平成29年３月23日

公益財団法人　金融情報システムセンター

第４回　金融機関におけるFinTechに関する有識者検討会　議事録

Ⅰ　開催日時：

平成29年３月23日（木）15:45～15:30

Ⅱ　開催場所：

FISC会議室

Ⅲ　出席者（順不同・敬称略）

座長	岩原　紳作	早稲田大学　大学院法務研究科　教授
座長代理	渕崎　正弘	株式会社日本総合研究所　代表取締役社長
委員	安冨 潔	慶應義塾大学名誉教授・弁護士
	上山 浩	日比谷パーク法律事務所 パートナー弁護士
	田中 秀明	株式会社みずほフィナンシャルグループ IT・システム企画部 システムリスク管理室 室長
	山田 満	株式会社南都銀行　システム統括部 部長
	吉本 憲文	住信 SBI ネット銀行株式会社 FinTech 事業企画部長
	真田　博規	住友生命保険相互会社 情報システム部 担当部長
	黒山 康治	（代理出席） 東京海上日動火災保険株式会社 IT 企画部部長 兼 リスク管理グループリーダー
	植村 元洋	野村ホールディングス株式会社 IT 統括部次長 兼 IT 管理課長 (エグゼクティブディレクター)
	Mark Makdad	一般社団法人 FinTech 協会　理事
	内波 生一	（代理出席）株式会社マネーフォワード アカウントアグリゲーション本部 本部長
	轟木 博信	株式会社 Liquid　経営管理部長 弁護士

	村上 隆	株式会社ＮＴＴデータ 第四金融事業本部 企画部ビジネス企画担当 シニア・スペシャリスト
	長 稔也	株式会社日立製作所 金融システム営業統括本部 事業企画本部 金融イノベーション推進センタ センタ長
	加納 清	（代理出席）日本電気株式会社 パブリック企画本部シニアエキスパート
	梅谷 晃宏	アマゾンウェブサービスジャパン株式会社 セキュリティ・アシュアランス本部 本部長 日本・アジア太平洋地域担当
	平原 邦久	日本マイクロソフト株式会社 第一インダストリー統括本部 シニアインダストリマネージャー
	酒井 慎	（代理出席）デロイトトーマツコンサルティング合同会社 銀行・証券ユニット　シニアマネジャー
オブザーバー	神田　潤一	金融庁 総務企画局 企画課 信用制度参事官室 企画官
	片寄　早百合	金融庁　検査局 総務課 主任統括検査官 兼 システムモニタリング長
	中井 大輔	日本銀行 金融機構局 考査企画課 システム・業務継続グループ企画役
	希代 浩正	（代理出席）経済産業省 商務情報政策局 サイバーセキュリティ課 課長補佐
FISC(事務局)	渡辺　達郎	理事長
	髙橋　経一	常務理事
	水野　幸一郎	総務部　部長
	郡山　信	総務部　特別主任研究員
	小林　寿太郎	企画部　部長
	藤永　章	企画部　次長
	大澤　英季	企画部　主任研究員
	中山　靖司	調査部　部長
	西村　敏信	監査安全部　部長

Ⅳ　議事内容

１．【議事１】FinTechに関する安対基準適用上の課題

○岩原座長　本日１つ目の議事は、「FinTechに関する安対基準適用上の課題」でございます。FISC企画部藤永次長、よろしくお願いします。

○藤永次長　議事１という資料をご用意ください。

この議事は、今まで取り上げてきましたタイプⅠ並びにタイプⅢという形態に加えましてタイプⅡという形態の議論が残っておりまして、そのタイプⅡの議論の論点メモとしてご用意したものです。したがいまして、今まで検討会でご提示させていただきました「FinTech に関する安対基準適用上の課題」という論点メモの最後に追加するよう、本日は、追加部分のみご用意しております。

「６．タイプⅡの特性を踏まえた補足的検討」です。従前からこの検討会で取り上げてきましたタイプⅠ並びにタイプⅢに関する検討を踏まえた上で、その派生形であるタイプⅡが安全対策上どのような特性を有するか、また、どのような補足が必要か、ということが論点メモの趣旨です。

１つ目として、これまでの議論を踏まえて、タイプⅡの特性が、どのように理解し得るかということございます。タイプⅡは、FinTech 企業が金融機関の子会社になるケースです。「金融機関は、子会社に対して、当該子会社の金融グループ経営上の位置づけや役割、あるいは規模等に応じて、個別の経営管理契約を結んだうえで、管理・統制を行っている。例えば、リスク管理状況のモニタリング等を通じて助言・指導を恒常的に行う、あるいは、重要事項の報告義務を定めること等を通じて情報の適時適切な把握を行っている」という現状にあります。「したがって、FinTech 企業に対して子会社に対する責任も生じるタイプⅡ」という類型につきましては、「外部委託先に対する統制に加えて、こうした子会社に対する統制が付加される」ことになります。

これはどういうふうに理解し得るかということですが、統制面では、「タイプⅡは、他タイプと比較して、統制の接点が多く、かつ実効的な情報開示も担保されている」ということで、「FinTech 業務において目指されるべき『関係者間の協調による適切な安全対策の実施』」が、「金融機関と FinTech 企業の両者において、比較的円滑に可能となると考

えられ」ます。

経営資源配分面では、「客観的評価の結果、FinTech 企業の安全対策遂行能力が十全でなく、かつ安全対策に追加的に配分可能な経営資源がない場合には」、従前の議論としましては、責務の再配分が可能であるということをご提案してまいりましたが、それだけでなく、「増資や人材の派遣等を通じて、FinTech 企業の経営資源を補強することも」金融機関側としては、「選択することが可能」となります。

「以上のことから、統制と経営資源配分の両面から、タイプⅡは、金融機関およびFinTech 企業にとって、システムの安全性を確保しつつイノベーションの成果を享受するという」本検討会の「目的に対して、一つの解決策を提供する類型である」のではないかと考えられます。

そのうえで補足的検討をおこなっているのが（２）です。「金融機関の内部では、経営管理と外部委託管理が、異なる窓口部署・管理項目・管理周期で行われる場合がある」という現状にあります。これについては裏面の図表２を参照ください。まだ FinTech 企業が子会社という事例がなかなか登場していない中で、当センターでは、システム子会社を例に取りまして、金融機関が、経営管理と外部委託管理をどのように行っているか、システム子会社を傘下に保有する複数の銀行の協力を得てまとめたものがこの資料です。

ご覧いただいておわかりのとおり、経営管理と外部委託管理の窓口部署として、前者は、経営企画部門・システム企画部門、後者は、リスク管理部門、システム担当部門となっており、必ずしも同じ部署であるとは限らないということです。

管理項目の例につきましても、経営管理においては「重要事項の決定の事前承認」として「株主や役員の変更」等が取り扱われ、かつ「事業計画の実施状況の把握」として「リスク管理状況の把握」が行われています。一方、外部委託管理については「再委託管理状況の把握」「委託業務の実施状況の把握」「システムリスク管理状況の把握」が行われています。両者で類似の確認項目があるものの、必ずしも同一ではありません。

管理周期につきましても、それぞれの銀行が定める管理項目に応じて都度、あるいは定期という形で実施されており、必ずしも同一でないという実態があります。

なお、本文の脚注１ですが、ここではシステム子会社の例を取り上げておりますが、これはシステム子会社と FinTech 企業を同列に扱うべきと意図しているわけではありません。当然のことながら、「FinTech 企業に対しては、金融グループ内での位置付け等実態に応じて、金融機関において区々の管理が行われるものである」と承知しております。

以上の調査結果を踏まえて「補足」です。「FinTech 企業においては、同一金融機関とのやりとりであるにも関わらず、別個の対応を求められる」ような場合もあり得るのではないか。「これは、FinTech 企業において負担となる局面も予想される」ため、「負担を求めることがイノベーションを損なう可能性がある」。そうしたことが、危惧される場合には「経営管理と外部委託管理を行う部署間で連携をして、FinTech 企業に過度な負担が生じないように注意を払うことが望ましい」のではないか、と補足的に提言してはどうかという提案でございます。

なお、脚注２ですが、「金融機関においては、経営管理と外部委託管理は、それぞれ異なる観点から行われており、どちらかを省略できるというものでは」ありません。一方で、既に経営管理と外部委託管理をグループ経営の中で行っている金融機関においては、管理の効率化として、さまざまな工夫が行われています。図表２の下ですが、我々がヒアリング調査した中では、例えば、親会社と子会社が同一の建物に入居している、親会社が子会社に対して研修を実施している、拠点内であれば再委託先については定例報告を省略している、規定を共通化している、あるいはメールなどのシステムを共通化しているといったようなさまざまな取り組みが既に行われてます。これらは、FinTech 企業が子会社となった場合に参考としていただけるのではないかということで、記載しています。

