平成 29 年６月 13 日
公益財団法人　金融情報システムセンター

第６回　金融機関における FinTech に関する有識者検討会　議事次第

Ⅰ　日時
平成 29 年６月 13 日（火）　15:45～17:45

Ⅱ　場所
FISC 会議室

Ⅲ　議事次第
１．　15:45　開会
２．　15:50　【議事１】本検討会の報告書についての説明・論議
３．　16:50　【議事２】API接続先チェックリストワーキンググループの検討状況
４．　17:20　理事長挨拶
５．　17:35　事務連絡
６．　17:45　閉会

Ⅳ　資料
【資料１】　金融機関における FinTech に関する有識者検討会　座席表
【資料２】　本検討会の報告書に対するご意見及びご回答
【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
（修正箇所抜粋・修正履歴有り）
【資料４】　金融機関における FinTech に関する有識者検討会報告書
（修正履歴無し）
【資料５】　API接続先チェックリスト ワーキンググループ活動実績について
【資料６】　API接続チェックリスト（試行版）(Draft)
【資料７】　API接続チェックリスト（試行版）取扱説明書（Draft）
【資料８】　「API 接続チェックリスト（試行版)」利用のお願い

Ⅴ　事務連絡

今後の予定
１．報告書の PDF 頒布
（６月末までに、HP にて一般向けダウンロード提供）
２．第６回議事録・会議資料の提供
（６月末までに、HP にて一般向けダウンロード提供）
３．報告書に関する全国説明会
（7/27 札幌、7/28 仙台、8/3 名古屋、8/4 大阪、8/17 福岡、8/18 岡山、8/24 東京）

Ⅵ　その他
本日の検討会終了後に、同じ場所にて懇親会を予定しております。

以 上

【資料１】

第６回金融機関におけるFinTechに関する有識者検討会　座席表

平成29年６月13日

※代理出席

ＡＢ会議室

中山　調査部長　○
水野　総務部長　○
髙橋　常務理事　○
渡辺　理事長　○
渕崎　座長代理　○
岩原　座長　○
小林　企画部長　○
藤永　企画部次長　○
大澤　企画部主任研究員　○
郡山　総務部特別主任研究員　○
和田　監査安全部長　○

金融庁　神田様○
金融庁　片寄様○
日本銀行　中井様○
経済産業省　※ 希代様○
デロイトトーマツコンサルティング合同会社　荻生様○

○日比谷パーク法律事務所　上山様
○株式会社三井住友銀行　持田様
○株式会社南都銀行　※　大石様

○日本マイクロソフト株式会社　平原様
○アマゾンウェブサービスジャパン　梅谷様
○日本電気株式会社　岩田様
○株式会社日立製作所　長様
○株式会社エヌ・ティ・ティ・データ　村上様
○株式会社Liquid　轟木様
○株式会社マネーフォワード　※　内波様
○Ｆｉｎ Ｔｅｃｈ協会　マークマクダッド様
○野村ホールディングス株式会社　植村様
○東京海上日動火災保険株式会社　黒山様
○住友生命保険相互会社　真田様
○住信ＳＢＩネット銀行株式会社　吉本様

