平成 29 年 8 月 8 日
公益財団法人 金融情報システムセンター

第 55 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 8 月 8 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
２．	15:10	【議案１】基礎基準に対する委員意見反映版の検討
３．	15:50	【議案２】外部委託管理関連基準の検討
４．	16:20	【議案３】安全対策基準「読みやすさ」対応について
５．	16:50	事務連絡
６．	17:00	閉会

Ⅳ　資料

【資料１－１】　基礎基準案に関するご意見について
【資料１－２】　基準一覧（追加基礎基準案）
【資料１－３】　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）
【資料２－１】　外部委託管理関連基準の統合・整理について
【資料３－１】　安全対策基準「読みやすさ」対応について
【資料３－２】　安全対策基準の再構成について
【資料３－３】　「読みやすさ」向上に関する対応
【資料３－４】　安全対策基準・解説の記述ルール（案）
【資料３－５】　新基準構成案
【資料３－６】　基準原案サンプル
【資料４－１】　改訂原案（安全対策基準前説）最新（事後送付）
【資料４－２】　改訂原案（前説）に対する各委員からのご意見（事後送付）
【資料５－１】　検討事項に関するご意見（メール回答用）

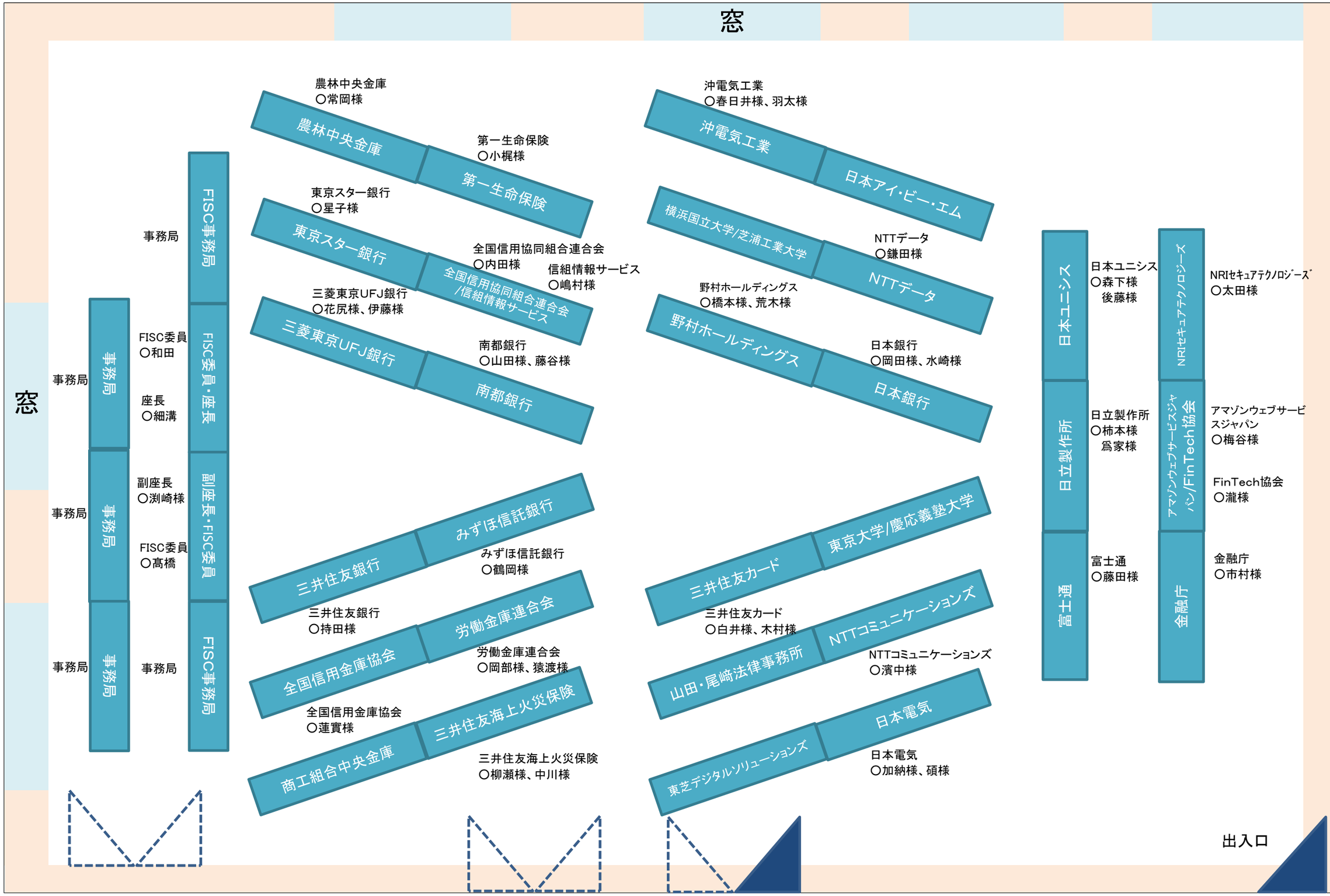
Ⅴ　今後の予定

○第 56 回　安全対策専門委員会
（予定）平成 29 年 9 月 12 日（火）15:00～17:00　FISC 会議室

以上

第55回「安全対策専門委員会」座席表

平成29年8月8日



【資料１－１】
平成 29 年８月８日
公益財団法人 金融情報システムセンター

基礎基準に関するご意見について

I. 主たるご意見

○ 複数の委員の方々から、「基礎基準」の追加に関するご意見が提示された。追加候補となるのは、４４基準（【資料１－２】「基準一覧（追加基礎基準案）」参照）。

II. ご意見の反映方針

○ 「『基礎基準』の選定にあたっての考え方」を以下のとおり変更する。

＜前回＞

- ✓ 統制・監査に関する基準
- ✓ 顧客データの漏えい防止に関する基準
- ✓ コンティンジェンシープラン策定に関する基準

＜今回＞

- ✓ 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

○ 「基礎基準」の追加候補について

追加候補となる基準は、①システムの不正使用防止に関する基準、②システムの運行管理に最低限必要な基準に分類することができる。

- ①は、顧客データの漏えい防止策と共通する面が多いことから、「顧客データの漏えい防止に関する基準」を「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」に改め、「基礎基準」に取り込む。
- ②は、新しい選定の視点として設定し、「基礎基準」に取り込む。

○ ご意見の反映による基準件数の内訳

この結果、「基礎基準」、「付加基準」の数は、以下のとおりとなる。

内訳			前回提示	**今回提示**
基準総数			162	162
	基礎基準		71	115
		事務局案	71	71
		追加対象	－	44
	付加基準		91	47

※外部の統制基準を除く

以上

【資料１－２】
平成29年8月8日
公益財団法人　金融情報システムセンター

基準一覧（追加基礎基準案）

構成	基準大項目	基準中項目	新基準番号（暫定）	基準小項目	基礎基準	基礎基準				三菱東京UFJ銀行 伊藤様	野村ホールディングス 荒木様	三井住友カード 白井様	ｱﾏｿﾞﾝｳｪﾌﾞｻｰﾋﾞｽｼﾞｬﾊﾟﾝ 梅谷様	旧基準番号
						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					
Ⅰ　統制基準	1　内部の統制	(1) 方針・規定	統1	セキュリティ管理方法を具体的に定めた文書を整備すること。	○	○								運1
			統2	セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。	○	○								運2
			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4	各種規定を整備すること。	○	○								運10
			統5	セキュリティ遵守状況を確認すること。	○	○								運10-1
		(2) 組織体制	統6	セキュリティ管理体制を整備すること。	○	○								運3
			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12	業務組織を整備すること。	○	○								運9
		(3) サイバー攻撃対応態勢	統13	サイバー攻撃対応態勢を整備すること。	○	○								運113
		(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
			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	要員の健康管理を行うこと。	○	○								運86
	2　外部の統制	(1) 方針・計画	外部委託検討の中で整理する。	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。										
		(2) 契約・業務管理		外部委託先の選定手続きを明確にすること。										
				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。										
				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。										
				外部委託にあたって、データ漏洩防止策を講ずること。										
				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。										
				外部委託契約終了時の情報漏洩防止策を講ずること。										
		(3) 金融機関相互のシステム・ネットワークのサービス	統28	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。										
Ⅱ　実務基準	1　入退管理	(1) 入退館（室）管理	実1	資格付与およ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
	2　運用管理	(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化すること。	○		○							運18
		(3) 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
		(4) 入力管理	実14	データの入力管理を行うこと。	○				○	●				運24
		(5) データファイル管理	実15	授受・管理方法を定めること。	○		○							運25
			実16	修正管理方法を明確にすること。	○				○	●		●		運26
			実17	バックアップを確保すること。	○			○						運27
		(6) プログラムファイル管理	実18	管理方法を明確にすること。	○				○	●				運28
			実19	バックアップを確保すること。	○			○						運29
		(7) 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
		(8) ネットワーク設定情報管理	実21	設定情報の管理を行うこと。	○				○	●		●		運31
			実22	設定情報のバックアップを確保すること。	○			○						運32
		(9) ドキュメント管理	実23	保管管理方法を明確にすること。	○				○	●				運33
			実24	バックアップを確保すること。	○			○						運34
		(10) 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
		(11) 出力管理	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
		(12) 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
			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
		(13) 暗号鍵の管理	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
		(14) 厳正な本人確認の実施	実34	本人確認を行うこと。	○				○	●				運44
			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
		(15) 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	監視体制を明確にすること。										運46
			実38	防犯体制を明確にすること。										運47
			実39	障害時・災害時の対応方法を明確にすること。										運48
			実40	関係マニュアルの整備を行うこと。										運49
		(16) 渉外端末の管理	実41	運用管理方法を明確にすること。	○		○							運50
		(17) カード管理	実42	カードの管理方法を明確にすること。	○		○							運51
			実43	顧客に対して犯罪に関する注意喚起を行うこと。										運51-1
			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
		(18) 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
		(19) 資源管理	実47	能力及び使用状況の確認を行うこと。	○				○	●				運54
		(20) 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
		(21) 機器の管理	実50	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	保守方法を明確にすること。										運59
		(22) 運行監視	実53	監視体制を整備すること。	○		○							運60
		(23) コンピュータ室・データ保管室の管理	実54	入室後の作業を管理すること。	○		○							運61
		(24) 障害時・災害時対応策	実55	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
		(25) 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

