平成29年10月17日

公益財団法人　金融情報システムセンター

第57回　安全対策専門委員会　議事録

Ⅰ　開催日時：

平成29年10月17日(火)15:00～16:40

Ⅱ　開催場所：

ＦＩＳＣ会議室

Ⅲ　出席者(順不同・敬称略)

座長	細溝　清史	公益財団法人金融情報システムセンター 理事長
副座長	渕崎　正弘	株式会社日本総合研究所 代表取締役社長
専門委員	花尻　格	株式会社三菱東京ＵＦＪ銀行 システム企画部　副部長
	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
	山田　満	株式会社南都銀行 システム部　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　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
	猿渡　耕二	（代理出席）労働金庫連合会 統合リスク管理部　システムリスク管理グループ 次長

常岡　良二	農林中央金庫 ＩＴ統括部　主任考査役
高橋　祐二	（代理出席）株式会社商工組合中央金庫 システム部　リスク管理グループ　調査役
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
中川　彰男	（代理出席）三井住友海上火災保険株式会社 ＩＴ推進部　ＩＴ管理チーム　次長 兼コンプライアンス部　情報資産管理チーム　次長
橋本　伊知郎	野村ホールディングス株式会社 参事 Co-CIO 野村證券株式会社 経営役　業務企画、ＩＴ基盤、国内ＩＴ担当
白井　大輔	（代理出席）三井住友カード株式会社 システム企画部　上席審議役
岡田　拓也	日本銀行　金融機構局　考査企画課 システム・業務継続グループ長
相田　仁	東京大学大学院 工学系研究科　教授　工学博士
安冨　潔	慶應義塾大学　名誉教授 京都産業大学　法務研究科客員 法教育総合センター長 弁護士（渥美坂井法律事務所・外国法共同事業）
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
濱中　慎一	（代理出席）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 担当課長
粟津　濃	沖電気工業株式会社 金融・法人ソリューション事業部 プロジェクトマネジメントオフィス　室長
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
	柿本　薫	株式会社日立製作所 金融第一システム事業部　事業推進本部　本部長
	服部　剛	（代理出席）富士通株式会社 金融・社会基盤営業グループ 金融リスクマネジメント室　室長
	太田　海	（代理出席）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 上級セキュリティコンサルタント
	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
	瀧　俊雄	一般社団法人 Fintech 協会 アドバイザー
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
検討委員	伊藤　武男	株式会社三菱東京ＵＦＪ銀行 システム企画部　事務・システムリスク統括室 サイバーセキュリティ推進グループ　上席調査役
	山口　康隆	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 システムリスク管理グループ　グループ長
	大門　雄介	（代理出席）株式会社南都銀行 経営企画部　東京事務所　協会担当
	吉原　丈司	株式会社東京スター銀行 ＩＴ戦略部　部長
	嶋村　正	信組情報サービス株式会社 企画部　部長
	今嶋　治	農林中央金庫 ＩＴ統括部　副部長

	佐々木　達典	（代理出席）第一生命保険株式会社 課長補佐
	荒木　冬湖	野村ホールディングス株式会社 ＩＴ統括部　ヴァイスプレジデント
	鈴木　健一	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　課長
	羽太　英哉	沖電気工業株式会社 金融・法人ソリューション事業部 プロジェクトマネジメントオフィス シニアスペシャリスト
	碩　正樹	日本電気株式会社 プラットフォームサービス事業部　主任
	後藤　茂成	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 チーフ・コンサルタント
	宮崎　真理	株式会社日立製作所 金融第一システム事業部　事業推進本部 システム統括部　CSIRT グループ　主任技師
オブザーバー	市村　雅史	金融庁 検査局　システムモニタリングチーム専門検査官
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
	和田　昌昭	公益財団法人金融情報システムセンター
FISC(事務局)	小林　寿太郎	企画部 部長
	松本　浩之	監査安全部 総括主任研究員
	丸山　亨嗣	監査安全部 総括主任研究員
	名取　政人	監査安全部 総括主任研究員

Ⅳ　議事内容

１．開会

○和田監査安全部長　それでは、お時間になりましたので、「第 57 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してまことにありがとうございます。まずは事務事項について、公益財団法人金融情報システムセンター監査安全部の和田からご説明いたします。よろしくお願いいたします。

（資料確認、委員紹介等のため省略）

それでは議案に入る前に、今後の予定についてご説明させていただきます。お手元の【資料０－１】をご用意ください。前回の委員会で 11 月 21 日に追加の委員会開催をご了承いただきましたので、今後の予定について一覧にまとめてあります。本日は第 57 回になりますので中央のオレンジの網かけ部分になります。基礎基準の整理につきましては、本日、考え方についてご承認いただいて、基準原案につきましては、本日ご議論をいただき、次回 11 月 21 日にご承認いただければと思っております。

読みやすさの対応についての、基準構成、読みやすさ向上と統制基準の再編は、他の議案の最終案を受けての整理となりますので、全て 11 月 21 日に他の議案と合わせてご承認いただく予定です。

外部委託基準の統合整理につきましては、本日考え方の整理についてご承認いただき、基準原案につきましては、本日もご議論いただいて 11 月 21 日にご承認いただけるようにしたいと思っております。

前説のほうですが、これも他の議案の最終案を受けての加筆修正となりますので、11 月 21 日にご承認をいただく予定です。

11 月 21 日には全ての議案についてご承認いただき、その後、会員意見の募集に入る予定です。今回の改訂は内容も多岐にわたり、ボリュームもかなり多いので、会員意見募集期間はある程度期間が必要と考えております。ですから 1.5 カ月を設定する予定です。

また、会員意見募集後の各委員様や会員への事前説明にも、一定の期間が必要と想定しておりますので、改訂内容を確定させる第 60 回専門委員会は、２月上旬ごろになると考えております。その日程につきましては、また日程が確定次第、ご連絡さし上げようと思っております。以上、今後のスケジュールについてのご説明になります。

２．議案１

〇渕崎副座長　副座長の渕崎です。

それでは議案１「基礎基準・付加基準の整理に関する方針及び対応」について、事務局の松本総括主任研究員よりご説明をお願いします。

○松本総括主任研究員　事務局の松本です。よろしくお願いいたします。

【資料１－１】から【資料１－５】をご用意ください。資料が大変多く恐縮でございます。

【資料１－１】のご説明は、前回の専門委員会の議案についてのご意見をまとめております【資料１－２】とあわせてご覧願います。

まず【資料１－１】のⅠ番目で、前回の専門委員会でお示しした論点５つを記載しております。各論点に関するご意見をご紹介させていただきます。

まず、論点１及び論点２でございますが、こちらは解説部分の位置付けについての論点でございました。解説部分において、「必要である」という語尾が記載されている対策については、各基準の必須対策として位置付け、また語尾が「望ましい」、あと例示で示されている対策ついては全てリスクベースアプローチによって選択的に適用するものとして位置付けることを提示させていただきました。