私の説明は以上です。

○岩原座長　ただいまのご説明に対して質問はございませんでしょうか。よろしいですか。特にないようでしたら先に進めさせていただきます。

それでは藤永次長、どうもありがとうございました。

２．【議事２】「同等性の原則」という考え方

○岩原座長　続きまして、２つ目の議事は「『同等性の原則』という考え方」についてでございます。引き続きFISCの藤永次長にお願いいたします。

○藤永次長　議事２という資料をご用意ください。

「『同等性の原則』という考え方」という資料です。従来から本検討会で、「同等性の原則」という言葉を使って説明してきたのですが、わかりにくい、もう少し背景も含めて丁寧な説明を、という要望をいただいており、今回皆様の理解が進むようにという観点で、資料をご用意しました。「『同等性の原則』とは、金融業務を担う情報システムの安全対策の効果は、安全対策上の関係者に関わらず、同程度に確保されるべき」という考え方です。この原則がどのような意味を持つかということについて、「リスク評価から安全対策の決定・実施にいたるプロセスを紐解きながら、責務の再配分ルールとの関係に触れつつ」、整理をしています。

まず１番目として、「安全対策の基本原則に沿った安全対策の実施にいたるプロセス」です。安全対策の基本原則とは、金融機関における外部委託に関する有識者検討会において提言された基本原則のことで、この原則に沿ったプロセスを整理しています。絵を見ながらお聞きください。

金融機関は、情報システムのリスク評価活動を定期的に行っています。リスク評価を通じて、リスクを特定し、リスク特性を把握した後、経営層が、情報システムのリスクをどの程度低減するか、あるいは受容するかを決定します。

脚注１ですが、低減と受容以外にも、「移転」や「回避」という手段もあります。

次に、「リスクを低減するための手段として、安全対策の達成目標を決定する」。そうした、「安全対策の達成目標および個々の安全対策は、リスク特性によっては、安対基準を参考としながら、決定され」ます。

「経営層は、安全対策に対する資源配分について、経営資源全体との調整等企業価値の最大化を目指して決定」していく。「その際に、低減のために行われる安全対策の費用と」、上の図で事後対策と書いておりますが、そうした「安全対策を実施しないことで生ずる事後対策の費用も比較衡量しつつ、達成目標と相互調整を行」います。以上が、外部委託の検討会で提言された「基本原則に従ったITガバナンス」です。

２ページは、そうした安全対策の達成目標が、実際どのように IT マネジメントとして実現されるかということです。「経営層によって、安全対策の達成目標と経営資源配分が決定された後は」、IT マネジメントを担う「管理者」、これは、システム部長、あるいは CIO、さまざまなケースがあると思いますが、「管理者」のもとで複数の関係者によって、安全対策が実施されます。「実施にあたっては、個々の安全対策に応じて関係者間で担われる役割」、これは本検討会では、「責務」と通称していますが、それが、特定（配分）されます。

この「安全対策の責務は、安全対策の技術的側面を担う外部委託先と金融機関の２者に配分されるのが一般的」でした。その際、金融機関は、あらかじめ外部委託先の安全対策遂行能力を評価したうえで、能力を有する委託先を選定します。また、「外部委託先において責務を担うために発生する費用は、最終的には、委託料として金融機関が負担する」こととなります。「こうして、安全対策の効果が達成され、経営層の受容可能な程度まで、システムリスクが低減されることを目指す」ということが、今までの基本的な責務の考え方です。この考え方を踏まえて、今回、FinTech を論じる際に「同等性の原則」という言葉が出てきました。

その下の２番ですが、「FinTech 企業が安全対策の関係者として加わる FinTech 業務」と書いてありますが、２者でやっている業務と、FinTech 企業が加わって行われる FinTech 業務が、類似の金融関連サービスであれば、「金融機関と IT ベンダーの２者で行われているのと比較して、同程度までリスクが低減されるよう取り組むことが必要である」、これを「同等性の原則」と通称しています。

これは、単純化しいますが、関係者が２者から３者にふえると、コミュニケーションが複雑になり、リスクが増加する場合も当然あると思いますが、ここでは、単純化して書いているものとご理解ください。要は、FinTech 企業が登場しようとも、もともと金融機関が決定している受容可能な程度までリスクを低減していくことは、何ら変わらないということです。

次の３ページですが、「FinTech 企業が加わった場合に、従来 IT ベンダーに求めていた責務を、FinTech 企業に求めることとなれば、IT ベンダーと同様の責務が担える FinTech 企業のみが選定されること」となってしまう。これは、「FinTech においては、『イノベーションの成果を享受する』という観点」が重要であるとしている中では問題であることから、この問題を解決するために、「責務の再配分ルール」を本検討会で提言しているとい

うことです。

「責務の再配分ルール」がどういうことかといいますと、図をご覧いただきながら聞いていただきたいのですが、金融機関が、FinTech 企業と IT ベンダー選定時の評価の結果、「FinTech 企業の安全対策遂行能力が十全でない場合に、イノベーションの成果の享受とシステムの安全性の確保を両立させるための方策として、責務の再配分を行う」としています。図の真ん中の点線のところで、不足している部分がある場合です。その部分について、金融機関が代替する、補完する、ことによって最終的なリスクは、従来と同程度に低減されることを目指していくということです。

「再配分の極端な例として、FinTech 企業の責務をゼロにすることも」、当然想定されますが、これについては、本検討会で取り上げました「金融関連サービスの提供に携わる事業者を対象とした原則」では、「何ら安全対策を実施しない、ということは適切ではない」としており、「FinTech 企業においても、最低限担うべき責務、分配不可能な責務がある」としております。

「また、責務の再配分と同等性の原則は、金融機関が金融関連サービスを主導している場合」のみならず、本検討会で議論しているタイプⅢ、すなわち、FinTech 企業がサービスを主導している場合においても、適用可能な考え方であると考えています。

この意味するところは、顧客の立場に立てば、安全対策上の関係者や主導者がいかなるものであろうとも、同様の金融関連サービスには同程度の安全対策の効果が確保されることを、顧客の皆様は期待されているのではないか、ということです。

なお、責務の再配分は、何も新しい考え方ではなく、金融機関が従来から任意で有している選択肢であります。ただし、この考え方を積極的に明示することで、FinTech 企業と金融機関の関係が進展して、イノベーションが促されるのではないかと期待して、今回取り上げています。

この中で、「安全対策遂行能力」というやや堅い言葉が出ていますが、これがどういう意味を持つのか、少し口頭で補足させていただきます。

「安全対策遂行能力」とは、例えばある時点において個別の安全対策が実施できているといった、形式的に確認できることのみを必ずしも意味していません。「安全対策遂行能力」とは、事業者が内部統制を実質的に機能させる能力をいいます。

例えばでいいますと、安全対策上の問題があれば自らそれを特定して、自らそれに対処し、そうした問題の抽出と対処という改善活動を自ら継続的に実施できる能力のことで

す。もう少しかみ砕いていいますと、安全対策の PDCA サイクルを十全に機能させる能力のことです。

この能力は、例えば内部監査では、方針規定などのルールや組織といった管理体制を確認する「整備状況評価」、そのルールどおり運営されているか確認する「運用状況評価」というプロセスで検証されます。ご存じの方には蛇足ではあったかもしれませんが、補足説明させていただきました。私からの説明は以上でございます。

○岩原座長　ただいまのご発表についてご質問ございませんでしょうか。

○黒山委員代理

念のために確認させていただきたいのですが、１ページの真ん中の図のところに経営資源配分ということで、「安全対策と事後対策の比較衡量」、「新規開発等の調整」、「経営資源全体との調整」、３つの図がありますけれども、真ん中の「新規開発との調整」です。ここが意図しているところですけれども、仮に開発ということで、ヒト、モノ、カネとかそういったものを意識しているのであれば、「経営資源全体との調整」に入ると思いますし、あるいは事業内容、リスク評価をした上でどういうふうにやっていくかという形であると、事業あるいはそういう目的に沿っているかどうかという調整になると思いますので、この新規開発という単語を使うとちょっと趣旨がわかりにくいなと思いまして、念のためここの目的、意図しているところを確認させていただきたいのが１点目。

もう１つが３ページですが、図の下の５行目に、「再配分の極端な例としては」というところで、「「金融関連サービスの提供に携わる事業者を対象にした原則」では、「何ら安全対策を実施しない、ということは適切でない」とされており、」とあり、また文末に「最低限担うべき責務、分配不可能な責務があるものとされている」とあって、これは前提ということでそのような文章にされているのでしょうが、１個目の「されている」は、前提でよいと思うのですけれども、２つ目のところの「されている」というのは、今回の趣旨からいうともう少し強く「責務があるものと考える」等、強く主張したほうが、全体の文章の趣旨に合うかなと思うのですけれども、その意図を確認させていただきたいと思います。