基準一覧（追加基礎基準案）

構成	基準大項目	基準中項目	新基準番号（暫定）	基準小項目	基礎基準	基礎基準				三菱東京UFJ銀行 伊藤様	野村ホールディングス 荒木様	三井住友カード 白井様	ｱﾏｿﾞﾝｳｪﾌﾞｻｰﾋﾞｽｼﾞｬﾊﾟﾝ 梅谷様	旧基準番号
					基礎基準	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					
	3 システム開発・変更	(1) ハードウェア・ソフトウェア管理	実59	ハードウェア、ソフトウェアの管理を行うこと。	○				○	●		●		運66
		(2) システム開発・変更管理	実60	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
		(3) ドキュメント管理	実63	作成手順を定めること。										運70
			実64	保管管理方法を明確にすること。										運71
		(4) パッケージの導入	実65	評価体制を整備すること。										運72
			実66	運用・管理体制を明確にすること。										運73
		(5) システムの廃棄	実67	廃棄計画、手順を策定すること。	○		○							運74
			実68	情報漏洩防止対策を講ずること。	○		○							運75
	4 各種設備管理	(1) 保守管理	実69	管理方法を明確にすること。	○				○	●				運76
			実70	保守方法を明確にすること。	○				○	●				運77
		(2) 資源管理	実71	能力および使用状況の確認を行うこと。	○				○	●				運78
		(3) 監視	実72	監視体制を整備すること。	○				○	●				運79
	5 インストアブランチ	(1) インストアブランチ	実73	出店先の選定基準を明確にすること。										運92
	6 コンビニATM	(1) コンビニATM	実74	出店先の選定基準を明確にすること。										運93
			実75	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	障害時・災害時対応手順を明確にすること。										運95
			実77	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	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	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	(1) デビットカード・サービスの安全性確保	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	口座番号、暗証番号等の安全性を確保すること。										運100
		(2) 顧客保護	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
		(3) 顧客への注意喚起	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 オープンネットワークを利用した金融サービス	(1) インターネット、モバイル	実84	不正使用を防止すること。	○		○							運103
			実85	不正使用を早期発見すること。	○		○							運104
			実86	安全対策に関する情報開示をすること。										運105
			実87	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化すること。										運106
		(2) 電子メール	実89	電子メールの運用方針を明確にすること。										運107
	9 共同センター	(1) 共同センター	外部委託検討の中で整理する。	共同センターにおける有事対応方針を明確にすること。										
	10 FinTech・クラウド関連	(1) FinTech・クラウド関連		（現時点では勘定系クラウドとオープンAPIが入る想定）										
	11 ハードウェアの信頼性向上対策	(1) 保守管理	実92	予防保守を実施すること。										技1
		(2) 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
	12 ソフトウェアの信頼性向上対策	(1) 開発時の品質向上対策	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
		(2) メンテナンス時の品質向上対策	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
	13 運用時の信頼性向上対策	(1) 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
			実109	CD・ATM等の遠隔制御機能を設けること。										技19
	14 障害の早期発見・早期回復	(1) 障害の早期発見	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
		(2) 障害の早期回復	実112	障害時の縮退・再構成機能を設けること。										技22
			実113	取引制限機能を設けること。										技23
			実114	リカバリ機能を設けること。	○				○		●			技24
	15 災害時対策	(1) 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
	16 データ保護	(1) 漏洩防止	実116	暗証番号・パスワード等は他人に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
		(2) 破壊・改ざん防止	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
		(3) 検知策	実123	伝送データの改ざん検知策を講ずること。	○		○						●	技33
			実124	ファイル突合機能を設けること。	○		○						●	技34
	17 不正使用防止	(1) 予防策(アクセス権限確認)	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
		(2) 予防策(利用範囲の制限)	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
		(3) 予防策(不正・偽造防止対策)	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。	○				○	●				技40
			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
			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
			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
		(4) 外部ネットワークからのアクセス制限	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
		(5) 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
		(6) 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
	18 不正プログラム防止	(1) 防御策	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
		(2) 検知策	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
		(3) 復旧策	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
Ⅲ 設備基準														
Ⅳ 監査基準	1 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
					115	21	51	9	35	37	4	10	4	162

【資料１－３】
平成29年8月8日
公益財団法人　金融情報システムセンター

■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.	記載箇所	ご意見の概要	ご意見者	対応方針
1	基準一覧（基礎基準案）　統4	統4は統1を包含する内容と思われるため、順序としても統1より前に配置しては如何でしょうか。	NRIｾｷｭｱﾃｸﾉﾛｼﾞｰｽﾞ 太田様(検)	ご指摘の基準は、その対策や目的等から現在の基準小項目が抽象的すぎると考え、基準小項目を「手順書・マニュアルを整備すること」に修正し、適切な配置先に移動させたいと考えております。詳細につきましては、本日のテーマ「安全対策基準『読みやすさ』対応について」で、ご説明させていただきます。
2	（全般）	基準の各基準小項目について、その項目が「基礎基準」に該当するかどうかわかるように、基準小項目の各ページに掲載してほしい。また、「旧基準番号」も同様に掲載してほしい。	三井住友海上火災保険株式会社 中川様(検)	「基礎基準」につきましては、各頁で判別できる項目を記します。「旧基準番号」との繋がりにつきましては、新旧対比表で示す方法を考えております。
3	基準一覧（基礎基準案）　統13	攻撃発覚を起点とする体制は安全対策基準として求められるものとして明示された記載があると認識にありますが、攻撃を早期に把握等の観点で、平時を含む常時の監視、分析体制の整備について、明示した基準の構成等の検討は、できないでしょうか。	日本ユニシス 後藤様(検)	監視、分析体制の整備について具体的な対策等が記載されています『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』を参照する文書を追加したいと考えます。
4	（全般）	「基礎基準」か「付加基準」かが判る様にして頂くと良いかと思います。	野村ホールディングス 荒木様(検)	No2参照

【資料２－１】
平成 29 年８月８日
公益財団法人 金融情報システムセンター

外部委託管理関連基準の統合・整理について

Ⅰ 外部委託関連基準検討の背景

「金融機関におけるクラウド利用に関する有識者検討会」（以下、「クラウド有識者検討会」という）において、クラウドサービスを利用するにあたっての安全対策の在り方が議論され、ＦＩＳＣ安全対策基準（以下、安対基準）に、外部委託に関する基準（以下、「外部委託基準」という）の特則として、クラウドサービスに関する基準（以下、「クラウド基準」という）を追加した（安対基準 第８版追補改訂＜平成２７年６月発刊＞）。その後、金融機関等における外部委託への依存度の高まりを背景に、「金融機関における外部委託に関する有識者検討会」（以下、「外部委託有識者検討会」という）及び、「金融機関における FinTech に関する有識者検討会」（以下、「FinTech 有識者検討会」という）において、外部委託管理の在り方や共同センターにおける安全対策の考え方、また、重要な情報システムにおけるクラウドサービス固有のリスク管理策が議論された。

以上を踏まえ、以下の観点から外部委託管理関連基準の統合・整理について検討を進めていく。

１．外部委託基準とクラウド基準の統合・整理
（重要な情報システムにおけるクラウドサービス利用時の固有の安全管理策の規定含む）
２．金融機関相互のシステム・ネットワークに関する安全管理策の位置づけ
３．共同センターに関する固有の安全管理策
４．FinTech に関する固有の安全管理策の要否

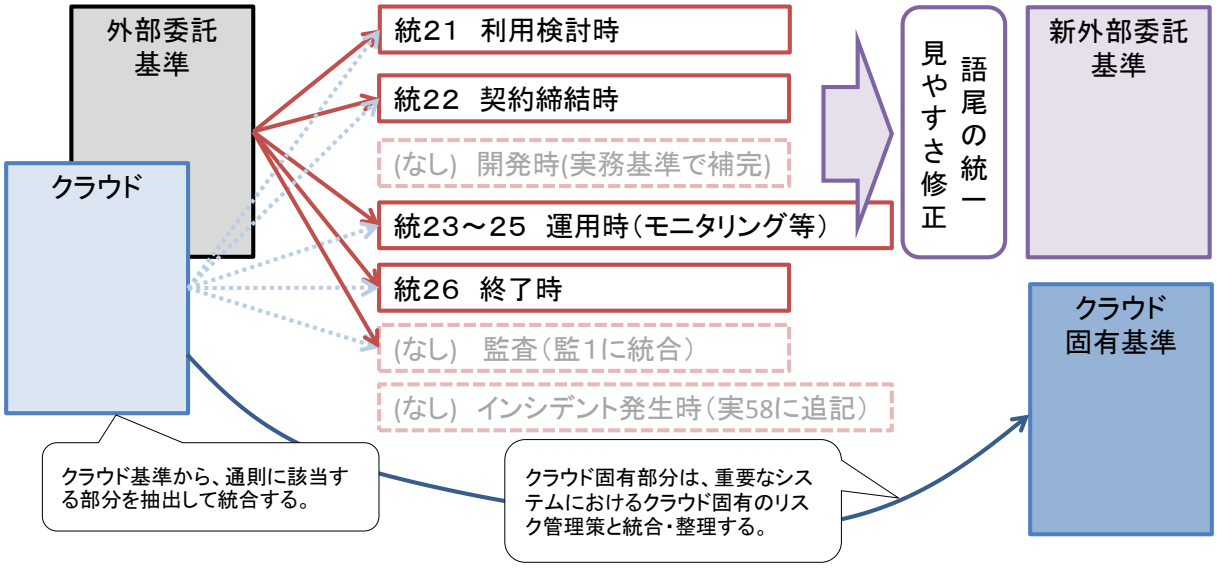
Ⅱ 検討テーマ

論点１　外部委託基準とクラウド基準の統合・整理

クラウドサービスの利用は外部委託の一形態であり、FinTech 有識者検討会において、クラウドサービス固有の性質と重要な情報システム（＝特定システム）で利用する場合のリスク管理策が整理されたことから、外部委託基準とクラウド基準を統合・整理することが適当である。つまり、外部委託に関する共通の基準（以下、「通則」という）と、クラウド固有の基準とに整理して規定する。

具体的なプロセスとしては、まず、外部委託有識者検討会及び、FinTech 有識者検討会の提言内容を踏まえ、外部委託基準とクラウド基準からクラウド固有の安全対策を除いた部分とを統合する。この際、外部委託有識者検討会での整理をもとに、外部委託管理に関する各フェーズ（利用検討時、契約締結時、運用時（モニタリング等）、契約終了時）ごとに基準を統合する。また、クラウド固有の基準は、FinTech 有識者検討会で提言された、特定システムにおけるクラウド固有のリスク管理策の内容と照らしたうえで、必要に応じて加筆・修正を行い、新たな基準として規定する。また、監査等、それ以外の関連する基

準についても併せて統合・整理を行う（図表１参照）。



図表１　外部委託基準とクラウド基準の統合・整理

統合・整理の結果、外部委託基準は以下のようになる。

フェーズ	外部委託基準	クラウド基準	新基準
利用検討時	【運 87】、【運 87-1】	【運 108】	【統 21】
契約締結時	【運 88】	【運 109】	【統 22】
運用（モニタリング）	【運 89】　※１	－	【統 23】
	【運 90】　※２	－	【統 24】
	－	【運 110】　※３	【統 25】
契約終了時	－	【運 111】	【統 26】

※１　外部委託先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

※２　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

※３　外部委託にあたってデータ漏洩防止策を講ずること

内容によって、クラウドには適用されない旨を記載するかどうかを検討する必要がある。

また、クラウド基準から分離したクラウド固有の安全管理策については、FinTech 有識者検討会にて提言された、クラウド固有のリスク管理策をもとに、「統制対象クラウド拠点の把握」「監査権の明記」「監査人等モニタリング人材の配置」等に関する安全対策と統合・整理し、外部の統制の一つとして、クラウドサービス利用に関する基準【統 27】を新設する。

安全管理策の要素	新基準
【運 108】～【運 111】よりクラウド固有の安全管理策として分離した部分	【統 27】
FinTech 有識者検討会で定義された特定システムにおけるクラウド固有の安全管理策	

その他の外部委託に関連する基準については、以下のとおり統合・整理する。

(1) クラウド基準における監査に関する基準【運 112】は、【運 91】（新基準上の【監 1】）に、外部委託に関する内容として統合する。
(2) 外部委託有識者検討会にて提言された有事対応に関する内容（特定システムに関する業務を再委託する場合、ＣＰは委託先、再委託先を含め策定する必要がある）については、ＣＰ策定に関する基準【運 65】（新基準上の【実 58】）に追加する。

その他整理の内容	整理後
【運 112】（クラウドにおける監査）を【運 91】の「外部委託に関する考慮事項」に追加する	監査に関する基準を【運 91】（【監１】）に統合
外部委託有識者検討会における特定システムに関するＣＰ策定に関する内容	【運 65】に委託先、再委託先を含むＣＰの策定に関する内容を追加

クラウド基準の統合・整理以外の観点については、以下のように整理する。

論点２　金融機関相互のシステム・ネットワークに関する基準（【運 90-1】）の整理

標記の基準では、全銀システムや統合ＡＴＭ等、金融機関相互のシステム・ネットワークに接続等を行う場合に考慮すべき安全対策を示している。これらのシステムは、外部委託有識者検討会において、「外部委託とは異なる形態」として整理されている（同報告書 p10）。このため、標記基準は外部の統制の中に「金融機関相互のシステム・ネットワークのサービス」というカテゴリを設け、【統 29】として配置する。

なお、コンビニＡＴＭについては、外部の統制の一形態として位置付けることも考えられるが、一部では自社保有のＡＴＭを運用しているケースがあるため、実務基準として整理し、個別のカテゴリ（コンビニＡＴＭ）として配置する。

論点３　共同センターに関する安全対策基準の新設

外部委託有識者検討会報告書（p50）で提言された、共同センター固有のリスク（有事における初動対応。「時間性」の問題。）に対するリスク管理策について、【統 28】として

基準を新設する。

基準小項目は、「共同センターにおける有事の際の安全管理策を講ずる」とし、具体的な対策等を例示することで、各金融機関等が有効に活用できるようにする。

論点４　FinTech に関する基準新設の要否

FinTech に関しては、外部の統制の考え方を前説に記載しており、タイプＡに関しては、通則に包含されるため、基準として追加される要素は無いと判断している。また、タイプＢについても、基準の適用方法が異なるだけで、こちらも基準そのものを新設する要素は無いと判断している。従って、FinTech については、特段基準の変更・新設は行わないこととした。

