IMES DISCUSSION PAPER SERIES

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

まつもとつとむ　いわしたなおゆき
松本 勉・岩下直行

Discussion Paper No. 2002-J-12

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

IMES Discussion Paper Series 2002-J-12
2002年3月

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

松本 勉[*1]・岩下 直行[*2]

要　旨

インターネットの急速な拡大を背景に、インターネットを利用して金融サービスを提供する金融機関が増えている。インターネットは世界中の利用者に開かれたネットワークであるため、利便性と効率性が高い反面、セキュリティ上の様々な脅威が存在することが指摘されている。インターネットを経由して金融サービスを提供する際には、金融機関もこうした脅威に対する適切な対策を講じておく必要がある。

インターネット・バンキングを提供する金融機関が最も重視しなければならないセキュリティ対策は、無権限者による成りすましなどの攻撃によって、正規の利用者や金融機関自身の財産が被害を受けないようにすることにある。そのような効果を実現する上で鍵となるのは、インターネット上での利用者の認証方式である。そこで、本稿では、現在のインターネット・バンキングの多くで利用されている、SSL、パスワード、乱数表を組み合わせた認証方式にスポットを当てて、考えられる攻撃法について分析した。

その結果、現在の認証方式は、システムの設定次第では、情報の一部が漏洩した場合に成りすましの攻撃を受けるとか、乱数表の情報の一部を推定されるといったセキュリティ侵害のリスクが存在することが分かった。こうしたリスクは、現時点では深刻な問題とは言えないものの、将来、インターネット・バンキングがより広範に利用されるようになると、実際の被害に繋がりかねないものと思われる。わが国の金融機関が、今後、インターネットによる金融サービスを拡大して行くためには、こうしたセキュリティ上の問題点について、適切に対処していくことが望ましいと言えよう。

キーワード：インターネット・バンキング、セキュリティ対策、認証方式、SSL、パスワード、暗証番号、乱数表

JEL classification: L86、L96、Z00

*1 横浜国立大学 大学院 環境情報研究院（E-mail: tsutomu@mlab.jks.ynu.ac.jp）

*2 日本銀行 金融研究所 研究第2課（E-mail: iwashita@imes.boj.or.jp）

本論文は、2002年2月28日に日本銀行で開催された「第4回情報セキュリティ・シンポジウム」への提出論文として作成されたものである。

目　次

頁

１．はじめに

インターネットの急速な拡大を背景に、インターネットを利用して金融サービスを提供する金融機関が増えている。多くの金融機関がインターネット・バンキングの提供を開始している[1]ほか、インターネット取引を業務の中心に据えたネット専業銀行も立ち上がり、振込手数料の引下げ等の効果もあって利用者数も急速に拡大してきている[2]。インターネット・バンキングは、金融機関の有力なデリバリー・チャネルとして定着しつつあり、それに伴って利用者の利便性も大きく向上していると言えるだろう。

その背景としては、ひとつには、各金融機関が、インターネットは安いコストで高度な金融サービスを提供できる有望なチャネルであるとの判断に基づき、積極的に経営資源を投入してサービスを立ち上げたことが挙げられる。また、利用者側の事情としては、インターネットを利用した株式売買やオークション、通信販売の利用者を中心に、自宅のパソコンから振込や残高照会といった金融機関のサービスを利用したいというニーズが強まっていたことが、普及の原動力となった。加えて、店頭で取引するよりも振込手数料等が安いという点もインセンティブとなって、利用が拡大したものと考えられる。

インターネットは世界中の利用者に対して開かれたネットワークであり、金融機関が従来利用してきたクローズドなネットワークに比べ、利便性や効率性が格段に高い反面、様々なセキュリティ上の脅威が存在している。インターネッ

---

[1] 金融情報システムセンターが全国 684 の金融機関を対象に平成 13 年 3 月末に実施した「金融機関業務のシステム化に関する動向調査」によれば、インターネットを利用したサービスのうち、①残高照会については 43.0%の先が、②資金移動（振替、振込等）については 30.7%の先が「実施済み」と回答している。特に、都市銀行については、全先が「実施済み」と回答している。

[2] わが国におけるインターネット・バンキングの利用者数については、金融機関毎のインターネット・バンキング対象預金口座数、取引件数といった基礎データが公表されていないため、確実なデータは存在しない。しかし、これまでに発表されている様々な調査結果をみると、ここ１、２年で利用者数が急速な伸びを示していることが窺われる。

例えば、IT 専門調査会社 IDC Japan によれば、インターネット・バンキングの利用者数は、2001 年 3 月末現在で 250 万人を超えると推計されている。1998 年頃は、大手銀行でもインターネット・バンキングの利用者が数千人程度しか存在しないと言われていたことを考えれば、急速な伸びと言えるであろう。

また、マイボイスコム株式会社が定期的に実施しているアンケート調査において、「インターネット・バンキングを利用したことがある」と答えた回答者の比率は、1999 年 9 月 9%→2001 年 1 月 22%→2002 年 1 月 44%と著増している。同アンケート調査は、インターネット経由で実施されたものであるため、サンプルに偏りがあるものの、時系列で比較した増加テンポは極めて速いと言えよう。

トを経由して金融サービスを提供する際には、金融機関もこうした脅威に対する適切な対策を講じておく必要がある。

２．金融機関のセキュリティ対策は何が特殊なのか

インターネットを利用したシステムのセキュリティ対策を巡る議論において、金融機関は、「特別に高いセキュリティを必要とする存在」と位置付けられている。信用を重んじる金融機関にとって、セキュリティ対策が重要と考えることは当然のことのように思われるが、具体的な業務内容との関係を考えたときに、何故、金融機関は特別に高いセキュリティを必要とするのであろうか。

インターネット・バンキングを提供する金融機関の多くは、自らのホームページにおいて、採用しているセキュリティ対策の概要を紹介し、様々な脅威に対して万全の備えを講じていることをアピールしている。セキュリティ対策の具体的な内容はあまり詳細には説明されていないものの、強固なファイアウォールを設定して不正アクセスを防止していること、ウィルスチェック・プログラムによる検知を徹底していること、アクセス状態を 24 時間常時監視していることなどが開示されている。

こうしたセキュリティ対策を充実させること自体は、金融機関として望ましいことであり、それを適切に開示することも、利用者の信頼感を醸成する上で有効であろう。ただし、こうした一般的なセキュリティ対策は、金融機関が、他業種の企業や公的機関と比べて特別に注意しなければならないことという訳ではなさそうである。預金口座の取引データや暗証番号を除けば、金融機関に届け出られている個人情報は、他の企業の顧客情報とさほど異なるものではない。ホームページの改竄等による風評被害や、サービス停止攻撃の影響も、他の業種と同程度の脅威であるにすぎず、その意味でも特別ではない。実際、金融機関が採用しているネットワーク･セキュリティ対策は、いわば汎業界的な技術として確立されているものであり、金融機関だけが特別な技術を採用している訳ではない。