○藤永次長　１点目につきましては、ここは外部委託に関する有識者検討会の報告書

の文章を絵で表したものです。「新規開発との調整」とは、情報システムの部門内で資源配分を判断するときに、安全対策であるからといって優先的に資源を配分することは適切ではない、情報システムの新規開発を含む全体を踏まえて情報システムの予算内で調整すべきである、ということです。一方、「経営資源全体との調整」というのは、情報システムを越えて金融機関全体の中で資源配分を経営陣がどういうふうに判断するかということです。情報システム内の調整、金融機関全体の調整と、それぞれスコープを分けているというのが、ここでの趣旨です。

２点目につきましては、ご指摘を踏まえて修正させていただくのが適切と思います。ご指摘の箇所は、FISC が従来対象としない FinTech 業務についてどのような意見表明をすべきかという中で、検討されてきたものです。「分配不可能な責務がある」という部分は、ご指摘のとおり、語尾を明確にしたほうが、これまでの議論にふさわしいと思います。前回の検討会で取り上げたとおり、分配不可能な責務として「必要最低限の安対基準」を今後 FISC が策定していく、それによって具体的な責務を示していく、と言ってきましたので、語尾のところは強い表現に修正させていただきます。

○岩原座長　よろしいですか、黒山さん。

ほかに何かご質問ございますでしょうか。よろしいですか。特にございませんか。

特にないようでしたら、さらに先に進めさせていただきたいと思います。

藤永次長、どうもありがとうございました。

３．【議事３】クラウドサービス利用時のリスク管理策に関する補足的検討（プレゼンおよび第３回事後意見を踏まえた修正案の提示）

○岩原座長　続きまして３つ目の議事は、「クラウドサービス利用時のリスク管理策に関する補足的検討」であります。

こちらは前回第３回の席上や事後にたくさん意見を頂戴しております論点であります。最初にクラウド事業者様よりプレゼンテーションをいただきまして、続いて事務局より第３回検討会事後意見へのご回答と資料修正案についてご説明し、その後に討議の時間を設けさせていただきます。

まず、アマゾンウェブサービスジャパン株式会社の梅谷委員よりご発表をいただきます。配付資料はございませんので、スクリーンをご覧ください。それでは梅谷さん、よろしくお願いいたします。

○梅谷委員　アマゾンの梅谷です。お時間をいただきましてありがとうございます。最初に私のほうから、クラウドにおけるログや構成管理サービスを活用した効率のよい監査ということでお話をさせていただきます。これは議事のページ７の一番下の脚注18にも関連しています。クラウドサービスに関して、監査で積極的に使える機能があるという趣旨の発言を前回もさせていただきましたが、その内容を補完するような形で、現在クラウド環境の中でどういった効率的な監査が行えるのか、クラウドベンダーとしてどのようなサービスをお客様に提供しているのかという観点から情報の提供をさせていただきます。

クラウドについては、利用分だけの支払いが発生する等、クラウドのコストをはじめとしたビジネス観点での利点については、これまでにもいろいろ議論されているかと思いますが、セキュリティ・コンプライアインス上でも同様に利点があると我々は考えています。こうした内容を考えるにあたっては、システムの自動化と、システム・インフラの高度な抽象化という点が重要になります。クラウド環境上では、様々なログや構成情報が、例えば構成ファイルの中身を参照する、あるいは、コマンドを実行することで取得が容易になっています。そうした情報を活用することで、従来はなかなか実現の難しかった監査ができるようなシステム構成や、監査の体制を構築していくことができる、という考え方をしております。

その前提として、責任分界とクラウド技術の要点という、２つ重要な点がありますの

で、クラウド技術の要点からお話しさせていただきます。

クラウドベンダーは各々が自社の環境を独自の方法で、解説されているかと思いますが、一つの考え方として、クラウド環境のことをSoftware Defined Infrastructureという捉え方があります。要するにAPIを通じてソフトウェア的なプログラムが可能なインフラであるという考え方です。従来のホストベースの仮想化や、オンプレミスの環境と比較すると、物理レイヤーに存在するシステムと、その上に構築されたお客様に使っていただく抽象的な仮想化レイヤーというのが高度に分離されており、お客様に操作していただく箇所は、仮想的なシステムの立ち上げ、仮想的なネットワークの構成、仮想的なシステム操作に係るプロセスの構成の変更ですとか、そういった形になりますが、全てソフトウェア的に抽象的な世界で実行されるというのが重要な点になります。

例えば、実環境で人間が手動で操作して手順書を見ながら実施し、紙のシートに内容を書き込んで、チェックをして完了といった形で運用がなされているところを、クラウド環境上ではソフトウェア的な手順として、つまりAPIやコマンドを使ったプログラムを書いて実装し、実行することになります。１度定義した手順を同様に繰り返し実行、検証できるようになります。また、そういった操作には実行した際に付随する様々なログが生成されます。そのため、意図したとおりにプログラムなり、操作が実行されたのか、その実行結果を確認しましょう、監査をしましょうとなった際のログの確認が容易であるという点がポイントです。

もう１つのポイントとしましては、クラウドの責任共有モデルということで、いろいろなところでこれは語られているかと思います。クラウドの評価といったときには画面の責任共有モデルのオレンジ色の部分に該当する箇所の議論がこれまでは多くなされてきたと思います。要するにクラウドベンダーが自身の環境の統制をどのようにしているのか、SOC1、SOC2といった形で、その第三者の評価をどのように受けているのか、ISOの認定は取得しているのかといったような議論です。クラウドのセキュリティやコンプライアンスの議論については、少々そこに比重が置かれ過ぎていたかなという印象を私どもは持っています。しかし、様々なコンプライアンスの要求事項を整理していくと、クラウドベンダー側で明確に責務を持って要件を満たすべき箇所は勿論様々に存在しますが、クラウド環境上に構築されたシステムにおいてどのようにシステムの操作や管理をしなければならないのか等、お客様に関係する要求事項の比重がより大きいと感じております。そのため、クラウド事業者は、そうしたお客様が対象となるコンプライアンス上の要求事項、それか

らお客様の操作運用の要件を満たすためのサービスの拡充に取り組んでいるという認識です。

また、画面の責任共有モデルでいいますと、緑色の箇所になりますが、お客様がクラウド環境上に構築したシステムにおいて、様々な要件や基準を満たすためにどのような運用をしていただくのか、そのためにクラウドベンダーがどのようなサービスを提供しているのか、それから、そのサービスを使って、お客様がどのような監査を実施可能かといったことについてお話をさせていただきます。

クラウド環境上のシステム運用ということで、画面にモデルを示させていただきました。従来のITのシステムの運用とほぼ同様であると思います。これからお話させていたくのは、監視、ログ管理、構成管理、変更管理といった点になりますが、他にはAPIやコマンドをどのように利用するのか等もあります。こういった一連のサイクルに従って、監視をしてなんらかの不備、あるいはコンプライアンス上の要件を満たしていないという箇所を、ログを参照しながら確認し、構成変更を実施していく、システム設計の見直しをしていく、というような運用がクラウド環境上では標準的なシステム運用の手順になっています。

ログの管理サービスということで、AWSの名称は画面にはでていませんが、AWSのサービスを参考にお話しをさせていただきます。ただし、クラウドサービスを提供されている事業者はほぼ同様のサービス内容をご提供されているという認識です。ログの管理サービスによってどのような内容が取得できるかという例ですが、あるユーザーのログインの成功や失敗、あるいはユーザーがあるシステムへの操作が新規に必要になったため、該当ユーザーに新しいアクセス権限を付与して該当システムへの操作を実行できるようにしますといった権限変更等の内容が時系列を伴って詳細に出力されます。後に実環境で取得したログを用意していますのでご覧いただきますが、要するに、誰が何を実行したのかという内容が詳細に取得可能です。

次に構成管理サービスの話です。誰が何をしたかという点に加えて考慮されるべき点になります。例えば、仮想サーバー、仮想のストレージ、仮想ネットワークのインタフェース、ファイアウォールの設定、ルーティングテーブル等のクラウド環境上のシステムを構成する要素はたくさん存在しますが、そういった構成要素の変更も時系列を伴ってどのようにシステム構成が変化したかという内容が取得可能です。

このようなデータが取得可能になると、クラウド環境上のシステムに対して、誰が何

時何分にどのような操作を、どのサーバーのどのネットワークインタフェースに対して実行したかといった内容が取得可能になります。そうすると何らかのインシデントや、セキュリティ上の問題が起こった際に、こうした時系列を伴った詳細なログを追うことで何が起こったか把握可能になります。あるいは、セキュリティポリシー通りにシステムが運用されているのか等の観点から、こうしたログを監査に用いることが可能になると考えています。

