日銀レビュー

2007-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――2007 年

決済機構局　中山　靖司

Bank of Japan Review

2007 年 12 月

インターネット・バンキングを巡る犯罪が昨年度後半以降広がりつつある。金融機関は、本人認証の強化、不正取引監視等に加え、さらに高度な攻撃を想定したセキュリティ対策を講じる一方で、利用者が晒されているリスクや、利用者が自らの資産を守るために実施すべき事項などに関し、適切な情報提供を行うことが求められている。

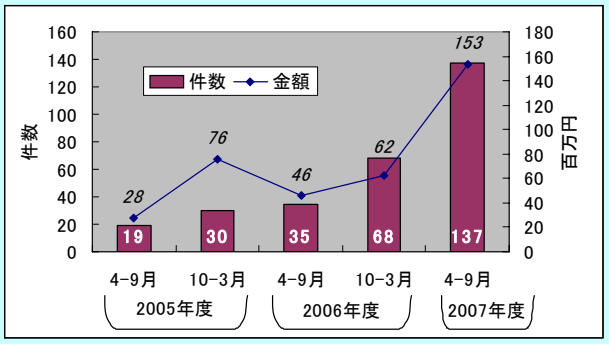
はじめに

偽造キャッシュカード等による預金の不正引出しによる被害を金融機関が補償する「預金者保護法」[1]が施行されてからまもなく２年が経過する。同法では、インターネット・バンキングによる被害は保護の対象外とされ、被害状況の把握などを十分行った上で、２年を目途に見直すことが附帯決議されている。同法施行後のインターネット・バンキングによる被害発生状況を見ると、昨年度後半以降、被害件数、被害総額ともに拡大し始めている。これまでのところ、金融機関が自主的に被害を補償するケースが増えていることもあって、社会問題化する事態には至っていないが、これ以上被害が広がるのを防ぎ、金融機関が信頼を失わないようにするためには、セキュリティ対策を始めとする適切な対応を行うとともに、利用者に対する情報提供を十分に行うことが必要と考えられる。

こうした中、金融機関では徐々にインターネット・バンキングのセキュリティ強化を図る先がみられるようになってきたが、全体から見れば一部に留まっており、また、今後広がる可能性がある新たな脅威に対しては必ずしも対応が十分とはいえない状況にある。

本稿では、昨年７月公表の日銀レビュー「インターネット・バンキングの安全性を巡る現状と課題」の続編として、この一年間の動向を振り返りつつ、あらためてセキュリティ対策の必要性について述べることとしたい。

【図表】インターネット・バンキングによる預金等不正払戻し（被害発生状況）



（金融庁とりまとめ）

インターネット・バンキングを巡る犯罪動向

インターネット・バンキングによる預金等不正払戻しの被害発生状況を見ると、07 年度 4~9 月期の被害件数は 137 件と前年度（年間で 103 件）に比べ急速に増加している[2]。昨年以降、各金融機関が一日あたりの利用限度額引き下げ等の対策を行っていることから、1 件あたりの平均被害額は 06 年度 106 万円、07 年度 4~9 月期 112 万円と、

[1] 「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」（平成 17 年 8 月制定、18 年 2 月施行）

[2] 被害が落ち着きつつある偽造キャッシュカードによる不正払戻しの被害件数（07 年度 4~9 月期 247 件）より依然少ない水準であるが、足元の増加率を勘案すると超えるのは時間の問題とみられる。

【ＢＯＸ①】「インターネット・バンキング関連の攻撃」の日本における最近の事例

■「セキュリティ・カード」の全文字を搾取しようとするフィッシング

偽のウェブサイトに誘導し、本人認証に使用する「セキュリティ・カード」の番号表の全文字を入力させて(※1)搾取しようとするフィッシングメール（英語）が発見された。同金融機関の口座保有有無に関わらず無差別に送信されたものであり、被害も報告されていない（2007 年 7 月頃）。