にもかかわらず、金融機関が特別に高いセキュリティ対策を必要とすると考えられているのは、金融機関が顧客の金融資産の管理を任されており、金融機関の情報システムの中に、その管理用データが格納されている、という特性に因るものであろう。例えば、製造業の企業であれば、顧客にとって大切なのは、製造された製品の品質であるから、極論すれば、その企業の事務所や工場の情報システムが何らかのセキュリティ侵害を受けたとしても、顧客が購入した製

品に問題がなければ顧客に被害は及ばない。しかし、金融機関の場合、万一、その情報システムがセキュリティ侵害を受け、顧客との取引データや残高情報が破壊・改竄されると、多くの利用者に甚大な被害をもたらすこととなる。そのため、金融機関は自らの情報システムのセキュリティを守ることが特別に強く求められているのであろう。

また、金融機関の場合、単にシステムを破壊・停止しようとする愉快犯からの攻撃に加えて、悪意を持って業務データを改竄する攻撃に備えなければならない。攻撃者は、金融機関の情報システムを不正に書き換えて、他人の財産を減らし、自分の財産を増やすような操作を行うかも知れない。正規の顧客に成りすまして取引を入力し、その財産を奪おうとするかもしれない[3]。時には金融機関の内部者が協力した攻撃という形態をとるかも知れない。攻撃が成功すると不正な利益を得ることができるというインセンティブが存在する場合、計画的、組織的な攻撃のリスクが高まる。金融機関は、そうした攻撃に特に注意して対策を検討しなければならない。

こうした観点に立った場合、インターネット・バンキングを提供する金融機関が最も重視しなければならないセキュリティ対策とは、インターネット・バンキングにおいて、正規の利用者からの資金振替指図などの指示を間違いなく実行すること、言い換えるならば、無権限者による成りすましなどの攻撃によって、正規の利用者や金融機関自身の財産が被害を受けないようにすることにあるのではないか。そのような効果を実現する上で鍵となるのは、インターネット・バンキングにおける利用者の認証方式と考えられる。そこで、以下では、この点にスポットを当てて分析を行うこととしたい。

３．インターネット・バンキングにおける利用者の認証方式を巡って

以下では、現在のインターネット・バンキングにおけるセキュリティ対策について、利用者の認証方式を中心に見ていくこととしよう。

インターネットを利用した金融取引がここ１、２年で急速に拡大した大きな

[3] 金融機関の正規の利用者に成りすまして取引を入力し、その財産を奪おうとした事例として、1994 年 12 月に発生した、ある都市銀行のファーム･バンキングのセキュリティ侵害事件が挙げられる。この事件の犯人グループは、当該銀行のファーム･バンキング・サービスに参加した上で、当該銀行の内部協力者から正規の取引先企業の暗証番号等を入手し、それらの企業に成りすましてファーム・バンキング端末から 16 億円を超える資金を不正に送金した。この事例は、インターネット・バンキングの安全性を検討する上でも参考となる。

理由のひとつとして、「利用者の認証方式が、利用者にとって手数の掛からない、簡便な方式に変更された」ことが挙げられる。1997 年以降、わが国の金融機関がインターネット・バンキングを導入し始めた頃は、セキュリティを高めるために、SET[4]や SECE[5]と呼ばれる比較的厳格な利用者の認証方式を実現する通信プロトコルを採用する先が多かった。利用者が SET や SECE を使うためには、金融機関が提供するソフトウエアをパソコンにインストールする必要があったほか、利用者一人一人について、認証サービス会社の提供する公開鍵証明書を取得し、それをシステムに組み込む必要があるなど、金融機関にとっても利用者にとってもコストと運用の手間が掛かるものであった。その複雑さ故に導入を諦める利用者も多く、複雑な認証方式の採用が、わが国においてインターネット・バンキングが普及しない理由のひとつとさえ言われていた。金融機関にとっても、そうした認証方式を利用している限り、ユーザー用ソフトの開発、配布や、公開鍵証明書の取得などにコストが掛かるため、高額の手数料が徴求できないのであれば、インターネット・バンキングを積極的には売り込みにくいと言われていた。

しかし、2000 年頃から、パソコン等に予め組み込まれている SSL[6]と呼ばれる暗号プロトコルとパスワードを組み合わせて認証を行うインターネット・バンキングのサービスが提供され始め、普及に弾みがついた。先行して SET や SECE を採用していた金融機関も、こぞって「SSL＋パスワード認証」に移行したため、現在では、殆どの金融機関のインターネット・バンキングが「SSL＋パスワード認証」によるものとなっている。「SSL＋パスワード認証」とは、「入力されたパスワードが通信経路上で盗聴されるのを防ぐために SSL の暗号通信機能を使う」という意味であり、利用者の認証そのものは、パスワードの一致のみを条件としている。

こうした動きに対しては、インターネット・バンキングのセキュリティが低下することを懸念する見方もある。実際のところ、この「SSL＋パスワード認

---

[4] SET（Secure Electronic Transactions）：VISA と MasterCard によって提案された、インターネット上で安全にクレジットカード決済を実施するための通信プロトコル。

[5] SECE（Secure Electronic Commerce Environment）：インターネット上で安全に金融機関口座を利用した決済を実施するための通信プロトコル。SET をベースに、富士通、日立製作所、NEC によって共同開発された。

[6] SSL（Secure Socket Layer）：Netscape 社が提唱する暗号通信、認証等のセキュリティ機能が付加された暗号通信プロトコル。

証」は、どの程度安全なのだろうか。例えば、従来のクローズドな利用環境で、CD/ATM を通じた預金の引出しや資金振替等が、磁気カードと 4 桁の暗証番号という認証手段で安全に利用されてきたことと対比すれば、SSL による暗号化とパスワードを組み合わせることにより、インターネット・バンキングの安全性が十分に確保できると言えるのだろうか。

ここで意識しなければならないのは、インターネット上で金融サービスを提供する場合、従来のクローズドな環境とは本質的に異なる脅威が存在するということである。以下では、実際に利用されているセキュリティ技術の概要を紹介するとともに、幾つかの攻撃法を想定して、インターネット・バンキングにおける脅威の具体的なイメージをつかむことにしよう。

（1）SSL の仕組みと安全性

まず、現在のインターネット・バンキングにおける認証方式の基盤として利用されている SSL の仕組みと安全性について見てみよう。SSL は、インターネット上で Web サーバーにアクセスする際に、暗号通信、サーバー認証、クライアント認証を実現するための暗号プロトコルである。Netscape Communicator や Internet Explorer といった無償で配布されているクライアント・ソフトに予め組み込まれている。一般の利用者にとっては、わざわざ自分のパソコンに新しいソフトウエアをインストールしなくても使用できるため、SSL は広く普及しており、インターネット金融取引においても広く利用されている。その基本的な仕組みは、図 1 のとおりである。

