平成29年５月15日

公益財団法人　金融情報システムセンター

第５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５月15日（月）15:45～17：10

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
	持田　恒太郎	株式会社三井住友銀行 システム統括部　システムリスク統括室　室長
	大石　秀一	（代理出席）株式会社南都銀行
	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	東京海上日動火災保険株式会社　IT企画部参与
	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 FinTech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
	西島　孝生	（代理出席）日本マイクロソフト株式会社 クラウド＆ソリューションビジネス統括本部 ソリューションスペシャリスト
	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
	希代　晃彦	経済産業省　商務情報政策局 サイバーセキュリティ課長
	今野　孝紀	（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
FISC(事務局)	渡辺　達郎	理事長
	高橋　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
	中山　靖司	調査部　部長
	和田　昌昭	監査安全部　部長
	大澤　英季	企画部　主任研究員

Ⅳ　議事

１．【議事１】金融機関におけるFinTechに関する有識者検討会 報告書（案）（第４回席上意見・事後意見等を踏まえた修正案の提示）

○岩原座長　座長の岩原でございます。それでは本日１つ目の議事は金融機関におけるFinTechに関する有識者検討会報告書案でございます。FISC企画部の藤永次長、よろしくお願いいたします。

○藤永企画部次長　企画部の藤永です。それでは議事１のご説明をさせていただきます。報告書の案をご説明する前に、参考資料としてA4横でつけております、「第４回FinTech有識者検討会に対するご意見およびご回答」の資料をご用意ください。

今回は事後の意見を11件いただきました。南都銀行様とAWS様からいただいています。

１番。「FinTech企業が負うべき安全対策の責務を金融機関が負担する図式が例示されている」。これは前回「同等性の原則」としてご説明した資料です。「FinTech企業が提供する新規業務について、各金融機関が運用設計を行ったうえリスクの許容範囲の合意を行い、負担割合を決定するのは、各金融機関の事業判断であり問題ないものの、FinTech企業においては、少なくともシステムリスクに関する説明責任があることを明確にすべきと考える」というご意見です。

この「少なくとも」という意図は、優先事項を決められているというよりは、報告事項、説明責任を負うものの中の１つとして、必ずシステムリスクを含めるべきであるというご趣旨であると確認させていただいております。そうしたご趣旨を踏まえて、事務局回答ですが、「FinTechに関する安対基準適用上の課題　５．関係者間の協調」で追記させていただきました。詳細は後ほど報告書の全体をご説明する中で説明します。

２番。「安全対策の実施について、同等性の原則が用いられることについて異論はないものの、遂行能力がない（若しくは不十分）という理由で、配分を見直すことや、再配分の考え方を取り入れる」。これは手前どものこの検討会で従来から再配分ルールとして取り上げてきたものですが、このルールが適用されるということを明示的に言うことによって、FinTech企業がみずから行う努力や教育を阻害することに結びつかないか、ということが懸念される。これはモラル低下の懸念についてご意見をいただいています。基本的な考え方としては、金融機関とFinTech企業双方の負担というのを『PAY AS YOU USE』という言

葉で表現されていますが、責務を負担した者に応分の利益が還元されるということが必要ではないか、という趣旨のご発言と確認しています。

事務局の回答は、先ほどと同じ部分に追記ということで、脚注になりますが、FinTech企業に生じる可能性のあるフリーライダーの指向を抑止するために、「責務を負担した関係者に応分の利益が還元される公正なスキーム」、これを「関係者であらかじめ合意しておく」。そういう方法もひとつ考えられるのではないか、ということを追記しました。

３番。これはある意味、再確認が必要ではないかということで、ある意味念押しのご要望でございます。FinTech企業にもしっかりと責務を果たしていただく必要があると考えるので、そうしたことを示す表現を加えるべきであるということでございます。

これにつきましては事務局回答として、同じく「FinTechに関する安対基準適用上の課題５.関係者間の協調」に追記しました。

４番。「『金融機関がイノベーションの成果を、どの程度享受できるかといった観点』は、業者選定の大きな要素となる」のでAPI接続先チェックリストワーキンググループの議論においても同様の観点のルールを盛り込んでほしいというご要望です。

これについては、API接続先チェックリストワーキンググループの検討において参考とさせていただきます。

５番。これはクラウドの補足的な検討の部分に対する指摘です。「大規模なシステム障害が発生した場合、～～～～有事対応の責任は金融機関が負うべきものである」ということで前回論点を提示させていただきましたが、これをそのまま読むと金融機関に責任100％で外部委託先には０％との誤解が生じる。一義的な責任が金融機関で、技術面でのパートナーとしての責任がFinTech企業の意味合いの表現をつけ加えていただきたい、というご意見です。

事務局回答としては、「金融機関の特性から発生していることから、金融機関が一義的に負うべきであり」ということで「一義的」という表現を追記させていただきました。

６番。ここからはAWS梅谷委員からのご意見です。今回の検討の中で「一般の情報システム」という言葉を使っているが、これは重要な情報システムではない、それ以外の情報システムという意図で使っているということを統一したほうがわかりやすいのではないかというご意見です。

事務局回答ですが、実は第１回の論点メモ「FinTechに関する安全対策検討の在り方」というところで、それ以外の情報システムを「一般の情報システム」呼称するという記載が

既にありますので、ここでご指摘の趣旨が達成できていると考えています。

７番。情報処理の広域性というクラウド事業者の特性に対して、「クラウドサービスでは、情報処理拠点を含む事業拠点も、複数の国にまたがり広域に及ぶ」と断定的に書いておりました。必ずしもそういう場合のみとは限らないだろうということで、「及ぶ場合がある」というふうに修正してはというご指摘です。ご指摘のとおりですので、修正を加えさせていただいております。

８番。実質的な統制を行う権利を金融機関が確保する必要があるということを論ずる中で、その権利を明記する文書として契約書という表記をしておりましたが、それを契約書「等」というふうに明記するほうが実務にかなうのではないか。硬直的に契約書という名前でないといけないというふうに金融機関に誤解が生じないようにすべきではないか、というご指摘です。

ご趣旨のとおりですので、「必要となる権利を確保するためにクラウド事業者と交わす契約書等にその権利を明記する」と補記しました。

９番。これは前回FISCで行った米国の監督当局のヒアリング結果への指摘です。もともと、内部で実施した場合と比較してクラウドで利用した場合にはリスクが拡大しないように統制の強化を求めている、と我々のほうで付加しておりましたが、必ずしもヒアリング結果を見ると強化を求めているとは限らないのではないか、というご指摘です。

