平成29年５月23日

公益財団法人　金融情報システムセンター

第51回　安全対策専門委員会　議事録

Ⅰ　開催日時：

平成29年５月23日（火）15:30～17:12

Ⅱ　開催場所：

FISC会議室

Ⅲ　出席者（順不同・敬称略）

座長	渡辺　達郎	公益財団法人金融情報システムセンター　理事長
委員	花尻　格	株式会社三菱東京ＵＦＪ銀行 システム企画部　副部長
	中村　友紀	(代理出席)株式会社三井住友銀行 システム統括部システムリスク管理グループ 室長代理
	山田　満	株式会社南都銀行　システム部長
	堤　英司	みずほ信託銀行株式会社 ＩＴ・システム統括部　システムリスク管理室長
	星子　明嗣	株式会社東京スター銀行　執行役
	蓮實　豊	(代理出席)一般社団法人全国信用金庫協会 業務推進部　主任調査役
	内田　満夫	全国信用協同組合連合会　システム業務部　部長
	岡部　剛久	労働金庫連合会　統合リスク管理部　部長
	常岡　良二	農林中央金庫　ＩＴ統括部　主任考査役
	小梶　顯義	第一生命保険株式会社 ＩＴビジネスプロセス企画部　部長
	五十嵐　逸郎	東京海上日動火災保険株式会社 執行役員　ＩＴ企画部長
	植村　元洋	(代理出席)野村ホールディングス株式会社 ＩＴ統括部　次長

	木原　眞一	三井住友カード株式会社 経営企画部長兼調査室長
	岡田　拓也	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　グループ長
	安冨　潔	慶應義塾大学名誉教授 ・弁護士（山田・尾﨑法律事務所）
	鎌田　正彦	株式会社ＮＴＴデータ 金融事業推進部技術戦略推進部 プロジェクトサポート担当部長
	松野　徹	ＮＴＴコミュニケーションズ株式会社 ソリューションサービス部 第二プロジェクトマネジメント部門 第一グループ担当部長
	羽太　英哉	(代理出席)沖電気工業株式会社 金融・法人ソリューション事業部 ＰＭＯ　シニアスペシャリスト
	堀井　康司	日本アイ・ビー・エム株式会社 金融インダストリーソリューション 第一ソリューション推進 ソリューションマーケティング担当　営業部長
	加納　清	日本電気株式会社 金融システム開発本部　シニアエキスパート
	森下　尚子	日本ユニシス株式会社 ファイナンシャル第三事業部 ビジネス企画統括部　次世代ビジネス企画部 事業推進グループ事業推進グループマネージャー
	宮崎　真理	(代理出席)株式会社日立製作所 金融第一システム事業部　主任技師
	藤田　雅人	富士通株式会社 金融・社会基盤営業グループ シニアディレクター
	上田　直哉	ＮＲＩセキュアテクノロジーズ株式会社 マネジメントコンサルティング部　部長
オブザーバー	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
FISC 委員	髙橋　経一	公益財団法人金融情報システムセンター 常務理事

FISC 委員	和田　昌昭	公益財団法人金融情報システムセンター 監査安全部　部長
FISC(事務局)	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
	加藤　史宏	調査部　総括主任研究員
	松本　浩之	監査安全部　総括主任研究員

Ⅳ　開会　～　FISC　渡辺理事長　挨拶

○和田監査安全部長　それでは、お時間になりましたので、第51回安全対策専門委員会を開催いたします。

本日はお忙しい中お集まりいただき、まことにありがとうございます。また、委員の皆様にはご多用の中、本専門委員会の委員をお引き受けいただき、まことにありがとうございます。私は、公益財団法人金融情報システムセンター監査安全部長の和田と申します。本日は第１回の会合ということで、私が議事の進行を進めさせていただきますので、よろしくお願い申し上げます。

それでは、専門委員会の開催に先立ちまして、当センター理事長の渡辺より挨拶をさせていただきます。

○渡辺理事長　公益財団法人金融情報システムセンター、FISC 理事長の渡辺でございます。皆様にはご多忙の中、本委員会にご出席いただき、心より御礼申し上げます。

近年、金融機関におきましては、外部委託への依存度が非常に高い水準で推移するとともに、クラウドサービス利用が進展する等、外部委託の形態が多様化しております。また、その一方で、金融機関、業界団体及び監督当局等においては、イノベーションの成果の享受を目指して、FinTech への取り組みが急速に活発化しているところでございます。

このように、金融情報システムを取り巻く環境が、従来見られないほど急激に変化する中で、FISC に対しましては、金融機関がシステムの安全を確保しつつ、企業価値の最大化に取り組める環境を整備するよう、会員にとどまらず、社会的に強く期待・要請されているという状況にございます。

そうしたことから、平成 27 年の安対基準改訂からこれまでの間、FISC では、外部委託に関する有識者検討会及び FinTech に関する有識者検討会というものを設置いたしまして、金融審議会の会長でもいらっしゃる岩原先生を座長にお招きし、２年間という長期にわたりまして、深度ある検討を行っていただきました。その中では、安全対策の考え方に関しまして、海外先進諸国の動向を踏まえながら、将来に向けて、原理原則に立ち返り、その根本から本質的な議論を行っていただいております。

こうして、昨年の６月に外部委託に関する有識者検討会のご報告いただいたんですけれども、この６月には FinTech に関する検討会の報告書がそろうというところまできてお

ります。

今回の安対基準改訂は、前回の改訂と同様、有識者検討会の提言内容を踏まえてご議論いただくこととなりますけれども、有識者検討会では、原理原則に立ち返った議論が行われた関係上、その提言内容は抽象的なものとなっており、必ずしも安対基準を利用される現場の皆様が理解しやすく、利用しやすいものであるとは残念ながら言えないという内容になっております。

したがいまして、委員の皆様におかれましては、有識者検討会の提言内容を安対基準に反映いただくに当たりまして、その内容が現場の実態に裏づけられた、理解しやすく利用しやすいものとなるようご議論いただきたいと思います。

また、両検討会の提言内容につきましては、既に検討段階から、金融庁や業界団体を初め金融情報システムの関係者から高く評価いただいており、今般の安対基準の改訂におきましては、有識者検討会の提言内容と整合的な改訂が遅滞なく行われる、この遅滞なくということが非常に大事だと考えておりまして、そういう要請にできるだけ応えるように審議の運びにいたしたいと考えております。

そうしたことから、今回の専門委員会の運営に当たりましては、大きく３点の対応を新たに行う予定でございます。

第１点。改訂を遅滞なく行うためには、多岐にわたる議論を効率的に行う環境が必要であるということから、委員会の運営方式を従来から見直しまして、従来は検討部会で行われていた具体的事項の審議も、検討委員の陪席のもと、技術的な部分については検討委員の参加を求め陪席をしてもらいまして、専門委員自身で行っていただき、審議の一本化を図るということにいたしたいと思います。

したがいまして、専門委員の皆様におかれましては、事前にご説明申し上げたよりもご参集いただく機会は増えることになりますけれども、この点ご理解いただき、何とぞお願いしたいと考えております。

第２に、有識者検討会の提言内容が安対基準へ適切に反映され、かつ、現場の実態を踏まえた円滑な議論が行われるよう、委員構成も一部見直しを行います。まず、議事進行を担う役職として副座長、座長は規則上私ということになっているんですけれども、副座長というものを新設いたしまして、議事進行を担っていただく。

副座長には、外部委託と FinTech の両有識者検討会の座長代理を務められ、かつ、金融情報システムの現場の実態に精通された第一人者であられる渕崎正弘様にご就任いただ

くということにしております。また、有識者検討会では、クラウドサービスや FinTech に関しても踏み込んだ検討が行われたことから、FISC の会員であるアマゾンウェブサービスおよび FinTech 協会から新たに１名ずつ専門委員としてご就任いただき、審議に参加していただくという予定でございます。

第３に、改訂後の安対基準をシステムの現場の方々に円滑にご利用いただくためには、FISC 会員であるか否かに関わらず、安対基準を利用されている全ての方々に、早い段階から改訂への理解を深めていただく必要がございます。そのため、専門委員会で FISC から提出する資料やその議事内容等につきましては、原則として開催の都度、FISC ホームページを通じて一般に公開させていただくことといたします。

