが望ましいと記述している（FISC [2009] の技術 35-1）。特に、生体情報は通常変更困難であることから、いったん参照データが漏洩した場合、当該生体認証システムを利用できなくなる可能性がある。

生体認証システムの情報漏洩への対策に関しては、近年、学界において盛んに研究開発が行われている。特に、参照データが漏洩したとしてもそのままではなりすましに利用することができないように、参照データに特殊な変換を行い、変換した状態のまま照合を行うという方式が活発に研究されている。こうした方式を総称する用語は学界において定まっていないことから、本稿では「テンプレート保護型生体認証技術」と呼ぶことにする。本技術の研究動向をみると、ネットワーク上のサーバーがユーザーの参照データを一元管理し照合を行うというタイプの生体認証システムが想定されることが多い。一方、ATM で利用されている生体認証システムをみると、参照データが個々のユーザーの IC カード内に格納されており、学界で検討されているシステムのタイプとは異なっている。こうしたことから、ATM で利用されるシステムに現在学界で検討されている方式を適用した際の効果については明確になっていないのが実情である。また、本技術は研究が活発化してきているものの、評価方法が十分に確立されるまでには至っていない。

そこで、本稿では、ATM における生体認証システムのように参照データを IC カードに格納するタイプのシステムに焦点を当てて、そうしたシステムにテンプレート

保護型生体認証技術を適用した際の効果を分析するとともに、本技術の研究動向から今後の研究課題を考察する。

まず、平文の参照データあるいは暗号化した参照データを IC カードに格納するタイプのシステムを取り上げ、攻撃者が IC カードから平文の参照データを盗取するケース等ではなりすましが高い確率で成功する場合があることを示す。次に、テンプレート保護型生体認証技術を適用したシステムを取り上げ、システムからの漏洩情報を用いたなりすましへの耐性を分析し、IC カード内で特殊な変換と照合を行うという方式の場合には高い確率でなりすましが成功する可能性があることを示す。こうした分析結果を踏まえると、テンプレート保護型生体認証技術を導入する際には、適用対象となっているシステムの構成を十分に考慮したうえで、当該技術の効果を見極める必要があるといえる。今後学界においては、テンプレート保護型生体認証技術のセキュリティ評価方法の検討の進展が期待される。

以下では、まず、2 節において、平文の参照データあるいは暗号化した参照データを IC カードに格納するタイプの生体認証システムと IC カードや端末から情報を盗取する攻撃者を示し、各システムのなりすましへの耐性を分析する。3 節では、テンプレート保護型生体認証技術の基本アイデアと既存研究をベースにした評価の現状を説明し、4 節において、テンプレート保護型生体認証技術を適用したシステムのなりすましへの耐性を分析する。5 節では、金融機関が本技術を利用する際の留意点と本技術の今後の研究課題を示す。

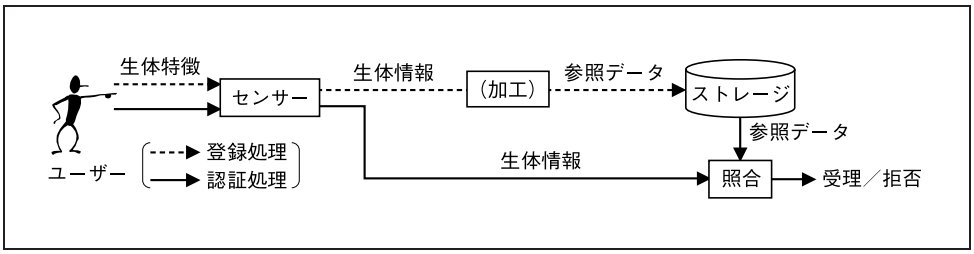
2. IC カードを用いた生体認証システムにおける情報漏洩の影響

(1) 検討対象とする生体認証システム

イ. 基本構成

生体認証システムにおいては、センサーを用いて生体特徴からデジタル化した情報（生体情報）を取得する。例えば、生体特徴として静脈パターンを用いる場合、生体情報は静脈パターンの画像や同画像から抽出した情報となる。登録時には、生体情報を加工して登録用のデータ（参照データ）を生成し、IC カード等のストレージに格納する。参照データは、漏洩への対策のために共通鍵暗号等のアルゴリズムによって暗号化されるケースも想定される。認証時には、提示された生体特徴から生体情報を取得し、参照データと照合する。本人と判断した場合には「受理」を、そうでない場合には「拒否」をそれぞれ出力する（図表 1 参照）。参照データが暗号化されるケースでは復号してから照合が行われる。なお、以下では、表記の簡略化のために生体特徴をセンサーで読み取る処理の記述を省略し、処理が生体情報の取得からスタートする表記とする。

図表 1　一般的な生体認証システムの処理フロー



ロ．検討対象の生体認証システム

（イ）IC カードを用いた 3 つの形態

本稿では、ATM における顧客の本人確認に利用される生体認証システムを想定し、個々の IC カードに参照データを格納するケースを検討対象とする。そうした生体認証システムには、①生体情報の取得や照合を IC カード外で行う「STOC（Store on Card）形態」、② IC カード外で生体情報を取得して IC カード内で照合を行う「MOC（Match on Card）形態」、③ IC カード内で生体情報の取得と照合を行う「SOC（System on Card）形態」が知られている（財団法人ニューメディア開発協会［2005］）。現行の ATM における生体認証システムは、IC キャッシュカード、ATM、金融機関のホスト・システムから構成されており、ATM において生体特徴の読取りを行っている。そこで、IC カード（参照データを格納）、端末（生体情報の取得）、サーバーからなるシステムに対応する STOC 形態と MOC 形態の生体認証システムを検討対象とする。なお、端末は、IC カードやサーバーと直接通信する一方、IC カード・サーバー間の通信は端末を介して行われると想定する。

（ロ）STOC 方式と MOC 方式

生体認証システムは、データの格納場所とその処理の実行場所によって分類することができる。こうした分類に基づき STOC 形態および MOC 形態の生体認証システムとしてさまざまなバリエーションが考えられるものの、本節では各形態に基づくシステムの一例として次の生体認証システムを検討対象とする（図表 2 参照）[1]。

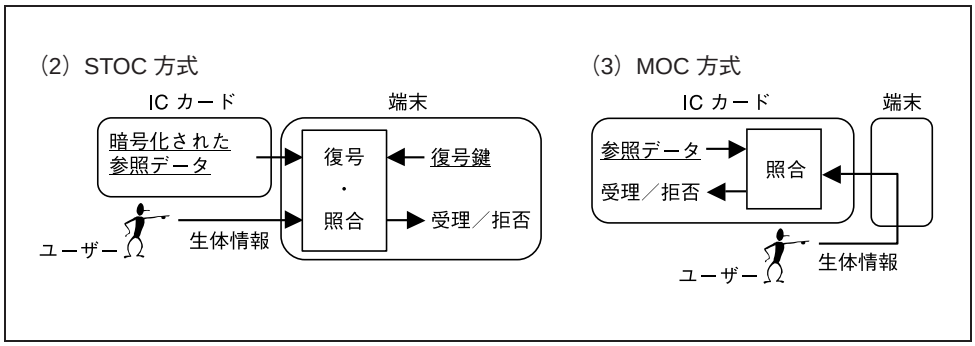
- STOC 方式：端末は、ユーザーから生体情報を取得するとともに、予め端末に格納された復号鍵を用いて暗号化された参照データを復号し、照合を行う。
- MOC 方式：IC カードは、参照データと端末から受信した生体情報を用いて照合を行う。

1 STOC 形態および MOC 形態の生体認証システムのうち、本節で取り上げないタイプのシステムについては補論 1 を参照されたい。

図表 2　STOC 方式と MOC 方式

(1) データの格納場所と処理の実行場所

	各エンティティにおいて格納されるデータ、および、実行される処理	
	IC カード	端末
STOC 方式	（データ）暗号化された参照データ	（データ）復号鍵 （処理）復号・照合
MOC 方式	（データ）参照データ （処理）照合	–



