

研究指導 中澤 真 助教授

金融機関における生体認証システムの在り方

後藤 千佳子

1. はじめに

近年、情報システムの安全性に対する要求が高まり、生体認証技術が急速に普及しつつある[1]。この認証技術は、電子パスポート¹や入退室管理システムなどにも用いられており、適用範囲に広がりを見せている。

金融機関においても、偽造・盗難キャッシュカード問題への対応策として、ICキャッシュカードと共に生体認証が導入され始めた。そして2006年10月には日本郵政公社も生体認証を導入し、現在も導入を検討している金融機関が増加しつつある[3]。

しかし、生体認証を導入・運用する場合には、利用者が認証を行う際に生じる問題や金融機関が運用する際に直面する問題などを想定し、その対応策も検討しなくてはならない。認証システムの安全性はもちろんのこと、銀行などの金融機関の場合は利便性についても考慮すべきである。

本研究の目的は、金融機関利用者にとっての安全性と利便性が考慮された認証システムを提供することである。したがってその実現のため、生体認証運用の現状を調査・検討し、金融機関における生体認証システムの在り方を提案する。

2. 生体認証の特徴

生体認証²とは、身体的特徴(以下、生体情報)など、各個人に固有の特徴を用いて個人の認証を行う技術を指す[4]。この認証では、指紋や静脈といった身体的特徴の他に、サインや声といった行動的特徴も用いることが可能である。生体認証では、自身の身体自身がパスワードであるため、従来の暗証番号のように記憶する必要がなく、ICカードのように紛失する恐れがないといった利点が挙げられる。そのうえ、暗証番号の場合は、生年月日など本人に関連する数字を利用者が設定することが多いため、第三者に推測されてしまう可能性が高いが、生体情報では推測というものが出来ないため、暗証番号に比べて「なりすまし³」が困難であるといえる。

ただし、生体認証においても「なりすまし」は不可能という

¹ 偽造パスポートを使った違法な出入国を防ぐため、本人確認用のICタグを埋め込んだパスポートのこと。「IC 旅行券」、「e-Passport」ともよぶ[2]。

² 生体認証は、「バイオメトリクス認証」、「バイオメトリック認証」ともよばれている。

³ 不正アクセス形態の一つ。情報システムにアクセスする際に、何らかの手段を用いて他人になりすましてしまうこと[5]。

わけではなく、指紋認証装置がゼラチンで作成した偽造指を認証してしまったという研究も発表されている[4]。つまり、机などに付着した指紋から生体情報を偽造することが出来れば、なりすましも可能である。したがって、この点の脆弱性については生体検知機能⁴が入った装置を導入するなどの対処が必要となる。

3. 金融機関における生体認証システムの現状

生体認証は新たな本人認証の1つとして金融機関においても注目されている。しかし、「導入すれば安全」というわけではない。利点だけに目を奪われずに、脆弱な要素についても正しく把握し、認証システムを構築する必要がある。また、ただ設置するだけでよしとするのではなく、利用場所に適したシステムを構築すべきである。金融機関というのはさまざまな人が訪れて財を取り扱う場所であるため、安全性はもちろん、利便性の点も十分考慮された認証システムが必要であるといえる。本章では、生体認証の導入背景、導入状況を調査したうえで、構築する際に考慮すべき点を明らかにする。

3.1 導入の背景

金融機関が次々とICキャッシュカード、生体認証を導入する背景として、盗難・偽造キャッシュカードに関する被害が深刻であるためと考えられる。実際に、その被害は社会的な問題となり、銀行の信頼が失われる原因となった。