以上のとおり、前例にとらわれることなく、実効的かつ効率的にご議論いただける環境を整えましたので、委員の皆様におかれましては、有識者検討会の提言内容を踏まえた改訂が遅滞なく行われることを目指して、精力的に取り組んでいただけますよう、よろしくお願いいたします。

なお、有識者検討会の主な提言内容のひとつとして、ＩＴ人材に関するものがございます。サイバーセキュリティを初めとしてＩＴ人材の確保・育成は、経営層を含め、金融機関全体にとって喫緊の課題でございますけれども、一方で、人材については金融機関の実態に応じて求められる質や量が区々まちまちであることから、安対基準に反映するということは、必ずしも適切でないと考えております。

むしろ、ＩＴ人材を確保・育成する手順をご提供するほうが、金融機関の課題解決に資するものと考えられることから、有識者検討会のＩＴ人材に関する提言内容につきましては、安対基準の検討とは切り離し、『ＩＴ人材の確保・育成計画策定のための手引書』の作成を目指すこととし、そのための検討部会を新設いたします。

ＩＴ人材の検討部会につきましては、座長には、特にサイバー人材に関する第一人者でいらっしゃる国立情報学研究所の高倉先生にご就任いただくとともに、検討に当たっては、サイバーセキュリティを初めとするＩＴ人材に関する専門的な知見を得ることが有益でございますことから、オブザーバーとして有識者の方々にご参加いただく予定でございます。

今回の安対基準の改訂は、その初版が策定された昭和 60 年以来の抜本的かつ大規模な改訂となる予定です。本日お集まりの皆様には、有識者検討会で提言された、来た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安対基準に反映され、その結果として、金融機関が将来にわたって環境変化に適切に対応しつつ、システムの安全性の確保と、イ

ノベーションの成果の享受等による企業価値の最大化を実現できるような改訂内容となるよう、合意形成を目指して活発にご議論をいただきたいと考えており、そのようにお願いしたいと思います。

以上、簡単ではございますが、開会に先立ちましての私のご挨拶とさせていただきます。ありがとうございました。

Ｖ．議事内容

１．説明（運営方法について）

○和田監査安全部長　続きまして、次回以降の専門委員会の運営方法についてご説明いたします。先ほど理事長の挨拶にもありましたとおり、今回の安対基準改訂につきましては、前回の第８版追補改訂時と同様に、有識者検討会の提言を踏まえてご議論をいただくことになります。安全対策基準の改訂を遅滞なく行うためには、多岐にわたる議論を有識者検討会の提言に沿って整合的、効率的に実施する環境が必要であることから、具体的な事項の審議に関しましても専門委員会でご議論いただくことといたします。以下の２点が主な運営方法のポイントとなります。

１点目。安全対策の改訂につきましては、専門委員会を月１回程度実施いたします。改訂に関する事項を専門委員会でご議論いただきます。また、検討委員につきましては、専門委員会に陪席いただき、幅広くご議論にご参加いただきます。

なお、副座長の渕崎様、アマゾンウェブサービス、FinTech協会の委員につきましては、次回の専門委員会よりご参加いただきます。

２点目。ＩＴ人材の手引書の作成に関しましては、検討部会で具体的な審議をいただき、その後、専門委員会に諮ることといたします。後ほど設置についてご審議いただくＩＴ人材検討部会には、座長として国立情報学研究所の高倉先生にご就任いただく予定です。

また、オブザーバーとして、株式会社野村総合研究所より松延様、株式会社ＮＴＴデータ経営研究所の大野様、独立行政法人情報処理推進機構より遠藤様、一般社団法人JPCERTコーディネーションセンターより洞田様、株式会社ラックより三宅様にご参加いただく予定です。

続きまして、資料の一般公開についてです。安全対策基準は社会において広く利用されている公共財であり、公益財団として、やむを得ない理由で公表できない場合を除き、広く一般に公開することはFISCの責務と考えております。

また、改訂後の安対基準をシステムの現場の方々に円滑にご利用いただくためには、FISC会員であるか否かに関わらず、安対基準を利用されている全ての方々に、早い段階から、改訂への理解を深めていただく必要があると考えております。そのため、専門委員会でFISCから提出する資料やその議事内容等につきましては、原則として開催の都度、FISCのホームページを通じて、一般に公開させていただくこととします。

これが今回、今年度の専門委員会の運営方法についてのご説明になります。以上の説明についてご不明な点はございますか。全国信用金庫協会、蓮實様。

○蓮實委員代理　蓮實でございます。事前説明のときにも私、１回事務局にも説明させていただきましたけれども、安全対策基準は金融機関が使う安全対策としてかなり個別具体的なことまで書かれているものでございます。ですから、これを審議途中の資料とはいえ、広くインターネットに公表するということは、金融機関のセキュリティの基準としてこういうものを最低限みんなやっているということを場合によっては犯罪者にも広く知らしめることになってしまうということになるかと思います。それは私ども金融機関にとっては余りいいことではないというか、具体的に言えばマイナスの話であって、ちょっとそれを諮るのではなく、もうそうさしていただくということをFISCさんがおっしゃるのはちょっと理解できないところなんですが、いかがでしょうか。

○和田監査安全部長　事務局の松本総括、よろしくお願いします。

○松本総括主任研究員　松本です。先日お伺いしたときにも事前にご意見頂戴しております。そちらのご意見を踏まえまして事務局のほうで検討を行いました。結果としましては、先ほどの繰り返しになりますけれども、この安対基準につきましては既に一般的に広く行き渡っており、公共的な性質を帯びていると思っております。

蓮實様が今おっしゃっているリスク的にというようなところでございますけれども、この安対基準につきましては既に広く知れ渡っている前提がある一方で、サイバー攻撃といったサイバーセキュリティに関するような、金融機関においてリスクが生じるような機

微な情報につきましては、今までも、これからも限定した情報開示とさせていただいておりますので、想定されるようなリスクにおいては、今のところ考えていないという結論に至っております。

○和田監査安全部長　はい、蓮實様。

○蓮實委員代理　私、ちょっと昔の話なので今の方たちは知らないと言われればそれまでなんですけれども、FISCさん、安全対策基準は、これは比較的金融機関がこういう質を保っていますよという話ですから、要するに一般個人が買いたいと言ったときにお売りになっているんですかというのを昔、聞いたことがあります。FISCとしても一応、売却させていただくときには相手を変な人ではないというのをある程度確認させていただいていますということをいただいていたんですけれども、今は例えば違うのでしょうかという話と、あと、FISCさんが公益財団になられるとき、一応私、当時の事務方ですから今の方は覚えていません、知りませんと言えばそれまでなんですけれども、公益財団化されることによってFISCの安対基準の内容とかが広く公共に示されてしまう可能性はないのですかと言ったら、そういうことは考えていないというお話をいただいたので、私、安心していたんですけれども、過去の話なので、もう今の事務方は知らないと言われてしまえばそれまでなんですけれども、私どもも一応この水準でやっていこうというのを長年にわたって決めてきて、そういうものを急に広く一般に公表しようじゃないかということをFISCさんのほうで一方的に決められるということ。要するに、諮るでもなく、こういう水準、こういうやり方でやりますと言われてしまうことにちょっと違和感を覚えております。

○松本総括主任研究員　まず、１点目の誰でも購入できるのかというご質問につきましては、当センターへのお問い合わせ、ご要望がございましたら販売しております。

２点目のお話でございますけれども、過去、販売対象先の確認を行っているとご説明した経緯や真意などは承知していませんが、当センターにつきましては、公益財団としまして公益に資する情報につきましては、公益認定の条件に照らし合わせても、一般公開していくことがFISCの責務というふうに我々としては考えておりますので、本日の結論に至った次第でございます。ご理解のほどよろしくお願いいたします。

○蓮實委員代理　じゃあ、もしどうしても公表に対して反対したい場合は、今回の改訂自体に反対するしかないということでよろしいんですか。

○松本総括主任研究員　公表自体への反対のご意見につきましては、各委員の方もそういったご意見があれば皆様のご意見を踏まえて、ご審議を諮る調整を考えさせていただきたいと思っております。

