金融機関の情報セキュリティ対策のあり方について

岩下直行（いわしたなおゆき）

要　旨

偽造キャッシュカードによる不正預金引出や、スパイウエアによる利用者の個人情報の漏洩、インターネット・バンキングでの不正送金など、利用者に実害の及ぶ金融ハイテク犯罪が増加するなか、金融機関にとって、適切な情報セキュリティ対策を講じることによってこうした被害を防止することが、重要な経営課題と位置付けられるようになった。しかし、金融情報システムの高度化・複雑化と、情報セキュリティ対策の技術的な難解さの故に、各金融機関にとって、どのレベルまで情報セキュリティ対策を行えばよいか、正確に見極めることが難しくなっている。

各金融機関は、自らが利用している情報技術と情報セキュリティ対策について、的確に評価したうえで、情報セキュリティ上の要請と自らのビジネスとに折り合いをつけながら、その時点で採用すべき最適なセキュリティ対策を選択していく必要がある。

そのためには、まず、各金融機関が情報セキュリティ対策の有効性、技術上の課題などについて情報を収集し、知見を深めていくことが必要であるが、業界全体として取り組んでいかなければ実効性の得られない対策も多いことを考えると、こうした金融機関の努力を支える役割として、業界団体や規制当局が、業界内での情報の共有を進めるための枠組みを提供していくことも、重要な課題であると考えられる。

キーワード：情報セキュリティ対策、偽造キャッシュカード、
インターネット・バンキング、偽造・盗難カード預貯金者保護法

本稿は、2006年3月28日に日本銀行で開催された「第8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。

岩下直行　日本銀行金融研究所情報技術研究センター長（E-mail: iwashita@imes.boj.or.jp）

無断での転載・複製はご遠慮下さい。

１．金融機関は情報セキュリティ対策をどこまで充実させるべきか

偽造キャッシュカードによる不正預金引出、スパイウエアによる個人情報の漏洩、インターネット・バンキングでの不正送金など、金融機関の情報システムの信任を脅かす事件が次々に発生し、マスコミでも大きく取り上げられ、利用者は不安をつのらせている。金融機関は、こうした脅威に対処し、利用者の信頼をつなぎとめていくために、情報セキュリティ対策を一段と充実させることが求められている。

しかし、金融情報システムの高度化・複雑化と、情報セキュリティ対策の技術的な難解さの故に、金融機関にとってどのレベルまで情報セキュリティ対策を行えばよいか、正確に見極めることが難しくなっているのが実情である。実際、偽造カード問題への対応ひとつみても、ATMに生体認証を導入すべきか、磁気ストライプ・カードをICカードに置換すべきか、その移行はどの程度のスピードと規模で実施すべきかなどについて、現時点では明確な指針となるものは存在していない。

もとより、金融機関がどこまで情報セキュリティ対策のために投資を行うかは、企業体としての経営判断の問題であり、あらかじめ模範回答が存在するわけではない。実際、金融庁・金融研究研修センターが2005年12月に開催した「金融機関と情報セキュリティ」をテーマとするフォーラム[1]の質疑応答のセッションにおいて、「金融機関はどこまでセキュリティ対策をすればよいのか」という論点を巡って討論が行われた際に、パネリストの1人は「リスクに見合った投資を行うべきで、1,000円のために100万円を使う必要はない」と述べた。これに対し、別のパネリストからは、「（顧客の個人情報を保護するという）コンプライアンスはコストにかかわらずやらざるを得ないもので、コストが合わないから違法な状態でもよいということではない」と、ニュアンスの異なる見解が示された。このフォーラムの席上では、この点についてさらに突き詰めた討論は行われなかったが、金融機関の情報セキュリティ対策のあり方について、いくつかの異なる考え方が存在することが浮き彫りになった。

こうしてみると、実際に、金融機関が情報セキュリティ対策のあり方について判断に悩む局面は多々あるものと思われる。本稿では、こうした問題について、いくつかの具体的なテーマに即して、情報技術的な観点から、どのような対応が望ましいと考えられるかについての判断材料を提供してみたい。

