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

エグゼクティブサマリー

平成 28 年６月

公益財団法人 金融情報システムセンター

近年、わが国金融機関の情報システム関連業務において、外部委託への依存度が、非常に高い水準で推移するとともに、共同センターに代表される情報システムの共同化の進展をはじめとして、その形態は多様化している。

一方で、銀行等の業務の再委託先等を、当局の報告徴求・立入検査の対象に加える銀行法等の改正があり、再委託管理の在り方を見直すことが必要となっている。また、共同化の進展等に伴い、IT 人材の育成・確保を課題とする金融機関の数が増えている状況にある。

以上のように、情報システムの外部委託を巡る環境は、近年非常に大きく変化しているが、これらの課題は、いずれも根の深い問題であり、情報システム部門単独で解決できるものは少なく、経営層を含む全社的な取組み、すなわち IT ガバナンスを、まず、考えなければならない。

翻って、金融情報システムセンター（以下「FISC」という）では、一昨年度に「金融機関におけるクラウド利用に関する有識者検討会」を開催し、わが国の金融機関が、クラウド技術の特性とリスクを正確に把握したうえで、リスクを最小限に抑えつつ、その最新技術のポテンシャルを最大限に活用するための安全対策の在り方について、議論していただいた。その結果を報告書として公表した後に、それをもとに『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）の改訂が行われ、外部委託の一形態であるクラウドのリスク管理策を拡充したところである。

そうした外部委託の特殊形態であるクラウドの考え方も取り入れつつ、それと整合性を取る形で、自行・自社システムの委託や共同センターといった、より一般的な外部委託に関しても、前述の課題に対応すべく、その管理策の見直しが必要であると考え、「金融機関における外部委託に関する有識者検討会」を立ち上げることとなった。

本検討会では、学識経験者や金融機関、ベンダー等の委員と官庁等のオブザーバーが参加し、わが国金融機関における外部委託管理の在り方について、IT ガバナンスやリスクベースアプローチの観点も踏まえて抜本的に検討を行い、外部委託管理の実効性向上に資する方策について、明確かつ具体的な指針を示すべく議論が行われ、本報告書が取りまとめられた。

Ⅰ　近年の外部委託動向と外部委託を巡る環境変化

◆外部委託先等で近年発生する不正事案

- FISC の取組み

  当面の対応として、コンピュータ室への入退室管理強化、システムへのアクセス権限の厳格化、不正使用の発見・防止のための監視方法の強化等については、昨年度の FISC 安全対策専門委員会・検討部会で議論のうえ昨年６月に安対基準を改訂し、必要な手当てを実施した。

- 課題認識

  リスク管理態勢を含めた根本的な対処方法については、IT ガバナンスの観点も含めた議論が別途、必要な状況にある。

  不正事案を受けて、中でも共同利用型のシステムについて、以下の課題が指摘されている。

  ・利用金融機関が共同でガバナンスを発揮する態勢構築の必要性

  ・共同監査の必要性

  これらを含めた外部委託本体の議論にあたり、クラウドのリスク管理策とも平仄をとりつつ、検討する必要がある。

◆共同化の進展

- FISC の取組み

  外部委託の一形態であるクラウドについては、一昨年度の「金融機関におけるクラウド利用に関する有識者検討会」を経て安対基準を改訂し、クラウドのリスク管理策（利用検討時における事業者選定手続きの明確化やデータ所在の把握、契約締結時における SLA の合意やベンダーロックイン防止策、サービス利用中のデータ漏洩防止策、第三者監査・モニタリング態勢整備等を策定、また、業務の重要度に応じ簡易なリスク管理策についての記載）を拡充した。

- 課題認識

  上記クラウドの有識者検討会から得られた知見をもとに、より一般的な外部委託における管理策の在り方についても、見直す必要がある。

◆人材育成の必要性

- FISC の取組み

  IT 人材育成に関して、FISC 調査部と金融庁とで共同研究を行おうとしており、具体的な育成計画や実施方法を示すほかに、中長期計画に IT 人材育成を織り込む重要性を明確化していくこと等を検討している。

➢ 課題認識

各々の金融機関において、経営目標、事業目標の達成に必要とされるITスキルや人員規模を明らかにしたうえで、それらを継続して確保していくために、人員計画をどう策定し、経営層の関与によりそれらをいかに実現していくのかを考えていく必要がある。

