

平成29年 6月13日

公益財団法人 金融情報システムセンター

第6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 6月13日 (火) 15:45~16:45

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	淵崎 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
	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 システム部 副部長
	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	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
	内波 生一	(代理出席)株式会社マネーフォワード アカウントアグリゲーション本部 本部長
	轟木 博信	株式会社Liquid 経営管理部長 弁護士

	村上 隆	株式会社NTTデータ 第四金融事業本部 企画部 ビジネス企画担当 シニア・スペシャリスト
	長 稔也	株式会社日立製作所 金融システム営業統括本部 事業企画本部 金融イノベーション推進センタ センタ長
	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・アシユアランス本部 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 金融サービス営業本部 シニアインダストリーマネージャー
	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 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
FISC(事務局)	渡辺 達郎	理事長
	高橋 経一	常務理事
	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
	和田 昌昭	監査安全部 部長
	水野 幸一郎	総務部 部長
	郡山 信	総務部 特別主任研究員

IV 議事内容

1. 【議事1】本検討会の報告書についての説明・論議

○岩原座長 座長を務めます岩原でございます。それでは本日、1つ目の議事は本検討会の報告書についての説明、論議でございます。FISC企画部の藤永次長、よろしくお願ひします。

○藤永次長 FISCの藤永です。

お手元に資料2をご用意ください。前回、報告書のドラフトを皆様にご提示させていただきましたが、それに対する事後意見として2件ほどご意見をいただいております。いずれも南都銀行様からいただいたものです。

1点目ですが、「有事における顧客への一義的な責任を金融機関が負い、また FinTech 企業に対する金融機関の管理において『外部委託基準』の準用ルールが適用される事業範囲はどこまでか確認したい」ということございまして、そうしたご質問をいただいた趣旨としては下のほうに書いてございまして、「当該ビジネスが提携銀行にとって委託業務となるか否かは、事業内容や個別の契約形態によって判断すべきであり、委託者としての権限が担保されない状態で管理責任のみが追及されることで金融機関に過度な負担がかかることがないよう配慮が必要と考える」というご指摘です。

冒頭部分につきましては、個別にご意見をいただいたご本人の方とお話をさせていただきまして、ここはクラウドに対する補足的検討とタイプⅢの議論をやや混同されていたことを確認させていただいております。そういった意味でご意見をいただいた方の趣旨としましては、タイプⅢのような、金融機関が必ずしも主導しない場合において、現在のドラフトにおいても、やや金融機関に管理責任が必要以上に求められるというふうに読まれかねないという点になります。そうしたことを踏まえまして、事務局回答としては、ご指摘を踏まえまして、原案の「FinTech企業に残る安全対策上の責任」に関して以下の修正を行います。

「FinTech企業は、みずからが主導して金融関連サービスを提供していることから、顧客に対する一義的な安全対策上の責任はFinTech企業が担うものと解される。そのため、FinTech企業は、外部委託にとどまらず、サービス全般において、適切な安全対策を実施

することが、社会的には期待されている」ということで、下線部分を加筆させていただいております。

2点目ですが、前回「リスク特性の分離可能性」という論点メモをご説明させていただきましたが、『リスク特性が顕著に異質』とは、実際にどのようなケースが該当するのか、具体的な事例等を示していただきたい」というご意見です。

ご指摘を踏まえまして、原案の「FinTech業務を担う情報システムの安全対策上の取扱い」という分離可能性に関して言及した部分に脚注を追加します。脚注としては、例えばということで、「システム全体では、顧客情報が保有されているが、該当のサブシステム内」、要は分離されるサブシステム内には「顧客情報が保有されていない場合等が考えられる」のではないかとということをございます。リスク特性の事例を顧客情報という具体的なものに紐付けて、脚注としてご説明させていただいています。

以上2点の事後意見とあと事務局側の若干の加筆修正をしておりますので、資料3、有識者検討会報告書の、前回ご提示したのものから修正した部分のみを抜粋した資料となりますが、お手元にご用意ください。まず10ページです。FinTechに関する安対基準適用上の課題と安全対策のあり方を考えるに当たって明確にしておくことが有益な事項の1つとして、目標とすべき安全対策の効果の程度というパートがございました。ここにつきましては、「効果」という言葉の中に「程度」の意味がある程度含まれているだろうということで、回りくどい「効果の程度」という長い言葉を使うのではなくて「効果」という形で言い切るような表現に修正しているというところです。

