平成 29 年 5 月 23 日
公益財団法人 金融情報システムセンター

第 51 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 5 月 23 日（火）　15:30～17:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．　15:30　開会
２．　15:30　FISC　渡辺理事長　挨拶
３．　15:40　【説明】
・自己紹介
・運営方法について
・資料の公開について
４．　16:05　【審議１】『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』改訂の着手について
・有識者検討会報告書について（FISC 企画部）
・改訂原案について（FISC 監査安全部）
５．　16:35　【審議２】『ＩＴ人材の確保・育成計画の策定のための手引書』作成の着手及び「ＩＴ人材検討部会」の設置について
・手引書原案について（FISC 調査部・監査安全部）
６．　16:55　事務連絡
７．　17:00　閉会

Ⅳ　資料

【資料１－１】　『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』改訂の着手について
【資料１－２】　改訂原案（安全対策基準前説）
【資料１－３】　補足資料（安全対策基準新構成案）
【資料２－１】　『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』作成の着手及び「ＩＴ人材検討部会」の設置について
【資料２－２】　手引書【概要】
【資料２－３】　手引書【原案】
【参考資料１】　委員名簿（専門委員）
【参考資料２】　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
【参考資料３】　金融機関における FinTech に関する有識者検討会報告書（案）

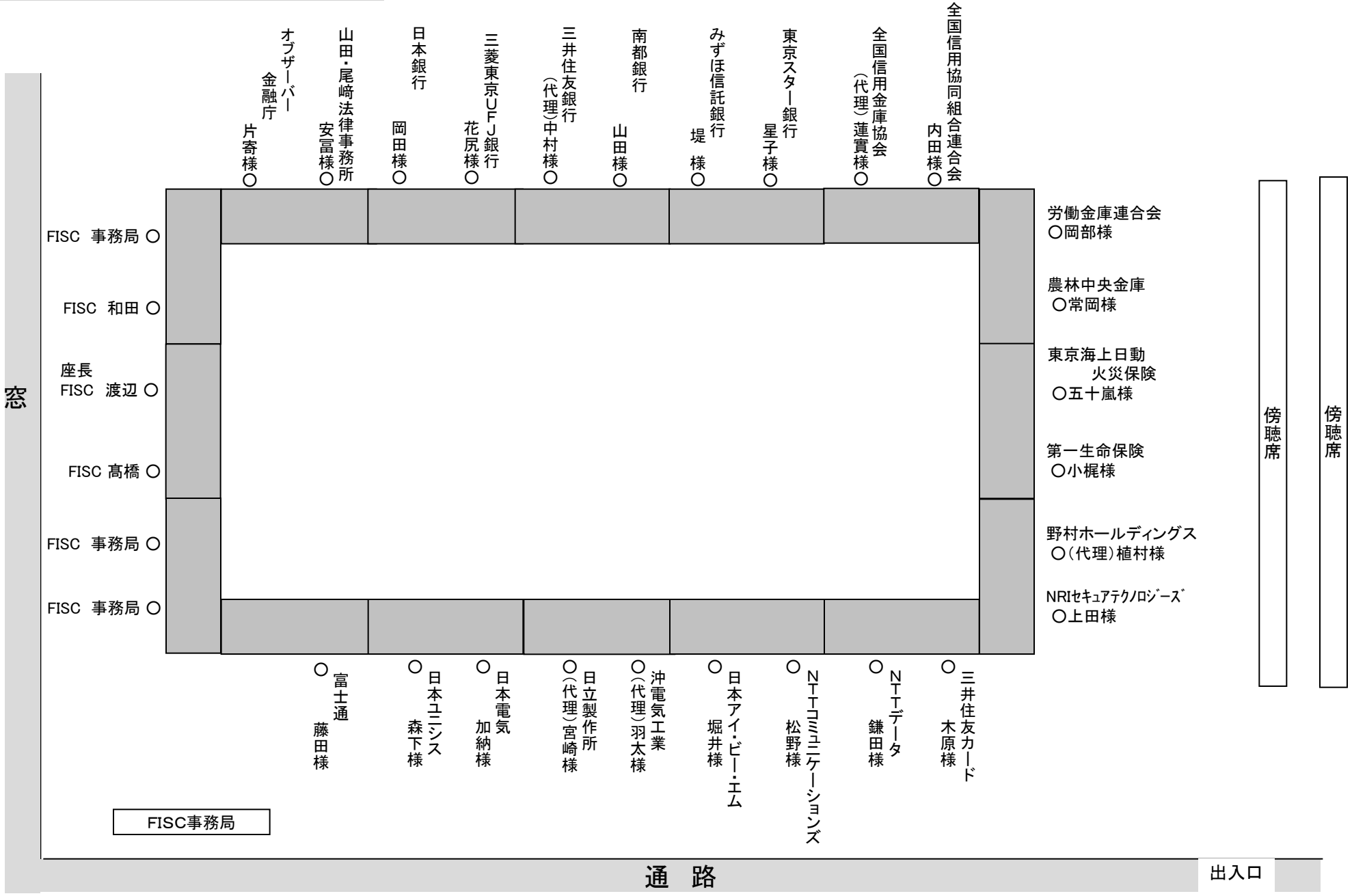
Ⅴ　今後の予定

○第 52 回　安全対策専門委員会
（予定）平成 29 年 6 月**日（**）15:00～17:00　FISC 会議室
○第１回　ＩＴ人材検討部会
（予定）平成 29 年 6 月 12 日（月）15:30～17:00　FISC 会議室

以上

第51回「安全対策専門委員会」座席表

平成29年5月23日



審議１

【資料１－１】
平成 29 年 5 月 23 日
公益財団法人 金融情報システムセンター

『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』改訂の着手について

Ⅰ 審議事項

『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『安全対策基準』という）について、安全対策専門委員会を月１回程度開催し、会員意見募集を経て３月末を目途に発刊できるよう、改訂作業を開始すること。

Ⅱ 改訂の背景

当センターにて開催した「金融機関における外部委託に関する有識者検討会」及び、現在開催している「金融機関における FinTech に関する有識者検討会」の報告内容・提言を受け、『安全対策基準』にリスクベースアプローチの考え方を取り入れるとともに、外部への統制を拡充させるなど、『安全対策基準』の構成・適用方法等を見直すこととした。

Ⅲ 改訂原案・補足資料

・【資料１－２】改訂原案（安全対策基準前説）
・【資料１－３】補足資料（安全対策基準新構成案）

以 上

【資料１－２】
平成 29 年 5 月 23 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）

Ⅰ．概説
１．安全対策基準の意義
２．安全対策の考え方
安全対策基準改訂の考え方
（１） ＩＴガバナンスとＩＴマネジメント
（２） リスクベースアプローチ
（３） 安全対策における基本原則
（４） 基本原則に従ったＩＴガバナンス
（５） 安全対策における経営責任のあり方
（６） 安全対策基準における「統制」のあり方

Ⅱ．フレームワーク
１．総論
（１） 本基準における定義
① 金融情報システム
② 特定システム・通常システム
③ 本基準の構成
④ 基準の分類（基礎基準に関する解説の一部は外部委託に合わせて検討の予定）
（２） 本基準の適用対象
（３） 本基準の適用方法
（４） コンティンジェンシープラン策定の必要性
２．統制（外部委託に合わせて検討の予定）
（１） 内部の統制
（２） 外部の統制
① 外部委託の管理におけるＩＴガバナンス
② 通則（基本形・派生形共通）
③ 基本形（二者間契約）における各論
④ 派生形（三者間契約）における通則
⑤ 派生形（三者間契約）における各論

Ⅲ．本基準の利用にあたって
１．基準・解説書の記述仕様
２．用語の解説
３．参照法令・参考文献等

【資料１－２】
平成 29 年 5 月 23 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、クラウド事業者や電子決済等代行業をはじめとする、新たな金融サービス（以下、「決済代行業等」とする）を提供する事業者（以下、「決済代行業者等」とする）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。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、金融機関等が信用を維持するためには、適切な安全対策の実施が不可欠であるが、一方で、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。また、問題発生時には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、当センターでは、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、経営資源の最適な配分に資するため、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の出現や、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。本改訂においては、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併せて示すこととした。

本基準は、公益財団法人 金融情報システムセンター内に設置された学識経験者、金融機関、保険会社、証券会社、クレジット会社およ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および、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、本基準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、各社が本基準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。

２．安全対策の考え方

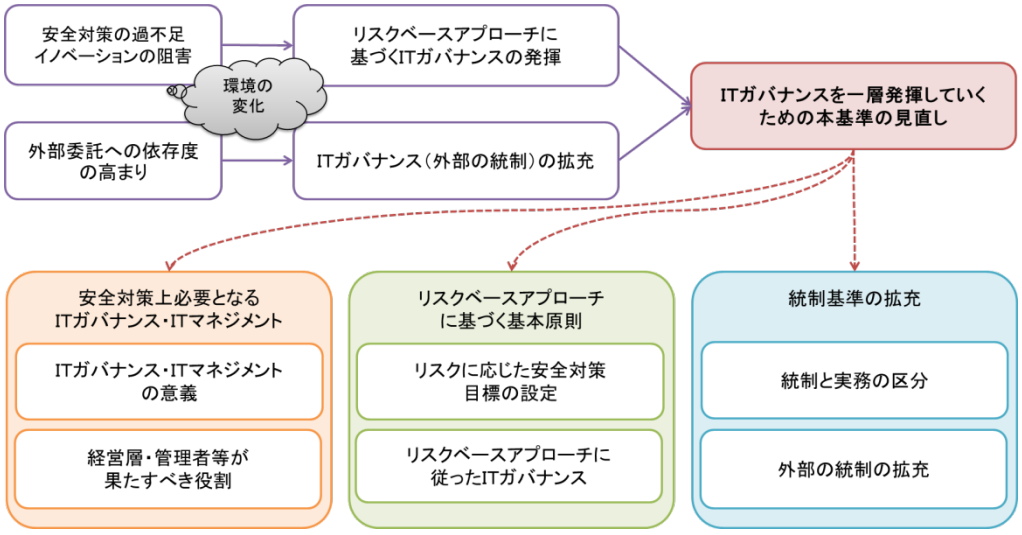
安全対策基準改訂の考え方

安全対策基準（以下、本基準）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、当初において本基準では、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、金融関連サービスなど、多様化してきている。

本基準は、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、多様化するそれ以外のシステムにおいては、その適用基準が不確実なままとなり、安全対策の程度に過不足を生じ、新規開発等への経営資源配分を抑制するなどの懸念が生じている。また、金融機関等において、システム開発・運用や、関連するサービスなど、外部委託への依存度が高まる中、統制に関する対策の重要性が増してきている。

本基準は、技術や経営環境の変化を受け、改訂を重ねており、「外部委託に関する有識者検討会」や「FinTech に関する有識者検討会」等において、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、本基準の見直しの方向性について論じられてきた。金融機関等に加え、金融機関等が提供するサービスを代行する企業が登場するなど、その適用範囲を含め、本基準における、安全対策の考え方を見直すべき時期が到来していると言える。（[図 1] を参照）

以上を踏まえ、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、統制基準の拡充について安全対策の考え方を示していく。



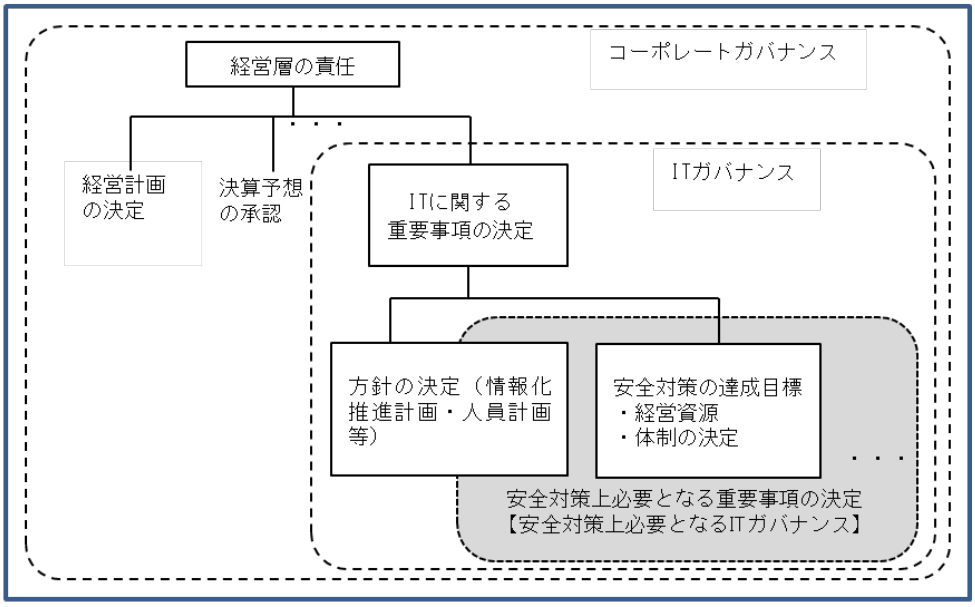
［図 1］安対基準改訂の考え方（概念図）

(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負うことが求められる。



［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ことが求められる（［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

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、リスク[1]特性に応じた目標設定を行う。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

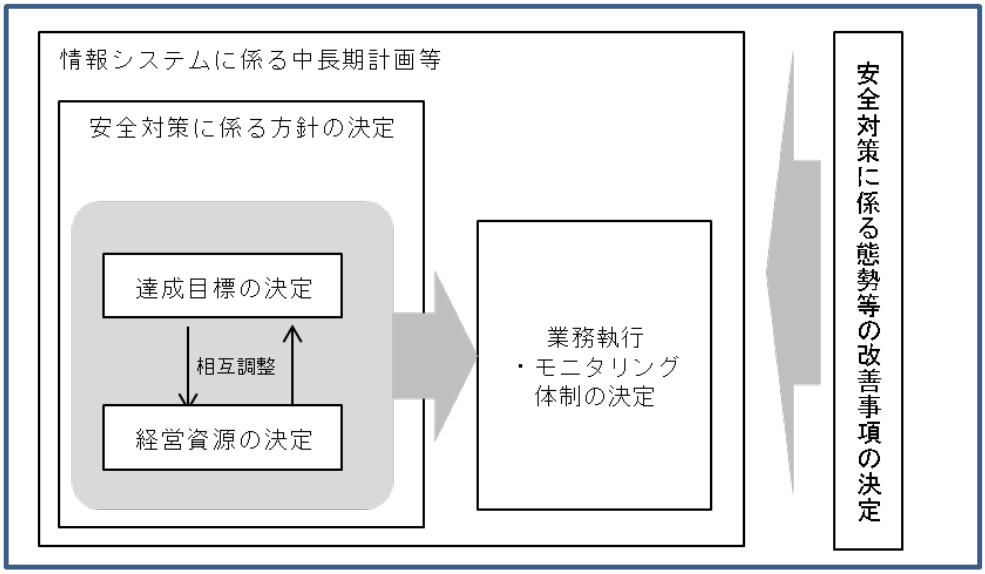
経営層は、安全対策の達成目標の決定と同時に、達成目標を実現するために必要となる経営資源の投下（費用・配分方針等）を決定する。経営層は、経営資源が有限であることを踏まえて、あらかじめ、保有する経営資源を踏まえた達成目標を検討するとともに、リスク特性に応じた資源配分を決定することが重要である。

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。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

[1] 本基準では、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ことや、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。

ンスのもとで、複数の関係者が必要な機能を発揮している。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。

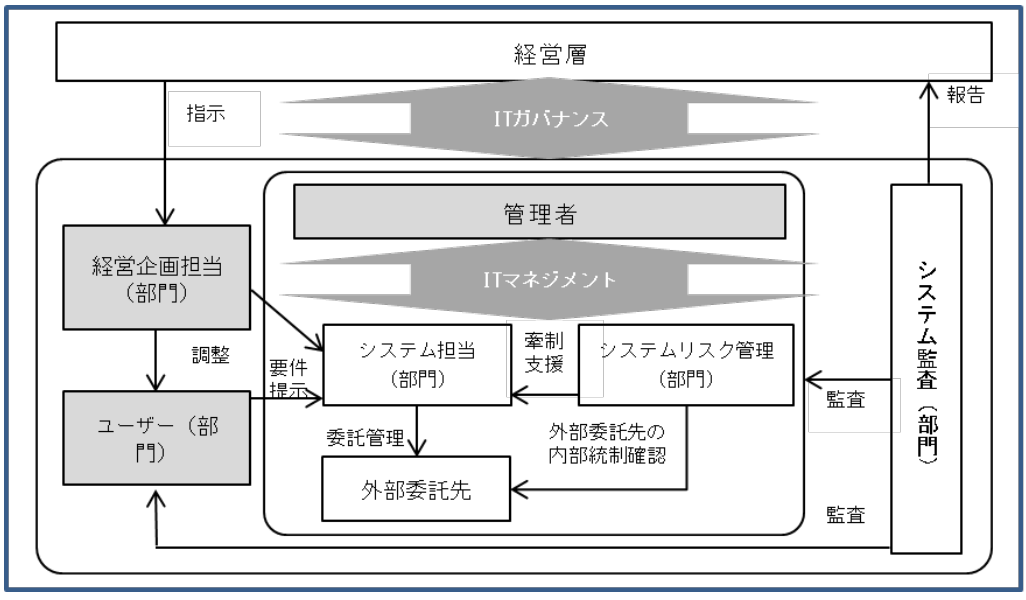
・内部規程・組織体制等の整備
・個々の情報システムに対する安全対策の決定
・内部規程・組織体制等の見直し
・安全対策上必要となる情報の経営層への報告

2）経営企画担当

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

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 本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、本基準を「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、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適正な水準以上の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、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、あるいはみずから徹底して追求してしまう。

② リスクベースアプローチの意義

本基準における、上記の課題を解決するためにも、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、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必要となる。さらに、リスクベースアプローチでは、リスク特性に応じた安全対策を実施することから、安全対策に対する費用は金融機関等の経営資源配分において、合理性を有することが求められる。これは、リスクゼロを必ずしも追求しない点を、金融機関等の経営層が理解し、金融機関等において、必要に応じてリスクを受容する判断が求められることを意味する。

このように、リスクベースアプローチの考え方を適用するためには、「金融機関等がみずから」その安全対策の目標を決定することが前提となる。つまり、リスク特性や安全対策は、監督当局や、その他ガイドラインによって指定されるものではなく、金融機関等が、統制を発揮させ、リスク特性を把握・分析し、経営資源配分の観点を考慮した上で、必要十分な対策を講じることが重要であり、金融機関等が企業価値の最大化を目指す上で、あるべき安全対策の考え方と言える。

(3) 安全対策における基本原則

リスクベースアプローチの考え方に基づき、適切に IT ガバナンスを発揮することで、これまで本基準が内包していた課題である安全対策の過不足を適正化することが期待される。

その一方、金融機関等は、社会性・公共性を有しており、リスクの発現による影響が、個別金融機関等による制御可能な領域を超えて外部に拡散（以下、「外部性」）する可能性や機微情報等の流出により、プライバシーなど個人の人権等を侵害する可能性を考慮すべきである。これらを踏まえ、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、本基準の考え方に取り入れている。

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。
○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。
○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、重大な外部性を有するシステムにおいては、個別金融機関等の内部への影響に加え、外部への影響を加味して安全対策が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く、こうした重大な外部性を考慮した社会的に合意されたガイドライン等[2]を踏まえた「高い安全対策」が必要となる。

また、金融機関等は、保健医療等の機微情報を保有するシステムについても十分な考慮が必要となる。機微情報は、流出した場合、プライバシー等、個人の人権等を侵害するといった広範な損失を発生させる可能性があり、その取扱いは社会的・公共的な性質を有することから、情報の機微性を考慮した社会的に合意されたガイドライン等を踏まえた「高い安全対策」が必要となる。安全対策は原則として、リスクベースアプローチを踏まえ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。

[2] 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。本基準も、金融機関や関連するベンダー各社等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。

・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からである。

・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」と「その他の個人情報」を分け、「機微情報」については、「高い安全対策」を適用することが妥当である。

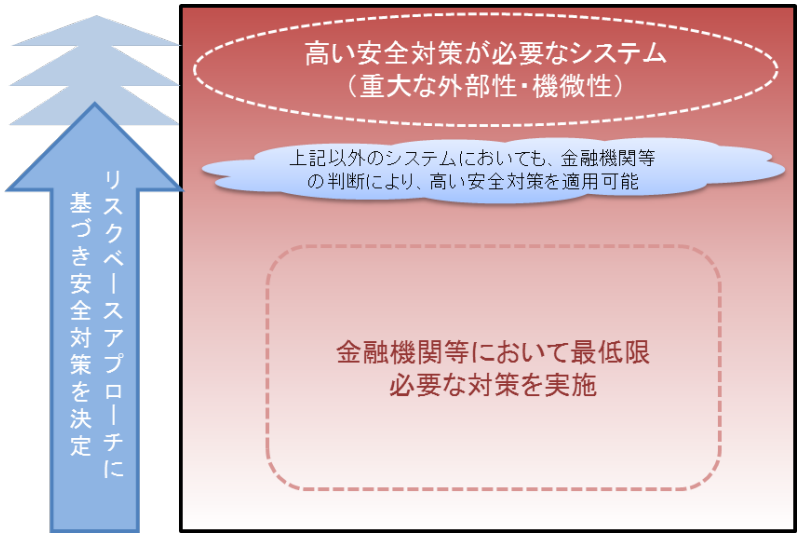
・「機微情報」は、本人等の許諾なく流出した場合、経済的損失に留まらず、プライバシー等、個人の人権等の侵害といった広範かつ甚大な損失を被る可能性がある。その取扱いは社会的・公共的な性質を有するものとも考えられることからも、「重大な外部性を有する」システムと同様に取り扱うことには合理性がある。

(4) 基本原則に従ったＩＴガバナンス

金融機関等に求められる安全対策については、安全対策の基本原則を念頭に、金融機関等がみずから検討することになるが、金融機関等の経営層は、適切に IT ガバナンスを発揮し、安全対策の目標を決定することが求められる。

金融機関等が具体的な安全対策を設定するに当たっては、その情報システムのリスク特性を分析し、「高い安全対策」を必要とするのか、あるいはリスクベースアプローチに基づき必要十分な範囲で、安全対策を決定し得るのかを、経営層の判断を踏まえ、決定することとなる。さらに、金融機関等においては、これら重大な外部性を有するシステムや機微情報を有するシステムと同等以上のリスク[3]を有するかどうかに着目し、「高い安全対策」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考えられる。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、原則として、経営層みずからが、経営資源配分の観点も含め、対象となるシステムの安全対策を決定することが重要となってくる。

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を考慮する必要がある。最低限の対策を示すことは、金融機関等が、リスクベースアプローチに基づき安全対策を選択する場合において、その不確実性を低減することに繋がることが期待される。（[図 5] を参照）



［図 5］基本原則に従った安全対策の考え方

高い安全対策が必要なシステムにおいて、そのシステム構成等に着目した場合、当該システムを構成する一部のサブシステム[4]において、システム障害等によるリスク事象を全体

[3] 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なども想定される。

[4] 金融機関等のシステム構成、管理単位等によって対象範囲が異なる。例えば、「決済系システム」や「勘定系システム」が表すシステムの範囲は、金融機関ごとに異なるため、リスク特性を共有しない一部のシステムが、システムに内包（サブシステム化）される場合や、独立した別個のシステムとして管理される場合もある。

へ波及しないよう防止できるなど、リスクが十分に低いとみなせる場合がある。こうした場合には、当該サブシステムにおいて、安全対策の目標を必要十分な内容で設定することが妥当であり、リスク特性に応じた安全対策を設定することに繋がる。

また、金融機関等の情報システムは多様化が進み、決済等代行業など、非金融機関が提供する新たなサービスが登場している。これらのサービスを利用・享受する顧客等の視点からは、その運用主体にかかわらず、サービスの提供者に求める安全対策の効果は不変である。そこで、本基準では、これら決済代行業者等が本基準を利用する場合についても解説を加えている。

(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、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。

○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（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。

○経営層が、諸法令を遵守するとともに、本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、本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、本基準において、統制面の対策を明示的に示すことが有効である。

① 本基準上における統制と実務の区分

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だけではなく、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、本基準では、「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、これら「統制」及び「実務」の状況を「監査」するための基準と区分している。また、「統制」以外の基準は、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「実務」に関する基準として、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
監　査		統制及び実務の状況を監査するための考え方・手法等
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］本基準における「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」で論じた内容と何ら異ならない。すなわち、金融機関等は、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。

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[5]。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、非金融機関等における決済代行業者等を含む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。

[5] 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、決済代行業者等の非金融機関等が、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) 本基準における定義

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[6]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

金融情報システムにおいて、「高い安全対策」が必要なシステムを、「特定システム」と定義する[7]。特定システムにおいては、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、機微情報の漏えい等により広範な損失を与える可能性があることから、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、個別金融機関等が、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においては、当該システムの一部分を特定システムから切り離し、「通常システム」として個別に安全対策を設定することが可能である。

③ 本基準の構成

本基準は、その目的や利用場面に応じて体系化され、「統制基準」「監査基準」「実務基準」「設備基準」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. 監査基準

統制および実務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。

---

[6] 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。

[7] 本基準における「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。

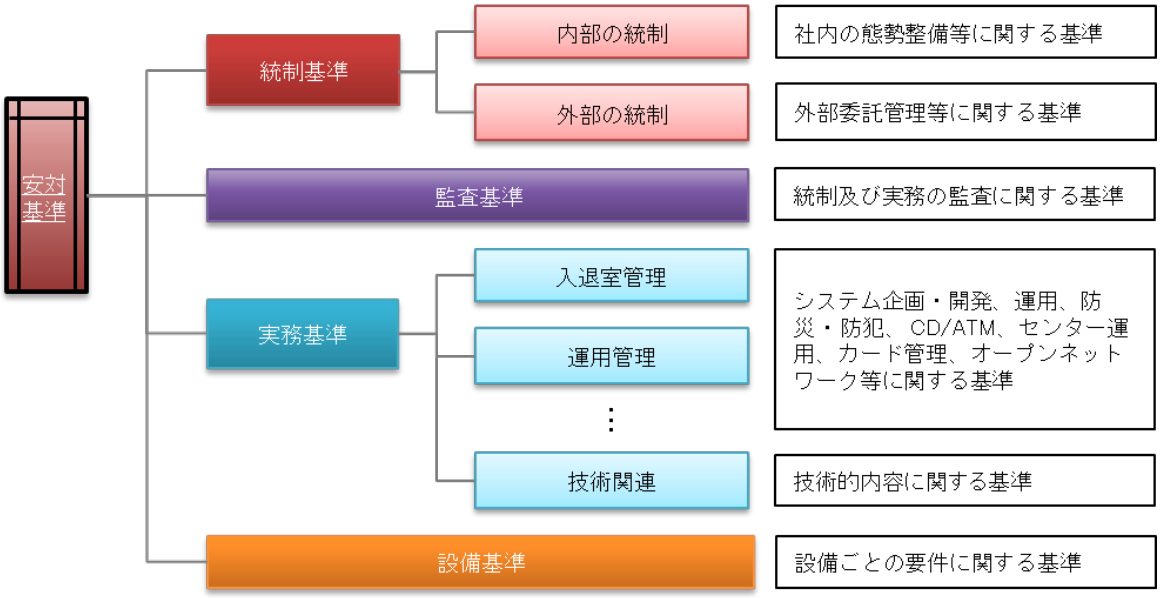
c. 実務基準

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・解説等から構成される。実務基準には、オペレーション等、管理者や作業者等が主体となる対策と、関連する技術的対策が含まれる。

d. 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および付帯施設および設備、本部・営業店等の建物および付帯施設および設備、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および付帯施設および設備に関する対策を記述する。



［図 7］本基準の構成

④ 基準の分類

本基準では、前述のとおり金融情報システムを「特定システム」と「通常システム」に分類しているが、それぞれのシステムにどの基準を適用すべきかといった観点から、本基準（設備基準除く）を「基礎基準」と「特定基準」に分類する。原則として、通常システムには「基礎基準」を適用し、特定システムは「基礎基準」および「特定基準」を適用する。（詳細は、(3)本基準の適用方法を参照のこと）

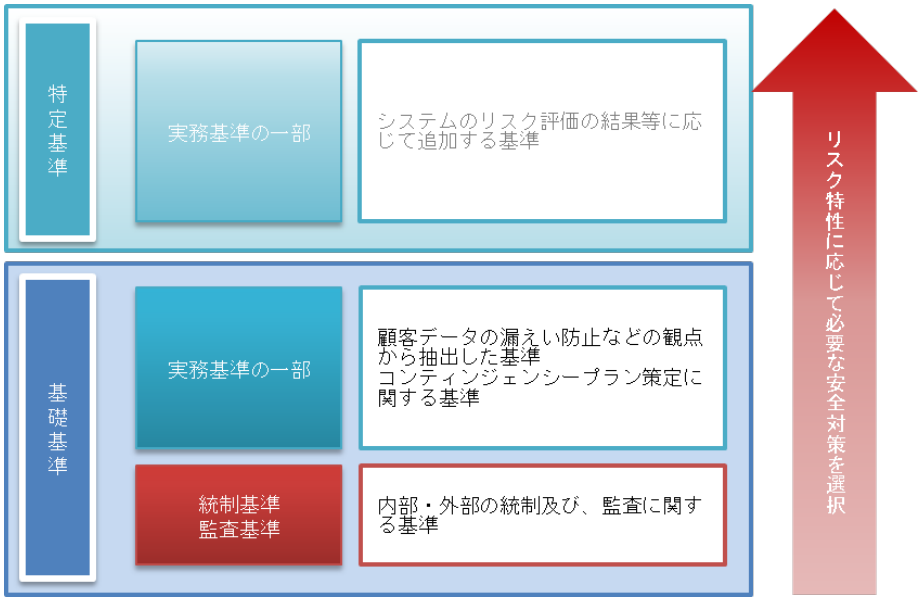
a. 基礎基準

金融情報システムにおいて、特定システム、通常システムによらず、実施すべき最低限の基準を「基礎基準」とする。「基礎基準」には、統制基準および監査基準と、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を含んでおり、金融機関等がリスクベースアプローチに基づき基準を選択するうえでの不確実性を低減させることを目的としている（[図 8] を参照）。

b. 特定基準

可用性や、完全性の確保など、各システムのリスク評価結果等に基づき、基礎基準に加えて実施する基準を「特定基準」とする。特定システムにおいては、原則として全ての特定基準を適用する。



［図 8］基礎基準と特定基準

（外部委託に合わせて検討の予定）

（補足１）外部の統制における「基礎基準」の記述様式について

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としての基準が示されており、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。これらの対策は、リスクベースアプローチの考えに基づき、リスクが高くないシステムにおいて選択可能としている。

（補足２）「基礎基準」の設定条件について

金融情報システムのリスク特性は、多岐にわたり、全てのシステムが満たすべき安全対策を一様に決定することは困難である。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に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、本基準では、顧客データの漏えい防止の観点を中心に基礎基準を選定した。上記を踏まえ、基礎基準において「重要なデータ」と記述されている場合は、顧客

情報を含むデータについては実施すべきものとなる一方、それ以外の情報[8]については、その重要度に応じて適宜取り入れることとしている。なお、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を踏まえ、顧客データの漏えい防止に関する基礎基準には、サイバー攻撃対策の観点も考慮し、対象となる基準を選定している。

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

一方、それ以外の観点で必要な安全対策については、システム毎に差異があり、個別金融機関等が、システム構成やリスク評価の結果等も考慮のうえ、適宜、特定基準から追加選択して適用することとなる。例えば、高い可用性が求められる通常システムにおいては、可用性の確保に関する基準を、特定基準から選択・追加することで、適切に安全対策を実施することが求められる。

上記を含め、「基礎基準の設定条件」を以下に示す。

・統制・監査に関する基準
・顧客データの漏えい防止において実施すべき基準[9]
・コンティンジェンシープラン策定に関して実施すべき基準[10]

決済代行業者等の非金融機関等が本基準を利用して安全対策を策定する場合、利用者視点において、金融機関等の実施する安全対策との整合性が保たれることが求められる。このため、これらの事業者によって策定される安全対策には、最低限実施すべき基準である「基礎基準」が含まれることが期待される。

なお、設備基準は、設備固有の要件により、実施する内容が特定されており、かつ各基準において、「すること」「望ましい」による使い分けをしているため、「基礎基準」及び「特定基準」の区分はしていない。

8 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が存在する。これらは、重要度に応じ、適宜、データ保護等に関する基礎基準を適用することが求められる。

9 個人情報等の重要な情報を保有するが、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な対策や、金融機関等の組織体制に応じて実施内容を決定可能な一部の基準については、基礎基準から除外している。

10 コンティンジェンシープラン（CP）策定、連絡態勢の整備等に関する対策を基礎基準とした。障害復旧マニュアル策定など一部の基準については、策定された CP によって適宜必要性を判断するものであり、これらは基礎基準としていない。

(2) 本基準の適用対象

本基準は金融情報システムに適用される。共同センター等[11]、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、本基準を適用する。

なお、金融機関相互のシステム・ネットワーク等は、金融機関等が部分的に管理責任を負う、「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基準を適用する[12]。

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、本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において、本基準を適宜取り入れることとする。また、非金融機関等における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、本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システムの分類

個別金融機関を通じた共通的なシステムの分類は、業態ごと[13]、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、どこに分類されるかは、個別金融機関等の実態に則して判断することが必要となる。本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。

---

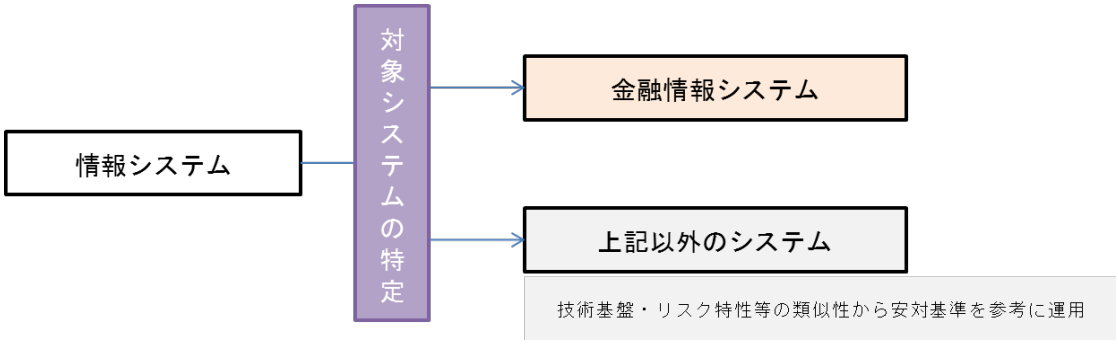
11 金融機関等がベンダーと契約するものや、協同組織等を通じてベンダーと契約するものなどが含まれる。

12 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。

13 一般に、預金取扱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金取扱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。

(3) 本基準の適用方法

金融機関等は、保有する情報システムから、本基準の適用対象となる金融情報システムを特定する。その後、対象システムに対し、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。金融機関等が、システムのリスク特性に応じ、経営資源配分を考慮した上で、これら全てに対し合理性をもった安全対策を決定していくためには、相応のリスク管理態勢等が整備されていることが必要と考えられる。



［図 9］本基準の適用方法（簡易法）

① リスクベースアプローチに基づく本基準の適用方法

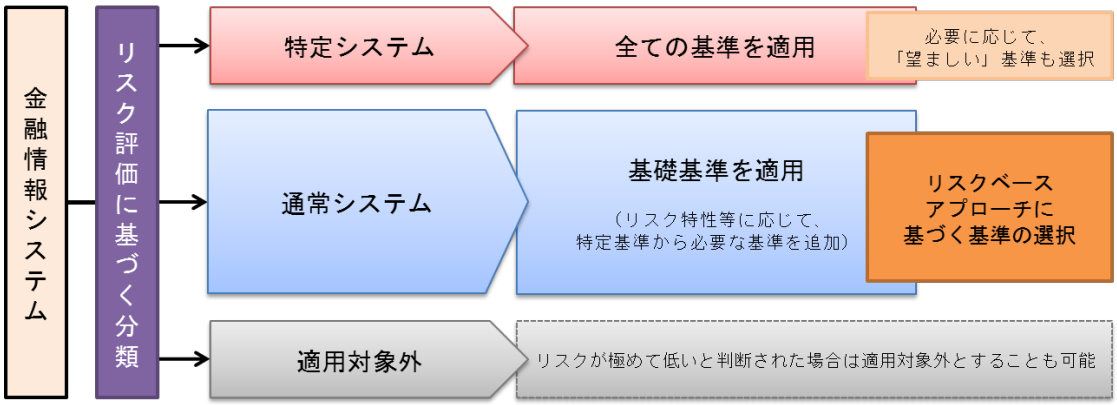
金融機関等は、金融情報システムに対し、各システムのリスク特性を分析し、必要となる安全対策を選択する。そのうえで、必要となる安全対策費用とその効果、及び新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮のうえ、最終的な経営資源配分を決定する。その結果、残存リスクが発生する場合は、必要に応じて、コンティンジェンシープランを策定する。この場合、原則として基礎基準を適用するとともに、適宜、特定基準から必要な基準を選択する。ただし、重大な外部性や、機微性を有する特定システムにおいては、高い安全対策が必要であり、原則として本基準を全て適用する。

② 簡易なリスクベースアプローチ

リスクベースアプローチを徹底し、基本原則に従った安全対策を決定するためには、経営資源等の制約から、実現が困難となる金融機関等が存在することも想定される。そこで、本基準では、リスクベースアプローチの考え方を効果的に活用するために、金融機関等が以下に示すような簡易法を採用することを認めている（[図 10]を参照）。簡易法では、リスク評価[14]に応じてシステムを３つのグループに区分し、それぞれのグループごとに本基準を適用する。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、本基準を適用することが望ましい。ただし、簡易的な手法を選択する場合、経営資源やリスク管理態勢等を考慮のうえ、経営層等におい

14 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、各金融機関の状況等に応じて検討されるものであり、本基準では、具体的手法については示していない。

て、その選択に合理性があると判断されることが必要となる。



［図 10］本基準の適用方法（簡易法）

「簡易法」を採用した場合の手順を以下に示す。

a. 保有する金融情報システムから、リスク評価の結果に応じて、「特定システム」「通常システム」及び「適用対象外」のシステムに分類する。
b. 特定システムにおいては、原則として、基礎基準と特定基準を全て適用する。ただし、特定基準のうち、「望ましい」と示された基準については、必要に応じて選択する。基礎基準において「～することも可能」とした対策は、原則として選択不可とする。
c. 通常システムは、基礎基準を適用する[15]。その上で、個々のシステムのリスク特性等に応じ、特定基準を追加することも可能とする。策定された安全対策は、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。
d. 金融情報システムにおいて、リスクが極めて低いと判断される場合は、本基準の適用対象外とすることも可能である。

(4) コンティンジェンシープラン策定の必要性

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、本基準においては、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。

15 システム構成等によって、明確に不要となる基準については、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。

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、本基準の「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、事前に十分に準備された計画が不可欠となる。

このための緊急時対応計画として、コンティンジェンシープランを事前に策定しておくことが必要であり、本基準でも、コンティンジェンシープラン構築の必要性を本基準の中で記述し、金融機関等が実施すべき重要な安全対策項目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。

２．統制（外部委託に合わせて検討の予定）

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[16]。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。本章では、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

本基準上の「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。

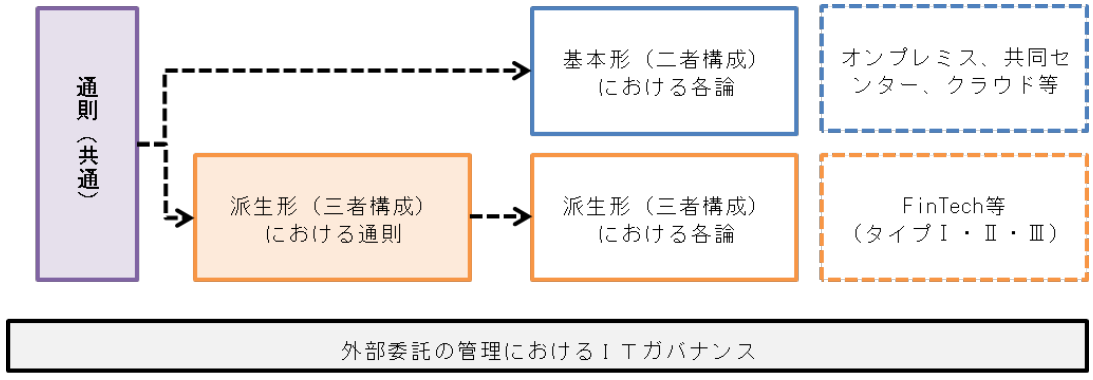
本基準上は、内部の統制を、以下のカテゴリーに分類している。

a. 方針・規程
b. 組織態勢
c. 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二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、三者間構成について、外部の「統制」における考え方について解説する。([図 11 を参照])



［図 11］外部の「統制」における考え方

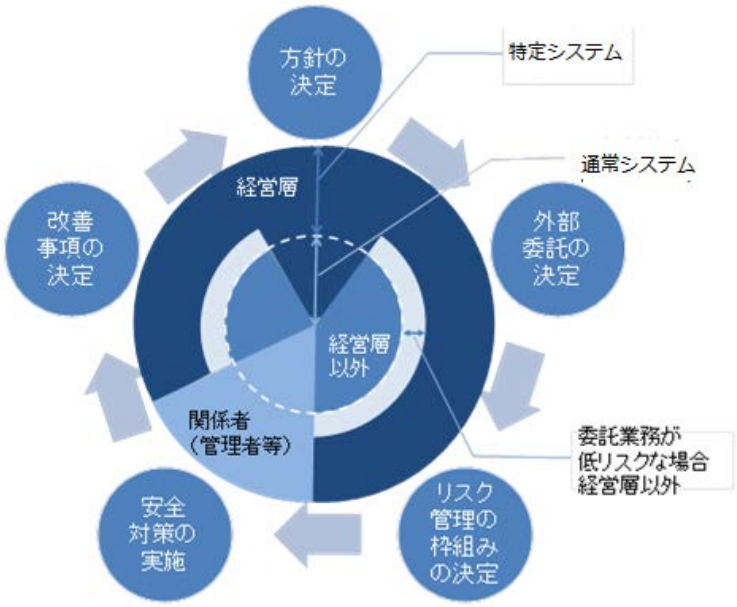
16 基礎基準のうち、「～することも可能である」として軽減策を示している場合、特定システムを除き、「可能である」とした内容を実施することができる（統制基準・実務基準共通）。

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、基本形である二者構成のみでなく、後述の派生形となる三者構成においても、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 12 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 12］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、委託先との委託契約の締結に当たっては、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、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、そうした検証結果の確認をもって、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、契約締結時には、監査権に関する条項を盛り込むことが必要である。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、システムに求められる可用性や完全性の程度に応じ、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、委託先等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（二者間契約）における各論

以下は、外部の統制における二者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、自社の設備において運用する環境において、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、有事の際の対応に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、有事に対する行動について、役割や態勢、手順等を整理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、利用形態によって、外部委託に準ずる管理を必要とするものがあり、リスク特性等に応じ、自営または外部委託と同等のリスク管理を行う必要がある。

クラウドサービスでは、安全対策を決定する役割がクラウド事業者に帰属することから、提供されるサービスの範囲を超えた場合に、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点で、基本形における、他の委託形態と性質が異なる。このような特性を踏まえ、金融機関等においては、クラウド事業者と締結する SLA 等において、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（三者構成）における通則

「派生形」については、「FinTech有識者検討会」及び、「オープンAPIに関する検討WG（仮称）」の検討結果を確認した上で、内容を確定させる。

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、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三者構成について、安全対策上考慮すべき点を整理する必要がある。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

本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三者関係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、従来の本基準において実現される二者関係における安全対策の効果と比較して、同程度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、三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、二者関係を念頭に置いた従来の本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、三者の各類型における役割や三者の安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分することを指す。

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、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本体全体のリスク特性と顕著に異なり、リスク事象を本体システム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（三者間契約）における各論

以下は、外部の統制における二者構成の代表的な形態におけるリスク管理策の考え方である。（[図 13] を参照）

a. タイプ I

タイプ I 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え方に、派生形の通則を付加した形態として整理できる。

タイプ I 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 ベンダーおよび決済代行業者等と合意の上、従来の本基準における外部委託の責務を、三者で再配分することが可能である。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。

b. タイプⅡ

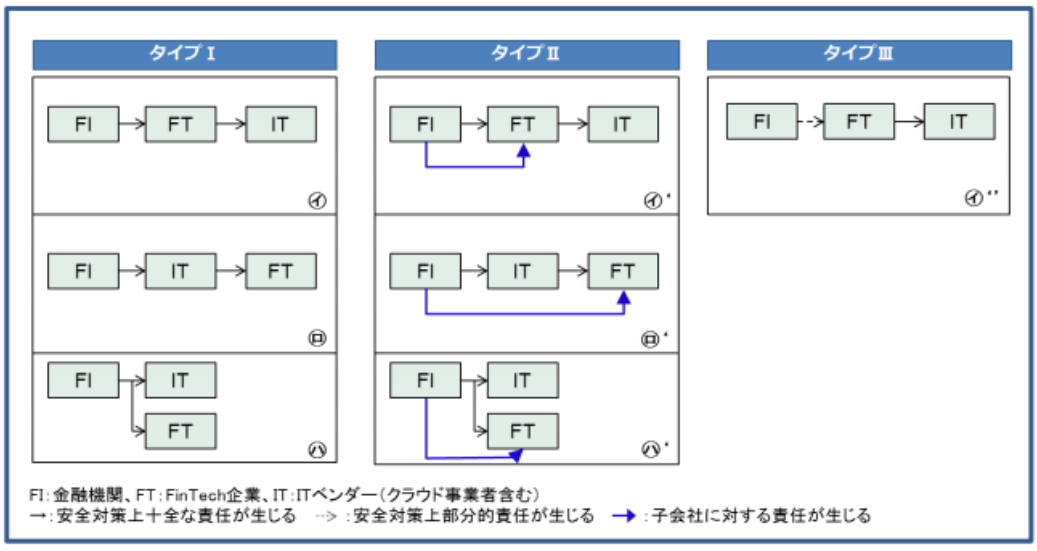
タイプⅡは、タイプⅠをもとに子会社に対する責任が付加されることで派生した形態である。

c. タイプⅢ

タイプⅢは、安全対策上の責任関係はタイプⅠの金融機関等が決済代行業者等に委託する類型と類似するが、その安全対策上の責任が部分的となることから派生する形態である。

タイプⅢ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、決済代行業者等は非金融機関と位置付けられるが、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、その一部を決済代行業者等が実施することとなる。

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、顧客情報の保全等について、金融機関等が統制を発揮する必要があり、安全対策を決定するうえで、本基準を準用[17]することが望ましい。



［図 13］決済代行業等において安全対策実施上の関係者のタイプ別類型

17 「準用」とは、本基準の中で、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、預金取扱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。

Ⅲ．本基準の利用にあたって

１．基準・解説書の記述仕様

(1) 適用区分

本基準では、基準の対象箇所を明確にするため、「適用区分」欄を設けている（[図 14]、[図 16]参照）。本欄では各基準及び解説等が、以下の箇所を対象とするか否かを◎ないし○で示している。

各記号の意味は以下のとおりである。

◎：基準及び解説等が当該箇所を対象としていることを示す。

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

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

※設備基準においては、「建物、チャネルに依存せず適用」の欄はない。

［図 14］適用区分の例

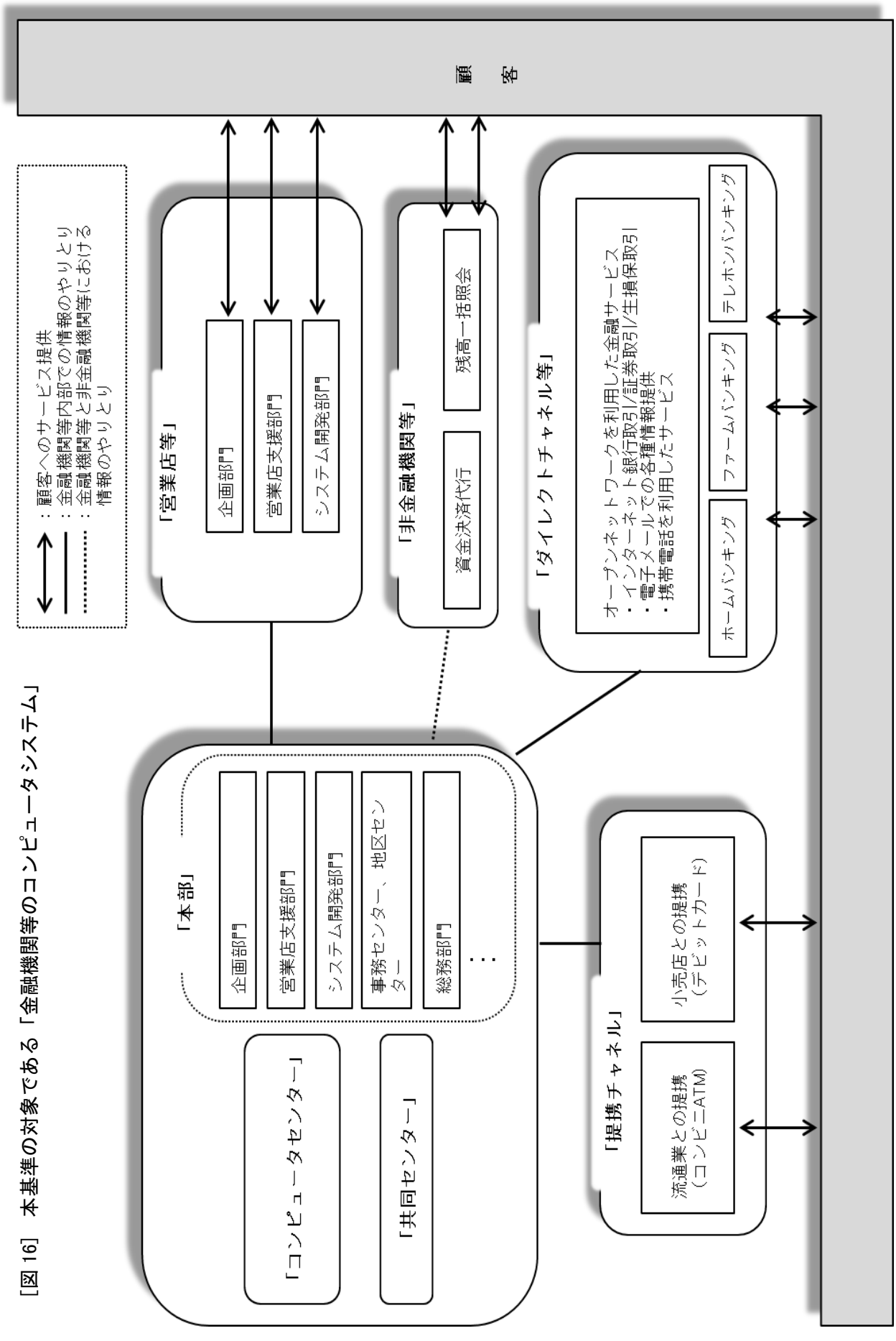
(2) 基礎基準

安全対策基準一覧上に、基礎基準であることを示すため、該当する基準には「 ◆ 」を表示した。なお、設備基準については、当欄は設けない。（[図 15］を参照）

大分類	中分類	小分類	基準項目	基礎
Ⅱ.実務基準				
	（Ⅰ）.入退館(室)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。	◆
			【実 2】入退館管理を行うこと。	◆