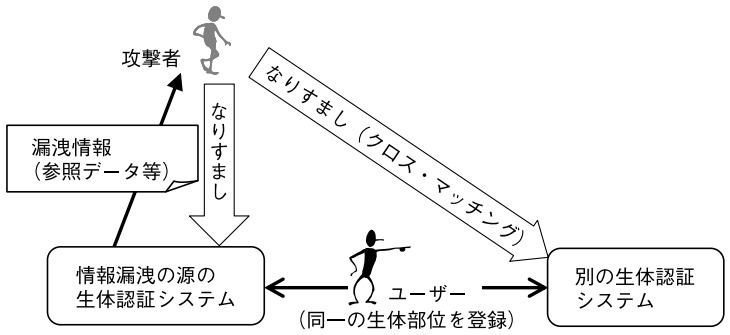
備考：下線は、IC カードや端末に格納されているデータであることを示す。

(2) 想定される攻撃

生体認証システムに対する代表的な脅威としてなりすましが挙げられる。本稿では、近年注目されている生体認証システムから漏洩した情報（参照データ等）を用いたなりすましを検討対象とする。こうしたなりすましにおいては、情報が漏洩した生体認証システムだけでなく、別の生体認証システムも攻撃対象となる可能性がある（図表 3 参照）。例えば、ユーザーが複数の生体認証システムにおいて同一の生体部位（同じ指や掌の静脈パターン等）を使用している場合、セキュリティ・レベルが相対的に低いシステムから参照データ等が漏洩し、他のシステムへのなりすましに悪用される可能性がある。こうした問題は「クロス・マッチング」と呼ばれている（Ratha, Connell, and Bolle [2001]）。クロス・マッチングによりなりすましが発生した場合、なりすましによる直接の被害を受けたシステムだけでなく、データを漏洩させたシステムもレピュテーションの低下等の影響を受ける可能性がある。

漏洩情報を用いたなりすましとして特に注目すべき攻撃として、「ブルート・フォース攻撃」と「ヒルクライミング攻撃」がある。ブルート・フォース攻撃は、多種多様な生体情報を用いて照合を行うことで、本人として誤って受理されてしまうような生体情報を探索する攻撃である。生体認証システムが他人を本人として誤って受理するケースは、一定の確率（「他人受入率」と呼ばれる）でしか発生しないものの、例えば、照合アルゴリズムが公開されており、攻撃者が参照データを入手している場

図表３　漏洩情報を用いたなりすまし



合には、本攻撃が実行可能になる[2]。ヒルクライミング攻撃は、照合時に算出される類似度が高くなるように提示する生体情報を修正していくことで、本人として誤って受理される入力を探索する攻撃である（Hill [2001]、Adler [2003]）[3]。

探索した生体情報を人工物によって物理的に再現し、生体認証システムに提示することでなりすましが成功する可能性がある。例えば、一部の市販のシステムにおいて、本人の指紋画像を基にゼラチン等の人工物で再現した偽物が誤って受け入れられてしまうという事例が報告されている（Matsumoto, Matsumoto, Yamada, and Hoshino [2002]）[4]。

本稿では、当該システムに対して主張される「本人」とは異なる攻撃者が生体特徴（あるいは人工物の物理的特徴）等を当該システムに提示したときに、当該システムが受理を出力することを「なりすましが成功する」とする。

(3) 検討対象とする攻撃者

攻撃者に関しては、①生体認証システムの構成に関する知識を有しているものの、②攻撃対象のユーザーの生体特徴を知らないほか、③参照データの暗号化等に用いられる暗号アルゴリズムを解読できないとする。そのうえで、IC カードの入手可能性や解析能力に応じて攻撃者の分類を行う（図表４参照）。

2 例えば、他人受入率が 0.01% の場合、適当に選択した生体情報を用いた照合を 1 万回繰り返せば確率的には受理されるような生体情報を見つけることができると考えられる。

3 Adler [2003] は、修正を 4,000 回繰り返すことで受理される顔画像を探索したと報告している。

4 人工物への対策として、生体認証システムへの提示物が生体か否かを検知する生体検知技術が知られているが、現在研究途上にあり、当該技術の評価方法の確立は今後の重要な課題となっている（鈴木・宇根［2009］）。

図表 4　検討対象とする攻撃者の各エンティティに対する能力

<table>
<tr><th></th><th colspan="3">各エンティティに対する攻撃者の能力</th></tr>
<tr><th></th><th colspan="2">IC カード</th><th>端末</th><th>サーバー</th></tr>
<tr><td>攻撃者 1</td><td rowspan="4">正規の IC カードを利用</td><td>同カードの解析せず</td><td colspan="2" rowspan="3">解析せず</td></tr>
<tr><td>攻撃者 2</td><td>同カードから送信される情報の盗取</td></tr>
<tr><td>攻撃者 3</td><td rowspan="2">同カード内部の情報の盗取</td></tr>
<tr><td>攻撃者 4</td><td colspan="2">端末やサーバーから IC カードに送信される情報を盗取</td></tr>
<tr><td>攻撃者 5</td><td rowspan="2">正規の IC カードを利用せず</td><td>端末に送信される情報の盗取</td><td>メモリー上のデータの盗取</td><td>端末に送信される情報の盗取</td></tr>
<tr><td>攻撃者 6</td><td colspan="2">端末や IC カードからサーバーに送信される情報の盗取</td><td>メモリー上のデータの盗取</td></tr>
</table>

イ．正規の IC カードを盗取して利用する攻撃者

キャッシュカードの紛失や盗難が少なからず発生している状況[5]を踏まえると、攻撃者が正規の IC カードを盗取するという状況を前提とすることが求められる。そうした攻撃者として攻撃者 1〜4 を次のとおり想定する。

- **攻撃者 1**：盗取した正規の IC カードの解析を行わず、同カードを端末に提示してなりすましを試みる。
- **攻撃者 2**：IC カード・端末間での正規の処理において IC カードから送信される情報を盗取し、その情報を利用してなりすましを試みる[6]。
- **攻撃者 3**：IC カード内部の情報（参照データや復号鍵等）を盗取し、それらを利用してなりすましを試みる。攻撃者 2 は認証時に IC カードから送信される情報のみを盗取する一方、本攻撃者はそうした情報に加えてカード内部の情報をすべて盗取するとする。
- **攻撃者 4**：IC カード内部に格納されている情報に加え、正規の IC カードの処理時に端末、サーバーから同カードに対して送信される情報を盗取したうえで、それらの情報を利用してなりすましを試みる[7]。

ロ．正規の IC カードを利用しない攻撃者

ATM や金融機関サーバー上での攻撃を想定する場合には、ATM 等に不正なソフトウエアを仕掛けて口座番号や PIN を盗取するといった可能性を考慮することが求め

5 例えば、盗難キャッシュカードによる被害は、届出のあった事例ベースで平成 20 年度に 4,927 件発生している（金融庁［2009］）。

6 こうした攻撃として、例えば、IC カードによる端末認証が適切に機能していないケースや、正規の端末の改変等によって不正端末を攻撃者が用意できる場合が想定される。

7 こうした攻撃として、例えば、攻撃者が IC カード・端末間および IC カード・サーバー間において正規の処理の手順に関する情報を入手しており、同情報によって IC カードを偽造して正規の端末（あるいはサーバー）から情報を得る、という場合が考えられる。

られる（Finextra [2009]）。そこで、正規の IC カードを利用しないものの、ATM やサーバーの情報を盗取する攻撃者として次の攻撃者 5、6 を想定する（図表 4 参照）。

- **攻撃者 5**：認証時に正規の端末のメモリー上に現れる情報を盗取し、それを用いてなりすましを試みる。正規の IC カードを盗取しないが、同カードやサーバーから端末に送信される情報や本人の生体情報を盗取する。
- **攻撃者 6**：認証時に正規のサーバーのメモリー上に現れる情報を盗取し、それを用いてなりすましを試みる。正規の IC カードを盗取しないが、端末や IC カードからサーバーに送信される情報を盗取する。

なお、本稿では、参照データの暗号化等に利用される暗号アルゴリズムは安全であり、いずれの攻撃者も暗号アルゴリズムの解読によって鍵を求めることはできないと仮定している。また、当該システムにおいて取り扱われる情報の漏洩の影響に焦点を当てることから、参照データとして登録されている情報を用いずに正規のユーザーの生体情報を推定する（例えば、本人から直接生体情報を採取する）というタイプの攻撃を検討対象としない[8、9]。

(4) 各攻撃者によるなりすましへの耐性

照合を端末で行う STOC 方式と照合を IC カードで行う MOC 方式について攻撃者 1～6 への耐性を分析する。まず、各攻撃者が各方式のシステムから入手する情報（生体情報、参照データ、暗号化された参照データ、復号鍵）およびなりすまし成功確率について分析すると次のとおりである（図表 5 参照）。

- STOC 方式と MOC 方式はいずれも生体特徴と IC カードによる 2 要素認証とみなすことができるが、IC カードを盗取した攻撃者（攻撃者 1～4）に対しては生体特徴のみの 1 要素認証と同程度の安全性であると考えられる。
- 攻撃者 1 は、正規の IC カードを利用するものの参照データ等を入手できない。攻撃者が盗取した IC カードの解析を行わずに適当に選択した生体情報（例えば、攻撃者自身の生体情報）を提示する方法が考えられるが、この場合、なりすましが成功する確率は当該システムにおいて他人受入が偶然発生する確率（他人受入率）程度になると考えられる。