○和田監査安全部長　「公益認定等に関する運用について」という内閣府が出している資料があります。FISCというのは、調査資料収集という項目のところで公益財団法人というふうに認定をされています。

そこのチェックポイントというところがありまして、「当該調査・資料収集が不特定多数の者の利益増進に寄与することを主たる目的として位置づけ、適当な方法で明らかにしているか。当該資料収集の名称や結果を公表しなかったり、内容について外部からの問い合わせに答えないことはないか」というように、公益財団法人として公開とするのは責務であるというところがまず１点あります。ここはぜひご理解いただきたいと思いますし、これは公益財団法人としてFISCがある以上、まず大前提になりますので、今回の安対基準の改訂を反対する・賛成するというよりも、もう少し上の理事会だとか、そういったところで財団法人としてどうするかというところに話がいってしまうことになります。

なので、まず我々としては、専門委員会は理事会のもとで動くものでありますから、まず公益財団法人ということを前提に今年度の審議を進めていただきたいと思いますし、そうあるべきだというふうに考えております。

○蓮實委員代理　もしそうであれば、FISCさんは公益財団法人だから、得た情報を全部公表しなければいけないのかということをおっしゃっているように思えるんですけれども、先ほど日々の情報、サイバーのような情報に関してはちゃんとうちは出さないですよということを言っているわけですよ。そこには整合性がない話であって、安全対策基準とサイバーに関する情報で、サイバーは出さないんだけれども、安全対策は出していいんだという基準は、FISCさんが勝手に決めているということですか。

例えば、FISCがやっている金融機関のアンケートとかそういうものを公表されることをだめと私は申し上げるつもりは全くないんです。ただ、どこまで出す。しかも、これは

私どもの自主基準という形でつくらせていただいているものなので、FISCさんにお任せはしていますけれども、我々の自主基準ですと。それを公表する・しないをFISCが勝手に決めてしまうというのであれば、それはちょっとおかしいんじゃないですかと申し上げているわけです。

○和田監査安全部長　今のご質問には２点あると考えております。１つは、まずどのレベルまで公表するのかという、サイバーだとかそういったところについては公表しないんだけれども、安対については公表するかという１点目と、すみません。もう１つ何でしたっけ。

○蓮實委員代理　要するに、同じことです。アンケートとかそういうものを出すのは全然おかしくないと思うし……。

○和田監査安全部長　基本原則として、全て公開していくというところになります。ただし、サイバーだとかそういったセキュリティにかかわるところについては公開しないと。

この安対基準というのをどの位置づけかというと、例えば、サイバーで必要な情報というのは、どういうパッケージをどのバージョンで持っているかというのを相手に知られると、それはそこの脆弱性とかあるので公表というのはすべきではないと考えています。

一方、安対基準というのはどういう位置づけなのかというと、いわゆる規範です。なので、たとえこの規範を読んだとしても、どこに脆弱性があるのかというのはわからないと思います。なので、これは公表すべき。それよりも、会員以外の方も今後FinTechだとか外部委託先だとかがきちっと理解して、金融機関の安全をきちんと考えていただけるというところで、公表は必須だというふうに考えております。

○蓮實委員代理　そうすると、程度観の問題ということになるんですけれども、私はそういうふうに思っていませんし、FISCさんがそうお考えになるのはちょっと不信感しか持ちませんということと、あと、どうしても、今、現実問題としてお問い合わせがあれば売ってしまっているのであれば、まして今回、FinTechの協会さんやアマゾンさんもこの委員会のご出席なさるのであれば、また、従前からベンダーさんやベンダーさんの取引

先であろう企業さんもFISCの安対基準、金融機関のシステムを開発するのであれば皆さん意識されていることになりますので、ここでインターネットで広く公表することが本当に必要なのかというのは別の話だと思うんです。

事実、皆さんにお問い合わせがあれば売ってしまっているのであれば、極端な話、悪い人が実名で、または偽名で買っていたとしてもしょうがないので、それは防ぎようがないんですけれども、インターネットということで公表するというのはまたさらに次元が違う話になりますということです。

これは程度の問題なので、議論しても結論が出る話ではないんですが、私はこれがインターネットで公表されるということであれば反対をしたいんですが、FISCさんはもうそういうふうに決めたんです。こういうふうに運営するんですということを曲げる気がないというのであれば、それが出さないためには、あとはこの改訂自体を反対させていただいて否決するしかないということになってしまうということだと思うんですね。今の状況だと。そういう理解でよろしいんですかね。

○松本総括主任研究員　今のお話しですけれども、後ほどご審議を諮らせていただきたいと思っておりますので、その場でご意見をいただければと思っております。

○蓮實委員代理　じゃあ、１点だけ。もしこの件、このままFISCさんがやるという形で、後で審議事項で今回の改訂について決をとるのであれば、きちんと挙手によって、誰が賛成したかを記録を残す形でとっていただきたい。それは、私はこれに関してきちんと反対意見を述べました。FISCの安対基準がインターネットで公表されるような事態に対して反対しましたという証跡が欲しいんです。また、逆にそれに賛成したのは一体誰なんだというのはきちっと残していただきたい。

○和田監査安全部長　蓮實委員のご意見は承りました。ほかにご意見等ございますか。

ないようですので、それでは１つ目の審議事項、「『金融機関等コンピュータシステムの安全対策基準・解説書』の改訂の着手について」より議事を進めてまいります。

２.【審議１】～

○和田監査安全部長　お手元の資料「資料１－１」をご用意ください。ご審議いただく事項は、専門委員会を月１回程度開催し、３月末の発刊を目指して検討を開始することでございます。

それでは、審議１の内容、ペーパーを読ませていただきます。

『金融機関等コンピュータシステムの安全対策基準・解説書』改訂の着手について

Ⅰ　審議事項

『金融機関等コンピュータシステムの安全対策基準・解説書』（以下『安全対策基準』という）について、安全対策専門委員会を月１回程度開催し、会員意見募集を経て３月末をめどに発刊できるよう、改訂作業を開始すること。

Ⅱ　改訂の背景

当センターにて開催した「金融機関における外部委託に関する有識者検討会」及び、現在開催している「金融機関におけるFinTechに関する有識者検討会」の報告内容・提言を受け、『安全対策基準』にリスクベースアプローチの考え方を取り入れるとともに、外部への統制を拡充させるなど、『安全対策基準』の構成・適用方法等を見直すこととした。

Ⅲ　改訂原案・補足資料

・「資料１－２」改訂原案

・「資料１－３」補足資料

なお、今回の安対基準改訂は、前回の改訂と同様、有識者検討会の提言を踏まえて次回専門委員会からご議論をいただくことになるため、まず「外部委託に関する有識者検討会報告書」と、「FinTechに関する有識者検討会報告書（案）」の概要を企画部よりご説明いただきます。その後に、『安全対策基準』原案を事務局よりご説明いたします。

企画部の藤永次長、よろしくお願いします。

○藤永次長　企画部の藤永でございます。私のほうから、有識者検討会のこれまでの検討内容についてご説明させていただきます。

まず、お手元に「金融機関における外部委託に関する有識者検討会報告書」をご用意ください。全部で70ページ程度のものになりますので、お持ち帰りいただいて、ぜひご一読いただければと思います。本日は、ポイントを何点かご説明いたします。

まず、１ページ。「はじめに」というところがございます。そもそも何のためにこの有識者検討会をやったのかということです。これにつきましては、書いてございますとおり、

近年、我が国金融機関の情報システム関連業務において、外部委託への依存度が急激に高い水準で推移をしているということです。既に90％以上の金融機関が、基幹系の情報システムを外部委託に依存している状況にあります。

一方、共同センターの利用も進んでおり、そうしたシステム共同化の進展を初めとして、その形態も多様化しているということです。

一方、皆様ご承知のとおり、銀行等の業務の再委託先に関する銀行法の改正が数年前にございまして、再委託管理のあり方を見直すことが必要となっているということです。あとは、本日のもう１つのお話でもありますけれども、ＩＴ人材の育成・確保というのも課題となっているということです。

