

第5章 非対面取引——インターネット・バンキングを中心に

能見善久・山下純司

1 総論

(1) 非対面取引の意義

非対面取引の厳密な定義をすることは困難であるが、大ざっぱな言い方をすれば、取引相手と対面しないために、相手方に関する情報が制限された状態で行われる取引が非対面取引であると言えよう。相手方を見ながら取引をする場合には、相手方の反応を確認できるので、相手方が取引内容について誤解していたりした場合にも、それがわかることがある。また、相手方が名乗っている名義の本人でないということがわかることもある（たとえば、女性の名義で取引をしている相手方が男性であるような場合）。要するに、対面取引では、相手方に関するいろいろな情報が伝わってくるのに対して、非対面取引ではこうした情報が極めて制約されている。

このような情報量が限定されているという意味での非対面取引としては、通信販売などが古くからある。ファックスによる送受信で取引を締結するのも非対面取引に該当しよう。しかし、以下で取り上げるのは、「電子的な手段を用いる非対面取引」である。相手方情報の限定性ということでは通信販売と本質的な差があるわけではないが、電子的手段を用いる場合には、通信に際して相手方に提供される情報が一層限定的・定型的である。そして、銀行取引を念頭におくと、電子的手段による取引では、顧客側は「人」が端末を操作するが、銀行側はコンピュータ・システム（プログラム）によって自動的に対応する（振込依頼などの場合、銀行側は機械を操作する「人」がいるわけではない）。これは、相手方（顧客）から提供される情報が限定的・定型的というだけでなく、それを受け取る側（銀行側）も、「人」を介さない機械的対応をすることを意味する。こうして、電子的取引では、銀行の構築した「システム」による取引がウェイトを占めるようになってくる⁽¹⁾。

以上のような特徴から、振込、送金などの銀行取引において、非対面取引がおこなわれるようになると、そこにいろいろなリスクが生じる。第1は、いわゆる「なりすましのリスク」

(1) システムという表現は曖昧だが、ここでは、コンピュータのハードウェアだけでなく取引に対応するプログラムを含めた意味で用いる。

である⁽²⁾。口座名義人(預金者)になりすました者によって振り込みなどがなされる危険である。要するに無権限取引である。第2は、操作ミスリスクである。第3に、取引そのものというよりは、それに関連する副次的なリスクとして、個人情報の流失・悪用といったリスクも考えられる。また、リスクのタイプの問題ではないが、銀行取引において以上のリスクが現実化したときの被害の大きさも、非対面的な銀行取引を考える際には注意すべき要素であろう⁽³⁾。

そこで、非対面取引においては、こうしたリスクにどのように対処するかが重要な課題となる。技術的な問題と法的な問題がある。技術的問題は、いうまでもなく、本人確認の方法や、通信途中で情報が盗まれないようする技術の向上を図ることである。こうした技術の向上をとまって初めて、リスクの大きい銀行取引における非対面取引が安心して使えることになる。法的な問題は、この報告書で検討することであるが、リスクが現実化したときに、法的にどう扱うかという問題である。銀行の責任の有無、その判断基準、顧客に求められる注意などが重要な検討課題である。また、法律の適用から当然に導かれる結論ではないが、一定の注意をした顧客については責任(負担)を一定額に限定するといった方策の可否という問題もある(但し、この報告書では政策に関する問題は触れない)。

(2) 銀行取引における非対面取引

銀行が一方当事者となる非対面取引としては、インターネット・バンキング、テレホン・バンキング、モバイル・バンキング、ATM取引などがある⁽⁴⁾。インターネット・バンキング、テレホン・バンキング、モバイル・バンキングは、いずれも顧客側が自分のパーソナル・コンピュータ、電話、携帯電話によってアクセスする。これに対して、ATMでは、顧客側が操作する端末は銀行が所有・管理する端末である(最近では、提携先の金融機関のATMが使えるが)。インターネット・バンキングなどの方が、何時でも、どこでもアクセスできるという点で顧客にとっては利便性が高いが、銀行側からすると顧客が操作する端末については銀行による管理が及ばない。また、インターネット・バンキング、テレホン・バンキング、モバイル・

(2) 飯田耕一郎「インターネット上の電子金融取引と本人認証・電子署名」金融法務事情 1630 号 42 頁では、「なりすまし」のほかに、顧客側が実際には操作したのにこれを「否認」する場合を問題として取り上げているが、故意に行われる否認はあまりないと思われるので、独立には取り上げない。故意による否認以外の場合で、銀行側には操作の記録があるのに対して、顧客が自分には操作した覚えがないと主張するときは、他人による無権限取引に該当するので、そこで検討する。

