平成28年10月26日

公益財団法人　金融情報システムセンター

第１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28年10月5日（水）15:30～17:30

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	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
	久井 敏次	東京海上日動火災保険株式会社 理事 IT 企画部長
	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
	今井 博善	(代理出席)株式会社 NTT データ 第四金融事業本部　企画部 ビジネス企画担当課長

	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
	内田 克平	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 金融インダストリー担当部長
	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 システムモニタリング長　主任統括検査官
	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
	大森 一顕	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長
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
	中山　靖司	調査部　部長
	西村　敏信	監査安全部　部長

Ⅳ　FISC　渡辺理事長　挨拶

○渡辺理事長　公益財団法人金融情報システムセンター理事長の渡辺でございます。

委員の皆様にはご多忙の中、本検討会の委員をお引き受けいただき、心より御礼申し上げます。

近年 FinTech と称されます IT を活用した金融サービスにつきまして、利用を促進すべきであるという声が社会的に高まっておりまして、金融機関にとどまらず、金融庁、全国銀行協会等におきましても、FinTech に関するさまざまな取組みが進められていると承知しております。

そうした中で金融機関の金融情報システムに関する安全対策を主な仕事としております当センターにおきましても、それらの取組みと歩調を合わせまして、FinTech に関する安全対策のあり方を明確にする必要があるのではないかと考えまして、本有識者検討会を立ち上げることにいたしました。

既に当センターでは、本年６月に終了しました、同じ岩原座長にお願いをした外部委託に関する有識者検討会におきまして、リスクベースアプローチや IT ガバナンスという新たな安全対策の枠組みを提案いただいており、金融情報システムにおける安全対策の考え方を、欧米先進国の動向等を踏まえまして、大きく舵を切った、ないしは前進させたというふうに考えているところであります。

このようなある意味の準備作業がちょうど出来たところでございまして、このタイミングで新しいリスクベースアプローチや IT ガバナンスといった成果を踏まえまして、我が国金融機関における FinTech への取組みの安全性の側面について皆様にご議論いただいて、どのようなやり方で安全対策を講じていったらいいかということを明確かつ具体的なご指針をお示しいただきたいということが本検討会にお願いする私どもの基本的な考え方でございます。

検討にあたりましては、我が国金融機関がシステムの安全性を確保するということが第一でありますけれども、同時に顧客のニーズに適応してイノベーションの成果を最大限享受するということ、即ち、安全性とイノベーションというのは、短絡的にいえば、トレードオフの関係というふうに考えられるかもしれませんが、できるだけ目一杯両立し、安全で、イノベーティブな業務が金融機関によって展開されるということを目指してご議論いただければというふうに考えております。

なお、FISC といたしましては、既にいただいております外部委託の報告書の内容に加えまして、今般ご検討いただきます FinTech の報告を合わせて、それらをもとにこの検討会終了後、安全対策基準の改訂作業に鋭意取り組んでいきたいというふうに考えております。

以上、簡単でございますけれども、開会に先立ちまして私のご挨拶とさせていただきます。

Ⅴ　議事内容

１.【議事１】金融機関におけるFinTechに関する有識者検討会規則について説明

○岩原座長

座長を務めさせていただきます岩原でございます。どうかよろしくお願いします。

それでは、本日１つ目の議事に移らせていただきます。本検討会の議事運営規則について、FISCの水野総務部長よりご説明をお願いいたします。

○水野部長

それではお手元、左手議事１と書いております、有識者検討会規則をごらんください。この規則は私どもが主催しております各種委員会並びに有識者検討会の規則、それに中央官庁でお作りになっておられます、各種委員会の規則等を参照して作成しているものでございます。

まず第１条でございますが、ここでは総則的な規定をさせていただいておりまして、位置づけ並びに目的を規定させていただいております。

第２条では、本委員会の構成についての規定でございまして、具体的には委員、座長、座長代理、オブザーバーの各々を規定させていただいております。

また、委員及びオブザーバーご本人がご出席できない場合の代理人や帯同される同行者について定めをしております。また、委員及び座長の委嘱、オブザーバーの依頼につきましては、理事長によるものでございます。

また、座長代理につきましては、万が一座長がご出席できない場合に備えまして、座長のご指名によるものとしてございます。

続きまして、３番目の第３条でございます。検討会の運営にかかわる規定でございます。第１項及び第２項では、検討会は座長より招集いただきまして、検討会の議長を座長にお願いしております。

第３項は、いわゆる参考人についての定めでございます。

第４項は議事資料についての規定でございまして、今後使います資料の記載内容に関して機密性が高いということで座長にご判断いただいた場合、また、同様の事由等によりまして資料をご提供いただく方からお申出があった場合には、傍聴の方への資料の配付制限や席上回収をさせていただく場合があることについて、規定してございます。したがいまして資料をご提出いただく方におかれましては、配付範囲の限定や席上回収の必要性がある場合については、その旨を事前にお申出いただければと思います。

第５項については議事録の規定でございます。

第６項ですが、先ほどございました当センターの会員ホームページで会員向けに情報開示をすることを規定してございます。資料につきましては、先ほどの第４項でございました配付範囲の限定とか、席上回収となった制限のないものを掲載させていただく予定でございます。

また、議事録につきましては機密度に応じまして、個別金融機関を特定できないように情報保護を講じた上で掲載させていただきます。これを踏まえまして、委員、オブザーバー、資料提供者の皆様におかれましては、議事録の調整段階におきまして必要に応じて黒塗り等の措置が必要な場合については、その旨お申出いただければと思います。

第７項になります。最終成果物の文書である報告書等の今後の開示についての規定でございまして、例えば報告書を冊子あるいはホームページ等に情報保護を講じた上で、公衆に開示する旨規定させていただいております。

第４条は謝礼についての規定でございまして、第５条は傍聴される方についての規定をさせていただいております。

第６条は機密保持の内容でございまして、傍聴の方を含めまして、検討会の参加者全員におかれましては、守秘に留意することを定めておりますので、何とぞどうぞよろしくお願いいたします。

第７条は最後のクロージングに向けてのプロセスについてでございます。検討会での議論が熟したという形で考えられる時に、座長にこれを判断いただきまして、報告書に取りまとめ、検討会の協議を経まして、最終報告をさせていただくという手順を踏む予定でご

ざいます。

最後、第８条でございますが、こちらは本規則で規定していない事項等が必要と認められた場合に、その場合において座長にご判断いただきますこと、それからまた本検討会の事務局については、当センターの企画部が務める旨規定させていただいております。私からの説明は以上になります。

○岩原座長

どうもありがとうございます。ただいまのご説明に対して何かご質問ございますか。よろしゅうございますでしょうか。

それでは、特にご質問はないようでございますので、ただいまよりこの規則に則って議事運営を進めさせていただきたいと存じます。

それから、運営規則の第２条第４号に沿いまして、万が一私が会議に参加できない場合に備えまして座長代理を渕崎委員にお願いしておりますので、その点、ご了承いただきたいと存じます。どうかよろしくお願いします。

２.【議事２】プレゼン

「国内外のFinTechに関する動向」（荻生委員）

「外部委託検討会報告書概要」（事務局）

○岩原座長

それでは、議事の２つ目のプレゼンテーションに移りたいと思います。初めに荻生委員より国内外のFinTechに関する動向についてご発表をいただきたいと思います。

○荻生委員

デロイトトーマツコンサルティングの荻生と申します。よろしくお願いいたします。

本日は、FinTech の世界的な動向、あとは一部、日本の動向というところもありますので、そちらについてお話をさせていただければと思っております。

お手元の資料は、「FinTech の概況」という議事２－１の資料を見ながらお話をさせていただければと思っております。１枚おめくりいただきまして、まず初めに「FinTech の発展の経緯」に関してお話をさせていただきます。FinTech の発展の経緯においては、そ

もそもなぜ金融業で、FinTech が発展してきたのかということについてお話しさせていただきます。

まず直近で顧客ニーズがどういう状況にあるのかというと、例えばモバイルを皆さんがかなり持たれるようになって、それによってインターネットに対するアクセスもしくはそれ以外の各種サービスに対するアクセスが高まり、それにつれニーズが高まってきました。

一方で、金融サービスはこれに対してどう追随しているのかというと、各金融機関が努力して取り組んではいますが、１つには規制が障害になっています。また一方、金融機関は巨大なシステムを作っており、その巨大なシステムに数々のセキュリティの対策を施しているので、新しい外部のサービスを簡単に受け入れられるような、もしくは新しいサービスを簡単に導入できるような仕組みにはなっていないため、徐々にニーズとサービスのギャップが広まってきています。そのギャップの広がりに対してサービスを提供しているのが、FinTech の企業であるという認識をしています。

３ページ目ですが、歴史的なところをもうちょっと深掘りしてみます。このニーズと実際のサービスの広がりは何に端を発しているかというと、もちろん時代の流れというところもありますが、一番大きなインパクトがあったのが、リーマンショックだと思っています。リーマンショックによって何が起こったかというと、まず１つは信用収縮が起こって、貸し渋り、貸し剥がしが起こりました。かつ、それに伴って各金融機関は個々の財務体質が悪くなったため、不採算なサービスもしくは会社を切り離し始めてしまいました。結果として顧客へのサービスについては、富裕層に対してのサービスはきちんと提供していたのですが、中間層未満へのサービスがだんだん行き届かなくなってきました。ここに対してFinTech のサービスというものが導入され、広まっていったと考えています。

