IMES DISCUSSION PAPER SERIES

リテール・バンキングのセキュリティ向上を目指して

岩下 直行（いわした なおゆき）

Discussion Paper No. 2007-J-7

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 2007-J-7
2007 年 3 月

リテール・バンキングのセキュリティ向上を目指して

岩下 直行[*]

要　旨

2004 年から 2005 年にかけて、わが国の銀行業界が偽造キャッシュカード問題への対応を巡って激しい批判を浴びてから、約 2 年が経過した。金融機関が ATM における引出限度額を引き下げたことや、利用者への注意喚起を行ったことの効果もあって、偽造キャッシュカードによる不正預金引出の被害金額は、このところ減少してきている。偽造・盗難カード預貯金者保護法が施行され、被害者に対する補償が進んだこともあって、銀行業界に対する批判はようやく鎮静化しつつあるように窺われる。

しかし、やや長い目でみたとき、わが国におけるリテール・バンキングのセキュリティには、未だに不安な要素が残されている。特に、偽造カード犯罪の未然防止対策として導入された IC キャッシュカードや生体認証といった新しい情報セキュリティ技術は、現時点ではあまり普及しておらず、その特性が十分に活かされているとは言いがたい状況にある。このため、今後、外部環境が変化すれば、再び偽造カード犯罪が増加しないとも限らない。これらの技術を活用してリテール・バンキングのセキュリティを抜本的に改善していくためには、アカデミックな知見を活用して技術の内容に関する詳細な検討を進めるとともに、業界全体として普及促進のためのグランドデザインを描いていくことが必要であろう。

キーワード：偽造キャッシュカード問題、リテール・バンキング、IC カード、生体認証、セキュリティ、偽造・盗難カード預貯金者保護法
JEL classification: L86、L96、Z00

[*] 日本銀行金融研究所参事役（E-mail: iwashita@imes.boj.or.jp）

本稿は、2007 年 3 月 6 日に日本銀行で開催された「第 9 回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている意見は、筆者個人に属し、日本銀行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個人に属する。

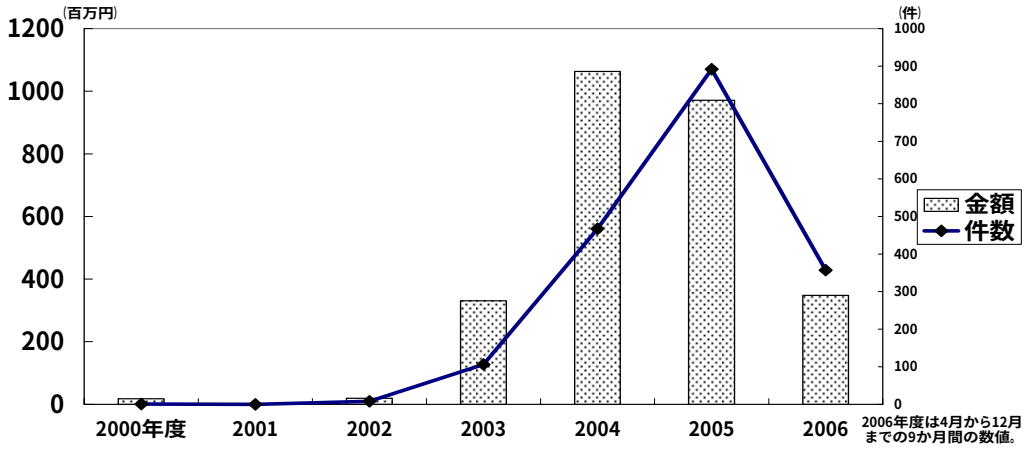
目　次

1．偽造キャッシュカード被害の推移

2004 年から 2005 年にかけて、わが国の銀行業界は、偽造キャッシュカード問題への対応を巡って激しい批判を浴びた。それまでほとんど発生していなかった偽造キャッシュカードによる不正預金引出の被害金額が、2004 年度には 10 億円に急増したのである。2005 年 1 月に、ゴルフ場の貴重品ロッカーからキャッシュカードを盗み出してスキミングする手口で不正預金引出を行っていたグループが逮捕され、その手口が大きな扱いで報道されると、テレビの報道番組や雑誌記事が相次いで被害の深刻さを伝え、金融機関の対応を批判する声が相次いだ。このため、銀行業界は、偽造キャッシュカードを作られないようにするために、キャッシュカードの IC カード化と ATM における生体認証による本人確認を導入することや、被害の拡大を防ぐために、キャッシュカードの利用限度額を引き下げること等について、各行が積極的に検討していくことを申し合わせたと発表した[1]。

