偽造カード問題は預金取引の位置付けの再考を迫る

預金者への被害補償を前提とした、犯罪防止対策とは何か

日本銀行　金融研究所
情報技術研究センター長
岩下　直行

日本銀行金融研究所は、金融業界が情報化社会において直面しているさまざまな課題に適切に対処していくことをサポートするため、〇五年四月一日付で「情報技術研究センター（ＣＩＴＥＳ・サイテックス）」を設立した（http://www.imes.boj.or.jp/citecs/）。本センターでは、金融サービスの発展や金融システムの安定確保を図っていく上で重要性が一層高まってきている情報技術の基盤構築に研究面から貢献していきたいと考えている。本稿では、金融ネットワークへの信頼性を維持するために金融機関が直面している課題を整理する。

偽造カード問題のインパクト

揺らぐ情報セキュリティへの信頼

偽造キャッシュカードによる不正な預金引出事件は、銀行が長年培ってきた情報システムのセキュリティ対策に対する信頼を大きく損なうものであった。偽造キャッシュカード問題は昨年急増したとはいえ、年間被害額で数億円のオーダーであり（別図）、過去に発生したクレジットカードやプリペイドカードの偽造犯罪の被害総額が数百億円に達していたのと比べて、とくに規模が大きいものとはいえない。

しかし、過去のカード偽造事件では、主としてカード発行者、システム運営者が損失を被ったのに対し、偽造キャッシュカード事件では、不正に預金が引き出された預金者個人に損失が発生し、被害が補償されなかった。このため、預金者のだれもが被害者になりうると受け止められ、人々の不安が高まり、社会問題化してしまった。

最大で一日当り数百万円もの預金引出しを可能とする認証手段として、磁気ストライプ方式のキャッシュカードと四ケタの暗証番号では強度が十分ではないという問題は、金融業界内でも以前からある程度は認識されていた。全国銀行協会は、八八年にＩＣカードの業界標準を制定し、その後の技術進歩に合わせて累次の改訂を行うなど、新技術の導入の準備を進めていた。しかし、実際には、① 過去三〇年間、磁気ストライプカードと暗証番号という技術が大きな問題もなく利用され続けてきたため、ＩＣカードなどの新しい技術に移行するきっかけがつかめなかったこと、② 従来の技術が金融業界全体の基本インフラとして利用されてきたため、業界内の幅広い合意がなければ新しい技術への移行がむずかしかったこと、等から、ＩＣ

カードや生体認証などの新技術の導入にかかる意思決定が先送りされてしまった。

今回、偽造キャッシュカード事件が社会問題化したことから、金融業界にとって、新技術の導入が急務となっている。しかし、こうした形で新技術の導入を急がざるをえないという事態は、金融業界にとってけっして望ましいことではない。短期間で結論を出さなければならないため、新技術に関する十分な評価ができない、技術の選択を誤り将来に禍根を残す、といったリスクが大きくなるからである。

だれを守るための対策か

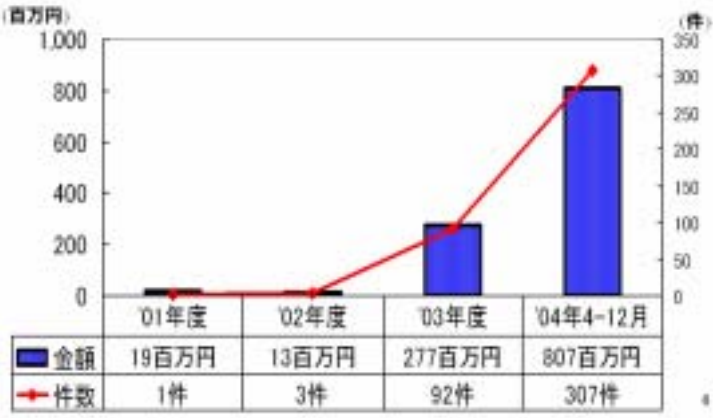
現在検討されている偽造カード対策は、主として「カード偽造団から預金者を守る」ことを目的に検討が進んでいる。①スキミングによる偽造被害を受けにくくするためにＩＣカード化する、②暗証番号を盗用されただけでは不正引出しができないように生体認証技術を組み合わせる、③一日の引出限度額を預金者の利便性を損なわない範囲内で引き下げられるように任意に設定できるシステムとする、といった対策である。しかし、各種アンケート調査をみる限り、預金者が実際に求めていたのは「銀行が被害を全面的に補償する」という対策であった。こうした声を背景に、金融業界は偽造カード被害を原則として補償するとの方針を表明し、そのための約款の改訂作業が進められていることが報じられている。