（※１）通常 4 マスの入力しか指示しないところを、5×10 マス全ての入力を要求。

■タイポスクワッティング

WEB のアドレス（URL）のタイプミスのアドレスに、本物と同一のデザインの偽のウェブサイトが用意されているのが発見された(※2)（2006 年頃）。

（※２）あるネット証券会社の URL の www の後の「ピリオド[.]」を省略したもの等がみられた。

■架空の金融会社を騙る等により個人情報の入手をはかるもの

実在する金融機関等に似せた架空の消費者金融会社等(※3)を名乗ってネット上で融資の勧誘を行い、個人情報の入力を促すものが多数発見された。入力された個人情報を転売したり、この情報を元に「過剰貸し詐欺」等を働くことにより悪用するのではないかと考えられている（2007 年 3 月頃）。

（※３）大手の消費者金融会社のほか、日本銀行の英語名称を騙るもの等がみられた。

05 年度（同 214 万円）に比べれば小額化しているが、抜本的な対策が講じられていない現状では、被害総額自体は拡大する傾向にある（07 年度 4~9 月期 153 百万円）。なお、インターネット・バンキングによる預金等不正払戻しの被害は、預金者保護法の対象になっていないこともあり、金融機関による被害の補償率は 76.3%であるが[3]、直近分（07 年度 4~9 月期）に関して言えば 90.2%と補償に応じるケースが増えているのが実態である（金融庁取りまとめより）。

最近の犯罪傾向

インターネット・バンキングを巡る犯罪手口は、昨年のレビューでも記したとおり、高度化している[4]。最近の傾向としては、高度なソーシャルエンジニアリング[5]の手法を取り入れた「標的型攻撃」[6]が主流になりつつあり、大量のフィッシングメールを無差別にばら撒くような目立った方法は下火になっていることがあげられる。フィッシングメールの内容も偽装サイトに誘導してパスワード等の個人情報を入力させるタイプとは限らず、トロイの木馬等の不正プログラムを実行させ[7]、利用者のパソコンから密かに情報を盗んだり、遠隔操作するもの等が増えつつある[8, 9]。

[3] インターネット･バンキングを利用して無権限者が不正に振り込み送金した行為について、預金者より銀行を被告として提訴された寄託金返還請求訴訟においては、免責約款による銀行の免責が認められた判例が出ている（東京地判平 18.2.13、東京高判平 18.7.13＜旬刊金融法務事情 1785 号 45 頁＞、大阪地判平 19.4.12＜旬刊金融法務事情 1807 号 42 頁＞）。

判例によると、セキュリティについては、「預金者保護の見地から、社会通念上一般に期待されるものに相応するものでなければならない」とする一方、「銀行による暗証番号の管理が不十分であったなど特段の事情がない限り」、免責約款により免責されるとしている。

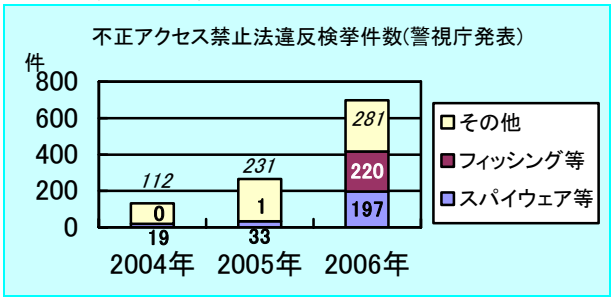
[4] 実際の犯罪手口としては、IT 等の手段を用いたものばかりでなく、本人確認情報を知る内部関係者による犯行も含まれると考えられる。

[5] ソーシャルエンジニアリング：人の心理的な隙や行動のミスにつけ込む等により、重要な情報を引き出したり、特定の行為を誘導したりすること。技術的な仕組みを利用するのではなく、詐欺等の社会的手段を用いることが特徴。

[6] 標的型攻撃：「特定の企業・団体等を標的とし、対象毎に攻撃を工夫して行われる攻撃」を標的型攻撃といい、特にフィッシングの技法を使うものをスピアフィッシングと呼ぶことがある。JPCERT/CC が 2006 年 6 月に公表した調査によれば、調査対象企業の 2.5%が、2006/4 月～2007/3 月の間にスピアフィッシングを受けたと回答している。