［図 15］安全対策基準一覧の例（実務基準）

［図 16］ 本基準の対象である「金融機関等のコンピュータシステム」



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

以下にモデル化された 5 つの機能要素について述べる。

・コンピュータセンター・共同センター

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

・本部・営業店等

・本部

コンピュータセンター以外の本部機能を指す。企画、経理、総務等の組織、営業店の支援等の内務事務を行う組織、事務センターや地区センター等から構成される。

・営業店等

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

・流通・小売店等との提携チャネル

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

・非金融機関等

決済代行業者等が提供するサービス（クラウドファウンディング、スマホ決裁等）を指す。利用形態としては、後述するダイレクトチャネル（インターネットバンキング等）に類似すると想定されるため、適用区分は「ダイレクトチャネル」としている。

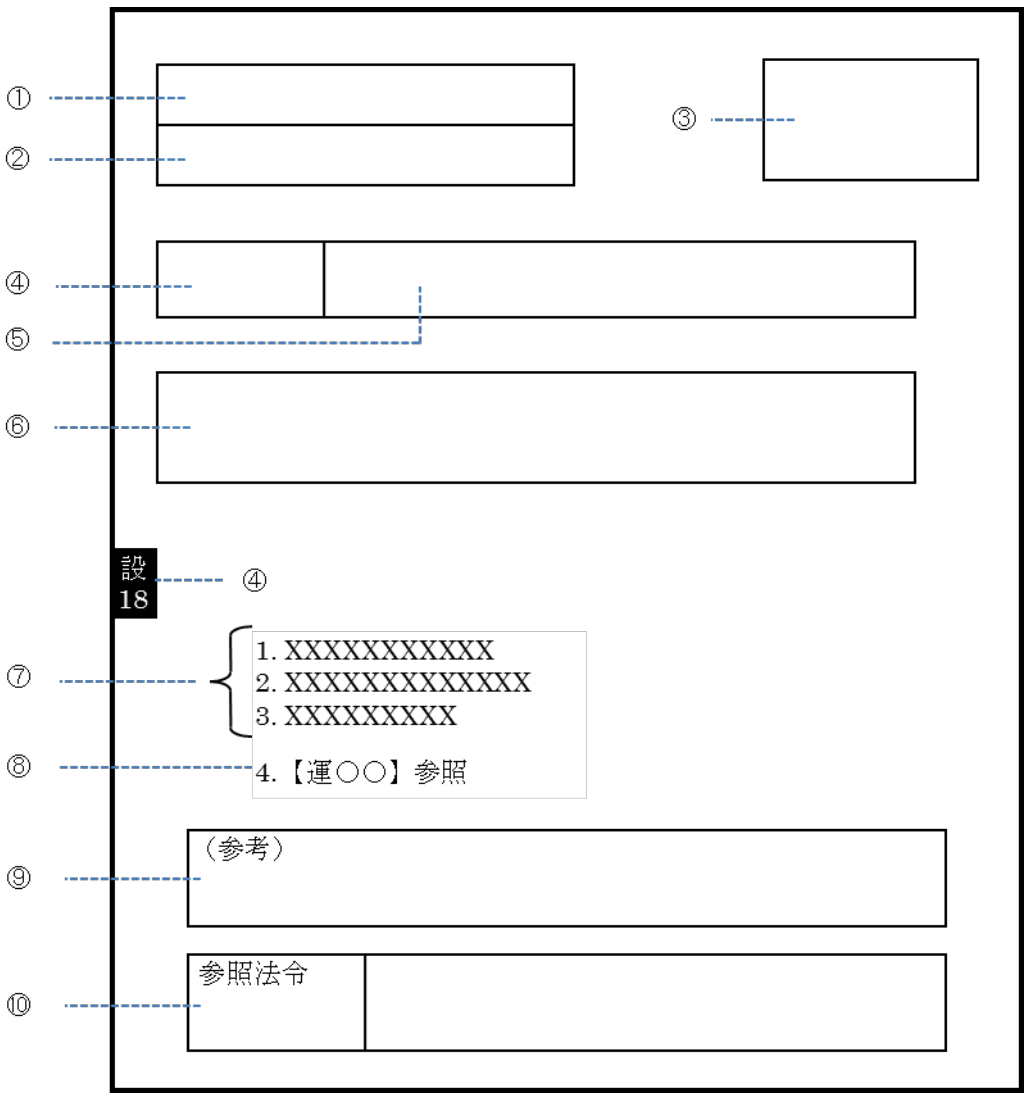
・ダイレクトチャネル等

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

(3) 各基準の記述様式

各基準は、図の様式で記述されている。各欄の意味は以下のとおり。（[図 17] を参照）

① ：基準大項目、当該基準項目がどの大項目に分類されるかを示す
② ：基準中項目、当該基準項目がどの中項目に分類されるかを示す
③ ：適用区分
④ ：設備、運用、技術の各基準内における当該基準項目の項番
⑤ ：基準小項目
⑥ ：適用にあたっての考え方
⑦ ：基準項目の目的、内容説明、具体例等の解説
⑧ ：当該基準項目と関連の深い基準内の他項目の項番
⑨ ：当該基準項目の解説に関連する参考事項
⑩ ：当該基準項目と関連の深い法令



[図 17] 各基準の記述様式（例）

（補足）「解説」の記述仕様

各基準の「⑦ 基準項目の目的、内容説明、具体例等の解説」欄には、例示・参考を除き、安全対策として実施する内容を具体的に記載しており、その内容は以下の表のように分類している。なお、本欄に例示・参考として示されている文章中に、「～すること」等の記載がある場合は、例示の一部として取り扱うため、これらは実施すべき基準または、解説としていない。（[図 18] を参照）

語尾	摘要
・「～すること」 ・「～が必要である」	当該基準または、解説の内容が、実施すべきものであることを示す
・「～することも可能である」	対となる基準または解説に対する、代替策または軽減策として、選択可能な対策であることを示す（特定システムは選択不可）
・「～が望ましい」	特定システム等において、必要に応じて選択する基準または、解説であることを示す
・「以下の例がある」 ・「～が考えられる」 ・「重要である」　等	例示・参考 （例示の内容に、「～する必要がある」等と記述されている場合も、例示の一部として取り扱う）

［図 18］本基準の「基準」「解説」の記載様式（凡例）

２．用語の解説

(1) 本基準における「重要な」の意味

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

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

経営層……	取締役会（理事会）等
暗証番号……	ATM 等で本人確認のために入力する、キャッシュカード取引における 4 桁の数字
空調設備……	コンピュータ室等の空気調和をする空気調和機、冷却塔及びその付属設備
顧客データ……	業務上収集、蓄積、利用される顧客に関するデータ データの範囲は、保有するすべての個人情報（氏名、生年月日、取引内容等）及び法人情報（代表者、決算内容、取引内容等）
個人情報[18]……	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できるものを含む。）をいう。
個人データ……	個人情報データベース[19]等を構成する個人情報をいう。
自動機器室……	営業店において CD・ATM 等を設置するコーナー、室
周辺装置……	ホストコンピュータを中心とするシステムでは磁気ディスク装置、半導体ディスク装置、磁気テープ装置、コンソールディスプレイ等の総称であり、サーバーを中心とするシステムではプリンター等の総称
渉外端末……	ハンディ端末、スマートデバイス、携帯型パソコン等、主に渉外担当者が携帯し、店舗外で利用されるコンピュータ機器
端末機器……	コンピュータに接続される、窓口装置、自動機器、ワークステーション、パソコン等の機器
端末系装置……	コンピュータシステムを利用するための入出力インタフェースとなる窓口装置、パソコン、渉外端末等の機器及びそれらを制御する装置の総称

18 個人情報」、「個人データ」の定義の詳細については、金融庁告示『金融分野における個人情報保護に関するガイドライン』を参照。

19 「個人情報データベース」とは、個人情報を含む情報の集合物であって、特定の個人情報をコンピュータを用いて検索できるように体系的に構成したもの。

通信系装置…… ホストコンピュータを中心とするシステムでは通信制御装置等、サーバーを中心とするシステムではルーター等

提携チャネル…… デビットカード及びコンビニ ATM の総称

電源設備…… コンピュータシステム等を作動させるための受電設備、UPS、自家発電設備等の設備及びその付属設備

電子署名…… 電子情報の真正性を確保するための技術であり、現在、公開鍵暗号方式に依拠したデジタル署名が一般的である。電子署名は、本人確認のほか、改ざんの防止、取引否認の防止にも有効である。なお、電子署名法上の電子署名はデジタル署名に限られない。

防犯カメラ…… 状況監視を行うためのテレビカメラ

防犯ビデオ…… 防犯カメラの映像、音声等の記録

ビデオ装置…… 防犯カメラの映像、音声等の記録・再生装置

不正アクセス…… 不正な手段により、ユーザー以外の者が行うアクセスまたはユーザーが行う権限外のアクセス

本体装置…… ホストコンピュータを中心とするシステムでは中央処理装置、主記憶装置、チャネル装置の総称であり、サーバーを中心とするシステムではサーバー自体

本部・営業店等…… コンピュータセンター以外の本部（具体的には、システム開発業務、営業店支援等の内部事務を行う組織、事務センター、地区センター等）及び顧客にサービスを提供する店舗（下記「無人店舗」や「インストアブランチ」を含む）の総称

無人店舗…… CD・ATM 等の自動機器のみで運用を行う店舗

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

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

オペレータ…… コンピュータセンターにおけるコンピュータ操作者

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

コンビニ ATM …… 金融機関がコンビニエンスストア内に設置した ATM

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

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

コンピュータ室…… コンピュータを設置する室

コンピュータセンター…… コンピュータシステムを運営するためのコンピュータを設置する建物または組織

サーバー…… LAN 等のネットワークで接続されたシステムにおいて、周辺装置、グループウェア、データベースなどの共用利用を主機能としたコンピュータ

システム管理者…… システムが正常に動作するよう保守、運用について統制・管理する者

スマートデバイス…… スマートフォン及び同様の機能を具備するタブレット型端末の総称

セキュリティ管理者…… 情報システムのセキュリティ全般を統制・管理する者

セキュリティポリシー…… 情報資産を適切に保護するための会社（または組織）としての安全対策に関する方針

ダイレクトチャネル…… オープンネットワークを利用したインターネットやモバイルによる金融サービスを営業店等を通さずに顧客に直接提供する方法の総称

データ…… コンピュータシステムの処理に適するように形式化された情報

データ管理者…… 保有する情報について統制・管理する者
データ利用状況の管理、アクセス権の承認等を行う

データ保管室…… データ、プログラムの記録媒体を保管する室

デビットカード…… 利用代金を顧客の口座から即時に引き落とし、利用店の口座に入金する即時決済サービスを提供可能なカードサービス

ドキュメント…… コンピュータシステムの開発、設計、作成、運用等に関する記録

ネットワーク管理者…… ネットワークの運用、セキュリティ、障害及びネットワーク関連機器を統制・管理する者

パスワード…… ネットワークやシステム等を利用する際に使用する、本人を認証するための、本人しか知り得ない文字列

パッケージ…… 他社から購入した業務ソフトウェア
パソコンを対象とした汎用ソフトウェアも含む

ファイル…… 記録媒体、または記憶装置に記録されているデータ及びプログラム

モバイル取引…… 携帯電話機を利用して金融機関等が行う銀行取引、証券取引、生損保取引等の金融サービスの総称

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

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

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

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

３． 参照法令・参考文献等

本基準における参照法令および参考文献等は以下のとおりである。

参考文献等は、発刊前までに最新版に修正する。

3.1 法令等

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

なお、条文は本基準発行時点のもの。

3.2 海外・国内規格等

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

(4)「ISO/IEC 15408 : 1999」（国際標準化機構／国際電気標準会議 ISO/IEC15408　システム評価基準等に関する国際標準）1999 年

(5)「ISO/TR 13569：1997 Banking and related financial services-Information security guidelines」（国際標準化機構 ISO/TR 13569　金融機関等の情報セキュリティ対策指針に関する技術報告書）1997 年

(6)「ISO/IEC TR 13335-1~5：Information technology-Guidelines for the management of IT Security」（国際標準化機構 ISO/IEC/TR 13335　IT セキュリティマネジメントのガイドライン）　1996～2004 年

(7)「ANSI X9.84-2003 Biometric Information Management and Security for the Financial Services Industry」（米国標準規格 X9.84 金融サービスのための生体情報管理とセキュリティ）ANSI（米国規格協会）2003 年

3.3 海外・国内ガイドライン等

(1) 「金融分野における個人情報保護に関するガイドライン」　金融庁 平成 16 年 12 月

(2) 「金融分野における個人情報保護に関するガイドラインの安全管理措置等に関する実務指針」金融庁 平成 17 年 1 月

(3) 「金融検査評定制度（預金等受入機関に係る検査評定制度）」　金融庁 平成 17 年 7 月

(4) 「偽造キャッシュカード問題に関するスタディグループ最終報告書～偽造・盗難キャッシュカード被害発生の予防策・被害拡大の抑止策を中心として～」　金融庁 平成 17 年 6 月

(5) 「金融機関における情報セキュリティの重要性と対応策」　日本銀行 平成 12 年 4 月

(6) 「金融機関業務のアウトソーシングに際してのリスク管理」　日本銀行 平成 13 年 4 月

(7) 「わが国金融機関におけるシステムリスクの管理状況と留意点」　日本銀行 平成 13 年 9 月

(8) 「金融機関の拠点被災を想定した業務継続計画のあり方」　日本銀行 平成 14 年 3 月

(9) 「金融機関における業務継続体制の整備について」　日本銀行 平成 15 年 7 月

(10)「金融機関の防犯基準」　警察庁 平成 11 年 10 月

(11)「コンビニエンスストア・スーパーマーケットの防犯基準」　警察庁 平成 15 年 12 月

(12)「単体で設置される現金自動預支払機（ATM）等の防犯基準」　警察庁 平成 15 年 7 月

(13)「現金自動支払機等の防犯基準」　警察庁 平成 3 年 6 月

(14)「情報システム安全対策指針」　警察庁 平成 11 年 11 月

(15) 「CD 等の技術的防犯対策について」　日本自動販売機工業会 金融システム部会 平成 2 年 6 月

(16)「ガラスの防犯性能に関する板硝子協会基準」　板硝子協会 平成 14 年 3 月

(17)「VDT 作業における労働衛生管理のためのガイドライン」　厚生労働省 平成 14 年 4 月

(18)「情報通信ネットワーク安全・信頼性のガイドライン」　平成 7 年 4 月
（編集）郵政省電気通信局電気通信事業部電気通信技術システム課
（発行）財団法人 日本データ通信協会

(19)「情報通信ネットワーク安全・信頼性基準」　郵政省 平成 6 年郵政省告示第 638 号
「情報通信ネットワーク安全・信頼性基準」の一部改正　総務省 平成 16 年総務省告示第 244 号

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

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

3.4 金融検査マニュアル

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

【資料１－３】

平成29年5月23日
公益財団法人　金融情報システムセンター

補足資料（安全対策基準新構成案）

↓①統制基準、②顧客データ等漏えい防止、③コンティンジェンシープラン　の観点で選定

カテゴリⅠ	概要	カテゴリⅡ	概要	カテゴリⅢ	概要	基礎基準	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」、および「監査」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	①	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
						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
						①	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
						①	統4	各種規定を整備すること。	運10
						①	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	①	統6	セキュリティ管理体制を整備すること。	運3
						①	統7	システム管理体制を整備すること。	運4
						①	統8	データ管理体制を整備すること。	運5
						①	統9	ネットワーク管理体制を整備すること。	運6
						①	統10	防災組織を整備すること。	運7
						①	統11	防犯組織を整備すること。	運8
						①	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	①	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	①	統14	セキュリティ教育を行うこと。	運80
						①	統15	要員に対するスキルアップ教育を行うこと。	運81
						①	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
						①	統17	障害時・災害時に備えた教育・訓練を行うこと。	運83
						①	統18	防災・防犯訓練を行うこと。	運84
						①	統19	要員の人事管理を適切に行うこと。	運85
						①	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	①	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
						①	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	①	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。	
						①	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。	
						①	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。	
						①	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。	
						①	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	①	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　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	統制及び実務 の状況を監査するための考え方・手法	(1)　システム監査	システム監査に関する基準	①	監1	システム監査体制を整備すること。	運91
Ⅲ　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		②	実1	資格付与および鍵の管理を行うこと。	運11
						②	実2	入退館管理を行うこと。	運12
						②	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		②	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
						②	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
						②	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		②	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		②③	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
						②	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		②	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		②	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
						②	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		②	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		②	実45	顧客データの保護策を講ずること。	運53
							実46	生体認証における生体認証情報の安全管理措置を講ずること。	運53-1
				(19)　資源管理			実47	能力及び使用状況の確認を行うこと。	運54

平成29年5月23日
公益財団法人　金融情報システムセンター

補足資料（安全対策基準新構成案）

↓①統制基準、②顧客データ等漏えい防止、③コンティンジェンシープラン　の観点で選定

カテゴリⅠ	概要	カテゴリⅡ	概要	カテゴリⅢ	概要	基礎基準	新基準番号案	基準小項目	旧基準番号
				(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
						②	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		②	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		②③	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		②	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		③	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		③	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		②	実67	廃棄計画、手順を策定すること。	運74
						②	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		②	実84	不正使用を防止すること。	運103
						②	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		②	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		②	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
						②	実118	蓄積データの漏洩防止策を講ずること。	技28
						②	実119	伝送データの漏洩防止策を講ずること。	技29
				(2) 破壊・改ざん防止			実120	ファイルに対する排他制御機能を設けること。	技30
							実121	ファイルに対するアクセス制御機能を設けること。	技31
							実122	不良データ検出機能を充実すること。	技32
				(3) 検知策			実123	伝送データの改ざん検知策を講ずること。	技33
							実124	ファイル突合機能を設けること。	技34

【資料１－３】

平成29年5月23日
公益財団法人　金融情報システムセンター

補足資料（安全対策基準新構成案）

↓①統制基準、②顧客データ等漏えい防止、③コンティンジェンシープラン　の観点で選定

カテゴリⅠ	概要	カテゴリⅡ	概要	カテゴリⅢ	概要	基礎基準	新基準番号案	基準小項目	旧基準番号
		17 不正使用防止		(1) 予防策(アクセス権限確認)		②	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
						②	実127	IDの不正使用防止機能を設けること。	技36
						②	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
						②	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		②	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
						②	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		②	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		②	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		②	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		②	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		③	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）								

68

（実務共通のみ）

39

審議２

【資料２－１】
平成 29 年 5 月 23 日
公益財団法人 金融情報システムセンター

『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』作成の着手及び「ＩＴ人材検討部会」の設置について

Ⅰ 審議事項

『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』（以下『手引書』という）を作成に着手することとし、そのため、安全対策専門委員会の下部組織として新たに「ＩＴ人材検討部会」を設置する。

Ⅱ 作成の背景

わが国の金融機関等におけるＩＴの利活用が大きく進展したことに伴い、それを支えるＩＴ人材の役割はこれまで以上に大きくなっている。また、最近では、金融情報システムを巡る環境変化に伴い、ＩＴ人材に求められる役割・スキルは、各金融機関の特性や実情に応じて多様化している。そのような状況を踏まえて、金融機関等が個別の経営判断により、ＩＴ人材の確保・育成を進めていく際に参考となる『手引書』の作成を行うこととした。

Ⅲ スケジュール（予定）

日 程	イベント	内 容
5 月 23 日	第 51 回安全対策専門委員会	・『手引書』作成の着手及び「IT 人材検討部会」の設置について審議
6 月 12 日	第１回ＩＴ人材検討部会	・『手引書』案の検討
8 月 3 日	第２回ＩＴ人材検討部会	・『手引書』案に対する意見反映結果提示 ・『手引書』案の検討
9 月下旬	第３回ＩＴ人材検討部会	・『手引書』案に対する意見反映結果提示 ・『手引書』案の取りまとめ
10 月**日	第**回安全対策専門委員会	・『手引書』案の確認 ・FISC 会員企業への意見募集実施について審議
11 月末まで	FISC 会員企業への意見募集	
12 月中旬	第４回ＩＴ人材検討部会	・FISC 会員企業意見に対する回答案の確認 ・『手引書』案に対する会員意見反映の確認
１月中旬	第**回安全対策専門委員会	・FISC 会員企業意見に対する回答案について審議 ・『手引書』案及び発刊について審議
3 月末目途	発刊	

※ 検討状況により、スケジュールの見直しおよび書面開催の場合あり。

審議２

【資料２－１】
平成 29 年 5 月 23 日
公益財団法人 金融情報システムセンター

Ⅳ 作成原案

【資料２－２】手引書【概要】及び【資料２－３】手引書【原案】　ご参照。

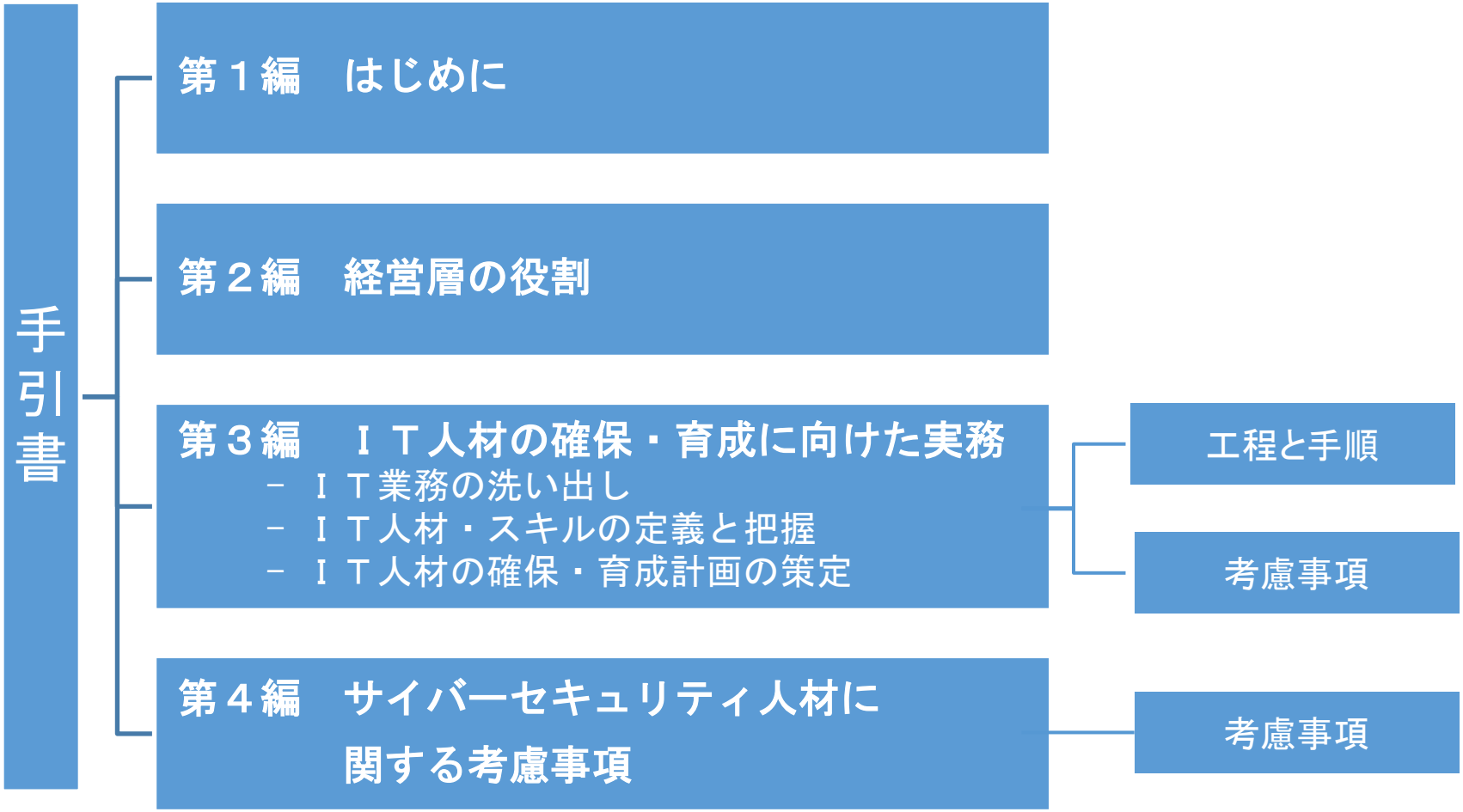
以　上

【資料２－２】
平成29年5月23日

『金融機関等における IT人材の確保・育成計画の策定のための手引書』 原案　概要

公益財団法人　金融情報システムセンター

全体構成



- **本手引書を作成する背景及び本手引書の位置付けを記載する。**

１．手引書作成の背景

- わが国の金融機関等におけるＩＴの利活用が大きく進展したことに伴い、それを支える人材の役割はこれまで以上に大きくなっている。以下に述べるような金融情報システムを巡る環境変化に伴い、システム戦略を実現するために必要な業務（以下「ＩＴ業務」という）は、システム部門だけに留まらず、システム部門以外の様々な部門に関わりが広がってきており、部門間、更には外部委託先等の社外との連携がより一層重要となっている。そして、システム戦略を実現するために必要な人材（以下「ＩＴ人材」という）に求められる役割・スキルは、各金融機関の特性や実情に応じて多様化してきている。
  （１）業務の外部委託化の進展
  （２）リスク管理の高度化・複雑化
  （３）サイバーセキュリティ対応
  （４）新しい技術やサービスへの対応

- このように、ＩＴ人材の確保・育成はシステム部門だけではなく、全社一体となって取り組んでいくことが求められる。そのため、金融機関等の経営層は、システム戦略に基づく、ＩＴ人材の確保・育成に向けた取組みに積極的に関わり、態勢を整える必要があると考えられる。

- 「金融機関における外部委託に関する有識者検討会（平成27年10月～平成28年6月）」においても、経営層は（１）人員数・スキルの種類とレベル・配置の把握、（２）全体の中長期計画に沿った人員の育成計画の策定について留意することが必要であると提唱されている。

- このような背景を踏まえ、金融機関等が個々の経営判断により、ＩＴ人材の確保・育成を進めていく際に参考となる手引書を作成する。

２．本手引書の位置付け、構成

- 本手引書では、システム部門以外の部門に所属しているＩＴ業務に携わる人材についても、『ＩＴ人材』と位置付けたうえで、より大きな枠組みでＩＴ人材の確保・育成に取り組んでいくことを前提としている。
- 本手引書は、金融機関等の特性や実情（規模やシステムの運用状況、外部委託状況等）に即して利用されることを想定している。すなわち、ＩＴ人材の確保・育成計画の策定について画一的な手順を示したものではなく、策定の考え方や留意すべき事項を記載したものであり、各金融機関等では記載内容のうち、該当する項目を選択して利用することを想定している。
- 本手引書の構成は、まず、第２編において経営層の役割について、第３編で経営層から指示を受けた実務部門等が実際に計画を策定していくための手順について記載している。
- サイバーセキュリティ業務は、インシデント対応組織の役割としてインシデント発生時の対応だけでなく平時からの運用も重要であり、様々な部門と連携しながら遂行される。サイバーセキュリティ人材の確保・育成については、その専門性、特殊性が高いことから『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（第３版追補３）』を参考に、第３編のＩＴ人材の策定手順における考慮事項として第４編として記載している。

- **計画策定における経営層の関与の重要性と役割を記載する。**

１．ＩＴ人材の確保・育成における経営層の関与の重要性

- 金融機関等の活動はシステムに大きく依存していることから、経営層はＩＴガバナンスを機能させることが必要である。

- ＩＴに関する重要事項の中には、システム戦略方針、システムリスク管理方針、ＩＴに投下する経営資源、ＩＴ業務の執行体制及びＩＴ業務のモニタリング体制等の決定がある。これらの決定事項を実現するためには、ＩＴ人材の確保・育成は非常に重要な事項の一つであり、経営層が積極的に関与していくべき事項である。

２．ＩＴ人材の確保・育成における経営層の関与の留意事項

- 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、必要となるＩＴ人材の人員数や質について、具体的に把握することが必要である。

- 全体の中長期計画に沿ったＩＴ人員の育成計画の策定

  経営層は、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ＩＴ人材の中長期的な確保・育成計画を策定し、周知徹底することが必要である。
  また、その計画では、対象範囲や対象期間等のスコープを明示することが必要である。

- ＩＴ人材の確保・育成計画策定時の態勢整備

  経営層は、ＩＴ人材の確保・育成計画策定に際して、必要に応じてプロジェクト組織を立ち上げる等、関連部門の相互協力が得られる態勢を整備することが必要である。

- ＩＴ人材の確保・育成計画策定後の態勢整備

  経営層は、ＩＴ人材の確保・育成を滞りなく遂行できる態勢を整備し、遂行状況を適宜確認し、必要に応じて計画を見直すことが必要である。

第３編　ＩＴ人材の確保・育成に向けた実務

- **経営層から指示を受けた実務部門等が計画を策定していくための工程・手順等を記載する。**
- **基本的な考え方や考慮事項を記載するにとどめ、イメージが掴めるよう参考例を掲載する。**
  （具体的な取組事例等については、機関誌レポート等にて還元予定）

本編に記載するＩＴ人材の確保・育成計画策定の工程

システム戦略・人材育成方針等

第１工程　現状および中長期的なＩＴ業務の洗い出し

- ✓ 自機関のＩＴ業務を網羅的に把握したうえで、それぞれのＩＴ業務を担うＩＴ人材の役割を明確にする。
- ✓ そのうえで、中長期的に必要となるＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。

第２工程　ＩＴ人材・スキルの定義と現状および中長期的に必要なＩＴ人材の把握

- ✓ 第１工程で洗い出したＩＴ業務に基づき、必要となるＩＴ人材像と人数、スキルを定義する。
- ✓ そのうえで、現状のＩＴ人材の人数・スキルを把握し、システム戦略の実現に必要なＩＴ人材の人数とスキル及び、それらの過不足を解消すべき時期を確認する。

第３工程　ＩＴ人材の確保・育成計画の策定

- ✓ 第２工程で分析した現状および中長期的に必要なＩＴ人材の過不足とその解消策の検討を行ったうえで、ＩＴ人材の確保・育成計画を取りまとめる。

全体の計画等への取り込み・反映

- ✓ 策定した計画は全体の計画等へ取り込まれ、反映される。
- ✓ ＩＴ人材の確保・育成計画は、PDCAサイクルを回し、必要に応じて見直しを図る。

第４編　サイバーセキュリティ人材に関する考慮事項

- **サイバーセキュリティ人材の確保・育成について考慮事項を記載する。**
  （具体的な取組事例等については、機関誌レポート等にて還元予定）

- 第１工程の業務の洗い出しおよび各業務における役割の明確化について、平成29年5月に発刊予定の『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（第３版追補３）』から、サイバーセキュリティ業務に必要な役割を示す。
  また、インシデント対応組織の役割から、業務特性や対応要員のスキルといった自機関の実態を踏まえて、自機関と外部委託を行う業務を明確にする等、サイバーセキュリティ人材の確保・育成に関して考慮事項を取りまとめる。

- サイバーセキュリティ業務において、人材像を定義する中で外部委託先を利用しながらも自機関で望まれる役割について考慮事項として取り上げ、また経営層とインシデント対応組織とのコミュニケーションが重要で社内の関係部門や社外関係機関との連携が不可欠なことから「橋渡し人材」の必要性について記載する。

- サイバーセキュリティ人材に求められるスキルとしてＩＴ人材と共通の部分が多いが、特にその特殊性から知識においては、一般のＩＴ知識のほかに、サイバーセキュリティ固有の知識および業務知識等が求められる。

- サイバーセキュリティ人材の確保・育成方法については、システム部門との連携、訓練・演習を通じたスキルアップや産官学連携した教育機関の利用等を記載する。

【資料２－３】
平成 29 年 5 月 23 日
公益財団法人 金融情報システムセンター

金融機関等における
IT人材の確保・育成計画の
策定のための手引書
【原案】

平成〇年〇月

公益財団法人　金融情報システムセンター

目次

第１編　はじめに

１．手引書作成の背景

わが国の金融機関等におけるＩＴの利活用が大きく進展したことに伴い、それを支える人材の役割はこれまで以上に大きくなっている。これまでは、金融機関等におけるＩＴを担う人材と言えば、システムの「開発」および「運用」に従事する人材がイメージされることが多かった。

ところが、最近では以下に述べるような金融情報システムを巡る環境変化に伴い、システム戦略を実現するために必要な業務（以下「ＩＴ業務」という）は、システム部門だけに留まらず、システム部門以外の様々な部門に関わりが広がってきており、部門間、更には外部委託先や関係機関等、社外との連携がより一層重要となっている。そして、ＩＴ人材[1]に求められる役割・スキルは、各金融機関の特性や実情に応じて多様化してきている。

(1) 業務の外部委託化の進展

システムの開発や運用については、共同センターを含む業務の外部委託化が進んでおり、それらのスキルを各金融機関がどのように維持していくかという点が課題として挙げられるようになっている。また、外部委託管理ができるＩＴ人材の重要性についてもクローズアップされてきている。

(2) リスク管理の高度化・複雑化

システム戦略は経営戦略、事業戦略と一体であり、ＩＴに関係する分野が広がるに伴い、そのリスクも高度化・複雑化してきており、それらのリスク管理に携わるＩＴ人材の重要性が増している。

(3) サイバーセキュリティ対応

金融機関等におけるサイバーセキュリティについては、DDoS 攻撃、標的型メールや不正送金などがあり、日々、高度化・巧妙化している。各金融機関はその対策を行う人材を必要としており、サイバーセキュリティ業務を担うための人材（以下「サイバーセキュリティ人材」という）が求められている。

(4) 新しい技術やサービスへの対応

近年、クラウド・FinTech・高度なデータ分析など、新しい技術やサービスが登場しており、それらをビジネスや業務にどのように活用していくのかという点を検討・提案するＩＴ人材が求められている。

---

[1] システム戦略を実現するために必要な人材を指す。本手引書における、ＩＴ人材の対象とする範囲は、システム部門も含めた全社とする（企画部門・リスク部門等の本部・本社組織とする。但し、営業店などシステムを利用する人材については含まない）。

このように、ＩＴ人材の確保・育成はシステム部門だけではなく、全社一体となって取り組んでいくことが求められる。そのため、金融機関等の経営層[2]は、システム戦略に基づく、ＩＴ人材の確保・育成に向けた取組みに積極的に関わり、態勢を整える必要があると考えられる。

また、当センターで開催した「金融機関における外部委託に関する有識者検討会（平成 27 年 10 月～平成 28 年 6 月）」においても、「安全対策上必要となるＩＴガバナンス」として、経営層は（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や（２）安全対策に係る態勢等の改善事項の決定について、役割と責任を果たすことが必要であるとしている。また、経営層は、システム戦略方針の１つとして、人員計画の決定に際して、（１）人員数・スキルの種類とレベル・配置の把握、（２）全体の中長期計画に沿った人員の育成計画の策定について留意することが必要であると提唱されている。

以上を踏まえて、金融機関等が個々の経営判断により、ＩＴ人材の確保・育成を進めていく際に参考となる手引書を検討するために、『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』を作成するための「ＩＴ人材検討部会（仮称）」を設置し、その検討結果に基づき、本手引書を作成した。

２．本手引書の位置付け、構成

これまで述べてきたようにＩＴ業務を推進していくためには、システム部門と関係する他部門、あるいは外部委託先等との連携が重要になってきている。従って、本手引書では、システム部門以外の部門に所属しているＩＴ業務に携わる人材についても、「ＩＴ人材」と位置付けたうえで、より大きな枠組みでＩＴ人材の確保・育成に取り組んでいくことを前提としている。

また、本手引書は、各金融機関等の特性や実情（規模やシステムの運用状況、外部委託状況等）に即して利用されることを想定している。すなわち、ＩＴ人材の確保・育成計画の策定について画一的な手順を示したものではなく、策定の考え方や留意すべき事項を記載したものであり、各金融機関等では記載内容のうち、該当する項目を選択して利用することを想定している。

本手引書の構成は、まず、第２編において経営層の役割について、第３編で経営層から指示を受けた実務部門が実際に計画を策定していくための手順について記載している。

第４編では、当センターで定めている、金融機関等におけるサイバーセキュリティ業務（「態勢整備」「平時の運用」「インシデント発生時の運用」）に基づき、第３編で記載した計画を策定する手順の中で各々の役割について必要となるサイバーセキュリティ人材の確保・育成に関して、考慮すべき事項を記載している。

---

[2] 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・執行役等までを指す。

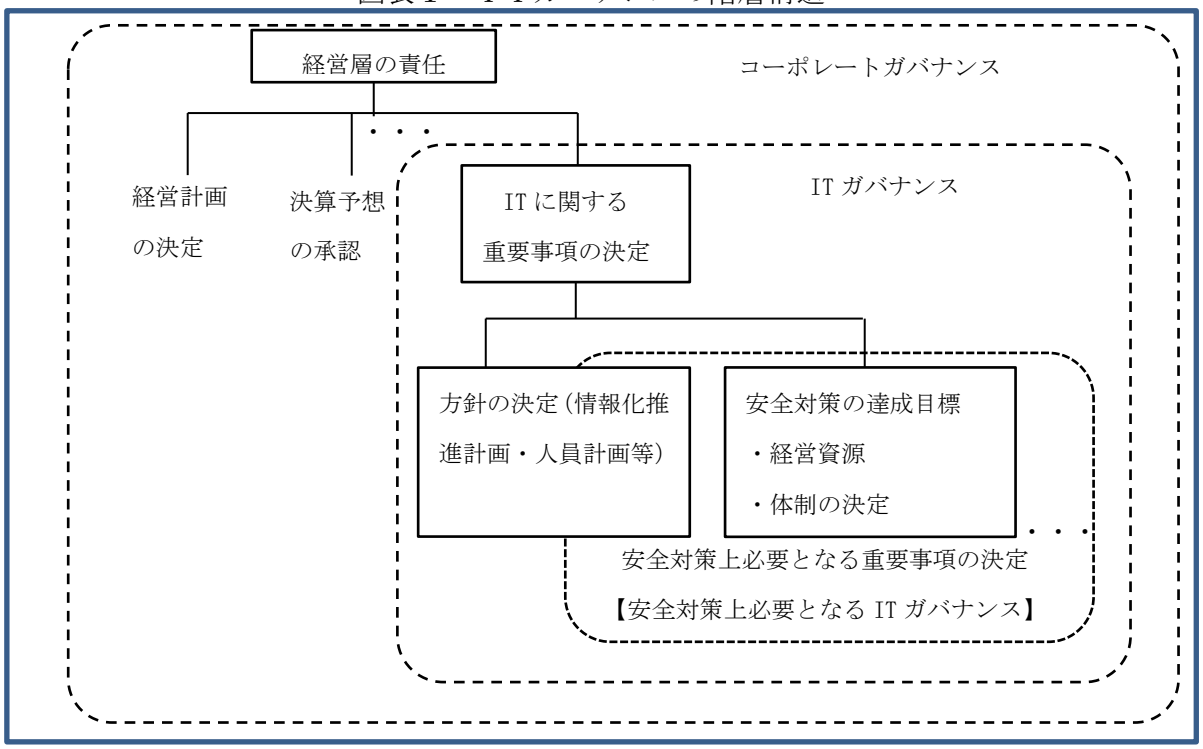
第２編　経営層の役割

１．ＩＴ人材の確保・育成における経営層の関与の重要性

金融機関の活動はシステムに大きく依存していることから、経営層はＩＴガバナンス[3]を機能させることが必要である。

ＩＴに関する重要事項の中には、システム戦略方針、システムリスク管理方針、ＩＴに投下する経営資源、ＩＴ業務の執行体制及びＩＴ業務のモニタリング体制等の決定がある。これらの決定事項を実現するためには、ＩＴ人材の確保・育成は重要な事項の一つであり、経営層が積極的に関与していくべき事項である。（図表１ を参照）

図表１　ＩＴガバナンスの階層構造



（『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』より引用）

[3]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、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指す

２．ＩＴ人材の確保・育成における経営層の関与の留意事項

経営層が、ＩＴ人材の確保・育成に関与する際、以下の点に留意する必要がある。

(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、必要となるＩＴ人材の人員数や質について、具体的に把握することが必要である。

ＩＴに係る経営資源の中で、ＩＴ人材は重要な要素の１つであり、経営層は、システムに対する投資額と同じく、ＩＴ人材の数及び質（保有するＩＴに関するスキルの種類とレベル・配置・年齢構成等）の実態を把握し、システム戦略を実現するために必要なＩＴ人材とのギャップを把握することが必要である。

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にも考慮が必要である。

また、システム戦略を全社一体で実現するためには、経営層と実務部門との連携が重要であるが、ＩＴ業務はサイバーセキュリティ業務をはじめとする専門性が高い分野が含まれているため、円滑なコミュニケーションが難しい面がある。このため、経営層の意図を実務部門に伝えることができ、逆に実務部門で把握した実情とそれへの対策案について経営層に伝え、指示を仰ぐことができるようなＩＴ人材（縦の橋渡し）が有用である点に留意する必要がある。また、部門間や外部委託先との調整を円滑に行うことができるＩＴ人材（横の橋渡し）が有用である点にも留意する必要がある。

(2) 全体の中長期計画に沿ったＩＴ人材の育成計画の策定

> 経営層は、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ＩＴ人材の中長期的な確保・育成計画を策定し、周知徹底することが必要である。また、その計画では、対象範囲や対象期間などのスコープを明示することが必要である。

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、ＩＴ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。その計画では、各金融機関の特性にあわせて、対象となる業務の範囲（システム関連会社の業務を対象とするか等）と対象期間（中長期計画に合わせて３年～５年／当該年度のみ 等）等を明確化して、周知徹底することが必要である。

策定されたＩＴ人材の確保・育成計画は、全体の計画等に織り込まれることとなる。

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

(3) ＩＴ人材の確保・育成計画策定時の態勢整備

経営層は、ＩＴ人材の確保・育成計画策定に際して、必要に応じてプロジェクト組織を立ち上げるなど、関連部門の相互協力が得られる態勢を整備することが必要である。

システム戦略を策定・実現していくためには、システム部門だけに留まらず、システム部門以外の様々な部門、或いは外部委託先等の社外関係者との連携が重要となっている。そのため、ＩＴ人材の確保・育成に関する計画策定は、全社一体で取り組むべき課題として、経営層の積極的な関与のもと、関連部門の相互協力を得られる態勢で進めることが必要である。

協力が得られる態勢として、プロジェクト組織を立ち上げる、あるいは計画策定の取りまとめを推進する部門を明確にする等が考えられる。

(4) ＩＴ人材の確保・育成計画策定後の態勢整備

経営層は、ＩＴ人材確保・育成計画を滞りなく遂行できる態勢を整備し、遂行状況を適宜確認し、必要に応じて計画を見直すことが必要である。

ＩＴ人材の確保・育成は中長期的に取り組んでいくものであり、その遂行状況や環境変化に応じて、ＰＤＣＡサイクル（ＰＬＡＮ⇒ＤＯ⇒ＣＨＥＣＫ⇒ＡＣＴＩＯＮ）を回しながら、継続的に行い、必要に応じて計画を見直すことが必要である。また、全社と部門、部門と部門の連携を取りながら、効果的にＰＤＣＡサイクルを回すことが必要である。

なお、遂行状況の評価を行う期間を設定する際には、以下の観点が考えられる（複数組み合わせることも考えられる）。

・定期的（１年ごと等）な期間設定を行う。
・ＩＴ中長期計画に沿った期間設定を行う。
・システムライフサイクルに沿った期間設定を行う。

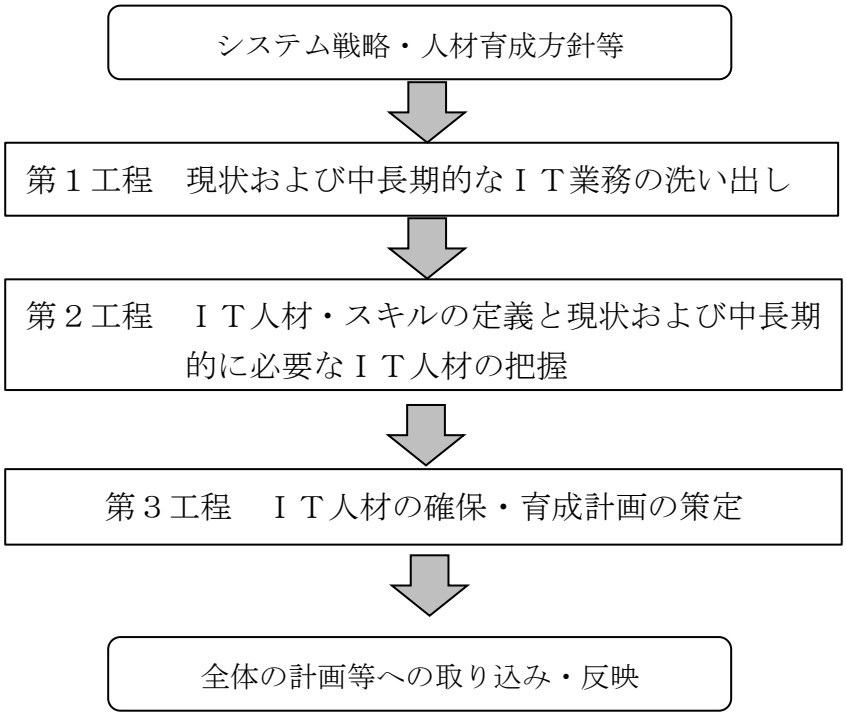
また、業務の追加・変更・廃止があった場合や、システムライフサイクルの変更があった場合等には、予め設定した期間に関わらず、計画の見直しが必要になることが考えられる。

第３編　ＩＴ人材の確保・育成に向けた実務

１．ＩＴ人材の確保・育成計画の策定の流れ

本編におけるＩＴ人材確保・育成計画の策定の流れを、以下の図表２に示す。

図表２　ＩＴ人材の確保・育成計画の策定の流れ



(1) 第１工程：現状および中長期的なＩＴ業務の洗い出し

自機関のＩＴ業務を網羅的に把握したうえで、それぞれのＩＴ業務を担うＩＴ人材の役割を明確にする。そのうえで、中長期的に必要となるＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。

(2) 第２工程：ＩＴ人材・スキルの定義と現状および中長期的に必要な人材の把握

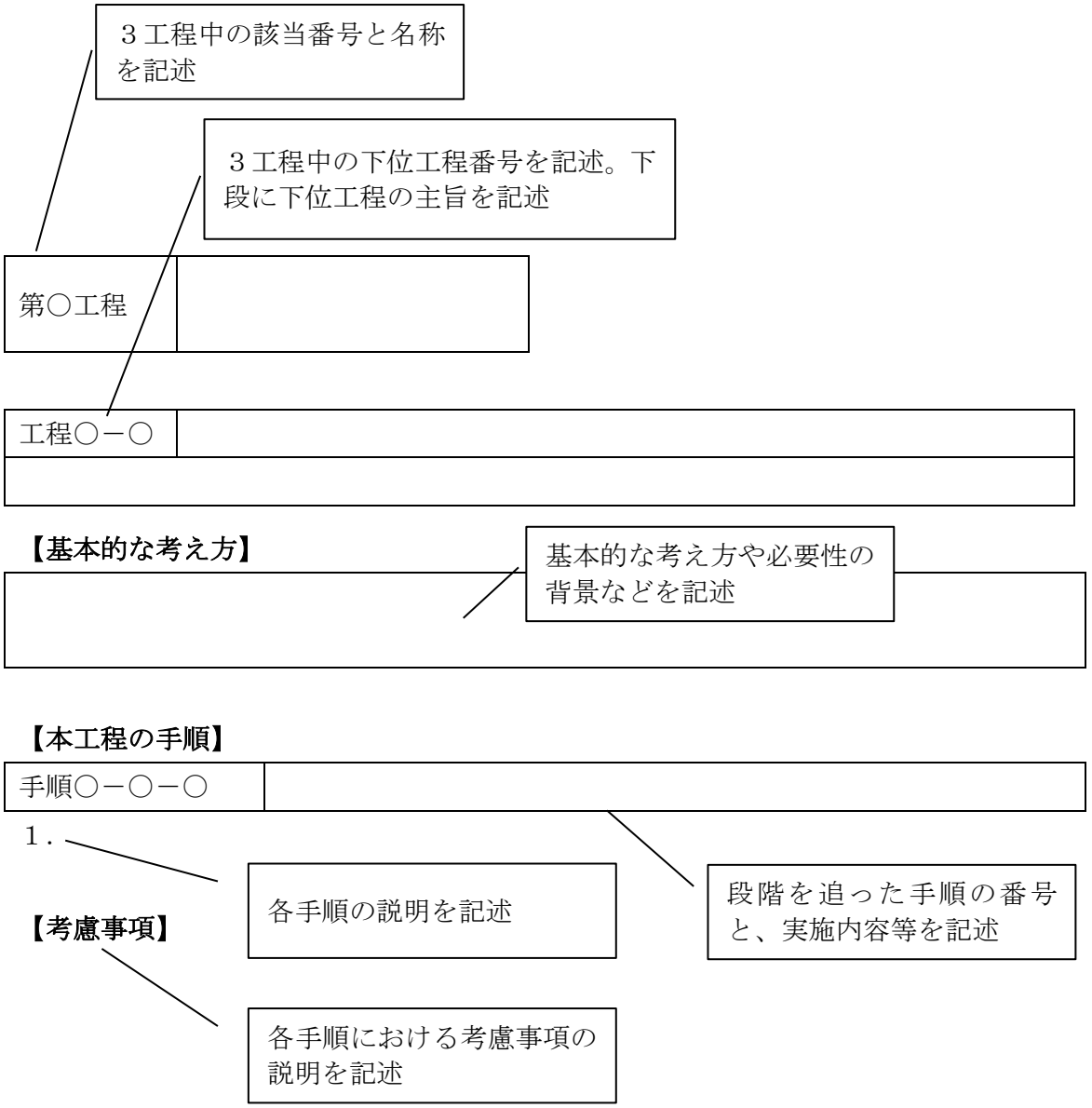
第１工程で洗い出したＩＴ業務に基づき、必要となるＩＴ人材像と人数、そのＩＴ人材に求められるスキルを定義する。そのうえで、現在および中長期的なＩＴ人材の過不足を確認する。

(3) 第３工程：ＩＴ人材の確保・育成計画の策定

第２工程で分析した現状および中長期的な必要ＩＴ人材の過不足とその解消策の検討を行ったうえで、ＩＴ人材の確保・育成計画を取りまとめる。

また、策定した計画は全体の計画等へ取り込まれ、反映される。なお、ＩＴ人材の確保・育成計画は、一度策定すれば完了するものではなく、ＰＤＣＡサイクルを回し、必要に応じて見直しを図っていく必要がある。

２．本手引書の記述様式


３工程中の該当番号と名称を記述
３工程中の下位工程番号を記述。下段に下位工程の主旨を記述
第○工程
工程○－○
【基本的な考え方】
基本的な考え方や必要性の背景などを記述
【本工程の手順】
手順○－○－○
１．
各手順の説明を記述
段階を追った手順の番号と、実施内容等を記述
【考慮事項】
各手順における考慮事項の説明を記述

３．計画策定の手順

本編では、経営層から指示を受けた実務部門やプロジェクト組織が実際に計画を策定していくための手順や考慮事項を記載する。

第１工程	現状および中長期的なＩＴ業務の洗い出し

工程１－１	現状のＩＴ業務の洗い出し

ＩＴ人材の確保・育成に関する計画を策定するにあたり、自機関においてＩＴ人材が担うＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。

