平成28年12月22日

公益財団法人　金融情報システムセンター

第２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12月１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
	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
	大石 秀一	(代理出席)株式会社南都銀行 システム統括部 副部長
	廣瀬 明倫	(代理出席)住信 SBI ネット銀行株式会社 FinTech 事業企画部 シニアマネージャー
	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
	村上 隆	株式会社ＮＴＴデータ 第四金融事業本部 企画部ビジネス企画担当 シニアスペシャリスト

	長 稔也	株式会社日立製作所 金融システム営業統括本部 事業企画本部 金融イノベーション推進センタ センタ長
	加納 清	（代理出席）日本電気株式会社 パブリック企画本部シニアエキスパート
	梅谷 晃宏	アマゾンウェブサービスジャパン株式会社 セキュリティ・アシュアランス本部　本部長 日本・アジア太平洋地域担当
	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 主任統括検査官　兼　システムモニタリング長
	中井 大輔	日本銀行 金融機構局 考査企画課 システム・業務継続グループ企画役
	希代 浩正	（代理出席）経済産業省 商務情報政策局 サイバーセキュリティ課 課長補佐
	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　議事内容

１.【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

〇岩原座長　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いたします。

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きましたご意見について、事務局からご説明をいただきたいと思います。FISCの小林部長、よろしくお願いします。

〇小林企画部長　それでは議事１の資料をごらんください。前回第１回の有識者検討会以降にいただいたご意見およびご回答をまとめさせていただいております。全部で３社の委員の方から７つのご意見を頂戴しました。簡潔に１つ１つご説明申し上げます。

いずれにしましても前回の議事３「安全対策検討のあり方」に関するご意見でございます。１番～３番は、デロイトトーマツの荻生さんからいただきました。

まず１番は、「安対基準の適用先について」。

現在、安対基準の適用先として想定しているのは、金融検査マニュアルに基づく監督が行われる銀行、保険会社を中心に、「金融、保険、証券、クレジット等金融業務を営む業界の各社」とされています。

一方、FinTechの発展に伴い、法的な枠組みとビジネスの実態に乖離が生じうることが明らかになっています。例えば決済においては、金額に差異はありますけれども資金決済法に基づく資金移動業者と銀行が同様のサービスを提供しているほか、資金決済法に基づく仮想通貨事業者はFXに類似するサービスを提供しています。また、店舗はカード会社（アクワイアラ）からも決済代行業者からもカード決済機能の提供を受けることができます。このように、現在では業態間の垣根が低くなり、同等のサービスが法的根拠の異なる事業者から提供されている状況にあります。安対基準の趣旨に照らし合わせれば、顧客が受ける便益やリスクが同様であれば、根拠法の違いによらず等しくシステムリスクへの手当てがなされるべきであるため、安対基準の適用先も幅広くカバーされるべきと考えられる、というご意見を頂戴しました。

回答欄をごらんください。この回答に限りませんが、議事４にて「安対基準の対象外となるFinTech業務の取扱い」として原案を作成していますので、後ほど詳しくご説明させていただきます。

同じデロイトトーマツさん、２つ目「金融機関の主導性の判断について」でございます。

論点２では「①検討対象となるFinTech業務のタイプ」として、金融機関の関与が主導的か受動的か、および金融機関の支配の有無に応じて、３つのタイプに類型化しています。特にFinTechに特徴的なサービスとして、金融サービスの提供主体がFinTech企業であり金融機関が従属的にデータ等を提供する形態についてタイプⅢが設けられています。これは前回ご説明したとおりでございます。

ここで、タイプⅠ～Ⅲの間で安対基準の内容が同一の場合は、いずれに分類されるかは問題とならないけれども、タイプⅠ～Ⅲの間で内容が異なる場合、事業者の判断を支援するため分類の考え方や基準を示すことが妥当ではないか。

例えば、米国P2Pレンディング大手のLending Clubなどは、自社サイトで借り手を募集する一方で、ローンの組成はIssuing Bankと呼ばれる提携銀行が実行しています。この場合、顧客接点はFinTech企業であるためタイプⅢと解されるけれども、一方でローン組成に関わるコンプライアンス等は全て銀行の責任で行っているため、タイプⅠとする余地もあります、というご意見を頂戴しております。

こちらはご意見として拝聴しまして、今後の日本国内におけるユースケースの出現状況を見ながら対応の要否を検討させていただきたいというふうに考えております。

おめくりください。デロイトトーマツさん、３つ目でございます。論点３の「外部委託の責任について」。

金融機関は常に委託元ということで、前回㋑、㋺、㋩の３つに類型化していますが、決済分野においては、例えば決済代行業がアクワイアラに対し加盟店開拓・管理の責務を負っている一方で、アクワイアラは決済代行業者に対して売上金の送金等カード決済機能を提供する責務を負っている。このように、関係者が相互に役割を担っていることから、「金融機関は常に委託元」とは解しきれないケースがあることに留意するべきである、というご意見を頂戴しています。

これも先ほどの１番と同じように、安対基準の対象外となるFinTech業務の取扱いということで、後ほどご説明させていただきます。

続く４、５、６の３つは南都銀行さんから頂戴しました。

４番、「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」ということでご意見を頂戴しています。金融機関が完全に受動的立場となる場合は金融機関には何らの統制の手段等が無いことから、金融機関において顧客に対する安全対策上の責任は生じないと解される前回お示しされた考え方に異論はない。しかしながら、FinTech企業のサービスにおいて万一事故が発生し、顧客から金融機関に対して、FinTech企業のサービスの利用に当たっての注意喚起が十分でなかった、といった安全対策上の部分責任が問われる可能性が否定できないのであれば、金融機関として講じるべき対策についても、要否を含めて議論してもよいのではないか。

いただいたご意見を踏まえ、議事３「FinTechに関する安対基準適用上の課題」の中で「金融機関に責任が生じない場合の取扱い」について、対策を原案として作成していますので、これも後ほどご説明させていただきます。

同じく南都銀行さん５番、これは「安対基準の対象とすべきFinTech業務のタイプ」についてでございます。

FinTech業務の金融業務と非金融業務の分類基準について、垣根が曖昧になっており、具体的な分類について検討しておく必要があるのではないかというご意見でございます。

我々の分類の中でも、一度は金融業務と非金融業務ということで分けておりますけれども、この区分を明確にすることは困難だと考えていまして、また適切ではないのではないかというふうに考えております。その理由の詳しいことについては、後ほど議事４「安対基準の対象外となるFinTech業務の取扱い」の中で詳しくご説明させていただきます。

南都銀行さん最後、６番でございます。金融業務を担うか否かにかかわらず、金融機関等のコンピュータシステムは、社会的責任を負っています。ということで、FinTech業務をまず金融機関「主導」「受動」で分類すべきではないか。その後で「金融業務」「非金融業務」で分類するほうが望ましいのではないかというご意見でございます。

最終的な結論は同じことになるかと思いますが、「金融機関が行う金融業務」を安対基準の対象としていることから、まずは「金融業務」「非金融業務」ということで分類させていただこうと考えております。

最後７つ目、みずほ銀行さんからいただきました。論点１に関してです。「金融機関受動」かつ「交渉なし」のモデルは安対基準の対象外ですが、顧客のID・パスワード・追加認証情報等を保持してスクレイピングを行っており、顧客保護の観点からリスクが高い

と考えられます。

「スクレイピング」に関する規制（PSD2では違法とみなされるケースがある。米国では認可制）について、安対対象外のFinTech業務への意見表明（論点１）の中で言及する必要があると思われます。

こちらもいただいたご意見を踏まえて、今回議事４の「安対基準の対象外となるFinTech業務の取扱い」の中で意見表明の原案を作成していますので、後ほどご説明させていただきます。私からは以上です。

○岩原座長（00:12:43～00:13:08）　それでは、ただいまのご説明に対してご質問ございますでしょうか。

特にございませんか。

２.【議事２】プレゼン「FinTechベンチャーのセキュリティ維持・向上に向けた当協会の取組み」（一般社団法人FinTech協会 理事 Mark Makdad委員）

○岩原座長　続きまして議事の２つ目としてマクダッド委員より、議事２についてのご発表をいただきたいと思います。マクダッド委員、よろしくお願いします。

○マクダッド委員　皆様、よろしくお願いします。

弊協会においては最初の頃から、結構セキュリティに関して、当局もしくは銀行に接するときはどうすればいいかという意見が当初からありました。本日は、弊協会、特にベンチャー企業、FinTech企業におけるセキュリティの考え方、あるいは、今後どういうふうにセキュリティに取り組んでいくか、さらに、FISC様に対して何を要望するかなど、簡潔に発表させていただければと思っております。

私は、FinTech協会において、APIとセキュリティの分科会の担当理事を務めているマクダッドです。まず最初に、FinTech協会について、まだご存じでいない方がいらっしゃるかと思い、FinTech協会について簡潔に紹介させていただきます。