2005 年 6 月には金融庁・偽造キャッシュカード問題に関するスタディグループの報告書[2]が公表された。2005 年 8 月には「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」（以下「偽造・盗難カード預貯金者保護法」という。）が公布され、2006 年 2 月から施行された。これにより、偽造・盗難キャッシュカードによる不正預金引出に伴う被害については、原則として金融機関が被害者に補償を行うこととなった。また、金融機関は、被害の補償に加え、偽造カード犯罪の事前予防策として、認証技術の強化等が義務付けられることとなった。

偽造キャッシュカードによる預金等不正払戻しの被害金額･件数の推移



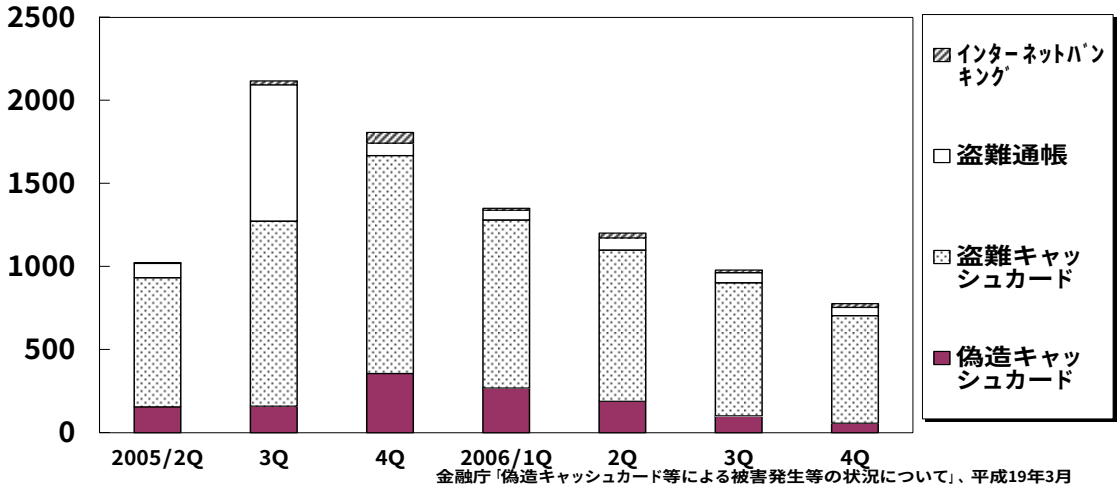
金融庁「偽造キャッシュカード等による被害発生等の状況について」、平成19年3月

[1] 全国銀行協会[2005]
[2] 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[2005]

偽造キャッシュカードの被害は、2004 年、2005 年と高水準で推移した後、2006 年度になって、件数、金額とも、大幅に減少しつつある。特に 2006 年度（4～12 月の 9 ヶ月間）の被害金額の水準は、社会問題化する以前の 2003 年度の水準にまで低下してきている。