その上で、同等性の原則という考え方をご説明させていただいていましたが、そこで期待される安全対策の効果が、どういうふうに導き出されてきて現在まで維持されているかということを少し加筆したほうがよいだろう、ということで、赤字の下線部分を追加しております。「金融情報システムに社会的に期待される安全対策の効果は、システム資源を自前で用意するのが一般的であった30年前に、安対基準の策定という形で初めて具現化されました。その後、安対基準に具現化された安全対策の効果は、金融機関に対する社会的期待の変化を反映」している。その一方で「ITベンダーへの依存度の高まりといった金融機関の事情」、都合による変化の影響というのは受けることなく、維持されてきた。したがって金融機関とITベンダーの2者関係という中でも安全対策の効果というのは、当初と同程度に維持されてきたと考えるということです。

したがって、金融機関がイノベーションの成果の享受を目指す中で仮に3者の関係

になったとしても、同程度に効果は維持されるべきであるということです。

その下のところですが、「同等性の原則」という言葉を使っていますので、「同程度」といっている部分について「同等」という言葉に変えても意味が変わらない部分については修正を幾つか加えているということです。16ページもそうした観点での修正になります。

続いて17ページです。ここは前回の席上で、轟木委員からご質問、ご指摘をいただいたことを踏まえまして、加筆修正を加えているところです。脚注の27ですが、「仮にFinTech企業の負担費用の最小化が選択される場合、金融機関がFinTech企業に代わって責務を負担することが明らかとなれば、FinTech企業には安全対策上の責務を全く果たさなくても、金融機関が負担してくれるのではないかという期待が生まれる可能性がある。」前回は「期待が生まれる」と断定的に書いていましたが、そういう可能性があるというふうに変えています。

あとは前回、「フリーライダー」という言葉を入れておりましたが、やや誤解を生じる言葉であるということで、これについては削除させていただきました。

一方、金融機関の費用負担の最小化が選択される。そういう選択肢も取り得るということで、そうした場合には、「FinTech企業に負担が求められることになり、FinTech企業は負担を逃れるために安全対策能力を過大に虚偽申告する可能性がある。」したがって「関係者が協調し、社会的な観点から負担費用の総和の最小化を検討されることが望ましい」という結論に至るのではないかということです。

そうした適切な情報開示等による協調を確実に実現するためには、これは前回ご提示したような、責務を負担した関係者に応分の利益が還元されるようなスキームを講じておくことも考えられるだろうということになります。

続きまして19ページです。ここはややわかりにくい言い回しであったところを、少し意図が正確に伝わるように加筆を加えています。これはタイプⅢにおいて金融機関の関心はデータの保全と本人確認に特定されるといった場合、その関心外のものについてどういう取り扱いをするか、という説明の文書です。「ただし、金融機関が関心を持たない項目があることに起因してFinTech企業において行われるべきシステムに対する統制全体の程度が低下」するような場合があり、「その結果、データの保全又は本人確認に係る安全対策の効果まで損なわれるというような場合には、金融機関は、FinTech企業に対して、関心外の項目に対しても、何らかの付加的な統制を講ずる必要があることに留意が必要である」ということです。

それに合わせまして下の枠線の中にも、一部「金融機関の責務部分以外に対しても」ということで加筆を加えているというところです。

その下の19ページの下のところは事後意見の1番の反映です。

続きまして、23ページですが、下の脚注の34も事後意見2番の反映になっております。

右側の35ページですが、ここもやや意図がわかりにくい表現だったところに加筆を加えています。「評価事項に、技術変化の影響を受けやすい設備基準や技術基準が、技術変化の状況を踏まえることなく、そのまま字義通りに利用される、といった不確実性が残る現状にある」ということをいっているということです。

36ページです。これは、前々回のご指摘を踏まえて、前回、機微情報と要配慮個人情報について脚注に追加したのですが、ややそれでも意図が伝わりにくいであろうということで本文のほうに追記しました。加筆としては、機微情報を説明する中に「(要配慮個人情報を含む)」というふうな記載の仕方しております。それに合わせて下の脚注も変更しております。

続きまして、37ページですが、これは書いてある本文の中身とタイトルが不一致であったところなので、「統制対象クラウド拠点の把握」というタイトルに変更しております。続きまして、39ページですが、これもわかりやすさの観点で修正したものです。統制の内容と統制の方法については前段のところでも図表をもってご説明していますので、その中身と整合的な内容に文章も変更したということです。

その下の何点かの修正につきましても同じように、意図が正確に伝わるようにという観点で修正を加えているというものです。

続いて40ページ右側のところですが、「銀行法等の一部を改正する法律案」としておりましたが、先般5月26日に法案として成立しましたのでアップデートしているというものです。

続きまして44、45、ここは委員・オブザーバーの皆様の名簿です。前回もお願い申し上げましたが、もしこの内容でも皆様の現在の役職と相違があるようなものがあれば事務局のほうに至急ご一報いただきまして修正を行いたいと思いますので、ご確認をお願いいたします。