これもご指摘のとおりですので、「統制の強化を求めている」ではなく、「統制を行い適切にリスクを管理すること求めている」と修正しました。

10番。「クラウド事業者が提供する暗号化ツールを利用する場合、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」と断定的なヒアリング結果として記載したところ、クラウド事業者の職員が暗号化を解くキーを持つ場合、持たない場合があるというご意見をいただきました。

我々は、ヒアリング結果のコメントをサマリーして記載していましたので、ヒアリング結果に忠実な詳細な記載内容に変更しています。「暗号化ツールを利用する場合がある。この場合、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場合は、職員に情報を見られるというリスクがある。一方、機械なのでメンテナンスも必要であり、クラウド事業者の職員がキーを持つことが必要であることは理解できる」と正確に補記しました。

11番。ここはSaaS、PaaS、IaaSに対するOCCのコメントですが、「パブリッククラウドについては、SaaSよりもPaaSやIasSのほうが金融機関にとっての負担は大きくリスクも高く

なる。金融機関がそれを理解していることが重要」としていましたが、「このままの表現では、IasS、PaaSのほうがSaaSよりも無条件にリスクが高い、という誤解を与えるような表現になっている」のではないかというご指摘です。誤解が生じないように、ヒアリングした当局のコメントを直すのではなく、我々が追記した部分に修正を加えています。「金融機関は、多様なクラウドの中から、みずからのニーズに適合する形態を選択することになる」。IasSがふさわしいのか、あるいはSaaSがふさわしいのか、あるいはPaaSがふさわしいのか。そして選択された形態によって責任分界が異なる。今回の検討会でも責任分界が異なることを金融機関が理解することが重要であるというご提言をいただいていますが、そうした部分において金融機関の管理すべきリスクも変わってくるであろうと。したがってそれを理解して適切にリスクをコントロールすることが求められるのである、という表現に補記しました。

以上の事後意見を踏まえまして、有識者検討会の報告書案について説明させていただきます。現時点で83ページになりますので、ポイントを絞って全体像を説明させていただきます。

まず目次ですが、各回の検討で提示させていただいた論点メモに事後の修正を加えたものを一体化した構成になっています。第Ⅰ章は第１回の論点メモ、第Ⅱ章、Ⅲ章は第２回の論点メモ、第Ⅳ章は第３回と第４回の論点メモです。第Ⅴ章「集合的な検討を踏まえた『オープンAPI』のあり方」これは今回新たに書き起こしているもので、後ほど詳細にご説明させていただきます。ほかの章でもオープンAPIに関連して加筆しているところが２カ所ございますので後ほど説明します。最後に第Ⅵ章ですが、これは第４回で提示したものです。

本文が40ページ程度、残りが資料編として、論点メモに付随したものを全部で９点そろえています。

まず１ページ「はじめに」ですが、これは本検討会を始めるに当たって設立趣旨として述べさせていただいたものです。

そこから先第Ⅰ章ですが、ここは提示させていただいた論点メモに事後の修正を反映したものとなります。なお、細かいところで、言い回しを直したり、趣旨が変わらない範囲で微調整は手前どもでやらせていただいています。そこは細かい話なので履歴はつけておりません。趣旨が変わるようなところ、あるいは追加したようなところに履歴をつけているということでごらんいただければと思います。

そうしますと最初に履歴がついていますのが、６ページのところです。金融機関が必ずしも主導的立場とならない業務形態を今回新たに想定すべきであるということで論点を出してきたものですが、やや文字だけだとわかりにくいということで、図表１として絵にしたということです。

その次をめくっていただいて８ページです。ここは先ほど申し上げましたオープンAPIとの関係で追加した２カ所のうちの１つです。（５）「『オープンAPI』との関係」ということで､従前は全銀協を事務局として行われている銀行のAPIの検討会についてのみ言及しておりましたが､その前段としてオープンAPIというのがどういうふうに理解し得るか､安全対策上どう捉えるべきか、ということを補記しております。

まず「タイプⅢの実現方法の１つとして『オープンAPI』と通称される方法がある。」これにつきましては､脚注14のとおり､金融審議会『金融制度ワーキング・グループ報告書』において言及されていることを参考にして書いています。

本文ですが、「『オープンAPI』ではFinTech企業と金融機関の合意に基づいて、情報システム相互をシステム的に接続することとなる。これによって、FinTech企業は、金融機関との多様な情報の結合と協調した安全対策が可能となり、顧客に対して、利便性が高くかつ安全なサービスを提供することが可能となる」｡これがオープンAPIであるとしています。

こうしたAPIによる事業者間のシステム連鎖、APIでシステム的に接続することによってシステムが連動連鎖していくということですが、これは「技術的には多対多でかつ多段階にわたり重層的に可能である」。したがって、金融機関がAPIを公開することによって、金融情報システムの連鎖に多様な関係者が携わることが可能となる。そうしますと情報の結合の種類も多用となって、その多様性によってまさに革新的なサービスの可能性が開かれてくるということです。こうしたネットワーク時代にオープン化がイノベーションをもたらすメカニズムについては脚注の15ですが、本検討会の委員でもあります国領委員のほうで、『オープン・アーキテクチャ戦略　ネット時代の協働モデル』という1999年に書籍を出されており、参考になるのでは、ということで脚注に追加しています。

本文ですが、社会的にはそうした取組みを「オープンイノベーション」と称しているであろうと。「そうした環境を涵養していくことが期待されている」のではないかと考えております。

一方で、それが安全対策上どう捉えられるかということですが、システム連鎖に携わる関係者が多くなれば、その相互作用というのが増えてくるだろうと。そうした中で「想定

しなかったリスクが顕在化する可能性が高まる」と考えられます。これについても脚注16ですが、同じく国領委員の『ソーシャルな資本主義　つながりの経営戦略』という2013年の書籍の中において、そうした趣旨の記載がされています。

本文に戻りまして、「そのため、安全対策に関しては、相互作用等に対処するために、」関係者をサービスごとに一つ一つ特定してやっていくというのはかなり難しい。要はシステム連鎖が複雑になって統制の難易度も上がってくるということであれば、オープンAPIに参画する可能性のある関係者が集合して、多面的な検討を行うことがある意味効率的でもあり有効でもないかということで、そうした「集合し多面的な検討を行うことが重要となる。」これを「集合的な検討」というふうに称して、後ほどそうした考え方を踏まえてさらに論点を深めております。