録音業者

窓

通　路

出入口

【資料２】

本検討会の報告書に対するご意見及びご回答

No	対象箇所	検討会後に頂いたご意見	事務局回答	ご意見元
1	第５回 議事１ （全般）	有事における顧客への一義的な責任を金融機関が負い、 またフィンテック企業に対する金融機関の管理において 「外部委託基準」の準用ルールが適用される事業範囲は どこまでか確認したい。 報告書には「金融サービス」と「金融関連サービス」、「金融業務」と「非金融業務」という概念が示されており、 上記の観点からの定義づけが必要と思われる。 例えば、フィンテック企業が従来の銀行業務から派生した新たなビジネスを展開する場合、 当該ビジネスが提携銀行にとって委託業務となるか否かは、 事業内容や個別の契約形態によって判断すべきであり、 委託者としての権限が担保されない状態で 管理責任のみが追及されることで、 金融機関に過度な負担がかかることがないよう 配慮が必要と考える。	ご指摘を踏まえて、原案の「Ⅱ４．（２）FinTech企業に残る安全対策上の責任」に、以下の修正を行います。 *（修正前）* *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。* *（修正後）* *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、顧客に対する一義的な安全対策上の責任はFinTech企業が担うものと解される。そのため、FinTech企業は、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。*	南都銀行 大石様
2	第５回 議事１ （Ｐ.23） 「７．（２）リスク特性の分離可能性」	「リスク特性が顕著に異質」とは、実際にどのようなケースが該当するのか、具体的な事例等を示していただきたい。	ご指摘を踏まえて、原案の「Ⅱ７． FinTech業務を担う情報システムの安全対策上の取扱い」に、以下の脚注を追加します。 *（脚注）* *例えば、システム全体では、顧客情報が保有されているが、該当のサブシステム内には顧客情報が保有されていない場合等が考えられる。*	南都銀行 大石様

第５回議事資料：

議事１：　金融機関における FinTech に関する有識者検討会報告書（案）

議事１（参考資料）：　「第４回 FinTech 有識者検討会に対するご意見およびご回答」

議事２：　API 接続先チェックリストワーキンググループ活動実績と今後の予定について

【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

平成 29 年６月

公益財団法人 金融情報システムセンター

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

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。

金融情報システムに社会的に期待される安全対策の効果は、システム資源を自前で用意するのが一般的であった３０年前に、安対基準の策定という形ではじめて具現化された。その後、安対基準に具現化された安全対策の効果は、金融機関に対する社会的期待の変化を反映する一方で、IT ベンダーへの依存度の高まりといった金融機関の事情による変化の影響を受けることなく、金融機関と IT ベンダーの２者関係の中でも維持されてきたものと考えられる。

したがって、金融機関がイノベーションの成果の享受を目指す中で、FinTech 企業という新たな関係者が登場する場合であっても、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、同等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者で同等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な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。

削除: の程度

削除: 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。

削除: その

削除: 程度

削除: 程度

[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。

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、同等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）。

削除: 程度

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とど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、外部委託にとど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

[27] 仮に、FinTech 企業の負担費用の最小化が選択される場合、金融機関が FinTech 企業に代わって責務を負担することが明らかとなれば、FinTech 企業には、安全対策上の責務を全く果たさなくても、金融機関が負担してくれるのではないかという期待が生まれる可能性がある。一方、金融機関の負担費用の最小化が選択される場合、FinTech 企業に負担が求められることとなり、FinTech 企業は負担を逃れるために安全対策能力を過大に虚偽申告する可能性がある。したがって、関係者が協調し、社会的な観点から、負担費用の総和の最小化が検討されることが望ましい。また、適切な情報開示等による協調を確実に実現するためには、責務を負担した関係者に応分の利益が還元されるスキームを、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。

削除: また、
削除: 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、
削除: 再配分を受入れ
削除: への投資を意図的に抑制するフリーライダーの指向
削除: このような関係者のモラルハザードを
削除: 抑止
削除: 公正な
削除: 関係者で

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又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、又は 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、又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、又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又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、金融機関が関心を持たない項目があることに起因して、FinTech 企業において行われるべきシステムに対する統制全体の程度が低下し、その結果、データの保全又は本人確認に係る安全対策の効果まで損なわれることとなる場合には、金融機関は、FinTech 企業に対して、関心外の項目に対しても、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。

削除: の

削除: 外となった結果、

削除: 全体として統制

削除: が得られない

削除: 場合は、

（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、又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、金融機関の責務部分以外に対しても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、顧客に対する一義的な安全対策上の責任は FinTech 企業が担うものと解される。そのため、FinTech 企業は、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。

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[34]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。