各国の状況は実際には違いまして、イギリス、アメリカといったところはこのようにリーマンショックの影響を大きく受けましたが、日本はリーマンショックの直接的な影響はそこまではありませんでした。もちろん日本にも影響はあったものの、政府系金融機関が支援したり入ったり、もしくは日本の企業もサービスをあまり縮小しなかったという実態としてあります。結果として、日本の FinTech のサービスの広がりというのは、欧米に比べると劣ってしまいました。

もう１つは、FinTech という、このサービスの担い手の供給の状況が違いました。欧米は大量のリストラを行い、そのリストラによって金融機関のビジネスを担当している方、もしくは技術を担当している方が市場に溢れ出てきました。そういった方たちが、

FinTech の会社を作っていきました。一方で、日本でもリストラは一部で行われましたが、大量にリストラを行ったというところはあまりないため、人材の供給が芳しくありませんでした。これらにより、FinTech のサービスの普及、人材の供給が欧米の状況と日本の状況では異なっていると認識をしています。

FinTech の成功要因は一体どこにあるのかということが、次のページになります。FinTech の成功要因というものは、まず１つ競争力の源泉として社会課題を解決するものなのかどうか、規制に守られてなかなかできないことが、どうしたらできるようになるのか、それでよりよいサービスを提供していけるのかどうかといったところが、まず社会課題解決の視点です。

革新的なビジネスモデルというのは、通常金融サービスは手数料によって成り立っていることが多いです。ですが、FinTech の会社というのは少なくともサービス導入時、顧客が入会し、サービスを開始する時は、無料にしていることが多い傾向があります。

もう１つが飛躍的顧客経験で、例えば、銀行でインターネットバンキングのサービスを利用したいというと、かなりの手続きを経ないといけなません。FinTech の会社ではできるだけ少ない手間で口座が開設できるよう、意図しているところがあります。

一方、技術としてどういうものを使っているのかというと、必ずしも新しい技術だけを使っているわけではなく、旧来の技術を組み合わせて効率的に仕組みを作っているということが１つ挙げられます。これにより大手金融機関がサービスを提供するよりも、同じサービスを安価で提供できることが特徴になっております。

次の５ページ目になりますが、FinTech の世界的な動向は、World Economic Forum の中で述べられており、６つの金融サービスに対して大きな変革が起こると言われています。この中で決済、市場予測、資産管理、資本調達、融資、保険という領域があり、中でも大きな激震が走るのはまず決済です。決済ではキャッシュレス化の波、もしくは新たな決済手段として、仮想通貨が登場しています。

資産管理に関しては、PFM、ロボアドバイザーが、普通はやりにくいはずの資産管理を劇的にやり易くしています。

あとは資本調達のクラウドファンディング、もしくは新しい融資の手法を使った P2P レンディングといったようなものがございます。

こちらに対し、実際にどういう技術的要素がこれを支えているのかというと、サービス、もしくは会社によってさまざまではありますが、１つはクラウドコンピューティングがあ

ります。クラウド自体は小さく始めて徐々に大きくできるという特徴がありますし、また一方、FinTech の会社はどちらかというと、アプリケーションに寄った人員構成をしているということがあると思います。世の中ではシステム基盤に詳しい方は中々いませんし、クラウドコンピューティングは安く始められるといったこともありますので、クラウドコンピューティングを使用するケースが多いです。

あと、データを扱うのが FinTech の特徴としてあります。FinTech の会社はデータを分析しそれによってマーケティングなどを行うといった特徴がありますので、ビッグデータ、もしくはそのデータを供給する IoT、もしくはこのデータをハンドリングするために一つ一つ手で回すのではなくて、人工知能を使ったオートメーションを行います。また、ブロックチェーンを使ってシステム自体を安く作り上げたりもしますし、もしくはウェアラブルのように手ぶらで、特に決済中心だと思いますが、いろいろなサービスを提供できるような技術が FinTech を支えているという認識をしております。

３つほど例を挙げさせていただきます。まず１つ決済では Apple Pay があります。Apple Pay は皆さんご存知かと思いますが、iPhone を使った決済の仕組みです。iPhone にクレジットカードを登録します。クレジットカードを登録するのですが、クレジットカードの番号をそのまま登録するわけではなく、トークナイゼーションといってクレジットカード番号ではない別番号としてそれを保存してそれで決済を行えるようになっています。これによってクレジットカード番号が流出しないというメリットがあります。もちろんモバイルですので普通にカードを出すわけではなく、自分で店舗の端末に対して iPhone をかざして、かつ指紋認証が iPhone ではできますので、その指紋認証を使って決済できるような仕組みになっています。

日本においてはこれまでおサイフケータイがあって、Suica、もしくは WAON、Edy に対応しています。Apple Pay が今月日本でも登場し、直近では Suica と iD と QUICPay が Apple Pay へ対応されるところです。

続きまして７ページ目になりますが、ビットコインです。ビットコインは何なのかというと、ビットコインは仮想通貨です。仮想通貨は何かと言われると、これはなかなか説明が難しいのですが、仮想通貨自体にはもともとの価値はない。ただ、ビットコイン自体に価値があることを認める方たちによって、価値が創造されている、というものになっています。ビットコイン自体は電子データでそれを送り合えるという特徴があります。

仮想通貨の特徴の１つは匿名性が高いことです。匿名性が高いとその代わりにマネーロ

ンダリングに利用されるということがあります。なぜかというと、実際に仮想通貨の世界では、ビットコインを送り合っているのを見ることができます。ただ見えるのはどのアドレスからどのアドレスに送られたか、これだけです。ですので、そのアドレスを誰が持っているかは分からないのです。ただし、今年改正された資金決済法で規定があり、アドレスを管理する販売所、取引所が本人確認の任を負うということになっていますので、アドレスと人がきちんと結びつくので、マネーロンダリングに利用されなくなっていく見込みです。

もう１つの大きな特徴というのは経済性が高いというところです。例えばどういうことかというと、送る時の手数料が極めて安いです。例えば、通常、数百万円をアメリカに送るとなると、手数料は数万円必ず発生します。ただ、実際ビットコインで送る場合、数百万円送っても大体 100 円するかしないかぐらいです。そして手数料は自分で決められます。最終的にそれが取引されるかどうかということは別なのですが、金額が高ければ高いほど早く決済されるといった仕組みになっています。ですので、極めて安価な手数料で海外に対してお金を送ることができるのが、ビットコインの特徴になっています。

次の８ページ目が新たな融資手法です。新たな融資手法というのはどこが新しいかと言うと、まず１つは使う情報が違います。通常、金融機関において融資する場合、個人、法人がありますが、個人に関しては外部信用機関の外部信用情報、もしくは内部信用情報を使って与信をします。一方、法人に関して、その会社の財務諸表等々を利用します。財務諸表に関しても、過去３年間というのが基本かと思います。

ただ、この新しい融資というのは使う情報が異なっていて、例えば自分たちが EC サイトを運営しているのであれば、その取引データを利用したり、もしくは会計データを使ったりします。もしくは PFM では個人がどれくらい預金を持っている、資産を持っているといったような情報から予測します。他方、特異な例としては Facebook のような SNS を使って融資をするのが１つの特徴です。

もう１つは資金の出し手が異なります。通常金融機関が資金を融資する場合には、必ず自分たちの、例えば銀行であれば預金を使って融資します。一方で、新しい融資では民間から募集するという形を取り、実際に資金の出し手が必ずしもその運営会社だけではなくて一般の法人もしくは個人から募集するという特徴があります。ただ、これを進めるにあたって、国内の法律では貸金業法の問題がありまして、海外で行える融資と日本で行える融資は、ギャップがあるという認識です。

最後に９ページ目になりますが、今後FinTechをどう伸ばしていくのか、活かしていくのかに関しては、FinTechの企業だけで勝手に伸びていくものではないと思っています。もちろん、FinTechのサービスを利用する金融機関の方々もいますし、あとはサポートするIT関係の会社の方もいますが、それ以外にアクセラレータと言われる、ビジネス、システム、もしくは法律に関して仲立ちになって、いろいろと調整役をする方たちがいることでFinTechは伸びていくと考えらえます。実際にこのようなモデルは、イギリスでもアメリカでも同様にありまして、日本ではこのアクセラレータのところがあまりうまくいっていないという状況があります。ただ、このアクセラレータが、全てのプレーヤーの仲立ちになってサービスが提供できるようになれば、今後、日本のFinTechは伸びていくであろうという認識を持っています。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。ただいまのご発表に対して何かご質問ございますでしょうか。いかがでしょうか、特にございませんか。

それでは、ないようでございますので、どうも荻生委員、ありがとうございました。

続きまして、FISCの藤永企画部次長より「外部委託検討会報告書の概要」についてのご発表をお願いします。

○藤永次長

FISC 企画部の藤永です。私のほうからは先般終了しました外部委託検討会報告書の概要をご説明させていただきます。お手元の資料でいいますと、右上に議事２－２というふうに書かれている A4 の資料でございます。

なぜこれをあらかじめ説明するのかといいますと、先ほど理事長の渡辺から話がありましたとおり、今回 FinTech を検討するにあたって、その外部委託の成果を踏まえて、ご検討をお願いしたいということによります。委員の中に外部委託の時から引き続き、お願いさせていただいている方もいらっしゃいますし、そうでいらっしゃらない方もおられますので、概略を私のほうからご説明します。

資料１ページをめくっていただきまして、「有識者検討会」とはという部分でございます。先ほどの運営規則にありましたが、当センターの理事長の諮問機関としてこの場を設けさせていただいているということです。