【基本的な考え方】

ＩＴ人材の確保・育成に関する計画を策定するにあたっては、まず自機関のＩＴ業務を網羅的に把握したうえで、それぞれのＩＴ業務を担うＩＴ人材の役割を明確にする。

【本工程の手順】

手順１－１－１	現状のＩＴ業務の洗い出しを行う。

１．自機関のすべてのＩＴ業務を把握する。

２．１.にて把握した業務を必要な粒度まで細分化する。その過程において、外部へ委託している業務についても明確にする。

手順１－１－２	現状においてＩＴ業務を担当する組織を把握する。

１．洗い出しを行ったＩＴ業務について、担当する組織を把握する。

【考慮事項】

○手順１－１－１

以下では、ＩＴ業務の洗い出しを行う際の作業例を記載するが、業務の定義・配置については、新たに作成するのではなく、既存のものを利用することも考えられる。

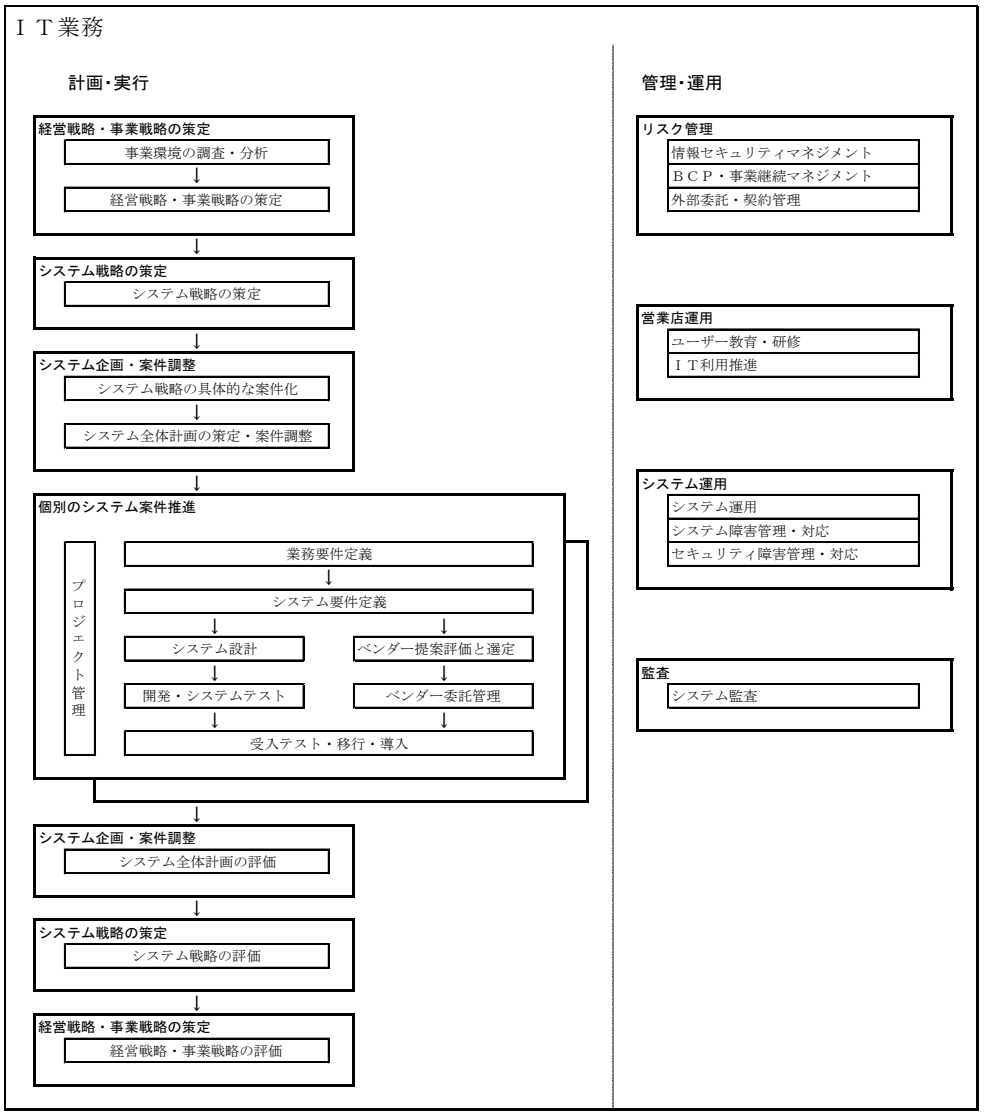
１．ＩＴ業務全体の洗い出し

システム戦略を実現するため、計画・実行サイクルを繰り返して推進する業務と、そのベースとなる恒常的な管理・運用業務に分けて整理する等、全体に漏れが無いよう考慮する（図表３　現状のＩＴ業務の洗い出しの例　を参照)。

従来のシステム開発及びシステム運用に関する業務だけでなく、関連部門におけるＩＴ業務も含めて洗い出しを行う（図表４　ＩＴ業務の洗い出し観点の例　を参照)。

なお、外部委託している業務については、システム関連子会社や共同センター、ベンダー等、委託先の形態により、その内容が大きく異なる点についても十分留意する。

図表３　　現状のＩＴ業務の洗い出しの例



（FISC にて作成）

図表４　ＩＴ業務の洗い出し観点の例

業務分類	ＩＴ業務の洗い出し観点
経営戦略・システム戦略の策定に関する業務	・自機関を取り巻くＩＴ関連の内外環境を把握・分析する。 ・マーケットや顧客のデータ分析により、顧客ニーズを把握・分析する。 ・経営層の意向等を踏まえ、経営戦略を策定するうえで、ＩＴの利活用や新たなＩＴの取込みを検討する。 ・経営戦略に基づき、投資配分の調整や各部門からの要望について優先度を判断・調整のうえ、システム戦略を策定する。 ・策定したシステム戦略に対し、全社の取り組み状況を把握し、経営層に対して進捗等を説明する。
システム企画案件調整に関する業務	・システム戦略を実現するため、具体的なシステム化案件を取りまとめ、全体スケジュールや工数の調整を行う。 ・ユーザー部門からのシステム化要望に対して、最新のＩＴ動向に基づき、導入するパッケージの提案、留意事項の助言などのサポートを行う。
個別のシステム案件推進に関する業務（ユーザー部門）	・新しい技術や他金融機関のシステム導入状況に対して、高くアンテナを張り情報収集する。 ・営業店や顧客目線でビジネスモデルを企画し、その業務要件をベンダーやシステム部門に伝える。 ・現場目線による端末オペレーションの改善や、法制度改正で必要となるシステム対応要件を、システム部門に伝える。 ・システム部門のメンバーおよびベンダー等と連携し、業務とシステム双方の視点を盛り込んだ、受入テストを行う。 ・システムの仕様や変更点などを理解したうえで、操作マニュアルや業務連絡文書を作成し、営業店の役職員に周知・説明する。
外部委託先管理	・情報システムの外部委託に係る方針を決定する。 ・外部委託先の各管理フェーズ（利用検討時・契約締結時・開発時・運用時・終了時・障害発生時等）における、安全対策のチェック事項など基準及び態勢を整備する。 ・外部委託におけるリスク管理に係る改善対策を実施する。
システムリスクを含めた統合リスク管理	・システムリスクを含めた、オペレーショナルリスクを把握し、他リスクとの統合管理を行う。 ・システムリスクを定性・定量的に分析し、リスクマネジメント計画を立てる。 ・リスク事象が発生した場合の影響を最小限にする施策をリスクの対応計画にまとめる。 ・情報セキュリティにかかる規程やマニュアル等を策定する。 ・インシデントの検知・対応をマニュアル化する。 ・災害発生時、中核となる事業の継続あるいは早期復旧を可能とするため、システム面を含めた事業継続計画（BCP）を策定するとともに、訓練等を通じて実効性を高める。
営業店運用	・オペレーション研修の実施等により、自機関におけるシステム利活用を推進し、役職員のＩＴリテラシー向上をはかる。 ・営業店への事務指導、事務ミス事例の分析・改善対応等を通じて、自機関の事務リスク削減を図る。
システム監査	・経営戦略及びシステム戦略に基づき、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・評価する。 ・経営層に対して、システム監査の結果を報告するとともに、改善のための提言を行う。

（金融機関等のヒアリング結果に基づき FISC にて作成）

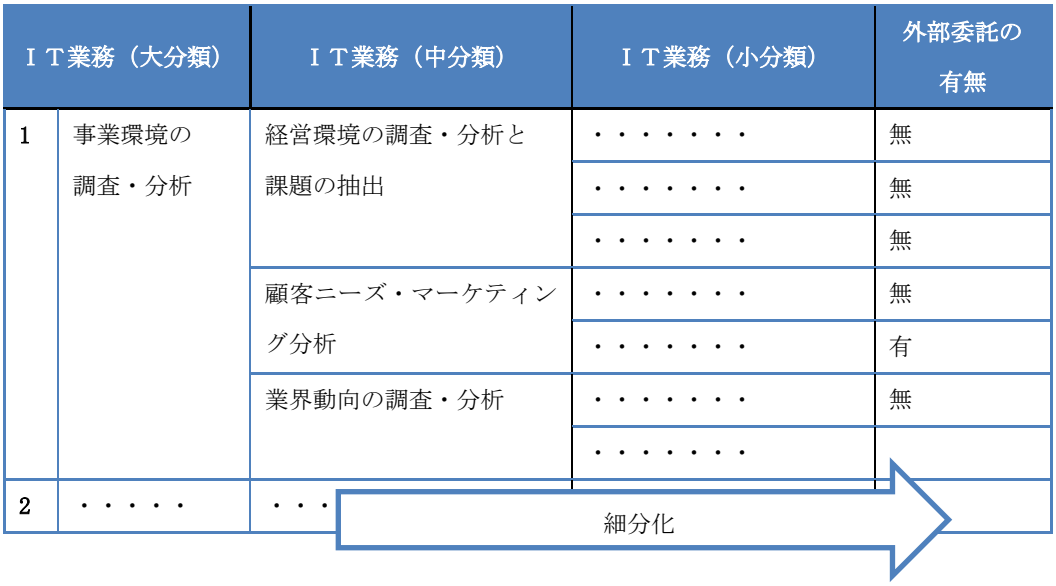
２．ＩＴ業務の細分化

・ＩＴ業務全体を整理したうえで、それぞれのＩＴ業務を段階的に細分化する。その際、ＩＴ人材が担っている役割がイメージできる程度まで細分化する。

・外部委託している業務についても対象外とせず、ＩＴ業務として定義する。

・サイバーセキュリティ業務など、専門性が高く、他の業務分野よりも詳細な分類段階（粒度）の定義が必要となる業務については、別表として定めることも考えられる。

図表５　業務の細分化の手順例



ＩＴ業務の整理については、以下の資料が参考になる。

（参考）

・『i コンピテンシ ディクショナリ（iCD)』独立行政法人情報処理推進機構（IPA）

○手順１－１－２

１．細分化したＩＴ業務について、現在担当している組織を把握する。

・部門横断で担当しているＩＴ業務については、主管部門と関連部門に区分けして把握する。

・一時的なプロジェクトチームなど、部門横断の人選によって組成され、部門による担当定義が困難なケースでは、当該組織を部門と見做して担当を定義する。

・外部委託している業務については、委託先との窓口となっている組織を把握する。

・ＩＴ人材の確保・育成を検討する対象範囲にシステム関連会社を含む場合、当該会社が担当するＩＴ業務についても把握する。

図表６　業務の担当組織を把握する手順例

（◎：主管部門　○：関連部門　□：外部委託窓口）

ＩＴ業務	ＩＴ業務（中分類）	ＩＴ業務（小分類）	外部委託の有無	経営企画部門	営業企画部門	リスク管理部門	事務企画部門	システム部門	…	…
事業環境の調査・分析	経営環境の調査・分析と課題の抽出	・・・・・	無	◎	○	○				
		・・・・・	無	◎		○	○			
		・・・・・	無	◎						
	顧客ニーズ・マーケティング分析	・・・・・	無	○	◎					
		・・・・・	有		□					
	業界動向の調査・分析	・・・・・	無	○				◎		
		・・・・・	無		○			◎		
		・・・・・	無							◎

第１工程	現状および中長期的なＩＴ業務の洗い出し

工程１－２	中長期的なＩＴ業務の明確化

中長期的に必要となるＩＴ業務の洗い出しを行い、各ＩＴ業務に求められる具体的な役割を明確にする。

【基本的な考え方】

現状のＩＴ業務に加え、中長期的なシステム戦略や経営層のビジョン等に基づき、必要となるＩＴ業務を明確にする。

【本工程の手順】

手順１－２－１	中長期的に必要なＩＴ業務を明確にする。

１．ＩＴ人材の確保・育成計画の対象となる期間において、新たに必要となる、あるいは不要となるＩＴ業務を明確にする。

２．業務を必要な粒度まで細分化する。

手順１－２－２	中長期的なＩＴ業務を担当する組織を明確にする。

１．ＩＴ業務を担当する組織を検討し、明確にする。

【考慮事項】

○手順１－２－１

１．中長期的に必要なＩＴ業務を検討、明確にするにあたっては、中長期的なシステム戦略や経営層のビジョンに基づいた検討を行う必要がある。また、その際、ＩＴ業務を外部委託するかどうかについても検討し、明確にする。

２．環境変化の考慮

ＩＴ業務が現状から変化するケースとしては、例えば以下のようなことが考えられる。

・制度対応や規制対応が必要な場合。
・新しいＩＴへの対応が必要な場合。
・ＩＴを利用した事業の改廃がある場合。

３．自機関のシステムライフサイクル状況の考慮

中長期的な観点から、自機関のシステムライフサイクルの状況を把握したうえで、必要なＩＴ業務を決定する必要がある。例えば、大規模なシステム更改が予定されているのであれば、それに応じた人員配置を行う必要が生じるほか、システム更改後の運用フェーズについても考慮することになる。これは外部委託先についても同様の考慮をすることになる。

４．技術力の維持に関する考慮

自機関における技術力の維持については、基幹システム等の保有形態に合わせて、以下のような方針が考えられる。

・自営システムであれば、システム部門が開発の中心となり、自機関で実際の開発を行える技術力を維持する。
・共同センター等の外部委託を利用する場合、外部委託先との円滑なコミュニケーションが可能となる程度の技術力を維持する。

○手順１－２－２

１．中長期的に必要となるＩＴ業務を担当する組織を検討するとともに、現状のＩＴ業務を担当する組織を見直すケースとしては、例えば以下のようなことが考えられる。

・複数部門で同一業務を実施していることが分かり、単独部門への統合を予定している場合。

・単独部門で実施していた業務を、関連部門を含めた部門横断の業務へと変更する場合。

２．部門横断で担当しているＩＴ業務については、主管部門と関連部門を区分けして、後工程でＩＴ人材配置を検討するうえで、求められるレベルをイメージしやすいよう考慮する。

３．一時的なプロジェクトチームなど、部門横断の人選によって組成され、部門による担当定義が困難なケースは、当該組織を部門とみなして、担当を定義する。

４．外部委託している業務については、委託先との窓口となって橋渡しの役割を果たすべき組織を定義する。

外部委託の検討においては、多岐にわたるＩＴ業務全体を俯瞰し、まず業務単位で外部へ委託するものがあれば、それを明確にしておく。外部へ委託するかどうかは組織の規模、ＩＴ予算、情報資産に対するリスク、セキュリティポリシーなどにより変化することが考えられ、自機関の状況に沿った選択が必要となる。

図表７　中長期的なＩＴ業務・担当組織の整理の手順例

＜経営層のビジョン（例）＞

・データ分析に関する業務が重要となるため、自機関でＩＴ人材を育成したい。

・ＩＴ動向は経営戦略・事業戦略内容にも大きく影響するため、経営戦略・事業戦略を策定する主管部門が、ＩＴ業界動向の調査・分析を主体的に行い、理解を深めるべき。

（◎：主管部門　○：関連部門　□：外部委託窓口）

ＩＴ業務	ＩＴ業務（中分類）	ＩＴ業務（小分類）	外部委託の有無	経営企画部門	営業企画部門	リスク管理部門	事務企画部門	システム部門	…	…
事業環境の調査・分析	経営環境の調査･分析と課題の抽出	・・・・・	無	◎	○	○				
		・・・・・	無	◎		○	○			
		・・・・・	無	◎						
	顧客ニーズ･マーケティング分析	・・・・・	無	○	◎					
		・・・・・	外部委託から内製化を図る。		□→◎					
	業界動向の調査・分析	・・・・・	無	○→◎				◎→○		
		・・・・・	無		○→◎			◎→○		
		・・・・・	無							◎
・・・・	・・・・・		無							

第２工程	ＩＴ人材・スキルの定義と現状及び 中長期的に必要となるＩＴ人材の把握

工程２－１　ＩＴ人材・スキルの定義

自機関のＩＴ業務において必要となるＩＴ人材（人材像）を定義する。
求められるＩＴ人材のスキルを定義するとともに、その評価方法を検討する。

【基本的な考え方】

自機関にて対応すべきＩＴ業務を明確にした後、その業務を実際に遂行するＩＴ人材とその人数、スキルを定義する。

ＩＴ人材像やスキルについては、現場へのヒアリングなどを通して新たに作成することも考えられるが、既存の資料（自機関で既に使用しているスキルマップや計画書等）をカスタマイズして作成することも考えられる。なお、ＩＴ人材像については、必ずしも役職を設定する必要はなく、役割等として定義し、既存の役職者が担うことも考えられる。また、スキルについては、詳細なものを作成する場合もあれば、概要のレベルに留めることも考えられる。後者の場合、必要に応じて細分化できるよう情報を整理しておくことが考えられる。

【本工程の手順】

手順２－１－１	ＩＴ業務に求められる役割からＩＴ人材を定義する。

１．第１工程で整理したＩＴ業務をもとに、それぞれの業務で求められる役割毎にグループ化して必要となるＩＴ人材を定義する。

手順２－１－２	求められるＩＴ人材のスキルを定義する。

１．求められるＩＴ人材のスキル（例として、知識／業務経験／技量 等）とその評価方法を定義する。

２．スキルの評価方法としては、知識については受講研修・取得資格、業務経験については実務上の立場・経験プロジェクト規模、技量(※)については面談や適性診断による確認等が考えられる。

※「技量」とは、コミュニケーション能力等のヒューマンスキルや、「新規開拓を求める」「安定維持を求める」などの行動特性・思考特性を総称している。

【考慮事項】

○手順２－１－１

１．ＩＴ人材の役割を整理する。

ＩＴ人材の役割の名称や区分けについては、必ずしも新たに定義する必要はなく、既に使用している名称など、自機関で馴染みのあるものを使用することが考えられる。

２．求められるＩＴ人材像とそのスキルを定義する。

１．に基づき、求められるＩＴ人材像とその人数を定義する。例としては、以下のような整理が考えられる。

図表８　ＩＴ人材の役割・人材像の整理の手順例

ＩＴ人材の役割		求められる業務役割（詳細）		ＩＴ人材像
		ＩＴ業務内容（中分類）	ＩＴ業務内容（小分類）	
1	戦略策定 経営戦略・事業戦略 システム戦略	経営・事業環境の調査・分析	経営環境の調査・分析と課題の抽出 業界動向の調査・分析	・ＩＴに関する知識は、専門家レベルである必要はないが、ＩＴソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をシステム戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やシステム戦略の企画・立案ができる人材。
		経営・事業戦略の策定	基本構想の策定 アクションプランの策定 事業戦略実行体制の確立	
		経営・事業戦略の評価	戦略全体の評価 費用対効果の検証 次期戦略への反映	
		システム戦略の策定	現状分析・ＩＴ動向分析 ＩＴ基本方針の策定 ＩＴ中期計画の作成	
		システム戦略評価・改善	戦略全体の評価 費用対効果の検証 次期戦略への反映	
2	システム企画	システム戦略の具体的な案件化	現行業務・システムの分析 投資規模の策定 全体構想のシステム案件化	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。
		システム全体計画の策定	全体開発スケジュールの作成 費用と投資効果の予測 全体工数による案件調整	
		システム全体計画の評価	計画全体の評価 投資管理・費用対効果の検証 次期計画への反映	
3	業務設計・システム導入	業務要件定義 （自機関内開発）	対象業務の課題整理 新業務モデルの作成 業務要件の定義	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、ＩＴ部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価および交渉することができる人材。 ・ＩＴ部門やシステムベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受入テストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。
		業務要件整理・要求定義 （外部発注）	対象業務の課題整理 業務要件の整理 提案依頼書の作成と発行	
		ベンダー提案評価と選定	提案書の比較検討 委託先選定 発注契約手続	
		ベンダー開発管理	委託業務の開始・管理 進捗状況の把握とリスク対策 成果物の検収	
		移行・導入	受入テスト マニュアル作成・研修 移行・導入実施	
4	・・・・・	・・・・・・	・・・・・・・	・・・・・・

○手順２－１－２

１．ＩＴ人材像（ＩＴ人材に求められる業務役割）から、求められるスキル（例として、知識／業務経験／技量 等）と評価方法を定義する。スキルの評価方法の策定については、試行・評価・改善を繰り返して精度を高めていく。そのため、まず小規模な範囲で試行する等を考慮する。また、評価方法については、評価対象者に合意されていることや、評価者向け研修等により自機関内の標準として認知されていることも考慮する。

図表９　ＩＴ人材に求められるスキルの整理の手順例

ＩＴ人材の役割		ＩＴ人材像	スキル		
			知識	業務経験	技量
1	戦略策定 経営戦略・事業戦略 システム戦略	・ＩＴに関する知識は、専門家レベルである必要はないが、ＩＴソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をシステム戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やシステム戦略の企画・立案ができる人材。	・社内外の事業環境 ・ＩＴ基礎知識 ・金融機関のＩＴ動向 ・新しいＩＴ ・ＩＴの活用事例 ・ＳＷＯＴ分析 ・業務改善技法 ・開発投資対効果 ・評価指標（KGI・KPI）	経営企画部門 ○年以上	コミュニケーション ネゴシエーション マネージメント 創造力
2	システム企画	・ＩＴに関するコスト感覚を持ち、工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。	・社内のＩＴ全般に関する知識 ・ＩＴポートフォリオ ・新しいＩＴ ・ＩＴの活用事例 ・開発スケジュール立案に関する知識 ・開発投資対効果 ・業務システムの主管部門と担当者	システム部門 ○年以上	コミュニケーション マネージメント 本質（目的）思考力
3	業務設計・システム導入	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、ＩＴ部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価および交渉することができる人材。 ・ＩＴ部門やシステムベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受入テストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。	・営業店業務知識 ・ＩＴ基礎知識 ・業務知識 ・新しいＩＴ ・ＩＴの活用事例 ・業務改善技法 ・開発投資対効果	営業店業務 ○年以上	コミュニケーション ネゴシエーション 本質（目的）思考力
4	・・・・・	・・・・・・			

第２工程	ＩＴ人材・スキルの定義と現状及び 中長期的に必要となるＩＴ人材の把握

工程２－２	現状のＩＴ人材の把握と中長期的に必要となるＩＴ人材の確認

現状のＩＴ人材の人数とスキルを把握し、システム戦略の実現に必要なＩＴ人材の人数とスキル、および、それらの過不足を解消すべき時期を確認する。

【基本的な考え方】

具体的なＩＴ人材像（又は役割）、スキル、スキルマップ等、全体像の把握が可能なものを作成し、ＩＴ人材の現状とシステム戦略を実現するために理想的な状況とのギャップを把握する。

【本工程の手順】

手順２－２－１	ＩＴ人材の現状（人数・レベル）と想定される今後の推移を把握する。

１．定義したＩＴ人材・スキルの自機関内／自機関外（外部委託）の実態を整理する。

２．現状の各部門におけるＩＴ人材の人数とスキルを確認する。

３．中長期的にみたＩＴ人材の増減（退職等による減少など）を把握する。

手順２－２－２	システム戦略に必要な中長期的なＩＴ人材の人数とスキルを定義する。

１． システム戦略に基づき、必要となるＩＴ人材の人数とスキルを定義する。

２． 定義したＩＴ人材・スキルの自機関内／自機関外（外部委託）の区分けを行う。

手順２－２－３	現状と中長期的な目標とのギャップ分析を行う。

１．自機関内／自機関外（外部委託）それぞれにおいて、ＩＴ人材の人数とスキルの過不足を分析する。

２．各業務のＩＴ人材不足が業務遂行に与える影響度を勘案しながら、ＩＴ人材の人数とスキルの過不足を解消すべき時期を検討する。

【考慮事項】

◯手順２－２－１

現状のＩＴ人材の人数とスキルを把握するにあたり、実際には関連部門に対して判定作業の依頼が必要となる場合もある。その場合、部門間でスキル判定などの基準が大きく相違しないよう考慮する。

なお、本手順において、現在、スキルを持った人材がＩＴ業務を行っていない組織に配置されている場合、ＩＴ人材として認識されない可能性がある。また、ＩＴ業務を行っている組織に配置されている場合でも、業務に必要のない個々人のスキルは把握されない可能性がある。そのため、配置転換検討など、第３工程で確保・育成計画を策定する際には、これらの点について考慮する。

◯手順２－２－２

中長期的に必要なＩＴ人材の人数・スキルの整理にあたっては、業務の優先度を勘案する。

◯手順２－２－３

ＩＴ人材とスキルの過不足の解消時期については、中長期計画との整合性を意識して整理する。

図表 10　ＩＴ人材の現状把握とギャップ分析例

	レベル判定の基準(例)
Level 4	全社的な第１人者として、主体となって推進できる。 他部署を含めて下位者の指導ができる。
Level 3	部署内の第１人者として、主体となって推進できる。 部署内の下位者を指導・サポートできる。
Level 2	担当する部分的な業務を独力で推進できる。
Level 1	上位者の指導・サポートを受けながら役割を遂行する。

必要に応じて各部門に基準を示し、判定作業を依頼する。

IT人材の役割	人材像	スキル			業務配置（◎:主管部門 ○:関連部門 ▲:外部委託窓口 ●:外部委託(一部含む)）															
		知識	業務経験	技量		経営企画		営業企画		事務企画		システム		リスク管理		・・・・		全社合計	
					レベル	Asis	Tobe	Asis	Tobe	Asis	Tobe	Asis	Tobe	Asis	Tobe			Asis	Tobe
1 経営戦略・ＩＴ戦略	・ITに関する知識は、専門家レベルである必要はないが、ITソリューションによって何ができるのかの絵を描ける人材。 ・部門横断的な企画の交通整理ができ、ＩＴの現況と方向性などについて経営層が判断できる資料提供と説明ができる人材。 ・経営戦略を実現するために、ＩＴを活用したプロセス改革などの具体的施策をＩＴ戦略として取りまとめる人材。 ・新しいＩＴ動向などにアンテナを高く保ち、最先端の施策やＩＴ戦略の企画・立案ができる人材。	・社内外の事業環境 ・ＩＴ基礎知識 ・金融機関のＩＴ動向 ・新しいＩＴ技術 ・ＩＴの活用事例 ・ＳＷＯＴ分析 ・業務改善技法 ・開発投資対効果 ・評価指標（ＫＧＩ・ＫＰＩ）	経営企画部門 ○年以上	コミュニケーション ネゴシエーション マネージメント 創造力		◎主管部門					○関連部門							
					Level 4	1	2					0						1	2
					Level 3	0	2					1						1	2
					Level 2	2						1	2					3	2
					Level 1	2						0						2	0
2 システム企画	・ＩＴに関するコスト感覚を持ち、システム工数や予算等、各部門との調整ができる人材。 ・システムの長期開発計画や年度計画が策定できる人材。 ・開発等も含めＩＴ全般に関し俯瞰的に判断、管理のできる人材。	・社内のＩＴ全般に関する知識 ・ＩＴポートフォリオ ・新しいＩＴ技術 ・ＩＴの活用事例 ・開発スケジュール立案に関する知識 ・開発投資対効果 ・業務システムの主管部門と担当者	ＩＴ部門 ○年以上	コミュニケーション マネージメント 本質（目的）思考力		○関連部門					◎主管部門							
					Level 4	0						1	3					1	3
					Level 3	1	2					1	3					2	5
					Level 2	3	2					3						6	2
					Level 1	2						2						4	0
3 業務設計・システム導入	・システム開発のスキルまでは必要ないが、ＩＴリテラシーが高く、顧客や現場の目線で必要とする機能を集約し、ＩＴ部門やベンダーに対して正しく伝えられる人材。 ・ＩＴに関するコスト感覚を持ち、ベンダーの提案内容やコストについて評価および交渉することができる人材。 ・ＩＴ部門やシステムベンダーから受領するシステム要件定義書などの内容を理解して、業務要件とギャップがないことを確認できる人材。 ・業務要件や様々な利用シーンを想定し、受け入れテストケースを作成・実施できる人材。 ・ユーザーが理解しやすい操作マニュアルを作成し、研修や通知等により周知できる人材。	・営業店業務知識 ・ＩＴ基礎知識 ・業務知識 ・新しいＩＴ技術 ・ＩＴの活用事例 ・業務改善技法 ・開発投資対効果	営業店業務 ○年以上	コミュニケーション ネゴシエーション 本質（目的）思考力				◎主管部門		◎主管部門		○関連部門							
					Level 4				0		1	1						1	1
					Level 3				0	2	2	4						2	6
					Level 2				1		3		8	6				12	6
					Level 1				4		2		6					12	0

・ＩＴ業務の主管部門と関連部門では、ＩＴ人材として求められるスキルにも違いが生じるものが考えられる。

・ＩＴ人材適正化の方法（育成・配置転換等）を検討するうえで、部門毎の各スキルに対応した人員数を確認し、あるべき姿とのギャップを把握することが考えられる。

第３工程	ＩＴ人材の確保・育成計画の策定

工程３－１	ＩＴ人材の確保・育成計画の策定

過不足が見込まれるＩＴ人材の人数とスキルの適正化を検討し、ＩＴ人材の確保・育成計画として取りまとめる。

【基本的な考え方】

具体的なＩＴ人材確保・育成の手段を策定する。

「確保」とは、自機関において要員を確保することに加えて、ＩＴ人材を外部から調達することも含まれる。「育成」とは、自機関のＩＴ業務に必要な人材を、自機関の要員として育成することである。

中長期的な観点からＩＴ業務を洗い出し、担当部門のＩＴ人材が不足した場合、組織に与える影響の大きさ、業務の優先度などを勘案して適正化の方策を検討する必要がある。

【本工程の手順】

手順３－１－１	過不足が見込まれるＩＴ人材の適正化方針の検討

１．過不足が見込まれるＩＴ人材の適正化策として、育成、採用、配置転換、外部リソースの活用等が考えられ、どのような方法を選択するかについて検討する。

手順３－１－２	育成による適正化の検討

１．現状の育成施策を把握する。

２．知識レベルの向上策として、研修、資格取得等が考えられ、どのような方法を選択するかを検討する。

３．経験レベルの向上策として、キャリアパス設定、ジョブローテーション制度等が考えられ、どのような方法を選択するかを検討する。

４．技量レベルの向上策として、研修、実務での経験等が考えられ、どのような方法を選択するかを検討する。

手順３－１－３	配置転換による適正化の検討

１．現状の配置転換施策を把握する。

２．過不足のあるＩＴ人材の配置転換の方法を検討する。

手順３－１－４	外部リソースの利用による適正化の検討

１．現状の外部リソース利用施策を把握する。

２．過不足のあるＩＴ人材の外部リソース利用方法を見直す。

手順３－１－５	採用による適正化の検討

１．現状の採用施策を把握する。

２．不足しているＩＴ人材を採用するための方法を検討する。

手順３－１－６	各適正化方策を補助する施策の検討

１．現状の補助施策を把握する。

２．ＩＴ人材のスキル評価とそのフィードバック方法を検討する。

３．人員が定着するための制度を検討する。

４．育成における知識レベルについては、研修や資格取得の補助制度を検討する。

【考慮事項】

○手順３－１－１

１．ＩＴ人材の適正化施策を検討する際には、その施策のコストと予算確保に留意する必要がある。また、限られた経営資源の中で、すべてのＩＴ人材について適正化を同時に進めることが困難な場合は、システム戦略等の観点から、優先度を考慮して、各ＩＴ人材における適正化の時期を検討する。

２．ＩＴ人材の適正化施策を検討する際には、組織全体としての採用、育成、配置転換、外部リソースの活用方針等との整合性を取ることが考えられる。

○手順３－１－２

育成策としては、次のようなことが考えられる。

１．現場での実践（0JT）

２．外部研修への参加

外部研修等への参加については、ベンダーやセキュリティベンダーが提供する研修への参加、大学が提供する社会人教育への参加などが考えられる。

３．資格取得の奨励

４．外部への出向

・システム関連子会社への出向

ＩＴ業務を担う子会社を有しているのであれば、そこにＩＴ人材を出向させることは有効な手段と考えられる。

・共同センターへの出向

・ＩＴベンダーへの出向等

業務委託先であるベンダーへの出向や、ベンダーとの対応窓口を担わせるのも有効な手段であると考えられる。

５．外部ＩＴ人材の受け入れによるノウハウの習得

ベンダーやシステム関連子会社からの出向者を自機関のシステム部門等に受け入れ、自機関の社員とともに業務を担ってもらうことで社員にノウハウを吸収させることも考えられる。

○手順３－１－３

１．手順２－２－１にて記載の「現状のＩＴ人材の把握」が実施された時点で、スキルを持った人材がＩＴ業務を行っていない組織に配置されている場合、ＩＴ人材として認識されない可能性がある。また、ＩＴ業務を行っている組織に配置されている場合でも、その業務に必要のない個々人のスキルは把握されない可能性がある。組織の人的リソースをさらに有効活用するための配置転換を検討するにあたっては、これらの点について考慮する。

２．高いスキルを持つ人材の定年退職やジョブローテーション等に備え、後進を育成できるような配置について考慮する。

○手順３－１－６

１．スキル評価と人事評価との関連

スキル評価と人事評価（待遇・報酬に結び付く評価）との関連については、スキルの評価基準・評価方法を定義し、その評価プロセスが適切に運用されるよう整備した上で検討

することが考えられる。

２．研修の奨励

自機関内外の研修による育成を行う場合、その研修期間は業務を離れることになるため、そのことを奨励あるいはある程度の強制力を持った制度を作ることも考えられる。また、業務の現場にて各人がその必要性を認識するような教育も考えられる。

第４編　サイバーセキュリティ人材に関する考慮事項

１．策定の手順

(1) 本編の使用方法

本編では、サイバーセキュリティ人材を確保・育成するにあたっての考慮事項をまとめている。本編の使用は、第３編「ＩＴ人材の確保・育成に向けた実務」にて記載のＩＴ人材の確保・育成に向けた各工程の手順から、サイバーセキュリティ業務から役割の洗い出し、サイバーセキュリティ人材の実態把握およびその確保・育成に関して考慮すべき事項について記載する。

(2)『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（第３版追補３）』（以下、『コンテ手引書』という）との関係

本編では、サイバーセキュリティ業務の分類やインシデント対応組織[4]の役割など当センターが発刊した『コンテ手引書』から引用している。詳細については、『コンテ手引書』を参照のこと。

２．本編で使用する用語

本編で使用する用語について、以下のとおり定義する。

・インシデント

一般的には、自組織のシステムにおいて発生する可能性のある事故・事象を指す。[5]

本編では、インシデントと呼称する場合、特にサイバー攻撃等により発生する事故・事象を指す。

・サイバーセキュリティ

サイバー攻撃により、情報の漏えいや、期待されていた情報システム等の機能が果たされないといった不具合が生じないようにすること。[6]

[4] インシデントに実際に対応する組織を指す。代表的なものとして、CSIRT（Computer Security Incident Response Team）がある。

[5] インシデントハンドリングマニュアル、一般社団法人　JPCERT コーディネーションセンター、2015。

[6] 同上。

第１工程	現状および中長期的なＩＴ業務の洗い出し

工程１－１	現状のＩＴ業務の洗い出し
ＩＴ人材の確保・育成に関する計画を策定するにあたり、自機関においてＩＴ人材が担う業務の洗い出しを行い、各業務に求められる具体的な役割を明確にする。	

【本工程の手順】

手順１－１－１	現状のＩＴ業務の洗い出しを行う。

【考慮事項】

１．サイバーセキュリティ業務における役割の洗い出し

本工程では、第３編において洗い出されたサイバーセキュリティ業務に求められる具体的な役割について記載する。

(1) 役割の分類

金融機関等は、サイバー攻撃を受けた際に迅速かつ的確に対応するために、サイバーセキュリティに関する責任者（CIO[7]、CISO[8]等）を配置し、その配下にインシデント対応組織を設置することが有効である。

また、自機関のサイバー攻撃対応に必要な役割を検討したうえで、それらを担うインシデント対応組織を整備する。インシデント対応組織は、インシデントの検知及び対応等のインシデント発生時の役割のみならず、平時の運用を担うことにより、サイバー攻撃対応態勢の実効性を高めることができる。

経営層と十分に連携できる組織を整備することで、自機関としての対応方針の決定や社外への公表等の対応が迅速に行うことができる。

『コンテ手引書』では、経営層など組織の責任者等およびインシデント対応組織の役割として、以下のように言及している。

[7] 「Chief Information Officer。企業の情報システム部門の最高情報責任者を指す[7]。経営層に含まれる。システム戦略策定やコスト管理・リスク管理方針等、情報システムのパフォーマンスの最大化に向けてバランスを取りながら推進する。」日本 CIO 協会

[8] 「Chief Information Security Officer。経営陣の一員、もしくは経営トップからその役を任命された、情報セキュリティ対策を実施する上での責任者を指す。」サイバーセキュリティ経営ガイドライン Ver1.1、経済産業省、独立行政法人 情報処理推進機構、2016。

図表 11　組織の責任者等の役割の例

組織の責任者等	役割の例
経営層	・サイバー攻撃リスクの把握 ・態勢整備計画の決定（対応方針の策定・経営資源の投下） ・外部委託先を含めた態勢整備の実施状況の把握 ・コンティンジェンシープラン発動の判断　等
サイバーセキュリティに関する責任者（CIO、CISO 等）またはインシデント対応組織の管理者	・業務的視点及び専門的視点の双方を踏まえた対応方針の確認 ・執行部門と経営層との連携・調整・対応指示 ・サイバー攻撃リスクの管理・評価・報告 ・態勢整備計画の策定・報告・実施 ・外部委託先を含めた態勢整備の実施状況の管理・評価・報告 ・コンティンジェンシープラン発動の該当事象の発生報告 ・即時の対応が要求される事態における判断・承認　等

経営層の役割については、『企業経営のためのサイバーセキュリティの考え方』（内閣サイバーセキュリティセンター（NISC））、『サイバーセキュリティ経営ガイドライン Ver 1.1』（経済産業省、独立行政法人　情報処理推進機構（IPA））も参照のこと。

（『コンテ手引書』より引用）

経済産業省が定める『サイバーセキュリティ経営ガイドライン Ver. 1. 1』の、「情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」の中に、「方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としての CISO 等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。」のような記載があり、サイバーセキュリティに関する責任者の役割の明確化が示されている。

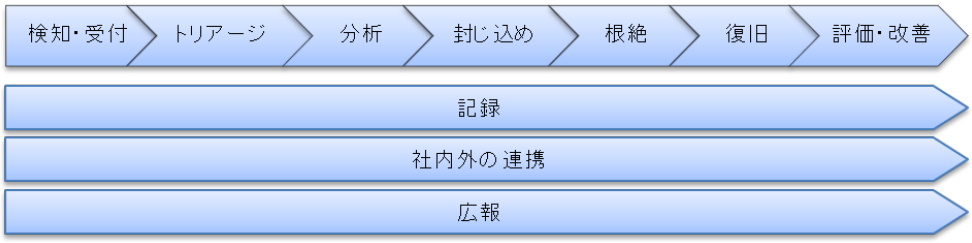
図表 12　インシデント対応組織の役割の例

対応の分類	役割の例
態勢整備	・サイバー攻撃対応手順等の整備・見直し ・自機関内外の対応窓口の設置・周知 ・ログの取得・保全 ・サイバー攻撃対応に関する教育・訓練・演習の企画・推進　等
平時の運用	・窓口における情報の受付・連携 ・監視・分析 ・情報共有・情報収集 ・脆弱性情報・脅威情報への対応 ・脆弱性診断 ・セキュリティ対策や監視等に関する評価・見直し　等
インシデント発生時の運用	・インシデントの受付 ・インシデントへの対応 ・経営層や関係部門等との調整・報告 ・外部機関との連携 ・フォレンジック[9] ・情報共有・情報収集　等

（『コンテ手引書』より引用）

インシデント対応組織の平時の運用では、インシデント発生時に迅速かつ確実に対応するために、監督官庁や金融 ISAC、JPCERT/CC 等、また同業他社との連携を行うために窓口の役割が重要となる。

図表 13　インシデントの発生から対応収束までのプロセス



出所：（米国国立標準技術研究所（NIST）『コンピュータセキュリティインシデント対応ガイド』などをもとに FISC にて作成）

[9]デジタル・フォレンジックのことをいう。デジタル・フォレンジックとは、インシデントレスポンスや法的紛争、訴訟に対し、電磁的記録の証拠保全、分析を行うとともに、電磁的記録の改ざん、毀損等についての分析、情報収集等を行う一連の科学的調査手法、技術のことをいう（非営利活動法人 デジタル・フォレンジック研究会の定義）。

これらのサイバーセキュリティ業務を所管する部門については、各社の体制に応じて異なるものであり、一意に特定はできない。システム障害など発生時の対応態勢や自機関で検討しているサイバー攻撃対応態勢を踏まえ、適切に役割を各部門と協議し、配置する。

インシデント対応組織の役割については、その業務の特性や、対応要員及びそのスキルといった自機関の実態を踏まえて、外部委託を行うことも考えられる。金融機関において行う業務と、外部委託を行う業務を明確にする。ただし、外部委託先を含めた全体統括や業務影響の評価、対応策の判断等については、金融機関等で担うべき機能と考えられる。

(2) インシデント対応組織に関する考慮事項

インシデント対応組織の在り方については、自機関のサイバーセキュリティに対する方針によって様々な対応態勢となる。インシデント対応組織は、自機関の方針に適した態勢を取ることが望ましい。インシデント対応組織を考えるにあたっては、設置する際の観点も含め、以下のような考察点がある。

①インシデント対応組織の態勢および対応要員の在り方について

インシデント対応組織と、その対応要員については、以下の２つの態勢がある。

a. 専任組織による態勢

自機関に専任のサイバー人材を配置する方法のことである。自機関内外に対するサイバー攻撃に関する問合せなどのインシデントの受付業務や、インシデント対応業務に専任者を配置できる場合、迅速な情報連携・共有が可能になり、インシデント発生時の迅速な対応につながることが考えられる。

b. 兼任組織による態勢

ＩＴ部門やリスク管理部門等、インシデント対応組織を担う人材が本業と共にサーバー業務を担う方法のことである。専任者を配置することは人員数等の都合上から困難である場合が多く、兼任という考え方がある。兼任組織では、複数の部門から選出された要員を組織に含める態勢を取ることもできる。

例えば、システム部門、リスク管理部門、事務部門、広報部門等が該当する。このような態勢では複数部門の横の連携が取りやすいために、インシデント発生時には関係部門と密な連携が可能となる。

ただし、本来業務の都合でサイバーセキュリティ業務に注力できず、迅速な対応が困難になる可能性がある。

なお、短期的には兼任組織として運用し、人材育成も含め、中長期的に専任組織に切り替えていく方策も考えられる。

②インシデント対応組織の主管部門

インシデント対応には複数の部門が関わることが想定されるため、自機関の方針に基づき、関連する部門の中で、事務局に該当するインシデント対応組織の主管部門を予め決める。

例えば、主管部門となるのは、以下のような部門が考えられる。

a.　システム部門

サイバーセキュリティ分野をＩＴ分野の延長線上にあるものとして、システム部門がリードする場合には、インシデントをシステム障害対応業務の一環と捉え、システム部門を主管としたインシデント態勢を構築することになる。

b.　リスク管理部門

サイバーセキュリティ分野をリスク管理分野の延長線上にあるものとして、リスク管理部門がリードする場合には、リスク管理部門を主管としたインシデント態勢を構築することになる。

c.　経営管理部門

経営管理部門に配置することで、全社的な取り組みとしてインシデント対応組織を構築することになる。

③外部委託先（共同センター、クラウドベンダー等）の活用

金融機関等の外部委託先がサイバー攻撃を受けた場合、金融機関等に被害が発生する可能性がある。そのため、金融機関等は、リスクに応じて外部委託先のサイバー攻撃対応態勢の整備状況について自社が求める水準と同等またはそれ以上であることを確認する。

共同センターやクラウドサービスを利用する場合、利用するサービスや取り扱う情報の重要度に応じて、適切なリスク管理レベルが確保されているか考慮する。また、他社へのサイバー攻撃によって、自社にシステム停止等の被害が波及する可能性があるため、他社への攻撃に起因して自社にも影響が及ぶ場合における、情報連携や補償について契約や SLA の内容を確認する。

第２工程	ＩＴ人材・スキルの定義と現状及び 中長期的に必要となるＩＴ人材の把握

工程２－１	ＩＴ人材・スキルの定義

自機関のＩＴ業務において必要となるＩＴ人材（人材像）を定義する。
求められるＩＴ人材のスキルを定義するとともに、その評価方法を検討する。

【本工程の手順】

手順２－１－１	ＩＴ業務に求められる役割からＩＴ人材を定義する。

【考慮事項】

１．組織の責任者等の必要性

サイバー攻撃を受けた際に迅速かつ的確に対応するために、経営層はサイバーセキュリティに関する責任者（CIO、CISO 等）やインシデント対応組織の責任者を配置し、それらの者が平時からサイバー攻撃が自機関に与える影響を十分に認識するとともに、インシデント発生時には主導的・中心的な立場で対応を牽引する。また、適切な権限を委譲することも有効である。

２．サイバーセキュリティにおける「橋渡し人材」の必要性

サイバーセキュリティ業務では、経営層とインシデント対応組織との間を取り持つとともに、自機関における関連部門間の調整を行う橋渡し人材が必要となる。[10]

橋渡し人材は、実務者の報告を理解し、指示できるだけのＩＴおよびサイバーの知識、自機関の金融業務および自機関のＩＴについても経験・知識が必要となる。さらに、経営層が理解できるよう報告を行うためのコミュニケーション力等も必要となる。

また、橋渡し人材は、自機関の情報システムに精通する必要があることから、外部から即戦力を確保することが困難であり、所要の知識・経験を習得するには相応の時間を要するものと考えられるために、自機関において育成することが望ましい。

[10] 参考文献。
・『新・情報セキュリティ人材育成プログラム』、情報セキュリティ政策会議、平成 26 年５月。
・『サイバーセキュリティ人材育成総合強化方針』、サイバーセキュリティ戦略本部、平成 28 年３月。
・『サイバーセキュリティ人材育成プログラム（骨子案）』、NISC、平成 29 年。

３．サイバーセキュリティ人材について

(1) サイバーセキュリティ人材の定義

サイバーセキュリティ人材の定義には、主に以下のものが挙げられる。

（参考）

①『セキュリティ知識分野（SecBoK）人材スキルマップ 2016 年版』、NPO 日本ネットワークセキュリティ協会、平成 28 年４月

②『「産業横断サイバーセキュリティ人材育成検討会」第一期最終報告書』、産業横断サイバーセキュリティ人材育成検討会、平成 28 年９月

③『セキュリティ対応組織の教科書～機能・役割・人材スキル～　第 1.0 版』、日本セキュリティオペレーション事業者協議会、平成 28 年 11 月

④『CSIRT 人材の定義と確保（Ver.1.5)』、日本シーサート協議会、平成 29 年３月

⑤『ITSS+』、独立行政法人　情報処理推進機構、平成 29 年４月

上記の内、①②については CISO を含む経営層、実務者層を網羅している。③はインシデント対応組織、運用監視組織の人材について、④は実務者層の中でもインシデント対応組織の人材に特化しており、⑤は実務者層全般に関する定義となっている。

(2) 自機関でのサイバーセキュリティ人材に望まれる役割の例

『コンテ手引書』では、自機関内で保有が望まれる役割に関して、サイバー攻撃対応の考慮事項におけるインシデント対応組織の整備及び役割の明確化の項において、「外部委託先を含めた全体の統括や業務影響の評価、対応策の判断等については、金融機関等で担うべき機能と考えられる」としており、サイバーセキュリティ業務に必要な人材の役割は、以下と考えられる。

図表 14　サイバーセキュリティ人材に望まれる役割の例

担当	役割	人材像（参考文献）
① CISO	社内の情報セキュリティを統括する。セキュリティ確保の観点から、CIO（最高情報責任者）、CFO（最高財務責任者）と必要に応じて対峙する。	CISO（『SecBok』）
②情報セキュリティ担当	自機関の事業計画に合わせてセキュリティ戦略を策定する。現在の状況と Tobe 像の Fit&Gap からリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、改善計画に反映する。	ソリューションアナリスト（『SecBok』）
	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自機関または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。	情報セキュリティアドミニストレーション（『ITSS+』）
③インシデント対応管理担当	自機関で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関しては CISO や経営層との情報連携を行う。また、CISO や経営者が意思決定する際の支援を行う。	コマンダー（『SecBok』、日本シーサート協議会）
	自機関で起きている情報セキュリティインシデントの全体統制を行うとともに、事象に対する対応における優先順位を決定する。重大なインシデントに関しては CISO や経営層との情報連携を行う。また、CISO や経営者が意思決定する際の支援を行う。	CSIRT コマンド（『ITSS+』）
④インシデント対応担当	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。	インシデントハンドラー（（『SecBok』、日本シーサート協議会）
	自機関または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携する。情報セキュリティインシデントへの対応状況を管理し、CSIRT コマンドのタスクを担当する者へ報告する。	インシデントハンドリング（『ITSS+』）
⑤情報連携担当	社外向けでは JPCERT/CC、NISC、警察、監督官庁、NCA、他 CSIRT 等との連絡窓口、社内向けでは IT 部門調整担当社内の法務、渉外、IT 部門、広報、各事業部等との連絡窓口となり、それぞれ情報連携を行う。	PoC（『SecBok』、日本シーサート協議会）
	自機関外の関係機関、自組織内の法務、渉外、IT 部門、広報、各事業部等との連絡窓口となり、情報セキュリティインシデントに係る情報連携及び情報発信を行う。必要に応じて IT 部門と CSIRT の間での調整の役割を担う。	CSIRT リエゾン（『ITSS+』）

手順２－１－２	求められるＩＴ人材のスキルを定義する。

【考慮事項】

１．サイバーセキュリティ人材に求められるスキル

金融機関等におけるサイバーセキュリティ人材に求められるスキルとして、知識／業務経験／技量等がある。サイバーセキュリティ業務の専門性・特殊性から知識においては、以下の３つが考えられる。なお、業務経験、技量については、第３編工程２－１手順２－１－２を参照のこと。

(1) ＩＴ知識

サイバーセキュリティ業務を遂行する際のベースとして、ＩＴ知識が求められる。ネットワークモニタリングや、異常な通信のログの保全・解析はＩＴ知識が必要となる。脆弱性情報に基づいて行われる OS やアプリケーションのアップデート、ウイルスソフトのパターン更新などは通常のＩＴ業務の延長線上で対策が行われる。