FinTech協会は設立されて、２年たったところです。もともと、2014年に、いろんなFinTech企業がミートアップで集まっておりまして、とてもカジュアルな場で、ビジネスチャンスなどの情報交換をしたりという、ネットワークの場がありました。そういうのを開催し始めると、毎回毎回FinTechという言葉の認知が高まるにつれ、参加人数がだんだんふえまして、第１回のときはわずか20名しかいなかったんですけれども、FinTech協会という設立を発表した６回の時には、170名にもなっていました。

ミートアップの過程で、次第に、協会を設立しようという話が、みんな共通の話題となりました。ベンチャー企業は、４～５人の組織ですので、例えばFISC様に対してなかなか意見を伝えられない、とかそういう課題があり、協会になることによって、共通な課題の解決に取り組んでいこうということになって、去年の９月30日に一般社団法人FinTech協会が結成されました。

FinTech協会の概要ですけれども、設立以来１年ちょっとたったところですが、理事は11名おりまして、皆FinTech企業の本業をやりながら、FinTech協会の業務をやっています。資料の一番下をごらんいただきますと、弊協会のミッションとして「FinTechベンチャー企業及びFinTech生態系の成長を支援し、個人及び法人により便利で役に立つ金融サ

ービスの提供を目指して」おります。そして、日本のみならず「日本から世界へ」という視野も持っていまして、それと同時にグローバルでの情報を日本にも流せれば、と考えております。また、協会はオープンな組織で、一般企業及びその関係者、法人会員もしくは個人会員としても、入会いただいております。

現在、ベンチャー会員は50社以上（56社ぐらいだと思うんですけれども）、幅広くいわゆるFinTech企業として、PFM、会計、決済、資産運用、仮想通貨、セキュリティなど、いろんなFinTechの中の業種のベンチャー企業に参加いただいております。

一方、法人会員は、言うまでもなく金融機関様ですとか、クレジットカード、生保損保、証券会社、ITベンダー、通信関連、コンサル会社などに、会員になっていただいております。

次のスライドは、最近どういう活動をしているかということですが、まずはそもそもFinTech協会は、ミートアップの場として始まりましたので、一般向けのイベントを開催しております。一番直近は先々月１周年のイベントで約150人に参加していただいて、ネットワーキングを行いました。

また、各理事は分科会を担当しておりまして、例えばコンプライアンスの分科会では、中間的事業者と銀行代理業務とそういったテーマに取り組んでいます。APIセキュリティ分科会では、私が担当理事となっています。会計分科会では、最近ですと電子レシート、eレシートというのに取り組んでいます。

分科会の活動以外では、コンファレンスも主催しており、完全にPRになってしまいますけれども、本日から渋谷のベルサールで、「FinTech Japan2016」を開催しています。既に700人の登録をいただいているんですけれども、皆様、もし明日お時間がありましたらぜひベルサールのほうにお越しいただければ、FinTech関連の話を盛りだくさん聞いていただけます。

そしてもう１つ、協会の活動として、官公庁及び民間団体と情報連携があり、まさしく本日私がここに座っているこういう活動です。

次に、本題に入らせていただきたいと思っていますが、最初に申し上げましたように、FinTech協会ではなくFinTechミートアップだった頃から、経営者同志で「こういうのはどうすればいいですか」というテーマが幾つかありまして、その１つは「IT関連でいうとセキュリティはどうすればいいですか」というものです。特に少人数の組織で、FinTechという金融周りのサービスを作っていく中で、どうセキュリティを丈夫にしてい

くかという共通の課題がありまして、官公庁では制度はどうなっている、法律はどうなっている、ということを、互いに相談し合ったりしていました。

そうした中で、APIセキュリティの分科会の担当理事として、私がことしの３月からAPIセキュリティ分科会を開始して、主に共通課題であるセキュリティなどを、解決ではないんですけれども、まずは第一歩としてベストプラクティス的なところについて、協会内で情報を共有できればと思い取り組んでいます。

その悩みでいうと、読み上げなくても大丈夫だと思うんですけれども、まず、基本的にクイックレファレンスみたいなものがない、ことがあります。つまり起業をしたときに、ITに詳しくても詳しくなくても、大体どういうリスクがある、どういうところが（金融機関から）見られているというのが、例えばFISCに詳しい方だと恐らくすぐ言えるかと思うんですけれども、起業したばかりの経営者は、なかなか持っていない情報なので、そういうのを提供しておきたいというのがあります。

起業した後に、ある程度事業が拡大し、例えば金融機関様と協業する際、また新しくいろんな悩みが出てきまして、書かれていますように、チェックリストの項目、安対基準のようなチェックリストが（金融機関から）配られるんですけれども、例えば検討会でいうタイプⅠ、Ⅱ、Ⅲとかそういうことに関係なく、ASP利用だとしても、基本的にチェックリストが渡されます。それを、どう埋めればいいか、我々データセンター営んでいないのに、（データセンターに関するチェックに対して）どうすればいいですか、とかそういうのが結構あり、FinTech企業と金融機関の間のコミュニケーションコストが非常に高いというふうに感じています。

そしてワークスタイル、もう少しソフトなところなんですけれども、多分今まで銀行様だとかベンダーに対して、ベンダーと一緒に２者でITなどを導入してきたかと思うんですけれども、ベンチャー企業のように、10人とか20人ぐらいの組織だと、やはりワークスタイルが、何千人のベンダーと比べて全然違うところがあるので、それをセキュリティを確保しつつも、整理しておく必要があるのではないか、と思っています。

そうしたことから、弊協会としてはセキュリティガイドラインを策定することとしました。世の中に使えるガイドラインが無いか、といろいろ探しましたけれども、例えばISO27001であれば、余りにもちょっと抽象的な内容で、FinTechベンチャーとして第１段階としてはちょっとニーズが合わない。PCI DSSになりますと、カード業界でよく使われているセキュリティに対するガイドラインだと思うんですけれども、基本的にカード情報

に関わるものなので、カード情報を持っていないFinTech企業が大半であり、ちょっと合わないところがありまして、ある意味で具体的過ぎるというのもあります。

FISC安対基準になりますと、金融機関のための基準ではありまして、全くの素人もしくは経営者にとってはすぐ読んでわかりました、ITこうしろというような内容になっていないので、もう少しクイックレファレンスとして使えるものがあればいいな、ということになりました。

そして先ほどの説明と同じなんですけれども、FinTech企業のワークスタイルと乖離がありまして、例えばこのIPアドレスからじゃないと、このシステムにアクセスできない、というのがあり、結果としてリモートワークが禁止になってしまう。でもリモートワークが禁止になると、例えば本当に10人ぐらいの組織になると、システム上で何か問題があった、運用上で問題があったときは、その人が実は事務所まで行かないと対処できない、ということになり、結果としてダウンした時間が長くなったという、逆に悪い影響も出てくるかと思います。そのため、リスクを見ながらワークスタイルの違いを見たほうがいいのではないかと、そういう悩みがあります。

会員の悩みについて、アンケートや関係者とのヒアリングによって情報を集めて、左側に３つの枠で整理しておきました。まずは先ほど私が案内したガイドラインの構成としてクイックレファレンスということ。次に、もう１つリスクベースアプローチというところなんですけれども、それはある程度、FinTech企業と協業する際にどういうふうにリスクを見積もるというのは、金融機関に豊富な経験、十分あるスキルだと思うんですけれども、FinTech企業にそのようなスキルがあるかといえば、必ずしもそうではないところもあるので、そうしたリスクの考え方について、FinTech企業を教育しないといけないな、と思っています。

それと同時に、aのところですけれどもFinTechはスマートデバイスが主という点について、技術の変化に伴ってどういうリスクを見ればいいか、ある程度フォーカスしないと話が抽象的になっていて使えないということで、基本的に「スマートデバイス」そして「ウェブクラウド」にフォーカスしています。

最後に金融機関との協業にあたり、リスクについてコミュニケーションを上手にとる。そして、FinTech企業、少人数とはいいつつも金融サービス業である訳ですから、一定の水準のセキュリティを確保しないといけないと弊協会は思っています。

右側の弊協会の取り組み、どういうことをやっていくのか、ということですけれども、

ガイドライン自体については、クイックレファレンスとして、考え方としては２つの編、概念編とチェックポイント編というふうに作っていこうと考えております。概念編というのは、とある会社の例えばＣＥＯが読んでもなるほど何となくわかりました、というようなところ、チェックポイントはどちらかというと、システムの方がこれは本当にちゃんとやっているかどうか、確認できるようなものを作っていきたい、と思っています。

次のスライドですけれども、これは既存のFISC安対基準など公的なガイドラインで対象としている項目のうち、弊協会としてはクイックレファレンスにするために、どうしても割愛しないといけないところがありまして、どういうところが一番大事か、と整理してみました。説明に時間がかかる図なんですけれども、我々が優先的に対象としているかどうか、という○×△が付してあり、その上に例があります。

