日銀レビュー

2006-J-14

インターネットバンキングの安全性を巡る現状と課題

決済機構局　中山　靖司

Bank of Japan Review

2006 年 7 月

金融機関は偽造キャッシュカード問題への対応に加え、インターネットバンキングを対象とした犯罪についても、対策を進める必要がある。最新の犯罪動向およびその対策方法をフォローしつつ、被害が深刻化する前に、本人認証の強化、不正取引監視等の適切な対策を講じること、また、利用者に対する啓蒙を一段と進めることが重要である。

預金者保護法制定後の状況

①偽造キャッシュカード問題

昨年 8 月、「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」（通称預金者保護法）が制定（本年 2 月施行）され、偽造キャッシュカードあるいは盗難キャッシュカードによる不正な預金引出しにより、個人預金者が被害を受けた場合は、原則、全額金融機関が補償することが義務付けられることとなった。これを受け、金融機関はセキュリティの確保を経営問題としてとらえ、キャッシュカードの IC カード化、本人確認手段としての生体認証の導入、リスクに応じた利用限度額の設定等セキュリティ向上のための取り組みを進めている。しかしながら、セキュリティ対策に多大なコストをかけるよりも、当面は保険でカバーしつつ様子を伺おうとする先も見られ、対応が順調に進捗しているとは必ずしも言い難い状況にある。

例えば、キャッシュカードの IC カード化の進捗度合いを見ると、カード総発行枚数に占める IC カードの割合は 1.2%、全 ATM に占める IC 対応 ATM の割合は 9.9%に過ぎない（金融庁「偽造キャッシュカードに対する金融機関の取り組み状況」17 年 12 月より）。しかも、IC カードの大半は、IC 非対応の ATM（提携先金融機関やコンビニの ATM）での相互運用性を確保するために、磁気ストライプカードとしても使えるようになっており、従来同様の脆弱性が依然として残っている。盗難対策として、その有効性が期待されている生体認証にしても、導入済みの金融機関は昨年末で導入予定の先を含めても 11.5%に過ぎない。また、現状では、当該金融機関の本支店に設置された IC 対応の ATM でしか利用できない[1]ため、生体認証機能付き IC カードに切り替えた顧客はそれほど多くない模様である。

【図表 1】偽造キャッシュカードによる被害状況

（単位：件、百万円）

	件数	金額
13 年度	1	19
14 年度	4	16
15 年度	111	302
16 年度	437	981
4 ～6 月	56	186
7 ～9 月	74	276
10～12 月	218	390
1～3 月	89	129
17 年度	552	690
4～6 月	108	135
7～9 月	126	160
10～12 月	164	249
1～3 月	154	146

出所：全銀協「偽造キャッシュカードによる預金等不正引出し」に関するアンケート結果

[1] 本年 3 月、全銀協 IC カード標準仕様の改定が行われ、IC カードに生体認証機能を実装する際の仕様が取り決められた。これに基づいた実装を行えば、ATM に複数の異なる生体認証機器を搭載したり、同じ生体認証方式を採用する金融機関同士の相互運用性を確保したりすることが可能となった。

こうした中で、ほとんどの金融機関では、セキュリティレベルの低い磁気ストライプカードを使った取引にかかる利用限度額を引下げ、リスクを低減しようとしているのが実態である。その結果、偽造キャッシュカードによる不正な預金引出しは、1 件あたりの被害額こそ小口化しつつあるものの、被害件数は今のところ減少に転じる気配を示していない（図表１）。

②インターネットバンキングにかかる犯罪等

この預金者保護法は、インターネットバンキングにかかる犯罪には適用されない。したがって、現時点では、個人の預金者が被害を受けた場合でも、金融機関にはこれを補償する義務はない。これは、制定を急いだ同法案が検討されていた当時は、被害が出始めたばかりで、その実態把握すら難しかったことが背景にある[2]。