SSL の仕様書には、暗号鍵の生成、鍵交換、データの暗号化などの手順が、詳細に定められている。このうち鍵交換の手順については、最近の証明可能安全性を巡る研究などを踏まえると、やや古典的な技術が使われており、安全性が数学的に証明されている訳ではない。また、これまでのところ、SSL の安全性が信頼の置ける第三者機関によってきちんと評価された実績もない。SSL は、国際的に広く利用されている標準的な暗号プロトコルであるが、その利用に際しては、こうした安全性評価の現状をも考慮に入れておくことが望ましいと考えられる。

SSL の安全性を巡っては、①SSL の仕様書そのものに欠陥はないか、②仕様書の内容を実装した製品に欠陥はないか、という 2 つの観点から検討が必要となる。これまでのところ、①については、少なくとも最新版である SSL Ver 3.0 は問題が指摘されていないが、②については、問題点が顕現化した事例がいくつか知られている。

図 1　SSL による暗号通信の概要

クライアント		サーバー	概要
①交信要求メッセージ {ｸﾗｲｱﾝﾄ乱数､ｾｯｼｮﾝ ID、 利用可能認証方式ﾘｽﾄ等}	→→		ｸﾗｲｱﾝﾄからｻｰﾊﾞｰに交信を要求。乱数､ID、認証方式リスト等を送信。
	←←	②交信受諾メッセージ {ｻｰﾊﾞｰ乱数､ｾｯｼｮﾝ ID 利用認証方式等}	ｻｰﾊﾞｰが応答。乱数と ID を交換し､使用する認証方式等を決定。
		●ｻｰﾊﾞｰ公開鍵証明書 ●ｻｰﾊﾞｰ鍵交換情報 ●ｸﾗｲｱﾝﾄの証明書送付要求 ③送信完了メッセージ	ｻｰﾊﾞｰが、決定された認証方式に基づき、必要に応じて、ｻｰﾊﾞｰの証明書やｸﾗｲｱﾝﾄへの証明書送付要求を送信。
●ｸﾗｲｱﾝﾄ公開鍵証明書 ④ｸﾗｲｱﾝﾄ鍵交換情報 ●ｸﾗｲｱﾝﾄ公開鍵証明書検証データ	→→		ｸﾗｲｱﾝﾄが､必要に応じて証明書やその検証ﾃﾞｰﾀを送信し、鍵交換情報(ｻｰﾊﾞｰの公開鍵で乱数を暗号化したもの)を送信。
⑤暗号パラメータ交換 ⑥送信完了メッセージ			①②④で交換した乱数を組み合わせてｾｯｼｮﾝ鍵を生成し､事前に共有した乱数を暗号化してｸﾗｲｱﾝﾄから送信。
	←←	⑦暗号パラメータ交換 ⑧送信完了メッセージ	ｻｰﾊﾞｰも同様にｾｯｼｮﾝ鍵を生成した上で､事前に共有した乱数を暗号化して送信し､疎通を確認。
アプリケーションのデータ	◆▬▬◆	アプリケーションのデータ	交換されたｾｯｼｮﾝ鍵を用いて共通鍵暗号により暗号通信を実施。

○：必須項目、●：オプション項目

過去に発生した有名な例としては、1995 年 9 月に、Netscape Navigator Ver.1.2 における SSL の鍵生成部分の実装プログラムに問題点があることが指摘された事件が挙げられる[7]。当時、SSL をインフラとしてインターネット・バンキングのサービスを提供していた米国の銀行は、「SSL に欠陥あり」との報道を受けて、相次いでサービスの停止に踏み切った。この事件は、暗号技術の欠陥が金融機関の業務に大きな影響を及ぼしたという意味で、注目に値する事件

[7] この事件は、Netscape Navigator Ver.1.2 において、鍵生成プログラムに欠陥があり、暗号が容易に破られてしまうことが分かったというものであった。この事例では、善意の解析者が問題点を指摘したために､結果として個々の利用者の被害が未然に回避され､暫くして問題点を修正したプログラムが Netscape Navigator Ver.2.0 として配布されたことによって解決された。

であった。

最近発生した類似の事例としては、インターネット・バンキングを含む複数の電子商取引サイトについて、「クロスサイト・スクリプティング攻撃[8]」と呼ばれる攻撃法に対する脆弱性が指摘されたという事件が挙げられる[9]。これは、SSL の暗号プロトコルそのものの問題ではないが、利用者の個人情報やパスワードの送受信を SSL による暗号化で保護している実装環境においても、この脆弱性を利用してクッキー[10]の情報を奪取することによって、個人情報やパスワードが漏洩するリスクがあることが指摘されたものである。こうした指摘を受けて、インターネット・バンキングなどのシステム設計者は、こうした攻撃法の存在を意識した設計を行うことが必要となっている。

SSL は多くの機能を持つ暗号プロトコルであり、実際に実現する機能は、システム設計者が必要に応じて選択する。その選択によっては、比較的安全性の高い暗号通信とサーバー認証、クライアント認証を行うこともできるし、強度の弱い暗号通信しかできない場合もある。選択できる主なパラメータを整理すれば、表 1 のようになる。

表 1　SSL において選択できる機能と主なパラメータ

機　能	選択できる主なパラメータ
サーバー認証	公開鍵証明書あり／公開鍵証明書なし
クライアント認証	公開鍵証明書あり／公開鍵証明書なし
公開鍵暗号（鍵交換）アルゴリズム	RSA、Diffie-Hellman
公開鍵暗号の鍵長（法のサイズ）	1024 bit、768 bit、512 bit
共通鍵暗号アルゴリズム	トリプル DES、DES、IDEA、RC4、RC2
共通鍵暗号の鍵長	168 bit (トリプル DES)、128 bit (RC4、IDEA)、56 bit (DES)、40 bit(DES、RC4、RC2)

現在、SSL を用いて実用化されているインターネット・バンキングの例を見ると、サーバー認証、128 ビットの RC4 共通鍵暗号、1024 ビットの RSA 公開

[8] クロスサイト・スクリプティング攻撃： 攻撃者が攻撃対象のクライアントのブラウザに JavaScript などのスクリプト言語で書かれたコードを実行させ、他のサイトのサーバーからそのクライアントに関する情報を不正に攻撃者へ転送させるという攻撃。この事例も、善意の研究者が問題点を指摘することによって発覚したものであった。

[9] 高木、関口、大蒔［2001］は、わが国における 73 の電子商取引関連サイトのうち 56 サイトが、クロスサイト・スクリプティング攻撃に対して脆弱であるとの調査結果を報告している。

[10] クッキー（cookie）：サーバーがクライアントを識別し、過去のアクセス履歴等を把握するためにブラウザに送るデータ。

鍵暗号を利用しているケースが多いが、利用者側のクライアント認証に SSL を利用している例は皆無である。この場合、SSL は暗号通信機能しか提供しないこととなり、SSL が実現する通信経路の守秘によりパスワードの盗聴を防いだ上で、クライアント認証はパスワードを利用して行うこととなる。

