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　議事次第

Ⅰ　日時

平成 29 年 10 月 17 日（火）　15:00～17:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．	15:00	開会
		次第説明・専門委員会の今後の予定について
２．	15:10	【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
３．	15:30	【議案２】「読みやすさ対応」について
４．	15:50	【議案３】外部委託管理関連基準の改訂について
５．	16:20	【議案４】前説原案について
６．	16:50	事務連絡（事後意見・委員会開催日程について）
		委員登録内容変更届の提出依頼について（該当委員のみ）
７．	17:00	閉会

Ⅳ　資料

【資料０－１】　安全対策専門委員会　今後の予定について
【資料１－１】　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
【資料１－２】　基礎基準に対する各委員からのご意見・対応方針
【資料１－３】　付加基準追加候補
【資料１－４】　新基準構成案
【資料１－５】　改訂原案
【資料２－１】　読みやすさ対応について
【資料２－２】　読みやすさに対する各委員からのご意見・対応方針
【資料２－３】　「重要である」を含む基準一覧
【資料２－４】　前文の構成・変更内容
【資料２－５】　安全対策基準一覧表（原案）
【資料３－１】　外部委託関連基準の整理方針について
【資料３－２】　外部委託関連基準に対する各委員からのご意見・対応方針
【資料３－３】　改訂原案
【資料４－１】　前説原案の修正内容について
【資料４－２】　前説に対する各委員からのご意見・対応方針
【資料４－３】　改訂案２（前説Ⅰ・Ⅱ）
【資料４－４】　改訂原案（前説Ⅲ（利用にあたって））
【資料５－１】　検討事項に関するご意見（メール回答用）

Ⅴ　今後の予定

○第 59 回　安全対策専門委員会
（予定）平成 29 年 11 月 21 日（火）15:00～17:00　FISC 会議室

以上

【資料0－1】
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

安全対策専門委員会　今後の予定について

		基礎基準の整理		読みやすさ対応			外部委託基準の統合・整理		前説	
		考え方の整理	基礎基準の確定	基準の再構成	読みやすさ向上	統制基準の再編・見直し	考え方の整理	基準原案確定	（概要・フレームワーク）	（利用にあたって）
第54回	7/11	方針の説明 （事後意見7/18締切）	事務局案提示						（ご意見募集）	
第55回	8/8	方針の説明 （事後意見8/22締切）	委員意見反映版の提示	方針の検討			方針の検討 （事後意見8/22締切）		（ご意見募集）	
		（各委員訪問・考え方意見交換）			原案確認依頼 メール送付（8/30）		（各委員訪問・原案説明）			
第56回	9/12	方針の説明 （事後意見9/22締切）	委員意見反映版の提示	構成案の検討	↓	基準原案の検討 （事後意見9/22締切）	方針の検討 （事後意見9/22締切）	原案確認依頼 （事後意見9/22締切）	（ご意見募集）	
					原案確認依頼 （9/29締切）					
第57回	10/17	ご意見に対する回答案提示 考え方の確定（承認）	基礎基準（最終案）提示 （事後意見10/31締切）	構成案の検討 （事後意見10/31締切）	ご意見に対する 修正方針の説明		ご意見に対する回答案提示 方針の確定（承認）	原案修正方針の説明 原案の提示	原案修正内容説明 （事後意見10/31締切）	原案説明 （事後意見10/31締切）
			（各委員訪問・意見交換）		原案確認依頼 （10/23までにメール送付）			↓	（各委員訪問・原案説明）	
					↓			↓		
					原案確認依頼 （10/31締切）			原案確認依頼 （10/31締切）		
事前 送付	11/14		構成案（最終）の送付		基準原案（最終）の送付			基準原案（最終）の送付	原案（最終）の送付	
第59回	11/21		構成案の確定（承認）		基準原案の確定（承認）			基準原案の確定（承認）	原案の確定（承認）	
会員意見募集		会員意見募集（11/28～1/12）								
第60回	*/*	会員意見結果の確認・回答案（原案修正方針）の検討								
		発刊承認								

会員意見募集はある程度の期間が必要となるため、1.5か月間で設定している。

→各委員や会員への事前説明の期間を取り、第60回で内容を確定させる予定である。
（従って、開催時期は２月とする予定）

※第58回安全対策専門委員会はＩＴ人材手引書のみ開催予定（書面開催）

【資料１－１】
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

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

Ⅰ. 前回提示した論点

論点１	「基礎基準」や「付加基準」において、「解説部分」で「必要である」と記載されている対策をすべて各基準の「必須対策」と位置付けて良いか。
論点２	「解説部分」で「望ましい」と記載されている対策、例示されている対策は、すべて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位置付けて良いか。
論点３	「基礎基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されているものがあるが、その取扱いをどうするか。
論点４	「基礎基準」の候補のうち、個別のシステムや業務に関する基準は、すべ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」と位置付けることとしてはどうか。
論点５	「付加基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されているものがあるが、その取扱いをどうするか。

Ⅱ. 方針案

前回の専門委員会において提示した論点に対する事後意見（別紙【資料１－２】「基礎基準に対する各委員からのご意見・対応方針」参照）を基に、各論点の方針案を以下のとおりとする。

※「論点３」から「論点５」の対象基準は、【参考】「検討対象基準」を参照。

1. 「論点１」について

「基礎基準」や「付加基準」において、「解説部分」で「必要である」と記載されている対策をすべて各基準の「必須対策」と位置付ける。

2. 「論点２」について

「解説部分」で「望ましい」と記載されている対策、例示されている対策は、すべて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位置付ける。

3. 「論点３」について

「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一する。

・ 「付加基準」とすることで「解説部分」に「必須対策」が示されていない基準は、「論点５」の方針とする（実 51、実 106、実 117）。修正した原案は、別紙【資料１－５】「改訂原案」を参照。

4. 「論点４」について

個別のシステムや業務に関する基準は、すべ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」と位置付ける。

5. 「論点５」について

「適用に当たっての考え方」の文末を「～すること」に修正する。そのうえで、「解説部分」に「必須対策」が示されていないもの（「望ましい」または例示のみを記載）は、そのままの表現する。（ベストプラクティスのみの基準とする）。

III. 論点

1. 論点１：「実 13」基準の見直しについて

【主なご意見】

「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」という記述がありますが、記述された時点でホストシステムに対する対比の上でクライアントサーバーという記述がなされたと思われます。現在では、ほとんどのシステムが分散型のいわゆるクライアントサーバー・システムとして動作しており、「実 13」の内容をみると今日では通常の運用内容として常識的に実施されている内容かと思われます。よって、「Ⅱ.実務基準 3 運行管理」の中扉にクライアントサーバー・システムを含む旨の記載を記述し、「実 13」を削除する、あるいはクライアントサーバーの記述についての見直しを提案します。

○ 対応案

当該基準の対策の目的と同一の基準（「実 10」「実 11」「実 12」）に統合のうえ「実 13」基準を廃止する。なお、安全対策基準で示すコンピュータシステムの定義に、クライアントサーバーが含まれるように用語解説を修正する。

2. 論点２：「Ⅱ.方針案　4.」に基づく「付加基準」の追加候補について

事後意見に基づき、以下の基準を追加で「基礎基準」から「付加基準」へ変更する。基準原案は、別紙【資料１－３】「付加基準追加候補」を参照。

基準中項目	番号	基準小項目
インターネット・モバイルサービス	実 34	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。
顧客データ保護	実 46	生体認証における生体認証情報の安全管理措置を講ずること。
予防策（ｱｸｾｽ権限確認）	実 126	生体認証の特性を考慮し、必要な安全対策を検討すること。

3. 論点３：「基礎基準」の選定について

「Ⅱ.方針案」及び事後意見に基づき「基礎基準」案を更新。別紙【資料１－４】「新基準構成案」を参照

＜参考＞基準の内訳

内訳		今回※	前回
基準総数		**168**	162
	基礎基準	**103**	115
	付加基準	**65**	47

※前回未反映だった外部の統制（基礎基準）が反映されたため総数増加。

Ⅳ. 今後の予定

本日ご説明した上記論点について、10/31（火）までに事後意見をいただきたい。事後意見をもとに原案等の修正を行い、次回委員会において修正原案を提示し、「基礎基準」を確定する。

日程（予定）	内容
10 月 17 日（火）	第 57 回安全対策専門委員会審議（本日論点説明）
10 月 31 日（火）	第 57 回専門委員会事後意見の締切
11 月 21 日（火）	第 59 回安全対策専門委員会審議

以　上

【参考】検討対象基準

（論点３）:「基礎基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されている基準

番号	基準小項目
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。
実 51	ネットワーク関連機器の保護措置を講ずること。
実 106	オペレーションの自動化、簡略化を図ること。
実 117	相手端末確認機能を設けること。
実 118	蓄積データの漏洩防止策を講ずること。
実 119	伝送データの漏洩防止策を講ずること。
実 123	伝送データの改ざん検知策を講ずること。
実 131	カードの偽造防止対策のための技術的措置を講ずること。
実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。
実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

（論点４）:「基礎基準」の候補のうち、個別のシステムや業務に関する基準

基準中項目	番号	基準小項目
渉外端末	実 41	運用管理方法を明確にすること。
カード管理	実 42	カード不正使用を防止すること。管理方法を明確にすること。
ｲﾝﾀｰﾈｯﾄ、ﾓﾊﾞｲﾙ	実 84	不正使用を防止すること。
	実 85	不正使用を早期発見すること。
予防策（不正・偽造防止策）	実 131	カードの偽造防止対策のための技術的措置を講ずること。
	実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。
	実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

（論点５）:「付加基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されている基準

番号	基準小項目
実 86	インターネット・モバイルサービスの安全対策に関する情報開示をすること。
実 96	回線の予備を設けること。
実 115	バックアップサイトを保有すること。

【資料１－２】
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

■改訂原案（基礎基準）に対する各委員からのご意見（対応方針）

No.	カテゴリー	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	原案反映 No
1	「解説部分」の位置付け	Ⅱ．方針案	（1ページ目下段の表） リスクベースアプローチの考え方からすると、「付加基準」には「必須対策」〇を設けるべきではなく、選択的に適用する基準と位置付けたほうがよいと思われる。	三井住友海上火災保険 中川様(検)	特定システムの場合には、付加基準は原則として適用となるため、必須対策を明確にしておく必要があります。従って、付加基準についても「必須対策」が必要と考えます。 そのうえで、方針案、特定システム、通常システムへの基準の適用方法の説明を以下の通り再整理したいと考えております。 ＜方針案＞ 「基礎基準」の「解説部分」の、全ての金融情報システムにおいて適用さ れるべき最低限必要な対策を「必須対策」と呼ぶ。具体的には、「必要である」と 記載されている対策を「必須対策」とする。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする。 「付加基準」の「解説部分」の中で、当該基準を適用する場合に必須となる対策 を「付加基準」の「必須対策」と呼ぶ。具体的には、「必要である」と記載されて いる対策を「必須対策」とする(特定システムでは、「付加基準」の「必須対策」 は、必ず適用されることとなる)。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする。 この結果、特定システム、通常システムへの基準の適用方法は、下表のとおりとなる。 ・「〇」は、適用。 ・「△」は、選択的に適用。 なお、以下を本文や表の脚注および前説「Ⅰフレームワーク1.総論 (4) 安全対策決定のプロセス」に記載したいと考えております。 　システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。 　また、「必須対策」には、「重要度を勘案し、個人データ等を扱うシステムの場合等には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。	要	【資料１－５】 改訂原案 前説 (2) 基準の分類 (4)安全対策決定のプロセス ③安全対策の目標設定
2	「解説部分」の位置付け	Ⅱ．方針案	方針案で、 ・「基礎基準」の「解説部分」の、全ての金融情報システムにおいて適用さ れるべき最低限必要な対策を「必須対策」と呼ぶ。具体的には、「必要である」と 記載されている対策を「必須対策」とする。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする。 ・「付加基準」の「解説部分」の中で、当該基準を適用する場合に必須となる対策 を「付加基準」の「必須対策」と呼ぶ。具体的には、「必要である」と記載されて いる対策を「必須対策」とする(特定システムでは、「付加基準」の「必須対策」 は、必ず適用されることとなる)。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする。 と記載されているのに、下段の表で、下記赤字部分が反する事を記載しており、方針がぶれてる印象 この結果、特定システム、通常システムへの基準の適用方法は、下表のとおりとなる。 ・「〇」は、適用(ただし、システムの特性等から適用する必要がない、あるいは適 用できない場合には、適用は不要)。 ・「△」は、選択的に適用。	日本アイ・ビー・エム 鎌田様(検)	No.1と同様	要	【資料１－５】 改訂原案 前説 (2) 基準の分類 (4)安全対策決定のプロセス ③安全対策の目標設定
3	「解説部分」の位置付け	論点１	基本的な考え方は、提案の内容でよいと思われる。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、「基礎基準」や「付加基準」において、「解説部分」で「必要である」と記載されている対策をすべて各基準の「必須対策」と位置付けたいと考えております。	要	【資料１－５】 改訂原案 前説 (2) 基準の分類
4	「解説部分」の位置付け	論点２	基本的な考え方は、提案の内容でよいと思われる。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、「解説部分」で「望ましい」と記載されている対策、例示されている対策は、すべて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位置付けたいと考えております。	要	【資料１－５】 改訂原案 前説 (2) 基準の分類
5	「解説部分」の位置付け	実68	「当該コンピュータシステムの重要度を考慮し」と言ってしまうと、それ自体がリスクベースになり、基礎基準にそぐわないのではないか?	農林中央金庫 常岡様(専) 今嶋様(検)	「読みやすさ」の対応に基づく、変更、修正にあたっては、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ことを前提としており、原案のままとさせていただきたいと考えております。なお、「必須対策」においても一定の条件の下において適用されることを明確に示す必要があると考え、NO．１で記載した修正を行うこととします。	要	【資料１－５】 改訂原案 前説 (4)安全対策決定のプロセス ③安全対策の目標設定

No.	カテゴリー	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	原案反映 No
6	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実118	この基準だけでなく、全体的に言えることであるが、「適用にあたっての考え方」の表現と、その後に続く本文の記述は、「読みやすさ」の観点から表現をあわせることが望ましいのではないか。 例えば、本基準の場合、「適用にあたっての考え方」に「重要なデータについてはデータ保護の対策を講ずること」とあるので、そのあとの本文部分1．においては「暗号化することが望ましい」ではなく、「データ保護の対策を講ずること」とするのが、文章として自然である。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、以下のとおり修正いたしました。 1．ファイルの不正コピーや盗難の際にも、データの内容がわからないようにするため、重要なデータについてはデータ保護の対策を講ずることが必要である。 「実119」も同様の考え方で、以下のとおり修正いたしました。 1．データ伝送時に盗聴された場合にもデータの内容がわからないようにするため、重要なデータについては、データ保護の対策を講ずることが必要である。	要	【資料1－5】 改訂原案 実118 実119
7	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実131	サブタイトル中に「望ましい。」の表記が残っている。 キャッシュカードにかかる基準であり，付加基準としたうえで，基本的には語尾を「必要である。」として，付加基準の必須対策と位置付けることが適当と思料。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	要	【資料1－5】 改訂原案 実131
8	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実134	サブタイトル中に「望ましい。」の表記が残っている。 電子メールの送受信やホームページの閲覧にかかる基準であり，付加基準とすることが適当と思料。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	要	【資料1－5】 改訂原案 実134
9	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実106	【資料1-1 p.1～2、資料1-3 p.3～5】 ・「オペレーションの自動化、簡略化」については効率化の観点となるため、要件でなく、ベストプラクティスとした方が望ましいと思います。	NTTデータ 鎌田様(専) 鈴木様(検)	ご意見を踏まえ、「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一したいと考えております。	要	【資料1－5】 改訂原案 実106
10	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	論点3	「基礎基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されているものの取り扱いについては、現行基準への既存対応を考慮すると案1のとおり「付加基準」とするべきである。なぜならリスクベースアプローチの考え方で採用せずと判断できるものが、すべて必須対策となってしまいかねない。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一したいと考えております。	要	【資料1－5】 改訂原案 実51、実106、実117、実118、実119、実123、実131、実132、実134
11	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	論点5	「付加基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されているものの取り扱いについては、ご提案の通り、リスクベースアプローチで考えるなら「望ましい」の表現そのままのほうがよい。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、「適用に当たっての考え方」の文末を「～すること」に修正したうえで、「解説部分」に「必須対策」が示されていないもの（「望ましい」または例示のみを記載）は、そのままの表現したいと考えております（ベストプラクティスのみの基準とする）。	要	【資料1－5】 改訂原案 実86、実96、実115
12	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実106	サブタイトル中に「望ましい。」の表記が残っている。 内容は「望ましい。」ものであり，付加基準とすることが適当ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一したいと考えております。	要	【資料1－5】 改訂原案 実106
13	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実117	サブタイトル中に「望ましい。」の表記が残っている。 内容は「望ましい。」ものであり，付加基準とすることが適当ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一したいと考えております。	要	【資料1－5】 改訂原案 実117
14	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実119	サブタイトル中に「望ましい。」の表記が残っている。 内容は「望ましい。」ものであり，付加基準とすることが適当ではないか。 オープンネットワークを介する場合には，暗号化は必須（付加基準の必須対策）と言えるが，見落としがちな記載になる可能性があり，表記上は工夫が必要とも考えられる。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一したいと考えております。	要	【資料1－5】 改訂原案 実119
15	「適用にあたっての考え方」が「望ましい」と記載されている基準の扱い	実123	サブタイトル中に「望ましい。」の表記が残っている。 他の基準との比較。記載された文言からは，付加基準とすることが適当と思料。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「付加基準」として位置づけたうえで、「適用にあたっての考え方」の末文「望ましい」は、「～すること」に統一したいと考えております。	要	【資料1－5】 改訂原案 実123
16	基準の廃止	実13	該当箇所と意見 「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」という記述がありますが、記述された時点でホストシステムに対する対比の上でクライアントサーバーという記述がなされたと思われます。現在では、ほとんどのシステムが分散型のいわゆるクライアントサーバー・システムとして動作しており、実13の内容をみると今日では通常の運用内容として常識的に実施されている内容かと思われます。よって、「Ⅱ.実務基準 3 運行管理」の中扉にクライアントサーバー・システムを含む旨の記載を記述し、実13を削除する、あるいはクライアントサーバーの記述についての見直しを提案します。	アマゾンウェブサービスジャパン 梅谷様(専)	ご意見を踏まえ、「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」は削除し、「実10」「実11」「実12」に統合する方向で検討したいと考えております。	要	【資料1－5】 改訂原案 実10、実11、実12
17	基準の廃止	実13	本基準については、廃止してよいのではないか。 （理由） データ、プログラムのバックアップ等の運用については、【運】に照らして管理可能であり、あえてクライアントサーバー・システムに特化した基準を設ける必要性はないため。	日立製作所 宮崎様(検)	No.24と同様	要	【資料1－5】 改訂原案 実10、実11、実12

No.	カテゴリー	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	原案反映 No
18	基礎基準の追加	実23	運用管理のドキュメントの管理方法の基準であるが、「実64」のシステムドキュメントの管理方法の基準との違いは、開発と運用での引き渡しをしなさいという点だと思料。基準としてはまとめてはどうか。「実24」では運用管理ドキュメントとシステムドキュメントを統合して記載されている。「実64」は付加基準であるが、「実23」は基礎基準となっている。「実64」についても基礎基準としてはどうか（まとめたうえで基礎基準で良いのではないか）。	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、「実64」はシステムの運行管理に最低限必要な基準として「基礎基準」とさせていただきたいと考えております。 「実23」と「実64」の統合につきましては、当該基準は運用工程と開発工程としてすみ分けられているため、「使いやすさ」の観点から、原案のままとさせていただきたいと考えております。	要	【資料１－４】 新基準構成案 実64
19	基礎基準の追加	実52	付加基準とされているが，機器の保守については，何らかの対処はすべきであり，基礎基準としたうえで，記載ぶりを工夫した方が良いのではないか。	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、システムの運行管理に最低限必要な基準として「基礎基準」とさせていただきたいと考えております。	要	【資料１－４】 新基準構成案 実52
20	個別のシステムや業務に関する基準の位置付け	論点４	「基礎基準」の候補のうち、個別のシステムや業務に関する基準は、すべ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」と位置付ける、との考え方はよいと思われる	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	否	
21	個別のシステムや業務に関する基準の位置付け	論点４	今回、インストアブランチやATMなど個別機能にかかる部分は、付加基準と位置付けられている。勘定系システム以外の情報システムを対象とする基準とするという趣旨からは一層の付加基準へのシフトが適当と考えられる。	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	否	
22	個別のシステムや業務に関する基準の位置付け	実34	「口座開設等を行う場合は，本人確認を行うこと。」については，勘定系システム等，限定的なシステムを対象とする基準であり，付加基準とすべきではないか。	農林中央金庫 常岡様(専) 今嶋様（検）	本基準は、インターネット・モバイルサービスの口座開設等を行う場合の本人確認に関する基準であるため、個別のシステムや業務に関する基準として「付加基準」と位置付けたいと考えております。なお、こうした内容であることを明確化するために、基準の大・中・小項目を修正しました。	要	【資料１－３】 付加基準追加候補 実34
23	個別のシステムや業務に関する基準の位置付け	実42	「カードの管理方法を明確にすること。」について，「キャッシュカード等の管理方法を・・・」としたうえで，付加基準となるのではないか。	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。ただし、安対基準に該当するカード類は、数多くあるため、原案のままとさせていただきたいと考えております。	否	
24	個別のシステムや業務に関する基準の位置付け	実46	「生体認証における生体認証情報の安全管理措置を講ずること。」については，生体認証情報を活用する場合であり，付加基準ということではないか。	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	要	【資料１－３】 付加基準追加候補 実46
25	個別のシステムや業務に関する基準の位置付け	実84	インターネット・モバイルサービスを提供する場合であり，付加基準とすることが適当ではないか（実85も同じ）	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	否	
26	個別のシステムや業務に関する基準の位置付け	実103	パッケージを導入する際の基準であり，付加基準とすることが適切ではないか。	農林中央金庫 常岡様(専) 今嶋様（検）	パッケージ導入は、システム運用における通常業務としての性質が強いと判断し、個別のシステムや業務に関する基準とせず、システム全般的な運用に関する基準としたいと考えます。したがって、原案のままとさせていただきたいと考えております。	否	
27	個別のシステムや業務に関する基準の位置付け	実104	営業店新設，機器増設時の定型的変更作業時の基準ということであれば，付加基準で良いのではないか。	農林中央金庫 常岡様(専) 今嶋様（検）	営業店新設、機器の増設等は、定型的変更作業の例であり、当該基準はパラメータ設定等の変更作業の管理を目的とした基準のため、営業店新設等の個別業務の基準と誤認されないよう修文したうえで、個別のシステムや業務に関する基準とせず、システム全般的な運用に関する基準としたいと考えます。したがって、原案のままとさせていただきたいと考えております。	否	
28	個別のシステムや業務に関する基準の位置付け	実126	生体認証を活用する場合の基準であり，付加基準とすることが適当と思料。	農林中央金庫 常岡様(専) 今嶋様（検）	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	要	【資料１－３】 付加基準追加候補 実126
29	個別のシステムや業務に関する基準の位置付け	論点４	賛同します。基本的に業務の特性が強いものは、なるべくすべて付加基準として金融機関自らが実施すべき統制として選択するほうが、サービス利用にあたっての検討や考慮点が明確化され、結果としてリスクを正しく把握し、コストを適切にリスクコントロールに反映できるため、長期的なリスクへの投資のコミットが期待できることになると思われます。	アマゾンウェブサービスジャパン 梅谷様(専)	ご意見を踏まえ、個別のシステムや業務に関する基準は、すべ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」と位置付けたいと考えております。	否	

個別業務・サービス	適用区分					基準分類
	共	セ	本	提	ダ	
インターネット・モバイルサービス			◎			付加

削除: システムの利用

削除: 厳正な本人確認の実施

削除: 基礎

実 34	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。

書式変更: インデント : 最初の行 : 0 mm

不正取引防止のため、口座開設等を行う場合は適切な方法により本人確認を行うこと。

1. インターネットバンキング等の非対面取引において、口座開設等を行う場合は不正取引防止のために、以下の手順等により本人を確認することが必要である。
   (1) 公的証明書の原本またはコピーの送付を受ける。
   (2) 顧客の住居に取引関連書類（キャッシュカード等）を書留郵便等で返送する。

2. 利用者からの暗証番号等の照会において、対面・非対面にかかわらず、十分な本人確認ができない場合には、直ちに回答するのではなく、別途、登録されている顧客情報をもとに、金融機関から電話連絡や書留郵便等の手段で本人であることを確認したうえで、回答する必要がある。

   不正取引を防止する策については、【運 103】を参照のこと。

参照法令	犯罪による収益の移転防止に関する法律 （旧 金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律）

システムの利用
顧客データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					付加

削除: 基礎

実 46	生体認証における生体認証情報の安全管理措置を講ずること。

顧客データを保護し、適正に利用するため、生体認証情報を安全に管理するための手順を定めること。

1. 生体認証情報を取り扱う各段階について、安全に管理するための手順を定めることが必要である。
   各段階において、取扱者は必要最小限に限定することが必要である。【運 53】を参照のこと。

   本項の対象となる生体認証と生体認証情報は、以下のとおり。
   生体認証・・・
   　生体認証情報を、本人の同意に基づき用いて、本人確認手段として実施する機械による自動認証。
   生体認証情報・・・
   　機械による自動認証に用いられる身体的特徴の情報のうち、非公知の情報を、コンピュータ等で扱えるデータに変換したもの。
   　（ここで身体的特徴の情報は、「金融分野における個人情報保護に関するガイドライン」第 5 条の機微（センシティブ）情報に該当するもの。）
   　（注１）①生体認証情報の例としては、静脈・虹彩等がある。
   　②一方、公知な情報としては、一般的な顔写真等があげられる。（ただし、医療用に撮影された顔写真等は除く）
   　③行動的特徴（キーストローク、筆順、筆速、筆圧、声紋等）は、非公知であるとしても、身体的特徴の情報ではないため、本基準でいう生体認証情報には含まない。
   　（注２）一般的に、「個人の身体的特徴及び行動的特徴を識別情報とした本人確認技術」や「身体的特徴及び行動的特徴の情報そのもの」を「バイオメトリクス」と呼ぶことがある。本項目においては、この概念から対象を上記のとおり絞って、「生体認証」及び「生体認証情報」という用語を用いる。

(1) 取得

①顧客の同意

事前に金融機関等は、顧客に対し、生体認証情報の利用目的、利用範囲、生体認証のシステム利用手順等について説明し、顧客より同意を得ることが必要である。

本人の同意に基づかない、もしくは、本人確認の目的以外で、生体認証情報を取得することは、「金融分野における個人情報保護に関するガイドライン」第 5 条に反する。

②厳正な本人確認の実施

生体認証に使用する生体認証情報を取得する場合は、「犯罪による収益の移転防止に関する法律」（旧「金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律」）に定める手段に準拠し、なりすましによる登録を防止し、本人であることを厳格に確認することが必要である。

（例：口座開設時の手続きの一環として、公的証明書（パスポートや運転免許証等）により、対面で確かに本人であることを確認したうえで、生体認証情報を取得すること等があげられる）

③本人確認に必要な最小限の生体認証情報のみの取得

生体認証情報の取得にあたっては、本人確認に必要な最小限の生体認証情報のみに限定することが必要である。具体的には、raw（生）データそのものを登録して使用することなく、特徴点を抽出して用いることが求められる。

(2) 入力

①テンプレートの登録

a. テンプレートの登録時には、新たに生成したテンプレートが、被登録者本人の認証に適合することを、利用開始に先立ち、確認することが必要である。

b. 金融機関等がテンプレートをコンピュータ上に登録する場合は、テンプレートの作成場所から保存場所への、安全な移送・伝送手順を明確にすることが必要である。（例、暗号の使用など）

c. 顧客が保持する記録媒体（以下、トークンという）にテンプレートを登録する場合は、トークンへテンプレートを安全に格納する手順、及び顧客への安全な発行手順を明確にすることが必要である。

d. 伝送データの漏洩防止については、【技 29】を参照のこと。

e. 蓄積データの漏洩防止については、【技 28】を参照のこと。

f. データ保護、破壊・改ざん防止については、【技 31】を参照のこと。

g. 外部ネットワークからのアクセス制限については、【技 43】を参照のこと。

（注）テンプレート・・・認証時に参照するために、事前に登録する生体認証情報のこと。

②顧客への通知

取引開始に先立ち、テンプレートの登録が完了した旨、顧客への通知を行うことが望ましい。（例：その場で本人に通知する。または、登録が完了した時点で、メールやはがきを出状する。）

③サンプル・データの消去

テンプレートを作成するために、顧客から取得したサンプル・データについては、その消

去の条件と方法を明確にし、安全な管理のもとに速やかに消去することが必要である。

（注）サンプル・データ　・・・認証の都度（日常取引や登録時等）、センサー等の機器を介して取得する生体認証情報のこと。

(3) 利用

①暗号化

a. 生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送する場合は暗号化することが必要である。

ここで対象となる生体認証情報としては、以下の例がある。

(a)テンプレート

(b)サンプル・データ

(c)ログに含まれる生体認証情報

b. また、テンプレートの改ざん検知策を講ずることが望ましい。

（例：メッセージ認証コードの使用など）

改ざん検知策については、【技 33】を参照のこと。

②暗号鍵の管理

利用する暗号鍵の管理方法を明確にし、運用することが必要である。

暗号鍵の管理については、【運 43】を参照のこと。

③サンプル・データの消去

日常取引において、顧客から取得したサンプル・データについては、その消去の条件と方法を明確にし、安全な管理のもとに速やかに消去することが必要である。

(4) 保存

①テンプレートの保存

a. 金融機関等が、テンプレートを保存する場合、安全に保存するための手順を定めることが必要である。

b. 金融機関等が、テンプレートをサーバー等の検索可能なデータベースに保存する場合は、「氏名等の個人情報」と「生体認証情報」を分別管理することが望ましい。ここで、「氏名等」とは、「氏名や顧客番号のように顧客を容易に特定できる情報」を指す。

（例：具体的には、データベースを分ける。サーバーを分ける。バックアップ先の媒体を分ける。等）

(a)伝送データの漏洩防止については、【技 29】を参照のこと。

(b)蓄積データの漏洩防止については、【技 28】を参照のこと。

(c)データ保護、破壊・改ざん防止については、【技 31】を参照のこと。

(d)外部ネットワークからのアクセス制限については、【技 43】を参照のこと。

②暗号化

登録された生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送、保管する場合は暗号化することが必要である。

ここで対象となる生体認証情報としては、以下の例がある。

a.テンプレート

b. ログに含まれる生体認証情報

③暗号鍵の管理

利用する暗号鍵の管理方法を明確にし、運用することが必要である。

a. 暗号鍵の管理については、【運 43】を参照のこと。

(5) 消去

生体認証情報、及びそれを記録した記憶媒体等を、本人確認に用いる必要性がなくなった場合、及び本人から消去の申し入れがあった場合には、速やかにこれらを消去するための手順を明確にし、安全な管理のもとに、実施することが必要である。

(6) トークンの取扱管理

①顧客が保持するトークンにテンプレートを保存する場合

a. トークンを顧客に安全に発行するための、手順を明確にすることが必要である。

b. また、発行後のトークンの使用停止、使用停止解除、再発行、消去を、安全に実施するための手順、及びトークンの紛失、盗難、汚損時等の取扱手順を明確にすることが必要である。

c. トークンを本人確認に用いる必要性がなくなった場合、及び本人から消去の申し入れがあった場合には、速やかにこれを消去するための手順を明確にし、安全な管理のもとに、実施することが必要である。

（例：顧客との授受や登録手続きを窓口で対面で確実に行う。受領確認を行い、そのログを記録する。顧客がトークンを保有する際は、生体認証情報の漏洩防止対策がなされている。等）

②不正アクセス技術の向上等に対応し、必要かつ適切な安全管理措置を実施する観点から、トークンの使用期限を考慮することが望ましい。

カードの管理方法の明確化については、【運 51】も参照のこと。

テンプレートの再発行については、【技 35-1】を参照のこと。

参照法令	・個人情報の保護に関する法律 ・個人情報の保護に関する法律についてのガイドライン ・金融分野における個人情報保護に関するガイドライン ・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

（参考）

「生体認証情報」を取り扱ううえで、安全対策基準に「重要」データ、「機密」データ等として記述がある下記の基準を参考にされたい。

【設 23、設 24、設 26、 設 31、 設 93、設 101、設 106、設 122、設 123】

【運 1、運 5、運 10、運 11、運 13、運 16、運 21、運 24、運 25、運 27、運 29、運 33、運 36、 運 37、運 57、運 58、運 61、運 71、運 74、運 75、運 76、運 79、運 80、運 87-1、運 88、運 90、運 107】

情報セキュリティ
不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

削除: 基礎

実 126	生体認証の特性を考慮し、必要な安全対策を検討すること。

生体認証の導入と運用にあたっては、不正使用防止のため、技術の最新動向等に留意し、その特性を十分考慮し、必要な安全対策を検討すること。

1. 生体認証の導入と運用にあたっては、不正使用防止のため、技術の最新動向等に留意し、その特性を十分考慮し、必要な安全対策を検討することが必要である。

生体認証の導入と運用にあたり、考慮すべき特性としては、以下のものがある。

(1) 認証精度

認証精度設定等の適切性の確認を行うことが必要である。（認証のしきい値を厳しく設定すると、一般に本人拒否率が高くなり、利用者はフラストレーションを引き起こすため、実務においては、これをゆるく設定しがちになる。しかし、しきい値をゆるく設定すると、他人受入率の上昇につながり、他人によるなりすまし等の可能性を高める。この観点から、両者のトレードオフを、（生体認証の結果が適用される）アプリケーションの特性を考慮し、調整することが重要となる。）

また、テンプレートを生成・発行する際は、テンプレートが十分なデータ・ポイントを有し、設定した精度を充足するように考慮することが必要である。

なお、顧客に対して認証精度を提示している時は、実装されている認証精度が提示値を充足することが必要である。

(2) 代替措置手続き

生体認証が機能しない場合（例、正当なアクセス権限を有する顧客から「認証時に拒否される旨」申告された場合等）に備えて、代替措置手続き及び手段を明確にすることが必要である。

なお、具体的策定にあたっては、代替措置手続き及び手段がセキュリティ・ホールとならないようにすることが必要である。

(3) 否認防止

「顧客による否認」防止の機能を用いる場合には考慮することが望ましい。

① 生体認証の結果を記録し、事後に検証する手段、手順、あるいは運用上の措置。

措置としては、以下の例がある。

a.IC カード発行時に、その IC カードが本人の認証に適合したことを、顧客本人に確認してもらいその記録を残す

b.防犯カメラによる日常の監視　等。【設 103】

②認証判定に使用された、サンプル・データとテンプレートの照合結果を記録する。

（注）「顧客による否認」として想定している状況とは、悪意を持った顧客や勘違いをしている顧客が、その本人の口座から、生体認証にて預金の払戻しをした後、その行為を否認して被害を訴え補償を求める場合等である。

(4) 不正認証（なりすまし）等防止

①生体認証情報の登録時、及び日常取引における認証時に、センサー等の機器を介して取得する、「真正な顧客」のサンプル・データに関して、本人ではない者による、その

a.不正入手

b.偽造

c.不正使用

等を防ぐ手段、運用上の措置を講ずることが必要である。

リスクと対応策としては、以下の例がある。

(a) 偽 ATM（偽センサー機器等）の設置による、生体認証情報のだまし取り。また、センサー部分の残存情報からの指紋等のコピー。対応策としては、防犯カメラによる監視、職員による巡回点検、利用者への注意喚起等。【設 103】

(b) 人工的に合成してつくった偽造生体を使った不正認証（なりすまし）。対応策としては、生体検知装置による確認、職員による対面確認等。

(c) ホスト照合の場合には、センサーで取得した生体認証情報をホストへ送信する際にスパイウェア、フィッシングなどにより詐取され、悪用される可能性がある。対応策としては、ホストへの送信時に、暗号化や生体認証情報の読み取り日時等の情報を付加するなど、照合時にチェック可能とすることにより詐取された情報の再利用を防ぐなどが考えられる。

② テンプレートの不正利用を防ぐ手段、運用上の措置を講ずることが必要である。

リスクと対応策としては、以下の例がある。

a.悪意を持った内部者や、ネットワークを経由等した外部者が、「真正な顧客」のテンプレートを、不正に入手・使用して、それをサンプル・データ等に不正流用し、認証をパスする。対応策として、そもそもテンプレートは、サンプル・データに流用できない設計とする。ほかに、テンプレートとサンプル・データの類似度が極端に高い場合は、認証をパスさせない。（センサー機器等へかざす生体の位置・角度やぶれ等により、100%の一致は、認証方式によっては不自然な場合がある。）

(5) テンプレート保護技術

テンプレートのデータ保護について、「取り消し可能なバイオメトリクス認証」（Cancellable biometrics）など技術動向を考慮することが望ましい。

（参考）
取り消し可能なバイオメトリクス認証とは、何らかの原因でテンプレートが流出した場合等に、以前のテンプレートを無効として新規のテンプレートを再発行できる方式である。
取り消し可能なバイオメトリクス認証では、サンプル・データと変換パラメータを入力として、不可逆関数を用いて変換し、テンプレートを作成する。不可逆関数を用いて変換した場合、元のサンプル・データを復元することは不可能である。
加えて、変換パラメータは必要に応じ変更可能なので、万一テンプレートの信頼性が失われた場合には、変換パラメータを変更することによりテンプレートの再発行が可能となる。

【資料1－4】
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

新基準構成案

構成	修正案　基準大項目	修正案 基準中項目	新基準番号（暫定）	基準小項目	旧基準番号	基礎基準	基礎基準				適用区分				
							統制・監査	顧客データ漏洩防止及びシステムの不正防止	コンティンジェンシープラン	システムの運行管理に最低限必要	建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
Ⅰ　統制基準	1 内部の統制	(1) 方針・計画	統1	システムの安全対策に係る重要事項を定めた規程を整備すること。	運1・2	○	○				◎				
			統2	中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。	新設	○	○				◎				
		(2) 組織体制	統3	システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること。	技7	○	○				◎				
			統6	セキュリティ管理体制を整備すること。	運3	○	○				◎				
			統13	サイバー攻撃対応態勢を整備すること。	運113	○	○				◎				
			統7	システム管理体制を整備すること。	運4	○	○				◎				
			統8	データ管理体制を整備すること。	運5	○	○				◎				
			統9	ネットワーク管理体制を整備すること。	運6	○	○				◎				
			統12	業務組織を整備すること。	運9	○	○					◎	◎		
			統10	防災組織を整備すること。	運7	○	○					◎	◎		
			統11	防犯組織を整備すること。	運8	○	○					◎	◎		
			統4	各種業務の規則を整備すること。	運10	○	○				◎				
		(3) 管理状況の評価	統5	セキュリティ遵守状況を確認すること。	運10-1	○	○				◎				
		(4) 人材（要員・教育）	統14	セキュリティ教育を行うこと。	運80	○	○				◎				
			統15	要員に対するスキルアップ教育を行うこと。	運81	○	○				◎				
			統17	障害時・災害時に備えた教育・訓練を行うこと。	運83	○	○				◎				
			統18	防災・防犯訓練を行うこと。	運84	○	○				◎				
			統19	要員の人事管理を適切に行うこと。	運85	○	○				◎				
			統20	要員の健康管理を適切に行うこと。	運86	○	○				◎				
	2 外部の統制	(1) 外部委託管理	統21	システムの開発や運用、サービス利用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。	運108他	○	○				◎				
			統22	安全対策に関する項目を盛り込んだ委託契約を締結すること。	運109他	○	○				◎				
			統23	外部委託先（再委託先を含む）の要員にルールを遵守させ、その遵守状況を管理、検証すること。	運89	○	○				◎				
			統24	外部委託における業務組織の整備と業務の管理、検証を行うこと。	運90	○	○				◎				
			~~統25~~	~~外部委託にあたって、データ漏洩防止策を講ずること。~~（廃止予定）			○				◎				
			~~統26~~	~~外部委託契約終了時の情報漏洩防止策を講ずること。~~（廃止予定）			○				◎				
		(2) クラウドサービスの利用	統27	クラウドサービス利用時の管理策を講ずること。	新設	付加基準と位置付けてはどうか（議案3で検討）					◎				
		(3) 共同センター	統28	共同センターにおける有事の際の安全管理策を講ずること。	新設						◎				
		(4) 金融機関相互のシステム・ネットワークのサービス	統29	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。	運90-1						◎				
Ⅱ　実務基準	1 情報セキュリティ	(1) データ保護	実116	他人に暗証番号・パスワード等を知られないための対策を講ずること。	技26	○		○			◎				
			実117	相手端末確認機能を設けること。	技27	~~○~~					○				
			実118	蓄積データの漏洩防止策を講ずること。	技28	~~○~~					○				
			実119	伝送データの漏洩防止策を講ずること。	技29	~~○~~					○				
			実121	ファイルに対するアクセス制御機能を設けること。	技31	○		○			◎				
			実122	不良データ検出機能を充実すること。	技32	○		○			◎				
			実123	伝送データの改ざん検知策を講ずること。	技33	~~○~~					○				
		(2) 不正使用防止	実125	本人確認機能を設けること。	技35	○		○			◎				
			実126	生体認証の特性を考慮し、必要な安全対策を検討すること。	技35-1	~~○~~					◎				
			実127	IDの不正使用防止機能を設けること。	技36	○		○			◎				
			実128	アクセス履歴を管理すること。	技37	○		○			◎				
			実129	取引制限機能を設けること。	技38	○				○	◎				
			実130	事故時の取引禁止機能を設けること。	技39						◎				
			実133	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。	技42						◎				
		(3) 外部ネットワークからの不正アクセス防止	実135	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。	技43	○		○			◎				
			実136	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。	技44	○		○			◎				
		(4) 不正検知策	実137	不正アクセスの監視機能を設けること。	技45	○		○			◎				
			実138	異常な取引状況を把握するための機能を設けること。	技46						◎				
			実139	異例取引の監視機能を設けること。	技47						◎				
		(5) 不正発生時の対応策	実140	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	技48	○		○			◎				
		(6) 不正プログラム対策	実141	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	技49	○		○			◎				
			実142	コンピュータウイルス等不正プログラムの検知対策を講ずること。	技50	○		○			◎				
			実143	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。	技51	○			○		◎				
	2　システム運用共通	(1) マニュアルの整備	実4	通常時マニュアルを整備すること。	運14	○				○	◎				
			実5	障害時・災害時マニュアルを整備すること。	運15	○			○		◎				
		(2) アクセス権限の管理	実6	各種資源、システムへのアクセス権限を明確にすること。	運16	○		○			◎				
			実7	パスワードが他人に知られないための措置を講じておくこと。	運17	○		○			◎				
			実8	各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること。	運18	○		○			◎				
		(3) データ管理	実15	データファイルの授受・管理方法を定めること。	運25	○		○			◎				
			実16	データファイルの修正管理方法を明確にすること。	運26	○				○	◎				
			実33	暗号鍵の利用において運用管理方法を明確にすること。	運43	○		○			◎				
		(4) オペレーション習熟	統16	オペレーション習熟のための教育および訓練を行うこと。	運82	○				○	◎				
		(5) コンピュータウイルス対策	実20	コンピュータウイルス対策を講ずること。	運30	○		○			◎				
		(6) 外部接続管理	実48	接続契約内容を明確にすること。	運55	○		○			◎				
			実49	外部接続における運用管理方法を明確にすること。	運56	○		○			◎				
	3　運行管理	(1) オペレーション管理	実9	オペレータの資格確認を行うこと。	運19	○		○				◎			
			実10	オペレーションの依頼・承認手続きを明確にすること。	運20	○		○				◎			
			実11	オペレーション実行体制を明確にすること。	運21	○		○				◎			
			実12	オペレーションの記録、確認を行うこと。	運22	○				○		◎			
			~~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。~~	~~運23~~	~~○~~						○	○		
		(2) データファイル管理	実17	データファイルのバックアップを確保すること。	運27	○			○		◎				
		(3) プログラムファイル管理	実18	プログラムファイルの管理方法を明確にすること。	運28	○				○	◎				
			実19	プログラムファイルのバックアップを確保すること。	運29	○			○		◎				
		(4) ネットワーク設定情報管理	実21	ネットワークの設定情報の管理を行うこと。	運31	○				○	◎				
			実22	ネットワークの設定情報のバックアップを確保すること。	運32	○			○		◎				
		(5) ドキュメント管理	実23	ドキュメントの保管管理方法を明確にすること。	運33	○				○	◎				
			実24	ドキュメントのバックアップを確保すること。	運34	○			○		◎				
		(6) 運行監視	実53	システムの運行状況の監視体制を整備すること。	運60	○		○			◎				
	4 各種設備管理	(1) 資源管理	実47	各種資源の能力及び使用状況の確認を行うこと。	運54	○				○	◎				
		(2) 機器の管理	実59	ハードウェア、ソフトウェアの管理を行うこと。	運66	○				○	◎				
			実50	機器の管理方法を明確にすること。	運57	○		○				◎	◎		
			実51	ネットワーク関連機器の保護措置を講ずること。	運58							○	○	○	
			実52	機器の保守方法を明確にすること。	運59	○				○		◎	◎		
			実92	機器の予防保守を実施すること。	技1							◎	◎		
		(3) コンピュータ関連設備の保守管理	実69	コンピュータ関連設備の管理方法を明確にすること。	運76	○				○		◎	◎		
			実70	コンピュータ関連設備の保守方法を明確にすること。	運77	○				○		◎	◎		
			実71	コンピュータ関連設備の能力および使用状況の確認を行うこと。	運78	○				○		◎	◎		
		(4) 入退館（室）管理	実1	入館（室）の資格付与、及び鍵の管理を行うこと。	運11	○		○				◎	◎		
			実2	入退館管理を行うこと。	運12	○		○				◎			
			実3	入退室管理を行うこと。	運13	○		○				◎	◎		
			実54	入室後の作業を管理すること。	運61	○		○				◎	◎		
		(5) 監視	実72	各種設備の監視体制を整備すること。	運79	○				○		◎	◎		
	5　システムの利用	(1) 取引の管理	実28	各取引の操作権限を明確にすること。	運38	○		○				◎	◎		
			実29	オペレータカードの管理を行うこと。	運39							◎	◎		
			実30	取引の操作内容を記録・検証すること。	運40	○		○				◎	◎		
			実31	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。	運41						◎				
		(2) 入出力管理	実14	データの入力管理を行うこと。	運24	○				○		◎	◎		
			実27	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。	運37	○		○			◎				
		(3) 帳票管理	実25	未使用重要帳票の管理方法を明確にすること。	運35						◎				
			実26	重要な印字済帳票の取扱方法を明確にすること。	運36	○		○			◎				

新基準構成案

構成	修正案　基準大項目	修正案 基準中項目	新基準番号（暫定）	基準小項目	旧基準番号	基礎基準	基礎基準				適用区分				
							統制・監査	顧客データ漏洩防止及びシステムの不正防止	コンティンジェンシープラン	システムの運行管理に最低限必要	建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
		(4) 顧客データ保護	実45	顧客データの保護策を講ずること。	運53	○		○			◎				
			実46	生体認証における生体認証情報の安全管理措置を講ずること。	運53-1	⊖					◎				
	6　緊急時の対応	(1) 障害時・災害時対応策	実55	障害時・災害時の関係者への連絡手順を明確にすること。	運62	○			○		◎				
			実56	障害時・災害時復旧手順を明確にすること。	運63	○			○		◎				
			実57	障害の原因を調査・分析すること。	運64	○				○	◎				
		(2) コンティンジェンシープランの策定	実58	コンティンジェンシープランを策定すること。	運65	○			○		◎				
		(3) バックアップサイト	実115	バックアップサイトを保有すること。	技25							○			
	7 システム開発・変更	(1) システム開発・変更管理	実60	システムの開発・変更手順を明確にすること。	運67	○				○	◎				
			実61	テスト環境を整備すること。	運68	○		○			◎				
			実62	本番への移行手順を明確にすること。	運69	○				○	◎				
		(2) システムドキュメント管理	実63	システムドキュメントの作成手順を定めること。	運70						◎				
			実64	システムドキュメントの保管管理方法を明確にすること。	運71	○				○	◎				
		(3) パッケージの導入	実65	パッケージの評価体制を整備すること。	運72						◎				
			実66	パッケージの運用・管理体制を明確にすること。	運73						◎				
		(4) システムの廃棄	実67	システムの廃棄計画、手順を策定すること。	運74	○		○			◎				
			実68	システム廃棄時の情報漏洩防止対策を講ずること。	運75	○		○			◎				
	8　システムの信頼性向上対策	(1) ハードウェアの予備	実93	本体装置の予備を設けること。	技2							◎	◎		
			実94	周辺装置の予備を設けること。	技3							◎	◎		
			実95	通信系装置の予備を設けること。	技4							◎	◎		
			実96	回線の予備を設けること。	技5							○	○		
			実97	端末系装置の予備を設けること。	技6							◎	◎		
		(2) ソフトウエアの品質向上対策	実98	必要となるセキュリティ機能を取り込むこと。	技8	○				○	◎				
			実99	設計段階でのソフトウェアの品質を確保すること。	技9	○				○	◎				
			実100	プログラム作成段階での品質を確保すること。	技10	○				○	◎				
			実101	テスト段階でのソフトウェアの品質を確保すること。	技11	○				○	◎				
			実102	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	技12	○				○	◎				
			実103	パッケージ導入にあたり、ソフトウェアの品質を確保すること。	技13	○					◎				
			実104	定型的変更作業時の正確性を確保すること。	技14	○					◎				
			実105	機能の変更、追加作業時の品質を確保すること。	技15	○				○	◎				
			実120	ファイルに対する排他制御機能を設けること。	技30						◎				
			実124	ファイル突合機能を設けること。	技34	○		○			◎				
		(3) 運用時の信頼性向上対策	実106	オペレーションの自動化、簡略化を図ること。	技16						○				
			実107	オペレーションのチェック機能を充実すること。	技17	○				○	◎				
			実108	負荷状態の監視制御機能を充実すること。	技18	○				○	◎				
		(4) 障害の早期発見・回復機能	実110	システム運用状況の監視機能を設けること。	技20	○				○	◎				
			実111	障害の検出および障害箇所の切り分け機能を設けること。	技21						◎				
			実112	障害時の縮退・再構成機能を設けること。	技22						◎				
			実113	障害時の取引制限機能を設けること。	技23						◎				
			実114	障害時のリカバリ機能を設けること。	技24	○				○	◎				
	9　個別業務・サービス	(1) カード取引サービス	実42	カードの管理方法を明確にすること。	運51	⊖						◎	◎	◎	
			実43	カード取引等に関する犯罪について注意喚起を行うこと。	運51-1								◎	◎	
			実35	CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること。	運44-1						◎				
			実44	指定された口座のカード取引監視方法を明確にすること。	運52	⊖						◎	◎	◎	
			実131	カードの偽造防止対策のための技術的措置を講ずること。	技40							○	○	○	
		(2) インターネット・モバイルサービス	実84	インターネット・モバイルサービスの不正使用を防止すること。	運103	⊖									◎
			実85	インターネット・モバイルサービスの不正使用を早期発見すること。	運104	⊖									◎
			実86	インターネット・モバイルサービスの安全対策に関する情報開示をすること。	運105										○
			実87	インターネット・モバイルサービスの顧客対応方法を明確にすること。	運105-1										◎
			実88	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確にすること。	運106										◎
			実34	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。	運44	⊖							◎		
		(3) 渉外端末の管理	実41	渉外端末の運用管理方法を明確にすること。	運50	⊖							◎		
		(4) CD・ATM等及び無人店舗の管理	実36	運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。	運45								◎	◎	
			実37	無人店舗の監視体制を明確にすること。	運46								◎		
			実38	無人店舗の防犯体制を明確にすること。	運47								◎		
			実39	無人店舗の障害時・災害時の対応方法を明確にすること。	運48								◎		
			実40	無人店舗の関係マニュアルの整備を行うこと。	運49								◎		
			実109	CD・ATM等の遠隔制御機能を設けること。	技19							◎	◎	◎	
		(5) インストアブランチ	実73	インストアブランチの出店先の選定基準を明確にすること。	運92								◎		
		(6) コンビニATM	実74	コンビニATMの出店先の選定基準を明確にすること。	運93									◎	
			実75	コンビニATMの現金装填等メンテナンス時の防犯対策を講じること。	運94									◎	
			実76	コンビニATMの障害時・災害時対応手順を明確にすること。	運95									◎	
			実77	コンビニATMのネットワーク関連機器、伝送データの安全対策を講ずること。	運96									◎	
			実78	コンビニATMの所轄の警察および警備会社等関係者との連絡体制を確立すること。	運97									◎	
			実79	コンビニATMの顧客に対して犯罪に関する注意喚起を行うこと。	運98									◎	
		(7) デビットカード・サービス	実80	デビットカード・サービスにおける安全対策を講ずること。	運99									◎	
			実81	デビットカードの口座番号、暗証番号等の安全性を確保すること。	運100									◎	
			実82	デビットカード利用時の顧客保護の措置を講ずること。	運101									◎	
			実83	デビットカード利用上の留意事項を顧客に注意喚起すること。	運102									◎	
		(8) 前払式支払手段	実32	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること。	運42						◎				
			実132	電子的価値の保護機能、または不正検知の仕組みを設けること。	技41	⊖					○				
		(9) 電子メール・イントラネットの利用	実89	電子メールの運用方針を明確にすること。	運107										◎
			実134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。	技42-1	⊖					○				
Ⅳ　監査基準	12 システム監査	(1) システム監査	監1	システム監査体制を整備すること。	運91	○	○				○	◎			
						168	103								