インシデント対応組織の役割の全部、または一部を外部委託している場合であっても、委託先への指示や、委託先からの報告を適切に理解できるだけの知識が求められる。

(2) サイバーセキュリティ固有の知識

サイバーセキュリティに関する攻撃は、日々、高度化・巧妙化しており、変化し続ける環境や攻撃手法に対応するため、研修等を通して知識・情報の最新化を行う。

インシデント対応組織の役割の全部、または一部を外部委託している場合であっても、委託先への指示や、委託先からの報告を適切に理解できるだけの知識が求められる。

(3) 業務知識

自機関の体制や業務及び業務に関連するシステムなどの知識が挙げられる。インシデント発生時には、どのような影響があるかを分析・判断し、適切な対応や経営層への報告ができる知識が求められる。

（参考）
- 『CSIRT 人材の定義と確保（Ver.1.0)』、同 Ver.1.5、日本シーサート協議会。
- 『組織内 CSIRT の要員』、JPCERT コーディネーションセンター。
- 『セキュリティ知識分野（SecBoK）人材スキルマップ 2016 年版』、特定非営利活動法人 日本ネットワークセキュリティ協会。
- 『ITSS+』、独立行政法人　情報処理推進機構。

第３工程	ＩＴ人材の確保・育成計画の策定

工程３－１	ＩＴ人材の確保・育成計画の策定

過不足が見込まれるＩＴ人材の人数とスキルの適正化を検討し、ＩＴ人材の確保・育成計画として取りまとめる。

【本工程の手順】

手順３－１－２	育成による適正化の検討

【考慮事項】

第３編工程３－１手順３－１－２項番１～５を参照のこと。

６．訓練、演習等

インシデント対応組織を中心とした自社で実施する訓練・演習、外部委託先等の関係組織と共同で実施する訓練、官公庁や業界団体が実施する共同演習などに参加することで、経営層へのサイバーセキュリティに関する意識啓発を図るとともに、サイバーセキュリティ業務におけるサイバー攻撃対応手順等の内容理解やスキルの向上を図る。

７．キャリアについて

自機関で確保・育成するサイバーセキュリティ人材については、ジョブローテーションの実施、および自機関におけるキャリアパスの構築を検討することが考えられる。

(1) ジョブローテーションの実施について

サイバーセキュリティ業務に関連する主な部門間を自機関のセキュリティ戦略に沿って計画的に経験していく方法がある。サイバーセキュリティ業務に関連する部門間で、適切な配属期間と育成計画を組み合わせて配置転換を行う。

(2) キャリアパスの構築について

自機関で、ある職位（セキュリティ責任者等）に就くまでに辿ることとなる経験や順序を構築する。なお、自機関の戦略や、人材の適性などを考慮して判断することが考えられる。

（参考）

・経済産業省、みずほ情報総研株式会社、『平成 24 年度情報セキュリティ対策推進事業（情報セキュリティ人材の育成指標等の策定事業）事業報告書　～第５編～情報セキュリティ人材のモデルキャリア』、平成 25 年。

・『CSIRT 人材の定義と確保（Ver.1.5）』、日本シーサート協議会、平成 29 年。

手順３－１－５	採用による適正化の検討

【考慮事項】

１．新人採用

新人採用時にサイバーセキュリティ人材を募集する。

産学連携に基づく教育機関におけるサイバーセキュリティ教育は近年充実し、演習などを交え、より実践的な教育が行われている。

ただし、就業後に金融業務知識が必要になるため、研修期間を設けるなど、業務面におけるフォローについて考慮する。

２．中途採用

中途採用によりセキュリティ人材を充当する方策となる。

中途採用を行う際は、自機関に必要なサイバーセキュリティ業務を洗い出し、その業務に求められる役割を鑑み、採用したい人物のスキルを明確にする。

なお、中途採用においては、スキルや能力の観点以外に、受け入れ側の体制や、環境面についても十分配慮する。また採用が決定した際には、コミュニケーションを充実させて、認識の合一を目指す。

３．システム部門からサイバーセキュリティ人材を登用

システム部門に配属された人員を対象に、スキルギャップを明確にし、不足スキルを育成等で補うことで、対応要員として早期の対応が見込まれる。

参考

平成 29 年 5 月 23 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（山田・尾﨑法律事務所）
〃	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
〃	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

参考

平成 29 年 5 月 23 日

公益財団法人 金融情報システムセンター

委　員	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
〃	アマゾンウェブサービスジャパン(株)から就任予定	
〃	一般財団法人Ｆｉｎ Ｔｅｃｈ協会から就任予定	
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

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。

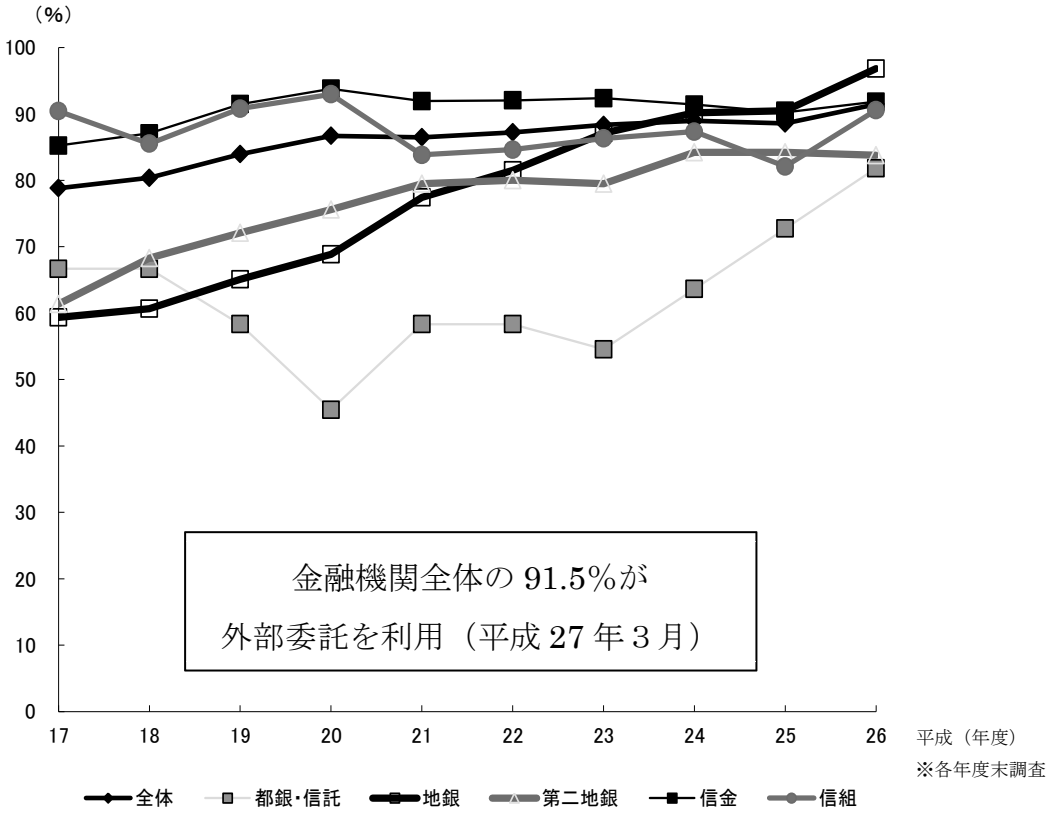
Ⅰ　近年の外部委託動向と外部委託を巡る環境変化

１．近年の外部委託動向

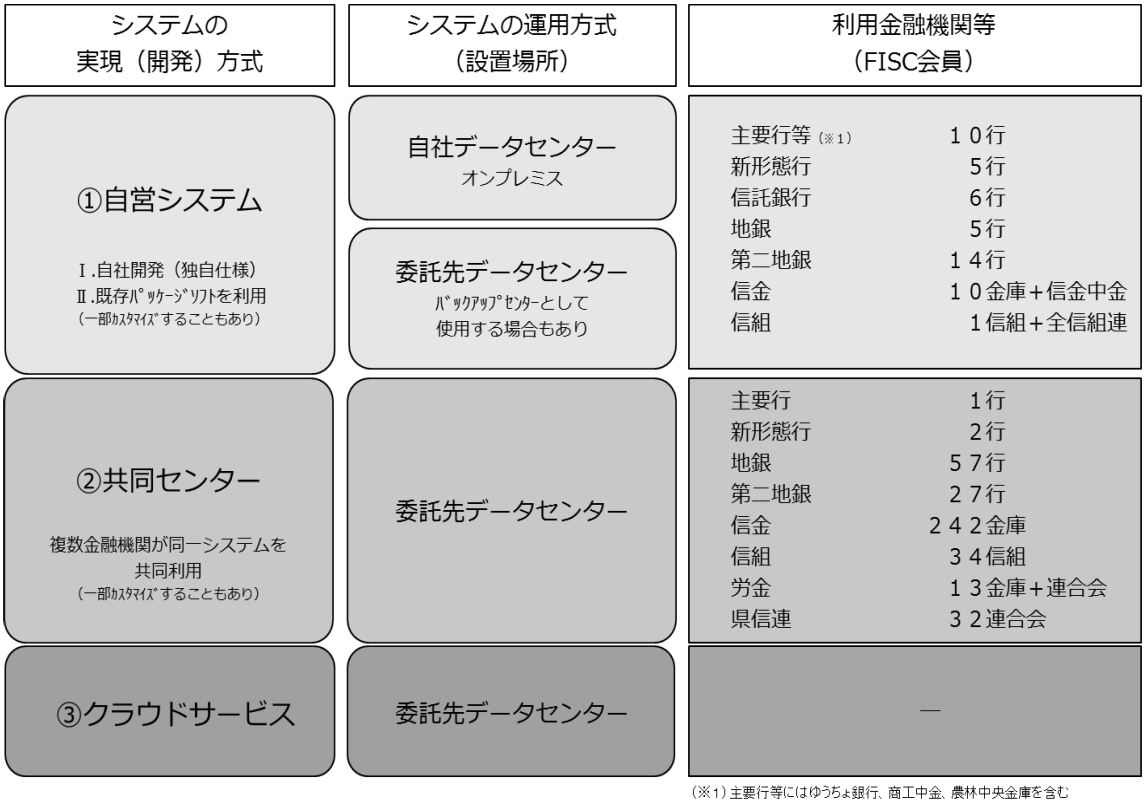
近年、金融機関のシステム関連業務における外部委託の進展が著しい。

・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

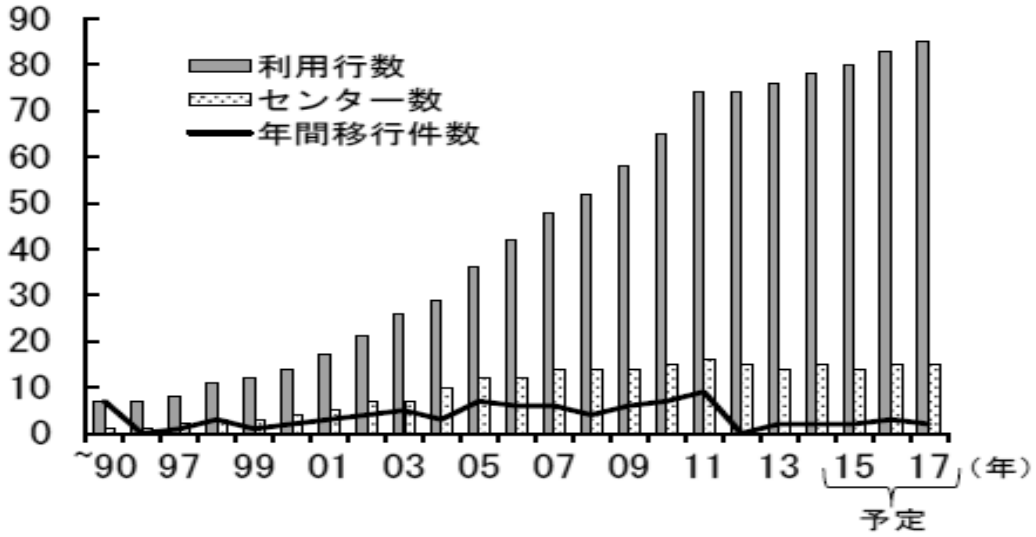
平成 24 年 11 月発表	共同センターの委託先社員によるキャッシュカード偽造事件
平成 26 年２月発表	地方銀行の再々委託先社員によるキャッシュカード偽造事件
平成 26 年３月	金融庁から金融機関に対し自主点検を要請

（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。

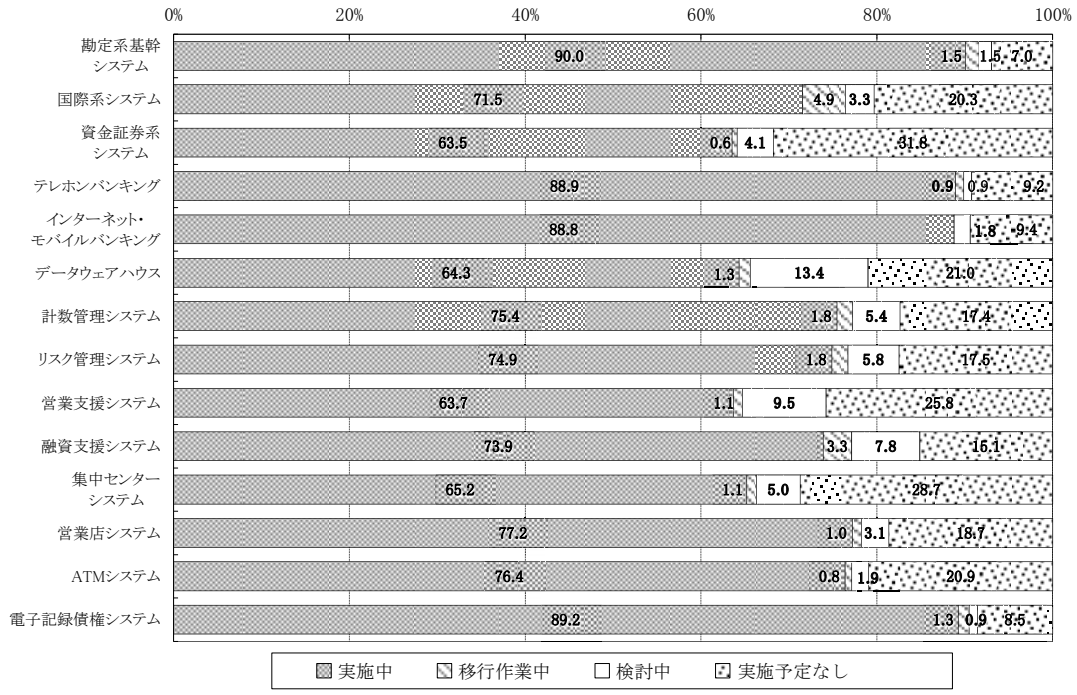
（図表４）勘定系システムの共同化の進展（地銀・第二地銀）

（平成 26 年 7 月金融庁 金融モニタリングレポートより）



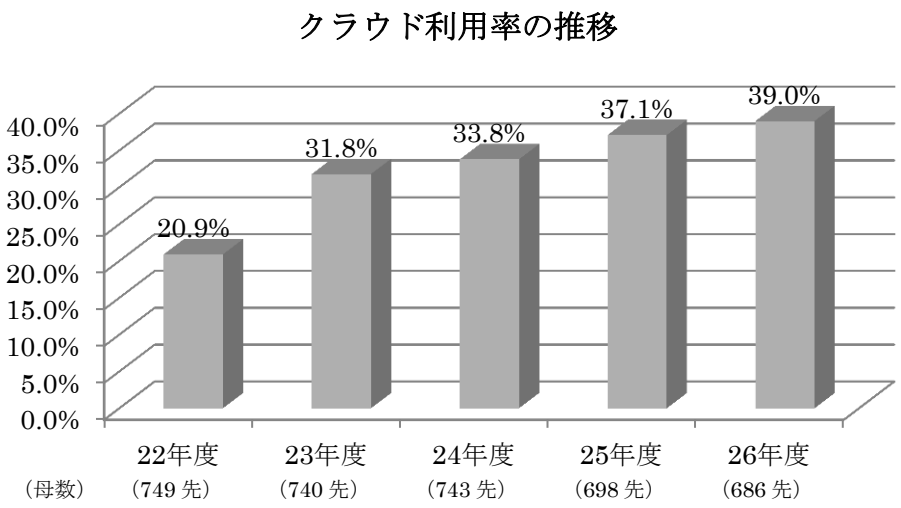
（図表５）多くのシステムで、共同センターが利用されている

（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）

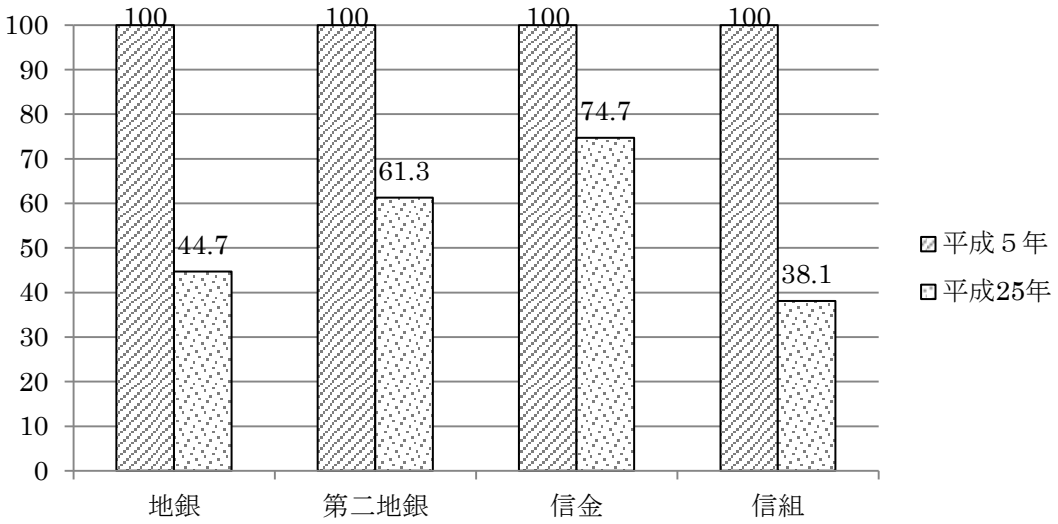
	利用比率	うち大手４社
生命保険会社(42 社)	83%	75%
損害保険会社(33 社)	76%	100%

（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。

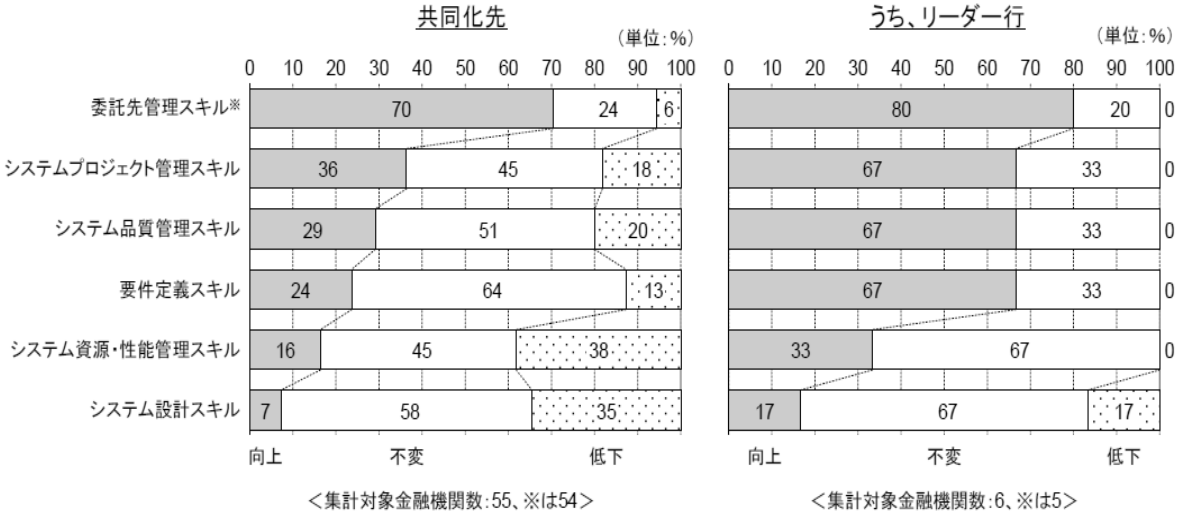
（図表８）システム部門の職員数の推移；平成５年度末を 100 とした場合の平成 25 年度末の割合（平成 26 年 FISC 調査）



（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。

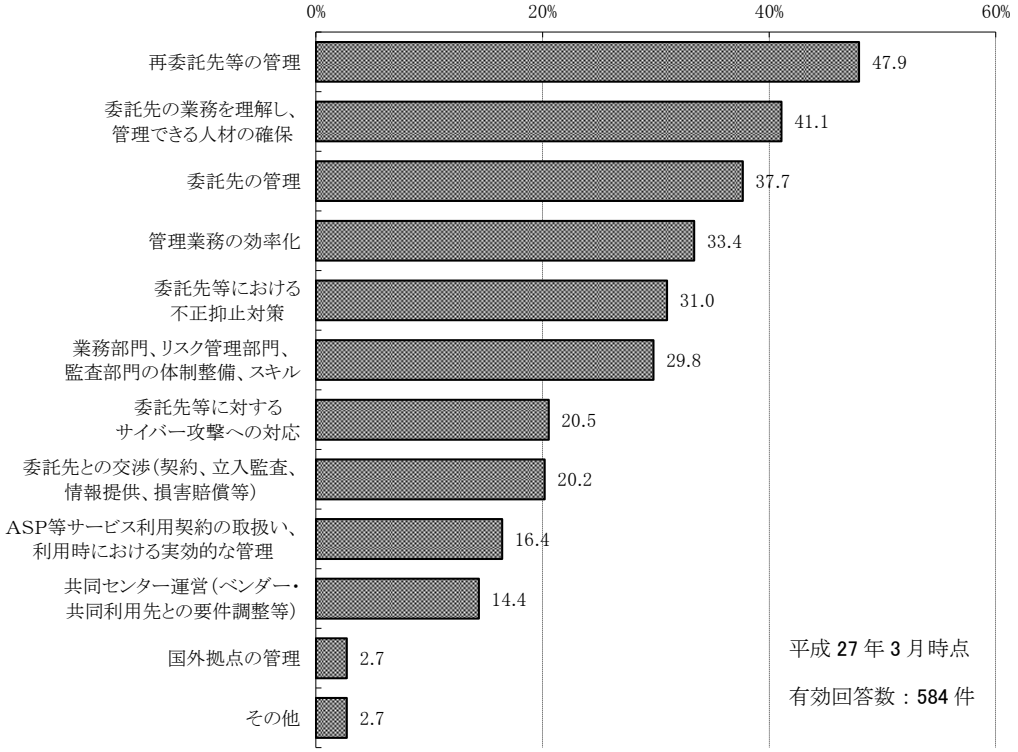
4．IT ガバナンス検討の必要性

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。

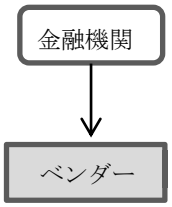
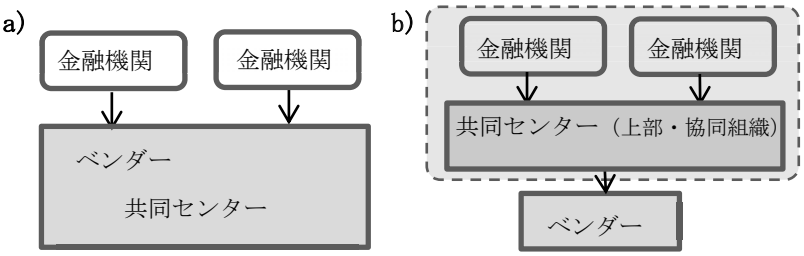
また、国内外の各種ガイドラインでは、システムの外部委託は一義的には IT マネジメントの一領域と位置づけられており、IT ガバナンスとともに IT マネジメントが重視されている。
検討に当たっては、こうした観点も参考としている[2]。

[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

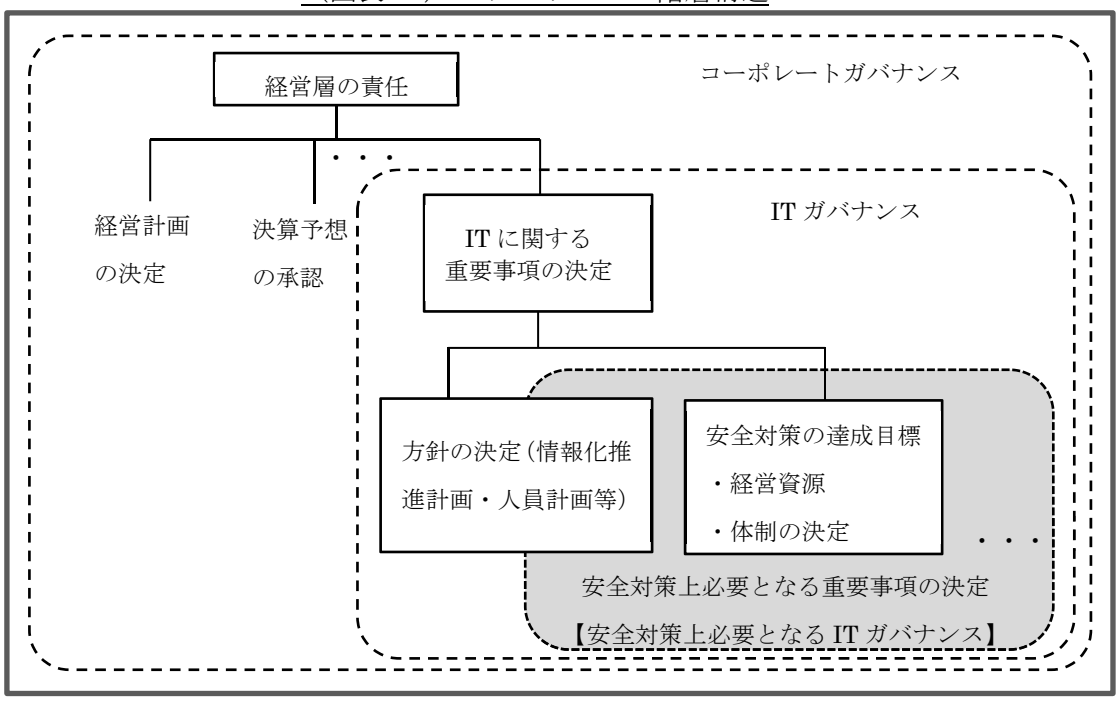
金融機関等の活動は情報システムに大きく依存していることから、情報システムの安全・安定の確保は、金融機関等の重要な経営課題である。そのため、経営層[10]はそれらに適切に対処するために、IT ガバナンスを機能させることが必要である。

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。

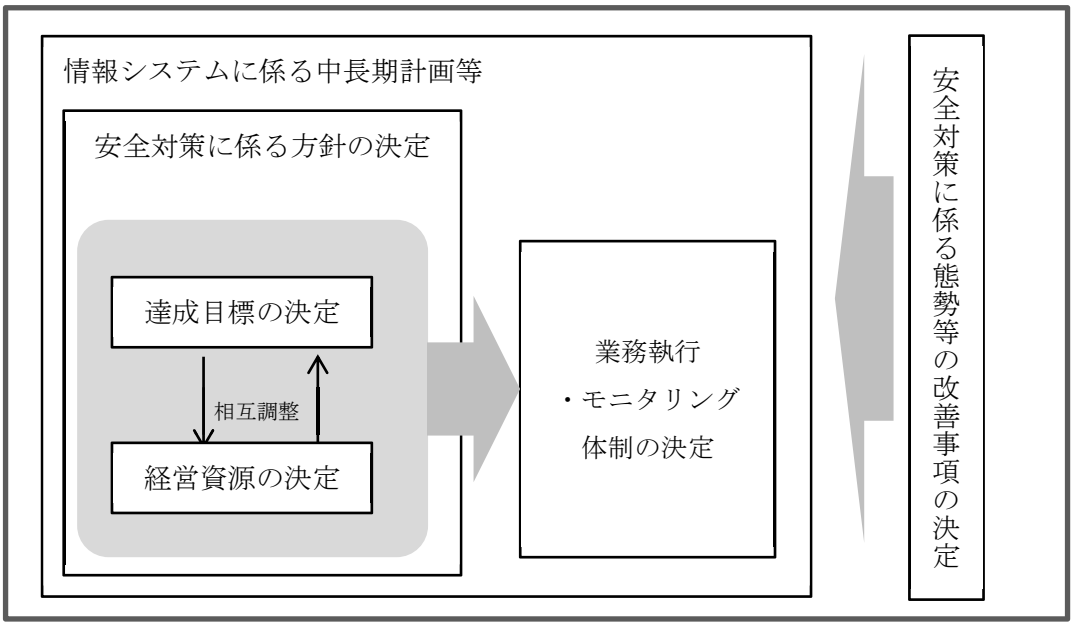
11 金融庁のコーポレートガバナンス・コードの策定に関する有識者会議『コーポレートガバナンス・コード原案（平成 27 年３月５日）』では「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえたうえで、透明・公正かつ迅速・果断な意思決定を行うための仕組み」と定義されている。

（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～

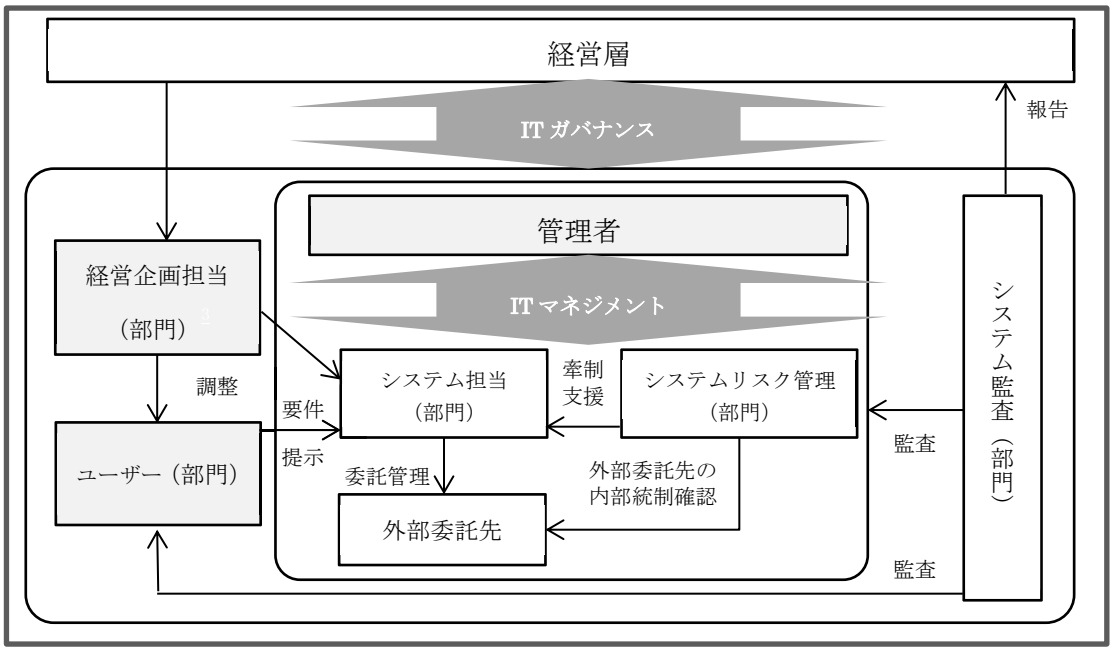
情報システムの安全対策において、経営層によるITガバナンスのもとで、例えば、下図のとおり複数の関係者が必要な機能を発揮している。（図表14参照）

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。

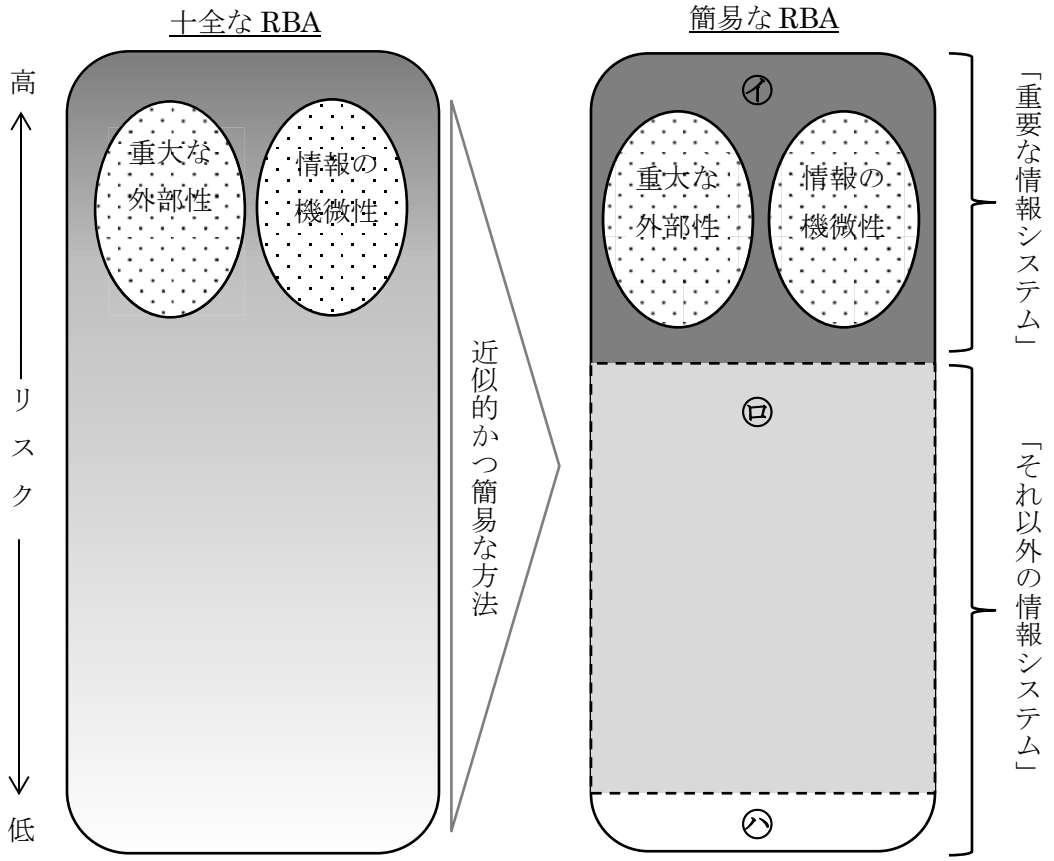
てリスクが低い情報システムであることから、そもそも安対基準の適用対象外とすることが可能である。内部への影響が軽微な情報システムとしては、機微情報を含む顧客情報を保有しない情報システム、あるいは、他の情報システムと連結していない情報システムが候補となる。こうした安対基準適用対象外とすることが妥当な低リスクな情報システムは、その選定に合理性があれば、金融機関等の実態に応じて、独自に定めることが可能である。

（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。

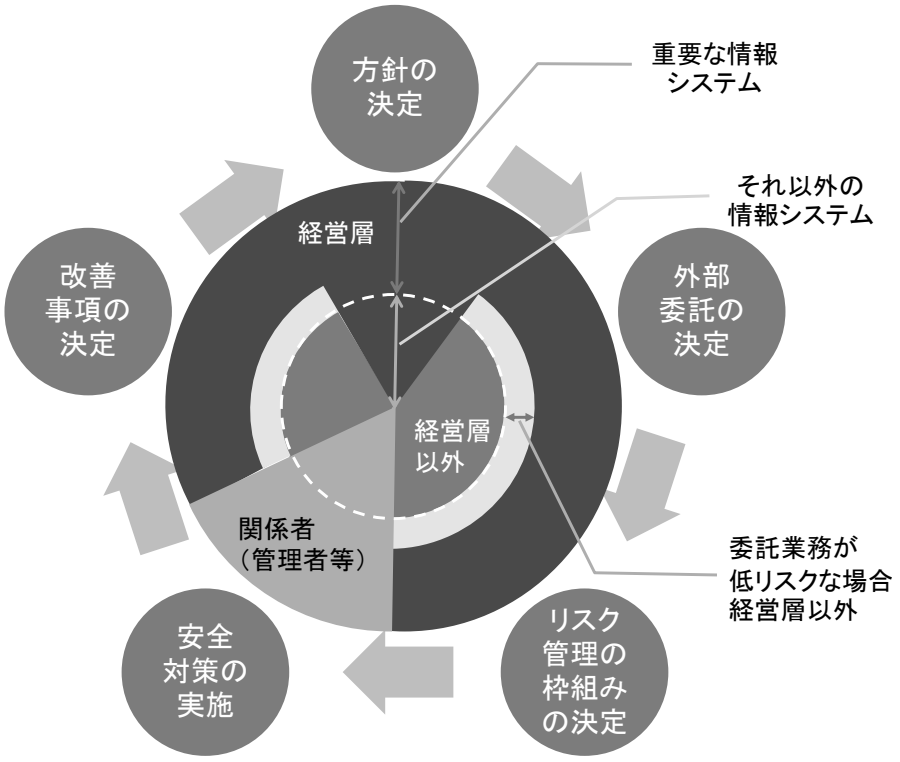
---

[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

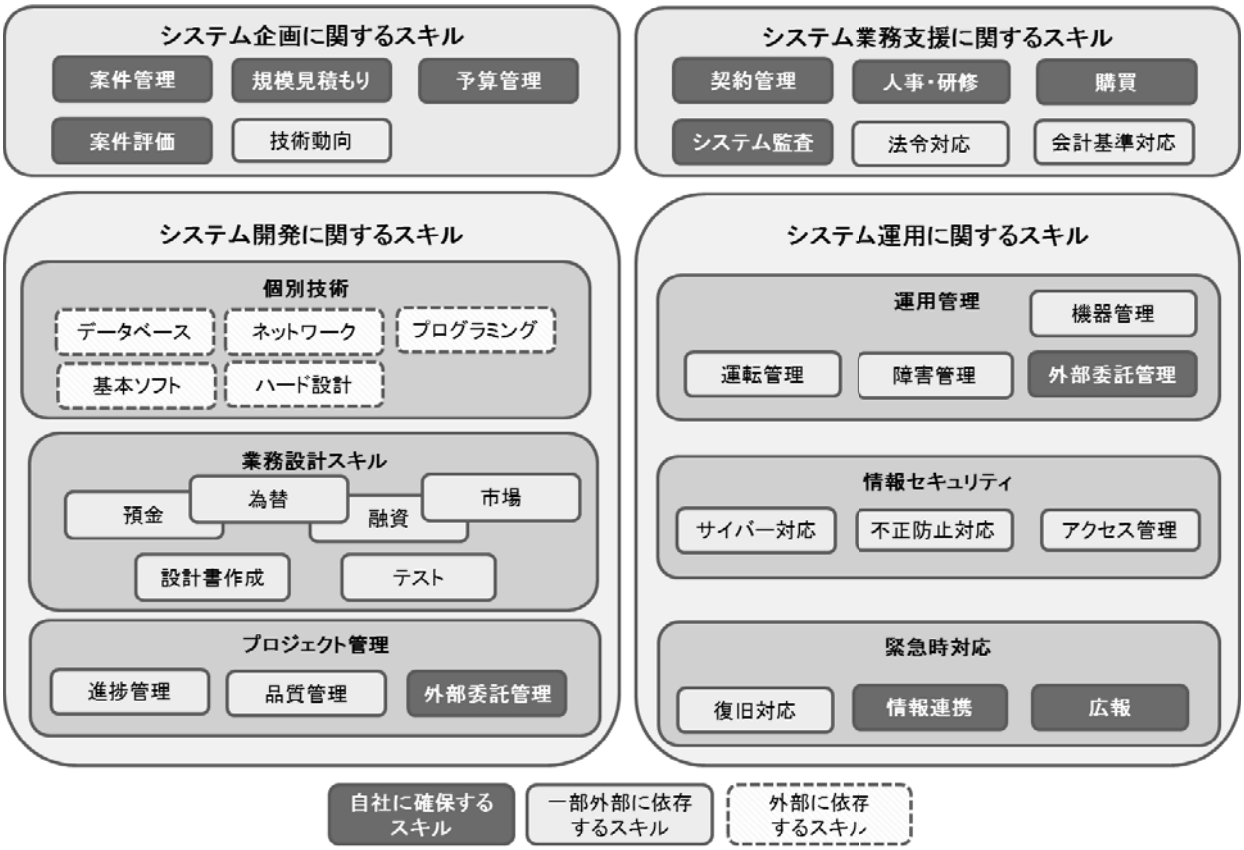
柴田　晃宏、宮原　武也（第４回まで）、仲程　文徳（第５回から）、岡本　一真、三浦　哲史（第５回から）

（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

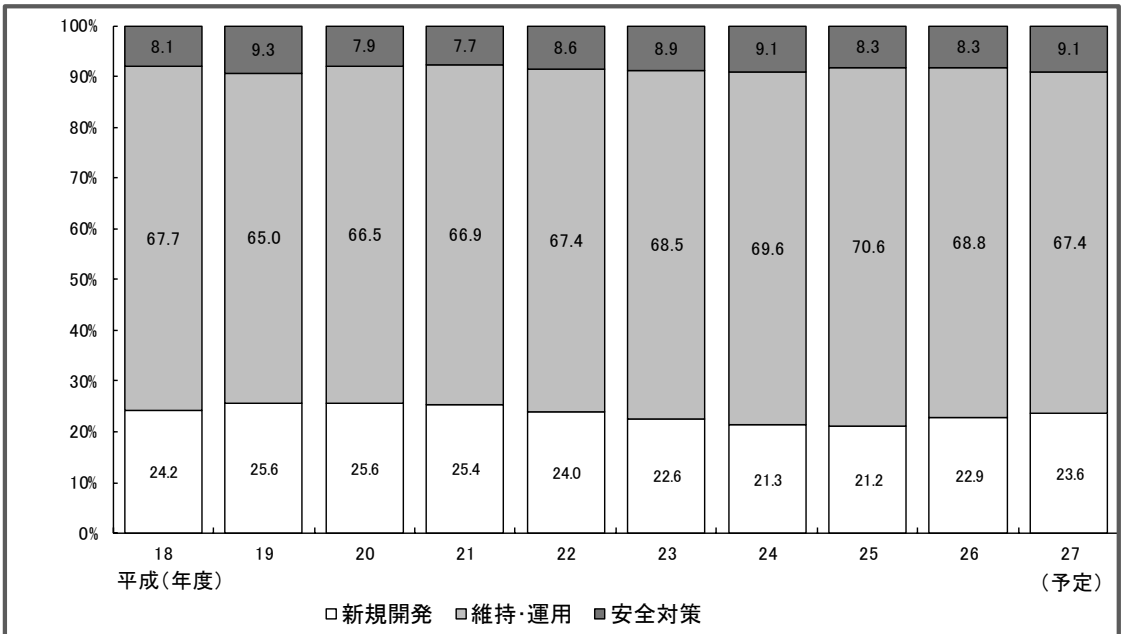
【資料１】IT スキルマップの一例



（出所）FISC にて作成

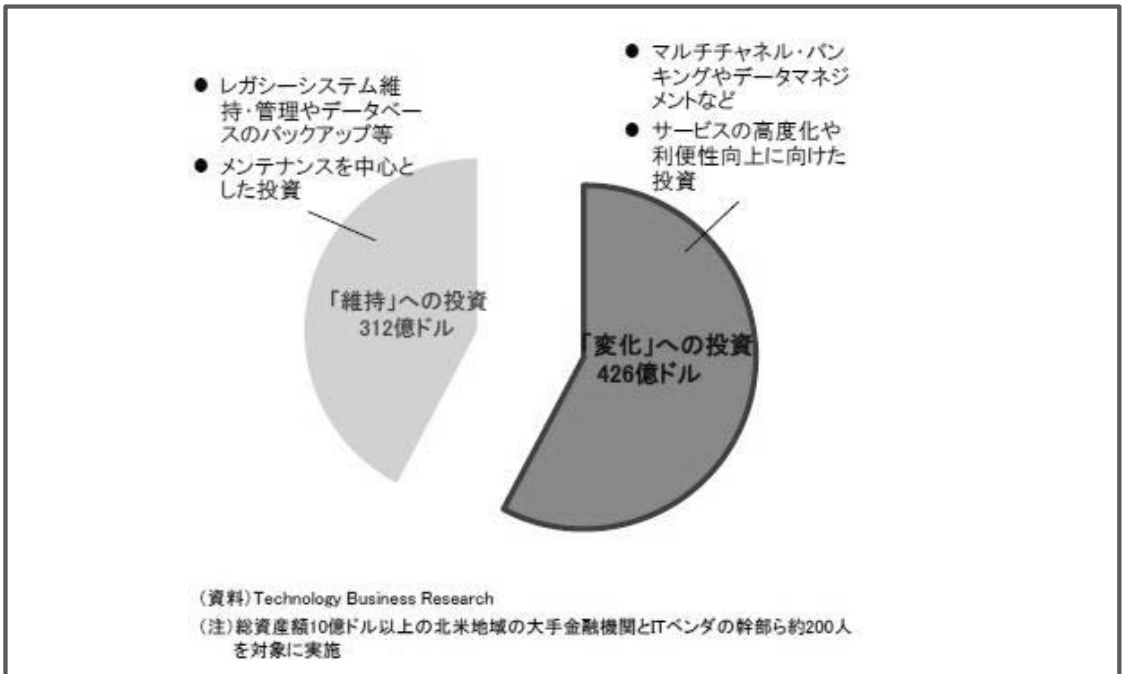
【資料２】システム関連経費の目的別内訳

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

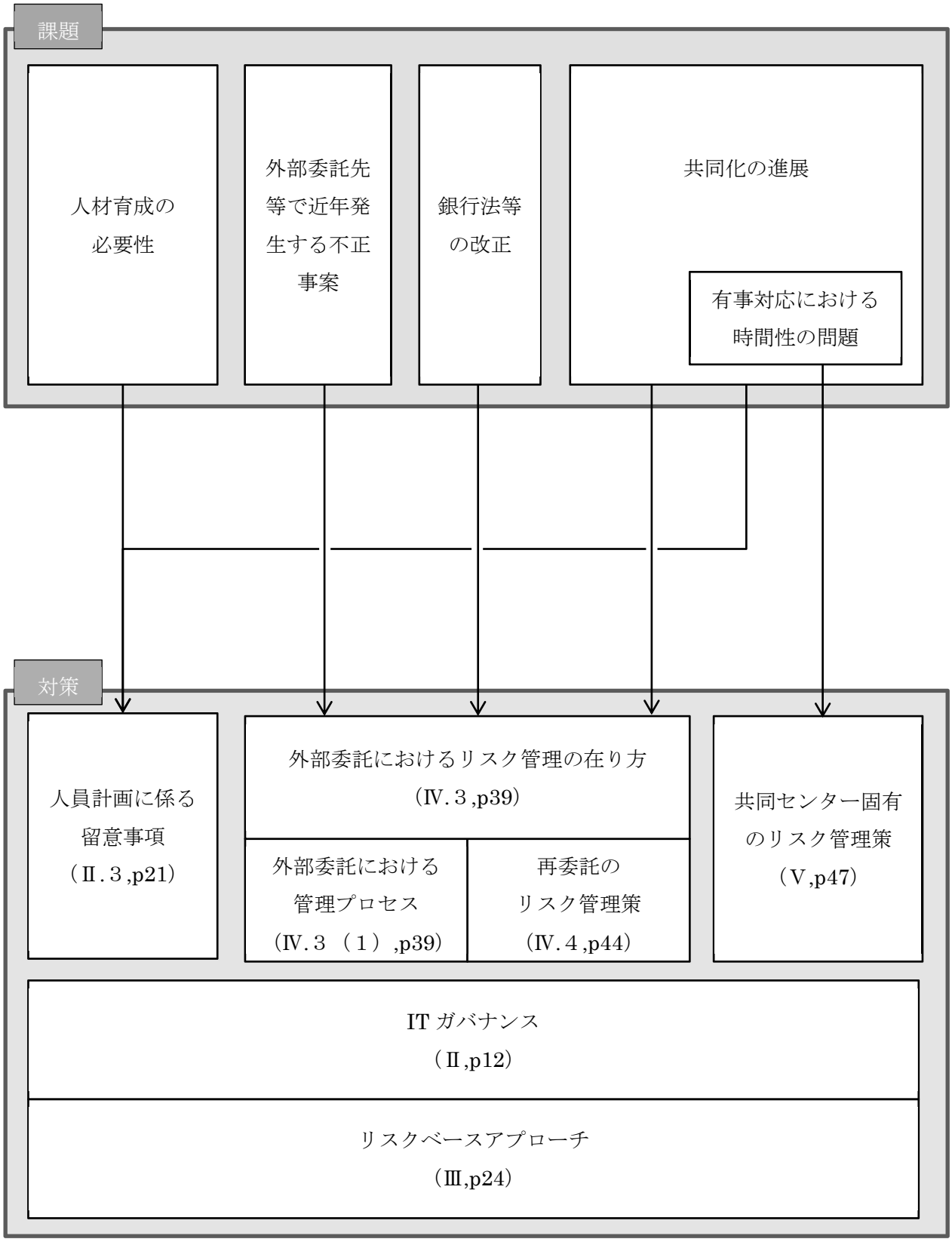
平成 28 年３月時点で勘定系システムの運用を共同化している金融機関の数及びその預金量の合計を以下のとおり集計した。

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



金融機関における FinTech に関する
有識者検討会報告書
（案）

平成 29 年　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、金融機関、業界団体及び監督当局等において、FinTech と総称される IT を活用した革新的な金融サービスへの取組みが、急速に活発化している。【資料編資料１参照】

こうした取組みの活発化の結果として、今後、多岐にわたる FinTech の出現が予想される中、金融情報システムセンター（以下「FISC」という）においても、金融機関等の動きと歩調をあわせて、FinTech に関する安全対策の在り方を、あらかじめ検討しておくことが期待されている。

既に、FISC では、昨年６月に終了した「外部委託に関する有識者検討会」（以下「外部委託検討会」という）において、リスクベースアプローチや IT ガバナンスという新たな枠組みを提言し、金融情報システムにおける安全対策の考え方を、欧米先進諸国の動向等を踏まえて、大きく前進させてきたところである。

そうした外部委託検討会の成果を踏まえたうえで、わが国金融機関における FinTech に関する安全対策の在り方について、明確かつ具体的な指針を示すために「金融機関における FinTech に関する有識者検討会」（以下「FinTech 検討会」という）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、わが国金融機関が、FinTech において、システムの安全性を確保しつつも、顧客のニーズに適応しイノベーションの成果を最大限享受しうることを目指して検討会が行われ、本報告書が取りまとめられた。

Ⅰ　FinTech に関する安全対策検討の在り方

１．検討の手順

まず、FinTechと総称される金融サービスに係る諸業務（以下、「FinTech業務」という）は多岐にわたることから、そうした業務を担う情報システムが、安対基準[1]の対象となるかどうか（あるいは対象とすべきかどうか）、その判別を行うための基準が必要となる。

次に、安対基準の対象となる FinTech 業務を担う情報システムに安対基準を適用するに当たって、どのような付加的検討がなされるべきか、を検討することが必要となる。

【資料編資料２参照】

FinTech 業務を担う情報システムが、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等（以下「重要な情報システム」という）に該当する場合は、安全対策における基本原則に従って、社会的・公共的観点から、その安全対策の達成目標の設定に当たっては、「高い安対基準」の適用を求めることとなる。そのため、重要な情報システムで使用される FinTech に係るテクノロジー等が、これまで安対基準で前提とされていない新たな性質を有している場合には、それを「高い安対基準」に反映する必要がある。