過去、サイバー攻撃対応、クラウド利用と有識者検討会を行ってまいりまして、ちょうど昨年の 10 月から約半年ほどをかけまして外部委託の検討会をやっております。座長につきましては岩原先生、座長代理は渕崎様という形で、この場と同じような委員構成で行われております。

報告書の内容につきましては、席上でお配りしています。これはお持ち帰りいただいても構いません。あるいは FISC のホームページを通じて一般に広く内容を公開しております。

その中で今回、FinTech をご検討いただくにあたって関連の深いところに絞って、ご説明をご用意しています。その下の２ページのところですが、外部委託という問題につきましては必ずしもシステム部門だけでは解決できない問題が多いということで、経営層がどういうふうに関与するか。すなわち、IT ガバナンスの問題が重要であろうということで、IT ガバナンスについてご議論をいただいております。

２ページ目のところの「経営層の役割と責任」ということで、安全対策に係る重要事項の決定、あるいはその改善事項の決定という役割と責任を果たすことが必要であるということを改めてご提言をいただいています。多くの金融機関において既に中期計画等においてそうしたご検討、あるいは、経営層の関与が行われているものと承知しておりますが、それを改めて我々のほうで整理させていただいたというところでございます。

１枚めくっていただきまして３ページでございます。IT ガバナンスと非常に密接な関係があるのが、一般に IT マネジメントと呼ばれるものです。要は経営層が決定された決定事項に従って、実際業務を執行する役割を担っている組織、あるいは担当の方のことをいいます。ここでは、例として、情報システムの安全対策に携わる関係者として IT マネジメントにかかわる方々を図式しております。

管理者というふうに書いてございますのは、例えばシステムの部長がお務めの会社もあるでしょうし、あるいは CIO ということで役員がお務めの場合もあるかと思いますが、そういう方を総称して、機能としての管理者が経営層と現場の橋渡しをされるという図式でございます。

金融機関の内部においては、非常に多くの方々が安全対策には携わっていらっしゃるのですが、当然その中の１つとして外部委託先の皆様も大きな役割を果たされているということでございます。あとはこの提言内容で特徴的なのがユーザーの役割ということで、ここでいうユーザーというのは、システムを利用されるユーザーではございませんで、一般

には企画部門あるいは業務部門という名称で呼ばれている組織でございます。そうした方々も、システムの安全対策上の役割を担われているということを明確に提言いただいているところでございます。

その役割には、３点ございまして、１点目がビジネスモデルを企画される役割を担われているユーザーにおいても安全対策に配慮することが必要であるということ。２点目がそうして作られたビジネスモデルを担うシステムについては、その投資効果の達成の責任をユーザーが負われているということ。３点目がそうした業務に関する要件をシステムに対して提示するという役割を担われているという、この３点を主な役割として安全対策上の役割としてご提言いただいているという、そうしたところが特徴的でございます。

そうした IT ガバナンス、IT マネジメントのご検討を踏まえまして、さらにより深いといいますか、根本的な部分についてもご議論をいただいているのが、その次の４ページのスライドでございます。これが通称リスクベースアプローチということで、今回の外部委託の検討の大きな柱の１つとなっております。

ではなぜそういうものを検討したのかというところが４ページに書かれているところですが、そもそも FISC の大きな役割の１つとして、安対基準を会員の皆様にご提供しているということがございます。そもそも安対基準の意義が何であるかというところを検討会では紐解いていただきまして、ここに書いてございますとおり、金融機関の皆様の自己責任と自主性尊重というのが、まず大原則としてある。ただ、金融業務を担われている皆様の公共性と社会的責任の大きさに鑑みて、その部分について対応を補完するものとして作られたのが安対基準であるということで、これは 30 年前から継続的にそういう位置づけであるということです。

ただ、30 年経つうちに問題が生じているというのが、その下のところでございまして、何かといいますと、公共性と社会的責任を果たすにあたって取り組まれるべき対象であるシステム以外のシステム、それが非常に増えてくる中で、そうした重要なシステム以外のシステムについて、金融機関としてどういう安全対策をとるべきかということについて、あまり明確にお示ししてこなかった。それによって、不確実性を含む環境となっていると書いてありますが、要は一律に過度な安全対策を招来してもやむを得ないような内容になっているということが、安対基準策定後 30 年経った現時点での評価です。それを踏まえて、改めて安全対策基準の考え方というものを整理したということになります。

１ページめくっていただきまして５ページですが、過去を振り返ったのと同時に、海外

ではどういう取組みが行われているかというところを整理いただいています。これは皆様よくご承知のとおり、金融機関と監督当局等を含めたリスクベースアプローチという考え方が共通認識となっているということでございます。

１点だけこのスライドで言及させていただきたいのが、米国の OCC という監督当局があるのですが、そこに FISC としてヒアリングをした時の言葉としまして、「成文化するとそれが絶対的になり、本当はもっとよい方法があるかもしれないのに、それを見逃し、イノベーションが起きないという問題がある。そういうことを配慮しながら、我々もガイドラインを作っていく必要がある」ということでございます。

その下６ページ目のところでございますが、そうしたリスクベースアプローチのご検討を踏まえて、安全対策基準の前提となる原則というものをご提言いただきました。これが、我々が今後、安対基準を策定していくにあたっての大きな考え方の基となるものでございます。

４つほどございまして、１つ目が個々の情報システムのリスク特性に応じて安全対策の達成目標を金融機関の中で決められるべきであるということです。過度な安全対策といいますか、リスクをゼロにすることを追求するというのはなかなか難しいところがありますので、そういうリスクゼロを追求しないということを明確にいっているのが、基本原則の１です。

そうした達成目標と関係性が深いものとして、経営資源配分をシステムに対してどう行うかということにつきましては、リスクが顕在化する前の事前の軽減策にコストをかけるだけでなく、事後の対策にもコストをかけるという考え方があるということと、最終的には企業価値の最大化を目指して、安全対策であるからといって優先的にシステム資源を配分するというものではないということを、これも改めて文字にして原則２としております。

原則３ですが、そうした前提においては、金融機関の皆様というのは、安全対策というのは独自に決定することが可能である。自己責任原則と自主性の尊重ということではないかと思っております。

ただ、基本原則４ということで、金融業務には固有の特性があるということで、そうした固有の特性があるがゆえに社会的なルールが必要であるということを提言しています。そうした固有の性質というものを表現する言葉として、システムの外部性と保有情報の機微性という２つの性質を提言いただいているということです。そうした外部性と機微性という性質を有する情報システムに対して作られているのが安対基準であるということでご

ざいます。

その次のスライド７ページ目ですが、外部性と機微性と、非常に難しい言葉でございますので、もう少し文字にしているということです。ここの説明は割愛させていただきます。後でお読みいただければと思います。

そうしたことを踏まえて８ページ目、これが非常に重要なところでございます。そうした今までの原則、リスクベースアプローチを踏まえた原則に従って、安対基準の適用方法というのが、今後、将来に向けてどういうふうになっていくかというところを整理しています。左側の十全なリスクベースアプローチでは、今基本原則１～４とお話ししたものをそのまま素直に絵にすると、重大な外部性と情報の機微性を有するシステムについては、安対基準が対象となる。上の２つのマルでございます。ここに適用されるルールは右側の四角で、安対基準の語尾というふうに書いてございますが、ご存じない方もいらっしゃるかもしれませんが、安対基準というのは語尾によって適用の強度というものを書き分けております。そういう意味では、強度が一番強いのは「望ましい」というふうに語尾がなっているものですが、その次が「すること」「必要である」という語尾でございます。それがまさに外部性と機微性を有するシステムに適用されるということを表現しております。かつ、それ以外のシステムも独自に安全対策の達成目標を設定し得るということでございます。

ただ、そうはいっても必ずしもそういう独自に設定することに、悩まれる金融機関の皆様も実情としてはあるということは承知しておりますので、我々の役割としてはそれに加えて、簡易なリスクベースアプローチということもあるのではないかと。要はこれが何をいっているかといいますと、重要な情報システム以外のシステムに対する基準も作る必要があるのではないかということでございます。それが右側のイ、ロ、ハのうちのロというところで、語尾が「可能である」という基準でございます。

これはクラウドの時から出来た簡易なリスク策というふうに通称されている基準でございます。要は、このリスクの程度に応じて必要最低限このぐらいまでやっておけばいいのではないかというルールです。そうしたルールがございませんと、重要でないシステムについても重要なシステム向けの基準が適用されて上振れしてしまうということがおきる。そういうことがないようにということで、「可能である」基準というのを、クラウドの時以来 FISC としては作ってきている。それを引き続き拡張していこうという考え方でございます。

その次のスライド９ページは、今ご説明した考え方を横にしてフローチャートに書き直したものでございます。詳細は先ほどと同じですが、１つだけお話ししておきたいのは、安全対策基準の対象という一番左側でございますが、これは実は 30 年前から金融機関等のコンピューターシステムを対象としているということです。これはそういう意味では所与の前提としてある意味 30 年前から取り扱ってきているということで、外部委託の検討の中には明確には書かれていませんが、このフローチャート上はそういう形で入れさせていただいているというところでございます。

その下の外部委託における管理プロセス、あるいはその次のリスク管理策というのは、以上の IT ガバナンスとリスクベースアプローチを踏まえて、個別に外部委託はどのようにあるべきかということをご提言している中身になっておりますので、説明は割愛させていただきたいと思いますが、１点だけいいますと、11 ページのところで、運用と開発はリスクの程度が違うということで「○」と「△」を書き分けているということでございます。要は開発時には何らかの問題が発生したとしても、金融機関の内部にその影響は留まるということで、運用とは性質が違うということで書き分けているということは１点ご説明させていただきます。