1 金融庁・金融研究研修センター［2006］を参照。

2．偽造カード問題への対策とその効果

(1) 偽造カード問題の経緯とそのセキュリティ対策の現状

偽造キャッシュカードによる不正預金引出が社会問題となり、金融機関の情報セキュリティ対策に関する世間の関心が高まったのは、2004年から2005年にかけてであった。その後、2005年2月には金融庁が偽造キャッシュカード問題に関するスタディグループを発足させ、2005年6月には報告書[2]が公表された。また、国会では、法律によって預貯金者の保護を図るべきという検討が行われ、2005年8月に、「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10日から施行された。

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。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、認証技術の強化などが義務付けられることとなった。キャッシュカードのICカード化、ATMにおける生体認証の導入など、偽造キャッシュカードに対するセキュリティ対策は、さまざまな選択肢がよく知られるようになってきたという意味で、この1年ほどで格段に視野が開けてきたように思われる。

しかし、実際にこうしたセキュリティ対策を導入し始めた金融機関はまだ限られており[3]、利用者の間での実際の普及率はあまり高くはない[4]。ICカードを導入した金融機関においても、コンビニATMや提携先ATMでの利用を可能とし、利用者の利便性を維持するために、ICカードに磁気ストライプを併用する先が多いが、その場合、磁気ストライプ部分のみであれば偽造することが容易であるため、偽造カード犯罪の事前予防策としての有効性はあまり期待できない[5]。結局、キャッシュカードによるATMでの預金引出においては、現在でも、磁気ストライプ方式のカードと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いる。すなわち、カードと暗証番号のセキュリティについてみた場合、スキミングなどによる偽造カード犯罪に対して脆弱な状態は、セキュリティ技術的には基本的には現在も変わっていない。

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］を参照。

3 金融庁［2006］によれば、2005年12月時点で、ICカードによるキャッシュカードを導入済みの金融機関は28先、ATMに生体認証を導入済みの金融機関は15先である（590先に対するアンケート調査）。

4 同じく、金融庁［2006］によれば、ICキャッシュカードの普及状況は全発行枚数の1.2%、対応ATMの普及状況は全設置台数の9.9%にとどまっている（590先に対するアンケート調査）。

5 磁気ストライプ併用型のICカードにおいては、ICカード部分を利用した取引と磁気ストライプ部分を利用した取引に、異なる預金引出限度額を設定することによって、磁気ストライプ部分が偽造されても利用者の被害を限定することができるような仕組みが提供されることが多い。この場合、適切に引出限度額が引き下げられれば、偽造カードによる被害を抑制する効果があると考えられる。しかし、預金者が希望すればセキュリティの劣る磁気ストライプ部分でも、高い限度額が設定可能となっている場合、むしろリスクが高まっている可能性がある。

この間、金融機関は、ATMでの預金引出限度額の引下げと、異常取引の検知[6]を行うことにより、偽造カードによる被害の拡大に対処しようとしてきた[7]。偽造カード問題が注目される以前は、ATMでの預金引出限度額は、金融機関ごとに一律の水準とされることが多く、1日当たり数百万円が平均的で、限度額が1,000万円近い金融機関や、限度額を設定していない金融機関も少なくなかった。しかし、偽造カード犯罪の増加を受けて、多くの金融機関で利用者に限度額を選択させるようになったほか、選択できる上限も引き下げられ、現在では1日当たり50万円や100万円といった低い水準に設定する先も増えてきている[8]。預金引出限度額の引下げと、異常取引の検知という対策は、偽造カード被害を防止することはできないが、仮に預金引出限度額が十分に低く設定されており、異常取引が適切に監視できていれば、偽造カードが使用された場合でも被害額を限定できる可能性がある。

偽造キャッシュカードによる不正預金引出事件が拡大した背景には、①偽造の容易な磁気ストライプ・カードと、②盗取・推定されやすい4桁暗証番号を、③高額の預金を1度に引き出すための認証手段として利用していたという条件が揃っていたことがあった。上記の対応は、①や②を急に変更することは難しかったため、当座の措置として、③の条件を厳格化したものといえる。