一方、FinTech 業務を担う情報システムが、重要な情報システム以外の情報システム（以下「一般の情報システム」という）である場合は、十全なリスクベースアプローチを採用する金融機関においては、安全対策は独自に決定することが可能であることから、本検討会において、達成目標等について特段の付加的検討は不要である。

他方で、簡易なリスクベースアプローチを採用した金融機関においては、まず「必要最低限の安対基準」を安全対策の達成目標として設定することとなる[2]が、多岐にわたるFinTech業務の登場が予想される中で、安対基準の取扱いが明確でないがゆえに、「高い安対基準」を適用せざるをえないとされることが想定される。

このように、FinTech 業務を担う情報システムに対して、安対基準が形式的に適用されることがないよう、あらかじめ、従来の安対基準が前提としている事項や、従来の安対基準が必ずしも想定していなかった事項等の前提を明らかにしたうえで、FinTech に関する安対基準適用上の課題と安全対策の在り方等を明確にしていくことが必要である。

---

[1] FISC『金融機関等のコンピュータシステムの安全対策基準・解説書』の略。ここでは、現行の第８版及び第８版追補改訂だけでなく、FISC『外部委託検討会報告書』の成果も含むものとして使用する。

[2] 「必要最低限の安対基準」の前提となる「簡易なリスク管理策」について、これまでの有識者検討会において「クラウドサービス利用」、「外部委託」について、それぞれの安全対策の在り方を踏まえて提言が行われており、一律に「高い安対基準」が適用されることが無いよう取組みが進んでいるところである。

２．安対基準の対象となる情報システムの判別基準

安対基準は、30 年以上前に策定されたその初版から一貫して「金融機関等[3]のコンピュータシステム」をその対象としてきた。「金融機関等のコンピュータシステム」とは、すなわち、金融業務を担う情報システムであり、かつ、その安全対策について金融機関等に責任が生じる情報システムのことをいう。したがって、FinTech業務を担う情報システムのうち、安対基準の対象となるのは、そのFinTech業務が金融業務であり、かつ、その安全対策について金融機関等に責任が生ずる情報システムである。

金融業務とは、金融機関等の業法等に基づいて、金融機関等が顧客に対して提供する金融サービスに係る業務である。したがって、顧客に対して提供するサービスであっても、例えば、商品等の売買を目的とする電子商取引業務を担う情報システムは、金融サービスに係る業務を担う情報システムとは解されないことから、安対基準の対象とはならない。また、金融機関等の内部のみで利用される情報システム（例：人事給与システム、経営情報システム等）は、安対基準の対象とはならない[4]。

一方、金融機関等以外の事業者が、金融機関等あるいは金融機関等の顧客と何ら関係なく、みずからのサービス利用者のために行う FinTech 業務は、金融機関等に何ら安全対策上の責任が生じないことから、その情報システムは安対基準の対象とはならない。

３．重要な情報システムで利用される FinTech に係るテクノロジー等の取扱い

重要な情報システムでの利用が想定されるFinTechに係るテクノロジー等として、ブロックチェーン技術やAI[5]が考えられる。検討に当たっては、これらの要素技術は、それを用いた業務の事例（ユースケース）は幅広いと考えられることから、それぞれのユースケースに応じた技術的特性に着目して、検討を進める必要がある。もっとも、現状では、重要な情報システムにおけるユースケースが出現していないことから、直ちに検討を行うのではなく、今後のユースケースの出現状況等をにらみながら、検討が可能となる時期を確定させていくこととする。

---

[3] 安対基準では初版（昭和 60 年 12 月）以来「金融、保険、証券、クレジット等金融業務を営む業界の各社」と表記されている。

[4] 安対基準初版では「本基準は金融機関等が顧客に提供するサービスに関連するシステムを前提にしている。しかしながら、金融機関等の内部のみに利用されるシステムについても、安全対策上参考となる部分について、本基準を適宜取り入れることとする。」とされており、現在まで、その考え方が基本的には踏襲されている。

[5] 人工知能。Artificial Intelligence の略。

４．FinTech に関する安全対策の在り方を検討するに当たっての前提

（１）安全対策実施上の新たな関係者となる FinTech 企業の登場

安対基準は、金融情報システムにおける安全対策実施上の関係者として、金融機関に加えて、情報システムの開発・運用の技術的役割を担う委託先であるITベンダー[6]の２者を念頭におき、策定されてきた。

しかしながら、FinTech業務を担う企業は、ITベンダーと類似の技術的な性質を有するとともに、金融関連サービスといったビジネスモデルの企画実施等を行う業務的な性質もあわせて有しており、こうした技術的な性質と業務的な性質[7]を同時に有する関係者は、従来の安対基準では、必ずしも明確に想定されてはいなかった。

したがって、安対基準を FinTech 業務に適用した場合に内在する問題を明らかにするに当たっては、金融機関、IT ベンダーに FinTech 企業を加えた３者関係を整理し、類型化したうえで、新たに登場した FinTech 企業等が果たすべき安全対策上の役割を検討することが有益である。

（２）金融機関が必ずしも主導的立場とならない業務形態の登場

安対基準では、金融機関が顧客に対して提供する金融サービスに係る業務を担う情報システムにおいては、金融機関に顧客に対する安全対策上の責任が存することを前提としてきた。これは、金融機関が顧客に提供する金融サービスに関して、金融機関がそのすべてを主導して決定する中では、当然の帰結である。

一方で、FinTechを巡っては、近年、顧客と金融機関の間に介在するFinTech企業が登場している[8]。その中には、金融機関のサービスを利用するために必要となるIDやパスワード等を顧客から提供され、それによって、みずから金融機関から顧客に関するデータを取得し、かつ、取得したデータに独自の価値を付加した後、顧客に対して直接的に金融関連サービスを提供している業者がある。このようなFinTech企業のサービスは、金融機関から取得するデータをサービスの源泉として利用しながらも、金融機関が顧客に対して提供するサービスでは得られなかった革新的なユーザー体験等を付加していること等が顧客から評価され、その利用が進んでいる状況にある[9]。

このようなFinTech企業が顧客に対して直接的に提供するサービスは、FinTech企業が

---

[6] 安対基準においては、「IT ベンダー」だけでなく、「ベンダー」「コンピュータメーカー」等の用語が使用されているが、ここではそうした技術的性質を有する当事者を「IT ベンダー」と総称する。なお、IT ベンダーには「クラウド事業者」も含むものとして使用する。

[7] FISC『外部委託検討会報告書』においては、業務的性質を有する関係者の安全対策における主な役割と責任として、「Ⅱ IT ガバナンスと IT マネジメント 2.(3)ユーザーの役割と責任」において、「①安全対策に配慮したビジネスモデルの企画」「②投資効果の達成」「③業務要件の提示」が挙げられている。

[8] 顧客と金融機関の間に介在する FinTech 企業の中には、本文でとりあげた以外にも、店舗や金利等金融機関がホームページ等を通じて一般的に広く公開しているデータ（オープンデータ）を利用する業者も考えられる。

[9] 金融審議会『金融制度ワーキング・グループ報告書』（平成 28 年 12 月 27 日公表）において「近年、金融機関と顧客との間に立ち、顧客からの委託を受けて、IT を活用した決済指図の伝達や金融機関における口座情報の取得・顧客への提供を業として行う者が登場・拡大している」とされている。

そのすべてを主導して決定し、金融機関と何ら交渉を行うことなく、一方的に金融機関から顧客に関するデータを取得することが可能な場合がある。こうした金融機関が完全に受動的立場となる場合は、金融機関には何ら統制の手段等が無いことから、金融機関において顧客に対する安全対策上の責任は生じないと解される。したがって、たとえ、金融機関の顧客に対して提供される金融関連サービスであっても、安対基準の対象とならないと解するのが妥当である[10]。

他方で、顧客に対して、直接的にはFinTech企業がサービスを提供するものの、FinTech企業と金融機関の間に交渉があり、その結果、金融機関がFinTech企業に提供するデータに関して、金融機関が決定を行うことが可能な場合がある。また、金融機関がFinTech企業から受入れるデータに関しても、金融機関が決定を行うことが可能な場合も考えられる。こうした、金融機関において、顧客に関するデータ[11]の提供または受入れに関して決定権が存する場合は、金融機関が部分的にせよ主導性を発揮しているものと考えられることから、金融機関に何らかの安全対策上の責任が生じていると解するのが妥当である。

したがって、FinTech企業が提供するサービスにおいて、情報システムにおける安全対策上の責任が、金融機関に部分的に生じる場合についても、安対基準の対象として、その安全対策の在り方を検討する必要がある[12]。

なお、こうした金融機関の安全対策上の部分責任は、顧客の許諾があるとはしながらも、もともと金融機関に管理責任が存する顧客に関するデータを、第三者に提供すること、または、第三者から受入れたデータに従い顧客に関するデータへ更新を行うこと、に由来するものである。したがって、提供または受入れに関するデータのリスク特性に着目し、それに応じて、安全対策の在り方を考えることとなる。その際には、リスクベースアプローチを踏まえると、データの提供に関しては、データの量のほか、データのリスク特性の１つである機微性の程度に着目することが適切である。機微性の程度とは、万一データがFinTech企業によって、本人の許諾した範囲を超えて利用された場合、あるいは一方的に外部に流出した場合等に、顧客が被ると想定される損失の程度のことをいう[13]。また、データの受入れに関しては、受入れたデータに従って行うデータへの更新の

---

10 英国の『Open Banking Standard』（2016 年２月８日）では、「スクリーンスクレイピング」を取り上げ、一方的に金融機関から顧客に関するデータを取得する場合の問題として「ウェブサイト側でアクセスをコントロールしたり規制することができない。」「何か問題が発生しても、利用者は問題解決の手段がなく、銀行に頼ることもできない。」等が挙げられている。なお、これはスクリーンスクレイピングが採用されていることをもって、直ちに問題があるわけではなく、本来的には金融機関と交渉なくデータが取得されることが問題である点に留意が必要である。

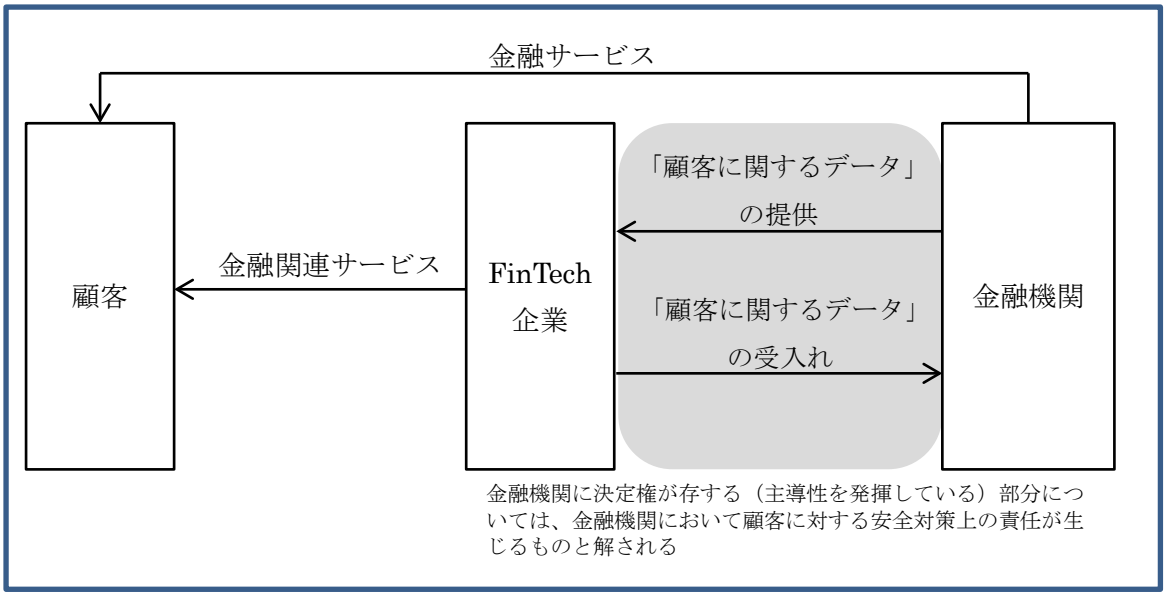
11 金融機関がFinTech企業に提供するデータとしては、例えば、顧客の取引履歴情報等がある。また、金融機関がFinTech企業から受入れるデータとしては、例えば、決済指図が考えられる。

12 なお、安対基準では、金融機関が主導的立場とならない場合として、【運 90-1】において「外部委託」とは異なる「サービス利用」に関する基準がある。この基準では「各金融機関が、外部委託の管理と全く同様に、サービスの提供元を複数の中から選定することや、独自にリスク管理を行うことは難しく、また非効率な場合が多い。」とされ、各金融機関が負担する安全対策上の責任の程度を一般の外部委託と比して、限定的に解すべきとしたものである。ただし、この基準は「金融機関相互のシステム・ネットワーク」を対象としており、今回検討の対象となっている顧客に対するサービスには該当しない。

13 FISC『外部委託検討会報告書』において、機微性の程度が高い機微情報に関しては「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」個人情報として、「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、

規模のほか、FinTech企業から受入れたデータが顧客の指示に基づくものであることを、FinTech企業が適切に確認しているかといった、FinTech企業による顧客の本人確認方法に着目することが適切である。

（図表１）金融機関が必ずしも主導的立場とならない業務形態

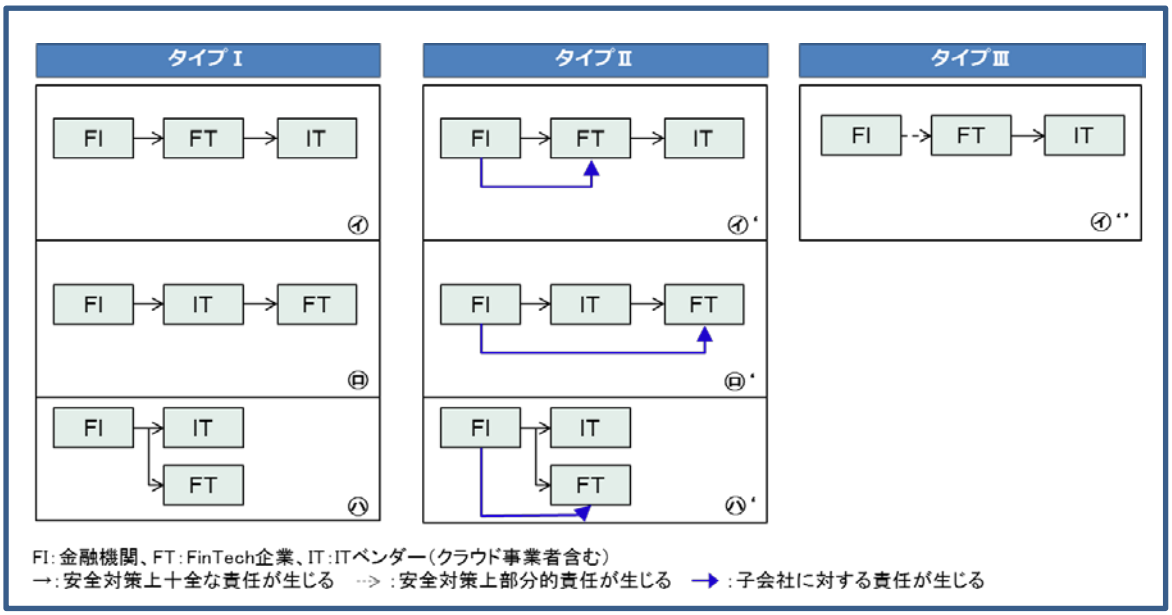


基本的人権の侵害といった広範な損失を被る可能性があることから、その取扱いには社会的・公共的な性質を有するもの」とされている。

（３）FinTech 業務タイプ別類型

以上の新たな関係者や業務形態の登場を踏まえると、本検討において前提とすべき、FinTech 業務のタイプ別の類型は以下のとおりとなると考えられる。【資料編資料３参照】

（図表２）FinTech 業務において安全対策実施上の関係者のタイプ別類型



タイプⅠは、外部委託関係として、３つの基本的類型となり、いずれも金融機関に安全対策上の十全な責任が生じる。タイプⅡはタイプⅠに、子会社に対する責任が付加されることで派生する類型である。タイプⅢは、タイプⅠと類似の類型だが、金融機関の安全対策上の責任が部分的となる。

以上の３タイプ７類型を前提に、従来の安対基準を適用した場合に内在する問題の有無について、具体的な検討を行う。

（４）FinTech 業務における安全対策の検討で考慮されるべき観点

問題の所在を明らかにするにあたり、そもそもどういう観点で問題を捉えるか、あらかじめ共有しておくことは有益である。

まず、本検討会の設立趣旨でもある「わが国金融機関が、FinTech において、システムの安全性を確保しつつも、顧客のニーズに適応しイノベーションの成果を最大限享受しうることを目指して」いくという観点が、考慮されるべきである。

そのうえで、FinTech 業務を実施するに当たって、様々な類型が展開されることが想定される中で、例えば、安対基準が特定の類型の採用にあたり抑制的な効果をもたらすことがないよう留意することが必要である。安対基準は情報システムを対象とした安全対策の基準であり、それ自体が、金融機関が様々に行うビジネスモデルの多様性を損なう

ようなことがあってはならない。仮に、特定の類型の採用に抑制的となる歪みがあるのであれば、問題として取り上げることが必要である。（安対基準の中立性）

一方で、金融機関に安全対策上の責任が生じる限りにおいては、その責任を果たすために、安全対策の実施に当たっては、その実現能力、すなわち、外部委託される場合は委託先や再委託先への統制能力が、十全に確保されることが必要となる。しかしながら、多岐にわたる FinTech 業務の類型においては、金融機関がその安全対策上の責任を果たすために必要となる統制能力が必ずしも十全に機能するとは限らない場合があるのであれば、問題として取り上げる必要がある。（安対基準の有効性）

次に、以上の、安対基準の中立性及び有効性といった観点は、必ずしも両立するものとは限らないことから、いずれの観点を優先させるべきか、あらかじめ、検討しておくことも考えられる。

仮に、中立性を優先させた場合には、多様なビジネスモデルを損なうことはなく、イノベーションの成果を享受し企業価値の最大化の実現に寄与することとなるものの、金融機関が顧客に対する安全対策上の責任を必ずしも果たせないこととなる懸念が生ずる。一方で、有効性を優先させた場合には、FinTech 企業や IT ベンダーに固有の負担を求める、あるいはそのビジネスの自由度を制約することが想定され、結果として FinTech 企業の革新性を損なうこととなる懸念が生ずる。

こうした中立性と有効性がトレードオフとなる問題は、多様な状況で発生すると考えられることから、あらかじめそのいずれを優先すると判断することは難しく、個々の状況に応じてケースバイケースで判断せざるをえないものと考えられる。

特に、簡易なリスクベースアプローチでは、従来の安対基準を適用した際に生じる個々の問題が明らかになった後に、中立性と有効性のいずれを優先させることが簡易なリスク管理策等を策定するに当たって妥当か、検討するのが適切であろう。

（５）「オープン API」との関係

タイプⅢの実現方法の１つとして「オープンAPI[14]」と通称される方法がある。「オープンAPI」では、FinTech企業と金融機関の合意に基づいて、情報システム相互をシステム的に接続することとなる。これによって、FinTech企業は、金融機関との多様な情報の結合と協調した安全対策が可能となり、顧客に対して、利便性が高くかつ安全なサービスを提供することが可能となる。

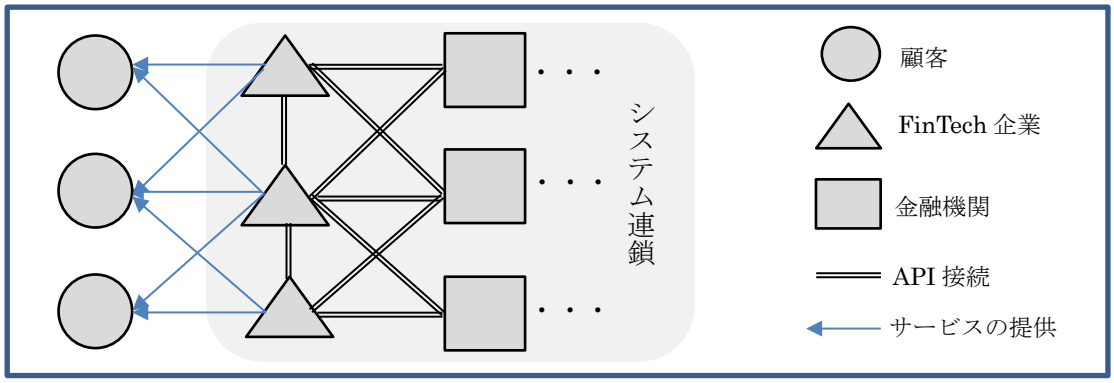
APIによる事業者間のシステム連鎖は、技術的には、多対多でかつ多段階にわたり重層的に可能である。したがって、金融機関のAPI公開により、金融情報システムの連鎖に多

[14] 金融審議会『金融制度ワーキング・グループ報告書』（平成 28 年 12 月 27 日公表）において「ここにおいて、API とは、銀行以外の者が銀行のシステムに接続し、その機能を利用することができるようにするためのプログラムを指し、このうち、銀行が FinTech 企業等に API を提供し、顧客の同意に基づいて、銀行システムへのアクセスを許諾することを、「オープン API」という」とされている。http://www.fsa.go.jp/singi/singi_kinyu/tosin/20161227-1.html

様な関係者が携わることとなれば、情報結合の種類も多様となり、その多様性によって、革新的なサービスの可能性が開かれる[15]。社会的には、このような「オープン・イノベーション」をもたらす環境を涵養していくことが期待されている。

一方で、システム連鎖に携わる関係者が多くなれば、その相互作用の中で、想定しなかったリスクが顕在化する可能性が高まると考えられる[16]。そのため、安全対策に関しては、相互作用等に対処するために、関係者が集合（collect）し多面的な検討を行うこと（以下「集合的な検討」という）が重要となる。

（図表３）オープン API におけるシステム連鎖関係



オープンAPIにおけるセキュリティの考え方に関する集合的な検討の１つとして、平成 28 年 10 月、一般社団法人全国銀行協会（以下「全銀協」という）を事務局、金融機関・IT関連企業・金融行政当局等をメンバーとする「オープンAPIのあり方に関する検討会」（以下「銀行API検討会」という）が設置された[17]。同検討会にはFISCもメンバーとして参加しており、本検討会は、銀行API検討会での議論[18]も参考にしつつ検討を行う[19]。

---

15 ネットワーク時代にオープン化がイノベーションをもたらすメカニズムについては、国領二郎『オープン・アーキテクチャ戦略　ネットワーク時代の協働モデル』（1999 年）が参考となる。

16 国領二郎『ソーシャルな資本主義　つながりの経営戦略』（2013 年）においては「多様な主体が発信する情報が結合する中から生まれる創発現象は、定義からいって完全にコントロールできるものではありません。しようとすると創発現象そのものが起こらなくなってしまいます」「特に多くのシステムをつないで連動させるようなときには、想定しなかったような相互作用の中で暴走が始まり事故が起こることを覚悟しておかなければなりません。そして、その対応策を考え続けることが、事故が起こった場合の被害を小さくします」とされている。

17 https://www.zenginkyo.or.jp/news/detail/nid/6752/

18 https://www.zenginkyo.or.jp/news/detail/nid/7670/　「オープン API のあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理（案）】」を以下「銀行 API 報告書」という。

19 その他にも平成 29 年３月から「クレジットカードデータ活用に係る API 連携に関する検討会」が経済産業省によって開催されており、クレジットカード会社や FinTech 業界代表者等が参加し、セキュリティ等の観点から、クレジットカード会社と FinTech 企業が満たすべき基準はどうあるべきか、等について検討を行うとされている。

Ⅱ　FinTech に関する安対基準適用上の課題と安全対策の在り方

１．課題検討に当たって明確にしておくことが有益な事項

（１）目標とすべき安全対策の効果の程度

安対基準の対象となる FinTech 業務を担う情報システムについて、金融機関と IT ベンダーに FinTech 企業を加えた３者関係を前提として検討することとなるが、どの程度の安全対策の効果を目標として検討を行うべきか、明確にしておくことは有益である。

顧客の立場に立てば、安全対策上の関係者が変わろうと、安全対策の効果が同程度で確保されることが期待されていると考えられる。したがって、FinTech 企業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、従来の安対基準において実現される２者関係における安全対策の効果と比較して、同程度となるよう留意することが重要である（以下「同等性の原則」という）。

また、２者と３者で同程度の安全対策の効果の実現を目指す場合、中立性及び有効性といった観点から、従来の安対基準に対する調整は必要十分な範囲にとどめることが重要である。すなわち、その調整によって、金融機関及び IT ベンダー等の負担が必要な範囲を超えて増加することが無いよう留意することが重要である。

（２）安対基準における検討対象領域

従来の安対基準には、「コンピュータシステムが収容される建物、設備」を対象とした設備基準及び「ハードウェア、ソフトウェア等」を対象とした技術基準のようにモノを対象とした基準と、開発・運用管理体制等を対象とした運用基準のようにヒトを対象とした基準があり、いずれの基準を主に検討の対象とするか、明確にしておくことは有益である。

モノを対象とする設備基準や技術基準[20]は、今後、多岐にわたるFinTechの出現が予想される中では、個別具体的な技術を前提として安全対策を特定することは困難であり、また、FinTechをめぐる環境が変化する中、個々の安全対策を確定的に設定することも適切ではない。そのため、設備基準や技術基準に関しては、金融機関において、個々のFinTech業務のリスク特性に応じた安全対策が独自に決定され、「安全対策における基本原則[21]」にしたがってITガバナンスが行われていれば十分である。

一方、ヒトを対象とする運用基準は、多岐にわたる FinTech の出現に際しても、その多種多様な技術等に左右されることなく適用可能なものと考えられることから、本検討においては、運用基準を主として対象とすることが適切である。

また、FinTech 業務は、金融機関の FinTech 企業に対する外部委託という形態で実現される場合があることから、運用基準の中でも、外部委託に関する基準を主な対象とし

[20] 技術基準の中には、技術変化の影響を受けやすい部分とそうでない部分が混在していることに留意が必要である。
[21] FISC『外部委託検討会報告書』で提言された、リスクベースアプローチを踏まえた４原則のこと。

て検討することが適切である。

（３）簡易なリスク管理策の性質

簡易なリスク管理策の検討に当たっては、その性質をあらかじめ明らかにしておくことが有益である。

簡易なリスク管理策は、まず重要な情報システムに対する統制が設定されていることを前提として、その統制を、一般の情報システムに対しては、緩和することで導出されるものである。その反面、「必要最低限の基準[22]」と表現されるとおり、「最低限ここまでは実施しておくべき」という拘束性も有している。

そのため、簡易なリスク管理策の設定が不適切であると、中立性や有効性を損なうのみならず、恒常的に、過度な安全対策あるいは不十分な安全対策を招来することとなることから、その検討に当たっては、FinTech 企業をはじめとする関係者が、個々の情報システムの現場で直面している、安全対策に関する問題認識が正しく反映されるよう留意するとともに、慎重な検討が行われることが重要である。

（４）クラウドサービスの利用に関する安対基準の取扱い

FinTech 企業においては、IT ベンダーの中でも、クラウド事業者に情報システムの運用を委託することが多いと言われていることから、あらためて、安対基準において「クラウドサービスの利用」に関する基準が、どのように位置づけられるか、確認にしておくことが有益である。

まず、安対基準において、クラウドサービスは外部委託の一形態として捉えられている[23]。さらに、「クラウドサービスの利用」に関する安対基準は、今後、クラウドサービス固有の内容等を除いたうえで外部委託全般の基準として参考としていくこととなっている[24]。こうした安対基準の改訂は、外部委託検討会及び本検討会の成果も踏まえて行われることとなっている[25]ため、現時点では、こうした整理が行われた後の外部委託の安対基準（クラウドサービスを含む）として、確定的なものは存在しないことに留意が必要である。

そのため、本検討会において、検討を行うのに必要な範囲で、暫定的に従来の安対基準のうち外部委託に関する基準の概要を明確にすることが必要である。

次に、「クラウドサービスの利用」に関する安対基準の前提となった FISC「金融機関

---

[22] FISC『外部委託検討会報告書』において、「必要最低限の安対基準の意義」について「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。」としている。また、「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。」としている。

[23] 安対基準の運用基準「（XIV）クラウドサービスの利用」において、「クラウドサービスの利用にあたって、（中略）外部委託管理の考え方に沿って、適切なリスク管理を行うことが必要である。」としている。また、FISC『外部委託検討会報告書』５．外部委託の概念において、クラウドは外部委託の範囲に含まれるものとして整理されている。

[24] FISC『外部委託検討会報告書』脚注 31 において、「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。」としている。

[25] FISC『外部委託検討会報告書』において、「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。」としている。

におけるクラウド利用に関する有識者検討会」（以下「クラウド検討会」という）報告書は、その後続の検討会である外部委託検討会報告書で提言された「重要な情報システムの意義」を踏まえているとは必ずしも言えないため、クラウド検討会報告書のリスク管理策が、「重要な情報システム」においてもそのまま適用可能か、不確実性が残る現状にある。

簡易なリスク管理策が、重要な情報システムに対する管理策をもとに、その統制の程度を緩和することで導出されることに鑑みれば、こうした事情にも留意することが望ましい。

以上の留意事項を解決するため、本検討会において、クラウドサービスを利用する場合の管理策について、外部委託検討会報告書の成果を踏まえて、補足的な検討を行う。これにより、重要な情報システムでクラウドサービスを利用した FinTech のユースケース（ブロックチェーン・AI 等）が登場した際にも、その前提が明確化されていることとなる。

２．　従来の安対基準に基づく関係者の責務

（１）関係者の責務

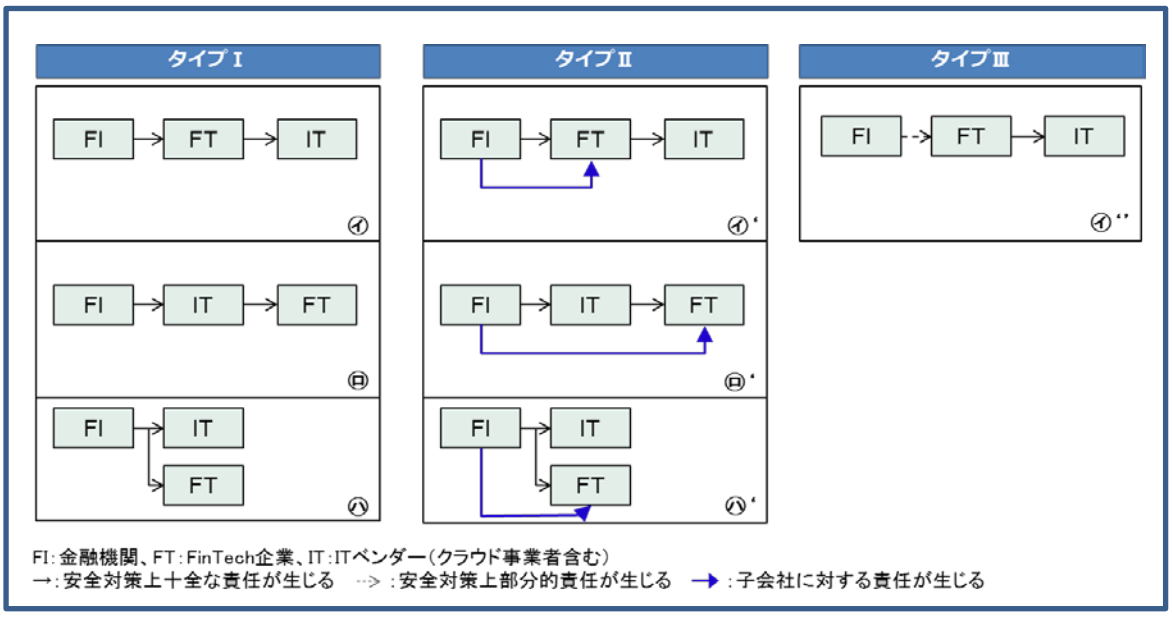
まず、内在する問題を検討するにあたり、「従来の安対基準の概要（外部委託関連）」を、タイプⅠの３者関係に置き直して整理を行った。【資料編資料４参照】

整理に当たっては、安全対策実施上の関係者それぞれの責務を以下のとおり分類している。

- 外部委託利用時の金融機関の責務　　・・【責務Ａ】
- 一次委託先の責務　　・・【責務Ｂ】
  - 金融機関の一次委託先として負う責務・・【責務Ｂ－１】
  - 金融機関の再委託先に対する責務　　・・【責務Ｂ－２】
- 金融機関の再委託先として負う責務　・・【責務Ｃ】

関係者が以上の責務を適切に果たすことで、FinTech においても安全対策の効果が実現できるが、その場合に内在する問題は、新たな関係者となる FinTech 企業において、具体的に認識されることから、FinTech 企業の責務に着目し、㋑㋺㋩のタイプ別類型で整理すると、次のとおりとなる。

（図表４）FinTech 業務において安全対策実施上の関係者のタイプ別類型



（図表５）FinTech 企業の責務例

【㋑の類型】

【責務Ｂ－１】金融機関の一次委託先として負う主な責務		注
a.利用検討時	金融機関が客観的評価を実施するために必要とする情報を、金融機関に提供する責務	3
	金融機関にデータの所在に関する情報を提供する責務	7
b.契約締結時	機密保護や安全な作業の遂行等を契約として、金融機関と締結する責務	11
	金融機関による再委託先への監査権を明記する責務	14
	金融機関が再委託先の事前審査を行うことに対応する責務	25
d.運用時	金融機関からデータ管理を受託する場合、漏洩防止策を講じる責務	28
	記憶装置の故障等により、機器・部品を交換する場合には、データ消去を含めた十分な管理を行う責務	29
	金融機関からの日常的監視を受忍する責務	30
	金融機関からシステムに関する総合的な監査・評価を受忍する責務	31
【責務Ｂ－２】金融機関の再委託先に対する主な責務		注
a.利用検討時	金融機関の再委託先を客観的に評価する責務 【簡】公開情報や業界における評判や実績等による評価でも可能	3
	データの所在を把握する責務 【簡】データの所在の把握について省略することも可能	7
b.契約締結時	機密保護や安全な作業の遂行等を契約として、金融機関の再委託先と締結する責務	11
	金融機関による再委託先への監査権を明記する責務 【簡】監査権を明記しないことが可能	14
	再委託先に対して適切な事前審査を行う責務	25
d.運用時	再委託先に金融機関のデータ管理を委託する場合、漏洩防止策を実施させる責務	28
	記憶装置の故障等により、機器・部品を交換する場合には、データ消去を含めた十分な管理を行わせる責務 【簡】消去・破壊プロセスの実効性を検証することで代替可能	29
	再委託先を日常的に監視する責務	30
	再委託先に対してシステムに関する総合的な監査・評価を行う責務 【簡】第三者認証等を活用することで代替可能	31

【㋺の類型】

【責務Ｃ】金融機関の再委託先として負う主な責務		注
a.利用検討時	IT ベンダーが客観的評価を実施するために必要となる情報を、IT ベンダーに提供する責務	3
b.契約締結時	機密保護や安全な業務の遂行等を契約として、IT ベンダーと締結する責務	11
	金融機関による監査権を明記する責務	14
d.運用時	IT ベンダーからの日常的監視を受忍する責務	30
	IT ベンダーからシステムに関する総合的な監査・評価を受忍する責務	31

【㋩の類型】

【責務Ｂ－１】金融機関の一次委託先として負う主な責務		注
a.利用検討時	金融機関が客観的評価を実施するために必要とする情報を、金融機関に提供する責務	3
b.契約締結時	機密保護や安全な作業の遂行等を契約として、金融機関と締結する責務	11
d.運用時	金融機関からの日常的監視を受忍する責務	30
	金融機関からシステムに関する総合的な監査・評価を受忍する責務	31

【簡】…既に策定されている簡易なリスク管理策　　注　…【資料編資料４】の通番を記載

（２）内在する問題へのアプローチ

以上の整理を踏まえて、従来の安対基準（外部委託関連）を FinTech 業務に適用した場合に内在する問題を検討するに当たっては、以下のアプローチで、タイプ別に検討を行う。

- タイプⅠの場合、従来の安対基準を適用することで、問題が生じることはないか。
- タイプⅢの場合、そもそも従来の安対基準を適用することが、妥当であるか。

なお、タイプⅡについては、タイプⅠに異なる責任が付加される類型であることから、個別に検討を行う。

３．タイプⅠにおいて内在する問題と安全対策の在り方

タイプⅠにおいて、FinTech 企業は、【責務Ｂ】あるいは【責務Ｃ】を担うこととなる。そもそも、従来の安対基準では、金融機関と IT ベンダーの２者を念頭に置き策定されてきたことから、【責務Ｂ】あるいは【責務Ｃ】は、IT ベンダーの安全対策遂行能力を念頭において策定されてきたものである。

したがって、【責務Ｂ】あるいは【責務Ｃ】を、FinTech企業が担う場合には、FinTech 企業の安全対策遂行能力[26]（保有する経営資源等）と比して、バランスを欠いたものとなっていないか、という問題が内在している。

そのため、FinTech 企業に対して、IT ベンダーに求めてきたものと同様の安対基準の適用を、形式的に求めた場合、安全対策遂行能力が IT ベンダーと同程度でない FinTech 企業においては、安全対策負担を過大とし、その負担を回避するインセンティブが生じることとなり、その結果として、FinTech 企業のビジネスモデルの選択に、歪みを与える可能性がある（中立性の観点）。あるいは、FinTech 企業が、過大な安全対策負担になんとか応えようとした場合、その結果として、内部の経営資源を安全対策に優先的に配分することとなり、そのイノベーションを損なう可能性がある（イノベーションの成果を享受する観点）。

一方で、FinTech 企業が加わる３者関係の場合であっても、その安全対策の効果は、従来の２者関係における安全対策の効果と比較して、同程度とすべきという考え方（同等性の原則）に立てば、単に、金融機関が、FinTech 企業の負担を、その安全対策遂行能力に見合う程度で十分として残存リスクを受容する、あるいは、FinTech 企業の安全対策遂行能力に合わせて、リスク管理策を調整することでは、本質的な問題は解決しない（有効性の観点）。

そもそも、金融機関は、企業価値の最大化を目指して、FinTech 企業の革新的な性質をみずからの業務で利用すべく外部委託を行うのであって、必ずしも FinTech 企業に IT ベンダーの役割を全面的に代替させるために外部委託を行うわけではない。

したがって、まず、金融機関は、FinTech 企業の安全対策遂行能力を確認したうえで、仮に FinTech 企業の能力を超える過大な責務があれば、その部分については、金融機関や IT ベンダーが分担することで、FinTech 企業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配慮して、取り組んでいけばよい。

すなわち、この問題を解決するには、２者関係を念頭に置いた従来の安対基準において求められる責務の総体を維持しつつ、その責務を、３者の各類型における役割や３者の安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分しうることを、明示的に認めることが適当である。

---

[26] 安全対策遂行能力のうち基礎的な部分は、安全対策に係る内部統制を実質的に機能させることができる能力であり、例えば、安全対策上の問題があればみずからそれを特定し、みずからそれに対処し、さらに、問題の抽出と対処という改善活動を、みずから継続的に実施できる能力である（安全対策の PDCA サイクルを十全に機能させられる能力）。こうした安全対策遂行能力の基礎的な部分は、金融関連サービスを担う FinTech 企業においても、最低限求められるべきものである。したがって、安全対策遂行能力とは、ある時点において、個別の安全対策を実施済みであるといった、形式的に確認できる状態のことを必ずしも意味しない。

なお、責務の再配分に際しては、責務を負担可能な関係者が複数いる場合は、安全対策における社会的な費用の最小化の観点から、追加費用負担が少ない者に責務を再配分することが望ましい[27]。

（再配分ルール）【資料編資料５参照】

金融機関、ITベンダー及びFinTech企業は、３者の合意の上、従来の安対基準における外部委託の責務を、３者で再配分[28]することが可能である[29]。
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。なお、追加負担費用が少ない関係者に責務を再配分することが、安全対策における社会的な費用の最小化に資することとなる。

なお、以上のルール及びサブルールは、タイプⅠ以外の類型や「重要な情報システム」においても妥当な考え方である。

４．タイプⅢにおいて内在する問題と安全対策の在り方

（１）金融機関の安全対策上の責任

タイプⅢは、FinTech 企業が金融関連サービスを主導する形態であり、金融機関とFinTech 企業の関係は、必ずしも外部委託と特徴づけられる形態に留まらない多様な形態を取りうる。そのため、タイプⅢでは、金融機関と FinTech 企業の関係が、外部委託に留まらない幅広い形態になった場合でも柔軟に対応しうるような、安全対策の在り方を検討する必要がある。

これについては、金融機関と FinTech 企業の関係がいかなる形態となるにせよ、金融機関の立場から FinTech 業務の実質的な内容をみれば、外部委託と共通する要素が見出される可能性が高い。他方で、従来の安対基準において、外部委託に関する基準は、環境変化等に応じて見直され、完備されてきたのに対して、それ以外の形態については、必ずしも明示的な基準は存在していない。したがって、タイプⅢにおける安全対策の在り方として、基本的には外部委託の基準を「準用」することとし、それでは対応できない個別の事情がある場合に、必要に応じて修正を行うことが妥当である。

次に、外部委託基準の準用を考えるに当たっては、そもそも、外部委託の基準には、

---

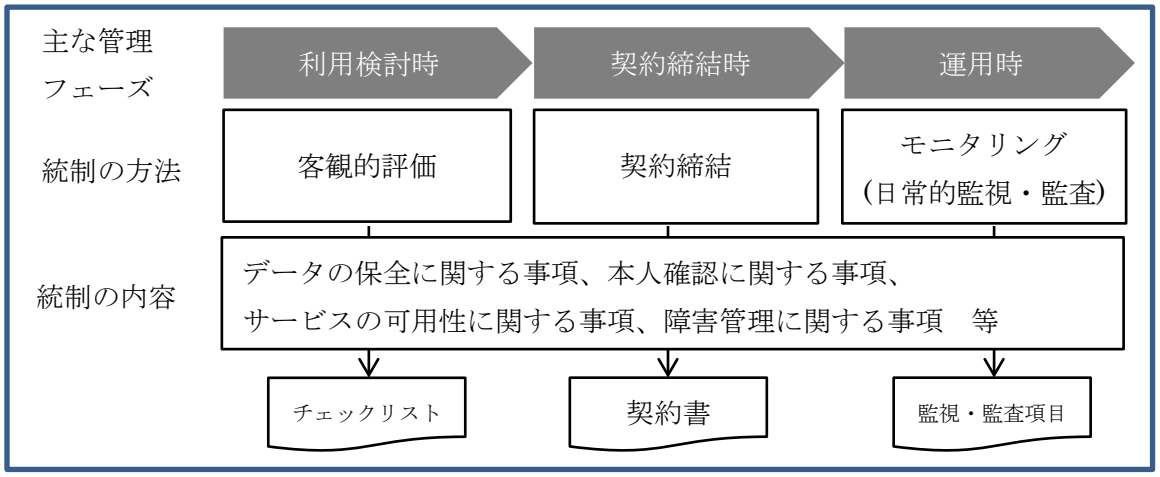
[27] また、責務の再配分に際して、関係者にモラルハザードが生じることが懸念される。例えば、金融機関が再配分を受入れることが明らかとなれば、FinTech 企業には、安全対策への投資を意図的に抑制するフリーライダーの指向が生まれる。このような関係者のモラルハザードを抑止するためには、責務を負担した関係者に応分の利益が還元される公正なスキームを、関係者であらかじめ合意しておくことが考えられる。

[28] 例えば、３者契約により、金融機関が、FinTech 企業に代わって、IT ベンダーを統制する【責務Ｂ－２】の一部を担うことで、金融機関みずからが IT ベンダーに統制を行うことが考えられる。

[29] FinTech 企業の規模や業態は多様であることから、責務の再配分の分担内容をあらかじめ確定的に定めることは適切ではない。金融機関は、外部委託を行う FinTech 企業や IT ベンダーの実態に応じて、合理的に、その分担内容を、区々に決定すれば十分である。あるいは、分担内容の見直しありきではなく、FinTech 企業がその安全対策上の責務を果たせるように、金融機関が研修等の支援を行うことも考えられる。

利用検討時・運用時等の管理フェーズにおける客観的評価・モニタリングの実施といった「統制の方法」に関する基準と、データ漏洩防止対策としての暗号化の実施といった「統制の内容」に関する基準があることに留意が必要である。

（図表６）統制の方法と内容



準用に当たっては、まず、統制の方法に関しては、金融機関に何らかの安全対策上の責任が生じる限りにおいては、程度の差こそあれ、外部委託と同様に実施されるべきものと考えられる。

（図表７）タイプⅢにおける金融機関の関心項目例（【責務Ａ】から統制の方法を抜粋）

a.利用検討時	客観的評価の実施	3
	FinTech 企業は、金融機関が有する安全対策上の管理責任と同等の責任を果たしうるか。あるいは、金融機関が FinTech 企業に求める管理責任を果たしうるか。例えば、FinTech 企業は、安全対策において必要となる安全対策遂行能力（保有する経営資源等）を有しているか。	
b.契約締結時	安全対策を盛り込んだ契約の締結	11
	FinTech 企業は、金融機関と安全対策を盛り込んだ契約を締結するか。また、FinTech 企業は、IT ベンダーと安全対策を盛り込んだ契約を締結しているか。 （例えば、データ漏洩時の通知や損害賠償等の取決め等）	
d.運用時	日常的監視	30
	FinTech 企業は、金融機関に対して、安全対策の実行状況を報告することが可能か。	
	システム監査体制の整備	31
	FinTech 企業は、監査・評価を受忍するか。	

注　…【資料編資料４】の通番を記載

一方で、統制の内容に関しては、安全対策上の責任が生じる部分についてのみ実施されれば十分と考えられる。金融関連サービスをFinTech企業が主導する場合においては、金融機関の安全対策上の部分責任は、顧客に関するデータの提供または受入れに由来することから、金融機関の統制の内容は、FinTech企業が提供したデータを適切に管理しているか、またはFinTech企業から受入れたデータが顧客の指示に基づくものであることを、FinTech企業が適切に確認しているか、という部分に集中することとなる。

以上のとおり、タイプⅢにおいて、金融機関がFinTech企業へデータを提供する、またはデータを受入れる際に負う責務は、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。

なお、タイプⅢにおいて、顧客に関するデータの保全または本人確認に係る部分以外の項目（例えば、システムの安定稼働等）については、金融機関の関心の外であり、金融機関の立場からは、特段の統制の必要は生じない。ただし、金融機関の関心外となった結果、全体として統制の程度が低下し、データの保全または本人確認に係る安全対策の効果が得られない場合は、金融機関は、FinTech企業に対して、何らかの付加的な統制を講ずる必要があることに留意が必要である。

（外部委託基準の準用ルール）

タイプⅢにおいて、金融機関は、従来の外部委託の基準を準用することが可能である。その場合、金融機関の責務は、FinTech企業における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。
なお、金融機関の責務以外の部分に由来して、金融機関の責務部分の安全対策の効果が得られない場合は、付加的な安全対策を講ずる必要がある。

（２）FinTech企業に残る安全対策上の責任

タイプⅢにおいては、FinTech企業は、情報システムの運用をクラウド事業者をはじめとしたITベンダーに委託して実施することが一般的である。したがって、外部委託の基準の準用という観点では、FinTech企業は、金融機関から求められる責務と一体不可分な形で、【責務Ａ】の一部を担うことが、社会的には期待される。

さらに、FinTech企業は、みずからが主導して金融関連サービスを提供していることから、外部委託にとどまらず、サービス全般において、適切な安全対策を実施することが、社会的には期待されている。

したがって、FinTech企業において、例えば、安対基準と整合的に業界の自主的基準が策定されること等を通じて、主体的に安全対策に関する取組みが進められることが期待される。（「Ⅲ　安対基準の対象外となるFinTech業務の取扱い」において詳述）

（３）金融機関に責任が生じない場合の取扱い

FinTech 企業が主導し、かつ、金融機関と何ら交渉を行うことなく、一方的に金融機関から顧客に関するデータを取得するような金融関連サービスにおいては、金融機関には安全対策上の責任は生じないと解することとなる。

しかしながら、顧客の立場に立てば、こうした金融関連サービスを利用した場合には、何か問題が発生しても金融機関に頼ることができない、といった事態となることから、金融機関は、みずからの顧客に対して、「一方的に金融機関から顧客に関するデータを取得するような金融関連サービス」を利用する場合の留意事項について、あらかじめ、注意喚起を行っておくことが望ましい。

５．関係者間の協調

上記検討から明らかなように、FinTech 業務における適切な安全対策の実施には、金融機関、IT ベンダー及び FinTech 企業の３者が、密接に協調することが不可欠であり、これを欠いた場合には、利用者に不測の損害をもたらすおそれがある。

こうした協調の最も中心的な部分は、利用検討時やインシデント発生時等、それぞれの管理フェーズにおいて、FinTech 企業から金融機関に対して、情報（システムリスクに関するものを含む）が適切に開示されることにあるが、他方で、これを FinTech 企業に対して必要な範囲を超えて求めれば、FinTech 企業に過度な負担を強いることとなり、そのイノベーションを損なうことにもなりかねない。

したがって、安全対策に係る情報開示が協調して適切に行われるよう、あらかじめ３者間で、合意をしておくことが望ましい。（協調の原則）

また、協調の手段として、外部委託先評価時に使用されるチェックリスト[30]を活用することが望ましい。そのためには、例えば、従来使用しているチェックリストを、協調を促すための情報共有手段としても位置付け、簡素化も含め内容を見直すことが考えられる。

FinTech 業務に携わる金融機関、IT ベンダー及び FinTech 企業の３者は、いずれの類型であったとしても、システムの安全性の確保とイノベーションの成果の享受を両立させるべく、密接に協調しながら、安全対策に取り組むことが必要である。

[30] 従来の安対基準においては、外部委託の利用検討時に「外部委託先を客観的に評価すること」とされており、実際の評価に当たって、金融機関は、システムリスクを含む外部委託全般に係るリスクを評価する汎用的なチェックリストを利用するのが一般的である。利用に当たっては、例えば、チェックリストを外部委託先に手交し自己チェックを依頼した後に、自己チェック結果に基づいてヒアリングを行う等の方法が取られる。

６．タイプⅡの特性を踏まえた補足的検討

上記検討を踏まえたうえで、派生形であるタイプⅡが、安全対策上どのような特性を有するか、また、どのような補足が必要か、個別に検討を行う。

（１）タイプⅡの特性

一般的に、金融機関は、子会社に対して、当該子会社の金融グループ経営上の位置づけや役割、あるいは規模等に応じて、個別の経営管理契約を結んだうえで、管理・統制を行っている。例えば、リスク管理状況のモニタリング等を通じて助言・指導を恒常的に行う、あるいは、重要事項の報告義務を定めること等を通じて情報の適時適切な把握を行っている。したがって、FinTech 企業に対して子会社に対する責任も生じるタイプⅡでは、外部委託先に対する統制に加えて、こうした子会社に対する統制が付加されることとなる。

これにより、統制面においては、タイプⅡは、他タイプと比較して、統制の接点が多く、かつ実効的な情報開示も担保されている場合があり、FinTech 業務において目指されるべき「関係者間の協調による適切な安全対策の実施」が、金融機関と FinTech 企業の両者において、比較的円滑に可能となると考えられる。