◆再委託管理を巡る諸問題（銀行法等の改正）

➢ 課題認識

銀行法等の改正により拡大された検査権限との関係で、再委託管理の在り方を見直す必要が出てきている。

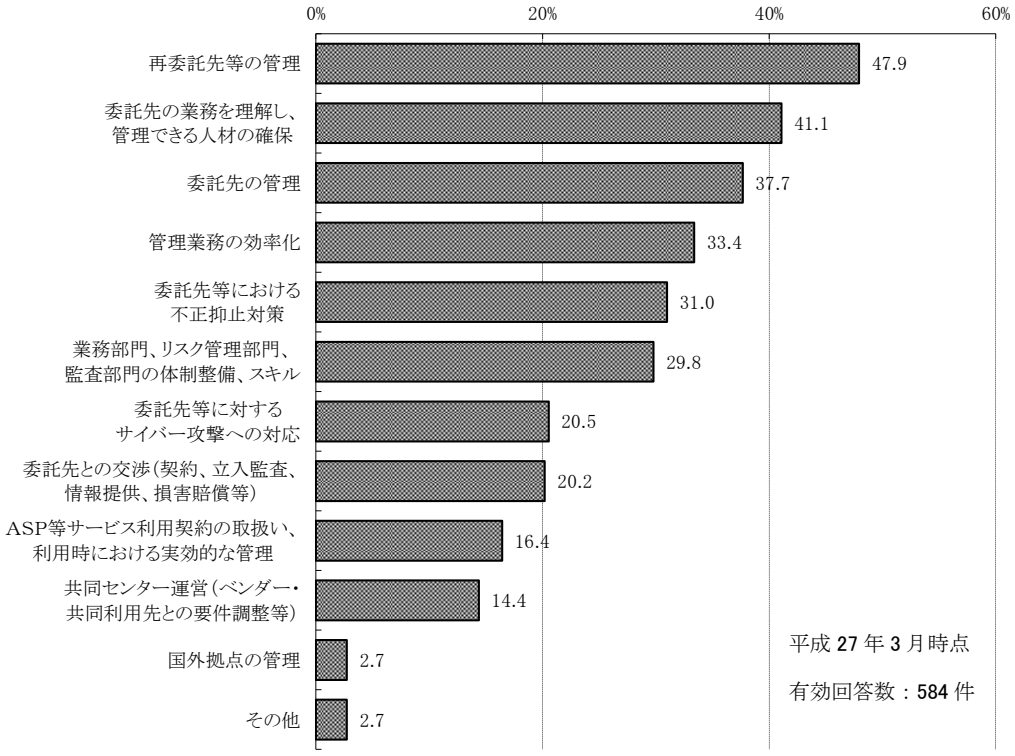
◆ITガバナンス検討の必要性

上記のいずれもが金融機関全体に及びうる課題であり、これらに適切に対処するには、それぞれのリスクを評価したうえで経営層が適切に関与していくこと、つまりITガバナンスの観点が不可欠となる。