(3) この点に配慮して、各銀行でATM取引では振込限度額を限定しているが、インターネット・バンキングでは、このような限度設定がされていないようである。

(4) 飯田論文(前掲注(2))のほか、飛松純一「インターネット・バンキングをめぐる法的問題——銀行規制との関係を中心に」金融法務事情 1631 号 50 頁以下、郷原淳良「我が国におけるインターネット・バンキングの現状」法とコンピュータ No.20 (2002) 29 頁以下などを参照。これらの問題についての本格的論文としては岩原紳作『電子決済と法』(2003)が必読である。

バンキングを比較すると、インターネット・バンキングは、コンピュータさえ有れば、自分のコンピュータでなくても、どこからでも利用できる点で顧客の利便性が高いが（但し、顧客が他人のコンピュータを使うとそのコンピュータにスパイウェアなどが入っていたりする危険がある）、これら3つの非対面取引における利便性の差は相対的である。そこで、以下では、顧客側の管理する端末を用いる非対面取引の代表として、インターネット・バンキングを対象として議論することにする。

インターネット・バンキングでは顧客は、自分が管理する端末で操作をするので、そこでのミス、情報漏洩（スパイウェアなどによる個人情報の流失）などについては、銀行側は直接的な関与はない。しかし、インターネット・バンキングという取引システムを提供し、銀行としてのコストや効率性の点で利益を上げている以上、そのシステムの設計が不適当であるために、顧客に被害が生じたという場合には、銀行側の責任が生じる余地もある。詳細は後で検討する。

(3) 非対面取引と消費者保護（預金者保護）

偽造カードおよび盗難カードを用いて無権限者がATMで預金払戻し等をした行為については、「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10日法律第94号）」（「預金者保護法」と略称する）が民法の特則および損失分担のルールを定める。すなわち、まず偽造カードによる払戻し等については、民法478条の適用が制限される（3条）。その結果、銀行側が無権限者に対する払戻しについて善意・無過失であっても免責されず、なお元の額の預金があるものと扱われる。但し、偽造カードによる払い戻しの場合に、預金者側に故意があるとき、または銀行が善意・無過失であり、かつ、預金者に重過失あるときは、預金者側が損失の全部を負担する（4条1項）。次に、盗難カードによる不正払戻しの場合、民法478条の適用は排除されない（3条但書）、銀行が善意無過失のときは免責され、預金者が損失を負担するが、預金者が一定の条件を充すと、損失の補填を銀行に求めることができる（5条）。

預金者保護法は、偽造・盗難カードによる被害について、損失分担のルールを定めるものであり、預金者保護にとって大きなステップであるが、この法律は、盗難通帳によって銀行窓口で無権限者が払戻しを受けた場合や、インターネット・バンキングによる被害については対象としていない⁽⁵⁾。通帳による窓口払戻しについては、従来どおりに、民法478条の「債権者

(5) なお、全国銀行協会では、先般、「預金等の不正払戻しへの対応について」（平成20年2月19日）を公表し、預金者保護法の対象となっていない盗難通帳やインターネット・バンキングにおける預金等の不正払戻しについても、銀行界の申し合わせとして補償の対象とすることとしている。<http://www.zenginkyo.or.jp/news/2008/02/19160000.html> 参照。

の準占有者に対する弁済」の法理が適用されるべきだとされ、インターネット・バンキングについては⁽⁶⁾、被害の実態調査などなお検討を要するとして先送りにされたが、この法律の施行後2年を目途に見直すものとされている（附則3条）。このように、預金者保護法は、インターネット・バンキングには適用がないが、ATM取引において偽造・盗難カードが用いられた場合と、インターネット・バンキングとで、損失分担ルールに差があってよいかについては議論があろう。

2 個別的論点

(1) 取引の成立・不成立

(a) 取引の成立

典型的なインターネット・バンキングの仕組みは、まず、①顧客が銀行と口座開設に関する契約を締結し、②インターネットを使った銀行取引（送金・振込・各種料金代金支払いなど）に関して、それに必要な資金を指定口座から引き落とすという契約をするものである。また、③インターネットで顧客が銀行からの借り入れをすることも可能である。②は指定口座からの資金の移動を伴うので、その際に、IDやパス・ワードによって本人確認が行われる。③については、顧客の指定口座に借入金振り込まれるが、顧客は、将来銀行に借入額を返済する債務を負担することになる。従って、インターネット・バンキングによる借り入れの場合にも、本人確認のためのパス・ワードが要求される。以下では、指定口座からの資金移動を生じる②のタイプの取引をインターネット・バンキングの典型として取り上げることにする。

