平成 30 年 2 月 23 日
公益財団法人 金融情報システムセンター

第 61 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 30 年 2 月 23 日（金）　15:00～16:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．　15:00　開会
２．　15:10　【議案１】安全対策基準改訂原案に対する会員意見募集の結果について
３．　15:45　【議案２】安全対策基準（第９版）の発刊等について
４．　15:50　事務連絡
５．　15:55　閉会

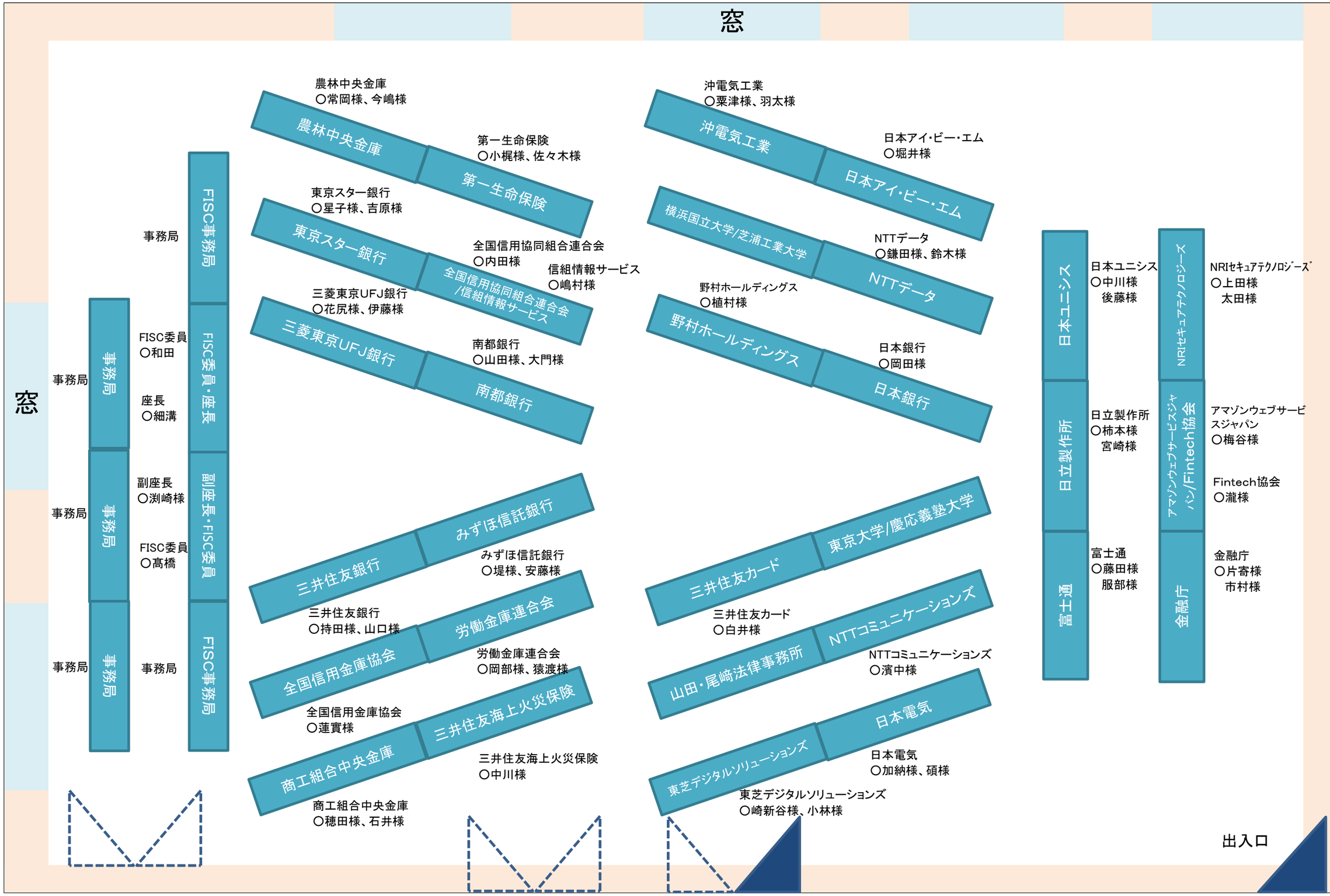
Ⅳ　資料

【資料１－１】　安全対策基準改訂原案に対する会員意見募集の結果について
【資料１－２】　安全対策基準改訂原案に対する会員からのご意見・対応方針
【資料１－３】　安全対策基準（第９版）（修正原案・会員意見反映版）
【資料２－１】　安全対策基準（第９版）の発刊等について
【資料３－１】　安全対策専門委員・検討部会委員名簿

以上

第61回「安全対策専門委員会」座席表

平成30年2月23日



【資料１－１】
平成 30 年 2 月 23 日
公益財団法人 金融情報システムセンター

安全対策基準改訂原案に対する会員意見募集の結果について

１．会員意見に対する回答について

平成 29 年 11 月 28 日より平成 30 年 1 月 12 日にかけて、安全対策基準改訂原案に対する会員意見募集を実施した。受領した意見に対し、事務局にて回答案（【資料１－１】安全対策基準改訂原案に対する会員からのご意見・対応方針）を作成したので、これに基づき会員への回答をおこなってよいか、ご審議いただきたい。なお、回答案が承認された場合は、当センターHP（会員用）上に「安全対策基準改訂原案に対する会員意見への回答」として、委員会終了後すみやかに掲載する予定である。

会員意見募集結果

○　意見数（会員数）　**122 件　/　16 先**

○　意見のうち、原案を修正したもの　54 件

○　意見のうち、今後の継続検討テーマとしたもの　42 件

２．継続検討課題への対応

継続検討テーマとさせていただいたものについては、早急に検討すべき内容も含まれていると考えており、平成 30 年度に安全対策検討部会にて審議のうえ、第 9 版追補（仮）の策定に向けた検討を開始したいと考えている。開催時期、運営詳細等については、当センターにて検討のうえ、専門委員及び検討委員へ別途通知させていただく。

以上

【資料1-2】
平成30年2月23日
公益財団法人　金融情報システムセンター

■安全対策基準改訂原案に対する会員からのご意見・対応方針

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
1	－	全般	－	FISC作成の「金融機関等におけるセキュリティポリシー策定のための手引書」に沿ってセキュリティポリシーを策定している銀行があることから、「金融機関等におけるセキュリティポリシー策定のための手引書」について、今回の安全対策基準の改訂内容と照らし合わせたうえで必要に応じて改訂を行い、整合性を図っていただきたい。	意見	ご意見を踏まえ、『金融機関等におけるセキュリティポリシー策定のための手引書』については、調査のうえ、必要に応じて改訂を行いたいと考えております。	否	●
2	－	全体	－	金融機関の**ブロックチェーンの活用**が活発に検討されており、プライベート・パブリックブロックチェーンを含めてさまざまな業務領域での本番事例の増加が予想されますが、分散型元帳技術の導入にあたり安全対策基準上の適用もしくは考え方を、今後の課題・方向性も含めて概説等でコメントいただけると大変助かります。	意見	ブロックチェーンについては、当センターでも調査・研究を進めているところです。 今後、安全対策の考え方や基準化が必要な状況になった際には速やかに検討テーマとして取り上げていきたいと考えております。	否	●
3	1	Ⅰ．概説	1	読みやすさの観点から「クラウドサービス事業者」という記載を「クラウド事業者」に統一してはどうでしょうか。	意見	ご意見を踏まえ、「**クラウド事業者**」に統一させていただきます。	要	
4	1	Ⅰ．概説	1	「安全対策の指針ととして作成され」とあるが、「安全対策の指針として作成され」に修正。	意見	誤植のため、ご指摘のとおり修正させていただきます。	要	
5	1	Ⅰ．概説	脚注1	「Ⅲ．４ 用語の～」は「Ⅲ．３ 用語の～」の誤りではないでしょうか。また、読みやすさの観点から他の脚注（5・22・24・26）においても、語尾の助詞や句点を統一されてはいかがでしょうか。	意見	誤植のため、ご指摘のとおり修正させていただきます。（語尾・助詞についても併せて修正）	要	
6	2	Ⅰ．概説	2	FISC外部委託に関する有識者検討会報告書において、再委託先における不正事案の発生も外部委託への依存度の高まりと同程度に重要な環境認識とされています。そのため、わかりやすさの観点から、環境認識や課題認識を記載されている部分に再委託管理に関して言及し明確化してはどうでしょうか。	意見	ご意見にある通り、外部委託に関する有識者検討会では、再委託先における不正事案を受け、再委託管理に関する安全対策の考え方について議論がなされたと認識しております。ご指摘の記載箇所は、そうした再委託管理も含み外部委託全般の問題認識を「概説」として提示している部分ですので、ここの記述は原案のままとさせていただきます。	否	
7	2	Ⅰ．概説	2	「ホストコンピュータ中心からクライアントサーバ等の」とあるが、3. (2)の主要用語の定義（33頁）では「サーバー」としているため、表記を統一する。 また、ルーターについても表記を統一する（3. (2)の主要用語の定義（38頁）では「ルーター」、実14（141頁）では「ルータ」となっている）。	意見	ご意見を踏まえ、「サーバ」は、「**サーバー**」に、「ルーター」は、「**ルータ**」に修正させていただきます。	要	
8	4	Ⅰ．概説	2.(1)①a	読みやすさの観点から「大きなセキュリティ上の脆弱性を残さないことに考慮する。」は続く文章の語尾と揃えて、「大きなセキュリティ上の脆弱性を残さないことが重要である。」としてはどうでしょうか。	意見	ここは、経営層が決定する重要事項について記載した箇所であり、「重要である」という表記は文脈上重複しております。従って、「考慮する」はこのまま残したうえで、続く文章にある「決定することが重要である」を「**決定する**」に修正させていただきます。	要	
9	5	Ⅰ．概説	2.(1)②a	FISC外部委託に関する有識者検討会報告書では、管理者はITマネジメントを「担当する」とされています。したがって、「安全対策上必要となるITマネジメントを推進する」でなく「安全対策上必要となるITマネジメントを担当する」乃至は「担う」と記載するほうがより正確ではないでしょうか。	意見	ご意見を踏まえ、「**ITマネジメントを担当する**」に修正させていただきます。	要	
10	6	Ⅰ．概説	2.(2)①	「コンピュータ・システム」とあるが、3. (2)の主要用語の定義（34頁）では「コンピュータシステム」としているため、表記を統一する。	意見	ご意見を踏まえ、「**コンピュータシステム**」に修正させていただきます。	要	
11	6	Ⅰ．概説	2.(2)①	読みやすさの観点から、「しかし、金融機関等を取り巻く環境変化の中で、大きな比率を」の「比率」を２頁記載と揃えて「ウェイト」としてはどうでしょうか。	意見	ご意見を踏まえ、「**大きなウェイト**」に修正させていただきます。	要	