続きまして1枚めくっていただきまして資料編の修正です。50ページの部分は、先ほどのようなご説明と同じ法案の成立に伴う修正です。

次の76ページ、これも同程度というのを同等に修正したというものです。

次の85ページ、ここにつきましてはAPI接続先チェックリストワーキンググループによる集合的な検討という説明から始まっているものの、銀行APIに必ずしも限らない、その他今後生じるかもしれないチェックリストの検討に対しても適用可能なような汎用的な記載にしたほうがいいのではないかということで、検討体の固有性を表現するような「ワーキンググループ」、あるいはそれに類する表現を落としているということをやっております。

そういった意味では資料9のタイトル自体も少し変更したほうがいいのではないかと事務局で今さらながらに思っていて、その部分については最終版、公開する版においては検討の上、必要な修正を加えようと考えております。

最後に裏面ですが86ページという報告書全体の一番最後のページに、本検討会で取り上げた課題とその対策を一覧としてご用意しています。今回多岐にわたる検討を行っていただきましたので、その課題と対策がどういう相関関係にあるのかということの一目でご理解いただけるようなものが必要であろうということでご用意したものです。

まず課題としましては、安対基準の適用対象と対象外について個別に取り上げています。適用対象については、FinTechの類型化を行ってタイプⅠ、タイプⅡ、タイプⅢと分けました。オープンAPIは、タイプⅢの個別のものとして課題を抽出しています。それぞれここに書いてありますとおり、タイプⅠについては「FinTech企業の安全対策遂行能力と比してバランスを欠く場合がある」というところが課題認識として始まりまして、対策として「再配分ルール」をご提言いただいた。この「再配分ルール」は必ずしもタイプⅠに限らずタイプⅡ、タイプⅢにおいても適用可能であろうということで、矢印が3つから伸びている。

一方、タイプⅡについては、「FinTech企業には金融機関による経営管理と外部委託管理への対応が負担になる場合がある」という課題認識を出発点として、対策としてタイプⅡの補足的検討を提言いただきました。

タイプⅢにつきましては、「幅広い形態に柔軟に対応しうる安全対策の在り方が必要」ということで外部委託基準の準用ルールについてご提言いただきました。タイプⅢの一種であるオープンAPIについては、「FinTech企業の統制対応負担の軽減」という課題がございまして、これについては前回、集合的な検討を踏まえた安全対策のあり方としてご提言をいただきました。

これら4つの対策、3つのタイプに通底するものとして分離可能なサブシステム、あるいは

はクラウドサービス利用時のリスク管理策に関する補足というのを行っていただきました。

一方、適用対象外につきましては、「FinTechと総称される金融関連サービス全般においてシームレスに一体不可分な形で適切な安全対策が実施されることを期待」するという
ことで、金融関連サービスの提供に携わる事業者を対象とした原則に関する意見表明を行っていただいております。

最後に、安対基準の適用対象、対象外であるかにかかわらず、金融関連サービスに携わる関係者の皆様が協調して安全対策を行うという「協調の原則」と、安全対策の効果は関係者がかわろうとも同等であるべきであるという「同等性の原則」が、最も基本的な原則として位置づけられたというところでございます。

以上の加筆修正を加えてでき上がっていますが、お配りしている資料4で、全部で86ページの報告書が、今回取りまとめられたということです。

私からのご説明は以上です。

○岩原座長 どうもありがとうございました。それでは、ただいまのご説明に対してご質問等ございますでしょうか。

特に無いようでしたら、報告書の内容につきましては、本検討会の終了後、最終版を確定させていただき、速やかに公表に向けた作業を進めたいと存じます。

この間、皆様に議論を尽くしていただきましたので報告書の最終版につきましては、座長一任にさせていただきたいと存じます。ご了承いただければ幸いです。

2. 【議事2】API 接続チェックリストワーキンググループの検討状況

○岩原座長 続きまして、2つ目の議事はAPI接続チェックリストワーキンググループの検討状況についてのご説明でございます。FISC企画部の藤永次長、よろしく願いいたします。

○藤永企画部次長 それでは、API接続先チェックリストワーキンググループの現在の検討状況についてご説明させていただきます。まず資料5ですが、これはこの場でも毎回ご提示させていただきましたとおり、本日時点で計9回の検討が行われています。

次回6月20日を最終回として予定しておるところです。

前回の第9回のとくに、ワーキンググループのメンバーがチェックリストのたたき台として合意できる案がほぼほぼ整えられておりまして、それがお手元の資料6です。これにつきましては、今後ワーキンググループのメンバーでさらなる修正といたしますか、ファインチューニングを行った上で6月20日のワーキンググループの場でご検討いただき、その後に6月末をめどに、FISCのホームページにて公開をする。そういう段取りで、今進みつつあるというものです。