図表３は「オープンAPIにおけるシステム連鎖関係」、今口頭で申し上げたことを少し絵にしているところでございまして、ポイントとしてはシステム連鎖は技術的には、FinTech企業と金融機関のみならず、FinTech企業同士でも起こり得るであろうということです。

脚注19です。平成29年３月から「クレジットカードデータ活用に係るAPI連携に関する検討会」というのが経済産業省によって開催されておりますので、その概要、公表内容を記載させていただいています。

続きまして10ページです。ここはFinTechに関する安対基準の適用上の課題としておりましたが、記載内容が安全対策のあり方も含んでおりますので、章のタイトルに「安全対策の在り方」と追記をしました。

脚注20です。既存の安対基準を構成するものが設備基準、技術基準、あと運用基準があり、それぞれの性質を本文に「モノを対象とする設備基準や技術基準は、個別具体的な技術を前提として安全対策を特定することは困難であり」、環境の変化が激しい中では確定的に設定することは適切ではないというふうに述べていますが、脚注の20で「技術基準の中にも比較的技術変化の影響を受けやすい部分とそうでない部分が混在して」改訂を繰り返されてきていることに留意が必要である、とし、今後の安対基準の改訂においては、そうした観点で仕分けを考えるという、目線も必要ではないかと、事務局で追記しています。

16ページです。タイプⅠにおいて内在する問題と安全対策のあり方ということを述べる中で、FinTech企業の安全対策遂行能力という言葉を使っていました。それがそもそもどういうことを意味するのかというところを詳細に書いておりませんでした。前回、検討会の席上で私のほうからその部分につき、口頭でご説明したものを脚注に追加しています。す

なわち「安全対策遂行能力の基礎的な部分」ということで、やはり「安全対策のPDCAサイクルを十全に機能させられる能力」、これは基礎的な部分としてFinTech企業に対しても、求められるものであることを記載しています。

17ページです。再配分ルールの必要性について言及をした後に追加をしています。責務の再配分に関しては当然再配分をした上で追加の手当をしていくことになるのですが、そのときにおのずと費用負担が生じるであろう。なので費用負担のあり方を言及する必要があるのではないかと、事務局として追加をしています。すなわち、責務を負担可能な関係者が単数である場合は問題は生じないのですが、複数いる場合の観点として「安全対策における社会的な費用の最小化」、「社会的な費用の総体の最小化」という観点から、追加費用負担が少ない者に責務を再配分することが望ましいのではないか､と追加しています。再配分ルールの本文ですが、「なお」ということで「追加負担費用が少ない関係者に責務を再配分することが、安全対策における社会的な費用の最小化に資することとなる」と追加させていただきました。その下のところで、「なお、以上のルール及びサブルールは」というところは、前回脚注に入れていたものを本文に入れたということです。

それとの関連で脚注27です。先ほど申し上げました事後意見の２番の対応です。FinTech企業に生じるモラルハザードに関する言及とそれに対する対策の１例ということで、脚注に追加させていただいております。

18ページです。従前から、統制の方法と内容を、タイプⅢについて言及する中でコメントさせていただいておりましたが、わかりにくいというご意見をいただいておりまして、事務局として、わかりやすさの観点から追加しています。そもそも外部委託についてはライフサイクルがあるだろうということで､ライフサイクルに応じた管理フェーズとして｢利用検討時」、「契約締結時」、「運用時」があると。そして管理フェーズに応じた統制のやり方、方法として、利用検討時の客観的評価、契約締結時の契約締結、運用時のモニタリングということを、従来、安対基準では定めている。さらにそうした統制の方法における統制の内容というのは、それぞれの管理フェーズで比較的共通する部分が多いということで、「データの保全に関する事項」、「本人確認に関する事項」、「サービスの可用性に関する事項」等々が、各管理フェーズを通じて類似もしくは共通したものとして捉え得る。そして、以上の方法と内容を掛け合わせますと、利用検討時の客観的評価に行う統制の内容を含むものとして「チェックリスト」があり、契約締結時のときは「契約書」があり、運用時のときには「監視運用項目あるいはモニタリング書類」みたいなものがある。

そうした関係を図示しています。

19ページですが、ルールに名前をつけたとか、ややわかりにくいところを補記した程度のものです。

20ページです。これは関係者間の協調として、事後意見1、2、3の部分を追加させていただいています。

23ページです。これは今回１枚新たに追加しており、背景も含めてご説明させていただきます。「FinTech業務を担う情報システムの安全対策上の取扱い」というタイトルです。まず、今までの検討は「FinTech業務を担う情報システムは、当初は、一般の情報システムである場合が大半であると想定して行ってきた」。これは第Ⅰ章においてもそのように書いています。「しかしながら、FinTech業務を担う情報システムにおけるリスクの顕在化が、重要な情報システムが提供するサービスに重大な影響を及ぼす場合には、FinTech業務を担う情報システムを重要な情報システムと一体とみなして、安全対策上取り扱うことが必要となる」。まず、これが基本的な考え方です。

「他方で、個々の情報システムの対象範囲は、金融機関において独自に判断される」のが一般的である。つまり、自社に情報システムが、何個あるか、ということは金融機関によって２桁のところもあれば、金融機関によっては３桁のところもある。その管理粒度を大きくされているところ、細かくされているところ、さまざまあるということです。したがって、「FinTech業務を担う情報システムにおけるリスクの顕在化が、重要な情報システムが提供するサービスに重大な影響を及ぼさないにもかかわらず、一体として、安全対策上取り扱われる可能性がある」。これは管理粒度を比較的大きく捉えられている場合に起こり得るのではないかと思っています。

「その場合、リスクの高いシステムに引きずられて、FinTech業務を担う情報システムにも『高い安対基準』の適用を求めざるをえないと判断される可能性があるとともに、その影響を受けて、金融機関のFinTech業務への取組みそのものが抑制的となる懸念がある」のではないかということです。

そうしたことから、今回の検討会で明示的に１つ提言してみてはというご提案なのですが、「イノベーションの成果を享受する観点からは、こうした問題にあらかじめ対処しておくことが望まし」いとしたうえで、以下の３要件を全て充足する情報システムを管理上分離できる、独立して取り扱うことが可能であるということを、積極的に言ってみてはと考えています。

条件として１つ目が「リスク顕在化時の影響の分離可能性」。そもそもの出発点のところで、いわばFinTech業務を担う情報システムへの影響がシステム全体に波及させないことが可能であるということ。２点目、３点目は管理上の問題ですが、リスク特性が顕著に異質であるということと、リスク管理が分離してできるということでございます。