以上の結果、外部委託関連基準については、以下の構成となる。

基準一覧（基礎基準案） ※外部委託関連のみ抜粋

構成	基準大項目	基準中項目	新基準番号（暫定）	基準小項目
Ⅰ 統制基準	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。
			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。
			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。
			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。
			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。
			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。
		(2) クラウドサービス	統27	重要なシステムにおけるクラウドサービス利用時の管理策を講ずること
		(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
		(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。
Ⅱ 実務基準	9 共同センター	(1) 共同センター	実務基準の新設なし	【統28】とする
	10 FinTech・クラウド関連	(1) FinTech・クラウド関連		クラウド固有部分は【統27】とする（APIは新設しない）
Ⅳ 監査基準	1 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。

Ⅲ 今後の検討について

本日ご説明した内容について、8/22（火）までに事後意見をいただき、基準原案に反映していく。

日程（予定）	内容
8 月 22 日（火）	第 55 回安全対策専門委員会事後意見の締切
9 月 12 日（火）	第 56 回安全対策専門委員会審議　※1
9 月下旬	第 56 回専門委員会事後意見の締切
10 月 17 日（火）	第 57 回安全対策専門委員会審議

※1　ご意見等を踏まえ、第 56 回安全対策専門委員会にて、基準原案を提示する予定

以上

参考　基準【運 87】原文

外部委託管理
外部委託に関する計画

適　用　区　分					参照項目
共	セ	本	提	ダ	外
◎					※

運　87	システムの開発や運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。

システムの開発や運用等で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ことが必要である。

1. システムの開発や運用で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こと。

2. 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) 委託先の選定条件
   (8) 外部委託に関する自社窓口と役割　　等

3. システムの開発や運用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。

【関連ガイドライン等】

システム監査指針	10-1-A　10-1-B　10-1-C
検査マニュアル　システムリスク編	顧保護Ⅱ.4.(1)　Ⅱ.4.(2)　ｵﾍﾟﾘⅢ.3　Ⅲ.5
検査マニュアル　システム統合編	Ⅱ.v

参考　基準【運 87-1】原文

外部委託管理		適用区分					参照項目
外部委託に関する計画		共	セ	本	提	ダ	外
		◎					※

運　87-1	外部委託先の選定手続きを明確にすること。

外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価すること。委託業者の決定にあたっては、責任者の承認を得ること。

1. 委託業者を選定するにあたっては、選定手続きを明確にすることが必要である。

2. 外部委託先を客観的に評価すること。評価する項目としては、以下のような例がある。
   (1) 安定性（財務内容）、健全性
   (2) 組織体制（コンプライアンス体制含む）
   (3) 信頼度および受託実績（類似システムの開発実績、他プロジェクトでの評判等）
   (4) 技術レベル（業務内容の理解度、業界に関する知識、情報収集能力、プロジェクト管理能力、導入サポート力等）
   (5) 委託費と支払い条件
   (6) セキュリティ対策の実施状況（機密保護状況含む）
   (7) 問題発生時の対応力
   (8) 保守体制等
   (9) 各種公的認証の取得状況

3. 委託業者の決定には、最終的には責任者の承認を得ることが必要である。

4. 外部委託先が所有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。

【関連ガイドライン等】

システム監査指針	10-1-B
検査マニュアル　システムリスク編	顧保護Ⅱ.4.(1)　Ⅱ.4.(2)　ｵﾍﾟﾘⅢ.3
検査マニュアル　システム統合編	

参考　基準【運 108】原文（コメント付）

クラウドサービスの利用	適用区分				
	共	セ	本	提	ダ
	◎				

運　108	クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。

クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。
また、事業者の決定にあたっては、責任者の承認を得ること。

1. クラウド事業者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。

2. 明確にすべきクラウドサービスの利用に関する事項としては以下の例がある。
(1) 利用目的
(2) 利用業務範囲
(3) 利用形式
(4) 利用期間
(5) 利用費用
(6) リスクの管理方法
(7) クラウド事業者の選定条件
(8) クラウドサービスに関する自社窓口と役割 等

3. クラウド事業者を客観的に評価すること。
クラウドサービスを利用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、その実現が可能なクラウド事業者を選定すること。その際、クラウド事業者の資質・業務遂行能力に関する情報や、クラウド事業者の内部統制や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（注）。評価にあたっては、クラウド事業者によって契約前の情報開示に消極的なケースもあるが、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。
（注）資源共有型であるパブリッククラウドの場合、クラウド事業者によっては、標準的な契約・SLA等の内容に関し個社からの変更要求に応じないことも想定されるため、各金融機関が特に重要であると判断した事項については、こうした変更要求の交渉が可能であるかを事前に確認しておくことが必要である。
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、クラウド事業者の公開情報や、業界における評判や実績等による客観的な評

コメント [A1]: 外部委託に関する基準の通則化のため、クラウドに関する記載を外部委託に変更。
以下、同様。

コメント [A2]: 外部委託に関する基準の通則化のため、「利用」の表現を「委託」に変更。

コメント [A3]: 外部委託に関する有識者検討会報告書の提言に従い、「再委託先」を含む記載に変更。

コメント [A4]: 前説 p25。
２．統制。
(2) 外部の統制。
③ 基本形（２者間構成）における各論。
c. クラウドサービス。
に記載の内容のため、削除。

価を行うことも可能である。

評価する事項としては、以下のような例がある。

(1) クラウド利用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での評判等）

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（クラウド事業者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) 情報開示姿勢

(6) 立入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) データの所在（データが保管される場所、または保管の可能性がある場所）

(8) 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

(9) 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）、日本語での対応）

(10) 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）とクラウド事業者側が提示する損害賠償・補償上限額とのバランス

(11) サービス利用廃止時の対応（ベンダーロックインリスク対応、データ消去等）

ただし、契約の中断・終了に伴うシステム移行作業（移行データの抽出方法と実際の移行作業内容）については、サービス利用前に把握することが望ましい。

(12) 個人データの取扱いの全部または一部を事業者に行わせることを内容とする契約を締結する場合は、「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」に準拠対応可能か

(13) 委託費と支払い条件

なお、(5)情報開示姿勢の中でも、リスク管理に直結する事項（注）については、十分に把握しておくことが必要である。このため、こうした情報の開示が必ずしも十分でないクラウド事業者と契約してよいか、慎重な判断が必要である。

（注） リスク管理に直結する事項には以下のようなものがある。

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

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 等

4. 紛争が生じた際にどの国の法律が適用されるのか、また、現地の公権力による捜査目的で、

コメント [A5]: 外部委託に関する有識者検討会報告書の提言に従い削除

コメント [A6]: 記載箇所の変更
上記(5)の内容のため、(5)の直下に移動

データが差し押えられるといった場合に、業務の継続性に影響がないかといった点には十分に配慮する必要がある。特に、重要業務を委ねる場合には、データが分散格納されている場合を含めて、データの所在を把握することが重要になる。

高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域（国、州等）を把握する必要がある。

勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する必要がある。

インシデント発生時にデータセンターへの立入が必要になる場合や立入監査を行う際には、具体的な所在地を把握する必要がある。

ただし、委託する業務の重要度に応じて、データの所在について把握する必要性や把握の詳細度に差異が生じることはあり得る。したがって、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には、データの所在地に関する情報の把握について省略することも可能である。

コメント [A7]: 外部委託に関する有識者検討会報告書の提言に従い削除。
なお、監査に関する内容については、監１において記載されている。

5. クラウド事業者との間で係争が生じた場合の準拠法や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、クラウド事業者の選定にあたって評価すべきリスクとしては、以下のようなものがある。

(1) 現地の各種法制や裁判制度の把握と分析
(2) 現地での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

6. クラウド事業者の決定には、責任者の承認を得ることが必要である。

7. クラウド事業者が提供するサービス等の導入に際しては、必要に応じて【運 72、運 73】も参照のこと。

コメント [A8]: 外部委託に関する基準の通則化のため、サービス利用に関する内容以外の記載を追記。

【関連ガイドライン等】

システム監査指針	10-1-A　10-1-B　10-1-C　10-2-A
検査マニュアル　システムリスク編	顧保護Ⅱ.4.(1)　Ⅱ.4.(2)　ｵﾍﾟﾘⅢ.3　Ⅲ.5.(1)　Ⅲ.5.(2)
検査マニュアル　システム統合編	

参考　新基準【統 21】原案（コメント付）

外部の統制	適用区分				
利用検討時	共	セ	本	提	ダ
	◎				

統　21	外部委託を行う場合は、事前に利用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。

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。

2. 外部に委託する業務として、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) ハードウェア及び回線の設置、入替、撤去
(5) 入力データの作成（端末オペレーションを含む）
(6) 記録媒体、ドキュメント及び帳票等の作成、保管、配送、廃棄
(7) 館内、構内及び店内の警備
(8) 電源、空調、防犯等設備の管理、保守
(9) 集中監視（CD・ATM 等）
(10) CD・ATM の現金等の管理

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。

3. 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（再委託先を含む）の選定条件
(8) 外部委託に関する自社窓口と役割 等

コメント [A1]:【運 87】、【運 87-1】及び【運 108】の「基準小項目」を統合。

コメント [A2]:【運 87】、【運 87-1】及び【運 108】の「適用にあたっての考え方」を統合。

コメント [A3]:【運 87】1.【運 87-1】1.及び【運 108】1.を統合。

コメント [A4]:【運 88】2.

コメント [A5]:【運 87】2.及び【運 108】2.を統合。

4. システムの開発や運用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。

5. 外部委託先（再委託先を含む）を客観的に評価すること。

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、その実現が可能な外部委託先を選定すること。その際、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、外部委託先によって契約前の情報開示に消極的なケースもあるが、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。

評価する事項としては、以下のような例がある。

(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での評判等）
  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) 情報開示姿勢
  情報開示姿勢の中でも、リスク管理に直結する事項については、十分に把握しておくことが必要である。このため、こうした情報の開示が必ずしも十分でない外部委託先と契約してよいか、慎重な判断が必要である。
  リスク管理に直結する事項には以下のようなものがある。
  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
  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 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）、日本語での対応）
(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

コメント [A6]: 【運 87】3.

コメント [A7]: 【運 87-1】2及び【運 108】3.を統合したうえで、整理・通則化.

コメント [A8]: 左記下線部分が該当.
＜参考＞【運 87-1】.
2. 外部委託先を客観的に評価すること。評価する項目としては、以下のような例がある。.
(1) 安定性（財務内容）、健全性.
(2) 組織体制（コンプライアンス体制含む）.
(3) 信頼度および受託実績（類似システムの開発実績、他プロジェクトでの評判等）.
(4) 技術レベル（業務内容の理解度、業界に関する知識、情報収集能力、プロジェクト管理能力、導入サポート力等）.
(5) 委託費と支払い条件.
(6) セキュリティ対策の実施状況（機密保護状況含む）.
(7) 問題発生時の対応力.
(8) 保守体制等.
(9) 各種公的認証の取得状況.

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）
ただし、契約の中断・終了に伴うシステム移行作業（移行データの抽出方法と実際の移行作業内容）については、契約の締結前に把握することが望ましい。
(11) 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」に準拠対応可能か
(12) 委託費と支払い条件

6. 外部委託先との間で係争が生じた場合の準拠法や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、外部委託先の選定にあたって評価すべきリスクとしては、以下のようなものがある。
(1) 現地の各種法制や裁判制度の把握と分析
(2) 現地での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

コメント [A9]: 【運 108】5.を通則化

7. 外部委託先の決定には、責任者の承認を得ることが必要である。

コメント [A10]: 【運 87-1】3.

