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

平成 28 年６月

公益財団法人 金融情報システムセンター

目　次

はじめに

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。

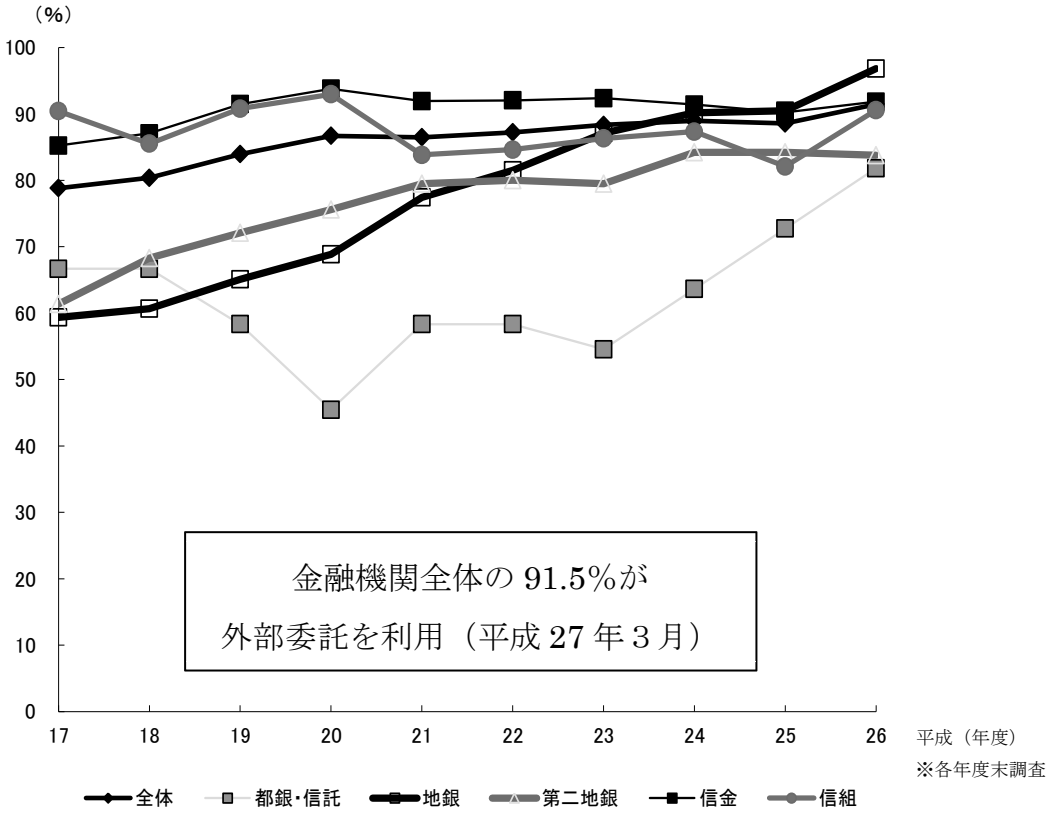
Ⅰ　近年の外部委託動向と外部委託を巡る環境変化

１．近年の外部委託動向

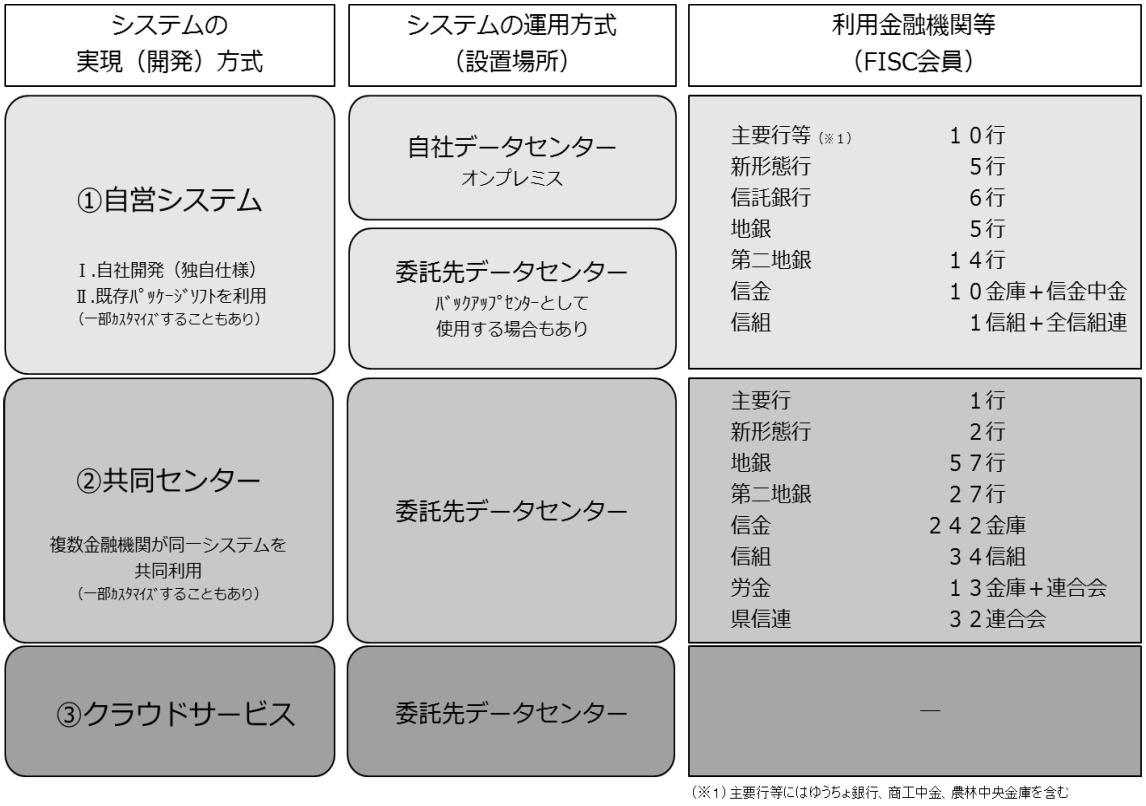
近年、金融機関のシステム関連業務における外部委託の進展が著しい。

・勘定系基幹システムにおける外部委託については、金融機関全体の 91.5%が利用している。（平成 27 年 3 月時点）

（図表１）外部委託の動向（FISC アンケートより）



（図表２）預金取扱金融機関の基幹システムの外部委託方式
（平成 27 年３月末時点　FISC 調査による）



（※1）主要行等にはゆうちょ銀行、商工中金、農林中央金庫を含む

２．外部委託を巡る環境変化

外部委託を巡る環境に最近大きな変化が生じている。

（１）外部委託先等で近年発生する不正事案

金融機関の再委託先、再々委託先で、スキルを有する管理者が不正事案を起こし、それらを契機として外部委託におけるリスク管理が見直され、FISC 安対基準も改訂されている。また、外部委託の現場においても、それぞれ管理策やノウハウの蓄積が進んでいる。

（図表３）近年の主な事案とその関連動向

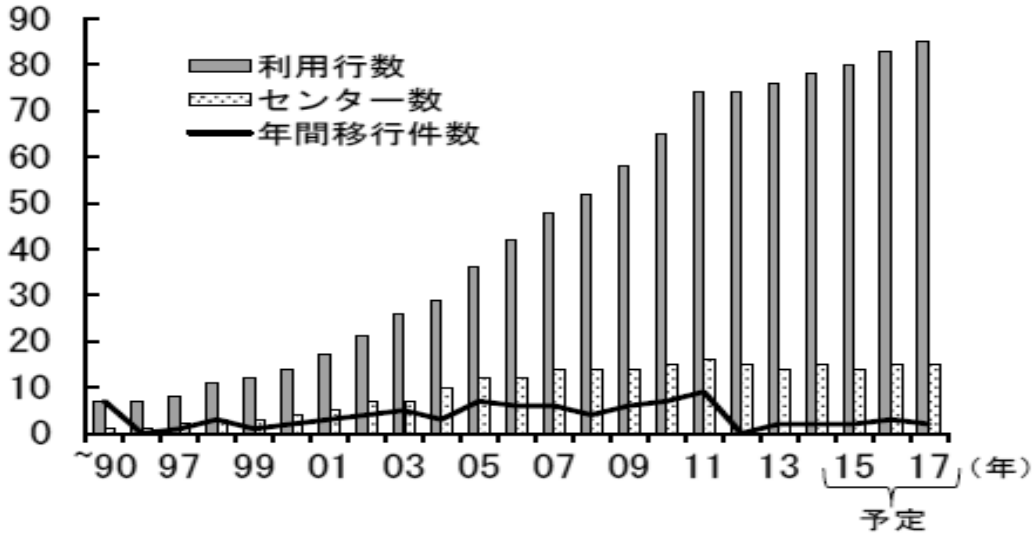
平成 24 年 11 月発表	共同センターの委託先社員によるキャッシュカード偽造事件
平成 26 年２月発表	地方銀行の再々委託先社員によるキャッシュカード偽造事件
平成 26 年３月	金融庁から金融機関に対し自主点検を要請

（２）共同化の進展

個社で委託するよりもコストメリットがより享受できることや、先行者のノウハウを活用できる観点等から、業態や対象業務を問わず、システムを共同して利用する形態が増えてきている。

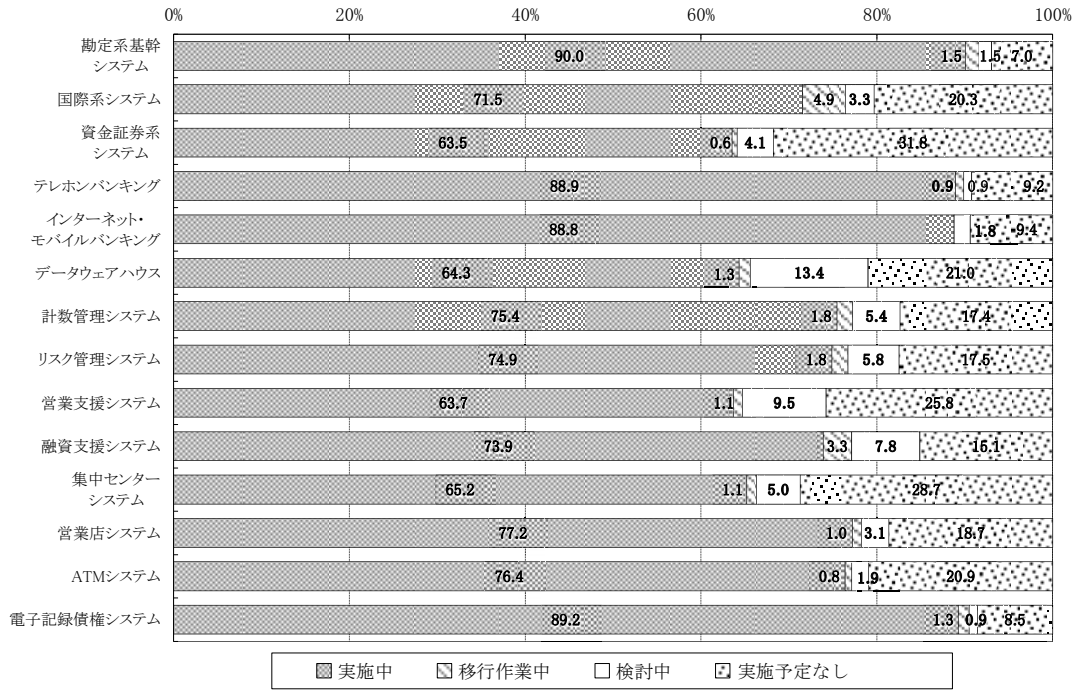
（図表４）勘定系システムの共同化の進展（地銀・第二地銀）

（平成 26 年 7 月金融庁 金融モニタリングレポートより）



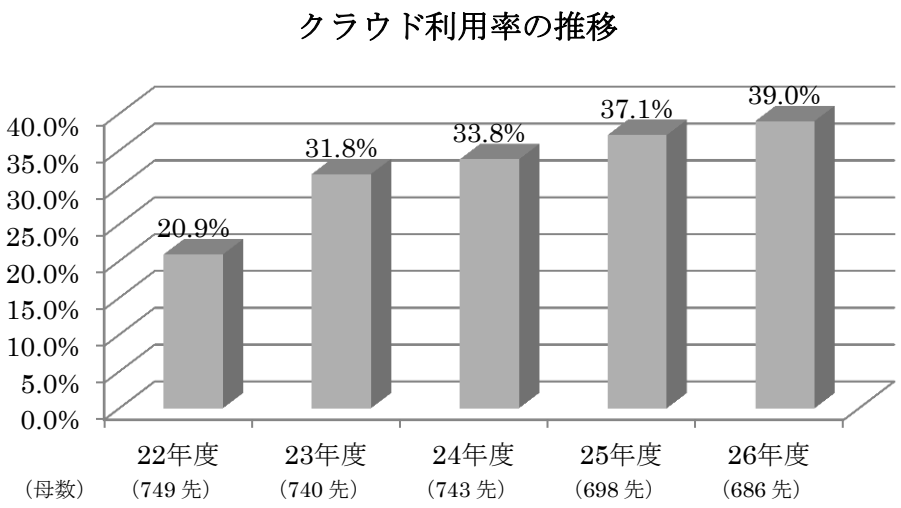
（図表５）多くのシステムで、共同センターが利用されている

（預金取扱金融機関）（平成 27 年 FISC アンケートより）



（図表６）クラウドの利用も増加傾向にある

（預金取扱金融機関、保険、証券、クレジット等）（FISC アンケートより）



（図表７）保険業界においては、クラウドの利用が進んでいる

（平成 27 年金融庁モニタリングレポートより）

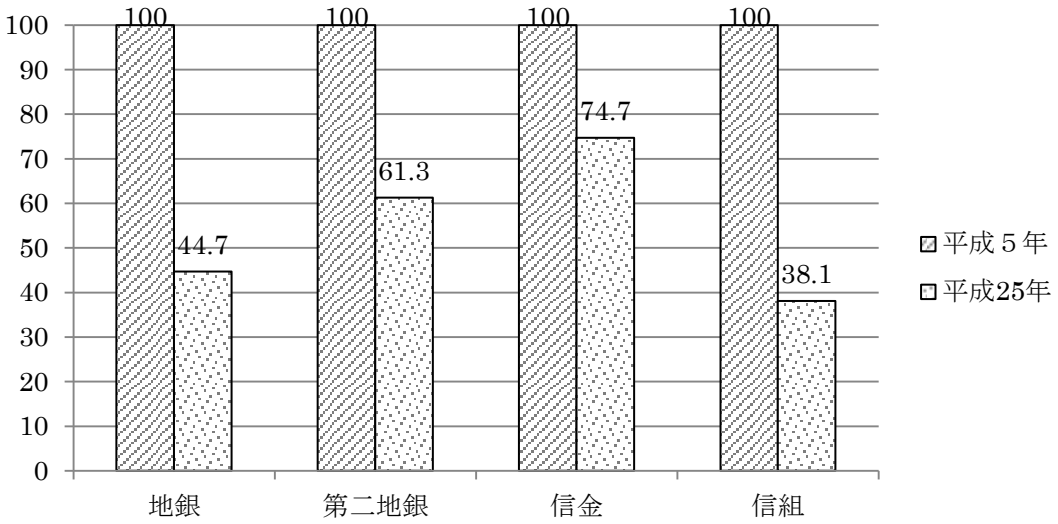
	利用比率	うち大手４社
生命保険会社(42 社)	83%	75%
損害保険会社(33 社)	76%	100%

（３）人材育成の必要性

システムの共同利用化の進展により、自社内の IT 人材が削減され、IT スキルの低下が課題となっている。

また、昨年 7 月に公表された金融庁の「金融分野におけるサイバーセキュリティ強化に向けた取組方針について」では、サイバー人材に関して、技術担当者だけではなく、意思決定や組織内への指示を行う経営層、さらにはこれを支える管理部門の職員に対しても意識の向上や知見の習得を求めており、スキル保有者の確保や育成が課題となっている。

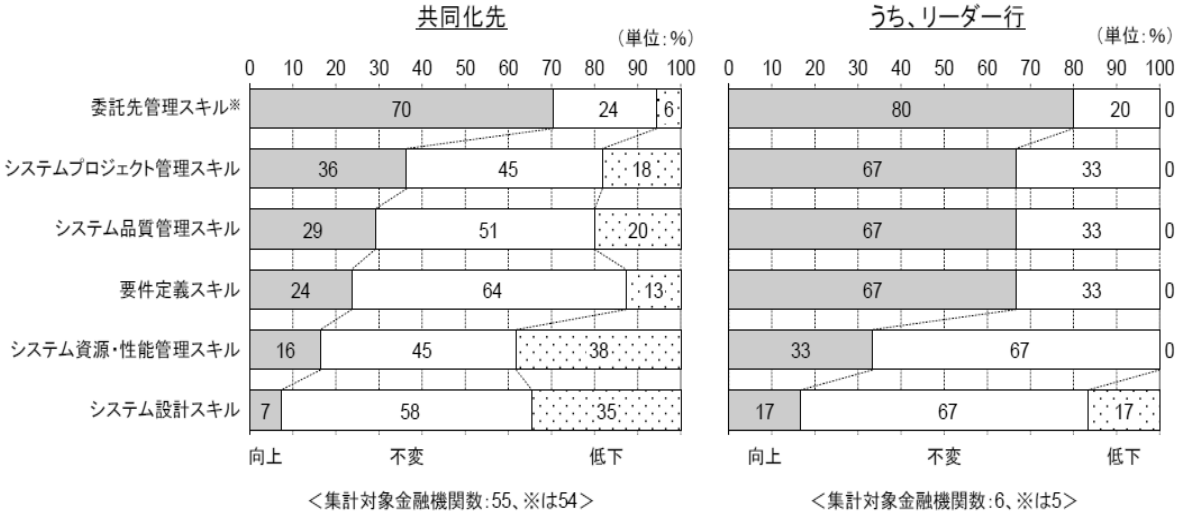
（図表８）システム部門の職員数の推移；平成５年度末を 100 とした場合の平成 25 年度末の割合（平成 26 年 FISC 調査）