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
12	6	Ⅰ．概説	2.(2)②	わかりやすさの観点から「リスクベースアプローチとは（中略）意思決定に活用する考え方をいい、ここでは特に（中略）経営資源全体の中で調整することもその考え方に含まれる。」としてはどうでしょうか。	意見	ご意見を踏まえ、以下のとおり修正させていただきます。 「リスクベースアプローチとは、リスク特性の分析結果を安全対策の優先順位など金融機関等が安全対策を決定するための合理的な意思決定に活用する**考え方をいう。この際、**金融機関等の経営資源が有限である点を踏まえ、リスクゼロを追求することは必ずしも合理的ではないという認識に基づき、安全対策に対する資源配分を経営資源全体の中で**調整していくこととなる。**」	要	
13	7	Ⅰ．概説	2.(3)	「金融機関等の情報システムの安全対策における基本原則」の1つ目の「〇」が「情報システムに対する安全対策は、以下の考え方に基づき、適切な意思決定が行われ、運営されるべきである。」とされていることを考えると、2つ目から4つ目の「〇」は行頭文字を変えるなど、箇条書きのレベルを下げた記述とすべきではないか。	意見	1つ目の「〇」の文章は、以下に続くものの上位としてではなく、「情報システムに対する安全対策は、適切な意思決定が行われ、運営されるべきである。」という内容であり、基本原則の1項目を示しています。従って、他の3つの「〇」と同じレベルの文章となることから、原案のままとさせていただきます。	否	
14	8	Ⅰ．概説	2.(3)	読みやすさの観点から「例えばATMや」は「例えば、ATMや」にするなど、読点の使用を統一されてはいかがでしょうか。（他にも脚注18や23頁本文中など同様の記載が見受けられます）	意見	ご意見を踏まえ、修正させていただきます。	要	
15	8	Ⅰ．概説	2.(3)	「本人の許諾なく流出した場合」とあるが、この文脈においては、「本人の許諾」の有無は本質的な論点ではなく読者を混乱させるおそれもあるため、単に「外部に流出した場合」にする等、表現を見直していただきたい。	意見	ご意見を踏まえ、「**外部に流出した場合**」に修正させていただきます。	要	
16	8	Ⅰ．概説	2.(3)	『「機微情報（要配慮個人情報を含む）」については、「重大な外部性を有する」システムと同様、「高い安全対策」を適用することが必要となる』とあるが、この表現では、機微情報以外の個人情報には高い安全対策を適用する必要はないと受け取れる。 個人情報保護法の趣旨からすると、個人情報の取扱いには高い安全対策が必要であり、機微情報（要配慮個人情報を含む）の取扱いには、特に高い安全対策が必要と考えられることから、個人情報保護法（「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」（第20条）等）を参考に、表現を見直していただきたい。	意見	当該箇所については、個人情報保護法等のフレームについて「遵守することが必要である」としたうえで、機微情報を取り扱う場合の安全対策と一般の個人情報を取り扱う場合においては、リスク特性に差があること及び、機微情報を取り扱う場合には「高い安全対策」が必要であることを説明しております。ただし、ご意見にあるような誤解を生じさせないためにも、最後の文章に以下の内容を追加させていただきます.。 修正後 「このような事態を避けるために、（略）「機微情報（要配慮個人情報を含む）」については、「重大な外部性を有する」システムと同様、「高い安全対策」を**適用し、一般の個人情報では、そのリスク特性に応じて必要かつ適切な安全対策を実施することが必要となる。**」	要	
17	8	Ⅰ．概説	脚注5	「第6条（機微（センシティブ）情報について）参照。」は「第5条（機微（センシティブ）情報）を参照。」の誤りではないでしょうか。なお、本指摘は改正個人情報保護法の施行（平成29年5月30日）による見直しにより生じた事象と思われますので、今後の改正に応じるためにも、施行日を付した記載としてはどうでしょうか。	意見	ご意見を踏まえ、修正させていただきます。	要	
★ 18	10	Ⅰ．概説	2	金融機関等の情報システムの安全対策における経営責任のあり方　3「客観的な立場から見れば、法的な責任を果たしているものとして評価されるべきである。」 とあるが、インシデントが発生した場合、それが予測困難なものであったとしても経営者は顧客保護、安全管理義務その他の責任が生じる可能性がある。 よって、「xxxとして評価されるべきである」という表現より、「xxxとFISCは考える」または「xxと考えられる」が適切と思われる。	意見	○経営層が、諸法令を遵守するとともに、（中略）客観的立場から見れば、法的な責任を果たしているものと**考えられる。** 併せて、脚注7 についても、分かりやすさの観点から、以下のとおり修正させていただきます。 7 ここで「法的な責任」とは、**民事法上の責任に限らず**、コーポレートガバナンス・コードに準拠した対応や、金融規制上の行動規範に準拠**した対応**など、経営層が広く日常において果たすべき行動や姿勢を尽くすことをいう。	要	
19	11	Ⅰ．概説	2.(6)②	わかりやすさの観点から「そのリスク特性に応じた統制を行うことが必要であり」を「そのリスク特性に応じた統制を経営資源と調整しつつ行うことが必要であり」としてはどうでしょうか。	意見	ご意見を踏まえ、「そのリスク特性に応じた統制を**経営資源配分を調整しながら**行うことが必要であり」に修正させていただきます。	要	

	No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
	20	11	Ⅰ．概説	2.(6)②	わかりやすさの観点から「適切な水準で外部に対する「統制」を行うことが必要となる。」を「適切に外部に対する「統制」を行うことが必要となる。」としてはどうでしょうか。「水準」という表現は何らかの客観的な指標が前提として想定されますが、統制は個々に目標は設定されるものの指標としてその程度を表現できるものではないと考えます。	意見	ご意見を踏まえ、「**適切に外部に対する「統制」を**行うことが必要となる。」に修正させていただきます。	要	
	21	12	Ⅱ．フレームワーク	脚注11	わかりやすさの観点から、「例えば、システム全体では、」を「例えば、特定システム全体では、」としてはどうでしょうか。	意見	ご意見を踏まえ、「例えば、**特定**システム全体**において**、機微情報が保有されている**もの**の、当該サブシステム内には機微情報が保有されていない場合が考えられる。」に修正させていただきます。	要	
★	22	13	Ⅱ．フレームワーク	1.(1)③	FinTechに関する有識者検討会報告書では、「設備基準や技術基準といった技術的な安対基準の取扱いについて明確化（中略）を行うことが適切である。」とされています。実務基準には取扱いについては「なお、（中略）必要がある。」と留意事項として明確化されている一方で、設備基準の取扱いが必ずしも明確に記載されていません。そのため、設備基準が形式的に客観的評価で使用されるという、報告書が指摘した問題に対処が進まないことが危惧されます。例えば、実務基準と同様の留意事項を記載するなどしてはどうでしょうか。	意見	今回の改訂では、考え方や基準の構成を含め抜本的な改訂を行っておりますが、設備基準については内容まで踏み込んだ見直しを行っておりません。ご指摘の点は、報告書の提言内容も踏まえ、設備基準に対する他のご意見と併せ、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
	23	16	Ⅱ.フレームワーク	1.(3)	金融関連サービスを提供するシステムにおいて、ベンダーがシステム開発等を受託する場合、安全対策基準を適用するか否かについて、判断基準を明確しておいた方がよいのではないか。金融機関等における外部の統制の範囲に応じてということであれば、場合によっては、金融機関等とFinTech企業の間に外部委託関係が存在するかどうかを確認し、安全対策基準の適用要否をベンダー側が確認する必要性が生じるといった懸念がある。	質問	Ⅱ.フレームワークでは、金融関連サービスを提供するシステムに関する業務の受託においては、金融機関等における外部の統制が及ぶ場合、部分的に及ぶ場合、全く及ばない場合に応じて、安全対策基準の適用方法に差がある旨を記載しました。これは、金融機関等からみて、外部の統制をどの程度行うのかという点を整理することが有益であるとしたFinTechに関する有識者検討会の内容を踏まえ、文章化したものです。金融関連サービスを提供するシステムの開発をベンダーが受託する場合には、金融機関等とFinTech企業との間で合意した安全対策の内容を要件として提示してもらい開発することになると考えられます。従って、ここで一律に判断基準を示すことは適当ではないと考えております。	否	
	24	15、 18	Ⅱ.フレームワーク	1.(2) 1.(4)②	「重大な外部性または機微情報を有する特定システム」（18頁）に対しては、「『付加基準』の『必須対策』を必ず適用するものとする」（15頁）とあるが、「付加基準」の「必須対策」について、「外部性」を有すること（他の金融機関や顧客に対し広く影響を及ぼし、社会全体に経済的損失を与える可能性があること）と、「機微情報」を有することのいずれの観点から求められる対策であるかが分かるように記載していただきたい（例えば、52～66頁の「2.基準一覧」に追加する等）。	意見	付加基準の必須対策には、「重大な外部性を有するシステム」に適用するものと、「機微情報を有するシステム」に適用するものとに一律に分類することが難しい対策（どちらにも適用される対策）が存在します。従って、一律の分類は行いませんが、リスクベースアプローチの考え方に基づき、保有する情報システムに対する適切な安全対策を自ら決定することが肝要であると考えております。	否	
	25	16	Ⅱ．フレームワーク	1.(3)	従来は、金融情報システム以外の情報システムについては、安対基準の適用対象外としたうえで「参考となる部分があると金融機関が独自に判断すれば」適宜取り入れるという考え方でしたが、原案は「その技術基盤（中略）必要となる対策を適宜取り入れる」とされており、従来以上に適用を求める記載とも読めます。「適用対象外」は金融情報システムを対象とする安対基準で記載すべき事項そのものの対象外であり、社会的規範性が対象外にも及ぶと受け止められかねない記載をすべきではなく、あくまでも金融機関各社の独自の判断に委ねられるべきと考えます。	意見	ご指摘の箇所については、金融情報システムと、それ以外のシステムにおいてセグメントやプラットフォームが分離されていないことが一般的であり、一方は適用、一方は適用外とすることが困難であるという委員からの意見を踏まえ、このように記載しました。ただし「適宜取り入れる」としていることから、実質的な強度は変更しておりません。従って、原案のままとさせていただきます。	否	
	26	17	Ⅱ．フレームワーク	1.(4)	わかりやすさの観点から、「効果が最大となるよう」と「効率が最大化されるよう」という記載は、効果と効率のいずれかに統一してはどうでしょうか。一般的には「経営資源配分」に対しては効果ではなく、効率という言葉のほうがなじむものと考えます。	意見	ご意見を踏まえ、以下のように修正させていただきます。 修正前（1行目） 「その経営資源配分の効果が最大となるよう、適切な内容で安全対策を決定していくこととなる。」 修正後 「その経営資源配分の**効率を考慮し、リスク特性に応じて**適切な内容で安全対策を決定していくこととなる。」 修正前（4行目） 「安全対策費用とその効果、新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮し」 修正後 「安全対策費用とその効果、新規開発投資とその効果、**それぞれが最大化されるよう経営資源配分を考慮し**」	要	

