平成29年２月24日

公益財団法人　金融情報システムセンター

第３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２月２日（木）15:45～17:40

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
	由井 敬人	（代理出席） 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 リスク管理企画チーム 調査役
	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
	瀧 俊雄	株式会社マネーフォワード 取締役Fintech研究所長
	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
	岩田 太地	日本電気株式会社 事業イノベーション戦略本部 フィンテック事業開発室 室長
	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
	荻生 泰之	デロイトトーマツコンサルティング合同会社 執行役員
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
	道方 孝志	（代理出席） 総務省 情報流通行政局 情報流通振興課 情報セキュリティ対策室 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
	亀水 宏次	（代理出席） 監査安全部　次長

Ⅳ　議事内容

１．【議事１】第２回 FinTech 有識者検討会に対するご意見及びご回答

〇岩原座長　座長の岩原でございます。それでは本日、１つ目の議事といたしまして、前回の検討会の後にいただいたご意見について、事務局よりご説明をお願いします。小林企画部長、お願いします。

〇小林部長　それでは議事１の資料をご覧ください。前回第２回の検討会以降にいただいたご意見として、マネーフォワードの瀧様から２件いただいておりますのでご紹介させていただきます。

１番、議事１「第１回 FinTech 有識者検討会に対するご意見及びご回答」について、これは前回ご回答した対象外の FinTech 業務についてです。金融機関の受動―交渉なしのモデルは対象外となりますが、そのモデルに当てはまることがある「スクレイピングはセキュリティ上の改善があるべき技術という認識はコンセンサスがあるものかと思います。しかし、こちらが昨今急にリスクが高くなったとする判断は、不確実性をもたらすものと考えております。順当な技術的理解のもとに、議論が行われていくことを望んでおります」。

冒頭申し上げましたとおり、問題なのは技術というより金融機関が受動―交渉がないというところにあると考えております。したがいまして、右側事務局回答のところをご覧ください、ご指摘を踏まえ本検討会第１回の議事『金融機関における FinTech に関する安全対策を検討の在り方』別紙１脚注 11 に以下のとおり補足いたします。

「〈補足〉なお、これはスクリーンスクレイピングが採用されていることをもって直ちに問題があるわけではなく、本来的には金融機関と交渉なく顧客に関するデータが取得されることが問題である点に留意が必要である」。

同じく瀧委員からいただきました２番をご覧ください。前回の議事３「FinTech に関する安対基準適用上の課題」についてです。

「現状、全国銀行協会での「オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方」の素案では API 接続先企業の事前審査につき、ある程度汎用的なチェックリストを作る試みへの言及があります。これは個別の企業にとっても対応負荷を

下げる良い取り組みと考えております。

FinTech の領域ごとにテンプレートは異なっていくものと考えておりますが、タイプⅢでは多数の金融機関にサービス提供するようなケースが多いため、テンプレートを作成していくような動きを促進できる表現を加えて頂くことを検討していただきたく存じます」。

前半部分は本日の議題の１つにも挙げております API 接続先チェックリストへの FISC の取り組みとしてご説明させていただきますが、右側をご覧ください。全体のご指摘を踏まえ、本検討会第２回の議事『安対基準の対象外となる FinTech 業務の取扱い』別紙１に『４．社会的に合意されたルールの形成に向けた FISC の役割』として補足いたします。この後すぐ該当部分をご説明申し上げます。

では、以上の部分を含め、第１回・第２回の論点メモの修正を次長の藤永からご説明させていただきます。

○藤永次長　企画部の藤永です。今説明がありました事後意見に関する回答及び前回席上で幾つかご指摘いただいた点等を踏まえまして、修正案を本日は用意しております。順番にご説明します。

最初に参考資料１として前回第２回の議事４「安対基準の対象外となる FinTech 業務の取扱い」に関して修正を加えております。資料をおめくりいただきまして６ページのところです。もともと第１回のときに、FISC が必ずしも対象としない部分についても意見表明を行うことが妥当であるということでご意見をいただいたのを踏まえまして、前回意見表明文というのをご議論いただきました。それを踏まえ、その意見表明の内容をさらに実効たらしめるために FISC として何らかの役割を果たすべきではないか、ということで、瀧委員からのご指摘の部分も踏まえまして内容をご用意しております。

社会的に合意されたルールの形成に向けた FISC の役割としまして、もともと従来金融情報システムの主たる関係者は、金融機関と IT ベンダーの皆様でございましたが、ほぼ FISC の会員となっていただいたというところもありまして、FISC の安対基準を見れば金融情報システムの担い手の意向や特性を概ね確認することができるという、そういう状態が続いてまいりました。しかし、これからオープンイノベーションが進展していくに従って、従来以上に複数の事業者が金融関連サービスの提供に携わることが予想される。これは前回の問題提起でございます。そうした中で必ずしも FISC の会員とならない事業者全ての意向や特性を安対基準に反映することは容易ではなくなる。当然、FISC としましても会員にな

っていただけるよういろんな取り組みはするものの、全ての方が会員になることはなかなか難しい、ということでございます。

また、一方、そうしたFISCの会員とならない方々が独自に安全対策の自主基準を策定されるということも考えられる。そうしますと、そうした自主基準が安対基準と何ら関係なく策定されてしまいますと、同じ金融関連サービスであるにもかかわらず、異なるルールが適用される、ダブルスタンダードの状態になってしまう。そうした問題をFISCとしてどうやって解決に向けた役割を果たしていくかということでございます。例えば、ということで、金融関連サービスの提供に携わる事業者の業界団体において独自の自主基準が検討されていれば、我々もその検討に参画して、社会的に合意されたルール形成に向けて必要となる支援を行おう、ということです。その結果として基準相互の整合性が確保されるよう努めていこう、そういう取り組みをすべきである、ということを今回言っております。

脚注７でございますが、そうした取り組みの１つとして先ほど瀧委員の事後意見でいただきました、全銀協様が事務局としてやられている各種取り組みに委員として参加させていただいているとともに、そこで提言されていますAPI接続先チェックリストの制定に関して、FISCとしても事務局として役割を担っていこうとしております。詳細は後ほどの議事でご説明します。

あるいは、この場の委員としてマクダッド様を推薦いただいたFinTech協会とも連携して、協会で取り組まれている自主基準策定にご支援させていただいているところです。そうした既にやっている取り組みをさらに拡張していこうということでございます。それはある意味で決意表明ではあるんですが、どういうやり方で自主基準相互の整合性を確保していくのかというところが、非常に難しい問題としてあります。そこについては、ここで１つやり方といいますか、整合性確保の手段をご提案しております。

外部委託の有識者検討会のときに、従来の安対基準はどちらかといいますとアッパーリミットを提言するだけにとどまっていたがゆえに、そのアッパーリミットに引きずられて過度な安全対策が取られてしまう。そうした現状を踏まえて、ローワーリミットとして必要最低限の安対基準というのを新たにご提供することによって、基準相互の相対的な関係というのが会員の皆様にご理解、ご認識いただけて、リスクベースアプローチの中でうまく利用していただけるのではないか、ということをご提言させていただいています。

今回我々の考えておりますのは、そうしたローワーリミットとしての「必要最低限の安対基準」というのは、違う観点で考えますと、金融関連サービスを担う情報システムにお

いてはある意味最低限実施されておくべき基準として考えられますので、そうした必要最低限の安対基準というのを、FISC 会員の内部的な利用だけにとどめるのではなく、この金融関連サービスに携わる事業者皆様に幅広くご提供してご理解を深めていただくような、そうした取り組みを通じて、自主基準、ルール相互がダブルスタンダードにならず、かつ整合的に安全対策に取り組んでいただけるような環境がつくれるのではないか、と考えております。そうした趣旨で今回修正を加えさせていただいたのが、１点でございます。

引き続きご説明させていただきますが、続いて参考資料２でございます。これは第１回の論点メモまでさかのぼっておりまして、修正のポイントは６ページです。資料はたくさんついていますが、修正したのは６ページの１枚だけでございます。これは簡単に趣旨だけご説明させていただきますと、従来金融機関が必ずしも主導的とはならない類型において、金融機関は部分的責任を果たすということを言ってまいりました。その部分的責任を果たすべき理由といいますか、要因としては、金融機関が FinTech 企業に顧客に関するデータを提供するところに由来すると言ってまいりました。そこの部分だけを言ってきたのですが、例えば FinTech 企業のほうから、金融機関が保有する顧客に関するデータの更新を行うためのデータを受領するというデータの流れもあるであろうと。つまり、金融機関から FinTech 企業に向かうデータの流れの一方向だけでなくて、顧客の意向を受けて FinTech 企業から金融機関に渡るデータ、その受領の部分も金融機関に責任が生じるとして付加すべきではないかということです。これは我々事務局のほうで考えまして、今回修正を行っています。