ご意見としましては【資料１－２】のご意見ナンバー３と４に記載しておりますが、皆様、論点１の方針につきましては、ご賛同いただけるご意見のみでございました。

続きまして論点３及び論点５についてです。こちらは「適用にあたっての考え方」に「望ましい」という記載がある基準に対する考え方でございます。まず、暫定的に基礎基準候補に挙がっておりました基準の「適用にあたっての考え方」に「望ましい」という記載があるものは、「望ましい」を「～すること」に統一して、基礎基準に選択された基準は、付加基準としたほうがよいというご意見でした。

付加基準候補の中で「適用にあたっての考え方」が「望ましい」という記載があるもの、こちらも同様に「望ましい」という表現については、「～すること」に統一したほうがよいのではないかというご意見です。

さらに、前回の論点で提示した、付加基準候補については、解説部分に必須対策となる表現「～することが必要である」という記載がないものがございました。したがいまして「望ましい」や例示のみが記載されているものについては改めて必須対策を追記するといった修文等を行う必要があるかどうかについても、論点としてお示ししたところでございます。そちらにつきましては、現状表現のままでよいのではないかというご意見のみでしたので、追記等の対応は行わないこととといたします。ご意見ナンバーはナンバー６～ナンバー15 でございます。

論点４です。こちらは基礎基準候補の中に挙がっているものの中で、個別のシステムや業務に関する基準の位置付けについて、これは全ての金融情報システムに該当するものではないので、付加基準と位置付けてはどうかという論点でございました。こちらについても、付加基準とするべきというご意見のみでございました。ご意見ナンバーは、ナンバー20～29 にお示ししております。

各論点に対するご意見をもとに【資料１－１】の「Ⅱ.方針案」に各方針を示させていただきました。まず論点１及び論点２、解説部分の位置付けですが、ご意見としましては、全て前回の論点にご賛同をいただいておりますので、基礎基準や付加基準において解説部分で「必要である」という語尾が記載されている対策につきましては、全て各基準の必須対策として位置付けます。「解説部分」で「望ましい」という語尾が記載されている対策や、例示におきましてはリスクベースアプローチによって選択的に適用されるものという位置付けとします。なお、この方針につきましては、前説でしっかりと記載していきたいと考えております。

続きまして論点３及び論点５です。「適用にあたっての考え方」が「望ましい」となっている基準についてでございます。まず基礎基準候補につきましては、付加基準へ変更したいと考えております。さらに「適用にあたっての考え方」に「望ましい」という記載につきましては、「～すること」に統一いたします。

また、付加基準候補に挙がっている基準も同様に「望ましい」という記載については、「～すること」に統一いたします。

「必須対策」が示されていない基準につきましては、現行のまま表記したいと考えております。

なお、論点３、礎基準候補に挙がっておりました「適用にあたっての考え方」が、「望ましい」という基準の中で、廃止したほうがよいのではないかというご意見がございましたので、そちらにつきましては、後ほど論点としてご提示させていただきます。

なお、この論点３及び論点５に該当する基準につきましては、別紙の【資料１－５】「改訂原案」にご紹介しておりますので、後ほどご確認いただければと思います。

論点４についてでございます。個別のシステムや業務に関する基準は、全ての金融情報システムには適用されないことから、付加基準としたいと考えております。なお、これも前回の論点４でご紹介させていただいております基礎基準候補以外の基礎基準の中で、同様の考え方に該当するのではないかというご意見がございましたので、こちらも後ほど論

点としてご提示させていただきます。

なお、論点３～４に該当する基準につきましては、【資料１－１】の４ページに掲載しておりますので、ご参考ください。

それでは戻っていただきまして、【資料１－１】の２ページ目の論点に移らせていただきます。先ほど申し上げました、廃止したほうがいいのではないかというご意見があった基準に対する論点でございます。まず、基礎基準候補のうち、【実 13】「クライアントサーバーシステムにおける作業の管理を行うこと」という基準がございます。この基準は、、安対８版の【運 23】にありますが、こちらの基準は今日的な意義がもうなくなっているために廃止することが適当であるというご意見が複数ございましたので、この基準について廃止したいと思います。なお、廃止に伴う対応案としましては、クライアントサーバーに関する基準の目的や対策につきましては、新基準番号【実 10】【実 11】【実 12】に同様の運用の基準がございます。違いは、対象がクライアントサーバーかコンピューターシステムかというだけになりますので、当該基準に統合し、クライアントサーバーについては、安対基準の用語解説に定めるコンピューターシステムの定義を修正し、クライアントサーバーも含まれるように、用語の修正を行う対応を考えております。

なお、本件のご意見は、【資料１－２】のナンバー16、17 に記載しております。以上が、論点１のご説明でございます。

続きまして、論点２です。暫定的な基礎基準の候補の中に個別のシステム及び業務に係る基準に該当するものがあるのではないかというご意見がございましたので、記載の３つの基準については、付加基準としてはどうかという論点でございます。実際の基準は別紙の【資料１－３】に基準をご覧ください。

なお、【実 34】につきましては、インターネット・モバイルの口座開設等を行う場合の本人確認に関する基準と記載しておりますが、既存の基準ではインターネット・モバイルサービスを対象とする記載がございません。実際本文を読みますと、インターネット・モバイルに関する口座開設の基準として書かれておりますので、基準の大項目・中項目・小項目を修正いたしまして、個別システム及び個別の業務に関する基準という位置付けとし、付加基準としたいと考えております。

論点３です。以上、今ご説明させていただきました方針並びに論点の提案をもとに整理した最新の基準内訳状況は、基準総数が 168 件になり、基礎基準が 103、付加基準が 65 となっております。基準総数は、これまで外部の統制に関する基準の件数を含めておりま

せんでしたので、今回から反映されたことによって総数が増加しています。基礎基準、付加基準においては、本日の論点に対し次回議論を行ったうえで先ほど冒頭で和田のほうからも説明がありましたとおり、次回の専門委員会で確定したいと考えております。

最後に【資料１－１】にはお示ししておりませんが、【資料１－２】のご意見ナンバー１番、２番、５番で、前回、専門委員会で、基礎基準、付加基準の整理に関する方針について提示した文章に対し不自然な点があるというご意見がございましたので、ご意見の対応方針をお示しさせていただいております。その内容を原案に反映させていただいている先が、別紙の【資料１－５】の２ページ目、３ページ目に黄色マーカー部分で記載させていただいております。

基礎基準の必須対策及び付加基準の必須対策においては、必ず適用されるものと位置付けておりますが、当然、その基準自体が該当しない先については、適用する必要はないといった考慮点を、脚注及び安全対策の目標設定のプロセスの中で、説明する形に修文させていただいております。

私の説明は、以上でございます。

○渕崎副座長　ありがとうございました。この案に対しましてご質問、ご意見等ございましたらよろしくお願いいたします。

よろしゅうございますか。多くの皆さんの意見をかなり反映したものになっていると思います。ここで思いつかなくても、後で気になった点があれば、事後意見としてお寄せください。本日の審議内容と事後意見を合わせまして、次回の専門委員会で、最終案をご説明させていただきたいと思いますので、よろしくお願いいたします。