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
27	18	Ⅱ．フレームワーク	1.(4)②	「利用する金融情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。」は、「利用する情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。」の誤りではないでしょうか。	意見	ご意見を踏まえ、「**利用する情報システムから**、安全対策基準の適用対象となる金融情報システムを特定する。」に修正させていただきます。	要	
28	18	Ⅱ．フレームワーク	1.(4)②	わかりやすさの観点から、「また、金融情報システムにおいて、内部だけで利用されるシステムや、」の記載は、FISC外部委託に関する有識者検討会報告書の記載と同様に「また、金融情報システムにおいて、他のシステムと連結していないシステムや、」としてはどうでしょうか。	意見	「内部だけで利用されるシステム」という表現については、様々な解釈がなされる可能性があるというご意見を踏まえ、「**外部性を有しないシステム**」という表現に修正させていただきます。	要	
29	18	Ⅱ．フレームワーク	1.(4)② 図表12	矢ばねの「機微性」は「機微情報」乃至は「情報の機微性」としてはどうでしょうか？FISCFinTechに関する有識者検討会報告書では機微性には程度があることが示されており、FISC外部委託に関する有識者検討会報告書では機微性を有する情報のうち高い機微性を有する「機微情報」について限定的に社会的・公共的性質があり特定システムとなるものと読めます。（上記内容で修正依頼する）	意見	ご意見を踏まえ、「**情報の機微性**」に修正させていただきます。	要	
30	21	Ⅱ．フレームワーク	2	日本語の「外部委託」という言葉は、システムの開発と運用いずれでも同じ言葉が使用されます。そのため、FISC外部委託に関する有識者検討会報告書では、開発時と運用時のリスクは明らかに異なるものと整理され、同じ言葉であるが故にリスクの程度が混同されることが無いように配慮されています。わかりやすさの観点から、外部委託に係る基準は、開発と運用ではリスク特性が異なることを、「概説」もしくは「フレームワーク」で明確にし、リスクベースアプローチがより適切に実施されるようにしてはどうでしょうか。	意見	ご意見を踏まえ、「Ⅱフレームワーク.2統制.(2)外部の統制の②通則」の一部を、以下のとおり修正させていただきます（No40、No41と併せて、以下のように修正）。 「なお、**外部委託する業務がシステム開発の場合とシステム運用の場合では、そのリスク特性が異なることが考えられる。また、委託する業務が細分化され再委託されることでリスク特性に変化が生じる場合がある。こうした点を踏まえ、**再委託先に対しては、委託する業務の範囲や重要度に応じて、外部委託先に対して実施する管理上の項目から必要な部分を選択し、実施することが考えられる。」	要	
31	21	Ⅱ．フレームワーク	2	FISC外部委託に関する有識者検討会報告書では、委託業務のリスクが高く高い安対基準の適用が妥当とされる場合にも、「委託業務が細分化された結果、再委託業務のリスクが十分に低いと判断しうる場合」には高い安対基準の適用不要という考え方が示されています。リスクベースアプローチがより適切に実施されるために、この考え方も記載してはどうでしょうか。	意見	上記のとおり修正させていただきます。	要	
32	21	Ⅱ．フレームワーク	2.(2)	3者構成に着目する必要性として、「FinTech企業等について、必ずしも委託関係にあるとは限らない企業」が出現したことであると説明され、契約内容の現象面に着目しているように読めます。一方で、FISCFinTechに関する有識者検討会報告書では、3者構成の検討が必要な説明として、「技術的な性質と業務的な性質を同時に有する」（つまり金融業務とシステム開発等業務のいずれにも明確に分類・分離できない関係者の登場）ことが挙げられており、説明が異なっています。後者の認識に従って記載してはどうでしょうか。	意見	ここでは、理解しやすいよう、委託関係に着眼して説明をさせていただいております。ご指摘の内容については、3者間構成における通則（p25 2.(2)④派生形（3者間構成）における通則）の中で（ご意見の内容に沿った形で）記載しておりますので、ここは原案のままとさせていただきます。	否	
33	25	Ⅱ．フレームワーク	2.(2)	同等性の原則が派生形における通則と記載されています。一方で、FISCFinTechに関する有識者検討会報告書では、「安対基準に具現化された安全対策の効果は、（中略）金融機関とITベンダー者関係の中でも維持されてきた」とされており、外部の統制全体の通則と位置づけられているものと理解されます。記載箇所を外部委託の通則に変更されてはどうでしょうか。	意見	システムの開発・運用が外部委託されることがごく自然な流れとなっている現状においては、2者間と3者間との間で安全対策の効果が同等となる説明の方が分かりやすいと考えております。従って、原案のままとさせていただきます。	否	
34	25	Ⅱ．フレームワーク	2.(2)	FISCFinTechに関する有識者検討会報告書では、3者における原則として「協調の原則」が記載されています。FinTechにおいては重要な原則とされていますので、フレームワークにも明確に記載してはどうでしょうか。	意見	「協調性の原則」は、2者間の構成においては当然のことと考えておりますが、3者間の構成においては、報告書の提言内容を踏まえ、改めて記載しておく方がよいと判断いたしました。したがって、3者間の構成の通則部分の記載について、p25の6行目に「**なお、安全対策に係る情報開示が協調して適切に行われるように、あらかじめ3者間で合意しておくことが望ましい。**」という文章を追加させていただきます。	要	

	No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
	35	26	Ⅱ．フレームワーク	2.(2)	金融機関等とフィンテック企業が、契約締結し、オープンAPIによりシステム接続して「支払・送金の指示」や「口座情報の取得等」を行っている場合、金融機関による外部統制が部分的と解して、安全対策基準を部分適用すると記載されている。具体的には脚注19に「データ保全」や「本人認証」と記載してあるが、今後、部分適用される安全対策基準を詳細に公表する予定等はあるのか？	質問	実施する安全対策は、基礎基準を踏まえて策定されたオープンAPIチェックリストや、委託元の要件等を基にして、リスク特性に応じて決定されるものとなるため、適用すべき安全対策基準を一律に示すことは適当ではないと考えております。	否	
★	36	34	Ⅲ．本書の利用にあたって	3.(1)	クラウドの定義としてNISTの定義が採用されています。クラウドに関する有識者検討会ではNISTの定義が参考とされたものの、その後の安対基準の8版追補改訂では定義が見送られています。そうしたことから、FISCFinTechに関する有識者検討会報告書では、固有のリスク管理をすべきクラウドの性質からその姿を明らかにする手法がとられています。そうしたFISCでの検討経緯※を踏まえると、定義は見送るか、NISTの定義は参考程度に留めるべきと考えます。※NISTの定義を使用した場合、本来、安対適用対象とすべきものが対象外と解釈されたり、対象外のものが対象と解釈されるなど、弊害があるものと考えます。そうした観点からも、欧米の当局においてもクラウドの定義に対しては消極的なスタンスであるものと理解しています。	意見	ご意見を踏まえ、用語を削除したうえで、クラウドの定義をp24脚注23にNISTの定義を参考とする内容を追記させていただきます。 脚注23 「一般的にクラウドサービスには、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）等があり、各形態ごとに提供されるサービスや利用上の制約が異なる。**なお、米国のNIST（National Institute of Standards and Technology：国立標準技術研究所）では、「最小限の管理負荷やプロバイダー交渉だけで、迅速に提供され稼働する構成変更自在のコンピュータ資源（ネットワーク、サーバー、記憶装置、サービス等）の共有プールに対する、ネットワークを通じた便利で随時のアクセスを可能とするモデル。」としてクラウドを定義している。**」	要	
	37	61	基準一覧	－	設備基準に「旧基準番号」列がありません。 今回、「および」⇒「及び」，「や」⇒「、」等の変更が既に行われていることから，新旧の項目は同じ「設xx」という番号を用いていても別物と位置づけるべきと考えます。また，それ以外に，今回寄せられるパブリックコメントを受けての内容変更も考えられます。 以上を考えると，一見無駄に見えても旧基準番号列を設け，「設1」のように明示しておくことが必要と思います。	意見	設備基準については、運用基準や技術基準のような構成変更を行っておりません。このため、基準番号一覧には新旧番号を表示は不要と考えております。	否	
	38	68	統1	4	「環境変化に対応し、当該規程を適宜見直し改訂することが必要である。」とあります。見直しが必須なことは自明ですが，改訂は状況に拠るため，「適宜見直し、**必要に応じて**改訂することが必要である。」といった表現が妥当のように思います。	意見	「見直す」には、「点検し、修正する」という意味があることから、ご指摘を踏まえ、以下の内容に修正させていただきます。 修正後 「環境変化に対応し、当該規程を**適宜見直す必要がある。**」	要	
	39	73	統4	参照 法令	参照法令として「不正アクセス行為の禁止等に関する法律 第2条～第5条」とあるが、同法第2条は用語の定義、第3条～第5条は不正アクセス行為等の禁止を定めており、「統4」の記載内容（セキュリティ管理体制の整備）との関連性は低いと思われる。 当該条項を参照法令とした意図を教えていただきたい。	意見	参照法令については、原則として内容の見直しを行っておりません。参照法令については、委員会での議論を経て修正等を行うべきと考えており、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
	40	74	統5	1	「未然防止策・事前対策、検知策及び対応策を検討し、態勢を整備することが必要」とあるが、米国NISTの「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」のフレームワークコアの4要素（特定、防御、検知、対応、復旧）に沿ってサイバーセキュリティリスクを整理している銀行もあることから、当該ドキュメントも参考に記載を見直してほしい。	意見	【統5】（旧【運113】）については、今回の改訂では内容の見直しを行っておりません。記載内容は、別途議論を得て追記等を行うべきと考えており、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
	41	75	統5	－	経済産業省の「サイバーセキュリティ経営ガイドライン Ver.2.0」の「3.サイバーセキュリティ経営の重要10項目」における「サイバーセキュリティリスクの管理体制構築」や「インシデント発生に備えた体制構築」等を参考としている銀行もあることから、当該ドキュメントも参考に記載を見直してほしい。	意見	【統5】（旧【運113】）については、今回の改訂では内容の見直しを行っておりません。記載内容は、別途議論を得て追記等を行うべきと考えており、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
	42	76	統6	3	「システム管理者に権限が集中することによる不正行為の発生を防ぐため、システム管理者を各機関の実態に合わせて権限を適切に分散し、相互牽制機能が働くようにすることが望ましい。」とあるが、読みやすさの観点から、「システム管理者に権限が集中することによる不正行為の発生を防ぐため、各機関の実態に合わせてシステム管理者の権限を適切に分散し、相互牽制機能が働くようにすることが望ましい。」とした方がよい。	意見	ご意見を踏まえ、「システム管理者に権限が集中することによる不正行為の発生を防ぐため、**各機関の実態に合わせてシステム管理者の権限を適切に分散し、**相互牽制機能が働くようにすることが望ましい。」に修正させていただきます。	要	