今日はこの場で有識者検討会の議論、報告書の中身と、今時点のチェックリストのたたき台の関係を少しご説明させていただければと思っております。お手元の資料4をごらんいただきますと、その一番最後85ページというところに資料9という形で「API接続先チェックリストワーキンググループによる集合的な検討」という論点メモを、前回ご提示させていただいたものです。この中で、チェックリストはどのようにあるべきか。どのように作られたチェックリストがこの報告書の一部として取り扱われることとなるか、ということで、何点か整理させていただいております。3段落目のところから書いていますが、まず「FinTech検討会におけるタイプⅢに関する提言内容と整合的に進められることが必要である」ということです。ここにつきましては、今回ご検討いただいた中で、本報告書の20ページのところに「関係者間の協調」という部分にチェックリストについても言及させていただいております。いわく「FinTech業務における適切な安全対策の実施には、金融機関、ITベンダー及びFinTech企業の3者が、密接に協調することが不可欠である」ということです。したがって「協調の手段として、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」ということが報告書の提言です。

「そのためには、例えば、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も位置づけ、簡素化も含め内容を見直すことが考えられる」ということとして、今回チェックリストワーキングで検討されているチェックリストもそのようにあるべきであるということです。

あと資料9のところに書いてありますが、「タイプⅢにおける『外部委託基準の準用ルール』」を踏まえる。ここは今回データの保全と本人確認について金融機関に安全対策上の部分責任が生じるというので、そうした部分についてはチェックリストに含まれる必要があるということです。

あと、「及び」ということで「必要最低限の安対基準」を踏まえらるる必要があるとい

うことです。ここについては、報告書の該当部分でいいますと、30ページのところになります。上のほうに、「金融業務を担う情報システムにおいて最低限実施されるべき基準として策定される『必要最低限の安対基準』は、FISC会員に限らず、金融関連サービスの提供に携わる事業者においても、踏まえらるべき基準であると考えられる」とされているところに由来するものでございます。

その上で資料9の続きですが、「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が必要である」ということで、これにつきましても報告書の30ページのところに図表10をもとに書かれております。このFinTechの検討会と全銀協様が事務局としてやられている銀行APIの検討会あるいはその他の検討会との関係というのを意識してつくられる必要があるということです。

資料9に戻りまして、それ以外でいいますと、こうしたチェックリストを「FinTech企業の負担軽減の観点から、社会的規範性を持ったチェックリスト」にするべく、「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」ということも要件として挙げています。

その上で最後ですが、次の段落の後半、「環境変化等が生じた場合にも、以上の集会的な検討が行われ、成果物の内容が継続的に見直され、実装・運用されることが期待される」ということが有識者検討会の検討内容になります。

それが今のチェックリストワーキングの検討状況に、適切に反映されているかどうかということです。それをご確認いただくに当たっては、まず資料7をご用意ください。チェックリストをまずご利用いただくに当たって、その使い方をご説明する必要があるだろうということで「API接続チェックリストの取扱説明書」というものを今回ご用意しようとしております。そこの冒頭の目的で書かれていますとおり、このチェックリストというのは、「銀行とAPI接続先が効率的にコミュニケーションを行うためのツール」であるというふうにいつています。要はこのチェックリストに書かれていることがAPI接続先において守られていないといけないというものではなくて、関係者が対話を行うためのあくまでもツールにすぎないといえますか、そういう位置づけにあるということを明確に書いているということです。これは「協調の原則」に適うところだと思います。

かつ、「機密性に関する確認項目を中心に策定したものである」ということです。外部委託基準の準用で語っていましたが、データの保全と本人確認というのは、そういう意味では機密性というものに包含されますので、そうした機密性に関する確認項目を中心に策定

されているという観点においては、外部委託基準の準用ルールを反映されているというふうに理解されると思います。

その下に今回のチェックリストの構成要素というものが、図表も含めて書かれています。その中でまず①番としまして、「全銀協が定める安全対策の遂行能力」ということで全銀協が取りまとめられた『『セキュリティ原則』に基づいて策定する』ということを確認しています。これはそういう意味では、安全対策に関する基準、ガイドラインを検討されるほかの集団の検討と整合的なチェックリストをつくろうとしているということが確認できると思います。

「②FISC安対基準の遂行能力」を取り込むということ、これは特に再委託管理に言及されている部分ですが、そうした観点においても、いろいろな集団で行われている検討と整合的なものをつくろうとしているということでございます。

③番目の「基礎的な安全対策の管理・運営能力」ということにつきましては、先ほどご説明しました必要最低限の安対基準というものを取り込むということで、ご説明した要件に適合しているものと思います。ただし、ここにつきましては、必要最低限の安対基準は今般の安全対策基準の改訂過程において初めて世に出てくるものでございますので、現時点においては存在しないということで、安全対策遂行能力のうち基礎的な部分ということで暫定的にチェックリストに加えているという位置づけになっております。