8. 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。

コメント [A11]: 【運 87-1】4及び【運 108】7.を統合

【資料３－１】
平成 29 年８月８日
公益財団法人　金融情報システムセンター

安全対策基準「読みやすさ」対応について

Ⅰ．対応の背景

『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：本書という）の基準項目数は、初版の 226 基準から現在は 311 基準まで増えているが、改訂を重ねる中で必ずしも記述の様式・表現の統一がなされていなかった。また、基準項目の構成（カテゴリ）が、自機関のホスト・勘定系システムにおける安全対策を実施することを前提とした構成となっており、特に新しい利用者にとっては戸惑うと思われる点も多く、「読みやすさ」に対する懸念がある。

今後、「リスクベースアプローチ」に基づき各金融機関が安全対策を決定するうえで、本書の記述内容を正しく理解する必要があるが、その上でも「読みやすさ」は重要となってきている。

Ⅱ．対応の内容

上記を踏まえ本書の「読みやすさ」の向上を目的とした変更、修正を実施したい。ただし、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する。**

【読みやすさ対応の内容】

①	基準の再構成	・基準のカテゴリ変更、並び替え等の変更をおこなう。 ・詳細は以下資料を参照。 【資料３－２】安全対策基準の再構成について 【資料３－５】新基準構成案
②	読みやすさ向上	・基準本文（主に解説部分）における対策・例示の明確化、記述方法の統一等の変更、修正をおこなう。 ・詳細は以下資料を参照。 【資料３－３】「読みやすさ」に関する対応 【資料３－４】安全対策基準・解説の記載ルール（案） 【資料３－６】基準原案サンプル

Ⅲ．今後の進め方

本日の内容について 8/22（火）までに事後意見をいただき、基準原案・構成案に反映していく。
※基準原案は８月末までに事前送付し、その後約１ヶ月程度で委員の皆様にご確認いただく予定。

～8/22	第 55 回安全対策専門委員会　事後意見の締切
8/25～8/31	基準原案の事前配布（複数回に分けてメール送付）
9/12	第 56 回安全対策専門委員会 ・基準原案（全文）の配布、事後意見の共有
～9/29	基準原案等についての事後意見の締切

以　上

【資料３－２】
平成 29 年８月８日
公益財団法人　金融情報システムセンター

安全対策基準の再構成について

Ⅰ．基本的な考え方

近年の金融情報システムにおいては、ネットワーク化の進展とともに、サイバー攻撃をはじめとする犯罪が巧妙化・大規模化するリスクが高まっている。また、外部委託の進展に加え、クラウドサービスや FinTech 企業の出現等により、システムの形態や利用するサービス及び安全対策の当事者が多様化しており、外部の統制の重要度が増加している。

こうした状況を踏まえ、今回の安全対策基準の改訂においては、統制面の安全対策を明示するため、基準の構成を「統制基準」「実務基準」「設備基準」「監査基準」に分類する予定であるが、安全対策の当事者にとって参照する機会が多い「統制基準」「実務基準」については、利便性確保の観点から並び順等を再構成することとしたい。

Ⅱ．統制基準の再構成

以下のとおり、基準項目の並び順を変更する。

- 安全対策の主たる実施者の階層を考慮し、主に経営層による承認を伴う基準項目、管理者が実施する基準項目を、担当者が実施する基準項目の前に設置する。
- 安全対策の実施に時間的な順序性（事前、事後等）がある基準項目については、順序性を考慮して並び順を見直す。

Ⅲ．実務基準の再構成

以下のとおり、実務基準の項目を再構成する。

１．情報セキュリティに関する基準の分類

金融情報システムの関係者が拡大する中、これら関係者の共通の関心事としては、顧客データの保護や、システムへの不正侵入防止にあると考えられる。そこで、情報セキュリティに関する基準をまとめて記載する。

２．システム運用に関する基準の再構成

共同センター利用をはじめシステム運用業務の外部委託化が進展していることに対応し、安全対策の実施者が明確になるよう、システムの運用に関する基準を以下のとおり再構成する。

基準大項目	内容	
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。	
運行管理	日々のシステム運行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）が実施する。	システム運用を外部委託した場合、金融機関が、「外部の統制」基準に基づき、委託先の実施状況を、モニタリングする。
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）が実施する。	
システムの利用	システムの利用に関する基準であり、利用部門（金融機関）が実施する。	
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。	

３．システムの信頼性向上策の分類

システムの開発・変更時に考慮すべき、信頼性向上策等の非機能要件を、「システムの信頼性向上策」としてまとめて記載する。

４．個別の業務・サービスを対象とした基準の分類

適用対象が個別の業務やサービスに限定される基準については、「個別業務・サービス」として分類する。これにより、対象外の業務・サービス及び関連するシステムにおいては、当該基準適用の検討を省略することを可能とする。

Ⅳ．基準の再構成において判明した課題の対応（基準変更）について

上記のとおり、統制基準の再構成を行ったところ、以下の課題が判明したことから、基準項目の一部を変更することとしたい。

次回専門委員会において、以下の基準の改訂原案を提示するのでご検討いただきたい。

統1（運1） セキュリティ管理方法を具体的に定めた文書を整備すること。

【課題】

- 本基準項目は、安全対策実施の根拠となる規程類の整備に関する基準項目であるが、「セキュリティポリシー」、「セキュリティスタンダード」についての記述はあるものの、「金融機関における外部委託に関する有識者検討会」報告書に記載されている上位規程（システムリスク管理方等）についての記述がない。
- リスク評価に関する記述が前説に記載されたリスクベースアプローチの記述と重複している。また、セキュリティ管理の実施に関する考慮事項が含まれている。
- 本基準項目では、「マニュアルや手順書」についても記述しており、統４（運 10）「各種規定を整備すること」と内容が重複している。

【対応案】

- システムリスク管理方針についての記述を追記する。
  「セキュリティポリシー及びセキュリティスタンダードの策定にあたっては、システムリスク管理方針等の上位規程と整合をとること。」
- リスク評価に関する記述を削除する。また、セキュリティ管理実施に関する記述は他の基準項目に移動するか削除[1]する。
- マニュアルや手順書に関する記載を、統４（運 10）に移行する。

統2（運2） セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。

【課題】

統１の規程類の評価・改訂について記述しているが、他の基準項目（統 13 や実 58）では同一基準項目内に記述している。

【対応案】

他の基準と記述内容の整合性をとるため、統２を統１に統合する。

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。

【課題】

安全対策にかかる重要事項が決定される「中長期計画」の策定に関する記述がない。

【対応案】

中期経営計画に沿った中期システム計画を策定することについて追記する。

以　上

[1] 他の基準項目と重複する内容の場合は削除する。

【資料３－３】
2017 年８月８日
公益財団法人　金融情報システムセンター

「読みやすさ」向上に関する対応

利用者の「読みやすさ」向上のため、基準の記述ルールを明確にして標準化を図る。

Ⅰ．対応方針

今回の改訂に合わせ、「読みやすさ」の向上を目的に対応方針をまとめた。

方針１：　実施すべき「安全対策」（…すること、必要がある）と「安全対策の例示」を明確に区分する。

【記述例】

「・・以下のようなことを考慮して手順を明確にすることが必要である。

(1)業務開始時の手順

(2)影響を局所化する縮退等」

【対応内容および対応例】

対策と例示を分離する。

「手順を明確にすることが必要である。明確にする事項としては以下の例がある。

(1)業務開始時の手順

(2)影響を局所化する縮退等」

方針２：　実施すべき「安全対策」を示す語尾を統一する。

【記述例】

「・・紛失、盗難、破損に関し、利用者が被る可能性のある損失及び責任を利用者に対して明示すること。」

【対応内容および対応例】

実施すべき「安全対策」を示す語尾を「必要である」に統一したうえで、解説部分の語尾は以下の３種類に整理する。

① 実施すべき「安全対策」　⇒　・・・が必要である。

② ベストプラクティス　　⇒　・・・が望ましい。

③ 例示・参考　　⇒　・・・が考えられる。・・・がある。

「・・紛失、盗難、破損に関し、利用者が被る可能性のある損失及び責任を利用者に対して明示することが必要である。」

方針３：　例示内の語尾を統一する。

【記述例】

「・・以下のような例がある。　①・・・する必要がある。」

【対応内容および対応例】

「・・以下のような例がある。　①・・・する。」

方針４：　理解するのが困難な文章または誤解を与えやすい表現を修正する。

【記述例】

「また、円滑な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・・・」

【対応内容および対応例】

今回の対応においては、明らかに問題がある場合かつ簡易な修正のみを対象とし、関係者の合意形成に時間を要する修正はおこなわず、次回改訂における検討課題としたい。

「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・・・」

方針５：　内容が古くなっている箇所を修正する。

【記述例】

「2.・・・ＩＣカード化等の高セキュリティ技術の導入がある。」

【対応内容および対応例】

今回の対応においては、簡易かつ影響が小さいと想定される修正のみを対象とし、一定の調査が必要な修正や、関係者の合意形成に時間を要する修正はおこなわず、次回改訂における検討課題としたい。

「2.・・・ＩＣカード化等の~~高セキュリティ技術の~~導入がある。」

Ⅱ．基準（・解説）の標準化

基準および解説の記述ルールを明確にし、将来にわたって「読みやすさ」を維持していく。

別紙：【資料３－４】安全対策基準・解説の記述ルール（案）

以　上

【資料３－４】
平成 29 年８月８日
公益財団法人　金融情報システムセンター

【安全対策基準・解説の記述ルール（案）】

【基準大項目】
【基準中項目】

【適用区分】 【基準分類】 基礎

【基準番号】 【基準小項目】

【適用にあたっての考え方】

【基準項目の目的、内容説明、具体例等の解説】

＜用語説明＞
〇〇〇〇は・・・・・・・・・を指す。

1.・・・・・・・・□□□□することが必要である。また・・・・・・・・望ましい。

□□する事項としては以下の例がある。
(1)・・・・・
(2)・・・・・

2..・・・・・・・・△△△することが必要である。
＜参照先＞
△△△については【実 xx】を参照のこと。

＜〇〇する事項としては以下の例がある。＞
(1)・・・・・する。
(2)・・・・・する。

（参考）

基礎基準か付加基準を明記する。

〇〇を～すること。〇〇の～をすること。
に記述を統一する。（目的語を明確にする）（※）

〇〇〇（実施目的）のため、・・・・・をすること。
に記述を統一する。（※）

用語説明は、＜用語説明＞といった形式で記述し、明確にする。（番号は付さない）

実施する「対策」については、要求レベルに応じて
①「～必要である」 ②「～望ましい」 ③考えられる　等
に語尾を統一する。（※）

解説欄に実施する「対策」の記述がない場合は、「適用にあたっての考え方」の内容を「対策」として補記する。

例示は、「以下の例がある。(1)(2)・・・」といった形式で記述し、明確にする。（番号は付さない）

関連する基準を参照する場合は、＜参照先＞といった形式で記述し、明確にする。（番号は付さない）

例示内に、実施する対策の事例を記述する場合は、語尾を「～する」「～をおこなう」に統一する。（実施する「対策」と語尾を区別する）

（※）は従来から適用されている記述ルール

【資料３－５】
平成29年８月８日
公益財団法人　金融情報システムセンター

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
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。 ~~セキュリティ管理方法を具体的に定めた文書を整備すること。~~	運1・2
			統2	~~セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。~~（統1に統合）	―
		(2)　組織体制	統3	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。 ~~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	セキュリティ管理態勢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	各種業務の手順書規定を整備すること。	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。	
			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。	
			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。	
			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。	
			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。	
			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。	
		(2)　クラウドサービス	統27	重要なシステムにおけるクラウドサービス利用時の管理策を講ずること。	
		(3)　共同センター	統28	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	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	~~暗証番号・パスワード等は~~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化すること。	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	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	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）の資格付与およ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

（前回構成案）

構成	基準大項目	基準中項目
Ⅰ　統制基準	1　内部の統制	(1)　方針・規定
		(2)　組織体制
		(3)　サイバー攻撃対応態勢
		(4)　人材（要員・教育）
	2　外部の統制	(1)　方針・計画
		(2)　契約・業務管理
		(3)　金融機関相互のシステム・ネットワークのサービス
Ⅱ　実務基準	1　入退管理	(1)　入退館（室）管理
	2　運用管理	(1)　マニュアルの整備
		(2)　アクセス権限の管理
		(3)　オペレーション管理
		(4)　入力管理
		(5)　データファイル管理
		(6)　プログラムファイル管理
		(7)　コンピュータウイルス対策
		(8)　ネットワーク設定情報管理
		(9)　ドキュメント管理
		(10)　帳票管理
		(11)　出力管理
		(12)　取引の管理
		(13)　暗号鍵の管理
		(14)　厳正な本人確認の実施
		(15)　CD・ATM等及び無人店舗の管理
		(16)　渉外端末の管理
		(17)　カード管理
		(18)　顧客データ保護
		(19)　資源管理
		(20)　外部接続管理
		(21)　機器の管理
		(22)　運行監視
		(23)　コンピュータ室・データ保管室の管理
		(24)　障害時・災害時対応策
		(25)　コンティンジェンシープランの策定
	3　ハードウェア・ソフトウェア管理	(1)　ハードウェア・ソフトウェア管理