あと瀧委員の事後意見のご指摘については、６ページ脚注 11、英国の OBS に関する言及の流れの中で追加をさせていただいたきました。参考資料２は以上です。

参考資料３でございます。こちらにつきましては、前回席上でのご意見を踏まえて何点か修正をしています。まず７ページをご覧いただければと思います。ここは事務局側で誤解が生じるのではないかということで直したところではあるのですが、従来タイプⅠ、外部委託に該当する場合の議論の流れの中から、再配分ルールというものを７ページの下の枠囲いの中でご提言しております。これについて、脚注の８を修正しておりまして、もともとの論点の出発点はタイプⅠではあるのですが、結果的にこういう再配分ルールの考え方というのは、タイプⅠ以外の類型においても妥当なものではないかと考えておりまして、タイプⅠだけのルールであると誤解が生じないように、脚注の修正をしているということでございます。

続きまして、８ページでございます。前回、我々としては、内容について抽象度を比較的高くしました、というご説明をさし上げる中で、席上で委員から、やはりどこまでの統制を講じるのかというところがやや曖昧ではないかというご指摘をいただいておりました。そこで修正しておりますのは、８ページ真ん中のところで、そもそも前回「外部委託を準用する」というふうに言っている、その準用の中身の解説を加えております。準用というのは何であるかということなのですが、まず外部委託の基準には統制の方法と統制の内容の２種類があるだろうということで、統制の方法といっておりますのは、ここに書いてあります管理フェーズにおける客観的評価・モニタリングの実施等のことを意味しております。

そうした統制の方法というのは、部分責任だから統制の方法も部分的になるということは余り合理的ではないと思っておりまして、少なくとも統制の方法については、責任が部分的であろうと同じように適用されるべきだろう、ということが１つです。一方、統制の内容については、個々の部分責任の由来するところとの関連性が深いところでございますので、その部分についてはまさに部分的に反映することを意味するということでして、そういう意味で「準用」という言葉を使っている、ということをここに書かせていただいております。

あと９ページにつきましては、今お話しした内容を踏まえまして、先ほどの論点メモの修正で加えました、FinTech 企業から金融機関が受け取るデータに関連する問題、これについては本質的にはFinTech 企業から受け取るデータが本当に顧客から生じたものであるかということを、FinTech 企業がいかに適切に確認しているかというところに金融機関の関心が集中するということで、「本人確認」を追加させていただいています。

それ以外、もう１つ席上で前回ご指摘いただいたことがあります。再配分ルールということはわかるのだけれども、必ずしもうまく機能しないのではないか。やはり会社の規模や実力でFinTech 企業が金融機関から責務を押しつけられるような、そういう関係性が起こり得るのではないかというようなご指摘をいただきました。これはなかなか難しい問題であるかと思っておりますが、１つの考え方として 10 ページのところに今回追加させていただいています。やはりそうした相互がどのような責務を果たすべきかというのは、それぞれがどのような統制能力を持つかというところを踏まえて、いかに３者が協調して、安全対策を実施するかということが非常に重要ではないかと、10 ページですが、前回ご提案させていただきました。そういう意味では、その協調を行うに当たっては、そこの入口と

なるところでいかに３者が相互に情報を提供し合いながら検討を深めていくか、役割を整理していくかというところが重要で、ここの入口のところに焦点を当てるのが非常に皆様にとって有意義ではないかと考えました。

では具体的にどういうことなのだということで、下線のところを今回追加させていただいております。「また、協調を実現する手段として外部委託先評価時に使用されるチェックリストを活用することが望ましい」ということで、これは皆様よくご承知のとおり、もともと従来の安対基準においては、脚注９ですが、外部委託の利用検討時に客観的評価をすること、と言ってまいりまして、実際金融機関においては昔から、システムリスクだけでなく、それを含む外部委託全般に係るリスクを評価する汎用的なチェックリストをご用意されている。それを委託先に渡されて検証といいますか、適格性審査の道具として使われてきた。これをもう少し協調が促されるようなそういうものとしてご活用されるようなことを何らか提言するのがよろしいのではないかということです。例えばですが、従来使用しているチェックリストを協調を促すための情報共有手段として位置づけて、簡素化も含めて改めて内容を金融機関の皆様が見直されて取り組まれるということはいかがかと。そうした関係者の協調あるいは責務の配分を検討される入口のところで、問題に対処するのが非常に重要なのではないか。そのチェックリストのあり方に着目することが重要ではないか。と考え、今回修正を加えさせていただいております。私からは以上です。

○岩原座長　どうもありがとうございました。ただいまのご説明に対してご質問、ご意見ございませんでしょうか。

○渕崎座長代理　今ご説明していただいた資料の参考資料３のまさに最後のところで、外部委託先評価のときのチェックリストの話が出てきておりますけれども、私自身もこういう方向で考えたらいいんじゃないかというふうに思っておりまして、この会の前の外部委託先検討会のときにも申し上げたんですけれども、発注元の金融機関から外部委託する際のチェックリストというのは大変細かくて大部なものになっておりまして、受託先とか再受託先だけでなくて委託するもとのほうの会社、金融機関にとっても大変な負担になっているというふうな話を聞いております。もともと当時の金融検査マニュアルを受けて、外部委託先管理のための実務用のチェックリストということで、2003 年平成 15 年にスタートしたというふうに聞いているんですが、その後の個人情報保護法の施行とか情報漏洩

のいろいろな不祥事があるたびにどんどん分厚く細かくなってきておりまして、大手の金融機関だと 3000 社とか 4000 社ある先にこういった何百項目にわたるチェックリストをやってもらっているということで大変な労力を使っているわけです。

今回、FISC でもリスクベースアプローチということで、システムとか業務の重要度によって管理にメリハリをつけていこうという方向を打ち出しているということでもありますし、今回ここに書かれているような FinTech 企業との協調ということであれば、従来ベースの詳細なチェックリストということでは、FinTech 企業のほうも倒れてしまいかねないというふうに思いますので、これを機に簡素化の方向で見直したらどうかなというふうに思います。

○岩原座長　どうもありがとうございました。ただいまの渕崎さんからのご意見について何かご指摘はございますでしょうか。よろしいですか。それでは事務局のほうも、そのような方向で考えていただくということになりましょうか。

○藤永次長　はい。チェックリストの話につきましては、前回の外部委託検討会のときも、渕崎座長代理から同様のご指摘がありました。また、この検討会を準備する過程においても、多くの皆様からチェックリストに関する多岐にわたるお話を伺っております。したがいまして、今渕崎座長代理のご発言を踏まえまして、FISC としても何らかの取り組みができればというふうに思っております。そのひとつとして、この後話が出てまいりますが、FISC として全銀協が取りまとめられた内容を踏まえて、API のチェックリスト検討に関する事務局をやるということがありますので、まずはそうした取り組みを初めとして、ご意見を踏まえまして何らか対応を考えていきます。

○岩原座長　よろしゅうございましょうか。渕崎さんもそういうことで結構でしょうか。

○渕崎座長代理　はい。

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

２．【議事２】プレゼン「オープンAPIのあり方に関する全銀協の検討状況」（一般社団法人全国銀行協会 副調査役 服部様）

○岩原座長　続きまして、２つ目の議事は一般社団法人全国銀行協会　副調査役　服部様より「全銀協におけるオープンAPIへの取り組みについて」発表いただきます。服部様、よろしくお願いいたします。

○服部様　全国銀行協会、服部と申します。本日はこのようなご説明の機会をいただきましてまことにありがとうございます。

私からは配付資料にもありますとおり、昨年11月から進めております全銀協が事務局となって設置している「オープンAPIのあり方に関する検討会」、こちらの検討状況を含めて全銀協の取り組みについてご説明させていただきます。