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

Ⅱ．フレームワーク

１．総論

(2) 基準の分類

本書では、金融機関等がリスク特性に応じた安全対策の目標を設定するにあたり、不確実性を低減させることを目的に、「基礎基準」を設定している。一方で、「基礎基準」以外の基準は、リスク特性に応じて追加・選択する「付加基準」としている。なお、「設備基準」については、収納するコンピュータシステムに求められる基準を一意に定めることが困難であることから、「基礎基準」及び「付加基準」を区分していない。

「基礎基準」は、特定システム、通常システムによらず、金融情報システムが最低限適用する基準として、以下の考え方に基づき設定している。

全てのシステムにおいて安全対策を決定、実施していくためには、セキュリティポリシーや、外部委託に関する方針等が整備され、必要な人員が確保・教育されるなど、ITガバナンスが適切に発揮されていることが必要である。このため、内部及び外部の統制並びに監査に関する基準は、これらをまず「基礎基準」としている。

また、一般に金融情報システムは、商品・サービスを顧客に提供するため、顧客データを保有または、顧客データに接続していると想定されることから、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ついても「基礎基準」としている。顧客データには、個人データ以外の重要なデータ[i]が含まれる場合があるが、この場合も顧客データ漏えい防止に関する基準が有効と考えられる。

また、近年において重要性が増しているサイバー攻撃対策に関する基準も、顧客データの漏えい防止に関する基準に含めている。

また、リスクベースアプローチの考えでは、必ずしもリスクゼロを追求しないことから残存リスクへの対応を考慮する必要がある。このため、コンティンジェンシープラン策定に関する基準についても、「基礎基準」としている。

さらに、システムの安定運用を実現するために必要な基準についても、これを「基礎基準」としている。

ただし、固別の業務またはサービスにおいて実施する基準（ＡＴＭ、クラウドサービスの利用など）については、全ての金融情報システムにおいて実施しないことから、これらは基礎基準としていない。

「基礎基準」の選定にあたっての考え方

○統制・監査に関する基準
○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
○コンティンジェンシープラン策定に関する基準
○システムの運行管理に最低限必要な基準

※個別の業務・サービスに関する基準は除く[ii]

上記以外の観点で必要となる基準については、各金融機関等が、システム構成やリスク評価の結果等を考慮のうえ、適宜、必要に応じて選択する「付加基準」となる。例えば、通常

システムにおいて高い可用性が求められる場合は、可用性を確保するための安全対策の目標を定め、「付加基準」の中から適宜、必要な基準を選択・追加することで、安全対策の水準を高めることとなる。

「基礎基準」の「解説部分」において、全ての金融情報システムにおいて適用されるべき最低限必要な対策を「必須対策」(注)と呼ぶ。具体的には、「必要である」と 記載されている対策を「必須対策」とする。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする(「Ⅲ.本書の利用にあたって 3.本書の記述仕様」を参照)。

「付加基準」の「解説部分」の中で、当該基準を適用する場合に必須となる対策 を「付加基準」の「必須対策」(注)と呼ぶ。具体的には、「必要である」と記載されて いる対策を「必須対策」とする(特定システムでは、「付加基準」の「必須対策」は、必ず適用されることとなる)。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする。

この結果、特定システム、通常システムへの基準の適用方法は、[図表 8]のとおりとなる。

	基礎基準		付加基準	
	必須対策	その他の対策	必須対策	その他の対策
特定システム	○	△	○	△
通常システム	○	△	△	△

・「○」は、適用。
・「△」は、選択的に適用。

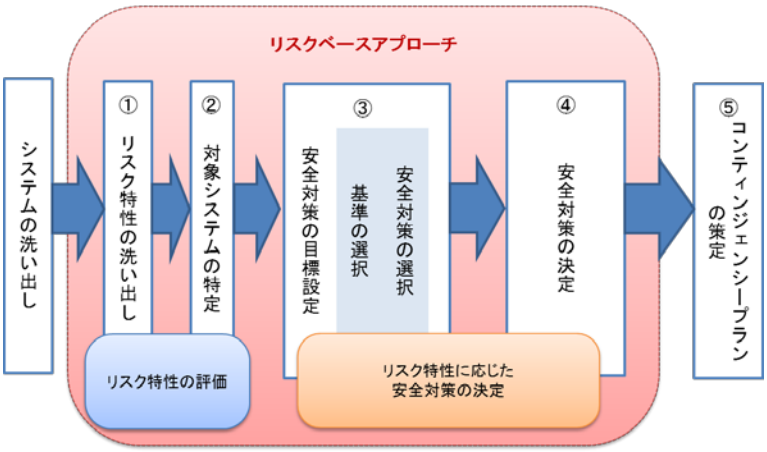
[図表 8] 特定システム、通常システムへの基準の適用方法

(4) 安全対策決定のプロセス

リスクベースアプローチでは、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。金融機関等は、安全対策基準の適用対象となる各システムのリスク特性を洗い出し、対象システムを特定した後、安全対策の目標を定め、必要となる基準及び安全対策の選択を行う。安全対策の目標に対し、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、最終的に安全

(注) システム構成等の観点から適用する必要がない、あるいは適用できない場合には、「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である)。また、「必須対策」には、「重要度を勘案し、個人データ等を扱うシステムの場合等には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。

対策を決定していく。その結果、残存するリスクを踏まえ、必要に応じてコンティンジェンシープランを策定する（[図表 10]を参照）。



［図表 10］安全対策決定のプロセス

③ 安全対策の目標設定（基準の選択・安全対策の選択）

対象システムを特定した後、個々のシステムのリスク特性の評価結果に応じ、安全対策の目標を設定する。個々のシステムに対する安全対策の目標設定では、例えば、保有するデータの種類や稼働率など、システムのリスク特性に応じて、選択した基準からどの対策を実施すべきかを選択していくことが考えられる。適切な目標を設定するためには、例えば、リスク事象ごとに定められた障害発生件数の抑制など、目標設定の方針が定められていることが必要である。目標設定の方針は、システムリスク管理方針や、セキュリティポリシー、経営資源配分等の観点を踏まえ、経営層の関与のもと決定されることとなる。

IT マネジメントを担う管理者等は、設定された安全対策の目標を達成するために、必要となる基準及び対策を選択する。

特定システムにおいては、原則として、基礎基準に示された対策及び付加基準に示された対策の中から必要な対策を選択する。

通常システムは、原則として、基礎基準に示された対策を選択した後、個々のシステムのリスク特性等を考慮のうえ、必要に応じ付加基準を追加していく。

なお、システム構成等の観点から適用する必要がない、あるいは適用できない場合には、「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。

また、「必須対策」には、「重要度を勘案し、個人データ等を扱うシステムの場合等には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある（「1.(2)基準の分類」を参照）。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

運行管理
オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実 10	オペレーションの依頼・承認手続きを明確にすること。

コンピュータシステムの不正使用を防止するため、オペレーションの依頼・承認手続きを明確にすること。

1. コンピュータシステムの不正使用を防止するため、オペレーションの依頼、承認は、オペレーション依頼票等を用いて行うなど、定められた手続きに従って行うことが必要である。

2. オペレーションが自動化されている場合は、スケジュールの作成、承認、及び自動スケジューリングプログラムへの登録等に関する手続きを明確に定めることが必要である。

3. 臨時処理やトラブル発生にともなう例外処理についても、手続きを明確に定めることが必要である。なお、処理を実行する際は、他処理への影響等を踏まえスケジュールに留意する必要がある。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

運行管理
オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実 11	オペレーション実行体制を明確にすること。

コンピュータシステムの誤操作、及び不正使用を防止するため、オペレーション実行体制を明確にすること。

1. コンピュータシステムの誤操作、及び不正使用を防止するため、オペレーション実行体制を明確にする必要がある。

ここでいうオペレーション実行体制とは、オペレーションにおけるオペレータチーム編成、及びオペレーション手順を指している。

オペレーション実行体制に係わる具体的な対策としては、以下の例がある。

(1) オペレーション依頼票等により、承認されたオペレーション依頼であることを確認する。

(2) オペレータは専任とし、オペレーションは複数のオペレータが行う。
オペレータの専任とは、運用規定によりあらかじめ定められた者を指し、専任とする目的として、以下のようなことが考えられる。
①責任の明確化
②不正使用防止
また、操作を複数のオペレータが行う目的として、以下のようなことが考えられる。
①オペレータ相互間の牽制効果による不正使用防止
②非常時対応

(3) 重要コマンド投入にあたっては相互確認を行う。
重要コマンド投入にあたって相互確認を行わせる目的は、誤操作による障害発生を防止することにある。なお、重要コマンドとして、以下のようなものが考えられる。
①オンライン開局処理
②オンライン閉局処理
③障害発生装置の切離し（中央処理装置、主記憶装置、チャネル装置、ファイル装置等）【技 22】
④回線の論理的切替え

(4) ジョブの実行者を明確にする。
ジョブの実行者を明確にする目的は、責任を明確にするとともに、障害が確認された際の原因究明を容易に行えるようにすることにある。なお、ここでいうジョブの実行者とは、コンソールから操作もしくは運行状況確認を行うオペレータまたはオペレータチー

ムを指している。

2. 事故や障害が発生した場合には、事故・障害状況等を速やかにオペレータを統括する担当責任者、システム運用部門の責任者等に報告することが必要である。

3. 誤操作によるコンピュータシステムの障害発生を防止し、業務を円滑に行うため、以下のような操作手順の標準化を図り、マニュアルとして常備することが必要である。
   (1) 各機器の操作方法
   (2) コマンドの使用法
   (3) コンピュータシステム運転手順
   オペレーションの自動化、簡略化については、【技 16】参照のこと。

4. 機密性の高いオペレーションを行う際は、要員を限定するなど特別な注意が必要である。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

運行管理
オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実 12	オペレーションの記録、確認を行うこと。

オペレーションの正当性を検証するため、オペレーションの記録、確認を行うこと。

1. オペレーションの正当性を確保するため、オペレーション実行時の運行状況を確認するとともに、依頼されたオペレーションが指示どおり処理されたことを確認できるように、オペレーション記録を残すことが必要である。

   オペレーション記録の具体的な対策としては、以下の例がある。

   (1) 運行状況を確認するチェックリストを作成する。
   運行状況を確認するチェックリストとして、以下のようなものが考えられる。
   ①オペレーション実施記録
   ②オペレーション予定・実績比較表
   ③オペレーション進捗状況表

   (2) オペレータ交替時の未処理、重複処理を防止するため、オペレーションを引き継ぐときの引継事項を明確にする。
   引継事項としては、以下の例がある。
   ①ジョブ処理状況
   ②障害発生状況
   ③その他連絡事項

   (3) オペレーション記録を残し、オペレーション結果を検証する体制を明確にする。
   オペレーション結果の検証方法としては、以下の例がある。
   ①運行状況チェックリストによる確認、検証
   ②自動運行確認リストによる確認、検証
   ③処理レコード件数の確認
   なお、確認、検証時に重大な不備等を発見した場合、オペレータを統括する担当責任者は速やかに運用管理部門の責任者に報告する。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

各種設備管理
機器の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎	◎		

実 51	ネットワーク関連機器の保護措置を講ずること。

不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成するネットワーク機器等は、適切な保護措置が講じられていること。

1. 重要なデータを扱うシステムの場合、MDF、IDF、ルータやファイアウォール等のネットワーク機器に関しても不正使用、破壊、盗難等された場合の影響が大きい。このため、ネットワーク機器も、必要に応じてサーバー設置場所に準ずる機器管理を行うことが望ましい。

(1)　サーバーの機器管理については【運 57】参照のこと。
(2) ネットワーク機器の設定情報管理については【運 31、32】参照のこと。

削除: 基礎
削除: ○
削除: ○
削除: ○
削除: が望ましい

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

個別業務・サービス
インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

削除: ○

実 86	インターネット・モバイルサービスの安全対策に関する情報開示をすること。

利用者が適切に取引機関や金融サービスの選択を行うため、安全対策に関する情報を開示すること。

削除: が望ましい

1. 利用者が適切に取引機関や金融サービスの選択を行えるよう、金融機関等はセキュリティ方針等を開示することが望ましい。

   開示内容としては、以下の例がある。
   (1) 情報漏洩防止のために暗号化していること。
   (2) なりすまし防止のために認証（パスワード、電子認証）を行っていること。
   (3) 顧客に関する厳密な守秘義務に基づき、顧客データを保護していること。

   また、開示方法としては、以下の例がある。
   (1) DM への記載
   (2) 店頭や自動機器コーナーのポスターへの記載
   (3) 金融機関等ホームページへの記載
   (4) 新聞広告等
   (5) 電子メール

2. 開示にあたっては図等を使用し、利用者に理解しやすいように工夫することが望ましい。

3. 利用者からの問合せ及び苦情に対応することが望ましい。
   (1) 相談窓口の設置
   (2) パンフレット、ホームページ等に連絡先を明記

   利用者への安全対策に関する情報開示を実施するにあたっては、当センター発刊の「安全対策に関する情報開示研究会報告書」等を参照のこと。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

システムの信頼性向上対策
ハードウェアの予備

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

削除: ○
削除: ○

実 96	回線の予備を設けること。

回線障害時の迅速な対応のため、重要な回線は予備を設けること。

削除: が望ましい

1. 回線障害時の迅速な対応のため、重要な回線は予備を設けることが望ましい。
   また、回線の予備については、以下の点を考慮することが望ましい。
   (1) 地点間（構外）の重要な回線は複数化するか、またはバックアップ回線を確保することが望ましい。なお、回線を複数化する際は、物理的別ルート化（別の収容交換設備等（旧電話局）を経由するもの）を図ることが望ましい。また、回線のルートや回線容量等は、通信事業者に該当の回線の利用目的等を明示し、適切な設計・構築を図ることが望ましい。
   (2) 構内回線についても、コンピュータセンター内の構内配線や、重要な部門 LAN については予備を設けることが望ましい。

2. 地点間（構外）の回線について
   (1) 予備の具体的な内容としては、以下の例がある。
      ①専用回線の複数化の例
         a. 端末系装置を 2 つのグループに分け、それぞれ別々の回線に接続する方法
         b. 回線の一方を予備とし、必要に応じて切り替える方法
      ②電話回線（xDSL を含む）、 ISDN 回線、回線交換回線、パケット交換回線、ATM 回線、衛星通信回線、光ファイバー通信網等を利用したバックアップ回線の確保（図 1）。

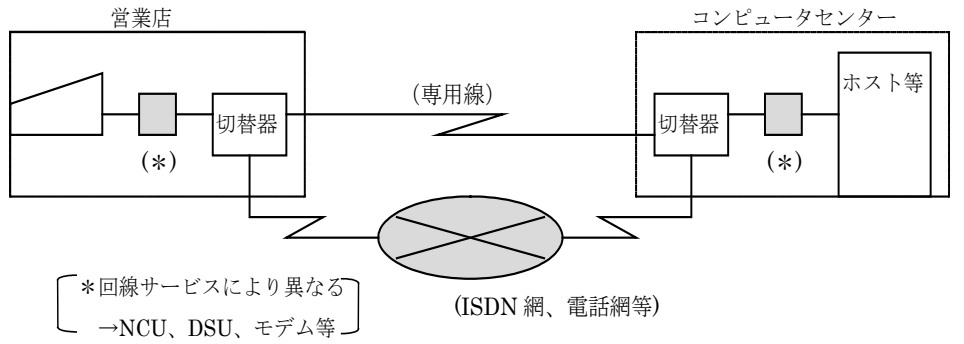


図 1　バックアップ回線の例

(2) 回線の別ルート化

回線ルートに障害が発生した場合に、全回線が同時に使用できなくなる事態を防ぐため、複数の回線により別々に接続し、並行して危険分散を図るための方法である。

単一の通信事業者を利用し、中継局を分ける（物理的に別ルートにする）方法と、複数の通信事業者を利用する方法がある（図 2、図 3）。

①単一の通信事業者の利用

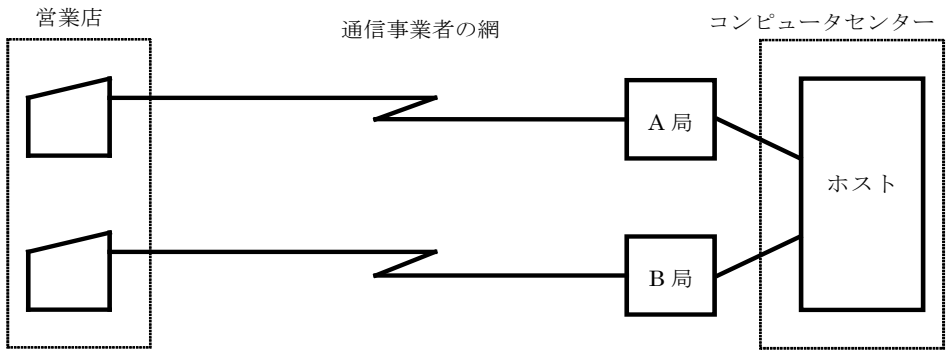


図 2　単一の通信事業者の利用例

②複数の通信事業者の利用

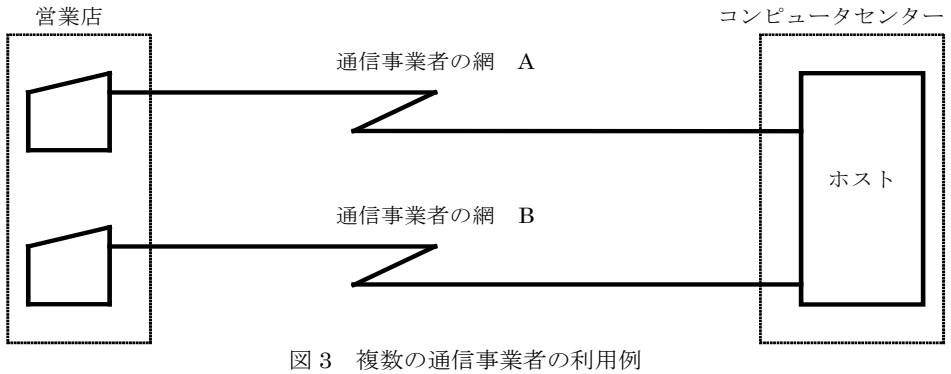


図 3　複数の通信事業者の利用例

(3) データ伝送経路の構成と留意点

代表的なデータ伝送経路の構成には、スター型構成（コンピュータセンター等の主要拠点と営業店等の拠点を 1 対 1 で接続する構成）や、ツリー型構成（コンピュータセンター等の主要拠点より事務センターや基幹営業店等の中継結節点を経由し、複数の営業店等の拠点を接続する構成）等がある。構成によって、障害時の影響範囲、通信量及びコスト等について留意する必要があり、選択にあたっては、各種構成の特徴を踏まえ、業務への影響等を勘案することが必要である（図 4、図 5）。

①スター型の構成

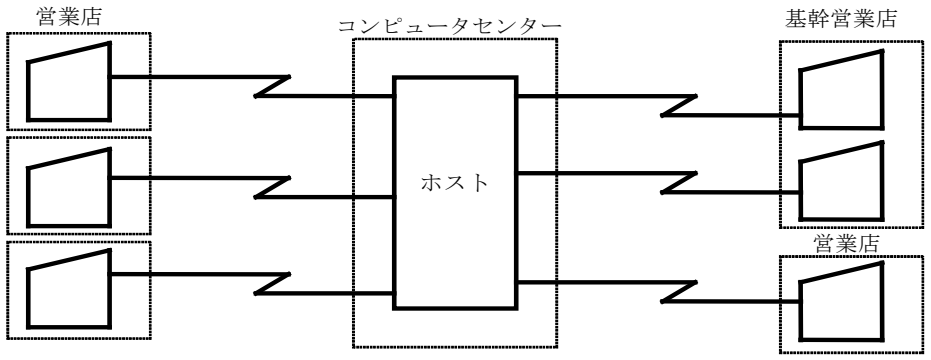


図 4　スター型の構成の例

②ツリー型の構成

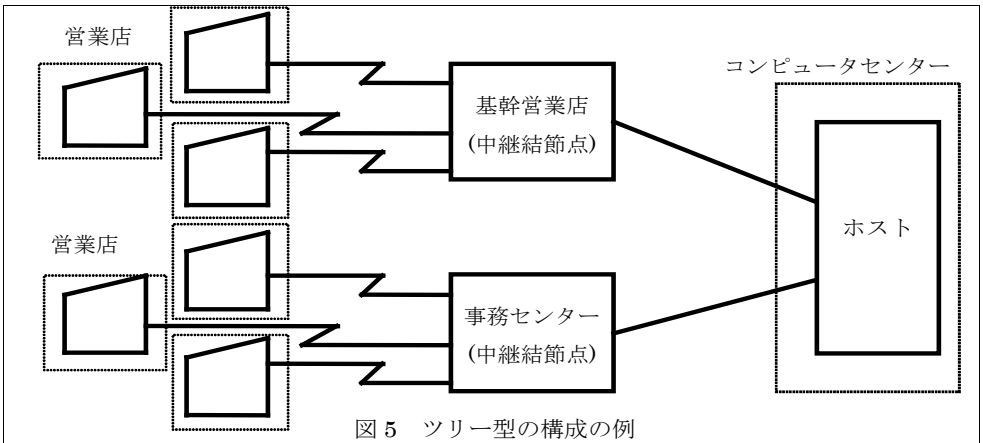


図 5　ツリー型の構成の例

3. 構内回線について

(1) コンピュータセンターにおける留意点

コンピュータセンターにおいては、回線関連設備から重要な各機器までの配線は二重化することが望ましい。特に、建物外の回線を二重化した場合、コンピュータセンター内において、MDF から通信制御装置等の重要な各機器までの配線を二重化することが望ましい。

(2) 構内 LAN の予備

構内 LAN についても、重要性に応じて予備を持つことが望ましい。構内 LAN の予備としては、以下の例がある（図 6）。

①基幹 LAN の多重化（図 6）

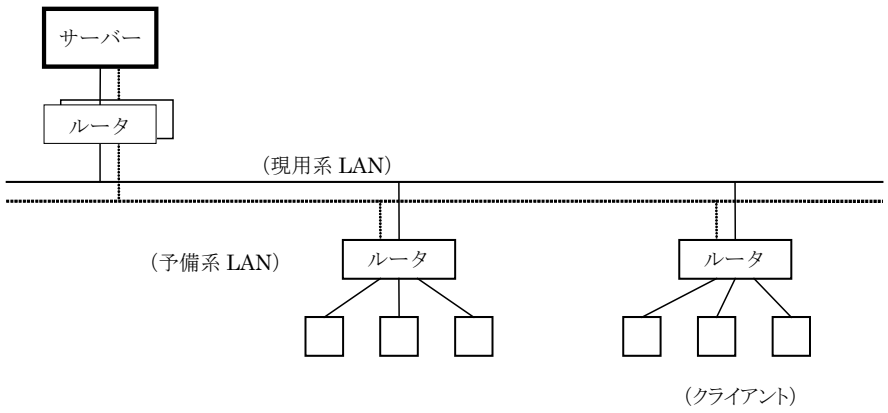


図 6　LAN の多重化の例

4. システムの目的や重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
   特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
   なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認する必要がある。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

システムの信頼性向上対策
運用時の信頼性向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					付加

削除: 基礎
削除: ○

実 106	オペレーションの自動化、簡略化を図ること。

オペレーションの信頼性を向上させるため、オペレーションの自動化、簡略化を図ること。

削除: が望ましい

1. 汎用機、サーバーのオペレーション

コンピュータセンター及び本部・営業店等におけるオペレーションの信頼性を向上させるため、ハードウェアやソフトウェアを利用してオペレーションの自動化、簡略化を図ることが望ましい。

オペレーションの自動化、簡略化としては、以下の例がある。

(1) コンピュータセンターにおけるオペレーション

①自動化

システムの起動や業務の開始を自動的に行う機能、ジョブの起動やジョブと記憶装置の対応を自動化する機能等、各種自動運転機能を活用する、またはそれぞれの実情に応じた機能を開発することなどによりセンターオペレーションの自動化を図るものである。

また、運用スケジュールの規模に応じてシステムの電源投入を自動的に行う機器、テープハンドリングを自動的に行う機器を活用することもオペレーションの信頼性、安全性、情報の機密保護を向上させるうえで有効である。

スケジュール化されたジョブグループのジョブシーケンスに従ったジョブの自動起動やタイマーによるジョブの時間起動のほかに自動化としては、以下の例がある。

a.電源投入からシステムの立上げ、オンラインジョブの起動、端末の開局等、業務が開始できるまでの一連処理の自動化

b.平常日、繁忙日、月末日、土曜日等パターンごとにスケジュール化された一斉同報通知の送出や端末モード変更の自動化

c.取引ジャーナル等のファイルのバッチジョブへの引継ぎの自動化

d.取引ジャーナル等のファイルの他システム（系）への引継ぎの自動化

e.端末の閉局からオンラインジョブの停止までの一連の処理の自動化

f.システム停止の自動化

g.テープハンドリングの自動化

なお、自動運用の注意事項として処理の順序や運転状況、条件の変更が生じた際にも、システム全体の運用に支障を来さぬように、自動化を変更できる機能を充実することが重要であり、変更内容としては、以下の例がある。

(a) 一斉同報通知や端末モード変更を行う時刻の変更
(b) システム（系）の変更（現用系から待機系への変更、またはその逆）
(c) 自動運用からマニュアル運用への変更
(d) ジョブネットワークへのジョブの追加、変更
(e) ボリュームの追加、変更
(f) 実行 JCL（ジョブ制御言語）の変更

②簡略化

コマンド体系の一元化を図ったり出力メッセージの日本語化を図るなどして、オペレータインタフェースを平易化する。さらに、運用をケースによりパターン化し、一連のコマンド列を一括実行できるように準備することなどにより、オペレーションを単純化、簡略化する。

オペレーションの単純化、簡略化としては、以下の例がある。

a.コマンド入力の極少化
b.テープハンドリングの極少化
c.異常終了後再開オペレーションのパターン化

③自動化、簡略化の留意点

センターオペレーションの自動化の推進は、オペレーションの信頼性向上のために有効であるが、過度の自動化は、機械運行の安全性を阻害する可能性もある。そのような場合には、単にオペレータへの通報にとどめる等、オペレータによる判断の余地を残しておく。

オペレータの応答を必要とするメッセージやオペレータに注意を喚起する必要があるメッセージ等は、高輝度出力、赤字出力やブザーを鳴らす（オペレータの応答で解除）方法等で重要メッセージの見落としを防ぐよう工夫する。さらに、大量メッセージによるシステム停止等を防ぐため、冗長なメッセージを抑止する等の仕組みを合わせて構築する。

(2) 本部・営業店等におけるオペレーション

本部・営業店等における重要なサーバーのオペレーションは、コンピュータセンターにおけるオペレーションに倣って自動化、簡略化を図る。さらに、本部・営業店等でコンピュータ運用に必要な知識や技能を持つ専門のオペレータを配置することが困難な場合には、自動化等の運用をリモート操作で行う機能を持つ。

①自動化

本部・営業店等のサーバーオペレーションの自動化としては、以下の例がある。

a.電源の投入やシステムの立上げ、業務アプリケーションの起動
b.バックアップの取得やデータベース更新手順
c.障害発生時の縮退運転の手順やシャットダウン手順

②簡略化

簡略化としては、以下の例がある。

a.オペレーション用のインタフェースを平易化（ユーザーフレンドリなインタフェースの採用）

b.一連のコマンドを一括実行しコマンド入力を極少化

c.異常終了時の再開オペレーションの単純化

2. データ入力作業（端末オペレーション）

コンピュータセンター及び本部・営業店等におけるオペレーションの信頼性を向上させるため、ハードウェアやソフトウェアを利用してデータ入力作業（端末オペレーション）の自動化、簡略化を図ることが望ましい。

オペレーションの自動化、簡略化としては、以下の例がある。

(1) 自動化

磁気ストライプ読取装置、現金処理機、OCR 等の活用により、手入力操作の一部またはすべてを削減する。

(2) 簡略化

オペレーションガイダンス機能の活用等により、入力判断の平易化やコード入力による簡略化を行う。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

緊急時の対応
バックアップサイト

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎				

削除: ○

実 115	バックアップサイトを保有すること。

コンピュータセンター等が災害等により機能しなくなった場合に備えるため、業務の優先度を考慮したバックアップサイトを保有すること。

削除: が望ましい

削除: 。

1. コンピュータセンター等が災害等により機能しなくなった場合に備えて、リスク分散の意味で、別の地域にバックアップサイトを保有することが望ましい。
   特に、資金決済等を行う重要なシステムについては、原則としてバックアップサイトを保有することが必要である。
   ただし、バックアップサイトを保有しない場合は、障害による社会への影響を十分に検討のうえ、他に代替する方法による業務継続態勢を整備し、経営層が承認する必要がある。

   バックアップサイトの運営形態としては、以下のものがある。
   (1) 自営センター
   　自社専用の代替施設として利用する。
   (2) 共同利用センター
   　複数企業が共同で代替センターを設立し、必要時に利用する。
   (3) 相互利用センター
   　別地域にある同一企業（グループ）内の事業部門と相互に被災時等にバックアップし合う。代替施設提供部門は、被災時等には緊急度の低い業務は一時運用を止めて対応する。
   　他企業（協力企業）間でバックアップし合う場合もある。
   (4) 代行処理センター
   　第三者にバックアップを委託し、必要時に利用する。

2. バックアップサイトを外部に委託している場合、複数の委託元で同時に緊急事態が発生するケースを想定して、バックアップを受ける優先順位、最低保証の範囲などのサービスを確認し、事務量の変化に対応して定期的に見直すことが必要である。

3. バックアップサイトの保有にあたっては、以下の事項を考慮し、総合的に判断することが望ましい。
   (1) コンピュータセンターと同一のリスク要因（火災、地震、停電等）を共有しないこと。
(2) 被災時の要員、データ、物資等の移動・移送時間を含む復旧時間を確認すること。

（参考）
バックアップサイトの立地条件については、コンピュータセンターの立地条件と同様に考える必要があるため【設 1】を参照のこと。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

情報セキュリティ
データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					付加

削除: 基礎

削除: ○

実 117	相手端末確認機能を設けること。

公衆通信網を通じて自動着信端末に出力する場合には、誤接続を防止するため、確認可能なものについては相手端末を確認する機能を設けること。

削除: が望ましい

1. 公衆通信網を通じて金融機関等から顧客に対して振込入金等の種々の金融情報を、自動着信機能を持ったファクシミリ端末を介して連絡する場合には、暗証番号等による本人確認ができないため電話番号の登録ミス等により誤った相手に出力する可能性がある。
   相手確認が可能な端末については、相手端末確認機能を用いることが望ましい。

   接続相手端末確認としては、以下の例がある。
   (1) 電話の発信者情報通知サービス、携帯電話の識別番号等の利用
   (2) ファクシミリの端末 ID の利用
   (3) 認証機関が発行する電子的な証明書【技 35】

2. 公衆通信網を通じてパソコンやコンピュータへ種々の資金移動や金融情報を通知する場合、接続する際に端末 ID や発信者確認コードの確認を行う等の機能を設けることが望ましい。【技 35】

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

情報セキュリティ
データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					付加

実 118	蓄積データの漏洩防止策を講ずること。

ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについてはデータ保護の対策を講ずること。

1. ファイルの不正コピーや盗難の際にも、データの内容がわからないようにするため、重要なデータについてはデータ保護の対策を講ずることが必要である。特に個人データを蓄積する場合には、暗号化・パスワード設定等ファイルの不正コピーや盗難の際にもデータの内容がわからないようにするための対策を講ずることが必要である。また、電子的取引において蓄積されるデータについても暗号化・パスワード設定等の対策を講ずることが必要である。

   パスワード設定の内容としては、以下の例がある。
   (1) データベース　：DBMS の備えるパスワード【技 31】
   (2) 文書ファイル　：文書そのものにかけるパスワード
   (3) ハードディスク：ハードディスクドライブにかけるパスワード。パスワードが知られない限り他の機器に接続しても読み取り不可能となる。

2. 外部持ち出しや他の媒体へのコピーが物理的に不可能なコンピュータ機器内の個人データの漏洩防止策としては、上記対策の他、本人確認機能を設けることにより、許可された者以外の者が当該データを判別できないようにする仕組みも有効である。本人確認機能については、【技 35】を参照のこと。
   また、ホストコンピュータ等でのみ読み出し可能な個人データを媒体に蓄積する際には、フィジカルダンプ等で断片化させて蓄積することにより、特定のソフトウェア・ハードウェアを用いなければ判別できないようにする方法も有効である。
   （注 1）ホストコンピュータ等：ホストコンピュータ、またはそれに準じるコンピュータ
   （注 2）フィジカルダンプ　　：ファイルレイアウト等論理的な構成を無視し、ディスクの先頭から順番にコピーすることにより、個別にファイルを復帰することができないようにすること。

3. 暗号の使用にあたっては、CPU 負荷の増大、業務処理遅延等の影響にも留意して、信頼のおける適切な技術を選択することが必要である。なお、適用する技術は、情報処理技術の発展とともにその強度が変化することに留意するとともに、その使用にあたっては、複数の方式を適切に組み合わせて使用することが望ましい。
   また、新規にシステムを構築する、あるいはシステムを更新する際には、技術の進歩により暗号

削除: 基礎
削除: ○
削除: 暗号化等
削除: が望ましい
削除: 暗号化する
削除: 望ましい

は脆弱になることや暗号技術も日々進化していることを踏まえ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」等に記載されている、安全性が継続的に検証されている暗号方式を採用することが望ましい。

4. IC カードにおける漏洩防止策としては耐タンパー性、その他蓄積媒体上の漏洩防止策としては暗号化が考えられる。

蓄積媒体上の暗号化として、以下のレベルがある。

(1) ファイルの中の重要な項目だけ暗号化
（例：暗証番号、パスワード、電子的価値情報等）

(2) 重要ファイルについて全項目を暗号化
（例：パスワードファイル、個人情報ファイル、電子的価値情報ファイル等）

5. 渉外端末の盗難・紛失時に備えた対策として、渉外端末内に重要なデータを蓄積する場合には、暗号化することが望ましい。なお、個人データを蓄積する場合には、暗号化・パスワード設定等の対策を講じる必要がある。

端末機器からの漏洩防止策としては、以下の例がある。

(1) 封印ラベル等による周辺機器との接続部分の固定や物理的封鎖、外部記憶装置の取り外し、ソフトウェアによる記録媒体の使用制限。なお、一時的な使用制限の解除が認められる場合には、使用制限の再設定手続きと定期的な制限の確認を行う。

(2) 使用する記録媒体内のデータの暗号

(3) CD・ATM 等を含む端末機器内部のデータに対するアクセス権限の制限【運 16】

（参考 1）
暗号化の方式としては、例えば以下のようなものがある。

(1) 共通鍵暗号方式
暗号化する時に使用した鍵と同じ鍵で復号する方式。

(2) 公開鍵暗号方式
ペアになった 2 つの鍵でデータを暗号化、復号する方式で、どちらか一方の鍵を公開する。

6. コンピュータ端末及び周辺機器から漏れる電磁波が盗聴され再現される危険性（テンペスト）があることから、対策を講じることが考えられる。

電磁波の盗聴対策としては、以下の例がある。

(1) 電磁遮蔽カバーの採用
機器そのものをカバーする例として、筐体全体を金属で覆う、導電性塗料を塗布する、導電性メッシュを一体成型した非透過性シールドを CRT 映像面に装着する等がある。
機器が設置されている部屋をシールドする例として、電磁波を通しにくいシールドフィ

ルム等を壁紙に使用する、窓ガラスに非透過性シールドを貼る等がある。

(2) 電磁波防止フィルターの採用

各種ケーブルのコネクター部に装着し、ケーブルから発生する電磁波を減少させるものが市販されている。

(3) 保護対象機器の設置場所から一定範囲内の侵入制限を行う

7. システム処理中に重要なデータを含む一時データファイルが生成される場合、重要なデータの漏洩を防止するため、利用状況に応じ不要となった時点で消去する機能を設けることが望ましい。

（参考 2）

1. 技術の進歩により暗号の脆弱性が増す事例には以下のものがある。

(1) コンピュータの処理能力の向上により、解読に要する時間が現実的な時間に収まる。

(2) 暗号アルゴリズムの脆弱性が発見される。

（注）内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）において、政府機関における SHA-1 及び RSA1024 の移行についての指針等を打ち出している事例がある。

（検討状況の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf

（指針の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf

2. 総務省と経済産業省が中心となって選定した「電子政府推奨暗号リスト」は平成 15 年 2 月に発刊されている。

また、平成 25 年 3 月には「電子政府推奨暗号リスト」を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が策定されている。

（CRYPTREC：URL）

http://www.cryptrec.go.jp/

3. 「電子政府推奨暗号」の利用方法に関しては、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」が平成 20 年 7 月に公開されている。

（参照 URL）

http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

（注）CRYPTREC とは Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。総務省及び経済産業省が共同で運営する暗号技術検討会と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が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。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

情報セキュリティ
データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実 119	伝送データの漏洩防止策を講ずること。

データ伝送時の盗聴等による漏洩を防止するため、重要なデータについてはデータ保護の対策を講ずること。

1. データ伝送時に盗聴された場合にもデータの内容がわからないようにするため、重要なデータについては、データ保護の対策を講ずることが必要である。特に個人データを伝送する場合には、暗号化・パスワード設定等データ伝送時に盗聴された場合にもデータの内容がわからないようにするための対策を講ずることが必要である。

   個人データを伝送する場合には、上記以外の対策としては、以下の条件を満たしセキュアな環境とすることで、光ファイバーの専用線を用いることも有効である。
   (1) 建物内に不正な機器が接続されていないことの確認
   (2) 切断などにより、漏洩のおそれがある場合にその分析ができること
   (3) 通信事業者における漏洩防止策を確認・評価していること

2. オープンネットワークや無線を利用して重要なデータを伝送する場合は、通信事業者と協力するなど暗号化対策を図り、十分な漏洩防止対策を講じておくことが必要である。

3. 開発時のドキュメント、ソースコード等もその重要性に配慮した伝送方式を考えることが望ましい。なお、構内 LAN においては、ネットワーク構成機器への未承認機器の論理的・物理的な接続を不可能とする仕組みも有効である。

削除: 基礎
削除: ○
削除: 暗号化
削除: が望ましい
削除: 暗号化する
削除: 望ましい

（参考 1）
無線 LAN を使用する際には、以下のような点を考慮する必要がある。
(1) 従来の無線 LAN 機器で使用されている、WEP（Wireless Equivalent Privacy）の RC4 という暗号化方式は、脆弱性を回避する手段がないことから、業務システムにおいては使用しない。
(2) 平成 29 年８月現在で望ましいとされる暗号化方式は、IEEE802.11i 通信規格の WPA（Wi-Fi Protected Access）または WPA2 の AES（Advanced Encryption Standard）と呼ばれる共通鍵暗号方式とされている。なお、WPA または WPA2 には TKIP（Temporal Key Integrity Protocol）と呼ばれる共通鍵暗号方式も存在する。この方式に確認されている脆弱性に対応するために、安全な設定値を利用すること。
(3) 無線 LAN が使用している電波が社外に漏れることを防ぐための対策として電波遮断シートの利用が挙げられる。
(4) 参照 URL として、以下のものがある。
①「無線 LAN セキュリティ要件の検討」
http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf
首相官邸各府省情報化統括責任者（CIO）補佐官等連絡会議
②「WPA の脆弱性の報告に関する分析（技術編）」
http://www.rcis.aist.go.jp/TR/2009-01/wpa-compromise.html
独立行政法人産業技術総合研究所 情報セキュリティ研究センター
③「一般利用者が安心して無線 LAN を利用するために」
http://www.soumu.go.jp/main_content/000183224.pdf
総務省

4. 暗号の使用にあたっては、CPU 負荷の増大、業務処理遅延等の影響にも留意して、信頼のおける適切な技術を選択することが必要である。なお、適用する技術は、情報処理技術の発展とともにその強度が変化することに留意するとともに、その使用にあたっては、複数の方式を適切に組み合わせて使用することが望ましい。
また、新規にシステムを構築する、あるいはシステムを更新する際には、技術の進歩により暗号は脆弱になることや暗号技術も日々進化していることを踏まえ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」等に記載されている、安全性が継続的に検証されている暗号方式を採用することが望ましい。

データ伝送上の暗号化としては、以下の例がある。
(1) 暗号化対象範囲によるレベル
①伝送データの一部のみ暗号化
（例：暗証番号、口座番号、電子的価値情報等）
②伝送データ全体の暗号化
（例：伝送するレコード全体を暗号化する）

(2) 伝送路上における暗号化レベル

①伝送回線上の暗号化

（例：伝送回線の両端に暗号化・復号装置を設置する方法）

②端末間の暗号化

（例：端末上の暗号化ソフトにより端末間の伝送データを暗号化する方法）

(3) (1)、(2)を組み合わせた暗号化

（例：暗証番号、口座番号、電子的価値情報等の暗号化をしたうえで、さらに暗号化装置を設置する方法）

（参考 2）

1. 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。SSL の暗号鍵は、数種類の鍵長が選択可能であるが、安全性を考慮すると 128 ビット以上の鍵長を使用することが望ましい。

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」に記載がある。

（参照 URL）

http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

3. Web アプリケーションの設計及び実装において、SSL を適切に使用し、重要な情報を漏れなく暗号化することが必要である。

例として以下のようなものがある。

(1) ID・パスワードや個人情報等の情報を入力させる際には、SSL を使用した画面（「https://」で始まる画面）とすること。

(2) 複数フレームを使用する際には、利用者が Web ブラウザのアドレスバーで、表示中のページが SSL で保護されていることを確認できる画面構成とすること。

(3) セッション ID 等ユーザーを特定するようなデータは常に SSL 通信を使用し、特にデータを cookie に格納する場合には、「secure」属性を付与するなどの実装を行うこと。

4. 参考文献として、以下のものがある。

(1) 「安全なウェブサイトの作り方 改訂第７版」
独立行政法人情報処理推進機構（IPA）セキュリティセンター

(2) 「安全な Web サイト利用の鉄則」
独立行政法人産業技術総合研究所情報セキュリティ研究センター

（参考 3）

1. 技術の進歩により暗号の脆弱性が増す事例には、以下のものがある。

(1) コンピュータの処理能力の向上により、解読に要する時間が現実的な時間に収まる。

(2) 暗号アルゴリズムの脆弱性が発見される。

（注）内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）において、政府機関における SHA-1 及び RSA1024 の移行についての指針等を打ち出している事例がある。

（検討状況の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf

（指針の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf

2. 総務省と経済産業省が中心となって選定した「電子政府推奨暗号リスト」は平成 15 年 2 月に発刊されている。

また、平成 25 年 3 月には「電子政府推奨暗号リスト」を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が策定されている。

（CRYPTREC：URL）

http://www.cryptrec.go.jp/

3. 「電子政府推奨暗号」の利用方法に関しては、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」が平成 20 年 7 月に公開されている。

（参照 URL）

http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

（注）CRYPTREC とは Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。総務省及び経済産業省が共同で運営する暗号技術検討会と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が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。

削除: .

―――――――――――――改ページ―――――――――――――

.