例えばなんですけれども一番左に各種ポリシー整備などが書いてあるんですけれども、それはFinTechサービスに余り関係なく本当に会社としてやるべきことなので、弊協会のガイドラインに敢えて記載するには及ばないと思います。その右のところを見ていただきますと、「FinTechサービスに直接影響するもの」と書いてあります。つまりFinTech企業が運営しているサービス、FinTechサービスに直接影響されるようなもので、さらに（B）のところを見ていただきますと、そのFinTechサービスが例えばアプリを開発していると、そのアプリ開発はそのものがFinTechサービスなのでそれは含まれる、とします。一方で「一般にクラウドサービスとして提供されるもの」と書いてあるんですけれども、FinTechサービスを例えば基盤としてクラウドのベンダーを利用している。当然そのサービスがクラウド上で提供されるものの、FinTech企業自身はデータセンターの建物や設備を管理している訳ではなく、確りとした事業者にアウトソーシングされていますので、優先順位は低いと考えて盛り含まないこととしてて×にしております。こういう整理をしておりますが、これは最終版ではありません。ぜひご意見があれば今日でもお伺いできればと思っています。

基本的にもう少し違う整理の仕方、もう少しFISCよりの整理をすると、データの管理、アクセスの管理、ログ取得、運用管理・監視、構成管理、あとは企画／開発／変更管理、こういった項目でこういったテーマでクイックレファレンスを作っていこうと思っていまして、そしてその中にチェックポイント的なところを各弊協会のベンチャー会員にチェックしていただきたい、と考えております。

そして次ですけれども、先ほどスマートデバイスと申し上げましたけれども、特に

FinTechの性質に応じたリスクを考えないといけないかと思っておりまして、特にAPIなどスマートデバイス、だんだんいろんなサービスが接続し合う中で、アプリケーション層とデバイス層のセキュリティはちゃんとなっているか。そういったところをFinTechとしての新しいリスク、リスクが高い領域と思っておりまして、特にデータ管理はとても大事だと考えております。

そしてこれはあくまでも想定しているチェックポイントの例ですけれども、時間の関係で割愛させていただいて、課題の認識のところで、ここまでの内容をガイドラインのベースとして策定を目指していきますけれども、各民間団体、もしくは本日、FISC様、あるいは全銀協様と協議をしながら、ガイドラインを来年の春ころに作っていく予定でございます。

そしてFISC様への要望なんですけれども、弊協会APIセキュリティ分科会での講演など結構いろんな発表をFISC様にいただいておりまして、基本的に引き続き協力しながら一緒に底上げといいますか、FinTech企業でも成功できるような仕組みを作っていただければなと思っています。

最後にスケジュールなんですけれども、未確定ながら来年の３月、４月あたりで弊協会のセキュリティガイドラインを発表したい、と考えています。ご静聴ありがとうございます。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。

３.【議事３】論点メモ「FinTechに関する安対基準適用上の課題」

○岩原座長　それでは、続きまして議事２つ目、論点メモ、議事３のご説明をFISCの藤永次長にお願いいたします。

○藤永次長　FISC の藤永です。お手元の資料の左上に議事３と書いてあるものをご用意ください。

まず最初に今回議事３と議事４と２つ用意していますが、わかりやすく言いますと、議事３は金融機関が FinTech に関してどういうふうに取り組むべきか、議事４は金融機関以外の FinTech 業務の担い手の方々がどういうふうに安全対策に取り組むべきであるか、期待しているか、ということをお話ししたいと思っています。

まず最初に議事３です。論点としては、表紙に書いてございますとおり、「金融機関における FinTech に関して、従来の安対基準を適用した場合に内在する問題に対して、どのようなリスク管理策を策定することが適切か？」ということです。

大きく５つお話ししようと思っています。まず検討にあたっての前提。その次にそもそも安対基準でどういうふうな責務を果たすことになっているか。その後にタイプⅠ及びタイプⅢに関する安全対策のあり方を、内在する問題を踏まえてご提案をしています。最後に関係者間の協調というテーマで１つご用意しています。

それでは早速、１ページおめくりください。まず、「検討にあたっての前提」です。前回お話ししましたとおり、FinTech 企業の担う情報システムに、従来の安対基準を適用した場合に内在する問題の有無を検討して、その後に安全対策のあり方、リスク管理策を検討するとしていましたので、本日はそうした最後のところまでの原案をご用意しています。

まず前提として認識しておく必要があるのではないか、ということで４点ほどかいつまんでご説明します。

１点目が「目標とすべき安全対策の効果の程度」ということでございます。これは第１回の検討会のときにお話ししましたとおり、FinTech 業務を担う情報システムについては、従来金融機関と IT ベンダーの２者で担っていたところに、FinTech 企業が加わる、そうした３者関係を前提とします。そのときに、安全対策の効果をどういうふうな期待値といいますか、目標として設定しておくように考えるのか、というところが非常に重要ではないかと思っています。

これについては顧客の立場に立てば、安全対策上の関係者が２者から３者に仮に変わろうとも、その効果が２者のときと同程度で確保されることが期待されているというふうに考えられます。これは我々のほうで「同等性の原則」と通称させていただこうと思っています。

また、２者と３者で同程度の安全対策の効果の実現を目指す場合は、前回お話ししました、中立性および有効性といった観点から、必要十分な範囲に留める。要は効果を２者のときよりも多く求める、あるいは少なくするというようなことではなくて、必要十分な範囲で調整を行うという観点が重要ということです。そういう意味では、金融機関、ITベンダー等の負担が必要な範囲を超えて増加することがないよう留意して検討がされるべきである、と考えております。

２点目は「安対基準における検討対象領域」を主にどこに定めるべきかという話でございます。「従来の安対基準」という言葉で前回もご説明していましたが、安対基準は非常に対象の範囲が広うございます。ここに書いてますとおり、「コンピュータシステムが収容される建物、設備」を対象とした設備基準、あるいは「ハードウェア、ソフトウェア等」を対象とした技術基準のようにモノを対象とした基準と、あとヒトを対象としたその開発管理、運用管理体制等を対象とした運用基準という２種類が大きくございます。

まず、モノを対象とする基準につきましては、やはり多岐にわたる FinTech 業務の出現が予想される中では、技術あるいはビジネスモデルなど環境が、かなり目まぐるしく変化していくであろうということでございまして、モノに対する基準については個々に各論をこの場で検討するのではなくて、FinTech 業務のリスク特性に応じた安全対策を金融機関において独自に決定されて、安全対策における基本原則（これは我々が外部委託に関する有識者検討会で定めたものですが）に従って IT ガバナンスが行われていれば十分であるのではないか、と考えております。

したがってこの場では、モノに対する基準ではなくヒトに対する基準、すなわち運用基準というものを主にご議論いただこうということを書いております。これは、多種多様な技術等に左右されることなく適用可能であるということでございます。

２ページですが、運用基準と一言に言ってもこれも非常に基準の数が多くありますので、その中で、特に今回 FinTech 業務において外部委託という形態で実現される、あるいはそれに近い形態で実現される場合があるということで、運用基準の中でも外部委託に関する基準を主な対象として皆様にご検討いただこう、と考えております。

その次３番目、「簡易なリスク管理策の性質」ということです。「簡易なリスク管理策」は修飾語に「簡易な」というふうに書いてございますとおり、重要な情報システムに対する統制が設定されることを前提として、それを一般の情報システムに対しては「緩和」することで導出されるという意味において「簡易な」という修飾語がついています。

ただ、これは別の面で考えてみますと、一般の情報システムにおいて簡易なリスク管理策をとるということは、すなわち安対基準においては「必要最低限の基準」というふうに表現されていますとおり、「最低限ここまでは実施しておくべき」ではないか、という拘束性も有しているという、そうした側面もございます。

したがいまして、簡易なリスク管理策を策定するにあたっては非常に慎重にやる必要があるだろうと。特に、FinTech 業務に関しては、前回お話ししたとおり、中立性や有効性を損なうという問題があるということで、そうした FinTech 企業を初めとして、携われる関係者の皆様の現場の声、その問題認識を正しく反映していく必要があるだろう、というふうに考えてございます。

最後に４番目ですが、「クラウドの利用に関する安対基準の取扱い」というところでございます。まずは FinTech 企業においてはクラウドサービスを利用されることが多いと思っていますが、クラウドサービスというのは、安対基準においては外部委託の一形態として捉えています。これは前回委員の方から、システムを利用するケースは必ずしも外部委託であるのかどうかというご意見をいただきましたが、安対基準の中ではクラウドサービスの利用というのも、外部委託の一形態としてまず捉えているということでございます。

クラウドサービスの基準というのは、先般の安対基準の第８版追補改訂から取り込まれていますが、当初有識者検討会で議論をしていただく中においても、クラウドに必ずしも固有の内容ではなくて、外部委託全般としても参考になる基準であるという認識を持っておりました。したがいまして、次回の安対基準の改訂においては、クラウドサービスでつくった基準というのを改めて外部委託全般に適用できるものは適用し、そうでないものはクラウド固有とするといったような整理が行われることが必要だ、ということを、外部委託の検討会で提言をいただいているというところです。

そうしたことがありまして、今時点でクラウドサービスを含む外部委託の全般的な安対基準というものが現状どういうものであるかというのが、今後の安対基準の改訂を待たないと存在しないということになっております。そうしますと、この検討会において実質的な検討はなかなか難しいということでございまして、暫定的にではございますが、今ま

