第１章　個人向けのインターネット・バンキング・サービスにおける不正送金に係る金融機関の責任範囲

――ソフトローおよび裁判事例を踏まえて

沖　野　眞　已

１　はじめに

インターネット・バンキング・サービスにおいて、本人（権利者）によらない他人名義口座への不正な送金、その形での預金の不正な払戻し[(1)]は、後を絶たない（後記２参照）。

本稿は、特に個人向けのインターネット・バンキング・サービスにおける不正送金・不正払戻しの場合の金融機関の責任範囲について、いわゆるソフトローおよび裁判事例を踏まえて、考察するものである。

すなわち、インターネット・バンキング・サービスを通じて預金口座から、権利者によらずに、したがって不正に、他人名義口座への送金がされ、そのような形で不正に預金等が払い戻された場合の金融機関の責任については、キャッシュ・ディスペンサー用カード（キャッシュカード）を用いたATMを通しての権利者によらない不正な払戻しについての「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」（以下「預貯金者保護法」という）のような特別の立法はない。民法478条によってこの問題を処理することの限界や不適切さはつとに指摘されており、また、キャッシュカードによる機械式払戻しと同様に、あるいはカードの所持による防護措置のないインターネット・バンキングについてはそれ以上に、預貯金者の保護およびそれを通じた預貯金に対する信頼の

(1)　不正な送金・振込を払戻しと同視してよいか、ひいては民法478条のもと預金債務の「弁済」と言えるかも一個の問題たりうる。送金・振込には預金の払戻しのみならず、振込先への送金が加わっているためである。従前より預金取引の場合には定期預金の期限前払戻し（解約＋払戻し）など払戻しと同視できるとして弁済の概念が拡張して解釈されており、インターネット・バンキングにおける不正な送金・振込についても払戻しと区別することなく扱われている。以下でも、この点はこれ以上、立ち入らない。詳細は、中舎寛樹「インターネット・バンキング・サービスにおける不正振込送金と銀行の免責」金法1812号13頁（2007）参照。

確保の必要があることは、一般に共有されていると言ってよい[(2)]。預貯金者保護法のような特別立法のないインターネット・バンキングにおいては、金融機関による自主的な取り組みがいっそう期待されるところ、平成20年には全国銀行協会（全銀協）の申し合わせが公表されている（後記**3**）。本稿が「ソフトロー」として対象とするのは、この申し合わせ（およびそれを踏まえた各行のインターネット・バンキング利用規定）である。また、インターネット・バンキングにおける不正送金による不正払戻しについては免責条項の効力という問題としてではあるが、わずかながら裁判例が存在する。そこで、本稿は、これらのソフトローおよび裁判例を確認し、そのうえで、金融機関の責任範囲のあり方について若干の考察を行う。

以下では、まず、各種の統計から、インターネット・バンキングにおける不正送金・不正払戻しの現状を確認したうえで（**2**）、全銀協の申し合わせの内容およびそれを受けた各行のインターネット・バンキング利用規定の内容から、ソフトローとしての規律内容を確認し（**3**）、裁判例を概観した後（**4**）、ソフトローのあり方に関して若干の考察を行う（**5**）。

2　インターネット・バンキング・サービスにおける無権限者による不正な送金の現状

インターネット・バンキングにおける不正送金・不正払戻しに関しては、警察庁、

(2)　例えば、中舎・前掲注（1）14頁は、インターネット・バンキングにおける不正送金・不正払戻し事案について預貯金者保護法の趣旨に照らしての解釈を説く。また、金融庁は、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を一部改正して、インターネット・バンキングの情報セキュリティ対策に関する事項を盛り込んでいる（平成19年1月23日から適用）。そこでは、インターネット・バンキングに関して「不正取引に係る損失の補償については、預貯金者保護法の趣旨を踏まえ、利用者保護を徹底する観点から、真摯な顧客対応を行う態勢が整備されているか」という一文が追記されている（主要行等向けの総合的な監督指針Ⅲ－３－８－２（３）、中小・地域金融機関向けの総合的な監督指針Ⅱ－３－５－２（３）。なお、「預貯金者保護法の趣旨を踏まえ」という部分は、平成27年4月、「預貯金者保護法および全国銀行協会の申し合わせの趣旨を踏まえ」と改正されている）。その含意に関し、インターネット・バンキングにおける預金の不正払戻しについては預貯金者保護法の対象外であり、そのため、民法478条により金融機関が免責されない場合を除き、補償は金融機関の経営判断によることとなるものの、預貯金者の保護を図るという預貯金者保護法の「趣旨は、当然にインターネットバンキングを含む預金関連業務全般に徹底されるべきものである」という考え方が示されている（藤山智博「ATMシステムとインターネットバンキングの情報セキュリティ対策にかかる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の一部改正の解説」金法1796号24頁（2007））。また、預貯金者保護法の附帯決議においても、インターネット・バンキングに係る犯罪等についての実態把握、その防止策および預貯金者等の保護のあり方の検討と必要な措置の実施が、要請されている。

金融庁の統計が公表されており、また、全銀協によるアンケート調査の結果が公表されている。

（1） 警察庁統計

警察庁の最新の[3]統計（平成26年）[4]によると、平成26年の発生状況は、件数にして1826件、被害額（犯人が送金処理を行ったすべての額）は約29億1000万円、実被害額（被害額から金融機関が阻止した額を差し引いた実質的な被害額）は約24億3600万円となっており、その前年・平成25年（1315件、14億600万円、13億3000万円）、前々年・平成24年（64件、4800万円、4800万円）217件、2億1300万円）と比べて、急激な増加をみせている。その特徴は、「被害が多くの地方銀行や信用金庫・信用組合に拡大するとともに、法人名義口座に係る被害が拡大している」とのことである。

このうち、個人名義口座の被害額が、約18億2200万円、法人名義口座の被害額が、約10億8800万円である。平成25年が、それぞれ、13億800万円、9800万円、平成24年が、4700万円、100万円であったことと比べると、確かに法人名義口座に係る被害の増加が顕著である。そのため、個人名義口座の被害の相対的な割合は低下しているものの、被害額において、個人名義口座のそれがかなりの部分を占めていることは確かである（被害額にして、平成25年は93.1％、平成26年は62.6％、実被害額では、平成25年は93.4％、平成26年は68.9％）。

（2） 金融庁統計

金融庁の統計によると、平成26年度については4月～9月までであるが、「インターネットバンキング犯罪」は、809件、平成25年度は、1954件、平成24年度は

---

(3) 本稿は、平成27年2月に行った金融法務研究会第2分科会での報告をもとにしている。「最新」というのは同報告時点でのものである。通常であれば、原稿作成時における「最新」のデータにアップデイトして記すものであるが、後述するとおり、平成26年5月および7月に、法人顧客についての、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関する対応および補償に関して、全銀協の申し合わせがされており、平成26年はその点で1つの区切りの年と考えられること、また、後述するように、その後の統計を見ると、特に法人名義口座についての不正送金事例の状況に変化が見られ、その変化をより明らかにする意味でも、平成26年を区切りとすることが有用に思われることから、便宜上、報告時（平成27年2月）段階で入手可能であった統計結果を維持し、フォローアップとしてその後についての統計を示すこととしている。

(4) 平成27年2月12日付け警察庁広報資料「平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について」（http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf）。

148 件である（偽造・盗難キャッシュカードや盗難通帳による被害に比して、平均被害額が大きいことも注目される。）。個人については、平成 26 年度（4 月～ 9 月）は、件数 721 件、金額 6 億 5500 万円、平均被害額が 90 万円、平成 25 年度は 1863 件、19 億 6700 万円、平均 105 万円である。平成 24 年度が、145 件、1 億 4100 万円、97 万円であったことと比べると、急増していると言える。

（3） 全銀協アンケート調査

全銀協のアンケート調査 (5) によると、ここでも件数、被害額の伸びが著しい。法人の被害が急増しているが、なお件数のみならず被害額においても個人顧客のそれの方が大きい。すなわち、平成 26 年度は 4 月～ 9 月までであるが、個人は 678 件、6 億 2200 万円、法人は 71 件、4 億 1700 万円。平成 25 年度は、個人が 984 件、12 億 5000 万円、法人が 35 件、1 億 8300 万円、平成 24 年度は、個人が 106 件、1 億 2000 万円、法人が 1 件、400 万円であった。

（4） 補償状況

金融庁の統計および全銀協アンケートでは、件数ベースの補償率が示されている。金融庁統計では、処理方針決定済みのものの内訳の数値として、平成 26 年度（4 月～ 9 月）は、84.5％、平成 25 年度が 90.8％、平成 24 年度が 70.5％である。一方、全銀協アンケートによると、平成 26 年度（4 月～ 9 月）が 93.7％、平成 25 年度が 98.9％、平成 24 年度が 94.1％である。補償対象とならないと判断されたのがどのような場合かについては、不明である。

（5） フォローアップ――平成26年以降の状況

① 警察庁統計

平成 28 年 3 月 3 日付け警察庁広報資料「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」(6) によると、平成 27 年の発生状況は、件数にして 1495 件、被害額は約 30 億 7300 万円、実被害額は約 26 億 4600 万円である。平成 26 年に比して件数こそ減少しているが、被害額、実被害額は増加している。法人名義口座の被害の増加、金融機関の種類としても被害が拡大している点は、平成 26 年と同様の特徴であるが、特に、法人名義口座の被害の増加によって、被害

(5) 191 行を対象とした平成 26 年 9 月末時点におけるアンケート調査である。（https://www.zenginkyo.or.jp/news/2014/11/27150000.html）

(6) https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf。

額が「過去最悪」を記録したこと、特に信用金庫の法人口座被害が急増していること、また、信用金庫・信用組合のほか、農協・労働金庫に被害が拡大していることが指摘されている。さらに、スマートフォン等にSMSを送信して偽サイトに誘導するフィッシングがはじめて確認されるなど、被害に至らしめる手法の多様化・巧妙化が引き続き見られるようである。注目されるのは、「被害口座名義人の多くがセキュリティ対策を未実施」「ただし、法人では、17%がセキュリティ対策実施（電子証明書利用）」と指摘されている点である。個人について見ると、セキュリティ対策としてワンタイムパスワードがとりあげられており、実施（利用）は9.7%、未実施（利用せず）が75%、不明が15.4%となっている。セキュリティ対策未実施が大半であるとともに、セキュリティ対策（ここでは個人の場合はワンタイムパスワード、法人の場合は電子証明書）の実施によって被害を完全に防げているわけではないことも明らかとなっている。

個人名義口座の被害額が、約16億700万円、法人名義口座の被害額が、約14億6600万円である。個人名義口座の被害額は、平成26年に比して減少に転じており、法人名義口座の被害額がなお伸びていることと対照的であるものの、それでも、個人名義口座の被害額はなお法人名義口座の被害額を上回っており、被害額において個人名義口座のそれがかなりの部分を占めている状況に変わりはない。

また、平成28年9月8日付け警察庁広報資料「平成28年上半期におけるインターネットバンキングに係る不正送金事犯の発生状況等について」(7)によると、平成28年上半期の被害の件数は、857件（平成27年下半期740件、同上半期755件）、被害額は、約8億9800万円（平成27年下半期・約15億3000万円、同上半期・約15億4300万円）、実被害額は、約7億7200万円（平成27年下半期・約12億6400万円、同上半期・約13億8300万円）となっている。