[34] 例えば、システム全体では、顧客情報が保有されているが、該当のサブシステム内には顧客情報が保有されていない場合等が考えられる。

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[54]。

（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[55]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、技術変化の影響を受けやすい設備基準や技術基準が、技術変化の状況を踏まえることなく、そのまま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[56]。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。

削除: が

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。

---

54 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。

55 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。

56 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。

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[57]。

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（要配慮個人情報を含む[58]）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[59]。

---

[57] 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。

[58] ここでいう機微情報は、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』に定める機微情報のことをいい、その内容には、改正個人情報保護法の要配慮個人情報が含まれる。（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。）

[59] 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

削除: を考えるに当たって

削除: が参考となる。

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）統制対象クラウド拠点の把握

削除: データアクセス

「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当たり対象となる事業拠点[60]（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[61]。

「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。

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。

[60] 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。

[61] 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。

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[62]。（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、データの保全・本人確認・サービスの可用性・障害管理等の「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、入口の利用検討時に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、金融機関と FinTech 企業で、集合的に検討し、合意形成することが考えられる[63]。チェックリストの共通部分を合意しておけば、その後の契約締結時や運用時に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軽

削除: 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

削除: 管理フェーズで

削除: その共通部分を、

削除: 管理フェーズ

削除: で

[62] 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。

[63] 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。

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[64]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[65]。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[66]。

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[67]。

---

64 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。

65 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。

66『銀行法等の一部を改正する法律』（平成29年5月26日成立）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。

67 例えば、FinTech企業集団の事業者団体が会員への指導・勧告に当たり、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。

削除: 国会に提出されている
削除: 案
削除: 3
削除: 3日
削除: 提出

「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 京都産業大学法務研究科客員教授・ 　法教育総合センター長 弁護士（渥美坂井法律事務所・外国法共同事業）
	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 情報通信国際戦略局 参事官（サイバーセキュリティ戦略担当）

Ⅶ　資料編

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 に取り組むに当たり、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等の改正

削除: 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、同年５月 26 日に成立した。

（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・検討会に参加）

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）[68] 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）[69]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

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

【資料５】「同等性の原則」という考え方

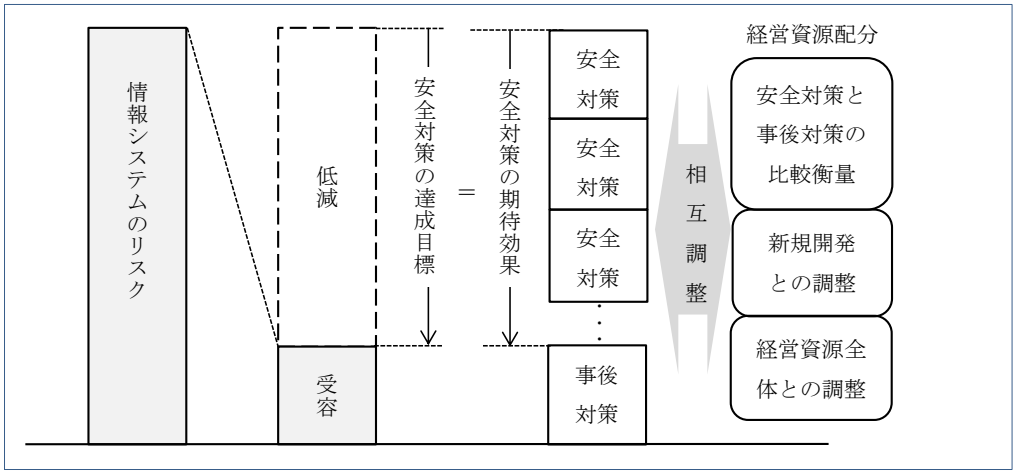
「同等性の原則」とは、金融業務を担う情報システムの安全対策の効果は、安全対策上の関係者に関わらず、同等に確保されるべき、とする考え方である。この原則について、リスク評価から安全対策の決定・実施に至るプロセスを紐解きながら、責務の再配分ルールとの関係に触れつつ、解説を行う。