表紙をおめくりください。１ページ目に本日ご説明する内容をお示ししております。最初に前置きとなりますが、“オープンAPI”とは何か、続きましてその意義をごく簡単に触れさせていただいた後に、全銀協としての取り組みをご説明させていただきます。

それでは、２ページに移らせていただきます。こちらは“オープンAPI”とは何か、についてでございます。本日お集まりの皆様はこの分野については詳しい方が多いかと存じますのでごく簡単にご説明させていただきます。オープンAPIそのものについては、銀行業に限らずさまざまな分野で活用されているテクノロジーではありますが、冒頭に記載させていただきましたとおり、「APIとは、あるアプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様等」を指しておりまして、このうちサードパーティからアクセス可能なAPIがオープンAPIと呼ばれております。つまり、簡単に申し上げますと、外部の事業者から銀行の保有する情報やシステムにアクセスする仕組みでございます。

図の右側にオープンAPIのOpenness、つまり開放度について幾つか類型をお示ししております。オープンAPIと一口に言ってもその開放度についてはさまざまな類型がございまして、アクセス権限を付与する相手が誰でもよいというケースはいわゆるPublic型と呼ばれるもの、それに一定条件を加えた類型が、その強弱に応じて、その下に幾つか並べさせていただいた類型になります。

おめくりいただきまして３ページにお進みください。APIではトークンといわれる許可

証によって中間的業者のアクセス権限をコントロールいたしますが、付与する権限の範囲によって、API は大きく参照・照会系、更新・実行系に大別されます。ここのページではご参考までに幾つか考え得る例を記載しておりますので、後ほどご覧いただければと思います。

それでは４ページにお進みください。こうしたオープン API に活用する意義についてでございます。記載にありますとおり、IT の進展が金融業のあり方を大きく変容させていくことが見込まれる中で、オープンイノベーションは今後の金融機関における基本的な戦略の１つと言われております。こうした中でオープン API はオープンイノベーションを実現していくためのキーテクノロジーの１つと位置づけられております。右の棒グラフをご覧ください。こちらは全世界で公開されている API の機能数の推移を示したものですが、2015 年時点では約 14,000 件、金融分野で見ると約 1,500 件の API が公開されている状況にあります。

５ページをご覧ください。日米欧の銀行業における主なオープン API の取り組み事例をまとめております。一つ一つの事例の紹介は割愛させていただきますが、我が国でも都市銀行さんに限らず地方銀行さんなどでも足許、オープン API を活用する事例が広がり始めている状況にございます。

６ページにお進みください。ここからは全銀協の取り組みについてご説明させていただきます。我が国でもオープン API に対する注目はここ数年急速に高まっておりまして、政府からも 2015 年 12 月の金融審議会“決済高度化ワーキンググループ報告書”、また 2016 年６月の“日本再興戦略 2016”においてそれぞれ官民連携したオープン API のあり方について検討する必要性について言及されております。

これを受けて全国銀行協会では昨年 10 月 21 日、「オープン API のあり方に関する検討会」を設置し、本日までに計６回の会合を開催させていただいております。

７ページにはその検討会の目的とメンバーをまとめております。本検討会の目的は目的欄の３つ目の「●」にありますとおり、「我が国の金融サービスの高度化、利用者利便性等の向上を実現するためのオープン API 活用促進に向けた、官民連携のイニシアチブを取りまとめる」こととしております。オープン API という１つのテクノロジーをどう活用するかについては、本来的には各銀行が戦略的に判断して取り組むべきことではございますが、後ほど申し上げますとおり、オープン API にはセキュリティや利用者保護、技術仕様などさまざまな論点がありまして、また、さまざまな FinTech 事業者と複合的につながっ

ていくAPIエコシステムの世界を理想とすれば、オープンAPIの活用促進、円滑化に向けて連携して取り組んでいくことも必要ではないかという問題意識に基づくものです。

そうした観点から、FISCさんも含めてさまざまな有識者、または金融庁さん、日本銀行さんなどの関係当局にもご参加をお願いしております。

めくっていただいて８ページ目になります。この検討会における主な検討事項でございます。点線で囲っております「3.2セキュリティ原則」と「3.3の利用者保護原則」につきましては、オープンAPIを進めていく上で特に重要な論点となることから、昨年はこの論点を優先的に討議してまいりました。途中段階のものではありますが、その成果として本年１月20日に中間的な整理（案）としてお示ししたのが、本日お配りしている「オープンAPIにおけるセキュリティ対策及び利用者保護に関する基本的な考え方【中間的な整理（案）】」でございます。

９ページにお進みください。本日は詳細な説明は割愛させていただきますが、背景、基本的な考え方を示した上で、この中のギリシャ数字のⅢ番で、オープンAPIにおいて想定されるリスクについて洗い出しを行っております。なお、検討会ではこのリスクについて詳細に分析の上、討議を行っておりますが、対外的にお示しする際は悪用リスクなどにも鑑みまして抽象化しておりますので、その点ご容赦いただけると幸いです。

その上で９ページ右側では、それらリスクに対応する形でセキュリティ原則、そして利用者保護原則を論点ごとに整理しております。

次の10ページ、11ページにそれぞれのエッセンスをまとめております。まず10ページをご覧ください。少しわかりづらいのですが、本日恐らくFISC事務局さんからご説明のあるAPI接続先チェックリストと申しますのは、こちらの真ん中の枠、API接続先のセキュリティ対策の適格性、こちらをチェックするためのチェックリストでございます。具体的には先ほどご説明させていただいた基本的な考え方（参考資料４）の６ページをご覧ください。チェックリストについては６ページ目の３つ目のパラグラフにおいて記載しております。読み上げさせていただきますと、「複数の銀行とAPI接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行がAPI接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API接続先チェックリスト」（仮称）を制定することが期待される」と記載しております。なお、この点については、金融審金融制度ワーキング報告書でも同様の要請があるところではございます。

若干補足させていただきますと、銀行はAPIを接続する際に、通常外部委託先管理などに準じまして、API接続先となる企業の適格性などをチェックいたします。例えばセキュリティ対策などが十分に行われているかどうか、といったような点でございます。他方、検討会の過程で幾つかのFinTech企業さんにお伺いしたところ、複数の銀行と接続するFinTech企業ではそうしたチェックリストへの回答に負担がある一方、各銀行のチェック事項というのは似通っている部分があり、セキュリティ目線がばらつかないようにするためには、ある程度提携的なひな型を定めたほうが、効率的かつ効果的ではないかというご意見をいただきました。そうしたことから多くの金融機関はオープンAPIの取り組みを健全に進めていけるよう、もし可能であればFISCさんにおいてこうしたチェックリストを策定できないかということをご相談させていただいた経緯でございます。

全国銀行協会といたしましては、こういう経緯でもございますので、可能な限りチェックリストの制定に貢献していく所存であり、FISCさんに新たに設置されるワーキンググループにも、会長行である三井住友銀行さんを初めとして、みずほ銀行さん、三菱東京ＵＦＪ銀行さんにもご参加をお願いしております。簡単ではございますが、ご説明は以上となります。ありがとうございました。

○岩原座長　どうもありがとうございました。ただいまのご発表に対してご質問ございませんでしょうか。よろしいですか。

特にご質問がないようでございます。服部様、どうもありがとうございました。

３．【議事３】API接続先チェックリスト（仮称）ワーキンググループの設置

○岩原座長　続きまして、３つ目の議事は論点メモ議事３のご説明でございます。FISCの小林部長、お願いいたします。

○小林部長　それでは、議事３の説明をさせていただきます。お手元の資料議事３「API接続先チェックリスト（仮称）ワーキンググループの設置」をご覧ください。

当検討会では第１回の会合において、先ほどの全銀協のオープンAPI検討会における議論を参考としつつ検討を行うこととしています。先ほど全銀協で取りまとめいただいているセキュリティ原則において複数の銀行とAPI接続する企業等における審査対応負担を軽減することを目的として、API接続先チェックリストの制定が期待されるとございましたが、FISCが策定のための事務局となることを検討しています。これは本検討会においてタイプⅢにおいて議論していることを踏まえて検討を行う予定にしていますが、その目的、メンバー、また当検討会との関連等について、大澤主任研究員よりご説明させていただきます。