（2）暗証番号・パスワード認証の問題点

現在のインターネット・バンキングで広く採用されている「SSL＋パスワード認証」においては、パスワードが一致すれば、正当な利用者からの入力と認識するという前提で、システムが構築されている。パスワードは最も基本的な認証方式であり、その信頼性は利用者によるパスワードの選定や管理に依存する。利用者が推定され易いパスワードを選択したり、適切な管理を怠ってパスワードを外部に漏洩させたりした場合、パスワード認証の安全性は確保することができない。また、システムの構成や運用管理方法によっては、総当たり攻撃や辞書攻撃によって破られるリスクもある。

「SSL＋パスワード認証」を利用している場合、これらのうちいずれかの理由でパスワードが漏洩したり、推定されたりしたときには、容易に不正アクセスが可能になる。そこで次に、暗証番号・パスワード認証に対する攻撃法について見てみることにしよう。

イ．暗証番号・パスワード認証に対する総当たり攻撃

現在のキャッシュカードで利用されている暗証番号は 4 桁なので、「0000」から「9999」まで、１万通りの番号を総当たりで入力して認証を通るかどうかを試せば、暗証番号を特定することが可能である。また、一般に暗証番号には記念日などの日付を使う人が多いと言われているため、月を 2 桁、日を 2 桁で表した 0101 から 1231 までの 365 通りの番号を試せば、更に効率良く攻撃することが可能な場合もある。パスワードは暗証番号に比べ、同じ桁数でも組合せの数が多いので総当たり攻撃はやや難しくなるが、利用者が記憶し易い単純な単語や固有名詞をパスワードとしている場合は、良く使われる単語を辞書から選び、次々に認証をパスするかどうかを試してみる攻撃が効果的である。この種の攻撃法に関する情報は、所謂ハッカーがネットワークに不正侵入するためのノウハウとして、インターネット上に掲載されていることも多く、攻撃を行うのに特別な技術は必要ないため、誰でも比較的簡単に実行できる。このため、ID とパスワード・暗証番号による認証だけでは、インターネットに接続されたシステムの安全性を守る上では十分ではないと考えられている。

従来、金融サービスを金融機関の店舗で提供している限り、このような脅威をあまり心配する必要はなかった。店頭の CD/ATM において、金融機関の職員や監視カメラなどが警戒する中では、暗証番号を何度も誤入力すると不審に思われ、すぐに検知されてしまうから、こうした素朴な手法を用いる攻撃者は殆どいなかった。また、暗証番号の入力を一定回数以上誤るとそれ以上の入力を受け付けないというシステム的な制限も設けられていた。

これに対し、インターネット上で同様の原理に基づき利用者を認証しようとした場合、脅威はより深刻なものとなる。インターネット経由であれば世界中どの端末からでもアクセスが可能であるから、店頭で CD/ATM を操作するときのような監視の目が行き届かない。暗証番号を手で入力するのではなく、スクリプト言語[11]等を利用してコンピュータに入力を指示すれば、連続して膨大な回数の攻撃を繰り返すことができる。もちろん、インターネット経由の取引においても、同一の ID に対して誤ったパスワード入力が繰り返されれば、それ以上の入力を受け付けないといったシステム的なガードが掛けられていることが普通である。しかし、パスワードを探索する際に、ID を固定せず、様々な ID とパスワードをランダムに組み合わせて数多くの探索を行った場合、「多くの利用者がたまたまパスワードを入力ミスした」という状態と区別がしにくいため、システム的なガードが働かない可能性がある[12]。このような探索では、特定の ID に対するパスワードを入手することは難しいが、全体としての試行回数を増やすことができるため、探索した数多くの ID のどれかひとつについて、パスワード認証を破り、成りすましを行うことができる可能性がある。

ロ．冗長な ID の利用による総当たり攻撃の防止

こうした攻撃を防止する手段のひとつとしては、ID の桁数を増やし、冗長性

---

[11] スクリプト言語：機械語への変換作業を省略して簡単に実行できるようにした簡易プログラムを記述するためのプログラミング言語。手間をかけずに実行することができ、一般のプログラミング言語に比べて機能は少ないが、習得が容易で記法も簡便であることが多い。代表的なものとして、Perl、VBScript、JavaScript などがある。

[12] ID とパスワードをランダムに変えて認証をパスしようとする攻撃をシステム的に防止するためには、例えば、インターネットからのアクセスを常時監視し、同一の IP アドレスから異なる ID で繰り返しアクセス要求があった場合に警告を発する、といった対応が有効かも知れない。ただし、そうした対応がとられたとしても、それを回避して攻撃を行うことは技術的に可能であり、新たな攻撃法の開発と対症療法の繰り返しとなる惧れが高い。こうした問題を抜本的に解決するためには、認証手段そのものの安全性を高めることが適当と考えられる。

を高めることが有効である。もし、ID を 1 番から連続して付番する、あるいは、利用者数との対比で最低限の桁数の ID を用いていた場合、攻撃者がランダムに発生させた数値がたまたま実際に利用されている ID と一致する確率が高い状況となる[13]。そして、仮にこうした攻撃で有効な ID とパスワードのペアが探索できれば、それを利用して真の利用者に成りすまし、不正な取引を入力することが可能となる。

実際のインターネット・バンキングに利用される ID が、全体の利用者数と対比して不必要と思えるほど長い桁数となっていることが多いのは、こうした攻撃を意識していることが一因と考えられる。例えば、預金者が 10 万人存在する金融機関において、10 万人に 5 桁（00000 番から 99999 番まで）の ID を順番に付与した場合、ランダムに発生した 5 桁の番号が ID として利用されている確率がかなり高いため、上記のような攻撃が容易に成立する。しかし、例えば、ID を 10 桁とし、そのうち上 5 桁は利用者毎に順次に付与し、下 5 桁はランダムな値を付与した場合、上記のような攻撃は実行が困難になる。ランダムに発生させた 10 桁の番号がたまたま ID として実際に利用されている確率は 10^{-5} 以下となり、攻撃者が上記のような試行錯誤を行うことが極めて非効率的になるからである。ただし、こうした効果を期待するためには、冗長性を付与する際に、攻撃者に推定できないランダムな ID を生成する必要がある。例えば、特定の桁が特定の数値に固定されている、あるいは ID の分布範囲が限定されている場合、攻撃者が冗長性を再現できるので、攻撃を抑止する効果が期待できなくなるからである。

（3）乱数表によるチャレンジ･レスポンス方式

（2）で述べたように、インターネット上で公開されているシステムへのアクセスを、パスワードや暗証番号だけで認証することにはリスクが大きい。特に、パスワードによる認証だけでインターネットからの資金振替指図の入力が

