金融庁金融研究研修センター
フォーラム「金融機関と情報セキュリティ」概要報告

- 開催日時：平成 17 年 12 月 7 日（水）14:00～17:00
- 場所：中央合同庁舎第 4 号館　2 階　220 会議室

12 月 7 日（水）、合同庁舎第 4 号館会議室において、金融研究研修センターフォーラム「金融機関と情報セキュリティ」を開催した。本フォーラムでは、パネリスト 3 名を含む約 130 名の参加により、金融機関における情報セキュリティ対策の方向性について、幅広い観点から議論が行われた。

Ⅰ．パネリストによる講演

はじめに、**岩下直行**日本銀行金融研究所情報技術研究センター長より、「金融機関を取り巻く情報セキュリティ問題の現状とその対策について」と題し、以下の講演が行われた。

(1)　ここ 1 年ほど、金融機関を対象とするハイテク犯罪が増加し、利用者の不安が高まっている。ＡＴＭコーナーに仕掛けた隠しカメラ、インターネットカフェでのキー・ロガー被害、フィッシング詐欺メールの送りつけ、金融機関の名を騙って送付されたＣＤ-ＲＯＭからスパイウェアに感染しファームバンキングのパスワードが盗み出されて不正利用された事例、クレジットカード番号の大量漏洩事件など、様々なセキュリティ侵害事件がニュースで取り上げられている。海外で起きた犯罪が日本に波及するまでのタイムラグも短くなってきており、利用者の不安は高まっている。その中でも特に、偽造キャッシュカード問題は、世間の注目を集めた。

(2)　偽造キャッシュカードの被害は、2003 年以降急激に増大しているが、2004 年の被害額は 10 億円程度。偽造クレジットカード（2004 年の被害額 100 億円程度）や同様の犯罪（偽造テレホンカード：被害額推計数百億円、偽造パッキーカード（パチンコ用カード）：被害額推計 630 億円、偽造ハイウェイカード：被害額推計 300 億円）と比較すると、犯罪としての規模はそれほど大きくない。

(3)　偽造キャッシュカード問題が、犯罪規模が小さいにもかかわらず大きな社会問題化したのは、クレジットカードのような被害に対する補償・保険制度がなく、キャッシュカードの所持者本人が被害者となったことが原因であり、この結果、キャッシュカードを使うことに不安を感じる人が多くなった。これまでは、社会全体が比較的安全であり、犯罪があまり発生しない或いは利用者に実害が発生しなかったことから、低セキュリティの状態にあっても利用者は安全であると思っていたが、

マスコミがセンセーショナルに事件を取り上げるようになったことから、危険な状態であるということが広く認知されるようになり、実際に預金者の方々は注意深く取引を行うようになった。今後、セキュリティの向上を図っていくプロセスで、利用者が疑心暗鬼に陥らないようにするためには、金融機関は、具体的に実効性のある対策をきちんと講じていることを利用者に具体的に示し、納得した上で利用してもらうことが重要。

(4)　金融機関のセキュリティ対策として、キャッシュカードのＩＣカード化が行われているが、ＩＣカードといっても従来の磁気ストライプがそのまま入っているものは、それを読み取る機械を入手すれば磁気カード部分を偽造することはそれほど難しくない。預金者の暗証番号に対する意識は変わってきているが、未だ誕生日や電話番号を使用している可能性もなきにしもあらずである。昨年以降、被害の補償、ＡＴＭ引き出し限度額の引き下げが行われたが、結局磁気ストライプと暗証番号で守っている状況は変わっておらず、スキミング犯罪の根は残念ながら絶たれていない。

(5)　インターネットバンキングについては、当初、ＳＥＴなどの技術を利用して安全性を追及した形で導入が図られたが、使い方が難しかったことから利用者は増えなかった。ところが 2000 年ごろにＳＳＬを使って、単にパスワードを入れて認証するという方式を導入したところ、一気に普及した。そうしたシステムでは、「128bitＳＳＬでお客様の情報を保護しています」という説明がよく使われるが、ＳＳＬはインターネットの中を電文が送受信される際に、インターネットにつながっている他のＰＣやサーバーからその内容が見えないようにしているだけであって、特別な認証技術ではなく、現実には認証はパスワードだけで行っているので、4 桁の暗証番号について 1 万通りの総当り攻撃を行ったり、特定の文字列を当てはめたランダムな辞書攻撃により破られる可能性がある。そういう攻撃に対する防御は、ある程度は講じられているが、あらゆる手口に対してきちんと防御できているのか、という点については安心できない。

