特集

金融機関における情報セキュリティの現状と課題

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. 金融機関は情報セキュリティを重視していかざるを得ない

偽造キャッシュカード問題の深刻化と預金者保護法の施行、インターネット・バンキングの普及と不正取引の増加、個人情報保護法の施行等に伴い、金融機関の情報セキュリティに関する世間の関心は近年とみに高まっている。金融機関の情報システムを舞台とした情報セキュリティ侵害事例が報道されるたびに、金融機関に対して厳しい目が向けられるようになった。今や、金融機関は、業務リスク管理の観点だけではなく、レピュテーション維持の観点からも、情報セキュリティを重視していかざるを得ない状況になっている。

現在、多くの金融機関が、インターネットのホームページに、自行の情報セキュリティが万全であることをアピールする説明文を掲載している。情報セキュリティの管理体制について、第三者機関から評価・認定を受ける金融機関も増えてきている[*1]。

今日では、金融機関が利用者にサービスを提供する際には、情報システムを活用することが不可欠となっている。そうした状況下において利用者からの信頼を維持するためには、無権限者による不正取引や個人情報漏洩が発生しないように情報セキュリティを適切に管理し、それを積極的にアピールしていくことが必要とされているのだ。

2. 安全対策から情報セキュリティへ

金融機関のシステム開発・運用の現場において「情報セキュリティ」というカタカナ語[*2]が普及したのは、比較的最近のことである。もちろん、それ以前から、金融機関にとって不正防止や個人情報保護が重要でなかった訳

＊1　わが国の金融機関における情報セキュリティ・マネジメント・システム（ISMS）の適合性評価制度による認証取得件数は、17件（07年４月時点）にのぼる。

＊2　「セキュリティ」という言葉は、国立国語研究所「外来語」委員会の第１回「外来語」言い換え提案（平成15年４月）の対象となっており、言い換え語として「安全」が提案されている。

ではないが、かつては「安全対策」という用語が一般的であった。例えば、1984年には、大蔵省銀行局長による最初の機械化通達（昭和59年蔵銀1234号）が出状されたが、その事務連絡のなかで、「安全対策については、コンピュータシステムの事故防止、取引者のプライバシー保護対策等に万全を期するための諸措置を講じさせる」ことが要請されている。1985年には、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」の初版が発行されている。そのような公式な日本語表現が用いられていたにもかかわらず、その後、カタカナ語が主流となったのは何故だったのだろうか。

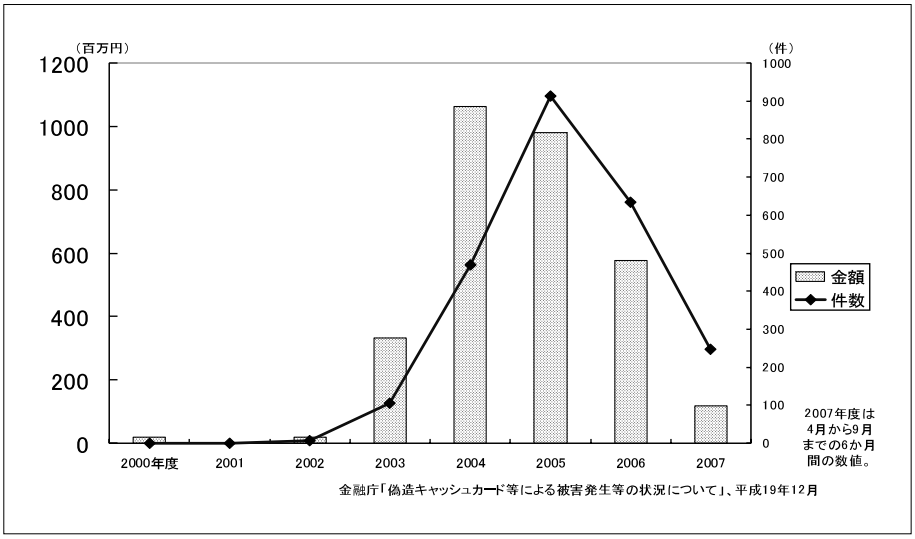
辞書的な説明になるが、「安全」を意味する代表的な英単語には、セキュリティとセイフティの２種類がある。セキュリティという単語は、警備員を指し示す場合にも用いられるように、単に安全な状態を意味するだけではなく、外敵からの攻撃を防御する手段という意味も持つ。これに対し、セイフティという単語は、自動車のシート・ベルトをセイフティ・ベルトと呼ぶように、不慮の事故や不注意による被害を予防するための手段という意味も持つ。日本語で「安全対策」「安全装置」といった表現を用いた場合は、どちらかというとセイフティの意味合いが強く出るようである。