インターネットを利用した個別の取引がどの時点で成立するかであるが、一般の契約理論によれば、離地者間の取引については、申込・承諾の内容が合致し、かつ、承諾の意思表示が発信された時が契約の成立時期である（民法526条）。但し、消費者と事業者の間の電子消費者取引については、承諾の発信主義を定めた民法526条の適用が排除されている（電子消費者契約4条）。従って、承諾については意思表示の一般原則が適用され（97条1項）、承諾の通知が相手方に到達した時点でその効力が生じ、契約が成立する。顧客による振込の場合を考えると、顧客が先に振込依頼の申込をするので、これを引き受けた旨の銀行の承諾通知が顧客に到達した時点で、契約が成立する。

(6) 金融庁の調査によれば、平成17年2月から平成19年4月までの間に、主要行において合計114件、金額にして約1億円の被害が発生している。これは盗難キャッシュカードによる被害（6921件、約39億円）、偽造カードによる被害（1270件、約19億円）と比べるとまだ少ない。

もっとも、インターネット・バンキングの約款では、契約の成立について、次のような規定をするところがある。すなわち、振込などの資金移動に関して言えば、①顧客からの振込依頼の通信、②これを受領した銀行が顧客に依頼内容（振込内容）の確認を求める、③顧客が確認を通信（画面上の確認ボタンなどを押す）、④銀行がこれを受領し、正当な顧客からの依頼であると認めた時点で契約が成立する、というものである。①の顧客の振込依頼が申込で、④が承諾であると考え、電子消費者契約では④の内容が顧客に届いた時点で（インターネット画面で表示されて）契約が成立する。単に、銀行が「正当な顧客からの依頼であると認めた」というだけでは承諾が顧客に到達していないから、電子消費者契約としては契約はまだ成立していないことになる。もっとも、実際のインターネット・バンキングでは、顧客からの振込依頼に関しては、「振込依頼を受け付けた」という表示が④の段階で画面にされるので、この時点で契約が成立する。

（b）取引の不成立

顧客が依頼した取引が振込などの場合には、①振込先口座の不存在（これは最近のシステムでは振込依頼を受け付けるときに振込先の口座番号と名義などをチェックするようになっていくことが多いが、そうっていないこともある）、②指定口座の残高不足（残高不足は顧客から振込依頼を受け付けるときに、銀行側のコンピュータでその場で判断できるであろう）、③銀行（仕向け銀行）のシステムの故障など、顧客から資金移動の依頼を実行できないことが生じることがある。そこで、インターネット・バンキングの約款には、これらの事由がある場合には、「取引の不成立」として扱うものがある。これは、インターネット・バンキングに特有の問題ではないが、振込に関する契約が成立した時点では障害事由がわからず、後になってわかるということが生じる（②についてはそのようなことが生じるのかどうかかわからないが、①③はありうる）。

こうした「取引の不成立」の取り扱いが生じた場合に、インターネット・バンキングの約款上は、そのことが当然には顧客に知らされることになっておらず、むしろ顧客が自分で口座残高を調べて、振込が実行されたか否かを確かめることを求めるものがある。確かに契約理論として当然にそのような通知義務が銀行にあるわけではないであろう。しかし、一旦成立扱いをした契約が不成立となった場合には、そのことを銀行は顧客に通知する義務（信義則上の説明義務）があるといつてよいのではないかと（①②は、顧客側に落ち度があることが通常であろうが、振込依頼を受け付けた後は、銀行が顧客よりも先に障害事由を認識するであろうから、それを知った銀行に通知義務を負わせることはおかしくない。③は銀行の支配領域で生じる障害事由であり、一層、銀行に通知義務を負わせることの合理性がある。）。もっとも、多くの銀行のインターネット・バンキングでは、顧客が登録したメール・アドレ

スに、銀行から取引不成立の通知がなされるようになっているようである。

そのほかに、取引の不成立の場合に関しては、次のような問題がある。

第1に、振込などの履行を実行することに障害がある場合に、顧客と銀行の間の振込依頼の契約が理論的にはどうなるかである。上述のように、銀行によっては、インターネット・バンキングの約款で「取引の不成立」としているところがある。しかし、意思表示が一旦合致して契約が成立したのに、履行の障害となる事由があったことを理由として、契約を不成立とすることができるか、また、それは合理的か。上記①②③などの事由が存在しないことを条件として契約が成立したと構成することは可能かもしれない。しかし、①②はともかく、③の場合にまで取引不成立とするのは説明がしにくい。③の事由が生じた場合には、銀行側に約定解除権が認められるということでもよいのではないか。それならば、①②も含めて全体を解除権の問題としてよいように思われるが、解除だと解除の意思表示をする必要がある点が面倒ということであろうか（前述の「通知義務」の問題とも関連する）。解除の意思表示が面倒だというのであれば、①②③を解除条件とすることでもよいであろう。ただし、その場合にも銀行に通知義務を負わせるのが適当であろう（通知義務はそれを怠っても、契約が失効するという効果には影響しないが、万一通知義務の不履行により顧客に損害が生じた場合に銀行の責任が生じる）。