それでは、議案２「読みやすさの対応について」、事務局の名取総括主任研究員より、ご説明をお願いします。

３．議案２

○名取総括主任研究員　事務局の名取です。【資料２－１】から【資料２－５】までをご用意ください。【資料２－１】に沿って説明をします。

まず１つ目「読みやすさ」に対するご意見ですが、【資料２－２】の一覧表にまとめて

おります。全部で131件のご意見がございまして、基準番号順で並べております。また、それぞれ分類の上、事務局で対応方針案、原案の修正要否、反映予定について記載しております。

なお、前回の委員会で原案を提示させていただきました「統制基準の一部再編・見直し」については、特段ご意見はございませんでした。よってこの一覧表にご意見をいただいた部分について、「修正要」とした部分について、今後原案のほうに反映させていきたいと考えております。

原案への反映予定については、後ほど説明させていただきますが、一部反映予定の日付が本日の日付になっているものがあります。これは基準小項目、いわゆる基準のタイトルに当たる部分でして、後ほど説明する資料に既に反映しております。

今回いただいたご意見の中で、特に本日この場でご検討いただきたい部分について、【資料２－２】の３ページ目、５ページ目、６ページ目の対応方針に網かけをしております。これは、全て語尾が「重要である」となっている文章に対するご意見となります。

ここからは【資料２－１】に戻りまして、「Ⅱ．語尾「重要である」の解釈について」を説明します。現在、基準の解説部分の語尾が「必要である」を必須対策として、その他の語尾や例示については選択可能な対策としています。この定義に従いますと、語尾が「重要である」の文章については必須対策とはなりません。しかし今回、語尾が「重要である」の文章について、複数の委員の方から、必須なのか例示なのかわかりにくいといった意見をいただいております。「重要である」は先ほど申しましたとおり、必須対策ではないと定義されていますが、その語感から必須対策の「必要である」に近いと読まれてしまう等のさまざまな解釈を生んでいると推察されます。

そこで今回、「重要である」を含む基準９つになりますが、利用者が統一した解釈を行うことができるように、対応を検討することにしたいと考えます。

対応案についてご説明させていただきます。【資料２－３】になります。まず、資料の見方ですが、左側に基準番号があり、対策本文、今回いただきました委員の方からのご意見、その右に対応案１、２、３と記載しております。

まず対応案１ですが、これら全ての「重要である」という文章について、必須対策ではない他の表現に一律変更する。つまり、「望ましい」といった表現に一律変更するという案となります。もともと「重要である」は必須対策として位置付けていなかったという経緯を踏まえますと、最も影響は小さく解釈がぶれない表現に変更できるというメリットが

あるかと思います。

続いて対応案２になります。こちらは実際の対策の記載内容を踏まえ、必須対策にするのが妥当であると考えられる場合は、語尾を「必要である」に変更し、それ以外については「望ましい」に変更する案になります。この案については事務局案として【資料２－３】で振り分けを行っておりますので、少し長くなりますが、それぞれ説明させていただきたいと思います。

まず１つ目の【実 28】になります。対策本文の「重要である」を含んでいる文章を読みます。「また、営業店以外の場所で１人で端末機操作が行える渉外端末等については、権限の範囲を明確にしておくことが特に重要である」について、対応案として、「必要である」に変更としております。これは類似の基準である【実 41】の「使用しないソフトウェアを制限する等セキュリティを考慮した設定とする必要がある。」と同様に「必要である」と変更するのが適当と考えています。

続いて【実 50】、「なお、システムの構成、使用形態、使用状況、設置台数等を把握しておくことも重要である」について、対応案として「望ましい」に変更するのがよいと考えております。使用形態、使用状況は、システムによっては把握が容易ではないケースがあり得るため、「望ましい」に変更することが適当であると考えています。

続いて【実 60】、「システムの信頼性向上を図るうえで、ソフトウェアの信頼性向上対策を講ずることが重要である」について、対応案として「必要である」に変更するのがよいと考えております。次の文章に「ソフトウェアの品質確保については、【技７～技 15】参照のこと」とありますが、これらの基準は、全て基礎基準となります。よって必須としての「必要である」に変更することが適当であると考えています。

続いて【実 62】、「また円滑に本番運用に移行するため、運用部門（運用担当者）への引き継ぎ、説明及びユーザーへの説明を十分に行い、準備状況を確認することが重要である」について、対応案として「必要である」に変更するのが適当と考えております。これは本基準の「適用にあたっての考え方」にほぼ同様の記載があり、「～すること」となっておりますので、「必要である」に変更することが適当と考えられます。

続いて【実 85】、前半と後半２つ「重要である」があります。まず１つ目、「特に、資金移動及び注文等の取引に関しては、不正使用の早期発見のため、処理結果が確認できる機能を提供することが重要である」について、類似の基準で【実 84】の対策１に、「特に資金移動および注文等の取引に関して、～必要である」となっているため、同様に「必要

である」に変更することが適当と考えています。そして２つ目の「重要である」ですが、「なお、不正に使用されていないかの確認を利用者自身が行うことを注意喚起することも重要である」については、類似の基準で【実 87】の対策３に「定期的に残高や取引履歴を確認するよう顧客に推奨することが望ましい」となっているため、同様に「望ましい」に変更することが適当と考えています。

続いて【実 99】、「ソフトウェアの品質を確保するためには、まず設計段階から品質を高めることが重要である。そのために考慮すべき点として以下のものがある」についてですが、これは「重要である」と書いてありますが、一般論を示しており対策ではないと考えられます。ただし、このまま「重要である」を残しておきますと、利用者の混乱を招く可能性がありますので、「重要であり、」とし、文章を続けるような変更にするのがよいのではないかと考えております。

続いて【実 105】、「機能の変更・追加作業時においては、変更、追加に伴うほかへの影響をチェックし、極小化することが重要である」について、「極小化」が容易ではないケースもあり得るということが考えられますので、「望ましい」に変更することが適当と考えてています。

続いて【実 125】、「コンピューターシステムの不正使用及びネットワーク拡大による種々の端末を使用した不特定多数のものからの不正アクセスを防止するため、正当な権限を保有した本人であるか、もしくは正しい端末に接続されているかなど、接続相手先の正当性を確認することが重要である」については、同じ基準の「適用にあたっての考え方」にほぼ同様の記載があり、「～すること」となっておりますので、「必要である」に変更することが適当と考えています。。

続いて【実 135】、「本人確認機能等をアクセス権限の確認と併せて本項の対策を行うことが重要である」については、この基準と【実 125】を併せて実施することが重要であるという意味ですが、必ずしもアクセス権限等の確認と併せて実施しないケースもありますので、こちらは「望ましい」に変更することが適当と考えられます。