この対応は、偽造カードが使用された場合でも被害額を限定できるという点で、金融機関経営上、実戦的な意味は大きい。しかし、そもそもこの対応は偽造キャッシュカード犯罪を根絶できるような対策ではなく、ある程度の規模の被害が継続することはやむをえないという考え方に基づくものである。実際、偽造カードなどによる被害額の推移[9]をみても、一時期に比べて落ち着いたとはいえ、預金引出限度額の引下げが実施された後も、引き続き高水準の被害が続いている。1件当たりの被害額は減少しているものの、その分、件数が増加しているからである。金融機関のATMがこうした犯罪の温床となっていることは決して望ましいことではない。

6 ATMでの預金取引において、異常な取引を検知するシステムは、クレジットカード取引において不正取引の排除のために利用されている技術を応用したもので、預金引出の場所、時間、金額などの取引情報を蓄積し、異常な取引を検知しようとするものである。ただし、クレジットカード取引においては、商品の購入履歴や利用加盟店の情報など、個人の行動パターンについての豊富な情報が利用可能であるのに対し、預金取引の場合、取引が異常か否かの判断に利用できる情報が少ないため、利用者の利便性を確保しつつ、効率的かつ適切に異常な取引を検知することは難しい面がある。

7 金融庁［2006］によれば、2005年12月時点で、キャッシュカード利用限度額の任意設定機能を導入済みの金融機関は491先（ただし、これら全ての先が限度額を引き下げているとは限らない）、異常取引検知システムを導入済みなのは319先である（590先に対するアンケート調査）。

8 一般に限度額は1日単位で設定されるため、偽造カードを用いて何日間か操作を続ければ、限度額を超える大きな金額を不正引出することは可能である。ただし、何日も連続で上限額に近い預金引出操作を続けた場合、異常取引を監視している金融機関や真正な預金者に発見・検知される可能性が高まるので、偽造カードによる不正預金引出の被害額を抑制する一定の効果が期待できる。また、預金引出限度額の引下げは、預金口座を利用したいわゆる「振り込め詐欺」の被害を抑制する効果もある。

9 全国銀行協会による「『偽造キャッシュカードによる預金等引出し』等に関するアンケート結果」による被害件数・金額の推移は、2003年度が111件・302百万円、2004年度が437件・981百万円、2005年度が552件・690百万円となっている。

また、「偽造・盗難カード預貯金者保護法」およびそれに基づくカード約款により、預金者の被害は原則として補償されることになるものの、その結果、預金者は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、金融機関の負担が増加することになる。さらに、犯罪者が「自ら偽造カードで引き出して被害者になりすます」ことにより、金融機関から補償金を詐取しようとする犯罪（「被害者なりすまし詐欺」）が発生するリスクもある。

「被害者なりすまし詐欺」が実際に発生するかどうかはまだわからないが、万一そのような詐欺事件が発生した場合、金融機関がそれを見破ることは非常に難しいだろう。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利用者の訴えを疑ってかかるような対応はできないし、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[10]。

さらに、預金引出限度額の引下げは、正規の利用者の利便性を犠牲にするものでもある[11]。

こうした観点からは、緊急対応としてのATMでの預金引出限度額の引下げと異常取引の検知は、最終的な到達点とは考えにくい。その次のステップとして、①磁気併用でないICカード化、および／または②生体認証の導入などにより、キャッシュカードとATMにおけるセキュリティ対策を抜本的に向上させ、そのうえで利用者の希望があれば、③預金引出限度額を一定限度まで引上げ可能とするという施策が考えられる。これは自然なステップではあるが、そのような対応を進める場合、システムに採用した本人認証方式の安全性を厳密に評価していく必要がある[12]。

単に「発行済みのキャッシュカードの一部をICカード化し、それ以外の磁気ストライプ・カードは使用を継続する」という対応は、偽造カード問題の事前予防策として有効ではない。海外の事例をみても、キャッシュカードやデビットカードのICカード化は、事前に移行スケジュールを設定し、業界全体で一斉に実施することが通例である。このような対策を進めることの要否について、金融業界内で十分な検討が行われることが必要であろう。