○大澤主任研究員　それでは、事務局を努めさせていただく予定の大澤から簡単にご説明させていただきます。既に今お話を今いただきましたとおり、全銀協様のほうで取りまとめを行っていらっしゃる基本的な考え方において、チェックリストの制定が期待されておりますので、それを受けてFISCのほうでは事務局となったり、このリストの原案の作成及び維持管理方法等まで、そういったものを検討するワーキンググループの運営を予定しております。

オープンAPIは本有識者検討会におけるタイプⅢの実現形態の１つといえますので、ワーキンググループの運営におきましてはこちらで議論いただいておりますタイプⅢのサブルール等、そういったポイントを踏まえて検討を進めさせていただくべきだと考えております。したがいまして、私どもといたしましてはワーキンググループにおける議論が適切に行われているか。そういったものを本有識者検討会の皆様にその都度検証していただく必要性があると考えております。また、最終的につくりました成果物に関しましても同様に本有識者検討会に上程させていただいて検証いただきたいというふうに考えております。

それでは、まず１番目、委員ということで次のページにメンバー、委員をお願いする予定の方々を載せておりますので、そちらをご覧ください。まず初めに前提としまして、今回、チェックリストを作成するのが短期間であるというふうになりますので、委員の方にはオープンAPIに精通した実務家の方にぜひお願いしたいと考えております。それから、比較的少人数で自由闊達な議論を行いまして、ワーキンググループの運営を着実に前に進めたいというふうに考えております。区分ごとに分かれておりますが、銀行の３名の方に関しては先ほど服部様のほうからもお話がありましたが、全銀協様のほうにご相談して調整していただきました。FinTech企業の部分に書いてある３名の方々に関しましては、FinTech協会の方々にご相談してご調整いただきました。ITベンダーのところに関しては、総合的な面で考え調整させていただいた結果となっております。あとFISCからは安対基準を主管しております監査安全部より１名、委員として参加させていただきたいと考えています。オブザーバーに関しては記載のとおり金融庁、日銀の３名の方にお願いさせていただきました。

表面に戻っていただきまして運営の方法です。運営の方法としましては既に出ております全銀協様のセキュリティ原則を踏まえて議論は行うこと。それから先ほど述べましたとおり、チェックリストを作成すること及び維持管理方法まで検討するというふうに考えております。

あと２つ、検討状況に関しましては先ほど申し上げたとおり、この場に都度報告させていただき皆様方に検証していただく。成果物に関しても同様でございます。

３番、開催予定ですが、２月上旬から６月末の５カ月間、予定している委員の方の日程調整の結果、来週火曜日10時からということで調整が済んでおります。

開催の頻度は現時点では各週開催を想定しておりますが、検討状況に応じて最終的には決定しようと思っておりますが、お尻は６月末と、これは確実に守りたいと思っております。簡単ですが、ワーキンググループの設置についてご説明させていただきました。以上です。

○岩原座長　どうもありがとうございました。ただいまのご説明に対してご質問、ご意見ございませんでしょうか。

○轟木委員　API接続先チェックリストの作成する方向性というか、もし決まっている

ことがあれば教えていただきたいんですけれども、先ほど全銀協の方からお話があったとおり、API は大きく２つありまして参照系・照会系 API と更新系・実行系 API。参照系というのは単に残高照会とかマネーフォワードさんのサービスとか、実際ある情報をとってくるようなサービスが参照系だと思うんですけれども、更新系というのは実際に送金をするとか、ただ情報をとってくるだけではなく実際勘定系システムを動かし、実際実行を伴うもので、それぞれ考え方からするとリスクが異なるのかなと思うんですけれども、接続先チェックリストをつくる上で、参照系 API をやる場合のチェックリストをそれぞれ別につくるのか。更新系と参照系は別なのか。それとも更新系をつくった上で、それを落とした、それより緩いリスクのない形で参照系を整理するのかとか、何か今決まっている考え方とかあれば、何か教えていただきたいと思っています。

○大澤主任研究員　ありがとうございました。参照系と更新系をどのように議論して分けるか、分けないかということに関しましては、今はまだ事務局としましては特に決定したり案を持っているわけではございません。今回お集まりいただく委員の方々にもその辺を含めていろいろご意見を伺いながら最終的にどうなるかというところかと思っております。以上です。

○岩原座長　よろしいですか。ほかに何か。

○長委員　先ほど全銀協さんのお話で最終的にはエコシステムを形成するということであるのであれば、金融業界全体で取り組むべき話であって、こちら銀行さんだけでいいんでしょうかというところが非常に気になっております。保険会社さん、証券会社さん、あるいはクレジットカードの皆さんにも視点を供給していただく必要がないのかというところが気になっているんですが、いかがでしょうか。

○小林部長　今銀行で先にいろいろと取り組みが進んでいるところがありますけれども、最終的なエコシステムという意味では、おっしゃるとおりに金融の中でも証券、保険、またそのほかの業態にも進んでいくということが考えられます。まず今回は、全銀協で取りまとめいただいたセキュリティ原則に基づき銀行が API で使用するチェックリストからスタートするのですけれども、これが将来ほかの業界にもつながっていくという意識は常

に持ちながら、検討を進めていきたいと考えています。

○岩原座長　よろしいですか。ほかに何かございますか。

○梅谷委員　質問です。チェックリストをつくられるということでクラウドベンダーの立場からは、どの程度クラウドベンダーや、インフラベンダーに関わるチェックリストの項目が入ってくるのかという点が気になるところです。例えば議事２の参考資料１の 11 ページの下段に青字で、API 接続先における内部不正対策ということで、一部インフラに関連する要求事項が記述されています。安全対策基準の中のインフラに関わる要求事項とこのチェックリストのインフラに関わる要求事項の関連性といいますか、お互いにどの程度影響があるのか、という点について少し教えていただければと思います。議事４に関連して、クラウドの議論が今日あるかと思いますが、その中で関連してくるのかなというところも鑑み、関連性を教えていただければと思います。

○藤永次長　当然今回クラウドをこの後、取り上げるというのも昨今の状況、オープン API の状況も含めてですが、それらを踏まえましてあらかじめクラウドについて整理が必要ではという観点からも、後ほどご説明させていただこうと思っています。そういう意味では、今後安対基準の改訂も検討されていますので、これからの議論あるいは将来に向けた方向性も踏まえて、いろんなことが同時に進んでいる中ではなりますが、API のチェックリストの検討も行うべきであると思っています。当然そのために、FISC が事務局をやるわけですが。
こうした　相互にいろんな検討、要素が絡み合っていますが、それらの結節点といいますか、全体の整合的なところを FISC として担いつつ、いろんなところに関係しながら並行して進めさせていただいているという状況でございます。

○梅谷委員　ありがとうございます。

○岩原座長　よろしいですか。ほかに何かご質問。特にないようでございましたら、先に進めさせていただきたいと思います。小林部長、大澤主任研究員、どうもありがとうございました。

４．論点メモ　「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」

○岩原座長　４つ目の議事は論点メモ、議事４のご説明でございます。FISC の藤永次長、お願いいたします。

○藤永次長　はい。ではお手元に左上に議事４とされた資料をご用意ください。前回の有識者検討会の際にも前提という章のところでご説明させていただきましたが、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な検討が FinTech の検討の中でも必要ではないかということで、今回具体的な論点をご用意させていただいております。論点としましては、FinTech 業務をはじめとして、重要な情報システムでクラウドサービスが利用される場合を想定して、従来のクラウドサービス利用時のリスク管理策に対して、どのような補足を行うことが必要となるか、という点でございます。

きょうご用意させていただいています原案の構成としては、１番目に、まず前提となる検討の観点ということで２つほど用意しています。なぜそういう検討を行うことが必要であるのかということと、この後、クラウドサービス固有の性質を特定しようとしていまして、それはなぜ特定する必要があるのかというところをご説明しようと思っています。また、前回のクラウド基準策定後、海外のガイドラインの策定状況のアップデートもしようと思っております。

２番目がクラウドサービス固有の性質ということで、本日のメインのご説明、ご確認いただきたい内容がこれになります。そもそもクラウドサービスにおいて安全対策上、特定しておくべき性質が何であるか、ということをこれまでの検討、議論を踏まえまして用意しております。そのうえで、どういう補足的な検討が必要であるかという対象を特定しています。

３番目にそうした作業を踏まえまして、個々のリスク管理策として、例えばこのような管理策をクラウド基準、従来の検討に補足してはどうか、ということで、ご提案を用意している、という構成になっております。