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針(案)	原案の 修正要否	継続 検討
43	80	統10	2.(1)～(5)	「防災組織を整備する際の留意点としては、以下の例がある。」として、(1)～(5)の留意点が記載されているが、これら留意点は、コンピュータセンターが共同ビル内にある場合に限定されないため、1. の「なお、防災組織の実効性を高めるため、業務組織に則した組織とし、役割分担ごとに責任者を明確にすることが必要である。」の前に記載した方がよい。	意見	ご意見を踏まえ、(1)～(5)の留意点について、1.の例示(「防災組織の例を図1に示す。」の後)として記載箇所を修正させていただきます。	要	
44	82	統11	2.(1)～(3)	「防犯組織を整備する際の留意点としては、以下の例がある。」として、(1)～(3)の留意点が記載されているが、これら留意点は、コンピュータセンターが共同ビル内にある場合に限定されないため、1.の「防犯組織の例を図1に示す。」の前に記載した方がよい。	意見	ご意見を踏まえ、、(1)～(3)の留意点及び防犯対策のための設備基準の紹介について、1.の例示(「防犯組織の例を図1に示す。」の後)とし、2.を図1の後に、それぞれ記載箇所を修正させていただきます。	要	
45	85	統12		「各種業務の規則」についても、統1の規程と同様に、承認、見直し・改訂、関係者への周知・教育等に関して記載した方がよい。	意見	「各種業務の規則」については、規則を管理する各々の組織ごとに管理プロセスがあると考えられ、一律に基準化することは適当ではないと考えております。従って、原案のままとさせていただきます。	否	
46	86	統13		統制は、組織体制・規程の整備⇒リスクの現状分析・評価⇒実務基準、設備基準に基づく管理活動および教育⇒管理活動の評価・見直しというプロセスであることから、Ⅱ. フレームワーク1. 総論(4)安全対策決定のプロセスの内容は、1統制基準1内部の統制に入れた方が良い。FAQⅠ－3にあるように、リスクベースアプローチの手順について詳細な内容を示せないとしても、示せる範囲で統制基準にあった方が良い。	意見	ご指摘にある「リスクの現状分析・評価」及び、安全対策決定のプロセスは、一つの考え方や手法を示しており、これ自体は安全対策の基準ではないと考えております。これを踏まえ、今回の改訂ではⅡ.フレームワークの中に記載していることから、原案のままとさせていただきます。	否	
47	86	統13		セキュリティなどの管理状況の評価は、リスクの現状分析・評価を実施し、そのリスク評価への対策(人材教育を含む)を実施した後に実施する内容であること、この順番では組織体制や規程の整備の次に実施する内容と誤解を与えることから、フレームワークの説明と整合させて、順番を統制基準の最後に下げた方が良い。	意見	今回の改訂では、これまでの安全対策基準上で分散していた「統制に関する基準」を集約しています。【統13】については、各種規程を整備し、管理体制を整備したうえで、実務基準にある対策を実施し、その状況を確認する基準として配置しています。なお、「人材の教育」については、組織横断的に実施する訓練等と合わせて統制基準としたものであり、安全対策を実施するための規程の整備及び組織体制の整備とは別に分類させていただいております。 今回は原案のままとさせていただきますが、基準の並びについては、多くの考え方があると考えております。ご意見も踏まえ、よりよい整理の考え方があれば、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
48	87	統14	1	統12では「各種業務の規則」を、「手順書及びマニュアル」の上位文書に位置づけていることから、セキュリティ教育に使用する文書として、「セキュリティポリシー」、「セキュリティスタンダード」、「マニュアル、手順書等」だけでなく、「各種業務の規則」も加えた方がよい。	意見	ご意見を踏まえ、「セキュリティポリシー、セキュリティスタンダード、**各種業務の規則、**マニュアル、手順書等」に修正させていただきます。	要	
49	88	統14	3	(注) ソーシャルエンジニアリングへの対策は、以下のものが一般的である。現記載は、ソーシャルエンジニアリング対策の例示としてはやや違和感がある。 -ポリシーによる規定 -運用手続きによる制限 -教育およびトレーニング	意見	ご意見を踏まえ、ソーシャルエンジニアリング対策に関する記載を修正させていただきます。 (注)「ソーシャルエンジニアリング」とは、不正侵入するのに必要なシステム情報を、正規のユーザーあるいはその同僚などから聞き出したり、ごみ箱に捨てられた記録紙から推測したりする手法のことである。対策としては、**「ポリシーによる規定」、「運用手続きによる制限」、「教育およびトレーニング」が挙げられるが、具体的な例として、**アカウント、パスワード、ネットワークアドレス等のシステム情報の厳重管理等がある。」	要	
50	91	統16	2	「訓練終了時には本番環境に戻した後、本番稼働に支障がないことを確認する必要がある。」とありますが,「訓練環境に切り替えた場合」という前提が省略されています。 「**訓練実施時に訓練環境に切り替えた場合、**終了時には本番環境に戻した後、本番稼働に支障がないことを確認する必要がある。」と言った表現をお願いします。	意見	ご意見を踏まえ、「**訓練実施時に訓練環境に切り替えた場合、**終了時には本番環境に戻した後、本番稼働に支障がないことを確認する必要がある。」修正させていただきます。	要	
51	95	統20	1.(4)	「プラットフォーム、アプリケーション等に関するサービスの利用」とあるが、サービスを利用するのは金融機関や顧客であり外部委託先ではないので、「プラットフォーム、アプリケーション等に関するサービスの提供」としてはどうか。	意見	ここは、クラウドサービスの利用を念頭に書いたものであり、金融機関等から見た場合、「サービスを提供する」業務を委託するものではないため、原案のままとさせていただきます。	否	

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針(案)	原案の 修正要否	継続 検討
52	96	統20	3	「外部委託先を評価する事項としては、以下の例がある。」として、(1)～(13)が例示されているが、「統20」のもととなった現行基準【運108】の3.の「(7) データの所在(データが保管される場所、または保管の可能性がある場所)」を記載しなかった理由を教えていただきたい。	質問	「データの所在確認」はクラウド固有の評価項目となるため、クラウド固有の管理策を記載した【統24】へ移動しました。 (なお、FinTech有識者検討会において、クラウドサービス固有の性質に関する補足的な検討がなされ、「データの所在確認」については、統制上必要となるデータへのアクセスが可能となる「統制対象クラウド拠点を把握することが必要であるとして対策が見直されたため、【統24】の対策として記載しております。)	否	
53	97	統20	3.(10)	契約終了時の対応(ベンダーロックインリスク対応、データ消去等) データの移行を意識された記述になっているが、実運用では、アプリケーションが対応できないと、データ移行の意味がないため、(移行データの抽出方法と実際の移行作業内容)の記述を(移行データの抽出方法とアプリケーションプログラムを含む実際の移行作業内容)としたほうが良い。	意見	ここでは移行作業として発生する可能性のあるものについて具体例を記載した部分となります。ご指摘の通り、データ移行はアプリケーション移行等の対応を伴うことが考えられるため、データ移行に特化した記載は適当ではないと考えております。このため、記載を以下のように修正させていただきます。 修正後 「システム移行作業(移行データの抽出方法と**アプリケーションプログラムを含む**実際の移行作業内容)など」	要	
54	99	統21	1	「また、委託契約に加え『機密保持に関する契約』または『リスク管理に関する契約』を締結することも考えられる。」との部分につきまして、委託契約とは別に機密保持又はリスク管理に関する契約を締結することが推奨されているわけではなく、委託契約に必要な項目が盛り込まれていれば別途の契約は不要、との理解でよろしいでしょうか。	質問	ご質問のとおり、委託契約とは別に機密保持又はリスク管理に関する契約を締結することを推奨しているわけではなく、委託契約に必要な項目が盛り込まれていれば別途の契約は不要と考えております。	否	
55	99	統21	1	「契約締結時に考慮すべき事項としては以下の例がある。」として、(1)～(16)が例示されているが、本基準項目のもととなった現行基準【運109】1.の「(13) 金融監督当局の検査等」を記載しなかった理由を教えていただきたい。	質問	安全対策基準では法令等で定められた対策まで基準化する必要がないため、今回の改訂において記載を削除させていただきました。	否	
56	103	統22	1,2	「統22」は、委託元金融機関が日常的に管理するエリア(自行コンピュータセンター)で遂行される委託業務とその委託先要員を前提とした基準になっており、委託先が管理するエリア(共同センター、クラウドベンダーのデータセンター)で遂行される委託業務とその委託先要員に対してそのまま適用することは難しい。 例えば、共同センターやクラウドベンダーのデータセンター内で、委託元金融機関が1.の「(1) 外部委託先の要員が遵守すべきルールの明示」や「(2) 外部委託先の要員が遵守すべきルールの周知徹底」を行うことは困難であり、また、2.の「金融機関等の各種資源及びシステムへのアクセス権限」の管理も共同センターのベンダーやクラウドベンダーが行うことが通常である。このため、「統22」については、委託元金融機関が管理するエリアと委託先が管理するエリアを分けたうえで内容を記載していただきたい。	意見	【統22】には「1. 外部委託先の要員が委託業務を遂行するにあたっては、金融機関等のセキュリティポリシーをはじめとした、外部委託先の要員が遵守すべきルールを委託業務の内容及び作業の範囲に応じて明確にし、これを遵守させる必要がある。」としております。金融情報システムの開発または運用業務を外部へ委託する場合、金融機関等は委託先におけるデータの保護・管理において、自社のセキュリティポリシーと照らして、妥当であるかどうかを確認することとなります。また、共同センターやクラウドサービスを利用する場合においては、利用規約(または契約書)、サービス内容において、自社のセキュリティポリシーを満たすかどうかを確認することとなります。いずれの場合も、結果として委託契約もしくはサービス利用に関する契約の中で、遵守すべきルールが明確となっており、それらが適切に遂行されているかを確認することで、ルールを遵守させていることとなることから、原案のままとさせていただきます。	否	
57	103, 104	統22,23	－	基準項目の順序が「統22 外部委託先の要員にルールを遵守させ、その遵守状況を確認すること」→「統23 外部委託における管理体制を整備し、委託業務の遂行状況を確認すること」となっているが、まず体制整備を行い、次にルール遵守の確認を行うことから、基準項目の順序を入れ替えて、「統22 外部委託における管理体制を整備し、委託業務の遂行状況を確認すること」→「統23 外部委託先の要員にルールを遵守させ、その遵守状況を確認すること」としていただきたい。	意見	【統22】はルールの遵守、【統23】は業務遂行状況の確認として、どちらも委託期間中における、委託先への統制(モニタリング)において実施すべき内容を示しております。このため、基準の順番に意味は持たせておりません。従って、原案のままとさせていただきます。	否	
★ 58	106	統24	1,2	「なお、特定システムにおいては、この措置は必要である。」ですが, p.15図表8の定義からすれば, 基礎基準で「必要である」なら, 「必須対策」となり, 「特定/通常に関わらず, 必須」とならないでしょうか？　敢えて書く意味がないように思います。(「なお、通常システムにおいては、この措置は必要ない」であれば有意となりますが, 図表8と矛盾します)	質問	ご指摘の箇所は、一定の条件下においてはリスク特性に関わらず実施すべきものがあることを明示するために記載した部分となりますが、読みやすさの観点から、以下のように修正させていただきます。 修正後 **「1.特定システムでクラウドサービスを利用する場合、クラウド事業者の選定時に、統制対象クラウド拠点(注)を把握する必要がある。また、統制対象クラウド拠点は、実質的な統制が可能となる地域(国、州等)に所在することが必要である。 なお、通常システムにおいては、利用するサービスの内容及びリスク特性等に応じて、これらの対策を実施する必要がある。」**	要	