10 全国銀行協会は、2006年1月に、「偽造・盗難キャッシュカードによる被害にあわれたお客さまから、銀行にいただいた被害に関する情報などを登録し、金融機関間で相互に利用することにより、補償手続きの迅速化、円滑化を図ること」を目的に、「カード補償情報センター」を設立した。同センターでは、「偽造・盗難キャッシュカード等の被害を偽装し金融機関に対して不正な請求が行われた事例に関する情報についても収集し、会員である金融機関からの照会に応じて提供する」ことも想定している（http://www.zenginkyo.or.jp/hosho/index.html）。このような業界全体としての体制整備を充実させるとともに、各金融機関が不正の拡大を未然に防止する努力を重ねる必要がある。

11 限度額を超える預金引出事務についてはATMから窓口にシフトすることになるため、金融機関の経営効率を損なうという問題もある。

12 ICカードを用いた本人認証方式の安全性評価をどのような観点から実施するかについては、例えば、田村・宇根［2006］を参照。

(2) 偽造カード問題の金融機関経営への影響

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、現在の預金取引のビジネス上の位置付けを考えると、コスト対効果の観点から、引き続き、預金引出限度額の低額化と異常取引検知で被害を効率的に限定するといった対症療法のみで対処する割り切りを選択しようとする金融機関があっ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、偽造カード犯罪自体を抑止するものではないので、結果として利用者の不適切な運用による被害を補填し続けるとか、「被害者なりすまし詐欺」の被害を広汎化させるなどの展開を辿った場合には、経営上大きな問題が生じるリスクもある点に留意する必要がある。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。このため、預金取引から得られる利鞘収益は限定的なものであり、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元本の毀損が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。

少なくとも、預金引出限度額の低額化と異常取引検知で被害を効率的に限定するといった対応をとる場合には、上述のような事態を防止するため、預金業務を「誰もが安価に利用できるライフライン的な業務」と位置付け、より戦略的な利益追求型のビジネスに抜本的に変えていくことが必要になる。従来から、都市銀行などは、いわゆる「家計のメインバンク化」戦略のように、預金業務を収益ビジネスにつなげるべく、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になる。その場合、例えば、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、取引開始時に融資の実行を前提とした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たうえで、取引実績に応じて限度額を引き上げるといったビジネス・モデルに変えていくことが必要になる。このように、情報セキュリティ対策の方向を限定的にする場合、ビジネス・モデルを大きく切り替えるといった視点が必要になるだろう。

3．インターネット・バンキングのセキュリティを巡って

(1) インターネット・バンキングにおける認証方式の変遷

インターネット・バンキングが普及するにつれ、その脆弱性を巡る話題も広く知られるようになってきた。最近では、利用者のパソコンに仕掛けられたキー・ロガーやスパイウエアによって、ログインIDやパスワードが盗み出され、不正送金が行われた事件に注目が集まった。そもそも、「パスワードが漏洩してしまうと、巨

額の不正送金が可能となる」というシステムの仕様自体が問題である。現在のインターネット・バンキングの認証方式は、キー・ロガーやスパイウエアなどの手口が現れる以前に考案されたものであり、新たな脅威を防ぎきれなかったものといわざるをえない。

インターネット・バンキングの利用がここまで拡大した背景には、利用者の認証方式が、複雑なものから簡便なものに変更されたことがある。1997年頃にインターネット・バンキングが開始された当時は、SET/SECEを利用した比較的厳格な利用者認証方式を採用していたが、利用者が専用のソフトウエアをパソコンにインストールしたり、公開鍵証明書を取得してパソコンに組み込んだりするための作業負担が大きく、あまり普及しなかった。ところが、2000年以降に、パソコンにあらかじめ組み込まれている暗号プロトコル（SSL）とパスワードを組み合わせて認証を行う「SSL＋パスワード認証方式」が導入されたところ、これが急速に普及した。

SSLは守秘や認証のためのさまざまな機能を有しているが、多くのインターネット・バンキングでは、暗証番号やパスワードの盗聴を防ぐための守秘機能のみが使われている。金融機関側における利用者認証はパスワードのみによって行われる。また、利用者側における金融機関サーバーの確認には、サーバー証明書が使われているものの、それが有効に確認されるか否かは、利用者のITリテラシーに依存している。