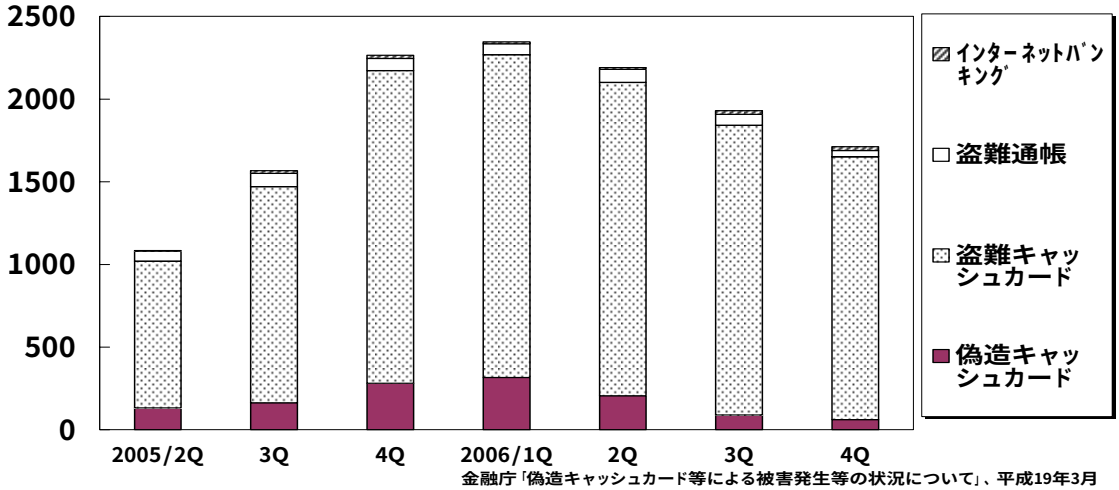
偽造・盗難キャッシュカード、盗難通帳、インターネットバンキングの不正預金引出の合計をみても、被害金額は、最近 1 年間は顕著に減少していることがわかる[3]。なお、この 4 つの犯罪類型の中では、盗難キャッシュカードによる被害のウェイトが最も高い。

（百万円）　犯罪類型別預金等不正払戻し被害金額の推移



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」、平成19年3月

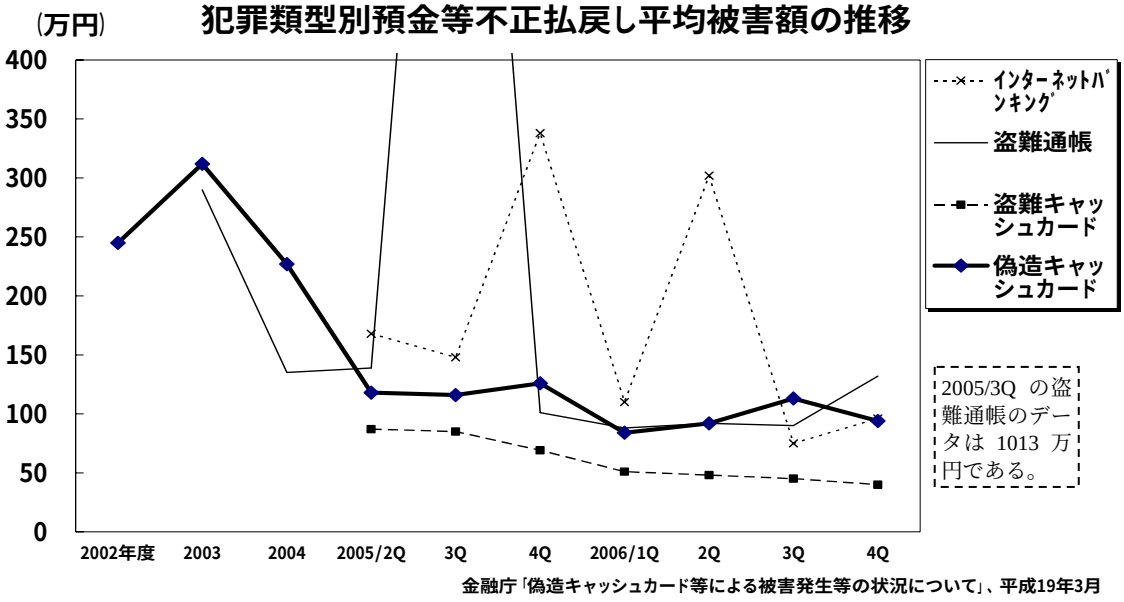
（件）　犯罪類型別預金等不正払戻し被害件数の推移



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」、平成19年3月

[3] 盗難キャッシュカードとインターネット･バンキングの被害金額･件数のうち 2005 年 1 月以前の統計は公表されていないため、図示した期間より前の被害の推移は不明である。