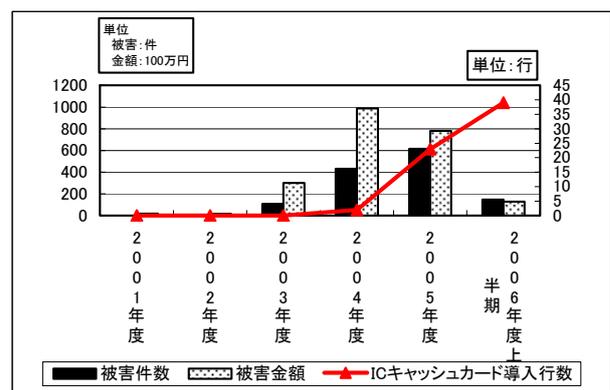


図1: 偽造キャッシュカードによる被害の推移

図1は年度別の偽造キャッシュカードによる被害の実態調

⁴ 認証の際、生体情報が生きた人間の身体から直接提示されているか否かを確認する機能のこと。人体の電気特性、光学特性、生理的特性などを用いて確認する[6]。

査結果[7]に関するグラフ⁵に、本研究で調査したICキャッシュカード導入銀行数の推移に関する結果を追加したものである。図1から読み取れるように、偽造キャッシュカードによる被害は金額、件数共に近年急激に増加している。このように被害が急増した理由としては、スキミング装置の入手が容易になったことや、カードデータを盗む技術の進歩などが挙げられる。

こうした盗難・偽造キャッシュカードによる被害の対応策として、金融機関は磁気キャッシュカード利用限度額引き下げやICキャッシュカードの導入を始めた。図1に示したように、ICキャッシュカードの導入行数が増加すると共に、偽造キャッシュカードの被害数は減少傾向になった。このことから、ICキャッシュカードは、スキミング⁶によるカード偽造の防止策として有効であるといえるだろう。

しかし、ICキャッシュカードも十分安全とは言い切れない。ICキャッシュカードにおける本人認証は暗証番号を用いているため、スキミング以外に関しては従来の磁気キャッシュカードと同様の脆弱性を持つ。そのため、ICキャッシュカードだけでは安全性が不十分とされ、次なる対策として生体認証に注目が集まり始めた。ICキャッシュカードと生体認証を共に導入することで、より確実な本人認証がされることを期待し、金融機関はこれらの導入を次々と進め始めている。

3.2 生体認証の導入状況

盗難・偽造キャッシュカード被害の対応策として注目されている生体認証だが、実際どの程度導入が進んでいるのか現状を調査した。以下は、インターネットを用いて都市銀行・地方銀行・第二地方銀行の計115行を調査した結果である。

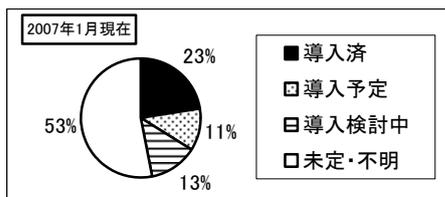


図2: 銀行における生体認証の導入状況(2007年)

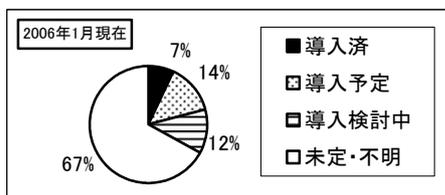


図3: 銀行における生体認証の導入状況(2006年)

図2は、銀行における生体認証の導入状況を表している。

⁵ 調査は、全国銀行協会が正会員・準会員(184行)を対象に実施した。

⁶ クレジットカードやキャッシュカードの磁気情報を不正に読み出してコピーを作成し、使用する犯罪行為のこと[8]。

2007年1月の時点では、全体の約2割の銀行が既に認証装置を導入済みであり、導入を予定、もしくは検討している銀行も合わせると、約半数が導入に肯定的な姿勢であることが分かった。ちなみに図3は2006年1月時点の生体認証導入状況である。2006年においては、肯定的な意見が3割にとどまっていたが、2007年では5割にまで増加した。この理由として、暗証番号を必要とするICキャッシュカードだけでは、利用者が安易な暗証番号を利用する可能性があるため、銀行は安全性をより高めるために今後も生体認証の導入を進めるであろう。