[7] 犯罪に不正プログラムを利用する場合も、未公表の脆弱性を狙う「ゼロデイアタック」（脆弱性が発見された際に、その情報や対応策が広く知られる前に攻撃で利用されること）が珍しいものではなくなりつつある。標的に応じて攻撃の度に微修正を繰り返すこともあり、セキュリティチェックソフトでのパターン検知では発見できないことも多くなっている。

[8] 警視庁発表資料によれば、検挙した不正アクセス禁止法違反に係る不正アクセス行為の手口を見ると、フィッシングサイトを開設して識別符号（ID/パスワード等）を入手したもの（2005 年 1 件、2006 年 220 件）、スパイウェア等の不正なプログラムを使用して識別符号を入手したもの（2005 年 33 件、2006 年 197 件）などが急増している。



[9] 金融機関のサイトに接続したときのキーボード入力情報

さらに、今後注意が必要なのは、正規のサイトと利用者の間に介在し、情報を盗んだり改竄したりする中間者攻撃（man in the middle attack）である。これは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見せかける攻撃である。さらに、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、途中で取引指図をリアルタイムに改竄する攻撃も可能である。海外ではすでにこうした攻撃が確認されているほか、簡単に中間者攻撃を可能とする攻撃ツールもインターネット上で販売されている。

安全対策基準等の改訂等の動き

金融庁は、ATM システムおよびインターネット・バンキングの情報セキュリティ対策について、「情報セキュリティに関する研究会」を開催（06 年 3 月から 6 月にかけ計 3 回、事務局：金融情報システムセンター）し、そこでの議論を踏まえ、07 年 1 月、「主要行等および中小・地域金融機関向けの総合的な監督指針」（以下「監督指針」という）を一部改正した。同指針においてはインターネット・バンキングの本人認証に関して、セキュリティ確保上の主な着眼点（「個々の認証方式の各種犯罪手口に対する強度を検証した上で、取引のリスクに見合った適切な認証方式を選択しているか」）が示されている[10]。さらに、金融情報システムセンターでも、07 年 3 月、「金融機関等コンピュータシステムの安全対策基準」（以下「安全対策基準」という）を改訂し、「一つの手口のみで破られない認証方式の採用」、「取引の重要度に応じた厳正な本人確認」等の項目を追加している。

金融機関のセキュリティ向上策

金融機関においては、セキュリティの確保を経営戦略の一部ととらえ、セキュリティに対する意識が高い企業であることをイメージづけ、他行との差別化を図ろうとする動きがみられる。

セキュリティ対策には完全はありえないこともあり、コストや利便性とのバランスを考慮して、個々の具体的な対策を採用することになるが、その場合、①本人認証の強化（利用者への成りすまし防止）、②サイト認証の強化（利用者が正当なサイトを判別する手段の提供）、③不正取引監視、④利用者啓蒙、等の側面からセキュリティの検討を行っておくことが最低限必要である。

以下、金融機関の取組み事例として、導入がみられるセキュリティ対策例を紹介する。

（1）本人認証の強化

①ワンタイムパスワード

ワンタイムパスワード（OTP）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ものである。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なるメリットがある。

今のところ、トークン型のワンタイムパスワード発生装置を使った認証方式を、有料で希望者に対してのみ提供する金融機関が多数派であるが、一部のインターネット専業銀行では全ての顧客に対して一律にトークンを提供している。さらに最近では、共同利用型のインターネット・バンキングサービスを提供するベンダーが、こうした認証手段をメニューとして提供し、これを地銀や信金が採用する動きがみられる。

また、コスト高となる専用トークンを使ったパスワード発生装置の採用を避け、携帯電話のローカルないしセンターのアプリケーションとして OTP 機能を提供する試みも始まっている。