（図表９）システム共同化を行う前後の自行職員スキルの変化

（平成 21 年日銀レポート『地域銀行 108 行へのアンケート調査結果』）

⇒共同化先（左）のスキル低下がリーダー行（右）に比して顕著である。



（４）再委託管理を巡る諸問題（銀行法等の改正[1]）

各金融機関においては、再委託先以降に関しても管理責任や説明責任が明示的に求められる一方で、どこまでやれば十分かが必ずしも明確でないこともあり、負担感は増している。

[1] 銀行等の業務の再委託先（二以上の段階にわたる委託を含む）を報告徴求・立入検査の対象先に加える。（平成 26 年 12 月１日施行）

３．これらの環境変化に対するFISCのこれまでの取組みと本検討会での課題認識

（１）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。

（２）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。

（３）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。

（4）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。

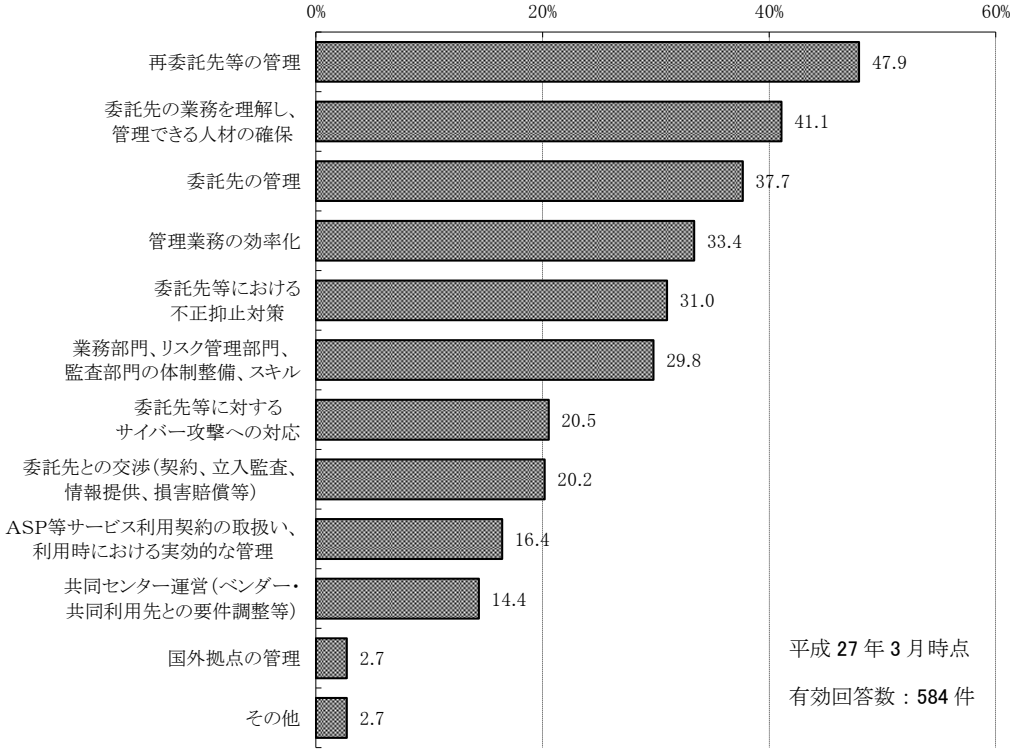
4．IT ガバナンス検討の必要性

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 10）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）



なお、検討に当たっては、IT ガバナンスについて、以下の定義を参考とする。

金融庁の定義（平成 27 年 7 月金融庁モニタリングレポートより）

> 金融機関において、経営戦略上重要な領域に適時・適切なシステム投資を行い、導入したシステムを効率的・安定的に運用すること、またこれらを適正に統制し、組織的に取り組むためのマネジメント態勢

IT ガバナンス協会の定義（FFIEC（米国連邦金融機関検査協議会）ガイドラインでも使用）

> 企業のガバナンス全体の構成要素であり、組織の IT が組織の戦略並びに目標を維持し、展開させることを保証するリーダーシップ、組織構造、さらにプロセスから構成されている。

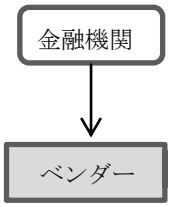
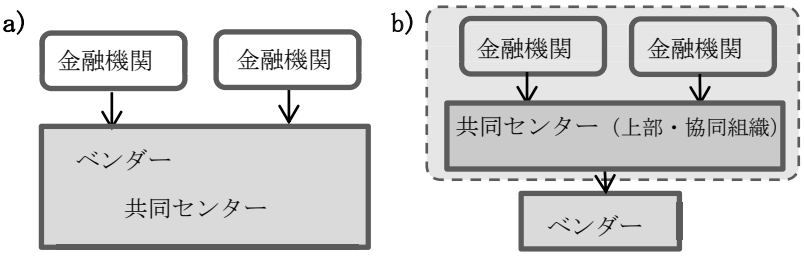
また、国内外の各種ガイドラインでは、システムの外部委託は一義的には IT マネジメントの一領域と位置づけられており、IT ガバナンスとともに IT マネジメントが重視されている。
検討に当たっては、こうした観点も参考としている[2]。

[2] その他に ISO38500（IT ガバナンス）等で定義されているガバナンスプロセス（評価、指示及びモニタ）も参考とした。なお、ISO に関してはガバナンス以外でも、ISO27014（情報セキュリティガバナンス）も参考としている。

５．外部委託の概念

なお、外部委託の概念については、金融機関がベンダーに委託、ないしはサービスを利用する場合を想定し、下表のとおり整理した。

（図表 11）システムに係る外部委託の範囲

対象	**【タイプＡ】　金融機関がベンダーに個別に委託（開発・運用）、ないしはサービスを利用する場合**	**【タイプＢ】複数の金融機関がベンダーへ委託（開発・運用）、ないしはサービスを利用する場合** （上部・協同組織が委託先の窓口となる場合を含む）
関係者	金融機関：ベンダー＝１：１	金融機関：ベンダー＝ｎ：１
モデル		
具体例	・自営システムの開発・運用（うち外部委託をしているもの） (パッケージのカスタマイズを含む) ・ハードウェア・ソフトウェア保守	**a)金融機関とベンダーが契約するケース** ・勘定系共同センター（地銀・第二地銀・信金・信組等） ・インターネットバンキング共同センター（ANSER 等） ・共同 CMS[3] ・クラウド ・データ保管サービス **b)上部・協同組織を通じてベンダーと契約するケース** ・SBK[4] ・アール・ワンシステム[5] ・JASTEM[6]

（注１）金融機関相互のシステム・ネットワークサービスの扱い

金融機関相互のシステム・ネットワークのサービスを利用する場合（全銀システム、統合 ATM、協同組織金融機関為替中継システム[7]等）は、金融庁の監督指針では「外部委託に準じたリスク管理を行う」としており、外部委託とは別の形態として整理できる。

⇒　先方との接続に際して、開始時・更改時等にシステム上の適切な対応がなされているかの確認や、疎通テストの実施等が求められるが、先方の運営状況の捕捉までは求められない（FISC 安対基準【運 90-1】）点で、上記の【タイプＡ・Ｂ】とは形態が異なるといえる。

[3] マルチバンクのファームバンキングサービスを提供するため、都市銀行をはじめ主要金融機関が共同で設立したセンター。
[4] 九州地区の第二地銀６行によりシステムセンターを共同運営する事業組合（共同センター）。
[5] 労金連合会が構築し、全国 13 労金と労金連合会が使用。
[6] 農林中央金庫が運営し、全国の農協・信農連が使用。
[7] 全信金システム（信金）、為替系システム（信組）、為替中継システム（農協）。

これらのネットワークは基幹インフラとしての機能を担っており、各金融機関が外部委託の管理と全く同様にサービス提供元を選択することや独自に提供元の管理を行うことは難しく、また非効率な場合が多い。

このカテゴリに分類されると考えられるその他の主なシステムは以下のとおり。
SWIFT、LINC[8]、損保ネット[9]、CAFIS

（注２）上記以外のシステムの扱い

上記のいずれにも当てはまらない、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については、金融機関が利用、または接続するシステムを運営する第三の事業主体がそれぞれみずからの業務として管理するシステムとして、【タイプＡ・Ｂ】や上記（注１）とは異なる形態として整理できる。

8 生保共同センター、生保協会が運営。
9 損保協会が運営。

Ⅱ　IT ガバナンスと IT マネジメント

サマリー

◆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

◆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。

１．安全対策上必要となる IT ガバナンス

～情報システムの安全対策における経営層の役割と責任～

（１）安全対策上必要となる IT ガバナンスの意義

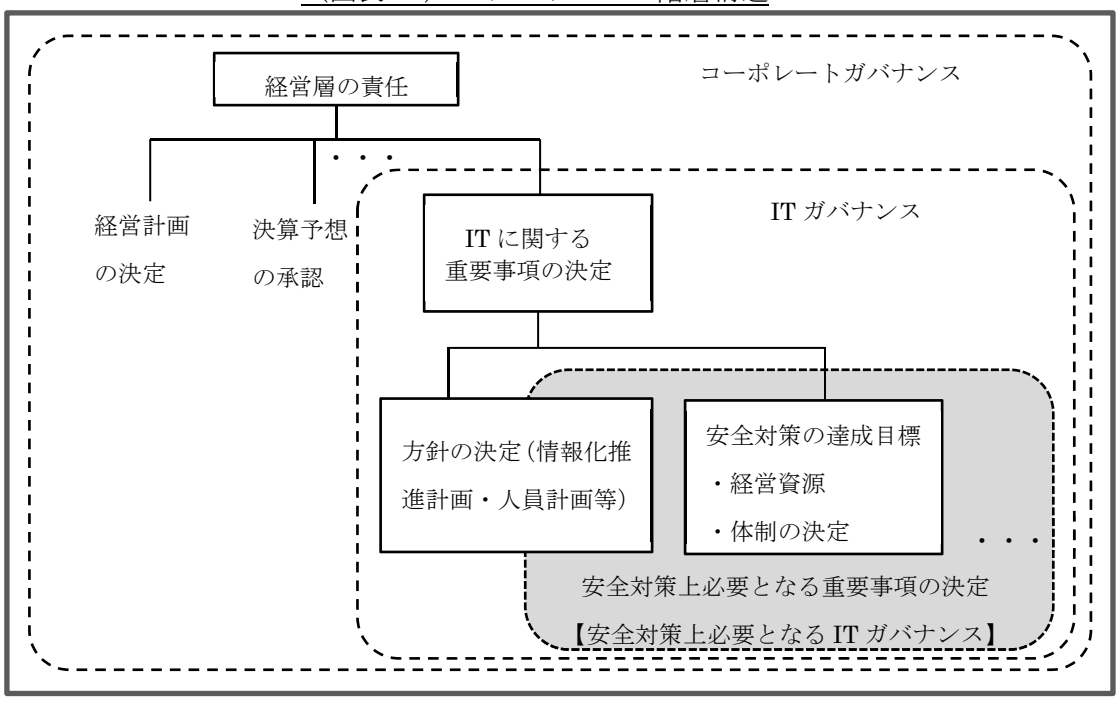
金融機関等の活動は情報システムに大きく依存していることから、情報システムの安全・安定の確保は、金融機関等の重要な経営課題である。そのため、経営層[10]はそれらに適切に対処するために、IT ガバナンスを機能させることが必要である。

一般的に IT ガバナンスとは、コーポレートガバナンス[11]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。そうした情報システムに関する重要事項の中でも特に情報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 12 参照）

したがって、システム担当取締役に限らず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。

（図表 12）IT ガバナンスの階層構造



10 金融機関等で取締役（システム担当取締役含む）及び取締役会等（常務会、経営会議、リスク管理委員会等経営に関する事項を決定する組織を含む）を構成する役員。協同組織金融機関については、金融機関の種類に応じて適用される法令の該当条文や文言に適宜読み替えるものとする。なお、FISC 安対基準では経営層を「取締役会（理事会）等」と定義している。

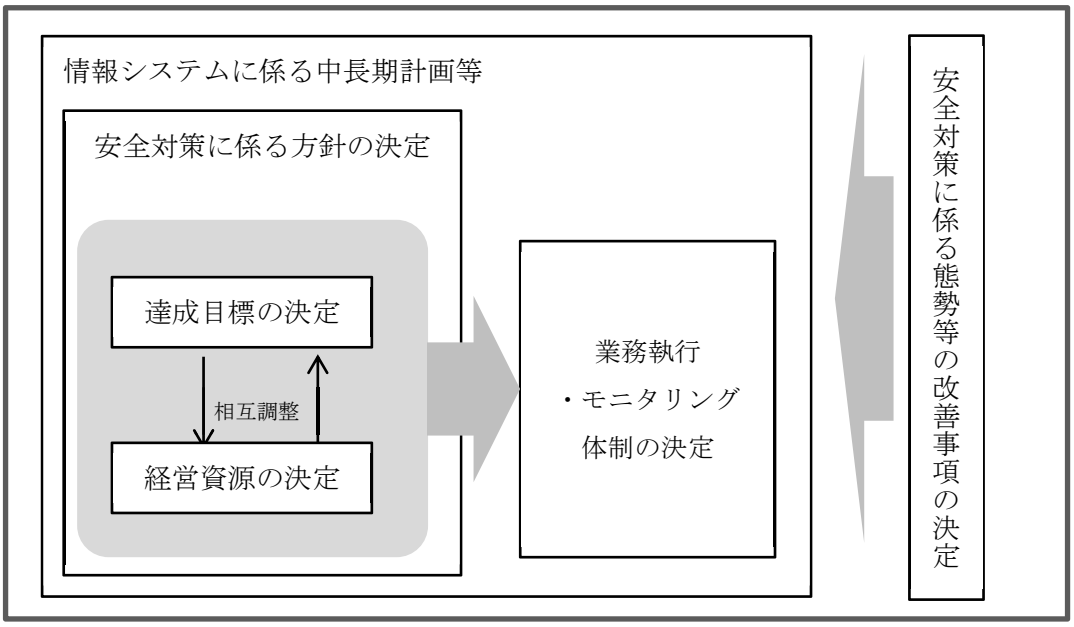
11 金融庁のコーポレートガバナンス・コードの策定に関する有識者会議『コーポレートガバナンス・コード原案（平成 27 年３月５日）』では「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえたうえで、透明・公正かつ迅速・果断な意思決定を行うための仕組み」と定義されている。

（２）安全対策上必要となるITガバナンスにおける経営層の役割と責任

社会的使命を担う金融機関等において、お客さまや株主等に対して責任を持つ経営層は、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必要がある。（図表13参照）

そのために、経営層は、安全対策上必要となるITガバナンスにおいて、主に以下の役割と責任を果たしていくことが必要である。

（図表13）経営層が決定すべき安全対策に係る重要事項



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

経営層は、情報システムの中長期計画等において、その重要項目として、以下の安全対策に係る重要事項を決定することが必要である。

a.安全対策に係る方針の決定

安全対策を含むITに関する重要事項の１つとして、取締役会は以下の方針を決定しておくことが必要である。

ⅰ.システム戦略方針の決定

システム戦略方針の以下の項目を、安全対策の観点を踏まえて[12]、決定することが必要である。

・情報化推進計画
・システムに対する投資計画
・IT人員の確保を目的とした人員計画
等

[12] 例えば、外部委託に係る方針（クラウド・アウトソーシング等）や基盤更改計画等において、安全対策目標と目標達成のために必要な費用を明示する、あるいは、人員計画において、システムリスク管理やサイバー攻撃対応に係る組織の要員数を明示する等が考えられる。

ⅱ.システムリスク管理方針の決定

システムリスク管理方針の以下の項目を、安全対策の観点を踏まえて、決定することが必要である。

・セキュリティポリシー等安全対策に関する内部規程の整備

・情報セキュリティ管理態勢の整備（サイバー攻撃対応態勢含む）

等

ⅲ.安全対策の達成目標の決定

経営層は、金融機関等として達成すべき安全対策の目標を決定する。経営層は、達成目標の決定にあたり、不備等が発生した際の影響範囲等が情報システムによって大きく異なることを踏まえて、例えば、不備等の発生によりお客さまや株主等に深刻な影響を及ぼす可能性がある情報システムに対しては、高い達成目標を設定する一方で、影響が金融機関等の内部の特定部署にとどまる情報システムに対しては、相応の達成目標を設定するといった、リスク特性に応じた目標設定の考慮が必要である。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が必要である。

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。

また、資源投下の決定に当たっては、情報セキュリティ等安全対策に係る環境変化等を踏まえて、資源の調達先に留意することが必要である。特に、資源を外部から調達する手段の１つである外部委託においては、内部[13]で調達する場合と比較して、直接把握できる範囲や深度が狭まり、内部統制が及びにくくなる場合があることに留意が必要である。

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ことが必要である。

業務執行体制のうち、情報システムに係る業務執行を統括する管理者は、安全対策に係る経営層の決定事項を実現するために、必要な内部規程・組織体制の整備やIT人員の配置､個々の情報システムに対する安全対策の決定及びその実効性の検証を行う。さらに、管理者は、経営層と執行部門の間に立ち、経営層の決定事項を適切に執行部