で我々が外部委託の検討会まで議論してきた内容を踏まえた、安対基準の暫定的なイメージというのを別添でご用意しているというところでございます。これが１つです。

もう１つのクラウドに関して認識が必要な事項としましては、クラウドの有識者検討会と外部委託の有識者検討会の順番が前後しているということでございます。クラウドの検討会の後に外部委託の検討会が行われて、「重要な情報システム」というのがどういうものであるか、明確に提言されております。したがいまして、クラウドの報告書の中でも重要な情報システムについての管理策は一定書かれてはいるのですが、外部委託の成果を踏まえたものとはなっていないということで、不確実性が残る現状にあるということです。

そうしますと、簡易なリスク管理策が重要な情報システムに対する管理策をもとに導出されるということに鑑みれば、こうした事情にも留意することが望ましいというふうに考えておりまして、「なお」というところですが、こうした問題は我々事務局としても認識しているというところがあります。

したがいまして、本検討会においてクラウドを利用する場合の管理策について、補足的な検討も行うことが必要ではないかと考えております。こういう補足的な検討をあらかじめ行っておく、すなわち重要なシステムでクラウドサービスを利用した場合に、どういうふうな管理策が望ましいか、ということを検討しておきますと、その後 FinTech のユースケース、「重要なシステム」のユースケースとしてブロックチェーン・AI が登場した際にも、タイムリーといいますか、より迅速な検討がなし得るのではないか、と考えてございます。以上が前提のお話でございます。

次、６ページですが、ここからは本論に入っていくことになります。「従来の安対基準に基づく関係者の責務」ということで、そもそも関係者がどういうふうな責務を負うことに、今の安対基準ではなっているのかということでございます。これについては先ほどお話ししましたとおり、確定的なものは安対基準の次回の改訂を待たないといけないんですが、我々のほうで、検討に必要な範囲で整理を行った資料を、本日はご用意しています。これは事前には間に合わなくてお配りできなかったのですが、今日は皆様の机上に配付させていただいております。「議事３－参考１」という資料になります。ページ数でいいますと 15 ページある細かい中身なので、この場ではこの表の見方だけをご説明させていただきたいと思います。

１ページ目の一番上の行ですが、左側に「管理フェーズ」ということで外部委託、クラウドのときに整理された利用検討時、あるいは契約締結時というフェーズに分かれてい

ます。その上でテーマということで、統制の分類を項目としてご用意しています。これが全部で外部委託の安対基準で 33 項目に及ぶということになります。その統制の強度と、この表のインプットとなりました安対基準の項番及び外部委託の有識者検討会の該当ページを、リファレンスできるようにしております。

その上で責務を当事者ごとに分けていまして、【責務Ａ】というのが金融機関が担うべき責務ということでございます。これはもともと安対基準を読めばこのように理解できるというものです。

それを踏まえまして、金融機関の一次委託先として負う責務を【責務Ｂ－１】、仮にその先に再委託が行われる場合には、一次委託先が再委託先に対して果たすべき責務ということで【責務Ｂ－２】、それを受けまして金融機関の再委託先として負う責務【責務Ｃ】という形で４種類の責務に整理しています。要は金融機関の責務を、その委託先において３つに分解して書いているという、そういう表になってございます。

なぜこんな表を作ったのかといいますと、もともとのページ、本文のほうに戻っていただきまして、先般第１回のときにお話ししましたように、タイプとか類型を踏まえてこの図表１のような類型があるというときに、まずは FinTech 企業がそれぞれの類型の中における位置づけにおいて、どのような責務を負うのであるのかというところを、わかりやすくご理解いただくために作ったものでございます。

この表をもとにしまして、FinTech 企業がそれぞれの類型で、どういう責務を負うことになっているのかというのを、主なものをピックアップしたのが、７ページ、８ページに記載してございます。それぞれ、㋑は FinTech 企業が金融機関と IT ベンダーの中間に存在する場合、㋺は再委託先となる場合、㋩が一次委託先として再委託先が存在しない場合ということで整理しています。

例えばでいいますと、㋑の類型ですと、利用検討時には金融機関が客観的評価を実施するために必要とする情報を金融機関に提供する責務を負われている。あるいは金融機関からデータ管理を受託する場合には、漏洩防止策を講じる責務を負われている。そういうふうな読み方になります。

さらにそれが IT ベンダーに再委託されている場合には、その下の【責務Ｂ－２】ですが、今度は逆の立場で金融機関の再委託先を客観的に評価する責務がある。あるいは、再委託先に金融機関のデータ管理を委託する場合は、漏洩防止策を実施させる責務がある、というふうに解することができるということでございます。

次に８ページをおめくりいただきまして、そうした責務を FinTech 企業が担うことを前提とした上で、タイプⅠの場合、従来の安対基準を適用することで問題が生じることはないか。タイプⅢの場合、そもそも従来の安対基準、外部委託の基準を適用することが妥当であるか、という、こうした２つのテーマについて考え方を論点・原案としてご用意しています。

まず、「タイプⅠにおいて内在する問題と安全対策の在り方」、８ページ下のところからご説明させていただきたいと思います。第１回から本日までの間にかけて、FinTech 協会あるいはマネーフォワード社、当検討会に参画いただいた FinTech 企業に、この責務表をごらんいただいて意見交換をさせていただきました。その中で、幾つかの細かい観点、粒度を含めていろんなご意見をいただいたんですが、そうしたことを踏まえまして、恐らくこういう観点で本質的な問題というものを捉えることが皆さんにとっていいのではないか、ということで、ご用意しているものでございます。

まずタイプⅠにおいては、FinTech 企業は先ほどの【責務Ｂ】あるいは【責務Ｃ】を担うこととなります。そうはいいながらそもそも従来の安対基準では、金融機関と IT ベンダーの２者を念頭に置き策定されてきていましたので、【責務Ｂ】あるいは【責務Ｃ】で書かれていることは IT ベンダーが担うシステム運用を主な対象とし、IT ベンダーの安全対策遂行能力、それは従来から念頭に置いて策定されてきたものでございます。したがいまして、こうした責務を FinTech 企業が担われる場合には、FinTech 企業の安全対策遂行能力、先ほどマクダッド委員のほうからスタートアップ企業が比較的多いというお話もありましたが、そうした保有する経営資源等に比してバランスを欠いたものになっていないか、という問題が内在しているのではないか、と考えています。

そのため FinTech 企業に対して形式的に安対基準の適用を求めようとしますと、安全対策遂行能力が IT ベンダーと同程度にない FinTech 企業においては安全対策の負担、ここまで求められるとそれはさすがに過大であるというふうな認識を持たれるのではないかと。仮に、その負担を回避したいというようなインセンティブが生じた場合は、その結果として FinTech 企業のビジネスモデルの選択にゆがみを与える可能性があるのではないかと考えております。

先ほどの類型でわかりやすくいいますと、㋑の類型と㋺と㋩の類型で責務の量は圧倒的に違うということで、㋑の類型を形式的に求めようとすると、ビジネスモデルが㋺と㋩になりがちではないかということが、中立性の観点から問題ではないか、ということでご

ざいます。これは同時に、FinTech 企業が仮に過大な安全対策負担に何とか頑張って応えようというような努力（従来からされていると思うんですが）それを必要以上にやられてしまった場合には、場合によっては、FinTech 企業は内部の経営資源を安全対策に優先的に配分することによって、イノベーションを起こす、革新的な部分に経営資源を配分することができなくなってくる。結果としてイノベーションを損なう可能性がある、というような問題を秘めているのではないかと思っています。

そうはいいながら、一方で、FinTech 企業が加わる３者の関係であっても、先ほどの同等性の原則ということは観点としては非常に重要ではないか、と思っています。仮に FinTech 企業の負担を金融機関が下げたいという場合に、その FinTech 企業の安全対策遂行能力に見合う程度で十分として残存リスクを金融機関が受容するということも考えられます。あるいは、FinTech 企業の安全対策能力に合わせて、この場もそうかもしれませんが、簡易なリスク管理策を調整するということも手段としては考えられます。ただ、そうしますと利用者の立場からは、２者であろうが３者であろうが同じ効果であるべきであるという同等性の原則に従いますと、やはり本質的な問題は解決しないのではないかと考えております。

このタイプⅠの場合、そもそも金融機関が、なぜ FinTech 企業を使われる、利用されるといいますか、連携を持たれようとしているのかといいますと、企業価値の最大化を目指してその革新的な性質を自らの業務で利用させていただきたい、ということで外部委託を行われるということで、FinTech 企業に IT ベンダーの役割を全面的に代替していただくために、外部委託を行っているわけではないということでございます。したがいまして、タイプⅠの場合ですが、安全対策の在り方としましては、まず金融機関は FinTech 企業の安全対策遂行能力を適切に確認し、そこでどこまでの遂行能力を持たれているのかというのを見た上で、FinTech 企業の能力を超える過大な責務を求めているというような部分があれば、金融機関や IT ベンダーがその責務を分担する、先ほどの責務の一覧にも非常に多くの責務が書かれていますが、これを金融機関や IT ベンダーが分担するということが、革新性を損なわずに安全対策の効果を達成するという観点においては、適切ではないかということでございます。

こうしたことは、従来の安対基準では明快に、明示的には言っておりませんでしたので、この問題を安対基準の中で解決するには、「まず２者関係を念頭に置いた従来の安対基準において求められる責務の総体を維持しつつも、３者の各類型における役割や３者の