---

[13] 類似の事例として、携帯電話に対してランダムに送信される「迷惑メール」への対策が参考となる。迷惑メールとは、携帯電話のメールアドレスのうち、電話番号に該当する 8 桁の数字部分にランダムに発生させた数字を当てはめる等の方法によって、無差別に発信される営利等を目的とした電子メールである。こうした行為は、ランダムに発生させた数字と実在する電話番号が一致する確率が比較的高いからこそ成立する。携帯電話会社では、迷惑メールの着信を回避する対策のひとつとして、携帯電話のメールアドレスに電話番号のほかにランダムな 4 桁の番号（シークレット・コード）を付加して冗長性を高め、ランダムに発生させた数字が偶然に電話番号と一致する確率を下げることを推奨している。

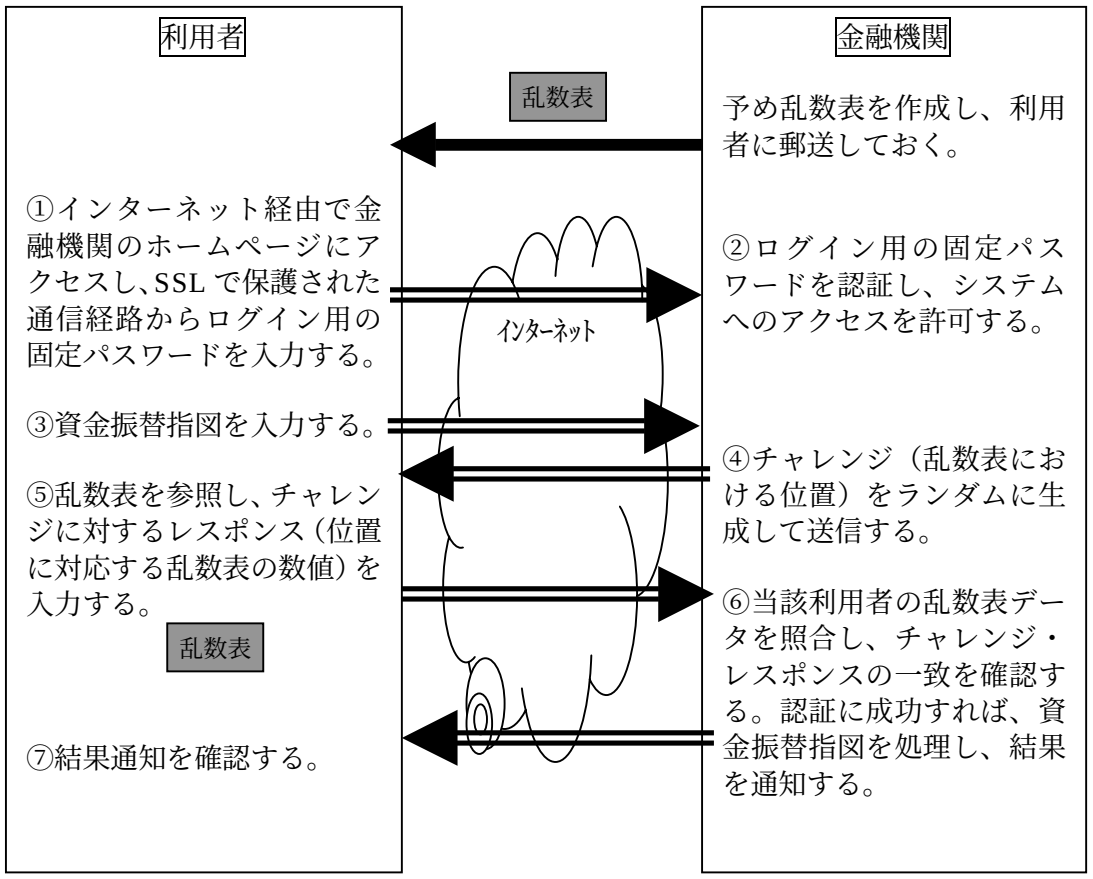
可能な場合、正規の利用者が成りすましによる不正送金の被害を受ける惧れがある。こうした問題に対処するために、最近のインターネット・バンキングでは、認証手段を二重化し、ログイン用のパスワードに加えて、特に重要な操作における認証手段として「乱数表[14]によるチャレンジ・レスポンス方式」を導入する先が増えてきている（図 2 参照）。この認証方式は、各金融機関が、予め利用者毎にランダムな数値を記載した乱数表を作成して利用者に配付しておき、資金振替指図の入力など、特にセキュリティの要請が高い局面で、その表の中の位置情報をランダムに質問し（この質問を「チャレンジ」という）、それに該当する数値を応答させる手法である（この応答を「レスポンス」という）。

例えば、ある金融機関のインターネット・バンキングでは、①～⑯までの枠に 16 個の数値（各々は 0 から 9 までの整数）が書かれた乱数表を利用者に郵送しておき、資金振替指図等を入力する都度、その中の 4 つの位置をランダムに（例えば、⑤⑬⑨①などと）指定して、各位置の数値（例えば、⑤=3、⑬=1、⑨=8、①=0 などと）を答えさせる、という認証方法を採用している。この場合、「⑤⑬⑨①」という質問が「チャレンジ」であり、「3、1、8、0」という回答が「レスポンス」となる。チャレンジは認証を行う都度異なる値をとるため、利用者は乱数表を参照して、それに対するレスポンスを作成することになる。

また別の金融機関では、5×5 の桝目の中にランダムに各々2 桁の数値が書かれた乱数表を利用者に郵送しておき、資金振替指図等を入力する都度、１つの桝目の位置をランダムに（例えば、3 行 2 列目などと）指定して、そこに記載されている 2 桁の数値（例えば、47 などと）を答えさせる、という認証方法を採用している。この場合、「3 行 2 列目」がチャレンジであり、「47」がレスポンスとなる。乱数表のフォーマットやチャレンジの出し方は区々であるが、インターネット・バンキングを提供している多くの金融機関において、単純な固定パスワードに変えて、このような認証方法が導入されている。

[14] ここで説明している「乱数表」は、金融機関が、「ID カード」、「お客様カード」、「ご契約カード」、「確認番号表」等と呼称しているものであるが、通称として良く利用されている表現であるため、以下では「乱数表」と呼ぶこととする。

図 2　乱数表によるチャレンジ･レスポンス方式を利用した
インターネット･バンキングの事務フローの例



イ．乱数表によるチャレンジ･レスポンス方式の有効性を検討する視点

こうした「乱数表によるチャレンジ・レスポンス方式」は、取引の都度、異なる暗証番号を利用することになるため、固定パスワードを利用するのに比べれば随分安全であるような印象を受ける。万一、入力した番号が盗聴されるか、当てずっぽうで入力した番号が認証をパスしても、次の取引で同一のチャレンジが出されない限り、盗聴・検知された番号では認証をパスしないという効果が期待できるからである。また、この方式は、利用者側に特別なハードウエアやソフトウエアを導入する必要がないため、取引の都度、乱数表を参照させること以外、利用者に特別な負担を掛けなくて済み、普及させ易いというメリットもある。しかし、インターネット・バンキングの認証方式として、乱数表が安全性をどの程度高めているのかは明確ではなく、追加的なセキュテリィ対策