「金融機関は以上の考え方に留意しつつ、FinTech業務を担う情報システムの安全対策上の取扱いを検討することが望ましい」と括っております。具体的にどういうことが起こりうるかということですが、脚注33にそれをイメージいただけるよう記載しています。決済指示をFinTech企業が仲介される場合、決済データが流れるということをもって、重要なシステムとして認識される場合があるのではないか、ということです。当然それは、影響を及ぼす場合にはそうであるのですが、相互影響、相互作用をある程度遮断できるのであれば、決済データが流れるといっても、一般の情報システムとして取り扱ってよいのではないか。そうした考え方を明確にしているということです。

第Ⅲ章です。特に大きな修正は加えておりませんが、最後の30ページ。ここにオープンAPIに関する加筆をしています。「なお」ということで、「FinTech業務における安全対策に関しては、各業界団体をはじめとして、様々な集団において」、先ほど申し上げました、「集合的な検討が進められて」いますということです。その相互関係については、「例えば、下図のように捉えることも考えられる」ということで、FinTechに関する安全対策を検討している集団の相互関係を整理してみました。参加者あるいは検討範囲が特化されているか、あるいは幅広いかということでまず縦の軸を切っております。そうしますと、恐らく一番幅広い参加者がいるのはこのFinTech検討会、この場ではないかと。その次に全銀協様で行われている銀行API検討会、次に、FinTech協会様で行われているAPIセキュリティ分科会、次に、サイバーセキュリティに特化されている金融ISACの検討というものが捉え得るのではないかということです。その他にも今後さまざまな集団の検討が行われるであろうということで、点線で書いています。

そうした参加者とか検討範囲の性質の違いによって合意事項の抽象度も抽象的なものから具体的なもの、すなわち枠組み、原則に関するものから技術、実装に関するものまで幅広く捉え得るということです。そうした多様な集団によって検討が行われるということを認識した上で、本文ですが、「それぞれの集団においては、検討内容の整合性確保の観点から、相互関係を意識して」、要はそれぞれの集団で同じものを対象にして検討を行いますと、ダブルスタンダード、あるいはトリプルスタンダードになる懸念がありますので、

集合的な検討の相互関係を意識して、それぞれが整合的に検討が進められることが期待されるのではないか、ということです。

続きまして第Ⅳ章です。34ページの真ん中の部分は、事後意見の７番の反映です。

35ページの脚注55、これも前回口頭でお話をさせていただきました。「ネズミの害を防止する措置を講じること」という設備基準を例にして、コメントしたものを文字にして追加しています。

36ページ。先ほど事後意見の５番、南都銀行様からいただいたものを反映しています。

脚注57。これは前回席上で、安冨委員からいただいたご指摘への対応です。機微情報といった場合、その対象を論じるに当たって、金融庁のガイドラインと改正個人情報保護法の記載内容について、補記をしております。

37ページ。事後意見８番を受けた修正です。

39ページ。第Ⅴ章ですが、今回、新たに事務局で書き起こした論点メモになります。この間皆様には、FinTechに関する総論的な枠組み、幅広い考え方をご議論いただいておりますが、そうしたところを踏まえたうえで、やはりこの間、FinTech企業の皆様、あるいは金融機関の皆様が特に関心の高い「オープンAPI」に関しまして、本検討会で何らかの提言をしては、とご用意させていただきました。タイトルは、「集合的な検討を踏まえた『オープンAPI』における安全対策の在り方」です。

まず「オープンAPI」においてどのような統制上の課題が考えられるかというところですが、先ほど来申し上げておりますとおり、「オープンAPI」はタイプⅢの実現手法の１つである。したがって、APIを公開する金融機関は外部委託基準を準用し、API接続先であるFinTech企業に対して統制を行うこととなる。これは脚注61で、そうした本検討会の提言内容と整合的な内容で、銀行APIの中間的整理報告書においても記載されています。

「したがって、今後、行政や業界団体等によって『オープンAPI』の環境が整備されれば、金融機関とFinTech企業のAPI接続が増大し、結果として、FinTech企業は多数の金融機関から統制を受けることとなる」。そうしますと、「形式的に、多数の金融機関が個別に統制を行うこととなれば、FinTech企業においてはその対応が過度の負担となり、イノベーションを大きく損なう」。結果として金融機関もイノベーションの成果を享受できなくなるということです。そこが課題、問題認識です。

解決の方向性としては、そもそも金融機関が行う統制は、金融機関で共通する部分が多いであろうと。現に安全対策基準のような社会的に合意されたルールを使用されていると

いうところを踏まえても、そうであろうということで、そうした統制の共通部分についてFinTech企業の負担軽減を目指して、関係者が集合的に検討し取り組むことができればよいのではないか、ということです。

では具体的にどういうことが考え得るかということが、「安全対策のあり方」です。ここは先ほど申し上げました、統制の内容と方法に分けて書いています。まず統制の内容ですが、一般的に金融機関では統制の内容については、安対基準や業界団体の自主基準などの社会的に合意されたルールを踏まえて、その上で金融機関独自の項目を追加して定められているということです。「したがって、まず、入口の管理フェーズで行われる統制の内容」、すなわち先ほどご説明しました「客観的評価で使用されるチェックリストの項目」について、その共通部分を金融機関とFinTech企業で集合的に合意形成するということが考えられるのではないか。これは脚注62ですが、銀行API報告書においてもそうした観点で整理がされておりまして、それを受けましてFISCでは、「API接続先チェックリストワーキンググループ」を現在設置して検討を行っているところです。

チェックリストの共通部分を合意しておけばどういう効果があるかということですが、先ほど統制の内容は他の管理フェーズに及ぶであろうということをご説明しましたが、チェックリストの内容をあらかじめ合意しておけば、その後の管理フェーズで行われる契約書や監視・監査項目にもおのずと反映することが可能となると。そうしますと金融機関とFinTech企業が安全対策に関して管理フェーズごとに個別に合意形成する負担というのは軽減されるだろうということでございます。

40ページですが、一方、統制の方法に関しては、金融機関の皆様では、モニタリングなど従来から共同で実施されているという実績があるということです。したがってそうした実績、「複数の金融機関が、意思統一を図りつつ、選定された幹事金融機関等」が、ここでは金融機関等の委託を受けた第三者監査人を含む場合もあると考えられますが、代表して統制を行いその結果を享受することができるのではないか。これはオープンAPIにおいても同様のことが可能であると考えられて、「幹事金融機関等が行った客観的評価の結果」やあるいは「締結した契約書」あるいは「監査結果をその他の金融機関が利用すること」となると、FinTech企業の負担軽減に資するのではないか。実際脚注63ですが、銀行APIの報告書、中間的整理においても、そうした言及がされているということです。