安全対策遂行能力に応じてその責務を合理的に再配分しうることをリスク管理策として認めること」でいかがでしょうか、というのが、今回のご提案です。

ご提案内容はこの四角の中に書いておりまして、「タイプⅠにおいて、金融機関、IT ベンダー及び FinTech 企業は３者で当然合意を行った上で従来の安対基準における外部委託の責務を３者で再配分することが可能である」というようなリスク管理策を策定してはということでございます。

「再配分に当たっては、「同等性の原則」に従って必要な範囲を超えて関係者の負担が増加することがないよう留意する必要がある」ということもつけ加えております。

ここで「再配分」という言葉は抽象的な言葉なので、脚注６で解説をつけております。例えば安全対策に関する３者契約を結んで FinTech 企業に代わって、金融機関が、（先ほどの中で言いますと【責務Ｂ－２】ですが）IT ベンダーを統制する責務の一部を担うということも考えられるのではないか、と思っています。

また脚注７ですが、こうした再配分の手段について細かく書くということもあるのはあるんですが、やはり FinTech 企業の規模や業態は多様であるということもありますので、それをあらかじめ確定的に定めることは適切ではなかろうと。そうした分担内容のやり方あるいは分担の割合等々は、実態に応じて区々に決定されれば十分ではないかというふうに思っております。あるいは、こうした分担の見直しから入るということではなくて、FinTech 企業がそうした安全対策上の責務を果たせるように金融機関がご支援をするというような、そうした関係性もあるのではないかということを補足しております。

こうした考え方というのは、何も今皆様に検討していただいております「一般的な情報システム」だけでなくて、「重要な情報システム」においても妥当なものではないかと考えています。以上がタイプⅠに対するご提案でございます。

続きまして、タイプⅢでございます。タイプⅢはやや性質が違うと思っています。タイプⅢは FinTech 企業が主導する形態ですので、金融機関と FinTech 企業の関係は必ずしも外部委託で特徴づけられる形態にとどまらないというふうに考えられます。先ほどマクダッド委員からの FISC に対するご要望の中に、（おそらくあれはタイプⅢを前提にしたものではないかと思いますが）外部委託と必ずしも捉えられないようにきちんと整理をしてほしい、というご要望をいただいておりましたが、そういった意味でここにこういう形で、まずは書かせていただいているというところでございます。

あとは監督当局における検討が進んで何らかの立法がなされた場合には、そうした関

係に新たな要素が加わることも予想されますということで、ここはなかなか今時点で今後いろいろな検討が進んでいく中で、どのような方向に進んでもおおよそ柔軟に対応しうるような内容を、今回ご用意させていただいているというところです。

ではどういうふうに考えていくかということなんですが、FinTech 企業の形態、金融機関との関係がいかなるものになるにせよ、実質的な内容から見れば外部委託と共通する要素が多いのではないかということと、安対基準の中では外部委託という基準は従来からずっと完備されてきているということがあります、ということで、今回のご提案としては、タイプⅢにおいては外部委託の基準は当然適用にはならないんですが、それを準用するような発想でできないか、ということがご提案でございます。

では「準用」とは何であるかということなんですが、これは第１回のときにご説明しましたとおり、金融機関の責任というのは顧客に関するデータを FinTech 企業に提供することに由来していますので、その範囲において外部委託の基準を準用してはどうかということでございます。そうしますと、例えば金融機関がどういうところに関心を持たれるかというところで、例えば客観的評価のときには、「FinTech 企業は金融機関から提供を受けた顧客に関するデータを管理するにあたり、金融機関が有する安全対策手法の管理責任と同等の責任を果たしえるでしょうか。あるいは金融機関が、FinTech 企業に求める管理責任を果たしえるか」ということを確認していくことになるかと思います。

11 ページですが、これらをまとめていいますと、金融機関が、FinTech 企業へデータを提供する際に負う責務というのは、突き詰めますと、先ほどを説明した金融機関の【責務Ａ】の中でも顧客に関するデータの保全に係る部分、そこに限定されるのではないか、ということでございます。金融機関はそこについてリスク管理策としてやっておけば十分ではないかということです。

それ以外の部分といいますと、例えばシステムの安定稼働ですが、そうした部分に関する統制もしくは責務ということについては、FinTech 企業が自ら行われるということになります。しかし、仮にこれを金融機関の関心の外として見なかった場合に、データの保全に係る安全対策の効果が得られないような事態が起きる可能性はないか。要は FinTech 企業からすると、データの保全に係る統制と安定稼働に係る統制というのは全く峻別して行われるというよりも、一体として行われているという場合が多い、と考えられるのであれば、そうした関係性にも留意する必要があるのではないかということを、ここでつけ加えております。

ですのでタイプⅢに関する今回のご提案は、「従来の外部委託の基準を準用するということとともに、金融機関の責務の中で自らが提供する顧客に関するデータの保全に係る責務を金融機関が負っているとすることが可能である」としてはどうかと思っています。

「可能である」とくくっている意図としましては、その次ですが、やはり「同等性の原則」にしたがって、追加的な安全対策を実施する場合があることも留意する必要がある」ということで「可能である」という表現にしているというところでございます。

最後に 12 ページでございます。今までのところはタイプⅢにおける金融機関の責任を論じておるところですが、今度はタイプⅢにおいて FinTech 企業に残る責任というのがないかというところでございます。まず、FinTech 企業はクラウド事業者をはじめとして、運用を IT ベンダーに委託されているということで、外部委託の基準というところで見ますと、先ほど【責務Ａ】の一部、あるいは【責務Ｂ】の一部を担うことが社会的には期待されているのではないか。さらにシステムの安定稼働等を含んだ金融関連サービス全般に関する安全対策も実施されることが、社会的には期待されているのではないかと考えております。

ここにつきましては、FinTech 業界の自主基準など（先ほど説明がありましたが)、策定されることを通じて取り組みが進められることが期待されているのではないか、と思っております。

３番目、「金融機関に責任が生じない場合の取扱い」、これは事後意見で南都銀行の委員及びみずほ銀行の委員からご意見をいただいたところですが、金融機関に責任がないとは言いながらも、やはり何かやっておくべきことがあるのではないか、ということで、ここではそうした金融機関に責任が生じない、一方的に金融機関から顧客に関するデータを取得するような金融関連サービスを、顧客が利用される場合の留意事項について、注意喚起を行っておくことが望ましいのではないか、と考えております。

最後に５番目に「関係者間の協調」というところです。今までお話ししたところからお気づきのように、FinTech 業務における安全対策の実施にあたっては、やはり３者が密接に協調することが不可欠であると考えております。その協調の中心的な部分というのは、やはり利用を検討されるときの情報開示あるいはインシデントが発生したときの速やかな通知など、それぞれの管理フェーズにおいて、金融機関に対して情報が適切に開示されることではないかと。

ただ、そうはいいましても、やみくもに何でもかんでも情報開示を求めますと、当然

FinTech 企業にとっては過大な負荷ということになりますので、そうした安全対策に係る情報開示が協調して行われるようあらかじめ３者間で何らかの合意をしておくことがいいのではないか。そうした合意を踏まえて、円滑な情報開示とそのコミュニケーションが進んでいくことが望ましい、ということを書かせていただいています。

今まで、縷々お話ししたように、今回は、かなり抽象度が高い内容になってございます。従来のリスク管理策、クラウドの基準の検討をご存じの方には、抽象度がかなり違いますね、というような印象を持たれたかと思います。これについてご説明させていただきますと、抽象度を低くしたときの問題がある、ということでございます。先ほどマクダッド委員の資料の中でご説明はされなかったところではありますが、資料の 14 ページに書いてございますとおり、「FISC 安対基準はその字義通りにのみ解釈され、管理手法や技術が趣旨に則っているのか検討されないまま不適とされてしまう恐れがある」ということです。要は抽象度を下げてしまうと、字義通りにそれが適用されてしまって、弾力的な運用が行われない。特に FinTech についてはさまざまな技術が次々と登場する。あるいはビジネスモデルが登場するという中で、特にやはり弾力的な運用ができるような、管理策が必要だろう、ということで抽象度を上げているというところでございます。

ただ、抽象度を上げると実用的でないというご意見もあると思いますので、そうした意味でこれも先ほどマクダッド委員からの資料でいいますと、コミュニケーションコストが高いので低くできるような基準であることが望ましい、というご意見だと思います。そうすると安対基準といいますか、この検討会のリスク管理策はこの抽象度であったとしても、やはり FinTech という業務、あるいは例えばタイプⅠとかタイプⅢですね。それぞれに応じての実用的な指針というのが別の形で何らか、もう少し抽象度の低い形でご要望があるのではないか、と思っています。そこも含めましていろいろ本日の席上及び事後で、ご意見を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　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。