前年の直近の半期（平成27年下半期）、前年の対応する半期（平成27年上半期）と比して、件数が増加しているが、被害額、実被害額はいずれも減少している。これは、「大口の法人口座の被害が減少したため」である。個人名義口座、法人名義口座別で見ると、個人名義口座の被害は、件数にして811件、被害額が、約7億6900万円、実被害額が、約6億7500万円である。一方、法人名義口座の被害は、件数にして、46件、被害額が、1億2900万円、実被害額が9700万円である。個人口座名義の被害は、件数にして大半を占めるばかりでなく、被害額・実被害額でも、それぞれ、85.6%、87.4%を占めるに至っている。

大口の法人口座の被害の減少の主要な要因は、「信用金庫の被害額の大幅な減少…

(7)　https://www.npa.go.jp/cyber/pdf/H280908_banking.pdf。

によるところが大きい。これは、ウイルス感染端末の早期検知等の対策によるものと考えられる」と分析されている。対応するかのように、法人口座では、電子証明書を利用しての被害はゼロとなっている。ただし、個人口座の方は、被害に係る口座名義人のセキュリティ対策として、ワンタイムパスワードを利用していたものが 31.4% となっている。個人口座の被害のうち、ワンタイムパスワードを利用していなかったものは 60.4%、不明が 8.1% である。

② 金融庁統計

金融庁の統計 [8] によると、「インターネットバンキング犯罪」は、平成 26 年度は 1407 件、平成 27 年度は 1541 件、平成 28 年度については 4 月～ 9 月までであるが、393 件である。

偽造・盗難キャッシュカードや盗難通帳による被害に比して、平均被害額が大きい点は変わりがない。

個人については、平成 26 年度は、件数が 1247 件、被害額が 13 億 9400 万円、平均被害額が 111 万円となっており、平成 25 年度に比して、件数および被害額は減少しているが、平均被害額は増加している。平成 27 年度は、件数が 1383 件、被害額が 14 億 6000 万円、平均被害額が 105 万円となっており、件数、被害額が前年度よりも増加しているが、平均被害額は 25 年度と同額となっている。平成 28 年度（4 月～ 9 月）は、件数が 365 件、被害額が 3 億 8900 万円、平均被害額が 106 万円である。

③ 全銀協アンケート調査

全銀協の平成 28 年 12 月末時点におけるアンケート調査が公表されている [9]。なお、平成 26 年からは特例会員を含めた 192 行を対象としたアンケート調査となっている。

「『インターネット・バンキングによる預金等の不正払戻し』等に関するアンケート結果」によると、平成 26 年度は、個人顧客は件数が 1094 件、金額が 12 億 1800 万円、法人顧客は件数が 121 件、金額が 4 億 6200 万円である。平成 27 年度は、個人顧客は、件数が 1218 件、金額が 12 億 6100 万円、法人顧客は、件数が 65 件、金額が 5 億 2100 万円である。平成 28 年度は第三四半期まで（4 月～ 12 月）で、個人顧客は、件数が 508 件、金額が 5 億 8500 万円、法人顧客は、件数が 46 件、金額が 1 億 8700 万円となっている。

---

(8) http://www.fsa.go.jp/news/28/ginkou/20161216-3.html。

(9) http://www.zenginkyo.or.jp/fileadmin/res/news/news290224_2.pdf。

④　補償状況

補償については、金融庁統計によれば、平成 26 年度 1173 件（84.1%）、平成 27 年度 1263 件（84.4%）、平成 28 年度（4 月～ 9 月）262 件（84.2％）である。また、全銀協アンケート調査の結果によれば、補償件数は、個人顧客の場合、平成 26 年度は 94.2%、平成 27 年度は 98.4%、平成 28 年度（4 月～ 12 月）は 93.1％である。

3　自主ルール――全国銀行協会申し合わせ

（1）　個人顧客に関する全銀協申し合わせ

全銀協では、個人顧客に関して、平成 20 年 2 月 19 日付け「預金等の不正な払戻しへの対応について」申し合わせを公表した。これに先立ち、偽造・盗難カード等による預金の不正払戻しについては、平成 17 年に、預貯金者保護法が制定され、平成 18 年に施行されていた。上記申し合わせにおいては、預貯金者保護法の対象とはなっていないインターネット・バンキング・サービスによる預金等の不正払戻しへの対応が含まれている。その対応内容は、インターネット・バンキングによる預金等の不正払戻しについて、銀行に過失がない場合でも、顧客自身の責任によらずに被害にあった場合には、その被害は補償するというものである。また、補償請求の際には、顧客にも銀行に対する被害内容の速やかな連絡、事情説明、捜査機関への説明などを求めることが併記されている。補償額については特段の限定は設けられていない。また、「インターネット・バンキングに係る補償の対象・要件・基準等について」が用意されており、それによれば、この申し合わせのもとでは、補償の有無は次のようになる。

まず、補償の要件として、金融機関への速やかな通知と十分な説明、捜査当局への被害事実等の事情説明（真摯な協力）が、掲げられている。また、消極要件として、金融機関への通知が被害発生日の 30 日後まで行われなかった場合、親族等による払戻しの場合、虚偽の説明を行った場合、戦争・暴動等の社会秩序の混乱に乗じてなされた場合が、あげられている。

そのもとで、「補償基準」として、預金者無過失の場合は全額補償、預金者に過失・重過失ある場合は個別対応、とされている。

盗難通帳の場合には、預金者の過失の場合には 75％補償、重過失の場合は補償しない、という補償基準が示されているのに対し、インターネット・バンキングの場合には「個別対応」となっている理由は、次のように説明されている。インターネットの技術や犯罪手口が日々高度化している中で、各行のセキュリティ対策を含めその

サービス内容が一様ではないため、重過失・過失の類型化やそれに応じた補償割合の定型的策定は困難であって、顧客の態様や状況等を加味して個別判断とならざるを得ない。

以上からすると、補償の有無は、速やかな通知や誠実な説明等の一定の手続要件が課されつつ、であるが、次のようになると解される。

① 銀行に過失があった場合には、金融機関が責任を負う。この場合、民法 478 条によっても弁済者保護は働かず、そもそも預金払戻しが効力を持たないため、顧客の責任によるかどうかを問わず、預金支払債務が存続する。もっとも、顧客の故意の場合は除かれるだろう。故意の証明は金融機関側がすることになろう。また、顧客に重過失があっても責任外とはならない。もっとも、額が全額となるのかは不透明である。過失相殺的処理がありうるかは、民法 478 条をめぐっても問題となり、また、別途顧客の重過失や過失による損害賠償が問題となり得、それとの相殺という処理もありうる。

② 銀行に過失がなかった場合にも、顧客の責任によらないときは、補償する。

③ 銀行に過失がなかった場合であって、顧客の責任による場合には、故意のときは補償しない。重過失や過失のある場合については、その事情により個別具体的に判断する。

なお、インターネット・バンキングについては過失・重過失の類型化は困難であるとされているが、盗難通帳による場合については、過失・重過失になりうる場合として、次の場合が示されている。

重過失については、（やむを得ない事情があるときを除き）預金者が他人に通帳を渡した場合、（やむを得ない事情があるときを除き）預金者が他人に記入・押印済みの払戻請求書や諸届を渡した場合、その他預金者にこれらの場合と同程度の著しい注意義務違反があると認められる場合、である。過失（軽過失）については、通帳を他人の目につきやすい場所に放置するなど第三者に容易に奪われる状態に置いた場合、届出印の印影が押印された払戻請求書・諸届を通帳とともに保管していた場合、印章を通帳とともに保管していた場合、その他本人にこれらの場合と同程度の注意義務違反があると認められる場合、である。

（2） インターネット・バンキング利用規定

前記（1）の全銀協申し合わせのもと、各行のインターネット・バンキング利用規定がどのように定められているかを確認すると、一例に、三井住友銀行の場合には、

次のような定めがされている[(10)]。

2. 本人確認

(2) 本人確認手続

1. 契約者が端末による取引の依頼を行う場合は、当行宛に契約者番号またはサービス利用口座のうち任意の口座の口座保有店の支店番号（または支店名)、サービス利用口座の科目番号（または科目名)、サービス利用口座の口座番号（以下「契約者番号等」といいます）または契約者が取引の依頼に使用する当行所定の端末の固有情報（以下「端末固有情報」といいます。）および第一暗証等の所定事項を当行所定の方法により正確に伝達するものとします。端末が店頭パソコンの場合は、契約者はキャッシュカードを店頭パソコンに挿入し、キャッシュカード暗証を当行所定の方法により正確に伝達するものとします。
2. 前記 2.（2）①の内容について、当行が確認した契約者番号またはサービス利用口座店の支店番号（または支店名)、サービス利用口座の科目番号（または科目名)、サービス利用口座の口座番号または端末固有情報および第一暗証が、もしくは端末が店頭パソコンの場合は、挿入されたキャッシュカードに記録された情報（以下「キャッシュカード情報」といいます。）および当行が確認したキャッシュカード暗証が、契約時に発行する契約者番号または契約者が当行宛に届出を行ったサービス利用口座（自動的に指定されるものを含みます。）の口座保有店の支店番号（または支店名)、サービス利用口座の科目番号（または科目名)、サービス利用口座の口座番号（やむをえない事情により口座番号等が変更された場合はその番号）または契約者が当行宛に届出を行った端末固有情報および契約者が当行宛に届出を行った第一暗証（契約者が前記 2.（1）（ア）又は（イ）により変更した場合は最新の第一暗証)、もしくは端末が店頭パソコンの場合は、サービス利用口座の普通預金のキャッシュカード情報および契約者が当行宛に届出を行ったキャッシュカード暗証と各々一致した場合には、当行は契約者からの取引の依頼とみなし、受付手続を行います。
3. 当行所定の取引については、契約者は、前記 2.（2）①で当行に伝達する内容に加え、ワンタイムパスワード（暗証カード方式を利用する場合は第二暗証、第三暗証（前記 2.（1）⑧（イ）により変更または再発行した場

(10) http://www.smbc.co.jp/kojin/direct/kitei1.html（下線は筆者による)。

合は最新の第二暗証および第三暗証）および各情報等の所定事項）を当行所定の方法により正確に伝達するものとします。 但し、端末が店頭パソコンの場合は当行所定の方法により確認するものとします。

4. 前記２．(2) ③の内容について、当行が確認したワンタイムパスワード（暗証カード方式を利用する場合は第二暗証、第三暗証および各情報等）が、当行が保有するワンタイムパスワード（暗証カード方式を利用する場合は第二暗証、第三暗証（前記 2.（1）（イ）により変更または再発行した場合は最新の第二暗証および第三暗証）および各情報等）と一致した場合には、当行は契約者からの取引の依頼があったものとみなし受付手続きを行います。

４．免責事項等

(1) 本人確認

前記 2.（2）により本人確認手続を経た後、取引を行った場合は、当行は利用者を契約者本人であるとみなし、端末、端末固有情報、暗証番号等について偽造、変造、盗用、不正使用その他の事故があっても、そのために生じた損害については、当行に責めがある場合を除き、当行はいっさいの責任を負いません。但し、損害の発生が盗取された暗証番号等を用いて行われた不正な振込等（以下「不正な振込等」といいます。）によるものである場合、契約者は、後記４の２による補てんの請求を申し出ることができるものとします。また、端末が店頭パソコンの場合、損害の発生が偽造カードまたは変造カードによるものである場合の当行の責任については、後記４の３によるものとします。

