ジュリスト 1308 号（3 月 15 日号）寄稿

偽造・盗難カード預貯金者保護法と金融機関のセキュリティ対策

日本銀行 金融研究所 情報技術研究センター長　岩下 直行

１．金融機関のセキュリティに対する利用者の不安の高まり

金融業界は、コンピュータによるネットワーク・システムを最も早い時期に整備した業種のひとつであった。1970 年代に開発が進められた第二次オンライン・システムは、金融機関内部の事務を飛躍的に合理化し、現在の金融機関による決済サービスの原型を形作った。現在利用されているキャッシュカードの磁気ストライプの形状や、CD/ATM の基本構造は、この第二次オンライン以来、30 年間以上にわたって維持されてきたものである。1990 年代にインターネットが普及する前は、コンピュータ・ネットワークといえば真っ先に金融機関のオンライン・システムが挙げられる存在であり、その頑健性、安全性に疑いが差しはさまれることはほとんどなかった。金融機関は、頑丈な建物や金庫によって守られるその物理的なセキュリティと同様に、情報システムのセキュリティについても、十分な安全性が確保されていると信じられてきた。

しかし、2003 年から 2004 年にかけて、偽造キャッシュカードによって不正に預金が引出される事件が急増し、大きな社会問題となった。その後も、ATM に仕掛けられた隠しカメラ、金融機関の名を騙って送りつけられるスパイ・ウエア入りの偽装 CD-ROM、無差別にばら撒かれるフィッシング詐欺メールなど、金融機関とその利用者を脅かす新手の金融ハイテク犯罪の手口が次々に出現している。こうした犯罪により利用者が実害を被る事例も相次いでいる。こうした中で、預貯金者保護法が施行され、偽造・盗難キャッシュカード被害における金融機関の責任範囲が規定されることとなった。金融機関は、この新しいルールの下で、より安全性の高いシステムを構築していくことによって、利用者の信頼を取り戻すという課題に挑戦していかなければならない。

本稿では、金融分野で利用される情報セキュリティ技術を研究する立場から、偽造・盗難キャッシュカード問題の現状と対策について考えてみたい。

２．偽造キャッシュカード問題の現状評価

偽造キャッシュカードによる不正な預金引出の急増は、金融機関が長年培ってきた業務面の信頼を大きく損なうものであった。とはいえ、これまでに判明している偽造キャッシュカードの累計被害額は十数億円である。偽造クレジットカードの被害額が年間百億円近くに達していることや、過去に発生した何種類かのプリペイドカードの偽造犯罪の被害額が、各々数

百億円に及ぶと推定されているのに対して、偽造キャッシュカードの被害は、特に規模の大きいものとはいえない。しかし、クレジットカードやプリペイドカードの偽造事件では、主としてカード発行業者、システム運営者が損失を被り、消費者に被害が及ばなかったのに対し、偽造キャッシュカード事件では、不正に預金が引出された預金者個人にまず損失が発生し、金融機関による被害補償も後手に回ってしまった。このため、預金者であれば誰もが被害者になり得ると受け止められ、一般の人々も不安をつのらせることとなった。

そもそも、１日当たり数百万円もの預金引出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４桁の暗証番号ではセキュリティの強度が十分でないということは、以前から指摘されてきた。1999 年 11 月に日本銀行で開催された第２回情報セキュリティ・シンポジウムでは、金融機関のキャッシュカードと暗証番号による認証方式の見直しの必要性について、次のように指摘されている。

> 「(a)様々な技術革新によって印鑑、印影、各種印刷物、磁気カード等の偽造が容易になっていること、(b)暗証番号の盗用や推定が巧妙に行われるようになっていること、(c)金融機関側も、店舗の人員削減等により、従来ほどのセキュリティ対策への配慮が期待できないおそれがあること、等を考えると、…既存の金融取引で利用される認証方式についても、磁気カードよりも安全性の高い IC カードの採用や、暗証番号に加えてバイオメトリック認証を導入するといった選択肢について、検討のスコープを広げていくべきであろう。」[i]

金融業界でも、こうした問題が存在することは以前からある程度は認識されていた。全国銀行協会は、1988 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 30 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難しかったこと、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、金融機関の情報セキュリティに対する利用者の信頼を大きく損なう結果を招いてしまった。