[13] 金融機関等が、例えば持ち株会社傘下で複数のグループ企業の一社として位置づけられている場合、「内部」には、グループ企業も含んで計画が策定される場合も考えられることに留意が必要である。

門に伝達するとともに、経営層に対しては安全対策に係る情報システムの実態を迅速かつ正確に伝える役割も果たす。このように、管理者は、いわゆるITマネジメントの中核として、重要な役割と責任を担うため、経営層は、管理者には、安全対策をはじめとした情報システムに関する十分な知識・経験を有するとともに、金融機関等の業務全般（リスク管理や監査を含む）にわたる知識を有する役職員を選任することが望ましい。

また、経営層は、システム監査の体制を整備し、システム監査部門に対して、みずからの決定事項を踏まえて、安全対策上必要なITマネジメント（業務執行体制等）が適切に機能していることを点検・評価させ、改善のための提言を行わせることが必要である。

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ことが必要である。

２．安全対策上必要となるITマネジメント

～情報システムの安全対策に携わるその他関係者の役割と責任～

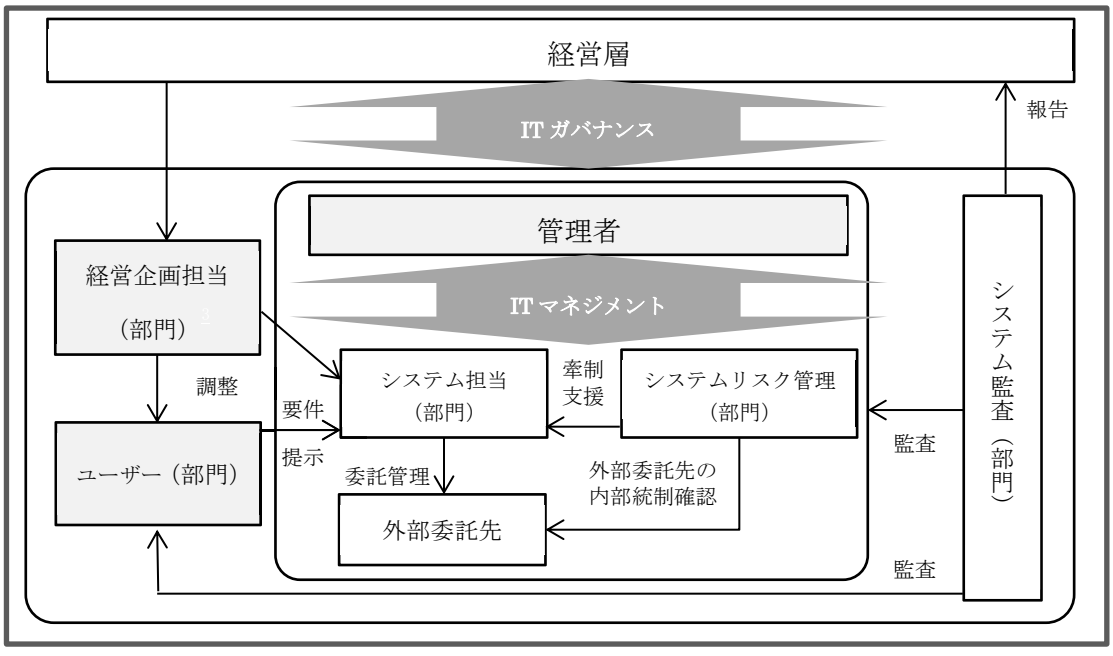
情報システムの安全対策において、経営層によるITガバナンスのもとで、例えば、下図のとおり複数の関係者が必要な機能を発揮している。（図表14参照）

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。

管理者は、安全対策に係る経営層の決定事項を実現するために、必要な内部規程・組織体制の整備や､個々の情報システムに対する安全対策の決定及びその実効性の検証を行う。さらに、経営層と執行部門の間に立ち、経営層の決定事項を適切に執行部門に伝達するとともに、経営層に対しては安全対策に係る情報システムの実態を迅速かつ正確に伝える役割と責任も果たす。

そうした管理者のもとで、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[14]）が安全対策を担っているが、そうした執行部門以外にも、例えば、経営資源投下の優先度評価等を行う経営企画担当及びビジネスモデルの企画等を行うユーザーも、安全対策上重要な役割を担っている[15]。

（図表14）情報システムの安全対策に携わる関係者（例）



[14] 図表14には記載がないが、オペレーショナル・リスクの総合的な管理部門は、システムリスク担当からの報告を受けて、システムリスクの状況について評価・判断等を行う役割を担っている。その他に、広報部門は、深刻なシステム障害発生時等に速やかな情報開示等の役割を担っている。

[15] 3線防御モデルとの関係では、図中の経営企画担当、システム担当、ユーザーは第1の防御線（業務ラインの管理）、システムリスク管理担当は第2の防御線（独立した全社的なオペレーショナル・リスク管理機能）、システム監査担当は第3の防御線（独立した検証）にそれぞれ該当する。一般的なオペレーショナル・リスクに関わる関係者については、『オペレーショナル・リスクの先進的手法のための監督指針』（バーゼル銀行監督委員会2011年6月）を参照願う。

（１）管理者[16]の役割と責任

管理者は、経営層によるITガバナンスのもとで、システム担当やシステムリスク管理担当等を統括し、安全対策上必要となるITマネジメントを担当する。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役割を担う。

①内部規程・組織体制等の整備

安全対策上必要となるシステムリスク管理規程等の規程・マニュアル等の整備を行うとともに、システムリスク管理部門やセキュリティ管理者・システム管理者・データ管理者・ネットワーク管理者等を設置し、システムリスク管理部門等必要な組織や体制を整備する。また、システムリスク管理やサイバーセキュリティ対応等に必要となるIT人材育成のために、研修・教育態勢を整備する。

②個々の情報システムに対する安全対策の決定

経営層が決定した安全対策の達成目標及び資源投下計画に基づいて、個々の情報システムに対する管理策を決定する。

③内部規程・組織体制等の見直し

システムリスク管理担当の職務の執行状況に関するモニタリングを継続的に実施するとともに、システムリスク管理態勢の実効性を検証し、必要に応じて内部規程及び組織体制の見直しを行う。

④安全対策上必要となる情報の経営層への報告

a.経営に重大な影響を与える、またはお客さまの利益が著しく阻害される事案の発生

報告内容例）　【都度】重大システム障害の発生、サイバー攻撃の発生、
重要な開発プロジェクトの遅延

b.システムリスク管理の状況

報告内容例）　【定期】安全対策の達成目標への到達状況、
システムリスク評価結果、BCP訓練結果、
セキュリティ対策の点検結果

c.他社における不正・不祥事件の内容

報告内容例）　【都度】他社情報漏洩事件等を参考とした自社のセキュリティ対策評価結果

d.重要なシステムリスクに係るコントロール方法

報告内容例）　【都度】サイバーセキュリティ態勢整備、
コンティンジェンシープラン改訂

e.システムの重要度及び性格を踏まえた、開発プロジェクトごとの進捗状況

報告内容例）　【定期】重要な開発プロジェクトの状況報告

---

16 ここでは、具体的な役職ではなく、安全対策上必要な機能（役割と責任）に着目して記載している。実際に、管理者の機能を担う役職者は、各金融機関等の実態に応じて、個々に判断されうる。

（進捗、品質、投資額、課題等）

f.影響度の大きい委託先の管理状況に対する確認結果、及び認識した問題点

報告内容例）　【定期】既存の委託先に対する評価結果

（技術力、対応力、品質、内部統制等）

【都度】委託先選定に係る評価結果

g.独立したシステム監査人によるシステムの総合的な監査・評価結果

報告内容例）　【都度】システム部門等に対する監査結果、

重要な委託先に対する監査結果

等

（２）経営企画担当の役割と責任

経営戦略や経営資源配分等に携わる組織又は担当者。通常は経営企画部門に配置されている。安全対策を含むシステム化事案の決定においては、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[17]の役割と責任

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）等の企画に携わる組織又は担当者。なお、システムを利用する営業店等は含まない。ユーザーの、安全対策における主な役割と責任は以下のとおりである。

①安全対策に配慮したビジネスモデルの企画

ユーザーは、情報システムの姿を決める第一線であることから、そのビジネスモデルに情報システムの安全・安定に脅威となる要素を作りこまない、あるいは情報システムを安全・安定に運用するためのコントロールを作りこむ等、システム担当やシステムリスク管理担当等と連携しながら、安全対策に配慮したビジネスモデルを企画することが必要である。

②投資効果の達成

経営戦略達成のために、各ユーザーは所管の業務において、安全対策をはじめとして必要なシステム化事案につき、管理者等へ要望を行う。その際に、ユーザーは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責任を負う。特に、システム化により達成されるべき効果については、システムの企画時にその見込を明らかにするとともに、システムの稼働後も、見込まれた効果が達成されたか否か、について引き続き管理者等へ説明する責任を負う。

---

[17] EUC（エンドユーザーコンピューティング）が認められている金融機関等では、ユーザーとシステム担当が同一部門に配置されている。また、業態等によっては、ユーザーの役割と責任の一部をシステム担当が担う場合がある。

③ 業務要件の提示[18]

ユーザーは、安全対策をはじめとして要望したシステム化事案が経営層及び管理者等によって承認された場合、そのシステム開発着手時に、システム担当に対して業務要件を提示する責任を負う。業務要件提示後、システム開発時の途中で業務要件が変更になった場合は、適時適切にシステム担当に対してその内容を伝えるとともに、システム担当はシステム開発途中の変更による影響を評価したうえで、変更を受け入れるか否かを判断する。なお、ユーザーはシステム開発完了後も、引き続きみずからが提示した業務要件の内容につき責任を負う。

[18] ユーザーが業務要件の提示だけでなく、システム開発の進捗まで管理している金融機関等もある。

３．人員計画に係る留意事項

経営層が、システム戦略方針の１つとして人員計画を決定するに際して、以下留意することが必要である。

（１）システム戦略を実現するための人員数・スキルの種類とレベル・配置の把握

> 経営層は、金融機関等の経営の基盤となる IT の維持・活用において、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。

IT に係る経営資源の中で、人員は重要な要素の１つであり、経営層は、情報システムに対する投資額と同じく、その実態につき把握するとともに、システム戦略を実現するために必要な人員とのギャップについて、把握することが必要である。

さらに、人員の数のみでなく、質（保有する IT に関するスキルの種類とレベル・配置等）を含めた IT 人材として、具体的に把握することが必要である。【資料編資料１参照】

なお、金融機関等の業態等によっては、人員の数が少数である現状も踏まえて、特定の人員が複数のスキルを包括的に保有することへも考慮が必要である。

（２）全体の中長期計画に沿った人員の育成計画の策定

> 経営層は、足元の IT 人材の現状を踏まえたうえで、中長期経営計画と整合性がとれた人材の中長期育成計画を策定すること。

経営層は、IT 人材について、例えばシステム戦略実現のために不足がある場合は、人員数を増やすだけでなく、人材を育成するという観点での計画策定についても、考慮が必要である。

なお、IT 人材として育成対象となる人員にはリーダーのほか、グループ会社の人員も含まれる場合があり、併せて、育成のための環境整備にも配慮が必要である。

また、計画策定に当たっては、人員の評価・処遇や登用の方法に関しても、考慮が必要である。

４．IT に関する重要事項に係る経営層の意思決定の在り方

近年、監査等委員会設置会社等、機関設計の選択肢が増加するとともに、金融持株会社形態を採用する金融機関が増加しており、安対基準において「経営層」と定義している対象についても、単に取締役会にとどまらず幅広く解しうる現状にある。

そうしたことから、IT に関する重要事項に係る「経営層」の意思決定の在り方について、実態調査を踏まえ、以下のとおり、整理を行った。

（１）IT に係る重要事項の審議・決定機関の在り方

IT に係る重要事項は、経営資源全体を視野に入れたうえで、情報システム投資効率の最大化等の議論が行われることが望ましいことから、経営層全体が参加した会議等での審議を経ることが望ましい。

また、決定機関は、当センターによる調査対象金融グループでは取締役会とされている(図表 15 参照)ものの、IT に係る重要事項は、業務執行に係る事項が大半であることから、取締役会に限らず、機関選択と権限移譲の実態に応じて[19]、取締役・執行役等の機関において決定することが可能である。

ただし、いずれの機関選択においても、「基本事項の決定」は委譲できない権限として取締役会に残るとされており、IT に係る重要事項においても、システム統合方針や大規模なシステム更改[20]等といった決定については、取締役会の権限に属すると考えられる。

（２）金融持株会社と事業会社における IT に係る重要事項決定の実態

金融機関が、持株会社を設立する目的は利益調整の必要性[21]等が考えられる。そうした金融持株会社形態がとられている主な金融グループにおいて、IT に係る重要事項が、持株と事業会社間で、どのように意思決定されているか、調査を行った。（図表 15 参照）以下の２ケースの傾向がみられ、これは、各グループの戦略等に応じて、金融持株会社と事業会社で意思決定が行われている実態にあるものと考えられる。

・持株会社に IT に関する役割を一元化されているケース
情報システム要員は持株会社に集約され、実際の開発は、情報システム子会社や共同センター等へ共同委託されている。また、IT に係る意思決定は、持株会社の機関で行われており、事業会社での意思決定は、内部統制等個社固有事項に最小化されている。

・個々の事業会社で IT に関する役割を担うケース
情報システム要員は個々の子会社が内部に保有し、個別に外部委託されている。また、IT に係る意思決定は、各事業会社の機関で行われており、持株での意思決定は、各社共通事項に最小化されている。

---

19 指名委員会等設置会社では、取締役会は監督が中心となり、取締役は原則として業務執行はできない。業務執行は執行役が担当する。監査等委員会設置会社では、業務の決定権限を取締役会から取締役に大幅に委譲することが認められている。

20 「大規模なシステム更改」とは、例えば基幹システムの再構築のように、システム統合と同程度に高いリスクを有すると考えられるシステム更改のことをいう。

21 岩原紳作『金融持株会社におけるグループガバナンス－銀行法と会社法の交錯（３）－』において、「金融持株会社形態が採られることが多いのは、グループ全体の経営管理として持株会社形態のほうが直接の子会社形態より適切だと考えられたためではなかろうか。例えば、メガバンク・グループ等においても、その中に占める銀行以外の業務の割合が大きくなっており、銀行業務との利益調整を必要とする問題も多くなっている。」とされている。

（図表 15）機関選択に応じた IT ガバナンスの実態調査

金融グループ	IT に係る中長期計画等の審議・決定		審議・決定を担う主体	持株と事業会社間の審議・決定プロセス	システム管理形態
	審議機関	決定機関			
A	委員会を経て経営会議	取締役会	持株	持株が提示した方針を元に、事業会社が審議・決定後、持株で同様に審議・決定。	持株で一元管理
B	委員会を経て経営会議	取締役会	持株	持株が審議・決定後、事業会社が審議・決定。（事業会社では内部統制等固有事項に限定）	持株で一元管理
C	委員会を経て経営会議	取締役会	事業会社	事業会社が個々に審議・決定。（持株は方針・ルールの決定や一部グループ共通の議題中心）	事業会社単位で個々に運営
D	経営会議	取締役会	業務別に持株と事業会社で分担	持株と事業会社の経営会議を合同開催。（ICT の分野は、持株会社が主導して、合同開催した経営会議にて同時「審議」している。ICT 以外の業務は、案件により主体が異なる）	持株で一元管理
E	委員会又は経営会議	取締役会	持株	持株と事業会社の経営会議を同時開催。（事業会社が主体となり決定するものもある）	持株で一元管理
F	委員会	取締役会	持株	持株が審議・決定後、別日に事業会社が同内容を審議・決定。	持株で一元管理
G	経営会議	取締役会	持株	持株会社と事業会社が事前調整のうえ、事業会社が審議・決定後、持株会社が審議・決定し、その結果を事業会社に示達。	事業会社単位で個々に運営

【社外取締役の支援事例】

・社外取締役を支援する専属スタッフを設置する。
・社外取締役の会議を設置し、問題意識の共有を行う。
・社外取締役が経営会議にオブザーブする。
・社外取締役に現場視察を案内する。　　等

Ⅲ　リスクベースアプローチ

～経営層等が情報システムに対する安全対策等を決定するための原則～

サマリー

◆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。

当センターが公表した『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』(平成 26 年 11 月）において、「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、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」として、「リスクベースアプローチを適用し、経営判断のもと適切なリスク管理策を策定」することが提言された。

「リスクベースアプローチ」は、一般的には、リスク特性を分析した結果を、対策の優先順位等の合理的な意思決定に活用するという考え方である。そのため、「リスクベースアプローチ」は、単にクラウド利用時の適用にとどまらず、金融機関等の経営層が、経営資源配分の決定において、その効率の最大化、いわゆる企業価値の最大化を追求する際に、重要な考え方にもなる。

こうしたことから、本検討会において、外部委託に関して、安全対策上必要となる IT ガバナンスを検討するに当たっては、まず、従来の安全対策の考え方をあらためて検証したうえで、海外事例を参考に、「リスクベースアプローチ」を踏まえた安全対策の基本原則を提言する。次に、安全対策の基本原則に従った IT ガバナンス等を明確にする。さらに、安全対策における経営責任の在り方を提言する。

こうして、本検討会において、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その経営責任の在り方とともに明確に示すことが、わが国が将来の金融ビジネスにおける優位性を確保するとともに、金融機関等の健全な成長と金融システムの安定の両立を実現するための一助となることを、期待したい。