一方、タイプⅡは、経営資源配分面においては、客観的評価の結果、FinTech 企業の安全対策遂行能力が十全でなく、かつ安全対策に追加的に配分可能な経営資源がない場合には、責務の再配分という方法だけでなく、増資や人材の派遣等を通じて、FinTech 企業の経営資源を補強することも選択することが可能となる。

以上のことから、統制と経営資源配分の両面から、タイプⅡは、金融機関及び FinTech 企業にとって、システムの安全性を確保しつつイノベーションの成果を享受するという目的に対して、一つの解決策を提供する類型であると考えられる。

（２）補足

金融機関の内部では、経営管理と外部委託管理が、異なる窓口部署・管理項目・管理周期で行われる場合がある（図表８参照[31]）。そのため、FinTech企業においては、同一金融機関とのやりとりであるにも関わらず､別個の対応を求められる場合も想定される。これは、FinTech企業において負担となる局面も予想されることから、負担を求めることがイノベーションを損なう可能性がある場合は、経営管理と外部委託管理を行う部署間で連携をして、FinTech企業に過度な負担が生じないよう注意を払うことが望ましい[32]。

---

[31] ここでは、図表８として、システム子会社の例を取り上げているが、これはシステム子会社と FinTech 企業で、全く同様の経営管理あるいは外部委託管理が行われるべきと意図しているわけではない。FinTech 企業に対しては、金融グループ内での位置付け等実態に応じて、金融機関において区々の管理が行われるものである。

[32] なお、金融機関においては、経営管理と外部委託管理は、それぞれ異なる観点から行われており、どちらかを省略できるというものではない。また、図表８にあるとおり、既に管理の効率化に関して様々な工夫も行われている。

（図表８）経営管理と外部委託管理の実態調査（システム子会社の例）　※１

経営管理			外部委託管理		
窓口部署	管理項目例	管理周期	窓口部署	管理項目例	管理周期
経営企画部門 ／ システム企画部門	重要事項の決定の事前承認 ・株主や役員の変更 ・大規模システム投資 等 事業計画の実施状況の把握 リスク管理状況の把握 ・リスク管理規程 ・大規模システム障害の発生 等	※2	リスク管理部門 ／ システム担当部門	再委託管理状況の把握 ・新規再委託先の事前審査 ・再委託先管理状況の把握 等 委託業務の実施状況の把握 ・作業実績 ・本番データ利用実績 等 システムリスク管理状況の把握 ・システムリスク評価結果 ・システム障害と分析結果 等	※2

※1　システム子会社を傘下に保有する複数の銀行に対して調査を実施した。

※2　管理項目によって都度もしくは定期に実施されているが経営管理と外部委託管理で必ずしも同一ではない。

【管理の実効性・効率性を向上させる工夫】

親会社と子会社が同一の建物に入居している。

親会社による研修を実施している。

拠点内再委託先は定例報告を省略している。

親会社と子会社で規定を共通化している。

メール等のシステムを親会社と共通化している。

等

７． FinTech 業務を担う情報システムの安全対策上の取扱い

本検討会では、FinTech業務を担う情報システムは、当初は、一般の情報システムである場合が大半であると想定して検討を行ってきた。しかしながら、FinTech業務を担う情報システムにおけるリスクの顕在化が、重要な情報システムが提供するサービスに重大な影響を及ぼす場合[33]には、FinTech業務を担う情報システムを重要な情報システムと一体とみなして、安全対策上取り扱うことが必要となる。

他方で、個々の情報システムの対象範囲は、金融機関において独自に判断されることから、FinTech 業務を担う情報システムにおけるリスクの顕在化が、重要な情報システムが提供するサービスに重大な影響を及ぼさないにもかかわらず、一体として、安全対策上取り扱われる可能性がある。

その場合、リスクの高いシステムに引きずられて、FinTech 業務を担う情報システムにも「高い安対基準」の適用を求めざるをえないと判断される可能性があるとともに、その影響を受けて、金融機関の FinTech 業務への取組みそのものが抑制的となる懸念がある。

イノベーションの成果を享受する観点からは、こうした問題にあらかじめ対処しておくことが望ましく、そのためには、以下の要件をすべて充足する情報システムを、「分離可能なサブシステム」として、独立して取り扱うことが可能であることを、明確にすることが考えられる。

（１）リスク顕在化時の影響の分離可能性

サブシステム内で発生したシステム障害等のリスク顕在化の影響を、システム全体が提供するサービスに波及させないことが可能であること。

（２）リスク特性の分離可能性

システム全体のリスク特性と比較して、サブシステムのリスク特性が顕著に異質であること。

（３）リスク管理の分離可能性

リスク評価、安全対策、リスク顕在化後の事後対策といったリスク管理を当該サブシステム内で完結して実施することが可能であること。

金融機関は、以上の考え方に留意しつつ、FinTech 業務を担う情報システムの安全対策上の取扱いを検討することが望ましい。

[33] 例えば、金融機関が、窓口を持たず、決済指図受入れ手段として、FinTech 企業との API 接続以外に手段が無い場合には、API 接続を行うシステムが停止すると、勘定系基幹システムが停止していなくても、結果として決済サービス自体が停止することとなる。

Ⅲ　安対基準の対象外となる FinTech 業務の取扱い

１．安対基準における従来の対象の取扱い

安対基準の対象となる情報システムは、金融業務を担う情報システムであり、かつ、その安全対策について金融機関等に責任が生じる情報システムである。これは、簡単に言えば、「金融機関が行う金融業務」を担う情報システムである。したがって、「金融機関が行う非金融業務」「非金融機関が行う金融業務」「非金融機関が行う非金融業務」を担う情報システムは、安対基準の直接的な対象とはならない。

ただし、「金融機関が行う非金融業務」を担う情報システムについては、同一金融機関の運営する情報システムであり、かつ、「安全対策に係る方針」のもとで、共通する安全対策も多いと想定されることから、金融業務の性質を前提とした安対基準をそのまま全面的に「適用」することは適切でないとしても、安対基準のうち非金融業務を担う情報システムの安全対策においても有益な部分については「参考」とする、すなわち、金融機関の業務の実態に即して適宜取り入れることが望ましい、という考え方に立っている[34]。

一方、「非金融機関の行う金融業務」（例えば非金融機関が行う資金決済法上の前払い式支払手段や資金移動といった業務）は、「金融機関の行う金融業務」と機能的に類似する部分があり、安対基準の安全対策が部分的に有益となることは否定できないにしても、以下の経緯から、その業務を担う情報システムは対象とされていないとするのが、従来からの考え方である。

- 安対基準は、FISC会員によって策定される自主基準である。一般的に、自主基準とは、「国家等によって明確に規定され、裁判所などを通じて強制的に執行される法律」（ハードロー）と異なり、「私的な取決めや申し合わせ」（ソフトロー）[35]の一種であり、その社会的規範性は、自主基準の策定過程に明示的に参画した当事者においてのみ生ずるものと解される。安対基準はその会員である金融情報システムを担う当事者[36]の中でも金融機関を中心に策定されており、その策定過程[37]に「金融業務を行う非金融機関」の業界代表等は、必ずしも明示的に参画していない。そのため、そうした非金融機関を、一方的に安対基準の適用対象とすることには無理がある。
- 安対基準は、金融庁の検査マニュアル等において言及されることにより、FISC 会

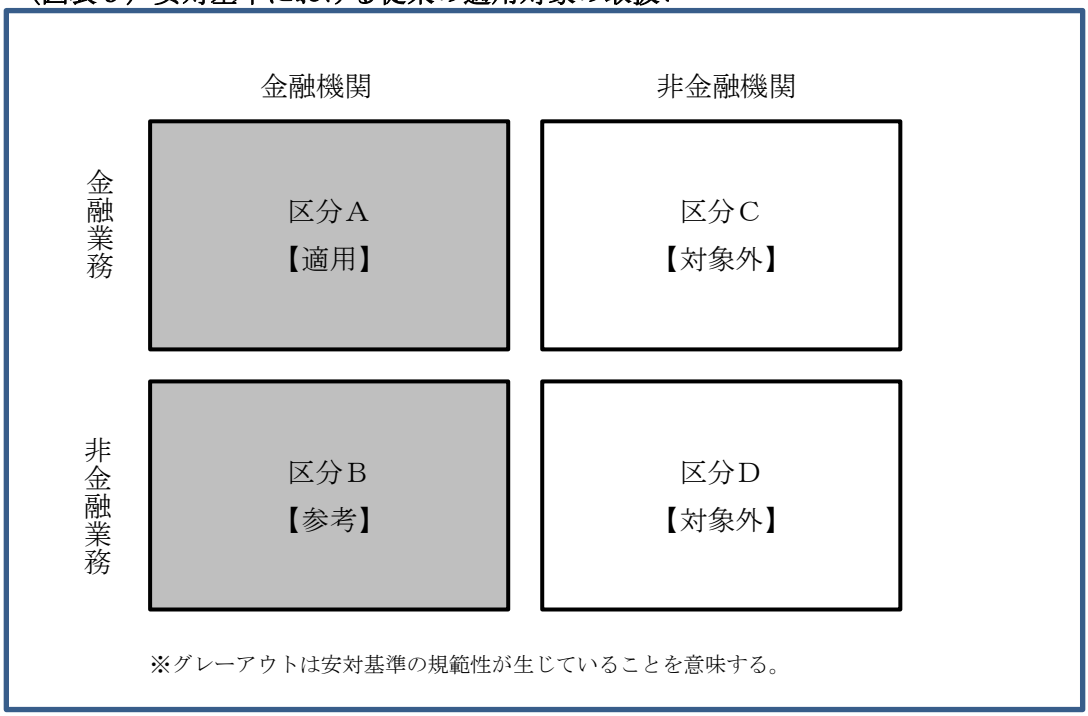
34 脚注４を参照。
35 ソフトローとハードローの説明については、中山信弘編集代表『ソフトローの基礎理論』（2008 年）中の第３部第１章瀬下博之『ソフトローとハードロー』から引用。
36 平成 29 年３月末現在、FISC 会員数 644 社のうち金融機関は 542 社と、その 84%を占める。
37 安対基準は FISC 会員代表者を中心に構成される安全対策専門委員会とその下部組織である安全対策基準改訂に関する検討部会で検討を行った後、会員への意見募集を経て策定される。

員の枠を超えて、金融庁監督下の金融機関が、事実上適用対象とされているが、その範囲を超えて、金融庁監督下に無い非金融機関まで適用対象とすることには無理がある。

なお、「非金融機関の非金融業務」を担う情報システムは、安対基準の対象と考えられたことはない。

以上の考え方を図表にすると以下のとおり。

（図表９）安対基準における従来の適用対象の取扱い



２．安対基準の対象外となる FinTech 業務の取扱いの方向性

FinTech と総称される金融関連サービスは多岐にわたるとともに、今後も新しいテクノロジーあるいは新しいビジネスモデルの登場が予想される中では、そうした状況を踏まえて、FinTech 業務の安対基準における取扱いについて、本検討会において、あらかじめ整理しておくことが期待されている。

一般的に、金融機関と非金融機関は、業法等の法規制に基づいて主体が特定され、比較的対象が明確であるのに対して、FinTechと総称される金融関連サービスにおいては、金融業務と非金融業務の境界が比較的曖昧となるという特徴があるとされている[38]ことから、例えばその機能面に着目して、個別具体的に業務を特定することで、金融業務と非金融業務

[38] 例えば、増島雅和／堀天子編著『FinTech の法律』（2016 年）において、「FinTech による業界構造や事業モデルの変化は、金融の業態間の壁を融解するだけでなく、金融と非金融の間の壁をも溶かすことにつながる。」とされている。

の区分の境界を明確にするというアプローチが考えられる。

しかしながら、このアプローチにおいても、多岐にわたるサービスが登場する中で、あらかじめ業務を個々に特定することは困難であり、また、仮に境界が明確にできたとしても、業務の機能面では大差が無いにも関わらず、安対基準上の取扱いが異なることとなり、その FinTech 業務の取扱いの適切性に疑義が生ずることが危惧される。

本来、利用者の立場に立てば、金融業務であるか否かは一義的な問題ではなく、また、金融機関と非金融機関のいずれが行う場合においても、FinTech 業務全体において、シームレスに一体不可分な形で、適切な安全対策が実施されることが期待されている、と考えられる。

したがって、こうした社会的期待に応えるためには、まず、わが国の金融機関が、従来からその業務において培ってきた社会的な信頼と、類似の信頼を FinTech 業務においても得ることが有益である。特に、情報システムにおける社会的信頼が形成されるに当たっては、社会的に合意されたルールである安対基準が役割として担ってきた一面があることから、多様な FinTech 業務の実態を所与の前提としたうえで、金融機関と非金融機関に関わらず、それらの業務の担い手において、いかに安対基準の社会的規範性が生じることが可能か、という観点から、整理することが有益である。

（１）区分Ｂの取扱いの方向性

本区分においては、従来から安対基準は「参考」という形で言及されてきており、金融機関の実態においても、セキュリティポリシーやセキュリティスタンダードにおいて、安対基準等のFISCのガイドラインが取り入れられ、金融業務と非金融業務に対して、一体的に安全対策が実施されているケースが多い[39]。

したがって、FinTech 業務のうち、非金融業務とみなされる業務があった場合においても、FinTech に関する安対基準が整備されれば、従来どおり、これらの基準を「参考」として、安全対策が実施されることとなり、特段新たに検討すべき問題はない。

（２）区分Ｃ・Ｄの取扱いの方向性

本区分においては、FinTech 業務のうち非金融機関が行う金融業務としては、例えば、FinTech 企業が主導する個人財務管理業務等の金融関連サービスや、米国で行われている P2P レンディング等がこれに含まれる。

本区分で安対基準における取扱いを検討するに当たっては、行政による制度変更を前提としないで考えるとすれば、非金融機関においても、安対基準の規範性が及んでいる

[39] 安対基準の「Ⅰ．安全対策基準の考え方」において、「全社で統一された情報の取扱いがなされるよう、セキュリティポリシーの策定が必要となっている。」とされている。また、「各金融機関等は、コンピュータシステムの利用状況、直面するリスクの種類と大きさ、保護すべき情報の重要性や、自社の規模・特性に応じたセキュリティスタンダード（自社の安対基準）を、自社のセキュリティポリシー（基本方針）に準拠しつつ、本基準を参考の上で策定し、実施することが必要である。」とされている。

ことが、利用者から安全対策上の信頼を得るためにも、期待される。

つづいて、こうした規範性を生ずるには、次のふたつの方法が考えられる。

①直接的に規範性が生ずる方法

非金融機関である FinTech 企業が個別に FISC の会員となり、安対基準の策定過程に明示的に参画するとともに、FinTech の観点からその基準策定に貢献するとともに、安対基準を遵守する。

②間接的に規範性が生ずる方法

FinTech 企業の業界団体が FISC 会員となり、業界団体が代表して、安対基準の策定過程に明示的に参画するとともに、FinTech 業界の観点からその基準策定に貢献する。また、安対基準と整合的な FinTech 業界の自主基準を策定し、業界団体の会員がそれを遵守する。

まず①については、既に、FISC の会員となっている FinTech 企業があり、今後、安対基準の策定過程に参画することが期待できる。また、②については、既に、FISC 会員となっている業界団体があり、本検討会にも委員として検討に参画いただいているところである。さらに、この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。

こうした取組みが進み、安対基準の規範性が、FISC の会員となった FinTech 企業や業界団体に及ぶことができれば、その結果として、金融機関と非金融機関に関わらず、FinTech と総称される金融関連サービス全般において、シームレスに一体不可分な形で、適切な安全対策が実施されることが期待できる。

ただし、業界団体の自主基準が安対基準と整合的な内容となるか否かは、最終的にその業界団体の検討に委ねられることとなるとともに、必ずしも FISC の会員とならない FinTech 企業や業界団体も存在しうることから、そうしたことを踏まえて、本検討会として、何らかの意見表明を行うことが妥当である。

３．FinTech 業務における安全対策に関する意見表明

以上のことを踏まえて、FinTech 業務全般における安全対策に関して、以下の意見表明を行う。

【意見表明】

FISC「金融機関におけるFinTechに関する有識者検討会」は、FinTech業務を実施するのが金融機関であるか否かに関わらず、FinTech業務を担う情報システムにおける安全対策の在り方について、高い関心を持っている。そうしたことから、FinTech業務に携わる事業者においては、本検討会が策定する以下の「金融関連サービスの提供に携わる事業者を対象とした原則[40]」を踏まえたうえで、適切な安全対策が実施されることを期待する。

（１）金融関連サービスの提供に携わる事業者は、その利用者が安心してサービスを利用できることを目指し、みずからが管理責任を負う情報システムに対して、適切な安全対策を実施する。
（２）金融関連サービスの提供に携わる事業者は、安全対策の実施に当たっては、イノベーションの成果が利用者の利便性向上に資するよう留意するとともに、金融機関とその他事業者がそれぞれ独自の優位性を活かせることを目指し、安全対策においても協調が促進されるよう留意する。
（３）金融関連サービスの提供に携わる事業者は、互いに協調して安全対策を実施するに際し、FISC 安対基準を含め、安全対策に関して社会的に合意されたルールが形成されるよう努める。

（１）

金融関連サービスの提供に携わる事業者として、金融機関や IT ベンダーに留まらず、FinTech 企業等多岐にわたる事業者が想定される。そうした事業者は、企業価値の最大化のためにも、金融関連サービスにおいては、何より利用者が安心して利用できることが重要であり、そのためには、サービスの提供に必要となる情報システムに対して、何ら安全対策を実施しない、ということは適切ではない。

（２）

FinTech にみられるとおり、金融関連サービスにおけるイノベーションにはめざましいものがあり、特に革新的なユーザー体験の提供などを通じて利用者の利便性向上に資するこ

[40] FISC『外部委託検討会報告書』において提言された「安全対策における基本原則」が、主に FISC 会員を対象とした基本原則であるのに対して、「金融関連サービスの提供に携わる事業者を対象とした原則」は、「安全対策における基本原則」をもとにしつつ、より幅広く金融関連サービスの提供に携わる事業者全般を対象とした原則である。

とから、その利用が進んでいる状況にある。したがって、安全対策の実施に当たっては、イノベーションを阻害することが無いよう留意されるべきである。

また、金融機関において、オープン・イノベーションが進められる中で、金融関連サービスの提供に、従来以上に複数の事業者が、多段階にわたり重層的に携わることも予想される。このように、事業者の関係が複雑になる中においても、複数の事業者が協調してサービスに携わることで、相互の優位性を取り込むことが可能となる。したがって、安全対策においても、互いに協調して取り組まれるべきである。

（3）

金融情報システムの安全対策については、金融機関等による自主基準である公益財団法人金融情報システムセンター「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」をはじめとして、社会的に合意されたルールが存在する。例えば安対基準においては、その策定過程に、金融業務や情報システムに係る業界の代表者等専門的・技術的知見を有する関係者が携わるとともに、金融情報システムの安全対策に責任を負い、安全対策の実施を現場で担う関係者が自主的に参画していることに特徴がある。【資料編資料6参照】

金融関連サービスに携わる事業者においては、社会的に合意されたルールが形成されるよう努めるとともに、こうしたルールと整合する安全対策が実施されることが望ましい。

4．社会的に合意されたルールの形成に向けたFISCの役割

従来、金融情報システムの主たる関係者は、金融機関等とITベンダーからなり、ほぼFISCの会員となっていることから、安対基準に、金融情報システムの担い手の意向や特性を十分に反映することが可能である。その結果、金融情報システムにおいて必要となる安全対策については、安対基準でおおむね確認することができる。

しかしながら、今後、オープン・イノベーションの進展に伴い、従来以上に複数の事業者が金融関連サービスの提供に携わることが予想される中で、必ずしも、FISCの会員とならない事業者も想定され、その場合には、安対基準にすべての事業者の意向や特性を十分に反映することが容易ではなくなることが予想される。

また、各事業者が、みずからのために独自に自主基準を策定することが考えられるが、仮に安対基準と何ら関係なく自主基準が策定されれば、金融関連サービスであるにもかかわらず、異なるルールが適用・運用されることとなる。

以上の、今後発生が予想される問題に対しては、FISCとしても社会的な役割を果たしていくことが必要である。例えば、金融関連サービスの提供に携わる事業者の業界団体において、独自の自主基準が検討されていれば、FISCは、その検討に参画し、社会的に合意されたルール形成に向けて必要となる支援を行い、基準相互の整合性が確保されるよう努めていく[41]。

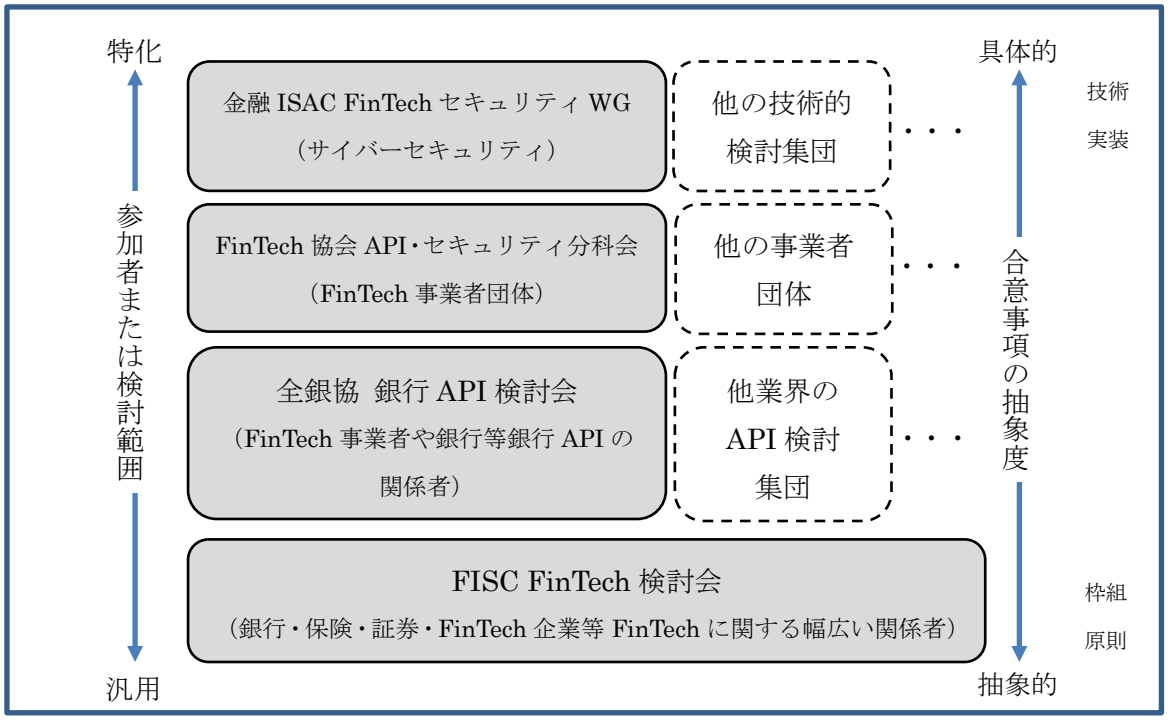
---

[41] 既に行われている自主基準策定の取組みとして、銀行業界においては、全銀協が事務局として、「オープンAPIのあ

社会的に合意されたルールの形成に当たっては、FISC が策定を予定している「必要最低限の安対基準」に着目することが有益である。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。

なお、FinTech 業務における安全対策に関しては、各業界団体をはじめとして、様々な集団において集合的な検討が進められており、その相互関係については、集団への参加者の性質や検討範囲に着目すれば、例えば、下図のように捉えることも考えられる。それぞれの集団においては、検討内容の整合性確保の観点から、相互関係を意識して、集合的な検討を踏まえた取組みが進められることが期待される。

（図表 10）FinTech に関する安全対策を検討している集団の相互関係例



り方に関する検討会」が設置され、銀行業界の意向や特性を反映させた独自基準に関する検討が進められている。FISC は、その検討会に参画するとともに、そこで言及されている「API 接続先チェックリスト」（仮称）の制定に関して、事務局として支援を行っている。また、FinTech 企業の業界団体である FinTech 協会においても、協会の自主基準策定作業が進められているが、FISC はその検討に参画し、安対基準の解説等の支援も行っている。

Ⅳ　クラウドサービス利用時のリスク管理策に関する補足

～重要な情報システムでの利用を中心とした補足的検討～

１．補足的な検討の観点

「金融機関におけるクラウド利用に関する有識者検討会」（以下「クラウド検討会」という）報告書、及びそれを踏まえて安対基準第８版追補改訂において策定されたクラウドに関する基準（以下「クラウド基準」という）に関して、以下の観点から、補足的な検討を行うことが有益である。

（１）クラウド基準策定後の状況の反映

クラウド基準策定後、金融機関におけるクラウドの利用が進む[42]とともに、金融機関のFinTechへの取組みも急速に活発化する中で、FinTech業務ではクラウドサービスが利用される場合が多いことから、今後、クラウドサービスの利用がますます進展していくことが予想される。一方で、外部委託検討会が行われ、「重要な情報システム」の意義が明確化される等、クラウド検討会で提言されたリスクベースアプローチの議論がさらに深められてきた。そうしたクラウド基準策定後の状況を踏まえて、クラウド基準が「重要な情報システム」に適用される場合（FinTechのユースケースとしてはブロックチェーン・AI等）を想定し、クラウド基準の実効性をさらに高める観点から、クラウド基準をより明確化すべき点が無いか等、補足的な検討を行うことが有益である。また、補足すべきリスク管理策の観点を明らかにするためには、クラウドサービス固有の性質を特定することが有益である[43]。

（２）海外先進諸国の動向

クラウド検討会の前後で、海外先進諸国において、クラウドサービス利用に係るガイドラインの策定が進んでいることから、海外先進諸国のガイドラインを参考とすることが有益である。

海外先進諸国におけるガイドラインでは、わが国のクラウド基準と共通する点が多いが、例えば、特徴的なのは以下の点である。【資料編資料８】

- 金融機関は、外部委託された業務に関連するデータに、実効的なアクセスが可能となるよう要求されている。ここでいう「データ」には、金融機関のデータ、顧客のデータ、取引履歴データだけでなく、システムや手続きに関するデータも含

[42] クラウド検討会直前の平成 25 年度、クラウドを利用している金融機関等は 26.6%であったのに対して、平成 27 年度には、36.5%と増加している。【資料編資料７参照】

[43] クラウドサービス固有の性質を特定することは、今後、クラウド基準を外部委託全般に適用可能なものとクラウド固有のものとに整理する際にも有益である。詳細は、FISC『外部委託検討会報告書』脚注 31 を参照。

まれる[44]とされ、その範囲を狭めようとすることは適切でないとされている。また、そうした考え方に基づいて、アクセスの対象となる事業拠点に関しては、本社や事務センターを含み幅広く解される一方で、必ずしもデータセンターへのアクセスが必要とならない場合もありえるとされている。さらに、管轄権については、データアクセスの実効性を高める観点から、クラウド事業者との契約は、国内法の管轄下にあることをデファクトとしている。これらは、クラウドサービスの利用において、一般的に金融機関の統制の程度が低くなることを踏まえて、統制上必要となるデータへのアクセスに焦点を当てて、明示的に要求されているものと解される。

- 要求事項を設定する目的を、「金融機関が、外部委託先を利用することに伴うオペレーショナルリスクを、適切に特定し、管理するよう促すこと」にあるとし、そのうえで、「金融機関にオペレーショナルリスクが増大することがないよう」求められている。要求事項の多くは、リスク管理、監督といった一般的な統制の方法に関する事項が中心となっており、設備等技術といった統制の内容に関する言及はほとんどない。これは、外部委託の有無に関わらず、統制水準は同一に維持すべき（安全対策の効果は同等であるべき）という基本的な考え方を明確に示す一方で、それらが十分に理解されていれば、金融機関の特性や規模等で様々にとりうる個々の技術的なリスク低減策は、一義的には金融機関に委ねられるべきである、としているものと解される。

以上のことを踏まえ、まず、クラウドサービス固有の性質を詳述し、「重要な情報システム」でクラウドサービスが利用される場合を中心に、補足的な検討を行う。

２．クラウドサービス固有の性質

クラウド検討会では、クラウドサービスは「外部委託の一形態として扱うことが適当」であるとされた。ここでいう外部委託とは、システム資源の調達先を表した言葉であり、その一形態であるクラウドサービスは、システム資源の調達の観点から、その性質を整理することが妥当である。

そもそも、システム資源の調達について、安対基準が策定された当初に遡れば、調達形態は現在ほど多様ではなく、例えば、建物・電源・空調・水冷等の設備一式、業務アプリケーションの開発や情報システムの運用要員等は、基本的には金融機関が自前で用意するのが一般的であり、外部から調達するのは、せいぜいホストコンピュータやテープ装置等のハードウェアや、オペレーティングシステムやデータベースシステム等の基本ソフトウ

[44] 例えば、要員の身元調査手続き、システム監査証跡等も含まれるとされている。

ェア、そして一部の開発運用要員程度であった[45]。

その後、コスト削減や先進技術の利用等を目的に、情報システムの運用に係る資源をまとめて外部から調達する、いわゆるアウトソーシングが徐々に進展した結果、今や勘定系基幹システムにおいて、金融機関の 90%以上が外部委託を利用している現状にある。同時に、これによって、金融機関は、統制の重点を内部から外部にシフトさせる必要が生じるとともに、統制の重点がシフトする中においても、安全対策の効果は、自前で調達する場合と同等に維持すべく、付加的な安全対策を実施することが必要となった[46]。

このようなシステム資源の調達方法とそれに伴う統制の重点の変化の途上で、クラウドサービスが登場した。クラウドサービスは、システム資源の調達において、従来の外部委託と比べて、利用者のニーズに応じた柔軟な調達が可能[47]となることから、金融機関が多岐にわたるFinTechに取り組む中で、利用がいっそう進展していくものと予想される。

同時に、金融機関にとっては、統制の対象としてのクラウドサービスの位置づけが、従来にも増して高まることが予想され、近年のクラウドサービスの状況を踏まえ、その固有の性質を以下のとおり整理し、補足的検討が必要な観点を明らかにする。

（１）匿名の共同性

クラウドサービスは、複数の事業者が、単一のクラウド事業者に委託する形態として共同性という性質を有する一方で、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を有する。

そのため、クラウドサービスにおける安全対策を決定する主な役割は、個々の利用者ではなくクラウド事業者に帰属することとなり、例えば、個々の利用者からの個別の監査要求や、個別の改善要望の実現に対して、消極的となる傾向があるとともに、監査において必要となるデータセンターへの立入については、セキュリティ上の問題を惹起するとして、受入れを拒否することとなる。したがって、クラウド事業者に対しては、金融機関による統制が十全に機能せず、リスク評価やリスク低減策を適切に実施できない、という可能性が内在している。

一般の情報システムにおいては、そうした可能性を考慮に入れたうえで、適切にクラウド事業者の選定が行われ、金融機関がリスクに応じて統制の程度を決定すれば十分であるが、重要な情報システムにおいては、インシデント発生時の社会的影響が甚大であ

---

45 そのため、安全対策における統制に当たっては、金融機関の内部が主な対象となることから、安対基準の初版では基準全 113 項目のうち、外部委託に関する項目は２項目となっていた。

46 最新の安対基準第８版追補改訂においては、外部委託に関する基準は 11 項目に増加した（うちクラウドサービスの基準は５項目）。なお、統制の重点が内部から外部へシフトしていく実態を、安対基準の構成等に、適切に反映していくことが、今後の安対基準改訂において必要となると考えられる。

47 柔軟な調達の特徴として、費用の経済性・調達の即時性・調達手続きの容易性・システム管理の効率性が考えられる。「費用の経済性」とは、情報処理の規模が大きいことから、規模の利益が働き相対的に低廉に利用できる余地があることをいう。「調達の即時性」とは、利用を決定してから実際のサービスインまでの時間が相対的に短いことをいう。「調達手続きの容易性」とは、例えば、システムの利用要件をインターネットから簡単に設定できること等をいう。「システム管理の効率性」とは、例えば、ハードウェア個々の管理が不要となること等をいう。また、安全対策面の特徴として、金融機関と比べて、セキュリティ投資額が大きい点（毎年数十億円を投下しているクラウド事業者もある）、情報処理が広域に行われることでサービス継続性が高い点、が指摘されることがある。

り、特に有事において、金融機関には、従来の重要な情報システムの外部委託と同程度に、クラウド事業者に対する統制能力を十全に発揮することが必要となる[48]。統制の検討に当たっては、同様に共同性という性質を有する「共同センター[49]」において行われている統制の観点を踏まえてリスク管理策を検討することが考えられるが、一方で、特定の委託先が包括的に業務を受託する共同センターと異なり、クラウドサービスは、クラウド事業者が、情報システムのハードウェアや基本ソフトウェア等部分的に業務を受託する形態があることに留意が必要である。

以上から、重要な情報システムに関する補足的検討に当たっては、共同性という性質に関しては、共同センターに適用されるリスク管理策[50]を参考としつつ、クラウド事業者との責任分界等を理解したうえで統制の範囲や内容を決定することとなる[51]。また、匿名性という性質に伴う、統制の低下を補完するためのリスク管理策について明確化を行うことが適当である[52]。

（２）情報処理の広域性

クラウドサービスでは、利用者が広域に及ぶことから、情報処理拠点を含む事業拠点も、複数の国にまたがり広域に及ぶ場合がある。そのため、利用者は、事業拠点の大半が国内を中心とする従来の外部委託とは異なり、例えば、インシデント発生時に復旧や原因究明のために必要となるデータは、どこの事業拠点へ行けばアクセス可能か、その所在地をあらかじめ知っておきたい、という要望を持つことになる。また、復旧や原因究明とその後の再発防止策が実効的に行われることを担保するために、データにアクセス可能な事業拠点に対する監査権を契約書に明記したい、あるいは事業拠点に対して自国の法令が及ぶようにしたい、という要望を持つこととなる。

一般の情報システムにおいては、インシデント発生時は金融機関が個別に対処すればよく、統制の程度はリスクに応じて金融機関が決定すれば十分であるが、重要な情報システムにおいては、インシデント発生時の社会的影響が甚大であるため、金融機関は、

---

48 クラウド基準では、平時における統制能力の発揮を想定し、運用時のモニタリングにおいては、実効的かつ効率的な統制手法として、第三者監査の利用を選択肢として提言されるとともに、平成 28 年５月 FISC『システム監査指針（改訂第３版追補）（以下「監査指針」という）では、「クラウドサービス監査のポイント」として、第三者監査人を利用した共同監査方式について、そのプロセスや考慮点まで踏み込んだ具体的な提言がされている。

49 共同センターは複数の金融機関が共同で重要な情報システムの運用等を委託する形態であり、安全対策の効果が複数の利用者に及ぶ共同性という性質を有する点でクラウドサービスと同じ性質を有する。

50 FISC『外部委託検討会報告書』では、「共同センターにおけるリスク管理の在り方」として、特に、有事対応における時間性の問題を取り上げている。クラウドサービスでは、利用者間でコミュニケーションが無いことから、ある意味利用者の意思統一という問題は生じないものの、クラウド事業者は利用者全体への影響を考慮するため、対応に時間を要する可能性がある。したがって、有事対応における時間性の問題は、クラウドサービスの利用においても問題となることから、FISC『外部委託検討会報告書』で提言された「共同センター固有の IT ガバナンス（リスク管理策の在り方）」は参考となる。

51 安対基準（運 109）においては、クラウド事業者との契約締結時に考慮すべき基本的な事項の１つとして「クラウド事業者（複数のクラウド事業者がサービスの委託を受けた場合を含む）との間の管理境界や責任分界点に関する取決め」があげられている。

52 統制能力の向上策の１つとして監査があるが、クラウド基準では監査に関して、「システム監査やモニタリングを実施することが必要である」とされており、また、監査権については、「立入監査等を実施する権利を明記すること」が「望ましい」とされている。

データにアクセス可能な事業拠点という観点でもリスク管理策の検討が必要となる。

以上から、重要な情報システムに関する補足的検討に当たっては、インシデント発生時の復旧や原因究明等統制上必要となるデータへのアクセス可能な事業拠点に関して、リスク管理策の明確化を行うことが適当である[53]。

（３）技術の先進性

クラウドサービスでは、複数の利用者で効率的な資源の利用を可能とする仮想化技術や、利用者以外によるデータ閲覧・処理等を不可能とするデータの秘匿性を高める技術等、特にソフトウェアにおいて技術の進展が著しい。そのため、設備やハードウェアといった物理的な安全対策による効果が、ソフトウェア技術によっても同等程度に達成可能となる場合がある[54]とともに、ソフトウェア技術自体も、旧来の技術を塗り替える、より実効的な技術が次々と登場する場合がある。したがって、設備基準や技術基準といった技術的な安全対策を、あらかじめ一意に特定しておくことが、必ずしも適切ではないことが生じうる。

そうした中、従来の安対基準では、運用基準・設備基準・技術基準相互の取扱いの考え方が、必ずしも明確に示されていないため、例えば、クラウド事業者選定時の客観的評価において、評価事項に設備基準や技術基準が字義通りに利用される、といった不確実性が残る現状にある[55]。その結果、全体の安全対策の効果からみれば、金融機関として個別に統制を行うまでもない部分にまで形式的に統制が行われ、過度な安全対策を招来することが危惧される。

また、採用技術が先進的であるがゆえに、監査人はあらかじめクラウドサービスの採用技術等の詳細について十分に知悉しておく必要が生じるものの、金融機関が内部に保有する IT 要員やシステム監査要員が限られている場合、必ずしも実効的な監査が行えないことが危惧される。

一般の情報システムにおいては、安対基準の取扱いが明確化されれば、そのうえでリスクに応じて金融機関が決定すれば十分であるが、重要な情報システムにおいては、金融機関は、監査を行うことを前提としつつ、実効性を確保するという観点でも、検討が必要となる。

以上から、補足的検討に当たっては、設備基準や技術基準といった技術的な安対基準

---

53 クラウド基準では、所在地を確認すべき「データ」には、金融機関のデータが想定されている。そのうえで、業務の継続性の観点から所在地把握が必要とされている。また、管轄権については、「紛争が生じた際にどの国の法律が適用されるのか（中略）十分に配慮する必要がある。」とされている。

54 例えば、同等性の原則の立場に立てば、データの暗号化や複数データセンターへのデータの分散配置によって安全対策の効果が高まれば、個々のデータセンターの物理的な安全対策を従来ほど強く求めなくてもよくなる場合もありえる。

55 例えば、設備基準では設備 47「ネズミの害を防止する措置を講じること」がある。これはリスクとしては存在するものであるが、クラウド事業者が利用しているデータセンターの中には、このリスクは、金融機関によって明示的に確認が必要なほどは高くないケースがあることから、クラウド事業者の実態を踏まえて、この基準の利用の要否が判断されるべきである。また、技術基準では技術 28,29「データの漏洩防止策を講ずること」がある。この基準では、「暗号化を実施することが望ましい」とされ、技術的な対策が例示されているが、こうした技術は日々急速に進歩しており、技術基準の例示に形式的にとらわれてしまうと、クラウド事業者がより優れた技術を採用しているにも関わらず、評価を得られないことが危惧される。

の取扱いについて明確化したうえで、重要な情報システムにおいては、人材面等監査に関するリスク管理策の明確化を行うことが適切である[56]。

３．重要な情報システムの外部委託先に対する統制の考え方

クラウドサービス固有の性質を踏まえて、補足的なリスク管理策を検討するに当たっては、重要な情報システムにおける外部委託先に対する統制の考え方を明らかにすることが有益である。

まず、「重要な情報システム」とは「重大な外部性を有する情報システム」もしくは「機微情報[57]を保有する情報システム」のことをいうが、前者において大規模なシステム障害が発生した場合、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、後者において機微な個人情報が流出した場合、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可能性がある。このように社会的・公共的性質を有する情報システムにおける有事対応の責任は、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、外部委託を利用している場合であっても、技術的な側面を担う外部委託先が負えるものではない。したがって、金融機関には、有事において、その影響を最小化するとともに、情報システムを速やかに復旧させ業務の継続性を確保する責任があり、外部委託先に対して、内部の場合と同程度の統制が行えるように、あらかじめ十分な手当てをしておくことが求められる。

こうした有事における実質的な統制を可能とするには、平時から異常を見逃さない等システム運営状況を日常的に監視しておく必要があるとともに、定期的に外部委託先における内部統制状況をチェックし、有事の発生やその対応に影響を及ぼす可能性のある問題があれば、あらかじめ外部委託先に対処を促し、問題を解決しておくことが必要となる。

以上のことは、外部委託の一形態であるクラウドサービスにおいても同様であり、金融機関は、重要な情報システムでクラウドサービスを利用する場合は、クラウド事業者の責任分界を踏まえ、業務継続におけるクラウドサービスの位置づけ等に留意しつつ、実質的な統制を行うことが必要である[58]。

---

[56] クラウド基準では、監査の実効性を高めるために、「委託元金融機関の立入監査等が実効的でない場合などには、第三者監査により代替することも可能である」「既にクラウド事業者が受検している監査結果の内容を検証し、疑問点や不足する監査項目を中心にクラウド事業者に対する実地検証を行うことが有効である」とされている。

[57] ここでいう機微情報を考えるに当たっては、金融庁『金融分野における個人情報保護に関するガイドライン』が参考となる。同ガイドライン（平成 29 年５月 30 日施行）第５条１項においては「法第２条第３項に定める要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活に関する情報」が機微情報とされている。また、改正個人情報保護法第２条第３項においては「要配慮個人情報とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして、政令で定める記述等が含まれる個人情報をいう。」とされている。

[58] 金融機関においては、有事における影響の最小化と業務の継続性の確保が第一に求められることとなるが、これは、すべての金融機関において、クラウド事業者に一意なリスク管理策を求めることを必ずしも意味しない。例えば、有事には、クラウドサービスの復旧を待つことなく、有事用にスタンバイしているシステムを稼働させるような業務継続計画であれば、クラウドサービスの復旧を前提とした業務継続計画の場合とは、おのずとクラウド事業者に対するリスク管理策は異なるはずである。また、FISC『外部委託検討会報告書』で示されているとおり、委託業務が細分化された結果、クラウド事業者の受託業務のリスクが十分に低いと判断しうる場合には、リスク管理策は異なることとなる。したがって、金融機関は、重要な情報システムにおいて、クラウドサービスがどのように位置づけられるか、どのような利用形態をとっているか、によってクラウド事業者に対する具体的なリスク管理策を判断することとなる。

４．リスク管理策に関する補足

以上を踏まえて、クラウドサービス利用時に実質的な統制を行うためのリスク管理策について、以下の補足を提案する。

（１）データアクセス拠点の把握

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関は、クラウド事業者の選定時において、統制上必要となるデータ（以下「必要データ」という）へのアクセスが可能となる情報処理拠点等、実質的な統制を行うにあたり対象となる事業拠点[59]（以下「統制対象クラウド拠点」という）について把握しておくこと。

また、統制対象クラウド拠点は、実質的な統制が可能となる地域（国、州等）に所在すること。

（２）監査権等の明記

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関は、統制対象クラウド拠点に対して、実質的な統制を行うに当たって必要となる権利（監査権等）を確保するために、クラウド事業者と交わす契約書等にその権利を明記すること。

（３）監査の実施

金融機関は、クラウド事業者に対する監査に当たって、技術が先進的であることから、クラウド事業者がみずから監査人に委託して行った保証型監査の報告書を利用することが望ましい。また、その場合、統制が十全かつ実効的に機能するよう、安対基準と整合的な内容で検証が行われている報告書を利用することが望ましい[60]。

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関は、実質的な統制が十全かつ実効的に機能するよう、定期的に監査を実施すること。

（４）監査人等モニタリング人材の配置

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関の経営層は、クラウドサービスの採用技術が先進的であることを認識したうえで、クラウド事業者に対する監査等モニタリングを実効的に実施するために必要となる能力を有した人材を配置すること。また、こうした人材を金融機関内部で育成することが容易でない場合は、専門性を有する第三者監査人等を利用することが望ましい。

（５）客観的評価を実施する際の留意事項

クラウド基準では、金融機関は、クラウド事業者の選定時において、「クラウド事業者の資質・業務遂行能力に関する情報や、クラウド事業者の内部統制やリスク管理に関する状況等をもとに評価を行うことが必要である。」とされているが、これは、客観的評価

---

59 統制対象クラウド拠点は、クラウド事業者の本社、営業所、データセンター、オペレーションセンター等様々な拠点が候補となるが、実際には、金融機関によって、利用するクラウドサービスの内容やクラウド事業者の内部管理状況等を踏まえて、金融機関が個別に特定することとなる。したがって、統制対象クラウド拠点には、データセンターを含むことは必ずしも必要ではない。

60 その他に、実効的かつ効率的な監査を実施する手段として、インターネット等を通じて利用者に提供される監査証跡の閲覧等クラウド事業者がサービスとして提供する監査機能を利用することも考えられる。

を実施する際の評価事項に、安対基準の設備基準や技術基準を含めることを必ずしも意味しないことに留意が必要である。

Ⅴ　集合的な検討を踏まえた「オープン API」における安全対策の在り方

１．「オープン API」における統制上の課題

「オープンAPI」はタイプⅢの実現手法の１つであることから、APIを公開する金融機関は、外部委託基準を準用し、API接続先であるFinTech企業に対して、客観的評価やモニタリングといった方法で統制を実施することとなる[61]。（外部委託基準の準用ルール）

したがって、今後、行政や業界団体等によって「オープン API」の環境が整備されれば、金融機関と FinTech 企業の API 接続が増大し、結果として、FinTech 企業は、多数の金融機関から統制を受けることとなる。

その際、形式的に、多数の金融機関が個別に統制を行うこととなれば、FinTech 企業においては、その対応が過度の負担となり、イノベーションを大きく損なうことが危惧される。

そもそも、金融機関が行う統制は、安対基準等を踏まえて行われることから、統制の方法や内容は、金融機関で共通する部分が多いと考えられる。仮に、統制の共通部分について、FinTech 企業の負担軽減を目指して、API 接続に携わる関係者が集合的に検討し、取り組むことができれば、金融機関はイノベーションの成果を享受することが可能となる。

２．「オープン API」における安全対策の在り方

統制は、利用検討時・契約締結時・運用時といった各管理フェーズにおいて実施される「統制の内容」と、客観的評価・契約締結・モニタリングといった「統制の方法」に分けられ、それぞれにおいて、各金融機関で共通する部分が多い。

まず、統制の内容に関しては、金融機関では、安対基準や業界団体の自主基準等の社会的に合意されたルールを踏まえたうえで、独自項目を追加して、定められるのが一般的である。したがって、まず、入口の管理フェーズで行われる統制の内容、すなわち、客観的評価で使用されるチェックリストの項目に関して、「オープンAPI」に関する社会的に合意されたルールを踏まえて、その共通部分を、金融機関とFinTech企業で、集合的に合意形成することが考えられる[62]。チェックリストの共通部分を合意しておけば、その後の管理フェーズで行われる統制の内容として、契約書や監視・監査項目等に反映することが可能となる。これにより、金融機関とFinTech企業が、安全対策に関して個別に合意形成する負担が

---

61 銀行 API 報告書において、銀行は「他の事業者等との API 接続に先立ち、セキュリティ等の観点から、API 接続先の適格性を審査することが必要である」とともに「API 接続先の情報セキュリティに関連した適格性について、API 接続後も定期的に又は必要に応じて確認することが必要である」とされている。

62 銀行 API 報告書において「複数の銀行と API 接続する企業等における審査対応負担を軽減する観点からは、銀行が API 接続先の適格性を審査する際に使用する「API 接続先チェックリスト」（仮称）の制定が期待される。」と整理されたことを受けて、FISC が事務局となり「API 接続先チェックリスト（仮称）ワーキンググループ」を設置し、統制の内容の共通部分に関する検討等を行っている。詳細は【資料編資料９】を参照。

軽減される。

次に、統制の方法に関しては、金融機関では、モニタリング等の統制方法を共同で実施することは、従来から一般的であり、複数金融機関が、意思統一を図りつつ、選定された幹事金融機関等（金融機関等の委託を受けた第三者監査人を含む）が代表して統制を行い、その結果を共有することで、統制を効率化してきた実績がある。したがって、「オープンAPI」においても、共通のAPI接続先に対して、金融機関が共同で統制を行うことは可能であり、例えば、幹事金融機関等が行った客観的評価結果、締結した契約書、監査結果[63]を他の金融機関が利用することとすれば、FinTech企業は金融機関ごとに対応を行う負担が軽減される。

以上のように、金融機関が、あらかじめ関係者で合意された内容にしたがって、集団で統制を行うこととなった場合、FinTech 企業においても集団で統制への対応ができれば、さらに負担を軽減できる可能性がある。

行政や業界団体等による環境整備が進む中で、FinTech企業の集団組成に向けた取組みとして、「オープンAPI」に参画する事業者団体設立の動きがみられる[64]。仮に、そうした事業者団体が設立されることとなれば、あらかじめ関係者で合意された統制の内容を踏まえて安全対策に関する自主基準を策定するとともに、個々の会員における自主基準の遵守状況について、例えば、内部監査人等（事業者団体の委託を受けた第三者監査人を含む）が検証した結果を踏まえて、必要に応じて会員に対して指導や勧告を行うことが可能となる[65]。

以上のとおり、FinTech企業における集合的な検討を踏まえた取組みの進展が予想されることとなれば、金融機関集団がFinTech企業集団と安全対策に関する協議を開始し、総体的な安全性を確保しつつ関係者の負担を最小化することを目指して、両者で協調した取組みが進められていくことが期待される[66]。

---

63 銀行 API 報告書において「事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等における審査対応負担の軽減や銀行による事前審査水準の標準化の観点から、当該銀行の責任においてほかの銀行に委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる」「モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任においてほかの銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる」とされている。なお、共同監査方式については、監査指針「共同利用型システム監査のポイント」「クラウドサービス監査のポイント」が参考となる。

64 一般社団法人 FinTech 協会は、平成 29 年 3 月 3 日『認定電子決済等代行事業者協会に向けて』という文書を公表し「改正銀行法案において定めのある認定電子決済等代行事業者協会について（中略）複数の企業で設立に向けた準備を行」い、「新しく設立される協会では、必要な規則の制定及び利用者からの苦情対応業務を含む認定事業者協会の業務として改正銀行法に定められた業務を提供するほか、より良い金融機関 API のあり方を検討していく予定」としている。

65 国会に提出されている『銀行法等の一部を改正する法律案』（平成 29 年 3 月 3 日提出）においては、例えば第五十二条の六十一の二十において、認定電子決済等代行事業者協会の業務として「会員の営む電子決済等代行業の適性化並びにその取り扱う情報の適正な取扱い及び安全管理のために必要な規則の制定」と「規則を遵守させるための会員に対する指導、勧告その他の業務」が挙げられている。

66 例えば、FinTech 集団の事業者団体が会員への指導・勧告にあたり、会員の自主基準遵守状況の検証作業を行うこととなれば、その作業は、金融機関集団が客観的評価やモニタリング時に FinTech 企業に対して行う検証作業と、主体が異なるとはいえ、実質的には重複する部分が多いと考えられることから、関係者の負担の最小化の観点からは、共同実施スキームを検討することも考えられる。

Ⅵ　今後の安対基準等改訂の考え方

本検討会の後に、FISC では、外部委託検討会及び FinTech 検討会の提言を受けて、安対基準等ガイドラインの改訂が進められることとなる。その際には、以下をはじめとして、両検討会報告書の内容を踏まえた改訂が行われ、金融情報システムの安全対策に携わる多岐にわたる関係者において、安全対策の考え方を中心に理解が得られるものとなることが期待される。