「SSL＋パスワード認証」については、インターネット・バンキングにおいて、無権限者によるなりすましなどの攻撃を防止し、正規の利用者や金融機関自体に損害が生じる事態を回避するうえで、十分なセキュリティ対策とはいえないのではないかとの指摘がある。例えば、①考えられる全ての暗証番号を試してみる、あるいは、②パスワードによく使われる単語を辞書から選び、次々に試してみるなど、暗証番号・パスワードに対する基本的な攻撃への脆弱性がある。金融機関側のシステムで、パスワード相違の認証エラーが一定回数を超えると入力を制限するといった防御機構が採用されている場合であっても、さまざまなIDとパスワードをランダムに組み合わせて大量の試行を行えば、防御機構を回避してIDとパスワードの組合せを推定できてしまう可能性がある。

このため、インターネット・バンキングにおける認証手段を二重化し、ログイン用のパスワードに加えて、特に重要な取引に関する操作については、「乱数表によるチャレンジ・レスポンス方式」[13]による認証を導入する金融機関が多くなっている。しかし、残念ながら、乱数表によるチャレンジ・レスポンス方式にも問題点はある。乱数表の導入は、ある取引における認証データ（チャレンジと利用者のレスポンス）が何らかの理由で漏洩してしまい、攻撃者に察知されたとしても、ほかの取引の認証におけるチャレンジが、漏洩したチャレンジとたまたま一致する確率は低いため、攻撃者によるなりすましが困難となるという効果を期待したものである。しかし、金融機関側のシステムにおいて、攻撃者が取引入力のキャンセルを繰り返

13 あらかじめ利用者ごとに配付しておいた乱数表の中の位置をランダムに質問（チャレンジ）し、その位置に記された数値を応答（レスポンス）させる方式。

すことによって、自分にとって都合のよいチャレンジが出るまで「チャレンジの出させ直し」を行うことが可能な仕組みとなっていた場合、1回の取引における認証データが漏洩しただけでなりすましが可能となってしまう危険性が既に指摘されている[14]。また、攻撃対象者を次々に変更しながら当て推量の入力を繰り返す攻撃により、認証エラーが一定回数を超えたら入力を制限するという防御機構を回避して、乱数表の一部のデータを推定できてしまう危険性も指摘されている。

こうした犯罪者と金融機関とのいたちごっこは今でも続いている。一部の金融機関においては、指摘された認証方式の脆弱性を意識して、ワンタイム・パスワードによる利用者認証方式[15]を導入する先も現れている。

(2) セキュリティ・レベルの向上を図るためには発想の切り替えが必要

金融機関の側からみると、インターネット・バンキング用システムは、伝統的な金融機関の情報システムとは大きく異なる性格を持っている。具体的には、①ウェブサイトのプログラムの中身が公開されており、システムの仕組みを外部から解析可能であること、②利用者の脆弱なPCに依存しており、金融機関側のコントロールが徹底できないこと、③インターネットを経由して不特定多数の相手から攻撃を受けるリスクがあることといった点が、通常の金融機関のシステムとは大きく異なっている。金融機関としては、従来のシステム開発・運用の手順から発想を切り替えて、インターネット・バンキングの開発・運用を行っていく必要がある。

利用者のITリテラシー上の問題や、ウェブ・アプリケーションの実装上の脆弱性などの要因が複合的に作用して、外部からの攻撃により、利用者の個人情報が漏洩してしまうといった問題については、外部の専門家の意見に耳を傾け、指摘された具体的な問題点を解決していくとともに、積極的に情報を開示し、対策を進めていることをアピールしていく必要がある。また、利用者のITリテラシーの向上を企図した啓発活動に取り組む金融機関も増えている。インターネット・バンキングは「万人に開かれた金融情報システム」という性格を持つため、前向きの対応を続けていかないと、利用者の信頼を獲得していくことはできない。長い目でみれば、金融機関は、コストのかかる営業店での対面取引から、インターネット取引に利用者を引き寄せる戦略が合理的と考えられるが、セキュリティに対する信頼がないと、利用者を引き寄せられなくなるおそれがあるからである。