１．新たな安全対策の在り方の必要性

当センターのアンケート調査によれば、この 10 年以上の間、金融機関を取り巻く環境が大きく変化しているにも関わらず、安全対策・維持運用・新規開発の割合に大きな変化は見られず、例えば、新規投資の割合は、他の先進国と比して、相対的に低い状況にある。【資料編資料２参照】

これには、複雑な要因があると考えられるが、本有識者検討会においては、まず「安全対策上必要となる IT ガバナンス」の観点から、現在、安全対策への資源配分が適正に行われる環境にあるのか、その前提となる安全対策の考え方を切り口として、明らかにしたい。

（１）「安全対策基準の考え方」の見直しの必要性

わが国では、金融機関等が、情報システムに対する安全対策を検討するに当たっては、金融検査マニュアルとともに、当センターの安対基準が利用されており、安全対策の在り方については、安対基準冒頭記載の「安全対策基準の考え方」が参考とされている。

そもそも安対基準は、30 年前、金融機関のオンライン化の進展にあたり、金融機関の自己責任と自主性尊重を原則としつつも、その公共性と社会的責任の大きさに鑑み、個別金融機関による対応を補完するものとして、その安全性の確保を目的に、金融機関・ベンダー等の専門的・技術的知識を有する関係者が参加する当センターを創設し、はじ

めて策定されたものである。

それから、30 年が経過するなかで、安対基準は、環境変化を取り込みながら基準を改訂し版を重ね、現在では、業界共通のガイドラインとして金融機関等において広く浸透し、安全対策の重要性も強く認識されるに至っており、当初期待された役割は十分に果たされてきた。

一方で、情報化が急速に進展し、コンピュータの形態も多様化するとともに、国際競争の中で、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、金融機関等の情報システムに求められる役割が大きく変容するなかで、30 年間大きく変わらずにきた「安全対策基準の考え方」を見直すべき時期が到来している。

そうした中、今般、外部委託に関する有識者検討会で安全対策上必要となる IT ガバナンスを検討するにあたり、従来の「安全対策基準の考え方」をあらためて検証したうえで、海外先進諸国の動向を踏まえて、今の時代にふさわしい新たな安全対策の在り方を示すのが適当である。

（２）従来の安全対策の考え方とその課題

振り返ると、安対基準が最初に作られた 30 年以上前は、金融機関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。それ以外の情報システムはほとんど存在せず、基幹業務系のコンピュータシステムのみを念頭におけば十分であった。そのため、安対基準では、その適用対象とする情報システムを、30 年前の初版では「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、さらにはクラウドサービスまで多様化している。

そうした環境変化の中で、安対基準の適用対象については、現在の第８版においては、従来どおり「基幹業務のオンラインコンピュータ・システム」とする一方で、数が増加し形態が多様化している「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」については、安対基準を「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」という記載にとどまっている。この結果、大きな比率を占めるその他情報システムにおいては、最低限の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。

そのため、金融機関等において、以下のような状況にあることが危惧される。

・金融機関等の担当者は、「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考えるにあたり、適用基準をみずからが独自に選択し考えるのではなく、「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同一の安対基準を、その他の情報システムへも一律に設定しておけば安心とする、安全性に偏った選択を行う。

・「安全対策基準の考え方」には、安全対策への経営資源配分の上限や、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おらず、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、過度な安全対策の選択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徹底して追及されかねないといった、不確実性を含む現状においては、経営層は、システム障害を極力ゼロとするために、過度な安全対策を承認する、あるいはみずから徹底して追求する。

このように、「安全対策基準の考え方」は、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。

（３）リスクベースアプローチ

翻って、米英をはじめとした海外先進諸国では、金融機関等の安全対策及び経営資源配分等の決定にあたり、リスク特性を分析した結果を、対策の優先順位等の合理的な意思決定に活用する、一般的に「リスクベースアプローチ」と総称される考え方が、監督当局及び金融機関等における共通認識となっている。【資料編資料３参照】

その主な特徴は以下のとおりである。

・リスクの顕在化を予防する対策に無制限に費用を投下し、リスクゼロを追求することは、合理的でないとしている。これには、費用を投下してリスクゼロに近づくほど得られる効果が低減していくという考えや、予防的な投下費用とリスク顕在化後の事後的な投下費用を比較衡量し経済性の高い方を選択するといった考えが、底流にあるものと考えられる。経営資源が無尽蔵ではないなかで、こうした考え方が合理性を有することは、いうまでもない。

・監督当局は、リスク区分法やリスク管理策については、必ずしもこと細かく成文化しておらず、基本的に金融機関の判断に委ねている。これは、こと細かく成文化してしまうと、本当はもっと良い方法があるかもしれないのにそれを見逃し、金融機関のイノベーションを阻害する結果になることを踏まえたもので、いわゆる原則主義の考え方を採用していることによる。

・そうした中でも、監督当局は、外部委託等のガイドラインにおいて、「重要な銀行機能・共有サービスや顧客に深刻な影響を及ぼす業務」等を「重要業務」とし、特段の定義をするとともに、個別の管理策を示している。これは、そうした金融インフラの一部を構成する業務は、外部性を有しかつ高いリスクを持つことから、一義的には内部的な最大効率を追求する金融機関に、その管理策を全面的に委ねることは必ずしも適当でない、という、社会的・公共的な観点を踏まえたものと推察される。

以上を踏まえ、次項では、新たな安全対策の在り方について、まず、大きな前提として、安全対策における基本原則について、解説する。

２．安全対策における基本原則

リスクベースアプローチを踏まえた、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。

（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。

（１）

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の分析及び評価結果に基づいて、決定されるべきものである。また、経営資源の保有状況とも調整しながら、必要十分な内容で決定されるべきであり、リスクゼロを追求することには、合理性が無い。

（２）

安全対策への経営資源配分は、安全対策目標を達成するための費用であることをもって、直ちに優先的に配分されるべきものではない。まず、安全対策の費用と、安全対策を実施せずリスクが顕在化した場合の対応費用を比較衡量して、リスクテイクの選択肢も考慮し決定されるべきである。次に、情報システム予算内での、新規開発投資等のその他配分先との調整が行われるべきである。最後に、情報システム予算を越えて、経営資源全体で配分を調整することも視野に入れられるべきである。これらの調整は、資源配分効率の最大化、つまり企業価値の最大化のために必要なものであり、それを目的に行われるべきである。

（３）

経営層、管理者等は、これら（１）（２）の原則を遵守し、企業価値の最大化を目指して、妥当な意思決定あるいは適切な監督・管理を行うべきである。これにより、組織全体が適切に運営されている限りにおいては、情報システムに対する安全対策は、金融機関等の判断に委ねられており、独自に決定することが可能である。

（４）

金融機関等は、金融インフラの一部を構成し、リスク顕在化時に金融機関等の内部に

とどまらず、顧客や他金融機関等へ深刻な影響を及ぼす情報システムを保有している場合がある。そのため、こうした重大な外部性を有する情報システムに対する安全対策の達成目標は、内部影響だけでなく外部影響を加味して決定されるべきである。しかしながら、金融機関等がみずから外部影響まで評価することは容易でないことから、こうした重大な外部性を考慮した社会的に合意されたルールが必要である。

また、金融機関等は、保健医療等の機微情報を保有する情報システムを保有している場合がある。機微情報は、流出した場合、基本的人権の侵害といった広範な損失を被る可能性があり、その取扱いは社会的・公共的な性質を有することから、こうした情報の機微性を考慮した社会的に合意されたルールも必要である。【資料編資料４参照】

当センターは、そうした社会的に合意されたルールを策定するに当たって、必要な役割を果たす。

次に、以上の基本原則を踏まえて、それに従った IT ガバナンスの内容について解説する。

３．基本原則に従った IT ガバナンス

金融機関等の経営層は、情報システムに係る経営資源配分の最大効率を追求し、企業価値を最大化するために、その意思決定にあたり、リスクベースアプローチを十分理解するとともに、安全対策における基本原則を遵守することが望ましい。

（１）意義

「経営層が、安全対策に係る方針の決定に際して、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達成目標等について、包括的に決定する」ことをいう。

経営資源配分の考慮に当たっては、情報システムが経営において重要課題の１つとなっている現在においては、保有する経営資源全体を視野に入れたうえで、情報システム投資効率の最大化が議論されることが望ましい。したがって、システム担当役員だけでなく経営層全体が本意思決定に関わり、適切に IT ガバナンスを発揮することが必要である。さらに、そのためには、意思決定に携わる経営層は、当該金融機関等が保有する情報システムについて最低限の知識を有するとともに、一般的な情報システムに関する動向等についても知見を有することが望ましい。

経営層が、こうしたリスクベースアプローチを踏まえた基本原則に従って適切に IT ガバナンスを発揮している限りにおいては、情報システムのリスク区分や安全対策の具体的内容等は、基本的には、金融機関等が、みずから独自に選択することが可能である。

（２）重大な外部性を有する情報システム等に対するルール

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対しては、社会的に合意されたルールが必要であり、次のとおり、安対基準の適用が求められる。

まず、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は、高いリスク区分へ分類されることが必要である。そのうえで、経営層は、安全対策の達成目標の設定に当たっては、「高い安対基準」の適用を求める。ここでいう「高い安対基準」とは、従来から安対基準において、「すること」、「必要である」あるいは「望ましい」と表記上区分けされている基準を差す。また、安全対策の実施に必要となる経営資源の配分に当たっては、新規投資等と比較衡量したうえで、資源配分の効率が最大化されるといった観点を踏まえて、適切に配分されることが必要である。

（３）簡易な方法の必要性

リスクベースアプローチを徹底し、安全対策の基本原則を遵守すれば、情報システムのリスク区分や安全対策の具体的内容等は、基本的には、金融機関等が、みずから独自に選択することが可能とはするものの、これを十全な形で運用し、その意思決定の妥当性や運営の適切性について説明責任を果たすことは、簡単ではない。

例えば、リスク区分に当たっては、オペレーショナル・リスクの１つであるシステムリスクを、その他のリスクへ連鎖する性質も踏まえて、定量的に測定し、経営資源配分に当たっては、必要となる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な一致点を求め、最終的な経営資源配分を決定することが必要となる。

したがって、こうした十全なリスクベースアプローチが理想形であるとしても、実現可能な金融機関は限られるものと考える。

わが国の金融機関等の多くにおいては、従来からの安全対策の考え方が一般的であることも踏まえると、リスクベースアプローチを導入し、新たな安全対策の在り方がとられる一方で、結果的には現在の安全対策実施内容に激変を生じないようなアプローチも必要となる。

次項では、十全なリスクベースアプローチと近似的かつ簡易な方法で、所要の効果が得られるものとして、安全対策の基本原則に従った「簡易なリスクベースアプローチ」による IT ガバナンスについて、解説する。

なお、便宜的にここでは、簡易な方法について言及するが、金融機関等においては、こうした簡易な方法にとどまることなく、十全なリスクベースアプローチを目指して、より精緻なアプローチを進めることが望ましい。

４．簡易なリスクベースアプローチによる IT ガバナンス

（１）意義

「経営層が、安全対策に係る方針の決定に際して、情報システムをそのリスク特性に応じて、重要な情報システムとそれ以外の情報システムの大きく２つに区分し、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、区分別に必要十分な安全対策の達成目標等について、包括的に決定する」ことをいう。

（２）「重要な情報システム」の意義

重要な情報システムは、それぞれの金融機関等において、外部性や情報の機微性等の観点から、決済システムや顧客等への影響を鑑み、判断することが可能である。

まず、重要な情報システムには、「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」が含まれる。それ以外には、こうした情報システムと同等以上のリスクを有する点に着目し、「高い安対基準」を適用することが妥当と考えられる情報システムを、独自に選定することも可能である[22]。

なお、金融機関の業務が情報システムに大きく依存している現在においては、重要な情報システムは、原則として、経営層みずからが決定することが必要である。

（３）「重要な情報システム」に対する安全対策及び経営資源配分

経営層は、重要な情報システムに対する安全対策の達成目標の設定に当たっては、「高い安対基準」の適用を求める。ここでいう「高い安対基準」とは、従来から安対基準の中で、「すること」、「必要である」あるいは「望ましい」と表記上区分けされている基準を差す。安全対策の実施に必要となる経営資源の配分に当たっては、新規投資等と比較衡量したうえで、資源配分の効率が最大化されるといった観点を踏まえて、適切に配分されることが必要である。

（４）「それ以外の情報システム」に対する安全対策及び経営資源配分

それ以外の情報システムにおいては、安全対策の達成目標は、本来は独自に定めうるものではあるものの、前述のとおり明確に示さないことにより、かえって、一律に高い安対基準が適用される懸念があることから、ここでは、安全対策の不確実性を低減するために、次のとおり定める。

まず、経営層は、それ以外の情報システムに対する安全対策の達成目標の設定にあたっては、「必要最低限の安対基準」を適用することが必要である。その他の達成目標は、実態に応じて、独自に選択することが可能である。次に、安全対策の実施に必要となる経営資源の配分に当たっては、新規投資等を視野に入れたうえで、より効率的な経営資源配分を決定することが必要である。

また、外部性や顧客情報を持たず、かつ内部への影響も軽微な情報システムは、極め

[22] ここで例示した以外にも、例えば可用性や完全性等の観点から、重要な情報システムを選定することも考えられる。

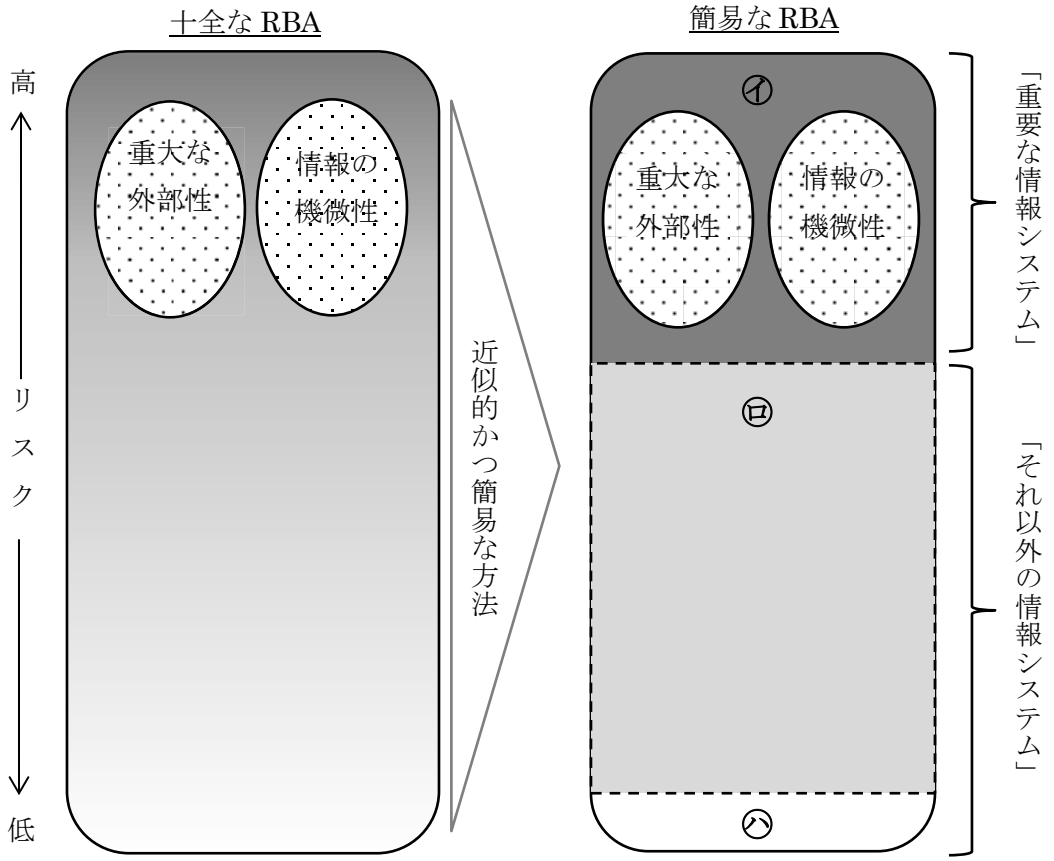
てリスクが低い情報システムであることから、そもそも安対基準の適用対象外とすることが可能である。内部への影響が軽微な情報システムとしては、機微情報を含む顧客情報を保有しない情報システム、あるいは、他の情報システムと連結していない情報システムが候補となる。こうした安対基準適用対象外とすることが妥当な低リスクな情報システムは、その選定に合理性があれば、金融機関等の実態に応じて、独自に定めることが可能である。

（５）「必要最低限の安対基準」の意義

これは、「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。

今般、従来の「簡易なリスク管理策」を「必要最低限の安対基準」として、再定義したうえで、今後の安対基準の中で、適宜定めていくこととする。ただし、前述のとおり、あくまで、十全なリスクベースアプローチの難易度が高く便宜的なアプローチをとる場合において、安全対策の不確実性を低減するという目的の範囲内で定められるべきものである。

（図表 16）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。

５．安全対策における経営責任の在り方

以上のとおり、新たな安全対策の在り方を解説してきたものの、経営層においては、前述のとおり、「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、過度な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、前述の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。

翻ると、こうしたリスク回避性向が高い認識は、日本固有の社会通念として深く根ざしているものではないかと考える。その社会通念の妥当性については、さまざまな考えがあるであろうが、こと企業価値の最大化を使命とする経営者においては、リスクを受容せず、リスクゼロを追求する、といったリスク回避性向の高い認識に合理性が無いことは、前述のとおりである。