としてどこまで信頼して良いか、その評価が難しい面がある。

むしろ、乱数表を導入することによって、逆にリスクを高めている部分があることにも注意が必要である。例えば、乱数表は金融機関が利用者毎に作成して郵送するものであるため、利用者がオンラインで随時変更できるパスワードとは異なり、作成、搬送のプロセスで秘密が漏洩するリスクがある[15]。また、ある程度長い期間、同一の乱数表が利用され続けることが想定されており[16]、秘密情報が漏洩した場合のリスクも、利用を継続する期間に応じて高くなる。乱数表が利用者の手に渡った後も、パスワードのように情報を記憶しておく訳にはいかないため、乱数表を手元に保管しておく必要があり、かえって盗難・紛失・盗み見のリスクが高くなる。乱数表には、これらのデメリットを補って余りあるようなインターネット・バンキングの安全性向上の効果があるのだろうか。

元々、乱数表によるチャレンジ･レスポンス方式は、通常の電話機から暗証番号を入力する「テレホン・バンキング」で利用されていたものであった。暗号通信を行わないテレホン・バンキングの場合、通信内容が秘匿できるとは限らない[17]ため、通常の暗証番号ではなく、取引毎に異なる番号を入力する仕組みが開発されたという経緯がある。しかし、通信内容が漏洩することを前提と考えるならば、このような乱数表を利用したとしても安全とは言い切れない。16～100 個程度の数値の記載された乱数表を金融機関と利用者との間で秘密に共有しただけでは、何回か利用しているうちに一度利用した秘密情報を再度利用せざるを得ず、乱数表の内容を推定され、正規の利用者に成りすまされるリスクがあるからである。以下では、このような乱数表による認証に対し、どのような攻撃が想定されるか、具体的に検証してみよう。

---

[15] 多くの金融機関では、書留郵便の利用や、郵送途上で乱数表を不正に覗き見ようとすると利用者に検知できるような特殊な包装手法を用いること等により、情報漏洩を防止しようとしているが、リスクを完全に回避できる訳ではない。

[16] 乱数表を導入している金融機関の多くでは、乱数表の定期的な更新は想定されていないようである。乱数表が盗難に遭うか、その内容が他人に露見した場合は、利用者からの依頼により再発行が可能な仕組みとなっている。しかし、利用者が気付かないうちに内容を盗み見られていた場合、当該乱数表は、無権限者からのアクセスのリスクを抱えながら利用され続けることになる。

[17] 例えば、ある種のコードレス電話は盗聴のリスクがあることが知られている。

ロ．乱数表によるチャレンジ･レスポンス方式に対する攻撃①：漏洩した通信情報を利用する攻撃

まず、16 個の数値が記載された乱数表を利用し、4 つの数値を答えさせる認証方法において、通信情報が漏洩したケースを考える。通常、送受信される乱数表の情報は SSL によって暗号化されているが、何らかの理由で１回分の利用者とのやり取りが漏洩して、16 個中 4 個の位置と数値が攻撃者に察知されたとしよう。固定パスワードであれば、１回分の通信情報が漏洩した時点で成りすましが可能となるが、乱数表を利用している場合、攻撃者が成りすましを行おうとしても、ランダムに表示されるチャレンジがたまたま漏洩した 4 個の数値と一致しない限り（その確率は 1/1820 にすぎない[18]）、正しいレスポンスを返すことができないため、一見、安全性にさほど問題は生じないように見える。これが、乱数表を利用することのメリットと考えられている。

しかし、もしも金融機関側のシステムが、攻撃者にとって都合の良い値が出るまで、「チャレンジの出し直し」をさせることができる作りであった場合、問題が発生する。こうした認証方式では、通常、暗証番号を試行錯誤的に入力する攻撃を回避するために、「チャレンジに対するレスポンスの入力エラーは３回以内」などといった制限を設け、制限値を超えると入力を規制するといった仕組みを採用することが多い。しかし、「チャレンジを表示させる回数」については、制限を設けていないシステムが存在するようである。そうしたシステムの場合、攻撃者は、不都合なチャレンジであればそれに応答しないで入力をキャンセルし、次のチャレンジを表示するよう依頼することにより、自分が正答できるチャレンジが表示されるまで、何度もチャレンジを表示させるという攻撃が可能となる。チャレンジがランダムに作成されると仮定すれば、平均的にみて、1261 回チャレンジの再表示を依頼し続けると、1/2 の確率で正答可能なチャレンジが表示されると期待できる[19]。

同一の乱数表について複数回の情報漏洩が発生し、攻撃者が 4 個を超える数値を知っていた場合[20]、より少ない回数の再表示要求で、正答可能なチャレンジ

---

[18] 16 個の乱数から 4 個を選ぶ組合せは(16×15×14×13)／(4×3×2×1)=1820 通りあるため。

[19] $(1-1/1820)^{1261} \fallingdotseq 0.5$。

[20] 複数回の情報漏洩が発生した場合、攻撃者が入手できる乱数表上の数値の数は、重複の可能性があるので確定しない。平均的に言えば、通信情報の漏洩が 2 回なら 7 個、3 回なら 9 個程度の数値が察知されることとなる。

を表示させることが可能となる（表 2 参照)。例えば、9 個の数値を知っていれば、10 回の再表示依頼で正答できるチャレンジを表示させることができる。

表 2　16 個の数値の書かれた乱数表から 4 桁を指定して答えさせる認証方式において、すべて正答できるチャレンジを表示させるための平均的な再表示依頼回数

攻撃者が知っている数値の数	4 個	5 個	6 個	7 個	8 個	9 個	10 個	11 個	12 個	13 個
平均的な再表示依頼回数	1261 回	252 回	84 回	36 回	18 回	10 回	6 回	3 回	2 回	1 回

同様の計算により、「5×5 の桝目の中にランダムに各々2 桁の数値が書かれた乱数表」において、１つの桝目の情報が漏洩した場合、平均的にみて、17 回チャレンジの再表示を依頼すると、1/2 の確率で正答可能なチャレンジが表示されることが期待できる[21]。

実際に提供されているインターネット・バンキングのシステムの作りをみると、こうした攻撃を意識して設計されたと思われるシステムでは、チャレンジの再表示依頼を暗証番号入力と同等の操作と認識し、再表示を繰り返させるとセキュリティ侵害と判断してそれ以上の入力を受け付けなくなる仕組みとなっている。こうした対策を講じていれば、万一乱数表の情報の一部が漏洩しても、それが悪用されることはある程度防止できる。これに対し、こうした仕組みがとられていないシステムでは、認証１回分の情報が漏洩すると攻撃が可能となり、乱数表によるチャレンジ・レスポンス方式のメリットが活かされない結果となる。