(2) 通信手段の障害等

以下の場合、そのために生じた損害については、当行に責めがある場合を除き、当行はいっさいの責任を負いません。

1. 当行および金融機関の共同システムの運営体が相当の安全対策を講じたにもかかわらず、通信機器、回線およびコンピュータ等の障害ならびに電話の不通等の通信手段の障害等により、取扱が遅延したり不能となったとき。
2. 当行および金融機関の共同システムの運営体が相当の安全対策を講じたにもかかわらず、当行が送信した情報に誤謬・遅延・欠落等が生じたとき。

(3) 通信経路における取引情報の漏洩等

公衆電話回線、専用電話回線、インターネット等の通信経路において盗聴・不正アクセス等がなされたことにより契約者の暗証番号、取引情報等が漏洩した場

合、そのために生じた損害については、当行に責めがある場合を除き、当行はいっさいの責任を負いません。 但し、上記により漏洩した暗証番号等の盗用により損害が発生した場合の当行の責任については、後記4の2による補てんの請求を申し出ることができるものとします。

(4) 印鑑照合等

契約者が届出た書面等に使用された印影（または署名）を、当行が届出の印鑑（または署名鑑）と相当の注意をもって照合し、相違ないものと認めて取扱を行った場合は、印章（または署名）またはそれらの書面につき偽造、変造、盗用その他の事故があっても、そのために生じた損害については、当行はいっさい責任を負いません。

4の2.【暗証番号の盗用等による振込等】

(1) 盗取された暗証番号等を用いて行われた不正な振込等（以下「不正な振込等」といいます。）については、次の各号のすべてに該当する場合、契約者は当行に対して後記(2)に定める補てん対象額の請求を申し出ることができます。

1. 暗証番号等の盗取または不正な振込等に気づいてからすみやかに、当行への通知が行われていること。
2. 当行の調査に対し、契約者より十分な説明が行われていること。
3. 当行に対し、警察署に被害届を提出していることその他盗取にあったことが推測できる事実を確認できるものを示すなど、被害状況、警察への通知状況等について当行の調査に協力していること。

(2) 前記(1)の申出がなされた場合、不正な振込等が契約者の故意または重過失による場合でなく、かつ、利用する端末の安全対策や暗証番号等の管理を十分に行っている等、契約者が無過失である場合、当行は、当行へ通知が行われた日の30日（ただし、当行に通知することができないやむをえない事情があることを契約者が証明した場合は、30日にその事情が継続している期間を加えた日数とします。）前の日以降になされた不正な振込等にかかる損害（手数料や利息を含みます。）の額に相当する金額（以下「補てん対象額」といいます。）を補てんするものとします（なお、契約者が無過失と認められない場合にも一部を補てんすることがあります）。

(3) 前記(1)、(2)は、前記(1)にかかる当行への通知が、暗証番号等の盗取が行われた日（当該盗取が行われた日が明らかでないときは、不正な振込等が最初に行われた日。）から、2年を経過する日後に行われた場合には、適用されな

いものとします。

(4)　前記（2）にかかわらず、次のいずれかに該当する場合には、当行は補てんを行いません。

1. 不正な振込等が行われたことについて当行が善意かつ無過失であり、かつ、次のいずれかに該当すること。

   A　契約者の配偶者、二親等内の親族、同居の親族、その他の同居人、または、家事使用人によって行われたこと。

   B　契約者が、被害状況についての当行に対する説明において、重要な事項について偽りの説明を行ったこと。

2. 暗証番号の盗用等が、戦争、暴動等による著しい社会秩序の混乱に乗じまたはこれに付随して行われたこと。

(5)　当行が前記（2）に定める補てんを行う場合、不正な振込等の支払原資となった預金（以下「対象預金」といいます。）について、契約者に払戻しを行っている場合には、この払戻しを行った額の限度において、補てんは行わないものとします。また、契約者が、不正な振込等を行ったものから損害賠償または不当利得返還を受けた場合も、その受けた限度において同様とします。

(6)　当行が前記（2）により補てんを行った場合には、当該補てんを行った金額の限度において、対象預金に関する権利は消滅します。

(7)　当行が前記（2）により補てんを行ったときは、当行は、当該補てんを行った金額の限度において、盗取された暗証番号等により不正な振込等を行った者その他の第三者に対して契約者が有する損害賠償請求権または不当利得返還請求権を取得するものとします。

4の3.【端末が店頭パソコンの場合の偽造カード等による振込等】

端末が店頭パソコンの場合の偽造カードまたは変造カードによる振込等については、契約者の故意による場合または当該振込等について当行が善意かつ無過失であって契約者に重大な過失があることを当行が証明した場合を除き、その効力を生じないものとします。この場合、契約者は、当行所定の書類を提出し、カードおよび暗証の管理状況、被害状況、警察への通知状況等について当行の調査に協力するものとします。

上記規定によれば、金融機関が責任を負うかどうかについては、次の規律となっている。

まず、所定の本人確認手続を経て取引を行ったときは、不正使用等の事故があっても、損害について一切の責任を負わない（免責規定４（１））。また、インターネット等による暗証番号等の漏洩があり、それにより生じた損害については、金融機関に責めに帰すべき事由があるときを除き、一切の責任を負わない（免責規定４（３））。ただし、いずれについても、次の場合には、補填請求ができる。

盗取された暗証番号等を用いて行われた不正な振込等による場合に、手続要件（速やかな通知、十分な説明、調査協力）のもと、不正な振込等自体についての故意または重過失でない、かつ、利用端末の安全対策や暗証番号等の管理などにつき無過失である場合には、対象額として、通知の日の 30 日前以降の損害額（通知できないやむを得ない事由があるときはその事情の継続期間部分で 30 日前より前のものを加算）を補填する。

さらに、消極要件（不正振込等について金融機関が善意・無過失であって、契約者と一定の関係にある者による行為、契約者の虚偽説明、暗証番号盗用等が著しい社会秩序の混乱に乗じ、または付随して行われたといういずれかの事情がある場合）がある。

なお、金融機関に過失がある場合には、そもそもが、免責の対象ではなく、顧客は預金債権を失わない。

また、補填請求についてのこれらの要件を満たさない場合にあっても、特に契約者が無過失であるとは言えない場合も、個別事情によってはなお補填が認められる場合があることが留保されている。

補填請求については、期間限定があり、暗証番号等の盗取が行われた日（それが明らかでないときは、不正な振込等が最初に行われた日）から、2 年を経過する日より後に通知が行われた場合には、補填請求の規定は適用されない。

一方、店頭パソコンによる場合の、偽造・盗難カードを用いての不正振込等については、別途の定めがあり、契約者が故意の場合、または銀行が善意無過失で契約者が重過失の場合、以外は振込等は無効とされている（金融機関が責任を負う）。すなわち、契約者が軽過失にとどまる場合には、振込等は無効であり、金融機関がなお払戻しの義務を負う。

以上のインターネット・バンキング利用規定においては、不正な振込等自体についての預金者の故意・重過失と並んで、利用端末の安全対策や暗証番号等の管理の過失（無過失）が要求されている点が注目される。一方で、インターネット・バンキング利用規定によっても、過失・重過失の内容や、過失があるとされてもなお補填が認められる場合がどのような場合なのかは、はっきりとしない。

（3） 法人顧客に関する全銀協申し合わせ

平成 26 年 5 月 15 日、全銀協では「法人向けインターネット・バンキングに係る預金等の不正な払戻しへの対応について」申し合わせを行い、さらに、同年 7 月 17 日、「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方について」申し合わせを行った。

5 月 15 日の申し合わせでは、被害補償についての基本的な考え方として、法人と個人とでは異なるという従前よりの考え方を確認しつつ、各行が個別にその要否を判断するという立場が示されている。

7 月 17 日の申し合わせでは、個人に比して法人の場合にはセキュリティ対策等への対応力は相対的に高いと考えられるとして、個人と法人との別という点を確認しつつ、金融機関に法的責任がないと考えられる場合にも法人顧客の被害補償につき個別行の経営判断として検討するという立場が示されている。そのうえで、考慮点として、法人顧客に求められるセキュリティ対策、補償の減額や否定となりうる場面が、より具体的に示されている。

すなわち、セキュリティ対策に関して、まず、銀行の側で講ずるセキュリティ対策として、電子証明書のセキュリティ強化策、認証方法の強化策、資金窃取を防止する運用、セキュリティ対策ソフトの提供、トランザクション認証の導入、リスクベース認証の導入・強化、不正なログイン・取引等の検知、顧客のセキュリティレベルに応じたサービス提供、その他各行が有効と考えるセキュリティ対策、これらの実施とともに、説明・周知措置、サポート対応が掲げられている。

法人顧客の側では、実施を求めるものと、推奨するものとが分けられている。求めるものは、銀行が導入しているセキュリティ対策の実施、インターネット・バンキングに使用するパソコンの基本ソフト等のソフトウエアの最新化、メーカーのサポート期限の経過したソフト等の利用停止、パソコンへのセキュリティ対策ソフトの導入と最新状態への更新、インターネット・バンキングに係るパスワードの定期的変更、銀行指定の正規の手順以外での電子証明書の利用の停止である。また、推奨されるセキュリティ対策として、インターネット接続時の利用をインターネット・バンキングに限定すること、パソコンや無線 LAN のルータ等について、未利用時は可能な限り電源を切断すること、取引申請者と承認者とで異なるパソコンの利用、振込・払戻し等の限度額を必要な範囲で極力低く設定、不審なログイン履歴や身に覚えのない取引履歴・取引通知メールがないかの定期的確認である。

補償の減額または否定となりうる事例として、個別判断ではあるという留保付きながら、次のような例が示されている。

第１は、環境整備といいうる点であり、上記の法人顧客に求められるセキュリティ対策の不実施である。第２は、不正取引があった場合の手続的要件ともいうべきものであり、身に覚えのない残高変動や不正取引が発生した場合に一定期間内に銀行への通知がされない場合、不正取引が発生した場合の一定期間内の警察への通知の不実施、不正取引が発生した場合の、銀行による調査や警察による調査への協力の不実施が、それに当たる。第３は、不正取引自体についての、法人顧客の「過失」と見られる場合である。正当な理由なく、他人にID・パスワード等を回答した、あるいは、安易に乱数表等を渡した場合、パソコン等が盗難にあった場合において、ID・パスワード等をパソコン等に保存していた場合、銀行が注意喚起しているにもかかわらず、注意喚起された方法でメール型のフィッシングにだまされる等、不用意にID・パスワード等を入力してしまった場合、があげられている。より一般的に、これらと同程度の注意義務違反が認められた場合、が挙げられている。第４は、消極的要件に関わると見られるが、会社関係者の犯行であることが判明した場合である。

以上が法人顧客の場合についての申し合わせである。法人と個人とでは、セキュリティ対策への対応力が異なり、また、被害についての耐性も異なることや、個人の生活との分断が困難であることなどの事情があるため、一般的に、法人顧客に要請されるセキュリティ対策や注意義務の程度までは、個人顧客の場合には要請されないことがあるとは言えよう。

そうだとすると、個人顧客の被害についての金融機関の責任分担を考えるときには、法人顧客についての責任分担における顧客負担が個人にとって最大限であると考えることができ、具体的には、個人であったときにはどれが緩和されうるかという観点から、具体的な場面を探ることができよう（後記**５（４）**）。