偽造キャッシュカードが社会問題化してしまい、預貯金者保護法が制定されたことを受けて、金融業界は、被害の補償を表明するとともに、ATM の引出限度額を引き下げるなど、被害を限定する対策を講じている。しかし、犯罪の未然防止のためのセキュリティ対策は十分とはいえない。金融機関では、IC カード化と生体認証の導入が進められてはいるものの、実際に対策を実施した先は限られており、実施した先についても、普及率はあまり高くはない。しかも、IC カード化については、預金者の利便性を維持するために、磁気ストライプ方式との併用とする先がほとんどである。この結果、金融機関における預金引出においては、磁気ストライプ方式と４桁の暗証番号による個人認証が引き続き主流を占めており、現時点でも、カード偽造犯罪の根は絶たれていないのが実情である。

３．カード犯罪の手口の変遷

カード犯罪の手口は、近年急速に高度化している。20 世紀までは、カード犯罪の主流はカードの盗用であった。暗証番号の入手方法も、かつては、「被害者と面識があり暗証番号を知っていた」、「被害者から直接聞き出した」といった素朴な手口が主流であった。暗証番号を推定した事例についても、被害者が暗証番号として生年月日や電話番号等の個人情報から容易に連想できる番号を設定しているケースにおいて、犯人がカードと一緒に入手した身分証明書等から暗証番号を推定するといった古典的な手口が多かった。

しかし、21 世紀に入ると様相が一変する。まず、カードの盗用に代わって、カードの偽造が主流となった。カード偽造に用いられる機器が安価に入手可能となるとともに、カードの磁気ストライプ情報だけを一瞬で読み取る「スキミング」と呼ばれる手口が普及したからである。カードを盗まれるのとは異なり、スキミングされた後でカードが戻された場合、被害者は偽造カードが作製されていることに気づかないため、攻撃者は不正預金引出のタイミングを自由に選ぶことができ、大きな被害が発生するようになった。

暗証番号の入手方法については、ATM での入力の動作を覗き見するといった能動的な手口が増えたほか、より巧妙な手口が利用されるようになった。例えば、あるゴルフ場では、４桁の暗証番号を入力するタイプの貴重品ロッカーにキャッシュカードを保管させ、当該ロッカーの管理者が入力された暗証番号をシステムで強制的に表示させてカードと暗証番号を入手し、スキミングにより偽造カードを作製した上でカードを戻しておくという手口で、大量の預金が不正に引出された。多くの利用者が、ATM の暗証番号と同じ数字を貴重品ロッカーでも使用していたために、暗証番号まで漏洩してしまったのである。

カード偽造のための情報獲得の手口としては、カードや ATM 取引とは無関係に入手した預金口座番号等の個人情報を利用するという手口も知られている。特に、預金口座番号と預金者の生年月日や電話番号といった個人情報を大量に入手して、その情報を元に偽造カードを作製し、生年月日等から暗証番号を推定して試行するという手口で不正に預金を引出した事件が知られている。なお、キャッシュカードの真偽チェックのために、カード表面の刻印にはない秘密コード[ii]を磁気ストライプの特定フィールドに記録する仕組みを採用している金融機関の場合は、この手口でのカード偽造を免れることができたようである。

更に巧妙な方法として、金融機関の ATM に隠しカメラを設置して、カードの表面と暗証番号の入力動作を盗撮し、そこで得た情報を元に偽造カードを作製して不正に預金を引出すという手口が現れ、実際の被害が生じている。この手口を用いれば、カードの表面に刻印された預金口座番号が入手できるが、金融機関によっては、その情報だけでキャッシュカードが偽造できてしまうことがあるため、被害に繋がったものである。この手口についても、秘密コードを磁気ストライプに記録している金融機関は、カード偽造を免れることができたものと思われる。

これらとはやや系列が異なる手口としては、金融機関の通信を盗聴することによって、通

信内容からカードの磁気ストライプ情報や暗証番号を入手し、偽造カードを作製するという方法が存在する。かなり古い事件ではあるが、この手口を用いて実際に偽造カードが作製され、預金の不正引出が行われた事例が知られている。この手口を予防するためには、ATM と金融機関との間の情報通信を適切に暗号化することによって情報漏洩を防止することが有効である。