【資料３－５】
平成29年８月８日
公益財団法人　金融情報システムセンター

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
			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
		(4) 厳正な本人確認の実施	実34	本人確認を行うこと。	運44
		(5) 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) ドキュメント管理	実63	ドキュメントの作成手順を定めること。	運70
			実64	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
		(5) 障害の早期回復機能	実112	障害時の縮退・再構成機能を設けること。	技22
			実113	取引制限機能を設けること。	技23
			実114	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	顧客に対してカード取引に関する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	不正使用を防止すること。	運103
			実85	不正使用を早期発見すること。	運104
			実86	安全対策に関する情報開示をすること。	運105
			実87	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化すること。	運106
		(3) 渉外端末の管理	実41	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	監視体制を明確にすること。	運46
			実38	防犯体制を明確にすること。	運47
			実39	障害時・災害時の対応方法を明確にすること。	運48
			実40	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	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	出店先の選定基準を明確にすること。	運93
			実75	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	障害時・災害時対応手順を明確にすること。	運95
			実77	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	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	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	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) 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
Ⅲ 設備基準					
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

（前回構成案）

構成	基準大項目	基準中項目
	3 システム開発・変更	(2) システム開発・変更管理
		(3) ドキュメント管理
		(4) パッケージの導入
		(5) システムの廃棄
	4 各種設備管理	(1) 保守管理
		(2) 資源管理
		(3) 監視
	5 インストアブランチ	(1) インストアブランチ
	6 コンビニATM	(1) コンビニATM
	7 デビットカード	(1) デビットカード・サービスの安全性確保
		(2) 顧客保護
		(3) 顧客への注意喚起
	8 オープンネットワークを利用した金融サービス	(1) インターネット、モバイル
		(2) 電子メール
	9 共同センター	(1) 共同センター
	10 FinTech・クラウド関連	(1) FinTech・クラウド関連
	11 ハードウェアの信頼性向上対策	(1) ハードウェアの障害予防策
		(2) ハードウェアの予備
	12 ソフトウェアの信頼性向上対策	(1) 開発時の品質向上対策
		(2) メンテナンス時の品質向上対策
	13 運用時の信頼性向上対策	(1) 運用時の信頼性向上対策
	14 障害の早期発見・早期回復	(1) 障害の早期発見
		(2) 障害の早期回復
	15 災害時対策	(1) バックアップサイト
	16 データ保護	(1) 漏洩防止
		(2) 破壊・改ざん防止
		(3) 検知策
	17 不正使用防止	(1) 予防策(アクセス権限確認)
		(2) 予防策(利用範囲の制限)
		(3) 予防策(不正・偽造防止対策)
		(4) 外部ネットワークからのアクセス制限
		(5) 検知策
		(6) 対応策
	18 不正プログラム防止	(1) 防御策
		(2) 検知策
		(3) 復旧策
Ⅲ 設備基準		
Ⅳ 監査基準	1 システム監査	(1) システム監査

【基準原案サンプル】

内部の統制
方針・規定

適　用　区　分				
共	セ	本	提	ダ
◎				

統 5	セキュリティ遵守状況を確認すること。

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、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ること。

1. コンピュータシステムを円滑かつ適正に運用するため､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、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ることが必要である。

2. セキュリティ遵守状況を確認するタイミングとしては、以下のようなものがある。
   (1) 新しいシステム及びサービスの導入時
   (2) 既存のシステム及びサービスに対して定期、不定期
   (3) セキュリティ関連文書に変更があった時
   (4) 異動等により人員の配置変更があった時

3. 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、セキュリティ対策及びセキュリティ遵守状況を把握しておくことが望ましい。

4. セキュリティ遵守状況の確認結果を評価し、セキュリティ関連文書の改訂に反映することが必要である。【運２】

5. セキュリティ遵守状況の確認結果を評価し、セキュリティ教育の内容等を見直すことが必要である。【運 80】

内部の統制
方針・規定

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 5	セキュリティ遵守状況を確認すること。

コンピュータシステムを円滑かつ適正に運用するため、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、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ること。

1. コンピュータシステムを円滑かつ適正に運用するため、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、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ることが必要である。

   セキュリティ遵守状況を確認するタイミングとしては、以下の例がある。
   (1) 新しいシステム及びサービスの導入時
   (2) 既存のシステム及びサービスに対して定期、不定期
   (3) セキュリティ関連文書に変更があった時
   (4) 異動等により人員の配置変更があった時

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、セキュリティ対策及びセキュリティ遵守状況を把握しておくことが望ましい。

3. セキュリティ遵守状況の確認結果を評価し、セキュリティ関連文書の改訂に反映することが必要である。【運２】

4. セキュリティ遵守状況の確認結果を評価し、セキュリティ教育の内容等を見直すことが必要である。【運 80】

運用管理
ドキュメント管理

適 用 区 分				
共	セ	本	提	ダ
◎				

実 23	保管管理方法を明確にすること。

不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理すること。

1. ここでいう運用管理におけるドキュメントとは、コンピュータセンターにおける運用管理に必要なオペレーションフロー、操作指示書、システム関連資料、及び端末操作マニュアル等を指している。

2. ドキュメントの管理方法として、以下のような例がある。
   (1) システム開発部門から業務を引き継ぐ場合は、定められた手続きに従いドキュメントの引渡しを受ける。
   (2) 追加、変更等が発生した場合は、定められた手続きに従い更新する。
   (3) 各種ドキュメントは、管理簿等で管理を行う。
   (4) 重要なドキュメントは、定められた手続きに従い、施錠可能なキャビネット等に保管する。
   (5) 他部門からの閲覧依頼に対しては、定められた手続きに従い行う。
   (6) ユーザーへ引渡しを行う場合は、定められた手続きに従い行う。
   (7) ドキュメントごとの保存期間を明確にする。

3. ペーパーによらないドキュメント（フロッピーディスク等）についても、上記 2.と同様に取り扱うことが必要である。

4. 重要なドキュメントの複写・複製については、管理方法を明確にしておくことが必要である。

運用管理
ドキュメント管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実 23	ドキュメントの保管管理方法を明確にすること。

不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理すること。

＜用語説明＞

ここでいう運用管理におけるドキュメントとは、コンピュータセンターにおける運用管理に必要なオペレーションフロー、操作指示書、システム関連資料、及び端末操作マニュアル等を指している。

1. 不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理することが必要である。

ドキュメントの管理方法として、以下の例がある。

(1) システム開発部門から業務を引き継ぐ場合は、定められた手続きに従いドキュメントの引渡しを受ける。
(2) 追加、変更等が発生した場合は、定められた手続きに従い更新する。
(3) 各種ドキュメントは、管理簿等で管理を行う。
(4) 重要なドキュメントは、定められた手続きに従い、施錠可能なキャビネット等に保管する。
(5) 他部門からの閲覧依頼に対しては、定められた手続きに従い行う。
(6) ユーザーへ引渡しを行う場合は、定められた手続きに従い行う。
(7) ドキュメントごとの保存期間を明確にする。

2　ペーパーによらないドキュメント（電子文書等）についても、上記 1.と同様に取り扱うことが必要である。

3　重要なドキュメントの複写・複製については、管理方法を明確にしておくことが必要である。

運用管理
データファイル管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 15	授受・管理方法を定めること。

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、データファイルの授受、保管は定められた方法によって行うこと。

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 等を指す。

2. データファイルはその重要度に応じた保管・管理方法を明確にする必要がある。

3. データファイルの授受・保管管理方法として、以下のような例がある。
   (1) 受渡し、持出し及び廃棄方法を定めるとともに、責任者を明確にする。
   ① データファイルの受渡しにおいては、不正使用、改ざん、紛失等を防止するため、以下のような項目を明確にして行うことが必要である。
      a. 使用目的
      b. 使用日時
      c. 使用者名
      d. 責任者の承認
      e. 入出庫日時
      f. 入出庫担当者名
   ② データファイルを外部に持ち出す場合、データ漏洩を防止するため、データの持出しに関する制限や管理方法を明確に定めておくことが必要である。
   ③ データファイルの廃棄においては、誤消去、データ漏洩等を防止するため、以下のような項目を明確にして行うことが必要である。【運 74、運 75】
      a. ファイル管理簿等による保存期間
      b. データファイルの機密度に応じた廃棄方法（消磁、裁断等）
      c. 廃棄確認方法
      d. 廃棄理由
      e. 廃棄日時
      f. 廃棄責任者
   ④ 磁気ディスクの障害等でディスクを交換または廃棄する場合は、適切な情報漏洩防止策を講ずることが必要である。【運 74、運 75】

運用管理
データファイル管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 15	データファイルの授受・管理方法を定めること。

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、データファイルの授受、保管は定められた方法によって行うこと。

＜用語説明＞

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 等を指す。

1. データファイルはその重要度に応じた保管・管理方法を明確にする必要がある。

データファイルの授受・保管管理方法として、以下の例がある。

(1) 受渡し、持出し及び廃棄方法を定めるとともに、責任者を明確にする。

① データファイルの受渡しにおいては、不正使用、改ざん、紛失等を防止するため、以下のような項目を明確にする。

a. 使用目的
b. 使用日時
c. 使用者名
d. 責任者の承認
e. 入出庫日時
f. 入出庫担当者名

② データファイルを外部に持ち出す場合、データ漏洩を防止するため、データの持出しに関する制限や管理方法を明確にする。

③ データファイルの廃棄においては、誤消去、データ漏洩等を防止するため、以下のような項目を明確にする。【運 74、運 75】

a. ファイル管理簿等による保存期間
b. データファイルの機密度に応じた廃棄方法（消磁、裁断等）
c. 廃棄確認方法
d. 廃棄理由
e. 廃棄日時
f. 廃棄責任者

④ 磁気ディスクの障害等でディスクを交換または廃棄する場合は、適切な情報漏洩防止策を講ずる。【運 74、運 75】

実 17	バックアップを確保すること。

重要なデータファイルの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。

1. 障害や災害等の発生により重要なデータファイルに破損等が発生した場合、そのファイルを早期に回復させる必要があるため、バックアップを取得し、保管管理方法を明確にすることが必要である。

なお、バックアップの取得、保管管理方法については、コンティンジェンシープランと整合性のとれたものとすること。

2. バックアップを取得するにあたっては、以下のような点に留意する必要がある。
   (1) 適切な世代管理レベル（二世代前、三世代前まで等）を設定すること。
   (2) 回復に要する時間、及びその間の影響を考慮して、取得サイクルを定めておくこと。
   (3) バックアップが正常に取得できていることを確認すること。
   (4) 必要に応じてバックアップ取得対象範囲の見直しを行うこと。例えば、データベースの拡張やファイルの新設を行った場合等がある。

3. バックアップを取得するにあたっては、データファイルの種類や更新タイミング等に応じて適切な保管サイクルを設定すること。保管にあたっては以下の方法がある。
   (1) 分散保管
   バックアップファイルを同一建物内もしくは比較的近距離の場所で保管する（火災等、局所災害に有効）。
   (2) 隔地保管
   バックアップファイルを遠距離の場所で保管する（地震等、大規模災害に有効）。

保管場所の選定にあたっては、本番ファイル保管場所（現有システム保有場所）とリスク要因（火災、地震、停電等）を共有しないこと、及び被災時の復旧に際しての現有システムへのファイル移送時間の考慮等も含め、総合的に判断することが望ましい。特に経営存続のために重要なデータファイルについては、大規模災害も想定して検討することが必要である。

また、保管を外部に委託する場合は、信頼性、安全性、利用体制（保管データを必要時にいつでも利用可能か、等）についても考慮する必要がある。

なお、定められた保管期間前の持出しにあたっては部門責任者の承認を得て行い、持出し記録については所定期間保存する必要がある。

4. バックアップデータの保管方法については、【運 25】も参照のこと。

5. イントラネットへの業務の依存度が高まっていることから、これらネットワーク上のデータ

についても、重要度を勘案し、バックアップを確保することが望ましい。

実 17	データファイルのバックアップを確保すること。

重要なデータファイルの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。

1. 障害や災害等の発生により重要なデータファイルに破損等が発生した場合、そのファイルを早期に回復させる必要があるため、バックアップを取得し、保管管理方法を明確にすることが必要である。