	No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
	59	106	統24	－	第59回FISC安全対策専門委員会にて、『【資料１－１】外部委託基準改訂の検討結果について』のなかで、「なお、特定システムにおいては、この措置は必要である。」と表記する扱いと整理されていますが、同一文内に「は」が複数存在するような記載ではなく、「なお、特定システムにおいては、この措置が必要である。」とした方が読みやすく、一般的な表現と考えます。	意見	ご意見を踏まえ、基準（【統24】）については記載を修正させていただきます。	要	
★	60	106	統24	1,2	・「１．」と「２．」に「～することが必要である。なお、特定システムにおいては、この措置は必要である。」と記載があるが、なお書きに何の意味があるのか疑問。 ・なお書きで「特定システム」に限定せずとも、その前の文章で（言外で全てのシステムを対象に）措置が必要であることを謳っていると読める。 ・かつ、該当項目は「基礎基準」であり「特定システム」と「通常システム」で差別はない。 ・強調の意図で「特定システムにおいては」と言いたいのならば、例えば「なお」⇒「特に」にするとか。それでもわかりづらい不要な強調の表現。	意見	ご意見を踏まえ、1.と同様、2.についても以下の内容に修正させていただきます。 修正後 「**2. 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、金融機関等は、統制対象クラウド拠点に対して必要となる権利（監査権等）を確保するために、クラウド事業者と交わす契約書等にその権利を明記する必要がある。** **なお、通常システムにおいては、利用するサービスの内容及びリスク特性等に応じて、この対策を実施する必要がある。**」	要	
	61	106	統24	1	クラウドサービスを利用する場合、（中略）統制対象クラウド拠点（注）を把握する必要がある。なお、統制対象クラウ ド拠点は、実質的な統制が可能となる地域（国、州等）に所在することが必要である。**なお、特定システムにおいては、この措置は必要である。**基礎基準なので、特定システムについて必須対策であることは自明であるのに、あえて”この措置は必須である”と記述する意味が必要性の強調なのか通常システムには不要という意味なのか、日本語としてわかりづらく解釈に迷うので（議論の調整結果であることは理解しておりますが）修正いただく必要があると思われます。	意見	ご意見を踏まえ、基準（【統24】）については記載を修正させていただきます。	要	
	62	106	統24	1.(注)	統制対象クラウド拠点とは、データや**システム**に対する実効的なアクセスを行う拠点。”データの所在”であれば比較的明確に特定が可能だと思われますが、”システム”が追加されたことにより、IaaS, PaaS, SaaSという利用形態を考慮すると、”統制対象拠点”の複雑化が避けられないと思量、”システム”は削除した方が良いのではないでしょうか？もしくはシステムが対象となっている理由を教えていただければ幸甚です。	意見	FinTechに関する有識者検討会においても「統制上必要となるデータへのアクセス」と記載されていることから、ここはご意見を踏まえ、「システム」の文言を削除させていただきます。	要	
	63	106	統24	3	「定期的に監査を実施する必要がある」とありますが、この場合の監査発注者は金融機関／クラウド事業者の双方があり得るため、「**定期的に監査が実施される必要がある**」といった表現のほうが適切のように思います。	意見	本書は金融機関等において実施される内容を記載するため、主語は金融機関等となります。このため、ご指摘の箇所については「監査を実施する」が適切であり、原案のままとさせていただきます。 一方、直前の文章については主語が混在する記載となっているため、以下のように修正させていただきます。 修正前 「監査の実施にあたっては、（略）クラウド事業者が監査人に保証型監査を委託し（略）、その監査報告書を利用することが望ましい。」 修正後 「監査の実施にあたっては、（略）クラウド事業者が**委託した保証型監査（略）の報告書**を利用することが望ましい。」	要	
	64	108	統25		「勘定系システム」について定義がされておらず、対象範囲が不明確となるリスクがあるため、「勘定系システム」の定義を入れる必要はないでしょうか。	意見	「勘定系システム」については、各金融機関等により範囲や対象が異なり、一律に示すことは困難であることから、定義を追加しておりません。従って、原案のままとさせていただきます。	否	
	65	109	統26	1	金融庁の「中小・地域金融機関向けの総合的な監督指針」の「Ⅱ-3-4-3-2 主な着眼点」の(1)においては「統合ATMスイッチングサービス、全国銀行データ通信システム等の金融機関相互のシステム・ネットワークのサービスを利用する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。」とある。 複数の金融機関が利用するシステム・ネットワークサービスの中には、利用契約上の制約により、外部の統制が限定的となるケースがあると考えられることから、当該基準の適用方法については、これらの現状を踏まえた記載内容を追加すべきではないか。	意見	Ⅱ.フレームワーク1.(3)において、「主にサービスの利用者の視点で実施すべき対策等、外部委託の統制面において必要となる安全対策基準を適用する。」としております。これは「外部委託に順じて、適切なリスク管理を行う」という監督指針の内容とも整合的であると考えており、このことを前提に、当該基準を適用することを想定しております。利用するサービスによって外部の統制が及ぶ範囲に差がある場合、一律に同じ内容で安全対策を実施するのではなく、リスク特性に応じて必要な統制を行うか、あるいは統制が行えない場合の対策を検討していくことが必要になると考えております。	否	