8 このほか、多くの参照データと誤って一致すると判定されるような入力（ウルフと呼ばれる）を用いたなりすまし（ウルフ攻撃）の可能性も指摘されている（Une, Otsuka, and Imai [2008]）。例えば、特定の照合アルゴリズムにおいて、あらゆる参照データと一致と判断されるウルフが存在することが指摘されている。ウルフ攻撃への対策の研究は近年活発化してきている（松本・宇根［2007］、Inuma, Otsuka, and Imai [2009]、村上・高橋［2009］）。本稿では、本攻撃への対策が講じられている生体認証システムを想定し、ウルフ攻撃を検討対象としない。

9 また、照合を行う関数や判定しきい値を改ざんして常に受理が出力されるようにする方法も考えられるものの、特定のユーザーの情報を用いる必要がないことから、本稿では検討対象としない。

図表 5　漏洩情報を用いたなりすましへの STOC 方式と MOC 方式の耐性

（1）攻撃者が入手するデータ

<table>
<tr><th></th><th>STOC 方式
（端末で照合）</th><th>MOC 方式
（IC カードで照合）</th></tr>
<tr><td>攻撃者 1</td><td colspan="2" rowspan="2">なし</td></tr>
<tr><td>攻撃者 2</td></tr>
<tr><td>攻撃者 3、4</td><td rowspan="2">暗号化された参照データ</td><td>参照データ</td></tr>
<tr><td>攻撃者 5</td><td>・生体情報
・暗号化された参照データ
・復号鍵</td><td>生体情報</td></tr>
<tr><td>攻撃者 6</td><td colspan="2">なし</td></tr>
</table>

（2）なりすまし成功確率

<table>
<tr><th></th><th>STOC 方式
（端末で照合）</th><th>MOC 方式
（IC カードで照合）</th></tr>
<tr><td>攻撃者 1、2</td><td colspan="2" rowspan="2">他人受入率程度</td></tr>
<tr><td>攻撃者 3、4</td><td>高い確率</td></tr>
<tr><td>攻撃者 5</td><td>高い確率</td><td rowspan="2">（正規の IC カードを利用できず、攻撃困難）</td></tr>
<tr><td>攻撃者 6</td><td>（暗号アルゴリズムを解読困難であり、攻撃困難）</td></tr>
</table>

備考：図表 5（2）では、本人が生体情報を提示した場合と同程度の高い確率でなりすましに成功する可能性があるケースは「高い確率」と記し、セルにシャドーを付けた。他人受入率程度でなりすましに成功するケースは「他人受入率程度」と記した。図表 11、図表 12、図表 A-4、図表 A-6 においてもこの表記を用いる。

- STOC 方式については以下のとおりである。
  - ➢ 攻撃者 2～4 は、正規の IC カードを利用するほか暗号化された参照データを入手するものの、暗号を解読して平文の参照データを求めることが困難であり、なりすましに成功する確率は他人受入率程度になると考えられる。
  - ➢ 攻撃者 5 は、参照データを入手しており、ヒルクライミング攻撃により本人の生体情報と高い類似度を有する入力を生成することができると考えられる。この入力を端末に提示することで、本人が生体情報を提示した場合と同程度の高い確率（以下では、単に「高い確率」と表記する）でなりすましに成功する可能性がある。
  - ➢ 攻撃者 6 は、適当に選択したデータを暗号化された参照データとして端末に入力する攻撃が考えられるが、暗号アルゴリズムは解読できないと想定していることから、攻撃実行は困難である。
- MOC 方式については以下のとおりである。
  - ➢ 攻撃者 2 は、攻撃者 1 と同様に、正規の IC カードを入手するものの参照データ等を入手することができないため、なりすましが成功する確率は他人受入率程度になると考えられる。
  - ➢ 攻撃者 3、4 は、STOC 方式における攻撃者 5 と同様に、ヒルクライミング攻撃により生成した入力を正規の IC カードに提示することで、高い確

率でなりすましに成功する可能性がある。

➢ 攻撃者5、6は、正規のICカードを入手しておらず、同カード内で認証処理を実行することができないため、攻撃実行は困難である。

こうした攻撃に対しては、次のような運用による対策が考えられる。

- 連続認証失敗回数（リトライカウンター）の上限を適切に設定し、上限を超えた場合にはアカウントをロックすることによって、他人受入率でのなりすましの成功を防ぐという対策。
- 高い確率でなりすましが成功しうるケースについては、情報の漏洩やなりすましを早期に検知して当該ICカードを無効化し、生体特徴の再登録や新しいICカードの発行を行うという対策。
- 偽造された生体情報を提示する人工物を検知・排除する生体検知技術の評価手法が確立し安全性の高い方式が利用可能になった場合には同技術を採用するという対策。

学界では、こうした問題を根本的に解決するために、「漏洩した情報を用いてもなりすましが成功しない」ようにするための対策が研究されており、次節でその概要を紹介する。

3. テンプレート保護型生体認証技術

本節では、生体認証システムにおける情報漏洩への対策として学界で研究されている技術の概要、実現方式のアイデア、評価の状況を説明する。

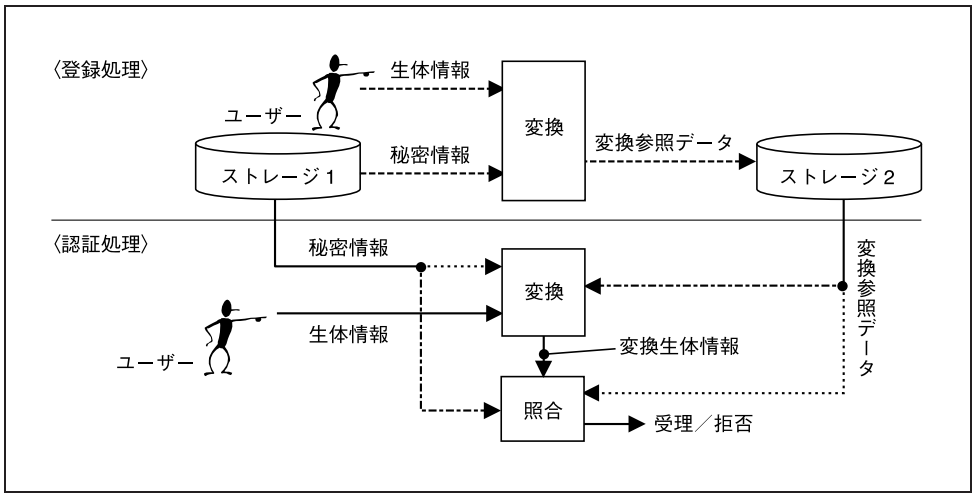
(1) 単なる暗号化を行う方式との差異

生体認証システムでは、登録時と認証時に取得された生体情報が完全に同一のデータとはならない。トリプルDESのような従来の暗号アルゴリズムを用いて生体情報を暗号化する場合、これらの生体情報のデータが1ビットでも異なれば、それらの暗号文間の相関は極めて小さくなるため暗号文のまま照合を行うことができない。このため、参照データを復号したうえで照合を行う必要があり、メモリー上に現れる平文の参照データの守秘が課題となる。

これに対して、テンプレート保護型生体認証技術では、生体情報に特殊な変換[10]を施すことによって元の生体情報との相関をある程度確保することが可能であり、両者の整合性を確認できるという点がポイントである。そのため、平文の参照データ

10 具体的な変換方法は提案方式によって多種多様であるが、例えば、指紋等の画像処理ベースの方式として、画像データ（参照データに対応）にフーリエ変換を行ったうえでランダムな画像データを乗算するといった方式が提案されている。

図表 6　テンプレート保護型生体認証の処理フロー（概念図）



が照合時にメモリー上に現れることがなく漏洩する心配がないというメリットがある。ただし、変換したまま照合を行うため、認証精度の低下や処理速度の増加といった性能面でのデメリットが発生する可能性がある。

(2) テンプレート保護型生体認証技術の処理フロー

テンプレート保護型生体認証技術では、登録時に、ユーザーから取得した生体情報と秘密の情報を用いて「変換参照データ」を生成する（図表 6 参照）。ここでの秘密の情報を以下では「秘密情報」[11]と呼ぶ。秘密情報と変換参照データはそれぞれストレージに格納される。認証時には、秘密情報あるいは変換参照データを用いて生体情報を変換し（この情報を「変換生体情報」と呼ぶ）、照合の処理を行う[12]。なお、登録時と認証時の変換の方法が異なるケースもある。