このため、実際には、金融機関の自主的な判断により、預金者に対する被害の補償が行われていることがほとんどのようであるが、被害が深刻化していない今のうちに、インターネットバンキングについても、早めに対策を講じることが必要である。

インターネットバンキングを巡る現状

インターネットバンキングは、今や金融機関の重要なチャネルとして認識され、サービスの対象となる口座数も 2005 年 3 月末現在、256 金融機関で約 1,630 万口座を数えている（金融情報システムセンター「金融基幹業務のシステム化に関するアンケート調査（2005 年 3 月 31 日基準）」より）。インターネットバンキングを専業とする銀行も現れ（口座数 246 万口座）、インターネット上の電子商取引サイトにおける決済サービス機能を提供する主体としても、重要性を増しつつある。

こうした中で、近年、日本においても、フィッシング等本人確認情報盗取による、インターネットバンキングを対象とした犯罪が問題になりつつある。金融機関からのメールを装って偽のサイトに誘導し、口座にアクセスするための ID やパスワードを騙し取ろうとする単純なフィッシングについては、すでに多くの事例が確認されている。さらに、実害が出た例としては、インターネットカフェにキーロガー（＝キーボード入力を秘密裏に記録するソフト）が仕掛けられ、インターネットバンクにアクセスするための ID やパスワードが盗まれた事件（2003 年）や、電子メールや CD-ROM でスパイウェアが送られてきて、これを言葉巧みに実行させられた結果、本人確認情報が盗取された事件（2005 年）等が知られている。現時点で判明している事件の被害総額は数千万円程度の模様であるが（図表２）、海外では米国等を中心に大きな被害が発生しており[3]、いずれ日本も同様の脅威に晒される可能性がある。

【図表２】インターネットバンキングの被害状況

（単位：件、百万円）

時期	17 年 4 ～6 月	7 ～9 月	10～12 月	18 年 1～3 月
件数	2	13	16	6
金額	1	12	13	4

出所：全銀協「インターネットバンキングによる預金等不正引出し」に関するアンケート結果

インターネットバンキングを狙った犯罪手口

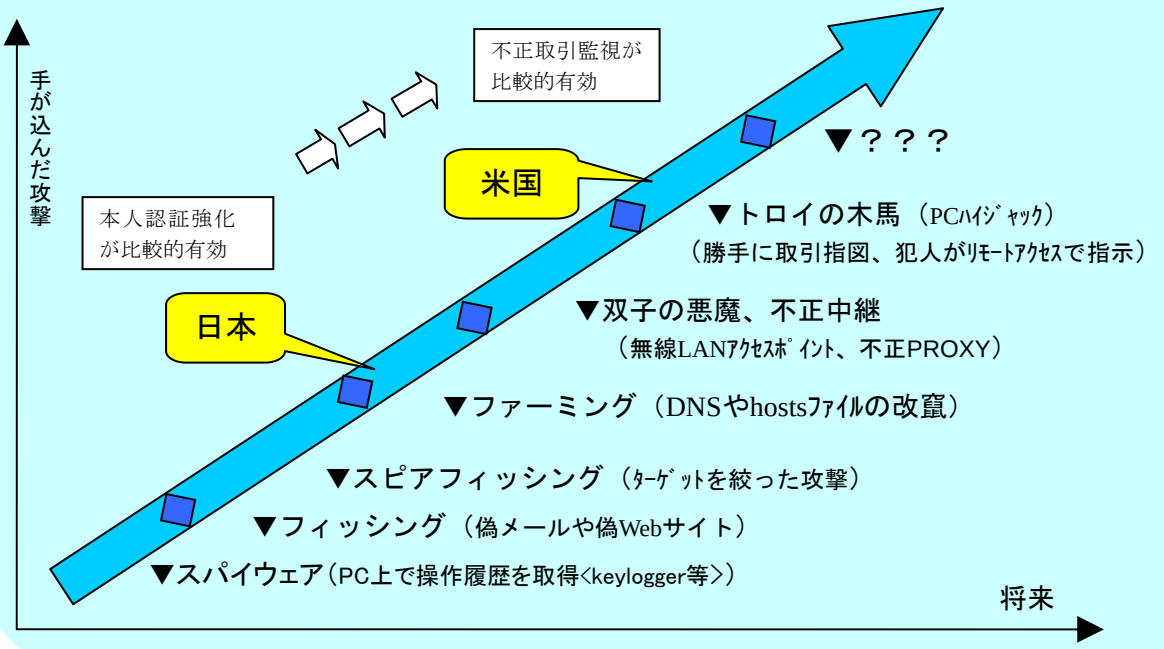
海外におけるフィッシング等の犯罪の動向に目を向けると、その手口は国境を越えて組織的に行われる万国共通のものであり、プロの犯罪であることが多い。不正に獲得された資金の多くはバルチック諸国に送られマネーロンダリングされていると言われており、追跡も容易ではない。