1 件当りの平均被害額の推移をみると、2004 年以前まで統計が遡ることができる偽造キャッシュカードについては、かつては 200～300 万円であったのに対し、2005 年以降は 100 万円前後となっている。最近 2 年間の統計しかない盗難キャッシュカードについても、この 2 年間で平均被害額が 80 万円前後から 40 万円前後に半減している。盗難通帳とインターネットバンキングについては、案件毎の被害金額の規模にばらつきがあり、平均被害額も振れている。



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」、平成19年3月

また、被害の補償状況についてみると、偽造キャッシュカードについては、調査対象期間を合計した値で、件数ベースで 98.1%、盗難キャッシュカードについては 67.3%が補償されており、特に、偽造・盗難カード預貯金者保護法施行後に発生した偽造キャッシュカード被害については、100%が補償されている。

犯罪類型別 預金等不正払戻しの補償の状況

（単位：件）

	調査対象期間の合計			うち 2006 年度中（4 月～12 月）		
	被害件数	補償件数	構成比	被害件数	補償件数	構成比
偽造キャッシュカード	1,617	1,587	98.1%	243	243	100.0%
盗難キャッシュカード	9,912	6,666	67.3%	3,794	2,402	63.3%
盗難通帳	1,347	282	20.9%	138	24	17.4%
インターネットバンキング	80	41	51.3%	33	11	33.3%

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」、平成 19 年 3 月
補償処理方針について調査・検討中のものを除いて集計。盗難キャッシュカードについては、一部補償を含む。

2．どの対策が有効だったのか

偽造キャッシュカード等による不正預金引出の被害が減少したのは、金融機関が講じてきた様々なセキュリティ対策が奏効したものと考えられるが、それらの中のどの対策が有効だったのだろうか。

最も有効だったと考えられるのは、2004 年頃から各金融機関が進めてきた、キャッシュカードの利用限度額の引下げである。この対策は、業態を問わず、ほぼ全ての金融機関で実施されてきた。偽造キャッシュカードが問題となる以前は、限度額を１日当り数百万円に設定するのが一般的であったが、現在では、IC カードや生体認証を利用した取引を除けば、1 日当り 50 万円程度に設定するのが一般的となっている。この対策が直接的に、1 件当りの平均被害額の低下に寄与し、被害金額を引き下げているのは明らかであろう。また、平均被害額の低下の間接的な効果として、犯罪者の立場からみたとき、偽造キャッシュカードによる預金不正引出の「身入り」が悪くなり、犯罪者にとって「割の合わないビジネス」となったことから被害件数も減少し、相乗効果で被害金額も減少したものと考えられる。

また、報道等を通じて利用者の間で偽造カード被害に関する認知度が上がったことや、金融機関が利用者に積極的に警告を発した効果により、利用者がカードや暗証番号を慎重に取り扱うようになったことも有効であったと考えられる。

これに対し、IC カードや生体認証などの事前予防対策が被害の減少に大きく寄与したとは考えにくい。2005 年末時点の調査では、IC キャッシュカードは全てのキャッシュカード発行枚数の 1.2%しか普及しておらず[4]、その後も IC カード化が急速に拡大する状況にはなかった。このため、「スキミング被害に遭ったキャッシュカードがたまたま IC カードだったために、不正預金引出の被害を免れた」ということが起こる蓋然性はかなり低いと考えられる。

更に、仮に生体認証付きの IC カードを利用しているケースであっても、不正預金引出の被害に遭わないで済むとは限らない。現段階で発行されている IC キャッシュカードのほとんどは、コンビニや提携先の ATM での利用を可能とするために、IC カードに磁気ストライプ（MS：Magnetic Stripe）が貼付された IC-MS 併用カードとなっており、コンビニや提携先の ATM では、生体認証機能のない通常の磁気ストライプカードとして認識される。IC-MS 併用カードは、磁気ストライプ部分のみを偽造することが容易であり、提携先 ATM で利用すれば、生体認証を使用することはできない。こうした現在の仕組みを前提とすれば、IC カードや生体認証といったセキュリティ対策に、不正預金引出の被害を減少させる強い効果を期待することは難しいといわざるを得ない[5]。