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

情報セキュリティ
データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

削除: 基礎

削除: ○

実 123	伝送データの改ざん検知策を講ずること。

データの改ざんを早期に発見するため、重要なデータの伝送において、改ざん検知のための対策を講じておくこと。

削除: が望ましい

1. データ伝送において、重要なデータについては、改ざん検知のための対策を講じておくことが望ましい。特にオープンネットワークを介してデータを伝送する場合は、伝送途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ている必要がある。

   暗号技術を活用した認証機能、改ざん検知機能としては、以下の例がある。
   (1) メッセージ認証コード
   (2) 電子署名

参照法令	電子署名及び認証業務に関する法律

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

個別業務・サービス
カード取引サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	
	◎	◎	◎		付加

実 131	カードの偽造防止対策のための技術的措置を講ずること。

不正使用防止のため、カードの偽造防止の技術的措置を講ずること。

削除: 基礎
削除: ○
削除: ○
削除: ○
削除: が望ましい

1. カード犯罪を防止し、カードを利用したサービスを安全に提供するため、カードの偽造防止のための技術的措置を講ずることが望ましい。

   カードの偽造防止対策としては、以下の例がある。
   (1) IC カード化
   (2) 磁気ストライプに偽造を判別するコードを記録する
   　なお、当該コードは、容易に推察されない仕組みとする。
   　利用者の利便性を考慮して IC と磁気ストライプを併用したカードを導入する場合、IC 単独のカードに比べ安全性が低いことに十分留意する。例えば、IC を使用した場合と磁気ストライプを使用した場合とで、利用できる取引の種類や金額を区別することが考えられる。
   (3) カードへ有効期限を設定し、期限経過時に更新
   (4) 顔写真、ホログラム等の券面への印刷

2. キャッシュカードの IC カード化にあたっては、「全銀協 IC キャッシュカード標準仕様」に要求される要件を満たすこと（セキュリティや互換性など）が必要である。また、IC カードの運用面や技術面について、セキュリティ対策上注意し、定期的に見直すことにより時々の技術水準を反映することが必要である。

   IC カードの運用面や技術面について、セキュリティ対策上注意すべき事項としては、以下の例がある。
   (1) IC カードの有効期限（電子証明書の有効期限）
   (2) 電子証明書の認証機関の信頼性（運用規定等）
   (3) 使用される暗号の強度
   (4) 耐タンパー性

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

個別業務・サービス
前払式支払手段

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					付加

削除: 基礎

削除: ○

実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。

電子的価値のコピー、二重使用等の不正行為に対処するため､データの保護機能を具備するか、あるいはその発生を検知できる仕組みを構築すること。

削除: が望ましい

1. 電子的価値を蓄積する機器、媒体あるいはそれに含まれるソフトウェアには、価値を保護する機能を具備することが望ましい。

2. 上記の機能がない場合には、改ざん､不正コピーによる二重使用等の不正行為を検出できる仕組みを用意することが望ましい。

3. セキュリティ確保のためには、複数の手段を組み合わせて総合的に対応する必要がある。
なお、セキュリティ技術は最新の技術の動向に留意し、その安定性、互換性、実装の容易さなどを適切に評価したうえで採用することが必要である。

セキュリティ確保のための手段としては、以下の例がある。
(1) IC カード型電子マネーにおける耐タンパー性を向上させる保護機能
(2) IC カード等には有効期限を設定するなどの偽造抑止対策
(3) シリアルナンバー方式による不正検知
(4) 証拠センター方式による不正検知

（注）・耐タンパー性　　：ソフトウェアやハードウェアの内部構造や記憶しているデータなどの解析の困難な状態。
・シリアルナンバー方式：電子的価値の使用単位ごとに固有の識別番号を付与し、同一番号のものが二重に使用されないようにチェックする方式。
・証拠センター方式　　：付与された電子的価値の総額に対して、実際の使用額と残額とを突合して不正使用をチェックする方式。証拠センターにおいて使用額と残額とが突合されるため、事後的なチェックとなる。

【資料１－５】
平成 27 年 10 月 17 日
公益財団法人　金融情報システムセンター

個別業務・サービス
電子メール・イントラネットの利用

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					付加

削除: 基礎

削除: ○

実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、不正使用防止対策を講ずること。

削除: が望ましい

1. 業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、セキュリティポリシーと整合性がある不正使用防止対策を講ずることが望ましい。なお、個人データを扱う場合には、この措置は必要である。

   業務目的以外の電子メールの送受信やホームページの閲覧等としては、以下の例がある。

   (1) 電子メールの送受信
   　①業務に関係しない私的な情報の交換・連絡
   　②業務上適切な範囲を逸脱した電子メールの利用（不適切なメーリングリストやメールマガジンの利用等）
   　③公序良俗に反する情報の送信
   (2) ホームページの閲覧
   　①業務に関係しないホームページの閲覧
   　②ホームページへの業務上適切な範囲を逸脱したコメントの掲載（掲示板等への公序良俗に反するコメント掲載等）

   また、業務目的以外の電子メールの送受信やホームページの閲覧等の不正使用防止対策としては、以下の例がある。

   (1) 電子メールの送受信やホームページの閲覧が可能な利用者を適切な範囲に限定する。
   【運 16】
   (2) メールフィルタリング等を導入し、電子メールの内容を判断し、不適切な情報の送受信を防止する。また、不適切な電子メールを送受信した利用者に対して適切な措置を行う。
   (3) 社外に送信された電子メールを自動的に送信者の管理者等に転送する。
   (4) コンテンツフィルタリング等を導入し、ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防止する。また、不適切なホームページを閲覧した利用者に対して適切な措置を行う。

2. 運用面においても、全役職員（外部要員を含む）に対するセキュリティ教育を行い、責任と

義務及び懲罰等について周知徹底を図ることが必要である。【運 80】

（参考）

メールフィルタリング：電子メールの内容を判断し、不適切な情報の送受信を防ぐ目的で利用されるソフトウェアであり、利用者が受信したくないメールアドレスを設定しスパムメールの着信を拒否できる機能も含めることがある。

コンテンツフィルタリング：ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防ぐ目的で利用されるソフトウェアであり、不適切なホームページを閲覧した利用者のアクセスログを取得する機能も含めることがある。

[i] 企業の公開前決算情報など、金融機関等において高い機密性が求められる情報を指す。

[ii] インストアブランチ、コンビニ ATM、インターネットの利用や、外部の統制におけるクラウドサービスの利用、共同センター、金融機関相互のシステム・ネットワークに関する基準など。

【資料２－１】
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

「読みやすさ対応」について

Ⅰ.「読みやすさ」に関する各委員からのご意見について

【資料２－２】「読みやすさ」に対する各委員からのご意見（対応方針）

Ⅱ. 語尾「重要である」の解釈について

・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、その他の語尾や例示については「選択可能な対策」としている。この定義に従うと語尾が「重要である」の文章は、必須対策とは位置付けられていない。しかし、今回、語尾が「重要である」の文章について、複数の委員から「必須なのか例示なのかわかりにくい」等のご意見を頂いている。

・「重要である」は必須対策ではないと定義されているものの、その語感から「必須対策」に近いものと読まれてしまう等、様々な解釈を生んでいると推察される。

・そこで、「重要である」（対象は９つの基準）について、利用者が統一した解釈を行うことができるよう対応を検討することとする。

以下の対応案についてご審議いただきたい。（【資料２－３】「重要である」を含む基準一覧参照）

対応案１

「重要である」を、必須対策ではない他の表現に一律変更する。（「望ましい」等）

対応案２

「重要である」を、記載内容を踏まえ、必須対策の場合は「必要である」、それ以外は「望ましい」に変更する。（事務局案を元に検討いただく）

対応案３

「重要である」は変更しない。（前説にて必須対策ではない旨を明記する）

※本日の審議結果を踏まえ、次回基準原案に反映する予定。

Ⅲ. 基準原案（基準構成案含む）の変更、反映について

(1)基準原案（変更後）・・・10/23（月）までにメール送付。

(2)ご意見締切・・・・基準原案（変更後）について 10/31（火）までにご確認いただく。

(3)最終基準原案・・・11/14（火）メール送付。

＜今後の変更・反映予定＞

	変更分類	基準原案への反映時期
①	基準構成の変更	・9 月末までのご意見を、(1)基準原案（変更後）に反映する。 ・10/31（火）までのご意見を、(3)最終基準原案に反映する。
②	基準内の対策・例示の変更	
③	対策の要求レベルの変更（語尾の変更）	

	変更分類	基準原案への反映時期
④	時代背景に沿った記載の見直し	「事務局一任作業」とし、(3)最終基準原案に反映する。
⑤	影響の小さい表現の統一・変更	
⑥	基準番号の変更	
⑦	関連ガイドラインの削除	
⑧	法改正等にともなう修正	

Ⅳ.「前文」内容の見直し及び一覧化について

・基準中項目単位の概要説明（前文）について、現行の記載内容を新基準構成に合わせて見直しする。

・その上で、現行の綴じ込み形式を変更し、「安全対策基準一覧表」として一覧化することで、読みやすさの向上を図る。

尚、「設備・運用・技術基準毎の概要説明」（中扉）については、前説Ⅱ「フレームワーク」1-(1)-③「安全対策基準の構成」に記載することとする。

【資料２－４】前文の構成・変更内容

【資料２－５】安全対策基準一覧表（原案）

※10/31（火）までに事後意見をいただきたい。事後意見を反映のうえ次回委員会にて最終原案を提示する予定。

以　上

【資料２－２】
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

■「読みやすさ」に対する各委員からのご意見（対応方針）

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
1	全般	－	基準書の記載として随所に出てくる「参考」と「参照」の使い分けについて、確認いたします。 参考は当該の項目を参考に利用者が考え、結果を求める、 参照は当該の項目を引用する事を意味しており、引用された基準が持つ意図と同じ取扱を求めていることを示している、 の理解で齟齬はございませんか。	日本ユニシス 森下様(専) 後藤様(検)	「参考」は、当該基準の記載内容に関連、付随する参考事項を記載したものです。 「参照」は、当該基準の記載内容と関連の深い他基準の番号を記載したものです。（必ずしも参照先基準と同様の取扱を求めるものではありません）	その他（確認等）	－	
2	全般	－	新基準番号（暫定）は、再採番において工夫をいただきたい。 大項目、中項目順になっていないので、基準番号順になると見づらくなる。	日本ユニシス 森下様(専) 後藤様(検)	基準構成確定後に大項目、中項目の順番に基準番号を再度採番します。	その他（確認等）	－	
3	全般	－	新旧の構成対比は、新を基準としたものが提示されているが、旧を基準としたものの提示は予定されているか？ 相互対比による整理などの妥当性確認がより容易となる事から、提供をいただきたい。	日本ユニシス 森下様(専) 後藤様(検)	現在のところ旧を基準とした資料の提示は予定しておりません。新旧を記載した構成案をEXCEL形式で提示しておりますので適宜変更してご利用いただきたくお願いいたします。	その他（確認等）	－	
4	全般	－	参考、参照の記載なく、基準番号が記載されている箇所は、どのような意味合いを持ちますか？	日本ユニシス 森下様(専) 後藤様(検)	当該基準を「参照」することを意味しています。	その他（確認等）	－	
5	全般	－	基準書の各項目で、例示として示されている物と記載が求められる項目の区別を解りやすくしていただけないでしょうか。 基準が求めていることの理解を助けるために、参考例示として記載されているものと必須要件としての記載に区別がなく、基準参照者が取扱に苦慮することが想定されます。	日本ユニシス 森下様(専) 後藤様(検)	今回の読みやすさ対応の中で、実施すべき対策（必須対策）は「～が必要で（が）ある」に語尾を統一しています。	その他（確認等）	－	
6	全般	－	基礎基準で「〇〇が必要である。 〇〇としては以下の例がある」の記述パターンの場合、例示されたものがどこまでできている必要があるのかはっきりしない。一つでもできれば良しとするのか?	農林中央金庫 常岡様(専) 今嶋様(検)	例示に記載された内容は必ず充足することを求めるものではありません。対策として記載された「～が必要である」の要件を満たせば良いということになります。	その他（確認等）	－	
7	全般	－	「運」「技」の記載を「実」「統」に定めたにも関わらず参照先として「運」「技」が出てくる。「運」「技」の基準は今後も使われるのか？	農林中央金庫 常岡様(専) 今嶋様(検)	参照先の「運」「技」については基準番号が確定次第、「統」「実」に更新します。	⑤表現の統一・見直し	要	11/14 反映予定
8	全般	－	従前は、運用基準、技術基準と分かれていたのでということかもしれないが、今回実務基準として並べるということであれば、重複感のある記述は統合するなり整理をした方が良いものと考える。参照する際に、タイトルから何ヵ所も確認する必要があるように見える。	農林中央金庫 常岡様(専) 今嶋様(検)	安全対策を、運用面からまとめた基準項目と、機能面（技術）からまとめた基準項目では、類似する対策が記載される場合があります。一方で、類似する対策を全て排除すると、基準項目として趣旨が伝わらなくなることも想定されます。また、参照項目が多くなると、読みにくくなる可能性があります。 重複感がある記述について、お気づきの箇所がありましたら、個別に検討させていただきたいと思います。	①基準構成の変更	－	
9	統5	2	「セキュリティ遵守状況を確認する者は、建屋内の点検や職員面接等の手段により」とあるが手段の例示がよく分からない。全般統制でいうセキュリティは建屋だけでなく、個別システムのセキュリティ対策も指すのではないのか。	三井住友銀行 持田様(専) 山口様(検)	システムのセキュリティ対策の実施状況ではなく、役職員の遵守状況を確認することが本基準の目的となります。	その他（確認等）	－	
10	統6	1,2	持ち株会社形態を想定した場合、個社毎の統制だけでなく、グループ横断的な統制が必要となるケースがあろうかと思います。この基準で「全社」「全社的」とは、「グループ内の各社」を意味するとの理解でよろしいでしょうか。	日本銀行 岡田様(専)	「全社」「全社的」は、「グループ内の各社」を意味します。	その他（確認等）	－	
11	統6	2	セキュリティの障害・事故・犯罪等　という表現が分かりにくい	三井住友銀行 持田様(専) 山口様(検)	「セキュリティ上の問題により発生した障害・事故・犯罪等」に変更します。	⑤表現の統一・見直し	要	10/23 反映予定
12	統6	参照法令	不正アクセス禁止法の第2条でないのか。3条から5条と直接関係していない	三井住友銀行 持田様(専) 山口様(検)	以下構成となっており、3条から5条も関連があると思われるため、参照法令としています。 第2条　（定義） 第3条　（不正アクセス行為の禁止） 第4条　（他人の識別符号を不正に取得する行為の禁止） 第5条　（不正アクセス行為を助長する行為の禁止）	その他（確認等）	－	
13	統8	2	統7の2において、システム管理者は「相互に連携を図った体制を整えることが望ましい」とあります。平仄の観点で、統8の2において、データ管理者に対しても同様の記載をしては如何でしょうか。	日本銀行 岡田様(専)	ご意見のとおり、2に以下を追加します。 「さらにそれぞれのデータ管理者の間で、相互に連携を図った体制を整えることが望ましい。」	②対策・例示の変更	要	10/23 反映予定
14	統10 統11	2	「コンピュータセンターにおいて共同ビルを利用している場合は、ビル全体の管理組織を踏まえ、コンピュータセンターとして独立した防災組織を整備することが必要である」とありますが、実際にどのようなコンピュータセンターをイメージしているのでしょうか。例えば、金融機関が大手ベンダーが提供するシステムセンターの1区画を利用しているケースにおいて、こうした防災組織を整備することは現実的に難しいかと思います。実態に合っていないのであれば、2.の2行を削除しては如何でしょうか。	日本銀行 岡田様(専)	共同ビルの中に、自機関のコンピュータセンターがあるケースを想定しています。	その他（確認等）	－	
15	統12	1	「コンピュータセンターにおける『業務組織の整備』としては、以下の例がある」とありますが、『業務組織を整備する際の観点』等とした方が良いかと思います。	日本銀行 岡田様(専)	「業務組織を整備する際の具体的な留意点としては～」に変更します。	⑤表現の統一・見直し	要	10/23 反映予定
16	統12	1	コンピュータセンターにおける業務組織の整備　とあるが、プログラム作成等はコンピュータセンターだけではない。コンピュータシステムに係わるの表現の方が適切では。	三井住友銀行 持田様(専) 山口様(検)	「コンピュータシステムに係わる業務組織の整備」に変更します。	⑤表現の統一・見直し	要	10/23 反映予定
17	統12	1	開発担当者が本番環境を利用できないことは、不正防止策として有効であるとあるとして、(1)～(3)が併記されているが、それぞれが例になっているわけではない。特に(3)は(1)の具体的事例では？ 開発環境と本番環境の完全分離は難しく、望ましいであることを明記した方がよい。	三井住友銀行 持田様(専) 山口様(検)	(1)の具体的な考慮点としての記載となるため、(1)に紐づけて記載します。（例示内の記載のため、語尾は原案のままとします）	⑤表現の統一・見直し	要	11/14 反映予定
18	統13	1	「・・・また、以下に示す例の他に・・・が必要である。」について、「以下の示す例」の例は、ベストプラクティクスベースと解される。であれば、下線の「必要である」は、「望ましい」ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘のとおり例示部分については選択して実施することが可能ですが、「～検討が必要である」については、必須対策となります。	⑤表現の統一・見直し	否	

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
19	統14	3	以下の重要性にサイバー攻撃を加えた方がよい	三井住友銀行 持田様(専) 山口様(検)	サイバー攻撃の対応については、「(3)システムの安全運用等についての対策」に包含されると考えます。また、教育テーマの例示にも(7)コンピュータウイルスへの対応(8)不正アクセスへの対応があり、その中に「サイバー攻撃」も含まれると考えます。	②対策・例示の変更	否	
20	統16	―	統制基準から実務基準に変更されたと理解でよいか？ 当初、統制基準の人材（要員、教育）に分類していたものを、実務基準に移したと思われるが、新基準番号が「統16」となっている。 実務基準に区分が、整理としてより妥当性が高いと理解できる。	日本ユニシス 森下様(専) 後藤様(検)	本基準は実務基準に移しておりますが、基準番号は当初案の「統16」としています。基準構成の確定後に、基準番号を一律更新します。	その他（確認等）	―	
21	統17	1	「『訓練』としては、以下の例がある」とありますが、『訓練の内容を検討する際の観点』等とした方が良いかと思います。また、タイトル「（3）所要時間」は、その後に記述されている「（3）訓練上の考慮点」等とした方が良いかと思います。	日本銀行 岡田様(専)	「訓練を計画するにあたり明確にすべき事項としては、以下の例がある」に変更します。 (3)所要時間は、後述の考慮点ではなく、訓練内容に含めるべき事項として原案のままが良いと考えます。	⑤表現の統一・見直し	要	10/23 反映予定
22	統19	1	「適切に行うことが必要である」との記述につき、「適切に」は不要（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	「適切に」を削除するよう修正します。（他の基準との記述を合わせる）	⑤表現の統一・見直し	要	10/23 反映予定
23	統19	2	スキル評価を行うは望ましいでよいのでは。必要とするなら、もう少し具体例を示すべき。	三井住友銀行 持田様(専) 山口様(検)	現状通りの表現（必須対策）であり、評価制度は異なるにせよ金融機関において何らかの評価は実施されてるものと考えます。	③要求レベルの変更 （語尾の変更）	否	
24	統20	小項目	タイトルの中の「適切に行うこと。」の「適切に」は不要。	農林中央金庫 常岡様(専) 今嶋様(検)	「適切に」を削除するよう修正します。（他の基準との記述を合わせる）	⑤表現の統一・見直し	要	10/23 反映予定
25	実1	2	2.(3)③「なお、入退室用識別コードの登録・変更にあたっては、容易に推測できない『番号』を選択する」とありますが、前段で「識別コード」としているので、後段も「番号」ではなく「コード」とした方が良いかと思います。	日本銀行 岡田様(専)	「番号」→「コード」に変更します。	⑤表現の統一・見直し	要	10/23 反映予定
26	実3	3	重要な室への入退室を許可された者に対する搬出入物品の確認について定めているが、実現方法は難しく、読み手にとって参考になるような具体例を記載すると良い。	三井住友銀行 持田様(専) 山口様(検)	コンピュータセンターにおいては、守衛による目視確認や、透明な袋に移し替えるといった例があり、実現は可能であり、その方法は各金融機関によって異なるものと考えます。	②対策・例示の変更	否	
27	実4	2	通常時マニュアルの整備に係わる具体的な対策としては、以下の例がある　とあるが、以下が例になっていない。文章が繋がっていない。	三井住友銀行 持田様(専) 山口様(検)	対策1と内容の一部が重複しており、例示としても適当ではないと考えられるため、対策1に含めて記載するよう変更します。	②対策・例示の変更	要	10/23 反映予定
28	実6	1	「また、アクセス手段を特定するとともに、必要最小限に限定することも考えられる」については「望ましい」の方が適当。	農林中央金庫 常岡様(専) 今嶋様(検)	アクセス手段の特定は、リモート保守等、対策を検討する環境が限定されることから、「望ましい」とせずに「考えられる」としています。	③要求レベルの変更 （語尾の変更）	否	
29	実7		米国ではNIST SP800-63の改正により、パスワードにランダムな文字列を強要することや、パスワードの定期変更を行うことがむしろ推奨されなくなってきているが、こうした情勢が踏まえられていないのではないか?	農林中央金庫 常岡様(専) 今嶋様(検)	NISTの改正から日も浅く、基準への反映に当たっては十分な調査と検証が必要になると考えます。	②対策・例示の変更	―	
30	実8	適用にあたっての考え方	サブタイトルの文章に「…各種資源、システムへのアクセスを管理するため、アクセス権限を与えるにあたってその手続きを明確に定めることが必要である。」とある。「が必要である。」は不要（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	「が必要である」を削除するよう修正します。	⑤表現の統一・見直し	要	10/23 反映予定
31	実8		「各種資源」とは何を指しているのか、分かりづらくないか。	三井住友銀行 持田様(専) 山口様(検)	「各種資源」は、「コンピュータシステムを構成する機器、ファイル等」を指しますが、本基準においてはその記載がないため、追記します。	⑤表現の統一・見直し	要	11/14 反映予定
32	実8	1 図1	アクセス権変更の際の手続は、新規利用のときと大きく変わらないので、記載していないという理解で良いか。	三井住友銀行 持田様(専) 山口様(検)	手続きの流れは新規利用時も変更時と同じであることから、現在の記載で問題ないと考えております。	②対策・例示の変更	否	
33	実8	2	2.「アクセス権限管理の具体的な注意点は、以下の例がある」の（8）の改訂案では、「ユーザーのパスワード失念時にパスワードを通知する場合」を「ユーザーのパスワード失念時にパスワードを通知したり再発行する場合」に修正しています。ユーザーの設定したパスワードは、パスワードそのものが復元できないようなハッシュ化されたデータとして保存されるのが一般的なシステムの造りかと思います。したがって、平文での「パスワードの通知」を例示する必要はなく、単に「ユーザーのパスワード失念時にパスワードを再発行する場合」とすれば良いかと思います。	日本銀行 岡田様(専)	「パスワードを再発行する場合」に変更します。	⑤表現の統一・見直し	要	10/23 反映予定
34	実8	2－(8)	「パスワードを通知したり再発行する場合」⇒「パスワードを通知したり再発行したりする場合」（～たり～たり）	農林中央金庫 常岡様(専) 今嶋様(検)	「パスワードを再発行する場合」に変更します。(No33参照)	⑤表現の統一・見直し	要	10/23 反映予定
35	実9		「オペレータ」の定義をするほうがよいのではないか。実29等他の項番におけるオペレータと同義であるか不明確である。	農林中央金庫 常岡様(専) 今嶋様(検)	前説の「主要用語」にて定義を記載しています。（現版では「コンピュータセンターにおけるコンピュータ操作者」と定義しています）	⑤表現の統一・見直し	―	
36	実12	1(1)	「運行状況を確認するチェックリストとして、以下のようなものが考えられる。」について、「以下の例がある」と記述（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘のとおり「以下の例がある」に修正します。	⑤表現の統一・見直し	要	10/23 反映予定
37	実13		クライアントサーバーのみを切り出しての基準は不要ではないか。必要に応じ、「実10、11、12」に追記するのがよいのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	実13については廃止する予定です。	①基準構成の変更	要	10/23 反映予定
38	実13		タイトルに「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」とありますが、記載の内容（1.）は、クライアントサーバー・システムに限ったものではないと思います。したがって、タイトル、1.の内容をより汎用的な表現に変更しては如何でしょうか。 また、クライアントサーバー・システムに関する記載は他の箇所にもあります（例えば実93）。これらについても、クライアントサーバー・システムに限定せず汎用的な表現に変更するか、クライアントサーバーシステムの技術特性に沿った記載にしてはいかがでしょうか（ホストコンピュータとの用語の対比だけであれば削除してはいかがでしょうか。	日本銀行 岡田様(専)	実13については廃止する予定です。	①基準構成の変更	要	10/23 反映予定

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
39	実15	1	「ここでいうデータファイルとは、・・・DAT等を指す。」について、この並びで言うと、今日的にUSBメモリ、フラッシュストレージ等も加えた方が良いのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	記憶媒体やストレージ等を含む表現に変更します。	⑤表現の統一・見直し	要	11/14 反映予定
40	実15	1	「ここでいうデータファイルとは、サーバー・パソコン等を含むコンピュータの磁気ディスク内のファイル、フロッピーディスク、光ディスク、磁気テープ、カートリッジ磁気テープ、DAT等を指している」となっており、前半はファイルを、後半はフロッピーディスクなどのハードウェア媒体を指しています。全体を通じてファイルを指すように、「ここでいうデータファイルとは、サーバー・パソコン等を含むコンピュータの磁気ディスク、フロッピーディスク、光ディスク、磁気テープ、カートリッジ磁気テープ、DAT等の中のファイルを指している」等の表現とした方が良いかと思います。	日本銀行 岡田様(専)	「～の中のファイル」を追記するよう変更します。	⑤表現の統一・見直し	要	11/14 反映予定
41	実15	1	USBメモリ等、最近の保存媒体について言及しなくてよいか。	三井住友銀行 持田様(専) 山口様(検)	記憶媒体やストレージ等を含む表現に変更します。	⑤表現の統一・見直し	要	11/14 反映予定
42	実17	2	「・・・・保管にあたっては以下の方法がある。」につき「以下の例がある。」と記述（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	記述が「以下の方法」であるため、例示ではなく「限定列挙」として記載しています。	⑤表現の統一・見直し	否	
43	実19	2	「バックアップを取得するにあたっては・・・取得間隔を定めておくことが必要である。」について、プログラムファイルのバックアップであり、「取得間隔を定めておく」は表現として適切では無いと考えられる。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘のとおり表現として適切ではないため、「取得タイミングを定める」等の表現に変更しま	⑤表現の統一・見直し	要	11/14 反映予定
44	実20		「コンピューターウィルス対策」について、「コンピューターマルウェア対策」の方が適切かと考える。	農林中央金庫 常岡様(専) 今嶋様(検)	一般には、悪意をもったプログラムは、マルウエアやコンピュータウイルス、不正プログラム等、複数の名称が使われていますが、FISC安全対策基準では、以前から知られている、「コンピュータウイルス」という名称を使っています。 なお、生物に感染するウイルスと区別するために、コンピュータウイルスとしていますが、マルウエアについてはそれ自体がプログラムを指す（ウエアはソフトウエアからきている）ので、単にマルウエアと表現されているようです。	⑤表現の統一・見直し	否	
45	実21	1	「ルータ等ネットワーク機器の設定は定められた手続きに従って変更されなければならない。また、設定が不正に変更されたり、障害などで設定情報が失われたりする場合に備えて、コンフィグレーション情報等を適切に管理することが望ましい。」について、前段の「定められた」は不要であり、語尾は「必要である。」にしてはどうか。	農林中央金庫 常岡様(専) 今嶋様(検)	・「手続き」とは「事を行う順序次第（広辞苑）」であり、事前に承認された順序次第という意味で、「定められた手続き」という表現を使っています。 ・語尾の「変更されなければならない」は実質的に必須の対応であることを要求しているため、「変更することが必要である」に変更します。	②対策・例示の変更	要	10/23 反映予定
46	実21	2	「特に、公衆回線（ATM、ISDNなど）が接続されているネットワーク機器についてはモニタリングを行うなど、適切な管理を行うことが望ましい。」のモニタリングは何をモニタリングするのか分かりにくい。今日的に、公衆回線に限定する意味も分かりにくい。	農林中央金庫 常岡様(専) 今嶋様(検)	現在の実態を踏まえ適切な表現に見直します。	④時代背景に沿った見直し	要	11/14 反映予定
47	実21	2	ATM（Asynchronous Transfer Mode）は伝送方式の種類であるため、公衆回線に限らず、専用回線でも使用される場合があると思います。したがって、「公衆回線（ISDNなど）」と「ATM、」を削除しては如何でしょうか。	日本銀行 岡田様(専)	現在の実態を踏まえ適切な表現に見直します。	④時代背景に沿った見直し	要	11/14 反映予定
48	実21	3	「ルータへのアクセスについては、ID、パスワードで保護するなどの不正アクセス対策が必要である。」について、極めて重要なセキュリティであり、通常のID、パスワードだけでなく、特権IDや可変パスワードとその管理、アクセスモニタリング、操作ログモニタリングなどもっと対処が必要ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	現在の記載は、ID、パスワードで保護すれば良いと誤認される表現となっているため、それ以外の対策も必要であることがわかるように表現を見直します。	⑤表現の統一・見直し	要	11/14 反映予定
49	実21	3	本対策のみ、ルータに限定されているが、ルータ等が適切。	三井住友銀行 持田様(専) 山口様(検)	「ルータ等」に記載を変更します。	⑤表現の統一・見直し	要	10/23 反映予定
50	実22	1	「ルータ等ネットワーク機器の設定が不正に変更されたり・・・が必要である。」について、実質「実21」の1.設定情報の適切な管理と同等であり、基準としてまとめてはどうか。	農林中央金庫 常岡様(専) 今嶋様(検)	「適切な管理」と「バックアップ」については、ネットワーク以外にもドキュメント、プラグラム等の基準において別々に策定しているため、整合性の観点からまとめない方が良いと考えます。	①基準構成の変更	否	
51	実25	1	「重要帳票とは、例えば～」の記載があるが、他の項目と同様、「～の内容としては、以下の例がある」と記述（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘のとおり「～の内容としては、以下の例がある」と修正します。	⑤表現の統一・見直し	要	10/23 反映予定
52	実26	1	「ここでいう重要な印字済帳票とは、・・・、コンピュータの処理結果として作成されたすべてのものをいう。」とあるが、「コンピュータの処理結果として作成されたすべてのもの」と定義してしまうと、2.～4.の管理において実現不能とならないか。	農林中央金庫 常岡様(専) 今嶋様(検)	「すべてのもの」の記載表現を見直し対象範囲を明確にします。	⑤表現の統一・見直し	要	11/14 反映予定
53	実26	4	廃棄にあたり、「責任者が～が実施されたことを確認」との記載があるが、実25の3では「責任者が～を確認」としている。どちらも帳票の廃棄方法であることから、廃棄方法は統一すべきであり、「実施されたことを」確認するほうが、実態に即していると考える。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘のとおり修正します。（実25の3を、「実施されたことを確認する」に変更）	②対策・例示の変更	要	10/23 反映予定
54	実27	1	「ここでいう出力情報とは、・・・コンピュータシステムの処理結果として作成されたすべてのものを指す。」について、ポイントや具体策はベストプラクティクスベースの記載とはいえ、実現不能とならないか。	農林中央金庫 常岡様(専) 今嶋様(検)	「すべてのもの」の記載表現を見直し対象範囲を明確にします。	⑤表現の統一・見直し	要	11/14 反映予定
55	実28	1	渉外端末の権限の範囲を明確にすることが特に重要であるとあるが、他の項目と平仄を合わせ、「必要である」に記載を変更すべきではないか。そもそも「実29」、「実30」のいずれかにまとめられないか。	農林中央金庫 常岡様(専) 今嶋様(検)	【資料２－３】「重要である」を含む基準一覧　参照。 基準の統合については、No57のとおり順序性を考慮した基準構成としているため、原案のままとさせていただきます。	③要求レベルの変更 （語尾の変更）	ー	
56	実28	1	「取引の重要度等により」は「取引対象商品の重要度等により」ということか。 同じ商品でも金額や取引先の大小（重要度が異なる）で操作権限を分けるというように読めるが意味が違うのではないか。	三井住友銀行 持田様(専) 山口様(検)	「取引の重要度」は、商品の重要度や取引先の大小等、各金融機関によって判断基準が異なると考えられることから、現状の表現のままとさせていただきます。	②対策・例示の変更	否	
57	実29、30		細かいことになるが、基準の番号に関し、小項目（取引の管理）の中で、基礎基準が付加基準よりも早い番号の方が分かりやすい。「29」と「30」の入れ替え。	農林中央金庫 常岡様(専) 今嶋様(検)	操作権限（実28）やオペレータカード管理（実29）といった環境を整えて取引（実30）に臨む、さらに、運用時に対応すべき事項（実31）という順序性を考慮して記載しています。	①基準構成の変更	否	

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
58	実30	基準小項目	タイトルが「取引の操作内容を記録・検証のこと」とありますが、ここでいう「取引の操作内容」とは「（取引に対する）端末機操作の内容」を指すと思われます。「端末機操作の内容を記録・検証のこと」とするか、単に「操作内容を記録・検証のこと」としては如何でしょうか。	日本銀行 岡田様(専)	基準小項目を「取引の端末機操作の内容を記録・検証すること」に変更します。	①基準構成の変更	要	10/17 反映済
59	実32	適用にあたっての考え方	「適用にあたっての考え方」およびその下の基準項目の説明等の欄に記述されている「電子的価値を蓄積する媒体」の「電子的価値を蓄積する」とは、「電子的に価値を蓄積する」としては如何でしょうか。	日本銀行 岡田様(専)	本基準書においては「電子的価値」を固有名詞として使用しており、プリペイドカード、電子マネーといったものを指します。よって現状の表現のままとさせていただきます。	⑤表現の統一・見直し	否	
60	実33	1	「金融機関等で利用する暗号鍵のユーザーへの配布と使用、鍵の紛失・損失時の回復、鍵の回収、有効期限等について・・・」について，鍵の紛失・損失時の回復，鍵の回収といった表現は適切か。	農林中央金庫 常岡様(専) 今嶋様(検)	調査したところ、「鍵の紛失・損失時の回復」については問題ありませんが、「鍵の回収」についてはおこなっていないと考えられることから削除します。	⑤表現の統一・見直し	要	10/23 反映予定
61	実36	基準小項目	タイトルについて，「CD・ATM等の」と枕詞は置いたほうが良い。	農林中央金庫 常岡様(専) 今嶋様(検)	基準小項目に「CD・ATM等及び無人店舗の」を追加するよう修正します。	①基準構成の変更	要	10/17 反映済
62	実36	5	ハードディスク等を使用して何を集中管理するか対象を明確に記載すべき。	三井住友銀行 持田様(専) 山口様(検)	対象である「防犯ビデオ」を追記します。	⑤表現の統一・見直し	要	10/23 反映予定
63	実36	6	「防犯ビデオは顧客からの届出状況等に応じて一定期間の保存を考慮することが望ましい」とありますが、ここでいう「顧客からの届出状況」とは何を指しているのでしょうか。単に「防犯ビデオは一定期間の保存を考慮することが望ましい」としては如何でしょうか。	日本銀行 岡田様(専)	「顧客からの届出状況等に応じて」の記載はわかりにくいため削除します。	⑤表現の統一・見直し	要	10/23 反映予定
64	実37	1	「無人店舗における異常状態を発見するため，管理センター等で監視することが望ましい。」と記載。一方で，実55では，3.にて「…無人監視による時間帯の連絡網，連絡方法…が必要である。」としており，無人監視を前提とする記述。実37について，付加基準の必須対策として語尾を「必要である。」が適当と思料。	農林中央金庫 常岡様(専) 今嶋様(検)	「管理センター」は自金融機関の管理センターを指していることから、設置が困難な場合を想定して「望ましい」としています。（対策2において「設置できない場合の代替策が記載されている）	③要求レベルの変更 （語尾の変更）	否	
65	実40	2	最新版を常備する旨の記載を追記した方がいい（実5－2の内容を踏まえ）	農林中央金庫 常岡様(専) 今嶋様(検)	修正します。2の「常備しておくことが必要である。」の前に「最新版を」を追加します。	②対策・例示の変更	要	10/23 反映予定
66	実43	タイトル	「実42」同様に「キャッシュカード等」とした方が良いのではないか（こちらは付加基準とされている）。	農林中央金庫 常岡様(専) 今嶋様(検)	キャッシュカード以外のカード（クレジット等）も想定しているため、「カード」と記載しています。	⑤表現の統一・見直し	否	
67	実44	タイトル	「実42」同様に「キャッシュカード等」とした方が良いのではないか（こちらは付加基準とされている）。	農林中央金庫 常岡様(専) 今嶋様(検)	キャッシュカード以外のカード（クレジット等）も想定しているため、「カード」と記載しています。	⑤表現の統一・見直し	否	
68	実49、141他		セキュリティホールという語句は、脆弱性が適切な場合が散見。	三井住友銀行 持田様(専) 山口様(検)	例えば、実141の「OS等のセキュリティホールを・・・」は、ご指摘の通り「脆弱性」が適切と考えます。他の箇所についても調査のうえ適切な表現に見直します。	⑤表現の統一・見直し	要	11/14 反映予定
69	実49、141他	2(5)緊急度や重要度の判断	最近の攻撃は、脆弱性を突かれるのは、外部ネットワークの接続部分に限らず、パソコンの脆弱性も対象となっているので、この緊急度・重要度の判断は、不適切。取り扱う情報資産の重要度、入口・出口対策を考慮した外部との不正アクセスの可能性等が妥当と思料。	三井住友銀行 持田様(専) 山口様(検)	例示の①は緊急度が高く速やかに適用するケース、②は影響を十分に確認してから適用するケースとなります。	②対策・例示の変更	－	
70	実51		基礎基準とされているが，すべてが「望ましい。」との記載になっている。 サブタイトル上の表記に，「望ましい。」が残置。	農林中央金庫 常岡様(専) 今嶋様(検)	サブタイトル（適用にあたっての考え方）については「～すること」に統一します。	⑤表現の統一・見直し	要	10/23 反映予定
71	実54	1(4)	外部記憶媒体も明記してはどうか。	三井住友銀行 持田様(専) 山口様(検)	「記憶媒体」を追記します。	②対策・例示の変更	要	10/23 反映予定
72	実55	2(1)(5)	例示について，(2)の自動車電話の記載は不要ではないか。 (5)についても、タブレットなど色々な態様があることから，パソコンではなく，インターネット等で良いのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	以下のとおり修正します。 ・自動車電話⇒削除 ・パソコン（インターネット等の利用）⇒メール・インターネット等	④時代背景に沿った見直し	要	10/23 反映予定
73	実55	2	メールがどこに含まれるのかよくわからないので、括弧書きで加えた方が良い。	三井住友銀行 持田様(専) 山口様(検)	(5)パソコン（インターネット等の利用）⇒(5)メール・インターネット等 とします。	②対策・例示の変更	要	10/23 反映予定
74	実57	6	「EUCシステムについても、取扱う業務の重要度や障害発生時の影響度に応じて、障害情報の収集・分析・障害対応・報告を行うための管理体制を整備することが必要である。」とあるが、「望ましい」のほうがよいのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	従来「・・・こと」と「・・・必要である」は同じ意味で使っており、今回後者に統一したものです。 なお、EUCにおいても、金額計算等の重要な業務で使用される場合があり、「重要度や障害発生時の影響度に応じて」必要であるとしたものです。	③要求レベルの変更 （語尾の変更）	否	
75	実58	1	中段の文章「本基準におけるコンティンジェンシープランとは、・・・障害等により重大な損害を被り業務の遂行が果たせなくなった場合に・・・緊急時対応計画のことである。」の「重大な損害を被り」について，損害とは事故などでの不利益を言うものであり，文章の趣旨からは適当ではないものと思料。「重大な被害を受け」としてはどうか。	農林中央金庫 常岡様(専) 今嶋様(検)	「被害」とすると外部要因のみを指し限定的となります。コンテ手引書の定義を引用しており、原案のままとさせていただきます。	⑤表現の統一・見直し	否	
76	実58	2	「上記コンティンジェンシープランの策定に際して考慮すべき内容(1)～(9)のうち，(3)～(6)に揚げた内容については手順書として文書化することが必要である。」について，(1)～(9)を指定されているが，基準項目の参照としてその後に(1)～(17)の表記もあり，番号の記載は工夫が必要(その前にも(1)～(8)の表記もある)。 また，(1)～(9)については，前段でベストプラクティクスとして例示されているものであり，「(3)～(6)につき，整理する場合には手順書として文書化することが必要である。」としてはどうか。また、(6)の「早期に事態を収拾して、平常業務への復旧を図るために必要な措置を明確にする。」については、状況に応じた対処が必要となり、事前に必要な措置を文書化することは、現実的には困難ではないか。 （「(3)～(6)に揚げた内容について」の「揚げた」は，「挙げた」もしくは「掲げた」が適当。）	農林中央金庫 常岡様(専) 今嶋様(検)	対策1の文章について「・・・例がある。このうち、(3)から(6)は、・・・手順書として文書化することが必要である」と修正します。また「揚げた」は誤字ですので「掲げた」に修正します。	⑤表現の統一・見直し	要	10/23 反映予定
77	実58	6	「障害時・災害時等におけるシステムの復旧やバックアップサイトへの切換えを行う際は、・・・・通常時と同等のレベルを維持することが必要である」 については、バックアップサイトにおける提供すべき機能の考え方は金融機関区々であり、必須対策には適応しないと考える。	農林中央金庫 常岡様(専) 今嶋様(検)	本対策は、「機能」のレベル維持を示しているのではなく、「セキュリティ」のレベル維持を示しており、必要なセキュリティのレベルは維持するという点で従来から「必要である」として賛同を得られているものと考えられます。	③要求レベルの変更 （語尾の変更）	否	

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
78	実59	6	「パソコン等を別の用途に再利用するときには、コンピュータウイルスや不正プログラムが混入されていないかチェックすることが必要である。」について，再利用を別の社員が使用する時と考えると，ウィルス，不正プログラムのチェック以外にも，データの初期化等考慮すべき事項があるものと思料。	農林中央金庫 常岡様(専) 今嶋様(検)	再利用先の環境により対応が異なると考えられ、必須の対策としては現状の記載のままで問題ないと考えます。	②対策・例示の変更	否	
79	実60	3	「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。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。」について，気持ちは理解できるが，語尾は「重要である。」ではなく，「必要である。」に統一した方が適切と思料。他にも何ヵ所かあるが，使い分けは難しいものと思料。	農林中央金庫 常岡様(専) 今嶋様(検)	【資料２－３】「重要である」を含む基準一覧　参照。	③要求レベルの変更 （語尾の変更）	―	
80	実61	1	1.(1)②において、「また、テスト用端末ではログオン手順やID体系を整備したり、～、本番端末との混同を避けることが望ましい」とあります。これまでの「例」では、「必要である」、「望ましい」といった「必要性のレベル感」については記述されていません。特に理由がなければ、「ことが望ましい」を削除しては如何でしょうか。	日本銀行 岡田様(専)	例示の語尾修正漏れ。「望ましい」を削除します。	⑤表現の統一・見直し	要	10/23 反映予定
81	実61	1	開発・テスト用のコンピュータ等の資源は十分に確保する望ましい。 文がおかしいので修正が必要。	三井住友銀行 持田様(専) 山口様(検)	例示の語尾修正誤り。「確保する」に修正します。	⑤表現の統一・見直し	要	10/23 反映予定
82	実62	1	字句の修正などの関係と思われますが、「行う」と「実施する」が混在しています。 表記の違いが意図する意味を解説願います。	日本ユニシス 森下様(専) 後藤様(検)	「行う」と「実施する」ともに行為としては同じですが、「実施する」は「計画・予定通りに行う」場合に使用しています。なお、今回の「読みやすさ対応」では従来の表現を維持しています。	その他（確認等）	―	
83	実62	1・2	実60と同様。「重要である」は「必要である」に統一すべき。	農林中央金庫 常岡様(専) 今嶋様(検)	【資料２－３】「重要である」を含む基準一覧　参照。	③要求レベルの変更 （語尾の変更）	―	
84	実62	1	語尾が重要であるになっている。	三井住友銀行 持田様(専) 山口様(検)	【資料２－３】「重要である」を含む基準一覧　参照。	③要求レベルの変更 （語尾の変更）	―	
85	実63		ここで言うシステムドキュメントとは，操作マニュアルのようなものを言っているのか，設計書類も含めて言っているのか分かりにくい。「作成対象とするものを決め」とあるが，実64とあわせ分かりやすくした方が良いものと思料。ものによっては，利用部門の責任者の承認は不要であろうし，操作マニュアル類であれば，内容によっては施錠保管が不要なものもあるのではないか。 （実23・24を含め、「ドキュメント」「システムドキュメント」を定義したほうがいい。）	農林中央金庫 常岡様(専) 今嶋様(検)	実23,24の「ドキュメント」については、運用時におけるシステムドキュメントであり、実63,64の「ドキュメント」は開発時のシステムドキュメントとなります。 実63,64の「システムドキュメント」には、実23,24の「ドキュメント」も含まれており表現として適切でないことから、以下のとおり修正します。 ・実23,24　：　運用時におけるドキュメント ・実63,64　：　開発時におけるドキュメント	①基準構成の変更	要	10/17 反映済
86	実67	3	実68の内容と重複するため、実67からは削除してよいのではないか。	三井住友銀行 持田様(専) 山口様(検)	重複しているため実68の3は削除します。	②対策・例示の変更	要	10/23 反映予定
87	実71	1	最初の文の後半「～管理者は各設備の容量及び性能を把握するとともに、以下のような点に留意することが必要である。」と次の文「要領及び性能を把握する際の留意事項としては、以下の例がある」の内容は重複しているため、一方に纏めては如何でしょうか。	日本銀行 岡田様(専)	「要領及び性能を把握する際の留意事項としては、以下の例がある」を削除します。	⑤表現の統一・見直し	要	10/23 反映予定
88	実71	1(11)	自動車電話は時代にあっておらず、削除して良いのではないか。	三井住友銀行 持田様(専) 山口様(検)	「自動車電話」は削除します。（実55も同様）	④時代背景に沿った見直し	要	10/23 反映予定
89	実73	2	具体的な例示がないまま、出店先の設備状況についても考慮とあり、設備に関するどのような点を考慮すべきかよく分からない。例示できないか。	三井住友銀行 持田様(専) 山口様(検)	設136「使用するストアの設備状況に応じて、適切な補強策を講ずること」を参照先として追加します。	②対策・例示の変更	要	10/23 反映予定
90	実84	2.(3)⑤	この検知策を記載するのであれば、複数IPアドレスからの同一アカウントによるログインの検知も記載すべき。	三井住友銀行 持田様(専) 山口様(検)	「同一IPアドレスからの複数アカウントによるログイン～」の例示は、過去のアカウント乗っ取りによる事故の発生を踏まえ追加するものです。	②対策・例示の変更	否	
91	実84	参考2	すでに第4次行動計画まで公表済み。	三井住友銀行 持田様(専) 山口様(検)	「重要インフラの情報セキュリティ対策に係る第２次行動計画」→「重要インフラの情報セキュリティ対策」に変更します。	④時代背景に沿った見直し	要	10/23 反映予定
92	実84		バイオメトリクスは実46の生体認証情報と同じと思われるので、用語を統一すべき。	農林中央金庫 常岡様(専) 今嶋様(検)	実46の1において、「生体認証情報」は、「バイオメトリクス」のうち行動的特徴、公知の身体的特徴を除く情報である旨定義しており、使い分けをしております。	⑤表現の統一・見直し	否	
93	実84	参考1	サイバーテロとサイバー攻撃には、安対基準上違いがあるのか?整理するべき。	農林中央金庫 常岡様(専) 今嶋様(検)	「サイバー攻撃」で統一します。 実84：サイバーテロ⇒サーバー攻撃に変更 実87（参考）、実88（参考）：警視庁　サイバー犯罪対策 についてはサイト名であるため変更しない。	⑤表現の統一・見直し	要	10/23 反映予定
94	実84、85	全般	標題は、不正使用防止と早期発見とで区別されているが、内容を見ると、金融機関による防止・発見と、利用者による発見とで区別されており、主体が異なることが標題で判るほうがよいと思料。若しくは、防止策と発見・検知策で分けるのであれば、発見策の中で、金融機関によるものと利用者によるものとを分けて記載すべきと思料。	三井住友銀行 持田様(専) 山口様(検)	実85「インターネット・モバイルサービスの不正使用を早期発見すること」 ⇒ 「インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること」に変更します。	①基準構成の変更	要	10/17 反映済
95	実85	1,2	実60と同様。「重要である」は「必要である」に統一すべき。 さらに、インターネット・モバイルサービスを提供する場合であり，付加基準とすることが適当ではないか。 そのうえで、2.の文章の語尾について、付加基準の中の必須対策として「注意すること」⇒「注意することが必要である。」としてはどうか。	農林中央金庫 常岡様(専) 今嶋様(検)	【資料２－３】「重要である」を含む基準一覧　参照。	②対策・例示の変更	―	
96	実85	1	重要である、は、必須か例示か区別がつかない。	三井住友銀行 持田様(専) 山口様(検)	【資料２－３】「重要である」を含む基準一覧　参照。	③要求レベルの変更 （語尾の変更）	―	
97	実85	2	本対策が、必要があるのか、望ましいなのか、明記されていない。	三井住友銀行 持田様(専) 山口様(検)	「注意すること」は「注意することが必要である」に変更します。	③要求レベルの変更 （語尾の変更）	要	10/23 反映予定

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
98	実87		顧客に注意喚起すべき事項に、クラウドサービスにて利用する外部ストレージにID・パスワード情報を残さないことを入れてはどうか?（実際に不正送金被害の原因にもなっているため）	農林中央金庫 常岡様(専) 今嶋様(検)	iCloud等のバックアップデータに金融機関のID、パスワードを残してしまうケースが想定されますが、実87に「～スマートデバイスにファイルで保管した場合に盗難のリスクがある）」という類似した例示があります。	②対策・例示の変更	否	
99	実88	1	文章中に(1)～(12)と(1)～(2)，(1)～(3)が重複。参照する際不便なので，記載上の工夫が必要と思料。	農林中央金庫 常岡様(専) 今嶋様(検)	同一対策に関する例示が複数ある場合は、指摘いただいたとおりの記載となります。明確に分離していることから大きな支障はないと考えていますが、良い記載方法があればご教示願います。	⑤表現の統一・見直し	否	
100	実88	小項目	本項は、インターネット・モバイルサービス　に統一しないのか？	三井住友銀行 持田様(専) 山口様(検)	「インターネットやモバイル等を用いた金融サービス」⇒「インターネット・モバイルサービス」に変更します。	①基準構成の変更	要	10/17 反映済
101	実92	1	前段の説明では、「重要度に応じ」となっているが、解説部分には重要度の説明なく「必要である」となっている。装置の特性や重要度に応じて実施が必要なケースと必要でないケースがあるのであれば、それに触れず予防保守が「必要である」というのは適切でない。	三井住友銀行 持田様(専) 山口様(検)	「装置の特性や重要度に応じ、予防保守を実施することが必要である」に修正します。	⑤表現の統一・見直し	要	10/23 反映予定
102	実92	2	上記コメントに関連するが、24時間稼働であっても、予防保守しないケースも考えられるのでは。	三井住友銀行 持田様(専) 山口様(検)	「システムの機能及び制約に応じた」予防保守をおこなうことになります。	その他（確認等）	ー	
103	実93	2	「システムの目的や重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。特に、24時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい」とあります。本章は、「障害に備えた予備」を記載している箇所であるため、一般的なキャパシティ管理の章（実71）の留意事項に記載場所を移設しては如何でしょうか（同様の観点は、実94、実95、実96、実97にもあります）。	日本銀行 岡田様(専)	移設先として記載頂いた実71は「状況確認」をおこなう基準であり、システム構築における留意点を記載したものでありません。一方実93は「予備」に関する基準であり、該当の文章の記載場所として特段問題ないと考えております。	②対策・例示の変更	否	
104	実93	2	「2.(4)マルチプロセッサシステム」の説明の中に、「なお、切り離して運用する場合でも、ある程度の能力が確保できるように、中央処理装置の能力には余裕があることが有効である。」とあります。 これと平仄をとるため、「2.(2)デュアルシステム」においても、この説明と同様、2行の説明の後に、「なお、残りの系だけで運用する場合でも、ある程度の能力が確保できるように、本体装置の能力には余裕があることが有効である。」を追加しては如何でしょうか。	日本銀行 岡田様(専)	デュアルシステムは一般的には業務継続を目的とし余裕を必要とする構成ではないと考えられることから、原案のままとさせていただきたいと思います。	②対策・例示の変更	否	
105	実94	2	文章の語尾について「考えられる。」とあるが，「必要である。」とすることが適切ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘の部分は、こうした方法もあり得るという意味であり、例示と同等の表現としています。	③要求レベルの変更 （語尾の変更）	否	
106	実95	3	文章について，最後のみ「必要である。」とされているが，文章の構成からは，「望ましい。」が適切ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	例示の中の「必要である」のため「必要である」を削除します。	⑤表現の統一・見直し	要	10/23 反映予定
107	実99	1	「・・・・そのために考慮すべき点として、以下のものがある。」につき「以下の例がある。」と記述（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	「以下のものがある」の記述から、例示ではなく「限定列挙」として記載しています。	⑤表現の統一・見直し	否	
108	実99	1	「そのために考慮すべき点として以下のものがある」とありますが、安対基準全体の平仄を踏まえると「そのために考慮すべき点として以下の例がある」としては如何でしょうか。また、例であるため（1）および（2）の記載にある「必要である」は削除するべきかと思います。	日本銀行 岡田様(専)	「以下のものがある」の記述から、例示ではなく「限定列挙」として記載しています。	⑤表現の統一・見直し	否	
109	実99	1	現在の工程を終了し次工程へ進む判断を行うための基準（工程完了判定のための基準）は、重要な要素であり、属人化を防ぎ標準化する場合もあると思います。 「設計工程の標準化」の「1設計工程」について、「設計の各工程ごとにおこなうべき作業、内容、範囲、完了条件等」と記載しても良いと思います。	日本銀行 岡田様(専)	「設計の各工程ごとにおこなうべき作業、内容、範囲、完了条件等」に変更します。	②対策・例示の変更	要	10/23 反映予定
110	実99	1	「品質確保のための具体的な対策としては、以下の例がある。」として、4つ例示されていますが、そのうえにある例2つと区別する必要はないため、項番を以下のとおり連続させては如何でしょうか。 （1）システム開発の前提となる要件の明確化⇒（3） （2）設計作業の標準化　　⇒（4）　以下同様	日本銀行 岡田様(専)	ご指摘のとおり区別の必要はありませんので構成を見直します。（前半の(1)と後半の(1)は内容が一部重複しているため統合し、前半の(2)を(5)として連続させます）	②対策・例示の変更	要	10/23 反映予定
111	実99	（参考1）	「1.(1)③　アジャイルモデル」の説明のなかに、「早い環境変化に対応し、」は「速い環境変化」が適当と思います。	日本銀行 岡田様(専)	ご指摘のとおり「速い環境変化」に修正します。	⑤表現の統一・見直し	要	10/23 反映予定
112	実100	1	コーディングにあたっては、コーディング対象の規模・特性と開発生産性を踏まえて作業管理するかと思います。「（1）標準化」「④その他」に「c.開発生産性に関する指標の活用」「プログラムの規模・特性（開発言語、バッチ・オンライン処理の方式、入出力インターフェース等）に応じた開発生産性の指標値を用いることで、コーディング計画の適切な策定・管理を行うものである。」を例示しては如何でしょうか。	日本銀行 岡田様(専)	実100は品質向上を目的とした基準であり、標準化についても品質面を考慮して記載しています。記載いただいた開発生産性は重要な要素でありますが、この基準に記載する内容ではないと考えます。	②対策・例示の変更	否	
113	実100	3	Webシステムだけでなく、スマートデバイス向けの脆弱性対策を明記しなくてよいか。	三井住友銀行 持田様(専) 山口様(検)	スマートデバイスに関する基準については調査、検討中であり今後の改訂に反映する予定です。	②対策・例示の変更	ー	
114	実101	2	以下のような事項に留意することが必要である　となっており、事例なのか必須項目なのか分からない。	三井住友銀行 持田様(専) 山口様(検)	「留意することが必要である」とは「気に留める必要があるが、実際に行うかどうかは判断が分かれる」という意味合いとして記載しています。	その他（確認等）	ー	
115	実101	2	テスト計画書で明確にしておかなければならない主要項目は以下のとおりである。は他の文章と文体（としては、以下の例がある）があっていない。	三井住友銀行 持田様(専) 山口様(検)	「以下のとおりである」の記述から、例示ではなく「限定列挙」として記載しています。	⑤表現の統一・見直し	否	
116	実102	3	プログラム配布前のウイルスチェックを必須項目とするのか？開発時のチェックがある中で必須項目とするのか。	三井住友銀行 持田様(専) 山口様(検)	従来よりプログラム配布前の（ウイルス）チェックは必須としています。	②対策・例示の変更	否	
117	実105	2	実60と同様。「重要である」は「必要である」に統一すべき。	農林中央金庫 常岡様(専) 今嶋様(検)	【資料２－３】「重要である」を含む基準一覧　参照。	③要求レベルの変更 （語尾の変更）	ー	
118	実107	1	(1)と(2)の位置付けが分からない。(1)(2)とも必須項目？	三井住友銀行 持田様(専) 山口様(検)	(1)は例示、(2)は必須対策となります。構成を見直します。	⑤表現の統一・見直し	要	11/14 反映予定