②携帯電話を使った認証

これは、携帯電話の個体認識番号を認証の要素（物理認証）として利用することによって、２要素認証を実現しようとするものである。インターネット・バンキングのログイン画面で、ID／パスワードを入力すると、毎回異なるランダムな数字

等を記録して、外部に送信するものが中心であるが、一部には勝手に資金移動指図を出して、金銭搾取を試みたり、マネーロンダリングに利用しようとする、いわゆる「PC ハイジャック型」のものもあるといわれている。

[10] 日本銀行でも、18 年 7 月に日銀レビュー「インターネット・バンキングの安全性を巡る現状と課題」において、「二要素認証の採用を含む本人認証の強化」や「不正取引監視等の導入」、「利用者啓蒙の一段の促進」に関して提言している。

が返され、これを携帯電話経由でサーバに送ることによって認証を完了する。利用者所有の携帯電話を利用することからトークン等の特別な機器を配布する必要がない点がメリットとされる。

③リスクベース認証

本人認証を強化する場合に、トレードオフとなるのが利便性の問題である。そこで、通常とは異なる特徴を持つアクセスや資金移動を伴う重要な指図等、リスクが高いと考えられる取引では強固な認証を実施する一方、リスクがあまり高くないと判断される取引では、利用者の利便性を優先して簡易な認証を行うシステムの導入を行う金融機関が複数行みられる。

不正な取引をリアルタイムで検知し、事前に被害の発生を防ぐ不正取引検知システムと併せた運用も可能とみられ、利用者の使い勝手にも配慮した仕組みとして期待される。

④電子証明書

電子証明書を使ったクライアント認証[11]は、導入や更新にかかる運用が煩雑で、利用者サポート等にかかる負担が大きく、また、アクセスする端末が電子証明書を導入した端末に限られるといった制約があることもあって、個人顧客向けに導入が成功した事例はほとんどない。ただ、法人向けに関しては、より大口の金額を扱うためリスクが高いということもあり、セキュリティを高める観点から採用する動きがみられる。

⑤IP アドレス認証

アクセスできる回線を予め登録した IP アドレスや ISP[12]に限定することによって、不正なアクセスを防ぐ仕組みであり、本人認証を補完する対策と位置付けられる。利用者の利便性が低下するというデメリットはあるものの、ID やパスワードが盗まれたとしても、登録されていない IP アドレス等からのアクセスは拒否されるため、比較的効果は高いと考えられる。

なお、今後普及することが見込まれている NGN（次世代ネットワーク）[13]を使った接続の場合には、発信者 ID による回線認証が可能となるため、IP アドレス認証よりもより確かな認証手段として期待されている。

以上のような、本人認証の強化は、単純なフィッシングによる ID／パスワードの漏洩に対しては効果が期待できるが、今後、攻撃が高度化するにつれて増えてくると予想される中間者攻撃やトロイの木馬等の不正プログラムによる PC ハイジャックに関しては有効な対応策とはなり難い。こうしたリスクまで想定すると、例えば、一定金額を超えるリスクの高い取引に対しては、個々の取引指示内容に対して、その正当性を個別に確認する「取引認証」を別途の経路で行う仕組みを考えることも必要であろう。

２）サイト認証の強化

通常、インターネット・バンキングサービスでは、金融機関の WEB サーバに SSL 証明書を搭載し、サーバ認証および暗号化通信を機能として提供している。以前は、URL が確認できかつ SSL 証明書を使った暗号化通信が行われることをもって、フィッシングサイトの可能性は低いと判断できたが、最近では紛らわしいドメインを取得した上で SSL 証明書を用意する不正なサイトも出現しており、脅威となっている。

こうした中、金融機関においては、サーバが正規のものであることを確認する手段を強化ないし別途提供しようとする動きがみられる。

①EVSSL（Extended Validation SSL）証明書

EVSSL 証明書とは、SSL 証明書の一種であるが、法人として登記されている等、実在証明にかかる審査基準を厳しくすることによって、発行に際して厳密な存在確認を行うことを要件とするものである。EVSSL 証明書対応のブラウザ[14]で EVSSL 証明書が導入されたサイトにアクセスすると、これまでの南京錠マークに加えアドレスバーが緑