また、その手口も年々巧妙になっている（図表３）。ターゲットを絞ることによってより言葉巧みに欺こうとする攻撃「スピアフィッシング（ターゲットフィッシング）」や、インターネットサイトの接続先情報を改竄し、顧客を不正サイトに誘導する「ファーミング」、不正な無線 LAN のアクセスポイントを使った「悪魔の双子(Evil Twin)」や「不正中継サーバ」等によって偽のサイトに誘導する等様々な手口が見つかっている。「不正中継サーバ」の場合は、中間者攻撃（man in the middle attack）

[2] 同法では、インターネットバンキングにかかる犯罪等については、「速やかに、その実態の把握に努めその防止策および預貯金者等の保護のあり方を検討し必要な措置を講ずること」が付帯決議されている。

[3] フィッシングの被害に関する統計は存在しないが、米国では年間で約7,300万人が平均50件以上のフィッシングメールを受け取り、その被害総額は約 9 億 3 千万ドル（約 1,000 億円）に達しているとの推計がある（米ガートナー社調べ）。なお、同推計には、インターネットバンキングの他、クレジットカードや Paypal 等の送金業者に対するフィッシング被害が含まれる。

【図表３】進化するフィッシング



といって、フィッシングサイトで実際に入力されたパスワード等の本人確認情報や取引指図を裏でリアルタイムに正規のサイトに繋ぎ、正しい結果の画面を利用者に返すなど、利用者から見れば正しく取引が行われているようにすることも可能であり、単に利用者に気づかれないように本人確認情報を盗取するだけでなく、途中で取引指図を改竄する攻撃も可能である。

最近では、さらに高度な機能を持った「トロイの木馬」（不正プログラム）も見つかっている。最新のトロイの木馬は、顧客の PC に感染しても通常は何もせずに潜み、インターネットバンキングで ID／パスワード等が入力され、認証が済んだ時点で初めて活動を始め、予め仕組まれた不正送金等の指図を勝手に行ったり、外部からリモートで指示を受けながら不正な指図を行ったりするようである（PC ハイジャック）。

このように、犯罪の手口はどんどん巧妙化しつつあり、将来どんな脅威に晒されることになるのか予想することも難しくなっている。

セキュリティ強化に向けて①

—— 推奨される二要素認証 ——

インターネットバンキングを巡るフィッシング等の犯罪は、利用者サイドから本人確認情報を盗取ないし詐取することによって行われるものが多い。したがって、利用者に対する注意喚起が最も大事なことである。実際、各金融機関では利用者のセキュリティ啓蒙に力を入れている。しかしながら、一方で、一般的な利用者に対し、専門的な知識を有するセキュリティ対策を完璧に実施させるのは実効的でないのも事実である。そこで、金融機関としては、正当な利用者であることを確認する「本人認証」手段を強化することによって不正行為者によるなりすましを困難にし、仮に利用者がフィッシング等の攻撃を受けても実害を被り難くすることが重要となってくる。