１ページめくっていただきまして別紙１ということでございます。補足的な検討の観点としまして、まず、ご存じの方が大半でいらっしゃると思いますが、FISC においては金融機関におけるクラウド利用に関する有識者検討会というのを、この２つ前の有識者検討会でやっております。それを踏まえて一昨年、安全対策基準の第８版追補改訂というのが、

策定されたところでございます。

こうして、前回クラウド検討会を開催してから３年たっている中で、どういう環境変化が起きているかということで、国内と海外についてご説明を書いております。まず国内ですが、クラウド基準策定後、金融機関におけるクラウド利用が進むということと、金融機関の FinTech への取り組みも急速に活発化している。かつ、FinTech においてはクラウドサービスが利用される場合が非常に多いのではないか、というふうに考えております。そうしますと金融情報システムにおいてクラウドサービスの利用がますます進展していくという環境にあるのではないか、と考えております。

クラウド利用の進展の状況としましては脚注１ですが、前回有識者検討会をやる段では 26.6%が利用されていたのが今や 36.5%。利用の検討まで含めると半数近くになっておりまして、FinTech に取り組まれる中では結果的に更にもっと増えていくのではないかと思っております。その一方で環境変化のもう１つとしまして、外部委託の検討会を行いました。もともとクラウド検討会のときにリスクベースアプローチというのを最初にご提言いただいたのですが、それを外部委託の検討会でさらに深い議論を行っていただきまして、その結果重要な情報システムという定義が明確になっています。クラウドのときはコア、セミコア､ノンコアということでリスクベースの考え方を提言させていただいたのですが、それをまさに深めた議論をしているということでございます。

そうした中、今後、FinTech のユースケースとして、ブロックチェーン、ＡＩなどを通じて重要な情報システムが結果としてクラウドによって担われることが想定されますので、あらかじめ整理しておくことが有益ではないか、ということです。

脚注２ですが、今後の安対の改訂を踏まえた内部的な事情の側面はありますが、外部委託の検討会のときにクラウド基準の中では外部委託全般に適用可能なものも含まれているだろうということで、それを外部委託全般に適用可能なものとクラウド固有のものに峻別する必要がある、という提言をいただいています。今後その作業を安対基準の改訂を行う中においては、クラウド固有の性質を特定しておくことが必要ではないか、ということでございます。以上が国内の変化です。

一方、海外の動向ですが、クラウド検討会の前後で日本と同じように海外先進諸国においてクラウドサービスのガイドラインが策定されています。特に去年、英国とシンガポールでクラウドに関するガイドラインがアップデートされており、そのポイントをご紹介しています。全般的にはリスクベースアプローチの採用、あるいはクラウドというものの定

義を明確にしない点、あるいは類型別にリスク管理策を整理しないほうがむしろ適切ではないかという点等、国内のガイドラインと共通する点が多いというのが第１印象ですが、特に特徴的な点として以下の２点を言及させていただいております。

１点目が、外部委託された業務に関連するデータに実効的なアクセスが可能となるということが要求されています。我が国のクラウド基準の中でもデータへのアクセスについては言及されていますが､英国のガイドラインの中でデータに関して解説がついていまして、金融機関のデータにとどまらず、顧客のデータ、取引データ、さらにはシステムや手続きに関するデータも含まれる、と。この手続きに関するデータというのは、要員の身元の調査手続きやシステム監査証跡など幅広く解される、ということで定義されています。また、そうした考え方に基づいてアクセスの対象となる事業拠点に関して、本社や事務センターを含み幅広く解されるというふうにされている一方で、必ずしもデータセンターへのアクセスが必要とならない場合もあり得るということが書かれています。

また、管轄権についてはデータアクセスの実効性を高める観点から、国内法の管轄下にあることを事実上デファクトとされているということで、これらの認識がなぜそうなのかという説明として、外部委託では一般的に金融機関の統制の程度が低くなることを踏まえて、いわゆる統制上必要となるデータというのが何であって、それにアクセスするのはどこで、どのようにすればアクセスできるのかということに関して、明示的な要求がされているということです。

もう１つの特徴としましては、要求事項を設定する目的を「金融機関が外部委託先を利用することに伴うオペレーショナルリスクを適切に特定し、管理するよう促すこと」にあるとしている上で、一般の外部委託あるいは自前でやる場合と比べてオペレーショナルリスクが増大することがないように、リスク低減策を打つという考え方、そういうある一定のベンチマークをもとにしてリスクコントロールをしていくとしています。我々の言葉でいうと安全対策の効果を同等に維持していくという、前回お話しした同等性の原則と同じような考え方です。そうした観点から、設備や技術の統制に関する言及は、ガイドライン自体にはほとんど無く、他の関連ルールをリファレンスしている。そういう作り方がされています。これはまさに統制水準を同一に維持することが重要であって、それに対する手段というのは、ある意味、一義的には金融機関にゆだねられるものであるというふうにされているのではないか。あくまでも金融機関のリスク評価、リスク管理の取り組みを促していくのがガイドラインの目的である、ということでございます。

そうしたところをまず確認した上で、今回「クラウドサービス固有の性質」をご用意させていただいています。前回のクラウド検討会では、クラウドサービスは外部委託の一形態として扱うことが適当だとされました。利用なのか、委託なのか、ということで活発な議論がされましたが、最終的には、言葉云々というよりもやはり金融業務を、金融機関以外の方が担われるという観点においては、委託という扱いで安全対策上整理させていただいているということです。そうしたことを踏まえまして、外部委託に関連するシステム資源の調達の歴史といいますか、そこからクラウドを読み解いては、ということで書いております。

システム資源の調達とは、安対基準が策定された当初はどのようにされていたか、といいますと、今のように調達形態は多様ではなくて、例えば建物、電源、空調、当時は水冷設備というのもございましたが、そうした一式とか業務アプリケーションの開発や情報システムの運用要員等は基本的に金融機関が自前で用意するのが一般的でした。外部から調達するのは、せいぜいホストコンピューター等のハードウエアやオペレーティングシステム等の基本ソフトウェアであったということでございます。要は金融機関が自前で調達するという前提でした。したがいまして脚注５ですが、安対基準においても外部委託に関する項目は、全 113 項目のうちわずか２項目であったというのが、もともとの出発点でございます。

その後、コスト削減や先進技術の利用を目的にアウトソーシングが進展して、外部委託の報告書でも確認されましたが、金融機関の 90%以上が今や基幹系のシステムを外部委託に依存しているということでございます。したがいまして、次のページですが、金融機関は統制の重点を内部から外部にシフトさせるという必要性が生じている。そうした中においても安全対策の効果は自前で調達する場合と同等に維持する必要があるということで、付加的な安全対策を実施することが必要となり、結果として安対基準においても外部委託の基準、あるいはクラウドの基準の策定が行われてきた。そういう歴史がございます。そうした議論の延長線上でクラウドがどのように理解されるか、ということが重要だろうと思っております。すなわち、システム資源の調達方法の歴史の中で、クラウドサービスは、従来の外部委託と比べて利用者のニーズに応じた柔軟な調達が可能である、という特徴があるのではないか、ということです。

この間いろいろなクラウドベンダーさんも含めてお話を聞かせていただいて書いているのが、脚注７です。詳細は書いてあるとおりなので読み上げませんが、費用の経済性、調

達の即時性、調達手続きの容易性、システム管理の効率性等書かせていただいております。あるいは安全対策の面ではセキュリティ投資額が大きいとか、分散配置されることで結果的にサービスの継続性が高いとか、これは何も我々が新しく言っているわけではなくて、従来からよく言われている特徴ではないか、と思います。

そうしたところもありまして、金融機関が今後多岐にわたるFinTechに取り組む中でもクラウドの利用は一層進展していくということで、やはりFinTechの議論をする中においてはクラウドの議論というのは避けられないといいますか、実際、FinTechのサービスの運用を担われるのはクラウド事業者であることが非常に多いのではないかということを考えると、クラウドに関する何らかの補足的な検討が必要ではないかということを、考えているところでございます。