その下の 12 ページですが、今後の安対基準等改訂の考え方としましては、やはりかなり今回大規模な改訂といいますか、考え方の変更を行っていますので、この改訂後の安対基準、これから FISC として取り組んでいきますが、それについては大きな変更を伴います。その変更自体がリスクやコストを生じるものであれば、やはりシステムの更改時や新システム導入時にそうした大きな作業を行えるタイミングに、新しい安対基準に移行したほうがよいのではないかということがいわれています。

もう１点が正にこの検討会との関連でございまして、先ほど理事長よりお話しさせていただきましたとおり、この検討会の検討結果を待って、安対基準の改訂に着手するということを考えてございます。私の説明は以上になります。

○岩原座長

どうもありがとうございました。

ただいまのご報告について、何かご質問ございますでしょうか。よろしいですか。ご質問等ございませんでしょうか。

それではないようでございますので、どうも藤永次長、ありがとうございました。

３．【議事３】論点メモ説明

○岩原座長

続きまして、議事の３つ目は論点メモのご説明でございます。引き続き、FISCの藤永企画部次長よりお願いいたします。

○藤永次長

では続きまして、本日の主たるご検討いただきたい内容のご説明に移らせていただきたいと思います。クリップ止めにしております左に議事３と書かれている資料をご用意ください。

本検討会では、FinTech に関する安全対策のあり方を最終的にはご提言いただければと思っているのですが、その安全対策のあり方を検討いただくにあたり、まずその検討をどういうふうに行うかということが、先ほど荻生委員からもお話がありましたとおり、多岐にわたる FinTech については重要ではないかと思っております。ですので今回ご用意させていただきましたのは、「本検討会として FinTech に関してどのような検討を行うことが適切であるか」という、ここに主論点を書いてございますが、この内容について事務局のほうで資料を用意させていただいているという形になります。

論点に係る原案の構成としまして、大きなご説明の流れとしましては、１つ目は検討の手順でございます。２つ目はその手順に従って、まずは安対基準の対象となる情報システムの判別基準、手順の第２としましては、重要な情報システム、先ほどご説明しました機微性と外部性を有する情報システムで利用される FinTech の取扱い、その次が手順の第３としまして、FinTech に関する安全対策のあり方を検討するにあたっての前提ということで、大きく２点、１点目は従来の安対基準で想定されていなかった事項というのがあるということ。もう１点目が、本検討会において前提とすべき、業務タイプ別類型といっていますが、どういうビジネスモデルを前提にご議論いただくのがいいのか。ビジネスモデルが多様でございますので、いろんな方々が、いろんな前提が異なるものをベースにご議論いただくのはやはり難しいということで、ある程度議論のベースをご用意しているということでございます。最後が全銀協で検討されています、オープン API との関係ということでございます。以上のような順番でご説明させていただきます。

裏面のほうに移りまして、別紙１というのがその主たる原案でございます。別紙２は別紙１の内容を A3 用紙１枚で概観しているものです。これはご参考でお付けしています。別紙３というのは最後にご説明しますが、今後の検討の進め方について、案をお持ちしていますのでご意見をいただければと思っております。

それでは、早速別紙１についてご説明をさせていただきます。「金融機関における FinTech に関する安全対策検討の在り方」ということでございます。先ほど来お話がありましたとおり、近年金融機関、業界団体及び監督当局等において、FinTech と総称される IT を活用した革新的な金融サービスへの取組みが急速に活発化しているということでございます。脚注の１でございまして、我々のほうで FinTech に関するプレスリリースの件数を調べたところ、対前年同期比で約７倍に増加しているというところでございます。あとは金融庁を初めとして、さまざまな団体で取組みがされているというのは、皆様よくご承知のとおりだと思います。

こうした取組みの活発化の結果として、今後多岐にわたる FinTech の出現が予想される中、先ほど理事長の渡辺からお話しましたとおり、我々も何らかの役割を果たすということが、この場で皆様にご議論いただきたいところでございます。

まず、手順ですが、荻生委員から非常に大きな視点でプレゼンいただきましたが、やはり FinTech と総称される金融サービスに係る諸業務というのは、非常に多岐にわたるということでございます。一方、先ほど私のほうからご説明しましたとおり、安対基準の対象として従来から前提としているものがあります。ですので、この検討会でご議論いただくにあたって、どういう FinTech を対象とするかということをまず整理する必要があるということが、１点目でございます。

その次に、安対基準の対象となる FinTech につきましては、まずは重要な情報システムについてどうするかということでございます。ここについては、高い安対基準の適用を求めることになるのですが、やはり FinTech に関していいますと、特にテクノロジー的な側面において、やはり変化が激しいということで、従来の安対基準で前提とされていない新たな性質を有しているものが、まずは注目されるのではないかということで、そうしたテクノロジー的な側面における FinTech については、高い安対基準で何らかの検討の俎上に乗るのではないかということでございます。

一方、重要な情報システム以外の情報システム、一般の情報システムというふうに取り扱おうとしていますが、そこについては十全なリスクベースアプローチを採用する金融機

関においては独自に決めていただけるというのは、これも先ほどお話ししたとおりです。ただ、一方、簡易なリスクベースアプローチを採用するといいますか、ご利用される金融機関においては、やはり必要最低限の安対基準が定められていれば、それをご利用いただくということになるのですが、クラウドの時、あるいは外部委託を通じて順次今必要最低限の安対基準を作っている中でございまして、必ずしも十分ではないのではないか。特にFinTech 業務を担う情報システムにおいては、そうした必要最低限の安対基準の前提となる簡易なリスク策を必要とされている環境にあるのではないかと考えています。これは「安対基準の不確実性を低減する必要がある」という言葉で１ページの下のところにご説明させていただいております。

次のページに移りまして、そうしたことから、今回は冒頭ご説明しましたとおり、従来の安対基準で必ずしも想定されていなかった事項を明らかにするとともに、検討をするにあたっての前提を整理させていただいた上で、２回目以降、それを踏まえて安全対策のあり方及びリスク管理策についてご検討いただきたいということでございます。

まず検討の手順の第１ということで、安対基準の対象となる情報システムは何であるかということでございます。安対基準は 30 年以上前に策定された初版から一貫して金融機関等のコンピューターシステムを対象としています。では、金融機関等というのは何かということなのですが、脚注の３に記載していますとおり、初版以来の括弧のところですが、「金融」これは、預金等取扱金融機関ですが、「金融、保険、証券、クレジット等金融業務を営む業界の各社」というふうに表記をし、その前提で基準を策定してまいりました。

では、金融機関等のコンピューターシステムとは何であるかということでございます。これは２つほど要素があるかと思っていまして、１つが金融業務を担う情報システムであるということ。もう１つがそうした情報システムに対する安全対策について金融機関等に責任が生じる。そうした類の情報システムのことをいうのではないかということで、ここでは整理させていただいています。ですので、FinTech 業務を担う情報システムを安対基準で取り扱うにあたっても、この要件というのがまず前提になるのではないかというふうに思っています。

では、金融業務というのは何かということですが、金融機関等の業法が定められておりますが、そういうものに基づいて、金融機関等が顧客に対して提供している金融サービスに係る業務であるということでございます。安対基準においてもそうした顧客に対して提供する金融サービスに係る業務というものを対象にしてきているというところでございま

す。したがいまして、例えば、銀行法等の改正に伴いまして、電子商取引を行う事業者を銀行、あるいは銀行の持株会社の傘下で持ちうるようになりますが、そうした電子商取引業務を行う情報システムというのは、金融サービスに係る業務とは解されませんので、安対基準の対象とはならないということでございます。

「また」というところで金融機関等の内部のみで利用される情報システム、例えば人事給与システム、あるいは経営情報システム等は、もともと安対基準の対象とはならないというふうに考えております。これは脚注４でその理由を書いておりまして、FISC の安対基準の初版においては、先ほどお話ししましたとおり、金融機関とか顧客に提供するサービスに関連するシステムというのを前提にしていますということです。そうした意味で対象というふうに申し上げております。

ただ、対象外のものはどうなのかということにつきましては、例えば金融機関等の内部のみに利用されるシステムについても、安全対策上参考となる部分というのがあるのではないかということで、「本基準を適宜取り入れることとする」というふうにしております。「参考」というのが非常に難しい表現ではありますが、要は安対基準の対象となるもの、対象とならないものを峻別して基準の適用を考えることが、むしろ非効率になるような場合というのも個々の金融機関等の実情においてはあるかということがあります。そうした時には、例えば一体で安対基準を適用するというケースもあるのではないかということでございます。あるいは、安対基準の一部を部分的に適用することが、適当であるようなケースというのもあるのではないかと思います。そうした意味で、安対基準を参考として利用していただいている歴史があるということでございます。

あともう１つが金融機関の責任の話でございますが、金融機関等以外の事業者の方が、金融機関等あるいは金融機関等の顧客と何ら関係なく自らのサービス利用者のために行われている FinTech 業務というのもあると承知しています。これにつきましては、金融機関等に何ら安対基準上の責任は生じないということで、そもそも安対基準の対象とならないのではないかというふうに整理させていただいております。

ただ、論点１ということで、そうはいいましても、安対基準の対象外となる FinTech 業務というものにつきましても、利用者保護等の社会的観点から、やはり何らかの安全対策が必要であるということは否めないというふうに考えております。ですのでこの検討会としても、直接的には安対基準の対象とならない FinTech 業務に対しても、何らかの意見表明を行う必要はあるのではないでしょうかということで、これを論点１として、皆様