以上、対応案２のほうを説明させていただきました。

残りの対応案３になりますが、こちらは「重要である」は変更しないという案となります。その場合は、前説等において「重要である」は必須対策ではないという旨をきちんと明記する必要があると考えております。以上３つの対応案について、後ほどご審議いただきたいと思います。

続いて、【資料２－１】の「Ⅲ．基準原案の変更・反映について」を説明いたします。

「読みやすさ対応」の基準原案になりますが、前回８月末に送付させていただいておりますが、今後、あと２回送付させていただく予定です。１回目は（１）に記載しております「基準原案（変更後)」になります。今回いただいたご意見について、10 月 23 日（月）までに反映の上、メールで送付させていただく予定です。

そして２回目は、この１回目に対していただいたご意見、また読みやすさ以外の議案も含めて、本日及び事後意見等を反映した「最終原案」となります。こちらは次回委員会の事前送付資料として 11 月 14 日にメールにて送付させていただく予定です。

なお、それぞれの原案の反映内容についての説明を下の表に記載しております。まず、１回目に反映する内容としては、ご意見の一覧で修正要とした項目のうち、①基準構成の変更や②基準内の対策・例示の変更、③対策の要求レベルの変更といった、比較的重要と思われる部分を原案に反映してお送りさせていただく予定です。

続いて次ページ④～⑧となりますが、こちらは表現の統一等の変更になりますので、事務局のほうに一任いただきまして、11 月 14 日の最終原案の送付までに反映させるということにさせていただきたいと考えております。

なお、今後この２回の原案を確認いただく際に、１点注意いただきたい点がございます。「⑥基準番号の変更」についてです。これは、10 月 23 日に送付する原案については、これまでと同じ基準番号でお送りさせていただきますが、11 月に送付する最終原案については、新しい構成で基準を並び替えますので、基準番号も新しくなるということにご注意いただく必要があります。

続きまして、「Ⅳ.「前文」内容の見直し及び一覧化について」を説明します。まず「前文」とは何かを説明させていただきます。いわゆる前説と呼んでいるものではございません。実際に見ていただきたいと思うのですが、お手元にある「安全対策基準」、茶色の冊子の 280 ページを見ていただきますでしょうか。「（Ⅲ）運用管理」の「３．オペレーション管理」の下に２行ほど説明が書いてありますが、これを「ぜんぶん」と呼んでいます。これは基準中項目の概要説明という位置付けとなります。

今回、「読みやすさ」の対応で構成を見直すことにより、前文についても内容を見直すことになりますが、現行の前文の内容を生かしつつ、より簡潔にしたいと考えております。

また、従来のページの綴じ込みの形式ではなくて、一覧表として記載するようにすることで、カテゴリーの構成や関連性がわかりやすくなるのではないかと考えています。

【資料２－４】になります。この資料は新基準構成における基準中項目が、現行の基準中項目のどこに該当するか。つまりどの前文に該当するかを比較した一覧表となります。先ほどご説明しましたとおり、現行の前文の内容を極力生かしつつ内容を見直しています。時間の関係で一つ一つ説明するところは省略させていただきますが、例えば１ページ目に、「外部の統制」とありますが、外部委託関連の前文については、今回再編しておりますので、新たに作成しますが、その他のカテゴリーの多くは、現行の前文の内容を流用するか、複数合体したうえで簡潔な表現に見直しております。

実際に変更した前文の内容については、【資料２－５】になります。左上に「安全対策基準一覧表【構成一覧】(原案)」というものになります。これまでご提示させていただきました基準構成案がありましたが、この一覧表は実際に第９版を発刊した際の様式になります。内容もこれまでの構成案には含まれていなかった設備基準の項目も含んでおります。全部で 13 ページありますが、前半の１～６ページまでが基準大項目、中項目の一覧となっており、後半の７～13 ページまでが基準小項目の一覧となります。

今回見直ししました前文は、前半の１～６ページ目までの右側に書いてある文章になります。先ほど申し上げましたが、前文については従来のページの綴じ込みという方式ではなくて、このように一覧化したいと考えております。

なお、【資料２－５】の７ページ以降ですが、委員の方からいただいたご意見を反映して、一部基準小項目の名称等を変更しております。変更箇所については網かけして赤字で記載しておりますので、別途ご確認いただければと思います。

最後にもう１点ございます。【資料２－１】に戻っていただけますでしょうか。先ほどのⅣの「尚、『設備・運用・技術基準毎の概要説明』については」というところですが、設備基準、運用基準、技術基準の概要について、前文と同じようにページ綴じ込みで説明があり、これを「中扉」と呼んでいます。この中扉についてですが、今回前説の「フレームワーク」に統制基準、実務基準、設備基準、監査基準に関する解説を記載しておりますので、綴じ込みはしないということにしたいと思っております。

本日ご説明しました内容及び原案につきましては、10 月 31 日（火）までに、事後意見をいただきたいと思っておりますので、よろしくお願いいたします。また、序盤にご説明しました語尾「重要である」については、本日、なるべく方針を固めさせていただきたいと思っておりますので、ぜひこの場でご意見をいただければと思いますのでよろしくお願いいたします。私からの説明は以上になります。

○渕崎副座長　名取さん、どうもありがとうございました。いろいろと資料があって大変ですが、ご意見をいただきたいと思います。特に、語尾「重要である」という部分について対応案１、２、３ということで事務局案としては、記載内容を踏まえて、内容に応じて「必要である」もしくは「望ましい」にするということで、対応案２を事務局案としておりますが、その案についても含めてご意見、ご質問等をいただきたいと思います。よろしくお願いします。

○白井委員　三井住友カードの白井でございます。先ほどご説明をいただきました【資料２－３】についてでございますが、やはり一律で「望ましい」とか「重要である」というところを変更しないというのは、なかなか項目が多岐にわたっているというところがございますので、この事務局の案をベースに検討していくという方針でよろしいのではないかと考えております。

○渕崎副座長　ありがとうございます。ほかにはいかがですか。

それでは、この場で思いつかなくても事後意見等で何か気づかれたこ点があれば、それからご意見があればいただきたいと思います。ご意見がなければ、先ほどいただきましたように、事務局の原案のほうで進めさせていただきたいと思います。よろしくお願いします。

それでは、次に議案３「外部委託管理関連基準の改訂について」、丸山さんのほうからご説明をお願いします。

４．議案３

○丸山総括主任研究員　事務局の丸山です。外部委託関連基準の整理方針について、【資料３－１】、【資料３－２】、【資料３－３】とした外部の統制の基準の原案、この３つをご用意ください。

まず【資料３－１】ですが、前回、前々回と外部委託の関連の基準について統合整理の方針についてご説明をしてまいりました。前回、論点１、２、３と内容をご説明いたしまして、ご意見を伺いました。「Ⅰ．論点に関する各委員からのご意見について」ということでいろいろ書いておりますが、大きく言いますと論点１と３については賛同であるとい