かつて、金融機関の情報システムは、企業内、業界内に閉じたクローズドなネットワーク・システムであった。巨大なコンピュータ・センターにメインフレームを並べ、支店、ATMとの間を専用回線でつなぐことにより、システムを外部から物理的に隔離すれば、システム全体を安全に保つことが可能と考えられていた。リテール・バンキングにおける顧客の認証も、磁気ストライプカードと４桁暗証番号の照合のみという素朴な認証方式が主流であった。暗号、電子認証、ICカード等の情報セキュリティ技術はほとんど利用されていなかったが、特に先端技術を導入しなくても一定の安全性が期待できる環境にあり、利用者が金融ハイテク犯罪の被害者となることはほとんどなかった。

そのような状況においては、金融機関の情報システムがかかえる主要なリスクは、システム開発時の人為的なミス等に起因するサービスの停止や、不注意による情報漏洩であった。金融機関に求められていたのは、システム開発と運用を確実に管理するとともに、機器類の物理的な保護を行うことであった。そういう対応について、「安全対策」という用語が用いられたことは自然であっただろう。

こうした「安全対策」が「情報セキュリティ」へと変わったのは、1990年代後半におけるインターネットの普及と電子マネーへの関心の高まりによるものであった。それまで情報システムの閉鎖性を安全のよりどころとしてきた金融機関においても、利用者の利便性と金融機関の効率化のために、新しいオープンな通信インフラを利用する動きが出始めた。金融情報ネットワークのオープン化が進められると、従来と同じ素朴な認証方式のままでは安全性が確保できない。物理的に外部

〈図〉 偽造キャッシュカードによる預金等払戻しの被害金額・件数の推移



とつながった環境においては、外部からの不正な侵入者・攻撃者を、暗号、電子認証、ICカード等の情報セキュリティ技術によって迎え撃つ必要がある。インターネット・バンキングにおいては、暗号通信プロトコルによって暗証番号や取引内容の機密を保護する必要が生じる。電子マネーを実現するためにも、暗号やICカードの技術は必須である。

このようにインターネット上での金融サービスの提供が進むにつれて、金融機関の対応は、不慮の事故を防ぐことを主眼とした「安全対策」から、外敵からの防御を主眼とした、より高度な対策として、「情報セキュリティ」に変化した。つまり、金融情報システムのオープン化に伴い、目的も手段も変化したために、より相応しい名称として、「情報セキュリティ」というカタカナ語が主流となり、それが現在も続いているのである*3。

3. 偽造キャッシュカード問題の衝撃

わが国の金融機関が情報セキュリティの重要性を痛感することとなった経緯を辿るうえで、2004年から2005年にかけて発生した偽造キャッシュカード問題を避けて通ることはできない。

2002年以前は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は、2003年度から急増し、2004年度には

＊3　なお、専門家による用語法においては、情報セキュリティという言葉は、より多義的に用いられている。例えば、ISMS認証基準を定めた標準規格JIS Q27001：2006では、情報セキュリティを、「情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追及性、否認防止及び信頼性のような特性を維持することを含めてもよい」と定義している。

10億円に達した。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に預金を引き出し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。この問題を受けて、2005年８月に預金者保護法が成立し､2006年２月から施行された。この結果、偽造・盗難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。

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、偽造キャッシュカードの被害額は最高でも年間十億円程度であった。偽造クレジットカードの被害額がピーク時（2002年）に年間165億円に達していたことや、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、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、不正に預金が引き出された預金者個人にまず損失が発生し、被害補償も後手に回ってしまった。このため、預金者の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。