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の 修正要否	反映予定
119	実107	2	以下の例があるとしか書かれておらず、必須項目なのかどうか分からない。	三井住友銀行 持田様(専) 山口様(検)	対策を追記します。（構成を見直し）	⑤表現の統一・見直し	要	11/14 反映予定
120	実108	1	「負荷状態の監視制御機能」の例のうち、(1)③は資源使用状況に関するデータを蓄積し、分析するというものなので、（リアルタイムでの）「（1）監視機能」の1項目ではなく、1.の本文に記載することとしては如何でしょうか。 例えば、「1.コンピュータシステムの安定稼働のため、『各種資源の使用状況に関する統計データを定期的にチェックし、事務量の変化等の傾向分析結果をもとに能力増強などの対策を事前に講じるとともに、』各種資源の能力や容量の限界を超えないように負荷状態を監視し、必要に応じて制御する機能を充実することが必要である。」としては如何でしょうか。	日本銀行 岡田様(専)	ご指摘のとおり(1)③は「機能」の説明とは言い難く、記載を見直した方が良いと考えます。 ただし例示であることから提案いただいた対策への記載ではなく、選択的に適用可能な例示として記載すべきと考えます。	⑤表現の統一・見直し	要	11/14 反映予定
121	実115	1（例示）	「バックアップサイトの運営形態としては、以下のものがある。」につき「以下の例がある。」と記述（他の記述との並び）。	農林中央金庫 常岡様(専) 今嶋様(検)	「以下のものがある」の記述から、例示ではなく「限定列挙」として記載しています。	⑤表現の統一・見直し	否	
122	実115	3	囲みの中に、「『業務の優先度を考慮した』バックアップサイトを保有することが望ましい」とありますので、3.（1）、（2）に加え、この際に、以下の２点について加えては如何でしょうか。 「（3）バックアップサイトで提供される資源で行える業務の範囲、メインサイトで行う場合と比べた処理能力を確認しておくこと。」	日本銀行 岡田様(専)	提案いただいた3は「バックアップサイトの保有」という物理的な観点における考慮事項のため、原案のままとさせていただきます。尚、ご指摘の「業務の優先度を考慮」については、1の「バックアップサイトを保有することが望ましい」の前に加えたいと思います。	②対策・例示の変更	要	10/23 反映予定
123	実118	6	「対策を講じることが考えられる」の記載が不自然。「望ましい」に修正すべき。	農林中央金庫 常岡様(専) 今嶋様(検)	過去にテンペストのリスクが指摘されて追加した対策ですが、実害は報道されていないので、ベストプラクティス「望ましい」ではなく、例示の位置づけである「考えられる」としています。	③要求レベルの変更 （語尾の変更）	否	
124	実118	1	「ファイルの・・・。特に・・・。また、・・・。」は同じことを書いているのではないか。1点目は「望ましい」、2点目、3点目は具体的なケースとして「必要である」ということか。	三井住友銀行 持田様(専) 山口様(検)	個人データまたは電子的取引において蓄積されるデータ ： 暗号化・パスワード設定等が必要 上記以外の重要データ ： 暗号化が望ましい という区分けとなります。	その他（確認等）	ー	
125	実119	参考2	SSL3.0でさえほぼ使われない現状では、「SSL」は「TLS」と改めるべき。	農林中央金庫 常岡様(専) 今嶋様(検)	現状ではSSLの方が一般的に認知されていることから記載はそのままとさせていただきます。	②対策・例示の変更	否	
126	実130	1	「設けること」の後に「が必要である」を記載すべき。	農林中央金庫 常岡様(専) 今嶋様(検)	修正します。（必要であるを追記）	⑤表現の統一・見直し	要	10/23 反映予定
127	実140		1.に対応策、復旧策が例示されていますが、何れも不正アクセスが発生した後の対応策・復旧策が記載されています。例えば、WEBサーバの脆弱性や攻撃コードが公開された場合など、不正アクセスが発生していない時の対応策も有効と考えられますがので、その旨追記しては如何でしょうか。	日本銀行 岡田様(専)	実141の2に記載頂いた内容と同様の対策があるため原案のままとさせていただきます。	②対策・例示の変更	否	
128	実141～ 143		コンピュータウィルスという表記について，コンピュータマルウェアへの変更の検討（実20での意見と同内容）。	農林中央金庫 常岡様(専) 今嶋様(検)	実20と同じ回答となります。	⑤表現の統一・見直し	否	
129	実141	1(1)④	「可搬記憶媒体等の媒体からの侵入」を挙げているが、防御策例の中に物理封印の媒体制御が載っていないが、例示として入れる必要はないか。	農林中央金庫 常岡様(専) 今嶋様(検)	「媒体の物理封印」は、一般的には外部へのデータ漏洩防止の対策として認知されており、外部侵入の防止策としては現在の例示にあるウイルスチェック等の対策になると考えます。	②対策・例示の変更	否	
130	実142	1.(1)	「現時点ではスパイウェアの定義が確定していないことから」 　抗ウイルスソフトによって、何を不正プログラムと判定するかが異なるということであれば、この記述は不要と考える。製品の実装の違いであって、時間により定義の統一化がはかられるものではない。	農林中央金庫 常岡様(専) 今嶋様(検)	「現時点ではスパイウェアの定義が確定していないことから」を削除します。	④時代背景に沿った見直し	要	10/23 反映予定
131	実142	1.(1)1	抗ウィルスソフトの古いパターンファイルでは未検出のウィルスがシステム内に潜在している可能性があるため、「最新のウィルスパターンファイルを利用する」と併せて「最新のウィルスパターンファイルで定期的にフルスキャンを実行する」との追記もご検討いただきたいと存じます。	NTTデータ 鎌田様(専) 鈴木様(検)	「なお、抗ウイルスソフト等の使用にあたっては、最新のパターンファイルを利用し、定期的にウイルスチェックをおこなう。」に変更します。	②対策・例示の変更	要	10/23 反映予定

「重要である」を含む基準一覧

【資料2－3】
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

No	新基準番号	基礎／付加	旧基準番号	基準小項目	対策本文	委員ご意見	対応案1	対応案2	対応案3
1	実28	基礎	運38	各取引の操作権限を明確にすること。	1. 不正、不当取引を防止するため、取引の重要度等により端末機操作者等が操作できる権限の範囲を明確にすることが必要である。 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。**	他の項目と平仄を合わせ、**「必要である」**に記載を変更すべきではないか。	必須対策ではない他の表現に一律変更する。(「望ましい」等)	「必要である」 に変更(「特に」は削除) 類似の基準である実41「渉外端末の運用方法を明確にすること」の対策8「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」に変更することが適当と考えられる。	「重要である」は変更しない。 (前説にて必須対策ではない旨を明記する)
2	実50	基礎	運57	機器の管理方法を明確にすること。	1. 機器については、管理責任者を明確にするとともに、以下のような点から管理することが必要である。 (1) 関係者以外容易に接近できない。 (2) 入力機器(端末機など)、出力機器(プリンターなど)及び重要なサーバー等は、許可された人のみ操作ができる。 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。**			「望ましい」 に変更 システムによっては「把握」が容易で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と考えられる。	
3	実60	基礎	運67	システムの開発・変更手順を明確にすること。	3. 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。** 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。	語尾は「重要である。」ではなく,**「必要である。」**に統一した方が適切と思料。他にも何ヵ所かあるが, 使い分けは難しいものと思料。		「必要である」 に変更 参照先基準が全て基礎基準であることから、「必要である」に変更することが適当と考えられる。	
4	実62	基礎	運69	本番への移行手順を明確にすること。	1. 本番への移行は、移行作業にともなう障害を防止することが重要であり、本番システムへの切替えを安全・確実に行うため、システムの特性に応じて移行手順を明確にすることが必要である。 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。**	・実60と同様。「重要である」は**「必要である」**に統一すべき。 ・語尾が「重要である」になっている。		「必要がある」 に変更 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ることから、「必要である」に変更することが適当と考えられる。	
5	実85	付加	運104	インターネット・モバイルサービスの不正使用を早期発見すること。	1. ユーザーID等が不正使用されていないか、利用者自身で確認可能にすることが必要である。特に資金移動およ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。** 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。**	・実60と同様。「重要である」は**「必要である」**に統一すべき。 ・「重要である」は、必須か例示か区別がつかない。		1つ目:「必要である」 に変更 類似の基準である実84「インターネット・モバイルサービスの不正使用を防止すること」の対策1「特に資金移動～必要である」と同様に、「必要である」に変更することが適当と考えられる。 2つ目:「望ましい」 に変更 類似の基準である実87「インターネット・モバイルサービスの顧客対応方法を明確にすること」の対策3「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」と同様に、「望ましい」に変更することが適当と考えられる。	
6	実99	基礎	技9	設計段階でのソフトウェアの品質を確保すること。	1. 設計段階でのソフトウェアの信頼性向上のため、開発の前提となる要件を明確にするとともに、信頼度設計の考慮や設計作業の標準化等を行い、ソフトウェアの品質を確保することが必要である。 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。			「重要であり、～」 に変更 一般論を示しており対策ではない。利用者の混乱を招かないように「重要であり、～」とすることが適当と考えられる。	
7	実105	基礎	技15	機能の変更、追加作業時の品質を確保すること。	1. 機能の変更、追加作業時におけるソフトウェアの品質を確保するため、開発時の品質向上対策を準用することが必要である。 2. 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。**	実60と同様。「重要である」は**「必要である」**に統一すべき。		「望ましい」 に変更 内容から見て「極小化」が容易でないケースもあり得るため、「望ましい」に変更することが適当と考えられる。	
8	実125	基礎	技35	本人確認機能を設けること。	1. コンピュータ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者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。** 2. インターネットを介した電子的な取引や支払指図の受付等を行う場合は特に、なりすまし等を防止するため、通信相手が正当な権限を持った者であることを確認できる仕組みが必要である。			「必要である」 に変更 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ることから、「必要である」に変更することが適当と考えられる。	
9	実135	基礎	技43	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。	6. 外部ネットワークに接続するネットワークと、接続しないネットワークを物理的に分離することや、接続用仮想環境等による遮断措置を利用したネットワーク構成を検討することも必要である。 7. 本人確認機能等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。**【技35】			「望ましい」 に変更 アクセス権限等の確認(【技35】=実125)と併せて実施しないケースもあり得るため、「望ましい」に変更することが適当と考えられる。	

前文の構成・変更内容

新構成	（新）基準大項目	新基準番号（暫定）	旧基準番号	基準小項目	（新）基準中項目（【新】前文構成）	（旧）基準中項目（【旧】前文構成）	変更内容
Ⅰ　統制基準	1　内部の統制	統1	運1・2	システムの安全対策に係る重要事項を定めた規程を整備すること。	(1) 方針・計画	管理体制の確立(セキュリティ管理と責任の明確化)	新設
		統2	新設	中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。	(1) 方針・計画	#N/A	新設
		統3	技7	システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること。	(2) 組織体制	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	合体（見直し）
		統6	運3	セキュリティ管理体制を整備すること。	(2) 組織体制	管理体制の確立(セキュリティ管理と責任の明確化)	合体（見直し）
		統13	運113	サイバー攻撃対応態勢を整備すること。	(2) 組織体制	サイバー攻撃対応態勢の整備	合体（見直し）
		統7	運4	システム管理体制を整備すること。	(2) 組織体制	管理体制の確立(セキュリティ管理と責任の明確化)	合体（見直し）
		統8	運5	データ管理体制を整備すること。	(2) 組織体制	管理体制の確立(セキュリティ管理と責任の明確化)	合体（見直し）
		統9	運6	ネットワーク管理体制を整備すること。	(2) 組織体制	管理体制の確立(セキュリティ管理と責任の明確化)	合体（見直し）
		統12	運9	業務組織を整備すること。	(2) 組織体制	管理体制の確立(組織の整備)	合体（見直し）
		統10	運7	防災組織を整備すること。	(2) 組織体制	管理体制の確立(組織の整備)	合体（見直し）
		統11	運8	防犯組織を整備すること。	(2) 組織体制	管理体制の確立(組織の整備)	合体（見直し）
		統4	運10	各種業務の規則を整備すること。	(2) 組織体制	管理体制の確立(各種規定の整備)	合体（見直し）
		統5	運10-1	セキュリティ遵守状況を確認すること。	(3) 管理状況の評価	管理体制の確立(セキュリティ遵守状況の確認)	流用（見直し）
		統14	運80	セキュリティ教育を行うこと。	(4) 人材（要員・教育）	教育・訓練(教育・訓練)	合体（見直し）
		統15	運81	要員に対するスキルアップ教育を行うこと。	(4) 人材（要員・教育）	教育・訓練(教育・訓練)	合体（見直し）
		統17	運83	障害時・災害時に備えた教育・訓練を行うこと。	(4) 人材（要員・教育）	教育・訓練(教育・訓練)	合体（見直し）
		統18	運84	防災・防犯訓練を行うこと。	(4) 人材（要員・教育）	教育・訓練(教育・訓練)	合体（見直し）
		統19	運85	要員の人事管理を**適切に**行うこと。	(4) 人材（要員・教育）	要員管理(要員管理)	合体（見直し）
		統20	運86	要員の健康管理を**適切に**行うこと。	(4) 人材（要員・教育）	要員管理(要員管理)	合体（見直し）
	2　外部の統制	統21	運108他	外部委託を行う場合は、事前に目的や範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	(1) 外部委託管理	外部委託管理(外部委託業務管理)	新設
		統22	運109他	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	(1) 外部委託管理	外部委託管理(外部委託業務管理)	新設
		統23	運89	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。	(1) 外部委託管理	外部委託管理(外部委託業務管理)	新設
		統24	運90	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。	(1) 外部委託管理	外部委託管理(外部委託業務管理)	新設
		統27	新設	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。	(2) クラウドサービスの利用	#N/A	新設
		統28	新設	共同センターにおける有事の際の安全対策を講ずること。	(3) 共同センター	#N/A	新設
		統29	運90-1	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。	(4) 金融機関相互のシステム・ネットワークのサービス	外部委託管理(外部委託業務管理)	新設
Ⅱ　実務基準	1 情報セキュリティ	実116	技26	他人に暗証番号・パスワード等を知られないための対策を講ずること。	(1) データ保護	データ保護(漏洩防止)	合体（見直し）
		実117	技27	相手端末確認機能を設けること。	(1) データ保護	データ保護(漏洩防止)	合体（見直し）
		実118	技28	蓄積データの漏洩防止策を講ずること。	(1) データ保護	データ保護(漏洩防止)	合体（見直し）
		実119	技29	伝送データの漏洩防止策を講ずること。	(1) データ保護	データ保護(漏洩防止)	合体（見直し）
		実121	技31	ファイルに対するアクセス制御機能を設けること。	(1) データ保護	データ保護(破壊・改ざん防止)	合体（見直し）
		実122	技32	不良データ検出機能を充実すること。	(1) データ保護	データ保護(破壊・改ざん防止)	合体（見直し）
		実123	技33	伝送データの改ざん検知策を講ずること。	(1) データ保護	データ保護(検知策)	合体（見直し）
		実125	技35	本人確認機能を設けること。	(2) 不正使用防止	不正使用防止(予防策(アクセス権限確認))	流用（見直し）
		実126	技35-1	生体認証の特性を考慮し、必要な安全対策を検討すること。	(2) 不正使用防止	不正使用防止(予防策(アクセス権限確認))	流用（見直し）
		実127	技36	IDの不正使用防止機能を設けること。	(2) 不正使用防止	不正使用防止(予防策(アクセス権限確認))	流用（見直し）
		実128	技37	アクセス履歴を管理すること。	(2) 不正使用防止	不正使用防止(予防策(アクセス権限確認))	流用（見直し）
		実129	技38	取引制限機能を設けること。	(2) 不正使用防止	不正使用防止(予防策(利用範囲の制限))	流用（見直し）
		実130	技39	事故時の取引禁止機能を設けること。	(2) 不正使用防止	不正使用防止(予防策(利用範囲の制限))	流用（見直し）
		実133	技42	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。	(2) 不正使用防止	不正使用防止(予防策(不正・偽造防止対策))	流用（見直し）
		実135	技43	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。	(3) 外部ネットワークからの不正アクセス防止	不正使用防止(外部ネットワークからのアクセス制限)	流用（見直し）
		実136	技44	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。	(3) 外部ネットワークからの不正アクセス防止	不正使用防止(外部ネットワークからのアクセス制限)	流用（見直し）
		実137	技45	不正アクセスの監視機能を設けること。	(4) 不正検知策	不正使用防止(検知策)	流用（見直し）
		実138	技46	異常な取引状況を把握するための機能を設けること。	(4) 不正検知策	不正使用防止(検知策)	流用（見直し）

前文の構成・変更内容

新構成	（新）基準大項目	新基準番号（暫定）	旧基準番号	基準小項目	（新）基準中項目（【新】前文構成）	（旧）基準中項目（【旧】前文構成）	変更内容
		実139	技47	異例取引の監視機能を設けること。	(4) 不正検知策	不正使用防止(検知策)	流用（見直し）
		実140	技48	不正アクセスの発生に備えて対応策、復旧策を講ずる~~講じておく~~こと。	(5) 不正発生時の対応策	不正使用防止(対応策)	流用（見直し）
		実141	技49	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	(6) 不正プログラム対策	不正プログラム防止(防御策)	合体（見直し）
		実142	技50	コンピュータウイルス等不正プログラムの検知対策を講ずること。	(6) 不正プログラム対策	不正プログラム防止(検知策)	合体（見直し）
		実143	技51	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。	(6) 不正プログラム対策	不正プログラム防止(復旧策)	合体（見直し）
	2 システム運用共通	実4	運14	通常時マニュアルを整備すること。	(1) マニュアルの整備	運用管理(マニュアルの整備)	流用（見直し）
		実5	運15	障害時・災害時マニュアルを整備すること。	(1) マニュアルの整備	運用管理(マニュアルの整備)	流用（見直し）
		実6	運16	各種資源、システムへのアクセス権限を明確にすること。	(2) アクセス権限の管理	運用管理(アクセス権限の管理)	流用（見直し）
		実7	運17	パスワードが他人に知られないための措置を講ずる~~講じておく~~こと。	(2) アクセス権限の管理	運用管理(アクセス権限の管理)	流用（見直し）
		実8	運18	各種資源、システムへのアクセス権限の付与、見直し手続きを明確~~化~~にすること。	(2) アクセス権限の管理	運用管理(アクセス権限の管理)	流用（見直し）
		実15	運25	データファイルの授受・管理方法を定めること。	(3) データ管理	運用管理(データファイル管理)	合体（見直し）
		実16	運26	データファイルの修正管理方法を明確にすること。	(3) データ管理	運用管理(データファイル管理)	合体（見直し）
		実33	運43	暗号鍵の利用において運用管理方法を明確にすること。	(3) データ管理	運用管理(暗号鍵の管理)	合体（見直し）
		統16	運82	オペレーション習熟のための教育および訓練を行うこと。	(4) オペレーション習熟	教育・訓練(教育・訓練)	流用（見直し）
		実20	運30	コンピュータウイルス対策を講ずること。	(5) コンピュータウイルス対策	運用管理(コンピュータウイルス対策)	流用（見直し）
		実48	運55	接続契約内容を明確にすること。	(6) 外部接続管理	運用管理(外部接続管理)	流用（見直し）
		実49	運56	外部接続における運用管理方法を明確にすること。	(6) 外部接続管理	運用管理(外部接続管理)	流用（見直し）
	3 運行管理	実9	運19	オペレータの資格確認を行うこと。	(1) オペレーション管理	運用管理(オペレーション管理)	流用（見直し）
		実10	運20	オペレーションの依頼・承認手続きを明確にすること。	(1) オペレーション管理	運用管理(オペレーション管理)	流用（見直し）
		実11	運21	オペレーション実行体制を明確にすること。	(1) オペレーション管理	運用管理(オペレーション管理)	流用（見直し）
		実12	運22	オペレーションの記録、確認を行うこと。	(1) オペレーション管理	運用管理(オペレーション管理)	流用（見直し）
		実13	運23	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。	(1) オペレーション管理	運用管理(オペレーション管理)	ー
		実17	運27	データファイルのバックアップを確保すること。	(2) データファイル管理	運用管理(データファイル管理)	流用（見直し）
		実18	運28	プログラムファイルの管理方法を明確にすること。	(3) プログラムファイル管理	運用管理(プログラムファイル管理)	流用（見直し）
		実19	運29	プログラムファイルのバックアップを確保すること。	(3) プログラムファイル管理	運用管理(プログラムファイル管理)	流用（見直し）
		実21	運31	ネットワークの設定情報の管理を行うこと。	(4) ネットワーク設定情報管理	運用管理(ネットワーク設定情報管理)	流用（見直し）
		実22	運32	ネットワークの設定情報のバックアップを確保すること。	(4) ネットワーク設定情報管理	運用管理(ネットワーク設定情報管理)	流用（見直し）
		実23	運33	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。	(5) 運用時ドキュメント管理	運用管理(ドキュメント管理)	流用（見直し）
		実24	運34	ドキュメントのバックアップを確保すること。	(5) 運用時ドキュメント管理	運用管理(ドキュメント管理)	流用（見直し）
		実53	運60	システムの運行状況の監視体制を整備すること。	(6) 運行監視	運用管理(運行監視)	流用（見直し）
	4 各種設備管理	実47	運54	各種資源の能力及び使用状況の確認を行うこと。	(1) 資源管理	運用管理(資源管理)	流用（見直し）
		実59	運66	ハードウェア、ソフトウェアの管理を行うこと。	(2) 機器の管理	システム開発・変更(ハードウェア・ソフトウェア管理)	合体（見直し）
		実50	運57	機器の管理方法を明確にすること。	(2) 機器の管理	運用管理(機器の管理)	合体（見直し）
		実51	運58	ネットワーク関連機器の保護措置を講ずること。	(2) 機器の管理	運用管理(機器の管理)	合体（見直し）
		実52	運59	機器の保守方法を明確にすること。	(2) 機器の管理	運用管理(機器の管理)	合体（見直し）
		実92	技1	機器の予防保守を実施すること。	(2) 機器の管理	ハードウェアの信頼性向上対策(ハードウェアの障害予防策)	合体（見直し）
		実69	運76	コンピュータ関連設備の管理方法を明確にすること。	(3) コンピュータ関連設備の保守管理	各種設備管理(保守管理)	合体（見直し）
		実70	運77	コンピュータ関連設備の保守方法を明確にすること。	(3) コンピュータ関連設備の保守管理	各種設備管理(保守管理)	合体（見直し）
		実71	運78	コンピュータ関連設備の能力および使用状況の確認を行うこと。	(3) コンピュータ関連設備の保守管理	各種設備管理(資源管理)	合体（見直し）
		実1	運11	入館（室）の資格付与、及び鍵の管理を行うこと。	(4) 入退館（室）管理	入退管理(入退館(室)管理)	合体（見直し）
		実2	運12	入退館管理を行うこと。	(4) 入退館（室）管理	入退管理(入退館(室)管理)	合体（見直し）
		実3	運13	入退室管理を行うこと。	(4) 入退館（室）管理	入退管理(入退館(室)管理)	合体（見直し）
		実54	運61	入室後の作業を管理すること。	(4) 入退館（室）管理	運用管理(コンピュータ室・データ保管室の管理)	合体（見直し）
		実72	運79	各種設備の監視体制を整備すること。	(5) 監視	各種設備管理(監視)	流用（見直し）
	5 システムの利用	実28	運38	各取引の操作権限を明確にすること。	(1) 取引の管理	運用管理(取引の管理)	流用（見直し）
		実29	運39	オペレータカードの管理を行うこと。	(1) 取引の管理	運用管理(取引の管理)	流用（見直し）

前文の構成・変更内容

新構成	（新）基準大項目	新基準番号（暫定）	旧基準番号	基準小項目	（新）基準中項目（【新】前文構成）	（旧）基準中項目（【旧】前文構成）	変更内容
		実30	運40	取引の端末操作の内容を記録・検証すること。	(1) 取引の管理	運用管理(取引の管理)	流用（見直し）
		実31	運41	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。	(1) 取引の管理	運用管理(取引の管理)	流用（見直し）
		実14	運24	データの入力管理を行うこと。	(2) 入出力管理	運用管理(入力管理)	合体（見直し）
		実27	運37	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。	(2) 入出力管理	運用管理(出力管理)	合体（見直し）
		実25	運35	未使用重要帳票の管理方法を明確にすること。	(3) 帳票管理	運用管理(帳票管理)	流用（見直し）
		実26	運36	重要な印字済帳票の取扱方法を明確にすること。	(3) 帳票管理	運用管理(帳票管理)	流用（見直し）
		実45	運53	顧客データの保護策を講ずること。	(4) 顧客データ保護	運用管理(顧客データ保護)	流用（見直し）
		実46	運53-1	生体認証における生体認証情報の安全管理措置を講ずること。	(4) 顧客データ保護	運用管理(顧客データ保護)	流用（見直し）
	6 緊急時の対応	実55	運62	障害時・災害時の関係者への連絡手順を明確にすること。	(1) 障害時・災害時対応策	運用管理(障害時・災害時対応策)	流用（見直し）
		実56	運63	障害時・災害時復旧手順を明確にすること。	(1) 障害時・災害時対応策	運用管理(障害時・災害時対応策)	流用（見直し）
		実57	運64	障害の原因を調査・分析すること。	(1) 障害時・災害時対応策	運用管理(障害時・災害時対応策)	流用（見直し）
		実58	運65	コンティンジェンシープランを策定すること。	(2) コンティンジェンシープランの策定	運用管理(コンティンジェンシープランの策定)	流用（見直し）
		実115	技25	バックアップサイトを保有すること。	(3) バックアップサイト	災害時対策(バックアップサイト)	流用（見直し）
	7 システム開発・変更	実60	運67	システムの開発・変更手順を明確にすること。	(1) システム開発・変更管理	システム開発・変更(システム開発・変更管理)	流用（見直し）
		実61	運68	テスト環境を整備すること。	(1) システム開発・変更管理	システム開発・変更(システム開発・変更管理)	流用（見直し）
		実62	運69	本番への移行手順を明確にすること。	(1) システム開発・変更管理	システム開発・変更(システム開発・変更管理)	流用（見直し）
		実63	運70	開発・変更時のシステムドキュメントの作成手順を定めること。	(2) 開発・変更時ドキュメント管理	システム開発・変更(ドキュメント管理)	流用（見直し）
		実64	運71	開発・変更時のシステムドキュメントの保管管理方法を明確にすること。	(2) 開発・変更時ドキュメント管理	システム開発・変更(ドキュメント管理)	流用（見直し）
		実65	運72	パッケージの評価体制を整備すること。	(3) パッケージの導入	システム開発・変更(パッケージの導入)	流用（見直し）
		実66	運73	パッケージの運用・管理体制を明確にすること。	(3) パッケージの導入	システム開発・変更(パッケージの導入)	流用（見直し）
		実67	運74	システムの廃棄計画、手順を策定すること。	(4) システムの廃棄	システム開発・変更(システムの廃棄)	流用（見直し）
		実68	運75	システム廃棄時の情報漏洩防止対策を講ずること。	(4) システムの廃棄	システム開発・変更(システムの廃棄)	流用（見直し）
	8 システムの信頼性向上対策	実93	技2	本体装置の予備を設けること。	(1) ハードウェアの予備	ハードウェアの信頼性向上対策(ハードウェアの予備)	流用（見直し）
		実94	技3	周辺装置の予備を設けること。	(1) ハードウェアの予備	ハードウェアの信頼性向上対策(ハードウェアの予備)	流用（見直し）
		実95	技4	通信系装置の予備を設けること。	(1) ハードウェアの予備	ハードウェアの信頼性向上対策(ハードウェアの予備)	流用（見直し）
		実96	技5	回線の予備を設けること。	(1) ハードウェアの予備	ハードウェアの信頼性向上対策(ハードウェアの予備)	流用（見直し）
		実97	技6	端末系装置の予備を設けること。	(1) ハードウェアの予備	ハードウェアの信頼性向上対策(ハードウェアの予備)	流用（見直し）
		実98	技8	必要となるセキュリティ機能を取り込むこと。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	流用（見直し）
		実99	技9	設計段階~~での~~におけるソフトウェアの品質を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	流用（見直し）
		実100	技10	プログラム作成段階~~での~~における品質を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	流用（見直し）
		実101	技11	テスト段階~~での~~におけるソフトウェアの品質を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	流用（見直し）
		実102	技12	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	流用（見直し）
		実103	技13	パッケージ導入にあたり、ソフトウェアの品質を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(開発時の品質向上対策)	流用（見直し）
		実104	技14	定型的変更作業時の正確性を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(メンテナンス時の品質向上対策)	流用（見直し）
		実105	技15	機能の変更、追加作業時の品質を確保すること。	(2) ソフトウエアの品質向上対策	ソフトウェアの信頼性向上対策(メンテナンス時の品質向上対策)	流用（見直し）
		実120	技30	ファイルに対する排他制御機能を設けること。	(2) ソフトウエアの品質向上対策	データ保護(破壊・改ざん防止)	流用（見直し）
		実124	技34	ファイル突合機能を設けること。	(2) ソフトウエアの品質向上対策	データ保護(検知策)	流用（見直し）
		実106	技16	オペレーションの自動化、簡略化を図ること。	(3) 運用時の信頼性向上対策	運用時の信頼性向上対策(運用時の信頼性向上対策)	流用（見直し）
		実107	技17	オペレーションのチェック機能を充実すること。	(3) 運用時の信頼性向上対策	運用時の信頼性向上対策(運用時の信頼性向上対策)	流用（見直し）
		実108	技18	負荷状態の監視制御機能を充実すること。	(3) 運用時の信頼性向上対策	運用時の信頼性向上対策(運用時の信頼性向上対策)	流用（見直し）
		実110	技20	システム運用状況の監視機能を設けること。	(4) 障害の早期発見・回復機能	障害の早期発見・早期回復(障害の早期発見)	流用（見直し）
		実111	技21	障害の検出および障害箇所の切り分け機能を設けること。	(4) 障害の早期発見・回復機能	障害の早期発見・早期回復(障害の早期発見)	流用（見直し）
		実112	技22	障害時の縮退・再構成機能を設けること。	(4) 障害の早期発見・回復機能	障害の早期発見・早期回復(障害の早期回復)	流用（見直し）
		実113	技23	障害時の取引制限機能を設けること。	(4) 障害の早期発見・回復機能	障害の早期発見・早期回復(障害の早期回復)	流用（見直し）
		実114	技24	障害時のリカバリ機能を設けること。	(4) 障害の早期発見・回復機能	障害の早期発見・早期回復(障害の早期回復)	流用（見直し）
	9 個別業務・サービス	実42	運51	カードの管理方法を明確にすること。	(1) カード取引サービス	運用管理(カード管理)	合体（見直し）

前文の構成・変更内容

新構成	（新）基準大項目	新基準番号（暫定）	旧基準番号	基準小項目	（新）基準中項目（【新】前文構成）	（旧）基準中項目（【旧】前文構成）	変更内容
		実43	運51-1	カード取引等に関する犯罪について注意喚起を行うこと。	(1) カード取引サービス	運用管理(カード管理)	合体（見直し）
		実35	運44-1	CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること。	(1) カード取引サービス	運用管理(厳正な本人確認の実施)	合体（見直し）
		実44	運52	指定された口座のカード取引監視方法を明確にすること。	(1) カード取引サービス	運用管理(カード管理)	合体（見直し）
		実131	技40	カードの偽造防止対策のための技術的措置を講ずること。	(1) カード取引サービス	不正使用防止(予防策(不正・偽造防止対策))	合体（見直し）
		実84	運103	インターネット・モバイルサービスの不正使用を防止すること。	(2) インターネット・モバイルサービス	オープンネットワークを利用した金融サービス(インターネット、モバイル)	流用（見直し）
		実85	運104	インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること。不正使用を早期発見すること。	(2) インターネット・モバイルサービス	オープンネットワークを利用した金融サービス(インターネット、モバイル)	流用（見直し）
		実86	運105	インターネット・モバイルサービスの安全対策に関する情報開示をすること。	(2) インターネット・モバイルサービス	オープンネットワークを利用した金融サービス(インターネット、モバイル)	流用（見直し）
		実87	運105-1	インターネット・モバイルサービスの顧客対応方法を明確にすること。	(2) インターネット・モバイルサービス	オープンネットワークを利用した金融サービス(インターネット、モバイル)	流用（見直し）
		実88	運106	インターネット・モバイルサービスインターネットやモバイル等を用いた金融サービスの運用管理方法を明確化にすること。	(2) インターネット・モバイルサービス	オープンネットワークを利用した金融サービス(インターネット、モバイル)	流用（見直し）
		実34	運44	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。	(4) 厳正な本人確認の実施	運用管理(厳正な本人確認の実施)	流用（見直し）
		実41	運50	渉外端末の運用管理方法を明確にすること。	(3) 渉外端末の管理	運用管理(渉外端末の管理)	流用（見直し）
		実36	運45	CD・ATM等及び無人店舗の運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。	(4) CD・ATM等及び無人店舗の管理	運用管理(CD・ATM等および無人店舗の管理)	流用（見直し）
		実37	運46	無人店舗の監視体制を明確にすること。	(4) CD・ATM等及び無人店舗の管理	運用管理(CD・ATM等および無人店舗の管理)	流用（見直し）
		実38	運47	無人店舗の防犯体制を明確にすること。	(4) CD・ATM等及び無人店舗の管理	運用管理(CD・ATM等および無人店舗の管理)	流用（見直し）
		実39	運48	無人店舗の障害時・災害時の対応方法を明確にすること。	(4) CD・ATM等及び無人店舗の管理	運用管理(CD・ATM等および無人店舗の管理)	流用（見直し）
		実40	運49	無人店舗の関係マニュアルの整備を行うこと。	(4) CD・ATM等及び無人店舗の管理	運用管理(CD・ATM等および無人店舗の管理)	流用（見直し）
		実109	技19	CD・ATM等の遠隔制御機能を設けること。	(4) CD・ATM等及び無人店舗の管理	運用時の信頼性向上対策(運用時の信頼性向上対策)	流用（見直し）
		実73	運92	インストアブランチの出店先の選定基準を明確にすること。	(5) インストアブランチ	インストアブランチ	流用（見直し）
		実74	運93	コンビニATMの出店先の選定基準を明確にすること。	(6) コンビニATM	コンビニATM	流用（見直し）
		実75	運94	コンビニATMの現金装填等メンテナンス時の防犯対策を講じること。	(6) コンビニATM	コンビニATM	流用（見直し）
		実76	運95	コンビニATMの障害時・災害時対応手順を明確にすること。	(6) コンビニATM	コンビニATM	流用（見直し）
		実77	運96	コンビニATMのネットワーク関連機器、伝送データの安全対策を講ずること。	(6) コンビニATM	コンビニATM	流用（見直し）
		実78	運97	コンビニATMの所轄の警察および警備会社等関係者との連絡体制を確立すること。	(6) コンビニATM	コンビニATM	流用（見直し）
		実79	運98	コンビニATMの顧客に対して犯罪に関する注意喚起を行うこと。	(6) コンビニATM	コンビニATM	流用（見直し）
		実80	運99	デビットカード・サービスにおける安全対策を講ずること。	(7) デビットカード・サービス	デビットカード(デビットカード・サービスの安全性確保)	合体（見直し）
		実81	運100	デビットカード利用時の口座番号、暗証番号等の安全性を確保すること。	(7) デビットカード・サービス	デビットカード(デビットカード・サービスの安全性確保)	合体（見直し）
		実82	運101	デビットカード利用時の顧客保護の措置を講ずること。	(7) デビットカード・サービス	デビットカード(顧客保護)	合体（見直し）
		実83	運102	デビットカード利用上の留意事項を顧客に注意喚起すること。	(7) デビットカード・サービス	デビットカード(顧客への注意喚起)	合体（見直し）
		実32	運42	前払式支払手段における機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること。	(8) 前払式支払手段	運用管理(取引の管理)	合体（見直し）
		実132	技41	前払式支払手段における電子的価値の保護機能、または不正検知の仕組みを設けること。	(8) 前払式支払手段	不正使用防止(予防策(不正・偽造防止対策))	合体（見直し）
		実89	運107	電子メールの運用方針を明確にすること。	(9) 電子メール・イントラネットの利用	オープンネットワークを利用した金融サービス(電子メール)	合体（見直し）
		実134	技42-1	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。	(9) 電子メール・イントラネットの利用	不正使用防止(予防策(不正・偽造防止対策))	合体（見直し）
Ⅳ 監査基準	12 システム監査	監1	運91	システム監査体制を整備すること。	(1) システム監査	システム監査(システム監査)	流用（見直し）

【資料2－5】
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

安全対策基準一覧表【構成一覧】（原案）

Ⅰ　統制基準

基準大項目		基準中項目	
1 内部の統制	内部の統制を行うために実施すべき対策及び、考慮すべき事項に関する基準項目	(1) 方針・計画	コンピュータシステムの安全対策を体系的かつ効率的に実施するために必要となる基本方針の整備及び必要な経営資源を考慮した中長期のシステム計画の策定に関する基準項目
		(2) 組織体制	安全対策の実施に係る方針に沿って、コンピュータシステムの安全対策を適切に実施するために必要な体制の整備（責任者の選任、所管部署の整備、各種規則の整備等）に関する基準項目
		(3) 管理状況の評価	コンピュータシステムを円滑かつ適正に運用するために、セキュリティ関連文書に定められた事項の遵守状況を確認し、評価するための基準項目
		(4) 人材（要員・教育）	コンピュータシステムを円滑かつ適正に運用するために必要となる、システムの開発・変更及び運用に携わる要員の人事管理及び健康管理、ならびに要員に対し実施すべきセキュリティ教育をはじめとした各種の教育および訓練に関する基準項目
2 外部の統制	外部の統制を行うために実施すべき外部委託管理及び、サービスの利用等における安全対策に関する基準項目	(1) 外部委託管理	外部委託管理を適切に行うため、利用検討時、契約時、運用時及び管理体制を整備するにあたって実施すべき対策に関する基準項目
		(2) クラウドサービスの利用	クラウドサービスを利用する場合における、金融機関等が実施すべき対策及び考慮すべき事項に関する基準項目
		(3) 共同センター	共同センターで勘定系システムを利用する場合における、迅速に初動対応が取れるようにするための緊急事態の発生に備えた安全対策に関する基準項目
		(4) 金融機関相互のシステム・ネットワークのサービス	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おいて実施すべき対策及び考慮すべき事項に関する基準項目

Ⅱ　実務基準

基準大項目		基準中項目	
1 情報セキュリティ	顧客データ漏洩、改ざんの防止、システムの不正使用の防止等の情報セキュリティ対策に関する基準項目	(1) データ保護	機密データや重要データの漏洩、破壊、改ざん、またこれらのデータへのアクセスに必要な暗証番号、パスワード等の漏洩を防止するための、データ保護対策に関する基準項目。
		(2) 不正使用防止	アクセス権限を持たない者による不正取引またはデータやソフトウェアの改ざん等を防止するために実施すべき、アクセス権限確認、利用範囲の制限等の対策に関する基準項目
		(3) 外部ネットワークからの不正アクセス防止	ネットワークを介した外部からの不正侵入によるコンピュータシステムの不正使用を防止するために実施すべき、外部からのアクセスを制限する等の対策に関する基準項目。

基準大項目		基準中項目	
		(4) 不正検知策	不正アクセスを早期に発見するために実施すべき、不正アクセスを監視する機能や異例取引、不正取引を監視、検知する等の対策に関する基準項目。
		(5) 不正発生時の対応策	不正アクセス、不正使用を検知した場合における、迅速に被害の範囲を調査・特定し被害の拡大を防止するとともに、システムの復旧を行うための対策に関する基準項目。
		(6) 不正プログラム対策	システムの安全性の侵害対策を講じるにあたり実施すべき、不正プログラムのシステムへの侵入や組込みを防止するための対策に関する基準項目。
2　システム運用共通	システムの運用部門（主に委託先）及び利用部門（金融機関）が実施すべき基準項目	(1) マニュアルの整備	コンピュータシステムを正確かつ安全に運用するために必要となる、通常時及び障害・災害時の各種運用手順のマニュアル整備に関する基準項目。
		(2) アクセス権限の管理	コンピュータシステムを構成する機器、ファイル等各種資源に対する破壊および不正使用を防止するために実施すべき、その重要度に応じたアクセス権限を設定し、適切に管理する等の対策に関する基準項目。
		(3) データ管理	データファイルの不正使用、改ざん、紛失等を防止するために実施すべき、データファイルの授受、保管等の対策、ならびに暗号鍵の漏洩、不正使用等を防止するための管理に関する基準項目。
		(4) オペレーション習熟	コンピュータシステムや端末の誤操作による事故を防止するために実施すべき、コンピュータセンター等におけるシステムの運転や、営業店等における端末操作に関する教育および訓練に関する基準項目。
		(5) コンピュータウイルス対策	コンピュータウイルス等不正プログラムによるプログラムの改ざん、破壊等を防止するために実施すべき、不正プログラムの侵入防止策や侵入した場合の検知策に関する基準項目。
		(6) 外部接続管理	外部との接続を安全かつ正確に行い、データ漏洩、不正アクセス等を防止するために実施すべき、接続先が正当であることの確認及び外部接続時の運用方法等を明確に定め適切に管理する等の対策に関する基準項目。
3　運行管理	日々のシステム運行に関する基準であり、システムの運用部門（主に委託先）が実施すべき基準項目	(1) オペレーション管理	コンピュータシステムの不正使用を防止し、運用の円滑化を図るために必要となる、オペレーションの依頼、承認、実行、記録、結果確認等の管理に関する基準項目。
		(2) データファイル管理	障害や災害等の発生やサイバー攻撃等による破壊・改ざんに備えて実施すべき、データファイルのバックアップ確保等の対策に関する基準項目。
		(3) プログラムファイル管理	プログラムの改ざん、破壊等を防止するために実施すべき、プログラムファイルの管理ならびに障害や災害等の発生に備えたバックアップの確保等の対策に関する基準項目。
		(4) ネットワーク設定情報管理	ネットワーク設定情報が不正に改ざんされないように実施すべき、ネットワーク設定情報の管理、障害や災害等の発生に備えたバックアップの確保等の対策に関する基準項目。
		(5) **運用時**ドキュメント管理	ドキュメントの不正使用、紛失等を防止するために実施すべき、ドキュメントの管理、障害や災害等の発生に備えたバックアップの確保等の対策に関する基準項目。
		(6) 運行監視	異常状態の早期発見のために実施すべき、コンピュータシステムの運行監視等の対策に関する基準項目。

基準大項目		基準中項目	
4 各種設備管理	コンピュータ機器や能力の管理に関する基準であり、システムの運用部門（主に委託先）が実施すべき基準項目	(1) 資源管理	コンピュータシステムの障害および処理能力の低下を回避するために実施すべき、各種資源の容量および性能の限界を把握する等の対策に関する基準項目。
		(2) 機器の管理	コンピュータシステムを構成する各機器の障害、不正使用、破壊、盗難等を防止するために実施すべき、各機器の重要性に応じた管理、保守方法を明確に定めるとともにハードウェアの障害の発生を極少化させるための予防保守を実施する等の対策に関する基準項目。
		(3) コンピュータ関連設備の保守管理	コンピュータシステムを円滑に運用するために実施すべき、電源、空調、給排水、防災、防犯、監視、回線関連等の設備の管理、保守方法を明確にする等の対策、ならびに各種設備の容量及び性能の限界と使用状況の把握に関する基準項目。
		(4) 入退館（室）管理	不法侵入、危険物持込み、不法持出し等を防止するために必要となる、コンピュータセンターやコンピュータ室等重要な室へ出入りする人・物の管理、また入室者の作業について管理する等の対策に関する基準項目。
		(5) 監視	異常状態の早期発見のために実施すべき、コンピュータシステムの稼働に必要な各種設備の稼働状況の監視等の対策に関する基準項目。
5　システムの利用	システムの利用部門（金融機関）が実施すべき基準項目	(1) 取引の管理	端末機操作による不正、不当取引を防止するために実施すべき、取引の操作内容の記録・検証、及び顧客からの届出の受付体制の整備に関する基準項目。
		(2) 入出力管理	システムに入力するデータの完全性を確保するために必要となる、データの入力管理ルールの作成及び遵守、また、出力情報の不正使用、漏洩等を防止し、機密性、プライバシー等を保護するために必要となる、出力情報の管理ルールの作成及び遵守に関する基準項目。
		(3) 帳票管理	帳票の不正使用、内容漏洩を防止するために実施すべき、重要な帳票の管理方法、廃棄手続きに関する基準項目。
		(4) 顧客データ保護	顧客データの取扱い、保護の対応、特に認証手段として生体認証を用いる場合における、生体認証情報の管理手順を定め安全管理措置を講ずる等の対策に関する基準項目。
6　緊急時の対応	システムの運用部門（主に委託先）と利用部門（金融機関）が協調して実施すべき基準項目	(1) 障害時・災害時対応策	コンピュータシステムの障害時・災害時における顧客、本部・営業店等への影響を最小限にとどめ、かつ、早期復旧を図るために実施すべき、障害時・災害時対応策に関する基準項目。
		(2) コンティンジェンシープランの策定	災害時・障害時等の緊急時に早期に業務の復旧を図るために必要となる、あらかじめ想定されるケースに基づいたコンティンジェンシープラン（緊急時対応計画）の策定に関する基準項目。
		(3) バックアップサイト	コンピュータセンター等が災害等により機能しなくなった場合に備えた、リスクの分散のために別の地域にバックアップサイトを設置するための基準項目。
7 システム開発・変更	システム開発部門が、開発・変更時におけるシステムの安全性を確保するために実施すべき基準項目	(1) システム開発・変更管理	システム開発・変更における内容の正当性と本番システムの安全性を確保するために実施すべき、システム開発・変更手順、テスト環境の整備などの総合的な管理に関する基準。
		(2) **開発・変更時~~システム~~**ドキュメント管理	開発・変更作業を円滑にし、改ざん、不正使用を防止するために実施すべき、システム開発・変更に係わるドキュメントの作成手順および管理方法を定める等の対策に関する基準。

基準大項目		基準中項目	
		(3) パッケージの導入	パッケージを導入する場合のシステム開発・変更を円滑に行うために必要となる、パッケージの信頼性、生産性、既存システムとの親和性などを評価する体制の整備及び、パッケージの運用・管理体制の整備に関する基準
		(4) システムの廃棄	システムの廃棄時における機密保護、プライバシー保護、不正防止等のために実施すべき、廃棄計画の作成、手順を定めて遵守する等の対策に関する基準項目。
8　システムの信頼性向上対策	システムの安定運用、信頼性向上のために実施すべき基準項目	(1) ハードウェアの予備	コンピュータシステムの信頼性を向上させるために実施すべき、コンピュータ本体および関連機器の障害発生を極力減少させる対策、ならびにハードウェアの構成要素の一部に障害が生じても、システム全体に影響が及ばないようにする対策に関する基準項目。
		(2) ソフトウエアの品質向上対策	システムの信頼性向上のために実施すべき、設計工程や製造工程及び本番適用段階においてソフトウェアの信頼性を向上させる対策、ならびにパッケージ等の利用にあたり既存システムとの整合性、親和性に留意する等の対策に関する基準項目。
		(3) 運用時の信頼性向上対策	コンピュータシステムの信頼性向上を図り、運用時の信頼性を向上させるために必要となる、オペレーションの自動化、簡略化等の対策、ならびに妥当性、正当性のチェック機能を充実する等の対策に関する基準項目。
		(4) 障害の早期発見・回復機能	障害が発生した際に、早急に障害状況を検出し、その影響を最小限に抑え、速やかに回復するために実施すべき対策に関する基準項目。
9　個別業務・サービス	固有の業務・サービスにおいて実施すべき基準項目	(1) カード取引サービス	カード取引サービスに係る事故・犯罪を防止し、安心・安全なサービスを提供するために実施すべき、利用者保護をはじめとする対策に関する基準項目。
		(2) インターネット・モバイルサービス	利用者との取引を安全に実施するために実施すべき、インターネット・モバイルサービスに関するさまざまな脅威に対する対策、ならびにサービス利用における本人確認や注意喚起等、顧客対応方法に関する基準項目。
		(3) 渉外端末の管理	システムの安全性の確保および処理の円滑化のために実施すべき、渉外端末等の可搬型端末の適切な管理、また不正使用の防止および破損、紛失、盗難等に備えた対策に関する基準項目。
		(4) CD・ATM等及び無人店舗の管理	CD･ATM等および無人店舗の円滑な稼働ならびに犯罪から利用者や機器等を保護するために必要となる、事故・犯罪の予防措置、ならびに障害・災害や犯罪発生時の対応方法を明確にする等の対策に関する基準項目。
		(5) インストアブランチ	インストアブランチの安全性を確保するために実施すべき、出店先地域やストアの選定基準を明確にする等の対策に関する基準項目。
		(6) コンビニATM	コンビニATM、その利用者およびメンテナンス要員等の安全性に考慮した運用を行うために実施すべき対策に関する基準項目。
		(7) デビットカード・サービス	デビットカード・サービスの安全性を確保するために実施すべき、サービスの提供形態に応じた、情報処理センターや加盟店等との総合的な対策に関する基準項目。
		(8) 前払式支払手段	プリペイドカード等の前払式支払手段における安全性を確保するために実施すべき、その電子的価値を記録したデータの破壊・改ざんを防止するための対策、及び電子的価値の利用に伴う注意点の利用者への明示等に関する基準項目。

基準大項目		基準中項目	
		(9) 電子メール・イントラネットの利用	電子メールを利用し、取引通知、情報提供等のサービスを行う場合において必要となる、対象業務の判断およびその運用方針を明確にすること、ならびに業務目的以外の電子メールの送受信やホームページの閲覧等に対処するために必要な不正使用防止対策に関する基準項目。

Ⅲ　設備基準

基準大項目		基準中項目	
1 コンピュータセンター	コンピュータセンターの建物・付帯施設及び設備に関する基準項目	(1) 建物(環境)	コンピュータセンターの建物において、災害、障害が発生した場合に被害を最小限にとどめ迅速に復旧させるために必要となる、立地する環境、建物周囲等の場所を考慮した対策に関する基準項目。
		(2) 建物(周囲)	
		(3) 建物(構造)	
		(4) 建物(開口部)	
		(5) 建物(内装等)	
		(6) コンピュータ室・データ保管室(位置)	コンピュータ室・データ保管室における、オンラインネットワークの中枢となる機器およびデータ記録媒体等の安全性を確保するために実施すべき、設備面での自然災害および不正行為等の発生防止策に関する基準項目。
		(7) コンピュータ室・データ保管室(開口部)	
		(8) コンピュータ室・データ保管室(構造・内装等)	
		(9) コンピュータ室・データ保管室(設備)	
		(10) コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	
		(11) 電源室・空調機械室	安定的な電力を供給するための電源設備が設置された電源室、及び安定的な温湿度を管理するための空調設備が設置された空調機械室において実施すべき、通常は無人状態であることを踏まえた障害等の早期発見と被害を最小限にとどめるための対策に関する基準項目。
		(12) 電源設備	電源設備における、停電、異常電圧、異常周波数、電源の瞬断、過電流、漏電および電源設備自体の障害によりコンピュータシステム等に影響を与えることのないように実施すべき、必要な電力を安定的に供給できる対策に関する基準項目。
		(13) 空調設備	空調設備において必要となる、適切な温湿度の清浄な空気が安定的に供給できるような対策、及び空調設備の一部の機器は建物の外部に設置されることを踏まえた、外部からの侵入や厳しい気象条件にも対応できるような対策に関する基準項目。
		(14) 監視制御設備	監視制御設備において必要となる、電源設備、空調設備、防災設備、防犯設備等の管理の中枢としての機能および障害発生時の早期発見、通報、回復機能を設ける等の対策に関する基準項目。
		(15) 回線関連設備	回線関連設備において必要となる、通信回線との接点としての、コンピュータシステムへの不正アクセス等を防止するための対策に関する基準項目。
2 本部・営業店等	本部・営業店等の建物・付帯施設及び設備に関する基準項目	(1) 建物(周囲)	コンピュータシステムの安定稼働のために、本部・営業店等において実施すべき、設備面の安全対策、及び自動機器等の無人運用を行う場合（店舗外現金自動設備を含む）における、周辺環境に適した防犯・防災措置に関する基準項目。
		(2) 建物(構造)	
		(3) 建物(開口部)	