からご意見をいただきたいと思っております。

検討手順の第２番目、３ページでございます。重要な情報システムと FinTech の関係ということです。ここにつきましてテクノロジーというお話を先ほどさしあげましたが、例えばブロックチェーン技術や AI というのが重要な情報システムに適用されるということは十分考えられると思っております。ただ、これを検討するにあたっては、これらの要素技術を用いた業務の事例としてさまざまなユースケースがあるだろうということでございます。それぞれのユースケースに応じた技術的特性に着目して検討を進める必要があるということでございます。ただ、現状ではそうしたユースケースの出現が、安全対策について議論をするほど具体的には出現していないというふうに承知しておりまして、今回の検討会として取り上げるべきタイミングにはないのではないかと、ただそうしたユースケースの出現状況等を見ながら、FISC としても有識者検討会の中で取り上げていくべき時期ということを確定させていきたいというふうに考えております。

次に４ページでございます。ここからが重要な情報システム以外のシステム、要は一般の情報システムに関するお話でございます。それにつきましては、不確実性を低減するという観点からご意見をいただきたいと思っているのですが、まずは、そのご検討いただくための前提を委員の皆様でまず共有、共通認識、議論をいただく土台を作りたいというのが今回の目的です。それにあたっては、ここに書いてございますが、従来の安対基準で想定しなかったことが２つほどあるというふうに、我々事務方では思っております。１つ目が、FinTech 企業、今日も委員でいらっしゃっていますが、何らかの安全対策実施上の新たな関係者となるということが考えられるのではないかということでございます。では、従来の安対基準はどうだったかといいますと、安全対策実施上の関係者、先ほど IT ガバナンスでご説明した例示に登場する方々、そこで書いてありますとおり、金融機関の内部の方が中心。それ以外ですと、外部委託先として IT ベンダー、その金融機関と IT ベンダーの２者を念頭に置いてきたということでございます。

しかしながら、FinTech 業務を担われている企業は、IT ベンダーと類似の技術的な性質を有していらっしゃるということ、先ほど荻生委員からアプリケーションの部分と言われた部分だと思います。それだけではなくて、金融関連サービスといったビジネスモデルの企画実施等を行う、この業務的な性質というふうに称しておりますが、それも有していらっしゃるというふうに考えています。ここでいう業務的な性質というのは、先ほどお話ししたユーザーの役割ということで、外部委託の検討会で整理されたようなビジネスモデ

ルに関する安全対策上の役割というふうに理解しております。そうした技術的性質と業務的性質を併せ持たれているというような特徴があるというのを、FinTech 業務を担う企業の性質として、明確にここでは取り上げてはと思っています。

そうした FinTech 業務を担う企業の性質を特定した上で、金融機関、IT ベンダー、FinTech 企業の３者の関係をもとにご議論いただく前提となるモデルを後ほどご説明させていただきます。

それにあたっては、２者関係の基本的類型の考え方を今まで安対基準でどう取り扱ってきたのかというのを簡単に（※）でご紹介しています。右の図表１と併せて見ていただければいいのですが、単数の場合は、もうここは特段議論することはないのですが、複数の場合、特徴的な議論を今までしてまいっております。１つは金融機関が複数の場合、ここにつきましては共同センターとクラウドを取り上げております。共同センターというのは、安全対策等の資源が効率化でき、その効果が複数の金融機関に及ぶ、これは共同性という性質といっておりますが、その一方で、複数の金融機関の意思決定が単一の場合と同程度に迅速とは限らないという、そういう時間性の問題というものをはらむというふうに、既に外部委託の時に整理しております。

クラウドサービスについては、共同性を有しながらも、共同委託者が互いに独立しているということで意思決定の時間性の問題はないのですが、一方、安全対策上、データの所在地等、固有の統制方法に留意が必要となるということで、これもクラウドの有識者検討会でご議論をいただいているというところでございます。そういう議論を既に済ませているということです。

あと IT ベンダーが複数となる場合につきましては、正に委託先が複数になる場合は個々の単数の場合とそれぞれ変わらないのでしょうけれども、多段階にわたって再委託が及ぶような場合、ここにつきましては統制が及びにくくなるという固有の性質があるということでございまして、これも既に外部委託の検討会の中で取り上げて議論を済ませているというものでございます。その上で３者の関係というのを今回ご議論いただきたいと思っています。

２番目がその次の５ページの上です。「金融機関が必ずしも主導的立場とならない業務形態の登場」のことでございます。安対基準では自らの顧客に対して提供する金融サービスに係る業務を担う情報システムについては、金融機関に安全対策上の責任があるということを、そういう意味では当然の前提としていた。なぜならば、その金融サービスの内容

について金融機関が主導して全て決定しているということでございます。

一方、昨今の FinTech をめぐっては、例えば金融機関と顧客の間に介在する FinTech 企業が登場しているということでございます。この FinTech 企業のタイプにはいろいろあると想定されるということで、脚注の９のところで例えば一般的に広く公開されている金融機関のデータを利用されている業者、あるいは金融機関に対する顧客の決済指示を仲介する業者、これは今後登場される可能性もあるのではないかと幅広くとらえております。

ただそうした中において、「その中には」というところで書いていますが、「金融機関のサービスを利用するために必要となる ID やパスワード等を顧客から提供され、それによって自ら金融機関から顧客に関するデータを取得し、かつ、取得したデータに独自の価値を付加した後、顧客に対して直接的に金融関連サービスを提供」されているような業者の方々が、今そのサービスの対象である利用者を拡大されているという状況にあります。

なぜ利用が進むのかということにつきましては、先ほど荻生委員からもお話がありましたとおり、やはり金融機関から取得するデータをサービスの源泉として利用されているとはいいながら、それに非常に革新的なユーザー体験等を付加されているということが、ユーザーから評価されているということが理由の１つではないかというふうに考えております。

このような FinTech 企業が顧客に対して直接的に提供するサービスに関するところでございますが、FinTech 企業が、その全てを主導して決定して金融機関と何ら交渉を行うことがないような、そうしたケースもございます。このように金融機関が完全に受動的立場となる場合には、金融機関には何ら統制の手段がありませんということで、統制の手段がないにもかかわらず、安全対策上の責任が生じるということはなかなか考えづらいということでございます。したがいまして、たとえ金融機関の顧客に対して提供される金融サービスというものであっても、今回の安対基準の対象とはならないと解するのが妥当ではないかというふうに、一旦整理させていただいております。

これは、脚注 11 をお付けしておりまして、英国の「Open Banking Standard」においてもこうした形態を「スクリーンスクレイピング」と称しておりまして、Web サイト側でアクセス、Web サイト側というのは金融機関側ですが、Web サイト側でアクセスをコントロールしたり規制することができない。あとは何か問題が発生しても、利用者は問題解決の手段がなく、銀行に頼ることもできないというふうな事態にあるということが取り上げられております。

ただ、そうしたサービスばかりではございませんで、「他方で」というところで、FinTech 企業と金融機関の間に交渉があるようなケースがございます。そうした場合においては、金融機関の側から見ますと、顧客に関するデータの提供に関して決定権が存する場合があるということでございます。そうした点においては、部分的にせよ金融機関が主導性を発揮していると考えられるということで、金融機関に何らかの安全対策上の責任が生じていると解するのが妥当ではないか、というふうに一旦整理しております。

ですので金融機関に何らかの責任が生じるのではないかということで、先ほどの判別基準で申し上げましたとおり、こうした部分的に責任が生じる場合についても、今回ご検討をいただく対象に含めてはということでございます。

では、そうした安全対策上の部分責任がどういうものに由来するかといいますと、やはりこれは金融機関が取扱う金融業務に関連するデータ、その顧客に関するデータを、第三者に提供することに由来しているのではないかというふうに考えております。したがいまして、こうした提供するデータのリスク特性に着目して、それに応じて安全対策のあり方を考えるということが適当ではないか。その際には、そのリスク特性というのは、先ほどお話ししましたとおり、リスクベースアプローチということにつながってまいりまして、それを踏まえて安全対策を考えるということでございます。

じゃあ、リスク特性とは何だということでございますが、データの量等さまざまな捉え方があると思いますが、外部委託の時に登場した、整理させていただいた言葉として、機微情報あるいは機微性というのがございます。機微性には程度があるということで機微性が最も高いのが機微情報でございます。その機微情報ほど機微性が高くないものもあるということで、その程度というのがあるだろうと。これは具体的には何かというと、顧客が被害を被ると想定される損失の程度というふうに解されるのではないかと。ではどういう時に損失を被るかといいますと、本人が許諾した範囲を超えて FinTech 企業がそのデータを利用する場合、あるいは一方的に外部に流出するようなことになった場合というふうに考えております。

ただ、ここにつきましては、（注）を書いてございます。現在、金融庁におきまして、そうした顧客と金融機関の間に介在する FinTech 企業に関連した検討が進められているということも我々は承知しておりますので、そうした検討結果も考慮していく必要があるというふうに考えております。ただ、そうしたご検討の結果を待っていますと、なかなかこの議論も進まないということで、今お話ししたような想定を置いてご検討いただいては

どうかというのが、今回のご説明の内容になります。

以上、２点お話ししましたが、論点２として必ずしも想定されていなかった事項としてそれで十分であるのかどうかということで、確認をさせていただきたいと思っております。

続きまして７ページでございます。以上、２つの想定しなかった業務、想定しなかった事項等を踏まえて、安対基準の対象となる FinTech 業務のうち、今度はさらにそれを３つに分類してより対象を具体的にしているというところがそこの図表２でございます。