「以上のように、金融機関が、あらかじめ関係者で合意された内容にしたがって、集団で統制を行う」ということは、やろうと思えば既に可能であるということですが、そうし

た場合、「FinTech企業においても集団で統制への対応ができれば、さらに負担を軽減できる可能性がある」ということを提言してはと思っています。具体的にはということですが、行政や業界団体による環境整備が進む中で、FinTech企業の集団組成に向けた取組みが既に見られています。脚注64ですが、Mark Makdad委員が理事を務められていますFinTech協会が、平成29年３月３日に『認定電子決済等代行事業者協会に向けて』という文書を公表されています。この中で改正銀行法において定めのある認定電子決済等代行事業者協会、ある意味オープンAPIに関して集合的な検討を行う集団になるかと思いますが、「複数の企業で設立に向けて準備を行い新しく設立される協会では必要な規則の制定及び利用者からの苦情対応業務を含む認定事業者協会の業務を行い」と、今後の方向性を示されているところです。これがまさにこれから今もう進められているところであるかと思いますが、「仮に、そうした事業者団体が設立されることとなれば」、「あらかじめ関係者で合意された統制の内容」、先ほどチェックリストのワーキンググループで合意することとなった統制の内容を、そうした協会の自主基準とすることは可能ではないかということです。

さらに加えて「個々の会員における自主基準の遵守状況について」、業界団体が「例えば、内部監査人等が検証した結果を踏まえて、必要に応じて会員に対して指導や勧告を行うことが可能となる」のではないかということで、脚注65に、今国会で審議されています銀行法の改正案の該当部分を記載させていただいているところです。

「以上のとおり、FinTech企業における集合的な検討」が進んでいくということが予想されている中で金融機関の集団とFinTech企業の集団が安全対策に関する協議を開始していくことが、FinTech企業の負担軽減に限らず金融機関にとっても負担軽減になるのではないかと考えています。まとめとして、「総体的な安全性を確保しつつ関係者の負担を最小化すると」ことを目指して、「両者で協調した取組みが進められていくことが期待される」ということを、この検討会として提言されてはどうかというご提案です。

では具体的に両者で協調した取り組みとして、どういうことが考えられるのかということについて、脚注66ですが、例えばということで、「FinTech集団の事業者団体が会員への指導・勧告」を業として行うという場合に、「会員の自主基準遵守状況の検証作業を行うこと」となるだろうと。恐らくその作業というのは、金融機関がAPI接続先に対して行う統制と重複する部分が多いのではないか。したがって「関係者の負担の最小化の観点からは」、両者が共同実施するようなスキーム、会員の自主基準遵守状況の検証を共同して行うようなスキームがアイデアとしては考えられるのではないかということです。これが妥当かど

うかというところは、皆様が検討を踏まえて判断されるものですので、必ずしも正解ではないと思います。それ以外にもさまざまな知恵は関係者が集合されれば出てくると思います。何より、そうした取組みが進められることが社会的にも期待されるのではないかということです。

41ページです。下のところで少しわかりにくかったので統制基準という言葉、本文にはもともとあったのですが、それをタイトルに追加してわかりやすく直しているというところです。

本文はここまででございまして、ページ42、43、44は委員、オブザーバーの皆様のお名前と役職、新旧交代を含めて記載しております。もし記載内容に間違っているところがありましたら、事務局にご一報をいただけますと助かります。

そこから先は資料編ですが、いろんな検討がこの検討会と並行して、当局並びに全銀協その他において進んでおりますので、そうしたアップデートをしているというところが、履歴でつらつらと書いてあります。

51ページですが、OCCにおいて昨年３月末に「責任ある革新」というペーパーが出された後、昨年12月には一部のFinTech企業に対して特別目的国法銀行の免許を付与するという案が公表されたことを追記しています。

資料２は、第１回でお配りした資料です。

53ページの資料３です。第１回の論点メモでタイプ別類型ということでかなりFinTech業務のタイプを、思考実験をしながら詳細に本文に記載しておりましたが、ここで考察という形で類型化の思考実験をまとめて資料編におきました。

57ページ、資料４です。これは、安全対策基準の改訂が行われていない中で、外部委託に関する安対基準の全体がわかるようにという趣旨で追加つけております。

資料５、74ページです。前回席上で黒山委員のほうから趣旨がわかりにくいというご意見をうけて、外部委託の有識者検討会報告書で書かれていた表現を74ページの下に追加しています。

76ページ。これも前回席上で黒山委員からメッセージとして明確にしたほうがいいのではないか、というご意見をいただいたものを反映しています。

77ページ資料６。金融機械化財団、現在、FISCという手前どもの団体のそもそもの設立趣意書です。既に昭和59年の段階から、金融情報システムに関しては関係者の十分な意思疎通のもとに諸施策が推進される必要があるということが提言されFISCが設立されており

まして、そうした考え方は、今FinTechを論じる中においても通用するものではないか、ということで古い資料ではありますが、報告書に含めております。

78ページ資料７。クラウドの利用状況、前回ご提示したのと同じであります。

79ページ資料８。79ページの修正は、事後意見の９番の反映。80ページの修正は、事後意見の10番の反映。81ページの修正は、事後意見11番の反映。以上、梅谷委員からのご指摘を反映しております。

最後に資料９。以上のとおり、FinTechに関する総論とあとAPI接続に関する個別の安全対策を提言として出させていただいておりますが、さらに現在検討していますチェックリストワーキンググループについても言及する必要があるということで、資料９として加えています。そもそも、第３回の有識者検討会において、チェックリストワーキンググループの設置についてご報告させていただきましたが、その際にワーキンググループの検討に本検討会の議論が適切に反映されているか、成果物をこの場で検証いただきたいというお願いをさしあげて、その上でワーキンググループの成果物は本検討会の提言事項の１つとさせていただきたいと報告しました。

この間ワーキンググループの検討状況を見ながら、どうしたご検討をこの場でいただくのがふさわしいのか、と考えてまいりましたが、やはりチェックリストの成果物の現物というものは､今後さまざまなAPI接続に関する取組みが進む中で中身もどんどん見直されて変容していくものであろうと。したがってチェックリストのその時点の現物そのものをこの場で検証していただくのは、あまりふさわしくないのではないか、と考えております。