[11] 金融機関が運営する認証局が発行するもので、公開鍵暗号を使って正当な利用者であることを確認する仕組み。

[12] ISP (Internet Service Provider) : インターネット接続サービスを提供する事業者。

[13] NGN (Next Generation Network) : 交換機による既存電話網を、IP 技術を使って置き換える次世代ネットワーク。高品質の IP 通信を標準で実現できることから、固定電話に限らず様々な上位レイヤーのアプリケーションサービスを可能にすると期待されている。

[14] 現在、Windows VISTA 上で動作する Internet Explorer7.0 が対応しているのみであるが、Firefox や Opera の次期バージョンでは対応予定。

色に変化するとともにバー上に Web サイトを運営する組織と証明書の発行認証局が明示されるため、利用者による確認が容易になっている。

これまでに数行が導入を決めたほか、既に切換え済みの金融機関も存在する。現時点では EVSSL 証明書に対応したブラウザの普及率があまり高くないため、その効果を疑問視する向きもあるが、追加的なコストがさほどかからないことからも、今後、インターネット・バンキングにおいては EVSSL 証明書がデファクトになっていくものと推測される。なお、中間者攻撃に対しても、有効な対策となりうると考えられる。

②フィッシングサイト警告ツール

地銀等を中心に、利用者のパソコンに導入した専用ツールから、認証サーバ等に問い合わせを行うことにより、正規のサイトであるかどうかを確認するサービスを提供する金融機関が多数みられる。必ずしも最新のブラウザでなくても対応している場合が多い。接続先サイトの URL や IP アドレスから正規のサイトかどうかを判断する仕組みのものが多いようであるが、中には表示画像に埋め込んだ電子透かしを応用するものなどもみられる。

もっとも、サイトの確認自体は、本来、SSL 証明書を始め、ブラウザの基本機能で確認できるはずのものであり、利用者のパソコンに専用のソフトウェアを導入し、その使い方を理解してもらうなどの追加的負担が生じることを考慮すると一概に利用者の利便性が高まるとはいえないとの見方もある。

③画像によるサイト認証

リスクベース認証を利用したシステムの中には、予め利用者が登録した複数の写真等を表示し、申告したとおりの順番を指示させるという本人認証方法を用意しているものもある。利用者ごとに登録された写真を表示することができるのは正規のサイトのみであるため、サイト認証としても同時に機能することとなる。もっとも、サイト認証として有効になるためには、サイトにアクセスした際に写真が表示されない場合には、利用者がサイトの偽装を疑うことが必要であるが、ある大学の研究によればなんら疑問に思わないで、パスワードを入力する人がほとんどだったという実験結果もある[15]。サイト認証全般に言えることであるが、利用者のリテラシーなくしては、効果は乏しいと言えよう。

なお、サイト認証画像の表示は予め設定した端末からアクセスした場合しか機能しないなどの制約がある。

④不正サイト閉鎖サービスの利用

万が一、偽の WEB サイトが発見された場合は、被害者の発生を抑えるためにも、出来る限り早く、偽サイトの存在を周知し注意喚起を図るとともに、ISP などと協力して偽サイト自体を封じ込めることが有効である。最近では、偽サイトの動向を監視し、発見した場合には早期に閉鎖するように手配を行う外部のサービスを導入する金融機関も増えている。多くの場合 5 時間以内に偽サイトをシャットダウンさせることに成功しているとのことである。

（3）不正取引検知システム

オンラインサービス上のトランザクションを監視し、利用者の取引パターンに基づいて不正取引を判定・検出するシステムを導入する金融機関もみられる。リスクの高い取引パターン（例えば、通常と異なる地域や IP アドレスからのアクセス、初めての口座への多額の送金、送金直前の個人情報の変更）を検出するためのルールを予め設定しておくことによって、不正取引を洗い出している。判定・検出結果によって、必要に応じてリスクベース認証を行ったり、一時的に取引指示を保留したりすることが可能となる。