チェックリストにはその他の確認項目として、「利用者保護態勢等」についても、メンバーの意見を踏まえて追加しているという構成になっております。

以上のことから、チェックリストは、有識者検討会の議論と整合的に行われていると考えられると思います。

実際にチェックリストの実物について、若干補足をさせていただきますと資料6にいろいろな具体的な項目がつけられています。

まず対象者ですが、お気づきの方もいらっしゃるかもしれませんが、このチェックリストのタイトルが、「API接続先チェックリスト」ではなくて、「API接続チェックリスト」としていることが、対象者のところを見ていただくとわかると思います。すなわち、API接続先が対象者とするだけでなく、対象者の中には銀行というものもあります。あるいは両者を合わせた共通というものもある。そういう意味においてはAPI接続に携わる関係者が適切に情報開示を行ってコミュニケーションを行うために必要な項目がピックアップされている。要は一方向でなく双方向であるということです。

あとは具体的な手法例ということで、縷々方策が提示されています。これにつきましても、コミュニケーションのツールとして使いますので、この手法例がとられていないといけないというものでもありませんし、これ以外の手法例がとられてはいけないというものでもないということでございます。あくまでも関係の皆様が効率化を目指して、あらかじめ共通部分について合意形成を行っておく、という趣旨の範囲内で具体例が挙げられるべきであると考えて、今時点で可能な範囲で挙げている、ということをご理解いただければと思います。

あとは本有識者検討会との関連についていいますと、資料で4ページ、通番でいいますと11、12、13のところに、外部委託管理という項目があります。この中で特に12あるいは13ですが、ここについては、API接続先が外部委託をしている場合に、その外部委託先をどのように管理しているのか、ということです。ここについては、従来再委託管理というのは、かなり多岐にわたる項目についてチェックが行われておりましたが、極めてシンプルな項目になっています。いわく、12番のところでいいますと、「外部委託事業者から保証型監査報告書を受領して説明を受けている」という極めてシンプルなチェック項目になっています。これにつきましては、今回の検討会の過程においてクラウドのリスク管理策を補完していただいた中で、保証型監査報告書の有用性をご提案いただいたところを踏まえたチェック項目になっています。例えばこうした工夫をしながら、チェックリストそのものの簡素化ということを、メンバーは意識して検討を行っているということです。

あとお手元に資料8をご用意ください。有識者検討会の報告書の中では、社会的規範性といいますか、いろんな方々に利用していただけるものにしようと、そうすべきだということで、このチェックリストの検討過程にできるだけ多くの関係者が参画していただくべきであるという提言をいただいています。それをどのように実現していくかということが、資料8です。

今回できたAPI接続チェックリストにつきましては、まず試行版という位置づけにしようという検討を行っております。この意図としましては、実際このチェックリストについて、現場の皆様にご利用いただいて、できるだけ多くの方々にご利用いただいた上で、その利用した中でのご意見あるいはご不明点など、さまざまな情報をいただくことによって、チェックリストの策定過程にできるだけ多くの方に参画していただくという工夫をしております。

したがいましてAPI接続チェックリストは、6月末時点では試行版という位置づけで公開する方向で今検討が行われています。いろんな多くの業態の方々にご利用いただいた上で、さまざまなご意見を取りまとめて最終の確定という手続きに進めていってはどういうふうに考えております。この有識者検討会の委員の方々にもぜひ試行していただいてさまざまなご意見をいただき、中身をブラッシュアップしていければということです。

その上で先ほど有識者検討会の報告書の中で残る1つが、これを継続的に見直していくということをどのように行っていくかということがあります。これにつきましては、まだチェックリストワーキングの場で議論しておりませんで、6月20日の場で議論した上でどのように継続的に見直していくかということを明らかにし、6月末のチェックリスト試行版の公開と合わせて、一般の皆様にご利用いただけるようにご提示しようと考えております。

以上ご説明しましたように、本有識者検討会の提言内容と整合的な形でチェックリストの検討が行われております。ですので、ぜひ委員の皆様には、そうした状況をご理解いただいた上で、このチェックリストについて、引き続き有益なご意見をいただければなと思っております。

私のほうからは以上でございます。

○岩原座長 ただいまのご説明につきまして、ご質問等ございますでしょうか。どうぞ、神田さん。

○神田オブザーバー 金融庁の神田です。API接続チェックリストの試行版についてご説明いただきまして、ありがとうございます。短期間でステークホルダーの方々のワーキンググループを取りまとめていただいて、こういう形でほぼ決着を見ることができるといことで、事務局の皆さん、あるいはワーキンググループの皆さん、大変お疲れさまでした。