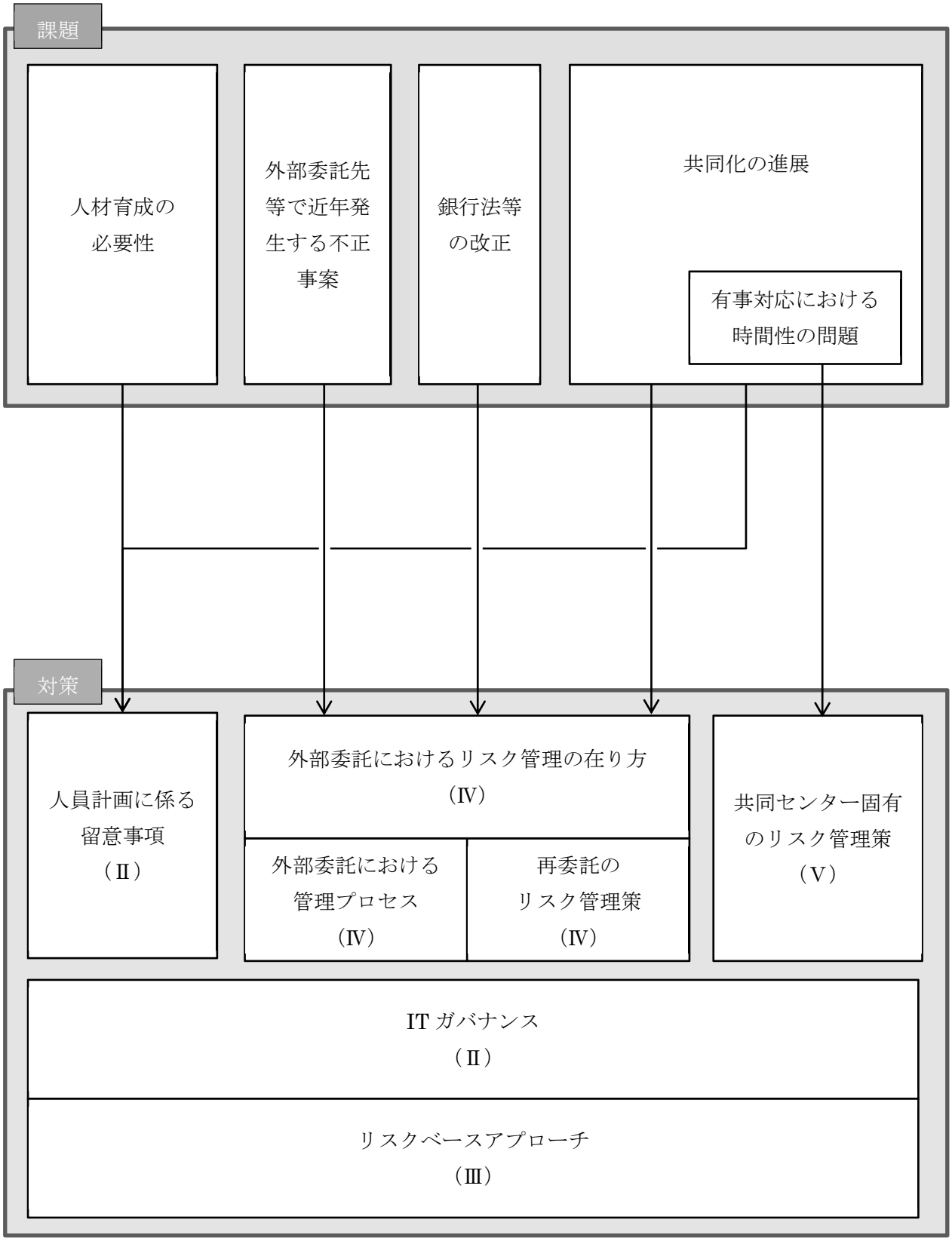
（図表）外部委託管理における金融機関の課題認識

再委託管理や人材確保をはじめ、経営層の関与が不可欠な課題が並んでいる。

（預金取扱金融機関、保険、証券、クレジット等）（平成27年FISCアンケートより）



（図表）本検討会で取り上げた課題とその対策



Ⅱ　IT ガバナンスと IT マネジメント

◆安全対策上必要となる IT ガバナンスにおいて、経営層は以下の役割と責任を果たすことが必要である。

（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

①安全対策に係る方針の決定

a.システム戦略方針

b.システムリスク管理方針

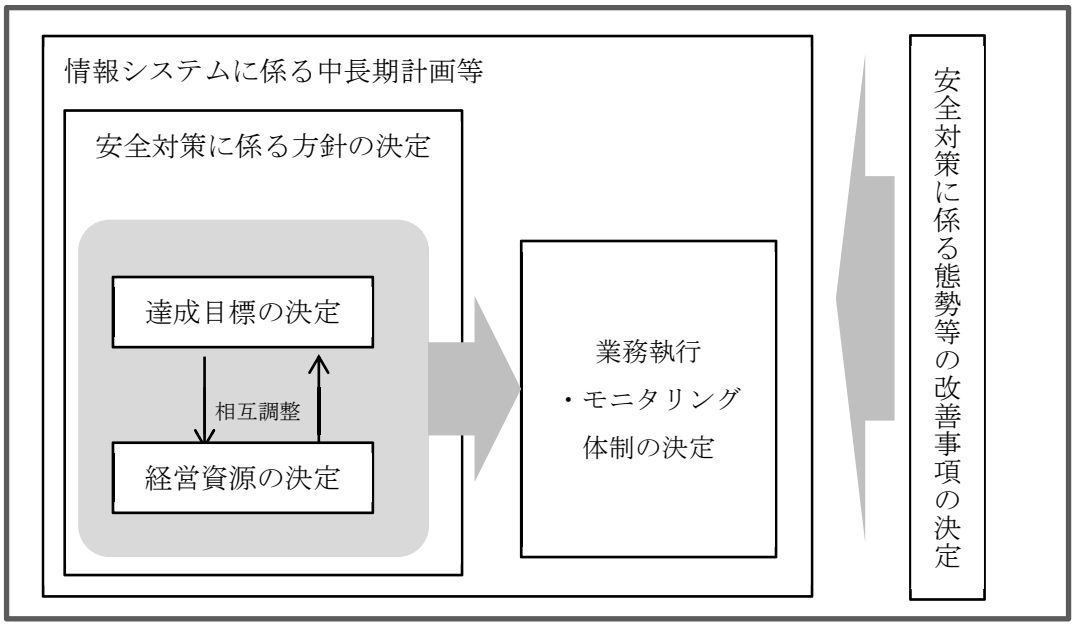
c.安全対策の達成目標

d.安全対策へ投下する経営資源

②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

（２）安全対策に係る態勢等の改善事項の決定

（図表）経営層が決定すべき安全対策に係る重要事項



◆安全対策上必要となる 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必要である。

（1）管理者