一方で、米英をはじめとした先進諸国では、一般的には、日本と異なりリスク選好性が高いものとされており、例えばFinTechにおいては、米英の金融機関は、いち早くITベンチャー等のノンバンクプレーヤーと連携・協働する等、新たな分野にリスクを取っていち早く参入する動きがみられる。これには、前述したとおり、リスクゼロの追求は合理的でないといった認識が、監督当局や金融機関等において共有されていることも背景にあるものと考える。

こうした中、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、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、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、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。

（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。

Ⅳ　外部委託におけるリスク管理の在り方

サマリー

◆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。

◆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。

一般的に外部委託は、直接把握できる範囲や深度が狭まり、統制を行う接点が限定的になるとともに、統制が及びにくくなるといった特性があり、再委託[23]においては、そうした特性がいっそう顕著となる。

そうした中、近年、複数の共同センターにおいて、再委託先社員によるキャッシュカード偽造事件等の不正事案が発生し、再委託に係るリスクがあらためて認識されている。また、そうしたリスクは、共同センターに限らず、外部委託全般に共通するものとして、銀行法等が改正され、金融機関等においては、再委託に関して、その管理責任や説明責任が明示的に求められる状況となっている。こうして、外部委託が金融機関等における主要な問題となったことを踏まえて、本検討会を開催することとなった。

一方、本検討会において、こうした外部委託の問題に対応するにあたり、これは「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ためには、IT ガバナンスの観点が不可欠」としたうえで、まず「IT ガバナンスと IT マネジメント」「リスクベースアプローチ」をテーマに検討を行ってきた。また、外部委託の一形態である「クラウドサービス」については、有識者検討会を経て、安対基準等が改訂され、既に新たなルールが整備された状況にある。

今般、外部委託全般に関して検討を進めるに当たっては、まず、再委託を巡る諸課題とそれへの対応の考え方を明確にしたうえで、これまでの有識者検討会等での検討内容を踏まえて、外部委託におけるリスク管理の在り方を見直す。そのうえで、再委託管理のリスク管理策を提案する。

１．再委託を巡る諸課題

地域銀行における複数の共同センターにおいて、スキル及び権限を有する再委託先の責任者がカード偽造を行うといった不正事案が発生していることから、再委託管理が課題としてあらためて認識され、一部の共同センター利用金融機関においては、独自の対策が行われているところである。

また、こうした不正事案を踏まえて、銀行法が改正されるなど、共同センターに限らず、外部委託全般において、再委託先に対しても当局の検査権限が及ぶこととなったことから、金融機関においては再委託に対する管理責任や説明責任が求められる状況となっており、再委託における責任の在り方の明確化が課題となっている。

不正事案は、共同センターにおいて集中して発生している問題であるものの、その根本原因は、統制が及びにくいなどの外部委託の特性に由来したものであることから、再委託を巡る諸課題は、まず外部委託全般に共通の課題として検討を行う必要がある。

---

[23] 二以上の段階にわたる委託を含む。

２．諸課題への対応の考え方

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。

本来、金融機関等はまず「会社」であり、企業価値の最大化を目指して事業が行われるものであるが、一方で、その事業は金融インフラの一部を構成するなど「公共性」を有するがゆえに、免許事業とされる等、健全性の確保が社会的に求められていると解される。

したがって、金融機関等の情報システムの相当程度が外部委託先で担われ、その依存度が高まる現状においては、情報システムの健全性の確保については、その管理責任や説明責任を、従来以上に強く求められるものと考える。

一方で、一般的に外部委託は、前述のとおり、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。すなわち、再委託先は、通常では、委託先を介して間接的にしか接点を持ち得ず、また、委託業務が分割され複数の先に再委託されれば、その接点は水平的に増加し、さらに、再委託先からその先にも再委託が進めば、垂直的にも階層が深くなっていく。したがって、ひとたび再委託が進んでいくと、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、自営に求められる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、金融機関等の経営層の責務でもある。

翻って、前述の再委託を巡る諸課題への対応であるが、「不正事案対策」に関しては、当センターでは、まず、昨年改訂された安対基準（第８版追補改訂）において、「不正な引出し事例への対応（暫定)」として、アクセス権限の制限等技術的な基準を見直したところである。しかしながら、こうした不正事案の発生の背景には、従来の安対基準では、再委託を含む委託業務の管理態勢において、公共性や委託先が取り扱う情報の機微性といった金融機関等の「重要な情報システム」の特性が十分に踏まえられていなかったことが、その原因の１つにあると考える。そうした反省に立ち、技術的な基準の見直しにとどまらず、外部委託におけるリスク管理の在り方といった根本対策が必要として、今回検討を行い、安対基準に反映することを目指していく[24]。

---

[24] FISC『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（第８版追補改訂)』（平成 27 年６月）の「改訂の概要」において、「外部委託先による不正な引出し事例への対応（暫定)」について「今回の改訂は暫定対応であり、外

一方、「再委託における責任の在り方の明確化」に関しては、「Ⅲ　リスクベースアプローチ　５．安全対策における経営責任の在り方」で論じられたことと何ら異ならない。すなわち、金融機関等は、前述の再委託における根本的な対策が安対基準へ反映された後は、それを踏まえたうえで、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、残るリスクに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。

以上から、委託先等との接点、すなわちその各管理フェーズにおいて、委託先等への最適な統制、すなわち最適な安全対策目標が設定されることを目的として、次項から、再委託に焦点をあて「外部委託におけるリスク管理の在り方」を検討する。検討に当たっては、「IT ガバナンスと IT マネジメント」「リスクベースアプローチ」を踏まえるとともに、外部委託の一形態である「クラウドサービス」に関しては、有識者検討会を経て、既に安対基準等の整備が進んでいる[25]ことから、その内容と整合的に理解されるよう配慮することが必要である。

部委託先管理態勢などの根本的な内容に関しては、別途、外部委託管理全般に関する有識者検討会における議論等を踏まえ、改訂検討を行う予定としている。」とされている。

[25] FISC では平成 26 年に「金融機関におけるクラウド利用に関する有識者検討会」が開催され、その成果等を踏まえて各専門委員会が開催され、平成 27 年６月に『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（第８版追補改訂）』が発刊されるとともに、平成 28 年５月に『金融機関等のシステム監査指針（改訂第３版追補）』が発刊された。

３．外部委託におけるリスク管理の在り方

外部委託におけるリスク管理の在り方を検討するにあたり、まず管理責任等を語るべくITガバナンスの観点から、外部委託における管理プロセスを特定しその内容等を明らかにする。そのうえで、外部委託の接点すなわち管理フェーズにおけるリスク管理策の考え方を整理する。

（１）外部委託における管理プロセス

これまでの検討会等での検討内容を踏まえて、その管理プロセスには、次のものが考えられる。

①情報システムの外部委託に係る方針の決定
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
以下の管理フェーズ[26]を踏まえて、安全対策目標及びその達成に必要となる経営資源、委託先管理等の体制を決定する。
a. 利用検討時
b. 契約締結時
c. 開発（パッケージ導入やシステム更改等も含む）時
d. 運用時（モニタリング等[27]）
e. 終了時
f. インシデント発生時
④各管理フェーズにおける安全対策の実施
⑤外部委託におけるリスク管理に係る改善事項の決定

①情報システムの外部委託に係る方針の決定

まず情報システムの外部委託に関しては、企業価値の最大化や健全性の確保を踏まえて、外部委託を選択するに当たっての考え方（利用目的等）、例えば、外部委託が可能となる業務、リスク管理の枠組み等を、その方針として明確に定めること。特に、再委託に関しては、いっそう統制が及びにくくなることから、例えば、方針に含まれるものとして、再委託が可能となる業務、業務に応じた再委託の階層や数の制限等、が考えられる。

---

[26] FISC『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』（平成26年11月）では、「経営陣の関与のもと、基本的な利用方針やリスク管理に係る方針を策定することが重要」としたうえで、その管理フェーズを「利用検討時」「契約締結時」「運用時」「契約終了時」に加え「インシデントの発生時」の５つに区分されている。クラウドサービスは、運用が主となる形態であるが、現行の安対基準の「外部委託管理」においては、「運用」とともに「開発」も対象とされていることから、新たに「開発時」として追加している。

[27] FISC『金融機関等のシステム監査指針』では、監視（モニタリング）について「内部統制が適切かつ効果的であることを確かめるためのプロセスがモニタリングである。これには、日々の業務活動を通じて各階層の管理者が行う日常的監視、各部門管理者によって定期・不定期に実施される自店検査、対象組織から独立した内部監査部門によって実施される内部監査などが含まれる。内部監査部門によって実施されるシステム監査は、独立的評価としての監視に含まれる。」とされている。

なお、本方針はすべての情報システムに包括的に適用されるべきものであることから、経営層が決定すること。

②個別情報システムの外部委託の決定

以上の方針に従って、個々の情報システムにおいて、外部委託の目的を明確にしたうえで、その妥当性を判断することとなる。

本決定は、「重要な情報システム」については、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する必要があり、特にその管理責任・説明責任が重く捉えられることから、経営層が決定すること。「それ以外の情報システム」については、経営層以外で決定することが可能である。

また、「重要な情報システム」が外部委託される場合でも、業務が細分化された結果等、委託業務のリスクが十分に低いと判断しうる場合[28]には、経営層以外で決定することが可能である。

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

次に、以上の決定に従って、委託先の選定等を進めていくこととなるが、外部委託においては、その「委託先等との接点において、最適な統制を決定すること」が重要となることから、各管理フェーズに応じて、安全対策の目標及び配分される経営資源、委託先管理等の体制といった管理の枠組みを、適宜検討することとなる。

「安全対策における基本原則」に従って、安全対策目標は、「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」であるとともに、配分される経営資源は、「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。

本決定は、「重要な情報システム」については、②と同様の理由から、経営層が決定すること。「それ以外の情報システム」については、経営層以外で決定することが可能である。

また、②と同様に、「重要な情報システム」でも委託業務のリスクが十分に低いと判断しうる場合には、経営層以外で決定することが可能である。

④各管理フェーズにおける安全対策の実施

上記の決定を踏まえて、実際の安全対策は、それぞれの管理フェーズにおいて、「安全対策上必要となる IT マネジメント」で例示された、安全対策に携わる関係者が、実施することとなる。

⑤外部委託におけるリスク管理に係る改善事項の決定

「安全対策上必要となる IT ガバナンス」で言及されたとおり、安全対策の実施状況については、関係者によって、運用時のモニタリング等を通じて確認・検証されたうえで、必要に応じて、安全対策に係る態勢等を継続的に改善していくこととなる。

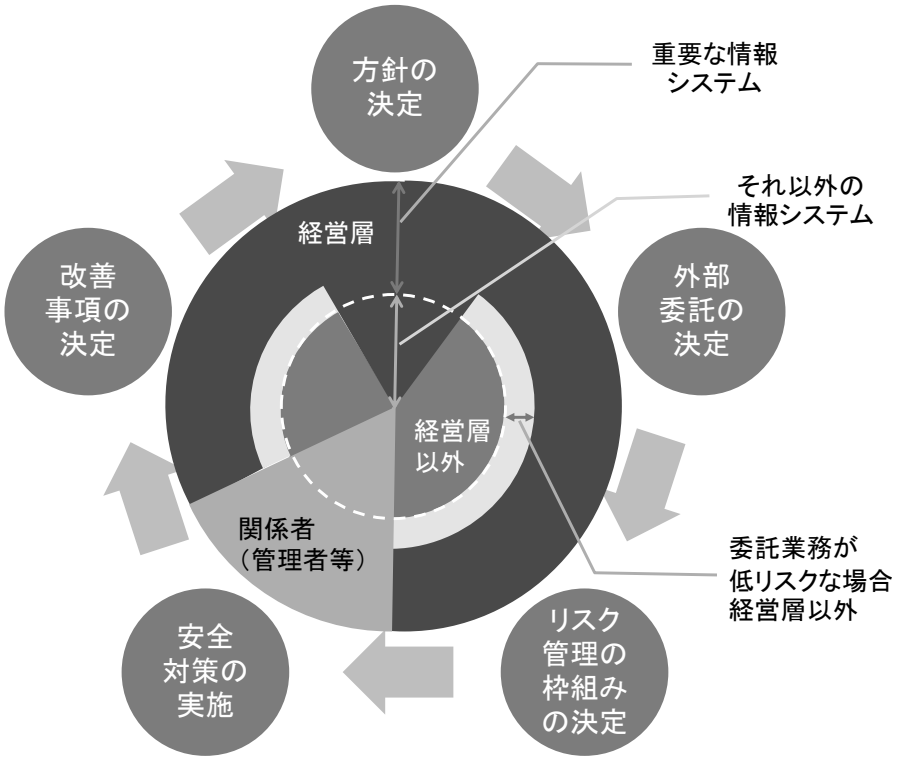
---

[28] 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。

本決定は、「重要な情報システム」については、②と同様の理由から、経営層が決定すること。「それ以外の情報システム」については、経営層以外で決定することが可能である。

また、②と同様に、「重要な情報システム」でも委託業務のリスクが十分に低いと判断しうる場合には、経営層以外で決定することが可能である。

（図表 17）外部委託の管理プロセスにおける IT ガバナンス



（２）各管理フェーズにおけるリスク管理策の考え方

まず、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。そして、その場合、管理フェーズの中でも、再委託先選定の妥当性のチェック、及び再委託先の業務運営を委託先が適切に管理・監督しているか、の２点が特に重要である。なお、それらの管理に当たっては、法令上[29]抵触がないよう留意することが必要である。

そうした考え方を踏まえて、再委託に焦点を当てて、各管理フェーズにおけるリスク

[29] 留意すべき法令として、「労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律」、「職業安定法」、「下請代金支払遅延等防止法」等がある。

管理策の考え方を整理した。

a. 利用検討時

現行の安対基準「外部委託管理」において、再委託に関する言及は無い。

一方で、安対基準「クラウドサービスの利用」においては、利用検討時（運 108）に、クラウド事業者の評価の一項目として再委託が視野に入れられており[30]、あらかじめ再委託を考慮した基準となっている。ただし、この基準には、「データの所在」といったクラウド固有の内容が含まれていることから、そうした部分等を除けば、「クラウドサービスの利用」に関する安全対策基準との整合性に配慮し、外部委託全般の基準として参考とすることが可能[31]である。

b. 契約締結時

現在の安対基準において、再委託に関しては、契約締結に関する考慮事項の１つとして言及されるのみにとどまっている[32]。

一方で、安対基準「クラウドサービスの利用」においては、契約締結時（運 109）に、契約に明記することが望ましいことの１つとして、「再委託管理」が詳細に定められており、「利用検討時」と同様に、参考とすることが可能である。

金融機関等は、再委託先選定の要件や手続きについて、委託先の判断の妥当性を金融機関等として独自の観点から検証することが必要である。特に、「重要な情報システム」の運用の再委託においては、業務に携わった以降は直ちにリスクが顕在化する可能性があることから、その検証は再委託先が業務に携わる以前に行われる必要がある。そうした観点から、個別のリスク管理策の検討が必要である。

c. 開発時

現行の安対基準「外部委託管理」においては、開発もその基準の対象としている。

一方で、安対基準「クラウドサービスの利用」においては、クラウドサービスが主に、既に構築された情報システムを前提としていることから、運用を中心とした基準となっており、開発に関する言及は無い。

そもそも、開発時にはシステムはいまだ本番運用されていないことから、仮に開発の外部委託でリスクが顕在化したとしても、その影響はせいぜい金融機関等の内部にとどまるものと考えられ、さらに機微情報を含む顧客情報が委託先や再委託先に提供されなければ、「重要な情報システム」としてのリスク特性は有していないものと考え

---

30 FISC『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』では、運 108 において、クラウド事業者を評価する事項の１つとして「内部統制やリスク管理等に関する状況（再委託先管理を含む）」とある。

31 クラウドサービスは外部委託の一形態であることから、外部委託全般に適用される基準は、既に策定されたクラウドサービスの基準と整合的に策定されることが必要である。すなわち、クラウドサービスの基準のうち外部委託全般に適用可能なものは参考とすべきであり、一方クラウド固有として考えられる基準は外部委託一般の基準にはしない、という整理を行う必要がある。

32 FISC『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』では、外部委託全般に関する部分（運 88）において、「契約締結の際に考慮する事項としては、以下のようなものがある。」として、機密保護や事故発生時における報告等と並んで「再委託（再委託にかかる責任の所在の明確化・金融機関等の事前承認の必要性等）」と記載があるのみである。

られる[33]。

したがって、リスクベースアプローチを踏まえれば、そうした考え方で、現行の安対基準「外部委託管理」における開発の基準を見直すべきである。また、「重要な情報システム」の開発の外部委託（開発時だけでなく、利用検討時、契約締結時、終了時も含まれる）においても、安全対策の不確実性を低減するという目的の範囲内で定められる「必要最低限の安対基準」の適用対象とすることが可能である。

d. 運用時（モニタリング等）

現行の安対基準「外部委託管理」及び「クラウドサービスの利用」においては、いずれも再委託に関する言及は無い。そのため、新たに再委託先に対する最適な統制としてリスク管理策を検討する必要がある。

委託先が再委託先の業務運営を適切に管理・監督しているか、を検証するに際しては、金融機関等は、委託先によるチェック（日常的監視、監査等）の妥当性もその対象とする必要がある。また、これらは委託先の立場とは必ずしも同一でない金融機関等としての立場から独自に行う必要がある。