タイプⅠというのは金融機関が、完全に主導するタイプということで、一般的に従来からも行われていた外部委託として、FinTech 企業に外部委託が行われるようなタイプということでございます。ここにつきましては、本日委員としてご出席いただいています Liquid 社も含めまして、そうしたタイプⅠの形態で行われているというふうに承知してます。

その右のタイプⅡというのは、ちょっとやや特殊なところでございますが、タイプⅠの特性に加えまして銀行法等の改正に伴いまして、そうした FinTech 企業を子会社に出来るというようなことが今後出現してくると思っております。ですので子会社にされた場合には、子会社に対する責任というのも外部委託に伴う責任と別に生じるということで、タイプⅠとタイプⅡで分けておるというところです。

そうした子会社に対する責任というのは何なのかというところは、脚注 14 のほうに書いてございますが、ここも銀行法等の改正の中に含まれています経営管理の充実ということで、持株会社等が果たすべき機能というのが明確化されているということと、あとは座長の岩原先生の論文にもございますが、既にそうした子会社との中で経営管理契約等を結んで経営管理が行われているような実態もありますので、そうしたところを踏まえてタイプⅡについては、議論を進めさせていただければというふうに思っております。

最後にタイプⅢですが、これが先ほどの部分的責任の部分でございます。ここにつきましては、本日委員としてお越しのマネーフォワード社、あるいはマーク委員の会社のマネーツリー社とかそうした個人財務管理業務をやっていらっしゃる会社が、この形態になるのではないかというふうに考えてございます。

以上３タイプを整理させていただいた上で、次の８ページでございます。要は２者関係だけ考えていれば良かったものが３者になったということで、それを議論する時にさまざまな組み合わせのパターンがある中で、やはり検討をいただくにあたって議論の俎上といいますか、土台をそろえておくという目的で図表３を含めてここでご用意しております。

まず、金融機関が、FinTech 企業と FinTech 業務をするにあたっては、その２者の関係だけというのがあり得るかというと、やはり先ほど荻生委員のほうからお話がありましたとおり、FinTech 企業は運用のリソースをクラウドコンピューティングを中心として外部から調達されるケースが一般的であるというふうに理解しております。したがいまして、やはり２者ではなく３者の関係として取り上げる必要があるだろうと考えてございます。

こうしたクラウドの特徴につきましても脚注の 15 でございますが、日本銀行のレポートにもそうですが、当方のクラウドの検討会においてもそうしたスタートアップの企業において、クラウドの利用というのが馴染んでいるといいますか、親和性が高いといったようなご提言がされているというところでございます。

では３者の関係を整理しましょうということでございます。図表３ということで３者がそれぞれ単数の場合というのはこの３つしかない、㋑、㋺、㋩というふうに書いています。やや抽象的なので、若干例として補記をしておりますが、㋑のパターンというのは、FT が FinTech 企業ですが、FinTech 企業が IT ベンダー（主にクラウドベンダーかもしれませんが）に運用を委託して既に実施されているようなサービス、これを、FI、金融機関が自らのサービスの一部として顧客に提供されるような場合があるというふうに考えています。

その下の㋺です。これは FT と IT を逆転しておりますが、金融機関が従来から共同センター等を通じて馴染みのある IT ベンダーを通じて提供している金融サービスの一部に FinTech のサービスを追加するような場合、そうした形態もあるであろうと考えています。

最後に㋩ですが、金融機関が FinTech 企業から何らかのソフトウェアやサービスの提供を受けて、先ほどお話ししましたが、その運用の部分を IT ベンダーに委託されるような場合があるであろうということでございます。㋑㋺㋩の関係性において、矢印が意味するのは、外部委託の責任が生じるということで書いている、というところでございます。

単数の場合はこの３つでしょうということですが、複数の場合はどうかといいますとここは非常に場合分けが多岐にわたるのでございますが、８ページ、９ページにいろいろ文字では書かせていただいておりますが、一言でいいますと、既に先ほどお話し致しました２者関係の時の複数の共同センター、クラウドサービス、あるいは再委託等の議論を既に済ませている現状においては、３者関係においての複数の部分について、特段固有の性質があるものとして取り上げておくものがないのではないかというふうにしているということです。

（注）というところでございまして、いや、ほかにもあるかもしれないという可能性は残るのでございますが、そこのところについて深くご検討いただくよりも、一旦は単数の場合を前提としてご検討いただいて、今後必要に応じて複数の場合も追加する、あるいはほかの類型を追加するという形で進めさせていただければと思っております。

次の 10 ページでございます。今お話した２つ、タイプⅠ、Ⅱ、Ⅲと㋑、㋺、㋩というものを掛け合わせると、おおよそご検討をいただく前提といいますか、土台としてイメージを持っていただく前提として、この７つのタイプをお示しさせていただいているというところでございます。

タイプⅠは外部委託の場合の３つの類型、タイプⅡはタイプⅠの類型で責任が新たに生じるということで青い色の矢印で書いてございますが、経営管理等の責任が生じる、別の責任が加わるというものでございます。タイプⅢというのは、部分責任。部分であるということを点線で表現はしておりますが、タイプⅠの㋑の派生形ではないかというふうに整理をさせていただいています。

こういう理論的な整理を何故しているかといいますと、今後、現在の安対基準をそうした FinTech 業務の利用に適用した場合にどういう問題が生じるかということを、第２回目以降ご提言いただこうと思っておりまして、その時に、例えばタイプⅠの㋑の場合にはこういう問題がありそうですね。あるいはタイプⅠの㋺の場合にはまた㋑と違ったこういう問題がありそうですねという、ご議論をいただく時のツールとしてご活用いただけるのではないかということでご用意しているということでございます。

論点３としては、この７つ以外に、この場で今後取り上げるべきものがあるか、ないかというところで確認をさせていただいております。

次の 11 ページでございますが、ここにつきましては、今後第２回目以降、問題の所在を明らかにしていただく、要は従来の安対基準をもとに、今の FinTech 業務に適用した場合にどういう安対基準の適用上の問題があるかということをご議論いただくのですが、何を問題とするのかということにおいては、やはりさまざまな観点があるだろうと思っております。そういう意味でどういう観点で問題をとらえるかということを、本日ご意見をいただくことが有益ではないかということでご用意させていただいております。

では問題を取り扱うにあたって大きな前提としましては、先ほどの本検討会の設立趣旨及び理事長からのお話のとおり、我が国の金融機関の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ことを目指していくというこの観点というのが、基本的にベ

ースにあるということでお願いしたいと思います。

その上でどういう観点があり得るかということで、１つ目が安対基準の中立性という観点でございます。これは何をいっているのかといいますと、先ほど７つほどの類型をご説明しましたが、FinTech 業務を実施するにあたってさまざまな類型がある中で、例えば安対基準が特定の類型、先ほどの例えでは㋑ではなくて㋺とかですね、そうした特定の類型の採用にあたり、抑制的な効果をもたらすということがないように留意しなければいけない。なぜならば、安対基準は情報システムを対象とした安全対策の基準ですので、金融機関がさまざまに行うであろうビジネスモデルの多様性を損なってはならないというふうに考えております。ですので、そういうことになるのであれば、その歪みと表現していますが、それを問題として取り上げではどうかということです。

もう１つが、安対基準の有効性ということでございます。中立性というのを踏まえながらも、やはり安対基準として安全対策を行う上では、それが十全に統制能力が確保されないといけないということでございます。統制能力というのは、外部委託先だけでなくて、再委託されている場合では当然再委託先までも及びますということで、そうした再委託先を含む外部委託先全般への統制能力というのが、当然のことながら十分に確保されていることが必要であるということでございます。仮に先ほどご説明した㋑、㋺、㋩その他の類型の中で、安対基準をそのまま適用すると統制能力が必ずしも十全に機能しないということが想定されるのであれば、それは問題として取り上げる必要があるというふうに考えております。

では、この中立性と有効性という構成というのはどちらを優先させるべきなのかということでございますが、中立性を優先させた場合には、ビジネスモデルを損なうことはないのですが、安全対策上の責任は金融機関が必ずしも果たせないこととなる懸念がある。一方、有効性を優先させた場合には、IT ベンダー、FinTech 企業に固有の負担を求めることになるのではないか。あるいはその結果、そのビジネスの自由度を制約するということになる可能性もある。そうした意味では、FinTech 企業の革新性を損なうこととなるような懸念がないかということでございます。

こうした中立性と、有効性は単純に考えればトレードオフとなるような場合もあり得るだろうということで、そういった意味では、この場でどちらを優先させるという結論を出すということは考えておりませんで、多様な状況で発生すると考えられますので、そうした個々の状況に応じてご議論をいただくのがいいのではないかというふうに考えておりま

す。ケースバイケースで判断せざるを得ないということです。

特に今回、簡易なリスクベースアプローチで必要最低限の安対基準を作っていただくという観点ですので、要は FinTech の利用が進むための基準を作るということでございますので、その個々のケースに応じてこの場合は中立性、あるいはこの場合は有効性という形で、今後議論をいただく時のツールとしてこの言葉を利用していただけるのではないかというふうに考えています。論点４として、それ以外に観点はありますかということで確認をさせていただいています。