基準大項目		基準中項目	
		(4) 建物(内装等)	
		(5) 建物(設備)	
		(6) 建物(回線関連設備)	
		(7) 建物(電源設備)	
		(8) 建物(空調設備)	
		(9) 建物(自動機器室)	
		(10) 建物(端末機器)	
		(11) サーバー設置場所(位置)	コンピュータ室外（本部・営業店等）に設置されるコンピュータシステムにおいて、サーバーを主体とした装置構成が取られることを踏まえて実施すべき、使用形態やサービス内容等に応じた対策に関する基準項目。
		(12) サーバー設置場所(構造・内装等)	
		(13) サーバー設置場所(設備)	
		(14) インストアブランチ	インストアブランチにおいて、ストアの既設設備を利用したり、ストア等との営業時間が異なる場合がある等を踏まえて実施すべき、設備の補強等の防犯措置を行い、破壊侵入等を防御する等の対策に関する基準項目。
3 流通・小売店舗との提携チャネル	流通・小売店舗等と提携してサービスを提供する場合の建物・付帯施設及び設備に関する基準項目	(1) コンビニATM	コンビニATMにおける、コンビニエンスストアという不特定多数の人が行き来する場所で自動機器室、機械室がなく単体で設置されることが多い点を踏まえた防犯対策に関する基準項目。

Ⅳ　監査基準

基準大項目		基準中項目	
1 システム監査	システムの監査体制の整備に関する基準項目	(1) システム監査	コンピュータシステムの有効性、効率性、信頼性、遵守性、および安全性を確保するために必要となる、システム監査体制の整備に関する基準項目。

【資料３－１】
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

外部委託関連基準の整理方針について

Ⅰ. 論点に関する各委員からのご意見について

○ 前回ご提示した論点について、各委員よりご意見をいただいた。

○ 論点１及び論点３については、「賛同する」とのご意見をいただき、その方針で修正を進めていく。論点２については、クラウド固有の管理策は、「外部の統制」の一部と見なすべきであり、かつ利用者視点からも「外部の統制」と位置付けた方がよいとのご意見があり、この方向で構成を見直すこととした。

○ なお、ご意見については【資料３－２】外部委託関連基準に対する各委員からのご意見・対応方針に一覧として掲載した。

論点１については、「賛同」のご意見をいただいた。

論点１ （再掲）	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は、新基準に記載しない（削除する）ことでよいか。
主なご意見	・賛同する。

論点２については、クラウド固有の管理策を「外部の統制」とするご意見をいただいた。当該基準を「基礎基準」とすべきか検討課題としている。

論点２ （再掲）	クラウド固有の安全対策として新設した【統 27】において、システムの重要度に関する表現（例えば、「特定システムでクラウドサービスを利用する場合には」といった表現）を記載しない（削除する）ことでよいか。 また、統制基準ではなく、実務基準として整理することが適切と考えられるがどうか。
主なご意見	・（一部抜粋）FinTech 有識者検討会の実例でもコア業務を含めた業務システムがすべてクラウドサービスで実行されるような例が出てきているという調査例が提示されており、そのような最新の状況を考慮しリスクを客観的に把握した上で将来にわたって定めた統制が有効であるような方向性で統制基準の見直しができるような内容にするためには、今後も技術の発展に関わらず有効で抽象度の高い内容を残したほうが良いと思われるため、統制２７を残すことを提案します。 ・見読み手の立場で考えると、大項目「外部の統制」に記載されている方が分かりやすく、見落としがないと思います。
対応方針	【統 27】として、当該基準を「外部の統制」に含める。 （課題）当該基準を「基礎基準」「付加基準」いずれとするか。（論点４）

論点３については、データ漏洩防止に関する対策を統合・整理する点について「賛同する」というご意見の他、統合したうえで、「データ漏洩に対する管理策を外部委託における各局面に沿って整理し、再定義してはどうか」というご意見をいただいた。このため、統制において契約締結時・契約中・契約終了時に必要な対策をどのように整理すべきかを新たな検討課題とすることとした。

なお、監査に関する記載についても、重複を排除するとした方針に対し「賛同する」との意見をいただいており、これを踏まえ、監査に関する記載について統合・整理を行うこととする。

論点３ （再掲）	実務基準との重複部分や、記載箇所が複数の基準に分散している内容を統合・整理することでよいか。
主なご意見	・「統 25　外部委託にあたって、データ漏洩防止策を講ずること。」に記載されている内容は、「契約締結時に確認する事項」であることが実態に即していますので、「案３」（統 22 に追加して統 25 は廃止）が妥当と考えます。 ・（一部抜粋）大枠では統２２への統合を提案します。ただし、委託先でのデータ漏洩に係る事象がこれまでも大きく注目されているなどの背景を考慮し、運用基準として統制２５、２６を統合した形で例えば、委託先のサービスを利用開始する時点、運用時、サービス利用終了時と大きく３つポイントを含んだ形で再定義することを提案します。
対応方針	・【統 22】にデータ漏洩に関する記載を統合する。 ・データ漏洩防止に関する対策について、外部委託における各局面を意識して整理することでよいか。（論点５） ・監査に関する基準について、記載の重複を排除し、統合・整理する。

II. 修正方針について

論点に対する各委員の意見を踏まえ、以下の新たな論点についてご審議いただきたい。（なお番号は、前回論点との混同を招かないよう、前回からの通番で付番している。）

論点４	クラウド固有の管理策とした基準【統 27】について、「基礎基準」「付加基準」いずれに整理するのが適当か。

○　FinTech に関する有識者検討会報告書では「重要な情報システム（新安対基準の定義では「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、固有の管理策が提言されている。

○　この報告書の提言を踏まえると、【統 27】は「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」に必要な安全対策となるため、「基礎基準」ではなく、「付加基準」となる。

○ 現在の前説では、「統制・監査に関する基準」はすべて「基礎基準」として位置付けているため、当該基準の位置付けを改めて整理・検討する必要がある。

○ 実務基準において「個別の業務・サービス」は「付加基準」と整理している。統制基準のうち、クラウドサービスの利用、共同センターの利用、金融機関相互のシステム・ネットワークのサービス利用はこれに該当すると言える。

○ これらの点を考慮し、【統 27】～【統 29】については、外部の統制における「個別の業務・サービスに関する基準」として位置付け、外部の統制における「付加基準」として整理する。また、前説における「基礎基準」の選定にあたっての考え方に所要の修正を行う。

○ なお、特定システムでは「付加基準」の必須対策が適用されるため、【統 27】において、「特定システムにおいて…」という表現は使用しない。

外部の統制において「付加基準」として整理するもの（３基準）

基準番号	基準小項目
統 27	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。
統 28	共同センターにおける有事の際の安全管理策対策を講ずること。
統 29	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。

論点５	外部委託先におけるデータ漏洩防止策に対する外部の統制について、外部委託における各局面に沿って整理すべきか。

○ 委託先におけるデータ漏洩防止策については、金融機関等において統制上重要な事項であり、契約締結時から契約終了時まで、局面に応じて統制を行う必要がある。

○ 契約締結の際、委託元である金融機関等が確認すべき事項については、【統 25】及び【統 26】から【統 22】に記載を統合させた（この中に、契約終了時に確認すべき事項も含まれている）。

○ 一方、契約期間中は、金融機関等は委託先におけるデータ漏えい防止策の遂行状況をモニタリングすることとなる。【統 25】【統 26】を廃止した場合、この部分は外部委託基準上で明確化されなくなるため、委託先の業務遂行状況を確認するとした【統 24】に、データ漏洩防止策の遂行状況のモニタリングを追加し、外部委託における各局面に沿った対策として再整理する。

○　基準原案については、資料【３－３】基準原案【統 22】【統 24】を参照。

委託先におけるデータ漏えい防止策に対する外部の統制の整理方針

局面	記載される対策
契約時	委託先のデータ管理体制の確認【統 22】
契約期間中	委託先が実施するデータ漏えい防止策の遂行状況のモニタリング【統 24】 機器の故障交換等におけるデータ漏えい防止策の確認【統 22】
契約終了時	委託先によるデータ消去（方法・証明手段等）、機器等の廃棄、文章等の回収に関する対策の確認【統 22】

III. 基準原案に対するご意見

基準原案に対しても、表現の見直し等の他、外部委託に関する有識者検討会報告書との関係など、多岐に渡るご意見をいただいた。（【資料３－２】外部委託関連基準に対する各委員からのご意見・対応方針　参照）

ご意見の中で、「理解しやすさ」「選択肢の追加」等については、ご意見を踏まえ、基準原案に反映している。詳細については、【資料３－２】及び【資料３－３】基準原案を参照いただきたい。

IV. 今後の予定

本日説明した内容について、10/31（火）までに事後意見をいただきたい。事後意見をもとに基準原案の修正を行い、次回委員会にて最終案を提示する予定である。

スケジュール

日程（予定）	内容
10 月 17 日（火）	第 57 回安全対策専門委員会審議（修正原案提示）
10 月 31 日（火）	第 57 回専門委員会事後意見の締切
11 月 21 日（火）	第 59 回安全対策専門委員会審議（最終原案提示）

以上

【資料３－２】
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

■外部委託関連基準に対する各委員からのご意見・対応方針

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	反映状況 コメントNo
1	資料２－１	論点２	統27　ではなく、実務基準144の付加基準とするほうが適切と考えられる理由が不明です。読み手の立場で考えると、大項目「外部の統制」に記載されている方が分かりやすく、見落としがないと思います。	三菱東京UFJ銀行 伊藤様(検)	クラウドサービスの利用における安全管理策は、クラウド以外の外部委託の統制の拡張部分と位置付け、改めて「外部の統制」として整理することが有益と考えました。ご意見を踏まえ、クラウド固有の管理策は、【統27】として整理することとし、各委員のご意見を伺いたいと考えております。 また、FinTech報告書の提言では、「重要なシステムにおける」という条件があることから、当該基準については個別の業務・サービスに関する基準、即ち「外部の統制における付加基準」と整理することとし、各委員のご意見を伺いたいと考えております。（No.20参照）	要	済
2	資料２－２	統21 1.	【資料 p.11】 ・「外部に委託する業務」を例示するのであれば、記載されている(1)～(10)の例が全てではないため、次の「明確にすべき外部委託に関する事項」と同様に最終行に「等」という記述を入れた方がよろしいかと思います。 ・「外部に委託する業務」の例として、企画提案やコンサル等の上流工程の例もあってもいいのではないかと思います。	NTTデータ 鎌田様(専) 鈴木様（検）	ご意見を踏まえ、「等」を追加いたしました。 上流工程におけるコンサルティング委託契約やアドバイザリー契約は例として追加することも可能であると考えておりますが、企画提案（例えばシステム化計画の企画提案）については、金融機関等から委託し、第三者へ提案する場面が想定できませんでした。ここは、委員の皆様からのご意見を踏まえ、追記したいと考えております。	要	済
3	資料２－２	統21 3.	【資料 p.12】 ・項番1.でも「外部に委託する業務」の例を記載しているのに、委託業務範囲にカッコ書きで敢えてクラウド（一部）のことに言及している点には違和感があります。	NTTデータ 鎌田様(専) 鈴木様（検）	ご意見を踏まえ、委託業務範囲のカッコ書きの記載を見直すことを検討いたします。 （No.22参照）	要	済
4	資料２－２	統22 1.(13)②	【資料 p.16】 ・「予め委託先と協議しておく」というのは、現実的には難しいのではないかと懸念いたします。	NTTデータ 鎌田様(専) 鈴木様（検）	現在の基準である【運109】では、「調査時に収集の対象となる証跡の範囲（中略）及び、抽出ツールの開発・検証のために必要となる費用負担について、契約締結時に合意を得ること。」となっています。 今回の改訂では、「調査に必要なデータの収集範囲や分析に必要なツール等の提供（提供されない場合は、分析に係る費用等）について、予め委託先と協議しておくことが考えられる。」とし、クラウド以外の外部委託にも適用するため、強度等を考慮して、あくまで対策例の一つ（考えられる対策の一つ）とさせていただいており、原案のとおりとさせていただきたいと考えております。	否	原案のままとさせて頂きたいと考えております
5	資料２－２	統25 2.	【資料 p.22】 「ただし」とした場合、「ただし」以後の文が「ただし」より前の文を受ける形となり、重要なデータにおいても代替可能と読み取れる内容と読み取れるため、「なお」などとした方がよいと考えます。	NTTデータ 鎌田様(専) 鈴木様（検）	No.6のとおり、【統22】統合のうえ、選択可能な対策として、以下の内容とさせていただきたい考えております。 統22.1.(14) 「また、記憶装置等の障害・交換におけるデータ消去については、消去証明書の発行・取得または、外部委託先に対する情報提出要請や、監査等の方法で消去・破壊プロセスの実効性を検証する。」	要	済
6	資料２－２	統25	【資料 p.22～23】 ・「統25　外部委託にあたって、データ漏洩防止策を講ずること。」に記載されている内容は、「契約締結時に確認する事項」であることが実態に即していますので、「案３」（統22に追加して統25は廃止）が妥当と考えます。	NTTデータ 鎌田様(専) 鈴木様（検）	ご意見を踏まえ、案3の方針にて統合・整理を進めさせていただきたいと考えております。	要	済
7	資料２－２	統26 5.	【資料 p.24】 ・「５．委託業務終了後、関連重要資料、文書等を回収する。」については、「廃棄させる」ケースも多いため、廃棄に関する追記を提案します。	NTTデータ 鎌田様(専) 鈴木様（検）	No.6のとおり、【統22】統合する方針です。ご意見を踏まえ、統合後の文章に反映させるか検討させていただきたいと考えております。	要	済
8	資料２－２	統26 5.	【資料 p.24】 ・開発用PC等からのデータ抹消も必要ではないかと思います。	NTTデータ 鎌田様(専) 鈴木様（検）	No.6のとおり、【統22】統合する方針です。（No.24参照）	要	済
9	資料２－２	統26 5.	【資料 p.24～25】 「統26　外部委託契約終了時のデータ漏えい防止策を講ずること。」に記載されている内容は、「契約締結時に確認する事項」であることが実態に即していますので、「案３」（統22を見直して統26は廃止）が妥当と考えます。	NTTデータ 鎌田様(専) 鈴木様（検）	ご意見を踏まえ、案3の方針にて統合・整理を進めさせていただきたいと考えております。	要	済
10	資料２－２	統28 5.	【資料 p.27】 ・「有事」という表現には戦争や事変が含まれますが、実58(p.33)での「想定される緊急事態」の記載の例のように、戦争発生時のことは対象外とした方がよいのではないかと思います。	NTTデータ 鎌田様(専) 鈴木様（検）	ご意見を踏まえ、以下のとおり修正いたしました。 勘定系システムにおいて共同センターを利用する場合、迅速に初動対応が取れるようにするため、緊急事態の発生に備えた適切な安全対策を講ずること。 1.（中略） 想定される緊急事態については、【実58】を参照のこと。	要	済
11	資料２－１	論点１－３	提案通りの案でよいと思われる。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、案の方針にて統合・整理を進めさせていただきたいと考えております。	要	済
12	資料２－２	統25	（検証のポイント） 重複をなくす意味でも案3を採用するのがよいと思われる。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、案3の方針にて統合・整理を進めさせていただきたいと考えております。	要	済

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	反映状況 コメントNo
13	資料2－2	統26	（検証のポイント） 重複をなくす意味でも案3を採用するのがよいと思われる。	三井住友海上火災保険 中川様(検)	ご意見を踏まえ、案3の方針にて統合・整理を進めさせていただきたいと考えております。	要	済
14	資料2－2	統22．1．（12）．⑤	統22．1．（12）．⑤に「費用負担」も追加していただきたい。 （修正案） ⑤ 監査等の指摘事項の扱い 監査等により判明した指摘事項への対応に関する取り決め（費用負担・対応期間など） （理由） 監査等により判明した指摘事項への対応が、当初契約していたサービスレベルを越え、新たに費用が発生する可能性もあるため。	日立製作所 宮崎様(検)	ご意見のとおり修正いたしました。	要	済
15	資料2－2	統22．2．（1）～（5）	統22．2．（1）～（5）の文末に、「又は目標　等」を追加していただきたい。 （修正案） (1) システム運用（可用性（注）、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、オンラインシステムの稼働開始時限）の保証又は目標　等 (2) サポート（障害対応、問合せ対応）の保証又は目標　等 (3) データ管理の保証（利用者データの保証）又は目標　等 (4) 統制環境（再委託先管理（再々以下の階層の先を含む）、機密保護の維持、統制環境の維持）の保証又は目標　等 (5) 開発業務を委託する場合の開発に要する人員や開発期間、期限の保証又は目標　等 （理由） SLOに記載される指標として、「目標」も例示に加えた方が適切であるため。	日立製作所 宮崎様(検)	ご意見をもとに確認したところ、「～の保証」という表現は、「SLA及びSLOに記載される指標としては、以下の例がある。」の例示としては適切ではないと考えました。従いまして、例示の記載を「～に関する事項」として、以下のとおり修正したいと考えております。 SLA及びSLOに記載される指標としては、以下の例がある。 (1) システム運用（可用性（注）、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、オンラインシステムの稼働開始時限）に関する事項（中略） (2) サポート（障害対応、問合せ対応）に関する事項 (3) データ管理（利用者データの管理等）に関する事項 (4) 統制環境（再委託先管理（再々以下の階層の先を含む）、機密保護の維持、統制環境の維持）に関する事項 (5) 開発業務を委託する場合の開発に要する人員や開発期間、期限に関する事項	要	済
16	資料2－2	統21．3	3．外部委託先（再委託先を含む）を客観的に評価することが必要である。 当該評価内容は、再委託先までに及ぶ内容として検討された結果でしょうか。 外部委託有識者検討会で、提言された「再委託先の選定要件をあらかじめ定めること」の内容と必ずしも同一にする必要はないと思いますが、例えば、損害賠償などは委託先であって、再委託先を直接評価する内容として妥当ではないものと思料します。	富士通 服部様(検)	ご意見を踏まえ、再委託先を含めて実施する部分については、「外部委託先（または再委託先）」という記述に修正いたしました。 さらに、報告書の内容を踏まえ、再委託先の選定要件の策定及び評価の方法について、以下のとおり記載を追加しました。 「また、委託業務が再委託される場合、外部委託先と同様、金融機関等は再委託先の選定要件を策定する必要がある。また、特定システムが再委託される場合は、委託先のみならず、金融機関等みずからも再委託先の評価を実施する必要がある。通常システムでは、外部委託先における再委託先の審査・管理プロセス及び運用状況が金融機関等と同等かそれ以上に実効的であるかを検証することで、再委託先の評価に代替することが可能である。」 また、委託先に対する統制が、全て再委託先に対する統制とはならないことから、以下の記載を追加することとしました。（【統22】にも、例示の対策は選択的である点を明記しました） 「なお、業務が再委託される場合、再委託される業務の内容やリスク特性に応じ、再委託先を評価する事項が外部委託先と異なる点に留意する必要がある。」	要	済
17	資料2－2	統22．1	(12)監査・モニタリング①監査等の権利の明記 外部委託有識者検討会では、RBAにしたがって監査権を明記しないことが可能である場合の条件が提言（報告書p46「再委託で新たに追加すべきリスク管理策」）されています。監査権を明記するかどうか有識者検討会で整理された条件は記載されない方針でしょうか？	富士通 服部様(検)	監査の方法を【監1】に集約し、【統22】から参照するよう見直しました。（No25参照） 【監1】においては、「特定システムが再委託される場合、金融機関等の責任において監査を実施する」とし、報告書の内容と踏まえ、監査の条件を明記することとしました。	要	済
18	資料2－2	－	「以下のような例がある」の扱いについて 例えば「必須対策」に付随して例示があります。この例示は個々金融機関のRBAにしたがって取捨選択してよいものかどうか、例示の取り扱いについて解説は必要ないでしょうか。 （必須対策にある例示は原則すべて適用すべきと解釈されます）	富士通 服部様(検)	これまでの安全対策基準では、解説部分に対する説明はありませんでした。今回の改訂にて、必須対策には「必要」と記載すると解説を加えることとします（前説Ⅲ「本書の利用にあたって」）。これにより、必須対策以外は、取捨選択可能なものとしており、読み手の解釈に幅が出ないようにしたいと考えております。	要	済
19	資料2－1	Ⅱ.改訂方針に関する論点	該当箇所と意見 論点1、賛同します。	アマゾンウェブサービスジャパン 梅谷様(専)	ご意見を踏まえ、統合・整理を進めさせていただきたいと考えております。	要	済
20	資料2－1	Ⅱ.改訂方針に関する論点	該当箇所と意見 論点2、「統制27が個別サービスを利用する場合の実務基準として整理することも考えられる」という記述がありますが、これは個別の業務で限定されたアプリケーションとして利用されるSaaSのような特定のクラウドサービスを指した場合には当てはまるかもしれません。しかしIaaS、PaaSなどより業務基盤そのものに広範囲に利用されるクラウドサービスの利用形態を考えると、FISC様で実施されたFinTech有識者検討会の実例でもコア業務を含めた業務システムがすべてクラウドサービスで実行されるような例が出てきているという調査例が提示されており、そのような最新の状況を考慮しリスクを客観的に把握した上で将来にわたって定めた統制が有効であるような方向性で統制基準の見直しができるような内容にするためには、今後も技術の発展に関わらず有効で抽象度の高い内容を残したほうが良いと思われるため、統制27を残すことを提案します。	アマゾンウェブサービスジャパン 梅谷様(専)	No.1の整理と同様、クラウド固有の管理策は、外部の統制として整理することで検討したいと考えております。	要	済
21	資料2－1	Ⅱ.改訂方針に関する論点	該当箇所と意見 論点3、賛同します。	アマゾンウェブサービスジャパン 梅谷様(専)	ご意見を踏まえ、統合・整理を進めさせていただきたいと考えております。	要	済

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	反映状況 コメントNo
22	資料２－２ （ページ１１）	統22, 1.(2)②	該当箇所と意見 統22, 1.(2)②「外部委託先（複数の外部委託先が業務の委託を受けた場合も含む）との間の管理境界や責任分界点に関する取り決め(例えばクラウドサービスにおけるIaaS, PaaS, SaaS等によって委託先の責務にさしが生じる場合がある）」の記述を下記のように変更することを提案します。 変更案 統22, 1.(2)②「外部委託先（複数の外部委託先が業務の委託を受けた場合も含む）への業務委託範囲や委託先のサービス性質や利用形態に関する委託元と委託先の責任分界点を考慮のうえ」とし、クラウドや共同センターに関わらず共通して確認が必要とされる記述に変更することを提案します。 また、「（クラウドサービスにおけるIaaS, PaaS, SaaS等によって委託先の責務にさしが生じる場合がある）」の記述は、クラウド特有の分類の記述であるため、統制27に4．を新たに設け、「クラウドサービスの利用にあたっては、新しい技術によってサービス内容や利用形態が変化する可能性があるため、検討時点から広義のIaaS, PaaS, SaaS等のクラウドサービスの形態に関する定義を参考にし、クラウドサービス利用側とクラウドサービスプロバイダーの責任範囲を明確にした上で利用を開始することが望ましい」等とすることを提案します。	アマゾンウェブサービスジャパン 梅谷様(専)	ご意見を踏まえ、統22の記載は汎用的な内容として見直したいと考えております。 さらに、統27にクラウド固有の考慮点として、ご意見にある責任範囲に関する記述を追加したいと考えております。 統22.1.(2)② 「外部委託先（複数の外部委託先が業務の委託を受けた場合も含む）への業務委託範囲や委託先のサービスの性質や利用形態を考慮した委託元と委託先との間の管理境界や責任分界点に関する取決め」 統27.4 「4. クラウドサービスの利用にあたっては、新しい技術によってサービス内容や利用形態が変化する可能性があるため、検討時点から広義のIaaS, PaaS, SaaS等のクラウドサービスの形態に関する定義を参考にし、金融機関等とクラウド事業者との責任範囲を明確にした上で利用を開始することが望ましい。」	要	済
23	資料２－２ （ページ２４）	統25, 26、（統22への統合）	該当箇所と意見 統制25, 統制26ともに統制22に統合するべきか、そのまま残してどのような記述にするかという議論に関してです。データの消去や漏洩に係る箇所だけ、統制22からより詳細な統制として2つの大きな統制が追加されており、クラウドのような大きなくくりで統制27に切り出されているものとは異なり、統制内容というよりは暗号化等実務的、技術的な内容であると思われます。そのため大枠では統22への統合を提案します。ただし、委託先でのデータ漏洩に係る事象がこれまでも大きく注目されているなどの背景を考慮し、運用基準として統制25、26を統合した形で例えば、委託先のサービスを利用開始する時点、運用時、サービス利用終了時と大きく3つポイントを含んだ形で再定義することを提案します。	アマゾンウェブサービスジャパン 梅谷様(専)	ご意見を踏まえ、見直しを検討いたします。 No.,9,13,14のご意見も踏まえ、統22へ統合いたします。 データ漏洩に関する基準については、統24を修正し、外部委託における各局面に沿った対策として整理したいと考えており、その方法について各委員にご意見を伺いたいと考えております。	要	済
24	資料２－２ （ページ２４）	統26	*統制２６の記述が残る前提での意見です。 該当箇所 統制26, 3.「外部委託先がデータ消去を実行する場合は、消去証明書などを受領することが必要である」という記述に変更されていますが、特定のベンダーに限らずクラウドサービス全般で消去証明の発行が難しいことが想定されるにも関わらず、最初にこのような記述があると監査で代替できることが見過ごされるあるいは、誤解を与えやすいことが考えられます。下記のような案に変更することを提案します。 変更案 「委託元は委託先でのデータ漏洩に関するリスクを考慮し、データ消去について確認する必要がある。委託元が委託先でのデータ消去の実行について確認する方法としては、例えば外部委託先がデータ消去を実行した場合に消去証明を発行することや、外部委託先が論理的消去も含めたデータ消去を外部委託契約終了時において実施することを契約書に記載し、外部の第三者が監査等においてデータ消去プロセスの有効性を検証しておくことが考えられる。	アマゾンウェブサービスジャパン 梅谷様(専)	No.23の整理と併せ、以下のとおり見直したいと考えております。 統22.1.(6)② ②　契約終了時における外部委託先によるデータ消去の実施（物理的消去または論理的消去等の方法、開発PCなど消去の範囲）及び実施時期、消去証明書等の発行（または消去プロセスの有効性に関する外部の第三者による検証）、文書等の廃棄・回収など	要	済
25	資料２－２ （ページ３１）	監1	解説6.(1)の本文と注意書きで主語が異なっているように見受けられます。 下線部： 委託先 二重下線部：金融機関 ---- （1）外部委託先の監査方法としては以下の例がある。 ②委託先の内部監査部門、または委託先みずからが依頼する外部の第三者による監査（注）を受け、監査結果を委託元に報告する。 また、・・・。 （注）第三者監査人を利用した監査人の選定は、顧客に対して責任を負う金融機関として、直接か関わっていない者から見た際に、委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定することが必要である。そのために、委託元金融機関等は、監査の対象期間において、委託先の会計監査に従事していない監査法人を選定することが必要である。 ----- 主語をそろえるため、上記の(2)に移動することを提案します。 変更案： (2)委託元金融機関等の監査等が実効的でない場合などには、第三者により代替することも可能である。（注）その際に考慮すべき事項としては以下の例がある。 ⑧・・・。 （注）第三者監査人を利用した監査人の選定は、顧客に対して責任を負う金融機関として、直接か関わっていない者から見た際に、委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定することが必要である。そのために、委託元金融機関等は、監査の対象期間において、委託先の会計監査に従事していない監査法人を選定することが必要である。	アマゾンウェブサービスジャパン 梅谷様(専)	【監1】における外部委託に関する対策は、以下のように全体を見直したいと考えております。 （1）金融機関等がみずから監査を行う場合 （2）委託先にて内部監査を行う場合 （3）認証機関やホワイトペーパーなどの報告とする場合 この際、現在の原案にある「金融機関等が第三者監査人」を選定する場合は、（1）に含め、詳細な方法については必要な部分を残して簡略化したいと考えております（実際のケースとして、金融機関等が第三者監査人を利用した監査は殆ど行われていないとの意見あり）。 また【統22】【統24】【統27】にも監査の記載が残りますが、それぞれの基準で必要な内容を残しつつ、対策については【監１】に統合いたしました。	要	済

No.	記載箇所	項番 （基準番号）	ご意見の概要	ご意見者	対応方針	原案の 修正要否	反映状況 コメントNo
26	資料２－２	P16（統22.1） （12） 及び P31（監1.6） 3、4行目	「①監査等の権利の明記 委託先及び再委託先に対する委託元金融機関等の監査等を実施する権利の明記」 の記載があります。 この記述より、 「委託元金融機関が委託先と再委託先（委託先からの二次委託）に対しても監査を行う権利を明記」を求めていると理解しますが、再委託先との直接の契約当時者でない金融機関が再委託に対し監査や立入り検査を行うことは事実上、無理があると考えます。 このため、 「委託元金融機関は委託先に対して監査を行う権利の明記、委託先と再委託先の契約において監査を行う権利を明確にする」と契約関係を分けて記載すること などの、修文検討をいただけないか。 同様の事項は、「監　1」に記載されている「委託業務が再委託され、金融機関等がシステム監査を行う場合には、委託先同様、再委託先にも金融機関等の責任において監査を行う必要がある。」についても、同様の検討が必要と考えます。	日本ユニシス 後藤様(検)	ご意見にあるとおり、外部委託検討会報告書（p45）に、「重要な情報システム」を委託する場合、金融機関等は再委託先への監査権を明記すべきとしています。この場合、委託元金融機関が再委託先への監査を行う旨を、委託元と委託先との契約上に明記するとしており、ご意見にある「委託先と再委託先の契約において監査を実施する」という内容ではないという認識です。 【統22】の記載は【監１】に統合しました。（No.17、No.25参照） 【監１】において、「特定システムが再委託される場合、金融機関等の責任において監査を実施する」として、報告書の内容を反映させていただきました。 報告書の内容を踏まえ、ここは原案のとおりとさせていただきたいと考えております。	否	原案のままとさせて頂きたいと考えております
27	資料２－２	P14（統22.1） （1）	「（1）基本的な事項」の記載項目として 「預金保険事故(金融機関の経営破綻)発生時の対応条項」について、記載検討いただけないか。 委託先のサービス提供先金融機関に預金保険機構による立入り検査が行われた場合、委託先にも各種の質問や関連資料等の提出が依頼され、対応している事実があります。 これまでの委託先へ上記検査時の質問で数回、委託元金融機関の預金保険事故（経営破綻）が発生した場合の対応について、委託先と委託元金融機関との契約文書に記載があるかについて質問を受けている状況です。 この状況を受け、一部のサービス提供先の金融機関とのサービス仕様書に「預金保険事故発生時の対応」の条項を追加した例があります。 上記の状況を受け、【統22】には「預金保険事故発生時の対応を契約文書に網羅すること」を追記、修文の検討をいただけないか。	日本ユニシス 後藤様(検)	預金保険機構の検査（データ整備状況など）については、システム安全対策とは性質が異なるため、基準上には記載しない考えです。	否	ー
28	資料２－２	P11（統21）	「統　21」において、 業務委託先の安全性評価や選定を行うことが記載されています。 対顧客面で直接的な責任は金融機関にあり、クラウドサービスの利用や業務委託による事故や障害が発生した場合であっても、業務委託範囲の責任は金融機関であることに変わりないことは明記する等の修文を検討いただけないか。	日本ユニシス 後藤様(検)	ご意見の内容については、前説Ⅰ.(6)②「外部に対する「統制の在り方」に以下記載しておりますので、基準本文には記載しない考えです。 「委託する業務の内容や委託先の評価結果等を把握したうえで、そのリスク特性に応じた統制面での対策を決定することが重要であり、これは、リスクベースアプローチや「安全対策における経営責任の在り方」で示した内容と何ら異ならない。すなわち、金融機関等においては、顧客の利便性向上や企業価値の最大化を目指して経営資源配分と最適な安全対策が決定され、残存リスクに対し適切に対応されている限りにおいては、その責任は果たされていると解される。」	否	ー
29	資料２－２	P15　（11）	「① 再委託先に対する金融機関等の事前審査の実施」に関する記載について ｉ　表題の記載から得られる、その後の記載内容に関する理解について、確認いたします。 「再委託先に対する金融機関等の事前審査の実施」と表題に記載されています。この記載から、 「再委託先の評価を委託先の委託元である金融機関等が行う事は、再委託先に対する選定の結果責任は、金融機関等にも存在している事を意味している」と理解してよいか？ ⅱ　上記ｉの理解が適切である場合に、下記の記載について、修文の検討をいただきたい。 「委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等かそれ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ委託先の審査・管理プロセスの整備・運用状況の適切性を検証し、確認することで、個別の再委託先の事前審査に代替させることも考えられる。」 と記載されている部分について、 「委託先が再委託先に対して実施する「審査・管理プロセスの確認、評価」について、金融機関等が実施する場合と比較して、同等かそれ以上の実効性が認められると金融機関等が判断する場合は、委託先が行う報告結果を金融機関等の責任において、金融機関等が個別の再委託先に対して行う事前審査の結果とすることが可能である。」 などのような修文を検討いただきたい。	日本ユニシス 後藤様(検)	ｉについては、外部委託有識者検討会の報告書にも記載されており、金融機関等にも責任が存在するという理解で問題ないと考えおります。 ⅱについては、委託元が委託先の「審査・管理プロセス」の妥当性を確認することで、再委託先の審査・評価を委託先が実施することも可能としている内容であり、ご意見の内容を表していると考えております。従いまして、原案のままとさせていただきたいと考えております。	否	原案のままとさせて頂きたいと考えております

【資料３－３】
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

外部の統制
利用検討時

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　21	外部委託を行う場合は、事前に目的や範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。

削除: 利用

適切な外部委託先を選定するため、外部委託を行う場合は、事前に目的や範囲等を明確にするとともに、外部委託先の選定に際しては手続きを明確にし、外部委託先を客観的に評価すること。また、外部委託先の決定にあたっては、責任者の承認を得ること。

1.　外部委託先（再委託先を含む）を選定するにあたっては、事前に目的や範囲等を明確にしたうえで、選定手続きを明確にすることが必要である。なお、外部委託には、クラウドサービスの利用も含まれる。

コメント [A1]: クラウドサービス利用が含まれることを明記した。

外部に委託する業務としては、以下の例がある。

(1) オペレーション（バックアップサイトにおけるオペレーションを含む）
(2) システムの開発、変更
(3) ソフトウェアの開発、変更
(4) プラットフォームまたはアプリケーション等に関するサービスの利用
(5) ハードウェア及び回線の設置、入替、撤去
(6) 入力データの作成（端末オペレーションを含む）
(7) 記録媒体、ドキュメント及び帳票等の作成、保管、配送、廃棄
(8) 館内、構内及び店内の警備
(9) 電源、空調、防犯等設備の管理、保守
(10) 集中監視（CD・ATM 等）
(11) CD・ATM の現金等の管理 等

コメント [A2]: クラウドサービスに特有の委託業務を例示として追加。

コメント [A3]: ご意見 No.2

なお、これら金融機関等の情報システムに関する業務を全面的に委託する場合もある。

明確にすべき外部委託に関する事項としては、以下の例がある。

(1) 委託目的
(2) 委託業務範囲
(3) 委託形式
(4) 委託期間
(5) 委託費用
(6) リスクの管理方法
(7) 外部委託先（または再委託先）の選定要件
(8) 外部委託に関する自社窓口と役割 等

削除: を含む

削除: 条件

2.　外部委託先（再委託先を含む）を客観的に評価することが必要である。

外部委託する業務に求められる可用性・機密性等の観点及び自社の経営の視点から、リスクを分析・認識し、当該業務に求められるリスク管理レベルを検討のうえ、外部委託先の選定要件を策定する必要がある。選定にあたっては、委託業務範囲及び外部委託先のサービスの性質、利用形態に関する委託元と外部委託先の責任分界点を考慮のうえ、外部委託先の資質・業務遂行能力に関する情報、内部統制、及びリスク管理に関する状況等をもとに評価を行うことが必要である。評価にあたっては、外部委託先の情報開示における条件等を考慮し、必要に応じ機密保持契約を事前に締結したうえで開示を求めることが望ましい。

ただし、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合は、外部委託先の公開情報や、業界における評判や実績等による客観的な評価を行うことも可能である。

また、委託業務が再委託される場合、外部委託先と同様、金融機関等は再委託先の選定要件を策定する必要がある。また、特定システムが再委託される場合は、委託先のみならず、金融機関等みずからも再委託先の評価を実施する必要がある。通常システムでは、外部委託先における再委託先の審査・管理プロセス及び運用状況が金融機関等と同等かそれ以上に実効的であるかを検証することで、再委託先の評価に代替することが可能である。

評価する事項としては、以下の例がある。なお、業務が再委託される場合、再委託される業務の内容やリスク特性に応じ、再委託先を評価する事項が外部委託先と異なる点に留意する必要がある。

(1) 外部委託を想定する業務に係る実績、技術レベル
　① 信頼度及び受託実績（類似システムの開発実績、他プロジェクトやサービスにおける評判等）
　② 技術レベル（業務内容の理解度、業界に関する知識（金融機関等が委託する業務に関する専門性）、情報収集能力、プロジェクト管理能力（外部委託先が安定して業務に係る開発・運用をしているか等）、導入サポート力等）

(2) 事業継続性（経営方針、経営体力・収益力、人的基盤、被災時の BCM・データのバックアップ）

(3) サービスの可用性・データの安全性（機密性保護）・完全性の確保のための態勢、セキュリティ対策の実施状況（機密保護状況を含む）

(4) 内部統制やリスク管理等に関する状況（再委託先管理も含む）、外部監査の受検や各種公的認証の取得状況、組織体制（コンプライアンス体制を含む）

(5) 情報開示における条件

特に情報セキュリティに関する事項は、十分に把握しておくことが重要である。情報セキュリティに関する事項としては、以下の例がある。

　① データの入力・保管・処理・バックアップ・出力といった一連のフロー
　② 暗号方式、暗号化領域、非暗号化領域
　③ ログ（システムログ、業務ログ、操作ログ等）の取得範囲・取得頻度・保存期間・開示範囲

コメント [A4]: 利便性・読みやすさの観点から、内容の近い対策を統合（3 に統合）。

削除: 2　システムの開発や運用または、サービスの利用等に関する計画の承認時に、外部委託に関する事項についても責任者の承認を得ることが必要である。

削除: 適切な

削除: 選定

削除: その際

コメント [A5]: No.3,No.23

削除: （クラウドサービスにおける IaaS、PaaS、SaaS 等によって委託先の責務に差異が生じること等）

削除: を行う

削除: を

削除: する

コメント [A6]: No.16
外部委託有識者検討会の提言内容を踏まえ追加。

コメント [A7]: No.16

削除: での

削除: リスク管理に直結する

削除: リスク管理に直結する

削除: には

④　バックアップを含むデータコピーの取得内容・保管場所・保管期間
⑤　インフラのバージョンアップ作業及びネットワーク設定情報の変更　等

(6) 監査の受入に関する方針、訪問調査の受入スタンス、コミュニケーションルート
(7) 既存システムとの連携・新システムへのデータ移行の容易性
(8) 保守体制・サポート体制（サポートデスク、問題発生時の対応力（障害発生時におけるトレーサビリティの確保等）、日本語による対応）
なお、外部委託先が提供するアプリケーション、サービス等の導入に際しては、【実 65、実 66】も参照のこと。
(9) インシデントが発生した場合の想定損害額（直接損害・間接損害）と外部委託先側が提示する損害賠償・補償上限額とのバランス
(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）
契約の中断・終了に伴い発生する可能性があるシステム移行作業（移行データの抽出方法と実際の移行作業内容）など
(11) 個人データの取扱い
個人データの取扱いの全部または一部を外部委託先に行わせることを内容とする契約を締結する場合、「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」のⅢに定める「個人データ保護に関する委託先選定の基準」に対する準拠対応可否
(12) 委託費と支払い条件
(13) 係争時等における他国での裁判に関する事項
外部委託先との間で係争が生じた場合の準拠法及びこれを取り扱う裁判所に関する取決めが他国である場合に評価すべき事項など
他国での裁判に関する事項として評価すべきリスクとしては、以下の例がある。
①　現地の各種法制及び裁判制度の把握及び分析
②　現地における活動資格を有する弁護士の確保
③　地理不案内な遠隔地での打合せや出廷などに伴う経済的、人的負担
④　上記すべてについての外国語での対応

3　外部委託先（または再委託先）の決定には、責任者の承認を得ることが必要である。また、システムの開発や運用またはサービスの利用等に関する計画の承認時に、外部委託に関する事項についても責任者の承認を得ることが必要である。

4　委託契約期間中においても、継続的に外部委託先（または再委託先）を評価することが望ましい。

削除: での

削除: や

削除: や

削除: での

コメント [A8]: 2 を統合

コメント [A9]: 【統 22】から移動

削除: ＜参照先＞.
外部委託先が提供するアプリケーション、サービス等の導入に際しては、【運 72、運 73】も参照のこと。

外部の統制
契約締結時

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　22	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。

安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。

1.　金融機関等が外部委託した業務が安全に遂行されるために、機密保護や安定的なシステム運用等を契約として外部委託先と締結するとともに、その契約の遵守状況を定期的に確認することが必要である。また、委託契約とは別に「機密保持に関する契約」や、「リスク管理に関する契約」を締結することも考えられる。

契約時に考慮すべき事項としては以下の例がある。なお、委託する業務の内容、リスク特性、再委託の有無等によって、契約時に考慮すべき事項が異なることに留意する必要がある。

コメント [A1]: No.16 を受け、例示の内容は「選択的」であり、全てが一律適用されるものではない点を明記した。

(1) 基本的な事項

① 用語の定義、役割分担、責任範囲、債務不履行時の損害賠償範囲、準拠法、裁判管轄等
② 検収、納品の条件と手順、及び権利の移転の時期
③ 品質の保証と確認手順
④ 作業時間、立入場所等
⑤ 指示目的外使用
⑥ 契約変更の場合の手順
⑦ 仕様変更の取扱い

(2) 個別契約条件、サービス仕様、データ保護の管理策

① 利用する業務の期限、費用
② 外部委託先（複数の外部委託先が業務の委託を受けた場合も含む）への業務委託範囲や委託先のサービスの性質や利用形態を考慮した委託元と委託先との間の管理境界や責任分界点に関する取決め

コメント [A2]: No.23

削除:（例えばクラウドサービスの利用にあたっては、利用形態（IaaS、PaaS、SaaS など）によって責任分界点の考え方に差異が生じる場合がある）

③ サービス仕様（リソースの割当て等（仕様上の制限や変更に必要な時間等））
④ 機密保護
⑤ 金融機関等が守るべき法令や金融機関等のセキュリティポリシー等、外部委託先の要員が遵守するべきルール
⑥ セキュリティ管理方法及び体制
外部委託先におけるデータ漏洩防止に関する対策（暗号化等）、管理体制（暗号鍵の管理体制等）【実 33】【実 118】【実 119】

削除: の

コメント [A3]: No.6,13,24

⑦ データのバックアップ

(3) サービスレベル未達の場合の対応
(4) 情報開示範囲、監督当局等による検査等への協力義務、事業者と利用者間の報告・連絡等の運営ルール、インシデントレスポンスの取扱い
① 作業の報告方法と報告形式
② 作業の指示に関する取決め
③ 利用する業務における問題発生時の解決体制
④ 保守及び障害時等の回復作業・復旧手順、マニュアル整備及び教育・訓練
⑤ 目標復旧時間（RTO：Recovery Time Objective）
⑥ 事故発生時における報告
⑦ 情報漏洩等のインシデントが発生、または発生が疑われる場合における、トレーサビリティ確保のための調査協力義務
⑧ 利用する業務における外部委託先における対策を含むコンティンジェンシープラン（緊急時対応計画）【統 17】【統 18】
(5) 反社会的勢力・テロ組織と関わりがないことの表明・確約
(6) 契約の解除条件、契約終了時のデータの返却・消去等及び、契約終了時の原状回復・新システム移行時における協力義務
① 契約の解除条件（外部委託先の業務遂行に問題がある場合に、他の外部委託先等と契約する権利等）
② 契約終了時における外部委託先によるデータ消去の実施（物理的消去または論理的消去等の方法、開発ＰＣなど消去の範囲）及び実施時期、消去証明書等の発行（または消去プロセスの有効性に関する外部の第三者による検証）、文書等の廃棄・回収など【実 68】
③ 契約終了時における原状回復・データ移行作業等の協力義務
(7) 損害が発生した場合の協議や賠償に関する取決め
(8) 外部委託業務の成果の知的財産権や使用権等の権利の帰属
(9) 外部委託先からの情報開示
① 平常時における標準的な情報開示内容の明記
契約または SLA 等による情報開示の範囲に関する合意、開示請求の対象情報の機密性が高い場合における機密保持契約の締結など
② リスク顕在化時の情報開示
リスク事象が発生した際や、各種の資料により情報漏洩リスクが高まった、または外部委託先側の内部統制状況が悪化したなどと判断される場合の委託元金融機関等からの請求内容に応じた情報開示など
(10) 複数の外部委託先への委託
金融機関等と外部委託先間における責任関係の明確化、一元的な窓口機能や外部委託先間の相互調整機能を担う事業者の選定など
(11) 再委託管理
① 再委託先に対する金融機関等の事前審査の実施
再委託先の選定要件の策定、評価、選定プロセスなど
選定要件の策定及び、評価については、【統 21】を参照のこと。
② 損害賠償も含めた責任の明確化
再委託先が問題を発生させた際の委託先の管理責任及び、損害賠償の上限に関する条項など

コメント [A4]: （12）監査権の明記と内容が重複するため削除
削除: 金融機関による監査受入、
削除: での
削除: 原状回復・新システム移行時の協力義務、
コメント [A5]: No.8
削除: 等
削除: もしくは
コメント [A6]: No.7,9,14,24
削除: 時期
削除: 【統 26】3.
削除: 委託元
削除: ・
削除: での
削除: 外部委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等かそれ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ外部委託先の審査・管理プロセスの整備・運用状況の適切性を検証し、確認することで、個別の再委託先の事前審査に代替させることも考えられる。

③　外部委託先・再委託先間の義務の明確化

外部委託先との契約において、外部委託先が金融機関等に対して負う義務（報告、内部統制確保など）に関する内容と同等の条項が外部委託先・再委託先間の契約上に明記されているか

④　再委託の中止の扱い

各種の報告資料等を踏まえ、再委託先の業務遂行能力に対し、問題視し得る状況が生じた場合、金融機関等は外部委託先に対し、再委託の中止を求めることができる条項、外部委託先が中止の求めに応じない場合の業務委託契約の解除に関する条項の設置など

(12) 監査・モニタリング【監 1】

①　監査等の権利

外部委託先・再委託先に対する委託元金融機関等の監査等を実施する権利の明記

なお、監査の方法については、【監 1】を参照のこと。

②　監査等の権利行使

委託業務において重要な脆弱性が判明した場合や、委託元金融機関等への影響が懸念される場合において監査等を実施する権利の明記

③　監査等の受入対応費用

監査等の受入対応の費用負担に関する取り決めの明記

④　監査等の指摘事項の扱い

監査等により判明した指摘事項への対応に関する取り決め（費用負担・対応期間等）の明記

(13) インシデント発生時の立入調査

①　情報漏洩等のインシデントが発生した場合、外部委託先における他の顧客に関わる領域でインシデントが発生した場合、または他事業者において委託業務と関連性を有するインシデントが発生した場合、もしくは発生が疑われる場合等において、委託元金融機関等みずから、または委託元金融機関等が指定するセキュリティ業者・デジタルフォレンジック業者が立入調査することについて外部委託先と予め協議しておくことが考えられる。

②　インシデント発生時において調査に必要なデータの収集範囲や分析に必要なツール等の提供（提供されない場合は、分析に係る費用等）について、外部委託先と予め協議しておくことが考えられる。

③　外部委託先の経営不安が発生した場合、委託元金融機関等みずから、または委託元金融機関等が指定する専門業者が、必要に応じ、外部委託先施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことについて、委託先と予め協議しておくことが考えられる。

(14) 記憶装置等の障害・交換

記録媒体等を障害や交換等の事情により施設外へ持ち出す場合には、記録済データをあらかじめ復元が不可能または著しく困難な状態とする。また、記憶装置等の障害・交換におけるデータ消去については、消去証明書の発行・取得または、外部委託先に対する情報提出要請や、監査等の方法で消去・破壊プロセスの実効性を検証する。

(15) 海外におけるデータ保管時の留意点

金融機関等における障害対応要員の現地の語学力が十分でない場合、日本語によるサポート、外部委託先の日本法人等の障害対応窓口設置を明確にする。

(16) トレーサビリティの確保

削除: る内容となっ

削除: や

削除: 、

削除: の明記

削除: 及び

コメント [A7]: 外部委託先、再委託先に対する監査の方法（代替策含め）については、【監１】に集約した。

削除: ②　監査等の代替手段 . 〈#〉金融機関等が直接、監査等を実施するのではなく、平常時には監査等のスキルのある外部の第三者が検証を代替する等の手段の明記 . ③

削除: を受ける外部委託先側

コメント [A8]: No.15

削除: 旨の明記

コメント [A9]: No.6,13,24

削除: 【統 26】

削除: での

削除: での

万一障害や情報漏洩等のインシデントが発生した際には、流出・毀損したデータの特定や原因究明のための作業が複雑化する場合があることが想定されるため、トレーサビリティ確保のための方策を準備する。

2. SLA の締結または SLO の確認により、サービスレベルについて合意することが望ましい。

削除: や

SLA 及び SLO に記載される指標としては、以下の例がある。

(1) システム運用（可用性（注）、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、オンラインシステムの稼働開始時限）に関する事項

コメント [A10]: No.16

削除: の保証

（注）システム運用の可用性に関する指標の評価にあたって考慮する事項としては、以下の例がある。

① 障害等に伴うシステムの停止時間

② システムの更新・保守（緊急的なセキュリティパッチ対応を含む）や新サービスの追加などシステムの品質・セキュリティ向上のための計画停止期間

(2) サポート（障害対応、問合せ対応）に関する事項

削除: の保証

(3) データ管理（利用者データの管理等）に関する事項

削除: の保証

(4) 統制環境（再委託先管理（再々以下の階層の先を含む）、機密保護の維持、統制環境の維持）に関する事項

削除: 保証

(5) 開発業務を委託する場合の開発に要する人員や開発期間、期限に関する事項

削除: の保証

削除: の保証

なお、広域災害等の影響により外部委託先が SLA どおりに委託業務を遂行できない場合の対応策についても、事前に考慮しておくことが望ましい。

4. サービスレベル合意の違反のほか、外部委託先や金融機関等の方針変更によって外部委託先との契約の続行が困難になるような場合でも、業務の継続を可能とする対策を講ずることが望ましい。

コメント [A11]: 外部委託先の評価に関する内容のため、【統 21】へ移動

削除: 3. 委託契約期間中においても、継続的に外部委託先を評価することが望ましい。

実施する対策としては、以下の例がある。

(1) 外部委託先による移行すべきデータの抽出方法の提供及び移行作業への協力義務に関する契約書への明記

(2) 契約の解約時におけるシステム移行作業にかかる費用負担の契約書への明記

（参考）

外部委託の形式について

(1) 派遣（労働者派遣）とは、派遣元事業主が自己の雇用する労働者を、派遣先の指揮命令を受けて、この派遣先のために労働に従事させることを言う。派遣労働者と派遣元事業主との間には雇用関係が、派遣労働者と派遣先との間には指揮命令関係がある。なお、派遣形態での契約における労働者の管理については、「労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律」を参照のこと。