第2に、③のシステムの故障などは、一時的な障害であるから、振込の実行が遅れるだけであるにもかかわらず、このような場合にも「取引の不成立」という扱いが適当かどうか問題となる。おそらく数時間の故障であれば、取引を不成立とする扱いは適当でないし、実際にも銀行はそのような扱いをしないであろう。しかし、故障の時間が長引くと、単に遅れて執行するというのではなく、「取引の不成立」という扱いをするということなのであろう。顧客からすると、③のような場合に、取引不成立になるのか、遅れて実行されるのかが明らかでない。取引不成立ならば、顧客としては、再度振込依頼するか別の手段を講じる必要があるが、それを決断するための情報が提供されないと困るであろう。

(2) ディスクロージャー・説明義務

銀行法では、預金の受け入れなどに関しては、一定の情報提供をすべきこと定めており（銀行法12条の2第1項）、従って、インターネット・バンキングでも預金取引（定期預金取引、外貨預金取引）に関しては、銀行法上の情報提供義務が課せられることになる。そして、これらの情報については、インターネットを利用しての提供が許容されている（銀行法施行規則13条の3）。インターネット・バンキングは、顧客も、銀行が管理するウェブ画面で操作するので、その画面上で情報提供されるのが合理的である。しかし、対面取引と異なり、非対面

取引では、顧客が情報や説明に気が付かない可能性もあり、対面取引とは異なる点もないわけではない。

送金などに関しては、法令上の情報提供義務は規定されていない。消費者契約法も、事業者の一般的な情報提供義務は定めておらず、単に契約の内容について、必要な情報を提供すべき努力義務がさだめられているにすぎない（3条）。もっとも、実際のインターネット・バンキングでは、振込手数料は表示されている。そのほかにも、振込依頼が執行される時期、振込先口座が存在しないなどで振込ができないときの扱いなど（指定口座に資金が戻されること）が画面で説明されていることがある。

以上のような法令上要求される説明義務のほかに、一般論としては、銀行がその情報を提供しなかったために、顧客が損害を被り、銀行の不法行為ないし債務不履行責任が問われうる場面で、その責任を根拠付けるための信義則上の説明義務が問題となることがある。このような信義則上の説明義務に関して、インターネット・バンキングなどの非対面取引においては、何か特徴があるであろうか。インターネット・バンキングにおいては、それが一定のリスクを有すること（暗証番号の管理などに関して）など、顧客に必要な注意を喚起することが必要だと考えられている。これなどは非対面取引特有の説明義務と言えるであろう。

金融庁の「主要行等向けの総合的な監督指針」によれば、「インターネット上での暗証番号等の個人情報の詐取の危険性、類推されやすい暗証番号の使用の危険性、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクについて、顧客に対する十分な説明態勢が整備されているか」を問題としている。これらが無いからといって直ちに銀行の説明義務違反による責任が生じるものではないが、具体的な状況のもとにおいて、これらの点について銀行の対応が不十分である場合には、銀行の責任が生じる可能性がある。

（3）誤取引

顧客の操作ミスなど、インターネット・バンキングにおいては、顧客側の誤取引が生じる可能性が、銀行窓口における対面取引と比べると高い。しかし、コンピュータのシステムで対応する銀行側からすると、顧客側の誤操作は容易にはわからない。銀行としては、できれば錯誤無効の主張は排除したいと考えるであろう。これに対して、顧客からすれば、誤操作をしやすいインターネット・バンキングだからこそ、錯誤の主張を簡単に認めてほしいと考えるところである。相対立する要請の中で、両者の調和点を探す必要がある。

電子消費者契約法では、民法 95 条但書きを排除している。従って、インターネット・バンキングに際して消費者である顧客が誤操作したことが「重大な過失」と判断されても、民法 95 条但書きによって錯誤無効の主張が排除されることはなくなった。しかし、事業者が顧客