金融機関等が検証を行う場合には、自身が行う場合のみならず、第三者に委託して行う方法も考えられるが、その場合でも、あくまで金融機関等の観点から行われるべきである。

以上の観点を踏まえて、個別のリスク管理策の検討が必要である。

e. 終了時

現行の安対基準「外部委託管理」及び「クラウドサービスの利用」においては、いずれも再委託に関する言及は無い。

終了時は、再委託先は委託先と何ら異なる要素はなく、委託先と同様のリスク管理策で十分であることから、現行の安対基準「外部委託管理」及び「クラウドサービスの利用」を、外部委託全般の基準として参考にすることが可能である[34]。

f. インシデント発生時

現行の安対基準では、金融機関等においては、有事対応として、あらかじめ CP を策定することとなっている[35]が、再委託を含む外部委託に関する言及は無い。『金融機関等におけるコンティンジェンシープラン策定のための手引書』（以下「CP 手引書」という）においては、委託先に関する言及はある[36]ものの、再委託に関する言及はない。

---

[33] 開発時のリスクとして、その他に、外部委託先において瑕疵が作りこまれるリスクへの対応は重要である。これは外部委託にとどまらず、情報システム全般のリスクであり、現行の安対基準等を参考として、必要十分な品質管理が求められる。

[34] FISC『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』では、終了時に関連して、運 109 において、契約上明記することが望ましい事項として「クラウド事業者の方針変更によって続行が困難となる」事態を想定した安対基準も設けられている。

[35] FISC『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』では、運 65 において、「不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧をはかるために、あらかじめコンティンジェンシープラン（緊急時対応計画）を策定しておくこと。」とされている。

[36] FISC『金融機関等におけるコンティンジェンシープラン策定のための手引書』では、リスクの洗い出しにおいて外

また、安対基準「外部委託管理」及び「クラウドサービスの利用」においては、インシデント発生時における再委託を含む外部委託に関する言及は無い。

インシデント発生時、特に重要な情報システムにおいて発生する有事対応は、リスクベースアプローチの「安全対策における経営責任の在り方」において、経営層が、法的責任を果たすための重要な要素とされていることから、CP 手引書だけでなく、安対基準においても、再委託を含む外部委託における有事対応に関するリスク管理策の検討が必要である。

なお、以上の整理は、重大な社会性・公共性を有する「重要な情報システム」に関するものであり、それ以外の情報システムに関しては、委託先が再委託先を適切に統制していることの確認をもって十分とすることも考えられる。すなわち、委託先が再委託先に対して行っている統制が、金融機関等が行っているのと同程度以上に適切に機能している場合は、それに依拠することは経営資源の観点からも有益である。

４．再委託のリスク管理策

以上の考え方を踏まえて、運用の外部委託における再委託のリスク管理策を提案する。

（１）再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、委託先との委託契約の締結に当たっては、適切な再委託先が選定されるよう、再委託先の選定要件をあらかじめ定めること。

選定要件には、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、再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、も含まれ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再委託先であっても、専門性等の理由により、再委託せざるをえない場合には、勤務場所を委託先の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。

次に、「重要な情報システム」が再委託される場合は、金融機関等は、以上の選定要件を踏まえて､委託先が再委託先を選定することを前提としその妥当性を検証するために、再委託先の事前審査を行うこと。

また、「重要な情報システム」以外の情報システムの再委託に際しては、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[37]ことで、そうした検証結果の確認をもって、個別の再委託

部委託も考慮すべきこと、緊急時体制は重要な外部委託先等との連携態勢についても考慮すること、外部委託先を含めた訓練を行うこと、等が定められている。

[37] 具体的な検証方法については FISC『金融機関等のシステム監査指針（改訂第３版追補)』「第１部　第Ⅲ章　５．クラウドサービス監査のポイント」「（２）クラウド事業者による再委託先審査・管理プロセスの実効性を確認するための検証事項」において、明確にされている。

先の事前審査に代替させることが可能である。

さらに、「重要な情報システム」が外部委託される場合でも、委託業務が細分化され再委託先に委託された結果、その再委託業務のリスクが十分に低いと判断しうる場合には、上記の簡易な手続きで代替することが可能である。

（２）再委託先への監査権の明記[38]

「重要な情報システム」が外部委託される場合は、委託先との委託契約の締結に当たっては、再委託先をチェックする仕組みを担保するため、金融機関等による再委託先への監査権を明記すること。

金融機関等は、委託先に対するのと同様に、再委託先に監査を実施する場合には、自己の責任において監査を行うことが必要である。「自己の責任において」とは、その監査項目も金融機関等が再委託先のリスク特性を踏まえて、みずからの検証ニーズに則って設定し、さらにその実施時期も委託先等に過度に配慮することなく、金融機関等がみずから適切と思われる時期に行うことをいう。監査に当たっては、みずからが実施する[39]以外にも、適切な監査人に監査を委託することも可能である。

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[40]。

また、「重要な情報システム」以外の情報システムが外部委託される場合は、委託先との委託契約の締結に当たっては、金融機関等による再委託先への監査権を明記しないことが可能である。

さらに、「重要な情報システム」が外部委託される場合でも、委託業務が細分化され再委託先に委託された結果、その再委託業務のリスクが十分に低いと判断しうる場合には、上記の簡易な手続きで代替することが可能である。

（３）有事対応

「重要な情報システム」（委託業務が細分化された結果、リスクが十分に低いと判断しうる再委託先を除く）が外部委託される場合は、CP は委託先や再委託先も含めて策定される必要がある。また、委託先等で CP を個別に用意する場合は、各金融機関等の CP と完全に整合し相互補完的な内容とする[41]こと。また、金融機関等は、平時は、委託先等と

---

38 監査権を明記すべき契約には、請負、委任といった契約形態は問わない。

39 監査の方法として、委託先に情報の提出を要請し、その内容の確認だけでは委託業務の適切性の検証が十分できない場合に、委託先に立入り実地で確認する方法、あるいは、既に委託先が受検している監査結果（SOC2、IT7 号等）が提出された場合は、その内容を検証し、疑問点や不足する監査項目を中心に委託先に立入監査を行う方法等がある。

40 FISC『金融機関等のシステム監査指針（改訂第３版追補）』「第１部　第Ⅲ章　５．クラウドサービス監査のポイント（１）クラウド事業者に対する第三者監査人を利用した共同監査の検討」において、監査人の選定として、「顧客に対して責任を負う金融機関として、第三者から見た際に、クラウド事業者との利益相反に疑義が生じるような外観を呈していない監査法人を選定することが必要である。そのために、委託元金融機関は、共同監査の対象機関において、クラウド事業者の会計監査に従事していない監査法人を選定することが必要である。また、クラウド事業者の SOC2、IT7 号の保証業務に従事している監査法人を選定する場合には、クラウド事業者の SOC2、IT7 号の保証業務に従事していない監査責任者を選定することが必要である。」とされている。

41 コンティンジェンシープラン（CP）の実効性確保における課題として、地方銀行の 57.1%、第二地銀の 67.7%、信用金庫の 44.2%、信用組合の 60%が、「業務継続に必要な関連先と自社のプランとの整合性」を挙げており、共同セン

の CP に基づき、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。

委託先や再委託先は、「重要な情報システム」で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 CP 発動に係る意思決定を支援する。また、CP 発動が決定された場合は、金融機関等は、その旨を委託先や再委託先へ伝達するとともに、委託先等の CP の実施状況を監督すること。

なお、「開発」の外部委託においては、「再委託先の選定要件の策定」は必要である。「再委託先の事前審査」「再委託先への監査権明記」は、「重要な情報システム」「重要な情報システム」以外の情報システムのいずれにおいても、上記の簡易な手続きで代替することが可能である。

（図表 18）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

ターの CP と利用金融機関の CP との整合性確保が求められている。（FISC 『平成 27 年度金融機関アンケート調査結果』）

Ⅴ　共同センターにおけるリスク管理の在り方

サマリー

◆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。

近年多くの金融機関が、勘定系システム等の重要な情報システムを中心に共同化を進めており、特に預金取扱等金融機関においては、実にその 90%が、勘定系システムで共同センターを利用している[42]。

共同センターは、外部委託の一形態として、勘定系システム等の重要な情報システムを、複数の金融機関が共同で委託していることから、金融インフラ全体に重大な影響を及ぼすリスクが委託先へ集中している形態である。

こうした中、複数の共同センターで、再委託先社員によるキャッシュカード偽造事件等不正事案が発生しており、そのリスクがあらためて認識される一方で、共同化の進展とともに金融機関のシステム部門の職員数が減少しており[43]、金融機関が共同センターに対して、新たなリスク管理策を求めるといっても、そのために必要となるスキルやノウハウを保有した人材の不足が危惧される。こうしたことから、共同センターの意義と課題を明らかにしたうえで、外部委託におけるリスク管理の在り方を踏まえて、共同センター固有の特性に対するリスク管理策を付加的に検討することが必要である。

１．共同センターの意義と特徴

（１）共同センターの意義

共同センターとは「特定かつ複数の金融機関が、共同で、特定の外部委託先に対して、重要な情報システムの運用等を委託する外部委託の一形態」のことをいう。

ここでいう、「共同」には、利用金融機関が委託先と共同委託契約を締結している場合だけでなく、利用金融機関が委託先と個々に委託契約を締結している場合でも、それぞれの金融機関の情報システムにおいて、個別金融機関のシステム障害等の影響が、直ちに他の利用金融機関へも及びうる程度に、実質一体となって運営されている場合も含まれる[44]。

（２）共同センターの特徴

共同センターは、システム投資の効率化等を目的に、古くは 45 年前から信用金庫においてその利用が始まり、現在では、金融機関が情報システムを運用する場合等において、一般的かつ主要な利用形態となっている。【資料編資料６～８参照】

①協同組織金融機関

およそ 30 年前、預金取扱等金融機関における第３次オンラインシステム[45]（以下「３

---

[42] 勘定系システムで共同センターを利用している地銀は 78.3%、第二地銀は 75.0%、信金・信組にいたっては、それぞれ 97.2%、 97.4%が共同センターで勘定系システムを利用している。（FISC にて調査）

[43] 勘定系システムを自営している場合は自機関のシステム要員数が平均 53.4 人であるのに対して、勘定系システムを自営していない場合は平均 12.8 人となっている。（FISC『平成 27 年度金融機関アンケート調査結果』）

[44] 本検討会第１回において、「システムに係る外部委託の範囲」として、全銀システム、統合 ATM、協同組織金融機関為替中継システム等の金融機関相互のシステム・ネットワークのサービス利用は、外部委託とは別の形態として整理している。

[45] 第３次オンラインシステムは、①業務処理のいっそうの合理化・省力化の推進、②業務分野の拡大への対応と新金融商品や機能サービス等の迅速な提供を可能とする、柔軟で拡張性のあるシステム基盤の整備、③対顧客ネットワークの充実、④収益管理やリスク管理、及び戦略的な営業展開を図るための情報機能強化等を目的としており、当時においては大規模なシステム投資を必要とするものであった。（FISC『平成 28 年版金融情報システム白書』）

次オン」という）の展開に当たり、都市銀行や多くの地域銀行は独自に開発を行ったのに対して、協同組織金融機関では、同一業態の金融機関どうしでベンダーと共同開発・共同運用を行うことで対応したことが、本格的な共同センター利用の始まりである。その後も、システムコストの削減、主要業務のコア戦力の集中化等を目的に、業態連携による共同センターの利用が継続されてきた。

協同組織金融機関においては、業態単位で、金融機関の出資により、開発・運用を一元的に行う管理組織が設立され、その管理組織が金融機関の合意形成を支援するとともに、委託先のベンダーを管理するといった機能を果たしている。こうした体制は、経営資源が限られているなかで、必要となるシステムの機能拡充といった新規開発、バックアップセンターの確保等の安全対策を、実効的かつ効率的に実施するために必要な体制として、45 年にわたり継続されてきたものと考えられる。

②地域銀行

第二地方銀行（当時の相互銀行）の一部においては、比較的早期からシステム共同化が行われているが、地方銀行においては、システムコストの抑制、システム化領域の広がりによるシステム要員の増員、高度化する技術への対応といった理由から、平成 10 年頃から順次共同センターの利用が始まっている。

協同組織金融機関のように運営組織を設立し、当該運営組織がベンダーに業務を委託するのではなく、個々の金融機関がベンダーに直接委託する形態がとられるとともに[46]、合意形成のためには、すべての利用金融機関の責任者が参加する会議体が組成されるのが、一般的である。

２．共同センターの課題

地域銀行における複数の共同センターにおいて、スキル及び権限を有する再委託先の責任者がカード偽造を行う等といった不正事案が発生した。一方で、共同化の進展に伴い、効率性を追求した結果として、システム部門の職員数は削減されており、金融機関においては管理責任を果たし主体的なリスク管理策を実行するために十分な経営資源がないことが危惧される。

前者の課題は、「Ⅳ　外部委託におけるリスク管理の在り方」、後者の課題は、「Ⅱ　IT ガバナンスと IT マネジメント　３．人員計画に係る留意事項」において、対策を提案済みである。

こうしたこれまでの検討結果を踏まえて、さらにその実効性を担保するために、共同センター固有の特性を明らかにしたうえで、補助ルールとして、付加的なリスク管理策の検討を行う。

---

[46] ベンダー選定に当たっては、参加金融機関の規模や IT 戦略を踏まえて決定されることもあれば、まず自営時代からなじみがあり安定稼働の実績があるベンダーが提供する共同センターに加入するといったこともある。（FISC 刊行物平成 22 年度地域金融機関 IT 研究会報告書『地域金融機関における IT ソーシング戦略再考』）

３．共同センターの特性

共同センターにおいては、委託先との関係において、複数の委託者の意思の統一とそのための手続きが必要となるが、その手続きに要する時間等その程度が、単一金融機関の場合と同程度まで完備されうるものとは想定しがたく、そもそも、単一金融機関の場合と同程度の迅速かつ円滑な意思決定が常に可能か、不確実性が残る[47]。

特に、一刻一秒を争う有事においては、上記の不確実性に基づく、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可能性がある。こうした有事対応における時間性の問題は、現在、よりその深刻さを増している。例えば、近年、サイバー攻撃が活発化しているが、特にその攻撃対象金融機関が共同センターを主として利用している金融機関にまで拡大している[48]。また、ソーシャルメディアの普及により、社会的な情報拡散のスピードが高速化しており、風評リスクが急速に増大しうる環境にある。さらには、決済の24時間365日化が進められており、日中深夜を問わず、信用不安が瞬く間に深刻化しうる環境にあることは、事実として、重く受け止められるべきと考えられる。

また、共同センターでは、障害等のシステム運営上の個別金融機関の問題の影響が、直ちに他の複数の利用金融機関へも波及するという特性を有する。

なお、このような特性に対して、協同組織金融機関においては、共同の出資による運営組織が設立されている場合は、その中で対処がなされている、あるいは今後進められていくものと考えられるが、その他の協同組織金融機関や地域銀行においては、参加行が少数となる、あるいは参加行の出入りがある、等の理由から、そうした対応は現実的ではないものと考えられることから、固有のリスク管理策の検討が必要である。

４．共同センター固有のリスク管理策の考え方

以上の共同センター固有の特性を踏まえて、リスク管理策の考え方を整理する。

まず、現行の安対基準「外部委託管理」においては、外部委託管理の冒頭やシステム監査において、共同センターについて若干の言及はある[49]ものの、前述の共同センター固有の特性を、必ずしも踏まえたものとはいえない。

---

47 そうした意思の統一に要する時間を短縮するために、共同委託者を少数にとどめている共同センターも存在する。また、リーダー行（幹事行）を設置し、その主導により、意思統一の時間短縮を図る共同センターもある。その場合でも「新サービスや機能強化など、独自機能を実現するための開発案件の採否決定に際しては、共同化グループ内での協議結果を待たなければならず、案件によっては時間がかかるものも少なくはない」という声がある。（FISC 刊行物平成 22 年度地域金融機関 IT 研究会報告書『地域金融機関における IT ソーシング戦略再考』）

48 平成 27 年のインターネットバンキングに係る不正送金事犯による被害額は、約 30 億 7,300 万円と 26 年をさらに上回っており、その被害の特徴としては、被害金融機関数が倍増し、特に信用金庫、信用組合に被害が拡大したこと、農業協同組合と労働金庫で被害が発生したこと等が挙げられる。（警察庁広報資料「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」）

49 FISC『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』では、外部委託管理の冒頭において「複数の金融機関等が、ホストコンピュータ等を共同で運用する「共同センター」の利用も一般的になってきた。」という認識が示されているものの、安全対策については「共同センター等委託元が複数の場合は、複数の委託元が共同で監査を行い個別の監査を代替することも可能である」「バックアップシステム（バックアップサイト設置分を含む）への切替え（強制切替え、システム運用時の諸制約等を踏まえた切替え判断及び運用手順、共同センターにおける切替え判断等を含む）」等の記載にとどまっている。

平時において、情報システムが安定的に運営されている場合には、利用金融機関の意思決定手続きの完備程度の相違が、決定的な結果を生ずるとは考えられないが、こと「インシデント発生時」特に「重要な情報システム」において発生する有事においては、意思決定の時間的な遅れが、深刻な結果をもたらす可能性があることは前述のとおりである。

このような有事対応における責任は、金融業務の特性から派生していることから金融機関が一義的に負うべきであり、情報システムの開発や運用に係る技術的な側面を担う委託先が負えるものではない。

こと「重要な情報システム」においては、「重大な外部性」を有していれば、その影響は顧客等の内部影響にとどまらず、金融インフラや経済の安定的な運営にも影響を及ぼす可能性があり、技術的復旧のみならず、こうした側面への十分な考慮をすることが必要である。また、「機微な個人情報」を有していれば、例えばその流出が、預金流出の端緒となり、信用不安を惹起し、金融機関の存立を揺るがす事態に発展することにもなりかねず、有事対応に当たっては細心の注意を払うことが必要である。