(2) 請負とは、請負者（企業）が労務提供の結果として請負った仕事を完成させ、注文者（企業）がその成果に対して報酬を支払うことを、約束する契約形態である。請負では請負者が従業員等をみずから指揮命令し、請負った仕事を完成させる。（請負の意義　民法第 632 条参照）

(3) 委任は、請負者が従業員等をみずから指揮命令し、労務を提供する点で、請負と同じである。しかし、請負では仕事の完成に対し報酬が支払われるが、委任では委任された労務の提供自体に対し報酬が支払われる点が異なっている。（委任の意義　民法第 643 条参照）

参照法令	労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律、民法第 632 条、643 条

【資料３－３】
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

外部の統制
外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

セキュリティ管理を適切に行うため、外部委託先（再委託先を含む。以下同じ）の要員に対し、委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、その遵守状況を管理、検証すること。

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や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。

具体的な取り組みとしては以下の例がある。

(1) 外部委託先の要員が遵守すべきルールの明示

業務遂行のマネジメントを含む委託の場合には、業務体制や監査等のセキュリティ要件を、外部委託先と合意のうえで契約、あるいはそれに準じた文書の中で列挙する。

なお、外部委託先の要員が遵守すべきルールとしては以下の例がある。

①　金融機関等のセキュリティポリシー
②　コンピュータセンターの入退館管理ルール、機器管理ルール
③　各種情報へのアクセス権限の管理ルール（ID やパスワードの付与、抹消ルール等）
④　開発工程において作成されたドキュメントや磁気媒体の管理手順

(2) 外部委託先の要員が遵守すべきルールの周知徹底

2.　外部委託先の要員に与える、金融機関等の各種資源やシステムへのアクセス権限は、業務遂行のために必要な範囲に限定する必要がある。なお、アクセス権限の取得及び見直しの手順については【運 18】を参照のこと。

3.　金融機関等は、上記のルールの遵守状況を確認する必要がある。そのためには、金融機関等は外部委託業務の内容や作業の範囲に応じて、外部委託先における業務の遂行状況について監査を行うことや、外部委託先からの業務報告を受けるなどの対策を講ずる必要がある。

監査については、【監 1】を参照のこと。

コメント [A1]: 遵守状況を「管理する」という表現が分かりにくいため、「検証する」も含め、「確認する」に見直した。

削除: 管理、検証

削除: 外部委託先（再委託先を含む）の要員の

コメント [A2]: 目的と手段が明確になるよう、文章を見直した。

削除: 委託業務の内容に応じて

削除: 周知徹底する

削除: と

削除: 管理、検証

【資料３－３】
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

外部の統制
外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 24	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。

外部委託先（再委託先を含む。以下同じ）のセキュリティ管理状況及び、委託した業務が適切に遂行されているかを確認するため、委託業務の内容または作業の範囲に応じて、外部委託管理体制を整備するとともに、委託契約に基づき委託業務の遂行状況を確認するこ

1. 外部委託の対象の業務を円滑及び適正に運営する観点から、委託業務の内容または作業の範囲に応じて外部委託管理体制を整備するとともに、委託契約に基づき委託業務の遂行状況を確認する必要がある。また、金融機関等自身と外部委託先の業務範囲及び責任を明確にし、相互牽制を有効に機能させる必要がある。

   なお、組織の整備及び相互牽制については【統 12】を参照のこと。

   業務遂行状況の確認方法としては、以下の例がある。

   (1) 委託先の管理状況を把握する。

   管理状況の把握方法としては以下の例がある。

   ① 管理責任者より状況を聴取する。

   ② 定期的に作業状況の報告を受ける。また、定められた場所以外で作業が行われていないことを確認する。

   ③ 作業の機密管理状況の報告を受ける。また、定められた場所以外には情報が持ち出されていないことを確認する。

   ④ 委託先における業務遂行に関する重要な事項の変更（管理責任者の交替、システム更新など）の報告を受ける。

   ⑤ セキュリティに関する事故及び犯罪の報告を受ける。

   (2) 委託先における業務の遂行状況について、監査等を行う。

   確認した結果及び認識した問題点については、その影響度に応じて、経営層へ適切な報告を行う。なお、監査については【監 1】を参照のこと。

   (3) 委託先における業務の遂行状況を定期的にモニタリングする。

   委託元は、担当要員を選定等して、委託先における顧客データ等の管理状況、データ漏えい防止に関する対策の遂行状況及び開発・運用状況等について把握する。

2. 外部委託先の業務の成果が金融機関等の求めるレベルに達しているか、金融機関等が把握する必要がある。例えば、システム開発を委託する場合は、機能要件の充足度、標準化遵守状況の確認及び異例処理を含んだ検証テストを行うことなどが考えられる。

   なお、この業務の成果を計測するために、ベンチマークである SLA をあらかじめ外部委託契

コメント [A1]: 外部委託における「業務組織」の整備を行うとした基準であるが、委託先組織の整備を金融機関等が行うのではなく、委託業務を遂行するための体制、業務遂行状況を金融機関等が確認することが求められると解し、全体を見直した。

削除: 業務組織の

削除: 管理、検証を行うこと

削除: 外部委託先（再委託先を含む）に

削除: 内容の実施状況を確認

削除: 業務組織

削除: を行う

削除: 管理、検証を行う

コメント [A2]: データ漏えい防止に関する基準の統合・整理を受け、運用時（モニタリング）における対策を当基準に明記した。

削除: 委託業務を遂行する業務組織

削除: （金融機関等自身と外部委託先の両者により構成される組織）の

削除: （再委託先含む）

削除: と組織

削除: する体制とする

削除: 組織の整備

削除: に関する具体的事例

削除: 業務処理

削除: 体制

削除: 実施

削除: 実施

削除: （Service Level Agreement）

約の１つとして金融機関等と外部委託先の間で締結し、これに対する評価を定期的に行うことが有効である。SLA の締結については、【統 22】を参照のこと。

　また、認識された問題点については、外部委託先に連携して速やかに対応することが必要である。

個別業務・サービス
クラウドサービスの利用

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

統27	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。

クラウド事業者に対する統制を十分かつ実効的に機能させるため、クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。

1. 金融機関等は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。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。

（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のことを示しており、クラウドサービスにおける情報処理の広域性（データの切片化、記録保管場所が時間軸に沿って流動的となる等の特徴）を勘案し、金融機関等が統制を行うべき対象となる。統制対象クラウド拠点は、クラウド事業者のデータセンター、オペレーションセンター、本社、営業所等様々な拠点が候補となるが、金融機関等によって、利用するクラウドサービスの内容やクラウド事業者の内部管理状況等を踏まえ、金融機関等が個別に特定することとなるため、上記の候補以外が対象となる場合もある。

2. 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とともに、定期的に監査を実施する必要がある。監査の実施にあたっては、技術の先進性などを考慮し、クラウド事業者が監査人に保証型監査を委託するか、同等の効力を有する監査を実施し、その監査報告書を利用することが望ましい。なお、監査の方法については【監１】を参照のこと。

3. クラウド事業者に対する監査及びモニタリングを実効的に実施するため、クラウド事業者において採用されている技術など専門知識を有する人材を配置することが望ましい。ただし、金融機関等内部で確保・育成することが困難な場合においては、専門性を有する第三者監査人等の利用を考慮することも考えられる。

4. クラウドサービスの利用にあたっては、新しい技術によってサービス内容や利用形態が変化する可能性があるため、検討時点から広義の IaaS，PaaS，SaaS 等のクラウドサービスの形態に関する定義を参考にし、金融機関等とクラウド事業者との責任範囲を明確にした上で利用を開始することが望ましい。

コメント [A1]: 個別の業務・サービスに関する基準として、「外部の統制における付加基準」と整理した。

削除: 基礎

削除: であり

削除: 金融機関みずからが監査を実施する方法以外にも、

削除: 、または同等の効力を有する監査

削除: も考えられる

削除: 実施にあたって

コメント [A2]: No.23

外部の統制
共同センター

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

統 28	共同センターにおける有事の際の安全対策を講ずること。

勘定系システムにおいて共同センターを利用する場合、迅速に初動対応が取れるようにするため、緊急事態の発生に備えた適切な安全対策を講ずること。

1.　勘定系システムにおいて共同センター（注）を利用する場合、緊急事態の発生に備えて適切な安全対策を講ずることが必要である。

共同センターにおいては、緊急事態が発生した際の関係者が複数金融機関等にまたがり、対応方針を相互に合意するのに時間を要する可能性がある。そこで、対応に関する意思決定を迅速化するため、コンティンジェンシープランには初動対応を決定するための手順を盛り込み、利用金融機関等及び共同センターと合意しておくことが考えられる。

想定される緊急事態については、【実 58】を参照のこと。

（注）勘定系システムにおいて共同利用型のクラウドサービスを利用する場合も対象となる。共同センターの定義については、本書Ⅲ.4 用語の解説を参照。

迅速な初動対応を可能とする手順としては、以下の例がある。

(1) 利用金融機関等の利益を代表する共同運営組織が有事の際の初動対応を決定する。
(2) 有事に初動対応を決定する金融機関等を事前に定めておく。
(3) 一定の影響範囲内の障害においては、共同センター側があらかじめ合意された対応を実施したうえ、利用金融機関等に事後報告する。
(4) 初動対応の定期的な訓練（机上訓練含む）
(5) コンティンジェンシープランの定期的な見直し　等

2.　安全対策の検討にあたり、有事等に備えて必要となる IT 人材を、継続して配置するために、利用金融機関等または委託先と共同で、人員計画を策定することが望ましい。

コメント [A1]: 個別の業務・サービスに関する基準として、「外部の統制における付加基準」と整理した。

削除: 基礎

削除: 管理策

コメント [A2]: 他の基準と表現を統一するため、「安全対策」に修正。（４箇所）

削除: 有事発生

削除: 管理策

コメント [A3]: 目的が明確になるよう、表現を一部修正。

コメント [A4]: 「有事発生」には、戦争やその他の事変が含まれると解される可能性があり、コンテ策定の際に考慮される「想定される緊急事態」という表現に見直した。

削除: 有事発生

削除: 管理策

削除: 有事の

削除: 管理策

外部の統制
金融機関相互のシステム・ネットワークのサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

統 29	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。

金融機関相互のシステム・ネットワークは、金融機関相互の金融取引の決済や CD･ATM オンライン提携などを行ううえで、基幹インフラとしての機能を担っている。仮に当該システム・ネットワークにおいて、障害が発生した場合は、その影響は決済システム全体及び顧客サービス全般に及びかねないことから、金融機関等は適切なリスク管理を行うこと。

1. 金融機関等がその業務を営むために必要な事務を第三者に「委託」する場合は、金融機関等みずからが、委託先の選定や委託内容（提供されるサービスの内容やレベル等）を取り決めることができるのが一般的である。

一方で、金融機関相互のシステム・ネットワーク(注1)の「サービス利用」については、当該サービスの提供元が限定されており、加えて数多くの金融機関等が共同で利用しているという特徴がある。

このため、各金融機関等が、外部委託の管理と全く同様に、サービスの提供元を複数の中から選定することや、独自にリスク管理を行うことは難しく、また非効率な場合が多い。

したがって、当該サービスの利用にあたっては、以下の観点で管理することが必要である。

(1) 金融機関等は、当該サービスの管理者(注2)に対して、システム上の適切な対応がなされていることを確認する。

具体的には、金融機関等は、①サービスの管理者から受領した監査報告を評価する、②金融機関等みずからが利用している範囲で、障害の発生を確認できる体制を構築する、などが考えられる。

なお、サービスの管理者が IT ベンダーの場合には、サービスを利用する金融機関の代表組織等が組織運営に関わることが多い。その際には、代表組織等が、金融機関等に代わり、当該サービスの管理者に対して、システム上の適切な対応がなされていることを確認し、各金融機関等に報告することも考えられる（以下、(2)、(3)も同様の扱い）。

(2) 当該サービスにおいてシステム更改を行う場合には、金融機関等みずからも、システム上の適切な対応がなされていることを、必要に応じて十分に評価・確認する。

具体的には、①当該サービスとの接続テストにより、金融機関等のシステム（外部委託するシステムを含む）のほか、当該サービスの更改後のシステムが正常に稼働することを確認する、②当該サービスの管理者から、プロジェクト管理体制やシステム品質状況等、システム更改の内容に応じた必要な報告を受けること、などが考えられる。

コメント [A1]: 個別の業務・サービスに関する基準として、「外部の統制における付加基準」と整理した。

削除: 基礎

削除: 受ける

削除: みずから

(3) 特に、当該サービスの運営、及び更改に係る意思決定において、金融機関等が主導的な役割を果たしている場合には、金融機関等は、当該サービスの管理者とともに、十分なリスク管理態勢、プロジェクトマネジメント態勢等を整備する。

具体的には、金融機関等みずからによる当該サービスのシステム・ネットワーク構成の確認、進捗会議等への参加、問題点への対処などを行うことが考えられる。

（注 1）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、信用金庫業界の ATM・為替のシステム、信用協同組合業界の ATM・為替のシステム、労働金庫業界の ATM・為替のシステム、農業協同組合業界の ATM・為替のシステム。

なお、金融機関等が上記以外のシステム・ネットワークサービスを対象とすることも考えられる。

削除: を妨げない

（注 2）金融機関等が利用する当該サービスを管理する組織。金融機関等により組成された組織のほか、サービスを提供する IT ベンダーとなる場合などがある。

改訂案

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

監１	システム監査体制を整備すること。

コンピュータシステム及びその管理について、有効性、効率性、信頼性、遵守性、及び安全性の面から把握、評価するため、システム監査体制を整備すること。

1. コンピュータシステムの運用、システム開発・変更等においては、コンピュータシステムの有効性、効率性、信頼性、遵守性、及び安全性を確保するため、コンピュータ部門から独立したシステム監査人がシステムの総合的な監査・評価を行い、経営層に監査結果を報告する必要がある。

　なお、被監査部門としては、コンピュータシステムに関して、その開発及び運用を担当する部門（外部委託先を含む）が該当するが、本部各部門や営業店などの利用部門、EUC（エンドユーザーコンピューティング）実施部門等においてもシステム監査またはそれに準じた監査を受けることが望ましい。特に、個人データを取り扱う情報システムの利用及び個人データへのアクセスの監視状況については、システム監査またはそれに準じた監査を受けることが必要である。

　システム監査を実施するにあたっては、当センター発刊の「金融機関等のシステム監査指針」、個人情報保護委員会並びに金融庁が策定した「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」等を参照のこと。

コメント [A1]: 重要な参照先の解説となるため、冒頭部分に移動した。

2. 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。

3. システム監査における指摘事項については、システム監査部門と被監査部門の間で、事実確認、及び十分な意見交換を行い、問題があると認められた点について適切な改善を行うことが必要である。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。

削除: 実施結果による

5. システム監査人として、コンピュータシステムに精通し、監査スキルを保有する人材を確保する必要がある。

6. 金融機関等が業務委託を行う場合には、委託した業務の遂行状況及び、外部委託先要員のルールの遵守状況等について検証・監査することが必要である。

　また、提出された情報のみで委託業務の適切性の検証が十分にできない場合は、外部委託先

削除: 及び委託した業務内容の実施遂行状況

のオフィスまたは、データセンターへの監査・モニタリング等により実地で確認することが必要である。なお、特定システムが再委託される場合には、外部委託先同様、再委託先に対しても金融機関等の責任において監査を行う必要がある。

削除: や

削除: 重要な業務

外部委託先の監査の方法としては、以下の例がある。

コメント [A2]: 以下、監査の方法について整理案を示させていただいた。（修正箇所が多岐に渡るため、修正履歴については省略させていただいている）。

(1)　金融機関等がみずから外部委託先の監査を行う。また、複数の金融機関等が同一の共同センター等を利用する場合は、金融機関等が共同で監査を行うことも考えらえる。なお、金融機関等の監査等が実効的でない場合には、第三者監査等（注）により代替することも考えられる。監査を行う際、外部委託先から提供されたデータ抽出のツールを利用したデータ検証を行うことも考えられる。

（注）金融機関等が監査法人を利用した監査を行う場合、監査の対象期間において外部委託先の会計監査に従事していない監査法人とし、また、選定した監査法人が外部委託先の SOC2、IT7 号の保証業務に従事している場合には、外部委託先の保証業務に直接従事していない監査責任者を選定するなどにより、外部委託先との利益相反に疑義が生じないような外観とすることが考えられる。なお、第三者監査人の適格性の担保のため、監査人(監査法人)が日本公認会計士協会等の指導や指針等に基づいて、適切な品質管理体制の整備、運用を実施することも考えられる。また、外部委託先のリスク特性を踏まえた検証、金融機関等の検証ニーズに則った検証を行う。

(2)　外部委託先の内部監査部門の監査結果報告について確認を行う。なお、共同センター等、委託元金融機関等が複数の場合は、監査結果を複数の委託元金融機関等に報告することも考えられる。

(3)　第三者認証(注)のレポート、または外部委託先が作成したセキュリティに係るホワイトペーパーについて確認を行う。

（注）各国の公認会計士協会や業界団体等が定める事業者等の情報セキュリティ体制やプライバシー保護体制の基準等に係る認証。代表的なものとして、ISMS(ISO27001)や PCI DSS level1、SOC1、SOC2、監査・保証実務委員会実務指針第 86 号、IT 委員会実務指針 7 号、プライバシーマーク等がある。

以下、一部（下線部）を除き削除の予定。（実態を捉え、改めて基準として記載すべき内容が少ないと判断したため）

(3) 委託元金融機関等の監査等が実効的でない場合などには、第三者監査により代替することも考えられる。その際に考慮すべき事項としては、以下の例がある。

① 検証項目については、外部委託先のリスク特性を踏まえた検証、金融機関等の検証ニーズに則った検証を行う。なお、金融機関等が単独、または他の金融機関と共同で第三者監査人と監査契約を締結し、外部委託先に対する監査を行う場合、既に外部委託先が受検している監査結果の内容を検証し、疑問点や不足する監査項目を中心に外部委託先に対する実地検証を行うことが有効である。

② 委託元金融機関等が、単独または共同で第三者監査人と外部委託先に対する監査に関する契約を締結し、外部委託先に対する監査を行う体制を選択可能とする。

③ 委託元金融機関等が、第三者監査に関する費用を負担(または分担)する体制に移行する。

④ 同一の監査責任者が長期間にわたり監査を行うことによる外観的独立性に対する疑念を払拭するため、適切なサイクルで交代させる。

⑤ 監査の品質を引き上げるために、SOC2 等、監査人側の損害賠償責任が契約書上明確化されている監査スキームを活用する。

⑥ 第三者監査人の適格性の担保のため、監査人(監査法人)が日本公認会計士協会等の指導や指針等に基づいて、適切な品質管理体制の整備、運用を実施する。

⑦ 第三者監査を効率的に行うため、複数の委託元金融機関等が共同で第三者に監査実施を委託する。

⑧ 海外におけるデータ保管時において、当該データセンターへの往査に必要な時間やコスト等を考慮する。

運用管理
コンティンジェンシープランの策定

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 58	コンティンジェンシープランを策定すること。

不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧を図るため、あらかじめコンティンジェンシープラン（緊急時対応計画）を策定すること。

削除: しておく

コメント [A1]: 表記の統一
「しておくこと」→「すること」

1. 不慮の災害や事故、あるいは障害時に、あらかじめ想定される複数のケースに応じてコンティンジェンシープランを策定することが必要である。

削除: しておく

なお、集中豪雨、降雪等による交通遮断や感染症のパンデミック発生などから生じる職員不在等の不測の事態についても、要員確保の観点から考慮することが必要である。
また、障害等が発生した時期、曜日、時間帯やシステム環境の違いにより対応する範囲や方法が異なる場合には、これらの対応を考慮する必要がある。
特に、広範囲に重大な影響を及ぼすような資金決済システム等の障害については、時限性や社内関連システム及び社外への影響等にも留意する必要がある。

本基準におけるコンティンジェンシープランとは、金融機関等のコンピュータシステムが、不慮の災害や事故・犯罪、障害等により重大な損害を被り業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務の復旧を行うためにあらかじめ策定された緊急時対応計画のことである。（「Ⅱ.1(4)⑤コンティンジェンシープランの策定」参照）

削除: 3

想定される緊急事態としては、以下の例がある。
(1) コンピュータセンター、本部・営業店等の全面被災、一部被災
(2) コンピュータ装置の破壊、損傷
(3) 端末機器等の破損、損傷
(4) 関連設備（電源、空調、給排水設備等）の破壊、損傷
(5) 回線の切断、通信設備の損傷
(6) 公共インフラの障害（停電、断水、交通遮断等）
(7) ソフトウェアの障害
(8) サイバー攻撃

また、コンティンジェンシープランの策定に際して考慮すべき内容としては、以下の例がある。
(1) 緊急事態を想定し、自社の業務や各種施設に対してどのような影響が起こるかを評価す

る。
(2) 緊急時における業務の継続の優先順位を評価する。
(3) 被災拠点及び対策本部における緊急時対応組織の体制（コンティンジェンシープラン発動権限も含む）や要員等を明確にする。
(4) 緊急事態発生時における、顧客・職員の安全確保、資産の保全、被災状況の把握等の措置を明確にする。
(5) 業務、顧客サービスの中断あるいは、中断による損失を極小化するために、業務の通常的な継続が困難な緊急事態のもとで、重要と判断される業務の暫定的継続を図るために必要な措置を明確にする。
(6) 早期に事態を収拾して、平常業務への復旧を図るために必要な措置を明確にする。
(7) 緊急時における要員の移動、機器等の物資の搬送手段及びルートを決めておく。
(8) プランの維持管理体制の確立を行い、定期的な訓練の実施とその結果に基づくプランの見直し等の維持管理を明確にする。
(9) 業務が外部委託されている場合は、委託先や再委託先（再委託には二段階以上にわたる再委託を含む）の役割等も明確にする（クラウドサービス、共同センターも含む）。

削除: 以上の

設備及び技術面の復旧策、並びに災害時・障害時等に備えた運用訓練については、以下の基準項目を参照のこと。また、コンティンジェンシープランを変更する際も、必要に応じて以下の基準項目を参照のこと。
(1) 環境 【設 1】
(2) 周囲 【設 2～設 4、設 7～設 9】
(3) 構造 【設 10～設 13、設 31～設 36】
(4) 開口部 【設 14、設 17～設 19、設 28～設 30】
(5) 内装等 【設 20、設 21】
(6) 位置 【設 22、設 25、設 26】
(7) 設備 【設 37～設 44】
(8) コンピュータ機器、什器、備品 【設 48、設 50、設 51】
(9) 電源室、空調機械室 【設 52、設 54～設 60】
(10) 電源設備 【設 62～設 71】
(11) 空調設備 【設 74～設 79】
(12) 監視制御設備 【設 80、設 81】
(13) 回線関連設備 【設 82、設 83、設 83-1】
(14) ハードウェアの予備 【技 2～技 6】
(15) 障害の早期回復 【技 22～技 24】
(16) 災害時対策 【技 25】
(17) 教育、訓練 【運 80～運 84】

なお、コンティンジェンシープランの策定に関する詳細内容については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照のこと。

2. 上記、コンティンジェンシープランの策定に際して考慮すべき内容(1)～(9)のうち、(3)～(6)及び(9)に掲げた内容については手順書として文書化することが必要である。【統 22】

削除: 揚げた

3. コンティンジェンシープランが策定された後においても、適宜見直しをすることが必要である。見直しを行う際は、事務手続き等の変更点にも考慮することが必要である。

   見直しが必要となる契機としては、以下の例がある。
   (1) 重要な業務についてその内容に変更が生じた場合
   (2) 従来、コンティンジェンシープランでは考慮していなかった業務についてその重要度が高まった場合
   (3) 上記業務遂行の前提となる組織や拠点施設、インフラ、システム構成等の条件に変更が生じた場合
   (4) 政府の取組みやガイドライン等が変更された場合
   (5) 定期的な検証　等

4. 組織図や緊急連絡網等については、最新の情報を維持するとともに、組織内に周知することが必要である。

5. コンティンジェンシープランの策定及び重要なプラン内容の見直しを行うにあたっては、経営層の承認を得ることが必要である。

6. コンティンジェンシープランは、対策本部、各拠点、バックアップサイトにおいて、必要な部分が常時保管され、全役職員が必要な部分を閲覧できる状態を保つことが必要である。なお、外部委託先や共同センター等に対しても保管され、利用可能な状態としておくことが望ましい。

7. 障害時・災害時等におけるシステムの復旧やバックアップサイトへの切替えを行う際は、セキュリティ管理のレベルが低下するおそれがある。当該事象が発生した場合のセキュリティについても通常時と同等のレベルを維持することが必要である。

8. 障害・災害によって生じる可能性のある損害賠償責任、逸失利益、業務継続に要する費用等に備えて、保険の適用を検討することが望ましい。

【資料４－１】
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

前説原案の修正内容について

Ⅰ．前説原案に対する各委員からのご意見について

各委員よりいただいた前説Ⅰ（概要）及び前説Ⅱ（フレームワーク）に対するご意見及び、対応方針については【資料４－２】に整理し、対応方針案を【資料４-３】の改訂案２に反映している。また、基礎基準（必須対策）の考え方について、方針案の内容を反映している。

【資料４－２】改訂原案（前説Ⅰ・Ⅱ）に対する各委員からのご意見・対応方針
【資料４－３】改訂案２（前説Ⅰ・Ⅱ）

Ⅱ．前説Ⅲ（本書の利用にあたって）について

本書の利用にあたり、基準構成、基準・解説の記述仕様、用語解説、参考文献等を、前説Ⅲとしてまとめた。また、今回の安対改訂において、適用までの経過措置（激変緩和措置）に関する記述を、「１．安全対策基準適用における経過的措置について」として記述した。

【資料４－４】改訂原案（前説Ⅲ（利用にあたって））

Ⅲ．前説原案最終案について

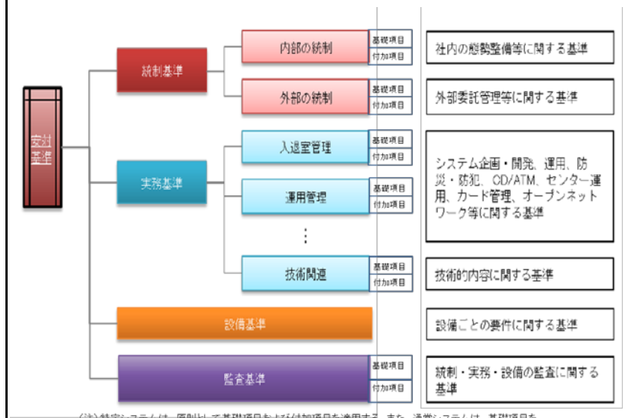
前説原案については、次回の委員会までに各委員の意見を反映し、最終案としてまとめる予定である。微細な修正については、ＦＩＳＣ事務局にて修正を行っていくこととさせていただき、それ以外のご意見については、個別に確認のうえ、次回の委員会までに反映方針を策定していくこととする。なお事後意見については、10/31（火）を締切とさせていただく。

以　上

【資料4－2】
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

■改訂原案（前説Ⅰ・Ⅱ）に対する各委員からのご意見・対応方針

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
*	3	－	（全般）	システムリスクの評価についてはこれまで各金融機関が個別に評価してきたものであるが、各金融機関が改めて「リスクベースアプローチの考え方」に基づくシステムリスクの評価を行うには相応の時間を要することが予想される。ついては、新しい安全対策基準の公表・発刊にあたっては、全金融機関が「リスクベースアプローチの考え方」を「一律的に、一斉に適用する」等の表現は避けていただきたい。	南都銀行 山田様(専) 藤谷様（検）	外部委託に関する有識者検討会の報告書でも述べられているように、リスクベースアプローチの考え方を導入するにあたっては、一律的、一斉に適用することは想定していません（激変緩和措置の必要性が述べられています）。例えば、システム更新の際に、順次適用していくことを想定しています。従って、新しい安全対策基準の記述においても、また対外公表に当たっても、その点を留意しながら作業を進めていくことを考えております。 →前説Ⅲ（利用にあたって）の冒頭に、「1. 安全対策基準適用における経過的措置について」とし、外部委託報告書の中で記載されている「激変緩和措置に関する対応」の内容を取込みました。	要	済
*	21	p1	（全般）	・金融サービスと金融関連サービス ・外部委託先と決済代行業者等 今回の改訂を機に新たなプレーヤーが基準を参照していく中で、上記の違いが明瞭な表現となることが必要と考えています。例えばAPIを活用する事業者は外部委託事業者ではないため、過度な統制を回避するためにも、個別の定義の記載を修正していく必要を感じております。	FinTech協会 瀧様(専)	「金融関連サービス」は金融機関等以外の事業者が金融サービスを補完する目的で提供するサービスであることを明確化するため、定義を用語解説に追加したいと考えております。また、本文中、金融サービスおよび金融関連サービスの語句については、実施主体を意識して必要な修正を加えています。 さらに、決済代行業者は、「FinTech企業等」という名称（No68参照）に暫定的に戻していますが、外部委託先＝FinTech企業とはならないケース（API連携など）を考慮し、関連する箇所に修正・補記を行っております。 用語定義に以下を追加し、意見を求めることにしました。 「金融関連サービス……　金融機関等（銀行等の預貯金取扱機関、信託会社、保険会社、証券会社、クレジット会社等をいう。ただし、電子決済等代行業者などの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」	要	済
*	72	p27	Ⅱフレームワーク 2. 統制 (2)外部の統制 ⑤派生形（3者間構成）における各論 b.タイプB	最後の段落の記載（新設部分）につき、銀行の参照系ないし更新系のAPIに接続する事業者が本人確認義務を負うシチュエーションは現状の業務と即していません。利用する口座は金融機関において開設されたものであり、二重の確認が発生する本記載は修正が必要と考えております。一方で、口座開設や取引の実行等、本来あるべき認証が必要なケースへの対応であれば、その旨が明らかとなる記載として頂ければと思います。	FinTech協会 瀧様(専)	ご指摘の点については、各論等を議論する中で、改めて整理させて頂きたいと考えております。	要	未
*	78	p17	Ⅱフレームワーク 1. 総論 (3)安全対策基準の適用対象	本件と「API接続先チェックリスト」の運用を行う際に、基礎基準を踏まえた安全対策を行うことが前説において定義されていますが、既に実効的なチェックリストの運用が行われている中で、基礎基準と「API接続先チェックリスト」とが2重に参照され実務上の混乱が生じないよう、前説に改めて、チェックリストに照らして適切な検討は、基礎基準との関係でも必要十分な検討であることに関し、言及をして頂きたく考えております。	FinTech協会 瀧様(専)	FinTech有識者会議における議論を踏まえ、内容を検討させて頂きたいと考えております。 →金融機関とFinTech企業等の間で、二者間にとどまらず広く共通的なチェックリストが存在する場合、チェックリストに基づく自主基準を策定することが可能であるとして、脚注に以下（下線部）を追加いたしました。 「金融機関等以外の事業者においては、各業界等で定める基準・ガイドライン等に従うことが想定されるものの、その際、金融機関等が最低限満たすべき「基礎基準」を踏まえた安全対策が選択・運用されることが期待される。例えば金融関連サービスの利用（API接続等含む）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。」 （金融機関等以外の企業については、No72を参照）	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
89 *	p13 p14	Ⅱフレームワーク 1．総論 (1)安全対策基準における定義 ③安全対策基準の構成	安全対策基準の構成は、「統制基準」「実務基準」「設備基準」「監査基準」の4編から定義され、『[図7]安全対策基準の構成』で図解されていますが、そのうちの一部基準はさらに「基礎基準」「付加基準」と細分化されて取扱うことにとなっています。また、P15上部の四角枠内の『「基礎基準」の選定にあたっての考え方』には「〇統制・監査に関する基準、〇顧客データの漏えい防止に関する基準、〇コンティンジェンシープラン策定に関する基準」と記載されています。 今回の原案で記載されている『基準』という字句は、それぞれ意図して使用されているものとは思いますが、それが多種多様のレベルで記載されているため、一般的には理解しにくいのでは？と感じます。 (例)『…安全対策基準では、統制基準の基礎基準である統制・監査に関する基準の基準小項目には「データ管理体制を整備すること」を定めているが、それは内部の統制に関することであり…』のように『基準』という字句を多く使用して説明せざるを得ない。 (対応案) ①「基礎基準」⇒「基礎項目」or「基礎事項」or「ミニマムスタンダード」、「付加基準」⇒「付加項目」or「付加事項」or「ベストプラクティス」などのように、『基準』という字句を他の字句に変更する。 ②全体像をイメージしやすくするために、『[図7]安全対策基準の構成』の4つの「統制基準」「実務基準」「設備基準」「監査基準」のなかにさらに細分化すべき「基礎項目」「付加項目」を記載し、『[図8]基礎基準と付加基準』は、図7の下部に注書きで記載する。(下図参照) ③P16の『「基礎基準」の選定にあたっての考え方』は、『基準』という字句ではなく、『観点』などの字句に変更し、「〇統制・監査に関する観点、〇顧客データの漏えい防止に関する観点、〇コンティンジェンシープラン策定に関する観点」に変更する。  [図 7] 安全対策基準の構成	労働金庫連合会 岡部様(専)	基礎基準の考え方について整理し、以下の図表を追加しました。基礎基準/付加基準との関係を含め、解説を加えさせていただきました(p15-p16に解説と図表8を追加しました)。 ・「〇」は、適用。 ・「△」は、選択的に適用。 [図表8]特定システム、通常システムへの基準の適用	要	済

	基礎基準		付加基準	
	必須対策	その他の対策	必須対策	その他の対策
特定システム	〇	△	〇	△
通常システム	〇	△	△	△

94 *	ー	(全般)	記述中に「等」や「など」が多数使われており、文意が不明確になっているかもしれないため、これらが何を指すかを明確にするか、使用箇所によっては「等」という表現を削除した方がよいのではないか？	慶應義塾大学 安冨様(専)	個別に確認のうえ、「等」・「など」の表現が不要な箇所があれば、見直しをさせていただきたいと考えております。	要	未
95 *	p1	Ⅰ.概説1.安全対策基準の意義	「…限りある経営資源を、安全対策のみならず、新規開発等にも適切に配分しいくことが重要となってくる。」について、 語尾は、「重要となってくる」ではなく、「重要である」若しくは「重要となる」ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	文脈より、ご意見にある「重要となる」が適切と判断し、「重要となる」に修正させていただきました。	要	済

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
*	96	p2	Ⅰ.概説2.安全対策の考え方	「…基幹業務系にとどまらず、情報系システムや部門システム等その範囲が広がり、基幹業務系以外のシステムがある程度大きなウエイト…。」について、 ・「基幹業務系にとどまらず」は繰り返し出てくるのでここでは不要。 ・「部門システム」は情報系との併記は適切ではないのでは。「情報系システム等」としてしまうか、「業務管理系システム」とするか。 ・「ある程度」は不要。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり修正させていただきました。 「金融機関等の情報システムは、情報系システム等その範囲が広がり、基幹業務系以外のシステムが大きなウエイトを占めるようになってきた。」	要	済
*	97	p2	Ⅰ.概説2.安全対策の考え方	「また、その形態や利用するサービスもホストコンピュータからクライアントサーバー、クラウドサービス、FinTech 企業等と連携した金融関連サービスなど、多様化してきている。」は、 「また、システムの構築方法は、オンプレミス開発でのホストコンピュータ中心からクライアントサーバーの増大、共同センターや外部委託、クラウドサービス利用の増加、FinTech 企業等と連携した金融関連サービスなど、大きく変化、多様化してきている。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり修正させていただきました。 「また、システム形態についてはホストコンピュータ中心からクライアントサーバなど分散処理型のシステムへの移行が進み、サービス利用についても共同センターやクラウドサービス利用の増加、FinTech企業等と連携した金融関連サービスの登場など、多様化してきている。」	要	済
*	98	p2	Ⅰ.概説2.安全対策の考え方	「また、金融機関等においては、システム開発・運用等における、外部委託への依存度が高まっているほか、金融関連サービスの利用が広がりをみせるなど、外部に対する統制の重要度が増している。」は、 「また、金融機関等においては、システム開発・運用等における、外部委託への依存度が高まっているほか、クラウドサービスやFinTech 企業等と連携した金融関連サービスの利用が広がりをみせるなど、外部に対する統制の重要度が増すとともに、統制のあり方も多様化してきている。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり修正させていただきました。 「システム開発・運用等における、外部委託への依存度が高まっているほか、クラウドサービスやFinTech 企業等と連携した金融関連サービスの利用が広がりをみせるなど、外部に対する統制の重要度が増すとともに、統制の在り方も多様化してきている。」	要	済
*	99	p5	Ⅰ.概説(1)ITガバナンスとITマネジメント	3)ユーザー(部門) 「金融機関等の本社主管部署で、…。」について、 「本社主管部署で、」は不要ではないか。各金融機関のシステム部門以外のガバナンス体系にまで話が及んでいる。	農林中央金庫 常岡様(専) 今嶋様(検)	ユーザー(部門)に対する説明について、「主管部署」といった組織に限定する必然性は低いため、ここでは「金融機関等の本社主管部署で、」とした部分を削除したいと考えております。	要	済
*	100	p6	Ⅰ.概説(2)リスクベースアプローチ	① 安全対策基準を取り巻く環境の変化 …大きな比率を占めてきたその他情報システムについては、…。 以下のように修正してはいかがか。 ・「占めてきた」は「占めるようになってきた」 ・「その他情報システム」はきちんと定義をする、若しくは長くとも同じ表現を使用したほうが良いと考える。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり修正させていただきました。 「大きな比率を占めるようになってきた基幹業務のオンラインコンピュータ・システム以外の情報システムについては、」	要	済
*	101	p6	Ⅰ.概説(2)リスクベースアプローチ	「…そのシステムにおいて適切ではない安全対策が最終的にそのまま実施されてしまう。」は、 「…そのシステムのリスク特性と比較しバランスを失した安全対策が最終的にそのまま実施されてしまう。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見にある「バランスを失した」という表現は、読者にとって容易にイメージできない恐れがあると感じました。ご意見にある「リスク特性と比較し」を活かし、以下のとおり修正させていただきたいと考えております。 「…そのシステムのリスク特性と比較し適切ではない安全対策が・・・」	要	済
*	102	p6	Ⅰ.概説(2)リスクベースアプローチ	…海外先進諸国の動向も踏まえ、…。 ←この記述は不要ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	外部委託有識者検討会の報告内容を受けて記載しておりましたが、ご意見を踏まえ、この記載は削除させていただきます。	要	済
*	103	p6	Ⅰ.概説(2)リスクベースアプローチ	…安全対策の優先順位等の合理的な意思決定に活用…。 は、 「…実施する安全対策の合理的な意思決定に活用…。」で良いのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり文章全体を修正させていただきました。 「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とともに、・・・」	要	済

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
*	104	p6	Ⅰ.概説(2)リスクベースアプローチ	「…金融機関等の経営資源が有限である点を踏まえ、安全対策に対する資源配分を経営資源全体の中で調整する考え方を言う。」は、 「…金融機関等の経営資源が有限である点を踏まえ、残るリスクを受容したうえで安全対策に対する資源配分を経営資源全体の中で調整する考え方を言う。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	No.105参照 「リスク特性の分析結果を安全対策の決定に活用する」としたうえで、「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考えに基づき」として、「安全対策に対する資源配分を調整する」として、ご意見を踏まえ、文章を見直させていただきました。 「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する考え方を言う。」	要	済
*	105	p6	Ⅰ.概説(2)リスクベースアプローチ	「つまり、限られた経営資源の中では、リスクゼロを追求することは合理的ではないという基本的な考え方を金融機関等の経営層が理解し、BCP 等の事後対策を手当てしたうえで、リスクを受容する判断も取りうることを意味する。」について、 BCP等事後対策を手当てすれば、リスクを受容することもありうると読める。基礎基準の趣旨とは矛盾するので、「つまり、限られた経営資源の中で最適な対策を講じ、残るリスクは受容するということを意味する。」で良いのではないか。 言葉足らずであれば、脚注に「ここで言う統制には、システム以外での統制やBCP等の事後対策等も含む」などと置けば良いのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	Np104を受け、文章の見直しをいたします。経営資源に関する説明は、安全対策の決定プロセスとして取込み、その結果発生する残存リスクに対しては、BCP等の対策を検討のうえ、最終的には「受容する」こともあり得るという内容としています。 つまり、限られた経営資源の中では、BCP等の事後対策を手当てしたうえで、リスクを受容する判断も取りうることを意味する。」	要	済
*	106	p7 p8 p9	Ⅰ.概説(3)基本原則 (参考「情報の機微性」) (脚注5)	「…個別金融機関等による統制可能な範囲を超えて外部に及ぶ場合(以下、「外部性を有する」という)や、機微情報(要配慮個人情報を含む)等の流出により、プライバシーなど個人の人権等が侵害される場合(以下、「機微性を有する」という)を考慮に入れるべきである。」について、 ・P9脚注5では「法人取引等に関する重要な機密情報を取り扱うシステム」を機微性を有するシステムと同等に扱うケースがあるとしている。 重要な機密情報の定義は各金融機関において違いがあるかもしれないが、金融機関等としてレピュテーションの観点などからも重要な機密情報であれば同等に扱うべきであり、P8「情報の機微性」においても明記すべきと思料。 ・P7の記述も人権等が侵害される場合に限定してあり、記述は工夫を要すると思料。	農林中央金庫 常岡様(専) 今嶋様(検)	「機微情報」は社会的にも高い安全対策を実施すべきものであるとしています。一方で、脚注にある法人取引などの重要な「機密情報」については、金融機関等から見れば、同等に扱うべきものと解されるため、金融機関等の判断に幅をもたせるために例示しております。しかしながら、機微情報と機密情報を同一と見なすと、金融機関等のシステムは、より高い安全対策に偏向することとなり、それを避けるためにもここを明確に区分しております。従って、原案のままとさせていただきたいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
*	107	p7	Ⅰ.概説(3)基本原則 (安全対策の基本原則)	「情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、適切な内容で決定されるべきである。」は、 「情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて決定されるべきである。」(「適切な内容で」をトル)としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	リスクベースアプローチの章において、「適切でない安全対策が実施されてしまう」とした部分と対になるものであり、原案のままとさせていただきたいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
*	108	p7	Ⅰ.概説(3)基本原則 (安全対策の基本原則)	「情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システムに係る予算内における新規開発等との調整のみならず、経営資源全体も視野に入れ、顧客の利便性向上や企業価値の最大化を目指して、決定されるべきである。」について、 経営資源配分は、リスク顕在化後の事後対策と比較衡量するものではなく、顕在化した場合のリスクそのものとの比較であるものと思料。	農林中央金庫 常岡様(専) 今嶋様(検)	経営資源(費用、人的資源など)を配分するにあたり、新規開発に係る費用と対になるのが、残存リスクが顕在化した場合の事後対策に係る費用等であり、比較の観点から「リスク」ではなく「リスク顕在化後の事後対策」という表現を用いております。従いまして、ここは原案のままとさせていただきたいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
*	109	p7	Ⅰ.概説(3)基本原則 (安全対策の基本原則)	「ただし、重大な外部性を有する情報システム及び機微性を有する情報システムにおいては、その社会的・公共的な観点から、このシステムの外部性や保有する情報の機微性を考慮に入れた安全対策の達成目標が設定されなければならない。」について、 「…その社会的・公共的な観点から、これらシステムが有するリスク特性を考慮に入れた安全対策の…。」(読みやすさのために重複する表現を除外)としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	「リスク特性」という表現では観点がやや曖昧となるため、ここは「外部性」または「機微性」を強調したいと考えております。従いまして、原案のままとさせていただきたいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
*	110	p8	Ⅰ.概説(3)基本原則 (参考「重大な外部性」)	「「外部性」には、当該金融機関等の顧客への影響は含まれない。なぜなら、これらの顧客に対しては、相手を個別に認識し個別に対処可能であり、損失額を内部的に算定できるからである。」について、 「外部性」を説明するうえで、2点目、3点目にてコストが算定出来るか出来ないかの違いのみで説明を展開しているが、これは、安全対策を決定するうえでコスト(費用対効果)のみで全てを判断する下地を作りかねず、賛同しがたい。 コストは極めて重要な要素ではあるが、例えば、レピュテーションのリスクはコストだけでは計れないものと思料。2点目、3点目の解説は不要と考える。	農林中央金庫 常岡様(専) 今嶋様(検)	「外部性」の持つ特徴を説明した部分となるため、説明自体は残すべきと考えております。しかしながら、「コスト」に限定した説明となると、ご意見にあるとおり「費用対効果」のみが論点となり、レピュテーションまで観点を広げることの妨げになる懸念もございます。このため、「影響・損失額等」を「把握する」という表現に変えたいと考えております。 「損失額を内部的に算定できるからである。」 ↓ 「影響や損失額等を内部的に把握できるからである。」	要	済

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
*	111	p9	Ⅰ.概説(4)ITガバナンス	「金融機関等の経営層は、情報システムのリスク特性を評価し、その評価された結果に基づき、新規投資等含め、投資効率の最大化を追求した経営資源配分を考慮したうえで、安全対策の目標を適切かつ包括的に決定する。」について、 1(1)「ITガバナンスとITマネジメント」では、P4にて「安全対策の達成目標の決定と同時に、達成目標を実現するために必要となる経営資源の投下を決定する。」これと整合性を欠いている。 また、「投資効率の最大化を追求した経営資源配分」という考え方は、全体を通じてこの文章にのみ出てくる。ここも「企業価値の最大化」といった表現の方が適切ではないかと思料。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、見直したいと考えております。 Ⅱ.1「安全対策決定ののプロセス」では、安全対策の目標を決定し(＝リスク評価の分析結果を踏まえ、必要な安全対策を選択する)、経営資源配分との調整を実施し(＝経営資源を投下しない対策について発生し得る残存リスクに対する対策(BCP、受容など)を検討する)、最終的に実施する安全対策を決定するとしており、これと整合的な内容となるよう見直しました。 p4「経営層は、安全対策の達成目標と、達成目標を実現するために必要となる経営資源の投下を決定する。」 p9「金融機関等の経営層は、情報システムのリスク特性を評価し、その評価された結果に基づき安全対策の目標を決定する。さらに、新規投資等含め、顧客の利便性向上や企業価値の最大化を追求した経営資源配分を考慮したうえで、実施する安全対策を決定する。」 「投資効率の最大化」については、ご意見を踏まえ修正いたしました。	要	済
*	112	p9	Ⅰ.概説(5)経営責任のあり方	「経営層においては、「ひとたび重大なシステム障害が発生した場合、その事実をもって、結果責任を追及されかねない立場にあることから、高い安全対策を求めない訳にはいかない」といった共通認識が存在することから、安全対策の基本原則の遵守に当たっては、そうした認識が阻害要因となることが危惧される。 わが国の将来の金融ビジネスにおける優位性を確保するためには、監督当局と金融機関等において、必ずしもリスクゼロを追求しないといったリスクベースアプローチの考え方を共通の認識とするとともに、リスクベースアプローチを実施した結果として、リスクが残存し、さらにそれが顕在化した場合においても、監督当局が金融機関等に対して、障害や事故が発生してリスクが顕在化したという結果だけをもってその責任を追及することは、リスクベースアプローチの考え方と整合的ではない、という認識まで含めて、共有されるべきものと考える。」について、 共有されるべき範囲には監督当局だけではなく、広くステークホルダーも含まれると思料します。	農林中央金庫 常岡様(専) 今嶋様(検)	当該箇所(経営責任の在り方全般通じ)は、外部委託有識者検討会において慎重な議論が尽くされ、策定された文章です。ただし、「認識を共有する範囲」については、再検討する必要があると考えております。すなわち、金融機関等の立場からすれば、ステークホルダーや社会全般においても認識が共有されることが重要であるため、この点を追加できないかどうか、検討させていただきたいと考えております。	要	未
*	113	p10	Ⅰ.概説(5)経営責任のあり方	「〇顧客の利便性向上や企業価値の最大化を目指した結果として、残るリスクについては、これを正当に認識したうえで、これに対応するために、その程度に応じて、コンティンジェンシープランを策定するとともに、環境変化に応じて見直すことが必要である。」は、 「…結果として、残存するリスクについては、これを認識・受容したうえで、これに対応するために必要に応じてコンティンジェンシープラン策定等の対策を実施するとともに、環境変化に応じて対策を見直していくことが必要である。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	リスクを「受容する」か、またはコンティンジェンシープランを策定し、対策を講ずるかは、その「程度に応じて」判断され、かつ「環境変化に応じて見直す」ものとしております。リスクは「受容する」ことが前提ではないため、当該箇所については原案のままとさせていただきたいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
*	114	p10	Ⅰ.概説(5)経営責任のあり方	「〇経営層が、諸法令を遵守するとともに、安全対策基準等の社会的に合意されたガイドライン(前述の安全対策における基本原則を含む)等を踏まえて、安全対策や残存リスクに対するコンティンジェンシープラン等を用意し、かつ、有事においては、これらを踏まえつつ臨機応変に対応している限りにおいては、客観的立場から見れば、法的責任を果たしているものと評価されるべきである。」は、 「…安全対策や残存リスクに対するコンティンジェンシープラン等を用意、適宜見直しをし、かつ、有事においては、これらを踏まえつつ臨機応変に対応している限りにおいては、経営責任は十分に果たしているとの立場をとる。なお、金融機関等は社会性・公共性を有していることから、これらの考え方は、ステークホルダーはもちろん、広く社会と共有していくべきである。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	外部委託有識者検討会において慎重に議論が尽くされ、策定された文章であるため、原則報告書原文のままで採用したいと考えておりますが、今一度表現方法等について検討することとします	要	未
*	115	p10	Ⅰ.概説(6)「統制」のあり方	「また、金融機関等において、外部委託への依存度が高まる中、安全対策基準は統制面での対策を拡充させていくことが求められる。」は、 「また、金融機関等において、外部委託やクラウド等外部サービス利用への依存度が高まる中、安全対策基準においては統制面での対策を整備していくことが求められる。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「外部委託やサービス利用への依存度が高まる」と修正いたしました。ただし、「統制面での対策」については、「拡充」のままとさせていただきたいと考えております。これは、報告書の提言を受け、再委託先に対する対策が補完されたことを意図し、考慮すべき点や、強化すべき点が増えつつあることをもって「拡充」という表現としています。	要	済