うことで、その方針で進めさせていただくこととします。

論点２については、後ほどご説明しますが、クラウド固有の管理策を実務基準と位置付けるのはどうかといったところ、これは外部の統制のほうがふさわしいというご意見をいただきましたので、この方向で構成を見直すこととしています。

ではその下、論点１以降をご説明していきます。まず、論点１につきましては、クラウド基準新設時に記載された「クラウドサービス利用における考慮点」等について、現時点では不要となった箇所について、ここをもう削除してよいか。例えばクラウドベンダーは情報開示に消極的であるとか、そういった当時の慎重な見方を反映した部分がございましたが、こちらを削除してよいかということについては、賛同であるということで、この方針で進めさせていただこうと思っています。

続きまして論点２ですが、こちらはクラウド固有の管理策として、FinTech の有識者検討会で論じられた部分です。クラウドサービスを利用することは、個別の業務サービスにあたるのでここは実務基準でよいのではないかというご説明をさし上げたところ、ここは外部の統制の一環として捉えるべきであるというご意見や、外部委託とクラウドが離れ離れになってしまうことで使いにくさが出るなど、利便性に問題が出るというご指摘もいただきまして、ここは外部の統制の１つとして配置するのがよいと考え、そのようにしたいと考えております。

その中で、FinTech の検討会の中では、重要な情報システムにおいてクラウドサービスを利用する場合という条件がついておりますので、これをそのまま反映させますと、全ての金融情報システムで実施すべき基準とはならないため、付加基準の位置付けになります。外部の統制は基礎基準と位置付けておりますため、この基準を付加とするか、基礎とするかということを課題として挙げております。後ほど論点としてご説明いたします。

では、資料２ページ目になります。続きまして、論点３についてです。こちらは今回、クラウド基準、外部委託の基準を統合して共通化するにあたりまして、もともとクラウドの基準【運 110、111】にあったデータ漏えい防止に関する基準については、現在の安対基準の運用基準にも重複する内容がありますので、そういった重複を排除して整理することでよいかというふうにお伺いしました。

こちらについては、統合整理の方針については賛同であるというご意見をいただきまして、さらに表の主なご意見の２つ目のところですが、今回を機に、データ漏えい防止に関する対策については、外部委託の契約の各局面、契約時、契約期間中、契約終了時、そう

いった観点で再定義してはいかがというご意見をいただきまして、この方針で今回見直し、整理をかけようと考えております。ですので論点３については賛同ですが、少しプラスして対応策を考えるというふうにして、新たな論点としてお示ししようと思っております。

以上、論点１～３についてのご意見は、このような状況でございました。

その他にもご意見を幾つかいただきまして、【資料３－２】に、今回ご説明は割愛いたしますが、こちらにご意見のほうを全て掲載させていただきました。ご意見の内容に沿って基準原案のほうを今回修正しておりまして、【資料３－３】のほうに反映しております。

今回ご意見をいただいた中で出た課題を改めて論点として切り出しましたので、【資料３－１】の２ページにお戻りください。

２ページ目の下段、「Ⅱ　修正方針について」を説明いたします。まず、先ほどの論点２の中でクラウドの固有の管理策を基礎基準とするか、付加基準とするか、どちらにするのが適当かというのが論点４になります。先ほども少し触れましたが、FinTech の報告書の中では「重要な情報システム」、今回でいうと特定システムにおいてクラウドサービスを利用する場合としての固有の管理策が示されております。

そうすると２ページ目から３ページ目にまたがるところですが、クラウドサービスを利用する場合、特定システムにおいて利用する場合ということになりますので、この基準自体は、基礎ではなく付加とするのが適当だろうと。ただし、現在の前説上は「統制・監査に関する基準」は全て基礎基準として位置付けておりますので、ここで１つ矛盾が生じます。さらにいうと実務基準では、先ほど基礎基準の考え方の中で、個別の業務・サービスについては付加基準として整理するという方針にしております。

以上を踏まえますと、クラウドサービス利用については、個別の業務・サービスを利用するということで、付加基準として位置付ける。つまり外部の統制の中の付加基準として位置付けるということで、前説の定義の部分については所要の修正を行ったうえで、外部の統制に付加基準というものを置くというふうに整理したいと考えております。

そうすると、共同センターですとか金融機関相互のシステムネットワーク、サービスの利用、こちらについても同様の整理ができると考えておりまして、３ページ目の真ん中の表にあります３つの基準については、外部の統制における付加基準として位置付けるという整理にしてはどうかというふうに論点４をまとめております。

続きまして論点５です。これはデータ漏えい防止策に関する基準、これを外部委託の契約の各局面に応じて整理すべきかという内容ですが、簡単にいいますと４ページ目に表を

つくっておりまして、契約時、契約期間中、契約終了時という中において、技術的ではない、統制面においてデータ漏えい防止策に必要な対策をそれぞれ配置するというふうに、今回しようと考えております。

契約時でいきますと、委託先のデータ管理体制の確認、契約期間中でいきますと、その防止策の遂行状況のモニタリングと機器の故障交換時におけるデータ漏えい防止策の確認、契約終了時には、委託先のデータ消去、機器等の廃棄、文書等の回収に関する対策の確認。

各基準【統 22】もしくは【統 24】に、こちらの内容を配置しまして、契約の開始から終了までデータ漏えいの防止策が網羅的に確認できる対策がとられるというように、今回整理しました。この中で、【統 24】にある遂行状況のモニタリングというのは、今の基準には書いておりませんので、ここは今回の整理にあたって遂行状況のモニタリングという対策を１つ追加しようと考えております。これをもって各局面の対策が網羅的になるというふうにしたいと考えております。

これらを基準原案のほうに反映しておりまして、こちらについて、事後意見としては 10 月 31 日までにご意見を伺いたいと考えております。ただ、内容も多岐にわたりますので、場合によっては、個別にご訪問させていただいてご意見を伺うというケースもあるかもしれません。その際はぜひともご協力いただきたいと考えております。

では論点４、論点５についてご意見を伺いたいと思いますが、一旦私のほうからの説明は以上となります。

○渕崎副座長　丸山さん、ありがとうございました。

それでは今ご説明しました内容につきまして、ご質問、ご意見等ございましたらよろしくお願いします。特に論点４、５についてご意見があれば、よろしくお願いいたします。

○伊藤委員　三菱東京ＵＦＪ銀行の伊藤と申します。論点４について、私は外部の統制に、（２）のクラウドサービスの利用というのを含めるという形にしたほうがわかりやすいのではないかと思ってます。、一方で、やはりもともとの考え方にあった統制基準に関しては、基礎基準として整理されているほうが、ガバナンスの観点で違和感がないと思っております。なので本日お話しいただいた、クラウドサービス利用とか共同センター、金融機関総合システムネットワークのサービス、これが付加基準とする案より１つ目の統制基準に関しては、全体的な考え方としてこういうふうにしてＩＴセキュリティのガバナンスを