---

[4] 金融庁[2006]

[5] IC-MS 併用カードは、IC カードとして利用する場合は限度額が高く設定でき、磁気ストライ

3．今考えるべき課題

ともあれ、偽造キャッシュカード問題を契機とする、わが国のリテール・バンキングのセキュリティに対する批判と不信感は、被害の減少という実績によって沈静化しつつある。偽造カード犯罪の根が絶たれたわけではないが、金融機関のセキュリティを巡る状況は、いわば緊急事態を脱し、平時に復したように窺われる。

2 年前、金融機関は、「セキュリティ対応を推進している」ことをアピールする必要があったこともあり、各種セキュリティ対策を精査し、偽造キャッシュカード問題に対する有効性を厳密に評価した上で、最も有効な形で導入する、という対応は難しかった。しかし、緊急事態を脱した今、やや長い目で、リテール・バンキングのセキュリティを向上させるためのグランドデザインを描くことが求められているのではないだろうか。

「実際に被害を押さえ込んだのだから、現在の対策を継続することでよいのではないか」という意見もある。被害金額の減少が、抜本的なセキュリティ対策の奏効によるものであれば、そのように考えることも可能であろう。しかし、現状は、偽造カードや振り込め詐欺の被害拡大による利用者の不安を背景として、主として利用者の利便性に制限を加え、利用限度額を引き下げることで被害金額を押さえ込んでいる状態にある。今後、被害の縮小により利用者の不安感が薄らいでくれば、利便性を向上させる動きが出ることも考えられ、そうなれば、また被害が拡大する可能性もある。磁気ストライプカードと 4 桁暗証番号という脆弱な個人認証メカニズムを利用している限り、新しい犯罪の手口を常に警戒していなければならない。

こうした視点に立てば、このタイミングでセキュリティ対策の手を緩めるのは適当ではないと考えられる。検討を行うための時間的猶予が生じたと受け止めて、従来十分には対応できていなかった、抜本的なセキュリティ対策の検討を進めるべき時期ではないだろうか。

実際、わが国におけるリテール・バンキングのセキュリティには、未だに不安な要素が残されている。カード偽造犯罪の未然防止対策として導入された IC キャッシュカードや生体認証といった新しい情報セキュリティ技術は、現時点では、その特性が十分に活用されているとは言いがたい状況にある。IC カードについては、多くの銀行で導入を開始したものの、その普及はごく低い水準にとどまっている。IC カードとして提携先 ATM で利用したり、IC カードとしてデビットカード取引に利用したりすることができないため、利用者の側からは、

プカードとして利用する場合は限度額が低く抑えられるのが一般的である。IC-MS 併用カードの磁気ストライプ部分がスキミングされ、偽造カードが作成されたとしても、低いほうの利用限度額が適用されるため、被害金額が限定されるという効果は期待できる。

あえて IC カード化することのメリットは感じられない。生体認証についても、一時的に注目度も上がり、世間の関心は集めたものの、あえて手間をかけて手続きをしようとする利用者はさほど多くはないようである。

この結果、IC カードと生体認証は、金融機関のセキュリティ対策の「旗印」として掲げられてはいるものの、やや中途半端な位置付けとなっている。もしも、IC カードと生体認証の活用によってキャッシュカードのセキュリティを引き上げることが重要という判断であるならば、例えば、既往発行分のキャッシュカードを IC カード化するように利用者に働きかけるとか、提携先 ATM でも IC カードと生体認証が利用可能なようなオンライン提携を実現する、といった対応が考えられるが、実際にはそのような取組みはあまりみられていない。現段階では、IC カードや生体認証をどの程度積極的に普及させていくべきかについて、各金融機関の中での方針が固まっていない状態と考えられる。

