平成29年８月８日

公益財団法人　金融情報システムセンター

第55回　安全対策専門委員会　議事録

Ⅰ　開催日時：

平成29年８月８日(火)15:00～16:30

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
	鶴岡　俊哉	(代理出席)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　調査役
	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
	柳瀬　俊也	三井住友海上火災保険株式会社　理事　ＩＴ推進部長
	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　グループ長
	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
	春日井　正司	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
	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
	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
	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
専門委員会	市村　雅史	(代理出席)金融庁　検査局
オブザーバー 検討委員		システムモニタリングチーム専門検査官
	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 システムリスク管理Gr　上席調査役
	藤谷　隆史	株式会社南都銀行　東京事務所　グループ長
	嶋村　正	信組情報サービス株式会社　企画部　部長
	猿渡　耕ニ	労働金庫連合会　統合リスク管理部　次長
	中川　彰男	三井住友海上火災保険株式会社　IT 管理チーム　課長

	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
	木村　淳志	(代理出席)三井住友カード株式会社
	水崎　玲	日本銀行　金融機構局　考査企画課　企画役
	羽太　英哉	沖電気工業株式会社　金融システム事業部 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
	爲家　康弘	(代理出席)株式会社日立製作所
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
	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
	大澤　英季	企画部　次長
	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 55 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、また大変お暑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よりご説明させていただきますので、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）

２．議案１

○渕崎副座長　副座長の渕崎です。

それではまず議案１、基礎基準のご意見について、資料１－１ですが、事務局の松本総括主任研究員よりご説明をお願いいたします。

○松本総括主任研究員　事務局の松本でございます。よろしくお願いいたします。

お手元の資料、資料１－１「基礎基準に関するご意見について」、資料１－２「基準一覧」、資料１－３「改訂原案に関するご意見」、をご用意いただけますでしょうか。

まず、Ａ４縦の資料１－１、「基礎基準に関するご意見について」とＡ３縦のカラー刷りになっております「基準の一覧（追加基礎基準案)」とあわせて、ご説明させていただきます。

まず１点目です。前回の専門委員会後に皆様からご意見をいただきまして、「基礎基準」の追加に関するご意見が 44 件ございました。一方で、前回事務局からご提案させていただきました基礎基準（案）に対して、取り下げたほうが望ましいのではないかというご意見は一件もございませんでした。したがいまして、今回 44 件の基準を加えた基礎基準（案）をＡ３縦の資料にお示しをさせていただいています。

なお、これまでは、資料１－３のフォーマットに沿った形で各委員からのご意見と対応方針お示しする形で委員会でご説明してまいりましたが、今回、基準の一個一個のご意見をご紹介するのではなく、一覧でお示しするほうがご確認いただきやすいと事務局で判断いたしましたので、字が小さくて恐縮ではございますが、前回ご提示させていただきました基準一覧にご意見いただきました委員の社名欄を追記し、対象の基準欄に「●」を記しております。

こちらの表全体の見方でございますが、前回の専門委員会で、ブルーの網かけにつきましては「統制・監査基準」、オレンジの網かけにつきましては「顧客データ漏えい防止に関する基準」、黄色に関しましては「コンティンジェンシープラン策定に関する基準」として事務局から提示させていただきました。したがいまして、緑色の網かけになっている部分につきましては、今回ご意見をいただいた基準として追加しているものでございます。

Ａ４縦の資料に戻っていただきまして、まず、ご意見の反映方針でございますが、前回の基礎基準のご説明の中で、前説の考え方に基づいて基礎基準の選定に当たっての考え方

を、「統制・監査に関する基準」、「顧客データの漏えい防止に関する基準」、「コンティンジェンシープラン策定に関する基準」、この３つの要素で基礎基準を選定する方針としておりましたが、ご意見の内容を確認したところ、やはりこの３つの要素でおさまらないものが幾つかございました。そちらの考え方をその下の○の中で整理させていただいております。

まず追加候補となる基準は、①システムの不正使用防止に関する基準と思われるものと、②システムの運行管理に最低限必要な基準に分類することができると判断いたしました。したがいまして、①は、不正防止に関する内容とデータ漏えい防止に関する考え方と顧客データの漏えい防止は共通する面が多いと判断し、今回、顧客データ漏えい防止に関する基準につきましては「及び」以降の文章を追加し、「顧客データの漏えい防止及びシステムの不正使用防止に関する基準」に変更しております。

②のシステムの運行管理に最低限必要な基準に関しましては、４つ目の要素として今回新たに設定しております。この考え方に基づいて前回の事務局案から今回ご提示している基準の件数をご参考までに、記載しております。

基準全体の数は、外部の統制基準を除き、162 基準で、前回事務局案として提示した基礎基準は 71 件でした。今回は 44 件追加になっておりますので 115 件が基礎基準となっております。したがいまして、付加基準としてリスクベースで判断する基準につきましては 47 件という内訳になっています。

本日以降の議論の進め方としましては、まず、前回からお示ししております基準については、まだ時間が足りてない部分もおありかと思いますが、本日ご意見等をいただければご議論していきたいと思っております。

なお、本日お示しした基準については、お持ち帰りいただいて具体的な内容を確認しないとなかなか議論ができないかと思います。よって、今後も引き続きご意見があるものだと考えますので、基礎基準の議論においては、継続的に検討してまいります。

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。きょうは考え方をお示しするという、たたき台、スタート台ということでありまして、この後、きょうのご意見、それからこの後いただく事後意見もあわせて最終案に持っていくわけですけれども、ここまでのところでご意見、ご質問等がございましたらよろしくお願いします。

