■11 群（社会情報システム）－ 7 編（金融情報システム）

3 章 インターネット・バンキングのセキュリティ

（執筆者：岩下直行）［2009 年 3 月 受領］

■概要■

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．特に，インターネット経由で，銀行預金の残高確認や振替を行うインターネット・バンキングと呼ばれるサービスは，現在ではほとんどの銀行によって提供されるようになっている．

インターネット・バンキング以前の我が国の金融業界におけるコンピュータ・システムのセキュリティ対策は，オンライン・システムの障害による業務の停止を防ぐための様々なバックアップ手段や，重要なデータに関する物理的なアクセス制御に重点が置かれており，通信の暗号化やディジタル署名といった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．機密漏えいや情報改ざんについては，専用線を利用したクローズドなネットワークであることを前提に，特殊な技術を導入しなくても防止できるという考え方が主流であった．

しかし，インターネットを利用して金融取引を行うようになると，そうした前提は崩れる．インターネット・バンキングの導入を進める過程で，我が国の金融機関は，それまで経験しなかったセキュリティ上の課題に直面し，対応を迫られることになった．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．我が国の金融機関は，試行錯誤を繰り返しながら，脅威に対抗する対策を導入するようになった．インターネット・バンキングの利用の裾野が広がるにつれて，不正取引の被害も増加傾向にあるが，現在までのところ，被害金額などからみたインパクトは，他の犯罪類型と比較して，なお限定的なものに止まっている．それはこうした金融機関の努力の奏効による面が大きいと考えられる．

本章では，金融分野で利用される情報セキュリティ技術を研究する立場から，インターネット・バンキングにおける顧客保護のための安全対策について検討する．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，無権限者によるな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うえで鍵となるのは，インターネット上での利用者の認証方式である．そこで，本章では，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する．

【本章の構成】

本章では，3-1 節で過去の金融情報システムと比較したインターネット・バンキングの特殊性について説明する．3-2 節では，インターネット・バンキングの認証方式の変遷をたどり，どのようにセキュリティ対策が高度化されてきたのかを述べる．3-3 節では，今後のインターネット・バンキングにおけるセキュリティ対策のあり方について述べる．

■11 群 － 7 編 － 3 章

3-1 インターネット・バンキングの特殊性

（執筆者：岩下直行）［2009 年 3 月 受領］

3-1-1 インターネットを利用した金融サービスの「守りにくさ」

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，従来，金融機関が利用してきたクローズドなネットワークとは本質的に異なる．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，脅威に対する適切な対策を講じておく必要があるといわれる．それでは，インターネットを利用した金融サービスは，それ以前の金融機関の対顧客サービスと比べ，具体的にどのような意味で特殊なのだろうか．サービスを提供する金融機関の側からみれば，次にあげるようないくつかのポイントについて，「システムの守りにくさ」を指摘することができる．

① 外部から「見える」システムであること：同じ対顧客取引でも，ATM による預金取引システムが顧客側からは中身の見えないブラックボックスであるのに比べ，金融機関のウェブサイトに設けられた顧客とのインタフェース部分のシステムは万人に公開されているため，誰でも解析ができてしまう．仮に，開発したシステムに潜在的な欠陥があった場合，攻撃者側がそれを知ったうえで，弱点を突く形で攻撃されるおそれがある．

② 脆弱な顧客所有 PC に依存していること：過去のファーム・バンキングなどでは，専用端末や専用ソフトを利用させることで利用者側のシステムに一定の枠をはめることができたが，現在のインターネット・バンキングは顧客が所有する 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．顧客の IT リテラシィは千差万別であり，不適切な使い方をされることを完全には防止できない．

③ 遠隔地からの攻撃を受けやすいこと：攻撃者は，世界中どこからでも，正体を明かさずに金融機関のサーバにアクセスすることができる．パスワードの全数探索などのためにシステム的に大量の試行を繰り返しさせることも容易であり，不正行為の監視が難しい．

3-1-2 金融機関は何を守らなければならないか

次に，このような「守りにくい」環境において，金融機関は，どのようなセキュリティ対策を講じることが期待されているのだろうか．通常，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」と位置づけられている．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，金融機関が特別に高いセキュリティを必要とするというのは自明なことではない．