そうしたことよりもむしろ、ワーキンググループでどうした検討がなされれば、この有識者検討会の報告の提言内容を踏まえたものだというふうに解し得るかということを、資料９として提言、確認いただくほうが、むしろ今後のチェックリストに関する議論においてふさわしいのではないかと考えています。銀行APIのチェックリストは、恐らく継続的に検討が行われるでしょうし、また、銀行APIに限らず、より幅広い業界でチェックリストの検討が始まる可能性もありますが、そうした点を考慮しても、資料９の整理がふさわしいのではないかということで、用意させていただきました。

中身ですが、まず第１段落。ここは全銀協が公表された中間的整理の事実を書いています。第２段落。そうした整理を受けてチェックリストワーキンググループというのをFISCが事務局となってやっているという、これも事実の記載です。第３段落、第４段落。ここがチェックリストワーキンググループにおいてどのような検討が行われていれば、本検討

会の提言内容を踏まえたものといえるかということで、２つほど要件を書いています。１つが「オープンAPIは、FinTech検討会におけるタイプⅢの実現方法の１つであることから、チェックリストWGの検討は」、「タイプⅢに関する提言内容と整合的に進め」ることが必要である。

ここでいう整合的と認められる要素は、３つあるだろうと。すなわち１つ目がタイプⅢにおける外部委託基準を準用することが可能であるといっているそのルールとの関係。２つ目が必要最低限の安対基準というのを踏まえているかという点。脚注の78ですが、API接続先を含む金融関連サービスの提供に携わる事業者において最低限踏まえられるべき基準として必要最低限の安対基準を取り上げてきましたので、当然、API接続先の客観的評価を行うチェックリストにもこうした観点は含められるべきであるということ。ただし、この必要最低限の安対基準は今後の安対基準の改訂後に初めて制定されますので、それまでの間の暫定措置が必要であろうということでチェックリストワーキンググループでも議論をしておりまして、先ほどご説明させていただきました脚注26の安全対策遂行能力の基礎的な部分を暫定措置に充ててはということです。整合的と認められる３点目の要素としては、先ほど申し上げました、FinTechに関する安全対策を検討している集団の相互関係を意識した検討が行われること。すなわち全銀協で行われているセキュリティ原則等の検討内容も、チェックリストワーキンググループの中身に適切に反映されるべきではないか、ということです。

２つ目の要件として、４段落目ですが、「FinTech企業の負担軽減の観点から、社会的規範性をもったチェックリストが制定されることが望まし」いのではないか。要は幅広い方々が自主的に守っていただけるようにしないといけないということです。そうした規範性を生じさせるためには、多くの関係者がその合意形成過程に参画する必要がある。これは本検討会で申し上げてきたことでございますので、「そのためには、金融機関、FinTech企業、ITベンダーといったAPI接続に携わる関係者が合意形成を目指して、チェックリストの検討過程に参画することが望ましい」ということです。

以上、２つの要件を満たしてチェックリストワーキンググループにおいて集合的な検討が行われていれば、その結果としてチェックリストなどの成果物が取りまとめられた場合には、FinTech検討会の提言内容の一部として取り扱われる。おのずとそうなるのではないかということでございます。

さらに今後環境変化等が生じた場合にも、それに応じて集合的な検討が継続的に行われ

る必要があるだろうということで、成果物の内容は継続的に見直され、実装・運用されることが期待されるのではないかということです。

そうした意味では本検討会からチェックリストワーキンググループに対するメッセージとしまして一番最後の段落ですが、「API接続に携わる関係者においては、その成果物を、有用なものとして、金融機関の実態に応じて」、要はここでいう金融機関にはさまざまな業態がいらっしゃいますので､そうした業態の固有の特性､実態に応じて利用された上で、総体的な安全性の確保とイノベーションの両立を目指されるということを、チェックリストワーキンググループ並びにその作成過程に参画された皆様に期待をしたい、と括っています。

以上、大変長くなりましたが、有識者報告会の報告書のドラフトをご用意しましたので、ご説明さしあげた内容、それ以外も含めまして、ご意見をいただければと思っております。私からは以上になります。

○岩原座長　どうもありがとうございました。それではただいまのご説明にたいしてご質問はございますでしょうか。いかがでしょうか。轟木さん、お願いします。

○轟木委員　Liquidの轟木でございます。１点質問なんですけれども、参考資料で２つ目にいただいていた、報告書の17ページの脚注27で追記していただいた部分、「FinTech企業には安全対策への投資を意図的に抑制するフリーライダーの志向が生まれる」と断定的に書かれているんですけれども、これは本当にそうなのかという点、あとそもそも責務の再配分とモラル低下の議論というのは無関係なんじゃないかなと思っております。具体的に申し上げますと、そもそも責務の再配分の議論が16ページに書かれておりまして、16ページの下から２段目「したがって」の段落で、要するにタイプⅠの場合に、金融機関というのはFinTech企業の安全対策遂行能力を確認すると。まずFinTech企業でしかできない部分、安全対策遂行能力を確認した上で、それを超える部分については、金融機関とITベンダーが分担する。このフリーライダーというのが、そもそもFinTech企業ができない、FinTech企業の能力を超える部分を指してフリーライダーといっているのかどうかというのもよくわからない。

逆にその部分に対して、安全対策の投資を抑制していることになるのかと。そもそもタイプⅠの場合に、FinTech企業ができる安全対策遂行能力をFinTech企業がやればいいだけ

であって、それを越える部分についてまでどうして再投資する必要があるのかという点について、記載の趣旨と合わせて確認させていただきたいと思います。

○岩原座長　藤永さんお願いします。

○藤永企画部次長　少し長い説明になるかもしれません。まず、「モラルハザード」についてはそうした事実があるというわけではありません。今後こうしたサービスがどんどん広がっていく中で、FISCが再配分ルールということの必要性を明示的に言ったときに、「モラルハザード」が起こり得る可能性があるのではないか。そうした可能性について言及しているということです。どうした可能性を考えているかというと、まず責務を金融機関がある意味、肩代わりするという前提になったときに、FinTech企業が金融機関に、自分たちはこれくらい安全対策をやっていますよ、と話すときに、安全対策をやっていない、やらなくていい、というふうにするインセンティブが働かないか。金融機関がどうせやってくれるのであるから、FinTech企業はできるだけやらないで、そこには経営資源を配分しないで済まして金融機関にかわりにやっていただくというような、そういう指向が生まれないか。要は金融機関の経営資源配分に、ただ乗りするというインセンティブが生まれないかという懸念。繰り返しですが、これはそうしたことがあるということではなくて、そうしたことが起こり得る可能性があるのではないかということです。