もはや従来型の認証手段であるパスワード等だけで十分なセキュリティを確保することは困難であり、本人確認情報は盗まれる可能性があることを前提とした対策が必要となっている。例えば、複数の異なる有効な認証手段を組み合わせた、いわゆる「二要素認証」ないし「多要素認証」によって認証を強化することが推奨される。

海外でも、公的な機関が二要素認証を推奨する動きが盛んである。米国では、2005 年 10 月、FFIEC（the Federal Financial Institutions Examination Council：米国連邦機関検査協議会）が、インターネットバンキングで用いられる認証に関する指針（Authentication in an Internet Banking Environment）を改訂し、2006 年末までに二要素認証を導入するよう推奨している。これを受け、迫りつつある本年末の期限を前にして、米国の金融機関は揃って対応に追われている。

フランスでは、2004 年 10 月、CFONB （Comité Français d’Organisation et de Normalisation Bancaire：仏国

金融標準化委員会）が、インターネットによるオンライン取引や金融サービスについて、ISO/IEC15408（セキュリティ管理にかかる国際標準規格）に準拠したプロテクション・プロファイル（PP：セキュリティ要求仕様書）を策定し（A protection profile for online banking and financial services）、金融当局も早期にこれに基づいた実装を行うことを推奨している。

また、ドイツでも ZKA（Zentraler Kreditausschuss：金融業界中央信用委員会）が金融取引サービスのセキュリティに関する標準 FinTS（Financial Transaction Service）を策定し、PIN/TAN（Personal Identification Number/ Transaction Number）と呼ばれるワンタイムパスワード（後述）等を使った認証の標準化を行っている。

さらに、金融当局が中心となって二要素認証を推進中の香港、台湾や、官主導で PKI（Public Key Infrastructure：公開鍵暗号に基づいて、電子署名や相手認証を実現するためのインフラとなる技術）の普及を図っている韓国といった事例もある。

セキュリティ強化に向けて②

―― 重要性を増す不正取引監視 ――

二要素認証はフィッシングに対する有効なセキュリティ対策であるが、利用者と金融機関の間に不正に介在して取引指図を改竄する中間者攻撃や PC ハイジャック型の「トロイの木馬」（不正プログラム）に対してはあまり効果がない。本人認証をパスする手順自体は正規の利用者に実行させ、認証が通ってから不正行為を働くからである。

このような PC ハイジャック型のトロイの木馬等に対しては、通常の方法で本人認証のセキュリティを強化するだけでは限界があり、被害を防ぐことは困難である。

【ＢＯＸ】本人認証とは

本人認証とは、本人の真正性、すなわちサービスを受けるためにあらかじめ契約を結んでいる本人に間違いないということを確認することを意味する。

本人認証の方法は、①本人所有によるもの、②本人知識によるもの、③本人固有の特徴によるものと、その利用する要素によって、大きく 3 つに分類することができる。「本人所有によるもの」は、鍵や ID カード等正当な本人しか持ち得ないはずの物を所有していることにより認証する方法である。鍵や ID カードが盗まれたり、複製が作られたりすると、第三者による成りすましを行うことが可能であるほか、本人が紛失する危険性もある。「本人知識によるもの」は、暗証番号やパスワード等正当な本人しか知らないはずの情報を示すことにより認証する方法であり、コンピュータ・システムのアクセス・コントロール等で使われている。ただし、他人が容易に想像できるようなパスワードを使用したり、他人に漏れたりすることによって、第三者に容易に成りすまされる危険性があるほか、本人が忘れてしまう危険性もある。「本人固有の特徴によるもの」は、いわゆる生体認証であり、指紋、静脈、虹彩、顔といった本人の特徴を使う場合と、声紋、筆跡、キーストロークの癖といった本人の特性を使う場合とがある。