○伊藤委員　三菱東京ＵＦＪ銀行の伊藤と申します。この中で【実 123】と【実 124】のところに関して少し確認させていただきたいと思っております。

【実 123】に関しては「伝送データの改ざん検知策を講ずること」とここでは小項目として書いてあるのですけれども、中身に関しては、重要なデータの伝送においては改ざん検知のための対策を講じておくことが望ましいという、望ましいという表現になっております。また、その伝送データは重要だという記載があります。それから大基準の中身を読むと、改ざん検知のための対策を講じておくことが望ましい、特にオープンなネットワークを介してデータを伝送する場合はソート中におけるデータ改ざんを検知するための対策が講じられることが必要であるという記載になっております。いわゆる行内ネットワークとか社内ネットワーク全般に対して改ざん検知策を講じるべきというよりも、どちらかというとリスクの高いインターネットを介した通信に関して改ざん検知のための機能をつくるべしという、割と限定的なことを推奨しているような記載になっておりますので、基礎基準として入れるのであれば、このあたりは明確にしておかないと、いわゆる社内ネットワークに関しても全て検知策を講じなければいけないとなるとかなり大きな話になってしまうのかなということが気になりました。

それからもう一点、【実 124】ですが、私の安全対策基準の理解も正確ではないのかもしれませんが、このファイル突合機能を設けることというのは、我々の解釈は、出てきたアウトプットを別の観点で検証して、マッチングして、正しいかというのをやるようなリコンサイル機能のことだというふうに理解してはいるのです。そうすると、全てのデータに関してリコンサイル機能もつくるというとかなり高コストな話になってしまいますので、やはりこれも重要なデータやリスクの高いデータに関してリコンサイル機能をつくるようなことを行内的にはやっています。もしここも基礎基準にするのであれば安対基準の記載として、こちらはどちらかというと全てのデータに関してこういったことを求めているような安対基準の中身になっているんですけれども、もう少し重要なデータはやるべしとか、やることが望ましいとか、ちょっと表現を見直さないとインパクトが大きいのかと思いました。今回リスクベースという考え方で、基礎基準というものがマストですというようなトーンで表に出していくとすると、ちょっとそのあたりの、安対基準の記載の中身を変えていったほうがいいのかなというふうに思いました。以上です。

○松本総括主任研究員　ありがとうございます。今をおっしゃっていただいたようなシステムの特性を考慮すると、文章の補記や修正等の対応も必要と考えています。また、そもそもすべての金融情報システムに最低限必要な対策ではない基準を基礎基準とするべきなのかについても議論しないといけないと考えております。

もう一つは望ましいという、ベストプラクティスで表現されている文書につきましては、今後も位置づけとしてはベストプラクティスの考え方として残そうと考えております。この後にもご説明させていただきますが、今回基準の内容の中の解説部分につきましては、文章の読みやすさを整理いたします。解説部分には、語尾が、「望ましい」や「すること」、「必要である」といったさまざまな表現がございますので、その示すところの考え方を整理し、読み取る方が誤解しないような形で整理していきたいと考えています。また、今ご意見をいただいたような内容につきましては、事務局としましても、今回の委員会後に委員の皆様あてにご訪問させていただきまして、ご理解を深めていきたいと考えておりますのでよろしくお願いいたします。

○伊藤委員　ありがとうございました。よろしくお願いします。

○渕崎副座長　ほかに。どうぞ。

○瀧委員　FinTech 協会の瀧でございます。

この１－２の資料で個別のご指摘に従って行数がどんどんふえているということだと思うのですけれども、そもそも前回ご提示されたときに、以前までの流れの中では外したはずの心といいますか趣旨がおありだと思うんですけれども、ある種、一つの委員からこういう形で追加があるたびにまずはその行をふやして、そこから外すようなことが今後の検討の形になるのか、どういう形で今後は数の調整をしていくのか、ちょっと議論の流れが追えていないことがありまして、お知らせいただければと思います。

○松本総括主任研究員　ありがとうございます。今回の安対改訂におきましては、有識者検討会の報告書がベースとなり、リスクベースアプローチの考え方が前提として整理されることになります。その前提に基づくと、今回の基礎基準として選択された結果がある意味リスクベースアプローチで判断するところが対象が減ってきているというご意見かと思

います。まさにそういったところの前提となる考え方についてはまだ、事務局としての説明が尽くされていない部分もございまして、先ほどの繰り返しになりますが、今後の委員訪問の中でしっかりとご説明をさせていただたいと考えております。

一方で、現時点では、基礎基準が増えているという現状がございますが、今後の議論としましては、前提となる考え方の合意形成を図ったうえで、基礎基準として残すべきか、外すべきかという検討を行い最終的に決着させていきたいと考えております。

○瀧委員　ありがとうございます。私はマネーフォワードの人間でもあるのですが、マネーフォワードとして例えば銀行のＡＰＩと接続していくときに、初期的なデューディリジェンスの度合いが結構異なっておりまして、同じ大手行の中でもある一行とある一行で対応工数が８倍ぐらい違うケースもございます。やはり一番ある意味バランス感のとれたところをもとに、リスクベースの基準は検討されるべきかと思っておりますので、そのような形で議論形成に貢献させていただければと思います。以上でございます。

○渕崎副座長　ほか、どうぞ。

○山田委員　南都銀行の山田でございます。

追加基礎基準案ですか、個々にさらっとですが見てみたのですが、やはりリスクベースにこのままではなじまないとか、検討の余地がないとか、そういう切り分けで言えば確かにそのとおりなんですけれども、先月、先々月に議論したリスクベースというふうな一つの大きな切り口でとらえるのであれば、でき上がりの数がこうであったのかというと、最終的な到達点というのはこれを利用して、自社のシステムがどうであるのかというあたりをクレンジングしていくような作業がつながる。そうすると、そのものにとっては、何だ、順番が変わっただけではないかとか、そういった印象をちょっと受けかねないのかというのが正直な思いです。さすればどうしたらいいのかというと、ＢＴＭＵ様がおっしゃったように、中身のほうもちょっと細かく砕いて足すなりというところで分けていくというのが現実的かと思います。ただそうすると、スケジュール的にどうなのかなというあたりが一番気がかりなところです。そのあたりはいかがお考えでしょうか。