偽造・盗難キャッシュカード犯罪の主な犯行手口とその対策

主な犯行手口		具体的な事例	当面有効なセキュリティ対策			
キャッシュカードの入手	暗証番号の入手		金融機関側		預金者側	
			キャッシュカード	暗証番号	キャッシュカード	暗証番号
カードを盗用	生年月日等の個人情報から推定／ATM での暗証番号入力を覗き見	過去に実害が生じた事例多数	―	生体認証、ATM での覗き見防止対策	カードの盗難対策	暗証番号の適正化／ATM での覗き見への警戒
スキミングによる偽造	生年月日等の個人情報から推定／ATM での暗証番号入力を覗き見	過去に実害が生じた事例多数	IC カード化	生体認証、ATM での覗き見防止対策	スキミングの予防	暗証番号の適正化／ATM での覗き見への警戒
スキミングによる偽造	貴重品ロッカーの暗証番号から推定	2004 年から 2005 年にかけて、あるゴルフ場で継続的に大量のスキミングが行われた	IC カード化	生体認証	スキミングの予防	キャッシュカード用暗証番号を他の用途に利用しない
別途入手した預金口座番号等から偽造	生年月日等の個人情報から推定／ATM での暗証番号入力を覗き見	1998 年、ある企業から漏洩した個人情報を元にカードが偽造され、使用された	IC カード化、磁気カードへの秘密コード付与	生体認証、ATM での覗き見防止対策	預金口座番号の秘匿	暗証番号の適正化／ATM での覗き見への警戒
ATM に仕掛けた隠しカメラの映像から偽造	ATM に仕掛けた隠しカメラの映像から入手	2005 年から 2006 年にかけて、首都圏の複数の金融機関の ATM コーナーでの盗撮が発覚	隠しカメラの排除、IC カード化、磁気カードへの秘密コード付与	生体認証、隠しカメラの排除	―	―
盗聴した金融機関の ATM との通信内容から偽造	盗聴した金融機関の ATM との通信内容から入手	1982 年に、北海道において金融機関が利用する専用回線を盗聴して情報を入手し、カードを偽造・行使	IC カード化、通信暗号化	生体認証、通信暗号化	―	―

４．具体的なセキュリティ対策とその有効性

(1) IC カード化

カードの盗用以外の手口については、「IC カード化」によってキャッシュカードの偽造を防ぐことが有効である。問題は、IC カードだけでは利便性が低いため、当面は、「磁気ストライプ方式併用の IC カード」とせざるを得ないことにある。一部の金融機関では、利便性が低下することを説明した上で、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、

ほとんどの金融機関は、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、併用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、スキミング犯罪を未然に防止できない。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。

IC カードが偽造に強いという効果が発揮されるためには、全てのカードが IC カード化され、全ての ATM が IC カード対応となり、磁気を前提とする全てのサービスが提供されなくなる必要がある。しかし、既に３億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、直ちにそれを実現することはできない。また、預貯金者保護法により偽造カードによる被害が補償されることを前提とすれば、預金者があえてコストと手間隙を掛けて 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様々な問題が指摘されている。既に、海外では、金融機関の発行した IC カードが偽造された事件も発生している。当面は脆弱な磁気ストライプが残るために、喫緊のリスクとしては意識されないが、将来を考えると、金融機関は、IC カードを偽造したり、その内部情報を解析したりする攻撃への耐性についても、知見を深めておく必要がある。また、万一 IC カードが解析され、内部に格納された情報が漏洩したとしても、システム全体のセキュリティが損なわれないような設計にすることも大切である。

(2) 暗証番号の適正化

キャッシュカードの所持に加えて、暗証番号という情報によって本人であることを認証する現在の枠組みを維持するのであれば、生年月日等、類推されやすい暗証番号を使用している預金者に、別の暗証番号へと変更して貰う「暗証番号の適正化」が必要になる。これに付随して、「キャッシュカード用暗証番号を他の用途に利用しない」ことに関する注意喚起や、「ATM での暗証番号の覗き見への警戒」についての働きかけも必要となるが、何よりまず、類推され難い暗証番号が利用されることが大切である。

これまで、わが国の金融機関における暗証番号の設定においては、預金者が生年月日等の類推されやすい番号を使用していても、金融機関がこれを是正するよう働きかけてはこなかった。その結果、生年月日や電話番号といった類推されやすい暗証番号を使用している預金者は、無視できない比率で存在するものと考えられる[iii]。最近は、金融機関が暗証番号の適正化に関する注意喚起を様々な場で行うようになったが、長年利用してきた暗証番号を変えたくないという預金者や、覚えられないから紙に書いておくという預金者も存在するであろう。しかし、「暗証番号は厳格に取り扱い、頻繁に変更する」ことが常識として身についていなければ、暗証番号に基づく個人認証の安全性を担保することはできない。金融機関と預

金者の双方にとって、管理コストが高まることは避けられないが、粘り強く適正化を進めていくことが必要であろう。

預貯金者保護法の国会審議の過程で、「生年月日等の類推されやすい暗証番号を利用している預金者に対し、別の番号に変更するよう、複数回にわたる働きかけが行われること」が、当該預金者の過失を問う前提であるという議論があった。このような「働きかけ」をどのように行うかは、極めて重要な問題である。