(6)　より安全そうなユーザー認証として、乱数表によるチャレンジ・レスポンス方式が導入され、多くの銀行のインターネットバンキングで使われている。しかし、これも完全なものではなく、一度使ったデータの値を再利用する仕組みであるため、認証情報が何度も漏洩したり、チャレンジの出し直しを何回もさせるという攻撃によってアタックされる可能性がある。特に最近は、フィッシングやスパイウェアによって認証情報が漏洩してしまうリスクが高まったため、対策として不十分ではないかという指摘がなされている。海外のインターネットバンキングでは、一定時間毎に自動的にパスワードを変更するワンタイム･パスワードというハードウェアを顧客に配布する銀行が増えており、今後は、こうした技術を導入しないと安全性が確保できないのではないかと思われる。

(7)　セキュリティ対策はある意味で限りのないもの。従来、金融機関は、カードは偽造できません、暗証番号は漏洩しません、銀行のセキュリティは万全ですという

立場をとっていたが、実際にはカードが偽造されることも暗証番号が漏洩してしまうこともある。ＩＣカード化しても偽造のリスクはあるし、静脈認証などの生体情報でも偽造される可能性はある。どこまで対応する必要があるのかということについてのレベル感を決めるのは難しい。参考になるものとしては、金融業務に利用する情報技術の国際標準を担当する委員会である ISO/TC68 で策定した国際標準やその審議内容が挙げられよう。無限にコストをかけることがよいわけではなく、ビジネス的にどの辺でマッチさせるかということはあるが、「知らなかった」ということがないよう知恵を磨いていく必要がある。また、セキュリティは掛け算であり、金融機関側と利用者の双方が対策を講じなければ効果はゼロになってしまう。利用者の管理負担とシステム構築やセキュリティのコストはトレードオフの関係にあり、現行の預金者保護法の下では預金者に一定の管理負担を要請しづらい状況になっているが、今後の役割分担のルール作りを業界の中で考えていくことがひとつの論点であると思われる。

(8)　銀行は情報システムの大規模ユーザーであり、それを適切に管理することが責務として課されているのであるから、情報セキュリティの専門家を内部で育成していくことが必要。外部からの提案をそのまま受け入れるのではなく、きちんと評価できるだけの能力を持った人間を育成していくことが必要である。

続いて、**内田勝也**情報セキュリティ大学院大学助教授より、「金融機関における情報セキュリティトラブル」と題し、以下の講演が行われた。

(1)　金額的には非常に小さくても、事件としていろいろな問題があることを考えれば、その部分に関しては対応していく必要がある。たとえば、生年月日を暗証番号に使うなというが、生年月日といっても月＋日以外にさまざまな種類があるにもかかわらず、金融機関のウェブ上では説明が足りない。こういう点は金融機関にもう少し考えていただきたい。

(2)　生体認証に関しては、テストの結果一度もエラーはなかったと言っても、統計上で考えれば、次のテスト結果もエラーにならないとは限らない。また、マレーシアでは3月に指紋でエンジンを始動する車を盗むために指を切り取るという事件が起こっており、こうした事件が起きた場合に金融機関はどうするのか。

(3)　ＩＣカードの採用もある程度有効であるが、今のスキミングでは、大部分が提携銀行やコンビニで引き出されていることを考えれば、引き出し金額の上限設定のみではなく、特定の支店でしか引き出せないとか一定時間内しか使えないというようなワンツーワンマーケティング的な発想があってもいいのではないか。

(4)　アウトソーシングに関しては、日本の場合、往々にして丸投げ的な形で全てを任せてしまうことがあるが、業務は委託できても責任は委託できないという点をもう少し考えていただく必要がある。米国ＣＳＩ及びＦＢＩの調査結果では、州政府や連邦政府を含めて 63%がセキュリティのアウトソースをしていない。また、アウ

トソースしている場合でも、81%以上しているところはない。セキュリティはそれほど重要なものであるという認識があるのではないか。

(5)　監査制度に関しては、直接的に監査する方法もあれば、クレジットカード会社の定めた認証制度で行うケースもある。また、当該企業の監査を利用することも考えられる。頻度についても考える必要あり。