画面に表示されている内容が実際のログになります。例えばユーザーの権限変更の例を先ほど申し上げましたが、そういったログが確認できるかと思います。

次に画面に表示されているのがもう１つの実際のログの例、ファイアウォールのログになります。何時何分にどこのIPアドレスからどこにアクセスがあったのか等という内容が取得可能です。

前回の検討会で言及させていただきましたが、こうしたログの取得や構成管理をハードウェア環境、いわゆるオンプレミスの環境でも、実施していくことは可能です。しかし、様々な機器から、時には人によるマニュアルオペレーションが介在し、あるいはシステム台帳などの紙媒体から情報を取得しなければならなくなる、等、一連のプロセスを平準化し、標準的に同質のログを取得するというのは難しいと感じるところがあります。クラウド環境の場合は先ほどの例のようにそうしたログや構成管理の仕組みが環境に統合されており、システムや運用のプロセスはより抽象化された情報、コマンド、APIという形で存在していますので、標準的に一連のログの取得が容易になっています。そうした情報を、どのように加工してどう活用していくのかというところが、お客様毎に工夫していただくところであり、クラウド事業者が努力しなければならない、あるいはお客様と協力して実施していかなければならない事であると考えています。

画面に出ている内容は具体的に、どのようにこうしたログ等の情報を使っていただけるのか、という例になります。例えば、サーバーで使用されるストレージは全て暗号化しなければならない、というポリシーが存在する場合は、そのサーバーについているストレージの暗号化のオプションが有効化されて暗号化が実施されているのかの確認です。あるいは、ファイアウォールに何か変更があった場合に、ログを出力し、その変更を自動的に検出し、何らかの方法でアラートを上げる、といったことが可能になります。クラウド事業者は同様の機能を実装していると思われます。こういった仕組みを活用することで、監査や確認のみならず、実際何かインシデントが起こったときの対応というところまで、あ

る程度自動化して、標準化できるような環境をつくり出せるというのが私どもの考え方になります。

次の画面はこうして出力されたログの処理に関する内容で、ファイアウォールのログ内容を解析してグラフィカルに表示したものです。クラウド環境では詳細なログが取得可能となりますが、人の目で見ていくのはなかなか難しい量が出力されます。また、サンプリングということになりますと、従来の監査とあまり変わらないのではないかといった視点もあるかもしれません。しかし、ビッグデータを活用した解析基盤や、このようにグラフ化する、可視化する標準的なツールも各ベンダー様から提供されていますので、そのようなツールとログを活用することでどこからのIPアドレスのドロップが多い、あるいは、セキュリティインシデントにつながるような動きがあるかどうか、等の兆候を把握可能な運用につなげられるようになります。

最後に２枚ほどお話しさせていただこうと思っています。クラウド環境上ではコンプライアンスやセキュリティ上の要求事項を満たすために利用可能な、該当するクラウドベンダーのサービスや、機能を特定し、あらかじめ該当の要件に見合った設定をしておくことで該当の要求事項をシステムの設計、設定の段階から織り込むことが可能になります。画面はPCI DSSというデータのセキュリティ基準を基に要求事項とクラウドの機能をマッピングしたものです。例えば、事前に設定した、要求事項を織り込み済みのシステム設計をテンプレート化して毎回システムを起動すれば、システムが立ち上がった段階で既に80％要求事項を満たしている、あとの20％はアプリケーションや運用で、設定漏れ等を少なくしていける、等といったことが実現可能になるということです。

最後の画面ですが、そうしたサーバー、ネットワーク、データベース、ログの機能等をテンプレート化した設計概念図になります。具体的にテンプレート化というのはシステム設計を、クラウド環境を起動させる構成ファイルとして作成しておくということです。その構成ファイルを利用してクラウド環境を起動させると、コンプライアンスの要求事項、あるいは、監査上必須となっているログ機能が有効化されたシステムを起動すると、監査の効率的な実行につながるのではないかという１例として、本日はお話しさせていただきました。お時間いただきまして、ありがとうございます。

○岩原座長　ただいまの梅谷委員のご発表について、何かご質問ございますでしょうか。

○酒井委員代理　大変勉強になりましてありがとうございます。１点念のための確認ですけれども、ちょっと保守的な質問になるんですけれども、こういったログの情報収集とか、設定情報というものをツールで自動化ということで理解をしました。そうしたときにそもそもそのツールとか、収集する、自動化するシステムの統制状況というのは、SOC2とか、先ほどのご説明範囲外で把握できるという理解でよろしいですか。

○梅谷委員　ご質問は、例えばログの管理をするサービスがISOの要求事項に見合ったものであるか、SOC1等の外部監査を受けているか、という趣旨のご質問でよろしいでしょうか。提供するサービスによって異なりますが、アマゾンの場合ですと、こういったログの管理のサービスはISOのスコープにも入っていますし、SOC1の監査のスコープにも入っています。

○酒井委員代理　ありがとうございます。

○岩原座長　ほかに何かございますでしょうか。よろしいですか。梅谷さん、どうもありがとうございました。

○岩原座長　次に、第３回検討会への事後意見へのご回答でございます。
FISC企画部の藤永次長、お願いいたします。

○藤永次長　議事３（参考資料１）という横書きの資料をまずご用意ください。前回の有識者検討会の後にいただいた事後意見のリストです。全部で 14 の意見をいただいています。
１番として、梅谷委員からのご指摘です。「API 接続先チェックリストワーキンググループにおいて検討される管理策については、FinTech 有識者検討会における内容、FISC 安全対策基準や監査指針に関する今後の検討の中で、整合性をもった検討がなされるかという点について確認させてください」という質問です。
事務局回答としては、「イエス」ということです。当然、整合性をもって検討を今後行っていきます。

２番目として、同じく梅谷委員からです。「地銀共同センターを比較対象としてクラウド環境に足りない統制を語るのではなく、クラウドそのものの特性をもう一度見直し、あるべき統制を考えるほうが実行力のある統制を実現できる可能性があがるのではないかと考えます」ということで、今ほどのプレゼンでもありました責任分界に関するご指摘です。

事務局回答としては、ご指摘を踏まえ原案の修正をしております。修正内容は、後ほど修正文をご説明する中でお話しさせていただきます。

続きまして３番目、これも梅谷委員からです。「クラウド環境における監査については、クラウド側で提供している監査機能やサービスを利用することによる、監査の効率化や高度化を実施可能になる場合もあるため、その点については特性を理解した上で積極的な活用も考えられるという点について記述を追加していただけませんでしょうか」。これも、今ほどプレゼンいただいた内容です。ご指摘を受け本文に脚注を追加しております。詳細は後ほどご説明します。

４番目は梅谷委員のご意見です。「安対基準の設備基準や、技術基準を含めることを必ずしも意味しないことに留意が必要である」「という点は現在の実務と照らし合わせた上で適切と考えます」というご意見です。

５番目も梅谷委員のご質問です。「統制対象クラウド拠点とは具体的にはどのような施設が対象に入るのでしょうか」。「どのような施設が国内に存在すればよいと考えられますでしょうか」。また、「国内にあることの実質的な意味を具体的に示していただけませんでしょうか」ということです。これにつきましては、原文に大幅な加筆を加えておりますので、後ほどご説明します。

６番目も梅谷委員の監査権に関するご質問です。「監査権はどのような監査権をさすのでしょうか」。あと「統制対象クラウド拠点とは具体的にはどのような施設を対象としてもよいと考えられるのでしょうか」ということで、これにつきましても本文に大幅な加筆を加えておりますので、後ほどご説明します。

７番目も梅谷委員からのご意見とご質問です。「保証型監査の報告書を利用することが望ましい」という点については賛同をいただいています。「また、『定期的に監査を実施する』という記述がありますが、これはどのような監査を想定しているのでしょうか」ということす。これも原文に加筆を加えていますので、後ほど説明します。

８番目も梅谷委員からのご意見で、「必要となる人材を配置すること」の記述に賛同いただいています。

９番目は、南都銀行からいただいたご意見です。「客観的評価のときに技術的基準を必ずしも取り入れることを意味しない」と書いた部分について、「安対基準を用いないとすれば、各行が区々の基準で対応することになるため、必要最低限の基準は明確にする必要があるのではないか」というご意見です。ここにつきましては、安対基準を用いるべきでないと言っているわけではなく、必ずしもその全てを形式的に取り入れることがふさわしくないという趣旨です。ただし、さはさりながらということで、今後安対基準の改訂によって必要最低限の安対基準の策定が予定されておりますので、いただいたご指摘も参考としながら検討を行ってまいります。

10 番目も南都銀行からのご意見で、統制対象クラウド拠点の所在を国内に限定することについては、そういう必要がないのではないか、というご意見です。本文に大幅な加筆を加えていますので、後ほどご説明します。