○瀧委員　マネーフォワードの瀧でございます。

10ページのタイプⅢに向けた文脈のところでございますが、まさに藤永様から最後に

ありましたように、字義通りという話がある中で「準用する」という言葉に恐らく従っていく中で、必ずセットでリスクベースの考え方というのがちゃんと浸透していることというのが重要と思っております。ケースによっては、恐らく字義そのままになるのかなみたいなところが思っておりまして、10ページから11ページにかけてのこの表、集中することになるといいながらも、最も保守的な運用を考えた場合には、大分かたいものになってしまうのではないかなというやや懸念がございまして、本日だけではなくて次回に向けてこのあたりはしっかりコメントを準備できればと思っておりますというのが１点でございます。

あとは一番最後のところで、みずほ銀行の田中様から頂戴しているところのスクレイピングに関する延長での考え方のところでございますが、ご意見の中で、PSD2では違法とみなされるケースがあり、また米国では認可制と書いてあるところはやや法的な基盤の違いからくる表現と、米国は認可制というファクトをちょっと確認したいなとは思っておりますので、当方でコメント等、次回に向けて準備させて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　よろしいでしょうか。ほかに何かございますでしょうか。どうぞ。

○加納代理　私の理解不足故の質問だと思いますが、タイプⅠ、タイプⅡ、タイプⅢでFinTech企業とありますが、FinTech企業というのはそもそもどういう定義であれば、FinTech企業ということになるのか。１回目でご説明があったのかもしれません。クラウドの有識者会議からずっと傍聴しておりましたが、今日の資料をみますとクラウドのビジネスを提供される方には結構厳しめで、FinTechの方にはイノベーションを損なう可能性があるのでちょっと緩めというような感覚があります。確かにクラウドのビジネスを提供される企業様には、規模は非常に大規模で、ワールドワイドで活動されていてもイノベーションを重ね、破壊的な価格を提供するというイノベーションを発揮されている企業さんもあるかと思っています。タイプⅠ、タイプⅡ、タイプⅢのところで、クラウドの有識者会議の報告書をベースにした安対基準と、今回のイノベーションを損なわないようにというところにターゲットを置かれて安対基準をとのバランスがとれていない気がしました。

例えばNECが大企業かどうかは別として、社内ベンチャーでイノベーティブなものを提供する場合は、これは、FinTech事業なり企業という位置づけになるのかどうか。

FinTech企業の定義的なところも含めてお尋ねできますでしょうか。

○岩原座長　藤永さん。

○藤永次長　まず定義ですが、これは、第１回のときに実はお話ししていまして、世の中にいろんな定義がされている。中には定義をするのが難しいという定義もされている、というような状況にあります。そうした中でも、「そうはいいながら」ということで、我々として、独自に定義を行い、対象をある程度特定して取り扱おうとしています。
我々なりに前回お示しした定義としては、FinTech企業、業務を担う企業というのは、「ITベンダーと類似の技術的な性質を有するとともに、金融関連サービスといったビジネスモデルの企画実施などを行う業務的な性質を合わせて有している」と考えております。そこがITベンダーとFinTech企業で異なるものとして捉えようとしている違いでございます。
したがいまして、先ほどクラウドベンダーさんとFinTech企業というのを言われていましたが、クラウドベンダーさんは主にシステムの運用を大きく担われる役割をビジネスとしてやられていると思っています。FinTech企業はどちらかというと、システムの運用というよりは、むしろもっと金融業務的なところに近いところと、あとアプリケーションの開発等を含めてやられているというふうに理解しております。今時点ではそうしたところまでを原案としてお示ししております。
あとはお話の中でクラウドにはきつくてFinTechには緩いというようなお話がありましたけれども、本日、同等性の原則という形でお話ししましたように、我々としましては利用者の立場に立って、同じような効果が得られるという観点が非常に重要じゃないかと思っております。したがいまして、緩む、緩めないという話ではなくて利用者の立場から見て適切な安全対策が、FinTech企業が参加される中においてもどのように行われるべきであるかという観点で、ぜひ皆様にご議論いただきたいと思っております。

○岩原座長　加納さん、よろしいですか。

○加納代理　ありがとうございます。いろいろもうちょっと読み込んで理解するようにいたします。

○岩原座長　ほかに何かございますでしょうか。マクダッドさん。

○マクダッド委員　マクダッドです。２つのコメントがございまして、１つは先ほどどうやってFinTech企業を定義すべきという、よくFinTech協会として受ける質問でございます。こういう条件を全部満たしていればFinTech企業です、とは当然言えないかと思うんですけれども、まさしくNEC様と三井住友銀行が共同しているブリースというベンチャー企業、社内ベンチャーがあるのですが、それはFinTech企業の１つと呼んでいいと思うんですけれども、そういった企業はやはり大きな組織から支援をいただいているということになります。協会としては、ベンチャーとして数名で起業をしてそういう大企業の支援を得られない会社についても、何か支援ができないかと頑張っている訳です。したがって、そうした大きな組織から支援を受けている企業は、FinTech協会の立場では、FinTech企業ではない、と。当然否定するつもりはないんですけれども、多分必要な支援は、企業によって違うかと思っています。

そのFinTech企業そのものの定義なんですけれども、対象とする利用者は消費者もしくは法人どちらの場合もありますが、直接に利用者との関係を持っている、という特徴があります。もちろん例外はあって、例えばセキュリティとかブロックチェーンといった要素技術のFinTechベンチャーは利用者との直接の接点をもたず、金融機関にサービスを提供して、OEMのようにFinTechベンチャーの名前が表には出ずに利用者に提供される場合はありますが、利用者がFinTech企業との何かリレーション、関係があるような、本当に３者、利用者、FinTech企業と金融機関が協業すると、そういうパターンをFinTech企業と呼ぶものと思います。

もう１つのコメントなんですけれども、藤永様の話の中で、私の資料にあったんですけれども時間が限られており言えなかったことについて、指摘いただいております。「字義通り」というところなんですけれども、先ほど利用者が入ってくるという話にも関わりがあるかと思うんですけれども、FinTech企業が、例えば銀行、金融機関と協業しようと思ったときに、多分今まで２者、ベンダーと金融機関の場合とは、結構違ってくるかなと思っています。例えば経営企画とか本当によりリテールビジネスサイドの方々とFinTech企業が協議をするんです。そこで、基本的にこういうシステム、こういう仕組みをやりましょうとなったときに、チェックリストへの回答を求められ、銀行のビジネス担当側、提携

を推進したい方が、システムリスクの担当者に対して、とにかく迅速に審査を通過させたい一心で、チェックリストに沿って字義通りに対応するようにFinTechベンチャーに求めるというふうになりがちなのではないかと思うんです。逆にリスクベースのほうが安全と私どもが思っているのは、個々の提携において、一番リスクがあるところについて、３者、FinTech企業と金融機関の中のシステムリスクの方々と、実際にビジネスをやろうとしている金融機関の間で、その３者が一番のリスクはここなんだよね、と対話を行う。そういう取り組みが、一番利用者を保護するのではないかと思っていますので、その字義通りというところのご指摘、とてもありがとうございます。改めて強調させていただければと思いました。ありがとうございました。

○岩原座長　はい。ほかに何か、どうぞ。

○荻生委員　デロイトトーマツコンサルティングの荻生です。資料９ページ目の一番下の囲みですが、弊社で金融機関、ITベンダー、FinTech企業と実証実験の取り組みをしていると、実態として、外部委託の責務を３者で再配分される気はしません。原則としてはそうかもしれませんが、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圧力は多少あると思っています。

ただ、この力関係をどう表現するかというのは極めて難しいので、答えがあるわけではないですが、実態に即すとやや無理があると思います。ですので、ここは、FinTech企業、金融機関、ITベンダーがお互いにきちんとリスクを定量化した上で、お互いができる範囲で責務を全うできるような、何らかの考え方や枠組みがあった方が実質的な安全対策基準となりうるのではないかと考えております。以上です。

○岩原座長　荻生さん、どうも。ほかによろしいですか。どうぞ。

○久井委員　すみません。今回お話しいただいている中で、特に10、11ページにかけてお話しいただいているタイプⅢにおいて、金融機関としてみると受動的な立場になるようなケースの中で、11ページに記載いただいている「金融機関は、FinTech企業に対して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」と、まさにそのとおりだとは思います。しかしながら、先ほど抽象度を高めているという話もあったところではあり

ますが、実際金融機関からしたときに、どこまでの統制を講じるのかというところが余りにも曖昧な感じがしておりまして、やはりレベル感をそれなりに合わせられるようなものをもう少し提示できないと。いかんせん、金融機関側がやるとすれば、それなりのレベル感に合わせていったほうがいいんじゃないかと思います。ちょっとできるかできないかわからないですけれども、そこが気になった点でございます。

○岩原座長　藤永さん。

○藤永次長　ありがとうございます。まさにそうしたご意見もあろうかと思っておりました。

今回、抽象度を上げていることの理由は、先ほどご説明したことと別に、もう１つありまして、金融庁で法制度が検討されていること、また、タイプⅢに関して、全銀協でオープンAPIの検討をなされていること、があります。全銀協では、セキュリティ原則を検討されようとしていまして、我々も委員として参加しているという状況があります。ですので、今日時点ですと、このぐらいの中身になってしまっているのですが、今後、金融庁、あるいは全銀協、さまざまな取り組みに我々も参画させていただく中で、より皆様に実用的に使いやすいものを考えていきたいと思っております。