(6)　暗号化に関しては、暗号化を行っていないデータを紛失した場合、どこが責任をとるのか。また、金融機関には、暗号化の仕組みがどうなっているのか、納得できるよう仕組みをオープンにしていただきたい。アメリカ重要基盤保護委員会のハワード･シュミット委員長も、ＳＳＬを利用したからといって安全ではない、ＳＳＬを使っているネットワークのところだけが暗号化されているのであってその先はまったくわからないということを言っている。

(7)　パスワードに関しては、1988 年に発生したインターネットワームでは、パスワードをハッシュ関数を使って暗号化（ハッシュ化）したパスワードを元に戻すことはできないが、ハッシュ化されたパスワードが同じだったら元も同じという考え方、現在は辞書攻撃と言っているもので攻撃を行い、当時の常識を覆した。国内では、毎回パスワードを変える都度振込のファームバンキングでパスワードをリセットすると元のパスワードに戻ってしまう安易な方法であったため、虚偽振込みをし、それを不正に引き出したという事件が起きている。重要なシステムでは、二者が結託しても破られないセキュリティを考えておく必要がある。

(8)　ソーシャルエンジニアリングという心理的な攻撃もある。振り込め詐欺などが最たるものであるが、たとえば、関係者しか知らない専門用語を使ってテストと偽って振り込ませたり、目の前ですぐ現金を持ってくるから先に記帳してくれと言って記帳させてしまったりした事例もある。人間自身がセキュリティ上で一番大きなセキュリティホールになっているのは事実なので、行員、お客様を含めてどうやって教育していくか考えておく必要がある。

(9)　これまでの外資系銀行、損害保険会社等での経験から、金融機関は、データや情報を処理することによって成り立っている最大の情報処理産業ではないかと考えている。情報セキュリティは、性悪説と言われるが、無実の従業員を疑うことをしない仕組みの構築は情報セキュリティで可能である。岩下さんのお話にあった、「安心・安全」に「信頼」を付け加える必要がある。

さらに、**岡村久道**弁護士（英知法律事務所）より、「情報セキュリティと法制度」と題し、以下の講演が行われた。

(1)　情報セキュリティの意義は、国際標準、国内標準的に、①機密性（Ｃ）、②完全性（Ｉ）、③可溶性（Ａ）である。1992 年のＯＥＣＤ情報セキュリティガイドライン(2002 年改訂)､国際規格である 2000 年の ISO/IEC 17799 と本年の ISO/IEC 27001、

2001 年に欧州評議会閣僚委員会が作り、昨年 4 月 21 日に国会承認、7 月 1 日から発効したサイバー犯罪条約の中でも、共通して機密性、完全性、及び可用性の維持と定義されている。

(2)　サイバー犯罪条約は、承認して発効した以上、これに合わせて国内法を整備しなければならないが、ウィルス処罰規定に関しては、現行法では対応が十分といえない。日本の場合、ウィルスで実害が出れば現行の刑法で処罰の対象となるが、ウィルスの作成段階では処罰の対象にはならない。既に 1 年ほど前から刑事法の改正案が国会に提出されているが、まだ通過していない。

(3)　法案の中で、「不正指令電磁的記録作成罪」では、行使の目的は必要であるが、ウィルス的なデータを取得又は保管した者、つまり持っているだけでも罪になる。これで形の上ではウィルスの処罰規定ができるが、ここでいう「不正指令電磁的記録」とは、人がコンピュータを使用する際に、意図に沿うべき動作をさせず、又は意図に反する動作をさせるべき不正な指令、つまり、コマンドを与える電子データという意味であるから、スパイウェアなども全て含めることができる余地がある。

(4)　日本には、情報セキュリティを包括的に保護する法律はない。法律の中では、未だに、コンピュータを電子計算機、電子データを電磁的記録、情報処理システムを電子情報処理組織と呼び、ＣＩＡに沿った体系化もされていないが、個人情報保護法に代表されるように「安全」という言葉は法律上にも出ており、同法中の「情報の漏洩、滅失又は毀損の防止その他の情報の安全管理（適切な管理）のために必要かつ適切な措置」を講ずるというところにはＣＩＡ全部が含まれていると見るのも可能ではないか。現状では、情報の管理者側に責任を負わせる法律が増えてきており、情報セキュリティという言葉は書かれていないが、安全という言葉で言い替えているのが今の日本の法制度の傾向である。