の意思表示が行われる際に、コンピュータの画面上で、顧客の意思表示を確認する方法が講じられている場合には、民法 95 条但書きは排除されない（消費者契約法 3 条）。従って、消費者の意思表示に重大な過失がある場合には、顧客から錯誤無効を主張することができない。インターネット・バンキングでは、顧客が振込などの資金移動を依頼する場合には、顧客に振込の内容を「確認」させることをしていると思われるので、民法 95 条但書きを排除する消費者契約法 3 条は適用されない。

(4) 不正取引

(a) 不正取引

不正取引とは、当該金融機関の口座について資金を移動する権限のない者がする取引である⁽⁷⁾。理論的には、その中に、①口座名義人になりすます場合と⁽⁸⁾、②口座名義人を代理する権限がないにもかかわらず、本人を代理して行う取引が考えられる（無権代理）。しかし、インターネット・バンキングでは、口座名義人が個人である場合は、その代理人であることを明らかにしてする代理取引は許容されていないが、法人の場合には、従業員が法人から与えられた権限に基づいて端末を操作するとすれば、これは代理である。

無権限者からの振込依頼であるにもかかわらず、銀行が正当な権限があると誤信して、振込依頼に応じたような場合に、法的にはどのように考えるべきか。振込依頼は、①振込先口座に資金を振り込むことの依頼と、②その資金を顧客の口座から引き落とすことからなると考えられている。①は、振込ないし送金契約であり、権限がないものが依頼した場合には、「なりすまし」の場合も含めて、本来は無権代理の問題と考えるべきであろう。従って、表見代理の規定が適用されるものと考えられる。②問題は、無権限者に対する弁済の部分であり、異論はあるが、一般には民法 478 条で解決されると考えられている。

しかし、実際にはインターネット・バンキングでは、約款中に、銀行が顧客の暗証番号を確認して依頼を受け付けた場合には、銀行はそれによって「顧客の被った損害について一切の責任を負わない」という内容の免責規定を有するのが一般である。免責条項の厳密な意味については後で検討する。

(7) アメリカの電子的資金移動法（EFT A）および Regulation では、無権限取引（unauthorised EFT）を定義して、その口座について権限のない者による資金の移動としている。岩原・前掲書 84 頁以下。

(8) 顧客本人の ID やパスワードをいろいろな方法で盗み出し（これを phishing という）、これを用いて本人になりすまして、預金などを自分の口座などに振り込むことが行われる。

(b) 銀行として要求される防止策(「システム上の過失」論)

- (i) 最高裁判平成15年4月8日判決(民集57巻4号337頁)は、ATM取引に関する事案であるが、預金者が預金通帳を第三者に盗まれ、ATMにおいて通帳を用いて払い出しがなされた場合に、銀行が預金者に通帳によっても機械式払い戻しが可能であることを説明しなかったことから、銀行の無過失を否定し、民法478条による免責の主張を斥けたものである。すなわち、判決は次のように言う。「このように機械払においては弁済受領者の権限の判定が銀行側の組み立てたシステムにより機械的、形式的にされるものであることに照らすと、無権限者に払戻しがされたことについて銀行が無過失であるというためには、払戻しの時点において通帳等と暗証番号の確認が機械的に正しく行われたというだけでなく、機械払システムの利用者の過誤を減らし、預金者に暗証番号等の重要性を認識させることを含め、同システムが全体として、可能な限度で無権限者による払戻しを排除し得よう組み立てられ、運営されるものであることを要するといふべきである。」

銀行側の478条による免責を主張するために必要な「無過失」の判断において、システム全体の設計・運営の仕方が考慮されるという意味において、「システム上の過失」とでも言うべきものが認められたことになる⁽⁹⁾。

このような考え方がインターネット・バンキングの場合にどのような帰結をもたらすかが注目されていたところ、最近2つの事件が裁判で争われた。1つは、東京高判平成18年7月13日(金融法務事情1785号)45頁、その原審東京地判平成18年2月13日(金融法務事情1785号49頁)である⁽¹⁰⁾。もう1つは、大阪地判平成19年4月12日(金融法務事情1807号42頁)である⁽¹¹⁾。

- (ii) 東京地判・東京高判の事件は、被告銀行とインターネット・バンキングの契約をしていた預金者の口座から、インターネット・バンキングのサービスを利用して何者かが2回、合計800万円を第三者の口座に振り込んだというものである。預金者から、同振込は無権限者による振込であるから、なお相当額の預金が残っているとして払い戻しを請求したのに対して、銀行が免責条項による免責を主張した。事実の部分での争いも多