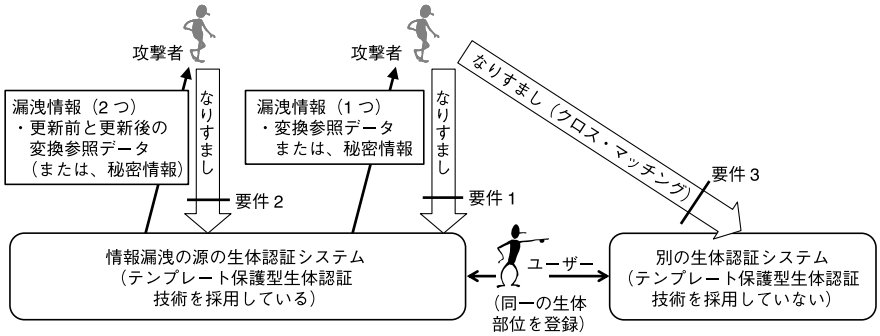
(3) セキュリティ要件

テンプレート保護型生体認証技術が対象としているセキュリティ要件は提案者によって異なるケースがあり、どのような要件が妥当かについても検討が行われている最中である（Ratha, Connell, and Bolle [2001]、Jain, Nandakumar, and Nagar [2008]、

11 例えば、指紋画像にフーリエ変換を行ったうえでランダムな画像データを乗算するケースでは、「ランダムな画像データ」が秘密情報に対応する。

12 既存の方式をみると、秘密情報で生体情報を変換して変換生体情報を生成し、これと変換参照データを照合するケースがあるほか、変換参照データで生体情報を変換して変換生体情報を生成し、これと秘密情報を照合するケースがある（図表 6 参照）。

図表 7　テンプレート保護型生体認証技術の主なセキュリティ要件

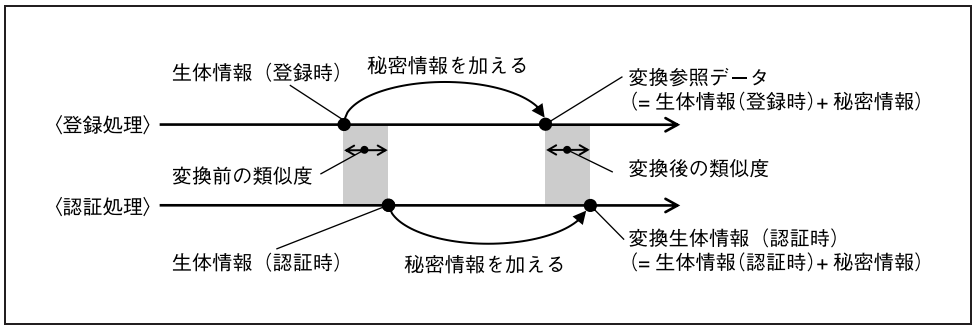


高橋・比良田・三村・手塚［2008］）。既知の主なセキュリティ要件としては次の 3 つが挙げられる（図表 7 参照）。

- **要件 1**：攻撃者が変換参照データと秘密情報のどちらか一方を入手したとしても、なりすますことが困難である。
  - 例えば、攻撃者が IC キャッシュカードを盗取し同カードから変換参照データを入手したとしても、当該ユーザーになりすますことが困難であるという要件。
- **要件 2**：攻撃者が更新前と更新後の変換参照データ（または、秘密情報）を入手したとしても、なりすますことが困難である。
  - 例えば、攻撃者に IC キャッシュカードを盗取され、再発行されたカードも同攻撃者に盗取されたとしても、同攻撃者によるなりすましは困難であるという要件。
- **要件 3**：攻撃者が変換参照データと秘密情報のどちらか一方を入手したとしても、本人の生体情報を復元することが困難である。
  - 例えば、攻撃者が IC キャッシュカードを盗取し同カードから変換参照データを入手したとしても、当該ユーザーの生体情報を推定したうえで、当該ユーザーが同じ生体特徴を登録している別の生体認証システムにおいてなりすまし（クロス・マッチング）を行うことが困難であるという要件。

テンプレート保護型生体認証技術において想定されるなりすましは、推定した本人の生体情報を用いる方法のほかに、変換生体情報を直接推定して用いる方法が考えられる。要件 1 はこれらの方法を対象にしているのに対し、要件 3 は本人の生体

図表 8　類似度保存アプローチの基本アイデア



情報の復元を対象にしている[13]。

(4) 2 つの実現方式

テンプレート保護型生体認証技術を採用したシステムに欠かせない特殊な性質を満たす変換アルゴリズムを実現した方式がこれまでに多数提案されているが、各方式のアプローチに注目すると「類似度保存アプローチ」と「鍵抽出アプローチ」の 2 つに大別することができる。

イ．類似度保存アプローチ

本アプローチは、登録時と認証時に取得した生体情報をそれぞれ秘密情報によって変換し、変換した状態のまま照合する。変換と照合に用いるアルゴリズムは、変換後のデータの類似度が変換前のデータの類似度と非常に高い相関を有する。

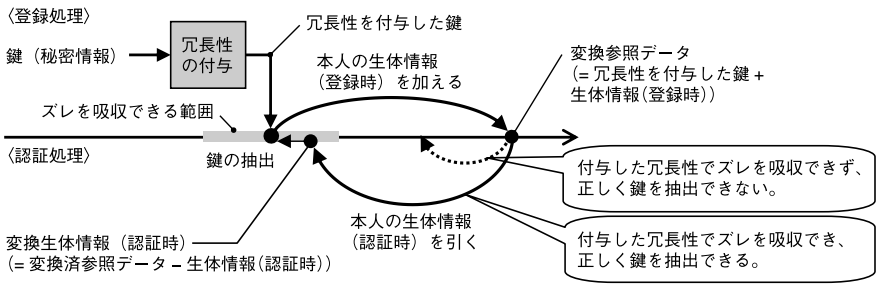
類似度保存アプローチの特徴を単純な例を用いて説明する（図表 8 参照）。生体情報と秘密情報がそれぞれ 1 つの数値で表されていると仮定し、登録時に取得した生体情報に秘密情報を加えた値を変換参照データとする。認証時に取得した生体情報に秘密情報を加え、変換参照データとの差分を類似度とする。この差分が判定しきい値よりも小さければ受理を出力する。このような生体認証システムの場合、登録時と認証時に同一の秘密情報を加えるという処理を行っており、登録時の生体情報と認証時の生体情報の差分（類似度）が変換後も保存されることとなる。

また、本アプローチにおいては、既存の生体認証システムの登録・認証の処理の流れを大幅に変更する必要がない方式も提案されており、実装面でのメリットがあると考えられる[14]。

13 生体情報から性別や病歴等の情報を抽出できるケースがあり、プライバシーの観点から「変換参照データ、あるいは、秘密情報から本人の生体情報の復元が困難であること」を要件として扱っている研究グループもある（Breebaart, Busch, Grave, and Kindt [2008]）。

14 例えば、虹彩認証システムについて本アプローチに基づく方式として太田・清本・田中［2004］が挙げられる。

図表９　鍵抽出アプローチにおける基本アイデア



ロ．鍵抽出アプローチ

本アプローチは、本人の生体情報であれば常に一定のデータを抽出可能であり、当該データを暗号鍵として暗号技術ベースの認証処理等を実行して受理や拒否を出力するというものである。こうしたアプローチとして、生体情報のハッシュ値を鍵として登録し、認証時に取得した生体情報のハッシュ値を再び鍵として利用するという方法がまず考えられる。しかし、こうした単純な暗号技術ベースの方法では、前述したように、登録時と認証時に取得される生体情報は本人の場合でも完全に一致せずズレが生じることから、常に同一の鍵を生成することが困難である。この問題を回避する方法として、生体情報のズレを吸収するように鍵に冗長性を付与する方法が採用されている[15、16]。

鍵抽出アプローチの特徴を単純な例を用いて説明する（図表９参照）。鍵（秘密情報）と生体情報はそれぞれ１つの数値で表されているとする。登録時には、鍵の値を決めたうえで冗長性を付与し、生体情報にこの値を加えた値を変換参照データとする。認証時には、変換参照データから生体情報を引いた値を求める。この値が一定の範囲に収まる場合には、鍵に付与された冗長性により正しい鍵を抽出することができる。

