平成 29 年 6 月 16 日
公益財団法人 金融情報システムセンター

第 52 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 6 月 16 日（金）　15:00～17:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．	15:00	開会
２．	15:00	副座長　挨拶 安全対策専門委員紹介（新任者等） 安全対策検討部会委員紹介
３．	15:15	【説明】 ・開催日程について
４．	15:25	【議案１】改訂原案（前説）に関する検討 ・検討の進め方（FISC 事務局） ・改訂原案説明（FISC 事務局） ・原案に対する検討
５．	16:55	事務連絡 ・事後（前説）意見募集について
６．	17:00	閉会

Ⅳ　資料

【参考１】	安全対策専門委員会委員名簿
【参考２】	安全対策検討部会委員名簿
【資料０－１】	平成 29 年度安全対策専門委員会開催日程
【資料１－１】	改訂原案（前説）に関する検討の進め方
【資料１－２】	改訂原案（安全対策基準前説）
【資料１－３】	説明資料（安全対策基準新構成案）
【資料２－１】	検討事項に関するご意見フォーム

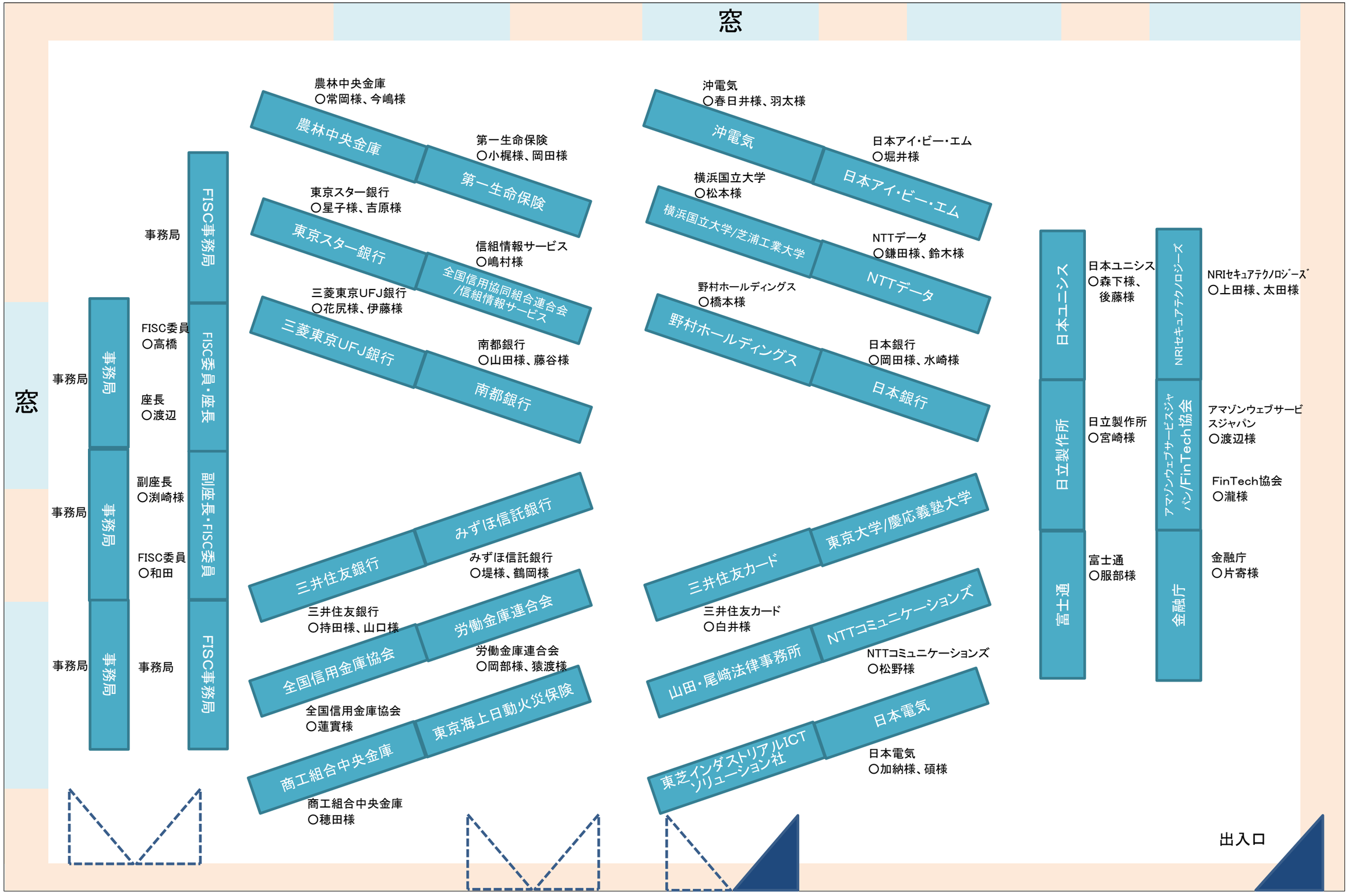
Ⅴ　今後の予定

○第 53 回　安全対策専門委員会
（予定）平成 29 年 6 月 28 日（水）15:00～17:00　FISC 会議室

以上

第52回「安全対策専門委員会」座席表

平成29年6月16日



参考１

平成 29 年 6 月 16 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委員名簿

（平成 29 年 5 月 23 日～）

（敬称略、順不同）
（所属・役職等は委員会開催時点）

座　長	渡辺　達郎	公益財団法人金融情報システムセンター理事長
副座長	渕崎　正弘	(株)日本総合研究所代表取締役社長
委　員	花尻　　格	(株)三菱東京ＵＦＪ銀行システム企画部副部長
〃	持田恒太郎	(株)三井住友銀行システム統括部システムリスク統括室長
〃	山田　　満	(株)南都銀行システム部長
〃	堤　　英司	みずほ信託銀行(株)ＩＴ・システム統括部システムリスク管理室長
〃	星子　明嗣	(株)東京スター銀行執行役
〃	高橋　義範	一般社団法人全国信用金庫協会業務推進部長
〃	内田　満夫	全国信用協同組合連合会システム業務部部長
〃	岡部　剛久	労働金庫連合会統合リスク管理部部長
〃	常岡　良二	農林中央金庫ＩＴ統括部主任考査役
〃	高橋　永泰	(株)商工組合中央金庫システム部部長
〃	小梶　顯義	第一生命保険(株)ＩＴビジネスプロセス企画部部長
〃	五十嵐逸郎	東京海上日動火災保険(株)執行役員ＩＴ企画部長
〃	橋本伊知郎	野村ホールディングス(株)参事 Co-CIO 野村證券(株)経営役業務企画、ＩＴ基盤、国内ＩＴ担当
〃	木原　眞一	三井住友カード(株)経営企画部長兼調査室長
〃	岡田　拓也	日本銀行金融機構局考査企画課システム・業務継続グループ グループ長
〃	相田　　仁	東京大学大学院工学系研究科教授工学博士
〃	安冨　　潔	慶應義塾大学名誉教授 弁護士（渥美坂井法律事務所・外国法共同事業）
〃	鎌田　正彦	(株)ＮＴＴデータ金融事業推進部技術戦略推進部 プロジェクトサポート担当部長
〃	松野　　徹	ＮＴＴコミュニケーションズ(株)ソリューションサービス部 第二プロジェクトマネジメント部門第一グループ担当部長
〃	春日井正司	沖電気工業(株)金融・法人ソリューション事業部 プロジェクトマネジメントオフィス室長
〃	崎新谷　毅	(株)東芝インダストリアルＩＣＴソリューション社 インダストリアルソリューション事業部 金融・情報ソリューション技術部 金融・情報ソリューション技術第一担当グループ長