(9) 平成15年の最高裁の事件では、銀行側は約款による免責ではなく、民法478条による免責を主張しているが、約款による免責を主張するケースにおいても、「システム上の過失」の考え方は同じく妥当すべきであろう。

(10) これらの判決については、島田邦雄・沖田美恵子「インターネットバンキングによる不正送金と金融機関の責任——東京高判18.7.13の射程範囲」金融法務事情1791号50頁、渡邊博己「無権限者によるインターネット・バンキング・サービスの振込取引と銀行の免責」銀行法務21、677号56頁、浅井弘章「インターネットバンキングと免責規定」銀行法務21、672号19頁などがある。

(11) この判決については、石毛和夫「金融商事実務判例紹介」銀行法務21、677号62頁がある。

いが⁽¹²⁾、法的な争点としては、①被告銀行の約款中にある免責規定（「当行が、本規定に記載された本人確認方法により本人からの依頼として取り扱いを受け付けたうちは、暗証番号等や宝くじ専用番号等に偽造、変造、盗用その他の事故があっても、それにより生じた損害については当行は一切の責任を負いません。」）によって被告銀行が免責されるか否か、②銀行に、免責条項による免責の主張を妨げるような過失（注意義務違反）があったか否か（被告銀行に過失があった場合には、この免責条項は適用されない、という理解を前提とする）、である。

東京地裁は、①については、約款で定められている本人確認手続きがとられた上で振込がされているので、銀行は免責条項に基づいて免責されるとした。但し、この免責条項は銀行側に過失がある場合についてまで免責を認めるものではないという理解をした（この過失の証明責任は、原告預金者側にあると考えているようである）。②の、銀行側に過失があったか否かの点については、インターネット・バンキングのシステムの構築・運営上の過失があるか否かを審理し（従って、弁済ないし資金移動の時点の過失だけでなく、構築されたシステム自体の安全性を問題にする平成 15 年の最高裁判決の立場を踏襲している）、本人確認の方法として被告銀行によって採用されている方式およびデータの通信方式が「全体として、可能な限度で無権限者による振込を排除し得よう構築し管理」されていたとして、銀行の注意義務違反を否定した。原告側は、本人確認方法として被告銀行が採用していた方法は乱数表を用いるというのではなく安全度が低いこと、当時すでにインターネット・バンキングでは無権限者による不正取引が発生しており、銀行側としてはより安全なシステムを構築すべきであったことなどを主張したが、認められなかった。控訴審も、原審と同様の理由で銀行側を勝たせた。

(iii) 大阪地判は、インターネット・バンキングのサービス提供を受けていた原告預金者の預金口座から合計 8 回にわたって約 798 万 2000 円が第三者の口座に不正に振り込まれたというものである。原告預金者から被告銀行に対する預金返還請求事件において、銀行が免責条項による免責を主張した。基本的に、東京地判・東京高判の事件と同じパターンである。ここでも、銀行側にシステム構築・運営上の過失があれば、銀行は免責を主張できないという理解を前提に（被告の免責約款の文言自体が「責めがある場合」

(12) どのようにして無権限者が暗証番号などを知り得たのかについては明らかになっていない。原告は、ハッカーが暗証番号などを用いることなく銀行のシステムに侵入したという主張もしているが、これは、暗証番号入力が記録上確認できるので否定された。また、スパイウェアによる暗証番号等の情報の流出についても、裁判所の認定は否定的である。むしろ、預金者がインターネット・バンキングを商売で使っており、従業員に暗証番号を教えたりしていることを問題視している。結局、どちらの過失も証明ができない状況で、損失だけは生じる、というのがこの種の事件の特徴と言えよう。

には免責されないとなっている)、被告のインターネット・バンキングにおいて「システム上の過失」があったか否かが争われたが、結論としては、銀行に「責めがある場合」には該当しないとして、顧客からの請求を棄却。具体的には、被告銀行側は、(1) 本人確認手続きが適正に行われていること、(2) 顧客と銀行ホストコンピュータ間のインターネット上のデータのやりとりについてのセキュリティ対策が十分行われていること、(3) 暗証番号の管理について顧客に対して注意喚起をおこなっていること、などをあげ、免責約款によって免責されると主張した。これに対して、原告は、暗証番号およびパスワードが原告のコンピュータ内にファイルとして保管していたものが何者かによってインターネット接続時に盗まれ、それが用いられて不正振込が行われたとし、被告銀行が暗証番号・パスワードなどのコンピュータ内保管が危険であることを注意喚起しなかったことが信義則上の義務違反となるから、銀行には「責めがある」と主張した。原告の重点は、上記(3)の注意喚起の部分にあるが、裁判では(1)(2)を含めて、銀行のインターネット・バンキングのシステム自体に欠陥がないか否かが争われた。結局、裁判所は、上記(1)(2)(3)いずれの点においても、銀行の「責めがある場合」に該当する事実がないと判断した。