次にそうしたことを踏まえて、ようやく、クラウドサービス固有の性質は何か、というところでありまして、安全対策上３つほど特徴があるのではないか、と整理させていただいております。１つは匿名の共同性です。クラウドサービスは複数の事業者が単一の事業者に委託するということで、共同性という性質を有する。従来、FISCが取り上げてきたものでいいますと共同センターなんかも共同性の性質を有する。ただ、一方、利用者間で何らコミュニケーションがないということで匿名の利用者である。すなわち、匿名の共同性を有するとしています。そういう利用形態によって何が起きているかといいますと、安全対策を決定する主な役割が本来は利用者側にあるはずであるものがクラウド事業者側に帰属するということで、その結果として前回のクラウド検討会でも確認されましたが、利用者からの個別の監査要求や個別の改善要望の実現に対して消極的となる傾向があるとともに、データセンターへの立入り、前回のクラウドの検討会では集中的に議論された点ですが、立入りがセキュリティ上の問題を惹起するという観点も指摘されています。

そうしたことから、金融機関による統制が十全に機能しない、リスク評価やリスク低減策を適切に実施できないという問題がもともと内在している利用形態ではないか、としています。ただ、リスクベースアプローチというのを前回外部委託検討会のときに提言いただいていまして、一般の情報システムにおいては、金融機関のリスクに応じて統制の程度を決定すればもう十分ですので､既に整理されている以上言及すべきことはないのですが、一方、重要な情報システムにおいては、インシデント発生時の社会的影響が甚大だということもありまして、やはりいかに従来行われてきた重要な情報システムの外部委託と同程度に、安全対策の効果をコントロールするか、ということが大きなポイントになると思っ

ています。そうした際に参考になるのが外部委託の検討会の報告書でも提言された、共同センターにおける統制水準が参考になるのではないかと思っております。したがいまして、この性質に関連する補足的な検討というのは、共同センターに適用されるリスク管理策を参考としながら、あとは匿名性という性質に伴う統制の低下をどのように補完していくか、ということで考えるのが適当ではないかと思っています。

次に情報処理の広域性という性質です。クラウドサービスでは利用者が広域に及ぶということで、情報処理拠点を含む事業拠点が複数の国にまたがり広域に及ぶという性質があります。一般的な外部委託ですと国内を中心としていたのに対して、クラウドのように広域に及んだ場合は、いざインシデント発生したときにその復旧や原因究明のために必要となるデータはどこに行けばアクセス可能か、ということに始まり、アクセス可能な所在地を知っておきたいという要望を持つことになります。これも前回クラウドの議論の中で意見として出ていたものでございます。そうした観点から再発防止策等が実効的に行われることを担保するためにデータアクセス可能な事業拠点に対する監査権を契約書に明記したり、事業拠点が国内の法令が及ぶところにあるほうが比較的アクセスが容易に可能なのではないか、ということで、管轄権に関する要望を持つこととなるのではないか、と思います。

これについても、一般の情報システムにおいては、先ほどお話ししたとおり、特に付加的な議論はないと思うのですが、重要な情報システムにおいては、やはりこうしたデータにアクセス可能な事業拠点という観点でもリスク管理策を検討することが必要となるのではないか。前回はデータの所在地を把握することは、何のためにそれを把握する必要があるのかということで、さまざまな議論がされていましたが、統制上必要なデータにアクセスするという観点から、前回の議論を踏まえまして、より明確な検討が必要ではないかということでございます。

３番目に技術の先進性という性質です。クラウドサービスでは仮想化技術、あるいはデータの秘匿性を高める技術などソフトウェアにおいて技術の進展が非常に著しいという特徴があります。それによってどういうことが起きるかということなのですが、設備やハードウエアといった物理的な安全対策による効果がソフトウェア技術によっても同程度に達成可能となる場合があるのではないか、あるいはソフトウェア技術自体も、どんどん日進月歩で旧来の技術をたちまち塗り変えるような技術が登場するのではないか。これによってどういうことが起きるかといいますと、FISC の安対基準の設備基準あるいは技術基準と

いった技術的な安全対策をあらかじめ一意に特定しておくことが、必ずしもクラウドのような先進的な技術が使われる場合には、適切ではないことが起きるのではないかということでございます。

従来の安対基準ではそうした基準相互間の取扱いの考え方が明確にされていないということもありまして、先ほどのチェックリストの話ともつながってくるんですが、客観的評価のときの評価事項としてチェックリストの中に、FISC の安対基準や設備基準や技術基準をそのまま字義どおりに盛り込まれるということが起き得るのではないか。それによって過度な安全対策を招来するようなことが起きてはいないか、ということでございます。

一方、採用技術が先進的であるがゆえに、監査がどのように実効的にしうるか、ということで、監査人はあらかじめクラウドサービスの採用技術の詳細について十分に知悉しておく必要がある、という一方で、金融機関が内部に保有する IT 要員やシステム監査要員は限られているということで、いかに実効的な監査を行うかという問題があります。一般の情報システムにおいては、ある意味、今お話しした安対基準の取扱いが明確化されれば、あとはもうリスクベースアプローチで対応するということになると思っておりますが、ただ、重要な情報システムにおいて監査を行うということは、ある意味大きな前提ではないかということでございます。そうしたときに監査の実効性を確保するということが非常に重要な問題になってくる。前回立入り監査、モニタリングについては、さまざまな議論がクラウドの検討会でも行われてきたものの、リスクベースアプローチを踏まえて監査権を明記することが重要なシステムにおいては必要だとか、そうしたところまでは必ずしも基準の中に盛り込まれておりませんので、リスク管理策の明確化を行うということが今回必要ではないかと考えております。

そこまでのところが、今回なぜこうした論点メモを出しているか、というご説明でございます。

続いて３番のリスク管理策に関する補足というところは、以上の認識を踏まえまして、こうした管理策が考えられるのではないか、というご提案になっています。ですので、語尾は疑問形にしているということです。

１つが客観的評価を実施する際の留意事項ということで、クラウド基準では客観的評価を実施し行うことが必要であると書かれていますが、そこに、「これは客観的評価を実施する際の評価事項に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、ということに留意が必要である」と積極的に書くことによって、基準が字義どおりに使わ

れることがないようにできないか、ということが１点目でございます。

２点目がデータアクセス拠点の把握ということで、これは重要な情報システムの場合ということですが、統制上必要となるデータへのアクセスが可能となる情報処理拠点など、そうした事業拠点について把握しておくこと、としてはどうかということでございます。統制上必要となるデータというのが何であって、事業拠点というのが具体的に何であるべきか、ということについてはさまざまなご意見、あるいはご理解があるとは思っておりますが、きょうは一旦こういう形で出させていただいたうえで、皆様のご意見をいただきたいということでございます。

統制を実効的に担保するためには統制対象のクラウド拠点というのは、原則としてやはり国内に所在することとしてはどうかと思っています。万一それが不可能な場合もあるとは思いますので、やはり何のためにそれを要求するのか、という目的適合的な観点から、例外の場合においては、金融機関が必要なデータに実効的にアクセスできる手段を手当てすることが必要ではないか、ということでございます。

３番目は監査権の明記ということで、今のクラウド基準では必ずしも重要な情報システムに関する言及が明確にはされていませんので、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、監査権を明記すること、としてはどうかと思っております。

４番目は監査の実施ということで、監査に当たっては、クラウド事業者が自ら監査人に委託して行った保証型監査の報告書を利用することが望ましい、としてはどうかということでございます。これはクラウド基準の中では、そういう保証型監査の報告書を利用することは可能である、というような基準になっているんですが、むしろ今の状況ですと、それを望ましい、と踏み込んで安対基準の中に盛り込んだほうがいいのではないか、というご提案です。さらにその統制が十全かつ実効的に機能するよう安対基準と整合的に検証が行われている報告書を利用することが望ましい、としてはどうかということでございます。これはやや説明が舌足らずではありますが、もともとクラウド基準がつくられた後にシステム監査指針の改訂がクラウドの安対基準の改訂に伴って行われておりまして、その中でこのような考え方がポイントとして示されております。そういう意味では監査指針の中に盛り込まれている視点というのを、安対基準の中にぐるっと回ってもう一度取り込んではということでございます。

５番目に監査人等モニタリング人材の配置ということで、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、これは経営層の IT ガバナンスに関してですが、クラウドサー

ビスの採用技術が先進的であることをまず認識していただきたいということと、クラウド事業者に対するモニタリングを実効的に実施するための人材を配置する、ということを経営者の責任として言及してはというご提案でございます。そうした人材を育成することが容易でない場合は、専門性を有する第三者監査人等を利用することがこれも望ましいということで、従来のクラウド基準よりはやや踏み込んだ形で、安対基準の中にリスク管理策として提言を行っては、ということで考えております。