11 番目から以降は、平原委員からのご質問です。「『重要な情報システム』『必要データ』『統制対象クラウド拠点』の詳細な定義についてご教示願います」ということで、重要な情報システムについては、外部委託に関する検討会報告書で定義を行っておりまして、「重大な外部性を有する情報システム」及び「機微情報を保有する情報システム」と説明しています。それ以外の２点については、前段の梅谷委員のご意見に対する回答とあわせて後ほど説明します。

12 番目、「『統制対象クラウド拠点』を『原則国内とする』必要はないのではないか」というご意見で、これも皆様からご意見をいただいていますので、後ほど詳細にご説明します。

13 番目、「『保証型監査』とは、JASA の整理する『助言型監査』と『保証型監査』の分類のうち、『保証型監査』を意味すると理解してよいでしょうか」ということですが、ここでいう保証型監査報告書とは、手前どもの「金融機関等のシステム監査指針（改訂第３版追補）」22 ページに記載をしているとおり「既にクラウド事業者が受検している監査結果」として、SOC2、IT７号について言及しています。米国公認会計士協会、あるいは日本公認会計士協会が定める内部統制報告の枠組み、フレームワークが既にありますので、それに基づいて策定された報告書を「保証型監査報告書」として、言及しているということです。

14 番目、「安対基準との整合性が確認できる報告書であれば、必ずしも、検証方法が安対基準と整合的に行われる必要はないのではないかと思料致しますがいかがでしょうか」

ということで、ここはもともとの原文が読みにくい内容になっていました。整合的にあるべきは「検証の方法」ではなくて、「検証の内容」と考えていますので、意図が明確になるよう修正を行っています。

○藤永次長　以上、14 項目のご指摘をいただきまして、原文を大幅に加筆修正を加えております。その中身のご説明ですが、議事３（参考資料２）という縦書きの資料をご用意ください。修正点を順にご説明します。

まず１ページです。「（２）海外先進諸国の動向」として、前回は英国の公表しているガイドラインをもとにまとめていましたが、今回、追加で米国の調査をこの間行っておりまして、参考２として英国並びに米国の最新動向の調査結果を追加しています。まず、その中身をご説明します。

参考２「クラウドサービスの利用に関する海外監督当局の動向」ですが、「近年、金融機関におけるクラウドサービス利用に関して、我が国のみならず海外先進諸国でもガイドラインの策定が進められている」という状況にあります。

米国では、2012 年７月 FFIEC と略称される、米国連邦金融機関検査協議会によって“Outsourced Cloud Computing”というガイドラインが既に公表されています。加えて、現在パブリッククラウドの利用が拡大している実態を踏まえて、新たな検討が FFIEC を中心として進められている状況にあることを確認しています。

一方、英国では昨年の 2016 年７月、FCA と略称されます金融行為規制機構によって、“Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services”というガイドラインが公表されています。

また、今回、我々は、３月初旬に OCC と略称されます米国通貨監督庁に対してヒアリングを行っており、公表文書とヒアリング結果をあわせて、ご紹介させていただきます。

まず１点目は「クラウドサービスに対するリスク管理の基本的な考え方」です。「金融機関には、クラウド事業者に業務を外部委託する場合においても、金融機関内部で実施した場合と同様の統制を要求するとともに、内部で実施した場合と比較してリスクが増大しないように、統制の強化を求めている」というところです。米国としては、「クラウドサービスを利用する場合においても、インハウスと同様のリスク管理が何らかの方法でなされていることを要求する。」英国におきましても「『デューデリジェンスの実施時に、外部委託により、金融機関にオペレーショナルリスクが増大しないことを確認すること』が求

められています。外部委託する、あるいはクラウドに委託するからといって、統制が低下していいということではないということです。

２点目は「統制に対する考え方」です。「統制にあたっては、利用検討時の客観的評価・締結する契約内容・運用時のモニタリングといった管理フェーズに応じて行われる」、こと、すなわち「統制の方法」が重視されています。

米国では、「パブリッククラウドを利用する場合にまず重要なのが、契約時のデューデリジェンスと契約の中身そのものである。さらに、契約後のモニタリングも重要であり、たとえばサービスレベルアグリーメントのモニタリングは」有効なモニタリングであるとされています。一方で、技術的な統制の部分、すなわち「統制の内容」は「金融機関に委ねられており、金融機関には技術を十分に理解し、適切に利用していることが求められている」。

米国では、「どの技術を利用するかは金融機関が決めることであり、それに対して当局が指示をするものではない。どの技術を利用するにしても、同様の内部統制や管理を要求することとなる」としたうえで、具体的な例を取り上げています。暗号化のキーの管理についてですが、キーについて、クラウド事業者がどのような目的でそのキーを使ったのかが把握できるような方策を取っていればよい、とし、ファイアウォールにしても、その仕組みを理解して正常に稼働するのかどうか、テストをしておく必要がある、と言われております。

３点目に「監査権に対する考え方」です。今回、多くの委員に事後意見をいただいたところですが、「金融機関に対して、クラウド事業者との契約書上、実質的な統制が行えるよう手当てをすることを求めている」ということです。英国では、「契約に、英国の法令が及び、かつ英国の裁判管轄に属することを確認すること」とされており、「そうでない場合は」、「実効的にアクセスする手段を手当てすることが必要である」とされています。

「米国では、個人を特定できる情報の取扱いに関する法令（グラム・リーチ・ブライリー法)」というのがあり、そうした法令に定める場合を除いては、「クラウド事業者に対する監査権を契約書上明記することを強制していない」ということです。この背景として、米国では、バンク・サービス・カンパニー法にという法律が古くからあり、監督当局が銀行の業務のアウトソーシングを受けているベンダーに対して、直接検査ができることもあるものと推測しています。

米国は、「銀行は、クラウドベンダーに対して監査権を持つべき」だとは思うし、契約

書にも定めるべきであるとは思うが、これはあくまでもベストプラクティスである。」としています。一方、多くの銀行が勘定系システムをアウトソーシングしているベンダーに対しては、OCC、FDIC、FRB などが共同で検査に入り、その報告書はベンダーを利用している金融機関に還元されている、という状況にあります。

一方、今回取り上げている保証型監査報告書の有効性についても調査をしており、その有効性が評価されています。

米国では「主要なクラウド事業者は、独立監査法人の監査を受け、米国公認会計士協会の規格に沿った保証型監査報告書」、SOC1、SOC2、SOC3 と通称されていますが、「を顧客に提供している。現実的には、多くの場合それらは範囲を含め十分な内容であるので、そうした報告を受けているのであれば、追加で金融機関が監査することが必要という状況ではない」ということです。「現実問題として、数千もの顧客を持つ主要クラウド事業者がいちいち顧客からの監査を受けていたらもたないだろう。しかしながら、もしその報告書が不十分なのであれば、追加で監査できるように契約しておくことが望ましい。」とされています。FISC のクラウド基準も、従来からそのような内容になっています。

４点目が「データの所在に対する考え方」でございます。ここも多くの事後意見をいただいた部分でございます。

「データを自国内で保存しなければならない」という規制はない。ただし、「いずれに所在しようとも、金融機関や当局による実質的なアクセスが可能となっていることが求められる。そのため、データの所在地を把握しておくことが求められる」。そこは変わらない。

英国ではこうしたデータというの実質的なアクセスが可能になるように要求されていますが、ここの「データ」というのはかなり広くとらえられています。金融機関のデータだけでなく、個人顧客のデータ、取引履歴データ、さらには先ほど梅谷委員からプレゼンがあった監査証跡もこれに該当するのではないかと思いますが、システム監査証跡あるいはスタッフのバックグラウンドチェックです。その手続きについても、データの中に含まれるということで相当幅広く解されています。

米国では、「データを米国内で保存しなければならないという規制はないが、データが米国内にある場合と同様に、必要な場合は必要なデータが入手できる状態にしていなければならない」。

かつ、「パブリッククラウドの場合でも、データが保管される地理的な範囲は決められ

ており」、要はわかるのではないかということで、銀行はある意味どこにあるのかということは知り得るし、モニタリングもできるのではないか。「監督当局は、銀行がデータが行ってはいけない場所に行っていないか、モニタリングしていることを検査する」ということに重点が置かれているということです。

５点目が「技術の先進性に対する考え方」です。「金融機関は、クラウドにはこれまでになかったリスクが発生する可能性があることを認識し、あらかじめその内容を理解し必要な手当てをしておくことが求められる。また、これまでになかったリスクとして」、匿名性という性質に基づく、システムを共同で利用しているのは誰かわからない、そのため、他の利用者の影響を受けることはあるのかないのか、という利用者同士のシステムが相互に影響を与えるリスクが重視されています。