	盗難通帳（個人）	IB 規定（個人）	IB 規定（法人）
銀行側の施策 銀行の「過失」		・所定の本人確認措置 ・不正振込等についての無過失 ・インターネット等による暗証番号等漏洩につき、無過失	各種のセキュリティ対策
顧客側の管理		利用端末の安全対策について無過失	セキュリティ対策（要請） ・銀行の導入するセキュリティ対策 ・基本ソフトウエアの最新化

			・サポート期限経過ソフトの利用停止 ・セキュリティ対策ソフトの導入・更新 ・パスワード等の定期的変更 ・不正規の電子証明書の利用停止
	重過失 ・他人に通帳を交付 ・他人に記入押印済の払戻請求書等を交付	暗証番号等の管理について無過失	他人に ID 等を回答 他人に乱数表等を渡す
	過失（軽過失） ・他人の目につきやすい場所に放置するなど、第三者に容易に奪われる状態に置いた ・届出印の押印された払戻請求書を通帳とともに保管 ・印章と通帳とを一緒に保管		盗難にあったパソコンに ID 等を保存
			注意喚起にもかかわらずそのままフィッシング被害にあう等の不用意な ID 等の入力
			その他同程度の注意義務違反
		不正な振込についての善意・無重過失	
			セキュリティ対策（推奨） ・インターネット接続時の利用限定 ・利用時外の電源の切断 ・申請者と承認者とで別パソコンの利用 ・限度額の最小化 ・不審なログイン等の履歴の定期確認
不正払出しに関する手続的要件	・速やかな通知 ・十分な届出 ・盗取の警察への届出	・速やかな通知 ・十分な説明 ・調査協力	・銀行への適時の通知 ・警察への適時の通知 ・調査への協力
消極要件	親族等の行為	配偶者、一定の親族等の行為	会社関係者の犯行
	虚偽説明	虚偽説明	

	虚偽説明 社会秩序の混乱に乗じた盗用等	社会秩序の混乱に乗じた盗用等	
対象額の限定	通知が被害発生後30日以内に行われなかった場合　※およそ補償否定？対象範囲について否定？	通知前30日より以降（やむを得ない事由による通知不能のときは拡張）の損害	

４　裁判例

インターネット・バンキングにおける不正送金・不正払出が行われた場合の金融機関の責任の有無が問題となった下級審裁判例に、次の３つがある。

大阪地判平成19年4月12日金融法務事情1807号42頁 (11)

東京高判平成18年7月13日金融法務事情1785号45頁 (12)

東京地判平成18年2月13日金融法務事情1785号49頁（上記東京高判の第1審）

いずれも、個人名義口座の例である（ただし、用途は必ずしも個人の生活用ではない）。また、インターネット・バンキング・サービス利用規定上の免責条項に基づく免責が認められている。

（1）　大阪地判平成19年4月12日金融法務事情1807号42頁

大阪地判平成19年の事案は次のとおりである。

原告Xは、A株式会社の代表取締役である。Xは、平成15年5月22日、被告Y銀行阿倍野支店で、残高別金利型普通預金口座を新たに開設し、800万円を預け入れた（本件口座）。この800万円はXの個人資金であるが、Xの経営するA社の運転資金上の必要があれば利用する予定であり、その必要がなければ引き出す予定はない金員であった。同日、Xは、Yの行員からの勧誘を受け、付加サービスとしてイン

(11)　評釈等として、石毛和夫・銀行法務21・677号62頁（2007）・同・銀行法務21・686号26頁（2008）、宮川不可止・金法1819号33頁（2007）、新井剛・ジュリスト1393号108頁（2010）。

(12)　評釈等として、中舎・前掲注（1）、石原全・私法判例リマークス35号46頁（2007）、渡辺博己・銀行法務21・677号56頁（2007）、丸山絵美子・金判1336号180頁（2010）、浅井弘明・銀行法務21・668号56頁（2006）・同・銀行法務21・672号19頁（2007）、島田邦雄＝沖田美恵子・金法1791号50頁（2007）。

ターネット・バンキング・サービスの利用契約を締結した。

平成17年10月4日、A社で1000万円程度の資金繰りが必要となったため、本件口座の800万円の資金を用意するために、口座残高を確認したところ、800万円あるはずの預金残高が1万8382円しか残っていないことを発見した。Xは、同日、Y阿倍野支店に連絡を入れ、Y担当者のもとへ話し合いに行き、警察署に被害届を〔Y阿倍野支店被害として〕提出した。

この間、平成17年7月19日から同月22日にかけて、インターネット・バンキング・サービスを利用して、8件の振込が、他行の別人名義の同一口座になされ、合計798万2000円が振り込まれていた（加えて振込手数料計3360円が控除されている)。1回の振込は、100万円または100万1000円であった。

この振込がXの意思に基づくものであったかどうかも争点の1つとなっているが、Xの意思に基づいてされたものとは認められないと認定されている。この振込については、主体も、暗証番号等入手の経緯も不明であるが、A社のパソコンの本体HDに情報として保管されていた暗証番号等の情報が何らかの形で流出し、第三者がそれを悪用した可能性が高いと判断されている。

顧客がインターネット・バンキング・サービスを利用する場合、本人確認情報として、ログインする際に、自らの契約者番号および第1暗証（顧客設定）を入力し、その後、各手続に応じて第2暗証（YがXに対して発行した暗証カード記載の乱数表の中からコンピュータが無作為に指定する可変数字)、第3暗証（上記乱数表のうち、顧客ごとに異なる特定の1マスに記載されている2桁の数字。暗証カード郵送時に同封のカード台紙に記載されている）を入力する。振込の場合には、第2暗証が必要であるが、登録先口座の場合は必要ではない。本件の8件の振込については、最初の振込について、契約者番号、第1暗証、第2暗証が入力されて行われているが、いずれも正規の数字と一致していた。最初の振込によって、振込先口座が登録されており、その後の7件の振込は登録先口座への振込として、契約者番号と第1暗証で本人確認が行われていた。

本件口座はXの個人資金の口座であったが、A社の運転資金に利用する可能性もあり、Xはその管理をA社経理担当のBに任せた。Xは、Bに暗証カードを見せ、第1暗証等の暗証番号や契約者番号を伝えた（暗証カードはXの自宅の金庫に保管した)。Bは、以前から、B自身の預金の口座番号や暗証番号、証券会社の口座番号や暗証番号、Bの自宅のガスや電気の顧客番号等の備忘録として「番号」というエクセル・ファイルを作成し、各番号等を書き込んでおり、A社の預貯金のみならず、運転資金用に開設されたX個人名義の預貯金については一部管理を任されるように

なったため、これらの口座番号等もこのファイルに書き込むようになっていた。そこで、Bは、Xから伝えられた本件口座のインターネット・バンキング・サービス用の契約者番号、第1暗証、第2暗証のための乱数表の数字、第3暗証を特定するための数字・文字を、同ファイルに入力・保存した。このファイルには、読み取り・書き込みのパスワードをかけて保存していた。平成17年10月4日の残高の発見もXから指示を受けたBが発見し、Xに伝えたものであった。

Xは、消費寄託契約に基づき、Yに対し、振込送金された当該金員および振込手数料分合計798万5360円の返還とそれに対する返還請求後の遅延損害金（年6%）の支払を求めた。

Yは、インターネット・バンキング・サービス利用規定（本件約款）の免責条項を援用し、①所定の本人確認をした後、取引を行った場合には、Yは利用者を契約者本人であるとみなし、端末、暗証番号等について偽造、変造、盗用、不正使用その他の事故があっても、そのために生じた損害については、Yに責めがある場合を除き、いっさいの責任を負わないとする、4条（1）項、②公衆電話回線、専用電話回線、インターネット等の通信経路において盗聴・不正アクセス等がされたことにより契約者の暗証番号、取引情報等が漏洩した場合、そのために生じた損害については、Yに責めがある場合を除き、いっさいの責任を負わないとする、4条（3）項による免責を主張した。

このほか、民法478条の該当性も争点となっているが、本件約款中の免責条項による免責が認められたため、判断はされていない。

大阪地裁は、約款4条（1）項による免責をとりあげ、この約款の規定はもとより有効であるとした上で、最高裁平成5年7月19日を参照しつつ、「銀行の設置した、契約者番号、暗証番号等により本人確認を行うインターネット・バンキング・システムを利用して、預金者以外の者が、当該預金から振込手続を行ったとしても、銀行が交付した契約者番号が使用され、正しい暗証番号等が入力されていた場合には、銀行による契約者番号及び暗証番号等の管理が不十分であったなどの特段の事情がない限り、銀行は、入力された契約者番号及び暗証番号等とシステムのデータベースに登録されている当該預金者の契約者番号、暗証番号等を確認して現金の振込を実行した以上、銀行に「責めがある場合」には当たらないと解すべきである」としている。

この枠組みのもとで、所定の本人確認措置がとられていることから、焦点は、Y銀行に「責めがある場合」と言えるか、「銀行による契約者番号及び暗証番号等の管理が不十分であったなどの特段の事情」があるか、に置かれた。

大阪地裁は、Yの「責めがある場合」といえるか否かについて、次の諸点を取り上

げている。①インターネット・バンキング・サービスにおける「本人確認情報の管理」の評価、すなわち、契約者番号と第１暗証の入力によるログイン、各手続に応じた第２暗証・第３暗証の入力、特に振込といった資金移動に関して可変暗証である第２暗証を用いることは、「本人確認情報の管理」としては有効な方法であると評価されている。付言して、暗証番号について異なる番号を所定の回数（3 回）以上連続して入力した場合には、契約者に対するサービスの利用を停止することになっていることがあげられている。②通信についての暗号化や外部侵入措置の実施、すなわち、顧客とＹのセンターコンピュータ間でインターネット上で行われるデータ通信に、「現時点」では最も解読困難であると言われる暗号通信方式が採用され、さらに、当該インターネット・バンキング・サービスのシステムには複数の外部侵入防止措置がとられている。③契約者への注意喚起、すなわち、Ｙは、本件約款および当該インターネット・バンキング・サービス利用の手引きにおいて、具体例もまじえて第三者に知られることのないよう厳重に暗証番号を管理するよう注意書きを記載しており、暗証番号についての注意喚起をしている。

大阪地裁は、これらの事情から、Ｙは、「本人確認情報（暗証番号等）の管理及びセキュリティ対策に有効な方法をとっている上、本人確認情報の管理について十分な注意喚起を行っている」とし、そうである以上、「契約社番号及び暗証番号等の管理について不十分であったなどの特段の事情が存在することを認めることはできず、Ｙの「責めがある場合」には当たらない」と結論している。

逆に、大阪地裁は、Ｘの次の主張については、これを退けている。④具体的な注意喚起について、Ｘのサービス申込み当時、複数の各種パスワード等をパソコンのエクセルファイルに保存する行為は通常行われており、遅くとも本件各振込が行われるまでに、Ｙは暗証番号をパソコン本体に保存している場合に何らかの形で第三者に暗証番号等を読み取られ、第三者が本人になりすまして振込送金の手続をする危険性を予見可能であったから、Ｙは、消費寄託契約に付随する信義則上の義務として、暗証番号等をパソコンに保存しないよう顧客に説明し、注意喚起する義務の主張に関し、平成 17 年 6 月の調査会社調査によれば、500 人中 55％の人が ID 番号やパスワードをパソコンのファイル等に記録する方法をとっている。しかし、本件では、上記パソコン内にある情報がウィルスソフト等によって読み取られたと特定することまではできず、また、仮にそのように読み取られたとしても、平成 17 年 7 月の時点で発生していたインターネット・バンキングのスパイウェアによる被害は、利用者がインターネット・バンキングを利用した際に入力したＩＤや暗証番号等を盗み取るものであり、パソコン内に保存していたファイルそのものが盗み取られ、不正に預金が送金さ