○松本総括主任研究員　ありがとうございます。やはり具体的な中身を分析しつつ、一件

一件議論していくというのは確かにスケジュール的にかなり厳しいかと思っております。今、前説で固めさせていただいた考え方、今回要素を１つ加えておりますけれども、まずそこの考え方に基づき議論を進めていくのが大前提だと思っておりますので、これから委員の方にご説明をさせていただいた上で、専門委員会でご納得、ご理解いただける考え方を事務局で整理いたしまして、スケジュールどおり改訂作業を進めて行きたいと考えております。

○山田委員　道順も大切だと思いますのでよろしくお願いします。

○渕崎副座長　今、いろいろとご意見をいただいている段階なので、いろいろなところで基準の漏れがないかという観点で出てきていると思うんですけれども、ベースとしてはリスクベースアプローチということなので、簡素化という観点でいろいろとこれから見直していくということになっていくと思います。

ほかにご意見は。どうぞ。

○持田委員　三井住友銀行の持田です。

重複する部分があるんですけど一応言っておきたいと思いまして。リスクベースアプローチというところがポイントだと思っています。お話がありましたとおり、ちょっと数がふえ過ぎてしまったなというのが印象としてありますので、中身を詰めていく段階で基礎基準のところの数をもう少し減らしていけたらと思っています。

それと、あと、ＢＴＭＵさんからもありましたけれども、その中に入っていったときにシステム特性によって同じ項目でも中身が変わってきます。前説の方でもありましたけれども、今までは基幹系システムを中心に基準が作られているところがあって、いろいろな懸案事項が出てきているという点を踏まえて、中身の見直しにおいては、しっかりと基幹系であるとか、情報系であるとか、情報系と基幹系ではリスク管理の度合いが異なるというところを詰めていく議論をきちんとやっていただけたらと思っています。

もう一点、ご説明はなかったのですが、今回、基準をきちんと見直すという観点では、今、この並びがもともとの技術基準、運用基準の並びでずっと並んでいるんですけれども、本来は、ＩＤ管理、ネットワーク管理等項目ごとにそれぞれ運用基準、技術基準、両方の対策があると思いますので、項目ごとにきちんと埋め込むような見直し方も検討していた

だければと思います。よろしくお願いします。

○松本総括主任研究員　ありがとうございます。まず項目の並びにつきましては、この後ご説明させていただく読みやすさ、構成の見直しで、具体的なご説明をさせていただきたいと思っております。現時点の案で示した基準のカテゴリーや並びは、原則的には、現在の安対基準における運用基準、技術基準の並びになっておりますが、今回は、基準のカテゴリー、並びも見直す予定ですので、よろしくお願いします。

○渕崎副座長　ほかに何かございますか。どうぞ。

○梅谷委員　アマゾンの梅谷と申します。よろしくお願いします。私どもから意見を出したことについてお話がありましたので、少しお話をさせていただきます。

検知策のところで●の箇所のアイデアを出させていただきましたが、意図はデータの漏えい＋データの改ざんについて、FinTech 企業の方等がインターネット越しにデータをやりとりする場合に、データの改ざん、その検知等関連する箇所のセキュリティはどのように管理していますか？というように、大手の金融機関様から指摘されて、どのように回答すれば良いか私どもに相談が入ってきたりします。そのため、一アイデアとして、データの漏えい＋データの改ざん・検知についての視点があったほうがいいのではないか？ということで案を出させていただきました。

三井住友様、東京三菱様からも話がありましたように、あるいは FinTech 協会の方からもお話がありましたように、業務の特性に応じて選ぶところが変わってきますし、それから扱うデータとかシステムの規模ですとか、それから他の金融機関さんへの影響ということも考えると、なかなか一概に決めるのは難しいのかと思います。

追加策の意見を出した本人が言うのもなんですが、基準が多すぎるのはどうかというのは正直意見としてあります。特に、これは各金融機関の方によって、それぞれの視点で話をしているということが背景にあります。特に我々のようなベンダーの立場ですと、FinTech 協会様に入っていらっしゃるのが FinTech の企業様と大手の金融機関様の間に挟まれるようなケースが多いのですが、そうすると両者の視点がよく見えまして、お互いに見ているところが違うという印象を持っています。データ漏えいしたときにホストに影響があるかもしれないという視点と、インターネット上におけるデータの漏洩だけを見てい

る視点というように業務特性によって異なりますので、一つのアイデアとしては業務の特性に例を何例かつくってみて整理する、あるいはデータの特性に応じてリスク度合いをちょっと整理してみるという形で、何軸か案として整理してみるのはどうかと思っている次第です。ありがとうございます。

○松本総括主任研究員　ご意見ありがとうございます。まさにシステムや業務の特性に応じて適用するべき基準をどうするかによって、基礎基準の位置付け、考え方が整理できるものと考えます。事務局からの論点の整理としましては、そこのリスクや業務の特性によって対策をするべきかしなくてもいいのか、要はリスクベースで判断できるのかといった部分を整理しまして、委員訪問でご意見をいただきながら方向性を固めていけたらと思っていますので、ご協力のほうをよろしくお願いいたします。

○渕崎副座長　はい、どうぞ。

○常岡委員　農林中央金庫の常岡と申します。よろしくお願いします。我がほうもリソースも能力もちょっと足りないので、まだ意見としてきれいな形になって出してはいないですけれども、前説も含めてもう少し見させていただきたいと思っています。

リスクベースアプローチという中で、前回、基準の一覧が出されたときに、まずびっくりしまして、多いなというのが第一印象でして、それについてさらに追加になっているのでどうしたものかと考えているところであります。そういった意味で、今、システムの特性に応じてというお話がありましたけれども、これをどんな形で付加基準みたいな感じにしていくのかとか、もう少し議論させていただきたいと思っているのが１点です。