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
*	116	p11	Ⅰ.概説(6)「統制」のあり方	「また、委託業務が分割され複数の先に再委託され、さらに、再委託先からその先にも再委託が進めば、委託先を通じた「統制」の構造が複雑化し、「統制」の難易度は極めて高くなることが危惧される。 当然のことながら、金融機関等が、外部に対して、「統制」を全く行わないことは、社会的・公共的な観点から適当でないことは自明であるものの、金融機関等の内部に求められるものと同程度まで完全な「統制」を行うと、コスト削減や先進技術の利用を目指して行われる外部委託本来の目的が損なわれるおそれがある。」について、 ・「統制」の難易度は極めて高くなることへの危惧の表明だけで、これに対しての解が無い。少なくとも工夫していくといった下りは必要ではないか。 ・「当然のことながら…自明ではあるものの」までは自明とあるとおり不要と思料。 文章は「一方」で接続すれば良いと思料。 ・「完全な「統制」」という表現の「完全な」は意味が曖昧と思料。重要な外部性を持つシステムと同じレベルの統制という趣旨か、リスクベースアプローチに則り同じレベルの統制という趣旨か、直接統制するという趣旨か。 これまでも外部委託については、自社が行う場合と同等の統制がなされていることが前提であったものと理解。リスクベースアプローチに則り統制レベルを決めたうえで同じレベルの統制という建付けと理解。 ・コスト削減や先進技術利用列挙して「本来の目的が損なわれる」と記述すると統制レベルは下げるべきと読める。冒頭の難易度が高くなるの記述からの流れが余計に統制レベルは下がって良いと受け止められかねない。あくまでリスクベースアプローチでの整理が必要と思料。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり修正・見直しを行いたいと考えております。 ・「統制」の難易度が極めて高くなることに対し、「金融機関等においては、これらのリスクに対して外部の統制に関する対策を検討することが必要となる」としました。 ・自明な部分であり、削除しました。ただし、文章の繋がりから、接続詞は「さらに」を用いました。(最終的には「最適な統制」に繋がりますが、再委託による統制の複雑化と、統制の強度を内部と同程度にすることによる外部委託のメリットが減少する点は、並列の内容となるため) ・「完全な統制」はご意見にあるとおり、「内部と同程度の統制」を指すため、誤解を招かぬよう、「完全な」を削除しました。 ・前後の文章の繋がりから、この文章だけをもって「統制のレベルをさげるべき」という解釈にはならないと考えておりますが、「外部委託の目的が損なわれるおそれ」という表現は、ご意見の中にあるとおり、意図的な誘導と取られかねません。このため、「目的が損なわれる可能性について考慮する必要がある。」として、文意が一方的にならないよう表現を修正いたしました。	要	済
*	117	p11	Ⅰ.概説(6)「統制」のあり方	「したがって、金融機関等の社会的・公共的な観点や委託目的を総合的に勘案した結果として、委託先及び再委託先との接点において、最適な「統制」を決定することが重要であり、これは、リスクベースアプローチや「安全対策における経営責任の在り方」で示した内容と何ら異ならない。」について、 リスクベースアプローチであれば、リスク特性に応じて統制レベルも決めるということであり、「したがって、金融機関等の社会的・公共的な観点や委託目的を総合的に勘案した結果として、委託先及び再委託先との接点において、最適な「統制」を決定することが重要」という表現には違和感。 また、この文章の「委託先及び再委託先との接点」や「最適な」の意味は曖昧で分かりにくい。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、以下のとおり見直したいと考えております。 「したがって、委託する業務の内容や委託先の評価結果等を把握したうえで、そのリスク特性に応じた統制面での対策を決定することが重要であり、」	要	済
*	118	p11	Ⅰ.概説(6)「統制」のあり方	「なお、FinTech企業との契約形態には、外部委託とは性質の異なるものが存在する。金融機関等においては、金融関連サービスを提供するFinTech企業等によって運用される情報システムに対し、金融機関等に安全対策上の責務が生じる範囲において、適切な水準で外部の統制を行うことが必要となる。」は、 「…金融機関等に安全対策上の責務が生じる範囲において、適切な水準で外部の統制を行うことが必要となる。」については、「性質の異なるものが存在する」ので、やれることをやれば良いというように読める。 サービスの形態により、リスクベースアプローチに則り求める統制レベルを決めたとしても、上手く適合出来ない可能性があるが、残存リスクを見極めリスクを受容するということではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	金融関連サービスを提供するFintech企業等が運用するシステムに対しては、安全対策基準がそのまま適用されないことから、金融機関等は外部委託と同じ統制が行えないため、「責務が生じる範囲において」という表現を使用しています。従って、ここは原案のままとさせていただきたいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
*	119	p12	Ⅱ.フレームワーク(1)安対における定義	脚注9「9例えば、システム全体では、顧客情報が保有されているが、当該サブシステム内には顧客情報が保有されていない場合等が考えられる。」について、文脈からすると「顧客情報」ではなく、「機微情報」で表現すべきと思料。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「機微情報」に修正させていただきます。	要	済
*	120	p13	Ⅱ.フレームワーク(1)安対における定義	「安全対策基準を適用するに当たっては、経営層が適切なIT ガバナンスを発揮したうえで、個別金融機関等におけるリスク評価や、経営資源配分等の観点を考慮したうえで対象となるシステムを決定することが求められる。」は、 「経営層が適切なIT ガバナンスを発揮したうえで、個別金融機関等におけるリスク評価をもとにシステムを分類し、安全対策基準の適用していくこととなる。」としてはいかがか。 (経営資源配分等の観点は別問題と思料)	農林中央金庫 常岡様(専) 今嶋様(検)	ここでは「特定システムは、最終的には金融機関等が判断するものであり、一律に対象となるシステムと明示することができない」理由を示しており、経営資源配分については、あくまで特定システムとして安全対策を実施するか否かにおいて考慮すべき観点であることから、「安全対策を適用するにあたっては、」以降の文章については削除することとしました。	要	済

【資料４－３】
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

改訂案２（安全対策基準前説）

【資料４－３】
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

Ⅰ．概説

１．安全対策基準の意義

わが国の金融機関等のコンピュータシステムは、企業間・個人間におけるネットワーク化を前提とした新たな技術・サービスの急速な展開や、クラウド事業者、あるいはFinTech企業[1]と呼ばれる革新的な金融関連サービスを提供する事業者の出現に伴う関係者の拡大を反映し、新たな局面を迎えつつある。また、ITの進展等により、システムに障害が生じた場合の影響が広域化・深刻化するおそれがあること、顧客データや企業の重要なデータ等を侵害するサイバー攻撃をはじめとする犯罪が巧妙化・大規模化するおそれがあることなどから、安全対策には多くの経営資源が必要とされている。

こうした中、金融機関等が信用秩序を維持し、利用者が安心してサービスを享受するためには、十分な安全対策の実施が不可欠であるが、一方で、金融機関等が顧客の利便性や企業価値[2]を高めるために、限りある経営資源を、安全対策のみならず、新規開発等にも適切に配分していくことが重要となる。

金融機関等のコンピュータシステムの安全対策は、第一義的には、システムを用いて金融サービスを提供する金融機関等の経営判断に基づいて実施されるべきである。その上で、リスク[3]が顕在化した場合に社会的に重大な影響を及ぼすシステムと、それ以外のシステムにおいては、それぞれのリスク特性に応じた安全対策の目標を設定することが妥当と考えられる。そこで、『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、「本書」とする）では、金融機関等のよりどころとなる安全対策基準の適用において、リスクベースアプローチの考え方を取り入れ、現実的かつ効果的な安全対策の考え方を示すこととした。

また、システムに対する安全対策の実施主体が外部の委託先等にも拡大している中、FinTech 企業等との新たな関係や、重要な情報システムにクラウドサービスを用いた場合の安全対策の在り方を改めて考える必要がある。本書では、これらの金融機関の外部に対する統制の在り方を改めて示すとともに、金融機関内部の統制及び、これら統制のもとで実施する実務的な基準等との関係を示している。

本書は、公益財団法人 金融情報システムセンター（以下、「当センター」とする）内に設置された学識経験者、金融機関、保険会社、証券会社、クレジット会社及びコンピュータメーカー、クラウドサービス事業者、FinTech 企業等の専門的知識を有する安全対策専門委員及び、検討委員において審議・作成されたものである。

金融業務を営む業界の各社においては、本書が業務内容やその重要度に応じて実施すべき安全対策の指針となること、各社がコンピュータシステムの状況等に即し漸次実施しうる内容となっていること等を勘案し、各社が本書を参考にしながら適切な安全対策を実施することが期待される。

---

[1] 電子決済等代行業など、IT 技術を活用した革新的な金融に関連するサービスは、将来において更に多様化することが想定されるが、本書においては、金融機関等以外の事業者が上記のサービスを提供する場面を想定し、当該事業者を「FinTech 企業等」と表現している。

[2]「企業価値の最大化」には、ステークホルダーへの還元のみならず、相互扶助の精神から地域の繁栄等を実現するという目的もあり、多様な目的を含めて使用している。

[3] 本書では、金融機関等が情報システムの導入・利用等で実現しようとする経営目標の達成を阻害する不確実性及び、情報システムの障害等によって社会的な影響・損失を引き起こす不確実性をリスクとしている。

コメント [A1]: No.21、No.68

コメント [A2]: No.36

コメント [A3]: No.95

削除: ってく

削除: が含まれる

【資料４－３】
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

２．安全対策の考え方

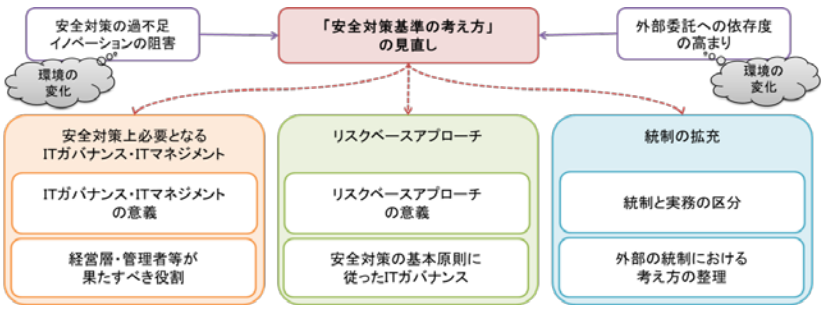
安全対策基準を取り巻く環境変化と対応

安全対策基準が作られた当初は、金融機関等の情報システムと言えば、基幹業務系のコンピュータシステムであった。そのため、安全対策基準の初版では、その適用対象とする情報システムを、「金融機関等のオンラインシステム」としていた。その後、IT の進展に伴い、金融機関等の情報システムは、情報系システム等その範囲が広がり、基幹業務系以外のシステムが大きなウエイトを占めるようになってきた。また、システム形態については、ホストコンピュータ中心からクライアントサーバなど分散処理型のシステムへの移行が進み、サービス利用についても、共同センターやクラウドサービス利用の増加、FinTech 企業等と連携した金融関連サービスの登場など、多様化してきている。

その過程で、安全対策基準は、基幹業務系システムの安全確保と安定運用という、当初の目的を果たしてきたものの、多様化する基幹業務系以外のシステムにおいては、適用の考え方が具体的に示されず、その結果、安全対策の程度に過不足が生じ、場合によっては、新規開発等への投資が抑制されるなど、経営資源が適切に配分されないといった懸念が生じている。また、金融機関等においては、システム開発・運用等における、外部委託への依存度が高まっているほか、クラウドサービスや FinTech 企業等と連携した金融関連サービスの利用が広がりをみせるなど、外部に対する統制の重要度が増すとともに、統制の在り方も多様化してきている。

そうした状況を受けて、当センターにおいて、「金融機関における外部委託に関する有識者検討会」が開催され、外部への統制の拡充のほか、リスクベースアプローチの考え方に従った IT ガバナンスなど、安全対策基準の抜本的な見直しを含む提言が行われた。さらに、つづく「金融機関における FinTech に関する有識者検討会」では、革新的な金融関連サービスが登場する中、金融機関等がシステムの安全性を確保しつつ、企業価値を高めることを目指して、安全対策の在り方について提言が行われた。

これらの有識者検討会の提言内容を踏まえ、以下では、安全対策の考え方・利用方法等について理解いただくことを目的に、安全対策上必要となる IT ガバナンス・IT マネジメントについて解説した上で、リスクベースアプローチに基づく安全対策の基本原則及び、統制の拡充についての考え方を示すこととする（[図表 1] を参照）。



［図表 1］安全対策基準を取り巻く環境変化と対応（概念図）

削除: 基幹業務系にとどまらず、
削除: や部門システム
コメント [A4]: No.96
削除: ある程度
削除: その形態や利用するサービスもホストコンピュータからクライアントサーバー、クラウドサービス
コメント [A5]: No.97
コメント [A6]: No.98
削除: 増している

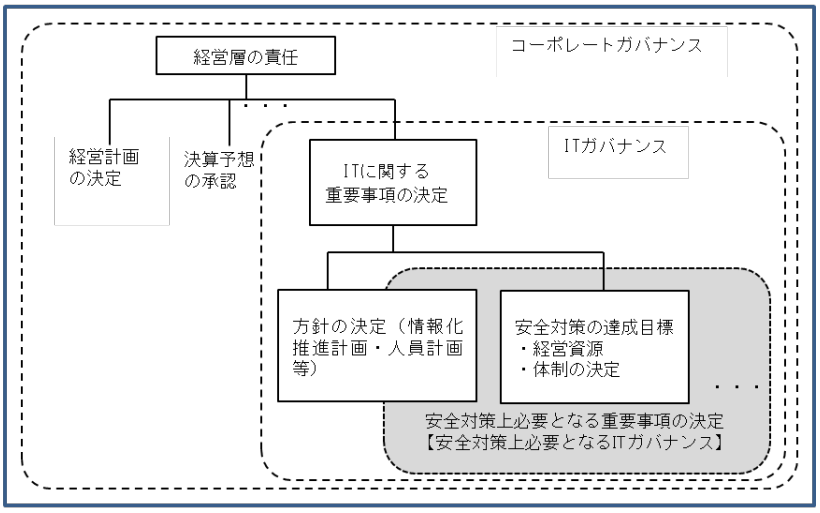
【資料４－３】
平成 29 年 10 月 17 日
公益財団法人 金融情報システムセンター

(1) IT ガバナンスと IT マネジメント

金融機関等の活動は情報システムに大きく依存しており、その安全・安定の確保は、金融機関等の重要な経営課題である。

① 安全対策上必要となる IT ガバナンスの意義

一般的に IT ガバナンスとは、コーポレートガバナンスの中で、特に IT に関する重要事項について経営層が意思決定を行うための仕組みのことをいう。そうした IT に関する重要事項の中でも特に情報システムに対するセキュリティ対策をはじめとした安全対策は、金融機関等の活動の根幹に関わるため、優先度高く取り扱われるべき事項である（［図表 2］を参照）。したがって、システム担当役員に限らず金融機関等の経営層は、安全対策上必要となる IT ガバナンスを機能させる責任を有する。



［図表 2］IT ガバナンスの階層構造

社会的使命を担う金融機関等において、経営層は、顧客や株主等のステークホルダーに対し責任を有しており、情報システムに対する安全対策の重要性を十分認識するとともに、その重要事項の決定を行い、情報システムの安全・安定の確保を推進していく（［図表 3］を参照）。

a. 中長期計画等における安全対策に係る重要事項の決定

(a) 安全対策に係る方針の決定

ⅰ. システム戦略方針の決定

経営層は、中長期計画（経営戦略・ビジネス戦略等）との整合性を踏まえたうえで、システム戦略方針を決定する。

ⅱ. システムリスク管理方針の決定

ⅲ．安全対策の達成目標の決定

経営層は、金融機関等として、リスク特性に応じ達成すべき安全対策の目標を決定する。また、その場合でも、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。

ⅳ．安全対策へ投下する経営資源の決定

経営層は、安全対策の達成目標の決定と、達成目標を実現するために必要となる経営資源の投下（費用・人材等の配分方針）を決定する。経営層は、経営資源が有限であることを踏まえて、あらかじめ、保有する経営資源を踏まえた達成目標を検討するとともに、リスク特性に応じた資源配分を決定することが重要である。

(b) 安全対策に携わる業務執行体制及びモニタリング体制の決定

ⅰ．安全対策に携わる業務執行体制の決定

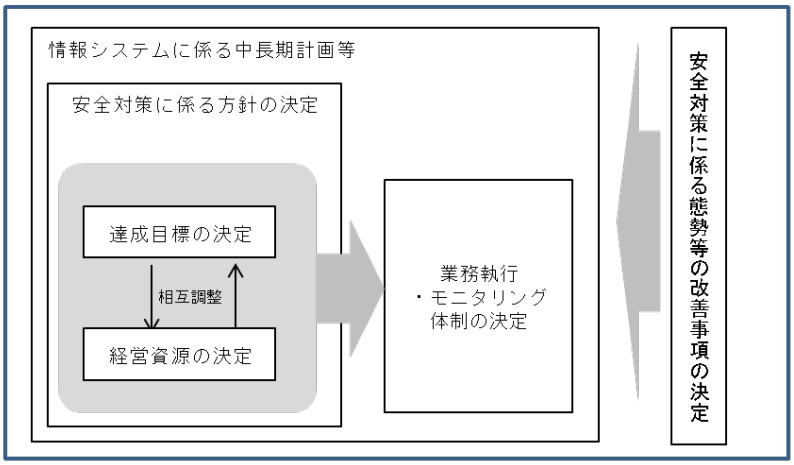
経営層は、安全対策の達成目標及び投下する経営資源の内容を踏まえ、必要に応じて、システム部門等の業務執行体制を決定する。

ⅱ．モニタリング体制の整備方針の決定

経営層は、安全対策の達成目標及び投下する経営資源の内容を踏まえ、必要に応じて、システム監査等のモニタリング体制の整備方針を決定する。

b. 安全対策に係る態勢等の改善事項の決定

経営層は、管理者（後述②1）を参照）からの報告やシステム監査報告等を通じて、みずからが決定した重要事項を踏まえて IT マネジメントが十分機能しているか検証したうえで、必要に応じて改善事項を決定し、安全対策に係る態勢等を継続的に改善していく。



［図表 3］経営層が決定すべき安全対策に係る重要事項

コメント [A7]: No.111

削除: 同時に

コメント [A8]: IT 人材の確保・育成に関する外部委託有識者検討会の提言をうけ追記した。

削除: 等

【資料４－３】
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

② 安全対策上必要となる IT マネジメント

IT マネジメントとは、経営層による IT ガバナンスのもとで、管理者が、情報システムの執行部門（システム担当・システムリスク管理担当等）に対して、IT に関する業務執行の管理等を行うことをいう。IT マネジメントにおいて、管理者等の関係者は以下の役割と責任を果たすことが求められる（［図表 4］を参照）。

a. 管理者

管理者は、経営層による IT ガバナンスのもとで、システム担当（部門）やシステムリスク管理担当（部門）等を統括し、安全対策上必要となる IT マネジメントを推進する。また、経営層に対しては、IT ガバナンスにおいて必要となる情報を、迅速かつ正確に提供する。

・内部規程・組織体制等の整備・見直し
・個々の情報システムに対する安全対策の決定
・安全対策上必要となる情報の経営層への報告

b. 経営企画担当（部門）

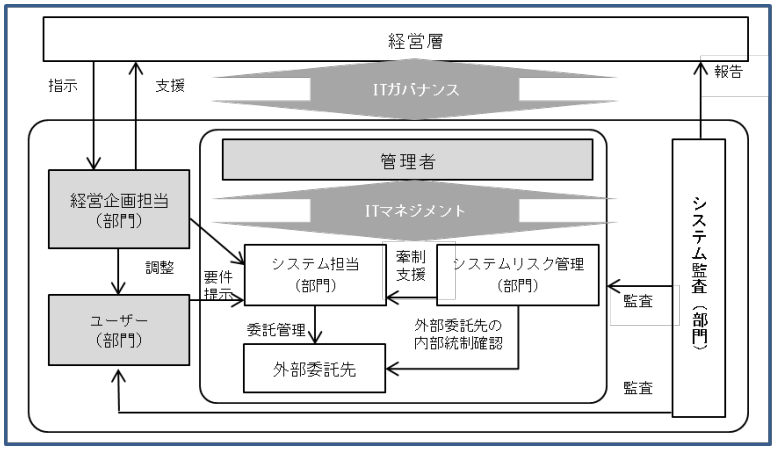
安全対策を含むシステム化事案の決定において、部門間の調整結果をもとに、必要に応じて経営資源投下に関する優先度を評価する等、経営層の意思決定をサポートする。

c. ユーザー（部門）

経営戦略実現のために、ビジネスモデル（商品・サービス・事務）等の企画に携わるとともに、管理者等に対してシステム化の有用性・経営戦略への目的適合性等の説明を行い、システム開発着手時には、システム担当に対して業務要件を提示する。

コメント [A9]: No.99

削除: 金融機関等の本社主管部署で、



［図表 4］情報システムの安全対策に携わる関係者（例）

【資料４－３】
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

(2) リスクベースアプローチ

① 安全対策基準を取り巻く環境の変化

これまでの安全対策基準では、「基幹業務のオンラインコンピュータ・システム」に適用する基準を明確化しているが、「基幹業務のオンラインコンピュータ・システム以外の情報システム」については、安全対策基準を「適宜取り入れる」あるいは「そのシステムによって提供されるサービスや扱う情報の重要性によって、個別に判断する」としてきた。

しかし、金融機関等を取り巻く環境変化の中で、大きな比率を占めるようになってきた基幹業務のオンラインコンピュータ・システム以外の情報システムについては、適用する安全対策の考え方が具体的に示されないまま、不確実性を含む環境となっているため、以下の状況が生じていることが危惧される。

- 「基幹業務のオンラインコンピュータ・システム以外の情報システム」に対する安全対策を「基幹業務のオンラインコンピュータ・システム」に設定されているのと一律に設定しておけば安心する、といった形式的で安全性に偏った選択を行ってしまう。
- 「安全対策基準の考え方」に、安全対策への経営資源配分や、安全対策と新規開発との経営資源配分の調整といった観点が示されていないことから、金融機関等の経営層の経営資源配分に係る決定プロセス等によっては、そのシステムのリスク特性と比較し適切ではない安全対策が最終的にそのまま実施されてしまう。
- 経営層の立場では、ひとたび重大なシステム障害が発生すれば、その事実だけをもって、直ちにその結果責任を追及されかねないといった懸念から、経営層は、システム障害を極力ゼロとするために、そのシステムにおいて適切な水準を超えた安全対策を承認する、あるいはみずから追求してしまう。

② リスクベースアプローチの意義

従来の安全対策基準が内包する上記の課題を解決するためには、一般的に「リスクベースアプローチ」と総称される考え方を取り入れることが有益である。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とともに、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する考え方を言う。つまり、限られた経営資源の中では、BCP 等の事後対策を手当てしたうえで、リスクを受容する判断も取りうることを意味する。

次に、こうした、リスクベースアプローチの考え方を導入する際には、「金融機関等がみずから」その安全対策の達成目標を決定することが前提となる。安全対策の達成目標を決定するためには、一義的には、金融機関等がシステムの安全性を確保しつつ、顧客の利便性向上や企業価値の最大化を目指し、IT ガバナンスが適切に発揮されることが重要となる。

コメント [A10]: No.100
削除: その他情報システム
コメント [A11]: No.101
削除: において
コメント [A12]: No.102
削除: 海外先進諸国の動向も踏まえ、
コメント [A13]: No.103
削除: 金融機関等の安全対策の決定にあたり、リスク特性を分析した結果を、安全対策の優先順位等の合理的な意思決定に活用するとともに、
削除: リスクゼロを追求することは合理的ではないという基本的な考え方を金融機関等の経営層が理解し、
コメント [A14]: No.104,105
削除: つまり、

(3) 安全対策における基本原則

金融機関等は、リスクベースアプローチの考え方に従い、IT ガバナンスを発揮しつつ、リスク特性を踏まえた安全対策を実施することが期待される。

ただし、金融機関等は、社会性・公共性を有していることから、リスクの顕在化による影響が、個別金融機関等による統制可能な範囲を超えて外部に及ぶ場合（以下、「外部性を有する」という）や、機微情報（要配慮個人情報を含む）等の流出により、プライバシーなど個人の人権等が侵害される場合（以下、「機微性を有する」という）を考慮に入れるべきである。

以上を踏まえて、金融機関等の情報システムに対する安全対策における基本原則を以下のとおり定めるとともに、本基本原則を安全対策基準の前提として位置付ける。

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

○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。
○情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、適切な内容で決定されるべきである。
○情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システムに係る予算内における新規開発等との調整のみならず、経営資源全体も視野に入れ、顧客の利便性向上や企業価値の最大化を目指して、決定されるべきである。
○ただし、重大な外部性を有する情報システム及び機微性を有する情報システムにおいては、その社会的・公共的な観点から、このシステムの外部性や保有する情報の機微性を考慮に入れた安全対策の達成目標が設定されなければならない。

基本原則では、金融機関等は、IT ガバナンスを適切に発揮し、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みずからが決定することができるとしている。

一方で、金融機関等の情報システムが、金融インフラの一部を構成している点を考慮し、重大な外部性や機微性を有するシステムについては、社会的・公共的な性質を持つことから、社会的に合意されたガイドライン等[4]を踏まえた「高い安全対策」が必要であるとしている。

[4] 監督当局の示すガイドラインや、業界団体等によって定められたガイドライン等を指す。本書に記載される安全対策基準も、金融機関等や関連するベンダー各社が定めるガイドラインとして、ここに含まれる。

【資料４－３】
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

（参考）「重大な外部性」の考え方

・まず「外部性」とは、例えば、個別金融機関等におけるシステム障害等によって、個別金融機関等のみならず、他の金融機関やその顧客に影響を与える可能性のある性質をいう。中でも、金融機関等における為替や預金を取り扱うシステムは、深刻なシステム障害が発生した場合、他の金融機関やその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「重大な外部性を有する」システムである。

・「外部性」には、当該金融機関等の顧客への影響は含まれない。なぜなら、これらの顧客に対しては、相手を個別に認識し個別に対処可能であり、影響や損失額等を内部的に把握できるからである。

・リスクベースアプローチに従って、適切に IT ガバナンスを発揮できる金融機関等であっても、「外部性を有する」情報システムに関する影響や損害額等を正確には把握できない。特に、「重大な外部性を有する」システムの障害等に伴う影響を正確に把握し、障害を防止するためのコスト等を事前に算定・内部化して、安全対策の立案に的確に反映させることは困難である。

・こうしたことから、金融機関等では「重大な外部性を有する」システムには、「高い安全対策」を適用することが必要となる。

・なお、金融機関等における決済システムのうち、一般的には為替や預金を取り扱うシステムは、「重大な外部性を有する」と解されるが、例えば ATM やインターネットバンキング等を、これらと同様のシステムとして取り扱うかどうかは各金融機関等の判断によるものと考えられる。各金融機関等は保有するシステムのリスク評価を通じ、「重大な外部性を有する」システムを特定することが必要となる。

（参考）「情報の機微性」の考え方

・個人情報については、個人情報保護法等の法的規制のフレームワークがあり、金融機関等がシステムの安全対策を行う際に、これらを遵守する必要がある。

・しかしながら、金融機関等が取り扱う個人情報は多種多様で、住所や氏名等の情報から、病歴を含む生活履歴等極めて機微にわたるものまである。こうした機微性を有する情報に関しては、一般の個人情報と区別せず取り扱うことは適当でない。

・なぜなら、「機微情報（要配慮個人情報を含む）」は、本人等の許諾なく流出した場合、経済的損失に留まらず、プライバシー等、個人の人権等の侵害といった広範かつ甚大な損失を被る可能性を有するからである。

・仮に、一般の個人情報と機微情報（要配慮個人情報を含む）が同一に扱われてしまった場合には、金融機関等のほとんどすべてのシステムに存在している個人情報が、この機微情報（要配慮個人情報を含む）に影響されて適切な水準を超えた安全対策目標が設定され、資源の過剰配分が行われるおそれがある。

・このような事態を避けるためには、個人情報を「機微情報（要配慮個人情報を含む）」と「その他の個人情報」に分け、「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。

コメント [A15]: No.110

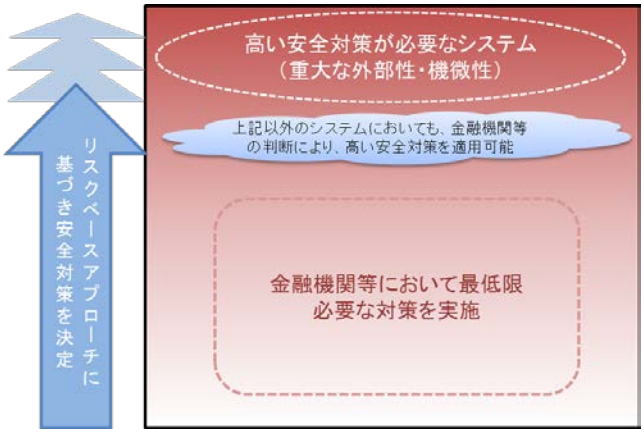
削除: 算定

【資料４－３】
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

(4) 基本原則に従った IT ガバナンス

金融機関等の経営層は、情報システムのリスク特性を踏まえた評価結果に基づき、安全対策の目標を決定する。さらに、新規投資等含め、顧客の利便性向上や企業価値の最大化を追求した経営資源配分を考慮したうえで、実施する安全対策を決定する。また、重大な外部性や機微性を有するシステムや、それらと同様の取扱いをする必要があると判断されるシステム[5]に対しては、「高い安全対策」を適用する。金融機関等の業務が情報システムに大きく依存している状況を踏まえ、経営資源配分の観点も含め、対象となるシステムを決定については、原則として経営層の判断が求められる。

「高い安全対策」が必要なシステム以外のシステムに対しては、金融機関等は、安全対策の達成目標を適切な水準で決定することとなるが、顧客データの漏えい防止等、金融機関等のシステムが満たすべき最低限の対策は、多くのシステムに共通すると考えられる。そこで、最低限の対策を予め設定することは、金融機関等が、リスクベースアプローチの考え方に基づき安全対策を決定する際、その不確実性を低減することに繋がると期待される（[図表 5]を参照）。



[図表 5] 基本原則に従った安全対策の考え方

(5) 安全対策における経営責任の在り方

経営層においては、「ひとたび重大なシステム障害が発生した場合、その事実をもって、結果責任を追及されかねない立場にあることから、高い安全対策を求めない訳にはいかない」といった共通認識が存在することから、安全対策の基本原則の遵守に当たっては、そうした認識が阻害要因となることが危惧される。

わが国の将来の金融ビジネスにおける優位性を確保するためには、監督当局を含むステークホルダーと金融機関等において、必ずしもリスクゼロを追求しないといったリスクベースアプローチの考え方を共通の認識とするとともに、リスクベースアプローチを実施した結果

削除: 適切かつ包括的に
削除: この際
削除: 投資効率の最大化
コメント [A16]: No.111
削除: する
削除: と
コメント [A17]: No.112（暫定）
対応方法について要検討

[5] 例えば、法人取引等に関する重要な機密情報を取り扱うシステムなどは、機微性を有するシステムと同等に扱うケースが想定される。

としてリスクが残存し、さらにそれが顕在化した場合においても、監督当局を含むステークホルダーが金融機関等に対して、障害や事故が発生してリスクが顕在化したという結果だけをもってその責任を追及することは、リスクベースアプローチの考え方と整合的ではない、という認識まで含めて、共有されるべきものと考える。

以上の考え方を踏まえて、安全対策における経営責任の在り方を以下のとおり示す。

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在り方

○経営層の使命は、顧客の利便性向上や企業価値の最大化であり、このことは、必ずしもリスクゼロを目指した安全対策の追求を意味するものではない。
○顧客の利便性向上や企業価値の最大化を目指した結果として、残るリスクについては、これを正当に認識したうえで、これに対応するために、その程度に応じて、コンティンジェンシープランを策定するとともに、環境変化に応じて見直すことが必要である。
○経営層が、諸法令を遵守するとともに、安全対策基準等の社会的に合意されたガイドライン（前述の安全対策における基本原則を含む）等を踏まえて、安全対策や残存リスクに対するコンティンジェンシープラン等を用意し、かつ、有事においては、これらを踏まえつつ臨機応変に対応している限りにおいては、客観的立場から見れば、法的責任を果たしているものと評価されるべきである。

(6) 安全対策基準における「統制」の在り方

「統制」とは、IT ガバナンスや IT マネジメントを行うための管理体制の整備のことを言う。金融機関等における経営層は、基本原則に従って IT ガバナンスを発揮していくことが求められる。また、金融機関等において、外部委託やサービス利用への依存度が高まる中、安全対策基準は統制面での対策を拡充させていくことが求められる。これらの課題を解決していくには、安全対策基準において、統制面の対策を明示的に示すことが有効である。

コメント [A18]: No.115

① 「統制」と「実務」の区分

IT ガバナンス及び IT マネジメントを適切かつ効果的に発揮していくためには、経営層が、既存の考え方に縛られることなく、多様で主体的な創意工夫を発揮し、安全対策における、統制と実務の適切なバランスを確保することが望ましい。

そこで、安全対策基準では、「統制」に関する基準と、「実務」に関する基準を明確に分離し、さらに、統制に関連した基準を自組織内に対する「内部の統制」と、外部委託管理等を通じて外部（委託先等の他組織）への統制を発揮していくための基準である「外部の統制」に分けている。一方、「実務」に関する基準は、新たなテクノロジーの出現等により、常に変化していく部分であり、IT マネジメントを具体的に実行するための基準として、対象とするシステムや、各局面等に応じたリスク管理策を設けている（［図表 6］を参照）。

区分		基準の内容
統制	内部（自組織内）の統制	金融機関等において、セキュリティポリシーの策定や、教育・訓練を含む、管理体制等を整備するために実施する対策
	外部（委託先等の他組織）の統制	契約締結や業務管理など、外部へ委託するうえで実施する対策
実　務		管理者がリスクの管理対象やリスクの程度に応じて、具体的に実施する対策

［図表 6］「統制」と「実務」の区分

② 外部に対する「統制」の在り方

金融機関等においては、外部委託やサービスの利用が拡大しており、外部に対する「統制」の重要性が増している。

内部に対する統制に対し、外部に対しては、一般的には「統制」が及びにくくなるといった特性があり、再委託においては、そうした特性がいっそう顕著となるものと考えられる。また、委託業務が分割され複数の先に再委託され、さらに、再委託先からその先にも再委託が進めば、委託先を通じた「統制」の構造が複雑化し、「統制」の難易度は極めて高くなることが危惧されることから、金融機関等においては、これらのリスクに対して外部の統制に関する対策を検討することが必要となる。

さらに、委託先に対し、金融機関等の内部に求められるものと同程度に「統制」を行うことで、コスト削減や先進技術の利用を目指して行われる外部委託本来の目的が損なわれる可能性について考慮する必要がある。したがって、委託する業務の内容や委託先の評価結果等を把握したうえで、そのリスク特性に応じた統制面での対策を決定することが重要であり、これは、リスクベースアプローチや「安全対策における経営責任の在り方」で示した内容と何ら異ならない。すなわち、金融機関等においては、顧客の利便性向上や企業価値の最大化を目指して経営資源配分と最適な安全対策が決定され、残存リスクに対し適切に対応されている限りにおいては、その責任は果たされていると解される。

金融機関等と委託先との間では、統制と実務において、各々が果たすべき役割（以下、責務という）が存在[6]し、安全対策の達成目標は、これら責務の分担と各々の責務の確実な遂行によって実現される。なお、FinTech企業等との契約形態には、外部委託とは性質の異なるものが存在する[7]。金融機関等においては、金融関連サービスを提供するFinTech企業等によって運用される情報システムに対し、金融機関等に安全対策上の責務が生じる範囲において、適切な水準で外部の統制を行うことが必要となる。

コメント [A19]: No.116

削除: 当然のことながら、金融機関等が、外部に対して、「統制」を全く行わないことは、社会的・公共的な観点から適当でないことは自明であるものの

削除: まで完全な

コメント [A20]: No.116

削除: おそれがある

コメント [A21]: No.117

削除: 金融機関等の社会的・公共的な観点や委託目的を総合的に勘案した結果として、委託先及び再委託先との接点において、最適な「統制」を決定することが重要であり、

[6] 一般には、金融機関等において、委託先に対する「統制」の責務が発生することになるが、委託先が再委託先を管理するための「統制」についても考慮する必要がある。

[7] FinTech 企業等が金融関連サービスを提供するシステムを運用し、金融機関等との接続を行う場合、運用主体である FinTech 企業等と、接続される金融機関との間には外部委託とは異なる性質の契約関係が存在し、金融機関等は、FinTech 企業等に対して外部委託先に対する統制をそのまま適用できない場合を考慮する必要がある。

【資料４－３】
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

Ⅱ．フレームワーク

１．総論

ここでは、安全対策基準の考え方を踏まえ、リスクベースアプローチの考え方に基づき安全対策基準を具体的に適用していくにあたり、対象システムや、基準の構成、分類、適用対象など、安全対策の決定に必要な定義やプロセスを示す。

(1) 安全対策基準における定義

① 金融情報システム

金融機関等が、業法等に基づき、顧客に商品・サービスを提供するために利用する情報システムを、「金融情報システム」と定義する。

② 特定システム・通常システム

金融情報システムのうち、重大な外部性を有するシステム（システム障害等が発生した場合の社会的な影響が大きく、個別金融機関等では影響をコントロールできない可能性があるシステム）や、機微情報（要配慮個人情報を含む）を有するシステム（機微情報（要配慮個人情報を含む）の漏えい等により顧客に広範な損失を与える可能性があるシステム）を、「特定システム」と定義する[8]。「特定システム」には、「高い安全対策」を適用する必要がある。

特定システム以外の金融情報システムを、「通常システム」と定義する。通常システムにおいては、そのリスク特性に応じた安全対策を適用することが可能である。

なお、特定システムの一部を、サブシステムとして独立して管理することが可能であり、かつ当該サブシステムにおいて発生したリスク事象がシステム全体へ影響を及ぼすことを防止できる場合や、当該サブシステムが停止する等の障害が発生した際、業務停止を回避するための代替策が可能な場合には、当該サブシステムを特定システムから切り離し、「通常システム」として安全対策を適用することが可能である[9]。

コメント [A22]: No.119

[8] 安全対策基準における「特定システム」とは、必ずしも監督当局等への報告対象となるシステムを指すものではない。「特定システム」は、あくまでその社会的影響を考慮して個別金融機関等が設定すべきものである点を補足しておく。

[9] 例えば、システム全体では、機微情報が保有されているが、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等が考えられる。

削除: 顧客

削除: 顧客

【資料４－３】
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

（参考）金融機関等における特定システムと通常システムの分類
個別金融機関等におけるシステムの分類は、業態ごと[10]、または個別金融機関等における取扱い業務の重要度の位置付けによって様々であり、それらを一律に特定し、列挙することは難しいため、どのシステムが「通常システム」または「特定システム」に分類されるかは、個別金融機関等が実態に則して判断することとなる。

コメント [A23]: No.120

削除: 安全対策基準を適用するにあたっては、経営層が適切なITガバナンスを発揮したうえで、個別金融機関等におけるリスク評価や、経営資源配分等の観点を考慮したうえで、対象となるシステムを決定することが求められる。

③ 安全対策基準の構成
安全対策基準は、その目的や利用場面に応じて体系化しており、「統制基準」「実務基準」「設備基準」「監査基準」の４編で構成される（[図表 7] を参照）。

a. 統制基準
IT ガバナンスや IT マネジメントを行ううえで必要な管理体制の整備のための「内部の統制」及び「外部の統制」に関する基準・解説等から構成される。内部の統制は、社内体制の整備や、方針の策定、人材育成・訓練等に関する対策を記載している。外部の統制は、契約手続きや委託先の業務管理等、金融情報システムを外部へ委託するうえで必要となる対策を記載している（詳細は「２．統制」を参照）。

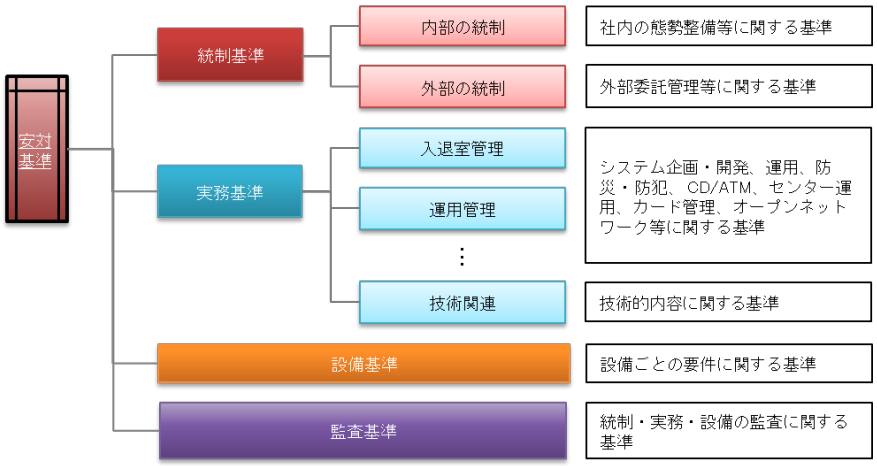
b. 実務基準
金融情報システムの信頼性・安全性の向上を図るために必要となる、システム企画・開発、運用、防災・防犯等に関する実務的な対策に関する基準・解説等から構成される。実務基準には、オペレーション等、管理者や作業者等が主体となる対策と、関連する技術的対策が含まれる。
なお、技術の進展が著しい環境下においては、その対策を字義通りに適用することが適当ではない場合があり、最新の技術動向等を踏まえ、金融機関等において適用の可否を判断されるべきものが含まれることに留意する必要がある。

c. 設備基準
コンピュータシステムが収容される建物や設備を自然災害、不正行為等から守るための対策に関する基準・解説等から構成される。
コンピュータセンターの建物・付帯施設及び設備、本部・営業店等の建物・付帯施設及び設備、流通・小売店舗等と提携してサービスを提供する場合の建物・付帯施設及び設備に関する対策を記述する。

10 一般に、預金取扱金融機関における為替システム、預金システム等は、重大な外部性を有すると想定され、生命保険会社等における、給付金査定等を行うシステムは、機微性を有すると想定される（Ⅰ.2.(3)「安全対策における基本原則（参考）」を参照）。証券会社におけるトレーディングシステムや、インターネットバンキングを主なチャネルとする預金取扱金融機関におけるインターネットバンキングシステムなどは、特定システムと同等に扱うことが考えられる。一方で、類似のシステムを有する金融機関等においても、そのシステム構成や、利用形態を鑑み、特定システムと判断しないことも考えられる。

d. 監査基準

統制、実務及び設備に対する監査を行ううえで必要となる、監査体制の整備や手順について記載している。



［図表 7］安全対策基準の構成

(2) 基準の分類

本書では、金融機関等がリスク特性に応じた安全対策の目標を設定するにあたり、不確実性を低減させることを目的に、「基礎基準」を設定している。一方で、「基礎基準」以外の基準は、リスク特性に応じて追加・選択する「付加基準」としている。なお、「設備基準」については、収納するコンピュータシステムに求められる基準を一意に定めることが困難であることから、「基礎基準」及び「付加基準」を区分していない。

移動（挿入）[1]

「基礎基準」は、特定システム、通常システムによらず、金融情報システムが最低限適用する基準として、以下の考え方に基づき設定している。

全てのシステムにおいて安全対策を決定、実施していくためには、セキュリティポリシーや、外部委託に関する方針等が整備され、必要な人員が確保・教育されるなど、ITガバナンスが適切に発揮されていることが必要である。このため、まず内部及び外部の統制並びに監査に関する基準を「基礎基準」としている。

また、一般に金融情報システムは、商品・サービスを顧客に提供するため、顧客データを保有または、顧客データに接続していると想定されることから、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ついても「基礎基準」としている。顧客データには、個人データ以外の重要なデータ[11]が含まれる場合があるが、この場合も顧客データ漏えい防止に関する基準が有効と考えられる。

なお、近年において重要性が増しているサイバー攻撃対策に関する基準も、顧客データの漏えい防止に関する基準に含めている。

削除: また

[11] 企業の公開前決算情報など、金融機関等において高い機密性が求められる情報を指す。

また、リスクベースアプローチの考えでは、必ずしもリスクゼロを追求しないことから残存リスクへの対応を考慮する必要がある。このため、コンティンジェンシープラン策定に関する基準についても、「基礎基準」としている。

さらに、システムの安定運用を実現するために必要な基準についても、これを「基礎基準」としている。

ただし、個別の業務またはサービス等において実施する基準[12]については、全ての金融情報システムにおいて適用されないことから、これらは基礎基準としていない。

「基礎基準」の選定にあたっての考え方

○統制・監査に関する基準
○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
○コンティンジェンシープラン策定に関する基準
○システムの運行管理に最低限必要な基準

上記以外の観点で必要となる基準については、各金融機関等が、システム構成やリスク評価の結果等を考慮のうえ、適宜、必要に応じて選択する「付加基準」となる。例えば、通常システムにおいて高い可用性が求められる場合は、可用性を確保するための安全対策の目標を定め、「付加基準」の中から適宜、必要な基準を選択・追加することで、安全対策の水準を高めることとなる。

次に、「基礎基準」の「解説部分」において、全ての金融情報システムに適用されるべき最低限必要な対策を「必須対策」[13]と呼ぶ。具体的には、「必要である」と 記載されている対策を「必須対策」とする。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする（「Ⅲ.本書の利用にあたって 3.本書の記述仕様」を参照）。

「付加基準」の「解説部分」の中で、当該基準を適用する場合に必須となる対策 を「付加基準」の「必須対策」[13]と呼ぶ。具体的には、「必要である」と記載されて いる対策を「必須対策」とする(特定システムでは、「付加基準」の「必須対策」は、必ず適用されることとなる)。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする。

この結果、特定システム、通常システムへの基準の適用方法は、[図表 8]のとおりとなる。

[12] インストアブランチ、コンビニ ATM、インターネットの利用や、外部の統制におけるクラウドサービスの利用、共同センター、金融機関相互のシステム・ネットワークに関する基準など。

[13] システム構成等の観点から適用する必要がない、あるいは適用できない場合には、「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。また、「必須対策」には、「重要度を勘案し、個人データ等を扱うシステムの場合等には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。

コメント [A24]: 個別の業務・サービスに関する補足事項を追加

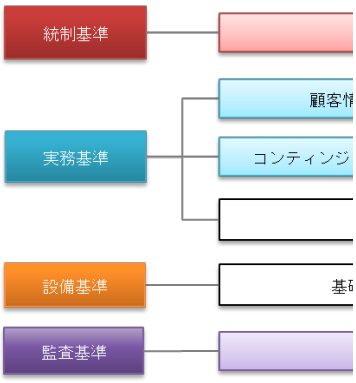
上へ移動 [1]: なお、「設備基準」については、収納するコンピュータシステムに求められる基準を一意に定めることが困難であることから、「基礎基準」及び「付加基準」を区分していない。

削除: .

.

安全対策基準の構成において体系化した統制基準、実務基準、設備基準ならびに監査基準と、基礎基準、付加基準の関係は以下のとおりとなる（[図表 8]を参照）。

.



［図表 8］基礎基準と付加基準の関係 .

改ページ

.