あるいは違う例として、金融機関がむしろFinTech企業に責務の負担を強く求めていくような流れになっているような場合、再配分ルールでFinTech企業はやっていませんというときに、金融機関が、「いやいや」と、「やっていないのではなくて経営資源を手当してそれを追加でやるのはやはりFinTech企業側ではないか」というふうに求めるようなことも、もしかしたら起こり得るかもしれないと。

そういう方向に金融機関が仮に流れますと、FinTech企業側からすると、安全対策ができていないにもかかわらず、自分たちは結構できていると、やっていますということを虚偽の申告をすることによって、追加の負担を求められないようにするようなインセンティブも生じるようなことがあり得ないかということ。以上の両面の可能性が、これはあくまでも可能性の議論であり得るのではないかということでございます。

そうした可能性があり得るということをご理解いただければ、あらかじめそれに対する対応というのを何ら言及しておいたほうがいいのではないか、ということです。南都銀行

さんからご意見をいただいたのも、そうした可能性、これは恐らく事実の指摘ではなくて、可能性を憂慮されて事後意見としていただいたのではないかと思っています。

ではそうしたときにどういう解決手段があるかということですが、きちんと追加で費用を負担するときに、FinTech企業側が経営資源を追加的に用意して対応する場合、あるいは金融機関が追加的に対応する場合、両方あり得るかもしれません。そうしたときに一方的にどちらかにその負担を求めるということではなくて、その対応、追加コストが安いほうにその負担を求めるほうが社会的には望ましいのではないかというのが、この本文の上のところで書いているところです。であればそうしたことをより実効的に促し得るために、脚注22に書いていますが、責務を追加で負担した人に、そのサービスで得られる利潤を、きちんと応分に還元するようなことが例えば考えられれば、フリーライダーや虚偽申告の指向とか、あるいは社会的な費用が最小化されないような問題に対して対処可能となるのではないかということです。

ただ、これが唯一の答えでもないですし、今後金融機関とFinTech企業においてビジネスモデルが検討される中で、FISCの有識者検討会の場でビジネスモデルに関して、確定的なことをいうことは好ましくないだろうということで、脚注でそうした可能性が危惧されるということを、今後ご検討される中で少しヒントといいますか、そうしたところを入れてみてはというふうに思って記載しているところです。

轟木委員からご指摘のとおり、以上の私のご説明した内容と合っていない記載、例えば、先ほどのところでいいますとフリーライダーの指向が生まれるというふうに比較的断定的に書いている部分については、そこは修正したいと思っておりますが、事後意見もありましたので、こうした記載や考え方を入れておきたい、というのが事務局の考えでございます。

○岩原座長　轟木さんよろしいですか。追加のご質問とかはないですか。

○轟木委員　１点だけすいません。具体的にタイプⅠの場合は、弊社の場合、例えば指紋認証技術については弊社の技術を使う。銀行が弊社に外部委託する場合、銀行側のセキュリティ等については、当然弊社は何もできないのでそちらでやってもらって、かつ外部委託を受ける弊社としては、その認証部分については、当然セキュリティ面をしっかり投資してやる。その分についてはお互いフリーライダーなのかなと。弊社の技術については

弊社がちゃんとやるので、それについてのセキュリティに別に銀行さんが投資するわけではないですね。そういう意味ではこの業務委託の場合でフリーライダーという言葉を使うのはどうかなと思い、このことを踏まえて検討していただければと思います。以上です。

○岩原座長　藤永さん。

○藤永企画部次長　今回再配分ルールを議論する前提というのは、従来の安対基準をそのまま適用した場合に生じる問題ということで検討しています。そうした観点において生じる可能性ということをいっておりますので、どちらかというと、14ページ、15ページのところで責務の細かいことを書いておりますが、１つ例示として取り上げますと、こういうケースがあるのではないかと思っています。外部委託の場合もそうだと思うんですけれども、例えばFinTech企業がクラウドサービスを利用されていると、金融機関から再委託先の統制というのは非常に厳格に求められています。それは委託先であるFinTech企業が再委託している場合には、金融機関は直接再委託先には統制は当然行えませんので、そうしますと金融機関は、FinTech企業に再委託先に対する厳しい統制を求めることになってしまいます。そうしたときにFinTech企業のイノベーションを阻害しかねないという、そういうシチュエーションを想定した上で、金融機関は合意に基づいてみずから再委託先に対する統制をFinTech企業にかわってできるようなことを考えていく必要があるのではないか。という議論です。

したがって、今轟木さんがおっしゃったように、FinTech企業としてきちんと自分の責任範囲はやっていらっしゃるという会社であれば全然問題はなくて、どちらかというとそこまではちゃんとできないような、スタートアップの皆さんでもイノベーションを持っていらっしゃるので金融機関として何とか利用したいというケースを念頭に置いた場合に関する言及になっています。ですので、恐らく轟木さんのイメージより我々の提言内容というのは、限定的といいますか、対象をある程度絞った上での意見になっていると思っております。

○岩原座長　轟木さん、よろしいですか。ほかに何か質問、ご意見等ございますでしょうか。瀧さん、お願いします。

○瀧委員　マネーフォワードの瀧でございます。今回、追加されました39ページの第Ⅴ章といいますか。そのパートについては大変同意するところでございまして、現下はまだどのような運用ルールが来年の実態を帯びる中で実現されていくかという非常に模索中のフェーズでもある中で、今後私とか横にいるマークさんの会社とか色々なところを含めながら、APIを用いる事業者の協会を設立する準備を行っている段階でございます。そこの運用資源がしっかりと確保できていくことを前提に、この部分のアップデーティングというのをやはり現場の人たちでやっていくというのも、非常に重要なポイントなのかなと思いますのと。

その協会は自主規制機関としての位置づけを帯びますので、その中で丁寧なアップデーティングを行っていければと思っていますので、ご関心のあられる方はこの２名等ほかにお声かけいただければと思っております。以上でございます。

○岩原座長　はい。どうもありがとうございます。ほかに何かご質問、ご発言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続きまして、２つ目の議事にまいりたいと思います。