(1)(2)は、インターネット・バンキングの技術的な安全性に関わるが、このうちの(1)の本人確認方法に関しては、被告銀行では、①第1暗証番号(顧客が指定した4桁の番号)、②第2暗証番号(乱数表を用い、ホストコンピュータが無作為に毎回ことなる番号を指定する可変暗証番号)、③第3暗証番号(乱数表を用いた暗証番号)が用いられ、登録された振込先以外への振込の場合には、①②③の3つの暗証番号によって本人確認手続きが行われるというものであった。裁判所は、これを「本人確認情報の管理として有効な方法である」と判断した。

また(2)のインターネット上行われるデータのやりとりの安全性については、現時点ではもっと解説が困難であると言われる128bitSSL暗号通信方式が採用されているなど、「セキュリティ対策も十分」であったと判断した。(3)は、顧客側の暗証番号等の管理について、銀行としてはどのような注意をすればよいのかという問題であるが、本件では暗証番号を厳重に管理するように十分な注意喚起がされているとされた。

(iv) インターネット・バンキングにおける不正取引に関するこれら裁判例は、次のような意義を有する。

第1に、これらの判決はいずれも、インターネット・バンキングについても、平成15年の最高裁判決で示された「システム上の過失」論を適用することを前提に判断していることである。だからこそ、弁済の際の狭い意味の弁済者の過失だけを問題とする

のではなく、より広く本人確認方法、インターネット利用上のリスクに対するセキュリティ、顧客に対する暗証番号管理上の注意喚起を問題としているのである。

第2に、現時点では、銀行の構築しているインターネット・バンキングのシステムとしての安全性は十分にあり、たとえ無権限者による不正取引が行われたとしても、銀行の過失（注意義務違反）はないと判断していることである。もっとも、東京事件、大阪事件のいずれも、預金者側の暗証番号管理に多少問題がある事例であり、仮に、預金者側の管理に全く問題がないにもかかわらずスパイウェア等によって暗証番号が読み取られたり、直接システムに入り込むハッカー行為が生じた場合に、どう判断されるかは明らかではない。そのときこそ、インターネット・バンキングの安全性が正面から問われることになる。その際には、インターネット・バンキングにおける不正利用がどの程度あるか、その原因が何であるか、安全性を高めるためにどのような技術的可能性があるか⁽¹³⁾、など多くの点を検討して判断されることになる。また、今までは裁判上、銀行の注意義務とはされていないが、インターネット・バンキングの不正振込の事件数が将来増えるようならば、顧客の口座の資金に異常な動きがある場合にそれをモニターする銀行の義務が問題となることもあろう。

（c）免責条項

インターネット・バンキングの約款には、「免責」に関する条項がある。その中にも、2種類の免責条項がある。すなわち、第1は、暗証番号の入力など、銀行の定めた本人確認手続きが行われた場合には、利用者は本人であるとみなし、たとえそれが権限のない不正利用であったとしても（暗証番号等の盗用など）、原告に生じた損害について、銀行は責任を負わないというものである。このタイプの約款において、銀行側に「責任があった場合」を除き、というような免責を制限する文言が入っている場合（上記大阪地判の被告銀行の場合）と、そのような文言がない場合とがある。第2は、インターネット上の通信経路において、不正アクセスなどで暗証番号・取引情報等が漏洩した場合の免責条項である。上記大阪地判の被告銀行の約款にはこのような免責条項があった。ここでも、銀行側に「責任があった場合」を除き、というような文言がある場合とない場合がある。

第1のタイプの免責条項の適用が問題となった事例としては、上記の東京地裁・東京高裁の事件と大阪地判の事件がある。ところで、この種の免責条項の意味については、多少不明確なところがある。大阪地判の事件における被告銀行の免責条項は、厳密に見ると実は2