①内部規程・組織体制等の整備

②個々の情報システムに対する安全対策の決定

③内部規程・組織体制等の見直し

④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

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

（3）ユーザー

安全対策に配慮したビジネスモデルの企画・投資効果の達成・業務要件の提示

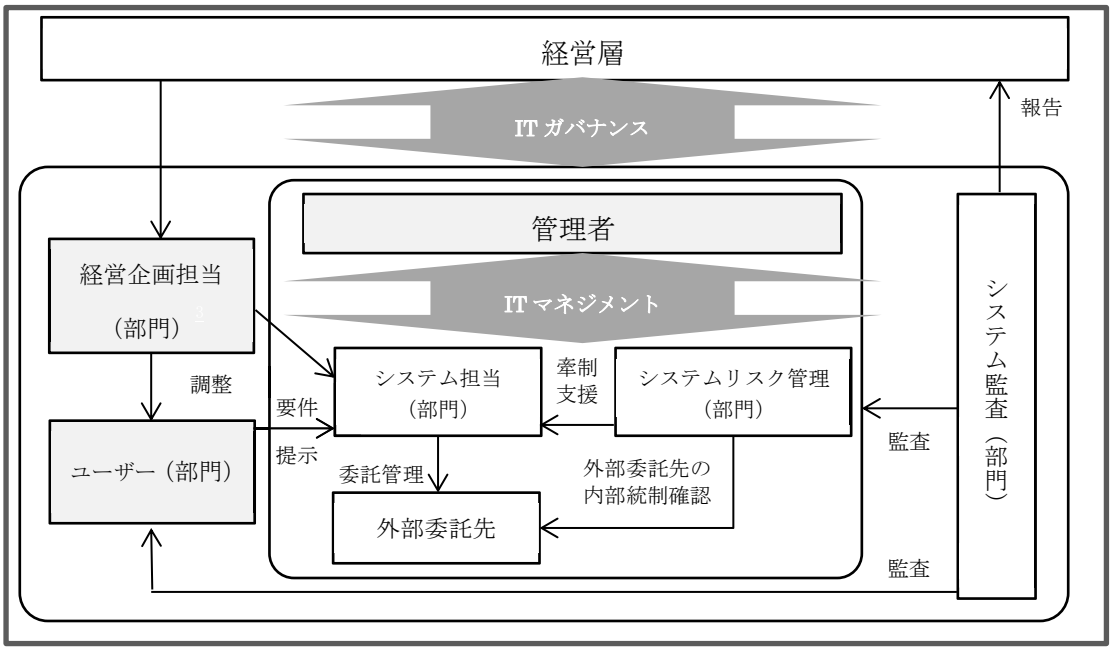
◆経営層は、「人員計画」を策定するにあたり以下の点に留意することが必要である。

（1）必要な人員数だけでなく、人員の質を含む IT 人材について、具体的に把握すること

（2）足元の IT 人材の現状を踏まえたうえで、人材の中長期育成計画を策定すること

◆ここで決定を行う「経営層」は、重要事項の内容に応じて、取締役会に限らず、権限移譲を受けた取締役・執行役等まで、幅広く解することが可能である。

（図表）情報システムの安全対策に携わる関係者（例）



Ⅲ　リスクベースアプローチ

◆リスクベースアプローチは、海外先進諸国においては、監督当局及び金融機関等の共通認識となっており、わが国の金融機関等が情報システムに対する安全対策の在り方を検討する際にも、その前提とされるべき重要な考え方である。