二要素認証および多要素認証とは、これらの二つないし二つ以上の異なる要素に分類される認証方式を組合わせた本人確認方法のことである。

【ＢＯＸ】ATM 取引は二要素認証か？

ATM 取引では、従来から「二要素認証」の考え方が採用されている。ATM から現金を引き出す場合には、①キャッシュカードを保持し、かつ②あらかじめ登録してある 4 桁の暗証番号を知っているということを確認することによって、口座名義の本人であることを判断している。しかしながら、①磁気ストライプ式のキャッシュカードは、カードの偽造や複製が容易であり、また、②４桁の暗証番号も高々1 万通りの組合せしか存在しないうえに、他の暗証番号と共用していたり、類推されやすい番号を使っていたりする利用者も少なくないことから、「二要素認証」に本来期待される役割を果たしているとは言い難い。

どのようなセキュリティ対策を講じるかは、各行が提供するサービス等とのバランスを考慮した経営判断が基本ではあるが、少なくともキャッシュカードの IC カード化は今や避けては通れないものと考えられる。

こうした攻撃に対応する一つの解決方法は、異なる通信経路を組み合わせる二経路認証の採用である。たとえば、インターネットで取引指図が送られると、事前に登録してある携帯電話にコールバックを行い、確認に対する返事の声で自動的に認証する（ボイス認証）方法なども考えられている。

また、すべての資金移動の取引指図をチェックする「トランザクション監視」を行うことも有効である。これは、個々の取引のトランザクションを監視し、過去の不正取引事例や各利用者の従来の取引パターンと比較することによってリスク評価を行い、通常の正当な取引とは異なる不規則な取引については、不正な取引指図の可能性があるとして一旦処理を止め、改めて追加で認証処理を行ったり[4]、電話等で直接確認が取れるまでは実行しないといった対応を行うものである。

こうしたトランザクション監視による不正取引検知は、偽造や盗難の被害が多いクレジットカードによる取引では普通に行われていることであるが、個別の金融機関だけで実施するより、不正な接続先 IP アドレス情報を交換する等、金融機関間で情報共有することが有用と考えられる。

セキュリティ強化に向けて③

—— 常に重要な利用者啓蒙 ——

利用者にインターネットバンキングを使うことに伴うリスクを正しく認識してもらい、必要な対策を周知するのは最も大事なことであり、また効果も大きいため、いずれの金融機関も熱心に取り組んでいる。パソコンのウィルス対策に始まり、適切なパスワードの管理方法、フィッシングに遭わないように正当なサイトを見分ける方法等について非常にわかりやすい解説を行っている金融機関も登場している。

ただ、利用者を啓蒙する際に「これさえ守っていれば安心という万全の対策は決して存在しない」ということも強調しておく必要がある。例えば、「正当なサイトの見分け方」にしても、最近ではルート証明書発行機関が認証した「正規」のサーバ証明書を持ったフィッシングサイトも見つかっており、今後、さらに予想も出来ないような手口が登場する可能性もある。

もちろん、フィッシングやスパイウェア等の犯罪は、金融機関だけが努力しても撲滅することは難しい。最近では、インターネットバンキングとはまったく関係のない WEB ページを閲覧したり、メールを開いたりしたのが原因で、利用者の PC にインターネットバンキングを標的とするスパイウェアが送り込まれることも多い。この場合、インターネットバンキングを利用する際にだけ、注意してもあまり意味がないことになる。

したがって、金融機関に限らず、PC ベンダー、プロバイダー、公的機関等、各方面が協力・連携し、様々な対策や啓蒙を行っていくことも課題となってくる。

各認証手段のセキュリティを考える

現在、インターネットバンキングにおける認証方式は、金融機関によって区々であり、ATM による現金引出しにおける認証手段が「キャッシュカード」＋「4 桁の暗証番号」と統一されているのと比べると対照的である。これは、インターネットバンキングは自行の顧客のみを対象とし、相互運用性を考慮する必要がないことから、独自性を発揮しやすいことが理由の一つと考えられる。