既存の預金口座において、生年月日と同一の暗証番号が利用されていることを預金者に注意喚起をする場合に、電話や郵送等で個別に「あなたの暗証番号は生年月日と同一ですので変更して下さい」と連絡することは、暗証番号そのものを電話や郵送で伝えるのと同じ位、大きなリスクである。誰かがその情報を盗み聞きし、偽造カードを作製して不正に預金の引出を試みるかもしれない。万一、「暗証番号が生年月日と同一の預金者リスト」が漏洩すれば、「暗証番号付きの預金者リスト」が漏洩したのに匹敵する被害が生じかねないことを考えれば、そのリスクの大きさは明らかであろう。そのような連絡を行わなければならないという前提で考えるのであれば、「生年月日と同一」といった具体的な情報を明らかにすることなく、不適切であることのみを指摘する方が安全である。

また、当該預金口座については、不正使用のリスクを意識して、慎重に監視していくことが必要であろう。暗証番号が生年月日と同一であるとか、同一番号の連続であるような預金口座については、暗証番号によって本人と確認すること自体に大きなリスクがある。その変更を促す場合、通常の預金口座のように、現行の暗証番号により本人認証を行って暗証番号を変更させることで良いのか、という問題もある。攻撃者があえて問題のない暗証番号に変更して不正引出しを行うかもしれない。そのような預金口座については、カードと暗証番号のみならず、他の手段、例えば顔写真付き身分証明書等を提示させ、窓口で本人確認を行った上で暗証番号を変更させた方が安全であろう。

(3) 金融機関内部における暗証番号の取り扱いの厳格化

暗証番号の適正化と同時に、金融機関内部における暗証番号の取り扱いの厳格化を進めていくことも大切である。わが国では、預金口座開設手続において、手書きで暗証番号を申込書に書き込むことが珍しくない。預金者の間にも、相手が銀行員であれば、暗証番号を知られても問題ないという認識が根強いようである。しかし、それでは万一、暗証番号が漏洩し、銀行員自身が漏洩に荷担しているのではないか、という疑いを掛けられた場合、それに反論できない。本来、金融機関の預金業務においては、暗証番号は、システムで照合さえできれば良いのであって、銀行員が預金者の暗証番号を知っている必要はない。こうした観点からは、預金口座の開設手続時には、応対している銀行員にも見えない工夫をした上で、預金者の手元から暗証番号を入力させるようにすることが望ましい。

その際、暗証番号の取り扱いに関する ISO/TC68（国際標準化機構・金融専門委員会[iv]）の国際標準である ISO 9564 が参考になるものと考えられる。この国際標準は、銀行取引カードと

共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取り決めたものである。例えば、ISO 9564 の 7.3.3.2 節では、金融機関における口座開設時に暗証番号をどのように定めるかについての規定が書かれている。金融機関は、預金者に対して適切な暗証番号の選択にかかる注意事項（連続番号や特定の日付の排除等）を示した上で、暗証番号を預金者に選択させる。金融機関の職員が預金者が選択した暗証番号を閲覧することは禁じられているため、預金者が選択した暗証番号のその適正性を判断することは想定されていない。預金口座開設時に預金者に適正な暗証番号を選択させるためには、人間ではなく、システムが連続番号や生年月日、電話番号等を除外する対応が必要となる。

単に、金融機関内部での暗証番号に対する取り扱いを厳格化するだけではなくて、システム的にも、金融機関内部から預金者の暗証番号が漏洩することを防止する必要がある。少なくとも「金融機関からは漏洩してない」と言い切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なる。具体的には、預金口座開設申込書への暗証番号の書き込みの回避から、ATM の通信回線の暗号化まで、全ての局面で、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。ISO 9564 では、例えば、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、仮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。暗号化に当っては、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して長さを揃えること）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、暗号鍵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踏まえたシステム対応が必要になってこよう。

(4) 生体認証の利用

偽造対策としてキャッシュカードを IC カード化したとしても、真正なカードの盗用までは防止できない。カード盗用による成りすましを防ぐ観点からは、暗証番号よりも高度な本人確認手段である「生体認証」を導入することが考えられる。生体認証とは、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。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金融機関が増えつつある。暗証番号による本人確認に比べると、IC カード、生体認証、暗証番号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いうことができる。

ただし、生体認証にもいくつかの問題点がある。まず、金融機関相互の CD オンライン提携が普及している状況の下で、生体認証技術間の相互運用性、互換性の問題が指摘されている。また、膨大な導入コストや代替手段との比較において、預金取引に対する信頼を取り戻す手段として、生体認証による安全性を適切に評価する必要がある。現在、「生体認証は究極のセ