◆リスクベースアプローチを踏まえて､安全対策における基本原則を以下のとおり定める。

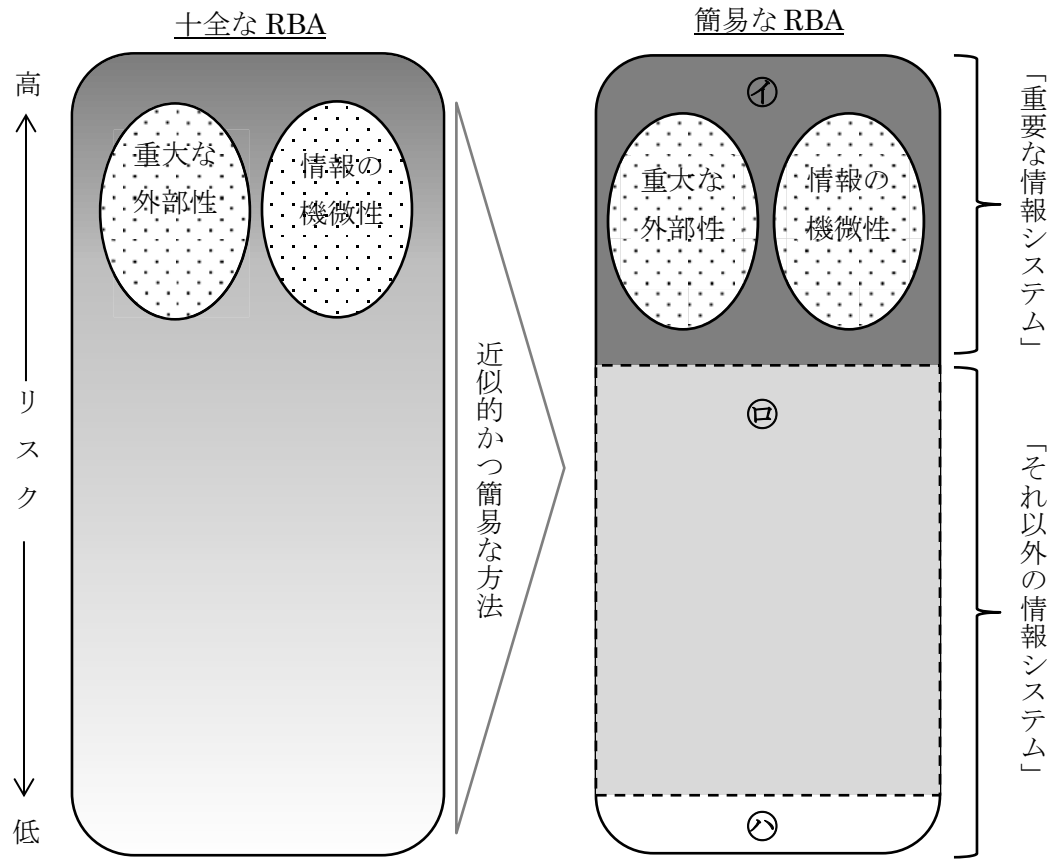
（1）情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、必要十分な内容で決定されるべきである。
（2）情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システム予算内での新規開発等との調整のみならず、経営資源全体も視野に入れ、企業価値の最大化を目指して、決定されるべきである。
（3）上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自に決定することが可能である。
（4）なお、金融機関等が保有する重大な外部性を有する情報システム及び機微情報を保有する情報システムにおいては、上記に加えて、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るべきである。

◆基本原則を踏まえて、金融機関等は、「十全なリスクベースアプローチによる IT ガバナンス」を目指すことが望ましい。なお、それを目指す過程においては、情報システムを「重要な情報システム」「それ以外の情報システム」に二分して個々に安全対策を実施する「簡易なリスクベースアプローチによる IT ガバナンス」を採用することが可能である。

◆基本原則等を踏まえて、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。

（1）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。
（2）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（以下「CP」という）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。
（3）経営層が、諸法令を遵守するとともに、安対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 CP 等を用意し、かつ、有事においては、CP を踏まえつつ臨機応変に対応している限りにおいては、客観的立場からみれば、法的責任を果たしているものと評価されるべきである。

（図表）リスクベースアプローチ（RBA）に従った安対基準適用方法



「重大な外部性」「情報の機微性」を有する情報システム等には【B】を適用。それ以外は独自に選定可能。	㋑には【B】を適用。 ㋺には【C】を適用。（【C】がない場合は【B】を適用。） ㋩は安対適用対象外。