以下では、これらのセキュリティ技術の将来像について考えてみたい。

4．キャッシュカードの IC カード化を巡って

(1) なぜ IC カード化するのか

キャッシュカードの IC カード化は、偽造キャッシュカード問題が深刻化するよりも前の段階から、銀行業界が当然取り組むべきプロジェクトと受け止められてきた。全銀協が IC カードの標準仕様の初版を策定したのは 1988 年であり、当時から、①利用者利便の向上、②ビジネス機会の拡大、③セキュリティ強化が、IC カード化推進の目的とされていた。具体的には、①銀行が発行する IC カードの領域を他者に貸与し、身分証明書や会員証など、様々な業務プログラムを載せることにより利用者の利便性を向上させる、②銀行がデビットカードや電子マネーなどのサービスを提供するためのプラットフォームとすることで銀行のビジネス機会を拡大する、③更に耐偽造性を高めることでセキュリティを強化する、という構想であった。

その後、いくつかの外部環境の変化が起きた。まず、かつては高価であった IC カードの価格が下がり、あえて共用化しなくても、様々な用途の IC カードが各々の発行主体によって発行されるようになった。従来主流であった接触型の IC カードのほかに、非接触型の IC カードが広く利用されるようになった。偽造犯罪の増加や個人情報保護法の施行等により、金融取引にかかるセキュリティへの要件が一段と強くなった。

こうした環境変化によって、かつてイメージされていたキャッシュカードの IC カード化に関する構想の多くは、既にビジネス的に主流とは言えなくなって

きている。実際、最近発行されている IC キャッシュカードは、もっぱらセキュリティ強化を目的としており、IC カード化により耐偽造性を高めるとともに、IC カードを生体認証のプラットフォームとして利用している。IC カードの記憶領域に生体情報を格納することによって、センシティブな個人情報を金融機関のホスト・コンピュータに格納したり、ネットワークで送受信したりすることを回避でき、個人情報の管理に伴うリスクから逃れられるからである。

(2) IC カードは金融機関のシステムのセキュリティを変える

現在、銀行の ATM で利用されている IC キャッシュカードは、ATM との間のやり取りだけが IC 対応となっており、金融機関のホスト・コンピュータへは、磁気ストライプカードを利用した場合と同じ情報しか届かないようになっている。そのような使い方をする限りにおいては、IC カードは単に「耐偽造性や生体認証対応能力を持った磁気ストライプカードの代替物」に過ぎない。しかし、IC カードには、金融機関のシステムにおけるセキュリティの設計思想を抜本的に変えていく潜在的な力がある。

現在の銀行のシステムにおけるセキュリティの設計思想は、センターのホスト・コンピュータから本支店の端末機、ATM に至るまでシステム全体を物理的に保護し、クローズド・ネットワークとすることでセキュリティを守るというものである。もちろん、そのような設計思想で巨大なネットワーク・システムを維持するにはコストがかかるが、その分、システムの変更や追加を行う場合も、外部と接続さえしないように注意していれば安全が確保できるという利点があった。しかし、リテール・バンキングの実務が様々な領域に拡大し、外部ネットワークとの接続を行うようになると、従来の設計思想のままでは、セキュリティが確保できなくなるという問題が発生してしまう。

一方、IC カードは、CPU と秘密鍵を内蔵しているため、通信を暗号化したり、通信先との間で相互に相手認証を行ったり、取引の都度、その証跡を安全に記録したりすることができる。このため、IC カードとホスト・コンピュータとが直接通信する仕組みを組み込んでさえいれば、ネットワーク全体のセキュリティが低くても、安全に取引を行うことができる。現在のわが国における IC キャッシュカードの中にも、このような方法で取引の安全性を確保する仕組みが作りこまれている。このような、IC カードによる「トランザクション単位のセキュリティ確保」というアプローチは、とりわけ、クレジットカード、デビットカードのような対顧客用ネットワークを利用する業務や、インターネットのような信頼性の低いネットワークを利用した業務を行う上で、有用な解決策と

なり得る[6]。

わが国においては、現時点では、銀行のシステムのセキュリティはクローズド・ネットワークで守るというコンセプトが主流である。しかし、IC カードを導入していくことで、それとは異なるアプローチも選択肢に加えることができる。金融機関が接続する外部ネットワークが増えている現在、金融機関のシステムのセキュリティの設計思想を大きく変え、こうしたアプローチを採用する選択肢を確保しておくことが大切と考えられる。