なお、バックアップの取得、保管管理方法については、コンティンジェンシープランと整合性のとれたものとすることが必要である。

バックアップを取得するにあたっての留意点として、以下のような例がある。

(1) 適切な世代管理レベル（二世代前、三世代前まで等）を設定すること。
(2) 回復に要する時間、及びその間の影響を考慮して、取得サイクルを定めておくこと。
(3) バックアップが正常に取得できていることを確認すること。
(4) 必要に応じてバックアップ取得対象範囲の見直しを行うこと。例えば、データベースの拡張やファイルの新設を行った場合等がある。

2. バックアップを取得するにあたっては、データファイルの種類や更新タイミング等に応じて適切な保管サイクルを設定することが必要である。保管にあたっては以下の方法がある。

(1) 分散保管

バックアップファイルを同一建物内もしくは比較的近距離の場所で保管する（火災等、局所災害に有効）。

(2) 隔地保管

バックアップファイルを遠距離の場所で保管する（地震等、大規模災害に有効）。

保管場所の選定にあたっては、本番ファイル保管場所（現有システム保有場所）とリスク要因（火災、地震、停電等）を共有しないこと、及び被災時の復旧に際しての現有システムへのファイル移送時間の考慮等も含め、総合的に判断することが望ましい。特に経営存続のために重要なデータファイルについては、大規模災害も想定して検討することが必要である。

また、保管を外部に委託する場合は、信頼性、安全性、利用体制（保管データを必要時にいつでも利用可能か、等）についても考慮する必要がある。

なお、定められた保管期間前の持出しにあたっては部門責任者の承認を得て行い、持出し記録については所定期間保存する必要がある。

＜参照先＞

バックアップデータの保管方法については、【運 25】も参照のこと。

3. ~~イントラネットへの業務の依存度が高まっていることから、これらネットワーク~~イントラネット上のデータについても、重要度を勘案し、バックアップを確保することが望ましい。

【事後送付資料】
平成 29 年 8 月 2 日更新
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）

【事後送付資料】
平成 29 年 8 月 2 日更新
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ってくる。

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、事業もしくは事業者に対し、現時点ではこれらを定義した画一的な名称が存在しない。本書においては、これら革新的な金融関連サービスを提供する事業者を「FinTech 企業等」と表現している。

[2] 相互扶助の精神から、地域の繁栄等を目的とする金融機関など、「企業価値の最大化」には多様な目的が含まれる。

[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。

【事後送付資料】
平成 29 年 8 月 2 日更新
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

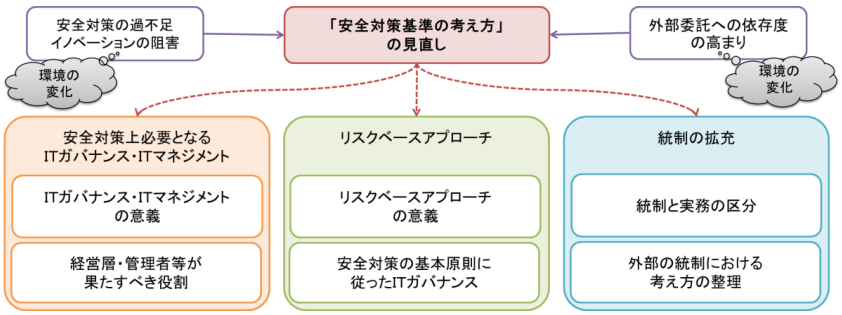
安全対策基準を取り巻く環境変化と対応

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、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を占めるようになってきた。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。

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、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。

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）

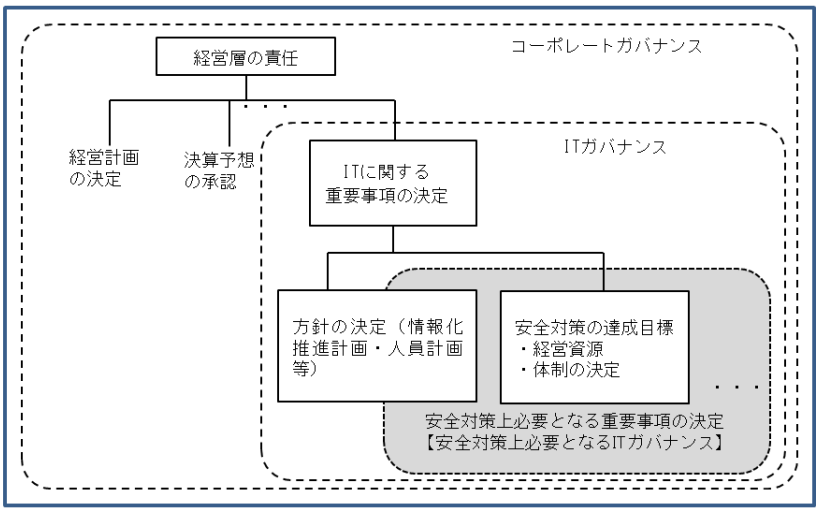
【事後送付資料】
平成 29 年 8 月 2 日更新
公益財団法人 金融情報システムセンター

(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（費用・配分方針等）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

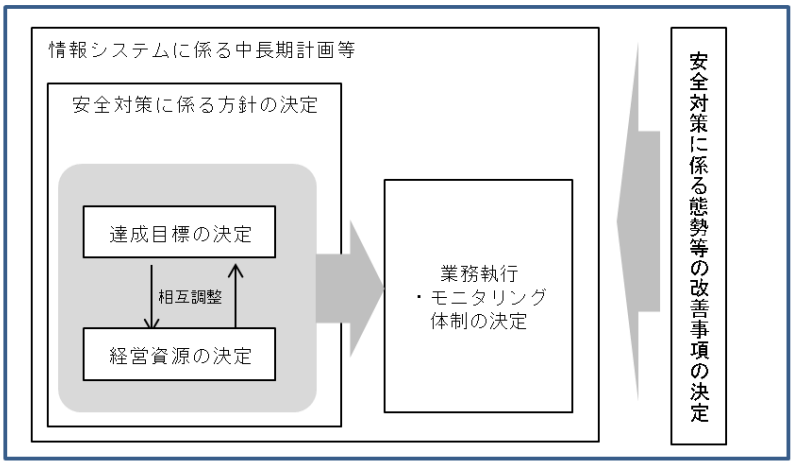
経営層は、安全対策の達成目標及び投下する経営資源の内容を踏まえ、必要に応じて、システム部門等の業務執行体制を決定する。

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

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。

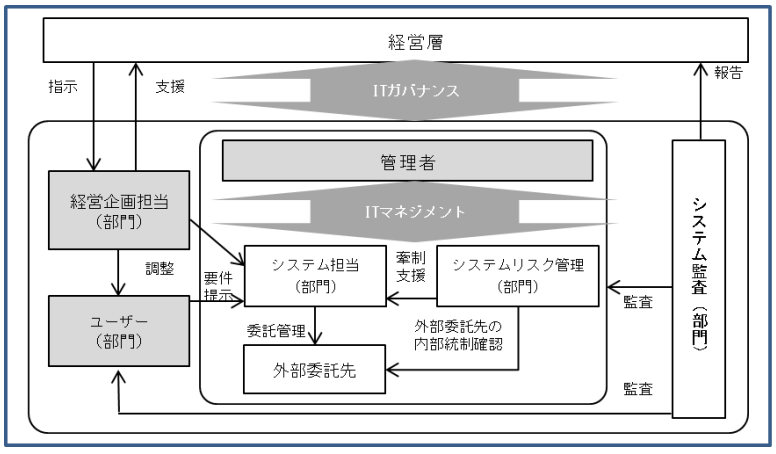
・内部規程・組織体制等の整備・見直し
・個々の情報システムに対する安全対策の決定
・安全対策上必要となる情報の経営層への報告

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）

金融機関等の本社主管部署で、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。



［図表 4］情報システムの安全対策に携わる関係者（例）

(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、大きな比率を占めてきたその他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。
- 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、海外先進諸国の動向も踏まえ、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、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、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。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。

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。つまり、安全対策の達成目標は、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 ガバナンスを発揮して、決定されることが重要である。

(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。

【事後送付資料】
平成 29 年 8 月 2 日更新
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、損失額を内部的に算定できるからである。

・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。

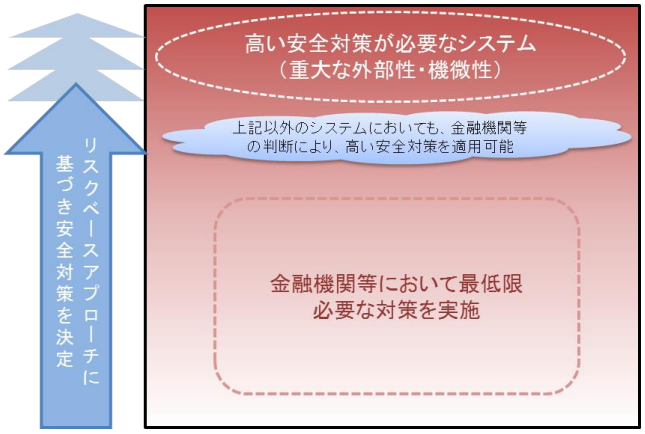
・仮に、一般の個人情報と機微情報（要配慮個人情報を含む）が同一に扱われてしまった場合には、金融機関等のほとんどすべてのシステムに存在している個人情報が、この機微情報（要配慮個人情報を含む）に影響されて適切な水準を超えた安全対策目標が設定され、資源の過剰配分が行われるおそれがある。

・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。

(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、安全対策の目標を適切かつ包括的に決定する。この際、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、

[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。

削除: 評価し、その

削除: された

削除: 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、

削除: 原則として、経営層みずからが、

削除: すること

コメント [FISC1]: No.85,86
ご意見を踏まえ、読みやすさの観点から、文章全体を修正した。

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。

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

〇経営層の使命は、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。
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。
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。

(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。

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。

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。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。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。

[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。

【事後送付資料】
平成 29 年 8 月 2 日更新
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 [FISC2]: No.82
『特定システムには「高い安全対策」を適用する。』という前文と対になるよう、文章を見直した。

削除: 基準

[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、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。

（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。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。

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

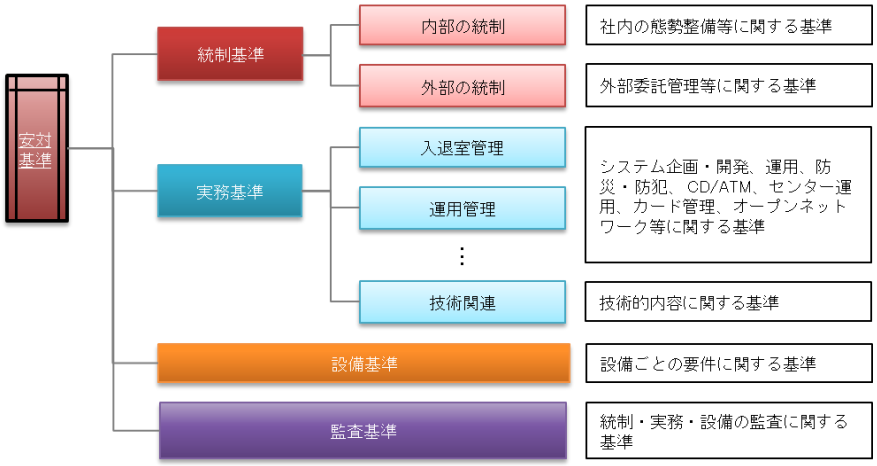
コンピュータシステムが収容される建物や設備を自然災害、不正行為等から守るための対策に関する基準・解説等から構成される。

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。

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。

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。

「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。

[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、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。