【A】「望ましい」＞【B】「すること」「必要である」＞【C】「可能である」

基準の語尾が【A】【B】・・・「高い安対基準」
基準の語尾が【C】　　・・・「必要最低限の安対基準」

注１　金融機関等は「重大な外部性」「情報の機微性」を有するものと同等以上のリスクを有すると判断したシステムについては、【B】を適用。金融機関等の判断により、さらに高リスクと認識された場合、【B】より厳格なルールである【A】「望ましい」、あるいは【A】以上に厳格なルールを独自に設定しうる。

注２　簡易な RBA は便宜的に「重要」と「それ以外」の２区分としているが、例えば「それ以外」をさらに細分化し、適用される基準を分けるなど、中間形態もありうる。

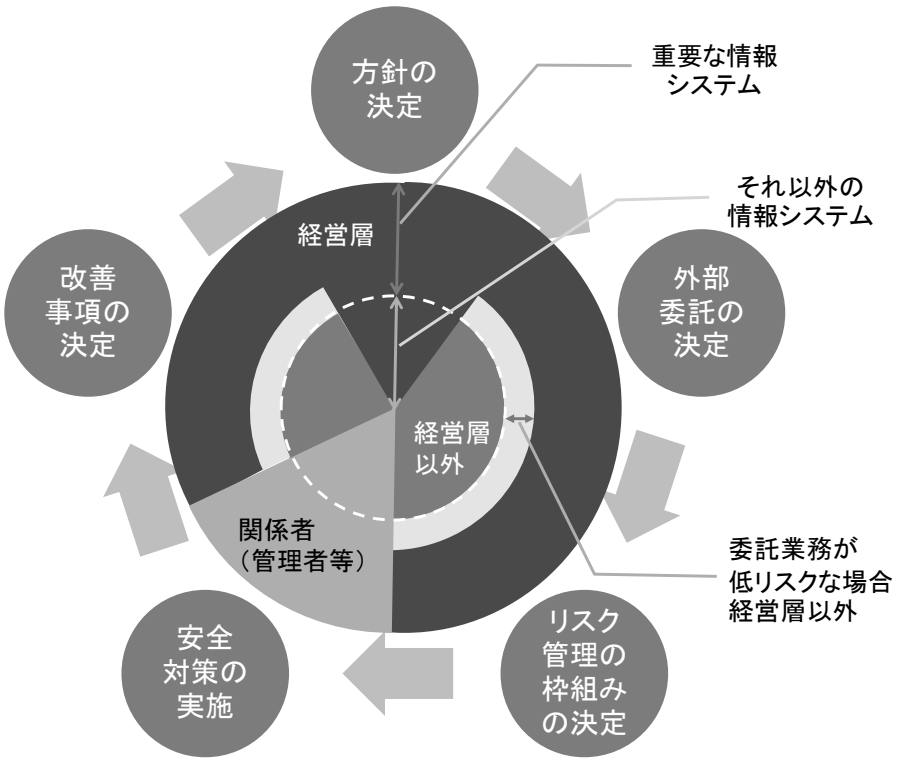
Ⅳ　外部委託におけるリスク管理の在り方

◆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、金融機関等の経営層の責務でもある。

◆再委託を巡る諸課題を踏まえ、外部委託における IT ガバナンスにおいて、経営層等は以下の役割と責任を果たすことが必要である。

（１）情報システムの外部委託に係る方針の決定（経営層）
（２）個別情報システムの外部委託の決定
（３）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
　外部委託の管理フェーズに応じた安全対策目標、経営資源配分及び管理体制の決定
（４）各管理フェーズにおける安全対策の実施（関係者）
（５）外部委託におけるリスク管理に係る改善事項の決定
※リスクベースアプローチを踏まえて、（２）（３）（５）は、「重要な情報システム」は経営層が決定し、「それ以外の情報システム」は経営層以外で決定することが可能。「重要な情報システム」でも、業務が細分化された結果等、委託業務が低リスクな場合も本代替策が可能。

（図表）外部委託の管理プロセスにおける IT ガバナンス



◆金融機関等は、委託先を通じた統制の構造が複雑化するなかにおいても、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。そのうえで、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。