14 松本・岩下［2002］を参照。

15 1回しか使えない「使い捨てパスワード」を生成するセキュリティ・トークンを利用した認証方式。現在の時刻や取引1件ごとに増加するカウンタ値などを基に、共通鍵暗号アルゴリズムの演算を行うことによって、取引の都度、一度限りしか使えないパスワードが生成・利用され、かつ、送受信される情報から共通鍵暗号の鍵を推定することが計算量的に困難となるような設計がなされている。リモート端末でコンピュータ・システムの内部リソースにアクセスする際の認証方式として従来から利用されており、信頼性は高い。固定パスワードや乱数表方式と比べて、なりすましや秘密情報の推定に対し、より高い安全性を達成しうると考えられている。

4．従来型システムにおける脆弱性への対応とその問題点

インターネット・バンキングの事例からも明らかなように、金融機関によるインターネットの利用の拡大や、金融機関のセキュリティに対する関心の高まりを受けて、金融機関の情報システムの脆弱性に関する外部の専門家からの指摘も増えてきている。これは、かつて、金融機関が大型コンピュータに独自開発のソフトウエアを搭載して運用していた時代においては、考えられなかった現象である。

かつては、金融機関のシステム開発と無関係の技術者・研究者は、金融機関の情報システムがどのような仕組みで動いているかわからなかったために、その脆弱性についてもコメントのしようがなかった。金融機関にとっても、ほかの情報システムの脆弱性情報は、特段、参考になるものではなかった。しかし、現在は、金融機関のシステムの多くがオープン化し、一般の情報機器ユーザーが利用しているものと大差ない機器構成で構築されているシステムも少なくない。このため、最近では、積極的に外部の知恵をシステムの改善に役立てていくことが可能になってきている。実際、そのような改善が進み、金融機関のシステムも、特にインターネットと接続した部分については、外部のセキュリティ・ベンダーの知恵を活用して、適切なセキュリティ対策がとられるようになってきている。

ところが、そうなると、金融機関が独自に構築し、運用を続けてきたシステムのセキュリティとの相性が問題となってくる。偽造カード事件で明らかになったように、「金融業界が長年にわたり維持してきた独自技術」は、インターネットで利用されるPKI技術やウィルスチェック技術のような「市場のふるい」を通っていない。これまで、その詳細が明らかにされることがなかったため、セキュリティ面で脆弱性を抱えるシステムが、そのまま利用され続けている可能性がある。もちろん、情報を開示しないことによって外部からの攻撃を受けにくくするという効果を期待している部分もあるが、短期的にはともかく、長い目でみた場合、秘密にしていた情報が漏洩する可能性もあり、セキュリティ確保の観点からは安定性に欠ける枠組みといわざるをえない。こうした対策の問題点が最初に露見したのが、偽造カード事件だったといえるのではないだろうか。

5．金融機関のセキュリティが失われることの本当のリスク

次に、偽造カードやインターネット・バンキングの不正送金といった当面解決すべき具体的な問題から離れて、少し長い目で、金融機関のセキュリティが失われることのリスクについて考えてみよう。

金融機関が、ほかの業種の企業に比べて、セキュリティをより重視すべきだと考えられているのは、万一、セキュリティ侵害が発生した場合の被害が、ほかの業種よりも大きくなる危険性が高いという、金融業界の特性によるものであろう。金融機関がその業務において取り扱うのは、取引金額や預貸金の残高、金利や為替レー

トといった、金銭的な価値にかかわる情報そのものである。情報通信技術を用いて電子的な方法で処理されているそれらの情報は、わずかな改ざんが加えられるだけで、巨額の不正に直結することになる。製造業やほかのサービス産業のように、ビジネスの具体的な対象物が限定されており、情報システムに不正があったとしてもそれだけでは大きな被害につながりにくい業種と比べ、金融機関の場合、セキュリティの侵害によって業務に深刻な影響を受けやすく、それを防御することが難しい。また、情報システムに対する攻撃の目的が、単なる業務妨害にとどまらず、攻撃者が不正に利益を獲得することを狙った攻撃を受けやすいというのも、金融機関の宿命である。