さらに、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。

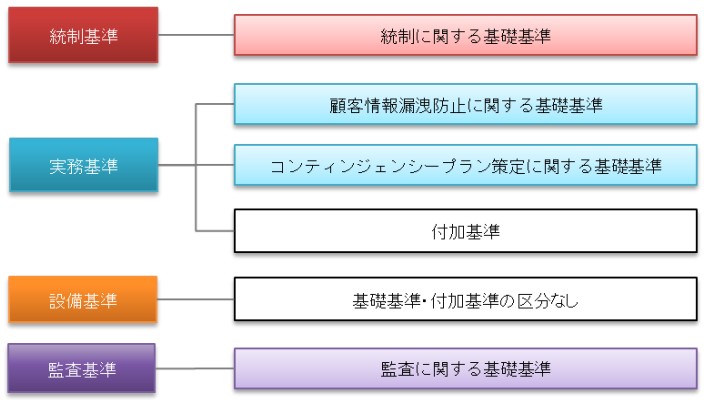
「基礎基準」の選定にあたっての考え方

○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

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。

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。

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

コメント [FISC3]: No.92
各基準と基礎基準・付加基準の関係が分かりやすくなるよう、図を追加した。

「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[12]」としている。

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[13]」としている（[図表 9]を参照、詳細は、(4)安全対策決定のプロセスを参照）。

	基礎基準	付加基準
特定システム	原則として適用	原則として適用
通常システム		リスク特性に応じて選択追加可

[図表 9] 基礎基準と付加基準

コメント [FISC4]: No.87
脚注 12「システムによっては適用除外」では「金融機関等によっては適用除外」とする方が適切であるとの意見を踏まえ、脚注の文章を修正した。

削除: 8

削除: 8

削除: システム

[12] 安全対策基準の中には、特定のシステムや業務（外部接続管理や渉外端末の管理に関する基準等）のみを対象とした基準が含まれており、これらは最低限の基準であっても、金融機関等によっては適用除外となる。こうした点を考慮して、「原則として適用」との表現を使用している。

[13] 重大な外部性を有するシステムと、機微性を有するシステムでは、適用する基準が異なることが想定される。また、特定のシステムや業務のみを対象とした基準が含まれる。こうしたことを考慮して、特定システムにおいても、すべての付加基準を適用するわけではないため、「原則として適用」との表現を使用している。

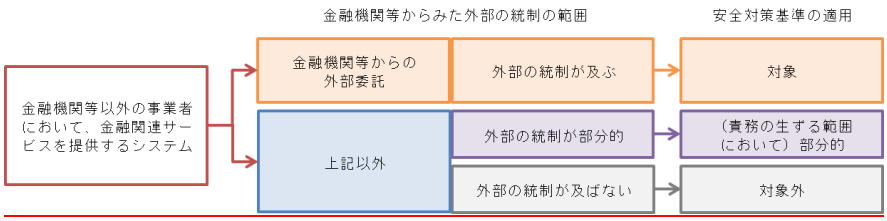
(3) 安全対策基準の適用対象

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[14]、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[15]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 10]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[16]。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[17]となる。



［図表 10］金融関連サービスにおける安全対策基準適用の考え方

コメント [FISC5]: No.88
脚注 17 の文章を修正。「データの保全」と「本人認証」については、実施状況の検証がどちらも必要になると考えられることから、表現を見直した。

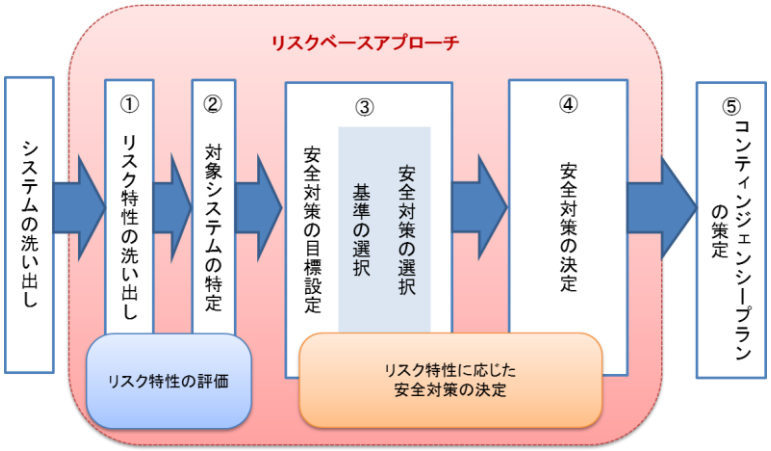
コメント [FISC6]: No.83
金融機関等以外の事業者において金融関連サービスを提供する際の、安全対策基準の提供について、関係性を示した図を追加した。

[14] 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。
[15] 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。
[16] 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。
[17] 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。

削除: または

(4) 安全対策決定のプロセス

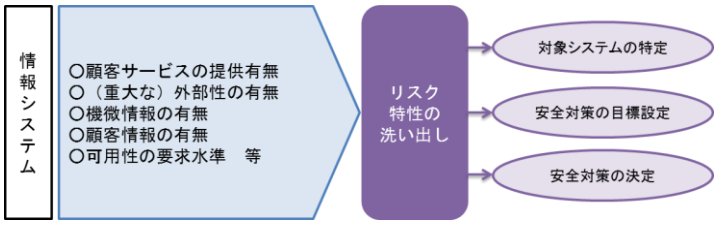
リスクベースアプローチでは、その経営資源配分の効果が最大となるよう、適切な内容で安全対策を決定していくこととなる。金融機関等は、安全対策基準の適用対象となる各システムのリスク特性を洗い出し、対象システムを特定した後、安全対策の目標を定め、必要となる基準及び安全対策の選択を行う。安全対策の目標に対し、安全対策費用とその効果、新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮し、最終的に安全対策を決定していく。その結果、残存するリスクを踏まえ、必要に応じてコンティンジェンシープランを策定する（[図表 11]を参照）。



［図表 11］安全対策決定のプロセス

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[18]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 12]を参照）。



［図表 12］リスク特性の評価

18 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。

コメント [FISC7]: No.80
残存リスクはゼロにならないことの方が一般的な考え方であり、発生することを前提とした記載に修正した。

削除: が発生する場合は

削除: 9

削除: 9

削除: 10

削除: 10

② 対象システムの特定

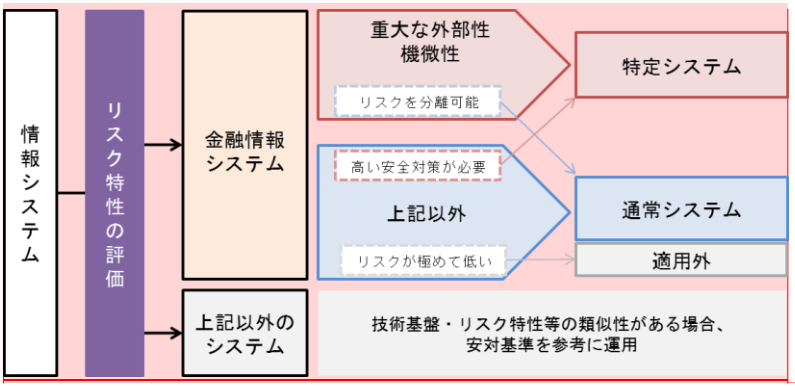
洗い出されたリスク特性を評価し、利用する金融情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。金融情報システム以外のシステムについては、その技術基盤やリスク特性に類似性がある場合、安全対策基準を適宜取り入れることとする。

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 13]を参照）。

削除: 11

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 13］対象システムの特定

コメント [FISC8]: No.84
ご意見を踏まえ、図を微修正した。

削除: 11

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、基準の選択及び対策の選択において、システム構成やリスク特性から、明確に不要な基準及び対策は適用除外となる[19]。

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。

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

下へ移動 [1]: この結果、残存リスクが発生する場合は、原則とし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。

コメント [FISC9]: No.80, 81
文の繋がりを分かりやすくするため、コンティンジェンシープランに関する記載を移動した。また、残存リスクが発生することが一般的という前提に立ち、文章を修正した。

移動（挿入）[1]

削除: が発生する場合は、原則として

19 「1.(2)基準の分類」を参照。

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。

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。

【事後送付資料】
平成 29 年 8 月 2 日更新
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。

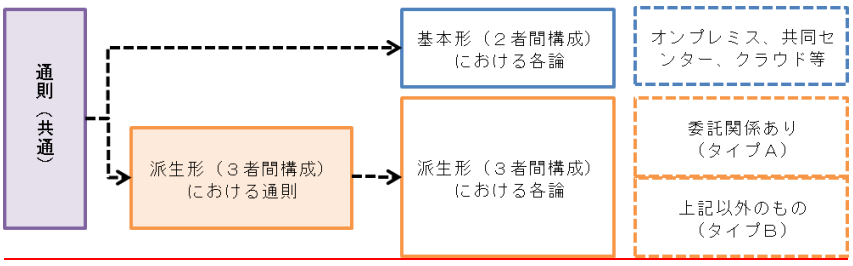
a. 方針・規程
b. 組織体制
c. サイバー攻撃対応体制
d. 人材（要員・教育）

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 14] を参照）。

削除: 12



[図表 14] 外部の統制における体系

コメント [FISC10]: No.61
３者間構成には委託関係にあるとは限らない企業が関与するケースを明示した。

削除: 12

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 15] を参照）。

削除: 13

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 15] 外部委託の管理プロセスにおける IT ガバナンス

コメント [FISC11]: No.62
図が複雑であったため、表形式に差し替えた。

削除: 13

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。

コメント [FISC12]: No.91
FinTech 有識者検討会における議論の内容を正しく反映するため、タイトル及び、文章の見直しを行った。

削除: 委託先への監査権の明記

削除: であり、これらは委託業務の内容等に応じて、金融機関等が適切に判断することが必要

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。

コメント [FISC13]: No.92
FinTech 有識者検討会の議論を踏まえ、報告書の内容を反映するよう、文章を見直した。

削除: や

削除: 必要な

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 16］を参照）。

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。

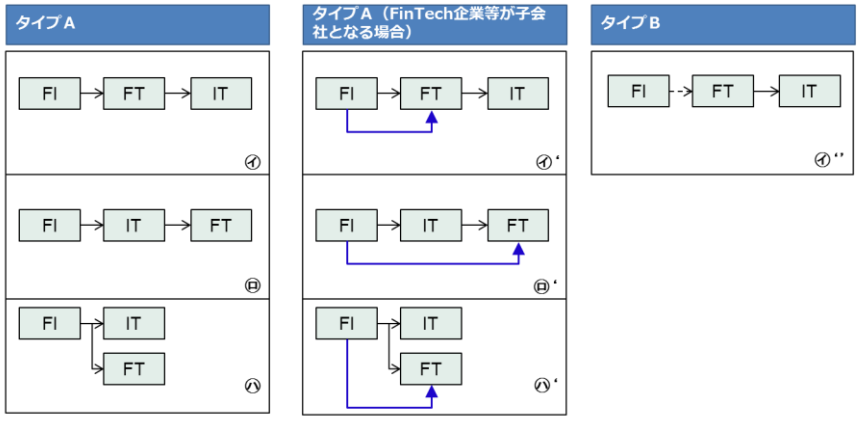
なお、FinTech 企業等が金融機関等の子会社となる形態も、タイプＡに含まれる。この場合、子会社に対する責任が金融機関等に付加される点を除いては、タイプＡのそれ以外の形態と安全対策上の差異はなく、金融機関等は、同等性の原則及び責務の再配分ルールを踏まえた統制を行うことが必要となる。

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 16］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