れたという被害の報告がされていたとは認められないため、本件各振込がされる時期までに、パソコン本体のファイルに保存された暗証番号等がパソコンを通じて読みとられる危険性があることをＹにおいて予見することはできなかったし、また、さらに、Ｘがサービスを申し込んだ当時やあるいは本件各振込がされた時点において、本件のように、銀行名、口座番号、インターネット・バンキングのホームページのURL、契約者番号、第一暗証、乱数表、第三暗証の全てを同一シートに記載し、パソコン内のファイルに保存することまでをＹが想定することもできなかったとして、Ｙとしては、上記程度の概括的な注意喚起の方法をとることで足りる。⑤Ｙによる当該インターネット・バンキング・サービスのシステムの安全性に関して、預金契約の存続する限り、具体的な危険性を顧客に周知させ、万一暗証番号等をパソコンに保存しているような場合には直ちに削除する義務の主張については、④についての判断が同様に当てはまるというものと見られる。⑥Ｙによる当該インターネット・バンキング・サービスのシステムの安全性に関して、インターネット・バンキング・サービスを利用して振込送金がされた場合には直ちに電子メールなどにより預金者に連絡する義務について、パソコン内に保存されていたファイルの内容が読み取られるという被害をＹにおいて予測することはできなかったというべきであるから、そのような被害を回避する方法として上記連絡義務を課することはできない。

大阪地裁は、これらの判断において、本人側の帰責性については掲げていない。Ｙによる被害の予測可能性の点において、すべての情報を１つのシートに記載して保存するというような方法をとることは想定外であるとしており、暗に、あるいは間接的に、そのような保存方法をとったことについてのＸの帰責を基礎づける事情と考えているかにも見える（なお、事実関係としては、そこに記載された各種の口座のうち、不正送金がされたのは、本件口座のみであった)。また、ＸがＢに口座の管理を一任し、契約者番号や暗証番号等をＢに知らせていたことや、Ｂによるそれらの管理状況、またパソコンへのアクセスの状況などは、本人の意思による振込と言えるかどうかの点、Ｂが使用していたパソコン内に書き込まれていた暗証番号等の情報が何らかの形で流出し悪用された可能性が高いという判断を導く事情として示されているにすぎない。

また、Ｘの帰責を正面から取り上げないという姿勢は、被害についてのＹの予測可能性のみを問題とする点にも現れ、あるいはつながっている。パソコン本体での情報保存が危険の高い行為であるとは予測できないというのは、Ｘにおいてはいっそう妥当する。それからすれば、そのようなリスクに対する分担のあり方として、それはＸ負担であるとなることが、適切であるのかが問われようが、大阪地裁の枠組みの

もとでは、Y の「責めがある場合」でないときは顧客負担ということになる。

（2） 東京高判平成18年7月13日金融法務事情1785号45頁、東京地判平成18年2月13日金融法務事情1785号49頁

東京地判平成 18 年、東京高判平成 18 年の事案は次の通りである。

原告 X は、平成 16 年 1 月 13 日、被告 Y 銀行と預金寄託契約を締結し、Y 銀行日野駅前支店に総合口座を開設し、インターネット・バンキング・サービスを申し込んだ。X は中古車販売を業とする A 有限会社に勤務し、A 社の取引に係る金銭の出入金に利用するための口座開設であった（なお、上記インターネット・バンキング・サービスは、その利用規定上、日本国内に居住する個人のみが利用対象者とされていた)。X は、インターネット・バンキング・サービスを利用していたが、それは A 社の端末（パソコン）を利用してアクセスをしていた（A 社の端末は、常時電源が入ったままの状態となっていた。）

平成 16 年 7 月 9 日に 500 万円、同月 11 日に 300 万円が、それぞれ、インターネット・バンキングにより、Y 銀行荻窪支店に開設された別人名義の口座に振込入金する操作がされ、上記 500 万円についてはその操作の同日（9 日）に、300 万円については翌日（12 日）に振込入金が実行された。

Y は、本件各振込の後、遅くとも、同月 12 日の夜頃までに、X に対し、電子メールで本件各振込が行われた旨の通知をした。

X は、平成 16 年 7 月 12 日に本件各振込が行われたことを知った。その経緯は次のとおりである。X は、同日昼頃に、A 社の従業員に本件口座の記帳を行わせたところ、本件各振込が記帳されていたとの報告を受けたため、A 社の他の従業員に X のお客様番号およびログインパスワードを知らせて、本件システムにアクセスさせ、本件口座の残高照会をさせた。

X は、同月 13 日、本件口座を解約し、Y に対し、寄託していた 800 万円の支払を請求した。Y は、保険金 50 万円を X に支払ったが、750 万円については支払を拒絶した。そこで、X が、750 万円の支払とこれに対する平成 16 年 7 月 13 日以降の遅延損害金（年 5%）の支払を求めた。

Y は、インターネット・バンキング・サービス利用規定における免責条項を援用し、所定の「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えは、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」との規定による免責を主張した。

争点となったのは、Y の免責の可否である。免責条項の有効性と、その解釈・適用との双方が争われている。このほか、X からは、システムへの直接ハッキングによる不正侵入の可能性も指摘されたが、本件システムへの不正侵入の形跡はなく、正しいお客様番号および暗証番号等が入力されていたことが認定されている。

免責条項の有効性について、X は、インターネット・バンキング・サービス上のリスクを一方的に預金者に負担させる規定となっているから無効であると主張した。一審、二審ともこの主張を退けている。一審判決は、Y が、本件システムにつき、暗号化、再暗号化してのデータベース格納、暗証番号等の入力を一定回数以上間違えたときの手続停止、振込手続き後の電子メールによる通知、システムの常時監視という措置がとられていることをあげ、Y は、本件システムにつき、不正送金等を未然に防止するための相応のセキュリティシステムを構築していたものと言えるから、X の主張は失当であるとしている。二審判決も、一審判決の判断を引用した上で、追加的に、本件免責条項は、Y に「預金寄託契約上の安全保管義務違反等が存在する場合には適用されず、Y が無条件に免責されるものではないと解されるから、本件免責条項が預金者に一方的に危険を負担させるものとして無効であるとは解されない」としている。

免責条項の適用に関して、一審判決は、Y が、「当該振込請求者が振込を請求する権限を有する者と信じたことにつき過失がある場合にまで免責を認める趣旨のものではな」いとし、その過失に関して、「インターネット・バンキング・システムを利用した振込に関して必要とされる銀行の注意義務は、預金者保護の見地から、社会通念上一般に期待されるところに相応するものでなければならない」という一般論を示す。続けて、しかし、お客様番号、ログインパスワード及び暗証番号等により本人確認を行うシステムを採用している銀行のインターネット・バンキング・システムにおいて、それを利用して預金者以外の者が当該預金から振込を行ったとしても、当該振込に際して、正しい情報入力がされていた場合には、「銀行によるお客様番号、ログインパスワード及び暗証番号等の管理が不十分であったなどの特段の事情がない限り」当該銀行は、入力された情報とシステム内のデータベースに登録されている情報とを突合して預金の振込を実行した以上、本件免責条項により免責されると解するのが相当であるとする。

本件システムにおいては、暗号化、再暗号化、常時監視システムによる不正侵入監視措置がとられている中で、突合が行われて、情報の一致を確認して、振込実行が行われたもので、本件各振込実行にあたり Y に過失があったとはいえず、本件免責条項により免責される、としている。

Xからは、インターネット・バンキング・サービスによる振込につき、Yには「無権限者が預金者の預金を不正に送金するという事故が起こらないようなシステムを構築すべき義務」があったにもかかわらず、Yが提供したサービスには安全管理上の不備があり、これに起因して本件の口座からの預金移動の事態を引き起こしたのであるから、免責はされないと主張された。Xが問題としたのは、乱数表による可変番号の仕組みをとっていないこと、利用する端末機を限定登録してそれ以外からはアクセスできない仕組みを採用していないこと、直接ダイヤルアップ接続してアクセスできる仕組みを用意していなかったこと、である。

一審判決は、これらの諸点に関して、そもそも、窓口における対面での確認方法、ATMによる機械式の方式による確認方法（通帳やキャッシュカードの真正など）とも異なり、インターネット・バンキング・サービスによる振込は入力された情報が銀行側のデータベースに格納された情報と一致することを機械的に確認する方法等によって、当該振込の請求者が正当な権限を判定するもので、①SSLの技術を用いたお客様番号、ログインパスワード、暗証番号等の暗号化、ログインパスワードと第2暗証番号についてはY独自の方法で再暗号化してデータベースに格納、②暗証番号の入力を一定回数以上間違えるとそれ以上手続を行えなくなる措置、③振込手続が行われたときは、速やかに、届出先のアドレスに電子メールで通知、さらに、④システムの常時監視、という措置をとっていたことを挙げ、「インターネットバンキング・サービスにおいては、当該振込の請求をする者の権限の有無の判定は、銀行側が構築するシステムにより、機械的、形式的にされるものであることに照らすと」、Yは、本件サービスを提供するについて、本件システムを、「全体として、可能な限度で」無権限者による振込を排除しうるよう構築・管理しており、Yに注意義務違反はないとした。また、具体的なXのあげる諸点について、インターネット・バンキングにおけるセキュリティの一手法であるが、セキュリティの方法には種々のものがあり得るのであって、これらの措置をとっていないことをもって、システムの構築・運営につき、注意義務違反があったということはできないとしている。

二審判決は、一審判決を引用しつつ、付加的な判断として、乱数表の不使用について、乱数表を用いた可変数字による暗証のシステムについて、実際、そのようなシステムをとっている銀行があるとしつつ、「上記サービスを提供している銀行のうち安全対策としてどれだけの割合で上記システムを採用しているかは明らかではないから、本件サービスを提供するに当たって上記システムを採用していなかったYが安全対策として特異の取扱いをしており、この点に預金寄託契約上の安全保管義務違反があったとは認められない」としている。

X側の保管・管理状況については、一審判決が、システムの構築・運営についての義務違反というXの主張に関連して、これをとりあげている。事情としては、その利用規定上、利用対象者を個人に限定しているにもかかわらずA社の取引に使用するために預った金銭の出入のために開設・利用していたこと、A社の従業員に口座記帳等を行わせていたこと、A社のパソコンを利用して本件システムにアクセスしていたこと、同パソコンは第三者が使用できないようにはなっていなかったこと、本件各振込の後にA社の従業員にお客様番号等を教え、本件システムにアクセスさせ残高照会をさせていたこと、をあげ、ここから、Xが、自らA社の従業員等にお客様番号等を教えたり、A社の従業員が同社のパソコンを利用して本件システムへアクセスしている際に、お客様番号等を知るなどしたことにより、Xのお客様番号等が第三者に漏洩したのではないかと思われる、としている。なお、スパイウエアによる漏洩については、それをうかがわせる証拠はないとしており、同様の判断を示している。

Yによる顧客への周知措置に関しては、一審判決が、不特定多数が利用する共用端末機で暗証番号等を入力する場合のリスク等をユーザーに対して積極的に啓蒙することが求められるというXの主張に対し、Yがホームページで、インターネットカフェなどにある、顧客の管理しているパソコン以外を利用するときは、入力した内容がパソコンに残ってしまい他人による悪用の可能性がある旨の注意喚起をし、警告措置をとっていたとして、対策に欠けるところはないとしている。