インターネット・バンキングを提供する金融機関は，自らのホームページで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．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，アクセス状態を 24 時間常時監視していることなどが説明されている．こうしたセキュリティ対策を充実させること自体は，金融機関にとっては当然なことであり，利用者から信頼されるためには，それを適切に説明していくことも必要である．

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というわけではない．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，ほかの企業の顧客情報とさほど異なるものではない．ウェブサイトの改ざんなどによる風評被害やサービス停止攻撃の影響も，ほかの業種と同程度の脅威と考えられる．金融機関が実際に採用しているネットワーク・セキュリティ対策は，汎業界的な技術として確立されているものばかりであり，金融用途向けの特別な技術を採用しているわけではない．

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，その情報システムのなかに管理用データが格納されている，という特性によるものであろう．例えば，製造業であれば，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・改ざんされると，多くの顧客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る．

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，悪意をもって業務データを改ざん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，自分の財産を増やすような操作を行い，あるいは正規の顧客になりすまして取引を入力し，その財産を奪おうとする．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こともある．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，正規の顧客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，無権限者によるな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といえる．そのような効果を実現するうえで鍵となるのは，インターネット・バンキングにおける利用者の認証方式である．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．

■11 群 － 7 編 － 3 章

3-2 インターネット・バンキングの認証方式の変遷

（執筆者：岩下直行）［2009 年 3 月 受領］

3-2-1 SET/SECE の時代

我が国において初めてインターネット･バンキングが導入されたのは 1990 年代の後半であるが，当初はあまり普及しなかった．金融機関は，インターネット経由で攻撃を受けることを警戒して，SET や SECE 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していた．利用者が SET や SECE を使うためには，銀行が提供するソフトウェアを PC にインストールする必要があったほか，利用者一人一人が公開鍵証明書を取得する必要があるなど，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かかるものであった．その複雑さゆえに導入を諦める利用者も多く，複雑な認証方式の採用が，我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一つとさえいわれていた．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・バンキングを普及させることは難しいといわれていた．

3-2-2 「SSL＋パスワード認証方式」の時代

2000 年頃から，パソコンなどにあらかじめ組み込まれている SSL 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．「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する「一要素認証」であった．

ところが，その後，この認証方式によるインターネット・バンキングが普及するにつれ，不正預金引出の被害が報告されるようになった．利用者のパソコンに仕掛けられたキー・ロガーやスパイウェアによってログイン ID やパスワードが盗み出され，不正な送金が行われてしまったのである．この方式は，キー・ロガーやスパイウェアなどの手口が現れる以前に導入されていたものであり，新しい脅威を防ぎ切れなかったものといわざるを得ない．

そもそも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．利用者が推定されやすいパスワードを選択するとか，キー・ロガーやスパイウェア，フィッシングなどの攻撃を受けてしまうなど，適切な管理を怠ってパスワードを外部に漏えいさせた場合，パスワード認証の安全性は確保することができない．

3-2-3 「乱数表によるチャレンジ・レスポンス方式」の時代

キー・ロガーやスパイウェアによる犯罪の増加と利用者の不安の高まりを受けて，「SSL＋パスワード認証」方式の抱える問題を回避するため，「二要素認証」を導入する動きが強まった．そこで主流となったのは，従来の固定パスワードによる認証に加え，「乱数表によるチャレンジ・レスポンス方式」を採用するというものであった．これは，各金融機関が，あらかじめ利用者ごとにランダムな数値を記載した乱数表を作成して配付しておき，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，その表のなかの位置情報をランダムに質問し，それに該当する数値を応答させる方式のことである（**図 3･1**）．乱数表のフォーマットや質問の仕方は区々であるが，この方式は，現在でもインターネット・バンキングの認証方式として広く利用されている．