日本の多くのインターネットバンキングで取り入れられている認証方式は、ID とパスワードに加え、予め配布した「乱数表」を繰り返し使用したり、第二、第三のパスワードを必要としたりするものである。先行する金融機関では様々な対策を試みており、そのいずれも、適切な実装を行っていれば、ある程度の効果が期待できるものと思われる。一方で、想定する脅威に対しては有効であっても、想定外の脅威に対しては効力を発揮できないことも多い。また、提供するサービスのレベル（振替可能金額の上限等）に比べてセキュリティレベルは十分か、という問題がある。

セキュリティ対策一般に言えることではあるが、リスクをゼロにすることは不可能であるため、採用しているセキュリティ対策がどのような有効性を持ち、その限界はどの辺りにあるのかを把握し、管理可能な範囲にリスクを押さえ込む、適切なリスクマネジメントが求められる。

以下では、現在選択肢として考えられる各認証

[4] リスク評価の結果に応じて、認証のセキュリティレベルを調整することから「リスクベース認証技術」と呼ばれる。サービス利用者に過度な負担をかけずに、リスクを回避する方法としても注目されている。

手段のセキュリティについて考察する。

（１）ID／パスワード

ベーシック認証と呼ばれ、実装が容易なことから様々なシステムで使われる基本的な認証手段である。セキュリティを確保するためには、十分な長さを持った一見ランダムな文字列からなるパスワードを用いることが必要とされているが、類推しやすい脆弱なパスワードを設定している利用者が多いのが現実である。なお、ほとんどの金融機関のインターネットバンクのログイン画面では、リトライ回数に制限があるため、全ての文字列の組合せを順番に試す総当り攻撃は簡単には成立しないと考えられているが、パスワードを固定して ID を色々と変えて試してみるという無差別攻撃もありうることには注意する必要がある。しかしながら、現在、何よりも脅威なのは、フィッシングやスパイウェア等による ID／パスワードの盗取であろう。

最近では、パスワードを最大 32 桁まで設定できる金融機関も存在する。利用者にセキュリティを高めるための選択肢を与えているという意味で望ましい対応であろう。ただし、パスワードは、長ければ長いほど安全である一方で利便性は低下する。覚えるのが難しくなるため、結果的に安易なパスワードが設定されるおそれがある。そして何よりも、フィッシングやスパイウェア等への対策としては、セキュリティの強化に繋がるものではない。

なお、第二、第三のパスワードを設定して認証を強化する方法も考えられる。複数のパスワードを破るにはそれなりに手間はかかるようになるが、やはり、フィッシングやスパイウェア等への対策としてはあまり有効ではない。

こうした中、昨年末頃より、金融機関の間でソフトウェアキーボードを導入することが流行っている。キーボードからの入力を記録するキーロガー等のスパイウェアへの対策として、画面上のバーチャルなキーボードをマウスでクリックして入力するというものである。ただし、マウスで特定のキーをクリックした瞬間の画面を犯人に送信するスパイウェアも発見されているので、万全な対策ではない。さらに、こうした脅威に気づいている金融機関の中には、ソフトウェアキーボードのキー配置をランダムにするとともにクリック時にキー表示を消す対応を図っている先もあるが、（暗号化される前の）送信データそのものが盗聴されるという脅威に対しては有効ではない。ソフトウェアキーボードによって安全性は幾分か向上するが、この対策には限界があることを認識しておくことも必要である。