きかせていくんだという考え方として基礎基準として提示がよいと思いました。

ちなみに少し気になったのが、クラウドサービスを利用するときの利用時の管理策を講じることというのが、安全対策基準に書かれている、特定システムだけの極めてリスクの高いシステムだけが講じる必要があって、その他の一般的銀行システムに対しては講じる必要はないという考え方もどうなのかなというところは気になりました。一般的な銀行システムであっても、例えばお客様の情報を保有するようなシステムであれば、クラウドサービス利用時の管理策というのは、講じていく必要があるのではないかと思いました。

○髙橋常務理事　付加基準と位置付けたとしても、特定システムには必ず適用されるとして、通常システムであっても、各行のそれぞれの判断で重要なものについては、適用することができるのですが、そうした形には違和感があるというお考えでしょうか。

基礎基準として位置づけてしまうと、全てのシステムに適当することになるので、リスクのすごく軽いシステムであっても、高い安全対策基準を適用してしまう惧れがあります。それを避けるために付加基準に位置づけてはどうかというのが、今回提示させていただいた考え方です。

○伊藤委員　わかりました。【統 27】に書いてあることが、高いハードルなのかどうかというところを改めて読ませていただきますけれども、基本的にお客様のデータを保有するようなシステムであれば、一定の管理策をちゃんととられているか確認する必要があるのかなと思って、申し上げた次第です。

○髙橋常務理事　ありがとうございました。

○渕崎副座長　ほかに何か、どうぞ。

○梅谷委員　アマゾンの梅谷です。ありがとうございます。今の議論に関連しまして、私の理解では、例えば【統 21】とか【統 22】、そういった基礎的なところはクラウドサービスの利用の際に検討されるという形で理解しています。大雑把には、さらにリスクが高い場合に検討する際の基準として【統 27】が位置付けられるという論点４の内容として読んでいます。そうしますと、クラウドサービスの利用にあたって何も確認しないというわ

けではなくて、最低限のところは確認されるようになると思います。また、【統 27】では、監査人に保証型監査を委託するとか、そういったお金、コスト、時間がかかるような、一般的に若干ハードルが高いがリスク上必要と思われる箇所を考慮に入るようにする、というような事務局案になっているという理解でいます。

三菱東京ＵＦＪ銀行様からのご意見はまた必要であれば追加いただければと思いますが、それに関連しまして、【統 21】のページ２についての意見です。ここで、前回アマゾンのほうから、責任分界に関して上から４行目、５行目あたりに、クラウドの性質とクラウドの責任分界点を理解した上でという事項が記載されても、違和感があるので抽象化したものにしていただいたらどうですかというのは、先ほど申し上げたような背景がありまして、私どもから意見を申し上げております。

さらに一番言いたいことをこれから申し上げますが、そうした背景も踏まえまして、【統 21】のページ２の「また、業務委託が再委託される場合」に関する箇所です。「また、業務委託が再委託される場合、外部委託先と同様」、というこれが追加されていますが、ここに特定システムが再委託される場合と通常システムではというふうに２つ入ってしまっています。そうすると、今もお話がありましたように、基礎基準と付加基準、それから通常のシステムと、特定のシステムでなかなか分離がしにくいといいますか、明確に分けて理解するのが難しいところがあると思います。【統 21】に入ってくる内容の案としては、通常システムに関しての再委託先に関する考慮事項は【統 21】に記載され、特定システムに関する考慮事項がここから抜けていていたほうが理解しやすいのではないかなという意見を持っています。

もう少し意見がありますが、とりあえず【統 21】と付加基準に関しては、今のような意見です。ありがとうございます。

○髙橋常務理事　ご意見ありがとうございます。今おっしゃったとおり、外部委託の有識者会議の報告書においても、再委託に関するリスク管理について、特定システムとそうでないものとの間で、一定のめりはりをつけるという内容でありました。今のご意見も踏まえながら、もう一回この文章の内容を検討してみたいと思います。

○渕崎副座長　ほかにいかがですか。

○梅谷委員　アマゾンの梅谷です。【資料３－３】の【続 27】、ページが 12 に関してです。クラウドサービス利用のところで１番にクラウドサービスにおける情報処理の広域性ということで、FinTech 有識者検討会のときにディスカッションがなされて、私も検討委員でしたのでこれは非常によく覚えていますが、ここで新しく赤で「データの切片化、記録保管場所が時間軸に沿って流動的になる等の特徴」とこれが入ってきています。この記述については若干違和感があります。これはクラウドサービスのストレージサービスの性質を表した表現となっており、そのサービスの性質に依存しますし、私が知る限りは、記録保管場所が時間軸に沿って流動的になるようなクラウドのストレージサービスなどというのは、存じ上げておりませんので、違和感がある表現であるというのが最初気がついたところです。

そこからそもそも情報処理の広域性については、いま指摘したような事項を言っていたかなという疑問に思っています。ここで今議論されようとして書かれたのは、データレジデンシーとよく言われるところかと思います。データがどの国の準拠法で保管されていますかというのは、よく議題になるんですが、そうしたときにデータが切片化されたり、記録場所がクラウドベンダーの都合によって移動されるのでリスクがあるという文脈は昔から議論としてあると思います。情報処理の広域性として FinTech の有識者検討会で議論がなされたのは、処理方法も含めたより広い定義だと思います。

FinTech 有識者検討会でデータといっているのは、お客様、例えば我々から見た金融機関様が取り扱う顧客データだけを指しているのではなくて、クラウドベンダーから出すデータも含まれるということだったと思います。例えばもうちょっと具体的な例を示していいますと、金融機関様のみならず日本企業様、製造企業様とかグローバルに様々なビジネスのプレゼンスがあると思います。ドイツにも支店があって、日本にも本社があってアメリカでも支店がありますといった形で、それぞれに現地で顧客をを抱えていて、顧客データを集めてきてそれを匿名化してビッグデータで東京で処理したいというような案件がよくクラウドベンダーに入ってくると思います。

そうしたときに例えばどこかで情報漏えいが起きました。そのときにどこで情報漏えいが起きて、どこに問い合わせをして、どういうデータを収集すれば、何でそれが起きたかという原因がわかるような特定が可能となります。

クラウドベンダーと一緒になって、そのような事象の防止策を考えていくという際に、情報処理の広域性があるがために、そうしたデータ、例えばリスクを検討する際のデータ

をどうやって手に入れるのかとかという点が論点になります。例としては、ドイツのクラウドサービスプロバイダーの拠点で問題が起きたときに、どうやってコンタクトして情報を入手するのかというようなリスクを検討していくのかという観点から、情報処理の広域性というのが出てきていると理解しています。

すみません。議論が散漫になってしまっていますが、ここで情報処理の広域性を出すのであれば、そういった金融機関様がグローバルに例えば何かアプリケーションを使う際のリスクの定義があって、クラウドを使う際には、実務的にはこういった契約をしてクラウドベンダーからリスクを軽減するための何らかの契約条項を引き出すとか、具体的な検討事項にそった形の定義があれば良いと思いました。