銀行が偽造カード被害を全面的に補償すれば預金者は守られるため、「預金者のため」にセキュリティ対策を導入する必要性は低下する。その結果、カード情報や暗証番号の管理にはむしろ無関心になるおそれがあり、結果として被害が発生すれば、銀行の負担が増加することになる。また、犯罪者が「自ら偽造カードで引き出して被害者に成りすます」ことにより、銀行から補償金を詐欺しようとする犯罪（「被害者成りすまし詐欺」）が発生するおそれもある。これまでそのような詐欺の発生が抑えられてきたのは、特別な理由がない限り、銀行が被害者への補償を行ってこなかったためと考えられる。

「被害者成りすまし詐欺」が実際に発生するかどうかは、改訂された約款が実務で利用されるようになってみないとわからないが、一つだけいえるのは、かりにそのような詐欺が発生した場合、銀行はそれを見破ることが非常にむずかしいということである。善良な預金者が被害者となった偽造カード事件が発生している状況下では、被害者の訴えを疑ってかかるような対応はできないし、かりに疑わしい部分があっても、銀行が確認できる範囲は限られている。

過去に発生したプリペイドカード、クレジットカードの偽造犯罪が組織的に行われてきたことを考えると、カードの偽造担当、不正引出担当、被害者役担当などの役割を分担した組織的な犯罪を警戒する必要があり、偽造カード対策は、「カード偽造団から銀行を守る」という視点で考えることも重要と考えられる。銀行は、預金者の啓発活動に力を入れるほか、自らが詐欺犯罪の被害者にならないために、カード偽造犯罪が発生しにくいような対策、かりに発生しても犯罪の手口が特定できるとともに、被害金額も限定できるような対策を講じていく必要があるだろう。

全国銀行協会「いわゆる偽造キャッシュカードによる預金等引出し」に関するアンケート結果



	'01年度	'02年度	'03年度	'04年4-12月
金額	19百万円	13百万円	277百万円	807百万円
件数	1件	3件	92件	307件

資料：全国銀行協会

偽造カード対策の有効性の検討

預金引出限度額の引下げ

それでは、具体的にどのような対策が有効なのか。短期的、中・長期的な対応策に分けて考えてみよう。

預金引出限度額の引下げは、実際問題として、短期的にとりうるほとんど唯一の対応策である。預金者の利便性とのトレードオフが存在するものの、窓口時間外における多額の預金引出ニーズが実際にどの程度あるのかを見極めて、リスクと比較考量のうえ、適切な水準に設定する必要がある。

この場合、利用者に限度額を自由に選択させることは有効であろうか。「不安に思っているお客様が限度額引下げを選択できる」という考え方であるが、「偽造カードによる被害は原則金融機関が補償する」という約款を前提とすれば、預金者はあえて限度額を引き下げて自らが不便となる変更を行わない可能性が高い。むしろ、「被害者成りすまし詐欺」をたくらむ犯罪者は、あえて限度額を引き上げ、大金の被害に遭ったと訴える可能性がある。

「カード偽造団から銀行を守る」という観点からは、少なくとも希望者が過度に高額に設定変更をできるようにすることは適当ではない。もしも、個人事業主等が高額の引出限度額を求める場合には、セキュリティ対策や補償の条件が一般預金者と異なる預金サービスを、別途手数料をとって提供することが必要ではないだろうか。

加えて、一日の限度額の設定で十分なのか、という問題も存在する。被害金額の上限が「一日の引出限度額×発覚までの日数」となることを考えると、被害者が預金が引き出されていることに長期間気づかなければ被害額が拡大してしまう。このため、たとえば、一定期間の累積引出額がＡＴＭ取引から窓口取引に誘導するという対応が考えられるかもしれない。