◆そのうえで、現行の外部委託の安対基準、及びクラウドサービスの安対基準を参考としながら、追加されるべき運用の外部委託におけるリスク管理策は以下のとおり。

（1）再委託先の選定要件を定めること

（2）委託先による再委託先選定の妥当性を検証するため再委託先の事前審査を行うこと

（3）委託先との契約締結時、金融機関による再委託先への監査権を明記すること

（4）再委託先へ監査を実施する場合、自己の責任において監査を行うこと

（5）重要な情報システムが外部委託される場合、平時に、CP を委託先等も含めて策定し、委託先等と共同で訓練を実施すること

有事に CP が発動された場合、委託先等の CP の実施状況を監督すること

※リスクベースアプローチを踏まえて、「重要な情報システム」以外の情報システムは、委託先の再委託先に対する事前審査の内容が金融機関等と同等以上であることをあらかじめ検証することをもって（2）に代替可能。（3）は監査権を明記しないことが可能。「重要な情報システム」でも、業務が細分化された結果等、委託業務が低リスクな場合も、（2）及び（3）において本代替策が可能。

開発の外部委託は、「重要な情報システム」以外の情報システム等と同様に本代替策が可能。

（図表）再委託で新たに追加すべきリスク管理策

	システム種別	選定要件策定	事前審査	監査権の明記	有事対応
運用の外部委託	重要な情報システム	○	○	○	○
	結果的に低リスクとなる場合	○	△1	△2	－
	それ以外の情報システム	○	△1	△2	－
開発の外部委託	重要な情報システム及びそれ以外の情報システム	○	△1	△2	－

○　リスク管理策の適用が必要

△1　委託先の再委託先に対する審査・管理プロセスの検証をもって、再委託先に対する個別の事前審査に代替させることが可能

△2　委託先との契約において再委託先への監査権を明記しないことが可能

Ⅴ　共同センターにおけるリスク管理の在り方

◆共同センターは、複数の金融機関の情報システムが委託される形態であることから、単一金融機関の委託と同程度まで、円滑に、委託者間の意思統一が可能とは、必ずしも考えられない。

◆特に、サイバー攻撃の活発化、IT の高度化による急速な社会的情報拡散、さらには決済の 24 時間 365 日化が進められる現況においては、万一の対策実施の遅れが、信用不安の拡大といった深刻な結果をもたらすという問題、すなわち「有事対応における時間性の問題」が、従来以上に深刻に受け止められるべきと考えられる。

◆こうした問題への対応に当たっては、有事に備えた経営資源配分等、経営層の役割と責任が極めて重要である。

◆そのため、まず、利用金融機関の経営層は、有事対応における時間性の問題の深刻化を認識することが必要である。そのうえで、利用金融機関の経営層は、共同で、その問題を解決するためのリスク管理策について、速やかに検討を進めることが必要である。

◆検討に当たっては、有事等に備えて必要となる IT 人材を、継続して配置できるよう、利用金融機関もしくは委託先と共同で、人員計画を策定することが望ましい。

◆リスク管理策は、システムが共同化されている程度や、利用金融機関相互の関係等を踏まえて、検討されるべきものであるが、例えば、利用金融機関から選定された責任者を共同センターに設置することも考えられる。

◆共同センターの監査に当たっては、クラウドサービスで検討された共同監査スキームを参考とすることが有益である。

Ⅵ　今後の安対基準等改訂の考え方

◆本検討会の提案に基づき、今後、安対基準等当センターのガイドラインの改訂を進めていくこととなるが、以下の点を考慮することが必要である。

（１）激変緩和措置の必要性

今回の改訂は、従来の改訂と異なり、安対基準適用の考え方から抜本的に変更を行うこととなり、安対基準を参考とする金融機関等においては、その影響は甚大であることが予想される。

そのため､こうした安対基準の変更自体がリスク要因となりうること等を勘案して、現在安定的に運営されている情報システムについては、従来どおりの取扱いを継続することとしつつ、システムの更改時や新システムの導入時に、変更後の安対基準等へ順次移行を図ることを可能とする。

ただし、現状で既に問題を抱え、変更後の高い水準でのリスク管理策の適用が要請されている場合においては、早期の移行が必要である。（例　共同センターの有事対応等責任者の設置等）

（２）FinTech に関する有識者検討会（仮称）との関係

当センターでは、今年度、外部委託に関する有識者検討会に続いて、FinTech に関する有識者検討会（仮称）（以下「FinTech 検討会」という）を計画している。FinTech と総称される高度な IT を利用した金融サービスは、外部委託の形態で利用されることが多いと考えられることから、外部委託に関する有識者検討会の成果に、修正や追加が必要となる可能性がある。