もう１点、FinTech の有識者検討会でも特定システムと通常システムの議論が少し混ざっていたと思います。そのためFinTechの有識者検討会の議論は、全て特定のシステムに適用されるというわけではなくて、通常システムも含んでいるものもあるかと思います。ただし、だからといって今の【統 21】から今現在なされている【統 27、統 28】それから【監１】までの整理をすべて見直すという意味ではなく、やはり基礎と付加をもう少し明確にするという観点が必要かと思います。基礎にもしかして特定システムの要求事項が入ってしまっているのであれば、それを分離するというような整理をする必要があるのではないかと思っています。

すみません、ちょっと長くなってとりとめもなくなりましたが、ポイントはFintechの有識者検討会の事項をもう少し正確に反映したいなという意向がありまして、文言については、私どもも今すぐここで考え出せないものがあります。後ほど何か皆様が納得されるような文言を考えて、提出させていただきたいというふうに思っています。ありがとうございます。

○丸山総括主任研究員　ありがとうございます。今のご意見、１つ目の情報処理の広域性について修文案はご意見を伺いながら見直しをしていきたいと思っております。位置付けとしては注意書きの中にありますので、できるだけわかりやすく解釈が、皆さんイメージ共有ができるようなものにしていきたいと考えております。

２つ目の通常システム、特定システム、基礎、付加のところのすみ分け、整理については、ここに限った話ではないというふうに伺いましたので、ほかの今回の外部の統制の基準全般にわたって峻別すべき部分がないかという確認をもう一度させていただきたいと思

います。ありがとうございます。

○小林企画部長　企画部の小林です。FinTech の有識者検討会の中で、クラウド固有の３つの性質をご提言いただきました。『匿名の共同性』、『情報処理の広域性』、それから『技術の先進性』です。これらについて今回の安対改訂の中でも触れていますが、この３つの固有の性質は当然、特定システムに限らず通常システムも含めたクラウド全般の固有の性質として、安対に反映すべきものです。

一方、検討会の最後に「リスク管理策に関する補足」として、今回、【統 27】で主にまとめられている内容が提言されていますが、これは先ほどのクラウド全般共通の３つの性質とは別に、重要な情報システム、すなわち特定システムでクラウドを利用する場合のリスク管理策としてご提言いただいています。いずれにしても、これらを通常、特定で適切に分けて記載するような形でまとめていければと考えています。

○渕崎副座長　ありがとうございました。ほかに何かご意見、ご質問、いかがですか。どうぞ。

○伊藤委員　たびたびすみません。三菱東京ＵＦＪ銀行の伊藤です。今の事務局さんのご説明だと、【統 27】というのは、特定システムのような極めてリスクの高いシステムがクラウドを使うときに適用される基準として書かれていますと。ということであれば、一方で、通常の銀行システムをクラウドを使う場合の基準というのは、ＦＩＳＣの安対基準では示されていないということになるんでしょうか。

○髙橋常務理事　そういうわけではなくて、特定システムには必ず適用し、それ以外のシステムについては選択的に適用します。高い基準が必要だというふうに判断されれば、それは各社が選択して適用することとなります。

○伊藤委員　ちなみにこの【統 27】が特定システムが対象になるんですよということは、どこから読み取れるということになるんでしょうか。

○髙橋常務理事　基準の定義で、特定システムは、付加基準を必ず選択すると書いていま

す。

○伊藤委員　わかりました。

○渕崎副座長　ほかに何かございますか。非常に重要な論点ですので、この場で頭の中が整理がつかないという部分もありましたら、事後的にいろいろとご意見をお寄せいただきたいと思います。そういった意見も反映しまして、次回のタイミングで、最終的な案を出していきたい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。

それでは議案４の前説の原案について、丸山さんのほうからお願いします。

５．議案４

○丸山総括主任研究員　では続きまして【資料４－１】から【資料４－４】までございます前説原案の修正内容についてご説明いたします。

まず【資料４－１】ですが、前説原案に対するご意見です。こちらは７月に考え方についてはほぼこの考え方でいきましょうということで進めておりますが、修正案につきましては、意見を常に募集しておりまして追加でご意見等をいただきました。現時点でご意見で残っているものを【資料４－２】のＡ３の資料に一覧化しております。

暫定的な対応というものもございましたので、意見として残っているのは、現在 30 件あまり残っております。そのうち反映済としたものについては、【資料４－３】、改訂案に反映しております。

【資料４－２】のご意見の中で、今回反映したものについて幾つかご紹介します。１／６ページのナンバー21 番です。金融関連サービスという言葉を今回前説で使っておりまして、金融機関等が顧客に提供する金融サービスと対比する形で、金融機関等以外の事業者が、金融サービスを補完するサービスとして、例えば決済代行等のサービスが挙げられます。そういったものを金融関連サービスとし、これを日本語で定義しようと考えておりまして、21 番の対応方針の内容を用語定義に追加しようと思っております。

金融機関等については限定列挙という形で、各金融機関の会社名、業界の名前を挙げておりまして、金融機関等各会社等をいう。ただし、電子決済と代行業者などの Fintech 企業等を除く、が各業法等に基づき顧客に提供する金融サービスを補完するため、金融機関等以外の事業者が提供するサービス、というような定義にしております。

これが正しいかというと、今は安対基準上の定義としては、これが精いっぱいかと思っておりますが、書きぶりといったところもご確認いただいて、もし事後意見がございましたらいただきたいと思っています。

続けて、ナンバー78 番です。こちらは、金融機関等以外の事業者において、安全対策基準を適用するのか適用しないのか、どのように適用するのかといったことを書いた箇所になりますが、その注釈として赤字にした部分についての修正案となります。「例えば金融関連サービスの利用（API 接続等を含む）検討時に行われる安全対策の策定に関して、『基礎基準』を踏まえ、あらかじめ金融機関等と金融機関等を以外の企業等との間で二者間に留まらず広く合意形成された共通のチェックリスト等があれば、その内容を踏まえて安全対策の自主基準を策定することも可能である」。

これは当センターで開催しておりました、ＡＰＩチェックリストもここに含まれると考えておりますが、そういったものを共通の対話のツールを使ってそれをもとに安全対策の自主基準を策定することが可能であるというふうに注釈に入れました。

金融関連サービスの実施主体、これは金融機関等以外の事業者になりますので、安全対策基準をそのまま適用するというわけではなくて、部分的な適用になることもございますが、その場合は「基礎基準」を踏まえて、さらに共通のチェックリスト等があればそれを活用していくということを、今回書き加えさせていただいております。

このような修正を原案に反映しておりますが、今回いただいた意見の中で、まだ修正案を原案のほうに反映できていないものが一部ございます。５/６ページにございまして、ナンバー112 番と 114 番になります。