こうした盛りだくさんのテーマ・課題というのを抱える中で、それにどう対処するかというところですが、やはり、これらはいずれも根の深い問題であるということです。何を言っているかといいますと、情報システムの現場の皆様だけでは解決できない問題が起きているということで、経営層を含む、会社全体の情報システムの課題への関与というのが非常に重要になってくるということで、ＩＴガバナンスという観点が必要であろうということです。

そうしたことを踏まえまして、金融審議会の会長でもある岩原先生に座長をお務めいただいて、日本総研の渕崎社長に座長代理になっていただいて、平成27年10月26日から計６回にわたり取りまとめられたのがこの報告書です。

報告書の中で、安対基準について触れられている重要な箇所が何カ所かありますので、次はそちらをご説明したいと思います。まず、25ページをごらんいただけますでしょうか。「新たな安全対策の在り方の必要性」というところがあります。今回、さまざまな困難な問題に対処するために、安全対策のその抜本的なあり方から見直すということを外部委託の検討でやっています。

その下の（１）で、「安全対策基準の考え方の見直しの必要性」が提言されています。これは何かといいますと、お手元にも安対基準ございますが、300を超える基準が含まれている、その前段、最初の数ページのところに「安全対策基準の考え方」という箇所があります。

そもそも安対基準は、30年前、金融機関のオンライン化の進展に当たって金融機関の自己責任と自主性尊重を原則としつつ、その対応を補完するものとしてFISCが設立されて、安対基準が策定されたという経緯があります。

26ページ。それから30年が既に経過する中で、安対基準は環境変化を取り込みながら、かつ、皆様にもご協力をいただいて改訂を重ねてきまして、我が国の金融機関においては安全対策の重要性が強く認識されるに至っているということです。

ただし、他方で副作用といいますか、いわゆる情報化が急速に進展してコンピュータの形態も多様化してきますと、国際競争の中で、我が国の将来の金融ビジネスにおける優位性を確保するためは、30年間大きな考え方を見直してこなかったものを、このタイミングで見直す必要があるだろうということが提言されているということが重要な点としてご認識いただきたいと思います。

では、例えば従来の安全対策の考え方にどういう課題があるのかということですが、一言で言いますと、30年前は、システムと言いましても、基幹系のコンピュータシステムぐらいしかなかったと。その後、情報化の進展に伴って、それ以外の情報システムが多種多様にふえてきている中において、安全対策基準というのは従来と変わらず、基幹系の重要な情報システム向けにずっと作られてきていました。したがいまして、金融機関の現場においては、重要でない一般の情報システムに対しても安対基準を適用せざるを得ない、そういう状況が安対基準に内在する課題として従来からあったと。

それがどういう課題を起こしているかというと、金融機関が安全対策を過度に意識して、安全対策に優先的に資源配分を行い、結果として企業価値の最大化等が実現できなくなる、そういう懸念があるということがこの報告書では提言されています。

それをどのように解決するかということが、次の27ページですが、解決策の検討に当たっては、米英の取り組みの調査研究を当センターで行い、参考にしているということです。一言で言いますと、皆様よく聞かれる言葉かと思いますが、重要なシステムとそうでないシステムでリスクに応じて安全対策を決定する、リスクベースアプローチが、米英では既に採用されており、遅まきながら、日本においてもそれを取り入れるべきであるということでございます。

そうした検討を踏まえまして、次の28ページのところですが、安対基準の前提となる考え方に、「リスクベースアプローチを踏まえた安全対策における基本原則」を４つ有識者検討会において提言いただいたということです。これが外部委託検討会での提言内容の大きなひとつです。

あとその次は、非常に長い報告書なので、最後の54ページをごらんいただきたいと思います。有識者検討会の提言内容の最後に、今後の安対基準改訂の考え方ということが示

されております。

これは皆様のご検討の前提になりますのでご説明させていただきますと、１番目は激変緩和措置の必要性ということです。金融機関の現場のさまざまなところで、ガイドライン含めまして安対基準というのをご活用いただいておりますので、安対基準の考え方から変えると金融機関の皆様にとっては大きな変更が必要になってくる。その変更することのコストや作業負荷が、現場にとっては大きな負担になるであろうということで、激変緩和措置が必要であるとしています。

具体的には、従来どおりの取り扱いを継続することとしつつ、システムの更改時や新システムの導入時に、こうした新たな安対基準等へ順次移行を図るということも可能とするという提言をいただいています。

もう１点が、FinTechに関する有識者検討会との関係で、外部委託の報告書が取りまとめられた後に、速やかに安対基準の改訂に着手するという考え方もあったのですが、その一連の関係性の中でFinTechに関する検討が社会的に求められているということで、そうしたFinTechに関する検討を行い、それと外部委託の検討結果をあわせた後、改訂を行うということが、提言されているということです。

続きまして、FinTechの有識者検討会の報告書をご説明をさせていただきます。これも80ページぐらいあるものでございますが、先ほどと同様に、「はじめに」というのがあります。

なぜFinTechを取り上げたかということですが、もうこれは皆様ご承知のとおり、金融機関、業界団体及び監督当局等において、FinTechと総称される金融サービスへの取り組みが今、急速に活発化しております。メディア等通じてニュースも日々出ているということです。

こうした取り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では、金融情報システムのガイドライン、安対基準を出しています当センターとしましても、そうした動きと歩調を合わせて、FinTechに関する安全対策のあり方を検討していくことが期待されているということで、FinTechの有識者検討会を始めたということです。

これも先ほどと同じく、座長・座長代理は同じメンバーで継続をさせていただきまして、平成28年の10月５日、昨年から既に計５回にわたって検討を重ねており、来月６月13日で最終の報告書は取りまとめられようという段階まで来ております。

こちらのFinTechの検討の１つの大きな前提といいますか、目的ですが、「はじめに」の一番下の段落のところに書いてありますが、FISCは従来安全対策のみを言ってきたわけですが、金融機関は、安全対策のために当然存在するわけではありませんので、安全対策とともに企業価値の最大化を目指したさまざまな取り組みが同時に語られるべきだろうということです。

特に、FinTechという文脈ですとイノベーションの成果を享受するということが金融機関の成長に資するものになる、あるいは、最終的には金融機関を利用されている顧客の利便性向上にも資するものになるということです。したがって、従来の安全対策のみを語っていたところに対して、イノベーションの成果の享受も目指すという新たな観点を追加しているということが、FinTech検討会の大きなポイントになっています。

２ページをごらんいただきたいのですが、検討の手順です。ここが今回特徴的なことで、そもそもFinTechと総称される金融サービスの中に、安対基準の対象のものとそうでないものがあるであろうということです。

FinTechにおいては、金融業務とは何であるのか、あるいは、非金融業務とは何であるか、といった境目がどんどん曖昧になっていく。そうした中において、安対基準の適応対象というものをどうとらえるべきか、という新たな論点が今、起きているということです。

もう１つが、安対基準の対象となる部分においては、既に安対基準ございますので、それをFinTech業務に適用したときに何か問題が生ずるかどうかという、付加的な検討をしているということが特徴です。

この場で皆様に共有させていただきたいのは特にその前段の部分で、対象外の取り扱いのところです。ここについては24ページに詳細が提言されております。安対基準というのはどういう性質のものであるかということが書いてありますが、先ほど来、皆様お話しされていましたけれども、安対基準というのはそもそも法律ではないですよね、ということです。法律のようなハードローではなくて、一般的にはソフトローと言われているものに当たり、要は、FISC会員によって策定される自主基準ということです。

ですので、その基準の社会的規範性というのは、その自主基準策定過程に明示的に参画した当事者においてのみ生ずる。したがいまして、その策定過程に参画されていない、策定過程というのはこうした専門委員会あるいは検討部会もそうでしょうし、事後のパブリックコメントに対する意見が出せるというところもありますが、いずれにしましても、そうした策定過程に参画したものにおいて生じる。要は、自分がそれでいいと言ったんだか

ら自分でその基準を守るという規範性が生じるということです。

ただ、そうは言いながら、安対基準は、もう少し違った性質を持っているというのがその下のところでございまして、金融庁の検査マニュアル等において安対基準がリファレンスされているという点です。これによって、事実上金融庁監督下の事業者において適用対象とされている実態があるということが、特徴的なところです。