4. 被害沈静化の原因と今後の対応

その後、偽造キャッシュカードの被害は、2006年度には件数、金額とも減少し、2007年度に入ってからも低水準で推移している。偽造キャッシュカード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、それらのなか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き下げである。この対策は、業態を問わず、ほぼすべ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、１日当たりの限度額は数百万円に設定されていたが、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日当たり50万円程度とすることが一般的となっている。この対策が直接的に、１件当た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ことは明らかであろう。また、犯罪者の立場からみたとき、ATMで偽造キャッシュカードを使って預金不正引出を行うという、最もリスクの高い行為の「実入り」が、最大でも50万円程度に下がり、カード偽造自体が「割に合わないビジネス」となった。このことが被害件数を減少させ、相乗効果で被害が沈静化したものと考えられる。

さらに、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思われる。

これに対し、IC カードや生体認証などの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。2007年 3 月末時点の調査では、IC キャッシュカードはすべてのキャッシュカード発行枚数の2.9%（うち、生体認証対応は0.6%）しか普及していないからである。

生体認証対応の IC カードを利用していても、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、提携先 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が貼付された併用カードとなっている。多くの提携先 ATM では、生体認証機能も IC による認証もない通常の磁気ストライプカードとして認識されるため、磁気ストライプ部分のみを偽造して不正に利用することが可能なのである。

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、偽造カード犯罪の根が絶たれた訳ではなく、新しい犯罪の手口を常に警戒していなければならない。全面的な IC カードへの移行など、より抜本的なセキュリティ対策の検討を進める必要性が高まっているように思われる。

5. 将来を見据えた検討の重要性

磁気ストライプカードと 4 桁暗証番号に限らず、金融機関の実務に利用されているシステムのなかには、か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ものが多く存在する。かといって、それらを直ちにすべて再構築することは難しい。さしあたっては、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、次世代のシステムのセキュリティを巡っては、最新のセキュリティ技術研究における理論的な検討結果から得られる警告についても対応を検討しておく必要がある。

例えば、セキュリティに問題のある IC カードや破られやすい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。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、セキュリティについて十分に検討し

ておく必要がある。そのためには、アカデミックな最新の研究成果を意識し、その情報を活用しつつ、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大切である。

6. 業界全体としての積極的な取組みを

情報セキュリティに対する関心の高まりは、金融情報システムのオープン化の帰結であった。こうしたシステム技術面の変化がさらに続いていった場合、金融機関はどのような影響を受けるのだろうか。

かつて、金融機関がレガシー系の技術で等質の情報システムを維持していた時代には、「金融機関であれば、どこのシステムも安全で信頼できる」という意味で、業界全体としてのブランド化が達成されていた。オープン系の安価な技術を導入せず、高価なレガシー系システムを使い続けることにより、そうした「業界ブランド」の価値が維持できてきたと考えられる。

現在、インターネット・バンキングのセキュリティ向上やICカード、生体認証等への投資を行っているのは、個別企業として、安全性、信頼性のブランドを向上させたいと希望する金融機関のようである。他方、そうした個別ブランド化を志向しない金融機関は、情報セキュリティ対策に、人的、システム的な投資を多くは振り向けていない。当面の間は、そのような投資判断でも特段の問題は発生しない。むしろ、過去からの慣性として、金融機関であればどこでも安全で信頼できるという「業界ブランド」が維持されている状況であれば、新しい技術にチャレンジせず、現状維持としていた方が短期的には効率的かもしれない。

しかし、今後、金融情報システムのオープン化がさらに進むなかで、金融機関の一部がシステムの現状維持を選択してしまうと、安全性、信頼性の観点から、業界全体のブランドが維持できなくなる惧(おそ)れがある。金融機関のシステムは相互に連携して機能するものであるため、個別企業のシステムだけが優れていても、全体としては利用者の安全を守ることはできないからである。

こうした観点から考えれば、現在進められているセキュリティの高度化は、広く業界全体が対応していかなければならない課題と受け止めるべきであろう。今後、金融情報システムの情報セキュリティを高度化していくためには、専門性を持った人材の育成と業界内での適切な情報共有が必要であり、金融業界全体としての積極的な取組みが求められているのである。

（文中、意見にわたる部分は筆者の個人的見解である。）

岩下　直行（イワシタ　ナオユキ）氏
昭和59年３月　慶應義塾大学経済学部卒業
昭和59年４月　日本銀行入行
　営業局、長崎支店、調査統計局、企画局、システム情報局を経て、平成６年７月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日本事務局長として金融情報技術の国際標準化を担当。
　平成18年４月　金融研究所情報技術研究センター設立と同時に、センター長に就任。