こうした問題に対処するには、有事の初動対応が決定的に重要であり、これが考えうる最善の対応となるよう平時から万全の対策[50]を講じておくことが必要なことから、既に安対基準等でもある程度ルール化されているところである。しかしながら、前述の「時間性」の問題を踏まえると、これでも万全とは言い難く、CP の想定外の事態の発生や、想定外の事態等を背景として不可避となる意思決定の時間的遅れが生じうることを考慮に入れることが必要である。

また、有事を踏まえた対応体制の整備等への経営資源配分、あるいは有事における重要な意思決定権限やプロセスの整備において、経営層の役割と責任が極めて重要であることから、IT ガバナンスの観点からも検討することが必要である。

なお、「運用時」は、安対基準「クラウドサービスの利用」においては、複数者が委託するという共同センター類似の形態という点において、共同監査について、参考となる基準として言及することが可能である。

それ以外の管理フェーズについては、共同センター固有の特性との関連性が薄いと考えられることから、付加的に考慮すべき事項はない。

５．共同センター固有の IT ガバナンス（リスク管理策策定の在り方）

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。

---

[50] 例えば、既に取り組まれていることの繰り返しではあるが、①意思決定手続きを可能な限り時間的にも完備なものに整備する。②想定する事態をすべて盛り込んだ CP を策定する。③平時から十分な訓練を繰り返し、習熟度を高める努力を怠らない。といったことが考えられる。

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、以下のような管理策が考えられる。

【例】有事対応等責任者の設置

利用金融機関の意思決定がなされるまでの間、CP の現場における委託先への指示等の業務を執行し、また、CP に想定されていない事態で、瞬時に対応する必要がある事態への対応を行うことを目的として、有事における対応等責任者を、任命・配置する。

有事対応等責任者は、上記の対応を行うに当たって必要となる権限を、契約[51]において利用金融機関からあらかじめ授権される。

また、有事対応等責任者は、有事において、金融業務の特性を踏まえ判断することが求められることから、利用金融機関から、有事対応等の適格性[52]を有する要員を選定する。

・有事対応等責任者の平時の役割

有事対応等責任者は、有事に対応を行うに当たって、平時から小さな異常も見逃さない等システムの運営状況に目を配っておく必要があることから、共同センターに対するモニタリング組織の長の役割も担う。

有事対応等責任者は、モニタリング活動への常時・継続的な参加に当たっては、利用金融機関の担当者にその役割を担わせ、担当者からの報告をもって、その活動に代替する等、実態に合わせて利用金融機関や委託先等から要員を集め、組織的な運営も考慮する[53]。

・有事対応等責任者の有事の役割

「重要な情報システム」における有事に際しては、有事対応等責任者は、利用金融機関の意思決定がなされるまでの間、CP の現場における執行を行うとともに、CP に想定されていない事態で、瞬時に対応する必要がある事態へ対応を行う。また、有事対応等責任者は、利用金融機関の意思決定がなされた後も、現場において、金融業務の特性に係る情報を収集し、利用金融機関へ適時適切に還元するとともに、事態への対応策について、現場の実態に照らして適切な助言を行う責務を負う[54]。

---

51 ここでいう「契約」には、共同センターの利用に当たって必要となる契約全般を差し、委託先を交えた契約だけでなく、利用金融機関間の契約も含まれる。

52 有事対応等責任者がその役割を果たすために必要となる適格性の要件としては、自然災害・大規模システム障害・サイバー攻撃等の有事に、業務執行可能であるために、共同センターの設置場所もしくは管理場所に速やかに駆けつけられる状態にあることも考えられる。また、例えば利用金融機関との連絡がとれないといった極限状態において、重要な判断を速やかに行うことが求められる場合も想定されることから、利用金融機関における一定の役職者であることも考えられる。

53 なお、モニタリング組織は、技術的な面もあり、大半が委託先のスタッフで構成される場合もあるものと考えられる。一方で、モニタリングという、委託元が委託先を管理するというその本来の性質上からも、モニタリング組織の長は、金融機関から選定されることの妥当性は明らかである。

54 サイバーセキュリティ対応として、共同センターに CSIRT が設置され、そこで技術的な業務（検知、分析等）のみならず、金融的な業務（発生事情を踏まえた金融機関としての対応判断、対顧、当局説明等）を担う場合は、有事対応等責任者がその役割を担うことが必要である。

その他に、監査に当たっては、共同センター利用金融機関の個別監査といった種々の監査方法を選択しうるが、監査の実効性や効率性の担保という観点から、クラウドサービスで検討された共同監査スキームを共同センターにおける監査の一手段とすることは有益である[55]。

[55] FISC『金融機関等のシステム監査指針（改訂第３版追補）』において「第１部　第Ⅲ章　５．クラウドサービス監査のポイント」として、共同監査スキームが提案されており、そのプロセスや考慮点が示されている。「共同監査体制の確立」といったクラウド固有の要素も含むが、「共同監査のプロセス」や「監査人の選定」「監査人の説明責任」等の考慮点は、共同センターにおいても有益となるものである。今後、監査指針の改訂においては、複数者で委託する場合の共同監査の方法として、クラウドサービス、共同センターを視野に入れて、統合的に整理していくことが考えられる。

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

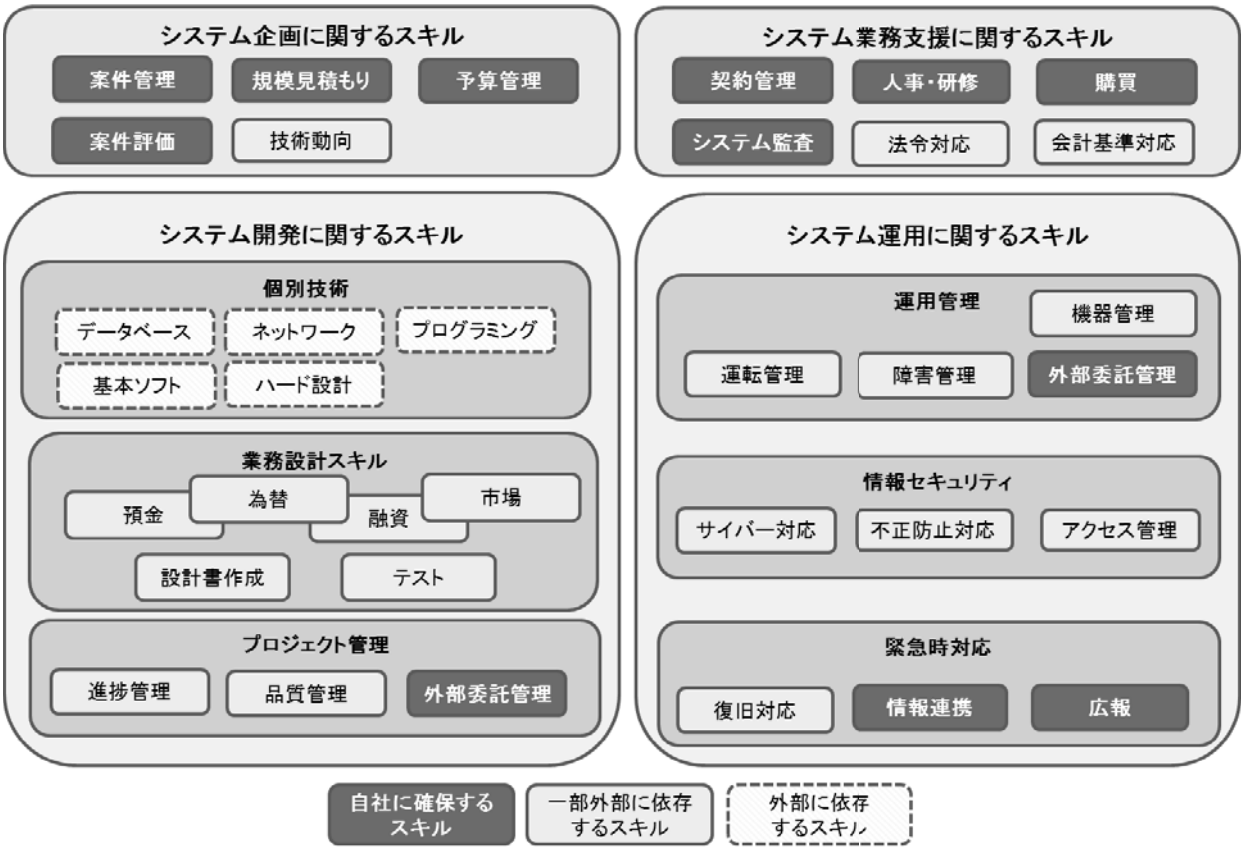
柴田　晃宏、宮原　武也（第４回まで）、仲程　文徳（第５回から）、岡本　一真、三浦　哲史（第５回から）

（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）

Ⅶ　資料編

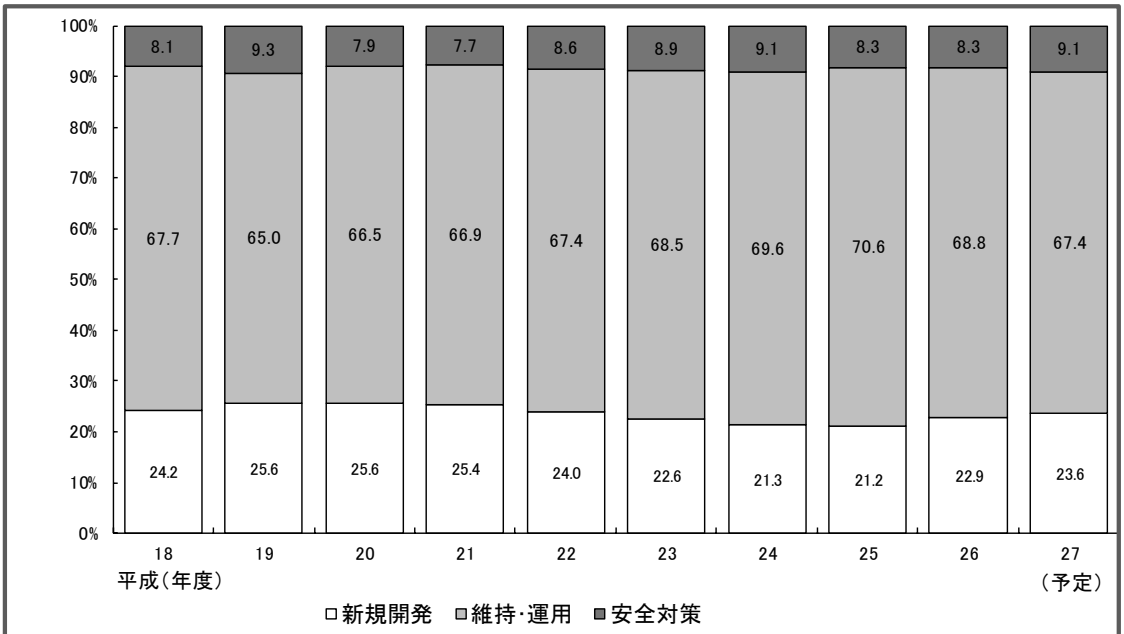
【資料１】IT スキルマップの一例



（出所）FISC にて作成

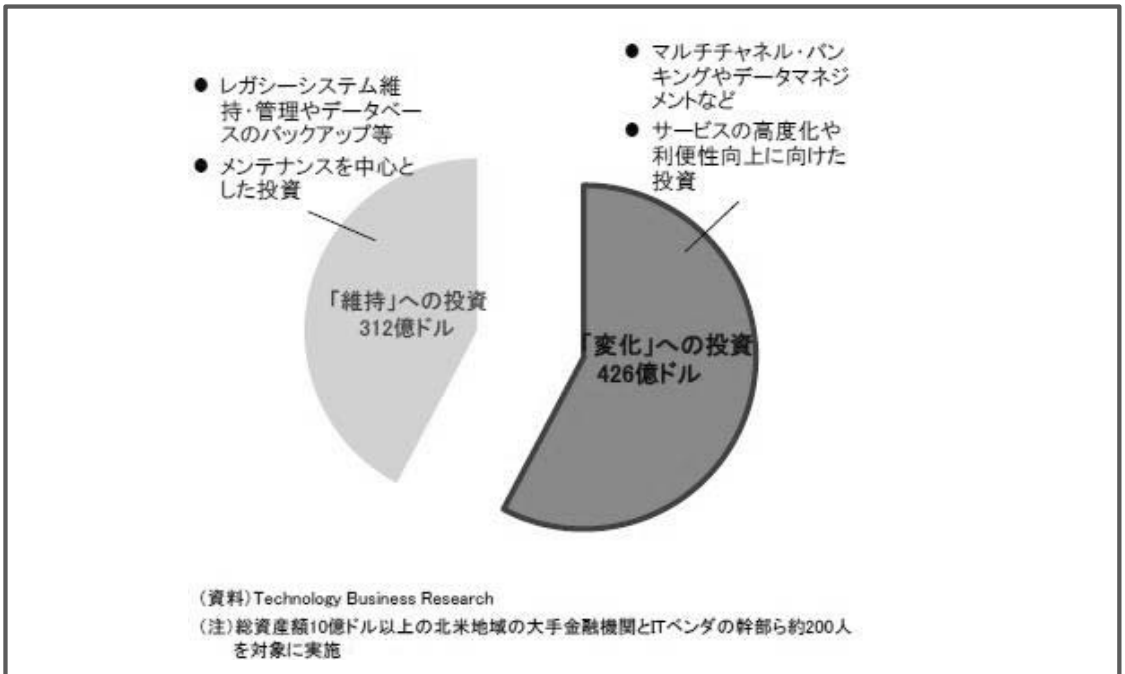
【資料２】システム関連経費の目的別内訳

邦銀のシステム関連経費の目的別内訳



（出所）FISC調査「平成27年度金融機関アンケート」（平成27年3月）

米銀のIT予算の優先投資分野(2014年)



（出所）金融審議会「決済業務等の高度化に関するスタディ・グループ第２回」（平成26年10月）

【資料３】リスクベースアプローチに関する海外監督当局等の動向

１．リスクベースアプローチの背景

英国では、2000 年に成立した金融サービス市場法を背景に、同年、旧金融サービス機構(FSA)より新しい規制アプローチとして「リスクベースアプローチ」を採用する旨が公表された。その後、リーマンショック等の金融危機を経て、2013 年に新たな金融監督体制が導入されたものの[56]、従来の「リスクベースアプローチ」の考え方に大きな変更は生じていない。

監督当局が示す「リスクベースアプローチ」の考え方は、監督当局の政策上の目的が達成されないリスクを基準として、外的なリスク要因に対して監督上の優先順位の設定や資源配分等を行うというものである。公表文書『Risk-based regulation in the UK（2005 年)』によると、リスク選好（Risk Appetite）を「影響度（Impact)」と「蓋然性（Probability)」の観点から決定し、「問題発生の可能性がある」だけではなく、「問題発生の可能性が高く、かつ影響度も大きい」ものについて優先的に対応するとしている。

また、同文書には、リスクベースアプローチの意義を、「経営資源は無限ではない。ゼロ停止を目指すといったアプローチすべてを実施することは不可能である。したがって作業の優先度付けの仕組みが必要である。経営資源を最適に配分して意思決定していく必要がある。」としている。

上記のとおり、英国のリスクベースアプローチは、リスク顕在化の可能性がどの程度高いか、またどの程度影響度が高いかという考え方を基準としているが、その実行は各金融機関の判断に委ねている。これは、従来英国金融監督当局が、金融機関の自主性を重んじる原則主義アプローチを採用していることに由来する。基本的には、各金融機関において適切なリスクコントロール手法の決定及び実践を期待しており、仮に適切かつ十分なリスクコントロールが行われていないことを確認した場合には、監督当局がアクションを起こすという考え方である。

米国でも、リスクベースアプローチが重要視されており、昨年度末の監督当局へのヒアリング結果によれば、「IT をリスクベースにしていることは、中小金融機関にとっては特に重要となる。IT の分野で 100 点満点を取ろうと思ったら、膨大なコストがかかる。コストと万一の場合の被害の大きさのバランスで、どこまでやるべきかを判断することになる。特に、中小金融機関の場合は経営資源が限定されているので、IT の特定の部門で 100 点満点をとるよりも、それにかかるコストを他の分野に振り向けた方がよい場合がある。」と、金融機関の IT ガバナンスに係るリスクベースアプローチを重要視していることが確認できた。

２．リスクベースアプローチに基づいたリスク管理策

①重要度に応じたリスク管理策

米英の監督システムは、原則主義であり、ガイダンスなどにリスク区分法やリスク管理策については必ずしもこと細かく成文化していない。昨年度末実施した米国の監督当局のヒアリングにおいても「成文化すると、それが絶対的になり、本当はもっとよい方法があるかもしれないのに、それ

56 一元的な監督当局であった FSA を解体し、新たに「金融政策委員会（FPC)」「健全性規制機構（PRA)」「金融行為規制機構（FCA)」の 3 つの機関を設立した。

を見逃し、イノベーションが起きないという問題がある。」と成文化していない理由を明確に述べている。

一方で、米国の監督当局では、金融機関に対し必要最低限の対策として以下の３点を要請していることがわかった。

A) グラム・リーチ・ブライリー法（情報漏洩防止等の情報セキュリティ対策）の遵守

B) 高リスク取引（資金移動等）に対して高いレベルのセキュリティ対策の実施

C) BCP の策定

米英の金融機関の取組みとして、CIA（機密性、完全性、可用性）に基づいた格付により、重要度を判定している事例や、金銭的な「損失」、対外的な「影響度」という要素に基づいて、重要度を判定している事例が見られた。重要度の判定結果は、システムオーナーがリスク管理委員会にて報告し、審議されることが通例とされている。