(5) 既存方式における評価の現状

こうしたテンプレート保護型生体認証技術の各種方式が提案されており、なりすましへの耐性、認証精度、処理速度といった項目に関する評価が重要となっている。

15 鍵への冗長性の付与の例として、2 ビットの鍵 01 と、鍵の各ビットをそれぞれ 2 回繰り返すという方法で冗長性を付与した鍵 000111 を考える。仮にこのデータに 1 ビットのエラー（生体情報のズレに相当）が発生し 001111 というビット列になったとする。先頭 3 ビット 001 は 000 にエラーが発生した値であると推測できることから、元の鍵は 01 であると推定できる。

16 より厳密には、鍵に付与した冗長性で吸収できる範囲のズレをもつ生体情報であればよい。この範囲を超える場合には、本人の生体情報であっても鍵を正しく抽出することができない。

しかし、こうした評価方法は現在研究途上にあり、まだ確立されていないのが実情である。

イ．なりすましへの耐性

なりすましに関するセキュリティ要件として本節(3)において3つの要件を説明した。まず、要件1（変換参照データと秘密情報のどちらかを入手しても、なりすまし困難）の充足度合いに関連する評価については、例えば、既存方式において変換参照データを入手した攻撃者を前提にすると、なりすましに必要な計算量が平均530億回の照合処理相当になるとの評価事例（Uludag, Pankanti, and Jain [2005]）や、変換参照データと秘密情報の両方を入手した攻撃者を前提にすると、なりすましに必要な計算量が平均16兆回の照合処理相当になるとの評価事例（Hao, Anderson, and Daugman [2006]）がある。ただし、こうした事例は非常に少ない。

要件2（更新前と更新後の変換参照データ等を入手しても、なりすまし困難）についても、厳密な評価が行われていないケースが多い。

要件3（変換参照データと秘密情報のどちらか一方を入手しても、生体情報を復元困難）については、変換参照データから本人の情報が漏洩しないことを情報理論的に証明している事例（Takahashi and Hirata [2009]）があるものの、どの程度復元すれば本人の生体情報が復元されたと判断するかに関する基準についての議論はほとんど行われていないのが実情である。

このほか、変換参照データをICカードに格納するタイプの生体認証システムに注目して、2節において想定した攻撃者1〜6によるなりすましへの耐性を分析するといった試みは、筆者たちが知る限りほとんど報告されていない。

ロ．認証精度

生体認証システムの性能を代表する尺度の1つである認証精度については、いずれのアプローチに基づく方式も他人受入率や本人拒否率（本人を誤って拒否してしまう確率）等を用いて評価されることが多い。その際、ユーザーごとに異なる秘密情報を設定して認証精度を測定するという方法（Jin, Ling, and Goh [2004]）や、各ユーザーで共通の秘密情報を用いて認証精度を測定するという方法（高橋・比良田［2008］）が利用されている。

ただし、変換参照データを用いて照合を行う際の認証精度と、変換していない参照データを用いて照合を行う際の認証精度を比較し、テンプレート保護型生体認証技術の導入によりどの程度認証精度が低下したかを評価するという事例（高橋・比良田［2008］）はほとんどない。そのため、テンプレート保護型生体認証技術を導入したときの認証精度への影響を比較することができない。また、通常の生体認証システムの認証精度の測定に用いられるサンプル数と比較すると、各事例で用いられ

ているサンプル数は少なく[17]、認証精度の測定結果が信頼できるものか否かについても明らかではない。

ハ．処理時間等

処理時間、変換参照データのサイズ、登録処理と認証処理における通信量については、いずれのアプローチに基づく方式も評価結果が示されていないケースが多い。

4．テンプレート保護型生体認証技術の利用の可能性

前節で述べたように、変換参照データをICカードに格納するタイプのテンプレート保護型生体認証技術を採用したシステムを取り上げて、攻撃者1〜6によるなりすましへの耐性を分析するという試みはほとんど報告されていないようである。本節では、攻撃者1〜6を想定した場合、テンプレート保護型生体認証技術を適用することによる効果を分析する。

(1) 検討対象とする生体認証システム

テンプレート保護型生体認証技術の2つのアプローチのうち、本節では、既存の生体認証システムの登録・認証の処理フローを大幅に変更することなく利用可能な類似度保存アプローチを検討対象とする[18]。本アプローチに基づく方式のうち、分析の一例として、「変換参照データをICカード内に格納するとともにICカードにおいて照合を行う」というタイプの2つの方式（MOC-α方式、MOC-β方式と呼ぶ）を取り上げて検討を行う（図表10参照）。

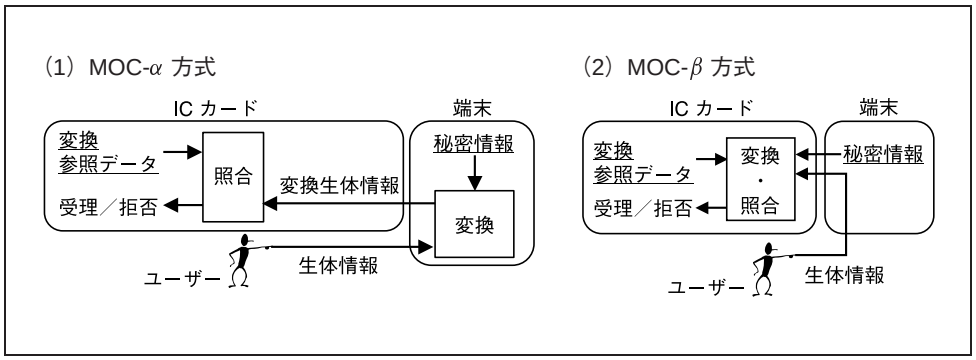
- MOC-α 方式：端末で生体情報の変換を行ったうえで、ICカード内で照合を行う方式であり、変換に用いる秘密情報は端末に格納される。
- MOC-β 方式：ICカード内において生体情報の変換と照合を行う方式であり、変換に用いられる秘密情報は端末に格納される。

なお、MOC-α方式とMOC-β方式の変換・照合のアルゴリズムは、3節の要件1〜3を満たしていると仮定する。

17 例えば、テンプレート保護型生体認証技術における認証精度評価の事例として紹介したJin, Ling, and Goh [2004]は100指を、高橋・比良田［2008］は181指を利用している。一方、市販製品の認証精度評価プロジェクト（IBG [2006]）では650指を、認証精度評価コンテスト（FVC [2006]）では450指が利用されている。

18 鍵抽出アプローチの方式を適用した生体認証システムの分析は補論2を参照されたい。

図表 10　類似度保存アプローチを適用した生体認証システムの例



備考：下線は、IC カードや端末に格納されているデータであることを示す。

(2) なりすましへの耐性

MOC-α 方式と MOC-β 方式において攻撃者 1～6 が各システムから入手するデータ、および、各方式のなりすましへの耐性を整理すると次のとおりである（図表 11 参照）。

- 攻撃者 1、2 は、正規の IC カードを利用するものの、変換参照データ等を入手できないため、どちらの方式においてもなりすましが成功する確率は他人受入率程度になると考えられる。
- 攻撃者 3 は、正規の IC カードを利用するほか変換参照データを入手するが、MOC-α 方式と MOC-β 方式のいずれの方式も要件 1（変換参照データを入手してもなりすましが困難）を満たすため、なりすましに成功する確率は他人受入率程度であると考えられる。
- MOC-α 方式における攻撃者 4 は、正規の IC カードを利用するほか、端末に生体情報を提示することで変換生体情報を入手できる。
    - ➢ 秘密情報を推定できる場合には[19]、ブルート・フォース攻撃（多種多様な生体情報を用いた照合により本人の生体情報に近い入力を探す攻撃）により高い確率でなりすましに成功すると考えられる。秘密情報の推定が困難であれば、他人受入率程度でなりすましに成功すると考えられる。
    - ➢ 端末に何度でも認証の試行が可能であれば、攻撃者はヒルクライミング攻撃（類似度が高くなるように生体情報を修正する攻撃）が実行可能になる[20]。

19 攻撃者が提示した生体情報とそれに対応する変換生体情報のペアから秘密情報を推定する方法が考えられる。

20 攻撃者は、なりすまし対象者の変換参照データを入手しており、端末から得た「変換生体情報」を用いて照合を行うことができる。照合時に算出される類似度も入手できる。

図表 11　漏洩情報を用いたなりすましへの MOC-α、β 方式の耐性

(1) 各攻撃者が入手するデータ

	攻撃者の能力		MOC-α 方式	MOC-β 方式
攻撃者 1	正規の IC カードを利用	同カードの解析せず	なし	
攻撃者 2		同カードから不正読出し		
攻撃者 3		同カード内の情報の盗取	変換参照データ	・変換参照データ ・秘密情報
攻撃者 4		同カード内の情報と同カードへの送信される情報の盗取		
攻撃者 5	正規の IC カードを利用せず	端末のメモリー上の情報の盗取	・生体情報 ・秘密情報 ・変換生体情報	・生体情報 ・秘密情報
攻撃者 6		サーバーのメモリー上の情報の盗取	なし	