１．安全対策の基本原則の導入

リスクベースアプローチを踏まえた基本原則を、安全対策の考え方として導入する。

２．安対基準の明確化

（１）安対基準の対象の明確化

安対基準が適用対象とする「金融情報システム」の定義を「金融機関が行う金融業務を担う情報システム」として明確化するとともに、それ以外の情報システムと安対基準との関係についても明確化する。

（２）「高い安対基準」・「必要最低限の安対基準」の定義と位置づけの明確化

「高い安対基準」を定義し、その対象が「重大な外部性を有する情報システム」「機微情報を保有する情報システム」であることを明確化する。また、「必要最低限の安対基準」を定義し、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であることを明確化する。

（３）技術的な基準の位置づけの明確化

技術の進展が著しい環境下では、技術的な基準とそれ以外の基準では、取扱いが異なるべきであることを明確化する。前者は、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、「高い安対基準」や「必要最低限の安対基準」を参考としつつ、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。

３．外部に対する統制基準の拡充

（１）統制の重点のシフトの反映

勘定系基幹システムをはじめとして、金融機関の外部委託への依存度が高まっている。こうした、統制の重点が内部から外部へシフトしていく実態を踏まえ、安対基準上で外部に対する統制基準を明確化する。

（２）多様な形態を踏まえた統制基準の整理

共同センター・クラウドサービス・FinTech 等の多様な形態を踏まえ、それぞれの性質に応じた統制の在り方にしたがって、基準等を整理する。

「金融機関における FinTech 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	安冨 潔	慶應義塾大学名誉教授・弁護士
	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
	上山 浩	日比谷パーク法律事務所 パートナー弁護士
	田中 秀明	株式会社みずほフィナンシャルグループ IT・システム企画部 システムリスク管理室 室長 （第４回まで）
	持田 恒太郎	株式会社三井住友銀行 システム統括部　システムリスク統括室　室長 （第５回から）
	山田 満	株式会社南都銀行 システム部 部長
	吉本 憲文	住信 SBI ネット銀行株式会社 FinTech 事業企画部長
	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
	久井 敏次	東京海上日動火災保険株式会社 理事 IT 企画部長（第４回まで）
	黒山　康治	東京海上日動火災保険株式会社 IT 企画部 参与（第５回から）
	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)
	Mark Makdad	一般社団法人 FinTech 協会 理事
	瀧 俊雄	株式会社マネーフォワード 取締役 Fintech 研究所長
	轟木 博信	株式会社 Liquid 経営管理部長 弁護士
	村上 隆	株式会社ＮＴＴデータ 第四金融事業本部　企画部　ビジネス企画担当 シニア・スペシャリスト

	長 稔也	株式会社日立製作所 金融システム営業統括本部 事業企画本部 金融イノベーション推進センタ センタ長
	岩田 太地	日本電気株式会社 事業イノベーション戦略本部 FinTech 事業開発室 室長
	梅谷 晃宏	アマゾンウェブサービスジャパン株式会社 セキュリティ・アシュアランス本部　本部長 日本・アジア太平洋地域担当
	内田 克平	日本マイクロソフト株式会社 クラウド&ソリューションビジネス統括本部 金融インダストリー担当部長 （第２回まで）
	平原　邦久	日本マイクロソフト株式会社 金融サービス営業本部 シニアインダストリーマネージャー （第３回から）
	荻生 泰之	デロイトトーマツコンサルティング合同会社 執行役員
オブザーバー	神田 潤一	金融庁 総務企画局　企画課 信用制度参事官室　企画官
	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
	中井 大輔	日本銀行 金融機構局 考査企画課 システム・業務継続グループ企画役
	師田 晃彦	経済産業省 商務情報政策局 サイバーセキュリティ課長
	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

（FISC 事務局）

理事長		渡辺　達郎
常務理事		髙橋　経一
企画部	部長	小林　寿太郎
企画部	次長	藤永　章
企画部	主任研究員	大澤　英季（第２回から）
調査部	部長	中山　靖司
監査安全部	部長	西村　敏信（第４回まで）
監査安全部	部長	和田　昌昭（第５回から）
総務部	部長	水野　幸一郎
総務部	特別主任研究員	郡山　信

◆事務局スタッフ

柴田　晃宏、仲程　文徳（第４回まで）、三浦　哲史、田　昊

（参考）検討会の開催日程

第１回（平成 28 年 10 月５日）、第２回（同 12 月１日）、第３回（平成 29 年２月２日）、第４回（同３月 23 日）、第５回（同５月 15 日）、第６回（同６月 13 日予定）

Ⅶ　資料編

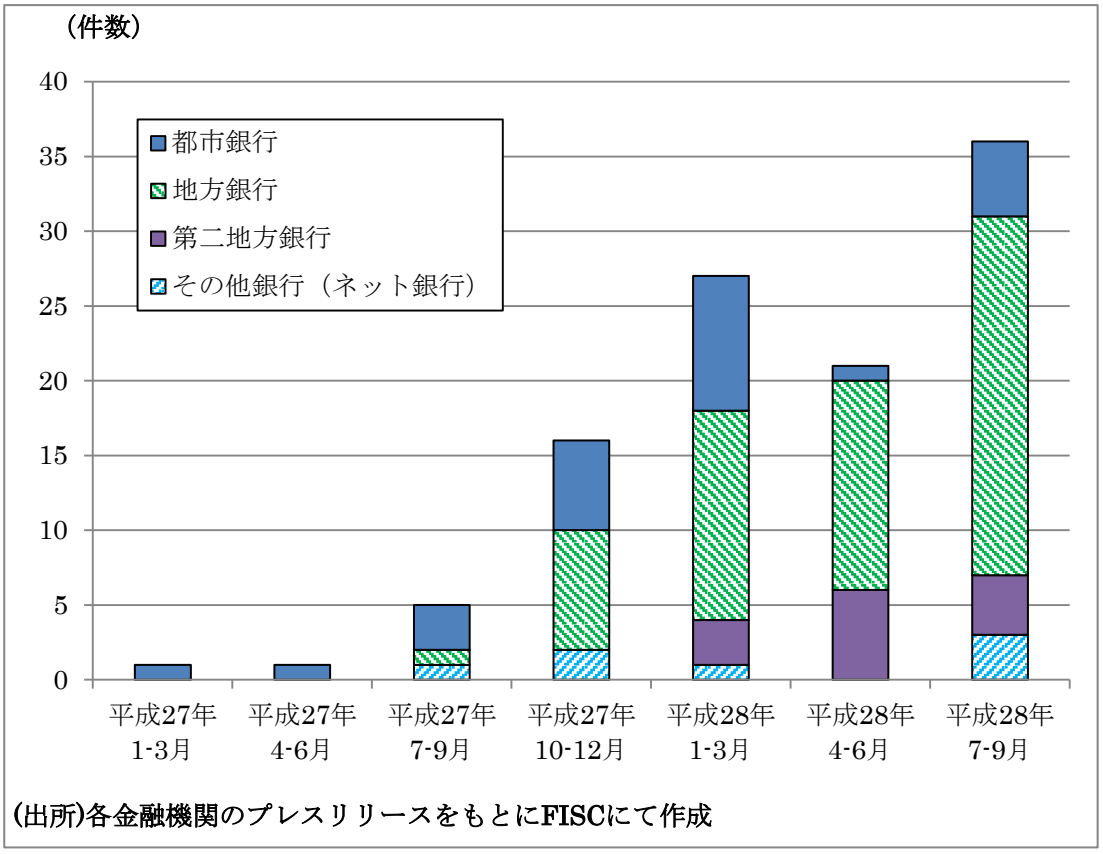
【資料１】金融機関等における FinTech をめぐる動向

１．国内金融機関の動向

平成 27 年から、都市銀行・地方銀行を中心として、国内金融機関の「FinTech」をキーワードとしたプレスリリースが急増している。主な内容は以下のとおり。

【平成 27 年 1-月】都市銀行が FinTech コンテストを開催
【平成 27 年 7-月】地方銀行のプレスリリースが増加
（FinTech 推進部署を設置　等）
【平成 28 年 1-月】都市銀行・地方銀行が新しい技術の実証実験開始
地方銀行が FinTech 企業と業務提携
【平成 28 年 7-月】都市銀行がブロックチェーンにより国内送金の実証実験を開始

国内金融機関の FinTech に関連するプレスリリースの件数



(出所)各金融機関のプレスリリースをもとにFISCにて作成

２．官公庁等の FinTech の定義例

「日本再興戦略 2016」（平成 28 年 6 月 2 日閣議決定）
近年、FinTechと呼ばれる金融・IT融合の動きが進展しており、金融業・市場に変革をもたらしつつある。
金融審議会「決済業務等の高度化に関するワーキング・グループ報告」 （平成 27 年 12 月 22 日）
FinTechとは、金融（Finance）と技術（Technology）を掛け合わせた造語であり、主に、IT を活用した革新的な金融サービス事業を指す。特に、近年は、海外を中心に、ITベンチャー企業が、IT技術を生かして、伝統的な銀行等が提供していない金融サービスを提供する動きが活発化している。
経済産業省「産業・金融・IT 融合に関する研究会（FinTech 研究会）について」 第一回配布資料（平成 27 年 10 月 6 日）
近年、フィンテック（FinTech）と呼ばれる IT を活用して革新的な金融サービスを提供するベンチャー企業が現れ、流通など伝統的な金融業以外の企業が新たな金融サービスを提供する動きが、世界中で見られる。
日本銀行「決済システムレポート」（平成 28 年 3 月）
FinTech とは、金融（Finance）と技術（Technology）を組み合わせた言葉であり、近年、急速に注目を集めている。このFinTechの定義は必ずしも明確に定められている訳ではなく、話者によって、その意味が異なることも多いが、一般には、情報通信技術など新しい技術を取り込んだ、新たな形態の金融サービスや、あるいは、そうした金融サービスを積極的に提供 していこうとする動きを指すことが多い。

３．日本の監督当局等の動向

（１）銀行法等の改正

平成 28 年５月に銀行法等が改正され、「銀行業の高度化若しくは利用者の利便の向上に資する業務又はこれに資すると見込まれる業務を営む会社」に対して、金融機関（あるいは金融グループ）が、当局の個別認可を得て出資し子会社とすることが可能となった。これにより、金融機関（あるいは金融グループ）が FinTech に取り組むにあたり、FinTech 企業を子会社とする事例が、今後出現してくることが予想される。

（２）金融制度ワーキング・グループ報告と銀行法改正案の公表

平成 28 年７月 28 日から、金融審議会「金融制度ワーキング・グループ」が開催され、中間的業者に対する規制の在り方を論点として取り上げ、審議を経て、平成 28 年 12 月 27 日報告書が公表された。この中で、オープン・イノベーションに向けて、電子決済等代行業者に対する制度的枠組み等が提言された。本報告書等を踏まえて、平成 29 年３月６日「銀行法等の一部を改正する法律案」が公表された。

（３）全銀協の取組み

全銀協では、平成 28 年８月４日に「オープン API のあり方に関する研究会」「ブロックチェーン技術の活用可能性と課題に関する研究会」が開催され、FinTech による金融革新の推進に関して、各銀行に対するアンケート結果を踏まえて、銀行業界としての検討が開始され、平成 29 年３月にそれぞれ報告書が公表された。（FISC も両研究会に参加）

全銀協のアンケートの中には、「FISC の金融機関等コンピュータシステムの安全対策基準等にて、銀行として取り組むべき安全対策等を示していただくことで、対策等の標準化が図られるとともに、検討時間、対応コストの削減が期待できる」といった、FISC に関するコメントも寄せられている。

（４）金融審議会における決済業務等の高度化に関する報告

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」中間整理（平成 27 年４月公表）[67] 及び金融審議会「決済業務等の高度化に関するワーキング・グループ」報告（平成 27 年 12 月公表）[68] において、情報セキュリティに関する課題等について以下のとおり報告されている。

「決済業務等の高度化に関するスタディ・グループ」報告中間整理

第４章　決済システムの安定性と情報セキュリティ　２．情報セキュリティ

（２）今後の課題

銀行における情報セキュリティについては、これまで、基本的に、外部接続先を主として金融業界内に限定することによって、セキュリティ侵害のリスクを低下させるとともに、万一問題が発生した場合の損失・責任については、基本的にサービス提供者側が負担することにより対応されてき

[67] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20150428-1.html
[68] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20151222-2.html

た。

他方、ITの発展等を背景に、ネットバンキングやモバイル送金などの例に見られるように、決済のインターフェイスは、銀行の外部へと拡大し、同時に、決済を中心とした銀行業務のアンバンドリング化が進行する中で多様なプレーヤーが決済情報のプロセスに組み込まれるようになっている。

こうした中にあっては、従来のように、サービスを提供する側が情報セキュリティ対策の責任を担い、外部とのネットワークを遮断することで情報セキュリティを構築するという手法では、十分な対策が講じられないおそれがある。

こうしたことを踏まえると、今後、ネットワークのオープン化に対応した情報セキュリティ対策を講じることがさらに重要である。このため、当面、例えば、以下のような課題について、検討を進める必要があると考えられる。

- *銀行のネットバンキングなどについては、監督指針やFISCの安全対策基準の整備等の取組みが行われてきたが、多様なプレーヤーが決済情報のプロセスに組み込まれる中にあっては、銀行のみならず、多様なプレーヤーにおける情報セキュリティ対策の向上が重要である。こうした観点からは、多様なプレーヤーが対応の拠り所とできる準則や業界における情報セキュリティ基準の設定、その実効性の確保のための方策が重要である。*
- *オープン化されたネットワークにおいて有効な情報セキュリティ対策を講じるためには、銀行その他の多様なプレーヤーと利用者が、それぞれ一定の責任を持って対策を講じることが必要である。そのためには、問題が生じた場合の責任・損失分担について、必要に応じ、一定の合理的なルールが形成されていくことが期待される。*
- *金融機関の外部も含め、オープンなネットワーク全体としてセキュリティ水準を向上させるためには、サービスを提供する側のみならずサービスを利用する側の情報セキュリティ対策が重要である。こうした観点からは、利用者のリテラシー向上も含め、利便性を考慮しつつも、幅広い関係者が情報セキュリティ対策を推進していくための方策が重要である。*

「決済業務等の高度化に関するワーキング・グループ」報告

第６章　決済高度化に向けた継続的取組み

決済業務等の高度化は、これまで述べてきた方向性に沿って、着実に行動に移していく必要がある。同時に、決済を巡る環境や決済サービスの変化・発展の可能性を踏まえれば、本報告書で述べた基本的な方向性を踏まえ、継続的に戦略的な取組みを実行していくことも必要である。

そのためには、決済高度化に向けた取組みの進捗状況をフォローアップするとともに、海外の動向や決済高度化に関連するイノベーションの状況等も踏まえながら、継続的に課題と行動を特定し、それらを官民挙げて実行に移していくことが必要であり、金融庁にはそのための体制の整備に向けた取組みが期待される。また、その際には、決済システムの安定性や情報セキュリティの確保という課題についても適切な対応がとられていくよう、留意していくことが重要である。

４．海外先進諸国の動向

（１）米国

2016 年３月末、米国通貨監督庁（OCC,Office of the Comptroller of the Currency）が、『連邦銀行システムにおける「責任ある革新」を支援する：OCCの考え方』という文書を公開し、広く意見を求めた[69]。

その中において、まず、国法銀行は、150 年以上前から革新の担い手であり、FinTech において伝統的な銀行業務のやり方が破壊されようとしている中でも、国法銀行が金融革新において優位性を有しており、引き続き国力の源泉であることが期待されている。

・*リンカーン大統領が 1863 年に国法銀行システムを創設して以来今日まで、イノベーション（革新）は、国法銀行システムの代表的な特徴である。特にこの１０年間、その革新精神に基づいて、国法銀行及び連邦貯蓄組合は、顧客のニーズの変化に対応すべく、商品、サービスやテクノロジーを開発導入してきている。*

・*銀行が革新を続ける一方で、金融テクノロジー、いわゆるFinTechにおいて、急速かつ劇的な進歩が起こっており、伝統的な銀行業務のやり方が「破壊」されようとしている。連邦銀行システムのその他の健全性規制当局と同様に、我々も国法銀行と連邦貯蓄組合が、こうした環境の中でも、力強く成長し、消費者、事業者、地域共同体に対して、活力をもって金融サービスを提供する役割を果たし続けることを望んでいる。*

そのために、OCC が、連邦認可金融機関において、「責任ある革新」が進められるように、それを支援する監督規制のフレームワークの準備を進めているとし、８つの原則を表明している。

1.「責任ある革新」を支援する
2.OCC 内部に「責任ある革新」を受入れる文化を醸成する
3.OCC の経験と技能を駆使する
4.金融サービスへの公正なアクセスが提供され、消費者が公正に取扱われるような「責任ある革新」を奨励する
5.効果的なリスク管理による、安全・健全な金融機関経営を促す
6.規模に関わらずすべての金融機関が事業戦略に「責任ある革新」を盛り込むよう奨励する
7.公式な「アウトリーチ（当局が現場に赴くこと）」を通して継続的な対話を促進する
8.他の監督当局と協力する

また、国法銀行と FinTech 企業の関係としては、それぞれの優位性を活かし、互いにコラボレーションしていくことを推奨している。

[69] https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-39.html

・*銀行とノンバンクイノベーターは、それぞれ独自の優位性を活かし、互いにコラボレーションすれば、利益を得ることが可能である。戦略的で思慮深いコラボレーションを通じて、銀行は、最新テクノロジーへのアクセス手段を手に入れ、ノンバンクイノベーターは、潤沢な資金や巨大な顧客基盤を手に入れることができるのだ。*

さらに、効果的なリスク管理が、必要条件とされている。

・*「革新」は、リスクから自由ではないが、適切に管理されている限りにおいては、リスクは進歩を妨げるものではない。実際に、効果的なリスク管理は、「責任ある革新」の必要条件である。銀行や当局は、リスクと革新の最適なバランスを心得なければならない。*
・*金融危機から学んだとおり、革新であれば何でもよいわけではない。（中略）OCC は、安全性、健全性、法令遵守、顧客の権利保護を堅持しうる「革新」を支援するものである。*

その後、2016 年 12 月、OCCは、一部のFinTech企業に対して特別目的国法銀行（Special Purpose National Bank）の免許を付与する案を公表した[70]。

（２）英国

英国金融行為規制機構（FCA,Financial Conduct Authority）は、2014 年 10 月から「Project Innovate」を開始、みずからイノベーションを涵養することで、金融サービスにおける効果的な競争を促すことを目的としている。この取組みの一環として、革新的なアイデアを実際の人々に対して試行するため「監督規制のサンドボックス」の実施計画を 2015 年 12 月に公表した。

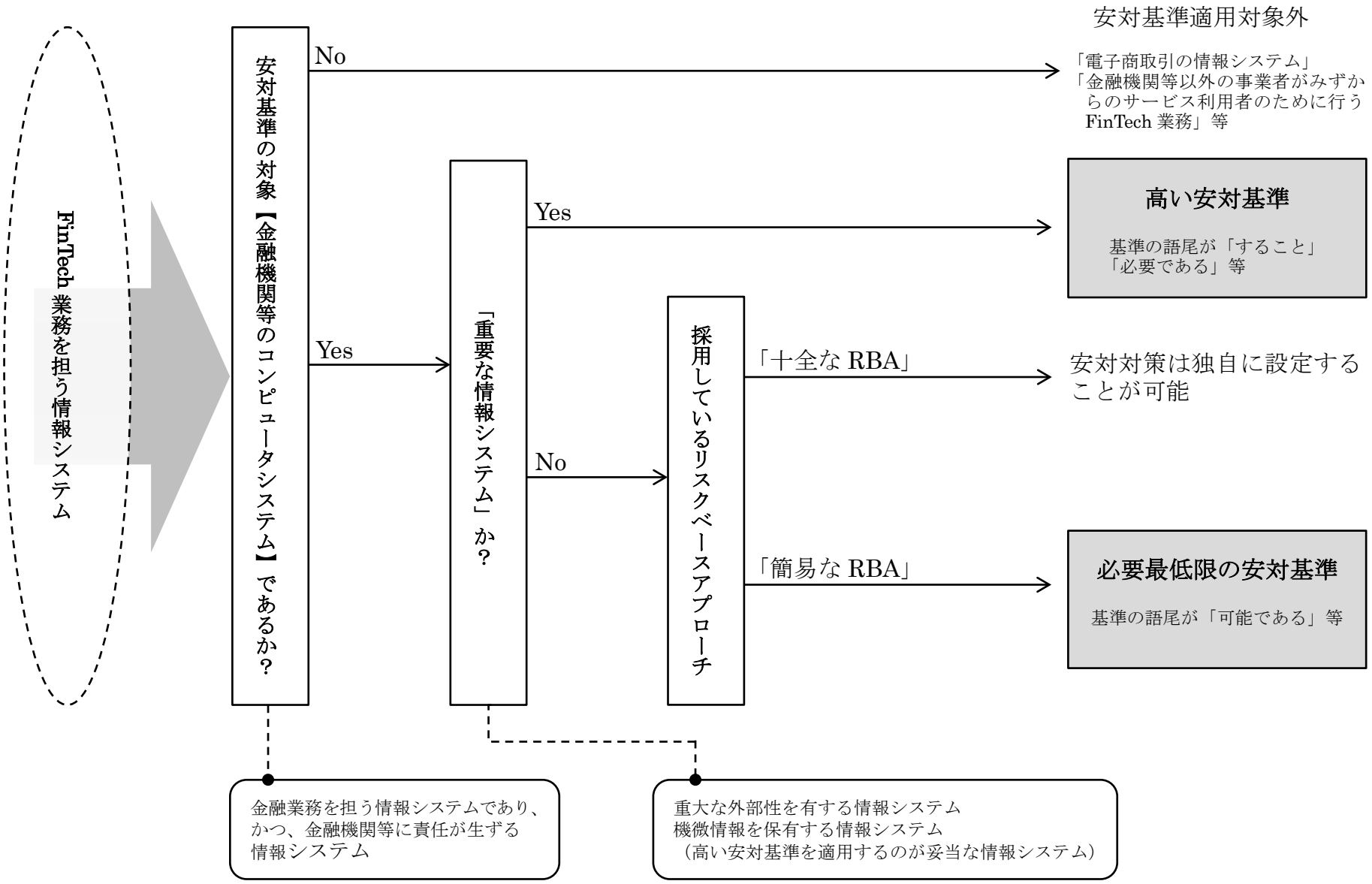
一方で、英国財務省の要請により 2015 年９月に「Open Banking Working Group」が設立され、英国銀行業におけるAPIのオープン標準推進に向けた検討が開始された。その検討の成果として、2016 年２月８日に「The Open Banking Standard」[71]が公表された。この報告書には、英国においてOpen Banking Standardを推進するための詳細なフレームワークが記載されているが、これは、英国がこの分野の国際的なリーダーシップを獲得し、世紀を超えて経済・産業の勝者であり続けることを目指した取組みであるとされている。

・*仮にこの分野で英国が国際的なリーダーシップを獲得できれば、他の多くの業界を先導することともなるであろう。すなわち、こうして強固なデータインフラが構築されることは、<u>今日の英国経済にとって重要であるだけでなく、今後一世紀以上にわたって、英国が経済界・産業界の勝者であり続けるためにも重要である</u>。*

（斜体部は FISC にて意訳。下線は FISC にて付す。）

[70] https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-152.html
[71] https://theodi.org/open-banking-standard

【資料２】安対基準の適用手順

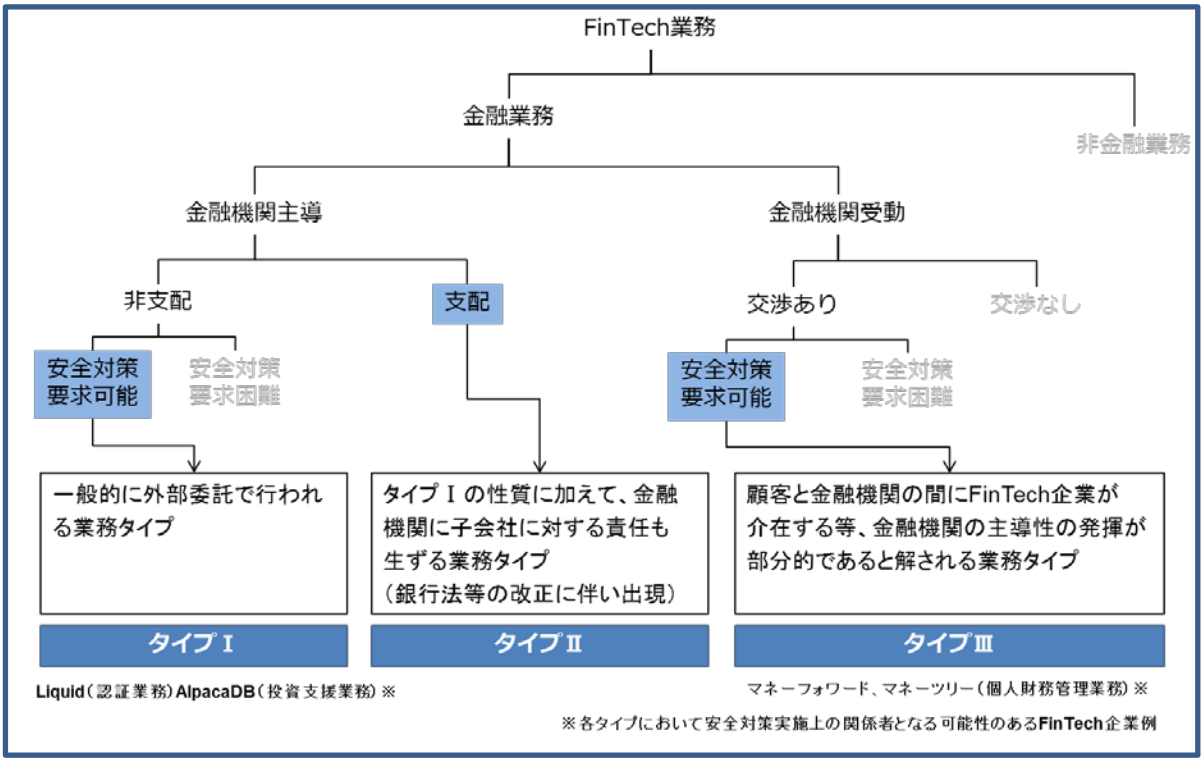


【資料３】FinTech 業務タイプ別類型に関する考察

１．検討対象となる FinTech 業務のタイプ

「安対基準の対象となる情報システムの判別基準」及び「金融機関が必ずしも主導的立場とならない業務形態」を踏まえると、本検討会の検討対象となる FinTech 業務を以下の３タイプに分類可能となる。

安対基準の対象とすべき FinTech 業務のタイプ



タイプⅠが、従来の安対基準で「外部委託」として捉えられていた基本的なタイプに該当する。タイプⅡは、先般、平成 28 年５月の銀行法等の改正によって、金融機関がFinTech企業を子会社とした場合に、安全対策上の責任に加えて、子会社に対する責任[72]も生ずることから、安全対策上の責任の在り方を検討するに当たっては区別している。タイプⅢは、タイプⅠ、Ⅱと異なり、金融機関の安全対策上の責任が部分的となることから区別している。

２．FinTech 業務における安全対策実施上の関係者の基本的類型

FinTech 業務における３者関係の整理に当たっては、２者関係の基本的類型の考え方を参考とすることが有益である。２者関係には、単数と複数の場合があり、単数は１類型のみとなる。次に、複数の場合には、金融機関が複数となる場合と IT ベンダーが複数となる場合がある。

前者は、安全対策上固有の性質が生ずるものとして対象とされた類型には、共同センターとクラウド

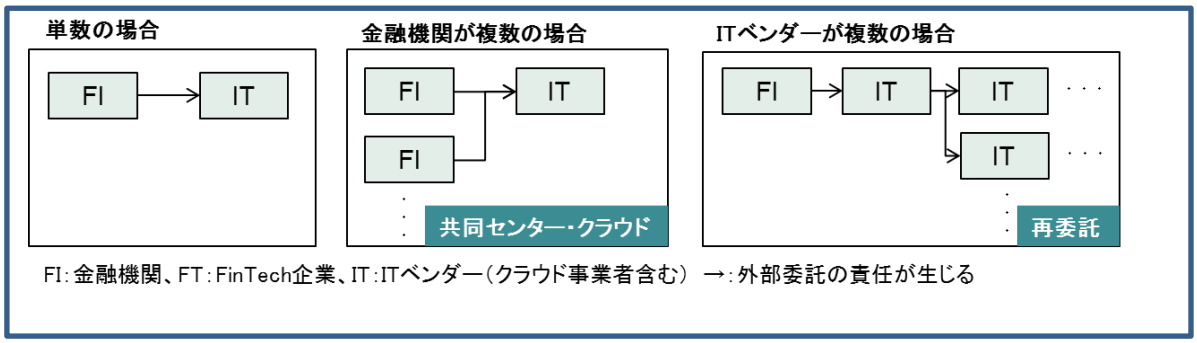
[72] 平成 28 年５月の銀行法等改正においては、あわせて「金融グループにおける経営管理の充実」のために、持株会社等が果たすべき「機能」が明確化された。また、岩原紳作『金融持株会社におけるグループガバナンス－銀行法と会社法の交錯（３）－』において「多くの金融持株会社は、（中略）子会社との間で経営管理契約を結んで経営管理のための助言・指導を行うことを定めている。」としている。

サービスがある。前者は、安全対策等の資源が効率化でき、その効果が複数の金融機関におよぶ（共同性）一方で、単一の金融機関の場合と同程度に迅速かつ円滑な意思決定が常に可能か不確実性が残るという問題（時間性の問題）を含む。後者は、共同性を性質として有する一方で、共同委託者が互いに独立しており相互の合意をとる必要が無い（匿名性）ものの、安全対策上データの所在地把握等の統制方法に固有の留意が必要となる。

後者は、まず、金融機関の委託先が複数となる場合には、統制が直接可能であることから、固有の性質は生じず単数の場合と何ら異ならず、再委託により間接的に委託先が多段階にわたり複数となる場合は、再委託先に対して金融機関による統制が及びにくくなることから、固有の性質がある類型となる（詳細は外部委託検討会報告書を参照）。

以上を、まとめると以下のとおりとなる。

２者関係の基本的類型



以上を踏まえて３者関係の類型を考えることとなるが、まず、３者の中の２者関係を類型化することは不要である。これは、金融機関が、FinTech企業とFinTech業務を実施するに当たっては、当然のことながら情報システムが必要であり、金融機関やFinTech企業においては、そのために必要となる情報システムの開発や運用といった資源を外部から調達すること、すなわちITベンダーに外部委託することが一般的であると考えられることによる。（特に、業務を開始したばかりのFinTech企業においては、ITベンダーの中でも、クラウド事業者に委託することが多いと言われている[73]。）

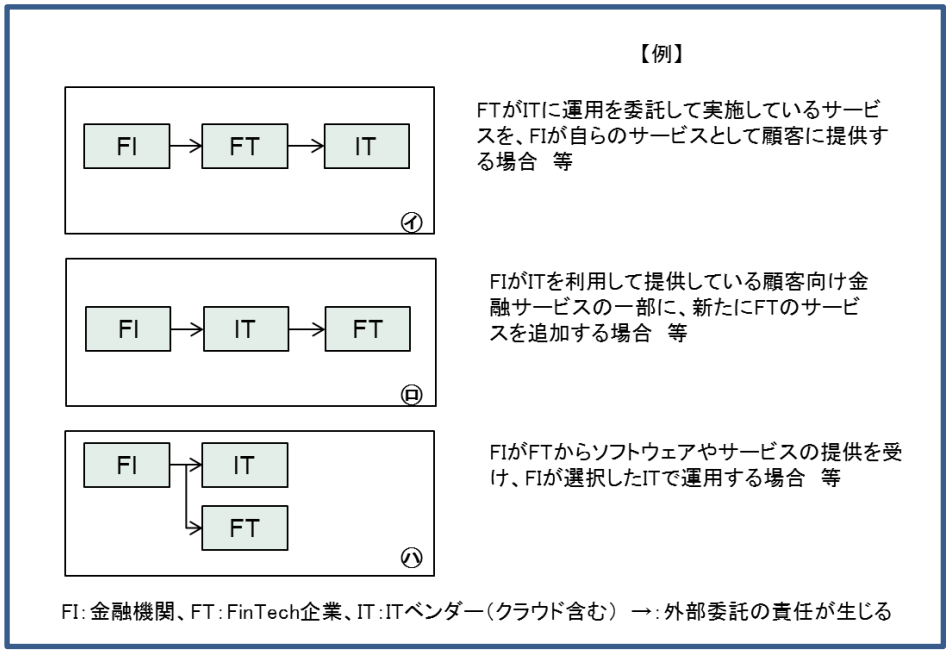
したがって、金融機関とFinTech企業、ITベンダーといった３者の単数及び複数の関係性を整理すれば十分[74]と考えられる。まず、３者がいずれも単数である場合については、金融機関は常に委託元となることから、残り２者の組み合わせに応じて、以下の類型が検討すべき類型として考えられる。

---

[73] 日本銀行金融システムレポート別冊シリーズ「IT の進歩がもたらす金融サービスの新たな可能性とサイバーセキュリティ」（2016 年３月）によれば、FinTech が、金融機関がこれまで提供してきた金融サービスと異なる点の１つとして「クラウドサービスやオープンソース・ソフトウェアのように社外の資産・サービスを積極的に活用することは、準備期間を短縮し、機動的にサービスを提供できる強みにもなっている。」としている。また、FISC『クラウド検討会報告書』によれば、クラウドは、スモールスタートに適する拡張性や柔軟性や、新技術導入スピードが速く、また、モバイル端末や SNS（ソーシャル・ネットワーキング・サービス）等との親和性が高いといった利便性や機能の向上、等のメリットを有しているとされている。

[74] なお、FinTech 企業の業務的性質と技術的性質が内部的に峻別可能であれば、２者関係に還元可能とする考え方も理論的にはありうるが、FinTech 企業の内部的な実態は多様であり、明確にその性質を峻別することは難しいものと考える。

３者が単数の場合に考えられる類型



次に、以上の類型において、３者のいずれかが複数となる場合について、取り上げるべき基本的類型があるかどうかを整理する。まず、IT ベンダーが複数となる場合は、２者関係の基本的類型の考え方を前提にすれば、新たな類型を想定することは不要と考えられる。すなわち、金融機関の委託先である IT ベンダーが複数となる場合は、金融機関による直接の統制が可能であることから、固有の性質は生じない。一方、IT ベンダーまたは FT 企業を通じて複数の IT ベンダーに再委託を行った場合は、固有の性質がある類型として、既に外部委託検討会において包括的に検討済みであることから、本検討会において個別の検討は不要と考えられる。

次に、FinTech 企業が複数となる場合は、FinTech 企業の業務的性質に着目すると、金融機関あるいは IT ベンダーが複数の FinTech 企業に対して個々の業務的役割を決定していると考えられることから、共同性のような固有の性質が生じることはない。また、FinTech 企業の技術的性質に着目すると、IT ベンダーが複数の場合と何ら異ならない。したがって、FinTech 企業が複数となる場合においても、個別の検討は不要と考えられる。

最後に、金融機関が複数となる場合は、既に２者関係の基本的類型の考え方で整理された共同性の性質以外に固有の性質はないと考えられる。

以上のことから、３者が複数となる場合は、いずれも検討は不要と考えられる。

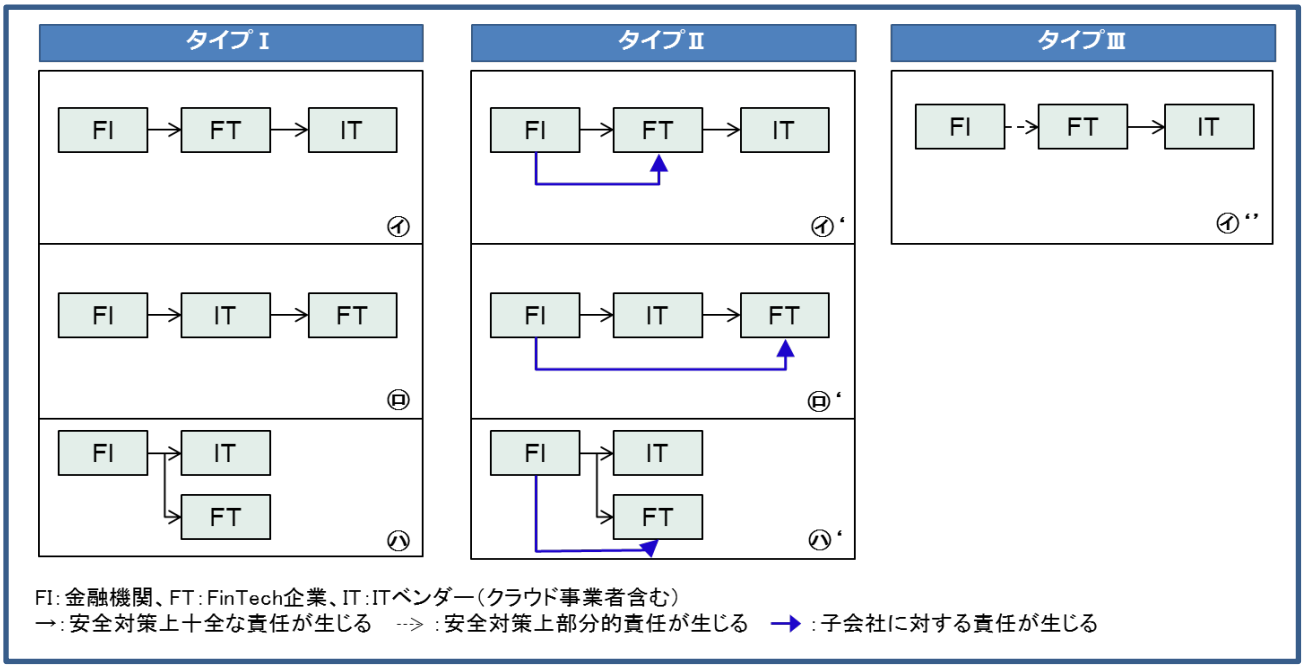
（注）　今後、金融機関に部分的に安全対策上の責任が生じる場合等 FinTech に関する安全対策の在り方を検討する中で固有の性質があるものとして、基本的類型が追加される可能性は残る。

しかしながら、３者関係における基本的類型の特定が、従来の安対基準を FinTech 業務に適用した場合に内在する問題を析出することを目的としていることに鑑みれば、現段階で、基本的類型の理論的正当性を議論するよりも、検討が必要であることが明らかな類型から、内在する問題の検討を進めるのが適切である。今後、新たな類型を取り上げることの必要性が明らかになれば、その際にあらためて立ち返って検討を行うこととする。

３．FinTech 業務タイプ別類型

以上の考察を総合すると、本検討において前提とすべき、FinTech 業務のタイプ別の類型は以下のとおりとなる。

FinTech 業務において安全対策実施上の関係者のタイプ別類型



【資料４】従来の安対基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注１）	金融機関の一次委託先として負う責務（責務B－１）	金融機関の再委託先に対する責務（責務B－２）	金融機関の再委託先として負う責務（責務C）
a.利用検討時	1	委託目的と範囲の明確化	必要	運 87 1. 2.	外部委託を行う場合は、事前に目的や範囲等を明確にすること。	－	－	－
			必要	運 108 1. 2.				
	2	選定手続きの明確化	必要	運 87-1 1.	外部委託先を選定するに当たっては、選定手続きを明確にすること。 （再委託先の選定要件をあらかじめ定めることを含む）	－	－	－
			必要	運 108 1.				
			必要	外部委託有識者検討会 Ⅳ.4.(1)				
	3	客観的評価の実施	必要	運 87-1 2.	外部委託先を客観的に評価すること。 なお、当該業務に求められるリスク管理レベルを検討のうえ、その実現が可能な外部委託先を選定すること。その際、外部委託先の資質・業務遂行能力に関する情報や、外部委託先の内部統制やリスク管理に関する状況等をもとに評価を行うことが必要である。	金融機関が客観的評価を実施するために必要とする情報を、金融機関に提供する責務がある。	金融機関の再委託先を客観的に評価する責務がある。	一次委託先が客観的評価を実施するために必要とする情報を、一次委託先に提供する責務がある。
			必要	運 108 3.				
	4	機密保持契約の事前締結	望ましい	運 108 3.	評価に当たっては、必要に応じ機密保持契約を事前に締結することが望ましい。	－	－	－
	5	（委託業務の重要度が高くない場合）公開情報や評判、実績等による客観的評価の実施	可能	運 108 3.	金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合は、公開情報や業界における評判や実績等による客観的な評価を行うことも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断した場合は、金融機関の再委託先の公開情報や業界における評判や実績等により、客観的な評価を行うことも可能である。	－
	6	契約中断・終了に伴う移行作業の事前把握	望ましい	運 108 3.(11)	外部委託契約の中断・終了に伴うシステム移行作業(移行データの抽出方法と実際の移行作業内容)については、サービス利用前に把握することが望ましい。	－	－	－

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注１）	金融機関の一次委託先として負う責務（責務B－１）	金融機関の再委託先に対する責務（責務B－２）	金融機関の再委託先として負う責務（責務C）
a.利用検討時	7	データの所在の把握	必要	運 1084.	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)を把握する必要がある。	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)について、金融機関に情報を提供する責務がある。	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)を把握する責務がある。	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)について、一次委託先に情報提供する責務がある。
			必要	運 1084.	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する必要がある。	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、金融機関等がデータセンターの立地状況等を見極める観点から、金融機関に詳細な所在地まで情報提供する責務がある。	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する責務がある。	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、一次委託先等がデータセンターの立地状況等を見極める観点から、一次委託先に詳細な所在地まで情報提供する責務がある。
			必要	運 1084.	インシデント発生時にデータセンターへの立入が必要になる場合や立入監査を行う際には、具体的な所在地を把握する必要がある。	インシデント発生時に金融機関がデータセンターへ立ち入る必要がある場合や立入監査を行う際には、具体的な所在地を金融機関に情報提供する責務がある。	インシデント発生時にデータセンターへ立ち入る必要がある場合や立入監査を行う際には、具体的な所在地を把握する責務がある。	インシデント発生時に一次委託先がデータセンターへ立ち入る必要がある場合や立入監査を行う際には、具体的な所在地を一次委託先に情報提供する責務がある。
		（委託業務の重要度が高くない場合）データの所在の把握の必要性	可能	運 1084.	金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合には、データの所在地に関する情報の把握について省略することも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断した場合は、データの所在地に関する情報の把握について省略することも可能である。	－
	8	他国で係争が発生することを想定して評価すべきリスク	必要	運 1085.	外部委託先との間で係争が生じた場合の準拠法やこれを取り扱う裁判所に関する取決めが他国である場合に、外部委託先の選定に当たってリスクを評価すること。	－	－	－

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
a.利用検討時	9	責任者による事業者決定の承認	必要	運 87-13.	委託業者の決定には、最終的には責任者の承認を得ること。	－	－	－
			必要	運 1086.				
	10	（パッケージ導入の場合） 評価体制の整備及び運営・管理体制の明確化	必要	運 87-14.	外部委託先が所有するアプリケーション、サービス等の導入に際しては、【運 72、運 73】も参照のこと。	パッケージを導入する場合、金融機関がパッケージの評価等を行うために必要とする情報を、金融機関に提供する責務がある。	パッケージを導入する場合、パッケージの有効性、信頼性、生産性等を評価する体制を整備する責務がある。また、パッケージの運用・管理体制を明確にする責務がある。	パッケージを導入する場合、一次委託先がパッケージの評価等を行うために必要とする情報を、一次委託先に提供する責務がある。
			望ましい	運 1087.	パッケージを導入する場合は、必要に応じて【運 72、運 73】を参照すること。			
b.契約締結時	11	安全対策を盛り込んだ委託契約の締結	必要	運 881.	外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として外部委託先と締結すること。	金融機関が外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として、金融機関と締結する責務がある。	外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として、金融機関の再委託先と締結する責務がある。	一次委託先が外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として、一次委託先と締結する責務がある。
			必要	運 1091.				
	12	事業者からの情報開示	必要（注 2）	運 1091.(9)	金融機関とクラウド事業者が協議のうえ、必要な情報をクラウド事業者が提供することを契約上明記すること。	金融機関が必要とする情報の提供について、金融機関との契約上明記する責務がある。	金融機関の再委託先と協議のうえ、必要な情報を金融機関の再委託先が提供することを契約上明記する責務がある。	一次委託先が必要とする情報の提供について、一次委託先との契約上明記する責務がある。
			必要（注 2）	運 1091.(9)	開示請求の対象情報の機密性が高い場合には、両者の間で機密保持契約を締結したうえで提供すること。	開示請求の対象情報の機密性が高い場合には、両者（金融機関と一次委託先）の間で機密保持契約を締結したうえで提供する責務がある。	開示請求の対象情報の機密性が高い場合には、両者（一次委託先と金融機関の再委託先）の間で機密保持契約を締結したうえで提供する責務がある。	開示請求の対象情報の機密性が高い場合には、両者（一次委託先と金融機関の再委託先）の間で機密保持契約を締結したうえで提供する責務がある。

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	12	事業者からの情報開示	必要（注 2）	運 109 1.(9)	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくはクラウド事業者側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けた時には、請求内容に応じた情報開示を行っていくべきことを契約や SLA に明記すること。	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくは金融機関の再委託先側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けた時には、請求内容に応じた情報開示を行っていくべきことを金融機関との契約や SLA に明記する責務がある。	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくは金融機関の再委託先側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けた時には、請求内容に応じた情報開示を行っていくべきことを金融機関の再委託先との契約や SLA に明記する責務がある。	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくは金融機関の再委託先の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、一次委託先からの開示請求を受けた時には、請求内容に応じた情報開示を行っていくべきことを一次委託先との契約や SLA に明記する責務がある。
		（委託業務の重要度が高くない場合）事業者からの詳細かつ厳格な情報開示	可能	運 109 1.(9)	金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合には、外部委託先に対し、リスク管理に直結する事項等の情報を詳細かつ厳格に求めないことも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断した場合は、金融機関の再委託先に対し、リスク管理に直結する事項等の情報を詳細かつ厳格に求めないことも可能である。	－
	13	（複数事業者へ委託する場合）事業者間の相互調整機能を担う事業者の事前決定	必要（注 2）	運 109 1.(10)	障害発生時等の迅速な対応のため、委託元金融機関の管理能力を踏まえ、委託元金融機関・外部委託先間での責任関係を明確にし、一元的な窓口機能や外部委託先間の相互調整機能を担う事業者をあらかじめ決めておくこと。 なお、この役割を委託元金融機関が担える場合においては、外部委託先側の相互調整機能を担う事業者は必要ではない。	－	－	－
		（委託業務の重要度が高くない場合）調整機能役の事業者設置の必要性	可能	運 109 1.(10)	金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合、かつリスク分析の結果として、障害発生時の影響範囲が限定的である、もしくは復旧自体が遅れてもその影響が軽微であると判断しうる場合は、相互調整を担う事業者を置かないことも可能である。	－	－	－

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	14	委託先への監査権の明記	必要	運 88 4.(15)	外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し契約を締結することが必要である。	金融機関が外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し、金融機関と契約を締結する責務がある。	外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(金融機関の再委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し、金融機関の再委託先と契約を締結する責務がある。	一次委託先が外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し、一次委託先と契約を締結する責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(2)	「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。	「重要な情報システム」を受託する場合は、金融機関との委託契約の締結に当たっては、金融機関の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責務がある。	「重要な情報システム」を金融機関の再委託先に外部委託する場合は、金融機関の再委託先との委託契約の締結に当たっては、金融機関の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責務がある。	「重要な情報システム」を受託する場合は、一次委託先との委託契約の締結に当たっては、金融機関の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責務がある。
			可能	外部委託有識者検討会 Ⅳ.4.(2)	監査に当たっては、みずからが実施する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。	－	監査に当たっては、みずからが実施する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。	－
			可能	外部委託有識者検討会 Ⅳ.4.(2)	「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。	－	金融機関が「重要な情報システム」以外の情報システムを外部委託し、かつ金融機関の再委託先への監査権を明記しない場合は、金融機関の再委託先との委託契約の締結に当たって、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。	－

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	14	委託先への監査権の明記	可能	外部委託有識者検討会 Ⅳ.4.(2)	「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。	－	金融機関が「重要な情報システム」を外部委託し、かつ再委託業務のリスクが十分低いと判断し、簡易な手続きで代替した場合は、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。	－
	15	立入監査等の権利の明記	必要（注 2）	運 109 1.(12)	業務委託契約に、委託元金融機関等の立入監査等を実施する権利を明記すること。	金融機関との業務委託契約に、金融機関等の立入監査等を実施する権利を明記する責務がある。	金融機関の再委託先との業務委託契約に、一次委託先が再委託先に立入監査等を実施する権利を明記する責務がある。	一次委託先との業務委託契約に、一次委託先等の立入監査等を実施する権利を明記する責務がある。
	16	立入監査等の代替手段の明記	必要（注 2）	運 109 1.(12)	委託元金融機関が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替することも可能とすること。	金融機関等が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替可能である。	一次委託先が金融機関の再委託先に直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替することも可能とする責務がある。	一次委託先等が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替可能である。
	17	立入監査等の権利行使の明記	必要（注 2）	運 109 1.(12)	クラウド技術に関する重要な脆弱性が判明した場合、クラウド事業者における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、委託元金融機関への影響を確認するため、臨時の第三者監査を行うことが可能となっていること。	クラウド技術に関する重要な脆弱性が判明した場合、金融機関の再委託先における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、金融機関等への影響を確認するため、臨時の第三者監査の実施が可能となっている責務がある。	クラウド技術に関する重要な脆弱性が判明した場合、金融機関の再委託先における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、金融機関等への影響を確認するため、臨時の第三者監査を行うことが可能となっている責務がある。	クラウド技術に関する重要な脆弱性が判明した場合、自社における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、一次委託先等への影響を確認するため、臨時の第三者監査の実施が可能となっている責務がある。

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	17	（立入監査等の実施が限定されている場合） 立入監査等の権利行使の条件の認識共有	可能	運 109 1.(12)	立入監査等に代替する第三者監査が行われない、または依拠できないと判断される場合に限定して立入監査等を行う運用形態を取る場合は、立入監査等の権利行使の条件を必要に応じ書面化し、委託元金融機関とクラウド事業者の両者が認識を共有することも可能である。	－	立入監査等に代替する第三者監査が行われない、または依拠できないと金融機関が判断した場合に限定して、立入監査等を行う運用形態を取る場合は、立入監査等の権利行使の条件を必要に応じ書面化し、一次委託先と金融機関の再委託先の両者が認識を共有することが可能である。	－
	18	立入監査等の受入対応費用の明記	必要 （注 2）	運 109 1.(12)	立入監査を受けるクラウド事業者側の受入対応の費用については、委託元金融機関、クラウド事業者側のいずれが負担するか、あらかじめ両者で協議しておくこと。	立入監査を受ける一次委託先側の受入対応の費用については、金融機関、一次委託先側のいずれが負担するか、あらかじめ両者で協議しておく責務がある。	立入監査を受ける金融機関の再委託先側の受入対応の費用については、一次委託先、金融機関の再委託先側のいずれが負担するか、あらかじめ両者で協議しておく責務がある。	立入監査を受ける金融機関の再委託先の受入対応の費用については、一次委託先、金融機関の再委託先側のいずれが負担するか、あらかじめ両者で協議しておく責務がある。
	19	再委託先への立入監査権の明記	必要 （注 2）	運 109 1.(12)	再委託する業務が重要な場合、再委託先等に対して、委託元金融機関とクラウド事業者間の契約に、金融機関による再委託先への立入監査を実施する権利を明記すること。	金融機関が再委託する業務が重要な場合、金融機関の再委託先等に対して、金融機関と一次委託先間の契約に、金融機関による再委託先への立入監査を実施する権利を明記する責務がある。	金融機関が再委託する業務が重要な場合、金融機関の再委託先等に対して、一次委託先と金融機関の再委託先間の契約に、金融機関による再委託先への立入監査を実施する権利を明記する責務がある。	金融機関が再委託する業務が重要な場合、金融機関の再委託先等に対して、一次委託先と金融機関の再委託先間の契約に、金融機関による再委託先への立入監査を実施する権利を明記する責務がある。
	20	立入監査等の指摘事項の扱いの明記	必要 （注 2）	運 109 1.(12)	立入監査等により判明した指摘事項については、対応の是非を含め、委託元金融機関とクラウド事業者の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にすること。	立入監査等により判明した指摘事項については、対応の是非を含め、金融機関と一次委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする責務がある。	立入監査等により判明した指摘事項については、対応の是非を含め、一次委託先と金融機関の再委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする責務がある。	立入監査等により判明した指摘事項については、対応の是非を含め、一次委託先と金融機関の再委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする責務がある。