また、日本では取引内容が預金通帳に記帳され、アメリカのように、定期的に預金者に取引内容を記載したステートメントを送る仕組みにはなっていないが、長期間記帳をしていない預金者については、ＡＴＭでの預金引出しを制限して窓口取引に誘導したり、記帳を促したりすることも一案であろう。

損害保険への加入

偽造カードによる損害を補填するための短期的対策として、銀行もクレジットカードと同様に損害保険に加入すればよいという声もあるが、それは実際にはむずかしいと思われる。一般に、クレジットカードは、利用者を審査し、利用可能限度額を最初は低く設定しておいて、利用者の信用が上がれば徐々に与信限度額を引き上げる仕組みで運用されている。クレジットカードが不正利用された場合の一人当りの損害金額には上限があるので、保険会社は、発生しうる損害の上限値を計算したうえで、保険を引き受けることができるのである。

ところが、現在のキャッシュカードでは、預金者の信用とは無関係に一日当り数百万円の高額の引出限度額が設定されている。数日間連続して引き出すことにより、限度額に数倍する現金を引き出すことも可能である。このような構造のまま、偽造カードによる被害を原則として銀行が無制限に補償することにすると、偽造カード犯罪が多発した場合、銀行が支払わなければならない金額がきわめて多額となり、損害が拡大する可能性がある。保険会社は、そのような高いリスクを全額カバーする保険商品を扱うことはできないであろう。実際、盗難カード保険や偽造カード保険がついている預金サービスも存在するが、それらはいずれも保険金支払の上限額として数十万～数百万円が設定されており、損害を全額カバーするものにはなっていない。

したがって、カードが偽造され、不正に預金が引き出されること

があり うるという前提に立ち、その被害をすべて補償する前提で損害保険による対応を図るためには、たとえば、クレジットカードのように保険に見合う手数料をとったうえで、一定期間の利用限度額を設けるなど、発生しうる被害に上限を設けるような商品設計が必要となるのではないだろうか。

ICカードへの変更

中・長期的な対応策として、現在の磁気ストライプカードをICカードに変更していくことは、明らかにカード偽造の防止に有効である。問題は、ICカードだけでは利便性が低いため、当面は磁気ストライプとのハイブリッド・カードとせざるをえないことにある。一部の銀行では、利便性が低下することを説明したうえで、磁気ストライプなしのカードを発行している例もある。しかし、ほとんどの銀行は、対応ATMがまだ十分に設置されていないこと、提携先である他行ATM、コンビニATM、デビットカード等での利用を可能とすること等の目的で、ハイブリッド・カードを発行している。ところが、カードの磁気ストライプに情報が記録されている限り、預金者がスキミングの被害に遭うことや、「被害者成りすまし詐欺」犯罪のリスクを防げない。磁気ストライプ部分だけコピーした偽造カードも、ATMで使うことができるからである。

したがって、ICカードの「偽造に強い」という効果が発揮されるためには、すべてのカードがICカード化され、すべてのATMがICカード対応となり、磁気を前提とするすべてのサービスが提供されなくなる必要がある。しかし、すでに三億枚も発行されている磁気カードを全廃するためには、相当な期間が必要であり、ただちにそれを実現することはできない。また、銀行が偽造カードによる被害を補償することを前提とすれば、利用者があえてコストと手間ひまをかけてICカードに切り替えるインセンティブは強くはない。普及率を引き上げるためには、クレジットカードのように、カード保有者の意思にかかわらず、ICカードに変更することが必要になろう。その場合の費用分担をどうするかも重要な論点である。

また、ICカードそのもののセキュリティについてもさまざまな問題が指摘されている。すでに、海外では、銀行の発行したICカードが偽造された事例もある。銀行は、ICカードの耐タンパー性の評価方法や、サイドチャネル・アタックと呼ばれる攻撃法への対策についても、知見を深めておく必要があるだろう。