（3） ATMを用いた無権限払戻しについての最高裁判決

上記の3つの裁判例は、インターネット・バンキング・サービス利用規定上の免責条項による免責を認めたものである。

このような免責条項については、そもそも、預金取引規定上の免責条項につき、民法478条との関係で、同条の定める責任を軽減するものではなく、いわば、「無過失」の前提となる注意義務の具体化を図るものと位置づけられている(13)。

また、非対面での預金取引について、ATMの機械式支払について、2つの判決が、これらの裁判例に影響をしていると思われる。最判平成5年7月9日判例時報1489号111頁・金融法務事情1369号6頁、最判平成15年4月8日民集57巻4号337頁である。前者は、（1）の大阪地判において援用されている。

最判平成5年7月9日は、真正カードによるATMでの無権限払戻しに関する免

(13) 最判昭和50年6月24日金融法務事情763号34頁、潮見佳男『債権総論Ⅱ（第3版）』249頁（信山社）(2005)。

責条項の適用について、「銀行の設置した現金自動支払機を利用して預金者以外の者が預金の払戻しを受けたとしても、銀行が預金者に交付していた真正なキャッシュカードが使用され、正しい暗証番号が入力されていた場合には、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、銀行は、現金自動支払機によりキャッシュカードと暗証番号を確認して預金の払戻しをした場合には責任を負わない旨の免責約款により免責されるものと解するのが相当である」としている。また、当該カードは、磁気ストライプ上に、顧客が届け出た暗証番号がコード化されて記録されており、このようなキャッシュカードは、市販のカードリーダーをパソコンに接続することにより、暗証番号を解読することができるものであった。同判決は、そのような方法で暗証番号を解読するためにはコンピューターに関する相応の知識と技術が必要であることは明らかであり、また、本件支払がされた当時、このような解読技術はそれほど知られていなかったから、銀行が「当時採用していた現金自動支払機による支払システムが免責約款の効力を否定しなければならないほど安全性を欠くものということはでき」ないとしている。

最判平成5年7月9日のもとでは、所定の本人確認措置が合理的なもの・適切なものであることを前提に、所定の本人確認措置がとられて、システムが利用された場合には、「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、免責が認められること、また、ATMによる支払システムの安全性が問題となり、その欠落によっては、免責約款の効力が否定されうることが示されていた。

最判平成15年4月8日は、預金通帳によるATMでの無権限払戻しの有効性が問題となったものであり、通帳機械払いに関する免責条項が存在していなかったため、民法478条の適用・類推適用が問題となった。同判決は、「無権限者のした機械払の方法による預金の払戻しについても、民法478条の適用があるものと解すべきであり、これが非対面のものであることをもって同条の適用を否定すべきではない」として、民法478条の問題としたうえで、「債権の準占有者に対する機械払の方法による預金の払戻しにつき銀行が無過失であるというためには、払戻しの際に機械が正しく作動したことだけでなく、銀行において、預金者による暗証番号等の管理に遺漏がないようにさせるため当該機械払の方法により預金の払戻しが受けられる旨を預金者に明示すること等を含め、機械払システムの設置管理の全体について、可能な限度で無権限者による払戻しを排除し得るよう注意義務を尽くしていたことを要するというべきである」とした。「機械払の方法による払戻しは、窓口における払戻しの場合と異なり、銀行の係員が預金の払戻請求をする者の挙措、応答等を観察してその者の権限の有無を判断したり、必要に応じて確認措置を加えたりするということがなく、専ら

使用された通帳等が真正なものであり、入力された暗証番号が届出暗証番号と一致するものであることを機械的に確認することをもって払戻請求をする者が正当な権限を有するものと判定するものであって、真正な通帳等が使用され、正しい暗証番号が入力されさえすれば、当該行為をする者が誰であるのかは全く問われないものである。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るよう組み立てられ、運営されるものであることを要するというべきである。」

（2）の東京地判および東京高判は、最判平成15年4月8日に明示の言及はしていないものの、その影響がうかがわれる。同判決によると、「銀行において、預金者による暗証番号等の管理に遺漏がないようにさせるため当該機械払の方法により預金の払戻しが受けられる旨を預金者に明示すること」「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、」「機械払システムの設置管理の全体について、可能な限度で無権限者による払戻しを排除し得るよう」同システムを組み立て、運営する注意義務が、課される。

なお、顧客と金融機関との間のリスク分担という点からは、顧客側の事情の考慮や、過失相殺的な処理の可否が問題となる。平成15年最判は、通帳機械払のシステムを採用している旨をカード規定等に規定せず、預金者に対する明示を怠ったため、顧客は通帳機械払いの方法により預金の払戻しを受けられることを知らなかったという点をとらえ、注意義務を尽くしていたとは言えないとしている。その際、顧客にも、本件の暗証番号を自動車登録番号の4桁の数字と同じ数字とし、通帳を当該車両のダッシュボードに入れたまま、自宅近くの駐車場に駐車していたため車両ごと盗難にあい、本件暗証番号を推知されて払戻しが行われたという事情を指摘して、本件払戻しがされたことについて顧客にも「帰責事由が存するというべきであるが、この程度の帰責事由をもってY〔銀行〕に過失があるとの前記判断を覆すには足りない」としている。したがって、金融機関の注意義務違反・過失判断において、顧客の事情や帰責が考慮されることが前提とされていると言える。

学説では、民法418条の類推適用や、顧客の帰責事由を基礎とした損害賠償責任との相殺による割合的処理も主張されている。

５　若干の検討

以上で、広い意味での現状、すなわち、被害等の実情、全銀協の申し合わせおよび金融機関の自主的な対応、免責条項をめぐる裁判例を確認した。以下では、このような現状を踏まえて、個人向けインターネット・バンキング・サービスにおける無権限の払戻し（具体的には、他人名義の口座への不正送金・振込の形をとる）がされた場合の金融機関の責任範囲（顧客との間の分担のあり方・基準）について、若干の点を整理・指摘しておきたい。

（1）　問題の性格

第１に、問題の性格である。現在、この問題は、3段階で扱われている。すなわち、民法 478 条の適用・類推適用による弁済の効力と弁済者の保護、約款規定における免責条項、約款規定における補塡・補償の3段階である。もっとも、約款規定における免責条項は民法 478 条の注意規定であり、民法 478 条において要求される注意義務と同様の注意義務を尽くすことを定めるものと解されており、さらには、民法 478 条は、対面での払戻しのみならず機械式の払戻しにも適用され、さらにその場合の弁済者の注意義務は、弁済行為に向けられた注意だけではなく、むしろ、システムの安全性と管理における注意義務であることが認められている（前記最判平成５年７月９日、最判平成 15 年４月８日）。

これに対し、預貯金者保護法においては、偽造カードについては[(14)]民法 478 条の適用が排除されて、その特則が設けられ、特に預金者の帰責性（故意の場合と重過失の場合）を正面から取り込んだ弁済者の免責の規律が打ち出されている。

しかし、権利者の帰責性についても、判例上、弁済者の過失判断の中で考慮要素として勘案する余地があり（前記最判平成 15 年４月８日）、478 条の要件としてこれを要求する見解も有力である。そうだとすると、確かに、民法 478 条は権利者（預金者）の帰責を正面から要件としては要求しておらず、また単純な金銭債務の履行についてはその規律が妥当するとしても、単なる金銭債務の履行にとどまらず、利用者に、提供するインターネット・バンキングというサービスを安心して用いることができるようにする（あるいは、安心して用いることのできるインターネット・バンキン

(14)　インターネット・バンキング・サービスの場合には、真正な暗証番号の不正入手として盗難カードに類似するとみることもできるが、しかし、預金者がシステムへのアクセス手段をコンピュータ外で別途管理することができず、同じ暗証番号等が重複して不正利用されても被害が発生するまで気づかないという点に着目して、むしろ偽造カードに類似するとみるのが妥当であると指摘されている（中舎・前掲注（1）14 頁）。

グ・サービスを提供する）という預金契約上の附随義務[15]の履行が問題となっているのがこの場面での問題であり、システムの設計・管理上の注意義務が弁済者の過失の前提となる場面であることからすると、預貯金者保護法の規律は、民法478条の適用・類推適用において達成しうるものとおよそ異質のものとは言えないと思われる。なるほど、偽造カードの場合には、預金者に軽過失がある場合で、金融機関が機械式預貯金払戻しについて善意無過失である場合は、有効な払戻しとはならない点（預貯金者保護法4条）では、民法478条のもとでの結果とは異なるようにみえるが、偽造カードを可能にするという点でのシステム設計・管理上の帰責があるという評価のもとでのことであるから、それを考慮すれば、民法478条のもとでは導かれない帰結を特別法によってもたらしているとは必ずしも言えない。むしろ、民法478条のもとでは曖昧であるところを、場面に即して明確に規律したと評価することもできるように思われる。

インターネット・バンキング・サービスの不正送金・不正払戻しの場合には、上記のとおり3段階で問題が構成されているために、補塡・補償による金融機関の負担は、金融機関が民法478条や免責条項のもとで、免責され、したがって本来なら責任を負わないところを、経営判断によって損失を負担しているかにとらえられなくもない。しかし、その補塡・補償を通じてなされる金融機関の損失負担は、民法478条の適用・類推適用から導かれうる範囲とも言え、ひいては免責条項によっても軽減されるものではなく（これを軽減するものだとすると、免責条項の不当条項性が問題となろう）、本来責任を負わない金融機関が顧客サービスのために損失を負担しているという性格ではなく、事象の性質上、帰されるべき負担を負っているという性格のものではないかと思われる。

（2） 双方無責の場合の負担を金融機関負担とすることの相当性

本場面への民法478条の適用・類推適用において、独立した要件ではなくとも預金者の帰責性が勘案され、弁済者・金融機関の免責には預金者の帰責性を要するという立場からすれば、双方無責の場合には、金融機関は免責されず、損失は金融機関の負担となる。このような処理は、システムの脆弱性が現実化したときの負担のあり方として、取引の実質に即した衡平の観点から支持されうるものと思われる。

また、「効率性」の観点からも、次のように分析されていることは示唆的である。すなわち、「効率性」の観点からの分析として、①損失分散原則（最小コストでのリスク中立性を達成できる主体に損失を負担させるべきであるとする原則）、②損失削

(15) 中舎・前掲注（1）13頁。

減原則（より低コストで損失の削減を実現しうる当事者に責任を課し、それによって損失削減のインセンティブ付けをすべきであるとする原則）、③損失賦課原則（責任の分配の実現の観点から、手続面において、簡明さと明確さを重視すべきであるとする原則。すなわち、簡明で明確な結果をもたらす損失分担ルールを望ましいとする）の３つの基本原則を基礎とし、その相互関係をふまえて、効率的な損失分担を考える見地から、金融機関による損失負担を基本とするのが合理的であるという。具体的には、①損失分散原則からは、不正払戻しにより生じる損失が保有資産比で大きくなりうることや、損失を分散することが金融機関に比して困難であることから、預金者に損失を負担させることは望ましくない(16)。②損失削減原則からは、その１つの要素である予防策とそのためのインセンティブという観点から、カードの仕様技術やインターネット・バンキングのセキュリティ技術等について金融機関は将来にわたって損失の発生をより低コストで抑えうる予防策にかかる技術的イノベーションを促進できるが、損失を基本的に預金者の負担とするルールのもとでは金融機関にこうしたイノベーションの促進に取り組むインセンティブを十分には与えられない。③損失賦課原則からは、発生した損失との対比でみた訴訟費用等が高すぎることを主たる要因として正当な権利が実現されない可能性があるという問題が、正当な権利者が預金者であるときにより顕著に顕れることから、不正払戻しから生じた損失を「第一義的に」預金者に負担させるルールは合理的ではなく、むしろ「第一義的な」損失を金融機関に負担させることが望ましい。以上からすると、全銀協の申し合わせやそれを受けた各行のインターネット・バンキング利用規定において、預金者の故意により預金の不正払戻しが行われたなどの一部の場合を除き、損失の大部分を原則として金融機関が負担するというあり方が、生体認証の利用等の技術的なイノベーションを進展させ、結果として社会全体の効率性を高めうる、という(17)。