そうしたことを踏まえて、安対基準の適用対象・対象外というのをどう考えるべきかということで、25ページ以降縷々書いていますが、結論としては26ページの上のところに書いています。要は、本来利用者の立場に立てば金融業務であるか否かは一義的な問題ではなくて、また、金融機関と非金融機関のいずれが行う場合においても、業務全体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が期待されているということです。

形式的に金融業務であるか否かということを分けてから物事を考えるのではなくて、利用者の立場に立って物事を考えていくということの重要性をここでご提言いただいています。

したがいまして、必ずしもFISC会員でいらっしゃらない方々も含めて、安対基準というのを幅広く世の中の皆様にご理解いただくということがこれから必要ではないかということを強く有識者検討会の委員の方々からご意見いただきまして、28ページですが、手前どもとしてはFISCの会員になっていただくようにどんどん取り組みを進めているとはいえ、やはり必ずしも皆様入っていただけるわけではないという前提で、そうした方々に対する意見表明を行っています。

この中で、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ということで、３原則をご提案しています。ぜひ金融情報システムに携わる皆様には、この原則をご理解いただいて取り組んでいただきたいということです。

特に３番目の原則でございますが、右側の29ページになりますが、既に社会的に合意されたルールが形成されており、安対基準はまさにそれにあたると。事業者は、今後もそうしたルールが形成されるよう努めるとともに、こうしたルールと整合する安全対策が実施されることが望ましいという提言をいただいています。

ここまで言いますと、FISCあるいは有識者検討会の委員が全く今までと違う新たなことを言っているのではないか、というふうに思われる方もいらっしゃるかもしれませんが、少し飛びますが、78ページをごらんいただきたいと思います。

78ページのところに資料６というものをつけていまして、これは金融機械化財団、要はFISCが設立される前の仮称の呼び名でして、その当時の設立趣意書、昭和59年９月につくられたものです。

「金融機械化システムの円滑な発展を図るため、安全性確保の問題も含め金融システムの機械化全般に関する諸問題を早急に解決し、これを着実に実行していくことが必要である」という方向性を示した上で、具体的には、「金融機関、保険会社、証券会社、ハード・ソフトメーカー、電気通信事業者、中央銀行、行政当局等の関係者の協力が不可欠である」と。したがって、「これら関係者の十分な意思疎通の下に、知識、経験、情報等を集約することにより、安全性確保のための諸施策を推進する」ということが言われています。

どういうことかといいますと、FISCの会員であるかないかということが物事の出発点ではないということですね。こうした社会的な大きな課題に対して、関係者が広く共通して取り組んでいくことがこの問題の解決に資するということを既に30年前のFISC設立のときから言われているということです。これは現在に至っても、脈々とFISCの中に受け継がれている考え方であるというふうに考えます。

したがいまして、28、29ページで意見表明を書かれていますが、これは何も新しいものを言っているわけではなくて、もともとFISCという成り立ち、なぜFISCをつくったか、あるいは安対基準がつくられたかという前提に関しては、当時と何ら異なっていないということではないかと思います。

したがいまして、FISCとしても「今後発生が予想される問題に対しては、社会的な役割を果たしていくことが必要である」。具体的には、いろいろなこれから集団で社会的に合意されたルールが取り組まれていく中で、そうしたルールの形成に向けて必要となる支援を行って、基準相互の整合性が確保されるよう努めていくべきであるということが提言されています。

その具体的な中身は次の30ページのところに書いてありまして、既にこの図表10にあるようなさまざまな団体によって整合的に安全対策が検討されている。そういう状況になっているというところです。要は、安対基準だけ見ていれば大丈夫ということではなく、いろいろな諸団体が相互に連携をしながら、整合性ある形で基準をつくっていくと。そうしたことによって金融情報システムの安全対策の全体の向上を図ろうとしているということが今、さまざまな集団において取り組まれているということです。

そうした中でFISCの役割としては、必要最低限の安対基準をご提供しようと考えています。これを、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れるべき基準であるとして、FISCの会員であるか否かにかかわらず、遵守いただきたいということを前提に、今回、安対基準の改訂の議論において、みなさまにご検討いただくものとされているということです。

最後に41ページをご覧いただきますと、以上の外部委託及びFinTechの報告書の内容を踏まえまして、今後の安全対策基準改訂の考え方が３点ほど示されています。「安全対策の基本原則の導入」「安対基準の明確化」、そして、「外部に対する統制基準の拡充」でございます。

こうした考え方を中心に、有識者検討会で提言された内容を十分皆様にはその背景・趣旨をご理解していただいた上で、今回、ぜひ検討をお願いしたいということが有識者検討会の事務方を所管しておりました企画部からのお願い事項ということです。私のほうからは以上でございます。

○和田監査安全部長　企画部の藤永次長、ありがとうございます。続きまして、引き続き次回の専門委員会からご審議いただく予定の「安全対策基準の原案」について、事務局、松本総括よりご説明いたします。

○松本総括主任研究員　松本です。まず、ご説明の前に一言お礼を述べさせていただきたいと思います。まず、今回の改訂を議論する内容は多岐にわたり、近年にない大規模な改訂を行う、今年度のFISCの活動における最大のミッションとして我々としては考えております。よって、これまで以上に慎重かつ丁寧に事前準備を行う必要があったため、今までは行ってこなかった、全ての専門委員の方と検討委員の方に事前にご説明にあがって、意見交換を行ってまいりました。

意見交換では非常に参考になるご意見や有益な情報を頂戴し、ご説明内容のご意見だけでなく、当事務局へのアドバイスや、運営上のご提案、また励ましの言葉をいただき、今回ご準備しました原案について、ご議論いただくまで、こぎつけることができました。本日ご承認いただければ、無事改訂のスタートが切れます。これも、委員の皆様からのご支援によるものと、一同感謝しております。

また、委員の皆様には大変お忙しい中、貴重なお時間を頂戴しまして、私どもにご協

力をいただきまして誠にありがとうございました。

それでは、原案概説のご説明をさせていただきます。お手元の資料１－２と資料１－３をご用意いただけますでしょうか。まず、ご説明します改訂原案ですが、机上でお配りしています安全対策基準第８版でいう、前半部分の「安対基準の考え方」「本書の利用にあたって」に該当する部分をお示ししております。現在は19ページ程度の内容でございますが、本日ご用意しておりますものが39ページですので、大幅に増加することを想定しております。

なお、この原案につきましては、次回以降にご審議いただきたい内容でございます。既に、皆様には事前に詳しくご説明させていただきましたが、改めまして簡単にご紹介をさせていただきたいと思っております。

まず、ゼロページ目です。こちらは本書の構成でございますが、今回は「Ⅰ．概説」「Ⅱ．フレームワーク」「Ⅲ．本基準の利用にあたって」という３つのフレームで構成をたてております。

１ページ目でございます。先ほど企画部の藤永から外部委託の有識者検討会の報告書の概要でもご紹介、ご説明いたしましたが、こちらは安対基準の意義として、システムの高度化・多様化による多くの経営資源が必要となってきている現状の中、限りある経営資源を適切に配分して、企業価値の最大化に取り組むこと。そのためには、リスク特性に応じた安全対策の目標を設定することが重要であるということを述べております。

２ページ目につきましては、こちらは今回の安対改訂のコンセプトを示しているページでございます。先ほどの繰り返しになりますが、そもそも現在の安対基準は30年前に、当時、基幹系システムの安定稼働と安全性、こちらを目的として策定しております。しかし、現在は情報系、部門系といったシステムの増加やクラウドサービスや共同センターといったサービス形態の多様化によって、より安全対策基準の適用に当たっての課題が生じてきており、よってその課題にに対する対策を下の図に示しております。

課題としまして、基幹系システム以外のシステムに対する適用基準の不確実性が生じており、安全対策の程度に過不足があるという実態です。それによって、イノベーションや新規開発への資源配分が抑制されていると、認識しております。