米英とも重要度に応じた管理策について当局から、基本的には各行の事情に応じた管理策の決定・実行が要請されている。

②重要業務の定義

そうした中でも、海外の外部委託に係るガイドラインにおいて、「重要な銀行機能・共有サービスや顧客に深刻な影響を及ぼす業務」等を「重要業務」として、特段の定義をするとともに、個別の管理策を示している。

英国では、金融行為監督機構（FCA）が定めるハンドブックの外部委託に係る項目「SYSC8」は「脆弱性、障害等により金融機関が原則を遵守し続けることへの深刻な影響を及ぼす可能性がある業務」と示した重要業務（critical or important functions）に対しての外部委託管理策の遵守を要請している。（届け出制）。

米国では通貨監督局（OCC）が第三者関係リスク管理に係るガイドラインにて「重要な銀行機能（支払、精算、決済、保管等）、重要な共有サービス（例：IT など）、又は顧客に深刻な影響を及ぼす可能性がある活動等が含まれる」と示した重要業務（critical activities）を外部委託する際には、取締役会の承認を前提とするなど、経営層の監督強化が要請されている。

星国では金融管理局（MAS）が IT リスク管理の原則及びベストプラクティスとして定めるガイドライン「TECHNOLOGY RISK MANAGEMENT GUIDELINES」にて、「当該システムの停止が金融機関の運営に重大な中断を誘発することや、金融機関の顧客へのサービスに多大な影響をもたらしうる」と示した重要システム（critical systems）には高可用性の実現を要請している。

３．IT ガバナンスに係るガイドライン

米国当局 FFIEC が 2015 年 11 月に公表した IT Examination Handbook「Management」には、金融機関における IT ガバナンス、IT リスク管理の位置づけが示されており、特に以下の３点が特徴として挙げられる。

①IT に関する取締役会の役割を具体化

A) 全社的な経営戦略に沿った IT 戦略方針（情報セキュリティ戦略やサイバーセキュリティ等を含む）をレビュー・承認

B) 効果的なITガバナンスを促進

C) 外部委託先の承認プロセスを監督

D) ITに係るプロジェクトや予算、優先度等のITパフォーマンスを監督

E) ITリソースの適切性を監督

F) 重要なセキュリティに係る事項について、経営層や委員会、政府当局等に報告/承認する態勢を定めた内部規程を承認

G) ITリスクの特定・方策・削減に係る管理責任

H) ITコントロールに係る効果的な監査を促進

②ユーザー部門のITにおける役割の明示

IT委員会の役割・責任[57]について明記しているが、本委員会は、経営層及びIT・リスク管理部署に加えてユーザー部門のスタッフにより構成することと規定している。また、ITリスク管理態勢においても、IT部署だけではユーザー部門に所属するマネージャーもITに係る業務について責務を負う旨が明記されており[58]、IT部署と関連するユーザー部門との連携を重視していることがわかる。

③外部委託管理の重要性の強調（取締役会での役割の明確化）

取締役会の監督責任の１つに「外部委託管理」を明記している。また、リスク管理の各プロセス（リスクの特定／評価／削減／モニタリング及びレポーティング）において、外部委託先のリスクを管理するよう明記されており、米国において外部委託管理が非常に重要視されていること、監督・管理の優先度が高いことがわかる。

57 ビジネスサイドの要請に応じたIT戦略の立案やITパフォーマンスの監督、IT業務に関連する事項の経営宛報告、ITに係る適切な情報の収集及び社内ITリソースのモニタリング、社員向けトレーニングの適切性の監督 等。

58 ビジネスサイドのニーズや新商品開発計画等につき、ITサポートやビジネス上のラインマネージャーに報告するプロセスを確立する等の業務が挙げられる。

【資料４】「外部性」及び「情報の機微性」という考え方

十全なリスクベースアプローチ（以下「RBA」という）を導入できる能力を有する金融機関等においては、みずからの力で、リスクの顕在化による経済的損失額等を正確に把握することが可能であることから、リスクの低減や受容といった判断、それに基づく安全対策や経営資源配分の効率的な決定等が可能であり、本来は、社会的なルールの提供は不要であるはずである。

それにもかかわらず、「重大な外部性」に対して、社会的に合意されたルールが必要と考えられる理由を以下に、『「外部性」という考え方』として解説する。

また、重大な外部性こそ有していないものの、個人情報の取扱いにはあらかじめ特段の考慮が必要であり、特に「機微性を有する情報」に対して、社会的に合意されたルールが必要と考えられる理由を以下に、『「情報の機微性」という考え方』として解説する。

■「外部性」という考え方

・ここでいう「外部性[59]」とは、例えば、個別金融機関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へ発展し、経済的損失が拡大する可能性のある性質を有する。

・ここでいう「外部性」には、個別金融機関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、十全な RBA を導入できる能力を有す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。

・事後的に社会に与えた損失額の一部は損害賠償等の形で還流してくる可能性があるが、それも、決済チェーンの遠隔部分での事案であれば、複合的な原因連鎖の中で当該金融機関の責任部分を特定することは困難である。（国を跨ぐ際の裁判管轄や法的執行力の問題、訴訟費用のハードル等の要因等まで含めると、還流してくるのはごく一部にとどまる。）

・このような状況下、金融機関等は上記理由や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又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して「…する必要がある」等のルール（＝高い安対基準相当）が必要となる。

[59] なお「外部性」とは　externality　を意味し、外部委託で使用される「外部」　outsourcing / third party　とは意味が異なる。

■「情報の機微性」という考え方

・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。

・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遍在している個人情報が、この機微情報に影響されて過度な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からである。

(参考)「金融分野における個人情報保護に関するガイドライン」

第６条 機微（センシティブ）情報について

1　金融分野における個人情報取扱事業者は、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下「機微（センシティブ）情報」という。）については、次に掲げる場合を除くほか、取得、利用又は第三者提供は行わないこととする。

①…（略）

⑧機微（センシティブ）情報に該当する生体認証情報を本人の同意に基づき、本人確認に用いる場合

・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」と「その他の個人情報」を分け、「機微情報」については、「重大な外部性を有する」システムと同様に「…する必要がある」等のルール（＝高い安対基準相当）を適用することが妥当である。

・「機微情報」は、本人の許諾なく機微情報が流出した場合、経済的損失にとどまらず、基本的人権の侵害といった広範な損失を被る可能性があることから、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。

ここまで述べてきた「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以外にも、金融機関等のシステムの中には、重大な外部性こそ有していないものの種々の要因からリスクの程度がそれと同等又はそれ以上に高い、と金融機関等が判断する情報システムは、当然ありうる。(p33（図表 16）簡易な RBA の㋑に含まれる情報システム）そうした情報システムに対して、各金融機関等が「…する必要がある」等のルール（＝高い安対基準相当）を適用することには一定の合理性があり、勿論、リスクに見合うとの判断からそれ以上の対策を講ずることも想定しうる。

【資料５】FFIEC　IT 検査ハンドブック「マネジメント：外部委託管理」

対策のサマリー

金融機関の外部委託におけるリスク管理策において、上級管理者は、委託目的が効果的に実現されるよう下記に留意することが必要である。
・金融機関の要件を適切に反映した契約条項となるよう十全な契約交渉を行うこと
・少なくとも年次で委託先から監査済み財務諸表を受領すること
・委託先における IT 統制に係る監査結果を確認すること
・委託先の金融機関への対応力を継続的に確認すること

近年、金融機関の外部委託への依存度が高まっている。金融機関の組織が、大規模化・複雑化するに従って、すべての委託先を対象として、組織的・統合的な外部委託管理が行われる傾向にある。IT 部門は、外部委託を利用し、データ処理、ソフトウェア開発、設備管理、事業継続、ストレージサービス、インターネット接続やセキュリティ管理等、さまざまなサービスを受けることが可能である。一方、組織が小規模化・単純化するに従って、オペレーション・財務・コンプライアンスの観点から、委託先を熟知している社員によって、委託先に応じて個別の管理が行われる傾向にある。

取締役会は、委託先を適切に監督する責任を担う上級管理者を設置することが必要である。外部委託の決定においては、経営目標を達成するために必要となるテクノロジーの有無が、外部委託するか否かの重要な判断要素の１つとなる。また、テクノロジーだけでなくガバナンスもそうした要素の１つとなる。そのため、外部委託におけるリスクを特定・評価・低減・監視するための効果的な管理態勢が必要となる。上級管理者は、金融機関全体の外部委託管理の方針と管理プロセスを策定することが必要である。管理プロセスには、外部委託の目的や戦略の決定、委託先の選定、契約締結、モニタリングが含まれる。

上級管理者は、「重要な情報システム」の外部委託においては、委託先の品質、統制環境、財務状況を評価することが必要である[60]。委託先には、金融機関の関連会社、その他の金融機関等が含まれる。委託先は、金融機関に遵守が求められる法令、規制、監督指針を同様に遵守することが必要である。上級管理者は、情報システムの重要度に応じた対応をすることが必要である。

上級管理者は、自営の場合と同等の統制が委託先において行われることを踏まえて、契約を締結することが必要である。また、上級管理者は、国外で活動する委託先を利用する場合は、必要に応じて、追加の統制を考慮することが必要である。国外に運用や開発を委託する場合は、その固有のリスクを踏まえて、固有のリスク管理策を検討することが必要である。

60 なお、重要業務の外部委託に関しては、英国では「金融機関は、重要業務を外部委託する予定がある際は、当局に届け出ること」、星国では「金融機関は、重要業務を外部委託する前、あるいは既存の重要な外部委託の調整事項を変更する前に、当局に届け出ること」とされている。

上級管理者は、実効的な外部委託管理を通じて、委託先のリスクに関する説明責任を果たす必要がある。
その際、上級管理者が、留意すべき事項は以下のとおり。
・委託先が金融機関の経営目標の達成に貢献しているか評価しているか。
・委託業務の範囲や重要度を踏まえて委託先を選定しているか。
・委託先に対するリスク評価結果を踏まえて委託先管理を見直しているか。

外部委託の重要度、要員の知識、情報システムの複雑さ等に応じて、委託先管理へ配分される経営資源は決定される。

（FISC にて意訳。下線は FISC にて付す。）

【資料６】共同センターの歴史

１．協同組織金融機関

信用金庫においては、昭和 46 年から全国７地区で共同事務センターを順次構築したことに端を発し、昭和 60 年に「株式会社しんきん情報システムセンター」[61]が設立され、昭和 62 年に各地区の共同事務センターを３次オンへ移行させた。その後、各地区の共同センターが東西の２センターに集約され、現在では、平成 25 年４月に設立された「一般社団法人しんきん共同センター」がその運営を担っている。現在、信用金庫全体の９割強（平成 27 年３月時点で 244 金庫）がしんきん共同センターを利用している。

信用組合においては、昭和 60 年に「信組情報サービス株式会社」[62]が「全国信組共同センター」[63]を設立し、平成３年に３次オンの稼働を開始した。現在までこの形態は維持されており、信用組合全体の９割強（平成 27 年３月時点で 146 信組）が利用している。

労働金庫においては、昭和 46 年に首都圏共同事務センターが組織化され、昭和 53 年に共同事務センターでオンラインの稼働が始まった。その後、平成元年に「労金総合事務センター」が設立され、平成２年に全国 13 労働金庫すべてが共同利用するオンラインシステム（ユニティ）が稼働を開始し、平成 26 年には、その後継となるオンラインシステム「アール・ワンシステム」が稼働を開始したところである。

農業協同組合（以下農協）においては、昭和 56 年に「株式会社農中情報処理センター」[64]が設立され、農林中央金庫が運営を担い[65]、平成 11 年から稼働を開始しているシステム（JASTEM）が、すべての農協において利用されている。

２．地域銀行

第二地方銀行（当時の相互銀行）の一部においては、昭和 50 年に九州地区に所在する８行向けの「事業組合 相銀九州共同オンラインセンター（SBK）」が設立されるとともに、昭和 52 年には共同オンラインサービスの稼働を開始しており、以降、勘定系システムの共同化や ATM・業務用端末の共同購入等を行ってきている。

地方銀行においては、システムコストの抑制、システム化領域の広がりによるシステム要員の増員、高度化する技術への対応といった理由から、平成 10 年頃から順次共同センターの利用が始まっている。現在では、ベンダー６社で 13 種類の共同センターが運営され、７割超の地域銀行が共同センターを利用している。主に営業基盤が競合しない地域銀行どうしで、同一の共同センターを利用し、システム経費やシステム要員の削減、先行者のノウハウの活用によるシステムの機能強化やサービスの充実等を図っている。

---

61 各信用金庫からの出資（合算 100%）で成り立っている。
62 出資割合は全信組連 90%、残り１割は各信組からの出資。
63 勘定系及び情報系システムを担う SKC センター（全国信組共同センター）と、主に決済業務に係る中央センターとしての全信組センターの２機能から構成される。
64 出資割合は農林中央金庫 90%、NTT データが 10%。昭和 59 年に農中情報システム株式会社（NIC）へ改称された。
65 開発・運用は、農中情報システム株式会社（NIC）へ委託されている。

【資料７】共同センター利用年表

業態	協同組織金融機関				地域銀行[66]	
	信用金庫	信用組合	労働金庫	農業協同組合	地方銀行	第二地方銀行
昭和40年～59年	S46.4 各地区の信金共同事務センター設立(順次設立)		S46.11 首都圏共同事務センター設立(以後各地域で設立)			S50 事業組合九州地区8相互銀行共同オンライン(以下SBK)設立
			S53.5 共同事務センター利用のオンライン稼働	S56.5 農中情報システム株式会社(NIC)設立		S52.10 共同オンラインシステム稼働開始
昭和60年～平成9年	S60.2 しんきん情報システムセンター設立 S62.11 各地区共同事務センターを3次オンへ移行	S60.5 信組情報サービス(株)設立、全国信組共同センター設立	H1.12 労金総合事務センター設立			
		H3.5 3次オン稼働	H2.5 新オンライン(ユニティ)稼働			H9.5 STAR-ACE稼働(長野銀行)※H25廃止
平成10年～平成19年				H11.10 JASTEMシステム稼働	H13.5 バンク・コンピュータ・サービス稼働(旧泉州銀行・鳥取銀行)※H27廃止 H14.3 じゅうだん会稼働(八十二銀行)	H12.1 STAR-21稼働(仙台銀行)※H25廃止 H13.1 第二地方銀行アウトソーシングセンター稼働(旧殖産銀行・福島銀行)
	H15.1 北海道信金アウトソーシングセンター稼働 H17.1 SBOC東京稼働 H18.4 しんきん共同システム運営機構設立 H18.9 信金西日本ソリューションセンター稼働			(H18.5 JASTEMシステムの展開完了)	H15.1 Flight21稼働(福岡銀行) H15.1 Banks' ware稼働(肥後銀行) H15.9 PROBANK稼働(東邦銀行) H16.1 地銀共同センター稼働(京都銀行) H19.1 Chance稼働(常陽銀行) H19.5 BankVision稼働(百五銀行)	H15.5 BankingWeb21稼働(八千代銀行) H17.5 Nextbase稼働(徳島銀行)
平成20年～	H23.9 東西2センターへのハード集約完了 H25.4 しんきん共同センターへ組織変更	H27.5 第6次システム稼働	H26.1 新オンラインシステム(アール・ワンシステム)稼働	H23.5 JASTEM次期システムへの移行完了(関東と九州の2センターへ集約)	H20.3 TSUBASAプロジェクト開始 H22.1 MEJAR稼働(横浜銀行) H22.10 STELLA CUBE稼働(東京都民銀行) H25.3 BeSTAcloud稼働(荘内銀行)	

(出所) FISC にて作成

66 カッコ内の金融機関は、最初にシステムを導入した機関。利用金融機関の業態が地方銀行と第二地方銀行を跨る場合は、最初にシステムを導入した金融機関に合わせて表示している。

【資料８】共同センターを利用している金融機関の預金量

平成 28 年３月時点で勘定系システムの運用を共同化している金融機関の数及びその預金量の合計を以下のとおり集計した。

業態	システム名	金融機関数	預金量（億円）*
信用金庫	信用金庫共同システム	244	1,002,298
	信金西日本ソリューションセンター	3	35,924
	SBOC 東京	3	33,061
	北海道アウトソーシングセンター	5	23,045
信用組合	SKC センター（全国信組共同センター）	145	176,201
	メイプルひろしま	4	6,012
労働金庫	アール・ワンシステム	14	178,509
農協	JASTEM システム	（47 信農連）	936,872
地方銀行及び第二地方銀行等	地銀共同センター	14	459,500
	Chance	7	300,017
	MEJAR	4	295,038
	BankVision	9	264,585
	じゅうだん会	7	208,524
	Flight21	4	187,813
	Nextbase	11	142,386
	TSUBASA	1	107,333
	Banks'ware	3	95,622
	STELLA CUBE	8	80,101
	PROBANK-R2	3	76,105
	BeSTAcloud	2	23,663
（以下参考・都市銀行）			
三菱東京 UFJ 銀行		-	1,245,909
三井住友銀行		-	942,600
みずほ銀行		-	935,283
りそな銀行		-	320,882

*1 平成 27 年３月時点の預金量とし、共同システムへの移行を予定している金融機関は集計の対象外とする。地方銀行、第二地方銀行、信用金庫、信用組合については、ニッキン金融手帳の預金量を元に、農協については、JA バンク HP「JA 貯金残高」を元にそれぞれ集計している。

（出所）FISC にて作成

【資料９】本検討会で取り上げた課題とその対策