（３） 預金者の一定額の当然負担について

前記（２）で言及した「効率性」の観点からの分析においては、一定額までをリ

(16) キャッシュカードによる支払免責条項の考察において、保険ないしはそれと同視される損害分散制度の利用可能性の観点から、リスクの同質性が高いため、保険料は金融機関が一括して負担し顧客に一律に転嫁する方が顧客が個別に保険を付すよりも効率性の面から好ましいという指摘として、山下友信「銀行取引と免責約款の効力」『石田喜久夫・西原道雄・高木多喜男先生還暦記念論文集下・金融法の課題と展望』198 頁（日本評論社、1990）。

(17) 大川昌男＝吉村昭彦「預金の不正払戻しに関する個人預金者と銀行との間の損失分担ルールについて――ハードローとソフトローの協働――」GCOE ソフトロー・ディスカッション・ペーパー・シリーズ 2009-5（2009）23 ～ 24 頁。ただし、同論文は、後述するように、預金者の一定額の当然負担を組み合わせることが効率的であるとしている。

テール顧客に無過失責任で損失を負担させ、一定額以上を銀行に無過失責任で損失を負担させるルールが望ましく、かつ、一定額は、原則として低額に設定すべきであると指摘され、また、全銀協の申し合わせ等の内容についての改善措置の１つとして提言されている[(18)]。

これは、損失削減原則から、つまり、その要素の１つである予防策の観点から、一定の範囲内で預金者に負担を求めることが肯定され、かつ、感応度の問題からその一定の範囲は多額のものとすべきではない、という。すなわち、インターネット・バンキングによる預金の払戻しの場合にも、金融機関だけではなく、預金者と金融機関の双方が損失を回避するための対策をとりうる場合に該当し、そのときは損失回避措置をとるためのインセンティブという観点により、かつ、全銀協の申し合わせや各行のインターネット・バンキング規定が採用する過失責任主義に基づくルールは、過失認定のための訴訟コストが高く、損失分担ルールとして望ましくないという[(19)]。

一定限度でのリテール顧客の当然の損失分担については、帰責性のない顧客が負担することの正当化の問題（さらには「納得」感の問題）がある。キャッシュカードによる機械式払いの分析においてであるが、この点を、保険のシステム（保険料）とみることで、正当化する見解もある[(20)]。

より問題なのは、一定範囲の負担（特に一定額の負担。一定割合とする場合もそこに上限額を組み合わせるなら同様の問題がある。）として、インセンティブと感応度との両方を勘案した適切な負担水準を一律に決めることができるのかであろう。過失の判断や認定の困難とコストはその通りであるとしても、それが、一律に適切な負担水準を決定することの方が容易であり、実現可能性が高いとは、言いにくいように思われる。

---

(18) また、インターネット・バンキングに関してではなくキャッシュカードによる支払免責条項に関する考察の中でではあるが、アメリカ合衆国やドイツの例などをも参考にして、顧客が損害の一定部分（一定額（50 ドル）の例と一定割合（10%）の例がある）を負担する解決が提案されている（山下・前掲注（14）197 ～ 201 頁。ただし、キャプテン端末を通じた資金移動取引などについては、キャッシュカードにかかる支払免責条項と同様の問題点もあるが、利用の状況にはかなり異なった面もあり、キャッシュカードに見られるリスクの均質性が失われているような場合には、そもそも単純に金融機関の損害負担が合理的だとも言えず、キャッシュカードについての立論がそのまま妥当しないとされている（同 201 頁））。

(19) 大川＝吉村・前掲注（15）23 頁、25 ～ 26 頁。

(20) 預金者に帰責事由があっても一定の例外を除いて損害を負担しなくてもよいこととの見合いとされる（山下・前掲注（14）199 頁）。システム利用者全般（それは金融機関によってコスト転嫁されることになる）ではなく、被害を受けた者のみの負担も保険料という説明が可能であるのか疑問がなくはない。また、キャッシュカード以外の支払手段について当然に妥当するかについては、上記論文において慎重な検討が必要とされていることにつき、同 201 頁（前掲注（16））参照。

また、インターネット・バンキングのみそのような手法をとることの問題もあろう。

そうであるならば、むしろ、どのような場合が過失や重過失と判断されるかの具体例や基準をガイドラインなどによって積み重ね、明確にすることで、過失の判断や認定の困難さとコストを減じることが有用ではないかと思われる[21]。

（4）「過失」、「重過失」について

① 全銀協の申し合わせから

全銀協の申し合わせ、平成20年2月19日の「預金等の不正な払戻しへの対応について」では、不正送金の場合に、銀行が善意無過失であって、民法478条が適用されるならば、免責される場合であっても、一定の場合には「補償」を行うことが示されている。

具体的には、顧客が無過失の場合（その責めによらずに被害にあった場合）には、その被害は補償するというものであり、基本姿勢は、このような不正送金についてのリスクは、銀行が負担することを基本姿勢としたうえで、顧客に「過失」があった場合には、補償は否定ないし制限されるが、その定型化は行わず（行えず）、それは個別事情を踏まえた、各金融機関における判断によるというものであった。ここでは、故意の場合は、補償対象とならないのは明らかであるが、重過失の場合に否定されること自体も示されていない。

盗難通帳についての扱いとの対比[22]では、重過失の例として示されている、他人に通帳を渡したり、他人に記入済みの払戻請求書等を渡した場合について、インターネット・バンキング・サービスの場合には、顧客番号、各種暗証番号等、インターネット・バンキング・サービスの利用に必要な情報を伝えることを対応する事情として想定できるが、通帳の交付等の場合はそれを用いて払戻しができ、逆にそれ以外の方法による払戻しであったという場合は考えにくいのに対し、インターネット・バンキング・サービスの場合には、たとえ、その形で他人に必要情報を伝えたとしても、不正送金との因果関係は不明であって、当該不正送金についての重過失と言えるのかは疑問である。また、そのような因果関係が特定できる場面は、伝えられた主体が行為を認めているなどの場合を除けば、稀であろう。そうすると、これらの情報、すな

(21) 預金者の当然の一部負担・上限設定との関係においてではないが、「利用者に過失がある場合」の類型化の必要性を指摘し、それを試みるものとして、森藤聡志「インターネットバンキングにおける不正利用への対応状況と金融実務」金法1937号46～47頁（2012）参照。

(22) ただし、前述のとおり、インターネット・バンキング・サービスの場合には、むしろ偽造カードに類似するとみるのが妥当であると指摘されている（中舎・前掲注（1）14頁）。

わちインターネット・バンキング・サービスの利用に必要な情報を他人に伝えたとしても、それ自体は、不正送金を引き起こした過失ではなく、日常的な管理方法の「落ち度」であって間接的なもの、危険を惹起させる行為にとどまる。また、それらの情報を他人に伝えたことをどう見るかについても、その重要性の認識を顧客が持つ必要があり、それが普遍化しているか、または、銀行において周知のための措置をとっている必要がある[(23)]。

盗難通帳について預金者の過失（75％補償）とされている事情と対比すると、第三者に容易に通帳を奪われる、押印された払戻請求書等を通帳とともに保管する、印章と通帳を一緒に保管するというのは、別々の管理によって単独では払戻しの措置がとることができないようなものについて、共に管理するなどの形で、不正払戻しを容易化する行為と言える。インターネット・バンキング・サービスの場合には、必要情報を一括してアクセスできるような状態に置いているという場合が想定されるが、「第三者に容易に奪われる」という中には、すべての情報を紙に書いて、あるいはプリントアウトして保管していたというような物理的保管については盗難通帳と並行して考えられるが、データとしてパソコンなどに保存されているケースにおけるスパイウェアによる情報流出などの場合に、「第三者に容易に奪われる」という状態がどのような状態なのか、それはありうるのかが問題になろう。

インターネット・バンキング・サービスの場合の「指針」としては、むしろ、法人向けの申し合わせにおいて示された考え方が、個人向けの場合に妥当するのかを考えるのがより有用なように思われる。

法人向けの申し合わせにおいて、銀行側のセキュリティ対策は、個人向けと抽象的・基本的には変わらないと思われる。顧客のセキュリティレベルに応じたサービス提供、説明・周知措置は、顧客が個人であることによって、具体的な内容が変わりうる（法人も様々であって、個人事業主と変わらないものもある）ということではないだろうか。

顧客の側での措置であるが、銀行が導入しているセキュリティ対策の実施、インターネット・バンキングに使用するパソコンの基本ソフト等のソフトウエアの最新化、メーカーのサポート期限の経過したソフト等の利用停止、パソコンへのセキュリティ対策ソフトの導入と最新状態への更新、インターネット・バンキングに係るパスワードの定期的変更、銀行指定の正規の手順以外での電子証明書の利用の停止のう

(23) これらの点は、平成20年当時はともかく、これだけインターネット・バンキング・サービスの被害が社会的にも注目を集めていることからすると、その重要性の認識は普遍化しているように思われる。

ち、インターネット・バンキングに使用するパソコンの基本ソフト等のソフトウエアの最新化、メーカーのサポート期限の経過したソフト等の利用停止、パソコンへのセキュリティ対策ソフトの導入と最新状態への更新は、個人にも期待できる事項に思われる。インターネット・バンキングに係るパスワードの定期的変更も実行できなくはなさそうであるが、他方で、個人であっても様々なパスワードを有していることを考えると、定期的変更がそれほど期待できるかどうか、当該パスワードの管理方法（頻繁に変えるならば記憶によることはできず、どこかにデータとして保管せざるを得ない）との関連にも留意する必要があると思われる。

法人顧客に推奨されるセキュリティ対策としてあげられる、インターネット接続時の利用をインターネット・バンキングに限定すること、パソコンや無線 LAN のルータ等について、未利用時は可能な限り電源を切断すること、取引申請者と承認者とで異なるパソコンの利用、振込・払戻し等の限度額を必要な範囲で極力低く設定、不審なログイン履歴や身に覚えのない取引履歴・取引通知メールがないかの定期的確認については、限度額についてはすでに銀行で措置が取られているのではないかと思われ、また、取引通知メールの確認は個人顧客にも求めることができるのではないかと思われる。

具体的な事例との対比では、正当な理由なく、他人に ID・パスワード等を回答した、あるいは、安易に乱数表等を渡した場合については、上記のとおりである。また、パソコン等が盗難にあった場合において、ID・パスワード等をパソコン等に保存していた場合については、個人顧客の場合、どこに保存するべきであったのか、そのような保存がされているパソコンについては盗難にあえばリスク負担ということになるとすると、個人顧客については妥当しないように思われる（が、どうだろうか)。銀行が注意喚起しているにもかかわらず、注意喚起された方法でメール型のフィッシングにだまされる等、不用意に ID・パスワード等を入力してしまった場合については、個人顧客にその認識をどこまで期待できるか、そのリテラシーの問題があるのではないだろうか。