(5)　日本の情報セキュリティ政策の中心となっているのがＩＴ基本法である。今年の 4 月より設置された内閣官房に情報セキュリティセンターの中には情報セキュリティ専門委員会が置かれ、2002 年のＯＥＣＤガイドラインに基づいて情報セキュリティ文化の醸成に取り組んでいる。現段階で法的拘束力はないが、特に民間部門に、情報セキュリティが常識として、社会秩序として、空気のような当たり前の存在となるようになるようにしようというものである。

(6)　日本の情報セキュリティのための法整備の事実上の中心は 4 月に全面施行された個人情報保護法であり、これを軸に民間では情報セキュリティ対策が進められている。ここでの特色は先に述べた「漏洩、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置」で、漏洩さえしなければよいというものではない。たとえば、大規模システム障害によって預金引き落としができなくなるといったことにも予防策が必要であり、別途、データの正確性の確保を求める規定も置かれている。これまでの日本の法律では、悪いことをした人を処罰するということが中心であったが、ここではむしろ、データの管理者側に責任を負わせ、その責任を果たすための管理策をきちんと行っていただくということに要点が置かれ

ている。実効性担保策としては基本的に主務大臣の関与によるとされ、今年の春に金融庁は青森の銀行に対して個人情報保護法上第1号となる勧告を行ったところ。

(7)　また、情報セキュリティ対策にコストがかかりすぎるのではないかという経済界の意向により、現在、従業員がその取り扱う個人データをみだりに漏洩した場合には直罰が下るという情報漏えい罪を入れるための個人情報保護法の改正が検討されている。しかし、金融庁や内閣府の公表資料によれば、従業員が故意にデータを持ち出したケースよりも、ついうっかりミスで紛失した状況で漏洩していることが多く、情報漏えい罪は過失の場合には無力なのではないかと言われている。このため、未然防止策としての管理策強化と、プライバシー権侵害として事後に民事責任を負わせるという両方の形でカバーせざるを得ない部分が残る。

(8)　情報の機密性についてみても、機密性を守るための包括的な法律はない。87年にコンピュータ犯罪のために刑法を改正したが、機密性だけは入れられておらず、窃盗にせよ業務上横領にせよ、有体物を盗らなければ処罰の対象にはならず、データをコピーしただけでは処罰されない。刑法の他、医師や弁護士などの資格に関係して罰則付きで守秘義務を課す規定や、客体となる情報の種類を限定して通信の秘密や営業の秘密などを保護するもの、特定の不正手段による機密性侵害を禁止する法律（不正アクセス禁止法）などもあるが、故意だけしか処罰されないので、過失に関しては民事責任、行政処分にゆだねざるを得ない。

(9)　機密性の侵害に関する損害賠償訴訟の例としては、①宇治市の住民基本帳データ流出事件、②北海道警のアンティニー感染による捜査情報漏洩事件などがあるが、民法の使用者責任は無過失責任であり、企業側に落ち度がなくても責任を負わなくてはならないという厳しい状態にある。また、不正競争防止法における営業秘密を持ち出した者などに対する民刑事責任の追及についても、企業側が保護されるためには、機密管理性の要件として判例が求めるアクセス制限の要件を満たしていなければ保護されない。なお、前橋信金事件でわかるように、企業側が情報漏えいした従業員を内規違反で懲戒処分しようとしても、絵に描いた餅のようなルールがあるだけではだめで、ルールに関する教育を実施するなど、あくまでも企業側が実効性確保のために汗をかいて初めて法的に保護してもらえるのである。

(10)　過失による民事事件は昔から多い。大和銀行株主代表訴訟第一審判決を背景として、企業会計審が7月に出した内部統制監査の6つの基本方針のうち6つ目には「ＩＴの利用」が入った。また、新会社法では、大会社に関しては委員会等設置会社を、それ以外の会社に関しても、広く法令及び定款に適合することを確保するために内部統制を行うこととされ、役員自身が責任を負わざるを得ない形となる。

(11)　最近問題になっているゾンビＰＣやボットネットなど、セキュリティが保たれていないＰＣに不正プログラムを送りつけて行う海外からの一斉攻撃とそれに対する各社の防御活動は今この段階でも行われている。こうした官民ともに攻撃を受けている状態の中で、是非とも情報セキュリティということを皆さんにもう一度考えていただきたいと思う。