削除: 程度

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[76]、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。

[76] 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。

【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」、及び「必要最低限の安対基準」[79]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。

チェックリストの制定に当たって、以上の集合的な検討が行われ、その結果として、成果物が取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。

削除: WG

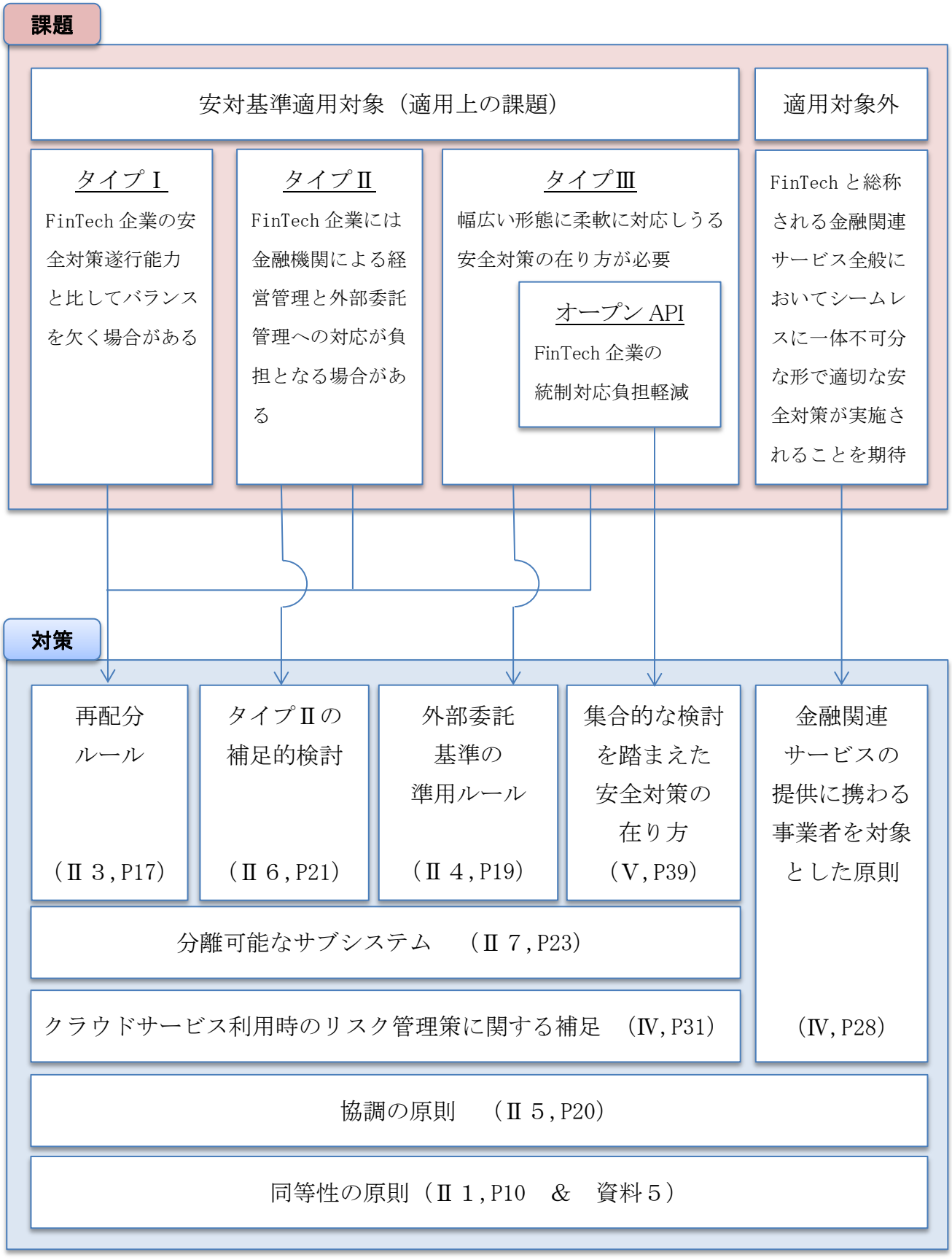
削除: WG

削除: において

削除: チェックリスト等の

[79] 「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。

【資料 10】本検討会で取り上げた課題とその対策



【資料４】

金融機関における FinTech に関する
有識者検討会報告書

平成 29 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、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な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者を念頭に置き、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 をめぐっては、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