② 裁判例から

インターネット・バンキング・サービスに関する裁判例は、いずれも、全銀協申し合わせ前の判決であり、かつ、免責条項の問題を扱うものである。全銀協申し合わせに即するなら、金融機関が善意無過失であることを前提としたうえで、顧客が無過失であるときは、補償を行うというのが基本姿勢であるから、金融機関の無過失と顧客の無過失が問題となり、特に、金融機関が注意義務を尽くしていても、顧客もまた求

められる注意を尽くしていたなら、顧客は補償請求ができることになるので、その点で、土台は違っている。また、特に、顧客の「無責」(「無過失」)が、裁判例でとりあげられる以上にクローズアップされることになろう。

とはいえ、そこで、金融機関の「帰責」を基礎づける事情や、顧客の「帰責」に関わる事情は、全銀協申し合わせのもとでも、なお参考になるものと思われる。

前記の裁判例から、挙げられた事情を列挙すると、次のとおりである。

①金融機関のインターネット・バンキングのシステムについてのセキュリティ対策

本人確認の措置の適切さ(ID、ログインパスワード、各種段階での暗証)

通信についての暗号化、特に、最新の解読困難な方法の採用

ログインパスワード等についての再暗号化してのデータベース格納

暗証番号について異なる番号を所定の回数以上連続して入力したときの手続・利用停止

外部からの侵入防止措置

常時不正侵入監視

乱数表など可変暗証の利用

利用端末の限定

ダイヤルアップ接続の利用可能性

どのくらいの銀行が、当該セキュリティ対策を実施しているのか(業界標準?)

振込の都度の、速やかな、届出先アドレスへの電子メールによる通知

②金融機関の顧客に対する説明・情報提供・注意喚起・警告

約款および利用の手引きにおける注意書

ホームページでの、共用端末利用の危険についての告知

スパイウェアの危険性についての警告、パソコンでのデータ保存の危険についての警告

〔パソコンに保存されたデータの削除〕

③顧客のID、パスワード等の保管

他人に管理を一任、他人にID・パスワード等を伝える

エクセルファイルに一括して記録・保存

ファイルについて、読み取り・書き込みパスワード設定

データの入ったファイルをパソコンに保存

データの入ったパソコンの利用の状況(使用中に他の者が横から見られる状態)

データの保存されたパソコンの利用者の限定(共用端末)の有無

④その他の顧客の事情

個人名義口座であるが、会社の運転資金、取引による金銭の出入のための利用

これら①～④に抽出した事項には、特に問題とならないとされたものがあるが、当時の状況においてであるため、現時、すなわち、インターネット・バンキング・サービスによる不正送金が急増しており、スパイウェアやフィッシングなどの手法も（少なくとも金融機関にとっては）よく知られるようになっており、可変暗証の重要性なども（金融機関において）共通理解となっていると思われる現時の状況においては、異なる判断となりうるだろう。

そのようなものとして、振込についての通知がある。「速やかな」通知が、東京高判平成 18 年 7 月 13 日における Y 銀行のサービスではされていたが、むしろ、「直ちに」通知することが、システム上も可能であるし、求められるのではないか。また、そもそも、この点についての大阪地裁の判断には批判が投げかけられている。また、周知・警告措置についても、約款や最初に交付・送付される手引きに書かれているとか、ホームページに記載がある（記載の仕方にもよる）というので、周知として十分とした点は、現在では疑問と言うべきだろう。スパイウェアやフィッシングなどの手法についての警告と対策の提示、パソコンでのデータ保存についての注意点の説明などは、現時点においては、当然に要請されよう。また、東京高判では、乱数表による可変暗証について、どのくらいの銀行が導入しているか不明である以上は、それを取るべきだったとは言えないという判断がされており、一種、業界での普及状況が問題とされているように見える。数だけではなく、その程度のセキュリティ対策が期待されるのか、という観点が基礎となるので、その点からすると、むしろ、現在では、可変暗証が求められるのではないかと思われる[(24)]。

(24) 不正送金そのものに向けられた過失ではなく、環境整備やシステムの設営を問題とするために生じる問題であるが、銀行に求められるセキュリティ対策に不備があった場合には、仮に、それが原因でなかったことが明らかになったとしても、なお、銀行の免責は否定されることになるだろうか。例えば、フィッシングなどの手法についての警告をしていなかった、スパイウエア対策について情報提供をしていなかったが、それとは別の方法で、情報が漏洩し、あるいは顧客がそれを他人に伝えたために、その他人が、不正送金処理を行ったという場合などが、想定場面である。債務不履行に基づく損害賠償であるなら因果関係の問題となりうる。システム設計・管理上の注意義務をいう場合、当該損害発生の回避に向けられた注意義務違反を問題とするのか、当該損害ではなくより一般的な安全性に向けられた注意義務違反を問題とするのか、後者であれば、リスク分担としては金融機関が負うことになるが、そのような場合には、割合的処理が妥当なように思われる（過失相殺的処理として 418 条の類推適用、または預金者の過失による損害賠償との相殺）。なお、この問題については、丸山・前掲注（12）182 頁も参照。

（5） 預金者の「過失」判断について

預金者の「過失」（重過失、軽過失）の判断については、最終的には個別の事情によるものの、一般的にはこうであるという具体例を明らかにしていくことが有用であると思われるが、一方で、次の３点に留意すべきであろう。

第１は、金融機関の注意義務についてもそうであるが、預金者の「過失」の内容および程度の判断基準として、技術の進展や社会情勢の変化によってそれは変わりうるし、また、その変化がこの分野は非常に速いと思われることである。たとえば、暗証番号を第三者から推測しやすい番号にすることを避けるべきことや、長期間同じ暗証番号を使うべきではないことは、金融機関による再三の告知等によって、かなり、一般的な認識になってきていると思われる[(25)]。

第２は、望まれる行動をとらなかったことと義務違反たる過失との相違である。上記のとおり、第三者から推測されやすい暗証番号を用いないことや暗証番号をそれなりの頻度で変更することは、現在では、預金者に望まれる行動といってよいであろう。しかし、第三者から推測されやすい暗証番号を用いていたことや、長期間同じ暗証番号としていたことが、直ちに預金者の「過失」（これだけならば、該当しうるとしてもおそらく軽過失であろうが）と言えるかはまた別問題である。ちょうど、事業者にとって、ベスト・プラクティスと注意義務とにはずれがあり、ベスト・プラクティスを履践していなかったとしても注意義務違反として責任や負担を負うかは別問題であるのに相応して、預金者の側でも、ベスト・プラクティスとして望まれる行動と過失と判断される注意義務違反とは必ずしも一致しないことを念頭に置くべきであろう。

第３は、望まれる行動をとっていないことにとどまるのか、それとも注意義務違反と判断されるのかについては、特に消費者の場合には、生身の生活者であるがゆえの限界を考慮する必要があると思われる。確かに、金融機関からの画面上等による再三の警告にもかかわらず第三者から推測されやすい暗証番号を長期間用いていることは、消費者の「落ち度」ではあろう。しかし、電子化された社会において、どれだけのIDとパスワードの中で生活しているかを考えるとき、すべてのパスワードを異なるものとして、かつ、頻繁に変更するということが、果たして、損失負担を正当化するほどの「落ち度」と言えるかは、この点も顧慮して判断する必要があろう（変更の頻度などの判断にもかかわろう）。

---

(25) 森藤・前掲注（20）42頁参照。

（6） 個人と法人

預貯金者保護法も、全銀協の申し合わせやそれを踏まえた各行のインターネット・バンキング規定の内容も、個人顧客と法人顧客という類型によって、損失分担を変えている。

預貯金者保護法が、対象を個人の預金者に限定したのは、「本法律の立案にあたり、資金面や人材面などで金融機関と個々の預貯金者との間には、一般的に大きな力の差があることにかんがみ、預貯金者を保護する必要があるとの消費者保護的な考え方をベースに検討されたため」と解説されている[(26)]。

キャッシュカードを用いた機械式払戻しにせよ、インターネット・バンキングの不正振込・払戻しにせよ、そのときの損失分担のあり方という問題を考える観点としては、払戻しのシステムの設計・管理上の安全性に関する利用者と提供者との間のリスク分担という観点と、消費者保護という観点の２つが考えられる。前者の観点から考えるとしても、分担は利用者の属性により影響を受けうるが、前者の観点からすれば、損失分担についての個人・法人を通じたルールが設けられ、そのルールの適用において、法人・個人、あるいは消費者といった属性が考慮され、注意義務の内容や程度、それを受けた具体的な分担の結果が変わりうることになろう。後者の観点からすれば、消費者ではない法人の問題は別問題となるが、その場合も、システムの悪用を防止しうる方策を利用者と提供者の両方がとりうる以上は、両者のそれぞれの注意義務、望まれる行動、損失分担という観点からの検討が法人（非消費者）について行われることになる。その意味では、個人と法人という区分や類型化は、連続的なものとも言える。損失分担のあり方としては、生身の生活者としての消費者、消費者保護の観点など、消費者には特有の考慮がありうること、法人と個人とを切り分けの基準とすることは保証の規律や債権譲渡登記の規律にも例があることを考えると、合理性を持つものと考えられる[(27)]。預貯金者保護法が、個人の預金者に対象を限定したことの

(26) 石田祐介「『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』の概要」金法 1751 号 23 頁（2005）。もっとも、法文上は「個人」が対象であるから、個人事業者もこれに含まれる（「偽造・盗難カード預貯金者保護法 Q&A」金法 1756 号 23 頁（2005）（佐伯聡））。

(27) それぞれの規律が法人と個人とで切り分けていることには、例えば債権譲渡登記であれば電子認証の手法との関係など、それぞれの理由があるのであって、およそ、法人と個人という区分が正当性を有するわけではない。また、消費者保護の観点を打ち出すなら、消費者契約法における消費者概念を採用し、消費者と事業者（非消費者）という区分を採用することも考えられる。もっとも、消費者契約法上の消費者概念や、消費者契約法の規律の妥当範囲については、団体の扱いや、消費者的事業者の扱いなどの問題も生じており、むしろ、法人と個人とで一応の区分とする（つまり、その注意義務の内容や程度はさらに個別の属性や耐性などを勘案して決せられる）ことも簡明であって、実践しやすい方法として合理的であると

問題は、それゆえに、法人についての特則が空白の状態に置かれた点にあると思われる。

（7） その他

全銀協の申し合わせやそれを受けた各行のインターネット・バンキング規定の内容の改善点として、効率性の観点から――前述のリテール顧客の一定範囲の当然負担と並んで――通知義務についての提言がされている。

すなわち、迅速な通知は損害の発生・拡大を抑止するための効果的な対策となり、そのためのインセンティブを与える観点から、具体的な経過日数に応じて一定の上限額を設定するという提案である[(28)]。

預金者から金融機関への通知を迅速に行うことおよびそのインセンティブの重要性には共感するものの、預金者の当然の一部負担および上限額設定との組み合わせの提言であり、当然の一部負担・上限額設定ではなく過失との組み合わせをとるとした場合に採用可能であるのか、そのときのあり方がどうなるのかは、なお一考を要しよう。

思われる。

(28) 大川＝吉村・前掲注（15）26 ～ 27 頁。