参考１

平成 29 年 6 月 16 日
公益財団法人 金融情報システムセンター

委　員	堀井　康司	日本アイ・ビー・エム(株) 金融インダストリーソリューション 第一ソリューション推進ソリューションマーケティング担当営業部長
〃	加納　　清	日本電気(株)金融システム開発本部シニアエキスパート
〃	森下　尚子	日本ユニシス(株)ファイナンシャル第三事業部 ビジネス企画統括部次世代ビジネス企画部 事業推進グループ事業推進グループマネージャー
〃	柿本　　薫	(株)日立製作所金融第一システム事業部事業推進本部本部長
〃	藤田　雅人	富士通(株)金融・社会基盤営業グループシニアディレクター
〃	上田　直哉	ＮＲＩセキュアテクノロジーズ(株) マネジメントコンサルティング部部長
〃	梅谷　晃宏	アマゾンウェブサービスジャパン(株)セキュリティ・アシュアランス 本部長日本・アジア太平洋地域担当（H29.6.16～）
〃	瀧　　俊雄	一般社団法人ＦｉｎＴｅｃｈ協会アドバイザー（H29.6.16～）
ｵﾌﾞｻﾞｰﾊﾞｰ	片寄早百合	金融庁検査局総務課システムモニタリング長主任統括検査官
FISC 委員	髙橋　経一	公益財団法人金融情報システムセンター常務理事
〃	和田　昌昭	公益財団法人金融情報システムセンター監査安全部長

参考２

平成 29 年 6 月 16 日
公益財団法人 金融情報システムセンター

安全対策検討部会委員名簿

（平成 29 年 6 月 16 日～）

（敬称略、順不同）
（所属・役職等は 6 月 16 日時点）

委　員	伊藤　武男	(株)三菱東京ＵＦＪ銀行システム企画部 事務・システムリスク統括室システムリスク管理Ｇｒ上席調査役
〃	山口　康隆	(株)三井住友銀行システム統括部システムリスク統括室 システムリスク管理グループ長
〃	藤谷　隆史	(株)南都銀行東京事務所グループ長
〃	鶴岡　俊哉	みずほ信託銀行(株)ＩＴ・システム統括部 システムリスク管理室調査役
〃	吉原　丈司	(株)東京スター銀行ＩＴ戦略部長
〃	蓮實　　豊	一般社団法人全国信用金庫協会業務推進部主任調査役
〃	嶋村　　正	信組情報サービス(株)企画部長
〃	猿渡　耕二	労働金庫連合会統合リスク管理部次席調査役
〃	今嶋　　治	農林中央金庫ＩＴ統括部副部長
〃	穂田　　猛	(株)商工組合中央金庫システム部次長
〃	岡田　潤一	第一生命保険(株)ＩＴビジネスプロセス企画部 サイバーセキュリティ対策室次長
〃	佐々木義顕	東京海上日動火災保険(株)ＩＴ企画部リスク管理グループ参事
〃	荒木　冬湖	野村ホールディングス(株)ＩＴ統括部ヴァイスプレジデント
〃	白井　大輔	三井住友カード(株)システム企画部上席審議役
〃	水崎　　玲	日本銀行金融機構局考査企画課企画役
〃	松本　　勉	横浜国立大学大学院環境情報研究院教授
〃	三好　　匠	芝浦工業大学システム理工学部電子情報システム学科教授
〃	菅谷　貴子	山田・尾﨑法律事務所弁護士
〃	鈴木　健一	(株)ＮＴＴデータ金融事業推進部技術戦略推進部 プロジェクトサポート担当課長
〃	濱中　慎一	ＮＴＴコミュニケーションズ(株)ソリューションサービス部 第二プロジェクトマネジメント部門第一グループ担当課長
〃	羽太　英哉	沖電気工業(株)金融システム事業部 プロジェクトマネジメントオフィスシニアスペシャリスト

参考２

平成 29 年 6 月 16 日

公益財団法人 金融情報システムセンター

委　員	小林　晴紀	(株)東芝インダストリアルＩＣＴソリューション社 インダストリアルソリューション事業部 金融・情報ソリューション技術部 金融・情報ソリューション技術第一担当参事
〃	鎌田美樹夫	日本アイ・ビー・エム(株)サービス事業統括 第一銀行･ＦＭソリューションズ担当部長
〃	碩　　正樹	日本電気(株)プラットフォームサービス事業部主任
〃	後藤　茂成	日本ユニシス(株)ファイナンシャル第三事業部 ビジネス企画統括部次世代ビジネス企画部事業推進グループ チーフ・コンサルタント
〃	宮崎　真理	(株)日立製作所金融第一システム事業部事業推進本部システム統括部 CSIRT グループ主任技師
〃	服部　　剛	富士通(株)金融・社会基盤営業グループ 金融リスクマネジメント室長
〃	太田　　海	ＮＲＩセキュアテクノロジーズ(株) マネジメントコンサルティング部上級セキュリティコンサルタント
ｵﾌﾞｻﾞｰﾊﾞｰ	市村　雅史	金融庁検査局システムモニタリングチーム専門検査官

【資料0－1】
平成29年6月16日
公益財団法人 金融情報システムセンター

平成２９年度　安全対策専門委員会開催日程

	日程		時間	テーマ		議案（予定）	参加者
				安対	IT		
第５２回	6月16日	（金）	15:00-17:00	●		・改訂原案（前説Ⅰ・Ⅱ）に関する検討	安対専門委員・検討部会委員
第５３回	6月28日	（水）	15:00-17:00	●		・改訂原案（前説Ⅰ・Ⅱ）に対する委員意見反映版の検討	安対専門委員・検討部会委員
第５４回	7月11日	（火）	15:00-17:00	●		・改訂原案（前説Ⅲ）に関する検討 ・基礎基準・基準改訂に関する検討	安対専門委員・検討部会委員
第５５回	8月8日	（火）	15:00-17:00	●		・改訂原案（前説Ⅲ）に対する委員意見反映版の検討 ・基礎基準・基準改訂に対する委員意見反映版の検討 ・外部委託管理（クラウド基準の統合）の検討 ・外部委託管理に関するその他の基準の検討	安対専門委員・検討部会委員
第５６回	9月12日	（火）	15:00-17:00	●		・外部委託管理に関する委員意見反映版の検討	安対専門委員・検討部会委員
第５７回	10月17日	（火）	15:00-17:00	●	○	・最終原案の承認・会員意見募集実施の承認	安対専門委員・検討部会委員
第５８回	12月19日	（火）	15:00-17:00	●		・会員意見に対する回答案についての承認 ・発刊の最終承認	安対専門委員・検討部会委員
第５9回	1月中旬		15:30-17:00		○	・会員意見に対する回答案についての承認 ・発刊の最終承認	安対専門委員