先ほど「望ましい」という表現とか、「べき」とか、これは共存させてという話もあったんですが、基礎基準の中にはやはり「望ましい」というのはないのではないかというのが第一印象でした。どういう形でパズルをはめ込むのかすごく難しいと思ってはいるんですけれども、一緒に考えさせていただきたいと思っています。よろしくお願いします。

○松本総括主任研究員　ありがとうございます。基礎基準として今ピックアップされている中に、「望ましい」と、ベストプラクティスの基準がまざっているという課題認識は我々も持っていまして、そういったところを委員の方からご意見を伺いながら、ベストプ

ラクティスは基礎基準から除外する、しないとった議論の必要性等についてもあわせて検討していきたいと考えております。

○藤田委員　富士通の藤田でございます。

皆さんの意見と私の意見は大分重なる部分もございますけれども、このように考えてはいかがかということを今後ご提案させていただきたいと思いますのでよろしくお願いします。

具体的に言うと、ＲＢＡに沿った検討を行うときに、その考察の単位を既存の、旧来の基準を単位に多い、少ないで考えていいのかどうかということを申し上げます。つまり一基準の中であってもベストプラクティスと必須であるものというふうに濃淡がつくはずなのです。ですから単純に基準数が多い、少ないではなく、その中身の濃淡でＲＢＡを検討するというのが本質ではないかと思います。具体的な是々非々で今後ご提案させていただきたいと思いますのでどうぞよろしくお願いします。

○松本総括主任研究員　ありがとうございます。現在の安対基準で基準として指していますのが基準中項目、基準の一番上段に書かれている文書です。おっしゃるとおり、解説部分の内容には、ベストプラクティスであったり、例示であったり、何々「すること」「必要である」といった、対策の強度を示す表現が混在しておりますので、そちらの内容の分類を整理することは一つのテーマとして考えております。その上で、またその基準が基礎なのか付加なのか、という議論を行うことが必要であると考えております。

○白井委員　三井住友カードの白井でございます。幾つか指摘をさせていただきましたので、基本的な考え方ということで補足をさせていただければと思います。

全体として今回はリスクベースということになりますので、基本的には事務局のほうでつくっていただいたものでおおむね問題はないかと思っています。

ただ、そういいましても、ここもとの状況を踏まえると、例えば【実 98】の必要となるセキュリティ機能を取り込むことといったものは、サイバー攻撃の脅威等が高まっている現状ではさすがにこれは必要ではないのかとか、また【実 59】のハードウェア・ソフトウェアの管理を行うこと、こういった項目はリスクベースといったところを加味しても必要ではないかなというところで、絞って指摘のほうをさせていただいたという次第です。

ただ、先ほどからもありましたとおり、システムの特性というところもありますので、そういった部分も踏まえて、皆様のほうでしっかり議論をしていただければと思います。

○松本総括主任研究員　ご説明、ありがとうございました。

○渕崎副座長　ほかはよろしいですか。とりあえず、ここまでご意見をお伺いしたということで、次のほうの議題に移らせていただきたいと思います。

それでは議案２、外部委託管理関連基準の統合・整理について、事務局の丸山さんからお願いします。

３．議案２

○丸山総括主任研究員　事務局の丸山です。よろしくお願いします。

お手元の資料２－１をご用意ください。とじ込みになっておりますが、量も少し多くなりますのでポイントを絞ってご説明したいと思います。

外部委託管理関連基準の統合・整理についてということで、まず一番に背景として、クラウド有識者検討会を経まして、第８版追補改訂の際に外部委託の附則としてクラウド基準というものを新設しております。その際に、外部委託の基準とクラウドの基準が並存するという状態が生まれておりまして、その後の FinTech 有識者検討会で、クラウド固有の性質ですとか、重要システムにおけるクラウドの固有の安全管理策といったものが整理されました。クラウド固有の基準というものが定義されたということで、外部委託に関する共通的な事項とクラウドの固有の事項というのが分離できる状態になったと考えておりまして、今回、外部委託基準の共通部分とクラウド固有部分を整理するということを考えております。

１ページ目の真ん中に、１番から４番までありますが、今、申し上げた内容は１番の外部委託基準とクラウド基準の統合・整備ということになります。その他、報告書の提言内容等を踏まえまして、個別のテーマですが２、３、４というふうに今回整理のテーマとして挙げております。順を追って説明してまいります。

まず１番目の外部委託基準とクラウド基準の統合・整理につきましては、論点１ということで下段から書かせていただいております。こちらについては、背景は今申し上げたと

おりですが、具体的な整理のプロセスとしましては、外部委託基準、これは【運 87】から始まる一連の基準ですが、これと、クラウドの基準【運 108】から始まる基準ですが、こちらの中から外部委託共通の基準、共通の項目を抜き出しましてマージしていくという一つの流れと、一方で、クラウド固有の管理策に当たる部分を抜き出して、これをクラウド固有基準として新設するというふうに整理したいと考えております。

イメージとしては次の２ページの上に図を入れさせていただきました。左側に現在の外部委託基準、【運 87】から始まるもの、それからクラウド基準、これが【運 108】から始まるものです。この中から外部委託に共通する項目を、利用検討時、契約提携時から終了時までの各フェーズに整理しまして、ここにそれぞれの基準に入っている共通項目を統合して新設の基準にしていくという流れです。

一方で、クラウドの固有の部分については、下側、青い矢印がぐるっと回って右側にクラウド固有基準となっておりますが、固有部分についてはクラウド固有基準として整理して新設します。

見やすさ、修正、語尾の統一というものが右側にあるのですが、外部委託の共通化をした結果、外部委託とクラウドサービス利用で同じ基準を使っていきますので、それに合わせた語句の統一ですとか、見やすさの修正を加えていきます。