米国では、「パブリッククラウドについては、SaaS よりも PaaS や IaaS の方が金融機関にとっての負担は大きくリスクも高くなる」。金融機関が責任を担う部分が多いから、ということであろうと思います。金融機関が自らの責任を理解していることが重要であるということです。また、よりコアに近い、重要な「システムをクラウドに移管すればその分リスクも高くなる。ただし、大手ベンダーのレベルと理解力は高いことは当局も実感しており、実際には金融機関側がベンダーに教わっていることが」実情としては多いと言われています。

また、「ハードウェア上、金融機関のデータが固まって保存されている」、要は金融機関だけで例えば特定のサイトに集中管理されているならばよいが、「例えばゲーム事業者と一緒であれば、それなりのリスクはあるかもしれない」ということで、「金融機関がハッキングされなくても、同じハードウェアにいる別の利用者がハッキングされて、その影響を受けないか、検証する必要がある」という観点が持たれています。

英国においても、「委託元毎で、データを分離する方法について留意すること（パブリッククラウドを使用する場合)」、とし、そうした留意点があるとされています。

こうした観点は、今後の我が国の安対基準の改訂において１つの参考になるものと思います。

６点目が「事業継続計画に対する考え方」です。これについては、「業務の継続計画について、委託先とあらかじめ協議し文書化するとともに、訓練を通じて、その実効性を定期的に検証することを求めている」。

米国では、「データの冗長性についてあらかじめ契約しておく必要がある。また、冗長

性を契約上持たせる場合でも、実際のところどのようになるのかを理解し、本当に想定どおりになるかをテストしておく必要がある」。

英国においても、「金融機関は外部委託業務が予期せず中断した場合にも、業務を継続できるよう、委託先と適切に協定しておく必要がある。その場合に、金融機関は、業務継続性の維持や復旧のための戦略を文書化すること、その戦略の適切性と有効性を定期的に検証すること等が必要である」とされています。

外部委託に関する有識者検討会においても、同様に、外部委託先とあらかじめ BCP を策定して、かつその訓練を行うということは、既に提言されています。

７点目が「その他」ということで、米国当局のコメントとして「クラウドベンダーは、規制業種である銀行のことをよく理解していないので、粘り強く交渉し、銀行に必要な条項を契約に盛り込む必要がある。これで相当程度、直接監査できない問題等に対応できる」と言われています。

我が国では、例えばクラウド事業者の皆様に FISC へ入会していただく、あるいは、この場のような有識者検討会等の会議体への参画等を通じて、クラウド事業者が、金融業務に対する理解を深める機会が、提供できているのではないか、考えています。

以上が、３月に調査したばかりの内容を盛り込んだ説明です。

本文にもどりまして、３ページです。前回席上でもご意見をいただいた箇所ですが、「サービス全体に責任を負うクラウド事業者」としていましたが、席上で責任分界のご意見があり、事後でもいただいていますので、「サービス全体に責任を負う」を削除した上で、「クラウドサービスにおける」という修飾語を付加しています。

その下ですが、「クラウドサービスに対しては」としていましたが、「クラウド事業者に対しては」とし、また、「問題が内在している」と断定的に書いていたのを、「可能性が内在している」と変更しています。続いて「そうした可能性を考慮に入れたうえで、適切にクラウド事業者の選定が行われ」ることが必要であろうとしています。

次に、共同センターとは同じようで違う点ですが、「同様に共同性という性質を有する『共同センター』において行われている統制の観点を踏まえてリスク管理策を検討することが考えられるが、一方で、特定の委託先が、包括的に業務を受託する共同センターと異なり、クラウドサービスはクラウド事業者が、情報システムのハードウェアや基本ソフトウェア等部分的に業務を受託する形態があることに留意が必要である」と修正しました。

さらに下のところで、「クラウド事業者との責任分界等を理解したうえで、統制の範囲

や内容を決定することとなる」とし、脚注の 11 を追加し、安対基準の中のクラウド基準においても既にそういう観点が織り込まれていることを補記、以上のとおり、梅谷委員からいただいた責任分界に対する考え方を明確に記載させていただきました。

あとその下の「金融機関は」というところは主語がわかりにくかったので、便宜的に追加しているところでございます。

５ページですが、第２パラグラフ目の「そうした中」の続きですが、「例えば、クラウド事業者選定時の客観的評価において、評価事項に設備基準や技術基準が字義通りに利用される、といった不確実性が残る現状にある」という課題認識を示しています。これについて、もう少し具体的にどういうケースがあるかということで、南都銀行からの事後意見も踏まえて、課題認識を、口頭で補足させていただきます。

例えば、設備基準の中には、設備の 47「ネズミの害を防止する措置を講じることと」いう基準があります。これはクラウド事業者と金融機関が、安対基準について、やり取りをされる中で、言及されることがあるのではないかと思います。ネズミの害は、当然リスクとして存在することは事実ですし、データセンターにおける安全対策として必要となる観点ではあるでしょう。ただし、自前で金融機関がコンピューターセンターをつくるときにはという点において。すなわち、本検討会で委員として出席されているようなクラウド事業者が使用されているデータセンターでは、ネズミの害というリスクは、改めて金融機関が明示的に確認が必要なほど高いかというと、そうではないだろう、と考えています。

しかしながら、設備 47 を含む、設備基準に書かれているもの全てを字義どおりにクラウド事業者に確認を求めると、ややコミュニケーションに不必要な時間を要するような、側面があるのではないか。字義どおりの利用ではなくて、より実質的な安対基準の利用をしていただくことが望ましいのではないか、と考えています。

同じような観点で、技術基準の 28、29 として、データの漏洩防止策を講ずることという基準があります。その中に暗号化を実施することが望ましい、とされ、技術的な例示が幾つか定められています。クラウド事業者では、データの漏洩防止策というのはさまざまに進歩し、日々改善されていると思いますので、必ずしも安対基準に書かれている内容を確定的に形式的に求めることは適切じゃないのではないか、ということです。以上のとおり、設備基準や技術基準といった、技術的な基準の課題をここでは取り上げています。

５ページの（４）ですが、今回事後意見をたくさんいただいた部分について、個々のご質問に対する個別の答えということではなくて、恐らく本質的に皆様にご理解いただか

ないといけない本質的なこと、紐解かないといけないこと、はこういうことではないだろうか、ということで、大幅に加筆した部分です。

それは「重要な情報システムの外部委託先に対する統制の考え方」です。「まず」というところで「『重要な情報システム』とは、『重大な外部性を有する情報システム』もしくは『機微情報を保有する情報システム』のことをいう」。これは、外部委託に関する有識者検討会報告書で提言されたとおりです。「前者において大規模なシステム障害が発生した場合、その影響は顧客等の内部影響にとどまらず、金融インフラや経済の安定的な運営にも影響を及ぼす可能性があり、後者において機微な個人情報が流出した場合、信用不安を惹起し、金融機関の存立を揺るがす事態に発展する可能性がある。このように社会的・公共的性質を有する情報システムにおける有事対応の責任は、外部委託を利用している場合であっても、技術的な側面を担う外部委託先が負えるものではない」ということで、「金融機関が負うべきものである。」としています。「したがって、金融機関には、有事において、その影響を最小化するとともに、情報システムを速やかに復旧させ業務の継続性を確保する責任があり、外部委託先に対して、内部の場合と同程度の統制が行えるようにあらかじめ十分な手当てをしておくことが求められる」。」、ここは先ほどご紹介した海外の監督当局の認識と整合的です。

加えて、「こうした有事における実質的な統制を可能とするには、平時から異常を見逃さない等システム運用状況を日常的に監視しておく必要があるとともに、定期的に外部委託先における内部統制状況をチェックし、有事の発生やその対応に影響を及ぼす可能性のある問題があれば、あらかじめ外部委託先に対処を促し、問題を解決しておくことが必要となる」ということで、これは日常的監視や監査という「モニタリング」として我々が言及してきたものです。ここで外部委託先に求めるものが、先ほどご説明した外部委託先の安全対策遂行能力となります。

「以上のことは、外部委託の一形態であるクラウドサービスにおいても同様であり、金融機関は、重要な情報システムでクラウドサービスを利用する場合は、クラウド事業者の責任分界を踏まえ、業務継続におけるクラウドサービスの位置づけ等に留意しつつ、実質的な統制を行うことが必要である」としています。

これだけですと、まだ抽象的ではないかというご意見を事前にいただいており、脚注16 にもう少しかみ砕いて解説を加えています。「金融機関においては、有事における影響の最小化と業務の継続性の確保が第一に求められることとなるが、これは全ての金融機関