※IT人材のテーマが「○」については、書面による審議とさせていただく場合があります。

※会場は、全日程ともFISC会議室で行う予定です。

※日程等については、進度、状況によって、追加・変更となる場合があります。

【資料１－１】
平成 29 年 6 月 16 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）に関する検討の進め方

Ⅰ 検討経緯

平成 27 年 10 月から平成 28 年 6 月にかけて「金融機関における外部委託に関する有識者検討会」を開催し、その結果を同 6 月に報告書として取りまとめた。

また、平成 28 年 10 月から平成 29 年 6 月にかけて「金融機関における FinTech に関する有識者検討会」を開催し、その結果を同 6 月に報告書として取りまとめる予定である。

本報告書の提言内容等を踏まえ、『金融機関等コンピュータシステムの安全対策基準・解説書』（以下「安対基準」という）において、以下３点を主なテーマとして安対基準の改訂を行うこととした。

① 安対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、金融機関等がより効果的に安対基準を活用することが、さらなるイノベーションの発揮や、金融機関等における効率的な経営資源配分に繋がると考えられる。

② 金融機関等における外部への依存が高まる中、安対基準に求められる役割が統制面の対策にシフトしていくと想定され、改めて安対基準における統制の位置付けについて、見直すべき時期が到来していると考えられる。

③ クラウドサービスを用いた重要なシステムの運用や、いわゆる FinTech と総称される新たな金融サービスが登場するなど、外部委託管理を中心として基準の新設を含む、統合・整理を行うことが有益と考えられる。

Ⅱ 検討事項

【資料１－２】として、改訂原案（前説）を提示する。改訂原案の内容をご確認いただき、以下の視点からご指摘・ご意見をいただきたい。（本文中に主な確認点をコメントで付記した）また、【資料１－３】「安全対策基準新構成案」を参考資料として添付するので、適宜ご参照願いたい。

No	記載箇所	主な確認のポイント
①	Ⅰ．概説	「外部委託報告書」「FinTech 報告書」を踏まえ、各金融機関等の実態に合った分かりやすい内容となっているか
②	Ⅱ．フレームワーク（１．総論）	用語等における定義は、分かりやすい内容となっているか
③		適用対象は具体的で、分かりやすい内容となっているか
④		適用方法は具体的で、分かりやすい内容となっているか
⑤	（２．統制）	「外部の統制」は、報告書を踏まえ、各金融機関等の実態に合った分かりやすい内容となっているか

【資料１－１】
平成 29 年 6 月 16 日
公益財団法人 金融情報システムセンター

Ⅲ 今後の検討について

今年度のスケジュールを遅滞なく進めるために、次回第 53 回専門委員会にて、前説原案については、ほぼ最終原案に仕上げる予定である。非常に短い期間での検討をご依頼することとなるが、事後意見については、6 月 21 日（水）までに、【資料２－１】のご意見フォームにて、電子メール＜fisc40@fisc.or.jp＞あてにご連絡いただきたい。

いただいたご指摘・ご意見を踏まえ、事務局にて検討・取込みを行い、次回の専門委員会にて議論する予定である。

以　上

【資料１－２】
平成 29 年 6 月 16 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）

【資料１－２】
平成 29 年 6 月 16 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、あるいは電子決済等代行業など（以下、「決済代行業等[1]」とする）の革新的な金融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、企業価値を高めるために、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、あるべき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、非金融機関等における決済代行業者等との関係や、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あ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あり方を改めて示すとともに、金融機関内部の統制及び、これら統制の下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、保険、証券、クレジット等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。

コメント [FISC1]:
脚注にも示したが、「FinTech 企業」という名称が永続的に使用されるかは不明である。また、オープン API 等、中間業者を指す「電子決済等代行業」では、本書の指す新たな金融サービスの範囲を正確に捉えていないため、「決済代行業」という名称とした。

[1] 電子決済代行業など、IT 技術を活用した革新的な金融関連サービスは、将来において更に多様化することが想定されるため、事業もしくは事業者に対し、現時点で画一的な名称を与えることが適当ではない。本書においては、便宜上、これら革新的な金融サービスを「決済代行業等」、それらを提供する事業者を「決済代行業者等」としている。

【資料１－２】
平成 29 年 6 月 16 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

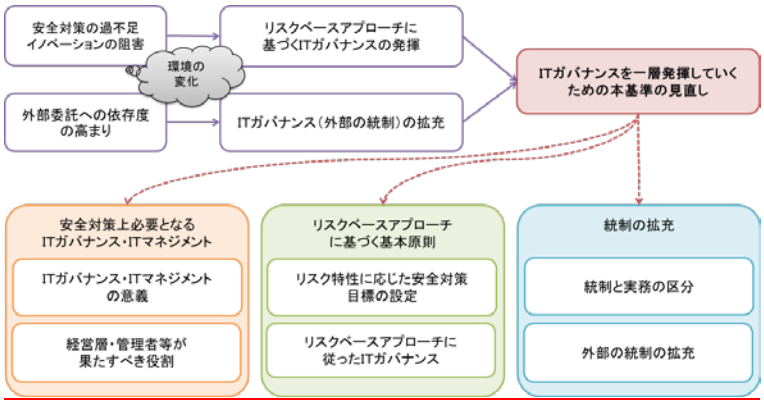
安全対策基準改訂の考え方

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、情報化の進展に伴い、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数が増加し、全体の中ではある程度大きな比率を占めるようになるとともに、その形態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、決済代行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、その適用基準が不明確なままであり、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、システム開発・運用、サービス利用等において、外部委託への依存度が高まる中、外部に対する統制の重要度が増してきている。

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ならびに、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、多岐にわたる決済代行業等が登場する中で、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、安全対策のあり方について提言が行われた。

本書では、以上の有識者検討会の提言内容を踏まえて、安全対策の考え方・利用方法等について理解頂くことを目的に、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安全対策の考え方を示していく。（[図 1] を参照）



［図 1］安全対策基準改訂の考え方（概念図）

コメント [FISC2]:
外部委託報告書 p 27 を**一部修正**
「初版から 30 年以上を経た現在においては、**過度な**安全対策を招来してもやむを得ない内容となっている。」
※過度な→過不足が生じ
従来の対策を一律「過度」とするのではなく、「不明確さにより過不足が生じる」として表現を改めた。

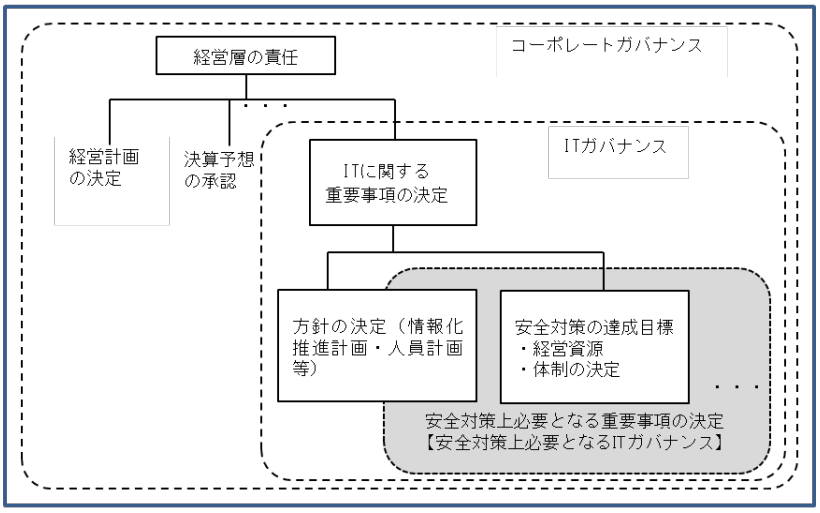
【資料１－２】
平成 29 年 6 月 16 日
公益財団法人 金融情報システムセンター