もう１点としましては、外部委託の依存度が高まっている状況においては、統制のあり方を明確にするという必要性が生じてきているという認識でございます。

以上の課題を解決するために、安全対策上必要となるＩＴガバナンス、ＩＴマネジメ

ントというテーマ、リスクベースアプローチに基づく基本原則、統制基準の拡充と、この３つを柱として今回安全対策基準の改訂を行っていく次第でございます。

いわゆる、これまでのルールベースから、リスクベースへの転換になると考えています。

３ページ目から５ページ目につきましては、こちらは外部委託の有識者検討会の中で議論されているＩＴガバナンスとＩＴマネジメントに関する内容をそのまま入れております。

続きまして６ページ目ですが、「安全対策基準の考え方」で述べた課題と解決策のうち、リスクベースアプローチの導入の背景と意義を詳細にご説明しています。

続きまして、７ページ目でございます。ここではリスクベースアプローチの考え方に基づいて、ＩＴガバナンスを発揮することが安全対策における基本的な考え方ということで、安全対策基準の基本原則を示しております。先ほど藤永からもご説明させていただきました。

この基本原則の４点目でございますけれども、一方で、ここはリスクベースアプローチと異なる定義が示されております。ここでは、金融機関等は、リスクの発現による影響が個別金融機関等で制御不可能になり外部に拡散する可能性や機微情報の流出により、プライバシー等を侵害するリスクを有するシステムは、「高い安全対策」が必要であると示しています。前者を、重大な外部性と定義し、後者を情報の機微性と定義しています。

用語の参考情報としまして、８ページに記載しております。こちらの内容につきましては、次回以降の審議において重要なポイントだと認識しております。

続きまして、９ページ目でございます。こちらは今、申し上げた基本原則に従ったＩＴガバナンスの内容を説明しており、模式的に図で紹介しております。まず、リスクベースアプローチを前提とした安全対策の目標設定の枠組みがこの図で示されております。ここでは、リスクとしては高い安全対策が必要な要素としましては、重大な外部性と情報の機微性としておりますが、各金融機関の判断によって、高い安全対策が必要なシステムを独自に選定することをこの内容で否定しているものではございません。その考え方については、図中の雲のような部分で示されています。

あと、必要最低限の安全対策という言葉が先ほど藤永のほうからもありましたが、そちらの位置づけがこの図中の点線枠で囲んでいる部分でございます。こちらにつきましても、今後のご議論いただく重要なポイントと考えております。

では、10ページ目でございます。こちらは安全対策における経営資源のあり方を示しておりまして、ここでは安全対策の基本原則に従って安全対策を実施した結果のリスクの顕在化は、結果責任を追及されないということを宣言する内容でございます。こちらにつきましては、外部委託の有識者検討会でご議論されたものをそのまま掲載しております。

続きまして、11ページ目でございます。11ページ目は、本基準上における統制と実務の区分を説明しております。今回の改訂のコンセプトでもあります安全対策上における、主に外部の統制のあり方、こちらを示すために、本基準を統制と実務に分離して整理する旨をご説明しております。ここまでが安全対策の概説部分になります。

続きまして、13ページ目になります。こちらはフレームワークといった実務的な内容を解説した章でございます。まず、こちらのフレームワークは、「総論」と「統制」に分かれます。

「総論」につきましては、定義や適用方法が示されておりまして、「統制」には主に外部の統制に関する考え方が示されております。

13ページ目から16ページ目には、言葉の定義や、基準の分類、構成といった内容が記載されておりますけれども、こちらにつきましては専門委員、検討委員の皆様に事前に詳しくご説明させていただいておりますので、次回以降の専門委員会でさらに詳しくご説明して、ご議論させていただきたいと考えております。

なお、14ページ目の図７の本基準の構成に基づき、新たな基準の構成に配置したものが資料１－３で、Ａ３縦の資料でございます。

17ページ目は本基準の適用対象でございます。こちらは、本基準が適用されるシステムですが、当基準の適用対象は、金融情報システムであるという前提に立って改訂を行ってまいりますが、そちらのシステムやサービス、外部委託の範囲を示す内容となっており、こちらも、次回以降の委員会でさらに詳しくご説明させていただいて、ご議論させていただきたいと考えております。

それでは、18ページ目から19ページ目でございます。こちらは本基準の適用方法をご説明しております。主にリスクベースアプローチに関する内容ですが、ここではリスクベースアプローチに基づく本基準の適用方法に関する基本的な考え方を示しております。

加えまして、経営資源等の制約からリスクベースアプローチの実現が困難な金融機関が存在するということを想定して、簡易法によるリスクベースアプローチによる本基準の適用方法をご説明しています。

では、19ページ目から20ページ目にかけてです。こちらはコンティンジェンシープランの必要性についてのご説明でございます。

それでは、21ページ目からになります。こちらからが「統制」に関する内容でございます。まず、ここからは統制に関する考え方や対策の内容をご説明している章でございますが、こちらの章につきましては、現在内容の取りまとめ段階に入っていますが、『FinTechの有識者検討会報告書』の提言をもとに、原案への反映を確定させる予定でございますので、現段階ではまだ仮置きした内容が記載されている部分がございます。

まず、21ページ目でございますが、こちらは内部の統制に関する基準要素が示されております。21ページ目の後段以降からは外部の統制に関する体系やサービス形態の考え方、それらに対するＩＴガバナンス・ＩＴマネジメント等のあり方を示しております。

24ページ目の後段から25ページ目は、いわゆるオープンＡＰＩに関する安全対策基準を利用するに当たっての原則的な考え方などをご説明しています。

25ページ目の後段から、決済代行業者が外部の統制先となる場合のパターンを紹介しているページでございます。

最後の27ページ目以降でございますが、こちらにつきましては本書の見方や記述様式、といったもので、これまでと同様の内容や、一部取り扱い方の変更内容をご説明しています。簡単にご説明させていただきましたが、以上が原案のご説明になります。

○和田監査安全部長　以上を踏まえまして、ご承認いただければ、次回からご審議いただくことになりますが、改めまして本審議事項『金融機関等コンピュータシステムの安全対策基準・解説書』について、安全対策専門委員会を月１回程度開催し、会員意見の募集を経て、３月末をめどに発刊できるよう改訂作業を開始すること」に関しまして、ご意見・ご質問等ございますでしょうか。

○蓮實委員代理　内容はこれ以降ということではあるんですけれども、１点だけ、10ページのところ。ほかにも前回、事務局にはこういうところおかしいんじゃないのというのをお渡しさせていただいたんですけれども、青い線で囲まれているところ。「経営層の使命は企業価値の最大化であり」という文言がございます。これも事務局には１回した話ですが、私ども信用金庫は共同組織の金融機関でございますので、株式会社組織ではございません。地域や会員皆様の相互扶助の精神に基づいた地域繁栄のために、一応、理念と

して金融機関をやらせていただいているという形になります。

もちろん、全く収益を上げないと自己資本比率が下がってお客様が苦しいときにお金を貸せなくなってしまいますから、もちろん収益を上げることも必要なんですけれども、「経営層の使命は企業価値の最大化である」ということを多くの金融機関の共通認識のように書かれてしまうのは、共同組織金融機関としてはちょっと受け入れがたいものがあるということをここで言わせていただきたいということでございます。

○和田監査安全部長　ご意見ありがとうございました。

○藤永次長　外部委託の有識者検討会において、まさに今ご指摘いただいたパートを書かせていただきましたのでコメントさせていただきます。まず、外部委託の有識者検討会の委員としては、巣鴨信金の鈴木様にもご参加いただきまして、そのときには蓮實委員が言われたようなご意見をいただいておりませんでした。だからといって、そうしたご意見を今後も受けないというわけではございませんで、先ほど理事長から話がありましたとおり、安対基準の改訂においては現場の実態を踏まえて皆様が利用しやすく、かつ理解しやすいものにするという観点でご議論いただきたいということで、まさに今、蓮實委員からご指摘いただいたことがまさにそれにあたるものと思います。有識者検討会は比較的抽象的な議論が中心となっていますので、ぜひほかの委員の方々にも、利用しやすく、理解しやすいものにするという観点から、皆様の業態・業界を踏まえたご意見をいただけるとありがたく思います。以上です。

○和田監査安全部長　内容につきましては、次回以降ご審議いただければと思います。ほかにご意見・ご質問等ございませんか。時間も予定より随分押していますので、もしなければ、本審議事項はご承認いただいたものとさせて……。