暗証番号の漏洩防止策

最近発生した偽造カード事件では、ゴルフ場のロッカーに利用した暗証番号が、銀行取引の暗証番号と同一であったことなどが悪用され、不正に預金が引き出される被害が発生している。このような、銀行システム以外での漏洩については、銀行としてはシステム上の対応はできないので、預金者への啓発を続けていく必要があるが、もしも漏洩が預金者の故意や重大な過失によるものであれば、補償においてその事情を考慮することが必要になる。

しかし、そのような対応を進めていくにあたっては、万が一にも、銀行システムの内部から暗証番号が漏洩することを避けなければならない。マスコミでは、ATMと銀行センターとの通信を盗聴して暗証番号を不正に入手しているのではないかとの疑いが報道されることもあるが、これまでのところ、通信事業者の内部者がかかわった数少ない犯罪事例を除けば、そのような形態での漏洩は確認されていない。とはいえ、少なくとも「銀行からは漏洩してない」といいきることができるためには、暗証番号の生成から廃棄まで、水も漏らさぬ機密保護が必要とされる。

具体的には、預金口座開設申込書への暗証番号の書込みの回避から、ATMの通信回線の暗号化まで、すべての局面で、暗証番号の機密をどう守るかについて、現在の業務内容をチェックする必要がある。その際、暗証番号の取扱いに関するISO／TC68（国際標準化機構・金融専門委員会）の国際標準であるISO9564が参考になるものと考えられる。

この国際標準は、銀行カードとともに利用される暗証番号について、その設定、保管、入力、送信等に関する一般的なルールをとりきめたもので、たとえば、暗証番号は四ケタ以上というルールもこの標準で定められている。

この国際標準では、たとえば、暗証番号はその生成から廃棄まで、常に物理的に安全な環境で保管することが求められており、かりにそれ以外の環境で利用される場合、あらかじめ定められた暗号アルゴリズムで暗号化することが求められている。暗号化にあたっては、適切なパディング（暗号化するデータにランダムな情報を付加すること）を行い、同一の暗証番号でも同一の暗号文にならないようにすること、暗号化方式を明らかにしないことによってではなく、暗号カギの秘匿によってその機密性を守ること等が規定されている。

欧米の金融機関のＡＴＭで利用される暗証番号は、原則、この国際標準に準拠してセキュリティが確保されている。わが国でも、こうした国際標準をふまえたシステム対応が必要になってこよう。

生体認証技術の採用

生体認証技術とは、指紋、虹彩、血管パターン等の個人特有の生体情報を利用して個人を自動的に認証する技術であり、最近、幅広い分野で採用されつつある。金融業界でも、この技術を、ＡＴＭにおける預金者の本人確認手段として採用する動きが出始めている。暗証番号による本人確認では不十分との判断から、ＩＣカードと生体認証を組み合わせた方式が、よりセキュリティの高い本人確認手段として注目されている。

確かに、生体認証技術を暗証番号、ＩＣカードと組み合わせて利用すれば、本人確認方式のセキュリティは格段に向上する。とくに、ＩＣカードが普及し、偽造が困難になった場合でも、ＩＣカードを盗用することは可能であるため、ＩＣカードだけでは、盗難カードを用いて他人が不正に預金を引き出すことを有効に防止できない。この点、生体認証を利用すれば、盗難カードを用いても他人が預金を不正に引き出すことはむずかしくなる。同様に、「被害者成りすまし詐欺」についても、実行がむずかしくなることが期待できる。

しかし、生体認証技術は、技術としての成熟度がまだ十分とはいえない状態にある点に注意が必要である。とくに、偽造された生体情報を誤って受け入れてしまうという脆弱性を示唆する研究成果が発表されており、その評価や対策に関する十分な検討が必要となってきている。拙速を避け、セキュリティ評価を適切に実施し続けることが必要と考えられる。

前記の対策以外にも、たとえば、携帯電話で預金引出機能のロック・解除を可能とするとか、預金引出可能ＡＴＭを指定するとか、暗証番号を四ケタよりも長くするとか、英字を可能にする等のセキュリティ改善策が提案され、一部は利用され始めている。これらはそれなりに対策として有効と考えられるが、付加的なセキュリティ対策にすぎず、すべての預金者のセキュリティを向上させることはできない。したがって、これらはあくまでも補助的なものと考えるべきであろう。