下の表に、利用検討時から終了時までのフェーズごとに、現在の外部委託基準とクラウド基準がどのような位置づけで配置されているかというものをおおよそ書いております。利用検討時でいいますと、【運 87】【運 87-1】、それからクラウド基準の【運 108】、こちらが利用検討時の内容、安全対策を書いているものですので、この内容を統合しまして、【統 21】という基準にするということを行います。

その結果、外部委託の共通の基準は【統 21】～【統 26】に整理しまして、クラウド固有の基準につきましてはここから抜き出しまして、表の下から続いて次の３ページの上の表になりますが、【運 108】～【運 111】の中からクラウド固有の部分を抜き出したものと、FinTech 有識者検討会で定義された特定システムにおけるクラウド固有の安全管理策を統合したものを【統 27】としてクラウド固有基準というふうに新設したいと考えております。

その他、外部委託に関連する基準としましては、例えば監査に関する内容は、その下の表になるのですが、新しく【運 91】を【監１】という名前にしますが、この【監１】という監査基準の中に外部委託に関連する内容を追加していく。もう一つは、コンティンジ

ェンシープランにかかる内容につきましては、【運 65】、これは【実 58】になるのですが、こちらに外部委託に関する内容を追加して整理するということで、外部委託に関連する基準を【統 21】～【統 27】までと、【監１】それから【実 58】、こちらのほうに統合整理させるということを考えています。

ここまでが論点１となります。

説明のほうを続けさせていただきます。続きまして論点２ですが、こちらは個別のテーマになってきますが、現在、安全対策基準【運 90-1】という基準がございます。こちらは金融機関相互のシステムネットワークに関する基準ということで、内容としては全銀システムや統合ＡＴＭに接続する場合に必要な安全対策が書かれています。外部委託の有識者検討会の中で、こちらは外部委託とは別の形で整理するというふうにしていますが、今回、この基準については外部の統制の基準の一つとして、独立したカテゴリーに配置させていただこうと考えております。これは内容自体は変えるものではございませんで、この基準の位置づけをどこにしますかということで、外部の統制の一つとして外部委託管理とは別の形でカテゴリーを新設しておくというふうに整理したいと考えています。

それから論点３ですが、共同センターに関する安全対策基準の新設です。こちらも外部委託の有識者検討会の中で共同センターにおけるリスクについて議論されております。特に有事の際の対応の初動の時間性の問題というのが報告書の中で記載されておりまして、これを受けまして、次の４ページ目の上に、共同センターにおける有事の際の安全管理策を講ずるという内容で基準を新設しようと考えています。

ただ具体的な対策については、共同センターの形態は多種多様となりますので、一律の基準としてではなく、対策を例示として記載していくことで有効に活用していただけるように整理したいと考えております。

それから論点４、FinTech に関する基準です。前説の中でも金融関連サービスを提供する場合の安全管理策に少し触れていますが、今回、FinTech に関して新たな基準を新設するということは考えておりません。FinTech に関しては、基準の適用の仕方が一部これまでと異なる、部分的に統制を働かせるとか、そういった適用の仕方が変わるものもございますが、基準そのものを新設するということにはならないと考えておりますので、論点４につきましては、要否と書いておりますが、今回 FinTech に関する新設の基準はつくらないというふうに考えております。

以上を踏まえまして、４ページの中段にございます表のように外部委託関連の基準を整

理するということです。

本日ご説明しているのはこのように進めていきたいと考えていますというご説明になりまして、実際の基準そのものを見ないとなかなか議論も深まらないと考えております。今後の進め方としては、基準の原案を各委員の方にご提示してご意見を伺いたいと考えておりますが、その際に可能な限り訪問させていただいて、ご説明のほうをさせていただきたいと考えております。

ちなみに５ページ目以降はサンプルのほうをつけておりまして、これが利用検討時における基準の統合はこのようなイメージになりますというものです。５ページが【運 87】、６ページ目に【運 87-1】、もう一つが７ページ目から始まる【運 108】、これがインプットとなります。【運 108】の中にクラウド固有のものがあればそこを省いた上で３つの基準をマージして、10 ページになります【統 21】の新基準原案という形で整理しようと考えています。

結果としてというか、もともと【運 108】がつくられた経緯からしますと、【運 87】と【運 87-1】の内容にプラス、クラウドで考慮すべき内容というものが加えられていますので、新しい【統 21】については【運 108】とほぼ同じような形に見えると思います。ここからクラウド固有の部分が除かれて【統 21】という形になっていますので、原案をお持ちする際も、どのような整理の仕方をしましたかという流れもご説明の上で、新基準について内容の漏れですとか、記載内容、レベル感とか、そういったところを確認いただきたいというふうに考えています。

私からの説明は以上となります。

○渕崎副座長　きょうは考え方をお示ししたのと、それから現状の基準が、例えば３つの基準を１つに整理したらこんなふうになりますという例示でイメージをわかっていただこうという話でございます。これから作業していく中でいろいろと出てくるかもわかりませんが、ここまでのところでご意見なりご質問があればよろしくお願いします。

どうぞ。

○鎌田委員　ＮＴＴデータの鎌田です。１点確認させてください。

結局のところ、見直し後の新基準としての改訂原案というんですか、いつ出てくるかというと、９月下旬ごろに出てくるという理解でよろしいですか。その日程感がよくわから

なかったのです。

○丸山総括主任研究員　原案につきましては、今はたたき台ではございますが、この会が終わった後、訪問のアポどりをさせていただきまして、原案をお持ちして、８月中旬頃からお見せするよう進めてまいりたいと思っております。その後、意見を集約し、９月の委員会にて改めて原案をこの場にご提示したいと考えております。