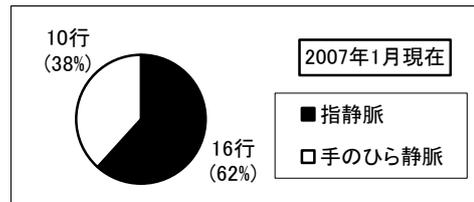


図4: 生体認証で取り扱う生体情報の内訳

次に、利便性を考慮するため「取り扱い生体情報の種類」について調査した結果を図4に示した。この図より、金融機関で採用されている生体情報は、指静脈もしくは手のひら静脈というのが現状であることが分かる。指静脈を採用している銀行が若干多いが、それ程大きな差ではない。しかし、今後生体認証を導入予定としている銀行も含めると、手のひら静脈は10行、指静脈は25行となり、その差が開きが出てくる。そのためATMの数や、提携銀行が限られてしまうといった点から、手のひら静脈認証を採用している銀行の利用者達は利便性が損なわれる可能性があるといえる。

3.3 従来の磁気カード・ICキャッシュカード・生体認証付ICキャッシュカードの相違点

ここでは、従来使用されている磁気キャッシュカード、ICキャッシュカード、生体認証付きICキャッシュカードの相違点について述べる。これらのキャッシュカードの安全性は、盗難・偽造という点から磁気キャッシュカードが一番脆弱である。逆に最も安全性が高いのは、生体認証ICキャッシュカードである。ICキャッシュカードの場合、偽造防止の点では安全であるといえるが、それ以外の点では磁気キャッシュカードと同様の脆弱性を持つ。

以下において、利用限度額、被害に対する補償という2点からキャッシュカードにおける差異を述べる。

3.3.1 利用限度額

現在では盗難・偽造キャッシュカード被害への対応策として、ほとんどの金融機関がATMにおける磁気キャッシュカードの利用限度額引き下げを実施している。その引き替えとして、生体認証を用いたATM利用の場合は磁気キャッシュカードでの取引に比べて、限度額も上限を高く設定している。

みずほ銀行の例を取ると、磁気キャッシュカードにおい

て1日の引き出し限度は最高200万であるが、生体認証を用いた利用であれば、引き出し限度は最高500万となる⁷。限度額の設定については各行それぞれ異なるが、どの銀行でも磁気キャッシュカードと生体認証ICキャッシュカードの間に限度額の差がみられた。しかし、磁気キャッシュカードとICキャッシュカードの場合にはほとんど限度額の差がみられないことが多かったため、ICキャッシュカードのみでの使用の場合、安全面が不十分であることが、このような運用面からもうかがえる。

3.3.2 被害に対する補償

増加し続ける偽造・盗難キャッシュカードを使った犯罪から預金者を保護するため、2006年2月に預金者保護法⁸というものが施行された。この法律は、偽造や盗難されたキャッシュカードによって不正に預貯金の引き出しなどをされた場合、金融機関が原則として全額被害補償⁹をするというものであり[9]、これはすべてのキャッシュカードに適用される。

では、金銭の補償ではなく、プライバシーに関する補償というものはどうであろうか。生体認証ICキャッシュカードにおける生体情報そのものの盗難・流出が発生した場合の補償について調査した。

都市銀行からの回答によると、現時点ではそのような補償を設けていないとの返答がきた。その理由として、生体情報は暗号化されたICチップの中に格納されているため、生体情報の漏洩の可能性がほとんどないという見解により、銀行側では特別に補償を設定していないということであった。銀行側の姿勢としては、生体情報の盗難や流出の発生、可能性が発覚した際に、補償なり対応を考えるというのが現状である。

3.4 対応ATMの普及

次に利便性に着目し、ICキャッシュカード、生体認証に対応したATMの導入状況についてを調査した。なお、導入調査の範囲は店舗内ATM、店舗外ATMの両方である。

3.4.1 ATMの普及状況

図5はICキャッシュカードに対応したATMの割合、図6は生体認証に対応したATMの割合を表したグラフである。これらはインターネットを用いて、ICキャッシュカードを導入している銀行42行のATM計18,342ヶ所、生体認証を導入している銀行23行のATM計12,879ヶ所を調査した結果である¹⁰。