1つお伺いしたいのは、細かい内容というよりは、やはりこれは銀行とFinTech企業が、このチェックリストをもとにしっかりと実務的につながっていけるかどうか、実務的に耐えられるかどうか、という点です。特にFinTech企業側にとって、納得できる内容かどうかという点だと考えています。今日いらしていただいているFinTech企業の方で、このチェックリストの検討に参加した、あるいはこの内容をごらんになってどういうふうにお考えになっているのかについて伺いたいと思います。

また、このチェックリストが、事業を始めたばかりの **FinTech** 企業にとってもやさしいものであるという点も重要だと思います。既に大きなビジネスをされているマネーフォワードさん、マネーツリーさん、freeeさんといったメンバーの方々には使いやすいけれども、これからビジネスを起こそう、あるいは大きくしていこうという方々にとっても使いやすいものかどうか、どういう形でご検討をいただいたのか、あるいは、どういったご感想をお持ちなのか、という点についても教えていただければというふうに思います。

○マクダッド委員 **FinTech** 協会のマクダッドです。神田さん、ありがとうございます。同じようなことを発言させていただこうと思っておりました。

まず、事務局の皆様へ感謝したい点ですが、チェックリストの内容がとても読みやすく、これは結構出発点としてとてもいいなと思っています。そして委員の皆様、大変お疲れさまでした。

まだ試行版ということですが、1つ気が付いた点は **UX** のところで、ソフトウェアと同様に **UX** がとても大事かと思うんです。先ほど神田様がおっしゃっているのは、このチェックリスト自体の **UX** は本当に小さい企業、起業したばかりの方々の方がこれを利用できるかという疑問があることだと思いますが、正直に言うと、私も同感です。**FISC** の安全対策基準に慣れている方ならば、ああ、わかりました。例えば運用の3、運用の4のところを書いてあるので、それを参照すれば、ああなるほど、なるほどとわかるんですけども、起業したばかりの方々にとっては恐らく難しいものであり、**UX** として重要な点は、どういったリスクに対して統制を行おうとしているか、それを分かり易くすることがとても大事なのではないかなと思っています。

例えば1つだけピックアップすると、ウイルス対策に関して最近では標的型の攻撃メールが大きな問題になっていると思います。安全対策基準に慣れている方は、今の内容でも標的型攻撃を発想できるかもしれませんけれども、本当に起業したばかりの人は、ああ、じゃウイルス対策ソフト入れたからもうそれで大丈夫です、と思ってしまうかもしれません。今後、このチェックリストの維持管理は **FISC** の仕事になるか **FinTech** 協会の仕事になるかわからないですけども、エコシステム全体での活用を想定した場合、チェックリストを見ればどういったリスクが存在しているかがわかる、教育的要素を含む内容にしないといけないのかなと、全面的にこれを拝見した感想です。

以上です。

○藤永企画部次長 補足をしますと、ワーキンググループの検討の中でも今神田様からいただいたご意見はありました。やはり FinTech企業の規模が多様である中で、果たしてどのくらいの規模を対象にするのか、あるいはあらゆる規模、存在している多様な規模を前提として個別につくるのかという議論はありました。そこについては、まずは一旦こうした形で試行版として世に出させていただいた上で、ぜひ、今マクダッド委員からいただいたようなご意見を踏まえて、さらによりよいものにしていきたいと思っております。

我々の議論の中で大きな前提としましては、ここで書かれていることができていないともう門前払いになるのか、というと決してそのようなことはなく、先ほどお話ししたようにあくまでもこれはお互いがどういう状況であるかということを確認するためのツールにすぎないので、この中でできていないことがあるからといってAPI接続しないということでは決してない、ということです。銀行の委員の方々からもそこは強調してほしいということをおっしゃっていますので、できるだけこのチェックリストがミスリードされないように、先ほどのUXの話もそうですけれども、ミスリードされないようにつくっていくのが重要かと思っています。えてしてこういう共通のものができて世に出ると、これがルールであるかのように受け止められかねない。ただ、これはルールでなくて、あくまでもコミュニケーションのためのツールであるということです。これができるかといけないという、そうした強制力を持ったものとして決して受け止められることがなく、かつ幅広い利用者の方々で利用しやすく理解しやすいものにこれからしていく、ということを前提に試行版ということで、世に出させていただければと思っております。

以上です。

○岩原座長 藤永さん、ありがとうございます。ほかに何かございますか。

轟木さん、どうぞ。

○轟木委員 API接続チェックリストについては、FISCに加盟しているかに関わらず、FinTech企業や色々な業態の方々には一般公開するとお聞きしておりますが、FISCの安対基準についても同様に、一般公開するという理解でいいのでしょうか。

○藤永次長 現在、安全対策基準の改訂を進めるための安全対策専門委員会というの

が5月の半ばから始まっております。当然その検討が行われた後の安全対策基準については、広く公開を一般にするということと、あとはその検討過程も早い段階から皆様に公開をするということで、5月に行われた安全対策専門委員会初回のときにそうした方向性が、委員の皆様によって確認されているということです。