○鎌田委員　８月中には事前に下書きが出るということでよろしいですか。

○丸山総括主任研究員　そのとおりで結構です。

○渕崎副座長　ほかに。

それでは、何かご意見やお気づきの点があれば、この後で結構ですので、事務局のほうにいただきたいと思います。議題１につきましても、先ほどからいろいろとご意見をいただきまして、皆様のおっしゃるとおりだと思うのですが、この後気づいた点があれば、議題１も含めてご意見をいただいて、それを事務局のほうで統合整理してまたたたき台をつくり直すということになっていきますので、よろしくお願いします。

それでは議案３の安全対策基準「読みやすさ」の対応について、名取さんのほうから説明をお願いします。

４．議案３

○名取総括主任研究員　事務局の名取です。お手元の資料３－１から３－６までありますので、そちらをご用意ください。

今回初めての議案となります「読みやすさ」の対応について、まず資料の３－１でご説明いたします。

まず、対応の背景になります。安全対策基準ですが、これまで改訂を重ねる中で必ずしも記述の様式・表現の統一がなされておらず、また、基準項目の構成（カテゴリー）についても、自機関・自社のホスト・勘定系システムにおける安全対策を実施することを前提とした構成となっておりますので、特に新しい利用者にとっては戸惑う点が多く、「読み

やすさ」という点では懸念があるということが一つあります。

また、今後、リスクベースアプローチに基づいて本書の記述の内容を正しく理解する必要があるかと思いますが、その上でも「読みやすさ」は重要になってくると考えております。

これらの点を踏まえて、今回、この改訂の中で「読みやすさ」の向上を目的とした変更、修正を実施したいと考えております。ただし、前提としましては、個々の安全対策基準の適用の目的、適用範囲、適用の強度（要求レベル）が変わらないように十分に配慮するということを前提としたいと考えております。

その上で、読みやすさ対応の内容になりますが、まず１つ目、基準の再構成・カテゴリー変更や並びかえ等の変更を行います。２つ目は、読みやすさの向上ということで、具体的には基準の本文（主に解説部分）における対策や例示の明確化、記述方法の統一といった変更、修正を行います。

資料３－１の「Ⅲ．今後の進め方」については後ほど説明しますので、まずは、対応の詳細について説明いたします。

資料３－２、３ページをご覧ください。１つ目の「安全対策基準の再構成について」になります。

まず、基本的な考え方は、２段落目のところですが、今回の改訂においては、特に統制面の安全対策を明示するため、基準の構成を「統制基準」「実務基準」「設備基準」「監査基準」という形で分類する予定ですが、安全対策の当事者にとって参照する機会が多い「統制基準」「実務基準」について、今回利便性確保の観点から並び順等を再構成することとしたいと考えております。

ここからは実際の再構成の内容について説明しますが、この資料の２つ下にＡ３の資料がございます。資料３－５、新基準構成案ですが、こちらもあわせてご覧ください。

こちらのＡ３の資料の見方を簡単にご説明します。資料の左側ですが、こちらは今回見直したカテゴリー（構成）を記載しています。右側の前回構成案と書いている部分ですが、こちらはこれまでご提示していたカテゴリーとなっております。また、上のほうに統制基準、その後実務基準と並んでおり、統制基準については大きな変更がございませんが、実務基準については並び順等を大幅に変更した案となっています。また、文字で赤字になっている部分ですが、文言を変更している箇所になります。

また、Ａ４資料の３ページに戻って説明いたします。

まず、２番目の統制基準の再構成ですが、主に並び順を変更しています。実施者の階層を考慮し、主に経営層が承認を行う基準を最上位とし、あとは管理者が実施する基準、担当者が実施する基準という形で順番を並び替えています。

また、安全対策の事前対策、事後対策といった時間的な順序性がある項目については、その順序性を考慮して並び順を見直しました。

続いて３番目、実務基準の再構成についてですが、まず、現在の安全対策の中でも重要な要素となる「情報セキュリティ」に関する基準は今バラバラになっておりますので、こちらを一つのカテゴリーとしてまとめました。

また、２つ目としまして、運用業務については外部委託化が進んでいるといったところも考慮して、安全対策の実施者が明確になるように「システム運用」に関する基準を再構成しています。４ページに運用に関する基準の構成の内訳を記載しておりますが、例えば「システム運用共通」、こちらは運用部門である主に委託先及び利用部門である金融機関の双方が実施する基準ということでまとめております。その次の「運行管理」については、主にシステム運用部門が実施する基準ということで、誰が実施するかという利用者の観点から分類をし直しています。

続いて３番目としまして、「システムの信頼性向上策」、いわゆる非機能要件についてまとめて、カテゴリーとして記載しております。

続いて４つ目としまして、カード類、コンビニのＡＴＭといったものは「個別の業務・サービス」というカテゴリーとして分類をしており、こういったサービスを実際に提供していないシステムについては、この分類項目自体を読まなくてもよいということにしています。

続いて、資料の４ページ目の下の、「Ⅳ．基準の再構成において判明した課題の対応（基準変更）について」の部分を説明いたします。

今回の再構成を行う中で、統制基準の記載内容において見直したほうがよいと思われる点が判明しております。例えば【統１】「セキュリティ管理方法を具体的に定めた文書を整備すること。」ですが、「セキュリティポリシー」、「セキュリティスタンダード」に関する記載はあるものの、その上位となる「システムリスク管理方針」に関する記述がないといった課題があります。こちらは「金融機関における外部委託に関する有識者検討会」の報告書には記載されていますので、そういったところとの整合性をとっていく必要があると考えております。

具体的にどういう対応をしていくかというところで、例えば【統１】に関しては、システムリスク管理方針についての記述を追記するということで、「システムリスク管理方針をつくる」というような基準化をするのではなくて、「セキュリティポリシー及びセキュリティスタンダードの策定に当たっては、システムリスク管理方針等の上位規程と整合をとること。」といったような関連性を明確にするといった追記をしたいと考えております。