においてクラウド事業者に一意なリスク管理策を求めることを必ずしも意味しない。」例えば、「有事にはクラウドサービスの復旧を待つことなく、有事用にスタンバイしているシステムを稼働させるような業務継続計画であれば、クラウドサービスの復旧を前提とした業務継続計画の場合とは、自ずとクラウド事業者に対するリスク管理策は異なるはずである。また、外部委託報告書で示されているとおり、委託業務が細分化された結果、クラウド事業者の受託業務のリスクが十分に低いと判断しうる場合」もある。そうした場合にも「リスク管理策は異なる」。要は、「金融機関は、重要な情報システムにおいて、クラウドサービスがどのように位置づけられるか、どのような利用形態をとっているか、によってクラウド事業者に対する具体的なリスク管理策を判断することになる」。したがって、FISC が一意にこういうことをやるべきだというリスク管理策を特定することは難しいというのが、クラウドの特徴ではないか、ということです。

そうした考え方を踏まえて、本文の「３．リスク管理策に関する補足」ですが、「実質的な統制を行う」ことが金融機関に必要ではないか。その実質的な統制が具体的にどのような中身であるかというのは、ある意味金融機関のクラウドサービスの位置づけとか利用形態によって金融機関が個々に判断するものではないか、ということでございます。そうした基本的な考え方に従って修文を加えています。

（１）番がデータアクセス拠点の把握です。「統制対象クラウド拠点は、実質的な統制が可能となる地域（国、州等）に所在すること」と修正しています。これは海外の監督当局の動向も踏まえて、整合性を取っています。

そのことが、具体的にどういうことを意味するか、事業拠点は何だ、ということなのですが、脚注 17 で、かみ砕いて解説しています。「統制対象クラウド拠点は、クラウド事業者の本社、営業所、データセンター、オペレーションセンターなど様々な拠点が候補となる」。重要なのは、どこに行けばコントロールができるかということですが、「実際には、利用するクラウドサービスの内容やクラウド事業者の内部管理状況等」、どこでどのような管理が行われるかということを踏まえて、統制を行うデータがどこで入手できて、どこの拠点で実質的なコントロールができるかということを「金融機関が個別に特定することになる」。あらかじめ、一意に特定できないということです。したがって、そこから導き出されるのが、「統制対象クラウド拠点には、データセンターを含むことは必ずしも必要ではない」ということです。データセンターに行った方もいらっしゃるかと思いますが、そこでどのようなコントロールができるかという観点に立って考えると、必ずしもデ

ータセンターに行けば、何でもコントロールできるということではない、ということはご理解いただけると思います。

その次の「監査権等の明記」ということで「等」という言葉を入れたことと、ここについても監査権というある意味包括的な権利を形式的に語るのではなくて、実質的な統制を行うに当たって必要となる権利、これには監査権も含まれるかもしれませんが必ずしもそれだけではない。それを「クラウド事業者と交わす契約書に明記する」ということにしてはどうかというご提案です。

その下の「監査の実施」のところはマイクロソフトの平原委員のご意見で、「整合的な内容で」ということで修正しています。

脚注 16 では、梅谷委員からのご意見を踏まえまして、「その他に実効的かつ効率的な監査を実施する手段として、インターネット等などを通じて利用者に提供される監査証跡の閲覧等クラウド事業者がサービスとして提供する監査機能を利用することも考えられる」ということで、そうしたクラウド事業者側の取り組みが進んでいくことを、我々としても期待しています。

以上が本文に対する修正でございます。あともう１点だけ、次の８ページの「クラウドの利用状況の表」でございますが、前回席上のご意見として、「利用中」と一括りにしていましたが、プライベート、コミュニティ、パブリックで違うのでは、というご意見をいただいていましたので、「利用中」の中を、プライベート、コミュニティ、パブリックというふうに色分けしました。これによれば、平成 27 年度の FISC の調査の結果では、パブリッククラウドを利用している金融機関は 17.4％という状況になっております。いずれにしましても、クラウドの利用は右肩上がりというとちょっと言い過ぎかもしれませんが、進んでいるという状況にあるということです。長くなりましたが、私からの説明は以上です。

○岩原座長　ただいまのご説明に対して何かご質問ございますでしょうか。

○安冨委員　５ページの最後の行、下のところです。「機微な個人情報が流出」という言葉が出てくるのですが、この検討会で触れるべきかどうかということは、私も今特段の意見を持つわけでもないのですが、ご案内のとおり、今年の５月から個人情報保護法が改正されて、要配慮個人情報という概念が導入されることになりました。金融庁のガイドラ

インで機微な個人情報という定義というか概念があります。それと要配慮個人情報というのは、かぶる部分とかぶらない部分があるのですけれども、そういう状況を考えますと、ここに機微な個人情報という表現が出てくると、これは多分、金融庁のガイドラインを想定されて表現されたのだと思うのですが。若干個人情報保護法上の要配慮個人情報との関連というか、ようなものも示唆するような、注書きでいいと思うのですが、何かあったほうが適当なのではないかなとも思うのですが、ご検討いただければと思います。

○藤永次長　ここで書いてある機微な個人情報につきましては、外部委託に関する有識者検討会の報告書の中で定義をしておりまして、ご指摘のとおり、金融庁の「金融分野における個人情報保護に関するガイドライン」に基づいています。個人情報保護法の改正につきましては、法律ですので、法令遵守は当然のことであり、個別に細かいことを本文では言及していません。しかしながら、ご指摘のとおり、法令との関係についてわかりにくさがあると思いますので、補足することを検討します。

○安冨委員　お願いします。

○岩原座長　ほかにいかがでしょうか。

○梅谷委員　ページ10の米国の監督当局様へのインタビューというところで、中段あたりの箇所になります。「例えば事業者が提供する暗号化ツールを利用する場合」という記述の箇所です。ここはインタビューの結果ということなので、FISC様からの意見ではないと理解しての発言ですが、印象としてクラウド事業者の職員も暗号化を解くキーを持つことになる、というふうなことを当局の方がおっしゃったようです。これは、ちょっと言い過ぎといいますか、そういう例もあるのかもしれませんけれども、例えばハードウェアセキュリティモジュールという、ハードウェア的に暗号鍵を安全に管理するような機構を使って、クラウドベンダー側が全くキーにアクセスできないというようなオプションを提供するベンダーも多く存在すると思います。これは一例であって、場合によるのかなという印象です。修正案というよりも意見として申し上げさせていただきますので、何かしら事務局の方から返答が必要とかそういう趣旨ではありません。

もう１つは、ページ７です。一番上の「監査権等の明記」ということで、これは実質

的な統制ということで藤永様からご説明いただいたとおり、実効的にするには何かということで大分練って事務局のほうで修正されたということを理解しております。「(監査権等)」という記述を含めて、いろいろ意見を交換された後で、「クラウド事業者と交わす契約書」という記述になったかと思いますが、例えば「クラウド事業者と交わす契約書」を「クラウド事業者と交わす契約書等」という形にしていただくなど、最終的な表現の形態をどうするかというのは、もう少し議論が必要かなというふうに考えております。

もともとのオリジナルの文章は「業務委託契約書」という形になっておりましたが、契約書に必ずしも書く必要があるのか、という意見を我々はもっておりますので、「等」という形で、形式は幅広くとっていただくような表現にしていただくのはどうか、ということを申し上げさせていただきます。ありがとうございます。

○藤永次長　前段の１点目の当局のヒアリングについては、実際のヒアリングペーパーはもっと長く、それをもとに、我々のほうでまとめています。その過程で誤解が生じるような書き方になったものですので、当局が断定的に言っているわけではありません。そこは誤解が生じないように正確な記載に修正します。

２点目については、契約書と呼ぶか、どういうふうに呼ぶか、はともかくとして、そうした金融機関側の権利を事前に担保しておく、すなわち、実質的な統制を行うことができるような権利を担保しておくことが必要である、という考え方に立っていますので、その観点において文章が適切に修文し得る案があれば、修正する準備はあります。

○岩原座長　ほかに何かございますでしょうか。

○酒井委員代理　今回の修正の箇所ではなくて恐縮なんですけれども、７ページ目の真ん中の（４）番の「監査人等モニタリング人材配置」のところです。ここの真ん中のところで「クラウド事業者に対する監査等モニタリングを実効的に実施するために必要となる能力を有した人材を配置すること」と書いてございます。こちらはすごく私どもも非常に賛成なんですけれども、逆に非常に難しいことだと思っています。私どもはいろんな金融機関、FinTechの小規模企業から大規模金融機関をサポートさせている立場からお話しさせていただくと、やはり、このリソース管理できる経営陣の認識というのは、企業規模によっても差異があると思っています。FinTech企業は、現場との距離も近いというとこ