15 マサチューセッツ工科大学（MIT）とハーバード大学の研究者チームが 2007 年 2 月 4 日に公表した研究成果（5 月の米国電気電子技術者協会（IEEE）セキュリティ・プライバシー関連シンポジウムで正式発表）によると、普段から金融機関のインターネット・バンキングを利用しているユーザーは、サイトが偽装されていることを示す重要な手がかりを見過ごす傾向が高く、特に「サイト認証画像はまったく効果がない」と結論づけている。

研究で行われた実験によると、「サイト認証画像」が表示されないのに気づいたのは、60 人中 2 人だった。しかも、実際に利用している金融機関のサイトにアクセスしてもらった実験では、サイト認証画像がないにもかかわらず、25 人中 23 人がパスワードを入力した。

なお、同時に行われた実験では、Web ブラウザの右下に表示される鍵のマーク等を削除したところ、67 名全員がそれに気づかずに取引を行った。また、パスワード入力画面において「サイトのセキュリティ認証に問題がある」という警告が表示された場合でも、57 名中 30 名がこれを無視してパスワードを入力した。

【ＢＯＸ②】分業化するフィッシング行為

フィッシングは、様々な作業に分業化され、責任の所在が曖昧にされた組織犯罪である。また、その対策も多岐に渡り、様々な立場の関係者の協力が必要となる。

	分業内容の一例	分業された行為の一例	対策の一例
①	ﾒｰﾙｱﾄﾞﾚｽ収集	・ﾌｨｯｼﾝｸﾞﾒｰﾙ送信先のﾒｰﾙｱﾄﾞﾚｽを収集し販売。 ――特定のｻｰﾋﾞｽ利用者等のﾀｰｹﾞｯﾄが絞られたｱﾄﾞﾚｽほど高価。	・顧客のﾒｰﾙｱﾄﾞﾚｽの一覧等の個人情報の漏洩対策。
②	ﾎﾞｯﾄﾈｯﾄ貸出し	・ﾌｨｯｼﾝｸﾞﾒｰﾙの送信等に使用するﾎﾞｯﾄﾈｯﾄの貸出し。 ――国内でも 40～50 台に 1 台はﾎﾞｯﾄに感染している可能性。	・ﾎﾞｯﾄ PC 撲滅のための利用者啓蒙等（ｳｨﾙｽ/ ｽﾊﾟｲｳｪｱ対策ｿﾌﾄ,ﾊﾟｰｿﾅﾙﾌｧｲｱｳｫｰﾙ等の対策を推奨）。
③	ﾌｨｯｼﾝｸﾞﾂｰﾙ作成	・ﾌｨｯｼﾝｸﾞｻｲﾄやﾌｨｯｼﾝｸﾞﾒｰﾙを作成するためのﾂｰﾙを作成し販売。	・早期に販売ｻｲﾄを発見し、閉鎖。
④	ﾌｨｯｼﾝｸﾞ実行	・ﾌｨｯｼﾝｸﾞﾒｰﾙを送信して、ﾌｨｯｼﾝｸﾞｻｲﾄに誘導し顧客の個人情報（ID／ﾊﾟｽﾜｰﾄﾞ等）を収集したうえで販売。	・早期にﾌｨｯｼﾝｸﾞｻｲﾄを発見し、閉鎖。 ・ﾌｨｯｼﾝｸﾞｻｲﾄとして利用されないようｻｰﾊﾞの脆弱性対策。 ・ｽﾊﾟﾑﾒｰﾙ対策（電子ﾒｰﾙ認証技術の導入） ・利用者啓蒙（ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ対策、ｳｨﾙｽ対策等） ・ﾌｨｯｼﾝｸﾞｻｲﾄ警告ﾂｰﾙ等（EVSSL 証明書等）
⑤	不正資金入手	・顧客情報を使って不正な資金移動を実施（架空名義口座に送金）。 ・移動した資金を引出し、犯罪組織に送金。 ・不正に入手した資金を洗浄。	・本人認証の強化、端末認証の実施、不正取引検知ｼｽﾃﾑ、個々の取引に対する認証。 ・振込先を事前登録先に限定、振込み限度額の引下げ ・不正の早期検知（前回ﾛｸﾞｲﾝ時刻の表示、取引結果のﾒｰﾙ通知） ・口座不正利用に伴う口座の利用停止・強制解約等、ﾏﾈｰﾛﾝ対策。