○蓮實委員代理　それはおかしいんじゃないですか。私、先ほど申し上げました。きちんと決をとって、賛成するということはFISCさんはそうされると言っているので、案が公表されるインターネットにおいてということにご賛同なされる委員さんがいらっしゃるのであれば、ぜひ賛成していただいて、私はぜひ反対をさせていただきたいと思っていますということです。

○和田監査安全部長　申しわけございません。

○藤田委員　すみません。１点だけよろしいですか。情報の公開については、その程度を含めて公益財団法人としての構成要件であるという説明が先ほどあったと思います。。そこの領域に踏み込んだ問題をここの場で討議するというのは、そういう権限があるのかという問題になり得るわけです。ですから、例えば公益財団であるということを今さらやめる・やめないということであれば、違う場で議論すべき話に、いい・悪いは別として、そういう話になる。

今の状況を認める前提の上での改訂を審議するというコンテクストの中で今やっているわけです。それに対して異議があるのであれば、ちょっと違う場にやはりならざるを得ない。この場は公表する・しないは程度の問題と言っているのは、ホワイトリスト方式で基本はする、しかしながら、重大な問題というものに関してはブラックリストでやるのか、あるいは、ブラックリストにしてホワイトリストにするか、いろいろな議論があるかと思うのですけれども、少なくとも正統性・レジテマシーに関わる領域をここでする、決をとるというのは、たてつけ上難しいと思います。

○和田監査安全部長　審議の中には資料の公開は含まれておりません。なので、まず整理したいのは、資料の公開については審議外であります。今回審議したいことは、今後コンピュータシステムの安全対策基準解説書のために安全対策専門委員会を月１回程度開催して審議をしていくというところです。

一方で、資料の公開については公益財団法人の構成要件にかかわることですので、ちょっとここではその審議の中に絡めるわけにはいかないというふうに考えておりまして、それは別というふうにさせていただきたいと思います。それを踏まえて、本審議についてご意見をいただければと思います。

○蓮實委員代理　先ほど私、申し上げたように、それをFISCさんがどうしてもやるということを決定されているのであって、我々に覆させないというのであれば、それが出ないようにするためには審議自体を否決するしかないと私は申し上げたんです。

○和田監査安全部長　ですのでご意見は伺ったんですが、そのとおりにするとは先ほどは言っております。

○蓮實委員代理　そうですね。ですから、私はしていただきたいという話と、そういう意味があるということを委員さんによくご理解いただいて、富士通さんにもよくご理解いただいて、それが金融機関にとってプラスになるのかプラスにならないのか。それをどういうふうに金融機関が思っているかということを鑑みていただいて、ご賛成いただけるのであれば賛成すればよろしいと思いますし、反対されるなり棄権されるなりというのはそれぞれのお考えだと思います。

○和田監査安全部長　何度もお話しさせていただきますが、資料の公開、議事録等の公開と今回の審議事項というのはちょっとレベルが違う話ですので、まずは今回の審議事項ですね。「金融機関コンピュータシステムの安全対策基準の改訂について、月１回程度会員の意見を経て３月末をめどに発刊できることについて改訂作業を開始すること」、これについてご承認いただければ、挙手お願いします。賛成多数ですので、審議承認とさせていただきます。

○蓮實委員代理　わかりました。では、私、反対票。手を挙げていないですけど反対なので、それは議事録に残していただけるということでよろしいですね。

○和田監査安全部長　わかりました。続きまして、ちょっとお時間も押しているんですが、２つ目の審議事項、「金融機関等におけるＩＴ人材の確保・育成計画策定のための手引書の作成の着手及びＩＴ人材検討部会の設置について」より議事を進めてまいります。お手元の資料、資料２－１をご用意ください。資料２－１でご審議いただく事項は、ＩＴ人材検討部会を設置し、３月末の発刊を目指して検討を開始することでございます。ＩＴ人材検討部会で検討しようとする内容については、調査部から説明をいたします。

３.【審議２】～

○中山調査部長　調査部長をしております中山です。ＩＴ人材検討部会を設置するこ

ととなった暁には、調査部及び監査安全部のサイバー対策室が事務局としてご準備していく予定ですので、よろしくお願いいたします。

○加藤総括主任研究員　調査部の加藤でございます。

それでは、お手元の資料のうち、右上に資料２－２と記載がございます「金融機関等におけるＩＴ人材の確保・育成のための手引書原案概要」をご用意ください。

まず、本題に入る前に御礼を申し上げたいと思います。安全対策の基準改訂同様、人材育成につきましても専門委員の皆様、検討委員の皆様にご多忙の中お時間をいただきまして、いろいろなアドバイス、ご助言をいただきました。ありがとうございました。この場をお借りしまして御礼申し上げたいと思います。

それでは、本題のほうに入らせていただきます。表題にございますとおり、『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』を名称案としております。こちらの資料は、もう１部Ａ４縦の手引書の原案、こちらの内容の概要をまとめさせていただいたものでございますので、このパワーポイントのＡ４横の資料をベースにご説明のほうをさせていただきます。

ページをおめくりください。１ページになります。本手引書では、４点で構成する案としております。第１編「はじめに」におきまして、手引書作成の背景や位置づけについて記載をしていこうと考えております。

第２編の「経営層の役割」におきましては、経営層の関与につきまして、重要性などについて記載をしていこうと考えております。

第３編の「ＩＴ人材の確保・育成に向けた実務」におきましては、実際の工程や手順及びそれぞれの考慮事項につきまして記載していこうと考えております。

第４編では「サイバーセキュリティ人材に関する考慮事項」を記載していこうと考えております。以上が構成になります。

次のページをごらんください。２ページになります。ここからは各編の概要についてご説明申し上げます。第１編「はじめに」についてでございます。ここでは本手引書を作成する背景及び位置づけについての記載になります。

まず１つ目でございますが、背景です。我が国の金融機関等におけるＩＴの利活用が大きく進展したことに伴いまして、それを支える人材の役割がこれまで以上に大きくなっているということが言えるのではなかろうかということでございます。

そして、システム戦略を実現するために必要な業務―手引書上はＩＴ業務とさせていただいておりますけれども、システム部門だけにとどまらず、システム部門以外の様々な部門に関わりが広がってきているというところもございますので、部門間、さらには外部委託先等の社外との連携というものがより一層重要となってくると思っております。

そして、その背景にはこちらの（１）から（４）までお示しした内容がその背景にあるのではなかろうかと考えております。若干、中身についての補足をさせていただきますと、「業務の外部委託化の進展」につきましては、システムの開発や運用につきましては、共同センターを含む業務の外部委託化というものが進んでおりまして、それらのスキルを各金融機関がどのように維持していくかという点が課題として挙げられるようになってきているということでございます。また、外部委託管理できるＩＴ人材の重要性についてもクローズアップされてきていると考えております。

２点目の「リスク管理の高度化・複雑化」でございますが、システム戦略は経営戦略、あるいは事業戦略と一体でございます。ＩＴに関係する分野が広がるに伴いまして、そのリスクも高度化・複雑化してきています。そして、それらのリスク管理に携わるＩＴ人材の重要性が増してきていると思います。

そして、３つ目の「サイバーセキュリティ対応」でございますが、金融機関等におきますサイバーセキュリティにつきましては、DDoS攻撃であるとか標的型メール、あるいは不正送金など、日々高度化・複雑化しています。各金融機関におかれましてはその対策を行う人材を必要としており、サイバーセキュリティ業務を担うための人材というものが求められているということでございます。

そして、４つ目は「新しい技術やサービスへの対応」でございますが、近年のクラウド、FinTech、あるいは高度なデータ分析など、新しい技術やサービスが登場してきております。それらをビジネスや業務にどのように活用していくかというところを検討、あるいは提案できる人材が求められていると考えております。

このように、ＩＴ人材の確保・育成というものはシステム部門だけではなく、全社一体となって取り組んでいくことが求められているのではなかろうかというところでございます。そして、そのためには金融機関の経営層は、システム戦略に基づく、ＩＴ人材の確保・育成に向けた取り組みに積極的に関わり、態勢を整える必要があると考えております。