(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 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 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 3］を参照）。

1）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

ⅱ. システムリスク管理方針の決定

コメント [FISC3]:
外部委託報告書 p 13 を**一部修正**
「金融機関等の経営層は、等しく、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負う。」
※責任を負う→責任を有する
ここでは一般論としての IT ガバナンスを説明することが目的である。したがって、「経営層等が実施する必要がある」等、安対基準の一部と解される表現は回避した。

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[2]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

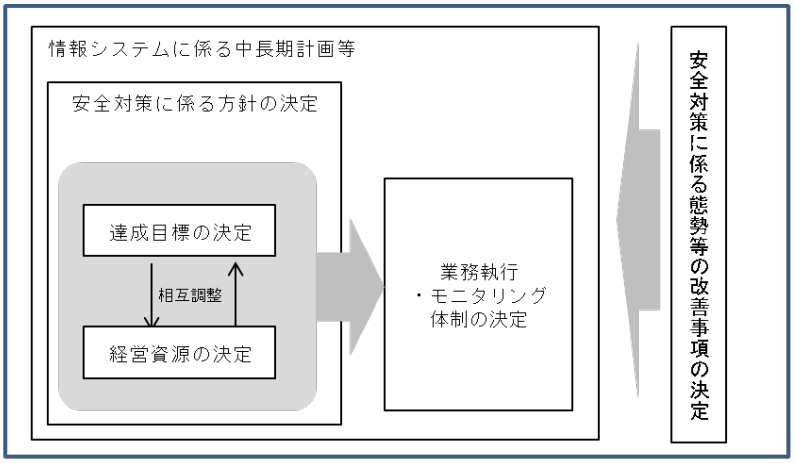
経営層は、安全対策の達成目標の決定と同時に、達成目標を実現するために必要となる経営資源の投下（費用・配分方針等）を決定する。経営層は、経営資源が有限であることを踏まえて、あらかじめ、保有する経営資源を踏まえた達成目標を検討するとともに、リスク特性に応じた資源配分を決定することが重要である。

b. 安全対策に携わる業務執行及びモニタリング体制の決定

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て、必要に応じてシステム部門等の業務執行体制及び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。

2）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 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

[2] 本書では、金融機関等が情報システムを導入・利用等すること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。

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 4］を参照）

1）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。

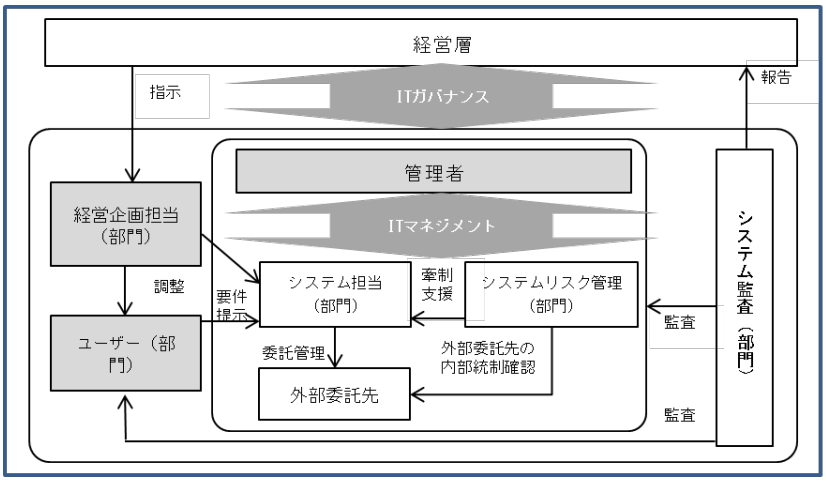
・内部規程・組織体制等の整備
・個々の情報システムに対する安全対策の決定
・内部規程・組織体制等の見直し
・安全対策上必要となる情報の経営層への報告

2）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。

3）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 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、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必要十分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正な水準以上の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では、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こととなる。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。

つぎに、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、第一義的には、金融機関等がシステムの安全性を確保しつつ、企業価値の最大化[3]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。

コメント [FISC4]:
外部委託報告書より、リスクベースアプローチ導入の考え方を記載。

コメント [FISC5]:
企業の業態等により、企業価値の意味するものが異なる。正しく表現するため、脚注にて多様性の説明を追加した。

[3] 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。

【資料１－２】
平成 29 年 6 月 16 日
公益財団法人 金融情報システムセンター

(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、その一方で、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を侵害する場合（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、必要十分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、情報システム予算内での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、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、金融機関等が保有する重大な外部性を有する情報システム及び機微情報（要配慮個人情報を含む）を保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。

○上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自に決定することが可能である。

基本原則では、金融機関等は、IT ガバナンスが適切に発揮されている限りにおいては、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安全対策を、必要十分な内容で、みずから決定することが可能としている。

一方で、金融機関等の情報システムは、金融インフラの一部を構成している。そこで、基本原則では、重大な外部性を有するシステムや、機微性を有するシステムについては、社会的・公共的な性質を有することから、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。

コメント [FISC6]:
改正個人情報保護法を受け修正。(機微（センシティブ）情報には要配慮個人情報が含まれるが、将来的に含む・含まないの議論とならないよう、明示的に含まれることを示した。

コメント [FISC7]:
外部委託報告書から抜粋のうえ、一部順番を入れ替えた。３番目の内容（ただし～）は、１及び２番目の内容に対するもの。
・安全対策の目標は必要十分な内容とする
・経営資源配分をもって決定されるべき
・ただし、個別企業の統制を超えて、社会的・公共的な観点から特例がある
・以上を踏まえ独自に決定することが可能という順番に整理

削除: 安全対策は原則として、リスクベースアプローチの考え方に従って講じられるべきとしつつ、これらの要件を、基本原則に取り入れている。

[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。

（参考）「外部性」の考え方

・「外部性」とは、例えば、個別金融機関等の決済システムにおけるシステム障害等によって、他金融機関等社会全体に経済的損失を与える可能性のある性質をいう。例えば、決済システムは個別金融機関等で深刻なシステム障害が発生した場合、他金融機関等への信用不安に発展し、経済的損失が拡大する可能性のある性質を有する。

・「外部性」には、個別金融機関等の顧客は含まれない。なぜなら、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可能であるからである。

・一方、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は正確には把握できない。つまり、個別金融機関等がシステム障害等に伴い社会全体に及ぼす損失額を正確に把握し、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。

・また、金融機関等の中には、インセンティブ上の問題（モラルハザード）等から、自社のシステム障害が引き起こす社会的影響の全部または一部を考慮の外に置いて、安全対策に係る意思決定を行う可能性もある。