(3) IC カード自体のセキュリティ低下にどう対処するか

IC カードが抱える現実的な問題点のひとつは、IC カードの導入が検討され始めてからかなり時間が経ったため、現在の標準的な技術が既に古いものになりつつあるということであろう。IC カードは、IC カード用端末との間で、真正なカードであることを確認したり、個々の取引データに対して固有の認証コードを生成したりする際に、標準化された暗号プロトコルを利用する仕組みになっている。IC カードは汎用のデバイスであり、標準仕様に則って製造されることによって互換性が担保されるため、早くから国際的な仕様の標準化が進められてきた。現在、IC カードの技術標準として利用されている EMV 仕様は、1990 年代前半にその基本が議論されたものである。その後、累次の改定を経てきたとはいえ、策定から 10 年以上が経過し、現在の暗号技術の視点からみればリスクのある記述が目に付く[7]。現在普及している IC カードに直ちに問題があるわけではないが、これから本格的に IC カード化を進めていく場合、実装段階においてこうした点にも留意し、必要に応じて見直していくことが、長い目で見て、IC カードの安全性を維持するとともに、円滑な普及に繋がるものと思われる。

5．生体認証をどう普及させるべきか

偽造キャッシュカード問題への対応という観点からみたとき、生体認証は、カードと暗証番号の管理に不備があった場合でも不正引出を防止できる、という点で注目されている。ただし、リテール・バンキング取引における認証手段としては、まだ登場して日が浅く、ユーザー側にもベンダー側にも、十分な技術蓄積が進んでいないという問題がある。このため、「究極のセキュリティ」と持ち上げすぎるのは、万一、問題が生じたときの反動を考えると適当ではない。その有用性とリスクについて、様々な角度から慎重に検討していくことが必要

[6] 田村・廣川[2007]
[7] 鈴木・神田[2007]

であろう。

2006 年度における不正預金引出の被害金額でいえば、偽造キャッシュカードよりも盗難キャッシュカードの被害の方が 7 倍も多い。IC カード化だけでは盗難の被害までは防げないので、偽造カードのみならず盗難カードの被害の補償を定めた偽造・盗難カード預貯金者保護法を前提とすれば、金融機関にとって、生体認証のような本人認証手段のセキュリティを高めていくことは、今後是非必要なことであろう。国際的にみると、リテール・バンキングにおける本人認証手段は暗証番号を用いることが一般的ではあるものの、わが国の場合、ATM 等での取引金額がなお高額であること、利用者における暗証番号の管理が緩に流れがちという実態があることを踏まえる必要がある。生体認証は、見方を変えれば、「利用者が意識しなくても厳格に管理される暗証番号」と解釈することもできる。

ただし、生体認証が広く利用されるためには、預金者の大多数に生体認証を登録・利用してもらうことが必要となる。現在のように、ごく一部の利用者だけしか利用していない状態では、暗証番号と同じような位置付けのものとして使うことはできない。十分に生体認証が普及した後であれば、例えば、生体認証を利用しない場合は、預金引出限度額を現在よりも引き下げるなどの方策により、利用者をセキュリティの高い方向に誘導していくことが考えられる。その前提としては、生体認証に対する理解と信頼を深めることが大切であり、現在行われている生体認証の導入は、そうした高セキュリティ化のための布石と位置付けるべきであろう。生体認証に関する多様な受け止め方が存在することを踏まえて、問題点を十分に検討し、その結果をオープンにしていくことによって、信頼を勝ち得ていくことが必要である。その意味からも、生体認証を含む本人認証システムの安全性評価に関する研究[8]が、今後益々重要になってくるものと考えられる。

6．短期的な課題と中長期的な課題

リテール・バンキングのセキュリティ上の問題を考える上では、解決しようとするのが短期的な課題か、中長期的な課題かを峻別して分析することが有用である。最新のセキュリティ技術に関する知見に基づく理論的な警告には、中長期的な課題に位置付けられるものが多い。例えば、暗号技術の脆弱性や生体認証に対する攻撃法には、「中長期的な課題」に含まれるものが多いだろう。