(2) なりすまし成功確率

	MOC-α 方式	MOC-β 方式
攻撃者 1〜3	他人受入率程度	
攻撃者 4	他人受入率程度[注)]	高い確率
攻撃者 5、6	(正規の IC カードを利用できず、攻撃困難)	

注) 攻撃者が提示した生体情報とそれに対応する変換生体情報から秘密情報の推定が困難、かつ、ヒルクライミング攻撃に耐性を有する照合アルゴリズムの利用が必要である。

- MOC-β 方式における攻撃者 4 は、正規の IC カードを利用するほか変換参照データと秘密情報を入手しており、ブルート・フォース攻撃により本人の生体情報に近い情報を推定可能であると考えられるため、高い確率でなりすましに成功する可能性がある[21]。
- 両方式における攻撃者 5、6 は、正規の IC カードを入手しておらず、同カード内で認証処理を実行することができないため、攻撃実行は困難である。

こうした分析をまとめると、MOC-α 方式については、①生体情報と変換参照データのペアから秘密情報の推定が困難、かつ、②ヒルクライミング攻撃への耐性を有した照合アルゴリズムの利用[22]を前提とすれば、MOC 方式よりもなりすましへの耐性が向上することがわかる[23]。MOC-β 方式については、MOC 方式より耐性が向上しているものの、IC カード内部のデータと IC カードに送信されるデータを盗取す

21 MOC-α 方式における攻撃者 4 が行うブルート・フォース攻撃は端末への問合せが必要であるのに対し、MOC-β 方式における攻撃者 4 が行うブルート・フォース攻撃では端末への問合せが不要である。

22 ヒルクライミング攻撃への対策として、類似度を手掛かりに入力情報を生成した場合に、当該入力情報が不自然になるようにする照合アルゴリズム（小松［2005］）や、ヒルクライミング攻撃により生成した入力に耐性のある照合アルゴリズム（村松［2008］）等が研究されている。

23 テンプレート保護型生体認証技術の方式によっては、要件 1〜3 を満たせばこうした追加的なセキュリティ要件を仮定せずに攻撃者 1〜6 によるなりすましに耐性をもたせることができる可能性がある（STOC-α 方式、補論 2 参照）。

る攻撃者を想定するとまだ不十分といえる。

このように、各セキュリティ要件を満たす方式を利用したとしても、そのシステム構成によってなりすましへの耐性が異なることがわかる。

5. 考察

本節では、ここまでの分析結果等を踏まえ、IC カードによる ATM における生体認証システムにテンプレート保護型生体認証技術を適用する場合の留意点と、本技術における今後の研究開発上の課題について考察する。

(1) テンプレート保護型生体認証技術の適用における留意点

本稿ではテンプレート保護型生体認証技術の 3 つのセキュリティ要件を示したが、既存の方式の中には、すべての要件を目標として設計されていないものがある。仮にすべての要件を満たす方式であっても、4 節において検討したようにシステムの構成によってなりすましへの耐性が異なる（図表 12 参照）。こうした点を考慮すると、テンプレート保護型生体認証技術の導入に当たり、まず、検討対象とする方式が満たす要件を把握することが求められる。さらに、候補となる方式を実装する際には、MOC-α 方式のように、変換参照データと秘密情報を格納する場所を分け、変換と照合を実行する場所も分けることが重要である。

また、テンプレート保護型生体認証技術の安全性と精度や処理時間といった性能がトレードオフの関係になるケースが多い。目標とするセキュリティ・レベルを満たすように方式のパラメータ（秘密情報等）を設定した場合、性能に関する要件を満たさなくなる可能性がある。性能に関する要件を優先する場合には、2 節で説明したように、性能を優先したパラメータを設定したうえで、カード認証の強化、リト

図表 12　漏洩情報を用いたなりすましへの各方式の耐性
（図表 5 (2) と図表 11 (2) の再掲）

<table>
<tr><th></th><th>テンプレート保護型
生体認証技術の利用なし</th><th colspan="2">テンプレート保護型
生体認証技術の利用あり</th></tr>
<tr><th></th><th>MOC 方式</th><th>MOC-α 方式</th><th>MOC-β 方式</th></tr>
<tr><td>攻撃者 1、2</td><td>他人受入率程度</td><td colspan="2" rowspan="2">他人受入率程度</td></tr>
<tr><td>攻撃者 3</td><td rowspan="2">高い確率</td></tr>
<tr><td>攻撃者 4</td><td>他人受入率程度[注)]</td><td>高い確率</td></tr>
<tr><td>攻撃者 5</td><td rowspan="2">（正規の IC カードを利用できず、攻撃困難）</td><td colspan="2" rowspan="2">（正規の IC カードを利用できず、攻撃困難）</td></tr>
<tr><td>攻撃者 6</td></tr>
</table>

注）攻撃者が提示した生体情報とそれに対応する変換生体情報から秘密情報の推定が困難、かつ、ヒルクライミング攻撃に耐性を有する照合アルゴリズムの利用が必要である。

ライカウンターや生体検知技術の導入、情報漏洩やなりすましの早期検知とICカードの無効化・再発行等の対策を併用していくことが考えられる。

(2) テンプレート保護型生体認証技術における今後の研究課題

3節(5)において述べたように、テンプレート保護型生体認証技術の各セキュリティ要件や性能に関する評価が十分とはいえない。

セキュリティ評価については、まず、①各要件がどの程度充足されているかを評価する方法を検討することが望まれる。その際、理論的なセキュリティ・レベルの見積りと画像データ等の生体情報を用いた実験の両面からの検討が望まれる。また、② ICカードに変換参照データを格納するタイプのシステムと攻撃者1〜6を想定した検討もATMにおけるシステムの利用を想定した場合には有意義であると考えられる。4節の分析結果において示したように、テンプレート保護型生体認証技術の方式によってはヒルクライミング攻撃に対する十分な耐性が必要となるなど、追加的なセキュリティ要件が求められるケースがある。テンプレート保護型生体認証技術の効果の限界を見極めるための検討が今後重要である。

認証精度については、測定に用いるサンプル数を増加させることに加えて、テンプレート保護型生体認証技術の導入前後の精度の変化に関する分析も求められる。このほか、処理時間、変換参照データのサイズ、登録処理と認証処理における通信量についても評価結果を明記していくことが求められる。

6. まとめ

金融分野では、ATMにおける顧客の本人確認の手段として生体認証システムが利用されるようになってきている。生体認証システムのセキュリティについては学界を中心に活発な議論が行われているが、最近では、生体認証システムから漏洩した情報を利用したなりすましへの対策としてテンプレート保護型生体認証技術が注目を集めている。

本稿では、ATMで利用されている生体認証システムに焦点を当てて、既存のテンプレート保護型生体認証技術を同システムに適用する場合、どのような効果が期待できるか、あるいは、どのような点に留意する必要があるかを検討した。その結果、テンプレート保護型生体認証技術を適用したとしても、ICカード内に格納される参照データの盗取によるなりすましを常に防止できるとは限らず、適用対象となっている生体認証システムの構成を注意深く考慮したうえでどのような保護方式が適当かを検討することが必要であることが判明した。これらを踏まえると、金融機関がテンプレート保護型生体認証技術を活用する際には、ベースとなる生体認証システムのなりすましへの耐性を明らかにしたうえで、どのように導入すれば耐性を向上

させることができるかを検討していくことが重要であるといえる。

テンプレート保護型生体認証技術は研究途上の技術であり、今後、なりすましへの耐性を含むセキュリティ評価の研究に加え、認証精度や処理時間等の性能面での評価についても今後検討が進展していくとみられる。金融分野においても、生体認証システムを活用して金融取引におけるセキュリティの維持・向上を図るうえで、テンプレート保護型生体認証技術は重要な技術の１つになるとみられる。今後の本技術分野の動向に注目していくことが有用であろう。

参考文献

太田陽基・清本晋作・田中俊昭、「虹彩コードを秘匿する虹彩認証方式の提案」、『情報処理学会論文誌』第 45 巻第 8 号、2004 年、1845～1855 頁

金融庁、「偽造キャッシュカード等による被害発生等の状況について」、報道発表資料、2009 年 10 月 9 日（http://www.fsa.go.jp/news/21/ginkou/20091009-1.html）