また【統１】以外に【統２】【統３】についてですが、セキュリティの文書の整備に関する基準で、一部重複している部分や、ほかの基準と整合性をとっていくような修正が必要と思われる点がありますので、こちらについてもあわせて対応したいと考えております。本日は改訂原案がまだできておりませんので、次回の委員会までにご提示をさせていただくこととし、その上で検討いただきたいと思っております。

続きまして資料３－３です。「読みやすさ」対応の２つ目になりますが、「読みやすさ」向上に関する対応について説明いたします。

こちらも利用者目線で「読みやすさ」の向上を目的に、まずは５つの方針で変更、修正を進めたいと考えております。対応方針のほうをご覧ください。

方針１としまして、実施すべき「安全対策」（～すること、～する必要がある）と「安全対策の例示」を明確に区分するというのを挙げております。

記述例を見ていただきたいのですが、「以下のようなことを考慮して手順を明確にすることが必要である。」こういった記述がありますが、これを対応例として、「手順を明確にすることが必要である。明確にする事項としては以下の例がある。」ということで、対策と例示を分離することを行います。

続いて方針２ですが、実施すべき「安全対策」を示す語尾を統一していきます。こちらは、先ほどベストプラクティスといった話もありましたが、現状としましては、解説部分の語尾を大きく３つに分類しております。１つ目は実施すべき「安全対策」で、こちらは「～が必要である。」、続いてベストプラクティスについては「～が望ましい。」、あとは例示や参考、それ以外のところは「～が考えられる。」「～がある。」、こういった３種類に整理してあるのですが、今回これに該当しない語尾の表現を統一したいというところです。記述例にありますとおり、「紛失、盗難、破損に関し、利用者が被る可能性のある損失及び責任を利用者に対して明示すること」となっているのですが、こちらについて、「すること」というのは実施すべき内容であるというところになりますので「することが必要である。」という形で語尾を統一していく。こういった対応をしたいと考えておりま

す。

８ページ目、方針３になります。例示内の語尾を統一するというところですが、こちらは幾つか該当する基準があります。「以下のような例がある」となっていて、その下の例示の中に「～する必要がある」という、例示なのに実施すべきという語尾を見直していくということで、「する必要がある」というのを「～する」というように変えていきます。

続いて方針４です。理解するのが困難な文章または誤解を与えやすい表現を修正するというところになります。記述例ですが、「また、円滑な運用に移行するため、」ということで、これは「本番移行」の基準になるのですが、「円滑な運用に移行」ということはよくわからないということで、対応例のとおり、「また、円滑に本番運用に移行するため」といった、文字を補記することで誤解がないような表現に修正していきたいと考えております。

続いて方針５です。内容が古くなっている箇所を修正していきます。記述例に「ＩＣカード化等の高セキュリティ技術の導入がある。」ということがあるのですが、今の技術水準からすると、「高セキュリティ技術」という表現はどうかというところで、こういったものを見直していくということになります。

古くなっている箇所の修正に当たっては、簡易かつ影響が小さいと想定される修正のみを対象とし、一定の技術的な調査が必要だったり、いろいろな関係者の合意形成に時間を要するといったところについては今回修正は行わず、次回の改訂における検討課題としたいと考えております。

以上のような方針で基準の本文の変更、修正を進めていくとともに、今回は記述ルールを明確にした上で、将来にわたって「読みやすさ」を維持できるようにしたい、つまり標準化を進めていきたいと考えております。

資料３－４になります。「安全対策基準・解説の記述ルール（案）」をご覧いただけますでしょうか。まず、左側のほうですが、安全対策基準のページのイメージとなります。全体の構成としては大きく変更はしておりませんが、一番のポイントとしましては、実施すべき対策に対する記述、あと例示等の記述を明確に分けるということになってくるかと思います。

右側に説明を記載しています。「※」をしてあるところが３カ所ありまして、ここについては従来から存在している記述ルールですが、一部そのとおりの記載になっていない部分もありますので、それを今回修正していくということになります。

それ以外の部分について説明していきますと、まず一番上ですが、今回、「基準分類」という欄を追加し、基礎基準か付加基準を明記することを考えております。

そこから３つ下ですが、用語説明が今は解説の中に対策と混在しているのですが、そういったものを＜用語説明＞といった形式で記述し、明確にわかるようにします。

２つ下ですが、解説欄に実際に実施すべき対策の記述がないケースがあります。例えば例示だけしかないとか、そういった場合は、実際に何をすべきかという対策を「適用に当たっての考え方」等から補充してくると言いますか、補記するといった記載方法に変更しようと考えております。

一つ下ですが、例示は、「以下の例がある。（1）、（2）といった形式に統一しまして、例示であることを明確にするということを考えています。

その一つ下ですが、関連する基準を参照する場合は、「～については【実××】を参照のこと」といった文章があるのですが、そちらも＜参照先＞といった形式で記述し、明確にしていきます。

一番下のところですが、例示の中に、実施する対策の事例を記述する場合は、「～をする」「～をおこなう」という形で語尾を統一するということで「対策」と「例示」が明確にわかるように記述を変更したいと考えております。

実際の変更例のサンプルを最後の資料３－６につけております。こちらはあくまでも現時点での変更例というところではありますが、変更のイメージが湧くかと思いますので、少し説明をさせていただきます。左側が現行の基準の本文になります。右側が今回の「読みやすさ」で変更した基準本文になります。

まず１ページ目の、「【統５】セキュリティ遵守状況を確認すること」になります。コメントに書いてありますが、「適用にあたっての考え方」に「～するために～をすること」という記述になるのですが、その目的が書いていないというところで、右側に目的を追加してあります。その内容は下の１の「コンピュータシステムを円滑かつ適正に運用するため」というところから持ってきております。

左側の解説２番ですが、「セキュリティ遵守状況を確認するタイミングとしては、以下のようなものがある。」ということで、これは例示になりますので、「以下の例がある」とし番号を外しており、例示であることを明確にするという表現に変更しております。