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
66	109	統26		当安全対策基準の対象は「金融期間等」ですが，「等」の文字が何箇所かで欠落しています。 基準中項目：「(4) 金融機関相互のシステム」⇒「(4) 金融機関等相互のシステム」 基準小項目：「金融機関相互のシステム」⇒「金融機関等相互のシステム」 適用にあたっての考え方：「金融機関相互のシステム」⇒「金融機関等相互のシステム」 「金融機関相互の金融」⇒「金融機関等相互の金融」	意見	「金融機関相互のシステム・ネットワーク」は、固有の名称として使用していることから、原案のままとさせていただきます。	否	
67	118	実3	（参考2） 3	・　ここでは、電子政府推奨暗号の利用方法に関して、「電子政府推奨暗号の利用方法に関するガイドブック」（平成20年）が紹介されていますが、内容の一部が陳腐化しており、それを補完する各種資料（CRYPTREC暗号技術ガイドライン(SSL/TLSにおける近年の攻撃への対応)、SSL/TLS暗号設定ガイドライン等）が公表されています。 それらは、「CRYPTREC報告書」のページに掲載されています。当該ページを紹介しないと、安全な実装にかかる適切な情報を得られない可能性があります。特に、平成27年公表の「SSL/TLS暗号設定ガイドライン」は、インターネットバンキング等において、サーバ側での適切なパラメータ設定の方法が詳しく紹介されており、有用な情報です。 ―― URLは「https://www.cryptrec.go.jp/report.html」です。 ・　そこで、「CRYPTRECから「電子政府推奨暗号の利用方法に関するガイドブック」が平20年7月に公開されている」と記述するのではなく、例えば、当該部分を、以下のように修文しては如何でしょうか。 （案） 3.「電子政府推奨暗号」の利用法に関しては、CRYPTRECから「電子政府推奨暗号の利用方法に関するガイドブック」、「CRYPTREC暗号技術ガイドライン(SSL/TLSにおける近年の攻撃への対応)」、「SSL/TLS暗号設定ガイドライン」等が公開されている。これらは、今後、暗号技術の進展や攻撃手法の高度化等に伴って適宜改訂されるほか、新しいガイドラインが適宜作成されることもある。 （参照URL）https://www.cryptrec.go.jp/report.html	意見	SSLに関する記載は、今回の改訂で見直しを行っておりません。ご指摘の内容は、別途議論を得て追記等を行うべきであることから、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
68	118	実3	（参考2） 3.注	・　CRYPTRECの注に誤りがあるため、以下のとおり修正しては如何でしょうか。 （現＜誤り＞）「～共同で運営する暗号方式委員会、暗号実装委員会及び暗号運用委員会で構成されている。」 ↓ （案＜正しい＞）「～共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成されている。」	意見	ご意見を踏まえ、修正させていただきます。	要	
69	121	実4	（参考2）	SSL／TLSについては、バージョン毎の脆弱性が既に発見されているなどの経緯があり、どのバージョンを適用することが適切かの情報を入手してコントロールすべきことを明記した方が良い。	意見	現状ではSSLの方が一般的に認知されていることから、原案のままとさせていただきます。 ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
70	121	実 4	（参考2）	「インターネットバンキング等における暗号技術はSSL（Secure Socket Layer）プロトコルが一般的になっている。」とあるが、SSL（3.0）は脆弱性が報告されており、「HTTPS（HTTP over SSL/TLS）」などの最新の情報を踏まえて記載を見直す必要がある。 例えば、TLSの実装については、2017年1月にIPAが公表した米国NISTのガイドラインSP 800-52 rev.1の日本語訳「トランスポート層セキュリティ（TLS）実装の選択、設定、および使用のためのガイドライン」を参考にしている銀行もあることから、本ガイドラインを参考に記載してはどうか。	意見	現状ではSSLの方が一般的に認知されていることから、原案のままとさせていただきます。 ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
71	121	実4	（参考2） 2	・　SSL／TLSの適切な利用方法についてガイドブックが参照され、URLが記載されていますが、参照先の資料は平成20年のもので陳腐化しており、その後、それを補完する資料（CRYPTREC暗号技術ガイドライン(SSL/TLSにおける近年の攻撃への対応)、SSL/TLS暗号設定ガイドライン等）が公表されています。それらは、「CRYPTREC報告書」のページに掲載されています。当該ページを紹介しないと、安全な実装にかかる適切な情報を得られない可能性があります。特に、平成27年公表の「SSL/TLS暗号設定ガイドライン」は、インターネットバンキング等において、サーバ側での適切なパラメータ設定の方法が詳しく紹介されており、有用な情報です。 ――　URLは「https://www.cryptrec.go.jp/report.html」です。 ・　そこで、「CRYPTREC公開の「電子政府推奨暗号の利用方法に関するガイドブック」に記載がある」と記述するのではなく、例えば、当該部分を、以下のように修文しては如何でしょうか。 （案） 2. SSLの暗号技術の適切な利用方法については、CRYPTREC公開の「電子政府推奨暗号の利用方法に関するガイドブック」、「CRYPTREC暗号技術ガイドライン(SSL/TLSにおける近年の攻撃への対応)」、「SSL/TLS暗号設定ガイドライン」等に記載がある。これらは、今後、暗号技術の進展や攻撃手法の高度化等に伴って適宜改訂されるほか、SSL／TLSに関する別の新しいガイドラインが適宜作成されることもある。 （参照URL）https://www.cryptrec.go.jp/report.html	意見	SSLに関する記載は、今回の改訂で見直しを行っておりません。ご指摘の内容は、別途議論を得て追記等を行うべきであることから、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
72	122	実5	2	2.「ファイルに対するアクセス制御のため、ネットワーク機器による、IPアドレスやポートのフィルタリング等がある。」とあるが、以降の例示はすべてファイルのアクセス制御である。 例えば、「3. アクセス権限チェックの内容としてxxxx」のように修正することが分かり易いと思われる。	意見	2.については、ファイルに対するアクセス制御の例示となるため、1.の中に記載されるべきものとなります。ここは、ご意見を踏まえ、1.の例示となるよう記載箇所を見直しさせていただきます。	要	
73	123	実6		主たる目的が不正なアクセスや改ざんからのデータ保護ではなく、基本的なデータ品質の確保であると考えられるため、大項目「システムの信頼性向上対策」の中に位置づけた方がよい。	意見	基準によっては、複数の基準大項目に関連するものがありますが、当基準は、データ保護の対策として策定された経緯があり（【技32】）、今回の構成変更において、情報セキュリティ／データ保護に関連する基準として整理させていただきました。従って、原案のままとさせていただきます。	否	
74	126	実8	2.(3)	バイオメトリクスの例示として、①指紋②声紋③掌紋④網膜パターン⑤虹彩⑥筆跡⑦顔とあるが、これに静脈を追記してはどうか。	意見	ここは基準の範囲を見直すこととなるため、原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
75	127	実8	2.(4)	磁気カードは、現状運用で多く利用されていることは理解しつつも、セキュリティ向上を意図してIC化する傾向にあると考えられることから、単一での認証方法としてここで記載することは好ましくない印象がある。	意見	磁気カードは、現状においても多く利用されており、原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
76	129	実8	（参考1） 8	・　項番8では、サーバー証明書の利用が望ましいことと、EVSSL証明書が望ましいことが述べられていますが、平成27年のCRYPTRECの「SSL/TLS暗号設定ガイドライン」では、サーバー証明書の上位の証明書（ルートCA証明書）のセキュリティも重要であることを謳っています。 ――　この背景には、平成23年にオランダの認証局DigiNotarが不正侵入を受け、サーバー証明書が不正に発行されていたことが判明したという事案（この事案はSSL/TLS暗号設定ガイドラインの中で紹介されています。48頁）等があり、ルートCA証明書やそれを発行する認証機関（ルートCA）の信頼性にも配意すべき、という機運が高まったことがあります。 ・　上記の点は、サーバー証明書を適切に使用するうえで重要と思われますので、項番8の現行の記述に以下の文章を追加しては如何でしょうか。 （案） 8. サイト証明書（サーバー証明書） Webサーバーに対して（中略）EV SSL証明書がある。 サーバー証明書の安全性は、それを発行する認証機関の安全性に加えて、上位の証明書（ルートCA証明書）や当該証明書を発行する認証機関（ルートCA）の安全性にも依拠している。そのため、CRYPTRECの「SSL/TLS暗号設定ガイドライン」には、サーバー管理者は、ルートCA証明書やルートCAについても、当該サーバー証明書と同様の安全性を実現するように選択する必要があるとの記載がある。 （参照URL） https://www.cryptrec.go.jp/report/c14_oper_guideline_SSLTLS_web_1_1.pdf	意見	SSLに関する記載は、今回の改訂で見直しを行っておりません。ご指摘の内容は、別途議論を得て追記等を行うべきであることから、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
77	133	実10	2	（本文） 監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とすることが望ましい。 なお、個人データを扱うシステムにおいては、この措置は必要である。 （改正案） 監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とし、迅速に対策を立てられるシステムを導入することが望ましい。 なお、個人データを扱うシステムにおいては、この措置は必要である。 分析・報告には、スピード感が必要であり、検出するだけではなく、対策が重要です。	意見	ご指摘の通り、分析・報告だけではなく、対策を講じることも重要であると認識しておりますが、安全対策の実施として必ずしもシステムを導入するとは限らないことから、原案のままとさせていただきます。また、「対策」の記載を追加すべきかどうかという点については、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
78	140	実14		「外部ネットワークからの不正侵入防止”機能”を設けること」とあるが、以降の適用に当たっての考え方以降の記述では″不正侵入防止策″とある。 対策を求めているのであれば防止策で統一とすることが分かり易いと思われる	意見	ご指摘のとおり、「策」と「機能」が混在している点については、他の基準も含めて統一すべきか検討が必要であると考えております。今後の改訂時に、用語の見直しに関するテーマとして取り上げていきたいと考えております。	否	●
79	152	実20	－	コンピュータウイルス等の不正プログラムへの防御対策に、昨年世界規模で被害が発生したランサムウェアに関する記載がないことから、追加してはどうか。	意見	コンピュータウイルスに関する記載は、今回の改訂で見直しを行っておりません。ご指摘の内容は、別途議論を得て追記等を行うべきであることから、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
80	158	実21	1.(1)	「検知対策としては、以下の例がある。」として、パターンファイルを利用した検知が例示されているが、「振る舞い検知」等の新しい検知技術が普及し始めており、最新の情報を踏まえて記載を見直していただきたい。	意見	検知策については、今回の改訂で見直しを行っておりません。記載内容は、別途議論を得て追記等を行うべきであることから、今回は原案のままとさせていただきます。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
81	165	実26	2	社内で使用するパスワード等について、「適宜変更することが必要」と定めていますが、昨今パスワードの定期変更の有効性に関する議論(*)があるなか、変更を必須という方向性は世間とずれるリスクがあり、「望ましい」とすることが適切ではないでしょうか。 (*)情報セキュリティ対策として定期的なパスワード変更をユーザーに強制するのは、攻撃者にとって推測しやすいものにしてしまう等、逆効果となる場合があるという議論。 ちなみに、NIST（米国国立標準技術研究所）が2017年5月に発行した『電子認証に関する ガイドライン（文書800-63C）』では「ユーザーが攻撃を受けた証拠がある場合を 除き、認証側は定期的にパスワードの変更を求めるべきではない」と明記されている。	意見	現時点では国内において「パスワードの定期的な変更は必要ない」とまで確認されているものではありません。ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
82	172	実31		通常時のオペレーションの教育及び訓練は実31（本基準）、障害時・災害時のオペレーションの教育及び訓練は統16と、別のカテゴリーに位置づけられているが、関連性が強いことから、同じカテゴリー（統制基準・人材（要員・教育））に位置づけた方がよい。	意見	統制基準は、すべての金融情報システムについて共通の対策が記載されているものを選定しております。【実31】は、教育・訓練に関する基準ではあるものの、個別のシステムごとに実施されるものであることから、統制基準には含めておりません。従って、原案のままとさせていただきます。	否	
83	191	実45		「ドキュメントのバックアップを確保すること。」とあるが、災害時の復旧対応が目的の基準であれば、「災害時のドキュメントのバックアップを確保すること。」が分かり易い。 なお、実44が、「運用時のドキュメントの保管管理方法を明確にすること。」という記述になっており、表現のレベルを合わせたほうが良いとも思料。	意見	ご意見を踏まえ、「**災害時の復旧対応に必要なドキュメントのバックアップを確保すること。**」に修正させていただきます。	要	
84	209	実55	適用にあたっての考え方	冒頭に追加された「コンピュータシステムの」が誤りです。当項目は設備管理のためのものであり，「コンピュータシステムの異常を発見するため」のものではありません。 「コンピュータ関連設備の異常状態を早期に発見するため」または旧の「異常状態早期発見のため」のほうがベターです。	意見	読みやすさ対応の一環として「コンピュータシステムの」を追加しておりましたが、ご意見を踏まえ、以下の通り修正させていただきます。 【変更前】 コンピュータシステムの～（以下、略） 【変更後】 コンピュータ**関連設備の**～（以下、略）	要	