最近、たまたまキャッシュカード取引やインターネット・バンキングといったリテール金融取引における不正行為に世間の関心が集まっているが、元来、リテールとホールセールで金融取引の仕組み自体が大きく変わるわけではない。書面と手作業で事務をとっていた時代においては、大口金融と小口金融では、業務の担い手や実務の枠組みが若干異なっており、金融機関内でも棲み分けがなされていたが、電子化が進んだ今日では、金融機関のシステムの内部構造の観点からは、両者の差異は大きくなくなってきている。例えば、小口預金者向けのインターネット・バンキングで利用されている暗号技術も、銀行間の大口決済システムで利用されている暗号技術も、利用されている暗号アルゴリズムやプロトコルは、同一のものであることが多い。ATMで本人認証を行うための技術と、大口金融取引用の端末で本人認証を行うための技術の間にも、大きな違いは存在しない。だとすれば、リテール金融業務において不正のリスクが高まっているということは、金融機関のほかの業務にも、同様の脆弱性が存在する危険性を示唆しているものと考える必要があるのではないだろうか。事実、金融機関間の国際決済ネットワークの端末にキー・ロガーを仕掛けてパスワードを入手し、その端末から不正アクセスを行って巨額の不正送金を企てた犯罪の未遂事件が発生しており、海外のメディアに大きく取り上げられている[16]。

少なくとも現時点では、偽造・盗難カードや盗難通帳による不正預金引出そのものは、その被害金額の規模からみて、各金融機関の経営を揺るがすような問題にはなっていない。しかし、将来について考えた場合、その示唆するところは重要である。考えてみれば、ATMでの不正預金引出も、盗難通帳と偽造印鑑による不正取引も、従来、「不正など起こるはずがない」と考えられていた領域で被害が発生したものである。現在、被害が発生していない領域だから安全とは言い切れない。また、その被害のインパクトも、過去の犯罪事例から予測される範囲内に収まる保証はない。電子的な金融取引においては、1,000円の取引であれ、100万円の取引であれ、10億円の取引であれ、技術的な処理の内容は同一であることが珍しくない。

16 TIMES ONLINE, “Police foil £220m plot by cyber thieves to rob bank,” March 18, 2005. http://www.timesonline.co.uk/article/0,,2-1530545,00.htmlを参照。

したがって、あらかじめ被害額を想定し、その範囲内で対策費用を賄うというアプローチでは、適切なセキュリティ対策を講じられるとは限らない。現時点での被害額の少なさに幻惑されて、過少な投資でよいと判断してしまう誤りに注意が必要だろう。

6．情報セキュリティ再点検の必要性

金融取引カードの偽造犯罪や、隠しカメラを利用した暗証番号の盗撮などの手口は、国内よりも、海外で先に発生していた。例えば、フランスでは、キャッシュカード、デビットカードの偽造犯罪に対抗すべく、早い時期から銀行取引カードの全国的なICカード化が進められてきたし、ドイツでも、独自のセキュリティ対策を施したCD・ATMを導入してきた。現在、英国でも、デビットカードのICカード化が進行中である。欧米では、カードを利用した取引の上限金額も低く抑えられていたし、被害者への補償も迅速に行われていた。

後知恵的に考えれば、わが国の金融業界も、こうした海外の金融犯罪動向に着目し、想像力を働かせて犯罪の事前予防策を進められていたならば、偽造カード問題が深刻な社会問題化することを回避できていたかもしれない。しかし、実際には、わが国では、そうした犯罪が多発する可能性についての認識を、関係者が広く共有することができなかった。わが国は相対的に犯罪の少ない安全な国と認識されていたためか、金融機関にとって情報セキュリティの確保がさほど大きな課題とは認識されていなかったこともあって、こうした海外のリテール金融業務の変化は見過ごされていた。わが国では、組織的にキャッシュカードを偽造し、暗証番号を盗み出して不正に預金を引き出すという犯罪が横行するとは考えられなかったのである。この結果、セキュリティ向上を目的とするICカードの導入という発想はほとんどなかった。わが国の金融業界でも、1980年代以降、何度となくキャッシュカードのICカード化が検討されてきたが、「キャッシュカードの多機能化による銀行ビジネスの拡大」が主たる目的と位置付けられており、喫緊の課題とは考えられてこなかった。少なくとも、「情報セキュリティのコンプライアンスのために全てのキャッシュカードをICカード化するべき」といった議論は皆無であった。