続いて３ページ目の「【実 23】保管管理方法を明確にすること」になります。こちらは、「基準小項目」に目的語がないということで、何を保管管理するのかという記述がありま

せんので、右側に「ドキュメントの保管管理方法を明確にすること」と記載をしております。

中の解説の１番ですが、「ここでいう運用管理におけるドキュメントとは」の部分は、用語説明になりますので、右側のほうに、用語説明という見出しをつけております。

解説の２番ですが、「ドキュメントの管理方法として、以下のような例がある」ということで、これは例示です。３番目、４番目は「～が必要である」という記述はありますが、実はこの基準は主に何をするのかというところが解説に書かれておりません。実際にすべき対策は「不正、改ざん、紛失等を防止するために、ドキュメントは定められた方法によって管理することが必要である」というところになりますので、この文言を「適用にあたっての考え方」から持ってきて、これを実施すべき対策として解説の中に記載しています。この文章を１番とし、「ドキュメントの管理方法として以下の例がある」という形で、もともと２にあった例をそこに紐づけていくということになります。

解説３番目のところに、「ペーパーによらないドキュメント（フロッピーディスク等)」という文言がありますが、「フロッピーディスク」ということで古い表現になります。他にもいろいろな媒体等がありますし、サーバーにファイルとして保管したりといったケースもあるかと思いますので、「電子文書等」という、これが適切かどうかというのはありますが、そのように古い表現を見直していくというものになります。

続いて５ページ目の「【実 15】授受・管理方法を定めること」になります。こちらも何を授受・管理するのかわからないので、「データファイル」ということを補記しております。

解説の１番ですが、用語説明になりますので、先ほどと同じく、用語説明を切り出してわかりやすくしています。

解説３番目ですが、「データファイルの授受・保管管理方法として以下のような例がある」というところですが、黄色いマーカーが引いてありますが、以下のような例があるとしながら、その後は「～を行うことが必要である」となっており、先ほど方針の中にもありましたが、こちらの語尾を見直すということで、右側に「～する」に語尾を変更するという対応をしています。

最後のサンプルになりますが、７ページです。「【実 17】バックアップを確保すること。」です。こちらもまず「データファイルのバックアップを確保すること」と変えております。

解説１番、３番ですが、「～すること」となっていますが、こちらを「～することが必要である」というように、実施すべき対策については「必要である」に語尾を統一していくこととなります。

解説４番ですが、「バックアップデータの保管方法については、【運 25】も参照のこと」、これは参照先についての記載です。こちらは先ほどの記述ルールにも記載のとおり、参照先ということがわかるように明確化しております。

解説５番ですが、「イントラネットへの業務の依存度が高まっていることから」となっていますが、当時の時代背景がそうだったということもあるかもしれませんが、これについては古い表現ということで、「イントラネット上のデータについても」に表現を見直すといった対応をしたいと考えています。

以上、幾つかの変更のパターンを説明させていただきました。

最後に、今後の進め方について説明いたします。資料３－１「Ⅲ．今後の進め方」になります。

まず、本日の内容について８月 22 日火曜日までに事後意見のほうをお願いしたいと思っております。また、本日はサンプルのみでしたが、基準の原案については、本日ご説明した内容をもとに８月末までに事前送付とし、８月 25 日～31 日にかけて、２回程度に分けてメールで送付させていただくことを予定しております。その後、非常に量が多いものですから、９月 29 日、約１カ月程度で内容についてご確認いただきたいと考えております。

今回幅広い変更となるため、委員の皆様には確認等のご負担をおかけすることになりますが、何卒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　ありがとうございました。この安全対策基準ができて 30 年たちますし、それからそれ以降改訂に次ぐ改訂ということで、統一感とか、そもそも表現が古くなっている等々がありまして、今回の大改訂でどういうふうに改訂していくかという作業方針みたいなことについて、今、ご説明したものであります。幾つか例示がありましたのでイメージをわかっていただこうということでありますが、ここまでのところでご意見、ご質問等がありましたらよろしくお願いします。

よろしいですか。現物がないとなかなか、見てからいろいろと言おうということかもわかりませんけれども、きょうでなくても、この後、事後意見ということでいただいて、そ

れをもとに改訂作業のほうに反映していく予定でありますのでよろしくお願いいたします。

それでは事務連絡等について、和田部長のほうからお願いします。

５、事務連絡

○和田監査安全部長　事務連絡は３点ございます。

まず１点目ですが、原案前説についてです。資料４－１、４－２についてですが、冒頭にもお知らせしましたように、原案前説に対してのご意見というのは引き続き受け付けております。この後、原案資料４－１、４－２を皆様のもとにお送りいたします。いただいたご意見をまとめて内容を更新した形でお送りさせていただきますので、内容のほうを皆様のほうでご確認をお願いしたいというところが１点目になります。

２点目です。本日の議案１、議案２、議案３、及び前説原案に対してのご意見がございましたら、資料５－１のフォーマットに従いまして８月 22 日 17 時までに電子メールにてお送りいただければと思います。フォーマットについては本日をお送りさせていただきますのでよろしくお願いいたします。

３点目ですが、議事次第の５になります。次回の第 56 回専門委員会の開催日時のご案内になります。次回は９月 12 日火曜日、時間・場所とも本日と同じ 15 時から 17 時を予定しております。議題の予定といたしましては、本日の議案１、議案２、議案３に対するご意見をもとにご議論をいただければと思っております。なお、次回の専門委員会のご出欠の確認につきましては別途ご案内させていただきますので、そのほうもよろしくお願いいたします。

以上が事務連絡となります。

○渕崎副座長　和田部長、ありがとうございました。ほかに全体を通して何かご意見、ご質問等がございましたらよろしくお願いします。よろしゅうございますか。

それでは第 55 回の委員会を終了いたします。お忙しい中ありがとうございました。

以上