結局、二要素認証のように、異なる性質を持った有効な認証方法を組み合わせることが、重要といえる。

（２）乱数表

金融機関から利用者ごとに異なる数字が羅列された表（例えば５×５等の二桁の数字）が予め配布され、ログインのたびに指定された箇所の数字を入力することによって認証するものである。仮に、キーロガー等によりログイン時に使用する本人確認情報が漏れたとしても、次回のログイン時は異なる箇所の数字を要求されるため、比較的安全とされている。しかしながら、たかだか２０数個程度の二桁の数字が繰り返し使用されるわけであり、認証時の入力が何回か盗聴されるとなりすましが可能になるおそれがある。

また、ログイン画面を開くたびにランダムな箇所の数字を要求し直すつくりになっている場合には、攻撃者がキャンセルを繰り返すことによって、自分にとって都合のよい箇所が指定されるまで「指示の出させ直し」を行うことが可能であり、一箇所の数字が漏洩しただけでも成りすましが可能になることが指摘されている。さらには、ソーシャルエンジニアリング[5]の技法を使って利用者を言葉巧みに欺き、一度に複数の任意の箇所の数字を効率よく入力させ、これを不正に入手する攻撃も考えられる。

（３）ワンタイムパスワード

ワンタイムパスワードは使い捨てパスワードとも呼ばれ、本人認証の都度、有効なパスワードが変化することから、仮にある取引においてパスワードを入力する場面を見られたり、盗聴されたりしたとしても、次回有効なパスワードを推測す

[5] 技術的な行為ではなく、社会的な手段によって、セキュリティ上重要な情報を見つけ出す行為の総称。代表的なものとしては、パスワードを入力するところを後ろから盗み見たり、オフィスから出る書類のごみをあさってパスワードや手がかりとなる個人情報の記されたメモを探し出したり、身分を偽って電話をかけて情報を聞き出すなどの行為がある。

ることが出来ないため、第三者による成りすましが困難というものである。

ワンタイムパスワードには、①事前にリストを配布するタイプ、②必要の都度トークン等の機器で発生させるタイプ、③必要の都度別の通信経路で連絡するタイプ等がある。

①事前にリストを配布するタイプ

50～100 個程度のランダムな数字が印刷されたスクラッチカードを予め渡され、取引の都度、順番ないし指示された箇所を削って現れた数字をパスワードとして使うものである。ドイツなどでは昔から iTAN と呼ばれ広く使われている。低コストで導入が可能なのがメリットであるが、未使用の複数箇所の数字を入力するよう促すフィッシング攻撃が行われた例もある。

②必要の都度トークン等の機器で発生させるタイプ

個々の顧客に割り当てられた専用の機器に表示される数字をパスワードとして使うものであり、一定時間毎（例えば１分毎）に数字が変わるタイムベースのものと、使用する度に毎回変化するイベントベースのものがある。さらに、単体で機能するトークンを使ったタイプと、ワンタイムパスワードを生成するソフトウェアを組み込んだ IC キャッシュカードを専用の表示装置に挿入して使うタイプのもの等が存在する。なお、トークン自体の盗難にも配慮し、使用にあたって PIN（暗証番号）の入力を求められる機器もある。これらの機器は比較的安全とみられているが、専用の機器を用意しなければならないためコストがかかるのが難点である。

導入コストを抑える観点からは、ワンタイムパスワードを生成するアプリケーション等を利用者の所有する携帯電話にダウンロードして動作させるソフトトークンタイプのものも存在する。ただし、携帯電話のアプリケーション機能の安全性は不明な部分も多く、コピーが作られる可能性が否定できないほか、タイムベースの場合、内蔵時計を意図的に進めることによって、将来の特定の時刻において有効となるパスワードを予め手に入れることが出来るといった点にも留意すべきである。

③必要の都度別の通信経路で連絡するタイプ

取引の都度、インターネットとは別の通信経路で、リアルタイムにパスワードが送られてくる方法等である。代表的なものとしては、あらかじめ登録されている携帯電話の SMS（ショートメッセージサービス）等にパスワードが送られてくる mobile-TAN 等がある。インターネット以外に別の通信経路を使っているため、「二経路認証」にもなっている。