キュリティ対策」というイメージが先行している一方で、実際のシステムに実装した場合の運用面を含めたセキュリティを正確に評価することが困難という問題もある。

生体認証の安全性については、安価な材料で作製された人工指が、市販の指紋認証装置において高い受入率を示したとの報告もある。生体認証を安心して利用していくためには、生体認証による安全性を、正確に評価するための枠組み作りと、正しい理解が重要である。特に、生体認証を利用したシステムに固有の「身体的特徴の偽造による攻撃」に対する安全性評価と、その対策（例えば、生体検知機能[v]の導入）などを考えていく必要がある。

以上の対策について、どの段階まで対応することが適当か、実際に犯罪が発生するリスク、ビジネスとしての採算性、レピュテーション上の問題等を考慮して、各金融機関が立ち位置を定めていく必要がある。その場合、「望ましい対策のあり方」の基準をどこに求めるべきであろうか。各金融機関の置かれている状況はそれぞれ異なるので画一的な答えを提示することは難しい。相対的に金融機関をターゲットとしたハイテク犯罪の事例の多い海外の金融機関における取り組み事例や、金融機関のセキュリティ対策に関する国際標準を参考にしながら、各金融機関がそれぞれに必要十分と考える対策を具体化していく必要があるだろう。

(5) 利用者の協力

もうひとつの視点として、利用者の協力を得ることも重要なポイントである。セキュリティ対策は「足し算」ではなくて「掛け算」で効いてくるとよくいわれる。金融機関側が万全の対策を講じていても、利用者が不注意であれば被害が発生し得る。このため、セキュリティ対策には利用者の協力が不可欠となる。もし、利用者が「金融機関が補償してくれるから」というモラル・ハザード的な認識でいると、セキュリティ対策の効果はあまり期待できない。また、(1)セキュリティ・レベル、(2)利用者の管理負担（例えば、利用限度額の引き下げによる提供サービスの低下）、(3)システム構築コストには、トレードオフの関係があることを認識すべきである。金融機関がビジネスとして金融サービスを提供する以上、システム構築コストには限界があるのだから、利用者にも一定の管理負担を求めていかないと、必要なセキュリティ・レベルを確保できない。従って、預貯金者保護法の下で、利用者に適切な管理負担を担って貰えるようなルール作りが、今後の重要な論点となるだろう。

５．キャッシュカードのセキュリティ対策は誰を守るものか

以上述べてきたようなセキュリティ対策は、主として「カード偽造団から預金者を守る」ことを目的としている。しかし、預貯金者保護法により金融機関が偽造カード被害を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惧れがあり、結果として被害が発生すれば、金融機関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出して被害者に成りすます」ことにより、金融機関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」）が発生する惧れもある。

「被害者成りすまし詐欺」が実際に発生するかどうかはまだ分からないが、ひとつだけ言えるのは、仮にそのような詐欺が発生した場合、金融機関はそれを見破ることが非常に難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、被害者かもしれない顧客の訴えを疑ってかかるような対応は採りにくいし、仮に疑わしい部分があっても、金融機関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る。

このように考えると、偽造カード対策は、むしろ「カード偽造団から金融機関を守る」という視点で考えることも重要と考えられる。金融機関は、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、仮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。

（文中、意見にわたる部分は筆者の個人的見解である。）

---

[i] **松本勉・岩下直行、「金融業務と認証技術」、『金融研究』第 19 巻別冊１号、日本銀行金融研究所**

[ii] **こうした秘密コードによるキャッシュカードのセキュリティ強化については、金融情報システムセンター、「キャッシュカードシステムの課題と欧米金融機関の対応例」、『金融情報システム』No.278 の説明が詳しい。ただし、この対策はカード表面の刻印や預金口座番号からカードが偽造されることを防ぐことはできるが、秘密コードもろとも磁気ストライプ情報がスキミングされた場合には、偽造を防ぐことはできない。**

[iii] **1995 年にある週刊誌がキャッシュカードの暗証番号についてのアンケート調査を行ったところ、回答者 194 人中、自分の生年月日を利用しているという回答が 53 人、自宅の電話番号を利用しているという回答が 17 人で、全体の 36%が「類推されやすい暗証番号」を利用していた（週刊文春 1995 年 10 月 12 日号）。**

[iv] **ISO/TC68 国内委員会ホームページ**: www.imes.boj.or.jp/iso/

[v] **人体の電気特性、光学特性、生理的特性等を用いて、身体的特徴が生体によって提示されたか否かを確認する機能。（宇根正志・田村裕子、「生体認証における生体検知機能について」『金融研究』第 24 巻別冊第 2 号、日本銀行金融研究所）**