---

[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。

が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]の提供又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、又は、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、提供又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。

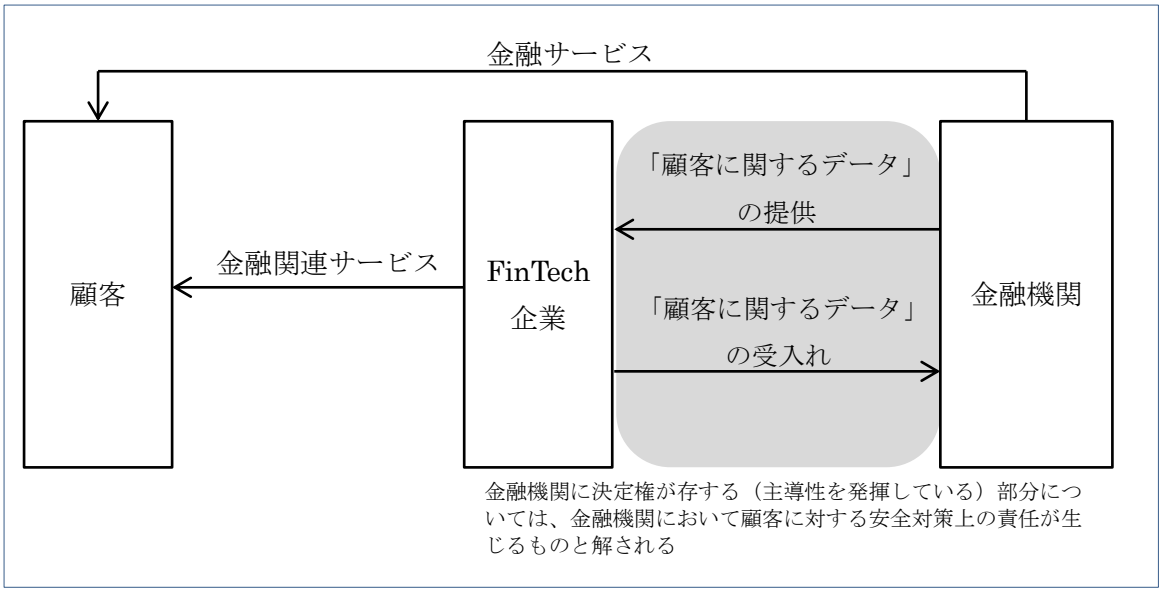
11 金融機関が FinTech 企業に提供するデータとしては、例えば、顧客の取引履歴情報等がある。また、金融機関が FinTech 企業から受入れるデータとしては、例えば、決済指図が考えられる。