Ⅱ．パネルディスカッション

パネリストによる講演終了後、会場内から集めた質問をもとに、以下 4 つの問い立てにより議論が進められた。（モデレーター：杉浦宣彦金融研究研修センター研究官）

１．　金融機関はどこまでセキュリティ対策をすればよいのか。

【岩下氏】基本的には各金融機関の経営判断によるが、ミニマムの基準は必要。セキュリティ対策は際限ない問題であり、どこまでやでも高くできるが、金融機関はビジネスでもあるため、発生被害額との比較で、どこまでの投資を正当化できるかということだと思う。ディスクロージャーや外部監査等様々な仕組みを使いながら対策案をプランニングし、その中で各企業が最適と思われる対策を講じていくべきではないかと思う。

【内田氏】どういうリスクがあるのかを計算し、それに見合った投資をすべき。問題は、銀行が単なる私企業ではないということをどう考えるかにあるが、少なくとも現状では、1000 円のために 100 万円を使う必要はない。

【岡村氏】わが国においては、個人情報保護法が事実上の情報セキュリティ法制。コンプライアンスはコストにかかわらずやらざるを得ないもので、コストが合わないから常識的な水準の管理策を講じず、違法な状態でもよいということではない。1000 円しか儲からないから違法でもいいというのは今の世の中では通用せず、コストが合わないなら当該個別領域から撤退するほかない。

２．　セキュリティレベルを保つための手法、適切なリスク計算方法、適切なコンティンジェンシー・プランとは。

【内田氏】ネットワークへの侵入の大部分は、パッチを当てていないか設定ミスとの調査結果が米国国防総省であった。逆に言えば守る側の問題。守る側がやっていない事が多すぎるのではないか。リスクの計算方法に正解はない。最近、日本でも情報処理システムに関しては、投資対効果を計算すべきとの議論が一部にあるが、セキュリティではほとんど行われていない感じがする。どのような方法で計算するかは重要であるが、工場では当たり前に計算している。

そのことを金融機関を含め、情報セキュリティ分野の人達は認識すべき。

【岩下氏】日本では、セキュリティ侵害は「起こってはならないもの」という前提であり、仮に侵害が起こった場合にも、被害額の事後分析が行われていなかったため、リスク計算ができていない。最近では、偽造キャッシュカード等の事件により、セキュリティ問題がタブーではなくなっており、セキュリティの侵害は今ここにある危機だという意識を持って取り組んでいく必要があるが、金融機関の意識変革が今一つ進んでいないのが実態ではないかと思う。

３．　アウトソースでのセキュリティ機能とは何か。海外でのアウトソースの現状について。

【内田氏】資料 P12 については、セキュリティ・ファンクションとしか書いていないので、それ以上は分からないが、セキュリティにはさまざまなものがある。63%がセキュリティをアウトソースしていないと答えているが、実際にＣＳＩのコンファレンスに出席しているが、かなりの企業では自分たちでやっているという印象を受けている。

【岩下氏】米国では、クレジットカードのプロセッシング業務を丸ごとアウトソースしており、今年の夏に起きたクレジットカード番号の大量漏洩事件というのは、その委託先に問題が生じ、そこを利用しているすべての銀行の顧客が被害にあったというもの。しかしながら、業務を丸ごとアウトソースするケースを別にすれば、海外の金融機関におけるシステム投資においては、システムの根幹となるセキュリティについては、委託元が責任を持ってハンドリングしている事例が多いように思う。これに対して、日本は、セキュリティ対策に関するチェックも委託先任せ切となっている事例があるように見受けられる。ＩＴガバナンスという観点からも、改善の余地があるのではないか。

【岡村氏】金融機関はアウトソース先に対してコンプライアンスレターを出し、問題点は生じていないか、大丈夫か、と期限を切って確認すべきである。おそらく、抽象的な答えが来ると思うが、具体的に何が問題なのか、それに対する改善案はどうするのかと文書で回答をもらうようにすること。こうした対応ができない業者であれば、委託契約を解除したほうがよい。定期的な監査・検査もあるが、例えば大きな脆弱性発見時には、臨時にコンプライアンスレターを送るなどし、問題があれば、第２第３の手を打てるように進めていかないと話にならない。なお、コンティンジェンシー・プランは、コールセンター用のシナリオ作成、ＦＡＱのホームページへの掲載、報道対応、本社への連

絡など、具体的に作るべき。ベンダーとしても、誠意をもって対応しないと、日本的ビジネスとして相手にしてもらえないということになろうかと思う。

４．　諸外国での被害状況如何。日本のセキュリティレベルは諸外国と比較してどのくらいの水準なのか。日本のコンピュータ犯罪の罰則は諸外国と比較してどのくらいの水準か。