その後、参考というところで、昨今のクラウドの利用状況をFISCのアンケート結果を踏まえて添付させていただいておりますので、これはご参考です。早口ではございましたが、私の説明は以上です。

○岩原座長　どうもありがとうございました。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。

○荻生委員　クラウドサービス利用時のリスク管理策の資料の全体的なトーンはパブリッククラウドを指しているように思えましたが、一方、参考のページに記載しているグラフは、プライベートクラウドが実際には多いのではないかと思っていますが、いかがでしょうか。

○藤永次長　FISCのアンケート上は分けてとっておりますが、本日はパブリッククラウド、コミュニティクラウド含めて合算数字を記載しております。もともと平成25年度のときは26.6%のうち16%程度がパブリッククラウドということでしたが、内訳については次回ご用意させていただきます。

○岩原座長　よろしいですか。ほかにご質問、ご意見ございますか。

○安冨委員　最後、７ページのところでリスク管理策に関する補足（１）で客観的評価を実施する際の留意事項として、従前の安対基準の設備基準と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、とお書きいただいているんですけれども、クラウド基準の評価の際に従前の安対基準にこういう意味での留保をつけるというのは、若干意図するところがわかりにくいかなという気もしたので、もう少しご説明をいただけるとあり

がたいと思います。

意見としては、明らかに性質が違うものをここまで明確に留意が必要である、というように強い口調での文言といいますか、そこまでリスク管理策に関する補足として求められるべき内容なのかというのは若干疑問に思います。

○藤永次長　なぜこのようなことをご提案しているかという出発点は先ほどお話ししたところにありまして、要はクラウドに対する客観的評価、これもまたチェックリストの話になるのですが、その中に設備基準をそのまま盛り込まれてクラウド事業に確認を求めているというようなことが、今実態としてどのくらい行われているかというところがあります。我々が聞いた中ではそういうことが行われている場合もある。これはぜひクラウド事業者の委員の方にもご意見をいただきたいと思っています。まずその事実認識の問題があります。

その上で、設備基準等がそのまま盛り込まれているとすると、もともと自前で金融機関がコンピュータセンターをつくる前提で策定された設備基準が、そのままクラウド事業者とのコミュニケーションに使われていますと､特に外資系のクラウド事業者側からすると、日本の基準の固有性といいますか、そういうところに関してご意見をいただくことがあるのではないか、ということでございます。

クラウド事業者と金融機関、今回の議論でいいますと、FinTech 企業も入ってこられるかと思いますが、そうした方々とのコミュニケーションをいかに円滑に進めていくかということが１つのポイントだと思っています。そうした観点では、もともと自前で金融機関がつくることを目的につくられた設備基準等をそのまま使われることは余り好ましくないということで、それをいかに円滑にコミュニケーションができて協調が進むようにできるか、というところが肝だと思っています。

その解決策として、今回リスク管理策としてご提案させていただきました。これが問題を解決できる手段であるかどうかということについては、ぜひほかの方法も含めてさまざまにご意見をいただきたいと思っております。ただ、こうした問題があるのかないのか。それが起きているのであれば、なぜそういうことが起きているのか。そうした点についてぜひこの場で委員の方からご意見をいただければと思っております。

○岩原座長　ただいまの藤永さんからのご指摘等についで何か。

○梅谷委員　今、藤永様からお話がありましたように、運用基準、設備基準に関するチェックリストがFinTech企業様に確認ということで回され、それがクラウドベンダーにそのまま流れてくる、そして、チェックリストの本来の目的、背景が不明確なまま、とにかくチェックリストを完成させていく、といった実務的な現状はございます。どの程度の割合で起きているのか、何件かというのは正確には申し上げられませんが、ほとんどの場合、そういった運用がなされているという認識です。FinTech企業様も、金融機関様のチェックリストのご担当の方もこうした現状に困難を感じている印象です。このような金融機関様、FinTech企業様、ベンダーと３者の立場で、それほど有益な議論がないまま、実務的な時間だけが過ぎるというふうな現状を、何とか別の手段、あるいはもう少し現実的な手段で解決すると、公益といいますか、皆様の便宜を図れるような実務が運べるのではないかというふうな意見を持っております。ありがとうございます。

○岩原座長　ほかにございますでしょうか。

○安冨委員　これまでの歴史経過を踏まえて、そして環境技術変化の中でクラウドが中心となってきたときの安対基準がどのように今後改訂されていくべきかという、そういう根本にかかわる問題が実はここにあるんだと思うんです。そういうところを、クラウド基準のところでは一歩引くというか、言葉は余り適切ではないかもしれませんが外すというか、そういう方法よりも、性格が違うんだということをもう少し明確に意識したような形でのご提案があったほうが、より一層チェックリストを作り，それを運用するときに有意に実効性を持つのではないかと思い、先ほどのような質問をさせていただいたということを意見の補足として申し上げさせていただきたいと思います。以上でございます。

○岩原座長　よろしゅうございましょうか。ほかに何かご質問等ございますか。

○梅谷委員　今議論がありましたように、クラウド特有の性質を踏まえた上で新しく基準をつくっていくというのは、皆様にとって有意義だと思います。その上で今の議事４、クラウドサービス固有の性質ということで藤永様のほうにいろいろご説明をいただきましたが、まず、１番の匿名の共同性という箇所についての質問です。ここに関しては匿名の

共同性という言葉について、個人的に印象が残りましたが、共同センターという概念が大前提として存在し、その上でクラウドサービスではどうか、という比較の考え方があるのかなという印象です。

そうしたときに、クラウド事業者から見て違和感があるポイントというのは、責任分界というクラウドサービスに特有の議論がここで抜けていることだと思います。あるいは、この匿名の共同性という概念の前提にもう一段、責任分界という視点があってもいいのかなという印象を持っています。例えば、文でいいますと、５ページ、匿名の共同性の上から４段目です。そのため以降です。安全対策を決定する主な役割は、という箇所で、その途中の文は抜かしますが、クラウド事業者にその責任が帰属することになりますという記述になっています。特に、アマゾンのサービスしか私個人は知りませんのでそこを意識してお話しさせていただきますが、お客様が統制を実現可能なサービスを提供するというのが、クラウドサービス事業者の責任として認識していまして日々努力しております。全体のシステムの統制という意味では、そういった我々クラウドサービスベンダーが提供する監査に使える機能であったり、セキュリティに使える機能であったり、あるいは暗号化といった具体的な機能を全て織り込んだ上で、お客様にとての全体のあるべき統制をとっていただくというような案内をしております。そういった意味では、クラウドベンダーにすべての統制の責任がある、というような書き方は違和感がある印象です。

今申し上げましたのは、議事１参考資料３のページ７の脚注の上部に四角囲みで補足が存在しますが、「金融機関、IT ベンダー及び FinTech 企業は３者の合意の上従来の安全対策基準における外部委託の責務と３者で再配分することが可能である」、という記述どおり、この議論を抜かしてクラウドベンダーはこうあるべき、あるいは金融機関はこうあるべき、あるいは FinTech 企業様はこうあるべきという議論をしていくと、先ほど問題点に挙がったような字義どおりのチェックリストによる運用に、再度帰結してしまうのではないかというふうな危惧がございます。ですから、この議論は少しテクニカルな議論も入りますので難しいと思いますが、例えば、アマゾンが提供していますインフラストラクチャーに近いようなクラウドサービスの場合は、若干金融機関様あるいは FinTech 企業様の責任範囲が少し増える、クラウドベンダーがアプリケーションのレイヤーまで、あるいは運用のレイヤーまで責任を持って提供するという場合には、もしかしたら金融機関様の統制の責任というのが減ってくるかもしれないという点を考慮する必要があります。世間一般的に言われています、いわゆる IaaS、SaaS、PaaS の分類に従って責任分界を補足する形

式でも構いませんし、アプリケーションのタイプ、それからデータのリスク分類という点など様々な考慮点はございますが、まずはクラウドサービスベンダーの立場としては、責任分界をクラウドサービスのタイプに従ってしてはどうかという補足を入れてはどうかという、僭越ながらご提案をさせていただきます。ありがとうございます。