ハ．乱数表によるチャレンジ･レスポンス方式に対する攻撃②：総当たり攻撃

ロ．で紹介した攻撃は、１回分の認証情報が攻撃者に漏洩するという前提からスタートするものであった。この前提については、「SSL を使って暗号通信を行っているのだから、情報漏洩することを前提とするのはおかしい」といった反論が可能かもしれない。しかし、システムの仕組みによっては、SSL を破ったり、利用者の不注意に付け込んだり、金融機関内部者の協力に頼ったりしなくても、類似の攻撃が可能となる可能性がある。以下では、特別な情報漏洩等を前提としないで、総当たり攻撃によって乱数表を利用した認証方式を破ることができないか、調べてみよう。

[21] $(1-1/25)^{17} \quad 0.5$。

そもそも、どのような乱数表を利用するにせよ、実際に利用者が認証のために入力するデータが 2 桁とか 4 桁の数値だとすれば、「当てずっぽうで入力した数値がたまたま一致する」ことによるセキュリティ侵害を排除することは難しい。例えば、先に検討した「16 個の数値の記載された乱数表から 4 つの数値を答えさせる認証方式」において、攻撃者が何回でも暗証番号を試行錯誤して入力できると考えた場合、毎回ランダムに表示されるチャレンジに対し、約 7000 回、当てずっぽうで暗証番号を入力すると、1/2 の確率で認証にパスすることが期待できる[22]。そして、一旦認証をパスすると、乱数表のうち、その認証に利用されたデータ 4 個分の位置と数値は露見してしまう。そうして得られた乱数表の一部の情報を手がかりに更に試行を続ければ、容易に探索を進めることができる。例えばチャレンジとして示された 4 か所のうち、3 か所の数値が既に知られていた場合、残りの 1 か所の数値を当てずっぽうで入力すれば、1/10 の確率で認証をパスできる可能性があるからである。平均的に見て、4 個分の情報を知っていて 5 個目を探索するためには 130 回、6 個目を探索するためには 70 回の試行を行えば、1/2 の確率で、追加的な乱数表の情報を得ることができる。そして、乱数表に対する一定量の情報を集めることができれば、イ．で紹介した手法により、成りすましによる攻撃が実行できる可能性がある。

もちろん、このような大量の試行錯誤を行おうとすると、認証エラーの制限値を超えてしまい、それ以上の入力が制限されることになるため、このような攻撃をそのまま実行することは難しい。しかし、（２）で示したように、大量の ID を用意し、試行１回毎に ID を変更するような攻撃が可能であれば、特定の利用者に認証エラーが頻発していることを露見させないようにすることができるかもしれない。その場合、認証エラーの制限値が大きい、寛容なシステムであるほど、大量の試行錯誤が可能になる結果、全数探索に対して脆弱となる[23]。乱数表による認証を採用する場合、こうした攻撃の可能性をも意識して、システム設計を行う必要があるだろう。

---

[22] 4 桁の暗証番号が偶然一致する確率は 1/10000。$(1-1/10000)^{7000} \fallingdotseq 0.5$。なお、入力させるのが 2 桁の数値の場合、偶然一致する確率は 1/100 となり、$(1-1/100)^{70} \fallingdotseq 0.5$ より、70 回程度の試行で乱数表の一部を推定することが期待できる。

[23] このため、認証エラーにどのように対応するかが、システム設計のポイントとなる。ただし、闇雲に制限値を小さくすると、利用者の利便性を損ねるほか、故意に認証エラーを発生させてサービス停止を狙う攻撃を受け易くなる可能性があり、注意が必要である。

ニ．乱数表によるチャレンジ･レスポンス方式に対する一応の評価

以上の分析により、現在のインターネット・バンキングで広く利用されている「乱数表によるチャレンジ・レスポンス方式」は、チャレンジの表示方法や認証エラー発生時の処理、ID の冗長性などの設定次第では、情報の一部が漏洩した場合に成りすましの攻撃を受けるとか、乱数表の情報の一部が推定されるといったセキュリティ侵害のリスクが存在することが分かった。

ログイン用のパスワードに追加する認証手段として考えた場合、この方式は、利用者が自由に設定・変更できる通常の固定パスワードと比べ、どの程度優れていると言えるのだろうか。情報漏洩時の耐性は乱数表によるチャレンジ･レスポンス方式の方が優れているものの、それは完全なものではない。乱数表によるチャレンジ･レスポンス方式では、チャレンジのとり得る範囲が限られており、何度か通信を繰り返すうちに同一のチャレンジが利用される可能性が高まるため、実装環境によっては、固定パスワードと同程度の安全性しか達成できないことが有り得る。イ．で紹介した、乱数表がそもそも持つデメリットと考え合わせると、両者を比較しても、明らかな優劣は付けられない。少なくとも、固定パスワードに代えて乱数表によるチャレンジ･レスポンス方式を導入することで、安全性が著しく高まると評価することはできないと思われる。

この点、これまでに開発されてきたインターネット上のクライアント認証に利用可能な認証方式の中には、固定パスワードと比べて、成りすましや秘密情報の推定に対し、より高い安全性を確実に達成し得ると考えられる方式も存在している。「ワンタイム・パスワード」と呼ばれる認証方式も、その一例である。同方式では、現在の時刻や取引１件毎に増加するカウンタ値等を基に、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。ただし、同方式の利用には、クライアント側に専用のハードウエアが必要となる。

４．今後のインターネット・バンキングにおける利用者の認証方式のあり方

本稿では、最近利用が拡大しているインターネット・バンキングにおけるセキュリティ対策、特に、SSL、パスワード、乱数表を組み合わせた利用者の認証方式の安全性を評価するために、具体的な攻撃法について検討してみた。その結果、現在の認証方式にはセキュリティ侵害のリスクが存在し、金融機関がシステムを運用していく上で、そうしたリスクに留意していく必要があることが分かった。インターネット・バンキングを提供している金融機関は、自らのシ

ステムが、本稿で紹介したような基本的な攻撃法に対して十分な耐性を持っているかを確認しておく必要があると考えられる。そして、将来的には、インターネットを利用して提供される金融サービスにおいて、成りすましを有効に防止するために、デジタル署名、バイオメトリクス、IC カードのような、技術的にその有効性が検証されてきた認証方式を利用していくことが必要とされるようになると考えられる。

しかし、インターネット・バンキングの認証方式が、SET や SECE から「SSL＋パスワード認証」に移行したプロセスを考えると、利用者に負担を掛けてまで、専用のソフトウエアやハードウエアを必要とする認証方式を導入することは、現実的ではないように思われる。少なくとも、利用者側が、セキュリティを高めることの意義を認め、導入に協力し、費用を負担するといった状況とならない限り、金融機関側のイニシアティブで普及を図ることは難しいと考えざるを得ない。しかし、現在のままの認証方式ではセキュリティ侵害のリスクが存在し、そうしたリスクがインターネット・バンキングの普及の障害となることも考えられる。