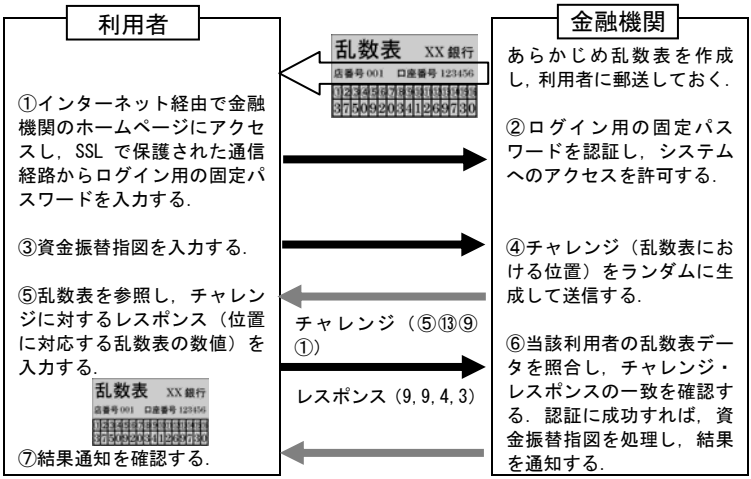

図 3・1　乱数表によるチャレンジ･レスポンス方式の例

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ェアやソフトウェ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かけなくて済み，普及させやすいというメリットもある．

しかし，この方式にも問題点がある．実装の仕方によっては，認証データが 1 回漏えいしただけでなりすましが可能となってしまう危険性があることや，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，乱数表のデータを推定できてしまうといった危険性が指摘されている [1]．一見複雑なので錯覚しがちだが，高々数十個の数字列を反復利用しているだけなので，固定パスワードよりも飛躍的に安全性が高まるわけではないのである．

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，乱数表は銀行が利用者ごと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えいするリスクがある．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，秘密情報が漏えい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．

3-2-4 ワンタイム・パスワードの登場

こうした指摘を踏まえて，乱数表に代わる認証方式として一部で導入が進められているのが，ワンタイム・パスワードである．内部のデータを読み出したり改変したりする攻撃に対して耐性を有している専用ハードウェア・トークンを利用する方式や，携帯電話にソフトウェアを組み込んで利用する方式がある．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，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暗号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．

ワンタイム・パスワードは，リモート端末からコンピュータ・システム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きたもので，その信頼性は高い．導入のコストは高いものの，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，極めて高い安全性を達成し得ると考えられている．

しかし，この方式も完ぺきとはいえない．例えば，トークンや携帯電話が盗用されたり，内部が解析されて秘密鍵が漏えいしたりして，パスワードが不正に入力されてしまうリスクがある．さらに，利用者の PC がスパイウェアなどに汚染されていた場合，入力された正規のパスワードを用いて，利用者の意図しない預金振替を指示するといった攻撃が存在する．この攻撃は，どのような認証方式を採用したとしても原理的に回避できない．利用者に，自らの PC がスパイウェアに感染しないように対策を講じて貰うことが必要である．

3-2-5 SSL に利用された暗号技術の安全性

これまで説明してきたインターネット・バンキングにおける認証方式の多くは，基盤として SSL（Secure Socket Layer）の仕組みを利用している．SSL の安全性を巡っては，①SSL の仕様（暗号鍵の生成，鍵交換，データの暗号化などの手順）そのものに欠陥はないか，②仕様を実装した製品に欠陥はないか，という二つの観点から検討されているが，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 3.0 は問題が指摘されていない．一方，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．

過去に発生した例としては，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あげられる．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，暗号技術の欠陥が銀行の業務に大きな影響を及ぼしたという意味で，注目に値する事件であった．

また，インターネット・バンキングのサービスを提供している金融機関にとっては，SSL に利用する暗号技術を適切に選択することも重要である．銀行のウェブサイトには，例えば，「当銀行のインターネット・バンキングは業界標準の 128bit SSL を用いており，安全にご利用いただけます」といった説明が掲載されていることが多い．ここでいう「128bit」とは，SSL に採用されている共通鍵暗号の鍵長（暗号鍵の長さ）のことである．このキーワードは，「SSL で利用される共通鍵暗号の鍵長」というたった一つのパラメータに焦点を当てているという意味で，ミスリーディングな面がある．

かつて，日本におけるインターネット・バンキングの黎明期には，米国政府の暗号輸出規

制の関係で，共通鍵暗号アルゴリズムが RC4 で，その鍵長が 40bit のブラウザしか利用できなかった．しかし，1990 年代後半に輸出規制が緩和されると，鍵長 128bit の RC4 が組み込まれたブラウザが利用可能になった．このパラメータは比較的違いが分かりやすいこともあって，「128bit SSL」というキーワードが安全性の証のように使われてしまった．