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針(案)	原案の 修正要否	継続 検討
85	212	実57	2	「入退資格が付与されている者であっても、夜間、休日の入退館については、入退館者名を入館受付に事前通知することや、入退館記録の事後チェックなど、手続きを明確にしておくことが必要である。」は，「夜間、休日などで、受付者の減少等、入退館管理体制が低くなる」ような環境(一般的なオフィスビルや銀行支店等？)を念頭に書かれていると思われますが，その暗黙の前提の説明が省略されており，読者の誤解を招いています。 「24時間体制で警備員による受付を置いており、入館管理態勢は昼夜で何も変わらない」ようなデータセンタービル等の場合は、無駄な追加措置を求められる事態にもなってしまいます。 例えば以下のように，当項が想定している前提の明示をお願いしたく思います。 「**夜間、休日の入退館管理体制が平日昼間時より低くなる場合は、**入退資格が付与されている者であっても、入退館者名を入館受付に事前通知することや、入退館記録の事後チェックなど、手続きを明確にしておくことが必要である。」	意見	ご指摘にある「夜間、休日」の意味は、定常の勤務時間帯以外、あるいはイレギュラーなタイミングとなり、そういった場合の入退館管理の手続きを明確化しておくことが必要であることを示しております。記載を修正するためには、別途議論を行う必要があると考えており、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
86	229	実69		金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針に基づき、「顧客データ」は、「個人情報」「個人データ」の定義からみて「従業者情報」など範囲が相違することから、上記実務指針の表現に忠実に準拠した表現とした方が良い。	意見	金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針において、「顧客データ」の定義はなされておりません。このため、安対基準では、従来より用語として「顧客データ」を定義しており、実務上の問題は無いものと考えております。従って、原案のままとさせていただきます。	否	
87	234	実71	3	「冗長構成によって信頼性を確保するシステムにおいては、冗長構成の機器が正常に稼動するか確認することが必要」と定めていますが、実施にあたっては大きな負担となることが考えられます。現状では「望ましい」とすることが適切ではないでしょうか。	意見	当該確認については、「定期的に確認する」となっており、かつ対象となる機器及び確認方法についても、金融機関等において判断されることとなります。また、今回の改訂では対策の強度についても見直しを行っていないため、ここは原案のままとさせていただきます。	否	
88	256～ 267	実84～88		日本語的に「～装置には予備を設けること」となるべきところが，多数の箇所で，「～装置は予備を設けること」となっていますので，修正をお願いいたします。 p.244.第1項:「の中核となる重要な本体装置には」 p.247.適用にあたっての考え方および第1項:「重要な周辺装置には」 p.249.適用にあたっての考え方および第1項:「重要な通信系装置には」 p.251.適用にあたっての考え方および第1項:「重要な回線には」 p.255.適用にあたっての考え方および第1項:「端末系装置には」	意見	ご意見を踏まえ、修正させていただきます。	要	
89	268	実89		「必要となるセキュリティ機能を取り込むこと。」とあるが、その他管理策では「機能を設ける」という表現が用いられているため、「必要となるセキュリティ機能を設けること。」 として、表現統一したほうが分かり易いと思われる。	意見	ここではシステム計画段階における品質向上策について記載しており、必要な機能を「取り込む」という表現を使用しております。従って、原案のままとさせていただきます。	否	
90	286 287	実97 実98		ソフトウェア(プログラム)とデータ(ファイル)とは、システム構成する別の要素であり、他の基準とは目的も異なることから、中項目は「ソフトウェアの品質向上対策」ではなく、新たな中項目(例:「データの品質対策」)に分類した方がよい。	意見	基準によっては、複数の基準中項目に関連するものがありますが、ご指摘にある「ソフトウェアの品質向上策」には、ファイル管理に関する基準を含むことから、ご意見を踏まえ、中項目の名称を「ソフトウェア**等**の品質向上対策」に修正させていただきます。	要	
★ 91	287	実98	基準 分類	「ファイル突合機能を設けること」が、基準分類上、「基礎基準」とされた理由を教えていただきたい(重要な情報を取り扱わない簡易なシステムにまでファイル突合機能を設けるのは現実的でないことから、「付加基準」とすべきである)。	意見	関連する基準である、【実97】「ファイルの排他制御機能を設けること」を「付加基準」としていることから、当該基準においても「付加基準」とするのが適当であると判断いたしました。したがって、【実98】については、ご意見を踏まえ、「付加基準」とさせていただきます。	要	
92	314 325 353 465	実112,実118, 実140,設74	(参考5) (参考) 1.(1)③ 1	今回の改訂で金融機関等が実施する対策については、語尾の統一化が図られたが(必須対策は「～必要である」、必須対策に対する代替策は「～可能である」、選択可能な対策は「～望ましい」、「～考えられる」とする)、「実112」の(参考5)、「実118」の(参考)、「実140」の1.(1)③、「設74」の1.については、対策の語尾が「求められる」となっていることから、語尾の統一化を図ってほしい。	意見	【実140】と【設74】以外はすべて参考の文書内(23箇所)であり、ここは対策として記載していないことから、このままとさせていただきます。 また、【実140】は「考えられる」と解釈できるため、語尾を修正させていただきます。 【設74】については、「～維持する機能が**求められるため**、熱源製造部分の～」として修正させていただきます。	要	
93	318	実115	2	「電子メールによる通知時には(中略)なりすまし防止、改ざん防止策を実施することが必要である」と定めていますが、メール送信時のなりすまし、改ざん防止の普及状況は現状ではまだ低いものと考えます。「望ましい」とすることが適切ではないでしょうか。	意見	当該確認については、今回の改訂で見直しを行っていないため、ここは原案のままとさせていただきます。記載を修正するためには、別途議論を行う必要がある考えており、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針(案)	原案の 修正要否	継続 検討
94	324	実118		小項目，適用にあたっての考え方で，「渉外端末」とありますが、下段で「可搬型」と補う構成となり，読みにくい記述方法になっています。以下で良いように思います。 「実118 可搬型渉外端末の運用管理方法を明確にすること。」 「可搬型渉外端末の不正使用を防止するため、運用管理方法を明確にすること。」 「1. 可搬型渉外端末の～」 「2. 可搬型渉外端末には～」 「4. ～可搬型渉外端末の管理者を明確にし、～」 「5. 可搬型渉外端末が～」 「6. 可搬型渉外端末の盗難～」 「9. 可搬型渉外端末～」	意見	渉外端末について基準本文の中に解説しているため、「可搬型」を追記することは不要と考えております。従って、原案のままとさせていただきます。	否	
95	355	実140	参照 法令	「個人情報の保護に関する法律についてのガイドライン」など複数のガイドラインが列挙されているが、ガイドラインは法令ではないため、「参照法令等」としてはどうか。	意見	ご意見を踏まえ、p28基準・解説の記述仕様にある「参照法令」について、「**関連する法令及びガイドライン等**」とさせていただきます。	要	
96	361	設1	（参考）	「全国地震動予測地図（地震調査研究推進本部地震調査委員会・平成22年5月更新）」は、2017年4月に2017年版が公表されていることから、記載を見直してほしい。 また、首都直下地震については、中央防災会議 防災対策推進検討会議 首都直下地震対策検討ワーキンググループより、2013年12月に「首都直下地震の被害想定と対策について（最終報告）」が公表されていることから、記載を見直してほしい。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
97	361	設1	1	全体として「望ましい」項目とされていながら、「立地している場合、または立地せざるを得ない場合は、各種災害及び障害に対する適切な対応策を講ずることが必要である。」と，必要項目に内容が入れ替わっています。 「望ましい」という基本線に合わせるためには，ここもトーンを揃えるべきと思います。	意見	適用区分が「〇」となっているため、必要に応じて取り入れる基準及び解説であることを示しております。（P29参照） 従って、原案のままとさせていただきます。	否	
98	371～ 541	設6 他		「～参照」という記述は項番を降った項目とするのではなく，「設29」や「参照法令」のように「無番+四角枠」に統一するほうが望ましいように思います。	意見	安全対策基準書内の参照箇所については、【XX】という表記にしております。また、参照法令の記載（無番+四角枠）につきましては、本書以外の法令を参照する際の記載としております。ここは、本書記載ルールの通りとさせていただきたく、原案のままとさせていただきます。	否	
99	385	設16	1.(1)	「警備員により入退館者を識別し」→「警備員、および受付システム等により入退館者を識別し」が望ましいと考える。 例示ではあるものの、コストや人不足などの理由により、警備員の代替として無人受付化が進むと考えられる。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
100	385	設16	1.(2)	1. 用語として、分かりづらい表記を修正して欲しい。例として以下表記の方が一般的に理解されると思われる。 ②カードセンサー装置→非接触型カードリーダー ③IC カード･光カード出入管理装置→接触型（挿入型含）カードリーダー また、顔認証装置、静脈認証装置などが一般的に市場に出始めていることから、今後導入される可能性を考慮して追記してはどうか。 2. 磁気カードに関しては、セキュリティ強化策としてIC化が求められる印象があるため、ここでは削除してはどうか。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
101	386	設16	2	データセンター等におけるUSBメモリや各種デバイスの持込・持出し確認ニーズを踏まえ、最新事例として空港等で利用される「ボディスキャナ」を追加してはどうか。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
102	386	設16	1.(1)	インターホンの表現に属すると理解しているが、視認性向上のためカメラ付インターホンのニーズが多いことから、インターホン（カメラ付等）とすることを検討されたい。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
103	385	設16等		設備基準上、「出入管理」と「入退管理」が混在していることから、統一させることが望ましいと考える。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
104	405	設30	3	「誘導灯及び誘導標識の基準（平成13年消防庁告示第39号）」は、2001年以降6回改正されており、最新は「平成27年消防庁告示第3号」であるが、今後も改正が予想されることから、消防庁の「誘導灯及び誘導標識の基準」とし、改正年および消防庁告示番号は記載しない方がよいのではないか。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
105	410	設35	2	「天井ボード等をビス等で固定することが必要である」とありますが，要件は「落下・損壊を防止する対策を行うこと」であり，ビス固定を必須とする表現は踏み込みすぎと思います。 例示に落とすか，または「天井ボードをビスで固定する等の対策を行うことが必要である」程度の表現が正しいように感じます。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
106	413	設36	（参考）	亜鉛ヒゲや消火ガス噴射音のような情報の共有は有益と思いますが，官公庁でない組織からの情報を，FISCのホームページ等ではなく公的な安全対策基準本体に含めることについて疑問があります。 特定団体の部材使用をFISCが公認・推奨していると邪推されることにもなりかねないと思いますので，HPへの移動もしくは設48程度の記述に落とすことをご検討戴ければと思います。 *個人的な意見ですが，フリーアクセスフロアの下は金属線の切片等を含む導電性の塵埃が突風にさらされている環境です。そうしたものへの言及がなく，亜鉛結晶といったレベルのものだけが取り上げられていることには不自然な感覚を持っています。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
107	417	設39	3	「ガス系消火設備」については、2013年11月26日施行の消防庁告示第19号により点検基準等が改正されており、改正内容を踏まえて記載を見直してほしい。 また、「ガス系消火設備」については、ガス系消化設備の放射音がハードディスクドライブに影響を与える可能性が指摘されていることから（2010年9月、日本建築学会大会より「音環境が精密機器に与える影響に関する考察：（その3）不活性ガス消火設備がHDD（ハードディスクドライブ）に与える影響に関する考察」と題する論文が発表されている）、最新の情報を踏まえて記載を見直してほしい。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
108	417 425	設39, 設43		スプリンクラー設備は、水使用設備と同義ではないと思いますが、下記の2基準番号間で矛盾しているように解釈される可能性があります。水使用設備（スプリンクラー設備を除く）等、表現の補記を検討いただけますでしょうか。 設 39（消火設備を設置すること。）では2.で「スプリンクラー設備も効果的」 とされている。 設 43（水使用設備を設置しないこと。）では 「漏水によるコンピュータシステムへの影響を防止するため、コンピュータ室・ データ保管室に水使用設備を設置しないこと。」とされているが、	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
109	426	設44	2	「設定された規模以上の地震に対して音、ランプによる警報を発し」とありますが，その必要はないように感じます。 周知方法は個々の管理形態や常時監視者の有無等によって決まる問題であり，例示に落とすべきと思います。	意見	適用区分が「〇」となっているため、必要に応じて取り入れる基準及び解説であることを示しております。（P29参照） 従って、原案のままとさせていただきます。	否	
110	426	設44	適用にあたっての考え方，3(2)	地震感知器の設置場所で，「コンピュータ室には」「コンピュータ室内またはその近くに」の記述がありますが，より加速度の大きい階に設置して管理しているビル等もあります。 要件としては地震に即応できる態勢とそのための測定機の話なので，場所を「室内」を中心にして要求する必要はないように思います。	意見	適用区分が「〇」となっているため、必要に応じて取り入れる基準及び解説であることを示しております。（P29参照） 従って、原案のままとさせていただきます。	否	
111	432 ～ 435	設50，設51	【資料3】	枝葉の話ですが，2400feet MTのような図があるため，そろそろカートリッジテープやディスク媒体の図に差し替えても良いのでは，とは思いました。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●