・これらの問題に適切に対処するためには、特にリスクが高い「重大な外部性を有する」システムにおいては、金融機関等共通の規範となるルール（＝高い安全対策）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亘るものまである。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がある。その取扱いは社会的・公共的な性質を有するものとも考えられることからも、「重大な外部性を有する」システムと同様に取り扱うことには合理性がある。

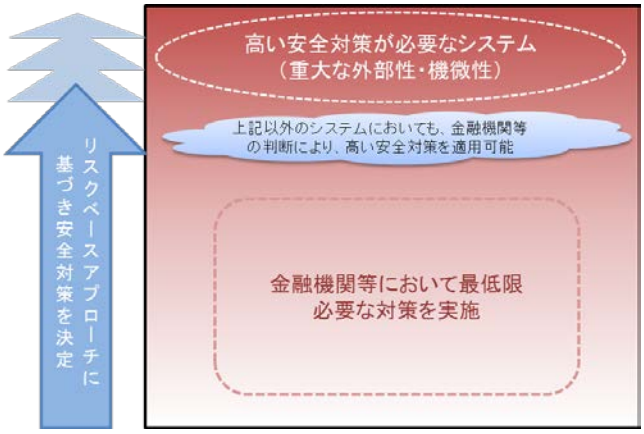
・仮に、これらが同一に扱われてしまった場合には、金融機関等のほとんどすべてのシステムに存在している個人情報が、この機微情報（要配慮個人情報を含む）に影響されて適正な水準以上の安全対策目標が設定され、資源の過剰配分が行われるおそれがある。

・このような事態を避けるためには、個人情報のうち、その保護のために最上位の安全対策目標が設定されるべき「機微情報（要配慮個人情報を含む）」と「その他の個人情報」を分け、「機微情報（要配慮個人情報を含む）」については、「高い安全対策」を適用することが妥当である。

(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、情報システムをそのリスク特性に応じて区分し、その評価された結果に基づき、新規投資等含めその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、必要十分な安全対策の目標を包括的に決定する。この際、重大な外部性や機微性を有するシステムや、それらと同等以上のリスクを有するシステム[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、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。

「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、必要十分な内容をもって、安全対策の達成目標を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で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 5] を参照）



[図 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とった結果として、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、機微性を有する情報を扱うシステムと同等に扱うケースが想定される。

コメント [FISC8]:
外部委託報告書より抜粋。
安全対策の基本原則に従って、経営層等が実施すべき内容に絞り込んだ。具体的には対象システムの決定、安全対策の目標の設定において、経営資源配分を考慮した意思決定を行うこととしている。

コメント [FISC9]:
「分離可能なサブシステム」など、フレームワークの記載と重複感があるため、削除した。

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あり方

○経営層の使命は、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。
○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」のあり方

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、過去のやり方を機械的に継続するのではなく、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「内部の統制」と、外部委託管理等を通じて外部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 6］を参照）

区分		基準の内容
統制	内部の統制	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、管理態勢等を整備するために実施する対策
	外部の統制	外部委託管理等に関する基準として、外部への統制を具体化した対策
実　務		管理者が場面やリスク管理対象に応じて、具体的に実施する対策

［図 6］「統制」と「実務」の区分

② 外部に対する「統制」のあり方

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」の重要性が増してきている。

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、委託先等に対して、「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等企業価値の最大化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、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、残るリスクが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）が存在する[6]。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ものであり、外部委託の一形態である「クラウドサービス」や、決済代行業等を営む事業者との新たな契約形態においても、これらの考え方と整合性が保たれることが必要である。

[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。また、決済代行業者等が、顧客への金融関連サービスを提供するシステムを運用し、その一部が金融機関等との接続を行う場合、運用主体である非金融機関と、接続される金融機関との間で、「統制」に係る責務の分担が発生すると想定される。

Ⅱ．フレームワーク

１．総論

(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運用または利用[7]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、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や、機微情報（要配慮個人情報を含む）の漏えい等により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」は、高い安全性の確保を必要とする。

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設定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おいては、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」として安全対策を設定することが可能である。

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 7] を参照）

a. 統制基準

「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、IT ガバナンスの発揮に必要な社内体制の整備や、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。

---

[7] 金融業及び、それに関連するサービスを共同センター等の形態で運用する場合、金融機関等は、そのシステムを利用する側面を持つため、「運用」以外の形態の一つとして、「利用」を記した。

[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。

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。

コメント [FISC10]:
FinTech 報告書 p 41 より
「技術の進展が著しい環境下では、、、すべての情報システムに対して字義通りに適用を求められるべきではなく、、、最新の技術動向等を踏まえ、金融機関において適用の可否が判断されるべきものであることを明確化する。」

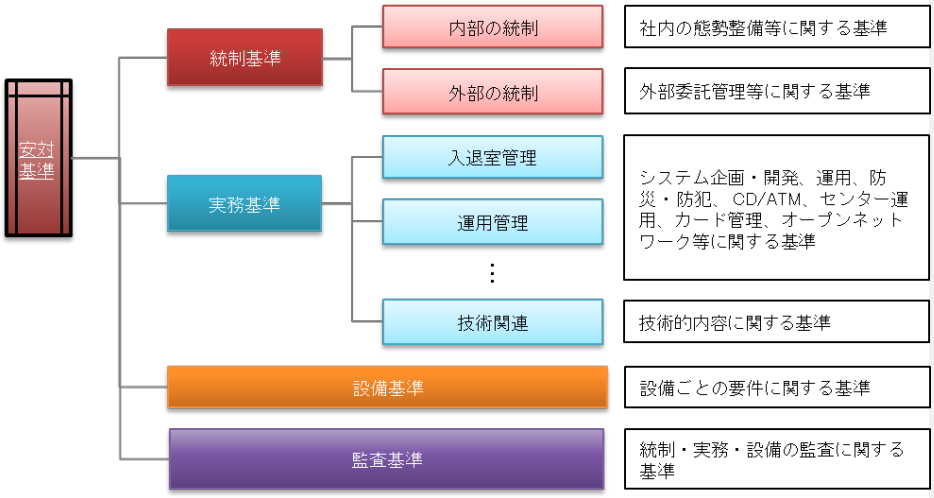
c. 設備基準

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。

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 7］安全対策基準の構成

(2) 基準の分類

コメント [FISC11]:
「特定基準」という名称が様々なイメージで捉えられるため、「付加基準」という名称とし、構成・内容を見直した。

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うえで、最低限の対策が実施されないといった不確実性を低減するために、安全対策基準の中から「基礎基準」を選定している。

基礎基準は、特定システム、通常システムによらず、金融情報システムに最低限適用する基準であり、統制基準、監査基準及び、実務基準のうち顧客データの漏えい防止等の観点から抽出した一部の基準で構成されている。

「付加基準」は、「基礎基準」以外の基準として、リスク特性に応じて追加・選択する基準である。

通常システムでは全ての「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」から必要な基準を適用する。特定システムでは、「基礎基準」及び、「付加基準」を全て適用する[9]。（[図 8]を参照）（詳細は、(4)安全対策基準の適用方法を参照）