コメント [A25]: 「必須対策」の考え方を整理し、反映した。

削除: 「基礎基準」は、特定システム、通常システムによらず、金融情報システムにおける最低限の基準として設定しているが、システム構成や、リスク特性の観点から全てが適用されないことを考慮し、「原則として適用」としている

【資料４－３】
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

	基礎基準		付加基準	
	必須対策	その他の対策	必須対策	その他の対策
特定システム	○	△	○	△
通常システム	○	△	△	△

・「○」は、適用。
・「△」は、選択的に適用。

［図表 8］特定システム、通常システムへの基準の適用方法

(3) 安全対策基準の適用対象

安全対策基準は金融情報システムに適用される。共同センター等[15]、金融機関等が統制を行うシステムは、外部委託と同等の性質を有するものとして、必要となる安全対策を設定する。なお、金融機関相互のシステム・ネットワーク等[16]は、金融機関等が共同して運営するものであり、個別金融機関等が負う管理責任が部分的となるシステムとして区分している。これらは、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を設定する。

金融機関等における、金融情報システム以外のシステムについては、安全対策基準の適用対象外であるが、その技術基盤（セグメント等）の共通性や、金融情報システムとのリスク特性の類似性がある場合は、必要となる対策を適宜取り入れることとする。

金融機関等以外の事業者が金融機関等の外部委託先として金融関連サービスを提供する場合、金融機関等による外部の統制を受けることとなり、当該金融関連サービスを提供する情報システムは、結果として安全対策基準の適用対象となる（[図表 9]を参照）。

一方で、金融機関等以外の事業者が金融機関等の外部委託先とはならず、主導的に金融関連サービスを提供する場合、金融機関等による外部の統制が及ばないか、または部分的となることが考えられる。金融機関等による外部の統制が及ばない場合は、当該金融関連サービスを提供する情報システムは、安全対策基準の適用外となる[17]。また、金融機関等における外部の統制が部分的となる場合、当該金融関連サービスを提供する情報システムは、金融機

[15] 金融機関等がベンダーと契約するものや、運営組織等を通じてベンダーと契約するものなどが含まれる。
[16] 全銀ネット、CAFIS、統合 ATM、協同組織金融機関為替中継システム、SWIFT、LINC、損保ネット等は外部のシステムと定義している。その他、日銀ネット、でんさいネット、ほふりシステム、証券取引所システム等も、ここに分類される。
[17] 金融機関等以外の事業者においては、各業界等で定める基準・ガイドライン等に従うことが想定されるものの、その際、金融機関等が最低限満たすべき「基礎基準」を踏まえた安全対策が選択・運用されることが期待される。例えば金融関連サービスの利用（API 接続等含む）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。

削除: 通常システムでは原則として「基礎基準」を適用するとともに、リスク特性を踏まえ、「付加基準」から必要な基準を選択・追加する。特定システムでは、「基礎基準」及び、「付加基準」を原則として適用[14]（[図表 9]を参照、詳細は、(4)安全対策決定のプロセスを参照）。

削除:

削除: 9

削除: 基礎基準と付加基準

コメント [A26]: No.26

削除: 10

コメント [A27]: No.78

関等に責務が生じる範囲において、結果として安全対策基準が部分的に適用対象[18]となる。

［図表 9］金融関連サービスにおける安全対策基準適用の考え方

削除: 10

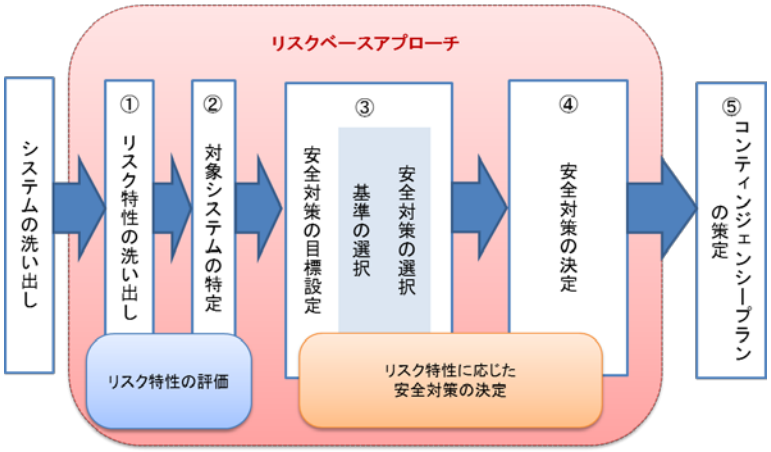
[18] 金融関連サービスにおいて、金融機関等に安全対策上の部分的な責任が生じる場合、金融機関等は金融機関等以外の事業者に対し、その責任が生じる範囲において有効な安全対策が実施され、その効果が発揮されていることを検証していくこととなり、これを外部委託基準の「準用」と呼んでいる。例えば、預金取扱金融機関における勘定系システムに対し、オープン API 等による接続が行われる場合は、当該システムはインターネットバンキングに類似するリスク特性を有していると解され、金融機関等は、FinTech 企業等に対し、「データの保全」や「本人認証」に係る安全対策の実施状況や、その効果について検証を行うこととなる。

【資料４－３】
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

(4) 安全対策決定のプロセス

リスクベースアプローチでは、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。金融機関等は、安全対策基準の適用対象となる各システムのリスク特性を洗い出し、対象システムを特定した後、安全対策の目標を定め、必要となる基準及び安全対策の選択を行う。安全対策の目標に対し、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、最終的に安全対策を決定していく。その結果、残存するリスクを踏まえ、必要に応じてコンティンジェンシープランを策定する（[図表 10]を参照）。

削除: 11



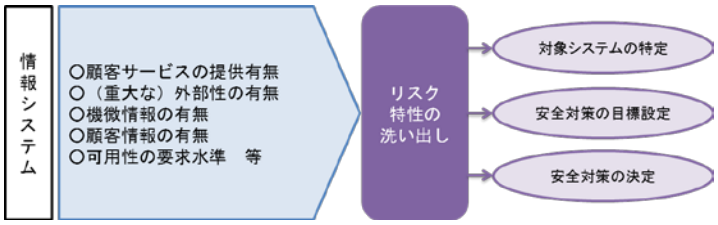
［図表 10］安全対策決定のプロセス

削除: 11

① リスク特性の洗い出し

金融機関等は、利用する金融情報システムを洗い出した後、リスク特性の評価[19]に必要となる、各システムのリスク特性の洗い出しを行う。リスク特性の洗い出しは、まず、金融サービスを顧客に提供するものかどうか、(重大な) 外部性、機微情報、顧客情報の有無、可用性の要求水準等の観点に基づき行っていく（[図表 11]を参照）。

削除: 12



［図表 11］リスク特性の評価

削除: 12

19 リスク評価の手法については、当センター発行の『金融機関等のシステムリスク管理入門』などを参考に、各金融機関等の実態を考慮のうえ、各金融機関等において有効な方法が選択されることを想定しており、本書では具体的な手法については示していない。

② 対象システムの特定

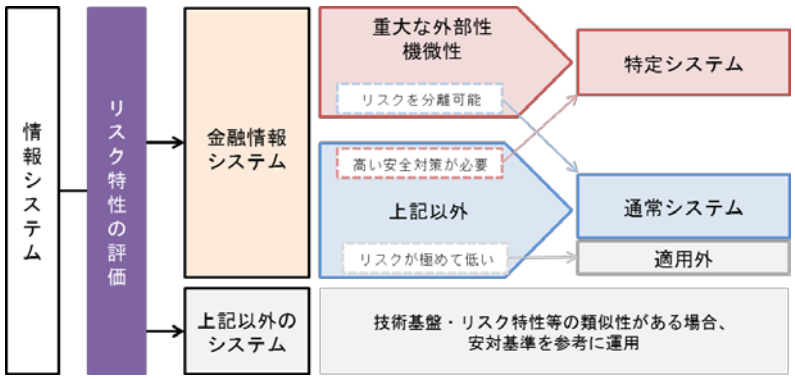
洗い出されたリスク特性を評価し、利用する金融情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。金融情報システム以外のシステムについては、その技術基盤やリスク特性に類似性がある場合、安全対策基準を適宜取り入れることとする。

次に、金融情報システムを、重大な外部性または機微情報を有する特定システムと、それ以外の通常システムに区分する。この際、各金融機関等の判断により、通常システムの中から、高い安全対策が必要なシステムを独自に選択することも可能である。一方で、特定システムの一部において、リスクが低いと判断されるサブシステムは、リスク管理上、当該サブシステムを分離することが可能な場合、これを通常システムとして取り扱うことも可能である（1.(1)②「特定システム・通常システム」を参照）。

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、顧客データを保有しないシステムなど、リスクが極めて低いと判断される場合は、安全対策基準の適用対象外とすることも可能である（[図表 12]を参照）。

削除: 13

金融機関等においては、システムの区分を更に細分化する等の方法も考えられるため、金融機関等のセキュリティポリシー等を踏まえた創意工夫によって、よりリスクベースアプローチの考えを反映した方法とすることも可能である。



［図表 12］対象システムの特定

削除: 13

金融機関等を取り巻く環境変化等により、保有するリスクの種類や程度は変動していくことが想定される。このため、金融機関等では、リスク特性の洗い出し及びリスク特性の評価を定期的に実施するとともに、適宜、対象システムの特定の結果を見直すことが必要となる。

③ 安全対策の目標設定（基準の選択・安全対策の選択）

対象システムを特定した後、個々のシステムのリスク特性の評価結果に応じ、安全対策の目標を設定する。個々のシステムに対する安全対策の目標設定では、例えば、保有するデータの種類や稼働率など、システムのリスク特性に応じて、選択した基準からどの対策

を実施すべきかを選択していくことが考えられる。適切な目標を設定するためには、例えば、リスク事象ごとに定められた障害発生件数の抑制など、目標設定の方針が定められていることが必要である。目標設定の方針は、システムリスク管理方針や、セキュリティポリシー、経営資源配分等の観点を踏まえ、経営層の関与のもと決定されることとなる。

IT マネジメントを担う管理者等は、設定された安全対策の目標を達成するために、必要となる基準及び対策を選択する。

特定システムにおいては、原則として、基礎基準に示された対策及び付加基準に示された対策の中から必要な対策を選択する。

通常システムは、原則として、基礎基準に示された対策を選択した後、個々のシステムのリスク特性等を考慮のうえ、必要に応じ付加基準を追加していく。

なお、システム構成等の観点から適用する必要がない、あるいは適用できない場合には、「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。

また、「必須対策」には、重要度を勘案し、「個人データ等を扱うシステムの場合等には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意が必要である（「1.(2)基準の分類」を参照）。

コメント [A28]: 「必須対策」における例外について、考え方を反映した。

④ 安全対策の決定

安全対策を選択した後、経営資源配分の観点等を踏まえ、最終的な安全対策を決定する。安全対策の決定においては、安全対策を実施した場合とリスクを受容した場合における費用等を比較衡量のうえ、安全対策の選択を見直すことも可能である。また、リスク特性や経営資源配分の観点から、安全対策の実施時期や、安全対策の程度[20]についても検討し、セキュリティ上の大きな脆弱性を残さないよう、安全対策を決定していく。

⑤ コンティンジェンシープランの策定

安全対策の決定の結果、残存するリスクを踏まえ、必要に応じてコンティンジェンシープランを策定し、適切にリスクに対応できる態勢を整備しておくことが必要となる。

コンティンジェンシープランとは、金融機関等のコンピュータセンター、営業店、本部機構等が、不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務を復旧するために、あらかじめ策定された「緊急時対応計画」のことである。

残存リスクに対するコンティンジェンシープランの策定は、金融機関等が策定する必要最低限の安全対策と位置付けている。ただし、リスク自体を単純に受容できるなど、コンティジェンシープランを策定する必要がない場合もあるため、残存リスクの特性に応じて、適切に策定されることが必要である。

20 安全対策を実現する技術や手法について、難易度や品質の程度を決定することを指す。例えば、本人確認において、生体認証方式や、ワンタイムパスワードを採用するなど、リスク特性に応じてより高度で優れた技術を採用する場合などが考えられる。

また、近年、自然災害以外の脅威として、サイバー攻撃や感染症のパンデミック等についても体制の整備や要員の確保の観点から考慮することが必要となっている。

コンティンジェンシープランの目的は、従来から推進されている安全対策の積み重ねを前提に、これらの対策では防ぐことのできなかった緊急事態に際して、可能な限り影響を軽減し、早期に業務を復旧させることにある。

影響範囲が限定された障害等の発生については、あらかじめ計画された回復措置等により、処置できるケースが多く、安全対策基準の「障害時・災害時対応策」の中でその対応手順を述べている。しかし広域災害のような、影響が広範囲にわたり金融機関等として統一された行動計画による対応が必要となる場合には、システム部門内にとどまらず、全社的にまとめられた、事前に十分に準備された計画が不可欠となる。

このための緊急時対応計画として、コンティンジェンシープランを事前に策定しておくことが必要であり、コンティンジェンシープラン構築の必要性を安全対策基準の中で記述し、金融機関等が実施すべき最低限の安全対策の一つと位置づけている。

コンティンジェンシープランの詳細については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照されたい。

【資料４－３】
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

２．統制

金融機関等においては、安全対策を決定するうえで、基本原則に従った IT ガバナンスを発揮することが前提となる。このため、これら統制に関する基準は「基礎基準」としている。統制には「内部の統制」と「外部の統制」があり、両者は「統制」の対象や統制の方法が異なる。ここでは、これら「統制」の内容と、ルールの導出に至る考え方について解説する。

(1) 内部の統制

安全対策基準上の「内部の統制」とは、金融機関等が、安全対策を策定・推進していくために自組織内で実施すべき対策を指す。具体的には、セキュリティポリシーの策定、規程等の整備、セキュリティ管理体制等の組織の整備、要員の教育・管理、訓練等を指す。

安全対策基準上は、内部の統制を、以下のカテゴリーに分類している。

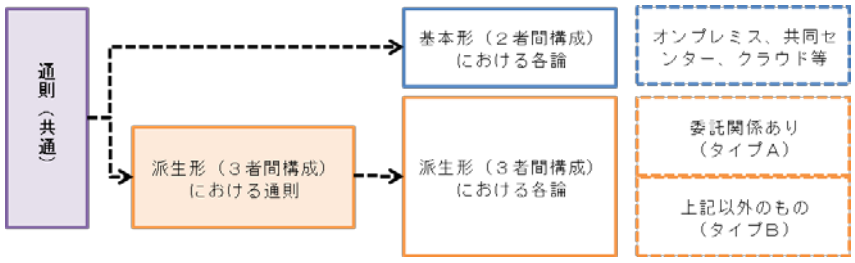
a. 方針・規程
b. 組織体制
c. サイバー攻撃対応体制
d. 人材（要員・教育）

内部の統制に関する方針・対策の決定には、多くの部門が関係することが一般的である。このため、内部の統制に実効性をもたせるためには、人員計画（ローテーション、キャリアパスの策定等）や経営資源配分など、経営層による意思決定が求められる。

(2) 外部の統制

金融情報システムにおける「外部の統制」は、以下のように体系化される。まず、IT ベンダー等とのシステムの開発・運用の委託や、クラウドベンダー等の利用など、２者間で構成される委託関係がある。次に、委託先に加えて、FinTech 企業等のように、必ずしも委託関係にあるとは限らない企業が関与する３者間構成がある。以下では、それぞれについて、「外部の統制」における考え方を解説する（[図表 13] を参照）。

削除: 14



[図表 13] 外部の統制における体系

削除: 14

【資料４－３】
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

① 外部委託の管理における IT ガバナンス

IT の進展や金融機関等の業務範囲の拡大等に伴い、国内の金融機関等では、コスト削減や先進技術の利用等により、顧客の利便性向上や企業価値の最大化を目指した結果、情報システムにおいて年々外部委託への依存度が高まっている現状にある。金融機関等は、外部委託に関する管理責任や説明責任を、より一層求められるものと考える。

外部委託全般における管理プロセスには、次のものが考えられる。これらのプロセスは、基本形である２者間構成のみでなく、後述の派生形となる３者間構成においても、共通で適用されるべきものである。これらのプロセスにおける決定は、委託業務の重要性等を考慮し、経営層等が実施することが望ましい（[図表 14］を参照）。

削除: 15

a. 情報システムの外部委託に関する方針の決定
b. 個別情報システムの外部委託の決定
c. 個別情報システムの外部委託におけるリスク管理の枠組みの決定
d. 各枠組みにおける安全対策の実施
e. 外部委託におけるリスク管理に係る改善事項の決定

	方針の決定	外部委託の決定	リスク管理の枠組みの決定	安全対策の実施	改善事項の決定
特定システム	経営層	経営層	経営層	関係者（管理者等）	経営層
上記のうち、委託業務が低リスクな場合※	経営層	経営層以外	経営層以外		経営層以外
通常システム	経営層	経営層以外	経営層以外		経営層以外

※委託業務の性質に加えて、量（例えば委託金額）によっても判断することが可能である。

［図表 14］外部委託の管理プロセスにおける IT ガバナンス

削除: 15

② 通則（基本形・派生形共通）

金融機関等は、委託先の選定から契約終了まで、その管理責任を有する。これには再委託を含む業務委託の全体を把握することが必要である。また、再委託先の統制の責任は一義的には委託先にあることから、金融機関等の再委託に関する主な責任は、委託先が再委託先を適切に管理しているかどうかをチェックすることにある。

外部委託における共通の管理項目は次のものが考えられる。

・委託先の選定要件の策定と事前審査の実施
・委託先への監査権の明記
・有事対応

上記について、外部委託管理における考え方を解説する。

a. 委託先の選定要件の策定と事前審査の実施

金融機関等は、委託先の選定に当たって、専門性（例えば資格保有状況等）や信頼性（例えば過去に問題を起こしたことが無いか等）等とともに、委託業務の内容に応じて必要となる相互牽制等の内部的なリスク管理態勢を整備する能力の有無を考慮することが必要である。なお、そうした管理態勢の整備が困難な委託先であっても、専門性等の理由により、委託せざるをえない場合には、勤務場所を管理可能な場所に限定するといった条件を付すことが考えられる。これは再委託先に対する確認の場合も同様であるが、再委託の場合は、委託先がそれら再委託先への評価を適切に実施しているかを金融機関等が確認することとなる。再委託先との接点が限られる場合、委託先への確認を通じて、再委託先を評価することとなるため、例えば情報セキュリティに関する管理状況など、その評価はリスク特性等に応じて、適切に実施する必要がある。ただし、委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等か、それ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ委託先の審査・管理プロセスの整備・運用状況の適切性を検証することで、個別の再委託先の事前審査に代替させることが可能である。

b. 委託先への実質的な統制

金融機関等は、契約期間中において、委託先及び再委託先における業務遂行状況のみならず、委託する業務内容や取り扱うデータ等を考慮し、そのリスク特性に応じてセキュリティ管理状況等を確認する必要がある。このため、委託先との契約締結時には、そうしたリスクの度合いや、外部の統制における 2 者間の構成などの統制の形態を金融機関等が適切に判断し、委託先のみならず、必要に応じて再委託先への実質的な統制を行うにあたって必要となる権利（監査権等）に関する条項を盛り込むことが必要である。

監査人の選定に当たっては、FISC『金融機関等のシステム監査指針（改訂第３版追補）』で定められた監査人の選定要件と整合的であることが必要である。

c. 有事対応

システムの運用等を委託する場合、再委託先も含めた委託先におけるコンティンジェンシープランは、個別金融機関等のものと完全に整合し、相互補完的な内容とすることが必要である。また、金融機関等は、平時は、委託先及び再委託先と共同で、定期的に訓練を実施することも重要である。

委託先や再委託先は、システム障害等が発生し、金融インフラ全体に深刻な影響を与える可能性があることを認識した場合には、その状況を即時に金融機関等に報告し、金融機関等のコンティンジェンシープランの発動に係る意思決定を支援することが期待される。

③ 基本形（２者間構成）における各論

以下は、外部の統制における２者間構成の代表的な形態におけるリスク管理策の考え方である。

a. オンプレミス

金融機関等が情報システムを自社で保有し、自社の施設においてシステムの開発や運用、サービスの一部または全部を、外部の企業などに委託する外部委託の形態である。外部の高度な専門能力やノウハウ、技術などを有効に活用し、コスト削減や業務の効率化を図ることが主な目的となるが、情報セキュリティに対する対応態勢を確認するなど、適切な委託先の選定、契約、管理が求められる。

b. 共同センター

共同センターは、外部委託の一形態として、複数の金融機関等が共同で委託している。多くの金融機関等が、勘定系システム等を中心に共同化を進めている状況にある。

共同センターにおいては、主に勘定系システムなど、高い安全対策が求められるシステムを運用しており、有事における初動対応は極めて重要なものとなる。このため、共同センター固有のリスクとして、有事の際、利用者間における意思決定に時間がかかることで、対応の遅れが発生しうるリスク（時間性の問題）を認識しておくことが重要である。そのうえで、利用金融機関等の経営層は、委託先及び他の利用金融機関等との間で、有事を踏まえた対応態勢を整備しておくことが求められる。

c. クラウドサービス

クラウドサービスは、外部委託の一形態として位置付けられ、いくつかの利用形態[21]が存在する。クラウドサービスの特徴として、複数の事業者が単一のクラウド事業者に委託する場合に、利用者間で何らコミュニケーションが無いという「匿名の共同性」、また利用者が広域に及ぶことにより情報処理拠点が複数の国や地域にまたがる「情報処理の広域性」、そして仮想化技術や、データの秘匿性等における「技術の先進性」などが挙げられる。

クラウドサービスにおいて、安全対策を決定する役割がクラウド事業者に帰属する場合は、クラウド事業者が金融機関等からの個別監査要求や改善要望に応えられない可能性があるため、金融機関等においては、クラウド事業者との責任分界点を理解したうえで、利用するクラウドサービスのリスクの特性に応じた適切な統制が行えるかどうかを確認することが重要となる。

④ 派生形（３者間構成）における通則

FinTech 企業等は、IT ベンダーと類似の技術的な性質を有するとともに、金融関連サービスといったビジネスモデルの企画実施等を行う業務的な性質もあわせて有しており、こうした技術的な性質と業務的な性質を同時に有する関係者を含めた、金融機関、IT ベンダー、FinTech 企業等を加えた３者構成の場合には、安全対策上、２者間構成である基本形

[21] 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、利用者のニーズによりサービス内容を選択する。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。

とは異なる点に留意する必要がある。金融機関等の経営層は、イノベーションの発揮によって得られるメリットと、リスク管理上の考慮事項を比較衡量のうえ、外部への統制を適切に実施することが求められる。

a. 同等性の原則

安全対策基準の対象となる金融情報システムについて、その安全対策の在り方を検討するに当たっては、金融機関と IT ベンダーに FinTech 企業等を加えた３者間構成を前提することとなるが、顧客の立場に立てば、安全対策上の関係者が変わろうと、安全対策の効果が同程度で確保されることが期待されていると考えられる。

したがって、FinTech 企業等という新たな関係者が登場する場合であっても、その安全対策の効果は、従来の安全対策基準において実現される２者間構成における効果と比較して、同程度（同等）となるよう留意することが重要である。

b. 再配分ルール

金融機関等は、FinTech 企業等の安全対策遂行能力を確認したうえで、仮に FinTech 企業等の能力を超える過大な責務があれば、その部分については、金融機関や IT ベンダーが分担することで、FinTech 企業等の革新性を損なわずに安全対策の効果を達成できるよう、３者間にて責務の再配分を行なうことが可能である。すなわち、２者間構成を念頭に置いた従来の安全対策基準において求められる責務の水準を維持しつつ、その責務を、３者の各類型における役割や、３者の安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分することができる。

c. リスク特性に合う管理策の適用

金融機関等の FinTech 企業等と接続する金融情報システムが、特定システムをはじめとする重要なシステムと連動する場合においても、それ自体一つのシステムとして完結性を有し、さらにそのリスク特性が金融機関等の特定システムのリスク特性と顕著に異なり、リスク事象を特定システム本体に波及させないことが可能な場合は、当該システムを通常システムとして扱うことが可能である。

⑤ 派生形（３者間構成）における各論

以下は、外部の統制における３者間構成の代表的な形態におけるリスク管理策の考え方である（[図表 15] を参照）。

削除: 16

a. タイプＡ（金融機関等が安全対策の決定を主導するケース）

タイプＡは、FinTech 企業等が、金融機関等の委託先となる形態である（IT ベンダーが金融機関等の委託先となり、FinTech 企業等が再委託先となる場合を含む）。

金融機関等は、FinTech 企業等の安全対策遂行能力を確認し、IT ベンダー及び FinTech 企業等と合意の上、安全対策に係る責務を、３者間で再配分することが可能である（「再配分ルール」）。責務の再配分に当たっては、「同等性の原則」にしたがって、関係者の負

担が必要以上に増加しないよう留意する。

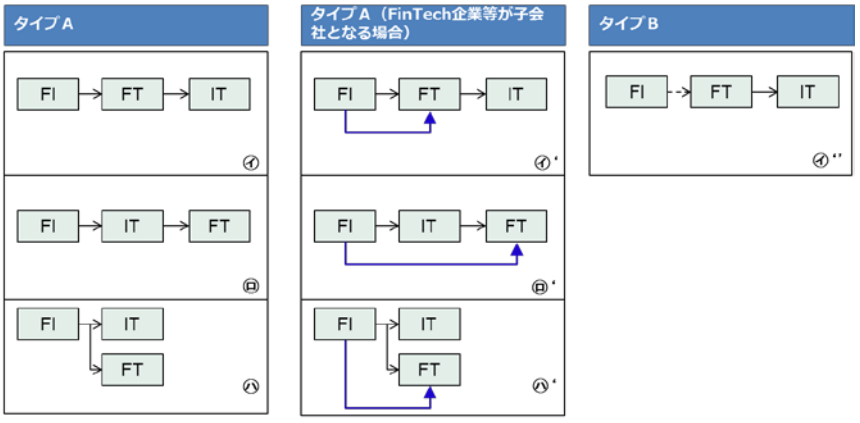
なお、FinTech 企業等が金融機関等の子会社となる形態も、タイプＡに含まれる。この場合、子会社に対する責任が金融機関等に付加される点を除いては、タイプＡのそれ以外の形態と安全対策上の差異はなく、金融機関等は、同等性の原則及び責務の再配分ルールを踏まえた統制を行うことが必要となる。

b. タイプＢ（金融機関等が安全対策の決定において部分的に責務を負うケース）

タイプＢは、FinTech 企業等が、金融関連サービスを主導して提供するケースである。金融機関等の安全対策上の責務が部分的となる点が、基本形またはタイプＡとは異なる。

例えば、FinTech 企業等が、顧客からの依頼に基づき預金取扱金融機関の勘定系システムに入出金の指示を行う場合、原則として、FinTech 企業等が、当該サービスに用いるシステムの安全対策を担うこととなる。この場合、金融機関等の責務は、本人確認及び FinTech 企業等における顧客に関するデータの保全に係る部分に限定される。金融機関等は、当該責務を果たすため、基礎基準で示した安全対策を準用することが可能であり、FinTech 企業等が運用するシステムに対し、本人確認手続きや顧客に関するデータの保全を求めることとなる。

タイプＢにおいても、同等性の原則、責務の再配分などを踏まえた安全対策を行うことが必要となる。



［図表 15］派生形（３者間構成）における安全対策実施上の関係者のタイプ別類型

削除: 16

【資料４－４】
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

改訂原案（安全対策基準前説）

Ⅲ．本書の利用にあたって

１．安全対策基準適用における経過的措置について

２．安全対策基準の構成について

３．基準・解説の記述仕様

（１） 基準・解説の記述仕様

（２） 適用区分

（３） 基準分類

４．用語の解説

５．参照法令・参考文献等

【資料４－４】
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

Ⅲ．本書の利用にあたって

１．安全対策基準適用における経過的措置について

今回の改訂は、従来の改訂と異なり、安全対策基準の適用の考え方から抜本的に変更を行うことから、安全対策基準を参考とする金融機関等においては、その影響が大きいことが予想される。

そのため、現在安定的に運営されている金融情報システムについては、従来どおりの取扱いを継続することとし、システムの更改時や新システムの導入時に、変更後の安全対策基準を適用するなど、順次移行を図ることとする。

コメント [A1]: No.3

２．安全対策基準の構成について

安全対策基準は、統制基準、実務基準、設備基準、監査基準から成り、それぞれが基準大項目、基準中項目及び、基準小項目によって構成されている。

安全対策基準の構成については、資料「安全対策基準一覧表（仮）」を参照のこと。

３．基準・解説の記述仕様

(1) 基準・解説の記述仕様

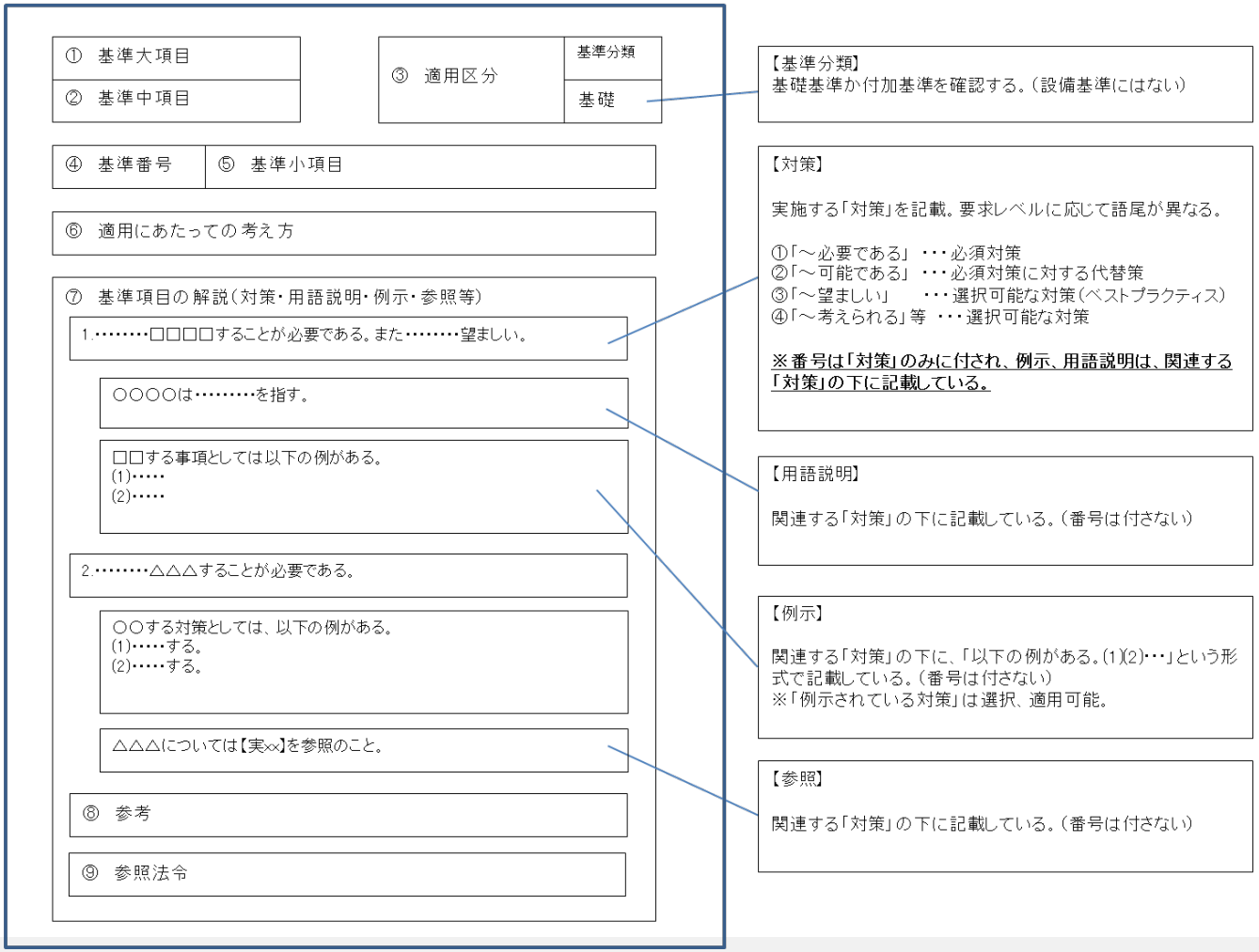
各基準は、図の様式で記述されている。各欄の意味は以下のとおり（[図表 16] を参照）。

① ：基準大項目、当該基準項目がどの大項目に分類されるかを示す
② ：基準中項目、当該基準項目がどの中項目に分類されるかを示す
③ ：適用区分・基準分類（設備基準には基準分類欄はない）
④ ：統制・実務・設備・監査の各基準内における当該基準項目の項番
⑤ ：基準小項目
⑥ ：適用にあたっての考え方
⑦ ：基準項目の解説（対策・用語説明・例示・参照等）
⑧ ：当該基準項目の解説に関連する参考事項
⑨ ：当該基準項目と関連の深い法令

「適用にあたっての考え方」について

基準小項目の目的および、実施すべき内容を記載している。なお、設備基準においては、適用が「望ましい」とした基準がある。（統制基準・実務基準・監査基準については、リスクベースアプローチの考え方に基づき実施する対策を選択するため、当該欄はすべて「すること」としている。）

［図表16］ 安全対策基準・解説の記述仕様



「基準項目の解説（対策・用語説明・例示・参照等)」について

基準小項目に対する具体的な対策を記載している。各対策は、以下のように分類される。必須対策以外は、リスクベースアプローチの考えに基づき、選択可能な対策となる。（[図表 17] を参照

語尾	摘要
・「必要」	必ず実施すべき対策（必須対策）
・「可能」	必須対策に対する代替策
・「望ましい」	選択可能な対策（ベストプラクティス）
・「以下の例がある」「考えられる」「重要である」「有効である」等	選択可能な対策（例示・参考）

［図表 17］基準項目の解説（対策・用語説明・例示・参照等）

(2) 適用区分

本書では、基準の対象箇所を明確にするため、「適用区分」欄を設けている（[図表 18]、[図表 20]参照)。本欄では各基準及び解説等が、以下の箇所を対象とするか否かを◎ないし○で示している。

各記号の意味は以下のとおりである。

◎：基準及び解説等が当該箇所を対象としていることを示す。(全基準共通)

○：当該箇所を対象とするが、金融機関等の業務の実態に照らし、必要に応じて取り入れる基準及び解説等であることを示す。したがって「適用にあたっての考え方」の欄を、「…望ましい」と記述する（設備基準のみ)。

適用区分				
建物、チャネルに依存せず適用 「共」と略記	コンピュータセンター 「セ」と略記	本部・営業店等 「本」と略記	ダイレクトチャネルでサービスを提供 「ダ」と略記	流通・小売店舗等との提携チャネル 「提」と略記
	◎	◎		

※設備基準においては、「建物、チャネルに依存せず適用」の欄はない。

［図表 18］適用区分の例

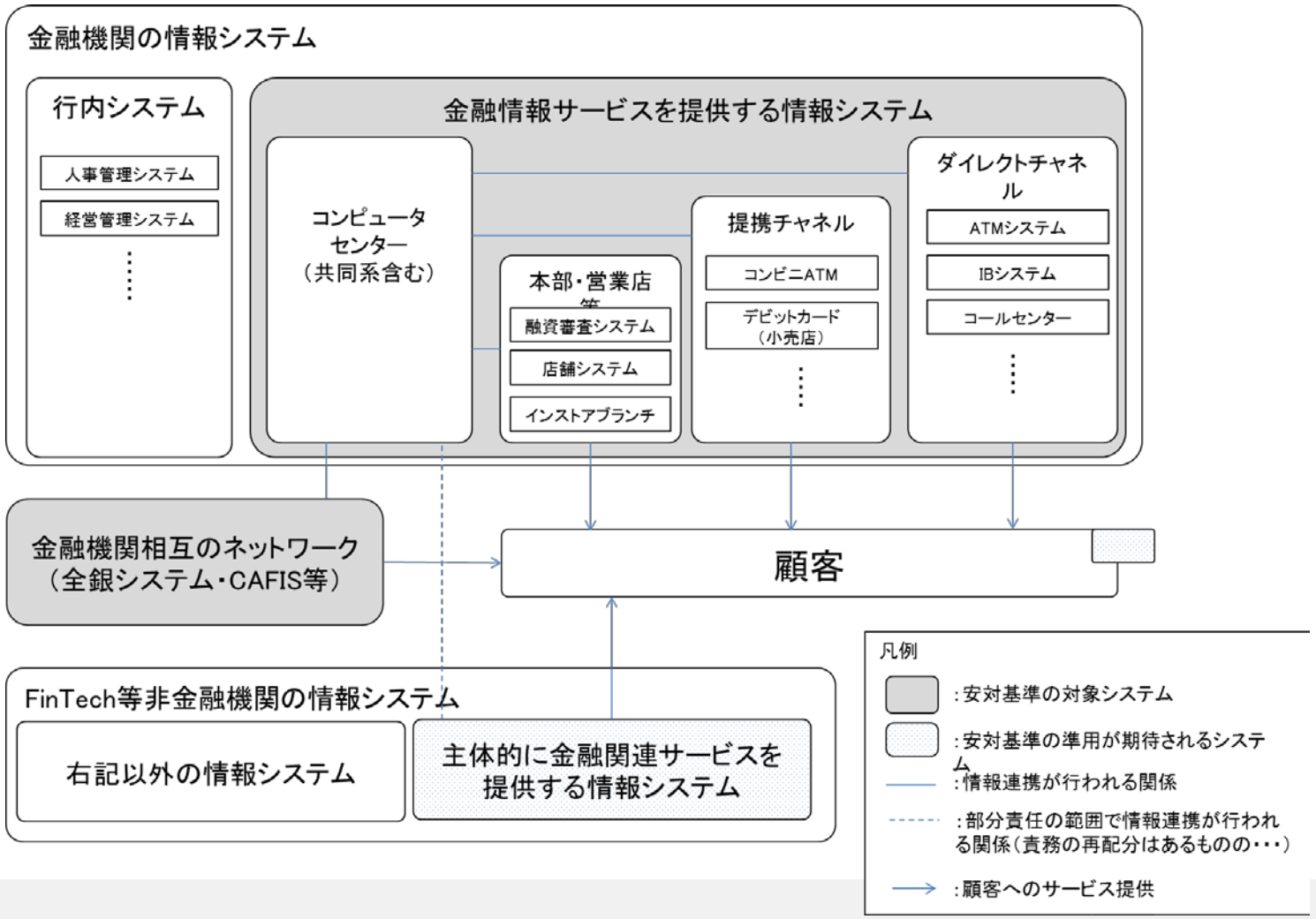
(3) 基準分類

当該基準が基礎基準か付加基準のいずれかを示している（「基礎」または「付加」と記載する。設備基準には当欄はない。）（[図表 19] を参照）。

基準分類
基礎

［図表 19］基準分類の表示例

［図表 20］　安全対策基準の対象である「金融機関等のコンピュータシステム」



各業界・業態によって本部・営業店等の運用形態や提供サービスの内容が異なる場合は、それぞれの実態に合わせて本書に記載の安全対策を適宜取り入れることとする。

以下にモデル化された 5 つの機能要素について述べる。

・コンピュータセンター・共同センター

コンピュータシステムを用いて金融機関等の業務を集中して処理しデータを蓄積する機能を有す。コンピュータ本体やそれを収容する建物、ソフトウェア、開発・維持組織や要員等から構成される。共同センターの場合、建物等の一部構成要素について、金融機関等の管理対象外となる場合がある。

・本部・営業店等

・本部

コンピュータセンター以外の本部機能を指す。企画部門、営業店支援部門、システム開発部門等の組織、事務センターや地区センター等から構成される。

・営業店等

顧客にサービスを提供する店舗機能を指す。有人の店舗（テラーが顧客対応する窓口で、CD・ATM が併設されている場合を含む）、CD・ATM が設置されている無人店舗、ショッピングセンターやスーパーマーケット等にインストアブランチとして設置された CD・ATM、および有人の店舗で勤務している要員等から構成される。

・流通・小売店等との提携チャネル

金融機関等が、金融機関等以外の業態と提携して顧客へのサービスを提供するデリバリーチャネル機能である。小売店舗を通じてサービスを提供する場合（デビットカードなど）や流通業を通じてサービスを提供する場合（コンビニエンス ATM など）を対象としている。

・金融機関等以外の情報システム

FinTech 企業等が提供する金融関連サービス（決済代行サービス等）を指す。利用形態としては、後述するダイレクトチャネル（インターネットバンキング等）に類似すると想定されるため、適用区分は「ダイレクトチャネル」としている。

・ダイレクトチャネル等

「営業店等」を介さずに、サービスを直接顧客に提供するデリバリーチャネル機能を指す。電話やインターネット、モバイル（携帯電話）による金融サービスの提供を想定している。

コメント [A2]: 金融機関等の定義を行ったうえで定義する必要。金融機関等については業法単位では定義できないことが難点（新しい業態は、銀行法、資金決済法で規定さているため）。

削除: 非

削除: 決済代行業者

削除: 電子

【資料４－４】
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

用語の解説は、発刊前までに最新版に修正する。

４．用語の解説

(1) 安全対策基準における「重要な」の意味

安全対策基準において、「重要な本体装置」「重要なデータ」等、「重要な…」と表記されている場合の「重要な」とは、「当該…に障害が発生した場合、金融サービス機能（現金引出、資金決済等）の提供という面で多数の顧客に影響を与え、かつ効果的な代替手段を講ずることが難しいと想定される…」、あるいは「当該…に破壊・改ざん等が発生した場合にコンピュータシステムの運転に重大な支障を来す…」、あるいは「顧客データそのもの」を意味する。

(2) 安全対策基準において用いる主要用語の定義または範囲は、以下のとおりである。

CVCF…… 電源の入力変動や出力負荷の変化に関係なく、コンピュータシステムへ供給する電圧及び周波数を一定に保つ装置、または電圧・周波数を安定化した電源のこと。以前は単独の装置だったが、現在では UPS（無停電装置）に機能として組み込まれることが多い。（Constant Voltage Constant Frequency Power Supply：定電圧定周波装置の略称）

IDF…… 回線がフロアに入る最初の場所に設置されるフロア配線盤（Intermediate Distributing Frame の略称）

MDF …… 回線が建物に入る最初の場所に設置される主配線盤（Main Distributing Frame の略称）

UPS…… 商用電源が短時間停電しても蓄電池から電力を供給し、運転を継続させる機能とともに CVCF（定電圧定周波装置）の機能を備えた装置（Uninterruptible Power Supply：無停電電源装置の略称）

インストアブランチ…… ショッピングセンターやスーパーマーケット等のストア（店舗）の中に設置してある金融機関等の店舗

オープンネットワーク…… インターネットに代表される、不特定多数の相手との自由な接続、通信が可能なネットワーク

オペレータ…… コンピュータセンターにおけるコンピュータ操作者

クラウド…… 米国の NIST（National Institute of Standards and Technology：国立標準技術研究所）におけるクラウドの定義を採用する。

【NIST におけるクラウドの定義】

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。

コンビニ ATM …… 金融機関がコンビニエンスストア内に設置した ATM

コンピュータ…… ホストコンピュータ、サーバー、ワークステーション、パソコンの総称

コンピュータシステム…… コンピュータ、端末機器、周辺装置、通信系装置、回線及びプログラム等の全部または一部により構成されるデータを処理するた

削除: ｸﾗｲｱﾝﾄｻｰﾊﾞｰ・ｼｽﾃﾑ …… ．ホストコンピュータを中心とした中央集中型のシステムに対し、LAN 等のネットワークで結合されたサーバーを中心とする資源の共有、分散処理を行う非中央集中型のシステム．

	のシステム。非中央集中型の分散処理システム（クライアント・サーバーシステム等）を含む。
コンピュータ室……	コンピュータを設置する室
コンピュータセンター……	コンピュータシステムを運営するためのコンピュータを設置する建物または組織
サーバー……	LAN 等のネットワークで接続されたシステムにおいて、他のコンピュータにファイルやデータ、プログラム等（サービス）を提供するコンピュータ
システム管理者……	システムが正常に動作するよう保守、運用について統制・管理する者
スマートデバイス……	スマートフォン及び同様の機能を具備するタブレット型端末の総称
セキュリティ管理者……	情報システムのセキュリティ全般を統制・管理する者
セキュリティポリシー……	情報資産を適切に保護するための会社（または組織）としての安全対策に関する方針
ダイレクトチャネル……	オープンネットワークを利用したインターネットやモバイル、または電話などにより、金融サービスを営業店等を通さずに顧客に直接提供する方法の総称
データ……	コンピュータシステムの処理に適するように形式化された情報
データ管理者……	保有する情報について統制・管理する者 データ利用状況の管理、アクセス権の承認等を行う
データ保管室……	データ、プログラムの記録媒体を保管する室
デビットカード……	利用代金を顧客の口座から即時に引き落とし、利用店の口座に入金する即時決済サービスを提供可能なカードサービス
ドキュメント……	コンピュータシステムの開発、設計、作成、運用等に関する記録
ネットワーク管理者……	ネットワークの運用、セキュリティ、障害及びネットワーク関連機器を統制・管理する者
パスワード……	ネットワークやシステム等を利用する際に使用する、本人を認証するための、本人しか知り得ない文字列
パッケージ……	特定の業務用にあらかじめ作成され、市販されているソフトウェア
ビデオ装置……	防犯カメラの映像、音声等の記録・再生装置
ファイル……	記録媒体、または記憶装置に記録されているデータ及びプログラム
モバイル取引……	モバイル端末を利用して金融機関等が行う銀行取引、証券取引、生損保取引等の金融サービスの総称
暗証番号……	ATM やパソコン、モバイル端末で本人確認のために入力する数字
金融関連サービス……	金融機関等（銀行等の預貯金取扱機関、信託会社、保険会社、証券会社、クレジット会社等をいう。ただし、電子決済等代行業者

	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
共同センター……	複数の金融機関等が共同で利用する勘定系システムを運用するコンピュータセンター。
空調設備……	コンピュータ室等の空気調和（温度・湿度・清浄度などの室内環境の調節）をするための空気調和機、冷却塔及びその付属設備
経営層……	取締役会（理事会）等
顧客データ……	業務上収集、蓄積、利用される顧客に関するデータ データの範囲は、保有するすべての個人情報（氏名、生年月日、取引内容等）及び法人情報（代表者、決算内容、取引内容等）
個人情報[1]……	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できるものを含む）をいう。
個人データ……	個人情報データベース[2]等を構成する個人情報
自動機器室……	CD・ATM などの現金自動支払い機等を設置するコーナー、室
周辺装置……	磁気ディスク装置、磁気テープ装置、コンソールディスプレイ、プリンター等の総称
渉外端末……	ハンディ端末、スマートデバイス、携帯型パソコン等、主に渉外担当者が携帯し、店舗外で利用されるコンピュータ機器
端末機器……	コンピュータに接続される、窓口装置、自動機器、ワークステーション、パソコン等の機器
端末系装置……	コンピュータシステムを利用するための入出力インタフェースとなる窓口装置、パソコン、渉外端末等の機器及びそれらを制御する装置の総称
通信系装置……	通信制御装置等またはルーター等
提携チャネル……	デビットカード及びコンビニ ATM 等の総称
電源設備……	コンピュータシステム等を作動させるための受電設備、UPS（無停電装置）、自家発電設備等の設備及びその付属設備
電子署名……	電子情報の真正性を確保するための技術であり、公開鍵暗号方式に依拠したデジタル署名が一般的である。電子署名は、本人確認のほか、改ざんの防止、取引否認の防止にも有効である。なお、電子署名法上の電子署名はデジタル署名に限られない。
防犯カメラ……	状況監視を行うためのテレビカメラ
防犯ビデオ……	防犯カメラの映像、音声等の記録

[1] 「個人情報」、「個人データ」の定義の詳細については、金融庁告示『金融分野における個人情報保護に関するガイドライン』を参照。
[2] 「個人情報データベース」とは、個人情報を含む情報の集合物であって、特定の個人情報をコンピュータを用いて検索できるように体系的に構成したもの。

不正アクセス……	不正な手段により、ユーザー以外の者が行うアクセスまたはユーザーが行う権限外のアクセス
本体装置……	中央処理装置、主記憶装置、チャネル装置等の総称
本部・営業店等……	コンピュータセンター以外の本部（具体的には、企画部門、営業店支援部門、システム開発部門等の組織、事務センターや地区センターなど等）及び顧客にサービスを提供する店舗（下記「無人店舗」や「インストアブランチ」を含む）の総称
無人店舗……	CD・ATM 等の自動機器のみで運用を行う店舗

【資料４－４】
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

４． 参照法令・参考文献等

安全対策基準における参照法令および参考文献等は以下のとおりである。

参考文献等は、発刊前までに最新版に修正する。

3.1 法令等

(1) 建築基準法
(2) 建築基準法施行令
(3) 電気事業法「電気設備の技術基準の解釈」
(4) 消防法
(5) 消防法施行令
(6) 消防法施行規則
(7) 昭和 48 年消防庁告示第 1､2 号
(8) 平成 13 年消防庁告示第 39 号
(9) 東京都火災予防条例施行規則
(10)不正アクセス行為の禁止等に関する法律
(11)組織的な犯罪の処罰及び犯罪収益の規制等に関する法律
(12)電子署名及び認証業務に関する法律
(13)消費者契約法
(14)金融商品の販売等に関する法律
(15)労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律
(16)建築物の耐震改修の促進に関する法律
(17)都市計画法
(18)民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律
(19)個人情報の保護に関する法律
(20)金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律
(21)偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律
(22)危険物の規制に関する政令
(23)犯罪による収益の移転防止に関する法律

なお、条文は本書発行時点のもの。

3.2 海外・国内規格等

(1)「British Standard BS7799-Part 1：1999 Information Technology － Code of Practice for Information Security Management」（英国標準規格 BS7799 情報技術－情報セキュリティマネジメントの実践のための規範）BSI（英国規格協会）1999 年
(2)「British Standard BS7799-Part 2：2002 Information Security Management － Specification with Guidance for Use」（英国標準規格 BS7799 情報セキュリティマネジメント－仕様及び利用の手引き）BSI（英国規格協会）2002 年
(3)「JIS X 5080：2002（ISO/IEC 17799:2000） 情報技術―情報セキュリティマネジメント実践のための規範」 日本規格協会

(4)「ISO/IEC 15408 : 1999」（国際標準化機構／国際電気標準会議 ISO/IEC15408　システム評価基準等に関する国際標準）1999 年
(5)「ISO/TR 13569 : 1997 Banking and related financial services-Information security guidelines」（国際標準化機構 ISO/TR 13569　金融機関等の情報セキュリティ対策指針に関する技術報告書）1997 年
(6)「ISO/IEC TR 13335-1~5 : Information technology-Guidelines for the management of IT Security」（国際標準化機構 ISO/IEC/TR 13335　IT セキュリティマネジメントのガイドライン）　1996～2004 年
(7)「ANSI X9.84-2003 Biometric Information Management and Security for the Financial Services Industry」（米国標準規格 X9.84 金融サービスのための生体情報管理とセキュリティ）ANSI（米国規格協会）2003 年

3.3 海外・国内ガイドライン等
(1) 「金融分野における個人情報保護に関するガイドライン」　金融庁 平成 16 年 12 月
(2) 「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関する実務指針」　金融庁 平成 17 年 1 月
(3) 「金融検査評定制度（預金等受入機関に係る検査評定制度)」　金融庁 平成 17 年 7 月
(4) 「偽造キャッシュカード問題に関するスタディグループ最終報告書～偽造・盗難キャッシュカード被害発生の予防策・被害拡大の抑止策を中心として～」　金融庁 平成 17 年 6 月
(5) 「金融機関における情報セキュリティの重要性と対応策」　日本銀行 平成 12 年 4 月
(6) 「金融機関業務のアウトソーシングに際してのリスク管理」　日本銀行 平成 13 年 4 月
(7) 「わが国金融機関におけるシステムリスクの管理状況と留意点」　日本銀行 平成 13 年 9 月
(8) 「金融機関の拠点被災を想定した業務継続計画のあり方」　日本銀行 平成 14 年 3 月
(9) 「金融機関における業務継続体制の整備について」　日本銀行 平成 15 年 7 月
(10)「金融機関の防犯基準」　警察庁 平成 11 年 10 月
(11)「コンビニエンスストア・スーパーマーケットの防犯基準」　警察庁 平成 15 年 12 月
(12)「単体で設置される現金自動預支払機（ATM）等の防犯基準」　警察庁 平成 15 年 7 月
(13)「現金自動支払機等の防犯基準」　警察庁 平成 3 年 6 月
(14)「情報システム安全対策指針」　警察庁 平成 11 年 11 月
(15) 「CD 等の技術的防犯対策について」　日本自動販売機工業会 金融システム部会 平成 2 年 6 月
(16)「ガラスの防犯性能に関する板硝子協会基準」　板硝子協会 平成 14 年 3 月
(17)「VDT 作業における労働衛生管理のためのガイドライン」　厚生労働省 平成 14 年 4 月
(18)「情報通信ネットワーク安全・信頼性のガイドライン」　平成 7 年 4 月
（編集）郵政省電気通信局電気通信事業部電気通信技術システム課
（発行）財団法人 日本データ通信協会
(19)「情報通信ネットワーク安全・信頼性基準」　郵政省 平成 6 年郵政省告示第 638 号
「情報通信ネットワーク安全・信頼性基準」の一部改正　総務省 平成 16 年総務省告示第 244 号

(20)「重要インフラの情報セキュリティ対策に係る行動計画」 内閣官房情報セキュリティセンター 平成 17 年 12 月
(21)「コンピュータウイルス対策基準解説書」 平成 7 年 7 月
（監修）通商産業省機械情報産業局 （発行）財団法人 日本情報処理開発協会
（コンピュータウイルス対策基準：平成 12 年通商産業省告示第 952 号）
(22)「システム監査基準解説書」 平成 16 年 10 月
（監修）経済産業省商務情報政策局 （発行）財団法人 日本情報処理開発協会
(23)「システム管理基準解説書」 平成 16 年 10 月
（監修）経済産業省商務情報政策局 （発行）財団法人 日本情報処理開発協会
(24)「コンピュータ不正アクセス対策基準解説書」 平成 8 年 11 月
（監修）通商産業省機械情報産業局 （発行）財団法人 日本情報処理開発協会
（コンピュータ不正アクセス対策基準：平成 12 年通商産業省告示第 950 号）
(25)「コンピュータセキュリティ基本要件」 社団法人 電子情報技術産業協会 平成 9 年 8 月
(26)「金融機関向け防犯カメラの性能基準」 社団法人 日本防犯設備協会 平成 16 年 3 月
(27)「情報システムの設備ガイド」 社団法人 電子情報技術産業協会 平成 15 年 3 月
(28)「IS(Information Systems)検査ハンドブック」 FFIEC（米国連邦金融機関検査協議会）2002 年
(29)「電子バンキングにおけるリスク管理の原則」 バーゼル銀行監督委員会 2003 年 7 月
(30)「BIOVISION, Privacy Best Practices in Deployment of Biometric Systems」 2003 年 8 月
(31)「全銀協 IC キャッシュカード標準仕様」 全国銀行協会 平成 13 年 3 月
(32)「暗号技術検討会 2002 年度報告書」暗号技術検討会 平成 15 年 3 月
(33)「金融機関等のシステム監査指針」 財団法人 金融情報システムセンター 平成 19 年 3 月
(34)「ATM 等の技術的防犯対策について」 日本自動販売機工業会 金融システム委員会 平成 12 年 12 月
(35)「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」 内閣官房情報セキュリティセンター 平成 21 年 2 月
(36)「電子政府推奨暗号の利用方法に関するガイドブック」 独立行政法人 情報通信研究機構、独立行政法人 情報処理推進機構 平成 20 年 3 月
(37)「フィッシング対策ガイドライン」 フィッシング対策協議会 平成 22 年 4 月
(38)「共通フレーム 2007―経営者、業務部門が参画するシステム開発および取引のために」 独立行政法人 情報処理推進機構ソフトウェア・エンジニアリング・センター 平成 21 年 10 月
(39)「安全なウェブサイトの作り方」 独立行政法人 情報処理推進機構セキュリティセンター 平成 22 年 1 月
(40)「安全な Web サイト利用の鉄則」独立行政法人 産業技術総合研究所 情報セキュリティ研究センター 平成 19 年 3 月

(41)「バックアップ・コンピュータセンターの実効性確保にかかる課題と対応策」 日本銀行 平成 22 年３月

3.4 金融検査マニュアル

(1) 「預金等受入金融機関に係る検査マニュアル」 金融庁 平成 11 年 7 月、最終改正平成 22 年９月
(2) 「保険会社に係る検査マニュアル」 金融庁 平成 12 年 6 月、最終改正平成 23 年 2 月
(3) 「金融商品取引業者等検査マニュアル」 証券取引等監視委員会 平成 13 年 6 月、最終改正平成 22 年３月
(4) 「システム統合リスク管理態勢の確認検査用チェックリスト」 金融庁 平成 14 年 12 月
(5) 「金融持株会社に係る検査マニュアル」 金融庁 平成 15 年 7 月、最終改正平成 21 年５月

【資料５－１】
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

平成29年度第57回安全対策専門委員会
検討事項に関するご意見（メール回答用）

電子メールにて、ご連絡願います。（fisc40@fisc.or.jp）

〆切　10/31（火）17:00

会社名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

お名前：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

資料番号	項番 （基準番号）	ご意見
（例） 資料２－１	（例） Ⅱ．１． （２）	・・・