○藤永次長　ご指摘のとおりだと思っています。前回のクラウド検討会のときにそうした責任分界ということの整理が特にクラウドにおいては非常に観点として重要だろうというご指摘をいただいて報告書も取りまとめられていますので、今回の論点で、先祖帰りするというか、立ち戻ることがないよう、正しくご理解いただけるように修正を加えたいと思います。

あともう１つ言いますと IaaS、SaaS、PaaS 等の分類というのは確かに一般的にはあるのですが、今後さまざまにクラウドサービスが出現して、FinTech の流れの中で重層的にいろんな事業者が登場してくるということを考えますと、必ずしも今ある類型に従って物事を整理することが適切ではないのではないか、というところもあります。そうした意味では、今ある類型ごとにリスク管理策を整理することまではやらないほうが良い、と思っていますので、そうした考え方も含めて正確に皆様にご理解いただけるように修正案を考えたいと思います。

○梅谷委員　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。特にございませんか。

○梅谷委員　ありがとうございます、もう１点、同じように議事４のクラウドの性質に関するお話ですが、６ページの３段目、技術の先進性という箇所についてです。「特にソフトウェアにおいて技術の進展が著しい」という記述は、ご指摘どおりという認識を私も持っております。恐らくほかのクラウドサービス・プロバイダーの方も同様のご認識ではないかと思われます。

その上で、例えば、新しいサービス、機能の提供によって今までできなかった監査が可能になるというふうな点を我々としては認識している点がございます。例えば、ベンダー固有のサービスになりますので、固有名称は省きますが、提供している各種サービスに関

して、誰が、どのように、何時何分に変更を行ったのかといった内容を取得できるログのサービスが存在します。これは監査の質を上げるという観点で貢献することになりますし、自動的にそのようなログを取得できるようになっています。例えば個人的な経験ですが、従来のハードウエア環境のように様々なベンダーの機器がありますと、ログのとり方も違いますし、そのフォーマットも違いますという中でどんな変更が起きたかというのを一元的に取得し、監査を実施するというのはなかなか難しいと思います。実施できなくはないけれども、なかなか難しい現状があるという認識です。しかし、クラウドサービス・プロバイダーのプラットホーム上で起きる変更、あるいは構成の何らかの変化に関しては一元的にログが取得可能な、そういったサービスが提供されますので、従来は実施が困難であった監査が実施できるようになる可能性があります。あるいは、そういった監査ログの解析というのは、なかなか人の手を介して実施することは難しいと思います。また、サンプリングによって、もしかしたら見逃していたところがあったかもしれません。現状では実現できていない点もありますが、機械的にログ取得し、それをビッグデータの基盤で解析することで、今まで実施できなかった、もしかしたら逸脱が発見できるかもしれないというような考え方もあります。従来と比較して、クラウドだからリスクがあるという視点とは別に、むしろクラウドだからこそ実施可能になることもあるという視点を、様々なクラウドサービス・プロバイダー様の意見を取り入れて、ぜひ技術の先進性というところに書いていただけますと、FinTech 企業様のみならず、金融機関様でも実効的かつ実務的な監査ができるのではないかというふうな意見を持っております。ありがとうございます。

○岩原座長　はい。ほかに何かございますか。

○マクダッド委員　FinTech 協会のマクダッドです。先ほど梅谷様のコメントについて補足、そしてFinTech 協会の要望についてちょっとコメントさせていただければと思うんですけれども。今後ワーキンググループの設置という、今日アナウンスがあったかと思うんですけれども、FinTech 協会の企業はクラウド利用率がとても高くて、従来の安対基準に基づいて該当するものを抽出して、そのままチェックリストにしましょう、というようなワーキンググループになってしまいますと、先ほど梅谷様がおっしゃったように、新しい技術の適用、チャンスを見逃してしまうということを皆心配しています。やはり最新の技術の進化によってよりセキュアにできるんじゃないかなと、私自身も思います。FinTech

協会としてはワーキンググループに、そおような期待をしています、ということをコメントさせていただければと思いました。以上です。

○岩原座長　ほかに何かご意見、ご質問。

○神田オブザーバー　金融庁の神田です。全体にかかわるコメントといいますか要望になります。本日は、API 接続先のチェックリストですとか、あるいはクラウドサービス利用時のリスク管理策についての補足的な検討ということで、非常に技術あるいはサービスの先進的な進展、あるいは拡大を眺めてタイムリーにスピード感を持った検討をしていただいており、しかもそれぞれの資料もこれまでの議論を踏まえつつ、新しい動きをしっかりと取り入れて、ロジカルに今後の対応の方向性についてきちんと示していただいているという意味で、FISC の事務局の皆さんの取り組みについては敬意を表するところです。

本日の議論を拝見していまして２つほど大事なポイントがあると思っています。１つはこうした議論が FISC さんの会員である金融機関の皆さん､あるいは関連するベンダーの皆さんだけではなく、やはりこれから新しい FinTech のサービスを担っていく会員以外の方々にも非常に大きな影響が及ぶ議論をここでしているというのが１点です。

もう１点は、これまでシステムのセキュリティに関して、枯れた技術を使って堅牢なシステムを構築するといった非常に保守的な対応がとられており、あるいはそういったことによって障害を起こさないということが重視される傾向があったと思いますが、ここで議論されていることは、セキュリティはきちんと確保しつつイノベーションを阻害しないことや、FinTech の事業者さんとのコミュニケーションをどうすれば円滑にしていけるのかといった、これまでとは違った、踏み込んだ形での議論が行われているというふうに考えています。

このように、会員の皆様だけにとどまらない、あるいはこれまでとは違った踏み込んだ議論がなされているという点は非常に大事なポイントだというふうに思っておりまして、外部の皆さんに対する非常に大事なメッセージを含んでいるのではないかというふうに考えております。そういう意味で、こちらは提案ですけれども、ここでの議論をできれば会員の皆さんだけでなくて一般の皆さんにも見えるような形で開示していくという方向性についてご検討いただければ、これから新しいビジネスに取り組んでいく FinTech の事業者さん、あるいはこれまでもセキュリティに取り組んでこられた金融機関のご担当の皆様に

も非常に大きなメッセージとして発信できるのではないかというふうに考えています。公表のあり方について少しご検討いただければという提案になります。

○岩原座長　はい、どうもありがとうございます。

○藤永次長　今いただいたご指摘は先ほどお話ししたFISCのこれからの役割ということを考えていきますと、当然結果的にそういう方向に帰着していくものであるというふうに、我々も考えております。

有識者検討会は、従来から慣習的に、最終的な報告書はホームページ上で公表して広くご利用いただいているのですが、それまでの議論のプロセスはFISCの会員限りで公表してきた、という実態があります。確かに今神田様が言われたとおりのことだと思っておりますので、今までの議論の議事録、そしてこれからの議論も含めて、会員限定とせず広く皆様に公開していくほうが有益ではないか、思っております。もし委員の皆様にご了解いただけましたら、そうした方向で事務局としてやらせていただければありがたいと思います。当然今まで公開した議事録は会員限りという前提で皆さんに発言等をレビューしていただいていたので、もう１回確認し直していただく必要があるとは思っています。ご異議なければ、基本的にそういう方向で、これから事務局周りの運営をさせていただければと思うのですが、いかがでしょうか。

○岩原座長　今のようなご提案がございましたが、皆様いかがでしょうか。

特にご異議はございませんか。それでは、ただいま藤永次長からございましたような公開に関する扱いとさせていただきたいと思います。よろしいでしょうか。

藤永次長どうもありがとうございました。ほかに何か。特にないようでございましたら、今後の事務連絡等について小林企画部長からお願いいたします。

５．事務連絡

○小林部長　皆さんどうもありがとうございます。２点、これまでと同じでございますが、まず１点目、本日の内容に関する事後のご意見等ございましたら、議事次第の５番に書いてありますけれども１週間後の２月９日木曜日夕方５時までに電子メールで事務局までいただけたらと思います。

２点目は第４回の検討会のご案内です。こちらも一番下に書いてありますけれども次回は、３月 23 日木曜日同じ時間３時 45 分から予定しておりますのでよろしくお願いします。

○岩原座長　よろしいでしょうか。小林企画部長どうもありがとうございました。

全体を通して何かご質問等ございますか。よろしいでしょうか。

それではこれにて、第３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。大変熱心なご議論をいただきましてどうもありがとうございました。

以上