そのため、安対基準等の改訂は、FinTech 検討会の終了を待って、外部委託及び FinTech の両検討会の成果を踏まえて、行うこととする。

◆なお、現時点で想定している安対基準の改訂方針は以下のとおりである。

（１）安全対策の基本原則等の追加

リスクベースアプローチを踏まえた、新たな安全対策の在り方を、安対基準の考え方として明記する。

（２）対象とするシステム及び適用に当たっての考え方の見直し

基本原則等を踏まえて、安対基準の対象とするシステム及び適用に当たっての考え方について見直しを行う。

（３）個々の基準の再整理

上記の改訂を踏まえて、まず、外部委託の基準について、個々に再整理を行う。それ以外の基準の再整理については、その後に検討を行う。

「金融機関における外部委託に関する有識者検討会」委員・オブザーバー名簿

（敬称略）

座長	岩原 紳作	早稲田大学 大学院法務研究科 教授
座長代理	渕崎 正弘	株式会社日本総合研究所 代表取締役社長
委員	國領 二郎	慶應義塾常任理事、慶應義塾大学総合政策学部教授
	堀江 正之	日本大学 商学部 教授
	上山 浩	日比谷パーク法律事務所 パートナー弁護士
	亀田 浩樹	株式会社三菱東京 UFJ 銀行 執行役員 システム部長 （第４回まで）
	米井 公治	株式会社みずほフィナンシャルグループ 執行役員 IT・システム企画部長 （第５回から）
	坂上 久司	株式会社池田泉州銀行 事務統括部長
	森田 英子	BNP パリバ証券株式会社 取締役 チーフオペレーティングオフィサー
	鈴木 正巳	巣鴨信用金庫 事務部 部長
	真田 博規	住友生命保険相互会社 情報システム部 担当部長
	浅沼 公誠	あいおいニッセイ同和損害保険株式会社 IT 統括部 システムリスク管理グループ長
	菱田 剛	野村ホールディングス株式会社 IT 統括部 IT 管理課（エグゼクティブディレクター） （第１回まで）
	植村 元洋	野村ホールディングス株式会社 IT 統括部 次長 兼 IT 管理課長（エグゼクティブディレクター） （第２回から）
	渡部 直人	日本アイ・ビー・エム株式会社 金融第三インダストリーコンサルティング アソシエイトパートナー
	石川 晃久	株式会社日立製作所 ICT 事業統括本部 OSS ソリューションセンタ 部長
	林 徹	株式会社 NTT データ 第二金融事業本部 企画部長
	藤田 雅人	富士通株式会社 金融・社会基盤営業グループ シニアディレクター
	田中 富士夫	日本ユニシス株式会社 金融システム第二本部 金融システム一部　信金アウトソーシングセンター長

	成田 光太郎	日本電気株式会社 パブリックビジネスユニット 主席システム主幹
	中村 元彦	日本公認会計士協会 常務理事（IT 担当）
オブザーバー	田部 伸夫	金融庁 検査局 総務課 主任統括検査官 兼 システムモニタリング長（第５回まで）
	片寄 早百合	金融庁 検査局 総務課 主任統括検査官 兼 システムモニタリング長（第６回）
	岡田 拓也	日本銀行 金融機構局 考査企画課 システム・業務継続グループ長 企画役
	大森 一顕	総務省 情報流通行政局 情報流通振興課 情報セキュリティ対策室長
	瓜生 和久	前経済産業省 商務情報政策局 情報セキュリティ政策室長

（金融情報システムセンター事務局）

理事長		渡辺　達郎
常務理事		高橋　経一（第６回）
企画部	部長	堀内　俊宏（第４回まで）
企画部	部長	小林　寿太郎（第５回から）
企画部	次長	藤永　章
調査部	部長	中山　靖司
監査安全部	部長	西村　敏信
総務部	部長	阪　　章伸（第４回まで）
総務部	部長	水野　幸一郎（第５回から）
総務部	特別主任研究員	郡山　信

◆事務局スタッフ

柴田　晃宏、宮原　武也（第４回まで）、仲程　文徳（第５回から）、
岡本　一真、三浦　哲史（第５回から）

（参考）検討会の開催日程

第１回（平成 27 年 10 月 26 日）、第２回（同 12 月１日）、第３回（平成 28 年２月３日）、第４回（同３月 23 日）、第５回（同５月 12 日）、第６回（同６月 27 日）