2007年1月時点で、ICキャッシュカード対応と生体認証対応のATMは共に6割を超えていることが明らかとなった。し

かし、全体的な設置箇所は生体認証対応ATMよりICカード対応ATMが多く、ICキャッシュカードの方が利便性が高いといえる。

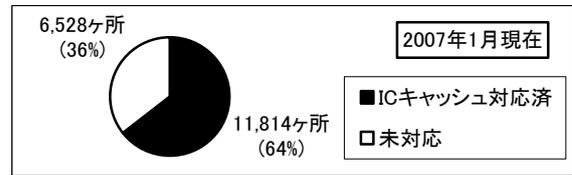


図5: ICキャッシュカード対応ATMの割合

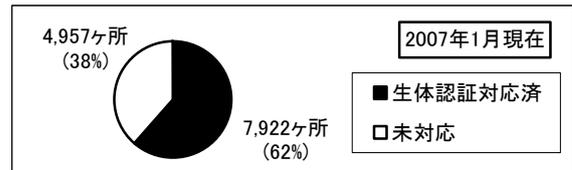


図6: 生体認証対応ATMの割合

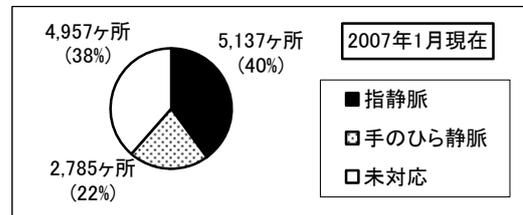


図7: 生体認証対応ATMの詳細

生体認証対応ATMの詳細については図7に示した¹¹。3.1で述べた通り、生体認証を導入している金融機関は指静脈もしくは手のひら静脈を生体情報として用いている。このような現状では、指静脈を採用している銀行と手のひら静脈を採用している銀行間の提携が進まない。その結果、利用者が利便性という点で不利益を被ってしまうといえる。それどころか、同じ生体情報を用いている銀行同士でさえ提携がなされていないため、生体認証付ICキャッシュカードを発行した銀行でのATMでしか利用できず、利便性は極めて低いといえる。

3.5 生体認証付ICキャッシュカードの詳細

現状として、認証の際に照合で必要となる自身の生体情報は、生体認証ICキャッシュカード内に格納されていることが多い。このような格納の仕方をストアオンカード方式[10]という。ストアオンカード方式ならば、銀行側が利用者の生体情報データベースを管理することがないため、個人の生体情報が大量に漏洩してしまうといった危険性もない。またICカード内では、生体情報が格納されている他、認証における照合も内部で処理される¹²。この利点については次章で述べる。

⁷ 磁気キャッシュカードに当初設定されている限度額は50万円、生体認証付ICキャッシュカードは100万円である。これらはそれぞれ磁気は200万円、生体認証は500万円と、限度額の変動が可能。

⁸ 正式名は「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」。

⁹ 補償は、預金者の過失の度合いによってその割合も変化する。

¹⁰ なお、生体認証対応ATM数が不明の4行は省略。

¹¹ 現在では郵政公社も指静脈を用いた生体認証サービスを始めたため、実際には図7以上に指静脈対応ATMが設置されている可能性が高い。

¹² ICカードに登録した生体情報と、自身が提示した生体情報を照らし合わせ、本人確認をする。

4. 運用システムの検討

4.1 カードの仕様

3.5で述べたように、生体情報をICカード内に格納する方式の場合、ICカードと生体情報は利用者の自己管理となるため、利用者にとっても安心感があるだろう。この理由として、銀行側で管理される場合、利用者にとってはその管理の部分が不透明であることや、大量漏洩の危険性があるといったことなどが挙げられる。

また、カード内で照合を行うということの利点としては、生体情報をカード外に出さないということであるため、カード内の生体情報が盗聴されるという危険性が比較的低下するということである。よって現在用いられているカードは安全性が考慮されている形であるといえる。