金融ネットワーク・インフラの再構築

より本質的なセキュリティ対策として、金融業界が利用しているネットワーク・インフラを、今日的なセキュリティ対策を織り込んで再構築していくことが考えられる。たんにカードをＩＣカード化し、カード保有者の本人確認手段を高度化しただけでは、将来予想される高度な攻撃に耐えられないおそれがあるからである。

金融業界として、決済システム全体のセキュリティ向上を図るためには、たとえば、ＩＣカードや生体認証を用いて生成した情報を、通信ネットワーク・インフラを通じてＡＴＭと金融機関センターとの間で送受信する仕組みを構築していくことが考えられる。こうした取組みについては、たとえば、欧米の金融業界では、ＩＳＯ／ＴＣ68 の国際標準である、ＩＳＯ８５８３（銀行カード用通信メッセージ）の改訂作業において検討されている。

わが国においても、金融機関向け通信ネットワーク・インフラの世代交代のタイミングをはかって、こうしたコンセプトを金融機関間で共有していくことが重要ではないだろうか。

銀行経営への影響

預金業務の位置付けの再考を

偽造カードによる被害を減らすための正攻法は、コストをかけて高度なセキュリティ対策を導入していくことである。しかし、現在の預金取引の銀行ビジネス上の位置付けを考えると、セキュリティ対策にはコストをかけず、損害の補償で対応するという道を模索する銀行が出てきても不思議ではない。

ただし、そのような選択肢をとった場合、偽造カード犯罪の展開によっては、銀行経営上の問題が生ずる可能性がある。預金取引は、クレジットカードのように、預金額や送金額に比例した手数料を徴収するビジネスモデルになっていないため、偽造カード犯罪が拡大した場合、取引金額に応じて一定の比率で発生すると考えられる損害を無制限に補償し続けることはビジネス的に困難だからである。

銀行が偽造カード被害を全額補償することを前提とすれば、銀行のリスク管理の観点からは、現在のような預金業務のビジネスモデルは維持できない。利用者の不適切な運用による被害を補填したり、「被害者成りすまし詐欺」の被害に遭って銀行が大きな損失を被るおそれがある。

そうした事態を防止するためには、預金サービスを「だれもが安価に利用できるサービス」との位置付けから、より戦略的な、利益追求型のビジネスに変えていくことが必要である。従来から、都銀等の「家計のメインバンク化」戦略に代表されるように、各銀行は預金業務を収益増につなげるべく、さまざまな工夫を重ねてきた。偽造カード問題がより深刻化した場合、これに対処していくためには、そのような方向での業務改革を加速することが必要である。

その場合、たとえば、預金者を「個人ローン、クレジットカード取引を含めた対個人取引のターゲット」と位置付けたうえで、取引開始時に厳格な本人確認と審査を行うとか、最初はＡＴＭの利用限度額を低く抑えるといった、米国型のビジネスモデルに変えていくことが必要になろう。

金融機関は、かつて、規制金利下において巨額のフランチャイズ・ベネフィットが存在したことから、預金業務をいわばライフライン的なサービスとして提供してきた。かつて、日本が貯蓄不足であったころに、厳しい店舗規制や他業禁止による消費者向けサービスの制限の下におかれたなかで形作られたそうした構造が、ここにきて金融機関の手足をしばっているように思われる。偽造カード問題は、休眠口座の扱いや、口座維持手数料の徴求など、銀行経営における預金取引の位置付けの再考を迫るものでもある。

「インターネットにコミットした」業界

偽造キャッシュカード問題と並んで、銀行が提供しているインターネット・バンキングへの攻撃を巡る話題も、最近、マスコミでさかんに報じられている。大手銀行の名前を騙ったフィッシング詐欺メールや、インターネット・カフェのパソコンに仕掛けられたキー・ロガーを用いて、インターネット・バンキングのログインＩＤやパスワードを盗み出そうという試み等である。インターネット・バンキングを提供するウェブ・ページのプログラム（ウェブアプリケーション）に攻撃を受けやすい問題点があるという指摘が聞かれることも少なくない。こうした問題についても、金融業界としての正確な認識と対応が必要となっている。しかし、こうしたインターネット・バンキングのセキュリティを巡る問題は、なぜか、「銀行の提供する情報システムの脆弱性」と位置付けられないで論じられることが多いように思われる。