○岩原座長　よろしいでしょうか。どうぞ中井さん。

○中井オブザーバー　オブザーバーの日本銀行の中井でございます。

先ほどのマクダッド様のリスクベースのアプローチのお話と、これまでのクラウドに関する有識者検討会で提示されましたリスクベースアプローチのところについて、若干両者のところでギャップがあるようにお見受けしたので申し上げさせていただきます。

クラウドの有識者検討会のときは、可用性であるとか機密性という観点でシステムをマッピングした上で、重要度が高そうなものについては網をかけていきましょうというアプローチだったと思います。このアプローチというのは今少なくとも日本の金融機関さんはかなりのところで一般的になっているのかなというふうに理解しているところでございます。

ただし、私の存じ上げる限り、そういったアプローチでは、リスクが低いと認められた

システムに対し、リスク評価項目をある程度削減しようというところがベースになっていると思うんです。外部委託先評価の項目でも、とても大事なシステムに関する先では全部確認するけど、大事じゃないシステムではチェック項目を減らすというようなアプローチになっていると思います。そこが多分まさしくおっしゃっていた、企画セクションのほうが通すというところの考え方はそこなんだろうなと思うんです。

一方、マクダッドさんがおっしゃっていたようなケースになると、リスク評価のアプローチというのがカスタマイズ、要は個々のFinTech企業様に応じてカスタマイズをしていかなければいけないと思いますので、今回仮に有識者検討会の中でこのリスクベースアプローチの部分を前回のクラウドの有識者検討会のところから見直しをされるのであれば、従来の議論のところとのギャップを整理する必要があると思います。日本の今の多くの金融機関様の考え方を準用された形というのがいくのか、FinTech様への適用に際しては少し見直す余地があるのかというところは、１つポイントになるのかなと思いましたので申し上げさせていただきたいと思います。以上です。

４．【議事４】論点メモ「安対基準の対象外となるFinTech業務の取扱い」

○岩原座長　それでは、続きまして、３つ目の論点メモの議事４のご説明をＦＩＳＣの藤永次長にお願いしたいと思います。

○藤永次長　それでは、右上に議事４と書かれている資料をご用意ください。こちらのほうは先般第１回のときに、皆様から席上で多数ご意見をいただきました「安対基準の必ずしも対象とならないFinTech業務に対しても、何らかの意見表明を行うべきではないか」という論点につきまして原案としてご用意したものでございます。本日は意見表明の中身の原案までご用意させていただいていますので、ご説明をさせていただきます。

１ページめくっていただきまして別紙１というところでございます。前回も簡単にご説明しましたが、安対基準において従来対象をどう取り扱ってきたのか、ということで、前回より細かいご説明をご用意しています。

安対基準の対象となる情報システム、これは簡単に言いますと「金融機関が行う金融業務」を担う情報システムでございます。したがいまして「金融機関が行う非金融業務」「非金融機関が行う金融業務」、もしくは「非金融機関が行う非金融業務」というのは、直接的な対象とはしてこなかった、ということがございます。

ただし、「金融機関が行う非金融業務」はやはり同一の金融機関で運営するシステムですので、安全対策に係る方針、一般的にはセキュリティポリシーもしくはセキュリティスタンダードなどが策定されていると思いますが、それのもとで非金融業務の担う情報システムについては安対基準を適宜取り入れるということが望ましい、というふうに、我々としても言っておりまして、そういう形で金融機関が参考として取り組まれてきているという現状でございます。

一方、「非金融機関の行う金融業務」、これも前回席上で委員のほうからご意見がありました、資金決済法の対象事業者等がこれに該当するかと思いますが、これにつきましては安対基準としては従来明示的には対象としてこなかったと理解しております。

理由は２つございます。１つは安対基準の基準としての性質でございます。安対基準は自主基準でございまして、自主基準というのは国家等によって規定されるハードローとは異なって、私的な取り決めや申し合わせ、ソフトローの一種でございます。そうしますと、その自主基準の社会的な規範性、要は社会から見てこういうルールを守るべきである

というそういう認識は、その自主基準の策定過程にその当事者が明示的に参画しておいて初めて生じると考えます。したがいまして、安対基準について言いますと、安対基準の策定過程に参加されていない事業者につきましては、そうした規範性を生ずることはありませんので、安対基準のほうで、いくらそうした当事者を「対象である」といったところで空しい、というところでございます。

ここで脚注をつけておりまして、脚注の３のほうを少しご説明しますと、安対基準の策定過程がどうなっているかというところでございます。安対基準につきましては、FISCの会員代表者を中心に構成される、約30名程度の「安全対策専門委員会」というのがございます。それとその下部組織である「安全対策基準改訂に関する検討部会」というのがございます。こちらのほうでまず検討が行われます。そこで原案ができまして、その後、FISCの会員に対して広く意見募集を行った上で策定されるという、そういう策定過程にございます。したがいまして、その策定過程に会員でなければ参画されないということで、適用対象とすることには無理があるということです。

そうはいってもというのでもう１つでございますが、金融庁の検査マニュアル等において安対基準が言及されているというようなことがございまして、FISC会員の枠を超えて金融庁監督下の金融機関が事実上、FISCの非会員においても適用対象とされているというような事実はございます。ただ、ここは金融庁の監督下にない非金融機関まで対象とするのは、さすがに無理があるということでございます。

そうした考え方を表にしたのが次のページの図表１でございます。こうした前提を踏まえましてどういうふうに取り組むべきであるかということが、次の「取扱いの方向性」でございます。ここについては何らかの整理を本検討会でしておくことが必要ではないかと、対象外についても整理が必要じゃないか、というのが前回の皆様からのご意見だったと思っています。

整理の仕方の１つのやり方として、事後意見でもいただきましたが、金融業務と非金融業務というものをまず線引きしては、というご意見がありました。ここにつきましては、多岐にわたるFinTechのサービスが登場する中で、あらかじめ業務を個々に特定することは困難であるという事情と、仮に境界が曖昧な中でそれを明確に線引きしたとすると、業務の機能面では大差がないにもかかわらず、安対基準上の取扱いが全く異なるということが、果たして取扱いの適切性として妥当なのか、ということが危惧されるということでございます。

９ページですが、本来立ち返って考えてみますと、利用者の立場に立てば金融業務であるか否かとか、金融機関と非金融機関のいずれが行っているか、ということについては一義的な問題ではなくて、やはりFinTech業務全体においてシームレスかつ一体不可分な形で適切な安全対策が実施されるということが期待されているのではないかと考えます。これは先ほどの２者関係、３者関係においても同等性の原則として効果が期待されているということと、同義でございます。

したがって、こうした社会的期待に応えるためにはどうするかということですが、まず我が国の金融機関が従来からその業務において社会的な信頼というのを培ってきたという認識がございます。その類似の信頼を、FinTech業務においてもまず得ることは有益ではないかと。これは情報システムにおける部分でいいますと、社会的に合意されたルールである安対基準がそうした信頼形成にも携わってきた一面があるということでございまして、まず考え方のアプローチとして、そうした金融機関と非金融機関にかかわらずFinTech業務の担い手において、安対基準の社会的規範性をどのように生じうるかということに着目して、整理してみました。

まず、金融機関の行う非金融業務、区分Ｂでございます。これは先ほど来ご説明しましたとおり、既にもう同一の金融機関が一体として、セキュリティポリシー、セキュリティスタンダードに従って取り組みが行われているということですので、FinTechにおいても同様ではないかと思っております。セキュリティポリシーとかセキュリティスタンダードについてご存じのない方は、脚注の５番につけておりますので後ほどごらんください。

次に、本日ご意見をいただきたい対象となります区分Ｃ、区分Ｄ、非金融機関が行う業務でございますが、ここにつきましては、どうやって安対基準の規範性が及びうるか、ということで２つほど方法があるとご提案しております。

次の６ページです。１つが「直接的に規範性が生ずる方法」ということで、これはもう非常にわかりやすいところですが、FinTech企業は個別にFISCの会員となられるということです。そうしますと安対基準の策定過程に明示的に参画可能となって、そうした安対基準に対してFinTech企業がご意見を反映することができる、ということでございます。それによって安対基準を遵守ということが実現できるのではないか。

もう１つの方法が「間接的に規範性が生ずる方法」ということで、FinTech企業の業界団体がFISC会員となって、代表してその業界の意見を安対基準の策定過程に反映させていくということがございます。この場合はもう１つ工夫が必要で、そうして策定された安

対基準と整合的な形でFinTech業界の方々の自主基準が策定されるということによって、会員に対してその効果が及ぶという方法でございます。

これについて実態は今どうなっているかといいますと、まず１ですが、これについては委員で参画いただいていますマネーフォワード社にはFISCの会員に既になっていただいているということで、１についても少しずつですが、そうした取り組みが進んでいます。２につきましても、先ほどプレゼンいただきましたマクダッド委員が理事を務められているFinTech協会がFISCの会員になっていらっしゃるということと、FinTech協会においては自主基準が策定されようとしている、という状況にあるというところでございます。そうした意味では、FinTech協会の自主基準と安対基準を整合的な形で策定していくということが、先ほどマクダッドさんのプレゼンにもありましたとおり、FISCとしても今後取り組んでいくべきことだと思っています。