これに対し、短期的な課題としては、金融機関の実務に利用されているシステムのセキュリティの実態に関するものが多い。金融機関の実務の中には、か

[8] 田村・宇根[2007]

つてセキュリティに対する意識があまり高くなかった時代に導入されたシステムがそのまま残ってしまっていることがある。磁気ストライプカードと 4 桁暗証番号による預金引出、ID とパスワードだけのオンライン・バンキング、カード番号と氏名を SSL 入力するだけのクレジットカード取引等、今日的な情報セキュリティの水準を満たさないシステムが、広く普及してしまっている。かといって、これらを全て再構築するわけにもいかない。さしあたり、リテール・バンキングのセキュリティを維持するためには、こうした短期的な課題について、運用面も含めた対策により、不正取引の防止に努め、もし不正取引が発生してしまったら、その被害を限定することに努めていくしかない。

しかし、こうした古いシステムは、時代の流れとともに、いずれは新しいシステムに置き換えられていくはずである。次世代のシステムに移行したときに、そのシステムのセキュリティのレベルが低いままとなってしまうことは、是非避けなければならない。この観点からは、短期的な課題に対処しつつ、次世代のシステムのセキュリティについて、中長期的な課題についても検討していかなければならない。

偽造キャッシュカード問題についてみると、現在の段階では、偽造による不正預金引出のリスクが相対的に高い磁気ストライプカードと 4 桁暗証番号が主流であるから、そのセキュリティのレベルがどの程度であっても、IC カードや生体認証を導入しさえすれば、セキュリティは改善するといえる。IC カードや生体認証の中にも、耐偽造性やなりすまし攻撃への対策が進んでいるものとそうでないものがあるが、その中からどれを選んだとしても、さしあたっては、現在の磁気ストライプよりは安全だからである。しかし、だからといって、中長期的な課題を無視することは適当ではない。もしもセキュリティに問題のある IC カードや生体認証の実装技術を選択してしまった場合、新旧の技術が共存する期間が過ぎて次世代の技術が主流となったときに、問題点が顕現化してしまう。このため、少なくとも導入時点で既知となっている脆弱性を持つ技術を導入することは推奨できない。特に、金融業界が一斉にある新技術を導入する場合においては、将来を見据えた選択が可能となるように、セキュリティにかかる十分な検討を行っておく必要があるだろう。

情報セキュリティ対策というのは、過去に発生した問題について後追い的に対応するだけでは駄目で、ある程度先を読んだ上で検討していくことがどうしても必要になる。世間の常識と同じレベルのことをやっていたのでは、対応が遅いと言われてしまうし、問題が生じてから対策を講じるまでのタイムラグを考えても、ある程度、将来発生する問題を予測しながら対策を講じていくことが必要となる。そのような予測を的確に行うためには、アカデミックな最新の研究成果を意識し、その情報を活用していくことが重要であろう。

参考文献

金融庁、『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

――、『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』、（http://www.fsa.go.jp/news/18/ginkou/20070301-1.html）、2007 年

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、「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.html)、2005 年 6 月

鈴木雅貴・神田雅透「IC カードに利用される暗号アルゴリズムの安全性について ―EMV 仕様の実装上の問題点を中心に―」、日本銀行金融研究所ディスカッション・ペーパー・シリーズ、DPS 2007-J-8、日本銀行金融研究所、2007 年

全国銀行協会、『「偽造キャッシュカード対策に関する申し合わせ」について』、（http://www.zenginkyo.or.jp/news/17/news170125.html）、2005 年

田村裕子・宇根正志、「IC カードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」、日本銀行金融研究所ディスカッション・ペーパー・シリーズ、DPS 2007-J-9、日本銀行金融研究所、2007 年

田村裕子・廣川勝久、「リテール・バンキング・システムの IC カード対応に関する現状とその課題」、日本銀行金融研究所ディスカッション・ペーパー・シリーズ、DPS 2007-J-10、日本銀行金融研究所、2007 年