したがって、安対基準については検討する過程から、随時広く一般の皆様に公開をさせていただいて、必要に応じてご利用いただけるものにしようと思っております。チェックリストの関係でいいますと、先ほど申し上げましたように、チェックリストはあくまでもルールではなくて対話のためのツールですので、そこが誤解が生じないような形で安対基準上位置づけるといいますか、ちゃんと安対基準との違いといいますか、そういうのを正しく皆様にご理解いただけるように、情報発信していく必要がある、と考えております。

以上です。

○岩原座長 ほかに何かございますか。

よろしいでしょうか。それでは、藤永次長、どうもありがとうございました。

検討会の閉会に当たりまして FISC の渡辺理事長よりご挨拶をお願いしたいと思います。
渡辺理事長、よろしくお願いたします。

3. 理事長挨拶

○渡辺理事長 理事長の渡辺でございます。皆様にはご多忙の中、6回にわたりました検討会にご参加いただき、まことにありがとうございました。

本検討会では、FinTech をテーマに取り上げるに当たりまして、まずその姿を明らかにすることからご検討をいただいたというふうに理解しております。

その結果、金融機関による統制という根本的な観点から、FinTech をタイプ別に類型化していくという、我々これを始めるに当たって世界でどういう取り決めがなされているかということ調査したのですけれども、ここまで類型化して整然と議論を進めているという国は今のところあまり見当たらないという意味で、世界でも類を見ない提言をいただいたと理解しております。

こうして **FinTech** の姿を明らかにしたことによりまして、問題を的確に特定する、どこにどういう問題が生じるかということ論理的に解明するということができ、かつ、それに対しまして効果的な対策、どういう対策をしたらいいのかということについても、論理的な観点からご提言をいただいたというふうに理解しております。

また、**FinTech** は多岐にわたるテーマでございますけれども、わずか9カ月の間、計6回の会議という短期間で報告書を取りまとめていただくことができ、これは政府を含めまして非常に時間のスケールと申しますか、スピードが大事だという認識がございますけれども、**FISC** としてもそういう観点からできるだけ全速力で走るということをしてきましたけれども、皆様のご協力、バックアップによってそれが可能になったというふうに理解しております。

そういうことができました前提としまして、我が国において当センターが30年以上にわたって安対基準をつくって維持してきたという過程で、金融情報システムの関係者が協調して集合的な検討を行う、先ほども報告書の最終バージョンの議論の中でも、協調して建設的に話し合うことが大事だということを提言しておりますけれども、この**FISC** の場というのもそういう具体的な場になっておったということが非常に大きな原因であったというふうに考えます。

すなわち、**FinTech** というものを検討するに当たりまして、我が国では、例えばほかの国で行われているように、新たにスクラッチからどういう関係者を集めたらいいかということで、関係者を集めて全くスクラッチから議論をするということは必要なく、既にある集合的な検討体、こういう有識者検討会でありますとか、今後予定されている安全対策の専門委員会という既にある場において、既にある安対基準を**FinTech** に適用した場合、拡張した場合にはどういう問題が生じるかというアドオンと申しますか、付加的な問題を検討するというだけで足りたということでございます。これが非常に短期間に建設的な成果をいただいた大きな原因であるというふうに、私は考えております。

当センターによって涵養されてきたこういった土壌というのは、非常に変化の激しい世の中におきましては、**FinTech** にとどまらず、今後さまざまに登場するであろう金融情報システムに関するいろいろな新しい動きについて、我が国が世界に先駆けてと申しますか、世界に遅れることなく効果的、弾力的にそれに対応するということができる、1つの源泉となるのではないかというふうに考えておりまして、こういう環境というのも**FISC** としては今後とも維持していきたいというふうに考えております。

他方で、本検討会では先に行われました岩原座長、瀧崎座長代理という同じメンバーで行われました外部委託に関する検討会の提言内容を踏まえて、その延長線上でさらに踏み込んだ検討を行っていただいたという側面がございます。これも物事をうまく取り運べた1つの大きな要因ではないかと思っています。例えば外部委託の検討会では、安対基準の考え方をベースとして、従来当然のことながらシステムの安全性の確保というのが、唯一の公準ということでありましたけれども、それに加えまして企業価値の最大化ということ、これも同様なしはそれ以上の価値がある。そういう追求すべき価値であるということをご提言いただきましたけれども、本検討会では、FinTech への取り組みを通じたイノベーションの成果の享受ということで、企業価値の最大化の具体的な方法ということになると思いますけれども、それを原則とルールという形でご提言いただいたというふうに理解しております。