最後に次の 12 ページですが、オープン API との関係について触れさせていただきます。オープン API とは一般的に金融機関が API を公開して、FinTech 企業等がその API を利用して自社サービスと金融サービスを連携させる方法ということでございます。一般的には先ほどお話ししたタイプⅢの形態がとられる場合が多いのではないかというふうに考えております。そうしたオープン API においてのセキュリティの考え方については、金融審の決済業務等のあり方に関するワーキンググループ報告書において、作業部会を設置の上、平成 28 年度を目処に報告書を取りまとめるということが提言されておりまして、今後、全銀協を事務局として、金融機関、IT 関連企業、金融行政当局等をメンバーとする検討会が本格的に設置される予定となっております。その検討会には FISC もメンバーとして参加する予定であります。あるいは今日お越しの委員の方も、そちらでも委員をやられる方もいらっしゃると思います。そうした形で、全銀協を事務局として行われる検討会での議論も参考にしながら、この検討を行いたいというふうに考えております。

以上が今日ご用意した論点ですが、あとは参考ということで若干補足させていただきますと、13 ページはプレスリリースの数が増えてますというファクトを我々が整理したものです。

14 ページは、こういう FinTech の話ですと、やはり定義はどうなんだというのがよく言われて最初に定義をみたいなことがあるのですが、先ほどお話ししたとおり、荻生委員からもお話があったとおり、定義は難しいものですので、一般的にこういう定義がされていますということで官公庁等の定義の例だけをお付けしております。日本銀行の中にも、FinTech の定義が必ずしも明確に定められているわけではないというふうな記載もございます。

その次の 15 ページは日本の監督当局等の動向ということで、先ほど来お話ししています銀行法等の改正、２番目が金融制度ワーキンググループの開始ということで、これは先

ほどお話しした顧客と金融機関の間に介在する FinTech 業務の１つである中間的業者に対する規制のあり方が今取り上げられているということ。

３番目が全銀協のオープン API の取組み。全銀協が実施されたアンケートの中に、FISC の役割というのが期待されているというふうなコメントもいただいているところです。

４点目以降は、実は事前送付資料には含まれておりませんで、その後に我々のほうで追加したものでございます。本文中の論点にもございますが、金融審議会における決済業務等の高度化に関するスタディグループ、あるいはワーキンググループ等において、情報セキュリティに関する課題について報告されていますので、その内容も検討にあたってご参考になると考えまして、その次の 16、17 ページにわたって掲載させていただいております。下線は FISC のほうで付させていただいているというものでございます。

その次の 18 ページは、海外の先進諸国の動向でございます。ここは若干ご説明させていただきたいのですが、米国においては米国通貨監督庁というのが今年の３月に「責任ある革新」を支援するという白書を公開しています。特徴的なのが、下の斜体で書いてありますが、リンカーン大統領が国法銀行システムを創設して以来、イノベーションは国法銀行システムの代表的な特徴であるということが言われています。したがいまして、その下の下線ですが、こうした革新が進む環境、要は銀行業務のやり方が破壊されようとしている中においても、国法銀行等が力強く成長していくことを望んでいるというふうに言及されているところでございます。そうしたことを踏まえまして、８点ほど監督当局としての取組みが期待されているということでございます。

あと、FinTech 企業との関連につきましては、18 ページの下ですが、やはりそれぞれの優位性を生かしてコラボレーションをしていくことが推奨されてます。

19 ページですが、そうした銀行とイノベーターは、それぞれの独自の優位性を生かし互いにコラボレーションすれば利益を得ることが可能だと。戦略的で思慮深いコラボレーションを通じて、銀行は最新テクノロジーへのアクセス手段を手に入れ、イノベーターは潤沢な資金や巨大な顧客基盤を手に入れるということができるということでございます。

一方、リスク管理については必要条件として言及されておりまして、革新はリスクから自由ではないということで、責任ある革新の必要条件として効果的なリスク管理があると。リスクと革新の最適なバランスを心得なければいけないということでございます。

金融危機、先ほど荻生委員からリーマンショック等のお話がありましたが、金融危機か

ら学んだとおり、革新があれば何でもいいわけではないということで、OCC はそういう意味では責任ある革新が行われるというものを支援するということでございます。

その下の英国の事例は恐らく皆様ある程度ご承知のところでいらっしゃると思いますが、１点だけ、Open Banking Standard という英国のさまざまな関係者が集まってオープン API の標準化をされている取組みの記載をさせていただいていまして、なぜその取組みをしているかというところに下線を引いています。一言でいいますと、今後、１世紀以上にわたって英国が経済界、産業界の勝者であり続けるための検討であるということでございます。以上が海外の事例のご紹介でございます。

あと別紙２のほうは今お話しした内容の俯瞰図です。

最後に別紙３「今後の検討会の進め方（案)」ということで簡単にご説明しますと、第１回は、安全対策のあり方を検討するにあたってのその前提です。残りの時間を通じて検討のあり方をご議論いただこうと思っております。第２回は、そこでご議論をいただいた上で、安対基準を FinTech 業務に適用した場合の問題について、幅広いご意見をいただきたいと思っています。第３回はそれを踏まえて、必要最低限の安対基準に結びつく簡易なリスク管理策をどのように整理していくことが望ましいかということで、安全対策のあり方をお示ししてご議論いただこうと思っております。

その後、オープンAPIの検討を取り扱ってはと思っておりまして、ただ、これにつきましては全銀協の検討がこれから本格的に始まる状況ですので、その状況を踏まえてこの場でもご紹介させていただきながら、適宜ご検討いただければというふうに思っております。最終的には本検討会は６月末までを目処に完了させていただければというふうに考えております。長くなりましたが、私からは以上でございます。

○岩原座長

どうもありがとうございました。

ただいまの藤永次長からのご説明につきまして、何かご質問ございますでしょうか。あるいはご意見ございますでしょうか。瀧さん。

○瀧委員

マネーフォワードの瀧でございます。１番目に関するところ、当社として考えているポイントをお伝えしますと、先ほど金融審議会のスタディグループの中間報告の引用もござ

いましたけれども、この FISC の場はさまざまな場所での検討から参照されてきておりまして、FinTech 企業が一般的にふるまうべきセキュリティスタンダードの１つの議論のベンチマークになっているという、そういう今までの過去の議論の形跡があります。直接の業務委託でないものの、例えばマネーフォワードというのはさまざまな銀行様に向けて家計簿のサービスを提供しております。そちらは個別に交渉等をしながらですのでタイプⅢに含まれてくるところではあるのですが、今までサービスを提供する際に、どのレイヤーで我々自身が、自らのセキュリティを表明して、また銀行さんもそれぞれ初の案件として、当社をどのように評価すればいいのかというのは、かなり個々に試行錯誤があったところでございます。毎回同じプロセスがあった中で、だんだんと慣れていったところもありますが、新しい FinTech 企業に毎回同じ審査が重複するというのは、社会的にロスが非常に大きいものだという認識がございます。

ですので非常に丁寧に議論を進めていく必要があるかと思うのですが、私どもとしては安対基準自体をどう運用していくかと、FinTech が仮に委託関係になくともどのような期待値でふるまうべきかについて、同じレベルぐらいの重みがある議論になるべきなのかなと考えている次第でございます。

もう１つ、今後の運営の中で気をつけなければなと思っておりますのは、こちらも金融庁さんとか全銀協さんでの議論を見ていて、全銀協さんのほうも FISC の動向を見ながらというのでお見合いが起きないかというところだけは、私も重複する形でいろいろな会議で発言させていただいている立場もありますので、適切な運営に貢献していければと思っております。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。マーク・マクダッドさんどうぞ。

○マクダッド委員

FinTech 協会のマクダッドです。先ほど瀧様がおっしゃったようなことの繰り返しになるかもしれませんけれども、FinTech 協会としては、これから起業する、そして起業して間もなくの会社の支援を１つの使命として努めてはいるんですけれども、多分多くの FinTech 企業は今後、金融機関と協業をしたい、FinTech ですから。「FinTech ですから」とあるのではないかと思うんですけれども、その起業する時にセキュリティの設計、シス

テムの設計をしますと、FinTech ですから当然 tech が入っています。現状ですと例えばFISC 様に電話をして、「安対の全てを教えてください」というと当然それはないことだと思うんです。なので、FinTech 企業から見ると、どうすればいいのかわからない企業が、FISC などを意識せず最終的にはサービスを作ってしまい、そして例えば金融機関様と協業しようとするとしましょう。その際、タイプⅠだと割とわかりやすいかなと思っているんですけれども、先ほどタイプⅢというお話、そのタイプⅢの中でもいろんな形がある中で、最終的に金融機関様に FinTech 企業が言われるのは「このチェックリストに記入してください」ということで、そのチェックリストはほぼ FISC に近い形だと思います。

なので、現状としてはもう FISC で評価されなくてもいいという話だとしても、そういうふうになると、弊協会の複数のベンチャー会員から伺っておりますので、論点１のところですけれども、意見表明を行う必要があるかというと、とても必要かなと思っています。どういうふうに金融機関が FinTech 企業を見るべきというのを、金融機関が主体なのであれば、それは FISC が関わったほうがいいのではないかと思うところです。以上です。

○岩原座長

轟木さん。

○轟木委員

株式会社 Liquid の轟木と申します。１点質問させていただきたいんですけれども、２ページ目の論点１に関してです。２ページ目真ん中辺で商品等の売買を目的とする電子商取引業務を担う情報システムは対象外だということ、端的にいうと、決済事業をやる事業者さんの情報システムは安対基準の対象とならないという理解で間違いないのかなと。ただ、Apple Pay だったり Google Pay であったり、そういった電子商取引業務を行う場合には、適用されないという理解でよろしいんでしょうか。

○藤永次長

そこについては多分ご質問としては、資金決済法の対象事業者が安対基準の対象であるのかどうかというご質問ではないかと思っています。そこにつきましては、経験的にという表現になるかもしれません。先ほど金融機関等というふうに書いてございました、金融、保険、証券、クレジット会社というものを従来 30 年前から変わらず対象としてきていま