また、先ほどもご説明させていただきましたが、「金融機関における外部委託に関する有識者検討会」この中におきましても、「経営層は」ということで２点提唱させていただ

いております。１つは人員数・スキルの種類とレベル・配置の把握、次に、全体の中長期計画に沿った人員の育成計画の策定について提唱させていただいています。

こういった背景を踏まえ、金融機関等が個々の経営判断により、ＩＴ人材の確保・育成を進めていく際に参考となる手引書というものを作成していきたいというものでございます。

それでは、次のページをごらんください。４ページになります。第２編「経営層の役割」についてです。ここでは計画策定における経営層の関与の重要性と役割について記載しております。

まず、経営層の関与の重要性についてでございます。大きく２つ述べさせていただいておりますけれども、１つは、ＩＴガバナンスを機能させるということの必要性です。もう一つは、ＩＴに関する重要事項の中ということで、システム戦略方針あるいはシステムリスク管理方針等々、さまざまな決定することがございます。これらの決定事項を実現するためには、やはりＩＴ人材の確保・育成というものが非常に重要な事項ということになってくると思われます。ですので、経営層が積極的に関与していくべき事項であるということを述べていきたいと考えております。

ページをおめくりください。５ページになります。ここではＩＴ人材の確保・育成における経営層の関与の中の留意事項について、いくつかお示ししております。上２つにつきましては、金融機関における外部委託に関する有識者検討会において提唱された事項になります。

下の２つでございますが、３つ目につきましてはＩＴ人材の確保・育成計画作成時の体制整備についてです。４つ目につきましては、策定後の体制整備について、お示ししています。

策定時の体制整備につきましては、「経営層は」というところで、必要に応じてプロジェクト組織を立ち上げるなど、関連部門の相互協力というものが得られる、そういう体制を整備していくことの必要性をお伝えしようと思っています。

策定後の体制整備につきましては、策定後、ＩＴ人材の確保・育成を滞りなく遂行できる体制を整備し、遂行状況を適宜確認し、必要に応じて計画を見直すということの必要性を述べていきたいと考えております。

それでは、６ページをごらんください。第３編ＩＴ人材の確保・育成に向けた実務についてのご説明になります。ポイントは上段の四角の箱に記載している内容になります。１

つ目ですが、経営層から実際に指示を受けた実務部門等が計画を策定していくための工程であるとか手順といったものを記載していこうと思っています。

２つ目ですが、本手引書では、基本的な考え方や考慮事項を記載するにとどめております。ただ、それだけですとイメージがわかないという点もございますので、イメージがつかめるような参考例を記載していこうと考えております。

金融機関の実例等が様々である点を踏まえまして、具体的な取組み事例などにつきましては、機関誌レポートなどで還元をしていこうと考えております。よって、本手引書と機関誌のレポートなどをセットでご活用いただくことを想定しております。加えまして、手引書とレポートの関連性というものがわかるような工夫を施すということも考えていきたいと思います。

なお、詳細につきましては今後、検討していきたいと思っています。

また、この手引書は発刊後、全国説明会等を通じまして、内容・考え方についてご説明を行っていくことを検討していきたいと考えております。

この箱の下の方に工程案を記載しております。各金融機関等におきまして策定されているシステム戦略の方針であるとか人材育成の方針といったものに基づいて、大きく３つの工程でＩＴ人材の確保・育成計画を策定していくという内容となっております。第１工程におきましては、ＩＴ業務の洗い出しということで、現状及び中長期的なものをまず洗い出しましょうというところです。

第２工程で、それを踏まえてＩＴ人材のスキル、人材というものを定義して、必要なＩＴ人材の把握をしていくと考えています。

この第１と第２工程を経て、具体的に計画を策定していくというところでございますけれども、その際、現状及び中長期的に必要なもの、ここの過不足というものが出てくるかと思います。その解消策の検討を行っていくということも述べていこうと思っています。解消策の策定に当たりましては、例えば知識レベル、経験レベルの向上策等の育成の検討、採用や配置転換等の検討等ついても記載していくことを考えています。

これらの第１工程から第３工程を経て策定された内容につきましては、全体の計画、例えば全社的な人事計画等に取り込まれて反映されるものと考えておりますし、また、策定後につきましてはＰＤＣＡサイクルを回し、必要に応じて見直しを図るということも必要になってくるものと考えております。

第４編、最後のページをごらんください。７ページになります。サイバーセキュリティ

人材に関する考慮事項を記載しています。サイバー攻撃につきましては、先ほど冒頭触れておりますけれども、日々高度化・巧妙化が進んでおりまして、その検知、被害の拡大防止のために対応態勢の整備が求められて、サイバーセキュリティ人材の確保・育成についても喫緊の課題となっております。

本編では、先ほど第３編で述べました実務部門等が計画を策定していくための工程手順等の観点で、サイバーセキュリティ業務について洗い出すとともに、人材の定義・スキル及び確保・育成に関して考慮すべき事項を取りまとめております。

サイバーセキュリティ業務と役割は、当センターで今月発刊予定の『金融機関等におけるコンティンジェンシープラン策定のための手引書』におきまして、態勢整備・平時からの運用・インシデント発生時の運用、この３つの観点から整理をさせていただいております。サイバーセキュリティ人材のスキルを定義するに当たりましては、インシデント対応組織の中でも外部委託先を含めた統括や業務影響の評価であるとか、対応策の判断、こういったものにつきましては自機関で望まれる役割になると考えられますので、考慮事項として取り上げております。

また、サイバーセキュリティ業務を確実かつ迅速に対応するためには、経営層とインシデント対応組織とのコミュニケーションが重要になってくると思います。社内の関係部門だけでなく、社外関係機関との連携が不可欠となることから、橋渡し人材についても触れようと思っております。

なお、スキルに関しましてはＩＴ人材と共通で、一般のＩＴ知識などが必要になってくると思われますけれども、変化し続ける環境や攻撃手口など、サイバーセキュリティ固有の知識及び業務への影響を評価するために、業務知識が求められます。

第３工程の確保・育成計画の方法につきましては、システム部門との人材交流、サイバー攻撃の訓練・演習などを通じまして、自機関の業務分析や対応人材のスキルアップ、また、大学など関係機関などを通じました産官学連携した教育機関の利用等につきましても記載をしております。

以上のように特筆する事項についても取りまとめをしまして、ＩＴ人材確保・育成計画手引書として、サイバーセキュリティ人材についても述べていきたいと思っております。

こちらのサイバーセキュリティ人材につきましても考慮事項の中で参考文献などはお示ししておりますが、具体的な取組み事例につきましては機関紙レポート等の中で皆様に還元していきたいと思っております。

以上が金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書の原案の概要となります。審議事項であります本手引書作成の着手並びにＩＴ人材検討部会の設置につきご承認いただきました後は、今年度末の発刊に向けまして、検討部会等を通じまして皆様からいろいろご助言等をいただきながら作業を進めさせていただければと思っております。よろしくお願いいたします。

私からの説明は以上でございます。

○和田監査安全部長　調査部の中山部長、加藤総括、ありがとうございました。ご承認いただければ、今後検討部会でご審議いただくことになりますが、改めまして本審議事項に関してご意見・ご質問等はございますでしょうか。ないようですので、それでは、本審議事項につきましてはご承認いただけたものといたします。ありがとうございました。

４．事務連絡

○和田監査安全部長　最後になりますが、事務連絡が２点ほどございます。まず１点目、お配りした参考資料３につきまして、資料の不備がございました。「FinTech に関する有識者検討会報告書（案）」の 58 ページでございます。印刷のずれがございました。取り急ぎ今、本ページのみ改めましてご用意させていただいております。差しかえページとして皆様に配布させていただきます。お持ち帰りください。資料準備の不手際、まことに申しわけございませんでした。

２点目は、今後の日程についてでございます。次回の専門委員会は６月を予定しておりますが、日程は近日中に皆様にご案内させていただきますので、大変申しわけございませんが、少々お待ち願います。

なお、先ほど承認いただきましたＩＴ人材の検討部会につきましては、６月12日月曜日、15時半から17時、FISC会議室にて開催を予定しております。

最後になります。お時間を大きくオーバーして大変申しわけございませんでした。全体を通して何かご質問等ございますか。ないようでございます。それでは、第51回安全対策専門委員会を終了いたします。本日はお忙しい中お集まりいただき、まことにありがとうございました。

以上