中長期的な観点からセキュリティ対策のあり方について考えるとき、情報技術の進展に伴い、かつては困難と考えられていたさまざまな攻撃手法が、さほど無理なく実行可能となっている点には注意が必要である。例えば、確実なセキュリティを保証してくれると思っていた証書や印鑑を利用した書面取引についても、その確認方法が旧態依然たるものであった場合、そのチェックを欺く偽造証書が出回っているかもしれない。巨額の資金移動を行う金融機関間の大口金融取引のクローズド・ネットワークを介した取引についても、その中身がブラックボックスのままでは安心はできない。金融機関の業務が、「この書面・システムは安全であるはず」という思い込みに大きく依存している場合は、その安全性をきちんとチェックし、それ

が信頼に足る書面・システムであることを、定期的に確認しておくことが望ましい。偽造カードやインターネット・バンキングのセキュリティを巡る問題を奇貨として、そうした抜本的な見直しに着手すべき時期ではないだろうか。

7．金融機関のセキュリティに対する信頼をつなぎとめるために

ここまでみてきた、偽造キャッシュカードやインターネット・バンキングの脆弱性のような、世間的に注目された具体的な問題点以外にも、わが国の金融機関が取り組むべき情報セキュリティに関する課題は少なくない。例えば、海外では、暗証番号はATMで暗号化して送信することが一般的だが、日本ではATMとセンターが専用線で接続されていることを理由に暗号化が必須とは考えられていない。現在、回線暗号やICカードで一般的に使われている暗号アルゴリズムは、あと5年で安全性の保証が切れる見込みにある。生体認証技術についても、生体情報の偽造を用いた攻撃法の存在が指摘されているが、中身がブラックボックスのため、どのようなリスクがあるのか評価しにくい。

金融業界が巨大な情報システムを管理する装置産業になっている以上、そこで利用されている技術を分析・研究し、脅威を未然に取り除いていくことは、金融業界自身の当然の責務である。金融機関は、そのような努力を重ね、成果をあげることによって、顧客の信頼をつなぎとめることが可能になる。とはいえ、現在、金融機関の抱えている情報セキュリティ上の問題点は多方面にわたっており、巨額の投資費用を必要とするものや、業界内の調整に時間を要するものも多いため、一朝一夕には対応できず、息の長い取り組みが必要となる。

金融機関が、以上述べてきたようなセキュリティ問題に対応していくためには、まず、自らが利用している情報技術を分析・研究し、さまざまな情報セキュリティ対策の効果について、詳細に評価したうえで、情報セキュリティ上の要請と自らのビジネスとに折り合いをつけながら、その時点で採用すべき最適なセキュリティ対策を選択していく必要がある。そのためには、おのおのの情報セキュリティ対策の有効性、技術上の課題などを十分に見極められる能力を持つ専門家の育成が必要であろう。そのうえで、組織として、十分な情報を収集し、知見を深めていくことで、適切な判断が行えるようになると考えられる。

また、これらの対策については、業界全体として取り組んでいかなければ実効性の得られないものも多い。業界内で話合いを進めていくための共通認識を固めていくことが大切である。こうした金融機関の努力を支える役割として、業界団体や規制当局が、業界内での情報の共有を進めるための枠組みを提供していくことも、重要な課題であると考えられる。

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）』、2006年（http://www.fsa.go.jp/news/newsj/17/ginkou/f-20060223-3.html）

――――・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～』、2005年（http://www.fsa.go.jp/news/newsj/16/ginkou/f-20050624-4.html）

――――・金融研究研修センター、『フォーラム「金融機関と情報セキュリティ」概要報告』、2006年（http://www.fsa.go.jp/frtc/kenkyu/event/01.pdf）

田村裕子・宇根正志、「金融取引におけるICカードを利用した本人認証について」、『金融研究』第25巻別冊第1号、日本銀行金融研究所、2006年、73～132頁（本号所収）

松本 勉・岩下直行、「インターネットを利用した金融サービスの安全性について」、『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年、207～225頁