先ほどマクダッド委員のほうからFISCへの要望ということで３ついただきました一番目のところです。ページ16ですが、「安対基準の一部として組み込みや連携を検討いただく」。これにつきまして、注をつけていただいていまして幾つかありますが、例えば「FinTech企業が実施すべき安全対策の目安となる基準等の公表を安対基準を通じて行う」というようなことをご提案いただいております。そうしたご要望をいただいているところを踏まえて、FISCとしてももう一段何らか積極的に、例えばFinTech協会と合同で検討を行っていく、というようなことも、必要ではないかと考えております。

こうした既にやっているような取り組みが少しずつ進んでいくことによって、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かつ一体不可分な形で、適切な安全対策が実施されることが期待できるのではないかとは思ってはおるんですが、FinTech企業の方々が全てFISCの会員になられるわけでは当然ないですし、FinTech業界の業界団体も必ずしもFinTech協会だけでなくて、ほかにもブロックチェーン関連でも業界団体がございますし、あるいは今後もそういう業界団体が新たに登場されるかもしれません。そうしたことを踏まえまして、やはり何らかの意見表明というのが必要ではないか、ということで、今日はその原案をご用意させていただきました。

次に７ページでございます。意見表明としまして、まず「『金融機関におけるFinTechに関する有識者検討会』は、FinTech業務を実施するのが金融機関であるか否かに関わらず、FinTech業務を担う情報システムにおける安全対策の在り方について、高い関心を持っている」。やはり安全対策を議論していますこの場としましては、そうした関心を持っ

ているということでございます。「そうしたことから、FinTech業務に携わる事業者においては、本検討会が策定する以下の『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』を踏まえたうえで、適切な安全対策が実施されることを期待する」というふうにくくっております。

この原則に関して、脚注の６のところで若干補足しています。外部委託の有識者検討会のときに「安全対策における基本原則」を策定しています。これは主にFISCの会員といいますか、金融機関向けにつくった基本原則であるのに対して、今回の原則は、より会員にとどまらず社会全体に発信していくメッセージになりますので、そうした、従来あった「安全対策における基本原則」をもとにしながら、それを社会的に発信するものとしてつくり直しているとご理解ください。

まず（１）としまして「金融関連サービスの提供に携わる事業者は、その利用者が安心してサービスを利用できることを目指し、自らが管理責任を負う情報システムに対して、適切な安全対策を実施する」ということです。

（２）として「金融関連サービスの提供に携わる事業者は、安全対策の実施にあたっては、イノベーションの成果が利用者の利便性向上に資するよう留意するとともに、金融機関とその他事業者がそれぞれ独自の優位性を活かせることを目指し、安全対策においても協調が促進されるよう留意する」。

（３）番目に「金融関連サービスの提供に携わる事業者は、互いに協調して安全対策を実施するに際し、FISCの安対基準を含め、安全対策に関して社会的に合意されたルールが形成されるよう努める」と、原案をご用意させていただきました。

それぞれで、書いていることの意図がその次に書いてございます。これをかいつまんでお話ししますと、（１）番につきましては、要は金融関連サービスにおいて安全対策をシステムに行わないということは適切ではないでしょう、ということです。そこをまず（１）番の原則で確認させていただいております。

（２）番の原則につきましては、安全対策がイノベーションを阻害することがない、そうした観点が重要ではないか。なぜかというとそのイノベーションは、利用者の利便性向上に資するものであるから、ということでございます。

あとは、今後、オープンイノベーションが金融機関において進められていくということが広く言われておりますが、そうしますと金融関連サービスに携わる事業者というのがどんどんふえていきますということです。それがアンバンドリングされていくことの意味

であると思っておりますが、そうしますと、多段階にわたって重層的に携わる方々が登場してくる。APIのケースでいいますと、APIを事業者間でつなぐことによって、重層的なAPI連携が行われていく。そうしたビジネスモデルが登場するということも容易に考えられます。そうした事業者の関係が複雑になる中においても、むしろそうした中においてこそ、複数の事業者が協調してサービスに携わるということが重要ではないか。安全対策においても特に協調というのが重要ではないかということを書いています。

（３）番目としてその協調をどのように行うかということで、FISCの安対基準を例として取り上げさせていただいています。「FISCの安対基準はそもそも、なぜ？どういう背景でつくられてきたか？」というところをご存じない方もいらっしゃるかもしれませんので、「参考１」ということで１枚おつけしています。「金融機械化財団設立趣旨書」ということでございましてこれは実は、FISC金融情報システムセンターの設立準備段階の名称は「金融機械化財団」というものでございました。その設立趣意書です。

そのときの趣旨としては、下線のところですが、「金融システムの機械化全般に関する諸問題を解決するためには、金融機関、保険会社、証券会社、ハード・ソフトメーカー等々、中央銀行、行政当局などの多数の関係者の協力が不可欠」であると。その協力を行うことによって、「知識、経験、情報等をそれらの方々を集約することによって、諸施策が初めて推進しうる」。そうしたことによって「諸問題を効率的かつ弾力的に処理していく」ということが特に金融システムの安全対策においては重要ではないかということが当時の精神でございます。それを実現するために、FISCがつくられたということです。

したがいまして設立後30年たった現在において、特にオープンイノベーションが進んで関係する事業者が、拡大していくことが予想される中においては、FISCとしても果たしうる役割というのがまた大きく前に進んでいくということがあるのではないか、と思っているというところです。

そうした取り組みをされているのは何も当センターだけではございませんので、そうした社会的に合意されたルールに関しまして、FinTech協会の自主基準もそうでしょうし、あるいは全銀協が検討されているセキュリティ原則もそうでしょうし、そうしたそれぞれのルールが整合的に形成されていくことに、皆様が取り組まれていく、ということによって、安全対策が金融関連サービスにおいて適切に実施されうる。それによって利用者の期待に応えうる、というふうに考えているというところでございます。

今日はそうした形で原案として用意させていただきましたので、席上、事後、幅広く

委員の皆様からご意見をいただいた上で、これを最終の報告書の中にまずは取り込んではということが今日のご提案でございます。以上です。

○岩原座長　どうもありがとうございました。ただいまの藤永次長からのご発表に対してご質問等ございますでしょうか。特にないですか。マクダッドさん。

○マクダッド委員　質問ではないんですけれども、６ページの上に直接的に規範性が生ずる方法と間接的にという話がありまして、それはまさにFinTech協会に関わるところかと思うんですけれども、弊協会の考え方について述べさせていただければと思っております。

FinTech協会は、もともとミッションとしてこういった場で参加できない、本当に零細企業などのプレゼンスを上げる、という考え方でイノベーションの推進を支援する組織でもあります。確かに間接的に多分しばらく、現状のまま続くかと思うんですけれども、「イノベーションとともに成長」という言葉も重要だと思います。弊協会の中にベンチャー会員というのがあるんですけれども、ベンチャーをどういうふうに定義するかというと、即答はできない方が多いと思うんですけれども、基本的に「設立10年以下」、そして「上場していない」という、簡単に２つの条件がございます。けれども、例えばなんですけれども弊協会のベンチャー会員、例えば私を通じて間接的にこういった場で意見交換などできればなと思っているんですけれども、その企業はいずれ例えば上場したりすると、もしくは大きくなったりすると自らFISCに入会したりすることも考えられます。まさしく藤永様のご指摘のとおり、例えばマネーフォワード様が１つの企業としてFISCに入会するのは、とてもロードマップ的に、企業の成長に伴ってとてもいいな、と思っておりまして、その点について、つけ加えさせていただければなと思いました。

○岩原座長　ほかに何か、ご意見、ご質問等ございますでしょうか。よろしいですか。どうぞ、神田さん。

○神田オブザーバー　オブザーバーですけど金融庁の神田です。今ご説明がありましたように、これまで安全対策基準の対象外とされてまいりました金融関連サービス事業者、あるいはFinTech業務につきましても、今回安全対策につきましてご説明があったような

意見表明というような形で、一歩踏み込んだ形で関与されようとしているということについては、非常に時宜を得た取り組みということで歓迎したいというふうに金融庁としても考えております。

また、FinTech協会におかれましても、現在策定が進められているこちらのセキュリティ原則、あるいは自主的なガイドラインなどについて、こちらのFISCの安全対策基準と整合的なものになるように、ご説明があったとおり取り組みを進めていっていただければというふうに考えております。

最後に１つお願いになりますけれども、こちらでもう少し議論をした上で取りまとめて、それから安全対策基準の策定という形で進むということになると思いますが、今FinTechの進展も非常にスピードが速いということで、こういった形で安全対策基準を取りまとめた後で、FinTechの事業者さんがそれに取り組んでいくという、その順序性を考えますと、議論の取りまとめは速やかに行っていただいて、さらに安全対策基準の策定、公表につきましても直ちに着手していただいて、できるだけ早く作業を進めていっていただくということにつきましても、引き続きご留意いただければというふうに考えております。よろしくお願いいたします。

○岩原座長　それではこれにて第２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大変ありがとうございました。

以上