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	21	金融監督当局の検査等の明記	必要（注 2）	運 109 1.(13)	当局の立入り検査等の円滑な実施を担保するため、委託元金融機関と外部委託先との間の契約に、外部委託先の当局検査等への協力義務を明記すること。	当局の立入り検査等の円滑な実施を担保するため、金融機関と一次委託先との間の契約に、一次委託先の当局検査等への協力義務を明記する責務がある。	当局の立入り検査等の円滑な実施を担保するため、一次委託先と金融機関の再委託先との間の契約に、金融機関の再委託先の当局検査等への協力義務を明記する責務がある。	当局の立入り検査等の円滑な実施を担保するため、一次委託先と金融機関の再委託先との間の契約に、一次委託先の当局検査等への協力義務を明記する責務がある。
			必要（注 2）	運 109 1.(13)	業務委託の再委託先(再々委託先を含む)に対しても、金融機関と元請け事業者との間の契約に、当局検査等への協力義務を明記すること。	業務委託の再委託先(再々委託先を含む)に対しても、金融機関と一次委託先との間の契約に、当局検査等への協力義務を明記する責務がある。	業務委託の再委託先(再々委託先を含む)に対しても、一次委託先と金融機関の再委託先との間の契約に、当局検査等への協力義務を明記する責務がある。	業務委託の再委託先(再々委託先を含む)に対しても、一次委託先と金融機関の再委託先との間の契約に、当局検査等への協力義務を明記する責務がある。
			必要（注 2）	運 109 1.(13)	当局検査等の指摘事項については、速やかに改善を図る旨の条項を契約に明記すること。	当局検査等の指摘事項については、速やかに改善を図る旨の条項を、金融機関と一次委託先との間の契約に明記する責務がある。	当局検査等の指摘事項については、速やかに改善を図る旨の条項を、一次委託先と金融機関の再委託先との間の契約に明記する責務がある。	当局検査等の指摘事項については、速やかに改善を図る旨の条項を、一次委託先と金融機関の再委託先との間の契約に明記する責務がある。
	22	インシデント発生時の立入調査の明記	必要（注 2）	運 109 1.(14)	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、クラウド事業者が情報提供に応じない、提供しても迅速性に問題があると金融機関が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、委託元金融機関みずから、もしくは委託元金融機関が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記すること。	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、金融機関の再委託先が情報提供に応じない、提供しても迅速性に問題があると金融機関が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、金融機関みずから、もしくは金融機関が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記する責務がある。	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、金融機関の再委託先が情報提供に応じない、提供しても迅速性に問題があると一次委託先が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、一次委託先みずから、もしくは一次委託先が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記する責務がある。	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、金融機関の再委託先が情報提供に応じない、提供しても迅速性に問題があると一次委託先が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、一次委託先みずから、もしくは一次委託先が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記する責務がある。

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	22	インシデント発生時の立入調査の明記	必要（注 2）	運 109 1.(14)	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、契約締結時に合意を得ること。	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、金融機関との契約締結時に合意を得る責務がある。	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、金融機関の再委託先との契約締結時に合意を得る責務がある。	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、一次委託先との契約締結時に合意を得る責務がある。
			必要（注 2）	運 109 1.(14)	クラウド事業者の経営不安が発生した場合、委託元金融機関みずからもしくは委託元金融機関が指定する専門業者が、必要に応じ、クラウド事業者施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことを認めるよう契約に明記すること。	金融機関の再委託先の経営不安が発生した場合、金融機関みずからもしくは金融機関が指定する専門業者が、必要に応じ、金融機関の再委託先施設に立ち入り、顧客データや関連著作物・成果物を保全することに協力することを契約に明記する責務がある。	金融機関の再委託先の経営不安が発生した場合、一次委託先みずからもしくは一次委託先が指定する専門業者が、必要に応じ、金融機関の再委託先施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことを認めるよう契約に明記する責務がある。	自社の経営不安が発生した場合、一次委託先みずからもしくは一次委託先が指定する専門業者が、必要に応じ、自社施設に立ち入り、顧客データや関連著作物・成果物を保全することに協力することを契約に明記する責務がある。
	23	（海外でのデータ保管時の場合） 日本語サポート及び障害対応窓口設置の明確化	必要（注 2）	運 109 1.(16)	金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、外部委託先の日本法人等の障害対応窓口設置を明確にすること。	金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、一次委託先の日本法人等の障害対応窓口の設置に関する情報を、金融機関に提供する責務がある。	一次委託先における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、金融機関の再委託先の日本法人等の障害対応窓口設置を明確にすること。	金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、一次委託先の日本法人等の障害対応窓口の設置に関する情報を、一次委託先に提供する責務がある。
	24	トレーサビリティ確保の準備	必要（注 2）	運 109 1.(17)	万一障害や情報漏洩等のインシデントが発生した際には、流出・毀損したデータの特定や原因究明のための作業が複雑化する場合があることが想定されるため、トレーサビリティ確保のための方策を準備すること。	万一障害や情報漏洩等のインシデントが発生した際には、金融機関からの求めに応じて、トレーサビリティ確保のための方策を準備する責務がある。	万一障害や情報漏洩等のインシデントが発生した際には、金融機関からの求めに応じて、トレーサビリティ確保のための方策を金融機関の再委託先に準備させる責務がある。	万一障害や情報漏洩等のインシデントが発生した際には、一次委託先からの求めに応じて、トレーサビリティ確保のための方策を準備する責務がある。

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	25	再委託先の事前審査の明確化	必要（注 2）	運 109 1.(11)	外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、委託業務を再委託する場合、再委託先に対する適切な事前審査を行うこと。 勘定系システムや機密性の高い顧客データを保管するシステム等、特に重要な業務を再委託する場合には、金融機関等みずからが事前審査をすること。	金融機関が外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、金融機関が委託業務を再委託する場合、金融機関の再委託先に対する適切な事前審査を行うことに対応する責務がある。	金融機関が外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、一次委託先が金融機関の再委託先に業務委託する場合、再委託先に対する適切な事前審査を行う責務がある。	金融機関が外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、金融機関が委託業務を再委託する場合、一次委託先が金融機関の再委託先に対する適切な事前審査を行うことに対応する責務がある
			必要	外部委託有識者検討会 Ⅳ.4.(1)				
		（「重要な情報システム」以外の情報システムの再委託の場合） 再委託先の事前審査の代替	可能	外部委託有識者検討会 Ⅳ.4.(1)	「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・運用状況の適切性検証することで、そうした検証結果の確認をもって、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。	－	－	－
		（委託業務の重要度が高くない場合） 再委託先の事前審査の簡易化	可能	運 109 1.(11)	金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合は、再委託先における委託元金融機関による事前の審査や日常のモニタリング等のリスク管理を簡易化することも可能である。	－	－	－
	26	サービスレベルの合意	望ましい	運 88 5.	SLA の締結や SLO の確認により、サービスレベルについて合意することが望ましい。	SLA の締結や SLO の確認により、サービスレベルについて、金融機関と合意する責務がある。	SLA の締結や SLO の確認により、サービスレベルについて、金融機関の再委託先と合意する責務がある。	SLA の締結や SLO の確認により、サービスレベルについて、一次委託先と合意する責務がある。
			望ましい	運 109 2.				

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
b.契約締結時	26	（委託業務の重要度が高くない場合） SLA 締結の省略	可能	運 109 3.	金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合には、クラウド事業者が提示する標準的な SLA を締結することや一般的な契約の締結のみを行い、SLA の締結を省略することも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断し、かつ金融機関の再委託先が提示する標準的な SLA を締結することや一般的な契約の締結のみを行い、SLA の締結を省略した場合は、金融機関の再委託先が提示する標準的な SLA を締結することや一般的な契約の締結のみを行い、SLA の締結を省略することも可能である。	－
	27	代替サービスや他への移行の事前準備	望ましい	運 109 4.	サービスレベル合意の違反のほか、クラウド事業者や金融機関の方針変更によってクラウド事業者との契約の続行が困難になるような場合でも、業務の継続を可能とするため、事前に代替のクラウドサービスや一般のアウトソーシングに移行する、もしくはオンプレミスの環境に移行することができるような対策を講ずることが望ましい。	－	－	－
		（委託業務の重要度が高くない場合） 外部委託先の協力を前提としないシステム移行準備	可能	運 109 4.	金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断しうる場合は、外部委託先の協力を前提とせず、別の外部委託先に移行するための準備をあらかじめ行っておくことをもって代替することが可能である。	－	－	－
c.開発時	開発の外部委託については、「必要最低限の安対基準」の適用対象とすることが可能（注 3）							

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
d.運用時	28	データ管理委託時の漏洩防止策の実施	必要	運 110 1.	外部委託先にデータ管理を委託する場合、漏洩防止策を講ずること。	金融機関からデータ管理を受託する場合、金融機関からの求めに応じて、漏洩防止策を講じる責務がある。	金融機関の再委託先にデータ管理を委託する場合、金融機関からの求めに応じて、金融機関の再委託先に、漏洩防止策を実施させる責務がある。	一次委託先からデータ管理を受託する場合、一次委託先からの求めに応じて、漏洩防止策を講じる責務がある。
		蓄積・伝送データの暗号化の実施	必要	運 110 1.(1)	機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じること。 なお、仕様上の制約から暗号化が不可能な部分(平文で処理される部分)でのデータ覗き見リスクを把握するため、暗号化の仕様を把握し、自社のリスク管理のポリシーに合致しているかどうか判断する必要がある。	機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じる責務がある。 なお、金融機関がリスク管理のポリシーに合致しているかどうかを判断するため、金融機関に暗号化の仕様に関する情報を提供する責務がある。	機密性の高い個人データ等が含まれているデータについては、金融機関の再委託先に対して暗号化等の管理策を求める責務がある。 なお、仕様上の制約から暗号化が不可能な部分(平文で処理される部分)でのデータ覗き見リスクを把握するため、暗号化の仕様を把握し、自社のリスク管理のポリシーに合致しているかどうか判断する責務がある。	機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じる責務がある。 なお、一次委託先がリスク管理のポリシーに合致しているかどうかを判断するため、一次委託先に暗号化の仕様に関する情報を提供する責務がある。
		暗号鍵の管理主体の適切性確認	必要	運 110 1.(2)	クラウド事業者に暗号鍵の管理を委ねる場合には、その管理策の概要を十分に把握し、自社のリスク管理ポリシーに合致していることを判断する必要がある。	金融機関の再委託先に暗号鍵の管理を委ねる場合には、金融機関がその管理策の概要を十分に把握し、リスク管理のポリシーに合致しているかどうかを判断するため、金融機関に暗号化の仕様に関する情報を提供する責務がある。	金融機関の再委託先に暗号鍵の管理を委ねる場合には、その管理策の概要を十分に把握し、自社のリスク管理ポリシーに合致していることを判断する責務がある。	金融機関の再委託先に暗号鍵の管理を委ねる場合には、一次委託先がその管理策の概要を十分に把握し、リスク管理のポリシーに合致しているかどうかを判断するため、一次委託先に暗号化の仕様に関する情報を提供する責務がある。
		暗号化の代替策の実施	必要	運 110 1.(3)	元データとトークンを金融機関側で持ち、クラウド環境下にあるデータを無作為な乱数に置き換え、実質的に無意味化するとしたトークン化技術を利用することが可能である。 ただし、トークン化を管理策として採用する場合には、金融機関におけるトークンマッピング(対応表)の管理についても相応の管理策が必要となる。	－	－	－

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
d.運用時	29	記憶装置等の障害・交換におけるデータ消去の実施	必要	運 110 2.	外部委託先の記憶装置の故障等により、機器・部品を交換する場合には、交換対象の記憶装置等の機器・部品に金融機関等やその顧客の情報等の機密性の高いデータが残存している可能性があるため、これらの記憶装置等に対して、データ消去を含めた十分な管理を行う必要がある。	一次委託先の記憶装置の故障等により、機器・部品を交換する場合には、金融機関からの求めに応じて、これらの記憶装置等に対して、データ消去を含めた十分な管理を行う責務がある。	金融機関の再委託先の記憶装置の故障等により、機器・部品を交換する場合には、金融機関からの求めに応じて、金融機関の再委託先に、これらの記憶装置等に対して、データ消去を含めた十分な管理を行わせる責務がある。	金融機関の再委託先の記憶装置の故障等により、機器・部品を交換する場合には、一次委託先からの求めに応じて、これらの記憶装置等に対して、データ消去を含めた十分な管理を行う責務がある。
		記憶装置等の障害・交換時の消去証明書代替策	可能	運 110 2.	契約中の記憶装置等の障害・交換における消去証明書の発行・取得については、クラウド事業者に対して情報提出要請や監査等の方法で消去・破壊プロセスの実効性を検証することで代替することも可能である。	－	契約中の記憶装置等の障害・交換における消去証明書の発行・取得については、金融機関の再委託先に対して情報提出要請や監査等の方法で消去・破壊プロセスの実効性を検証することで代替可能である。	－
		（重要なデータを扱わない場合）データ消去・破壊の必要性	可能	運 110 2.	外部委託先で重要なデータを扱わない場合は、記憶装置等の交換に際し、データの消去・破壊を実施しないことも可能である。	－	－	－
	30	委託業務の日常的監視	必要	運 89 1. 2. 3.	外部委託業務を円滑かつ適正に運営する観点から、委託先の業務範囲や責任、委託先要員の遵守すべきルールを明確にし、日常的に監視する必要がある。	金融機関からの日常的監視を受忍する責務がある。	外部委託業務を円滑かつ適正に運営する観点から、金融機関の再委託先の業務範囲や責任、要員が遵守すべきルールを明確にし、日常的に監視する責務がある。	一次委託先からの日常的監視を受忍する責務がある。
			必要	運 90 1. 2. 3.				
			必要	運 112 1. 2.				

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
d.運用時	31	システム監査体制の整備	必要	運 91 1. 2. 3. 4. 5. 6.	外部委託業務に関するコンピュータシステムの運用、開発・変更等において、有効性、効率性、信頼性、遵守性、及び安全性を確保するため、独立した監査人がコンピュータシステムの総合的な監査・評価を行い、経営層に監査結果を報告する体制を整備する必要がある。	受託業務に関するコンピュータシステムの運用、開発・変更等において、独立した監査人が実施するコンピュータシステムの総合的な監査・評価を受忍する責務がある。	外部委託業務に関するコンピュータシステムの運用、開発・変更等において、有効性、効率性、信頼性、遵守性、及び安全性を確保するため、独立した監査人がコンピュータシステムの総合的な監査・評価を行う責務がある。	受託業務に関するコンピュータシステムの運用、開発・変更等において、独立した監査人が実施するコンピュータシステムの総合的な監査・評価を受忍する責務がある。
		立入監査の実施	必要	運 112 2.	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、クラウド事業者のオフィスやデータセンターへの立入監査・モニタリング等により実地で確認することが必要である。	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、自社のオフィスやデータセンターへの金融機関による立入監査・モニタリング等により実地で確認を受忍する責務がある。	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、金融機関の再委託先のオフィスやデータセンターへの立入監査・モニタリング等により実地で確認する責務がある。	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、自社のオフィスやデータセンターへ立入監査・モニタリング等により実地で確認を受忍する責務がある。
		第三者監査の実施	可能	運 112 3.	外部委託先に対する実地調査(オンサイトモニタリング)が有効ではない場合などに、第三者監査で代替することが可能である。	－	金融機関の再委託先に対する実地調査(オンサイトモニタリング)が有効ではない場合などに、第三者監査で代替することが可能である。	－
			必要	外部委託有識者検討会 脚注 40 （注 4）	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。	第三者から見た際に、金融機関からの求めに応じて、金融機関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責務がある。	第三者から見た際に、金融機関からの求めに応じて、金融機関の再委託先に、金融機関の再委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定させる責務がある。	第三者から見た際に、一次委託先からの求めに応じて、一次委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定する責務がある。

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注１）	金融機関の一次委託先として負う責務（責務B－１）	金融機関の再委託先に対する責務（責務B－２）	金融機関の再委託先として負う責務（責務C）
d.運用時	31	（委託業務の重要度が高くない場合） 費用対効果を踏まえた管理策の実施	可能	運 112 4.	外部委託業務の重要度が高くない場合は、費用対効果を踏まえ、立入監査の代わりに、第三者認証等を活用することが可能である。	－	金融機関等が外部委託業務の重要度が高くないと判断する場合は、金融機関の再委託先への委託業務について、費用対効果を踏まえ、立入監査の代わりに、第三者認証等を活用することが可能である。	－
e.終了時	32	契約終了時の機密保護・プライバシー保護・不正防止対策の実施	必要	運 111 1.	外部委託契約を終了する場合、データ漏洩防止のため、機密保護、プライバシー保護及び不正防止のための対策を講じる必要がある。	外部委託契約を終了する場合、金融機関からの求めに応じて、機密保護、プライバシー保護及び不正防止のための対策を講じる責務がある。	外部委託契約を終了する場合、金融機関からの求めに応じて、金融機関の再委託先に、機密保護、プライバシー保護及び不正防止のための対策を実施させる責務がある。	外部委託契約を終了する場合、一次委託先からの求めに応じて、機密保護、プライバシー保護及び不正防止のための対策を講じる責務がある。
		データ消去方法の種類	必要	運 111 2.	データ消去に当たっては、物理的消去と論理的消去が考えられる。 なお、将来的なハードウェア更改・撤去時に物理的消去を行うことが望ましい。 （注）論理的消去の実施のみでも可	データ消去に当たっては、金融機関からの求めに応じて、論理的消去を実施する責務がある。	データ消去に当たっては、金融機関からの求めに応じて、金融機関の再委託先に、論理的消去を実施させる責務がある。	データ消去に当たっては、一次委託先からの求めに応じて、論理的消去を実施する責務がある。
		消去証明書等の受領	望ましい	運 111 3.	外部委託先がデータを消去する場合、消去証明書を受領することが望ましい。	データを消去する場合、金融機関に消去証明書を提出する責務がある。	金融機関の再委託先がデータを消去する場合、消去証明書を受領する責務がある。	データを消去する場合、一次委託先に消去証明書を提出する責務がある。
		消去証明書の代替手段の実施	可能	運 111 3.	外部委託先が論理的消去も含めたデータ消去を実施することを契約書に記載し、かつ外部の第三者が監査等において、消去プロセスの適切性を検証することにより、消去証明書の発行・取得の代替とすることも可能である。	－	金融機関の再委託先が論理的消去も含めたデータ消去を実施することを契約書に記載し、かつ外部の第三者が監査等において、消去プロセスの適切性を検証することにより、消去証明書の発行・取得の代替とすることも可能である。	－

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注 1）	金融機関の一次委託先として負う責務（責務B－1）	金融機関の再委託先に対する責務（責務B－2）	金融機関の再委託先として負う責務（責務C）
e.終了時	32	（機密情報を扱わない業務委託の場合）データ消去プロセスの簡略化等	可能	運 111 4.	顧客データ等の機密情報を扱わない業務を外部委託先に委ねる場合は、契約終了時のデータ消去プロセスを簡略化または不要とすることも考えられ、消去証明書を不要とすることも可能である。	－	－	－
f.インシデント発生時	33	（重要システムの場合） 再委託先を含めた有事対応	必要	外部委託有識者検討会 Ⅳ.4.(3)	「重要な情報システム」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。	「重要な情報システム」を金融機関から受託する場合は、自社の CP は金融機関や金融機関の再委託先も含めて策定する責務がある。	「重要な情報システム」を金融機関の再委託先に外部委託する場合は、金融機関の再委託先の CP は金融機関や一次委託先も含めて策定させる責務がある。	「重要な情報システム」を一次委託先から受託する場合は、自社の CP は金融機関や一次委託先も含めて策定する責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(3)	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こと。	金融機関等で CP を個別に用意する場合は、自社の CP と完全に整合し相互補完的な内容とする責務がある。	金融機関の再委託先等で CP を個別に用意する場合は、各一次委託先等の CP と完全に整合し相互補完的な内容とさせる責務がある。	一次委託先等で CP を個別に用意する場合は、自社の CP と完全に整合し相互補完的な内容とする責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(3)	金融機関等は、平時は、委託先等との 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。	平時は、金融機関等との CP に基づき、金融機関及び金融機関の再委託先と共同で、定期的に訓練を実施する責務がある。	平時は、金融機関の再委託先等との CP に基づき、金融機関及び金融機関の再委託先と共同で、定期的に実施する訓練に参加させる責務がある。	平時は、一次委託先等との CP に基づき、金融機関及び一次委託先と共同で、定期的に訓練を実施する責務がある。

		リスク管理の実施（注 5）		運 90-1				

（注 1）「外部委託利用時の金融機関の責務（責務A）」
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）」・「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）」・「金融機関における外部委託に関する有識者検討会　報告書」に記載された内容から該当箇所を転載

（注 2）「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）」22 ページ
『クラウド報告書』において契約書に明記することが「必要である」と記載されている項目は、オンプレミスや共同センターといった外部委託でも関連性があると思われる項目であることから、今回は「実施することが望ましい」という内容の記載にとどめることとした。

（注 3）「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」43 ページ
「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。

（注 4）「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」脚注 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。

（注 5）「金融機関における FinTech に関する有識者検討会　報告書」脚注 12
なお、安対基準では、金融機関が主導的立場とならない場合として、【運 90-1】において「外部委託」とは異なる「サービス利用」に関する基準がある。この基準では「各金融機関が、外部委託の管理と全く同様に、サービスの提供元を複数の中から選定することや、独自にリスク管理を行うことは難しく、また非効率な場合が多い。」とされ、各金融機関が負担する安全対策上の責任の程度を一般の外部委託と比して、限定的に解すべきとしたものである。ただし、この基準は「金融機関相互のシステム・ネットワーク」を対象としており、今回検討の対象となっている顧客に対するサービスには該当しない。

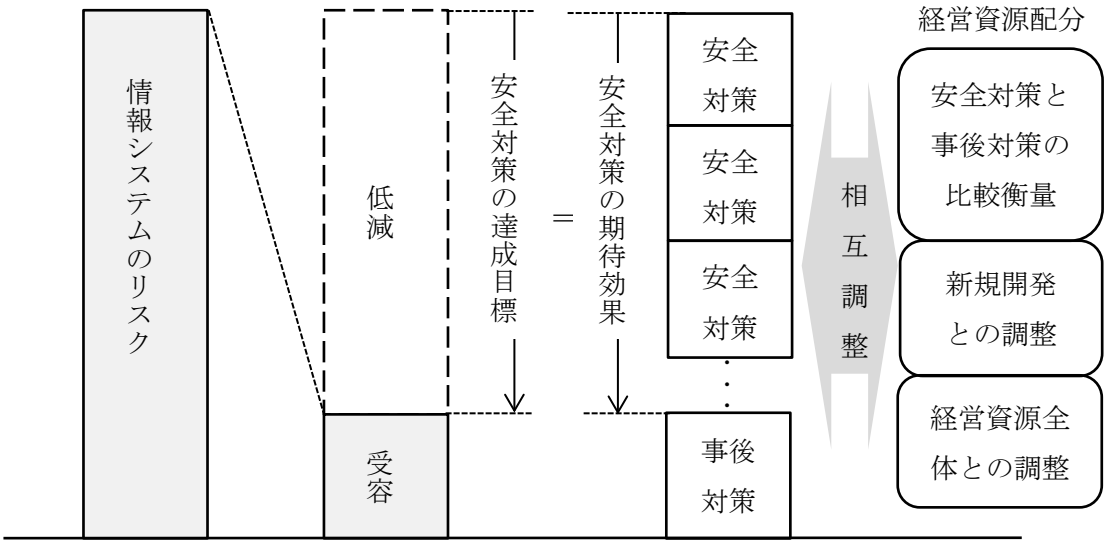
【資料５】「同等性の原則」という考え方

「同等性の原則」とは、金融業務を担う情報システムの安全対策の効果は、安全対策上の関係者に関わらず、同程度に確保されるべき、とする考え方である。この原則について、リスク評価から安全対策の決定・実施に至るプロセスを紐解きながら、責務の再配分ルールとの関係に触れつつ、解説を行う。

１．安全対策の基本原則に沿った安全対策の実施に至るプロセス

（１）リスク評価と経営層の決定

まず、安全対策の基本原則に従った IT ガバナンスに基づいて、安全対策の達成目標と個々の安全対策が導出される。



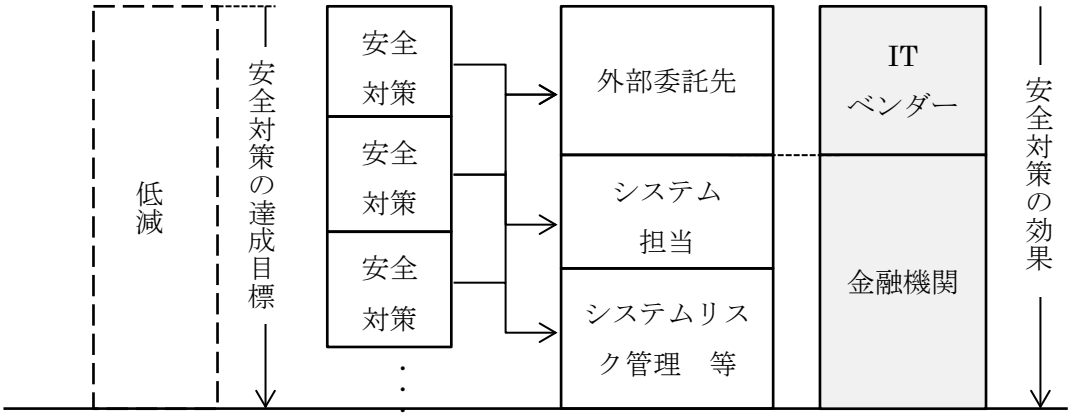
金融機関は、情報システムについて、リスク評価を通じてリスク特性を把握する。経営層は、情報システムのリスクに応じて、リスクをどの程度低減するか、あるいはどの程度受容するか[75]、を決定する。また、リスクを低減するための手段として、安全対策の達成目標を決定する。なお、安全対策の達成目標及び個々の安全対策は、リスク特性によって、安対基準を参考としながら、決定されることとなる。

また、経営層は、安全対策に対する資源配分について、経営資源全体との調整等企業価値の最大化を目指して決定する。その際に、低減のために行われる安全対策の費用と安全対策を実施しないことで生ずる事後対策の費用も比較衡量しつつ、達成目標と相互調整を行う。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。最後に、情報システム予算を超えて、経営資源全体で配分が調整される。

[75] 低減と受容以外にも、リスク顕在化時の損害を保険で手当てする「移転」や、そもそも管理責任を有する情報システムを保有しない「回避」という選択肢も取りうる。

（2）安全対策の責務配分と効果の達成

次に、導出された安全対策の責務を、関係者で配分し、安全対策を実施する。

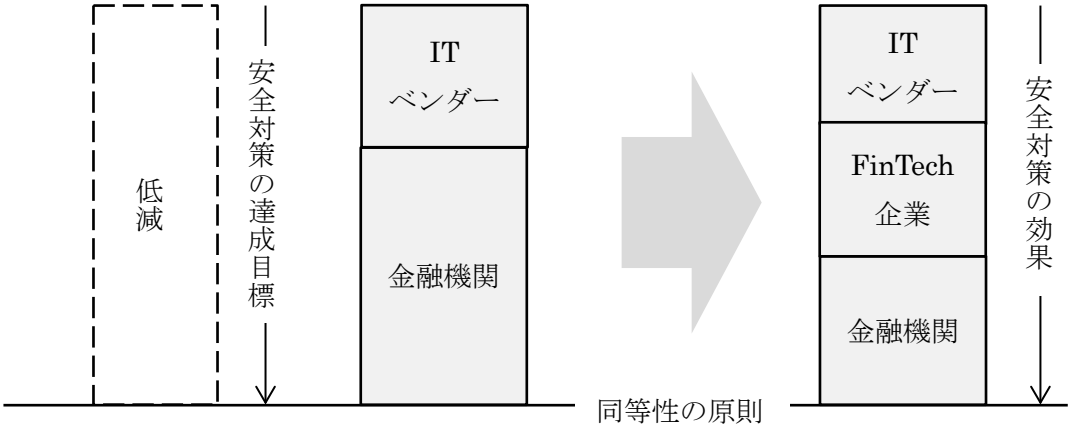


経営層によって、安全対策の達成目標と経営資源配分が決定された後は、管理者のもとで複数の関係者（システムリスク管理部門・システム担当部門・外部委託先等）によって、安全対策が実施される。実施に当たっては、個々の安全対策に応じて関係者間で担われる役割（責務）が特定（配分）される。

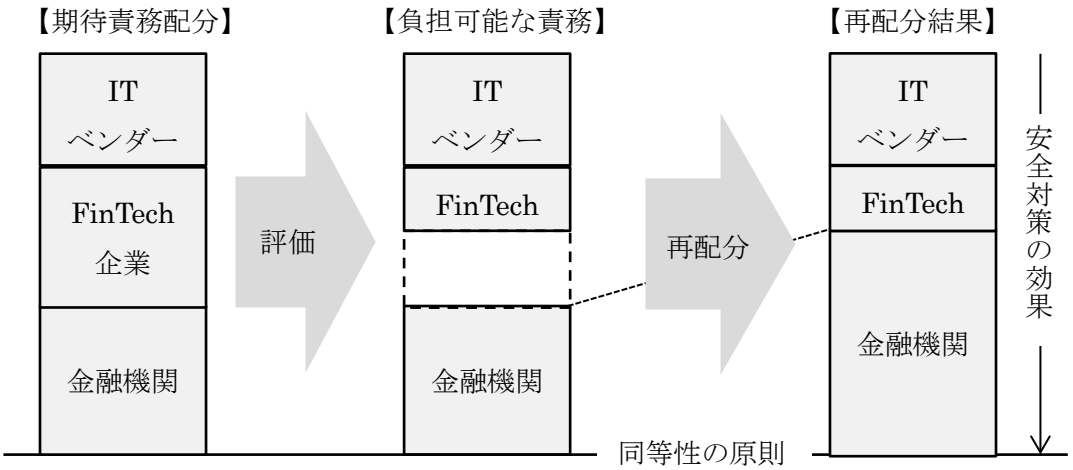
安全対策の責務は、安全対策の技術的側面を担う外部委託先と金融機関の２者に配分されるのが一般的であり、金融機関はあらかじめ安全対策遂行能力を有する外部委託先を選定するとともに、外部委託先において責務を担うために発生する費用は、最終的には、委託料として金融機関が負担することとなる。こうして、安全対策の効果が達成され、経営層が決定した受容可能な程度まで、システムリスクが低減されることを目指す。

２．FinTech 業務における安全対策の責務の配分と同等性の原則

FinTech 企業が安全対策の関係者として加わる FinTech 業務においては、該当する金融関連サービスが金融機関と IT ベンダーの２者で行われているのと比較して、同程度までリスクが低減されるよう取り組むことが必要である。これを「同等性の原則」という。



しかし、FinTech 企業が加わった場合、従来 IT ベンダーに求めていた責務を、FinTech 企業に求めることとなれば、IT ベンダーと同様の責務が担える FinTech 企業のみが選定されることとなる。しかしながら、FinTech においては、「イノベーションの成果を享受する」という観点が考慮されるべきであり、そのために、責務の再配分ルールが必要となる。



具体的には、選定時の評価の結果、FinTech 企業の安全対策遂行能力が十全でない場合に、イノベーションの成果の享受とシステムの安全性の確保（同等性の原則）を両立させるための方策として、責務の再配分を行うこととなる。上記の例では、金融機関が FinTech 企業の責務の一部を負担している。

再配分の極端な例としては、FinTech 企業の責務をゼロにすることも想定されるが、これについては、「金融関連サービスの提供に携わる事業者を対象とした原則」では、「何ら安全対策を実施しない、ということは適切ではない」とされているとおり、FinTech 企業においても、責任ある事業者として、最低限担うべき責務、分配不可能な責務がある。

また、責務の再配分と同等性の原則は、金融機関が金融関連サービスを主導している場合（FinTech 企業が外部委託先となる）、FinTech 企業が主導している場合（Fintech 企業に対して外部委託が準用される）のいずれにも適用可能な考え方である。

なお、こうした責務の再配分は、金融機関が従来から任意で有している選択肢の１つであるが、これを安対基準で積極的に明示することで、FinTech 企業との関係が進展し、イノベーションが促されることを期待している。

【資料６】金融機械化財団 （仮称）設立趣意書（抜粋）

昭和 59 年９月

趣　　旨

金融システムの機械化は、近年急速な展開を見せていますが、これは将来、金融機関の経営、金融業界とその他の業界との関係、ひいては我が国信用秩序に対して大きくかつ複雑な影響を与えることが予想されます。

特に、金融システムは、あらゆる経済部門の活動に必ず伴う資金決済の機能を有しており、また、金融機関と金融機関以外の第三者との間をオンラインで結ぶ第三次オンラインシステムの構築が急速に進みつつあることにかんがみれば、金融機械化システムの円滑な発展を図るため、安全性確保の問題も含め金融システムの機械化全般に関する諸問題を早急に解決し、これを着実に実行していくことが必要であると考えられます。

こうした問題については関係する業界が多岐にわたっているので、検討を行うに際しては、金融機関、保険会社、証券会社、ハード・ソフトメーカー、電気通信事業者、中央銀行、行政当局等の関係者の協力が不可欠であると考えられます。すなわち、これら関係者の十分な意思疎通の下に、知識、経験、情報等を集約することにより、安全性確保のための諸施策を推進するとともに、的確な企画・立案、開発、実施などを進めていく必要があると思われます。

このような見地から、金融機械化システムに係る諸問題を効率的かつ弾力的に処理していくことを目的として、上記関係者の参加する民間出資の第三者的中立機関を創設し、民間活力発揮のため環境整備を図っていくことが適当であると考えます。

各位には、上記の趣旨にご賛同いただき、なにぶんのご協力を賜わるようお願い申しあげる次第であります。

事業内容

（１） 金融機械化システムに係る金融取引、法律関係、投資、受益者負担、国際関係等に関する企画、調査及び研究。

（２） 金融機械化システムに係る障害・犯罪発生状況の把握・開示、安全基準の策定等による安全対策の推進。

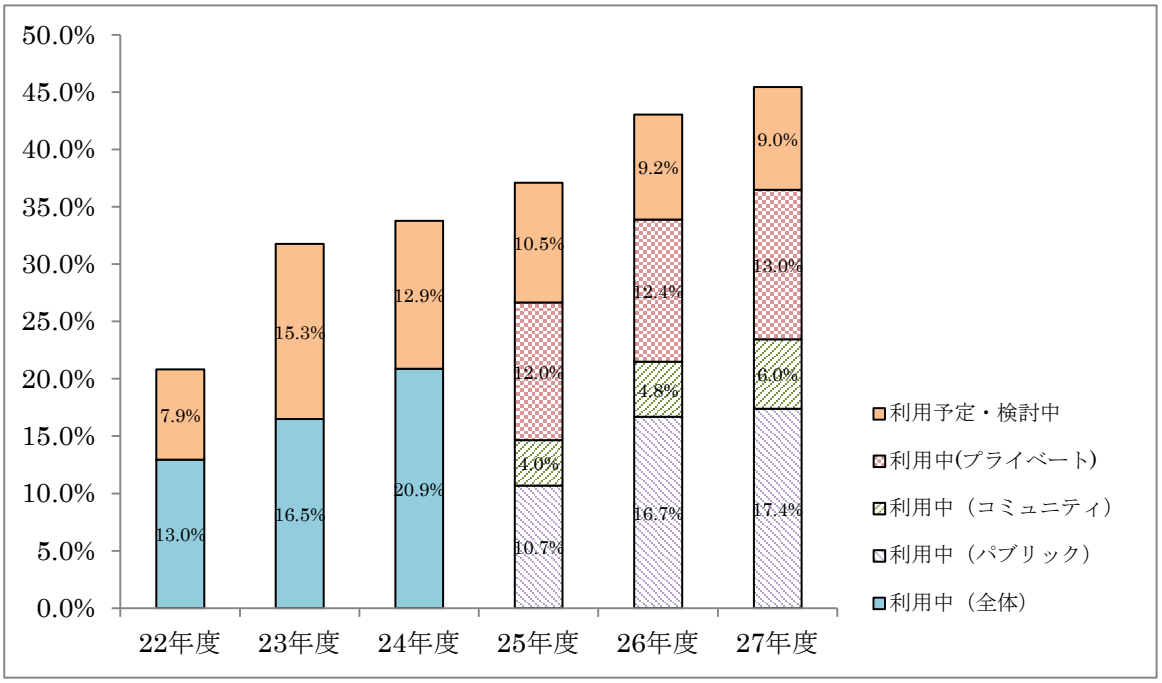
（３） 金融機械化システムに係る共同事業の調査・研究、金融機械化システムに係る斡旋・媒介、システム監査、研修・セミナー・広報等の実施。

（下線は FISC にて付す）

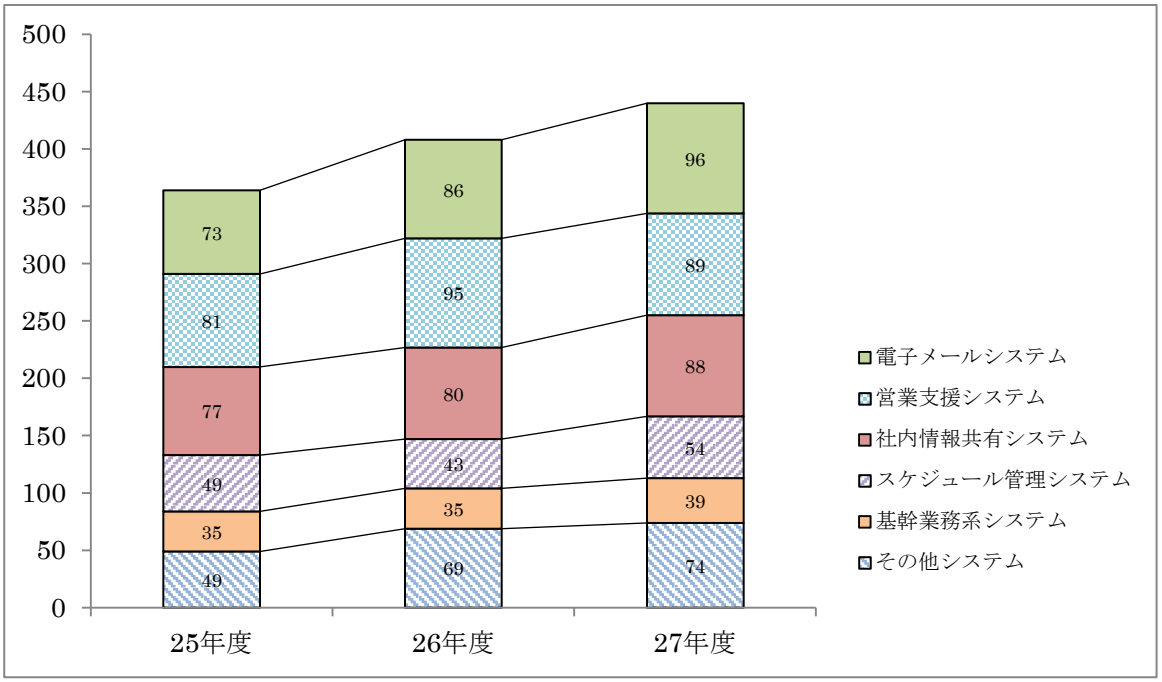
【資料７】クラウドの利用状況

金融機関等のクラウドサービス利用は、平成 27 年度では、約半数の金融機関等がクラウドの利用あるいは利用の検討を行っているとともに、特定のシステムに偏ることなく、年々増加している状況にある。

クラウドの利用推移



クラウドの利用環境



(出所)FISC 金融機関アンケート調査結果

【資料８】クラウドサービスの利用に関する海外監督当局の動向

近年、金融機関におけるクラウドサービス利用に関して、わが国のみならず海外先進諸国でもガイドラインの策定が進められている。

米国では、2012 年７月米国連邦金融機関検査協議会（Federal Financial Institutions Examination Council、以下「FFIEC」という）によって、“IT Handbook：Outsourcing Booklet： Outsourced Cloud Computing”が公表された[76]。また、現在、パブリッククラウドの利用が拡大している実態を踏まえ、新たな検討が進められている模様である。

英国では、2016 年７月金融行為規制機構（Financial Conduct Authority、以下「FCA」という）によって、“Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services”が公表された[77]。

ここでは、上記の公表文書及び当センターが米国通貨監督庁（Office of the Comptroller of the Currency、以下「OCC」という）に対して行ったヒアリング結果をもとに、米国と英国を中心とした海外監督当局の、クラウドサービス利用時の安全対策に関する考え方について解説する。

１．クラウドサービスに対するリスク管理の基本的な考え方

金融機関には、クラウド事業者に業務を外部委託する場合においても、金融機関内部で実施した場合と同様の統制を要求するとともに、内部で実施した場合と比較してリスクが増大しないように、統制を行い、適切にリスクを管理することを求めている。

「クラウドサービスを利用する場合においても、インハウスと同様のリスク管理が何らかの方法でなされていることを要求する。」 米国

「デューディリジェンスの実施時に、外部委託により、金融機関にオペレーショなるリスクが増大しないことを確認すること。」 英国

２．統制に対する考え方

統制に当たっては、利用検討時の客観的評価・締結する契約内容・運用時のモニタリングといった管理フェーズに応じて行われる統制の方法が重視されている。

「パブリッククラウドを利用する場合にまず重要なのが、契約時のデューディリジェンスと契約の中身そのものである。さらに、契約後のモニタリングも重要であり、例えばサービスレベルアグリーメントのモニタリングを行うことは、そのクラウド事業者に問題が発生すれば先行してわかるので、有効なモニタリングである。」 米国

76 http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
77 https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

一方で、技術的な統制の内容については、金融機関に委ねられており、金融機関には技術を十分に理解し、適切に利用していることが求められている。

「監督の基本原則は、どの技術を利用するかは金融機関が決めることであり、それに対して当局が指示をするものではない。どの技術を利用するにしても、同様の内部統制や管理を要求することとなる。」 米国

「セキュリティ対策については、暗号化をしなければならない、とかファイヤーウォールを設定しなければならない、など個別の技術に関して当局が指示するわけではない。技術は変わるからである。実質的に有効なセキュリティ対策がなされていればよい。例えば、クラウド事業者が提供する暗号化ツールを利用する場合がある。この場合、クラウド事業者の職員も暗号化を解くキーを持つことになる場合は、職員に情報を見られるというリスクはある。一方、機械なのでメンテナンスも必要であり、クラウド事業者の職員がキーを持つことが必要であることは理解できる。よって、その場合は、金融機関は、クラウド事業者の誰がどのような目的でそのキーを使ったのかを把握できるような方策をとっていればよい。ファイヤーウォールにしても、侵入検知システムにしても、金融機関は、その仕組みを理解して、正常に稼働するのかどうか、テストしておく必要がある。」米国

３．監査権に対する考え方

金融機関に対して、クラウド事業者との契約書上、実質的な統制が行えるよう手当てをすることを求めている。

「契約に、英国の法令が及び、かつ英国の裁判管轄に属することを確認すること。そうでない場合は、金融機関、監査人、関連当局が、データ及び事業者に対して、実効的にアクセスする手段を手当てすることが必要である。」 英国

米国では、個人を特定できる情報の取扱いに関する法令（グラム・リーチ・ブライリー法）に定める場合を除き、クラウド事業者に対する監査権を契約書上明記することを強制していない。これは、米国では、バンク・サービス・カンパニー法により、監督当局が、銀行の業務のアウトソーシングを受けているベンダーを直接検査できることも背景にあるものと推測される。

「銀行はクラウドベンダーに対して監査権を持つべきであり、その旨契約書に定めるべきである。ただし、これはベストプラクティスであり、監督当局として銀行に強制することはできない。法的には、契約書で定めるかどうかは任意である。」 米国

「多くの銀行が勘定系システムをアウトソーシングしているベンダーに対しては、通貨監督庁（OCC）、連邦預金保険公社（FDIC）、連邦準備制度理事会（FRB）などが共同で検査に入り、検査報告書はベンダーを利用している金融機関に還元している。」 米国

また、クラウド事業者がみずから監査人に依頼して作成する保証型監査報告書については、その有効

性が評価されている。

「主要なクラウド事業者は、独立監査法人の監査を受け、米国公認会計士協会の規格に沿った保証型監査報告書を顧客に提供している。現実的には、多くの場合それらは範囲を含め十分な内容であるので、そうした報告を受けているのであれば、追加で金融機関が監査することが必要という状況ではない。現実問題として、数千もの顧客を持つ主要クラウド事業者がいちいち顧客からの監査を受けていたらもたないだろう。しかしながら、もしその報告書が不十分なのであれば、追加で監査できるように契約しておくことが望ましい。」 米国

４．データの所在に対する考え方

データを自国内で保存しなければならない、という規制は無い。いずれに所在しようとも、金融機関や当局による実質的なアクセスが可能となっていることが求められる。そのため、データの所在地を把握しておくことが求められる。

「金融機関、監査人、関連当局が、外部委託された業務に関連するデータに、実質的にアクセスが可能となるよう要求されている。ここでいう「データ」という用語には幅広い意味があり、金融機関のデータ、個人顧客のデータ、取引履歴データだけでなく、システムや手続きに関するデータも含まれる（例えば要員の身元調査手続き、システム監査証跡等）。管轄上、英国の規制当局によるデータへのアクセスが実質的に禁じられているような場所にはデータを保存しないこと。」 英国

「米国では、データを米国内で保存しなければならないという規制はないが、データが米国内にある場合と同様に、必要な場合は必要なデータが入手できる状態にしていなければならない。」 米国

「パブリッククラウドの場合でも、データが保管される地理的な範囲は決められており、銀行はモニタリングできるものである。監督当局は、銀行が、データが行ってはいけない場所に行っていないか、モニタリングしていることを検査することになる。」 米国

５．技術の先進性に対する考え方

金融機関は、多様なクラウドの中から、みずからのニーズに適合する形態を選択することとなるが、形態に応じて責任分界が異なることを理解し適切にリスクをコントロールすることが求められる。また、これまでになかったリスクが発生する可能性があることを認識し、あらかじめその内容を理解し必要な手当てをしておくことが求められる。これまでになかったリスクとして、匿名の利用者どうしのシステムが相互に影響を与えるリスクが想定されている。

「パブリッククラウドについては、SaaS よりも PaaS や IaaS のほうが金融機関にとっての負担は大きくリスクも高くなる。金融機関がそれを理解していることが重要。また、よりコアに近いシステムをクラウドに移管すればその分リスクも高くなる。ただし、大手ベンダーのレベルと理解力は高いことは当局も実感しており、実際には金融機関側がベンダーに教わっていることが多い。」 米国

「ハードウェア上、金融機関のデータが固まって保存されているならよいが、例えば、ゲーム事業者と一緒であれば、それなりのリスクはあるかもしれない。例えば、金融機関がハッキングされなく

ても、同じハードウェアにいる別の利用者がハッキングされて、その影響を受けないか、検証する必要がある。」 米国

「委託元ごとでデータを分離する方法について留意すること(パブリッククラウドを使用する場合)」 英国

６．事業継続計画に対する考え方

業務の継続計画について、委託先とあらかじめ協議し文書化するとともに、訓練を通じて、その実効性を定期的に検証することを求めている。

「データの冗長性についてあらかじめ契約しておく必要がある。また、冗長性を契約上持たせる場合でも、実際のところどのようになるのかを理解し、本当に想定どおりになるかをテストしておく必要がある」 米国

「金融機関は外部委託業務が予期せず中断した場合にも、業務を継続できるよう、委託先と適切に協定しておく必要がある。その場合に、金融機関は、業務継続性の維持や復旧のための戦略を文書化すること、その戦略の適切性と有効性を定期的に検証すること等が必要である。」 英国

７．その他

「クラウドベンダーは、規制業種である銀行のことをよく理解していないので、粘り強く交渉し、銀行に必要な条項を契約に盛り込む必要がある。これで相当程度、直接監査できない問題等に対応できる。」 米国

わが国では、クラウド事業者の FISC への入会、あるいは有識者検討会等の会議体への参画等を通じて、クラウド事業者が金融業務に対する理解を深める機会が提供されている。

【資料９】API 接続先チェックリストワーキンググループによる集合的な検討

全銀協が公表した「オープン API のあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理（案）】」において、「複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される」と整理された。

こうした整理を受けて、平成 29 年２月、FISC が事務局となり、「API 接続先チェックリストワーキンググループ」（以下「チェックリスト WG」という）を設置し、入口の管理フェーズで行われる統制の内容、すなわち、API 接続先に対する客観的評価で使用されるチェックリスト（以下「チェックリスト」という）の共通部分に関する検討等を行っている。

オープンAPIは、FinTech検討会におけるタイプⅢの実現方法の１つであることから、チェックリストWGの検討は、FinTech検討会におけるタイプⅢに関する提言内容と整合的に進められることが必要である。すなわち、タイプⅢにおける「外部委託基準の準用ルール」、および「必要最低限の安対基準」[78]を踏まえつつ、FinTechに関する安全対策を検討している集団の相互関係を意識した検討が行われることが必要である。

また、FinTech 企業の負担軽減の観点から、社会的規範性をもったチェックリストが制定されることが望ましく、そのためには、金融機関、FinTech 企業、IT ベンダーといった API 接続に携わる関係者が、合意形成を目指して、チェックリストの検討過程に参画することが望ましい。

チェックリスト WG において、以上の集合的な検討が行われ、その結果として、チェックリスト等の成果物がとりまとめられた場合には、その成果物は、FinTech 検討会の提言内容の一部として取り扱われることとなる。また、環境変化等が生じた場合にも、以上の集合的な検討が行われ、成果物の内容が継続的に見直され、実装・運用されることが期待される。

API 接続に携わる関係者においては、その成果物を、有用なものとして、金融機関の実態に応じて利用し、総体的な安全性の確保とイノベーションの両立が目指されることを期待する。

チェックリストのイメージ

API 接続先チェックリスト

区分	セキュリティ目標	強度	手法例	回答欄	関連規定

78 「必要最低限の安対基準」は、API 接続先を含む金融関連サービスの提供に携わる事業者において、最低限実施されるべき基準としても制定される。その制定までの間は、少なくとも「安全対策遂行能力のうち基礎的な部分」（脚注 26）を踏まえて検討されることが望ましい。