小松尚久、「バイオメトリクスセキュリティ評価基準に関する研究」、『平成 16 年度経済産業省基準認証研究開発事業　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』、早稲田大学共同研究報告書、ニューメディア開発協会、2005 年

財団法人金融情報システムセンター（FISC）、『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 版追補改訂）』、FISC、2009 年

財団法人ニューメディア開発協会、『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』、第 4 部バイオメトリクス認証結果保証基盤の研究開発、平成 16 年度経済産業省基準認証研究開発事業、2005 年

鈴木雅貴・宇根正志、「生体認証システムの脆弱性の分析と生体検知技術の研究動向」、『金融研究』第 28 巻第 3 号、日本銀行金融研究所、2009 年、69～106 頁

高橋健太・比良田真史、「相関不変ランダムフィルタリングを用いたキャンセラブル指紋認証」、『2008 年暗号と情報セキュリティシンポジウム予稿集』、2B3-1、2008 年

――・――・三村昌弘・手塚　悟、「セキュアなリモート生体認証プロトコルの提案」、『情報処理学会論文誌』第 49 巻第 9 号、2008 年、3016～3027 頁

松本　勉・宇根正志、「バイオメトリクス認証の実用におけるぜい弱性と対策」、『電子情報通信学会会誌』第 90 巻第 12 号、2007 年、1051～1055 頁

村上隆夫・高橋健太、「Wolf 及び Lamb に対する安全性の高い生体認証の提案」、『コンピューターセキュリティシンポジウム 2009』、D4-3、2009 年

村松大吾、「ヒルクライミング法を用いたオンライン署名認証アルゴリズムの検討」、『2008 年暗号と情報セキュリティシンポジウム予稿集』、2B4-2、2008 年

Adler, Andy, “Can Images Be Regenerated from Biometric Templates?” Biometric Conference, 2003.

Breebaart, Jeroen, Christoph Busch, Justine Grave, and Els Kindt, “A Reference Architecture for Biometric Template Protection Based on Pseudo Identities,” *Proc. the Special Interest Group on Biometrics and Electronic Signatures (BIOSIG)*, 2008, pp. 25–38.

Finextra, “Criminal Malware Infection Hits Eastern European Cash Machines,” June 29, 2009 (http://www.finextra.com/fullstory.asp?id=20198).

Fingerprint Verification Competition (FVC), “Databases,” 2006 (http://bias.csr.unibo.it/fvc2006/databases.asp).

Hao, Feng, Ross Anderson, and John Daugman, “Combining Crypto with Biometrics Effectively,” *IEEE Transaction on Computers*, 55 (9), 2006, pp. 1081–1088.

Hill, Chirstopher James, “Risk of Masquerade Arising from the Storage of Biometrics,” Bachelor Thesis, Department of Computer Science, Australian National University, 2001.

International Biometric Group (IBG), “Comparative Biometric Testing Round 6 Public Report,” IBG, 2006 (http://www.biometricgroup.com/reports/public/reports/CBT6_report.htm).

Inuma, Manabu, Akira Otsuka, and Hideki Imai, “Theoretical Framework for Constructing Matching Algorithms in Biometric Authentication Systems,” International Conference on Biometrics (ICB), 2009.

Jain, Anil K., Karthik Nandakumar, and Abhishek Nagar, “Biometric Template Security,” *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008, pp. 1–17.

Jin, Teoh Andrew Beng, David Ngo Chek Ling, and Alwyn Goh, “Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenized Random Number,” *Pattern Recognition*, 37, 2004, pp. 2245–2255.

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino, “Impact of Artificial Gummy Fingers on Fingerprint Systems,” SPIE Optical Security and Counterfeit Deterrence Techniques IV, Vol. 4677, 2002.

Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle, “Enhancing Security and Privacy of Biometric-Based Authentication Systems,” *IBM Systems Journal*, 40 (3), 2001, pp. 614–634.

Takahashi, Kenta, and Shinji Hirata, “Generating Provably Secure Cancelable Fingerprint Templates Based on Correlation-Invariant Random Filtering,” IEEE Conf. Biometrics: Theory, Applications and Systems, 2009.

Uludag, Umut, Sharath Pankanti, and Anil K. Jain., “Fuzzy Vault for Fingerprints,” *Proceeding of International Conference on Audio- and Video-Based Biometric Person Authentication*, 2005, pp. 310–319.

Une, Masashi, Akira Otsuka, and Hideki Imai, “Wolf Attack Probability: A Theoretical Security Measure in Biometric Authentication Systems,” *IEICE Trans. Inf. & Syst.*, E91-D (5), 2008, pp. 1380–1389.

補論 1. STOC 形態と MOC 形態の生体認証システムのモデルと耐性

(1) STOC 形態の生体認証システム

STOC 形態では、参照データは IC カードに格納されるほか、照合は端末またはサーバーで実行される。また、参照データは、暗号化されるケースと暗号化されないケースに分けられるほか、暗号化されるケースでは復号鍵を格納しておく必要があり、その場所のバリエーションも考慮する必要がある。これらの項目に関する組合せに基づいて、次の 4 つの STOC 形態を検討対象とする（図表 A-1 参照）[24]。なお、下記の STOC-3 方式は、2 節の STOC 方式であり比較のために再掲する。

- **STOC-1 方式**：端末は、ユーザーから取得した生体情報と参照データを用いて照合を行う。
- **STOC-2 方式**：サーバーは、端末から受信した参照データと生体情報を用いて照合を行う。
- **STOC-3 方式**：端末は、ユーザーから生体情報を取得するとともに、暗号化された参照データを復号して照合を行う。
- **STOC-4 方式**：サーバーは、生体情報と暗号化された参照データを端末から受信し、暗号化された参照データを復号して生体情報との照合を行う。

(2) MOC 形態の生体認証システム

STOC 形態における議論と同様に MOC 形態の分類を考えると、IC カードにおいて参照データが格納されるほか、照合も実行される。したがって、参照データが暗号化されるケースと暗号化されないケースに分けられるほか、暗号化されるケースで

図表 A-1　STOC 形態の 4 種類の方式

	各エンティティにおいて格納されるデータ、および、実行される処理		
	IC カード	端末	サーバー
STOC-1 方式	（データ）参照データ	（処理）照合	–
STOC-2 方式		–	（処理）照合
STOC-3 方式	（データ）暗号化された参照データ	（データ）復号鍵 （処理）復号・照合	–
STOC-4 方式		–	（データ）復号鍵 （処理）復号・照合

24 なお、STOC-3 方式において復号鍵をサーバーに格納するという変更を加えた方式や、STOC-4 方式において復号鍵を端末に格納するという変更を加えた方式も想定される。これらは、後述するなりすましへの耐性に関する検討結果がそれぞれ STOC-3 方式と STOC-4 方式と同一となることから、ここでは取り上げないこととする。

図表 A-2　MOC 形態の 2 種類の方式

	各エンティティにおいて格納されるデータ、および、実行される処理		
	IC カード	端末	サーバー
MOC-1 方式	（データ）参照データ （処理）照合	–	–
MOC-2 方式	（データ）暗号化された参照データ （処理）復号・照合	（データ）復号鍵	–

図表 A-3　各生体認証システムにおいて各攻撃者が入手するデータ

<table>
<tr><th></th><th colspan="6">方式</th></tr>
<tr><th></th><th>MOC-1</th><th>STOC-1</th><th>STOC-2</th><th>MOC-2</th><th>STOC-3</th><th>STOC-4</th></tr>
<tr><td>攻撃者 1</td><td colspan="3" rowspan="2">なし</td><td colspan="3" rowspan="2">なし</td></tr>
<tr><td>攻撃者 2</td></tr>
<tr><td>攻撃者 3</td><td colspan="3" rowspan="2">参照データ</td><td colspan="3" rowspan="2">暗号化された参照データ</td></tr>
<tr><td>攻撃者 4</td><td>・暗号化された参照データ
・復号鍵</td></tr>
<tr><td>攻撃者 5</td><td>生体情報</td><td colspan="2">・生体情報
・参照データ</td><td>・生体情報
・復号鍵</td><td>・生体情報
・暗号化された参照データ
・復号鍵</td><td>・生体情報
・暗号化された参照データ</td></tr>
<tr><td>攻撃者 6</td><td colspan="3">なし</td><td colspan="2">なし</td><td>・暗号化された参照データ
・復号鍵</td></tr>
</table>

は復号鍵の格納場所によって分類される。これらの項目に関する組合せに基づいて、次の 2 つの MOC 形態を検討対象とする（図表 A-2 参照）[25]。なお、下記の MOC-1 方式は、2 節の MOC 方式であり比較のために再掲する。