(13) 現在の本人確認方法などについては、現時点でも技術的に問題があるという指摘もある。渡邊・前掲論文 58頁。

つの部分からなり、1つは、暗証番号などが正しく入力された場合には、その利用者を「本人と見なす」という部分である。もう1つは、暗証番号等が不正利用されたことで顧客に損害が生じて銀行は「責任を負わない」という部分である。この2つの部分の関係が必ずしも明らかでない。なぜなら、両者は少し異なることを問題としているが、それにもかかわらず1つの免責条項の中にあるからである。「責任を負わない」という部分は、銀行が顧客の口座から支払ったことの免責を定める部分であり、民法478条の債権の準占有者に対する弁済に相当する。これに対して、「本人と見なす」という部分は、いわば表見代理に相当する条項である。民法478条の債権の準占有者に対する弁済において表見代理の成否を問題としないのと同じように、銀行の免責だけを導くのであれば、暗証番号を入力した利用者を「本人と見なす」ことは必要はない。しかし、振込依頼などの場合には、その契約は、「資金移動に関する契約」と「その費用を顧客口座から引き落とす」部分からなるが⁽¹⁴⁾、後者は「弁済」に相当するが、前者は厳密に言えば弁済ではない。従って、資金移動に関する契約の部分の有効にするためには、本来は表見代理が成立する必要があるのである。「本人と見なす」条項は、この場合に表見代理が成立するのと同じ効果を生じさせることを狙うものであろう⁽¹⁵⁾。大阪地判の事件の被告銀行の約款では、この2つが1つの免責条項の中に組み込まれているが、両者を分けて規定する約款を持つ銀行もある。

第2のタイプの免責条項、すなわち、インターネット上で通信中に暗証番号などが第三者に盗まれた場合の免責条項は、インターネット通信上のセキュリティに関する。この種の免責条項の適用の可否が争われた事案はまだ公表判例にはないようである。大阪地判の事案でも、利用された暗証番号等は、銀行とのインターネット通信中に盗まれたわけではないようであり（どのように盗まれたかは解明できなかった）、従って、第2のタイプの免責条項は実質的には問題とならなかった。将来、実際に銀行と顧客の通信中に暗証番号等が盗まれた場合に、この種の免責条項がどう判断されるかは、今後の問題である。セキュリティの問題に関しては、「絶対安全」ということは科学的ありえない。現在のセキュリティが将来破られることもあろう。その時には、銀行の責任の有無が問題となりうるが、法的な責任（過失責任）は、予見可能性を前提とする注意義務違反の有無で判断される。従って、リスクがどの程度予見できるのかによって、過失の有無が判断されることになる。上記の大阪地裁

(14) 振込取引の法的構造についてはいろいろな問題があるが、岩原・前掲書67頁以下、森田宏樹「振込取引の法的構造」中田＝道垣内編著『金融取引と民法法理』所収123頁以下を参照。

(15) 仮に、資金移動部分については表見代理が認められず、また、暗証番号を使った利用者を本人と見なす条項を有しない場合には、資金移動契約部分は顧客との関係で効力が生じないが、銀行としてはそのような無効な契約のために顧客の口座から費用を支払ったことになる。しかし、この場合も、判例の立場では、民法478条の適用ないしそれに相当する免責条項が適用される余地はあろう。

の判決は、「現時点では」安全である（具体的なリスクが予見できない）という判断をしたものと解することができる。

(5) 銀行の調査義務

日本ではあまり議論されないが、アメリカの電子的資金取引法では、顧客が誤取引や無権限取引があった可能性があるとして、銀行に調査を求めた場合には、銀行は一定の期間内に調査をして、顧客に結果を通知する義務がある⁽¹⁶⁾。これは、インターネット・バンキングにおける紛争解決を図る上で、銀行と顧客を対等にする重要な制度である。なぜなら、無権限取引などに関する情報は、銀行側が保有しており、顧客側には無権限取引を証明する手段がない。銀行の調査義務は、銀行に調査をさせて結果を顧客に報告させることで、情報・証拠の偏在を是正することに資するものである。日本では、「信義則上の説明義務」が同様の機能を果たす可能性がある。

(6) その他の問題

インターネット・バンキングに関しては、以上のほかに、システム・リスク（システム・ダウンなど）への対応の問題、マネーロンダリングへの対策などの問題があるが、インターネット・バンキングに特有の問題ではないので、その検討は省略した。

(16) Error Resolution と呼ばれる。US Code 15.1693f およびこれに基づく Regulation E Sec.205.11 によれば、顧客が銀行から口座に関する計算書を送られてから 60 日以内に銀行に対して、自分がしたことのない「誤った資金移動 (error)」があったことを銀行に告げると、銀行は原則として 10 日以内に調査をして、その結果を顧客に伝える義務がある。「誤った資金移動」とは、無権限者による資金移動のほか、顧客の錯誤・誤操作による資金移動 (incorrect electronic fund transfer) も含まれる。なお、銀行が顧客からのクレームに対して調査を行わなかった場合には、3 倍賠償が課せられる (US Code Title 15.1693f(e))。