コメント [FISC14]: No.65
３者間構成における関係性を分かりやすくするため、図を追加した。

【事後送付資料】
平成29年8月8日
公益財団法人　金融情報システムセンター

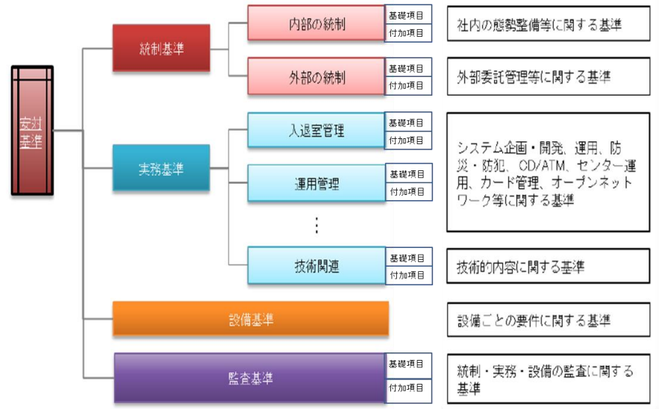
■改訂原案（前説）に対する各委員からのご意見（対応方針）

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	ー	（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。	要	未
71	p15	Ⅱフレームワーク 1．総論 (2)基準の分類 (補足2)外部の統制における・・	「可能である」という表現の使い方に何通りもあるように読めるため、全体として意味が理解しにくい。表現上の問題だけでなく、必要最低限の考え方も混入しているため、整理して分かりやすくした方がよい。	全国信用金庫協会 蓮實様(検)	ご指摘の通り、「可能である」には、必要最低限と位置付けられるものが混在しているため、全体として意味が分かりづらくなっています。「可能である」という表現は、主に「クラウドサービス利用」の基準において使用されていますが、当該基準は、8月8日専門委員会のテーマである「外部委託管理基準の検討」において審議していただく予定ですので、それまでに対応方針を整理したいと考えております。	要	未
61	P22	Ⅱフレームワーク 2．統制 (2)外部の統制	決済代行業者がいわゆる外部委託先と同じように書かれていますため、外部委託に関する概念は説明ないし整理が必要と思われます。外部委託ではないAPI連携等の場合の統制の考え方も内部、外部と並べて（しない場合ならその旨も明らかに）記載すべきと考えます。	FinTech協会 瀧様(専)	ご指摘を踏まえ、外部委託の関係にあるか否かを明示的に示すことで、サービス内容が多岐にわたるFinTech企業等と金融機関等との関係を分かりやすく表記することが適切であると考えました。2者間・3者間構成を表した図を修正し、必ずしも外部委託関係にない関係が存在する点を明記いたします。	要	済
4	ー	（全般）	基準の構成や分類、適用に関する記載は、実際の基準が示されていない中で、判断ができない。	全国信用金庫協会 蓮實様(検)	今後、基準内容の各論について整理を行った後、必要に応じて、基準の構成や分類、適用に関する記載部分を見直していく予定です。	要	未
20	ー	（全般）	個々の考え方や内容は理解できるが、実際の安全対策基準利用での全体感（どの様に具体的に適用されるや図7、図8、図11、図12の関連性が判る等）が整理された図や一覧等があると良いが。	野村ホールディングス 荒木様(検)	ご指摘の点について、検討を行いたいと考えております。	要	未
76	p11	Ⅰ概説 2．安全対策の考え方 (6)安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	外部に対する統制のあり方について、外部センターのシステムと自社センター内部のシステムと、具体的にどの基準について差を設けるかは、今後基準それぞれについて以下の観点でよく検討が必要と感じました。 ・リスクベースで考えると、障害発生時の影響は、外部センターのシステムか自社センターのシステムかによらない。 ・一方で、外部センターに対し、すべてにおいて自社内部と同等の統制を行うことが可能とは限らない。	東京海上日動火災保険 佐々木様(検)	ご指摘の点につきましては、今後「外部委託管理の検討」の中で整理させて頂きたいと考えます。	要	未
14	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	「コンビニATM」および「デビットカード」の安全対策基準について、地銀の中には、「コンビニATM」の安全対策はセブン銀行やイオン銀行などコンビニATM設置行、「デビットカード」の安全対策は日本デビットカード推進協議会が行っているとして、銀行は（「コンビニATM」および「デビットカード」の安全対策を自ら実施するのではなく）コンビニATM設置行や日本デビットカード推進協議会の安全対策を確認する態勢を整備するものと考えるところがある。 こうしたことから、これら項目は「実務基準」ではなく、「統制基準」として整理するのがよいと考える。「統制基準」として整理することが難しいならば、これら項目の順番を「実務基準」の一番最後にするのがよい。	南都銀行 山田様(専) 藤谷様（検）	「コンビニATM」および「デビットカード」の安全対策基準に関しては、ビジネスモデル等も踏まえ、今後、「外部委託管理基準の検討」の中で整理させて頂きたいと考えております。	要	未
62	p23	Ⅱフレームワーク 2．統制 (2)外部の統制 ①外部委託の管理におけるITガバナンス	[図13] 「経営層以外」の「層」の文字の右横に両矢印があるが、何を指しているのか判読しづらい。恐らく「委託業務が低リスクな場合は～」を指していると思われるが、吹き出し線の色が周囲とほぼ同色で判読しづらい。（他、数名「分かりにくい」との意見あり）	NTTデータ 鎌田様(専)、鈴木様（検）	ご意見を踏まえ、p22図表13について見やすさを改善しました。	要	済
65	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	3者間構成の各論について、タイプA、タイプBと各々文章での説明が続く。図式を用いるなど理解のし易さを考慮いただきたい。	NTTデータ 鎌田様(専)、鈴木様（検）	ご意見を踏まえ、タイプA、Bにおける3者間の関係を図示したものを追加しました。	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
追	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
追	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。	要	未
追	79	―	（基準一覧 実務基準） ※No78と関連するため、ここに記載	APIに関する記載が今後入るものと資料への記載がありますが、FISCにおいて検討が行われ、実用もされている接続チェックリストと重複した／異なる運用を招かないかを懸念しております。こちらにおける記載として、チェックリストを事例として記載頂き、リスクベースアプローチに基づいた、「金融情報システム」とは別個の、前説に書かれているタイプBであることを前提とした記載をお願いしたく存じます。	FinTech協会 瀧様(専)	オープンAPI等、FinTechに関連する基準の新設については、現時点では行わない想定です。新設基準が必要と判断した場合は、ご意見を踏まえ、基準の内容を検討していきたいと考えております。	否	現時点では前説へ反映しない考えです。
追	80	p18 p20	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ④安全対策の決定	一般に、残存リスクはゼロにはならない※ことから、「残存リスクが発生する場合は」という表現は、例えば「残存リスクを踏まえ、必要に応じて」のような、リスクの残存を前提とした(但し、CPが必要とは限らないことが明確になるような)表現にしていただいた方が良いかと思います。 ※「仮に安対基準の全項目を充足したとしても残存リスクはゼロではない」ことについて、必ずしも読み手にとって容易に腹落ちするとは限らないといった懸念があれば、その旨についても説明を補っていただいた方が良いかもしれません。	NRIｾｷｭｱﾃｸﾉﾛｼﾞｰｽﾞ 太田様(検)	ご意見を踏まえ、残存リスクがゼロとなる状態は考えにくいため、残存するリスクを踏まえ、必要に応じてCPを策定するという内容に見直しました。	要	済
追	81	p20	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ④安全対策の決定	「この結果」以降は(文頭を多少変更する必要はありそうですが)次の⑤に記載した方が、④⑤の棲み分けがより明確になるかと思いますが如何でしょうか。ご検討ください。	NRIｾｷｭｱﾃｸﾉﾛｼﾞｰｽﾞ 太田様(検)	ご指摘を踏まえ、当該箇所について文章を修正させていただきました。	要	済
追	82	p12	Ⅱフレームワーク 1．総論 (1)安全対策基準における定義 ②特定システム・通常システム	「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基準を適用することが可能である。」 の箇所において、下線部の「基準」は、その前の段落に記載のある「「特定システム」には、「高い安全対策」を適用する必要がある。」と平仄を合わせ、「安全対策」としたほうがよいと思います。	三井住友海上火災保険 中川様(検)	ご指摘を踏まえ、当該箇所について文章を修正させていただきました。	要	済
追	83	p17	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象	安全対策基準の適用対象について、「金融機関等以外の事業者が～」以降の箇所については、わかりやすさの観点から図表等を用いて説明したほうがよいと思います。	三井住友海上火災保険 中川様(検)	ご指摘を踏まえ、p18図表XXを追加させていただきました。	要	済
追	84	p19	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ②システムの特定	＜図11＞において、「リスクを分離可能」の枠囲いは、「重大な外部性・機微性」の矢羽の中に記載したほうが分かりやすい。また、同様にその下に記載がある「高い安全対策が必要」の枠囲いは、「上記以外」の矢羽の中に記載したほうがよいと思います。	三井住友海上火災保険 中川様(検)	ご指摘を踏まえ、p18図表11を修正させていただきました。	要	済
追	85	p9	Ⅰ概説 2．安全対策の考え方 (4)基本原則に従ったITガバナンス	以下の様に修正してはどうか。 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適切かつ包括的に決定する。その際は、新規投資等を含め、投資効率の最大化を追求した経営資源配分を考慮する。また、重大な外部性・・	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、当該箇所について文章を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
追	86	p9	Ⅰ概説 2. 安全対策の考え方 (4)基本原則に従ったITガバナンス	「原則として、経営層みずからが、対象となるシステムを決定することが求められる。」は「対象となるシステムの決定については、原則として経営層の判断が求められる。」	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、当該箇所について文章を修正させていただきました。	要	済
追	87	p15	Ⅱフレームワーク 1. 総論 (2)基準の分類	「システムによっては適用除外となる。」とあるが「金融機関によっては、適用除外となる。」ではないか。原案は「システムによっては、その基準が適用除外となる。」との意味だと思うが、本来、「金融機関によっては、その基準が適用されるシステムが無い（または重要ではない）ので基準が適用除外となる」のではないか。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、当該箇所について文章を修正させていただきました。	要	済
追	88	p17	Ⅱフレームワーク 1. 総論 (3)安全対策基準の適用対象	「データの保全」または「本人認証」・・　は「または」を「や」か「および」とした方が良いのではないか。	全国信用金庫協会 蓮實様(検)	ご意見を踏まえ、脚注17の文章を修正いたしました。「データの保全」と「本人認証」については、実施状況の検証がどちらも必要になると考えられることから、「または」という表現を見直しました。 「データの保全」や「本人認証」に係る安全対策・・・	要	済
追	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。	労働金庫連合会 岡部様(専)	ご意見を踏まえ、「基準」を読み替えるかどうかは、今後の基礎基準の選定、読みやすさ等を検討する中で、改めて整理したいと考えております。（各基準の関係については、No92のご意見を踏まえ、図を追加しています）	要	未
追	90	p24	Ⅱフレームワーク 2. 統制 (2)外部の統制 ①外部委託の管理におけるITガバナンス b.委託先への監査権の明記	安全対策基準の内容が、形だけの字義どおりの解釈と運用がなされ、リスクも利用形態も外部統制の在り方も把握しないまま監査権を要求することだけが独り歩きすることは、実施的な統制の実施にはつながらないのではないかと鑑みます。FinTechに関する有識者検討会における議論の内容が適切に反映されるよう、以下の文案に修正を検討いただけないでしょうか。 （修正案） 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。	アマゾンウェブサービスジャパン 梅谷様(専)	ご指摘を踏まえ、当該箇所について文章を修正させていただきました。	要	済

労働金庫連合会ご提案



（注）特定システムは、原則として基礎項目および付加項目を適用する。また、通常システムは、基礎項目を原則として適用し、リスク特性に応じて付加項目を選択追加する。

［図 7］安全対策基準の構成

	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
追	91	p25	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形（2者間構成）における各論 c.クラウドサービス	「（中略）情報処理拠点が複数の国や地域にまたがる「匿名の共同性」」という記述がありますが、FinTechに関する有識者検討会において、クラウドサービスのリスクや統制はその性質に応じてなされるという議論がなされていることから、その定義に関する文章は最新の情報を反映していただけないでしょうか。	アマゾンウェブサービスジャパン 梅谷様(専)	ご指摘を踏まえ、当該箇所について文章を修正させていただきました。	要	済
追	92	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	資料2-3「基準一覧（基礎基準案）」における基礎基準の分類（「統制・監査」「顧客データ漏えい防止」「コンティンジェンシープラン」）と＜資料番号、項番＞資料1-2 における分類（「統制基準」「実務基準」「設備基準」「監査基準」）の関係をご教示ください。	アマゾンウェブサービスジャパン 梅谷様(専)	基礎基準の分類で示した考え方に該当する基準を、統制基準、実務基準、監査基準から選定し、これらを基礎基準としています。具体的には「統制・監査」は、統制基準及び、監査基準を指し、「顧客データ漏えい防止」「コンティンジェンシープラン」は統制基準及び実務基準の一部の基準が該当します。これらの関係性が分かりにくいと思われるため、改めてp14に統制基準、実務基準、設備基準、監査基準と、それに含まれる基礎基準と付加基準を図示いたしました。	要	済

【資料5－1】
平成29年8月8日
公益財団法人 金融情報システムセンター

平成29年度第55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　8/22（火）17:00（基礎基準、外部委託、読みやすさ、前説）

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）	・・・