まず 112 番ですが、これは経営責任のあり方について記載した部分に対するご意見です。リスクベースアプローチの考え方を共通の認識とし、例えばそれを踏まえて安全対策が打たれているというような状況で、リスクが残存する。それが顕在化して障害事故に発生した場合、その結果だけをもって責任が追及されるということは、リスクベースアプローチの考え方と整合的でないという認識が共有されるべきだと書いておりますが、ここについては共有される範囲というものについて、もう少し金融機関等の実態に合わせて、記載を見直したほうがいいのではないかというご意見をいただいておりまして、これについてはそうすべきかどうかも含めて検討したいと考えております。

114 番は経営責任のあり方について同じく語っているところです。このご意見に書かれている内容です。コンティンジェンシープラン等を用意し、客観的な立場から見れば法的

責任を果しているものと評価されるべきである、等々書いている部分についても、修文案をいただいております。例えば共有されるべき範囲というのは、もう少し広めがいいのではないかといったところですとか。言葉のそれぞれの意味が、もう少しわかりやすくしたほうがいいのではないかというご意見をいただいておりますので、ここについても事務局のほうでもう一度検討させていただいたうえで、修正案をご提示したいと考えております。

その他もございますが、ご意見につきましては原案のほうに【資料４－３】、めくっていただきますとコメント等をつけて、それぞれの箇所に反映をしております。

先ほど基礎基準の整理のところで、必須対策等の考え方について述べた部分がございますが、【資料４－３】の 15 ページにその内容を反映させていただいております。

それから新構成案になりまして、それを受けて見直すべき部分ですとか、先ほど外部の統制についての議論がございましたが、こちらの内容を受けて最終的に見直すべき部分があるかという確認をしたうえで、次回の事前送付までに最終原案を固めてご提示したいというふうに考えております。これが【資料４－１】の１番目の話となります。

続いて【資料４－１】の２番目が前説３とした、【資料４－４】の「本書の利用にあたって」になります。これまでは「安全対策基準の考え方」と「本書の利用にあたって」というふうに構成が分かれておりましたが、後段部分の「利用にあたって」について今回初めてご提示させていただきます。

【資料４－４】をめくっていただきますと、「本書の利用にあたって」というところから、まず１番目に「安全対策基準の適用における経過的措置について」と書かせていただいております。ここは外部委託の有識者検討会の中で激変緩和措置という名前で出ておりまして、今回の安対基準の改訂は非常に内容、考え方、規模の大きなものになります。ですのでこれを急に適用することによって、それそのものがリスクになってしまうという可能性もあるという議論がされております。したがいまして適用にあたっては、例えばですがシステムの更改時とか新システムの導入時にリスクベースアプローチ、今回の安対基準の考え方を適用していくということも考えられるというようなことを書いております。

そこから始まりまして、安対基準の構成、基準・解説の記述仕様というふうに続いていきます。

ページ下に 30 ページと記載したページ、めくっていただくと２枚目の裏になりますが、語尾についての解説を加えております。こちら先ほど「重要である」ものについての取り扱いをどうするかという論点がございましたが、今現時点では「重要である」は「選択可

能な対策（例示・参考)」という位置付けに今はここに入れております。

今後の議論で「重要である」そのものがなくなるかもしれませんし、「重要である」はこの位置付けだということになるかもしれませんが、その結果に応じてここは修正を加えたいと考えております。

それから続いてページが飛びますが 33 ページになります。それぞれの基準の右肩に適用区分欄というのがございまして、その適用区分欄の指すものを説明しているページになります。これは従来の安対基準にもあったものですが、今回、ここに金融機関等以外の情報システムというのを加えております。ただ、適用区分自体は、新設するものではなくてここはダイレクトチャネルに含むというふうに一旦しています.

その以降のページから用語の解説になります。これまでの８版追補までの内容を、あと監査指針の改訂において追加された内容等を反映しております。

先ほどの金融関連サービスも含めますが、さらに監査指針の第３版追補の内容を踏まえますと、もう少し用語を追加しなければいけないと思っておりますので、ここは一旦事務局側で必要な用語の追加、もしくは不要な用語の削除、これはもう意味がほとんどないと思われるものについては、適宜削除、見直しをしていきたいというふうに考えております。

こちらが前説３となりますが、こちらもご確認いただき、事後意見等をいただければと思っております。以上、ご説明となります。

○渕崎副座長　丸山さん、ありがとうございました。それではご質問、ご意見等よろしくお願いします。

よろしゅうございますか。ここで思いつかなくても後で事後意見としていただければと思います。それを反映したうえで、次回の専門委員会のほうにかけさせていただきたいと思います。

次に、事務連絡等について和田部長のほうからお願いします。

６．事務連絡

○和田監査安全部長　監査安全部の和田です。事務連絡は３点ございます。１点目ですが本日の議案１、２、３、４に対するご意見は、【資料５－１】のご意見（メール回答用）にて 10 月 31 日 17 時までに電子メールでお寄せいただければと思っております。なお、いただいた後になると思いますが、次回の委員会を効率的に行うために個別に委員の方々

に、ご意見を伺いに行くこともあるかと思います。また訪問日程等についてご相談させていただくことになると思いますが、そのときはぜひご協力のほどよろしくお願いいたします。

２点目になります。議事次第にもございますが、委員登録、内容変更届の提出のご依頼です。当センターで管理しています委員名簿において、一部委員の登録情報と実際の情報に相違があるというところが確認されました。つきましては、各委員におかれまして現在、登録いただいています情報を確認いただいて、もし間違いがあれば変更届けを出していただきたいと思っております。個人情報ですので、各委員の皆様に個別に今当センター側で認識している皆様の情報をお送りいたしますので、もし相違があれば返信いただければと思います。よろしくお願いいたします。

最後に３点目になります。次回の予定です。今回 57 回で次回は 58 回の専門委員会になりますが、今年度安全対策基準の改訂と並行して、ＩＴ人材の育成確保における策定のための手引書、これをつくっております。その議案につきまして、書面開催で第 58 回は行わせていただこうと思っていますので、後日皆様に 58 回のＩＴ人材の育成確保の手引書に関しての書面をメールにてお送りさせていただきます。

ですので、安対改訂の専門委員会、次回お集まりいただく専門委員会は第 59 回になります。日程は 11 月 21 日火曜日、15 時から 17 時、ＦＩＳＣの会議室で行わせていただきますので、よろしくお願いいたします。以上になります。

○渕崎副座長　和田部長、ありがとうございました。全体を通してまして何かご意見、ご質問等ございますでしょうか。

○蓮實委員　信用金庫協会、蓮實でございます。11 月 14 日に事前送付いただける資料というのは、今までの反映とか今回の意見を踏まえ、あと個別に相談されたものを踏まえて、一応新しい安全対策基準の新しい構成の本１冊という形のものがご送付いただけると思っていてよろしいんでしょうか。その確認です。

○丸山総括主任研究員　はい。新安対基準の１冊の構成と考えております。

７．閉会

○渕崎副座長　ほかに何かございますか。

それでは、第 57 回の安全対策専門委員会を終了いたします。ありがとうございました。

以　上