２.【議事２】API接続先チェックリストワーキンググループ活動実績と今後の予定について

○岩原座長　２つ目の議事は、API接続先（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あります。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　チェックリストワーキンググループの活動状況について報告させていただきます。チェックリストワーキンググループの活動に関しては、今既に報告書案において、例えばチェックリストのイメージ図とかをお示しさせていただいておりますので、それ以外につけ足す内容に関して、簡単に報告をさせていただきます。議事２の資料になります。

現在、第７回５月11日まで表にある通り開催しております。会議開催自体はこのようになっていますが、この会議のほかに、銀行からご参加いただいている３人の方々や、FinTech企業の３つの会社の方々は、別途いろいろと精力的に会議等を個別に行っていただいてお

りまして、全体としてはかなり密度の濃い議論や検討を行っていただいているというふうに申し上げられるかと思います。

あと項番２ですけれども、本ワーキンググループの委員として、銀行様はメガバンク様だけになっている関係もありますので、その方々以外の方ということで下記にありますような団体、金融機関の方々に対して状況等の随時報告を行い、ご意見を承りながらこのチェックリストを幅広く金融機関の方にご利用いただくよう、事務局のほうで務めております。あと資料には記載はございませんが、ゆうちょ銀行様や国際銀行協会様にも今週事務局のほうでご訪問させていただいて、必要な情報提供等をさせていただく予定となっております。

項番３の今後の予定ですが、まだチェックリスト完成まではたどり着いておりませんので、完成に向けて鋭意作業をさせていただこうと考えております。簡単ですけれども以上となります。

○岩原座長　ありがとうございました。ただいまのご説明についてご質問等ございますでしょうか。梅谷さん、どうぞ。

○梅谷委員　アマゾン梅谷です。ありがとうございます。今のAPIワーキンググループに関して質問といいますか、教えていただきたいというお願いになります。議事１のページ83の青字の新しい箇所です。下部にチェックリストのイメージということで図を示していただいていると思いますが、セキュリティ目標や強度、手法例などから、大分テクニカルな内容も入っているのかなというふうに推測できますが、全てとはいわないまでも何例か具体例を示していただけると、どのように検討がされているか分かりますし、クラウド事業者として、どういった用意ができるのかなどの検討がしやすくなると思います。どこかのタイミングで１～２例、何か特徴的なものがあれば具体例を開示していただけませんでしょうか。

○岩原座長　大澤さん。

○大澤主任研究員　ありがとうございました。現状いろいろな委員の方々から情報提供をいただいておりまして、今事務局のほうで整理しております。それをもう一度委員の方

に見ていただいて確認をこれから行いますので、適切なタイミングで本検討会の委員の方にも一部ご確認いただこうと思います。ありがとうございます。

○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。神田さん、どうぞ。

○神田オブザーバー　金融庁の神田です。本日この有識者検討会の報告書の案ということで先ほどご説明をいただきました。本文が約40ページ、それから資料編も合わせて80ページを超える非常に大部の報告書ということですが、非常に内容の濃い、FinTechに関する安全対策のあり方だけではなくて、クラウドサービスの補足につきましても非常に踏み込んだ先進的な内容なのではないかと評価をしております。私は海外に出張で行く機会もあって、現地当局の人などとも意見交換をしていますけれども、海外のオープンAPIの取組みなんかの話を聞きますと、非常に苦労されています。何に苦労しているかというと、金融機関とFinTech企業とが接続をしていくという義務づけなども、海外では欧州などでなされていこうとしていますけれども、金融機関側として義務づけられてもなかなかFinTech企業のセキュリティのレベルですとか、あるいはどういうFinTech企業と何をチェックして接続をしていけばいいのかというのが、実務的なところがなかなかうまく取り決められず、その中で両者が疑心暗鬼のような形になって取組みが進まない、というような状況もあると聞いています。

そういう意味では日本は金融機関、FinTech企業、ITベンダー、関連する当局も含めて、オープンAPIの議論を進めてきまして、また法制面につきましても現在国会で議論されていますけれども、成立すれば、法制面それから実務面合わせて体制が整い、また関係者が、その間非常に密にコミュニケーションをとって信頼感も生まれてきているという意味で、非常に日本としては世界に誇っていける、世界にアピールしていけるFinTech企業と金融機関等の結びつきのあり方というのが今構築されつつある、というふうに考えています。

このFISCの今回の報告書についても、安全対策についての考え方をしっかりと示して、それに基づいて金融機関とFinTech企業が結びついていくというところを根本的な考え方からしっかりと書き起こしたものになっているのではないか、というふうに考えています。こういう日本の取組みを国内はもちろんですけれども、海外に向けてもしっかりと発信し

ていき、海外からの議論、あるいは日本の取組みを海外に対してしっかりと示していっていただきたいというのが、私どもとしてももう１つ事務局の皆さんにお願いしたいことになります。

そういう意味で、どういう形で国内に周知、あるいは海外に対してこの報告書をアピールしていくのかということについても、もう一段ご検討いただければありがたい、というふうに考えております。以上です。

○岩原座長　事務局から何かございますでしょうか。

○小林企画部長　どうもありがとうございます。後ほど申し上げますが、本日の内容はこれから報告書のまとめの作業に入っていきます。完成の暁には国内ではプレスリリースを速やかに行うとともに、全国への周知のための説明会の開催を予定しており、また、海外への周知についても速やかに英訳版を作成する予定です。本報告書は直前の外部委託に関する有識者検討会の考え方を踏襲しており、外部委託報告書の内容についてはこの４月に英訳版を公表しています。こうした動きに加え、広報活動には引き続き工夫を凝らしていきたいと考えております。以上、コメントさせていただきます。

○岩原座長　ほかに何かご発言等ございますでしょうか。よろしゅうございますか。

３．【事務連絡】

○岩原座長　それでは、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　３点ございます。１点目ですが、本日ご説明した報告書の案につきまして、追加のご意見等がございましたら、議事次第Ⅴにあります通り、１週間後の５月22日月曜日夕方５時までに電子メールにて事務局までお送りください。

続きまして２点目は先ほど申し上げました通り、本日の検討内容及び事後意見を踏まえ、報告書の最終版を作成させていただく予定です。第６回終了後に速やかに報告書の内容を確定できますように、引き続きまた皆様のご協力をよろしくお願いいたします。

最後に３点目は、次回第６回の検討会のご案内です。最終回となりますが、６月13日火曜日、時間は同じく午後３時45分から予定しておりますのでよろしくお願いいたします。以上でございます。

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

それでは特にご意見ございませんようでしたら、これにて第５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。熱心なご議論をいただきまして、まことにありがとうございました。

以上