	基礎基準	付加基準
特定システム	全て適用	全て適用
通常システム	全て適用	リスク特性に応じて選択可

［図 8］基礎基準と付加基準

なお、設備基準は、既に、コンピュータセンターに求められる基準と、本部・営業店等、各拠点に求められる基準を区分して記載しているため、「基礎基準」及び「付加基準」を区分しない。

コメント [FISC12]:
設備基準は基礎・付加基準の区分をしないことについて、説明を追加した。

（補足１）「基礎基準」とした安全対策について

金融情報システムのリスク特性は、多岐にわたり、全てのシステムが最低限満たすべき安全対策を一意に決定することは困難であるものの、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対策を、最低限の安全対策と位置付けている。なお、金融情報システムには、顧客データ以外の重要なデータ[10]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の対策が有効と考えられる。

また、近年において、サイバー攻撃対策の重要性が増してきていることから、顧客データの漏えい防止に関する安全対策には、サイバー攻撃対策として必要な対策を含めている。

さらに、リスクベースアプローチの考えでは、安全対策の設定において、必ずしもリスクゼロを追求しないことから、金融機関等においては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して実施すべき対策についても、基礎基準を設定するための条件としている。

上記以外の観点で必要となる安全対策については、システム毎のリスク特性に差異があり、各金融機関等が、システム構成やリスク評価の結果等も考慮のうえ、適宜、必要な対策を選

9 例えば機微性を有するシステムにおいて、可用性に関する安全対策を一部選択しないことも考えられる。各金融機関等は、みずから定めた安全対策の目標に応じて、付加基準を選択・適用していくことが必要となる。
10 法人情報や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。

択して適用することとなる。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、必要な対策を選択・追加することで、必要十分な安全対策となるよう考慮することが必要となる。

上記を踏まえ、「基礎基準とした安全対策」を以下に示す。

・統制・監査に関する対策
・顧客データの漏えい防止において実施すべき対策[11]
・コンティンジェンシープラン策定に関して実施すべき対策[12]

（補足２）外部の統制における「基礎基準」について

外部の統制における一部の基準には、ベストプラクティス（努力目標）としての対策が示されており、必ずしもすべてのシステムで実施すべき対策とはなっていない。このため、同基準には代替策として、「～することも可能である。」といった必要最低限の対策を示している。これらの代替策は、リスクベースアプローチの考えに基づき、通常システムにおいて選択可能としている。

（補足３）決済代行業者等における安全対策基準の適用について

決済代行業者等を含む一部の非金融機関が、金融関連サービスを提供するシステムの安全対策を策定する場合、サービスの利用者からは、金融機関等が提供するサービスと同等の安全性確保が求められる。このため、これらの事業者によって実施される安全対策は、基礎基準を満たすことが期待される。

コメント [FISC13]:
外部委託報告書 p 32 について補足
「「金融機関におけるクラウド利用に関する有識者検討会報告書」において、比較的低リスクな情報システムに対する安全対策として「簡易なリスク管理策」の通称で示され、安対基準の中では「可能である」と表記上区分されている基準と類似の性質を有する。」
→今回の改訂では「基礎基準」として再定義しているが、クラウド関連基準については、従来通り「可能である」とした簡易なリスク管理策はそのまま残している。

コメント [FISC14]:
FinTech 報告書 p 30 より
「金融業務を担う情報システムにおいて最低限実施されるべき基準として策定される「必要最低限の安対基準」は、FISC 会員に限らず、金融関連サービスの提供に携わる事業者においても、踏まえられるべき基準であると考えられる。」

[11] ハードウェアの保守等、対策を実施しないことで、ただちにリスク事象の発生に繋がらない予防的に実施する対策については、基礎基準としていない。
[12] システムごとの障害復旧マニュアル等は、コンティンジェンシープランの内容に応じて適宜必要性を判断するものであり、基礎基準としていない。

(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[13]、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[14]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「外部のシステム」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。また、非金融機関等が金融関連サービスを提供するシステムについては、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、安全対策基準を参考として運用されることが期待される。

（補足）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共通的なシステムの分類は、業態ごと[15]、または個別金融機関等における重要度によって様々であり、それらを一律に特定し、列挙することは困難であり、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、個別金融機関等の実態に則して判断することが必要とる。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上で対象となるシステムを決定することが求められる。

コメント [FISC15]:
外部委託報告書ｐ10 の図表より

コメント [FISC16]:
FinTech 報告書ｐ27 より
「業界団体においては、安全対策に関する自主基準の策定が予定されており、安対基準を参考としながら、業界団体の特性に応じた観点も反映させつつ、検討が進められている状況にある。

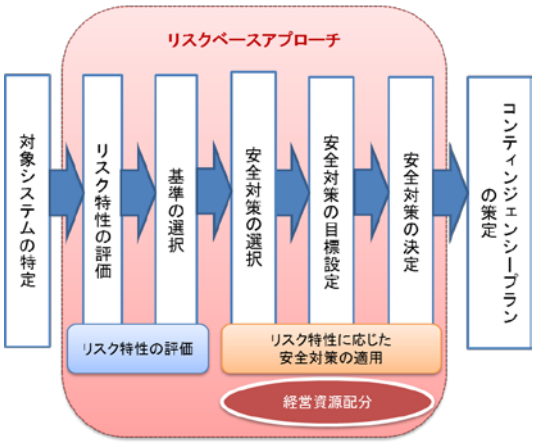
削除: な

[13] 金融機関等がベンダーと契約するものや、協同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。
[14] 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。
[15] 一般に、預取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。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取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可能である。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、特定システムとしない判断も可能である。

(4) 安全対策基準の適用方法

① リスクベースアプローチに基づく安全対策基準の適用

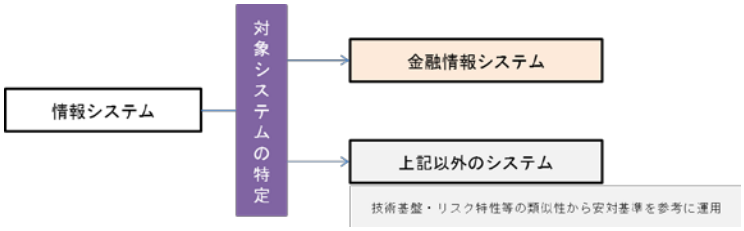
リスクベースアプローチでは、その経営資源配分の効果が最大となるよう安全対策を決定していく。経営資源配分の効果を最大化するためには、安全対策基準の適用対象となるシステムを特定した後、各システムのリスク特性を分析し、適用する基準及び、安全対策の選択を行う。さらに、リスクベースアプローチの考え方に沿って、経営資源全体を視野に入れ、情報システムへの投資効率の最大化を目指し、安全対策の目標を設定する。さらに、安全対策の目標に対し、安全対策費用とその効果、及び新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮のうえ、最終的に安全対策を決定する。その結果、残存リスクが発生する場合は、必要に応じて、コンティンジェンシープランを策定する。([図 9]を参照)



［図 9］安全対策基準適用のプロセス

② 対象システムの特定

金融機関等は、保有または利用する情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。金融情報システム以外のシステムについては、その技術基盤の共通性や、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。([図 10]を参照)