インターネットを通じた取引が急速に拡大した現在においても、銀行にとって、インターネットがどの程度大切なインフラなのかにつ

いて、コンセンサスが得られているとはいえない。銀行の情報システムの基幹ともいうべき勘定系システムは、インターネット技術ではなくレガシー技術で動いている。レガシー技術に基づいて提供された情報システムは、そのネットワーク全体が銀行に管理されているので、万一障害が発生して機能しなくなれば、これを解消する義務は銀行側にある。しかし、インターネットで接続している場合、ネットワークが接続している先は顧客が管理する領域であり、どのようなシステム構成になっているかわからないから、障害が発生しても、その原因の特定や責任の切り分けがむずかしい。

同様の議論は、社会の重要インフラにおける情報セキュリティ対策を検討するプロセスでよくみられる。重要インフラとされる業種のうち、たとえば電力、運輸、ガスなどは、その基幹システム(制御系)がクローズド(閉鎖的、自己完結的)なシステムであるため、かりに、インターネットを経由して攻撃を受けても、基幹システムに問題は生じにくいとされることが多い。

しかし、金融業界における顧客とのインターフェース部分には、インターネット技術が広く利用されており、この部分については、新たな脆弱性対策が必要とされている。顧客の指示に基づき資金の授受を行うというのが銀行の業務の基本である以上、かりに、そこに障害があれば、業務全体が滞ることになるし、万一、インターフェース部分で不正な取引が実施されてしまうと、その取引を引き継ぐシステムが正常でも全体としては正しくない処理をしてしまうことになる。こう考えると、金融業界は、電力、運輸、ガスといった他の重要インフラ業種と比べて、インターネットの脆弱性の影響をより深刻に受けるという意味で、「インターネットにコミットしてしまった業界」ということができるだろう。

そのような観点からは、金融業界にとって、インターネットのセキュリティ問題の影響は、少なくとも他の重要インフラ業種よりはるかに切実であり、早急な取組みが必要である。具体的には、銀行の情報システムの脆弱性を検知し、その情報を金融業界内で共有していく仕組みが必要とされているといえよう。

既存技術の脆弱性を点検する体制整備を

以上述べてきたように、現在、金融業界は、新手の金融ハイテク犯罪が増加するなか、セキュリティ対策として新技術の導入の必要性が高まっている。とくに、偽造キャッシュカード問題については、社会問題化してしまったことから、新技術の導入が急務となっている。技術革新が進んでいる今日、金融業界は今後、自らの判断で、将来発生しうる脅威を想定して、既存の技術の脆弱性を評価し、十分なセキュリティ・マージンとリード・タイムを確保したうえで、戦略的に新しい技術に移行していくというのが望ましい。

金融業界は、情報システムに巨額の投資をしているが、技術革新が進めば、既存の技術が陳腐化していくのは道理である。磁気ストライプカードの仕様が三〇年間維持されてきたということ自体、例外的な現象であって、業界内で利用するインフラ技術は、定期的に更改を行っていかなければならない宿命にあるといえる。

今回の偽造キャッシュカード問題をきっかけとして、今後、銀行の情報システムの脆弱性を正確かつタイムリーに検知し、その是正に戦略的に対応していくための体制を構築していくことが望ましい。そのための議論を始めるべき時期ではないだろうか。

(文中、意見にわたる部分は筆者の個人的見解である)

いわした　なおゆき
８４年慶大経済学部卒、日本銀行入行。調査統計局、企画局、システム情報局を経て、９４年より金融研究所にて金融分野に利用される情報セキュリティ技術の研究に従事。ＩＳＯ／ＴＣ６８日本事務局として金融技術の国際標準化を担当。金融庁偽造カード問題スタディ・グループにオブザーバーとして参加。