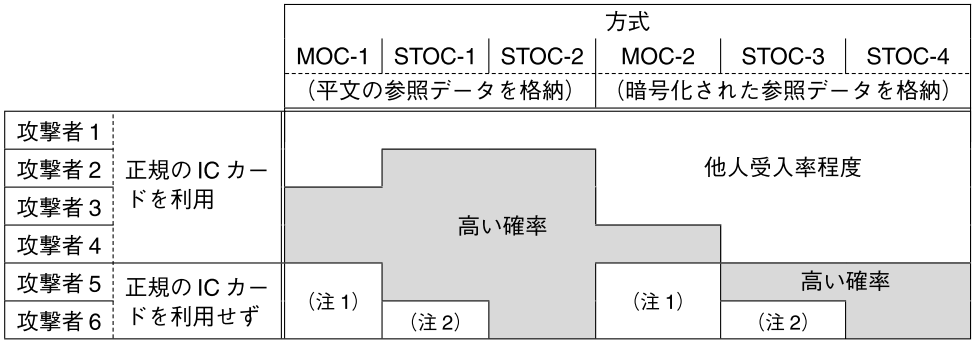
- MOC-1 方式：IC カードは、参照データと端末から受信した生体情報を用いて照合を行う。
- MOC-2 方式：IC カードは、暗号化された参照データを端末から受信した復号鍵で復号したうえで照合を行う。

(3) 各攻撃者によるなりすましへの耐性

STOC-1～4 方式と MOC-1、2 方式について攻撃者 1～6 への耐性を分析する。まず、各攻撃者が各方式のシステムから入手する情報（生体情報、参照データ、暗号化された参照データ、復号鍵）を整理すると図表 A-3 のとおりである。

25 なお、MOC-2 方式において復号鍵をサーバーに格納するという変更を加えた方式も想定される。本方式は、後述するなりすましへの耐性に関する検討結果が MOC-2 方式と同一となることから、ここでは取り上げないこととする。

図表 A-4　漏洩情報を用いたなりすましへの各方式の耐性



備考：（注 1）正規の IC カードを利用できず、攻撃困難である。
（注 2）暗号アルゴリズムを解読困難であり、攻撃困難である。

これらを踏まえてなりすましへの耐性を分析すると、どの方式もいずれかの攻撃者を想定すると他人受入率よりも高い確率でなりすましが成功するおそれがあることがわかる（図表 A-4 参照）。具体的には次のケースにおいて成功確率が他人受入率よりも高くなる可能性がある。

- ユーザーが IC カードを盗取されて利用されたり、不正端末によって当該カードから情報を読み出されたりする場合において（攻撃者 1、2 に相当）、参照データを暗号化しないで IC カードから出力する方式（STOC-1、2）を採用するケース。
- IC カードが盗取・解析されたり、偽造カードによって端末やサーバーから情報（復号鍵等）が不正に読み出されたりする場合において（攻撃者 3、4 に相当）、参照データを暗号化しないで IC カードに格納する方式（STOC-1、2、MOC-1）や IC カード内で復号・照合を行う方式（MOC-2）を採用するケース。
- 端末やサーバーのメモリー上のデータが観測される（攻撃者 5、6 に相当）可能性が想定される場合において、端末やサーバーにおいて照合を行う方式（STOC-1～4）を採用するケース。

補論 2. 鍵抽出アプローチに基づく方式を適用した生体認証システムの効果

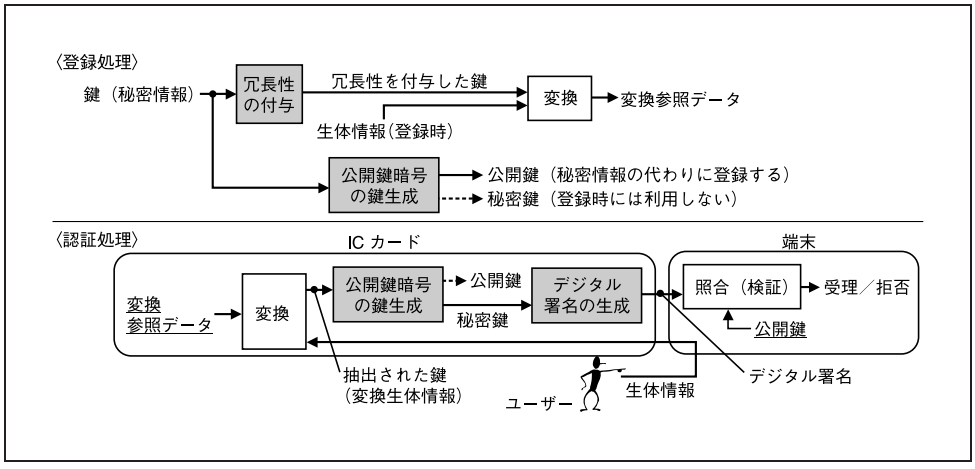
(1) 検討対象とするシステム

鍵抽出アプローチのメリットの 1 つは、変換参照データから抽出した鍵を用いた暗号技術ベースの認証を実行することができる点にある。そうしたメリットを活用した方式の一例として、抽出した鍵を用いたデジタル署名の生成と検証によって認証を行うという方式を検討対象とする。こうした方式にはさまざまなバリエーションが想定されるが、ここでは、IC カード内部においてデジタル署名を生成し、同デジタル署名を端末において検証するというタイプの方式の 1 つ（以下、STOC-α 方式と呼ぶ）を例として取り上げる（図表 A-5 参照）。

STOC-α 方式では、登録時に、予め設定した鍵から公開鍵暗号の公開鍵を生成し、秘密情報の代わりに端末に格納するほか、冗長性を付与した鍵と生体情報から変換参照データを生成し IC カードに格納する。認証時には、IC カードは、取得した生体情報を用いて変換参照データから鍵を抽出し、この鍵から公開鍵暗号の秘密鍵を生成する。さらに、この秘密鍵でデジタル署名を生成して端末に送信する。端末は秘密情報として格納されている公開鍵を用いてデジタル署名を検証する。

なお、STOC-α 方式に利用されている認証方式は 3 節の要件 1～3 を満たしていると仮定するほか、デジタル署名の生成・検証に利用する公開鍵暗号は安全であり、いずれの攻撃者も公開鍵から秘密鍵を求めるなどの署名の偽造は困難であると仮定する。また、デジタル署名の生成に当たり IC カードや端末で生成された乱数等を用いており、盗取したデジタル署名を再送するというなりすましは防ぐことができると

図表 A-5　STOC-α 方式の登録と認証の処理フロー



備考：下線は、IC カードや端末に格納されているデータであることを示す。

仮定する。

(2) なりすましへの耐性

STOC-α 方式について、2 節において定義した攻撃者 1〜6 によるなりすましへの耐性を分析すると次のとおりである（図表 A-6 参照）。

- 攻撃者 1 は、正規の IC カードを利用するものの変換参照データ等を入手できないため、なりすましが成功する確率は他人受入率程度になると考えられる。
- 攻撃者 2〜4 は、正規の IC カードを利用するほか変換参照データを入手するが、STOC-α 方式は要件 1（変換参照データを入手してもなりすましが困難）を満たすため、なりすましに成功する確率は他人受入率程度であると考えられる。
- 攻撃者 5 については、本人の生体情報や公開鍵等が利用できるものの、これらの情報から秘密鍵を求めることが困難であり攻撃実行が困難であると考えられる。
- 攻撃者 6 は、正規の IC カードを利用できないほか、変換参照データ等を入手していないため、攻撃者 5 と同様になると考えられる。

このように、STOC-α 方式は要件 1〜3 を満たしているという条件のもとで攻撃者 1〜6 に対して耐性を有しており、MOC-α 方式（類似度保存アプローチ）と同様に補論 1 で検討対象とした方式（STOC-1〜4、MOC-1、2）よりも攻撃者 1〜6 によるなりすましへの耐性が高いことがわかる。また、MOC-β 方式のように、要件 1〜3 を満たす鍵抽出アプローチに基づく方式を用いたとしても、システム構成によってなりすましへの耐性に差異があると考えられる。

図表 A-6　漏洩情報を用いたなりすましへの STOC-α 方式の耐性

	攻撃者が入手するデータ	なりすまし成功確率
攻撃者 1	なし	他人受入率程度
攻撃者 2〜4	変換参照データ	
攻撃者 5	・本人の生体情報 ・公開鍵 ・デジタル署名	（暗号アルゴリズムを解読困難であり、攻撃困難である）
攻撃者 6	なし	