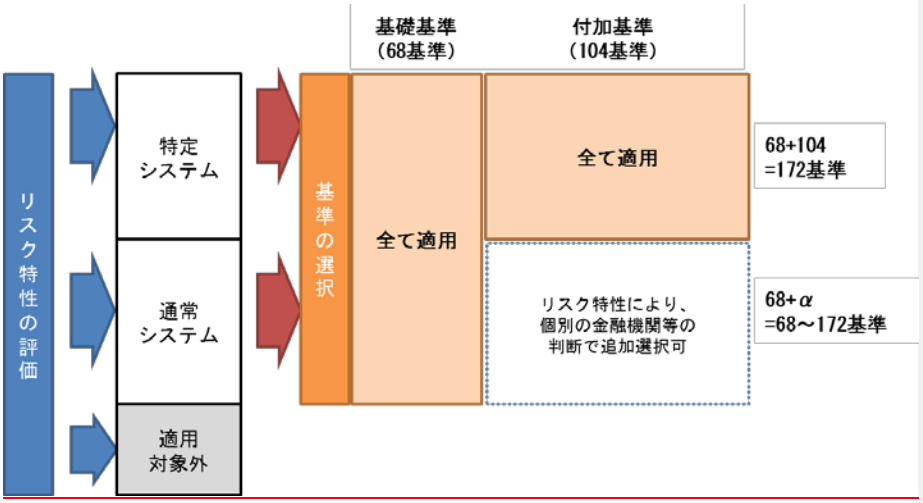
［図 10］対象システムの特定

コメント [FISC17]:
リスクベースアプローチに基づく安全対策の設定プロセスについて、委員からの意見・要望も多く、前後関係等を明確にして、全体的に構成を見直した。

③ リスク特性の評価・基準の選択

適用対象となるシステムを特定した後、システムのリスク特性を評価し、社会的・公共的に高い安全対策が求められる特定システムと、それ以外の通常システムを区分する。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。

リスク特性の評価結果[16]に応じ、区分されたシステムに対し、適用する基準を選択する。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。なお、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 11]を参照)



[図 11] システムの区分・基準の適用

④ 安全対策の選択

適用する基準を選択した後、システムのリスク特性に応じ、基準の中から適用する安全対策を選択する。

特定システムにおいては、原則として、基礎基準と付加基準に示された全ての対策を選択[17]する。ただし、各基準における簡易な安全対策（「～することも可能」等と記載）については、原則として選択不可とする。

通常システムは、原則として、基礎基準の中から、「～すること」「必要である」と示

コメント [FISC18]:
システムの特定から、適用する基準の選択までの流れについて、実際に対象となる基準数（小項目ベース）を付記し、適用のイメージが分かりやすくなるよう修正した。

基礎基準の内訳
・統制　28
・監査　1
・実務　39
付加基準の内訳
・実務　104

16 リスク評価に関する手法は様々であり、一律に示すことは困難である。一般的な手法については、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、各金融機関等の状況等に応じて検討されるものであり、安全対策基準では、具体的手法については示していない。

17 システム構成等、リスク特性等を分析した結果、明確に不要と判断できる対策については、一部省略することも可能とする。例えば、機微性を有するシステムにおいて、可用性に関する安全対策の目標を超える対策については、一部省略することも可能である。

した対策を選択する[18]。その上で、個々のシステムのリスク特性等に応じ、付加基準を追加していくこととなる。

⑤ 安全対策の目標設定

安全対策を選択した後、安全対策の目標を設定する。安全対策の目標は、各システムにおいて必要十分な内容で設定され、セキュリティ上の大きな脆弱性を残さないことが必要となる。安全対策目標を設定するためには、経営資源配分の観点を踏まえて検討されることが必要であり、経営層の関与のもと設定していく。

⑥ 安全対策の決定

安全対策の目標が設定された後、各システムのリスク特性に応じて、最終的に適用する安全対策を決定する。安全対策の決定では、必ずしもリスクゼロを追求しないことが前提となるが、リスクを正確に把握し、そのリスクに適切に対応できるものであるとともに、経営資源配分上、合理的なものであることが望ましい。この結果、残存リスクが発生する場合は、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求められる。

⑦ コンティンジェンシープランの策定

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。

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。

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災害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。

なお、安全対策基準においては、金融業務が情報システムに深く依存しており、その不具合が業務全般に及ぶことからコンピュータシステムを中心に言及している。

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。

[18] システム構成等、リスク特性等を分析した結果、明確に不要と判断できる対策については、一部省略することも可能である。例えば、外部ネットワークに接続しないシステムにおいて、外部ネットワークの機器設定に関する基準等は省略することも可能である。

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１－２】
平成 29 年 6 月 16 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対策は、原則として全て「基礎基準」としている[19]。統制には「内部の統制」と「外部の統制」に関する対策が含まれるが、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社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、セキュリティ管理態勢等の組織の整備、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。

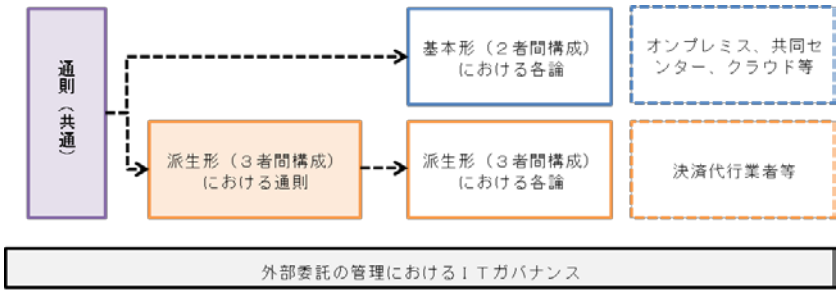
a. 方針・規程
b. 組織体制
c. サイバー攻撃対応態勢
d. 人材（要員・教育）

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。IT ベンダー等とのシステムの開発・運用や、クラウドベンダー等との２者間構成の委託に加え、決済代行業者等のように、IT ベンダーと金融関連サービスを提供する性質を併せ持つ関係者を含む、３者間構成について、「外部の統制」における考え方を解説する。（[図 12] を参照）

コメント [FISC19]:
外部の統制について、改めて整理した。
基本形（３者間）は主に外部委託報告書から、派生形（３者間）は主に FinTech 報告書から、考え方を取り入れている。



［図 12］外部の統制における考え方

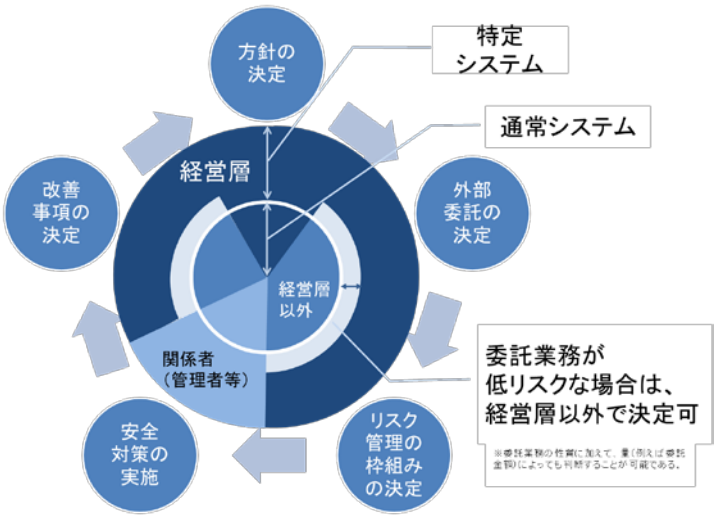
[19] 基礎基準のうち、「～することも可能である」として軽減策を示している場合、特定システムを除き、「可能である」とした内容を実施することができる（統制基準・実務基準共通）。