今後、インターネット・バンキングのセキュリティをより信頼できるものに移行させて行くためには、どのようなシナリオを想定すれば良いのだろうか。ひとつのシナリオは、金融機関の発行するキャッシュカードの IC カード化に合わせて、キャッシュカードをインターネット・バンキング用のハードウエア・トークンとして利用する、という構想である。IC カードのような耐タンパー性と計算力を有するハードウエア・トークンを利用者のパソコンから利用できれば、インターネット経由でも、極めて強力な認証方式を利用できる。IC カード内にデジタル署名用の署名鍵を格納し、金融業界が提供する PKI による公開鍵証明書を利用できるようにした上で、インターネット・バンキングで資金振替指図等を入力する際に、電文にデジタル署名を付与する方式が有力であろう。

問題は、そのような機能を実現するためには、利用者側のパソコンに IC カード・リーダーを装備させ、専用のソフトウエアをインストールさせる必要があるという点である。インターネット・バンキングを安全に実施するためだけに、利用者にそのような負担を要請することは現実的ではないだろう。しかし、安全なデジタル署名を生成するためのハードウエアとソフトウエアを整備することにより、インターネット・バンキングだけではなく、電子政府や電子商取引を安全に利用できるようになるとすれば、事情は異なってくる。利用者は、そのような幅広い分野で利便性を享受できるとすれば、喜んでセキュリティ確保

に必要な環境を整備するようになるかもしれない。そのようなシナリオを実現するためには、ある程度汎用的に利用できるセキュリティ機器を広く普及させるとともに、多くのサービスに同一のシステムを利用できるよう、インターネットを利用した様々なサービスの提供者が協力していくことが大切であろう。

５．おわりに

インターネット・バンキングの設計に当たっては、①利用者のニーズに合致したサービスが提供可能か（利便性）、②利用者に受け入れられるコストで提供可能か（効率性）、③成りすまし等のセキュリティ侵害のリスクが十分に低いか（安全性）、といった基準をバランス良く実現しようとするのが一般的である。ところが、これらの基準のうち「安全性」は、「利便性」、「効率性」とはトレードオフの関係となることが多く、また、中長期的な観点から評価することが難しいため、一般に、システム提供者はそのリスクを過小に見積り易い傾向がある。しかし、仮に将来、「安全性」が十分でないインターネット・バンキングが広く普及した後で大規模なセキュリティ侵害が発生した場合、単にシステム提供者が損害を被るだけではなく、決済システム全体の安定性が大きく損なわれることにもなりかねない。今回指摘したインターネット・バンキングのセキュリティ技術に関する問題点についても、このような観点から十分に検討される必要がある。

本稿で紹介した攻撃法はあくまでも理論的なものであり、インターネット・バンキングの認証方式を実際に破るために適用可能か否かが確認された訳ではない。多くの金融機関では、本稿で紹介した脅威についても考慮した上でシステムを構築・運用していると考えられるため、例えば、暗証番号を試行錯誤により全数探索しようとすることは、現実には実行困難なケースが多いと考えられる。また、仮にシステムの仕様上、何らかのセキュリティ・ホールが放置されており、本稿で示した攻撃が可能な作りとなっていたとしても、現状ではインターネット・バンキングの利用者がまだ一部に止まっているため、大量の利用者と大量の取引が存在することを前提とした攻撃を無理に実行しようとすると、金融機関に察知される可能性が高いと考えられる。しかし、今後、インターネット・バンキングの利用者数や取引量が増加してくると、攻撃がより容易に実行できるようになる可能性は否定できない。わが国の金融機関が、インターネットによる金融サービスを更に拡大していくに当たっては、こうしたセキュリティ上の問題点に適切に対処していくことが必要とされていると言えよう。

現在のインターネット・バンキングの安全性を巡る問題は、金融機関が採用

する情報セキュリティ対策について、何らかの公的な介入を行うことを正当化するものだろうか。仮に、有効な安全性基準やガイドラインを作成することが可能であれば、それもひとつの解となり得よう。しかし、インターネット・バンキングのセキュリティ技術の基礎となっているインターネット技術や暗号技術の進歩の速さを考えると、現時点において、公的当局がア・プリオリに固定的な規制やガイドラインを設けることは合理的でない可能性が高い。インターネット・バンキングは、様々な局面でセキュリティ侵害のリスクに晒されており、僅かなセキュリティ・ホールが重大な被害に繋がることがあり得る。たとえ、採用する認証方式に関する規制やガイドラインをある程度厳格に定めたとしても、それがシステム全体の破綻を生じさせないために十分なものであることは保証できない。そればかりか、固定的な規制やガイドラインが、むしろ民間におけるセキュリティ技術の進歩を阻害する懸念の方が大きいと思われる。

従って、現時点での現実的な対応としては、民間企業の技術者、学者、公的当局が密接に連携しあい、考えられるセキュリティ技術とそのリスクについて理解を深めていくとともに、望ましいインターネット・バンキングの認証方式に関する共通認識を醸成していくことが重要であろう。

【参考文献】

宇根正志、「金融分野における PKI：技術的課題と研究・標準化動向」、第 4 回情報セキュリティシンポジウム提出論文、日本銀行金融研究所、2002 年 2 月

金融情報システムセンター、「金融機関業務のシステム化に関する動向調査」、『金融情報システム』No.250、2001 年 11 月

齊藤真弓、「RSA 署名方式の安全性を巡る研究動向について」、第 4 回情報セキュリティシンポジウム発表論文、日本銀行金融研究所、2002 年 2 月

高木浩光、関口智嗣、大蒔和仁、「クロスサイト・スクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」、『コンピュータセキュリティシンポジウム 2001 論文集』、pp.247-252、情報処理学会、2001 年 10 月

日本銀行、「金融機関における情報セキュリティの重要性と対応策――　インターネットを利用した金融サービスを中心に　――」、2000 年 4 月

松本勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」『金融研究』第 18 巻第 2 号、pp.17-31、日本銀行金融研究所、1999 年 4 月

――・――、「金融業務と認証技術：インターネット金融取引の安全性に関する一考察」、『金融研究』第 19 巻別冊第 1 号、pp.1-14、日本銀行金融研究所、2000 年 4 月

――・――、「情報セキュリティ技術の信頼性を確保するために」、『金融研究』第 20 巻第 2 号、pp.21-32、日本銀行金融研究所、2001 年 4 月

Ross Anderson, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, John Wiley & Sons, Inc., 2001.

Federal Financial Institutions Examination Council, *Authentication in an Electronic Banking Environment*, July 30, 2001 (www.ffiec.gov/pdf/pr080801.pdf).

Alan O. Freier, Philip Karlton and Paul C. Kocher, *The SSL Protocol Version 3.0*, November 18, 1996.