また、外部委託の検討会ではリスクベースアプローチに従った安全対策基準の適用方法というのをご提言いただきましたけれども、本検討会ではさらにそれを深めて、そもそも安対基準の適用対象はどうあるべきか。そして安対基準の適用対象外に対して、FISC はどのように取り組むべきかという根本的な問題についても検討を進めていただき、それを踏まえた意見表明をいただいたと理解しております。

さらに外部委託検討会では、重要なシステムという概念について議論、意義とか外延内包を明確にされたことが非常に大きな収穫だったわけでありましてけれども、本検討会ではクラウドサービスが重要な情報システムで利用された場合についてご検討いただきまして、以前のクラウドに関する検討会では必ずしも十分な光を当てることができなかった部分についても光を当てていただきまして、その従来からの提言の内容を補完していただいたという側面もございます。

その検討過程では金融機関のシステム資源の調達といいますか、システムをどういう構成要素から構成していくかということの歴史まで振り返っていただきまして、その延長線上に金融機関におけるクラウドという現在の状況の歴史的意義のようなものを皆さんに議論していただきまして、さらにクラウドサービス固有の性質、今までのシステム、アプローチとどう違うのかということについても極めて明快な分析をされ、これについてもほかの国では必ずしもそこまで突っ込んだ議論はされていない部分であるというふうに理解しております。

このように外部委託と FinTech の両検討会を通じまして、一貫した深度ある議論をい

ただいて、その結果個別のリスク管理策から安対基準の考え方という原理原則、さらには、FISC のあり方まで含む、全体に非常に範囲の広い議論をされ、かつそれがそれぞればらばらに部品としてあるのではなくて、統合的な一体的な体系として提示していただいたということで、非常に貴重な議論をいただいたと理解しております。

こうして最終報告書をまとめることができましたけれども、両検討会を通じてご協力、ご指導いただきました、岩原座長、淵崎座長代理を初め、委員、オブザーバーの方が熱心かつ精力的にご議論をいただいたということの賜物でございまして、改めて深く感謝を申し上げます。

今後は両検討会の提言内容を踏まえまして、常設の安全対策専門委員会におきまして、安対基準の改訂、これが最終的なゴールだったわけでございますけれども、それが行われることとなります。そこではこの有識者検討会での原理原則に立ち返った提言内容を、実際に金融情報システムの運営、開発の現場におられる皆様方が理解しやすく利用しやすい、抽象的、高尚な哲学的観念論ではなくて、実際にそれを使って仕事ができる、そういう理解しやすく利用しやすいものにするという観点から、原理原則は曲げないにしても、そういう観点から議論していただくというふうに考えております。

また、今回の安対基準の改訂はその初版が策定されました、昭和 60 年以來の抜本的かつ大規模な改訂。考え方自体を抜本的に変えるわけですから、具体的なそのルールブックというものも抜本的に書きかえなければいけないという意味で、30 年来の抜本的な大作業になるという予定でございます。そこでは有識者検討会でご提言いただきました、来るべき時代の中核となる新たな安全対策の考え方が適切に反映され、その結果として金融機関が将来にわたって環境変化に対応しつつ、システムの安全性の確保と企業価値の最大化が可能となるよう、そうした安全対策基準というものをつくるべく最大限の努力をしたいというふうに考えております。

まことにありがとうございました。

○岩原座長 渡辺理事長、どうもありがとうございました。

以上で本日の議事は全て終了となります。全体を通して何かご質問等ございますでしょうか。

最後に、今後の事務局作業の予定について小林企画部長よりお願いいたします。

4. 事務連絡

○小林企画部長 皆様、どうもありがとうございました。これから我々事務局で報告書を取りまとめる作業に入っていきますけれども、今後の動きをご紹介させていただきます。

議事次第のローマ数字V番、事務連絡というところをご参照ください。今後、以下の作業を予定しております。

まず、報告書のニュースリリースと PDF の配布でございます。今月6月末までに FISC のホームページで一般向けのダウンロード提供を予定しております。

また、本日第6回の検討会の議事録・会議資料は、同じく6月末までに FISC のホームページで公開させていただく予定でございます。ただし、先ほどのAPI接続チェックリスト（試行版）ドラフト及び取扱説明書ドラフトは、6月末までリバイスを重ねる予定ですので、これ以外を今回の第6回の資料としては公開させていただく予定でございます。

3つ目でございますが、この報告書に関する全国説明会を、7月27日札幌を皮切りに、仙台、名古屋、大阪、福岡、岡山そして8月24日東京と、全国7カ所に説明に行脚する予定です。本報告書の要旨を1時間ほどで説明する予定にしています。また、外部委託の報告書と同様、この報告書の英訳版への作業にも着手する予定にしています。

私からは以上です。

5. 閉会

○岩原座長 それでは、これにて第6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。

これまで熱心かつ活発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