す。その後、資金決済法が整備された中で、その資金決済法の対象事業者を安対基準の対象とすることについては、明示的に取り上げられていませんので、経験的といいますか、慣習的といいますか、そういう理解としては、そうした資金決済法の対象事業者の業務を担うシステムが、安対基準の対象となるのかと言われると、我々の理解としては、ならないというふうに今までやってきていると考えております。

○轟木委員

例えばそういう事業者さんが決算のデータに基づいて融資とか与信判断をして、アマゾンさんもいらっしゃると思うんですけれども、その売買のデータに基づいてレンディングすると。その場合は当然従来の金融業には入ってくると思うので、規制の対象になるのかなと。FinTech 企業といっても、極めて議論は流動的かなと考えられまして、そこら辺をどう整理していくのか。例えば EU のように決済を横断的に規制をやるかとか、幾つか考え方はあると思うんですけれども。

論点１に関して、意見表明の点は例えば、Apple Pay、Google Pay といった企業が、FISC さんの基準を遵守すればセキュリティ的には問題ないというような形で参照できるような規定であれば、ぜひそういう人向けの基準のような形で設けるというのはありかなと思っています。ちょっと取りとめないですけれども以上です。

○岩原座長

轟木さんのご意見ですね。

○轟木委員

はい。

○岩原座長

田中さん。

○田中委員

みずほフィナンシャルグループの田中です。今までも出ていましたけれども、２ページの論点１に関係しまして、現在の安対基準はこれまで金融サービスの担い手は金融機関と

いうことを前提にしていると思うんですが、FinTech 事業者の方々もこれから金融サービスの担い手になるという可能性があるということを踏まえると、そもそもそういった方に対しても目安となるようなことを観点に、安対基準のスコープとか位置づけといったあたりも考えていく必要があるのではないかというふうに思います。以上です。

○岩原座長

安対基準の役割をもう少し広く考えてもいいのではないかということですね。それでは岩田さん。

○岩田委員

恐らく前の２つの疑問点と似たようなことになると思いますけれども、今回の大前提として金融機関というものに対するかかわりで、金融機関の前提は先ほどご説明いただいたとおりだと思いますが、いわゆる決済代行会社が金融機関なのかというところで、決済代行会社と関わるような FinTech サービスが増えてきています。一方で、決済代行会社のクレジットカードというものに対しては、経産省さんが新しいガイドラインを出されたりという動きもあると思いますし、一方で、またクレジットカードという EMV だとかに対しては PCI DSS というほかのガイドラインもありますので。あとは全体のスコープとして、FISC として深掘りするところはここであって、ほかは PCI DSS であり、経産省さんのクレジットカードの業務を扱われるガイドラインを参照にすべきだとか、そういう大前提の整理、議論のスコープをほかのガイドラインとか規制とも併せた上で、概要整理ができると、見ているほうというか一般の FinTech ベンチャーにとってもわかりやすいかなと思いました。

○岩原座長

ご要望として承ります。

ほかに何かございますでしょうか。マクダッドさん、お願いします。

○マクダッド委員

先ほど資料のところで、こちらからの指摘だけなのですけれども、先ほどのメモのところではなくて、こちらの外部委託検討会報告書の概要の 12 ページです。最後に、

「FinTech という金融サービスは外部委託の形で利用することが多いと考えられる」、というふうに書いてあるんですけれども、弊協会のベンチャー会員、FinTech 企業の中で、そうではなくて ASP 的な利用、サービス利用というのが逆に多いかと思いまして。Liquid さんが今日いらっしゃるので Liquid さんのお話はしないほうがいいかもしれませんけれども、タイプⅠなどの話は完全に外部委託というケースは当然ありますけれども、どちらかというとそういったケースは恐らくセキュリティ、生体認証、ブロックチェーン関連の FinTech 企業となりまして。情報処理というサービス面、何か情報を加工して付加価値を提供するようなサービスですと、恐らく外部委託ではないのではないかと思っています。以上です。

○藤永次長

我々が外部委託有識者検討会で取り上げる外部委託とは何であるかというのは、お手元の外部委託の報告書の 10 ページに整理させていただいているところでございます。これはこの場というよりは、今後、これを参考にご理解いただければいいかと思っています。

○岩原座長

神田さん。

○神田オブサーバー

金融庁の神田です。オブザーバーの立場ですが、金融庁ではさまざまなところで FinTech のセキュリティに関連した議論をしておりますので、その関係について簡単にご紹介しつつ、金融庁の取組みを少しご説明させていただきます。

先ほどからもご説明がありますように、セキュリティの主な論点になってくると思われる中間的業者、あるいはオープン API の考え方につきましては、金融審議会の金融制度ワーキンググループのほうで制度面、それから全銀協さんに事務局をしていただきますオープン API の検討会のほうで、技術あるいはシステム的な仕様、あるいは標準化といったような点について議論する予定となっております。こちらの FISC さんの有識者検討会の議論にも、それぞれ関わる部分が出てくると思いますので、その都度私のほうでも議論の進展についてご紹介させていただきたいと思います。

本日については、先ほど藤永次長からご説明いただいた 15～17 ページにかけまして、

特に決済業務等の高度化に関するスタディグループの報告のほうに、FinTech 業務に関するセキュリティについての、これまでの議論の流れが書いてあります。特に 16 ページの真ん中のところにあります点についてご紹介したいと思います。真ん中の黒いポチです。

「銀行のネットバンキングなどについては監督指針や FISC の安全対策基準等の取組みが行われてきたが、多様なプレーヤーが決済情報のプロセスに組み込まれる中にあっては、銀行のみならず多様なプレーヤーにおける情報セキュリティ対策の向上が重要である。こうした観点からは多様なプレーヤーが多様な拠り所とできる準則や業界における情報セキュリティ基準の設定、その実効性の確保のための方策が重要である。」という点が、「決済業務等の高度化に関するスタディグループ」の中間報告に盛り込まれておりまして、この考え方に則って、FinTech の情報セキュリティについても整備を進めていっていただきたい、と考えております。

そういう考え方を実際の FinTech のサービスにあてはめますと、FinTech の本質としましてユーザー目線、ユーザーファーストという考え方、ユーザーに寄り添ったサービスが提供されるという特徴があります。逆にいいますと、ユーザー側からすると、銀行が提供するサービスも、それから銀行以外の FinTech 業者などが提供するサービスも、シームレスに非常にストレスのない形で提供されることが想定されます。そこのところの区別が曖昧になると、誰がどういう形でサービスを提供して誰が責任をとるのかという点が、ユーザーにとって非常に曖昧になる、あるいは意識せずに利用するというのが、FinTech のサービスの特徴になってくるかと思います。

そういう意味でいいますと、この安全対策基準についても金融機関が提供するのか、あるいは金融機関が責任を有するのかという点は、FinTech のユーザーにとっては非常に不可分のところでサービスを利用することになるだろう、という点を意識しながら議論をしていく必要があるかというふうに考えております。

そういう点でいいますと、論点１で先ほど出ておりました安全対策基準以外の点についても議論の対象とすべきか、あるいは何らかの意見表明が行われるべきかという点は、やはりユーザーの目線に立つと、少し金融機関の安全対策の周辺部分として意識しながら議論をしていただく必要があるのではないかと考えております。先ほど瀧さん、マクダッドさん、轟木さん、それからみずほ銀行の田中さんもおっしゃっていたような論点とほぼ同じだと思いますけれども、金融庁としてもこれまでの議論の流れからはそういうふうに進めるのが適当と考えております。少し長くなりましたが、よろしくお願いします。

○岩原座長

どうもありがとうございます。

藤永さん。

○藤永次長

ご意見ありがとうございます。我々のほうとしまして、なぜ論点１を今回、取り上げたかというのを簡単にご説明させていただきます。

やはり当センターが過去から現在に至るまでの立脚点というのが、先ほどご説明した安対基準の対象というところがございます。そこを曖昧にしたままでは FinTech の議論はできないだろう、ふさわしくはないだろうということで、そこを明確にご説明させていただいたというところです。

過去の立脚点であるからといって、将来的にそうであるかということではございませんで、そうした意味で我々も含めまして将来に向けてどうした議論が今後必要であるかということで、論点１として個別に切り出してご意見をいただいたというところでございます。

この論点について事務方としまして、今日結論を出そうとは全く思っておりません。今後、次回以降、特に個々の現場で起きているさまざまな不安とか問題と感じられているところをご議論いただく中において、最終的に論点１の答えといいますか、皆様のご提言内容が取りまとめられればよろしいかなと、ありがたいかなと思っておりますので、今後、基本的には、安対基準が従来対象としてきたものをまずは中心にしてご議論いただくほうが効率的ではないかとは思っているものの、皆様の頭の片隅に、先ほど来多くの委員の方々からご意見をいただいた部分を置いていただいて、折に触れそうしたところも含めて、ご意見をいただければというふうに考えております。以上です。

○岩原座長

どうもありがとうございました。

いま藤永さんのほうからおっしゃっていただきましたように、この論点１等について、今後どこまで議論していくかということを、皆さんのほうからご意見をいただいて検討していければと思います。

よろしいでしょうか。ほかに何かご意見等ございますか。

それでは特にほかにご意見はないようでございますので、本日の議事はここで終了させていただきたいと思います。

それでは、これにて第１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。お忙しいところをお集まりいただき、熱心にご議論いただきましてまことにありがとうございました。

以上