【岩下氏】日本でも海外でも似たような犯罪は起こっている。件数的には、日本のほうが少なかったが、日本で問題が大きくなっているのは、一件当りの被害額がとても大きかったから。海外では、そもそもＡＴＭでの引き出し限度額が低いため、被害件数は多くても、金額が少なく、50 ドルルール等によりすぐに補償されるので、騒がれなかったというのが実態。

【内田氏】日本では、一般的に事後対応が悪い。問題は発生したトラブルの大きさではなく、事後対応。トラブルの起こった後の対応をきちんとすれば、ほとんどのトラブルは大きくならずに済むはず。日本の金融機関のセキュリティレベルは平均値で見れば低く、海外よりも 5～10 年遅れている。

【岡村氏】現実に起こっている漏洩事件は過失犯が大半であり、罰則を強化しても思うほど意味がない。故意の場合でも、残念ながら外国からの攻撃が多いので、日本の刑法で取り締まるのは困難。日本の罰則が軽いということではなく、摘発が難しく、外国政府との協力も難しいため、限界がある。なお、クレジット番号が漏れた場合、名無しでも使用できる状態になっており、悪用の恐れがあるが、提携カードであることが障害になってすぐに交換できない場合がある。提携カードも含めて、何かあった場合にすぐに対応できる体勢にしておくべき。また、インシデントが起こった時には、どこまでのリスクがあって何をすればよいのかをアナウンスし、混乱を避けるべき。対応を誤れば 2 次 3 次災害にもつながりうる。ユーザー側もやるべきことをやらなければ過失相殺事由になるが、前もって伝えるべきことを伝えておかないと、事故が起こった後からでは過失相殺とは言い出しにくくなる。

Ⅲ．質疑応答

最後に、上記パネルディスカッションを踏まえ、以下のとおり、質疑応答が行われた。

（質問 1）地銀から業務の委託を受けている。各委託元の監督基準はバラバラで特に指示もなく、自主的にセキュリティ対応状況報告等の情報を提供しているとことであるが、委託先の立場としてどういうところまで報告していけばよいのか。

【内田氏】　認証をとるかどうかは別として、ＩＳＭＳに準拠した仕組み作りをすることが必要。

【岩下氏】自分は、日本の銀行業界のセキュリティ対策に対して危機感を持っているが、残念ながら、問題に気づいていない人が多いように思う。もし気づいた問題があれば、早めに指摘するほうがよい。気づいていないことが一番のリスクである。

【岡村氏】委託先も事業者として個人情報保護法上の安全管理義務を負う。委託元がどう言おうが関係なく、法律は守らなければならないから、問題に気づけば対応を要し、報告しておけば万一のときに委託元に対して過失相殺を主張できる場合があるという利点もある。

（質問 2）欧米の金融機関でワンタイムパスワードを導入しているとのことであるが、欧米での最新のセキュリティ技術について教えていただきたい。

【岩下氏】欧米では、一部の金融機関で顧客にワンタイムパスワード生成機を配布している例があるが、日本のように紙のカードに乱数表を印刷して配っている事例は見たことがない。また、ＡＴＭに生体認証を導入している事例も、韓国等にはあるが、欧米には殆どない。欧米の金融機関の場合は、顧客をセグメント化し、大規模な取引を行うような顧客については特別なデバイスを提供するが、それ以外の顧客に対してはそもそも取引金額に上限を設ける等の実質的な対策を行っているようだ。これが絶対的というものはないが、セキュリティの基本的な前提に対する理解は割と共通しており、取引の電文の暗号化やＩＳＭＳの取得などをきちんとやっている銀行が多いという印象を持っている。

（質問 3）何か懸念事項があれば委託先に質問状を送るようにとのことだが、金融機関がベンダーに対して質問状を送った場合に、事実上の業界標準システムということなどから答えてもらえないような場合が少なからずある。業界全体で提供側として自ら公開するような可能性如何。

【岡村氏】基本的には、委託契約上で回答を義務付けるのがトレンドになっている。そういう契約に変えていかなければならない。

【内田氏】契約上、個人情報の漏洩で委託先に非があった場合、契約金以上の金額を支払うように契約書を変更していく等の方法を考えることが良いのではないか。

【岩下氏】業界標準システムというのは、皆が同じものを使っているので安心感があるが、実際には往々にして技術が遅れがち。業界標準であっても、セキュリティに問題がある場合は、それを変えていこうという声を上げることが大切。

（以上）