4.2 利便性の向上

生体認証を導入する金融機関が増加しているにも関わらず、その銀行間でのATM提携が進んでいないというのが現状の問題である。事実、着々と提携を進めている金融機関といえば日本郵政公社が挙げられるが、銀行では他銀行との提携に力を入れてるような姿勢があまりみられない。その原因として、磁気ストライプが併用された生体認証付ICキャッシュカードの存在が考えられる。銀行では利便性も考慮に入れ、磁気ストライプも付加された生体認証ICキャッシュカードを発行している場合が多い。しかしそういった場合、磁気ストライプ部分での被害が懸念される。キャッシュカードは個別に利用限度額が変更出来るため、銀行側では安全面から磁気ストライプの利用限度引き下げを推奨しているが、いくら利用限度額の変更が可能だとしても、それでは安全性が十分に考慮されているとはいえない。銀行間で生体認証対応ATMの提携を進めることによって、磁気に頼ることなく安全かつ便利に財の取引が出来る。したがって、安全性と利便性を確立するためにも、銀行は他銀行と生体認証対応ATMの提携を図るべきである。

4.3 偽造問題の対応策

生体偽造による不正な引き出しへの対応策として生体検知機能を搭載した認証装置が有効と考えられる。これによって、認証の際に生体情報が生きた人間の身体から直接提示されているか否かを確認することが可能である。現状では、銀行側でこうした対応策を導入していない。しかし2章でも述べた通り、生体情報は偽造が可能であるという研究も発表されているため、こうした対応策も今後視野に入れるべきである。

4.4 その他サービスの検討

ATMは利用者層が幅広いいため、その操作は容易である必要がある。したがって、認証における操作の指示が画面上に表示されることが望ましい。

また、利用者達にはあらかじめ、生体認証において本人拒否といった認証エラーが生じる可能性があることを把握し

てもらふ必要もある。利用者による生体情報の提示方法によっては、ICキャッシュカードに登録された生体情報と特徴点が一致しない場合があるため、こうした認証エラーが発生してしまうのである。利用者は拒否されることをあまり意識・想定しないため¹³、金融機関側が事前に何らかの形で告知しておくべきである。

5. むすび

本研究では、金融機関での生体認証システムの現状を調査したうえで、生体認証システムの在り方を提案した。この研究によって、現在の運用状態において解決すべき問題点が明らかになり、今後のシステム運用で検討すべきことが見えてくるだろう。そのことにより、利用者にとって不利益を被らない形のシステムを実現することも出来る。

現在、生体認証が金融機関という公の場所に次々と導入され始めている。預金者保護法も適用され、今現在では大きな被害が生じていることはないが、解決すべき課題も多く残っている。生体認証技術を用いる限り、本人拒否や個人情報に関する問題は避けて通れないものであり、アクセシビリティという点においても考慮が必要となる。しかし、これらの問題へと一つひとつ確実に対応することで、より安全で利便性の高い認証システムの構築が出来るだろう。

参考文献

- [1] 山崎恭, “安全性対策技術の動向,” 情報処理学会研究報告, vol.47, no.6, pp.600-604, 2006年6月.
- [2] http://itpro.nikkeibp.co.jp/a/biz/keyword/key0914/key_45.shtml, 今週のITキーワード, 日経BPネット.
- [3] 外昌弘, “我が国金融機関におけるバイオメトリック認証技術の活用について,” 情報処理学会研究報告, vol.47, no.6, pp.577-582, 2006年6月.
- [4] http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdf, 金融取引における生体認証について, 金融庁, 2005年4月.
- [5] 日経BP編, セキュリティ用語辞典, 日経BP社, 2002.
- [6] <http://www.imes.boj.or.jp/japanese/kinvyu/2005/kk24-b2-1.pdf>, 生体認証における生体検知機能について, 日本銀行金融研究所, 2005年12月.
- [7] http://www.zenginkyo.or.jp/news/19/pdf/news190215_2.pdf, 偽造キャッシュカード問題に関する実態調査結果, 金融庁.
- [8] <http://www.jilcom.or.jp/skimmingreport1.html>, スキミング犯罪対策レポート, 日本情報安全管理協会.
- [9] http://www.shugin.go.jp/itdb_housei.nsf/html/housei/16220050810094.htm, 偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律, 衆議院.
- [10] <http://itpro.nikkeibp.co.jp/artICle/COLUMN/20051110/224369/>, バイオメトリクスと連携するICカード, ITpro.

¹³ 従来のカードの場合、暗証番号を間違えることがなければ認証率は100%であるため。