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、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 13 を参照])

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



[図 13] 外部委託の管理プロセスにおける IT ガバナンス

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。これは再委託を含む業務委託の全体を把握することと同義である。特に再委託先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確実に実施しているかを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. 委託先への監査権の明記

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、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、委託先のみならず再委託先への監査権に関する条項を盛り込むことが必要であり、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、高い可用性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[20]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」や、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、SLA 等を締結するなど、必要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

決済代行業者等は、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、

コメント [FISC20]:
FinTech 報告書を基に特徴（定義）と考慮点を修正した。

20 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。

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、決済代行業者等を加えた３者構成について、安全対策上、２者間構成である基本形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決済代行業等に関する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 ベンダーに決済代行業者等を加えた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、決済代行業者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、決済代行業者等の安全対策遂行能力を確認したうえで、仮に決済代行業者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、決済代行業者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望ましい。すなわち、この問題を解決するには、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との整合性を維持しつつ、その責務を、３者間構成の各類型における役割や、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を指す。

c. リスク特性に合う管理策の適用

決済代行業者等のシステムが、金融機関等の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、リスク事象を金融機関等の特定システム本体に波及することを防止が可能な場合は、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。

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、金融機関等が IT ベンダーへ委託する形態において、決済代行業者等または、IT ベンダーが委託先となる形態である。この場合、委託先が IT ベンダー、再委託先が決済代行業者等という形態もあり得る。基本形における、オンプレミスと同様の考

コメント [FISC21]:
FinTech 企業を含む３者間構成の形態として、FinTech 報告書のタイプⅠⅡⅢを整理し、ⅠとⅡを統合してタイプＡ、Ⅲ（オープン API 等）をタイプＢとした。

え方に、派生形の通則を付加した形態として整理できる。

このため、タイプＡの安全対策の在り方としては、まず、金融機関等は、決済代行業者等の安全対策遂行能力を確認したうえで、IT ベンダー及び、決済代行業者等と合意の上、従来の安全対策基準における外部委託に関する責務を、３者間で再配分することを考慮する必要がある。再配分に当たっては、「同等性の原則」にしたがって、必要な範囲を超えて関係者の負担が増加することがないよう留意する必要がある。

また、決済代行業者等が金融機関等の子会社となる形態も考えられる。この場合、金融機関等において、子会社に対する責任が付加される点を除いては、考慮点に差異はなく、同等性の原則ならびに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、金融機関等以外の事業者が、金融関連サービスを主として提供するケースである。この場合、金融機関等が担う金融関連サービスに対する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、決済代行業者等が、利用者からの決済指示を受け、預取金融機関の勘定系システムに対し入出金の指示を行うなど、金融機関等に代わり、決済代行業者等が金融関連サービスを提供するため、システムの安全対策は原則的には決済代行業者等が担うものの、顧客データの保護など、一部の責務について金融機関等がその安全対策の確保を決済代行業者等に求めるなど、部分的な責務が金融機関等において発生する場合を指す。

タイプＢにおいて、対象となるシステムは決済代行業者等が運用することを想定しているものの、金融機関等においても部分的な責務が発生することから、これらは金融情報システムに準じて取り扱うことが妥当である。この場合、同等のリスク特性を持つ金融情報システムにおける安全対策に対し、同等性の原則、責務の再配分などを踏まえ、金融機関等が実施する金融関連サービスと比較し、安全対策の水準において整合性が保たれることが必要となる。

なお、決済代行業者等が運用するシステムが、金融機関等のシステムと接続する場合、本人確認手続きや、顧客情報の保全等は必要最低限実施すべき対策と考えられる。このため、これらの金融関連サービスを適用する場合においては、基礎基準で示した安全対策を準用[21]することが求められる。

コメント [FISC22]:
FinTech 報告書 p 19 を基に**追加**
「顧客に関するデータの保全、または本人確認に係る部分に限定されると解されることから、この部分について、FinTech 企業において有効な安全対策が実施され、その効果が実現されていることが検証できれば、金融機関のリスク管理策としては十分と考えられる。」

[21] 「準用」とは、安全対策基準の中で、限定的な一部の安全対策について実施することを言う。例えば、預取金融機関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、「情報の保全」「認証」に関連する安全対策を中心に、安全対策を選択することが求められる。

【資料１－３】

平成29年6月16日
公益財団法人　金融情報システムセンター

説明資料（安全対策基準新構成案）

カテゴリⅠ	概要	カテゴリⅡ	概要	カテゴリⅢ	概要	新基準番号案	基準小項目	旧基準番号
Ⅰ　統制基準	「内部の統制」及び「外部の統制」に関する基準・解説等から構成する基準	1　内部の統制	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、管理態勢等を整備するために実施する対策	(1) 方針・規定	セキュリティポリシーの策定に関する基準	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	セキュリティ管理体制の整備に関する基準	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	サイバー攻撃対応態勢に関する基準	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）	教育・訓練・要員管理に関する基準	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	外部委託管理等に関する基準として、外部への統制を具体化した対策	(1) 方針・計画	外部委託方針策定に関する基準	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。	外部委託関連基準として再編の予定
						統22	外部委託先の選定手続きを明確にすること。	
				(2) 契約・業務管理	外部委託契約の契約、業務管理、終了に係る手続き等に関する基準	統23	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24	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27	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	金融機関相互で利用するシステム・ネットワークのサービスに関する基準	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。	運90-1
Ⅱ　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、運用管理、システム企画・開発及び防災・防犯等に関する実務的な対策に関する基準・解説等から構成する基準	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

【資料１－３】

平成29年6月16日
公益財団法人　金融情報システムセンター

説明資料（安全対策基準新構成案）

カテゴリⅠ	概要	カテゴリⅡ	概要	カテゴリⅢ	概要	新基準番号案	基準小項目	旧基準番号
				(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
		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	共同センターにおける固有基準	実90	共同センターにおける有事対応方針を明確にすること。	新設予定
		10 FinTech・クラウド関連		(1) FinTech・クラウド関連	クラウド及びFinTech利用における固有基準	実91	（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) ハードウェアの障害予防策		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

【資料１－３】

平成29年6月16日
公益財団法人　金融情報システムセンター

説明資料（安全対策基準新構成案）

カテゴリⅠ	概要	カテゴリⅡ	概要	カテゴリⅢ	概要	新基準番号案	基準小項目	旧基準番号
				(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	（現在の構成と変更なし）							
Ⅳ 監査基準	「システム監査」のみで構成する基準	1 システム監査	統制、実務及び、設備に対する監査をするための体制の整備や手順	(1) システム監査	システム監査に関する基準	監1	システム監査体制を整備すること。	運91

【資料２－１】
平成２９年６月１６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52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　6/21（水）（改訂原案（前説）に対する事後意見）

会社名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

お名前：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

資料番号	項番	ご意見
（例） 資料１－２	（例） Ⅱ．１． （３）	・・・