ろもあり、リスク管理に関して非常に関心をお持ちの場合も高いです。特にクラウドの場合は、本質的なリスクですね。プロセスベースのコントロールではなくて、本質的なリスクをどう解決していくかというところの議論が、非常にクラウドの特徴だと思うんですけれども、逆に大企業の金融機関の場合は、こういったリスクの考え方の変化というところに、うまく経営の方も気づきにくい環境になっているのかなというのが印象にあります。

ですので、何が言いたいかというと、結局この人材配置というのは経営の方にいかに環境の変化で、ほかの議事でもあるリスクベースアプローチでこれから変わっていくんだというところがありますので、これは公表されるときでも結構ですけれども、ぜひともFISCのほうから市場に対して、特に経営者に対してこういった変化をアピールもしくは前文で言及いただくとかご検討いただければ幸いでございます。以上です。

○岩原座長　よろしいでしょうか。ほかに何かございますでしょうか。特にないようでございましたら、藤永次長、どうもありがとうございました。

４．【議事４】今後の安対基準等改訂の考え方

○岩原座長　続きまして４つ目の記事は、「今後の安対基準改訂の考え方について」でございます。FISCの藤永次長、よろしくお願いいたします。

○藤永次長　議事４の資料をご用意ください。今まで外部委託の検討会から FinTech の検討会にかけて、さまざまに皆様に検討いただいた中身について、今後の安対基準改訂に橋渡しできるよう、１枚で考え方をまとめています。FISC では、本検討会の後に、外部委託検討会および FinTech 検討会の提言を受けて、安対基準等ガイドラインの改訂が進められることとなりますが、その際には、以下をはじめとして、両検討会報告書の内容を踏まえた改訂が行われ、金融情報システムの安全対策に携わる多岐にわたる関係者において、安全対策の考え方を中心に理解が得られるものとなることが期待される、ということです。これは、ひとつには、FinTech に関連しまして安全対策に携わる関係者が多岐にわたってくるであろうということ。また、そうした皆様においても基準は当然のことながら、その前提となる考え方、外部委託から FinTech にかけてはその考え方について非常に紙を費やして提言をしていますので、考え方を中心に理解が得られるものということが期待されるのではないか、ということです。

資料では、主要なものを３点取り上げています。１つは「安全対策の基本原則の導入」。これは、外部委託のときに定めたものです。リスクベースアプローチ、IT ガバナンスを集約したものです。

２点目が「安対基準の明確化」で、その１点目が「安対基準の対象の明確化」。これは安対基準が対象とするのは金融情報システム、すなわち、金融機関が行う金融業務を担う情報システムである、ということを明確化するとともに、それ以外の情報システムと安対基準との関係についてもつまびらかにしては、ということです。２点目が外部委託の検討会の提言内容で、高い安対基準と必要最低限の安対基準を盛り込んでいくべきであろうということです。３点目が先ほど来口頭で説明したところですが、技術的な基準の位置づけを明確にしてはということです。技術の進展が著しい環境下では、技術的な基準とそれ以外の基準では、取扱いが異なるべきであることを明確化する。技術的な基準は、全ての情報システムに対して字義通りに適用を求められるべきではなく、「高い安対基準」や「必要最低限の安対基準」を参考としつつ、最新の技術動向等を踏まえ、金融機関において適

用の可否が判断されるべきものではないかということです。

３点目は、外部委託の検討会から FinTech の検討会にかけて、多くの紙数を費やしたメインイッシューですが、「外部に対する統制の拡充」です。統制の重点がシフトしている現状を反映すべきであるということです。今や勘定系基幹システムの９割以上が外部委託に依存している。今後その傾向が、クラウドの利用が進む中で、高まっていくであろう。こうした統制の重点が内部から外部へシフトしていく実態を踏まえ、安対基準の中で、外部に対する統制基準を明確にしていく。今三百数十ある基準のうち十数個しか外部委託の基準はないのですが、そこを明確化して拡充していくということです。また、外部に対する統制の形態の整理が必要であろうということです。この間、共同センター、クラウドサービス、FinTech 等々多様な形態が出現している中で、それぞれの性質に応じた統制のあり方を示した上で、それに従った基準の整理を行うべきであろうということです。

これ以外にも有識者検討会で多くの議論をしていただいていますが、まずは骨格となる主要なものを書いた上で、次の安対基準改訂の専門委員会に有識者検討会の委員の提言としてバトンタッチといいますか、橋渡ししていくという、そのために用意した資料です。以上です。

○岩原座長　ただいまのご説明についてご質問、ご意見ございますでしょうか。

特にございませんか。それでは、藤永次長、どうもありがとうございました。

５.【議事５】API接続先チェックリスト（仮称）ワーキンググループ
活動状況と今後の予定について

○岩原座長　続いて５つ目の議事に移らせていただきます。「API接続先チェックリスト（仮称）ワーキンググループ活動実績と今後の予定について」のご説明でございます。FISC企画部の大澤主任研究員にお願いいたします。

○大澤主任研究員　前回のこの場で委員の皆様にご承認いただきましたワーキンググループの活動について、その途中経過をご報告させていただきます。

まず初めにワーキンググループの委員の方は次ページに記載の通り10名の方で、オブザーバーの方は４名の方となっています。表上一番下は赤字になっておりますが、前回この場で出させていただいたものにミス等がありまして追加しております。そういう意味で赤字になっているというふうにご覧いただければと思います。

表面に戻っていただきまして開催実績等ですが、約１カ月半の間で４回ほど、会合を持っております。それぞれ２時間目いっぱい時間を使って委員の方にご発言と議論をしていただいております。

まず第１回目は、本有識者検討会の議論を踏まえてチェックリストの議論をしなければいけないというところがございましたので、検討の前提ということで、こちらの検討会の議論の内容をワーキンググループのメンバーの方にご確認いただきました。

その後は、第２回は委員の方から、自発的に発表されたいという方がいらっしゃいましたので、その方にたたき台等を踏まえて発表していただいたものも含めて、多方面から議論を始め、そして３回目、４回目は事務局案も出しながら今現在議論を進めている途中でございます。

もともとこのワーキンググループは６月末を目途に活動をしていますが、５月15日次回のこの本有識者検討会の席上にチェックリストの原案を上程させていただきまして、委員の皆様から多方面から見ていただいて、それを踏まえて６月末に完成する。そのように考えています。以上簡単ですが、ご報告させていただきました。

○岩原座長　ただいまのご説明に対してご質問ご意見ございますでしょうか。

○神田オブザーバー　ただいまご説明いただいたAPI接続先のチェックリストにつきましては、前回もご説明いただいておりますけれども、金融審議会の金融制度ワーキングの電子決済等代行業者に関する制度、それから、全銀協が事務局になって議論を進めて頂きました、オープンAPIの検討会からきます議論、これらを踏まえて銀行とAPIでつながっていくFinTech業者との接続の際のチェックリストをつくっていただくということで、非常に急ピッチで検討していただいているものと認識しております。

そういう意味では、制度と実務の両面から詰めていくことが非常に重要な項目と認識しておりまして、銀行とFinTech事業者双方にとって実務に沿った使い勝手のよいチェックリストにしていただくように、しっかりとご議論いただきたいと考えております。

私ども金融庁のほうでもオブザーバーに入っておりますが、皆様にもご協力いただいてしっかりしたものをつくっていただきたいと考えておりますので、よろしくお願いいたします。

○岩原座長　何かほかにご質問、ご意見ありますでしょうか。よろしいですか。

それでは、大澤主任研究員、どうもありがとうございました。

６．事務連絡

○岩原座長　最後に、今後の事務連絡等について、小林企画部長にお願いいたします。

○小林企画部長　皆様どうもありがとうございました。今後の事務連絡３点ございます。

１点目ですが、本日の内容に対する事後のご意見等ございましたら１枚目の下のほうに書いてございますけれども、１週間後の３月30日木曜日夕方５時までに手前ども事務局のほうまで電子メールで頂戴できたらと思います。よろしくお願いいたします。

２点目ですが本日第４回、次の第５回の検討会のご案内ですが、次回は５月15日月曜日同じ時間15時45分～17時45分を予定しておりますので、年度が変わるタイミングになりますけれども、皆様にはスケジュール調整をいただけたらありがたいと思います。

最後、３点目、これは念のためのご案内ですけれども、申し上げたように年度末ということで、このタイミングで委員の皆様、オブザーバーの皆様が交代されるというタイミングにあられる組織の方もいらっしゃると思いますので、そういった場合には可能でございましたら、何かわかり次第、早目に手前どもにご連絡頂戴できたらというふうに思います。以上でございます。

○岩原座長　どうもありがとうございました。全体を通じて何かご質問等ございますでしょうか。よろしいですか。

それでは、特にご質問ご意見等もございませんようですので、これにて第４回金融機関におけるFinTechに関する有識者検討会を終了いたします。どうもありがとうございました。

以上