しかし，共通鍵暗号の鍵長が 128bit であるか否かは，SSL のセキュリティ・レベルを規定するパラメータの一つに過ぎない．例えば，鍵交換やディジタル署名に利用される RSA 公開鍵暗号の鍵長や，公開鍵証明書に利用されるハッシュ関数について説明している金融機関はあまりないが，これらも SSL のセキュリティ・レベルを左右する大切な要素である．金融機関は，現時点で必要とされる安全性の水準を十分認識したうえで，パラメータを適切に選択することが大切である．

SSL においてどのような暗号アルゴリズムと鍵長が選択されるかは，銀行のサーバと利用者のクライアント PC の双方に依存する．2009 年時点で，多くの金融機関サーバが実装している SSL は，共通鍵暗号を「128bit の RC4」に限定しているわけではない．「128bit SSL」というキーワードを掲げる金融機関のインターネット・バンキングであっても，最新型のクライアント PC を用いて接続した場合，共通鍵暗号として，より安全性が高いとみられている「256bit AES」や「168bit 3DES」が選択可能となっていることは珍しくない．ところが，そうしたより安全な暗号アルゴリズムを利用可能にもかかわらず，より安全性の低いアルゴリズムを選択するといった望ましくない実装を行っている金融機関が多く存在することが指摘されている [3].

暗号アルゴリズムの強度は，時間の経過とともに低下する．攻撃者側の技術が向上することから，かつて安全と考えられていた暗号アルゴリズムと鍵長では，必要とされるセキュリティ・レベルを満たせなくなるからである．インターネット・バンキングで現在利用されている暗号アルゴリズムのいくつかについては，安全面の寿命が尽きつつあり，より安全性の高いものに変更しなければならなくなる時期が近づいている（2 章参照）．こうした観点からも，インターネット・バンキングの安全性について検討を続けていくことが求められているのである．

■11 群 － 7 編 － 3 章

3-3 インターネット・バンキングの将来

（執筆者：岩下直行）［2009 年 3 月 受領］

インターネット・バンキングのシステム設計に当たっては，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なりすましなど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よ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，そのリスクは過小に見積もられ勝ちになる傾向がある．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．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．そのためにも，金融機関は，高度化するセキュリティ対策をブラックボックスのまま導入するのではなく，その仕組みと有効性を正確に理解したうえで，その限界を把握して利用していくことが大切であろう．

インターネットが万人に開かれたネットワークであり，脆弱な利用者の PC 環境に依拠している以上，インターネット・バンキングのセキュリティを完ぺきに守ることはできない．どのような対策を講じようとも，その裏をかくことはできてしまうのである．このため，リスクをゼロにするような「決定版」の対策を探すことは無駄である．

仮に現時点でベストの対策を選択できたとしても，その効果が永続するわけではない．攻撃者側も含め，技術進歩のスピードが速いため，不断の見直しが必要である．現状のセキュリティ対策で十分と判断してしまうことは危険である．インターネット・バンキングのセキュリティについて，継続的な改善，見直しを行う仕組みを構築し，外部環境の変化に対応して常に及第点以上の対策を選択し続けることを指向することが大切である．

そういう観点からは，例えば，利用者の IT リテラシーを向上させるための啓発活動に取り組むことや，ウェブ・アプリケーションの実装上の脆弱性に迅速に対応する体制つくりが重要となる．また，EVSSL（Extended Validation SSL）証明書のような，利用者による確認が容易な安全対策を拡充していくことも重要である [2]．金融機関にとっては，そうした対応状況について積極的に情報を開示し，セキュリティ対策を進めていることをアピールしていくことが，利用者の信頼を獲得していくために必要なことであろう．

■参考文献■

1) 松本勉・岩下直行，“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，vol.19，no.s1，pp.1-14，日本銀行金融研究所，2000.
2) 中山靖司，“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，”日銀レビュー，日本銀行，2007.
3) 神田雅透・山岸篤弘，“暗号世代交代についての暗号学会とビジネスサイドのギャップをどう埋めるか ～SSL サーバの暗号設定の現状からの考察～，”2009 年暗号と情報セキュリティシンポジウム，2009.