なお、ワンタイムパスワードではないが、携帯電話を使った他のセキュリティ対策としては、携帯電話自体を認証トークンとして位置付け、取引の際に携帯電話にコールバックを行い、通常のパスワードを携帯電話経由で送信することによって認証するタイプのものや、予め携帯電話によって口座のロックを解除する連絡をしないと資金移動が出来なくするといった方法も存在する。

（４）PKI 認証

PKI を使った利用者認証は電子証明書を IC カードに格納する等、適切な管理を行えば安全性は高いと考えられる[6]。

公開鍵を使った認証では、いわゆるチャレンジレスポンス認証[7]を行うことが通常であり、回線を流れる情報が毎回異なるため、盗聴やフィッシングに対しても強い。ただし、導入コストが高い上に、ユーザーの運用負担が煩雑であるため、海外においてもあまり普及した例がない。ただし、韓国のように官主導で取り組んでいる国もあり、今後の動向が注目される。

（５）生体認証

ATM から現金を引き出す際の認証手段としては、指静脈認証、手のひら静脈認証を導入する金融機関が増加しつつある。こうした生体認証をインターネットバンキングにおいて使用することも考えられる。しかしながら、利用者の生体情報をどこで管理するのかといった問題に加え、利用

---

[6] IC カード認証の実現方式のひとつとして PKI を使った公開鍵認証がある。

[7] 相手に対してランダムな値（チャレンジ）を送信し、相手はこのチャレンジを暗号化（レスポンス）して送信元に返す。この返されたレスポンスと元のランダム値から自ら計算した値を比較することにより相手を確認する認証方式をチャレンジレスポンス認証という。認証の度に違うランダム値を使用するので盗聴などに対して強い。

者の管理するパソコンに生体認証読取機器等を取付けることによって生じるセキュリティ上の問題および当該機器の配布コスト、生体情報の登録／抹消を適切に運用するのにかかる負担、といった観点では、ATM 取引に比べると解決すべき問題は多いと考えられる。

（６）その他

予め利用者が登録した設問を表示し、これに答えることによって認証するチャレンジ質問といった認証手段も存在する。設問の表示と併せて、登録した画像やコメントを表示させることによって、逆に利用者が正当なサイトであることを確認することができるケースもある。こうした認証のセキュリティレベルは、その設定する設問の内容に拠る所が大きく、さほど強度の高い手段であるとは考えにくい。しかしながら、様々な取引監視機能と連動させ、評価したリスクが大きい場合には別の手段を用いる等、リスクに応じて適切にチャレンジ質問を活用するということであれば、取引の安全性を高めることに資すると考えられる。

最後に

最近では、フィッシングサイトを発見すると、これを削除する前に “おとり”のパソコンを用意して偽の本人確認情報を大量に入力し、騙された人の有効な本人確認情報を紛れさせてしまうといった積極的防御ともいえるようなユニークなサービスを提供するセキュリティベンダーもある。攻撃側の進歩にあわせ、守る側のセキュリティ対策も進化しているのである。

先々どのような攻撃が出現するかは予想出来ないのがインターネットの世界である。金融機関としては常に最新の犯罪動向およびその対策方法の動向を把握し、十分に効果を考えながら適切かつ機動的に対応していくことが求められている。

日銀レビュー・シリーズは、最近の金融経済の話題を、金融経済に関心を有する幅広い読者層を対象として、平易かつ簡潔に解説するために、日本銀行が編集・発行しているものです。ただし、レポートで示された意見は執筆者に属し、必ずしも日本銀行の見解を示すものではありません。
内容に関するご質問および送付先の変更等に関しましては、日本銀行決済機構局　中山　靖司（E-mail: yasushi.nakayama@boj.or.jp）までお知らせ下さい。なお、日銀レビュー・シリーズおよび日本銀行ワーキングペーパーシリーズは、http://www.boj.or.jpで入手できます。