No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
112	450	設64	1	「自家発電設備の構造、性能等については、商用電源が停電した場合に自動的に電圧確立および投入が行われるまでの所要時間は40秒以内とされるなど、自家発電設備の基準(昭和48年消防庁告示第1号)において定められている。」とあります。 確かにこちら http://www.fdma.go.jp/concern/law/kokuji/hen52/52030104010.htm にその記述はあるのですが，但し書きには「ただし、常用電源の停電後四十秒経過してから当該自家発電設備の電圧確立及び投入までの間、蓄電池設備の基準（昭和四十八年消防庁告示第二号）の規定（同告示第二第一号(七)を除く。）に適合する**蓄電池設備により電力が供給されるものにあつては、この限りではない。**」ともあります。 この蓄電池の記述が設64には反映されておらず，「すべての発電機で，40秒以内の電圧確立が必要である」と誤解される表現になっています。 また，そもそもこれは消防・防災系の自家発電機の話であり，もし，評価対象の発電機が電算システム専用の場合は，その縛りすらないように思います。 以上を前提に，**記述の見直し**をいただければと思います。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
113	506	設109	1	「太陽光発電等の代替エネルギーシステムの活用を含め」は1項の本質と関係ない主観的な意見であり，不要です。発電方式は負荷や給電要件にのみ基づいて定められるべきであり，自家発電の主力方式ではない太陽光発電をあえて明示することは，安全対策やセキュリティの文書として正しくありません。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
114	512	設113	4	「店舗外ブース 店舗外ブースは、～」の冒頭のタイトルは他の記述と表現を揃えると不要なように思います。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
115	517	設117	1,2	設113と同様に，以下の冒頭のタイトル部分（「自動運行設備　　ここでいう」「遠隔監視設備」）は不要なように思います。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
116	518	設117	2	安全対策基準の改訂の対象外に関する意見であり、ご参考までに表明するものです。 ・「遠隔監視設備」として、「無人運用を行う場合には、運用状況を監視するため、管理センター等に遠隔監視設備を設置する必要がある」と記載されていますが、「遠隔監視」については、外部のネットワークから不正侵入され、監視カメラの映像等が外部に漏洩する事案が近年多数発生しています。 　こうした状況を受けて、総務省と経産省は、IoTセキュリティガイドラインを平成28年7月に策定・公表しています。 ・　こうした点を踏まえ、遠隔監視設備の安全対策として、例えば、以下の文章を追加しては如何でしょうか。 （案） 無人運用を行う場合には（中略）する必要がある。 遠隔監視設備に関しては、外部のネットワークと接続されている場合、当該ネットワークから不正侵入され、防犯カメラの映像等のデータが盗取されたり、各種装置が不正に操作されたりするリスクが存在することを認識する必要がある。そのうえで、平成28年7月に総務省・経済産業省が公表した「IoTセキュリティガイドライン ver 1.0」等を参照しつつ、当該リスクを評価し、それに応じた対策を検討することが必要である。 （参照URL）http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf	意見	ご指摘については、金融機関等においてどの程度の影響があり、どういった対策をすべきかといった議論を経たうえで、基準への記載内容を検討すべきと考えております。ここは、設備基準に対する他の意見と同じく、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
117	519	設118	1.(1)①	「キャスタホルダー」については、「設118」の図1および411頁の図1で「キャスタホルダ」としているため、表記を統一してはどうか。	意見	設備基準については、改めて内容の見直しについて議論したうえで修正すべきことから、ご指摘の点は、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●
118	543	監1	3	監査に個別論を記述せず、「システム監査指針」参照とする方が良い。また、生体認証の外部監査は、スリーラインズオブディフェンスの第1線または第2線が導入すべきものであり、第3線（内部監査）はその実施方法、内容の妥当性を評価する役割であることを明記した方が良い。	意見	システム監査の実施にかかる詳細な事項等については、「金融機関等のシステム監査指針」等を参照することでよいと考えておりますが、システム監査体制の整備については、安全対策上必要なものとして、従来より安全対策基準の中の1基準として位置付けております。従って、原案のままとさせていただきます。	否	

	No.	頁	記載箇所 基準番号	項番	ご意見の概要	区分	対応方針（案）	原案の 修正要否	継続 検討
	119	543	監 1	－	「システム監査体制を整備すること」を監査基準とした理由を教えていただきたい（「監1」の内容は、内部統制の体制整備に関する事項であり、統制基準に記載すべきである）。	意見	内部の統制の状況についても監査の対象となることから、統制基準からは分離・独立した位置付けとさせていただきました。従って、原案のままとさせていただきます。	否	
	120	543	監1	3	システム監査の実施手段の1 つとして、内部者による監査に加え、外部の専門機関を活用することが望ましい。特に機微（センシティブ）情報を取り扱う場合は、外部の専門機関を活用することが望ましい。なお、機微（センシティブ）情報に該当する生体認証情報を取り扱う場合は、より客観性が求められることから、外部の専門機関を活用することが必要である。 ⇒特に機微（センシティブ）情報を取り扱う場合は、専門的能力を有する要員を活用することが望ましい。（なお以下は削除） ＊外部の専門機関活用ありきのように読めてしまうが、内部にも専門的能力を有する要員がいるケースもある。「専門的能力を有する要員の活用」が主旨であると思われる。 そもそも監査部門は独立性、監査人は客観性が求められているのであって、より客観性が求められるからと言って、生体認証情報を取り扱う場合には外部の専門機関の活用を必須とするのは、いかがなものか。	意見	ご指摘の点については、現在の安対基準（【運91】）に記載されている内容から変更を行っていません。『金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（7-2）』でも、「機微(センシティブ) 情報に該当する生体認証情報の取り扱いに関し、外部監査を行う」とされております。従って、原案のままとさせていただきます。	否	
★	121	543	監1	4	また、改善策の実施状況について、定期的にフォローアップすることが望ましい。 ⇒定期的にフォローアップする必要がある。 ＊IIA基準（内部監査の専門職的実施の国際基準）においても、「内部監査部門長は、・・・フォローアップ・プロセスを構築しなければならない。」としている。指摘した以上、フォロアップする必要がある	意見	ご指摘の点は、今後の監査指針の改訂の結果を踏まえ、改訂させていただきたいと考えております。	否	●
	122	544	監1	5.(1) （注1）	原案記載の、監査人の選定要件は、システム監査指針第3版では「必要である」とされています。これは、金融機関にとって、利益相反に疑義が生じる外観を呈しないために「必要である」とされたものと理解しており、原案のように例示として「考えられる」に留められたのは、どのような経緯からでしょうか。	意見	今回の改訂では、「例がある」の中に「必要がある」と記載された部分については、解釈の曖昧さを排除するため、語尾を「する」または「考えられる」としております。ご指摘については、今後の監査指針の改訂の結果を踏まえ、今後の改訂時の検討テーマとして取り上げていきたいと考えております。	否	●

【資料２－１】
平成 30 年 2 月 23 日
公益財団法人 金融情報システムセンター

安全対策基準（第９版）の発刊等について

１．安全対策基準（第９版）の発刊について

会員意見への対応方針に基づく所要の修正を行ったうえで、『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（第９版）という）』を発刊することをご承認いただきたい。

また、今回の作成範囲における参考文献等の最新化や誤字・脱字等、軽微レベルの字句・語句の修正については、事務局の判断にて適宜行うこととするので、併せてご承認いただきたい。

なお、発刊等の予定は以下のとおりである。

・平成 30 年３月　当センターHP 上にて PDF 版の公開（会員向け）
・　　５月　冊子の発刊
・　　７月　ガイドライン検索システムのリリース

２．「安全対策基準ＦＡＱ」の運用開始について

今後、安全対策基準（第９版）に対して会員から質問が寄せられることが考えられるが、それらの質問と回答については、広く情報共有することが有益であるため、当センターHP（会員用）上に「安全対策基準 FAQ」を開設し、会員からの意見と回答を掲載する予定である。

３．安全対策基準（第９版）の普及推進について

当センターでは、平成 30 年度に安全対策基準（第９版）の普及推進活動を行う予定である。平成 30 年６月より全国説明会を実施し[1]、同年８月以降、地区別セミナーのメニューに安全対策基準（第９版）の解説を追加する予定である。

以上

[1] 全国説明会では、『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』についても講演を行う予定である。