（４）利用者におけるセキュリティ強化

①利用者啓蒙

フィッシングの被害発生を抑えるためには、技術的対策だけでは限界があり、利用者のセキュリティリテラシーを向上させるための啓蒙が大事である。今やほとんどの金融機関がホームページ上で利用者啓蒙のためのセキュリティ解説ページを載せているようになってきている。もっとも、こうした解説へのリンクが分かり難くかったり、フィッシングに対する注意喚起が適切に行われていなかったりするケースがみられるとの指摘もあり[16]、啓蒙活動の一層の質の向上が期待されている。

②セキュリティ・チェック・サービスの提供

インターネット・バンキングに接続中、スパイウェアやウィルス等のマルウェアに感染していないかどうかをリアルタイムで監視するインストール不要のセキュリティ・チェック・サービスを提供する金融機関が地銀等を中心に増えつつある。正規のサイトへのアクセス時に、マルウェアに感染しているかどうかをチェックできる可能性はあるが、最新のマルウェアには対応していない場合も多い[17]ことや、そもそも不正サイトにアクセスしているときには起動されないことから中間者攻撃には効果がない。したがって、誤解に基づく安心感を与えて返って逆効果になることがないよう、利用者に対しては、どのようなリスクに対して有効な対策なのか、その限界を十分に説明し、油断することのないように注意を喚起することが必要である。

おわりに

インターネット・バンキングにおける不正払い出し等の犯罪は、正当な利用者に成りすますことによって行われる。したがって、正当な利用者であることを確認する本人認証の強化は大きな課題である。しかしながら、今後増加することが考えられる中間者攻撃[18]や PC ハイジャック型のト

[16] 監査法人トーマツが 11 月に公表した調査（全国 147 行を対象）によると、フィッシングに対する注意喚起や、関連したセキュリティ対策の整備、情報発信が十分とはいえないケースが 26%見られた。

[17] マルウェアの作者は、既存の主要なアンチウィルスソフトの最新版では検知できないことを確認したうえで、マルウェアを配布しているといわれている。

[18] 中間者攻撃に対しては、接続しているサイトが正しいかどうか確認するサイト認証が重要となってくる。サイト認証は、本来、もともとブラウザに備わっている標準的な機能を使うことで確認できるはずであるが、利用者が一定のリテラシーを保有することが前提となっていることが問題を複雑にしている。

ロイの木馬[19]を前提にすると、本人認証の強化だけでは限界がある点にも注意が必要である。

全ての取引をリアルタイムで監視して不正取引を事前に検知して防いだり、資金移動の指示を行うたびに、携帯電話へのコールバックで取引の正当な意思があるかどうかを確認する「取引認証」を導入するなど様々な対策の組合せで対応することが重要である。また、個々の金融機関がインターネット・バンキングというチャネルを経営戦略上どのように位置付けるかによっては、利便性を犠牲にすることになっても、利用可能限度額を引下げたり、事前登録先にしか資金移動できなくしたりする等の対応も選択肢として考えられる。

さらに、利用者は、金融機関がどのようなリスクを想定し、どのような対策を行っているのか、そしてその限界はどの辺にあり、何に注意を払う必要があるのか等、を正しく理解した上でインターネット・バンキングを利用することが求められる。金融機関はその点を踏まえて啓蒙していくことが大切であろう。

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。

[19] トロイの木馬については、金融機関と関係ないサイトにアクセスした際に感染している事例も多く、金融機関の努力だけでは限界がある。