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

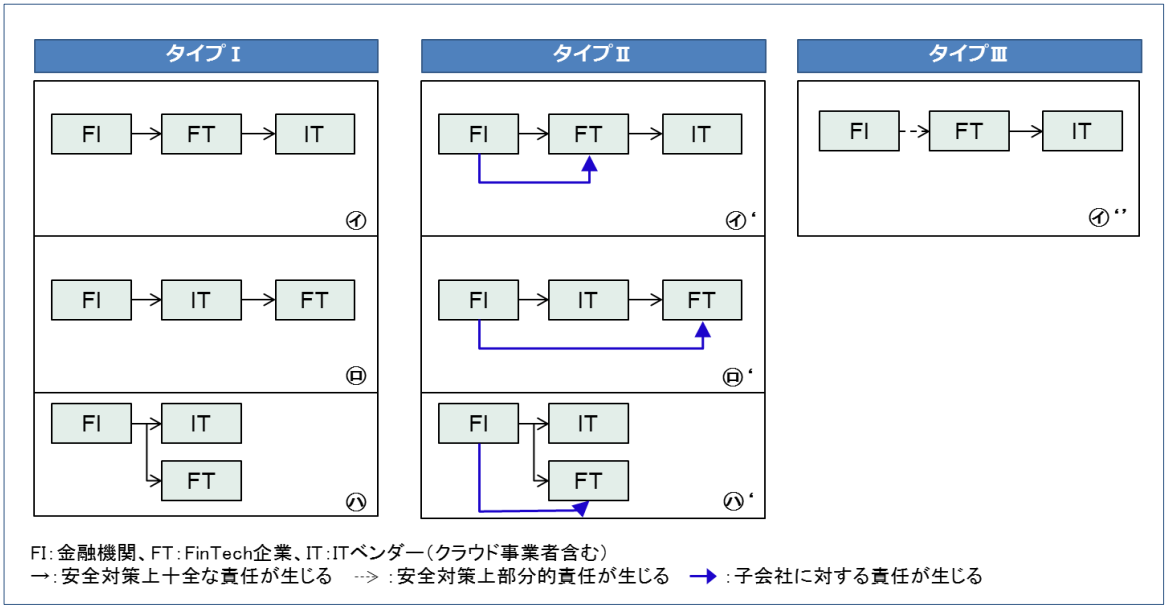


基本的人権の侵害といった広範な損失を被る可能性があることから、その取扱いには社会的・公共的な性質を有するもの」とされている。

（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当たり、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当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。

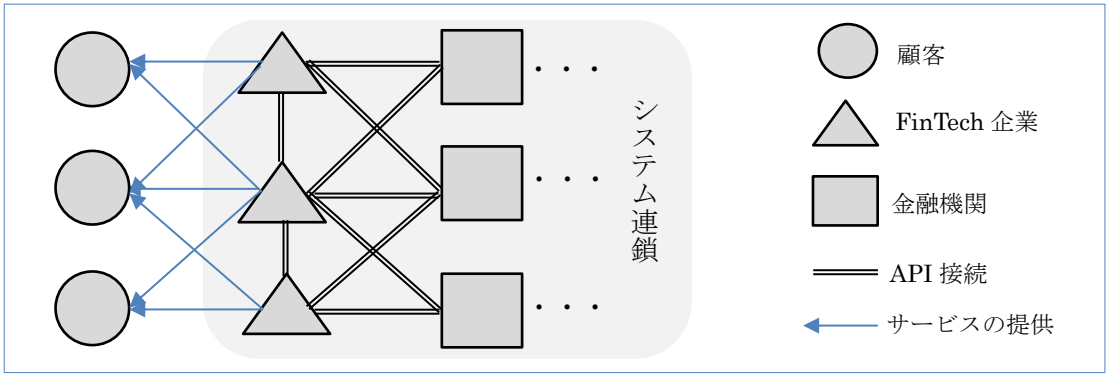
API による事業者間のシステム連鎖は、技術的には、多対多でかつ多段階にわたり重層的に可能である。したがって、金融機関の API 公開により、金融情報システムの連鎖

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

に多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

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。

金融情報システムに社会的に期待される安全対策の効果は、システム資源を自前で用意するのが一般的であった３０年前に、安対基準の策定という形ではじめて具現化された。その後、安対基準に具現化された安全対策の効果は、金融機関に対する社会的期待の変化を反映する一方で、IT ベンダーへの依存度の高まりといった金融機関の事情による変化の影響を受けることなく、金融機関と IT ベンダーの２者関係の中でも維持されてきたものと考えられる。

したがって、金融機関がイノベーションの成果の享受を目指す中で、FinTech 企業という新たな関係者が登場する場合であっても、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、同等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者で同等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な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。

---

[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。

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

---

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。

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

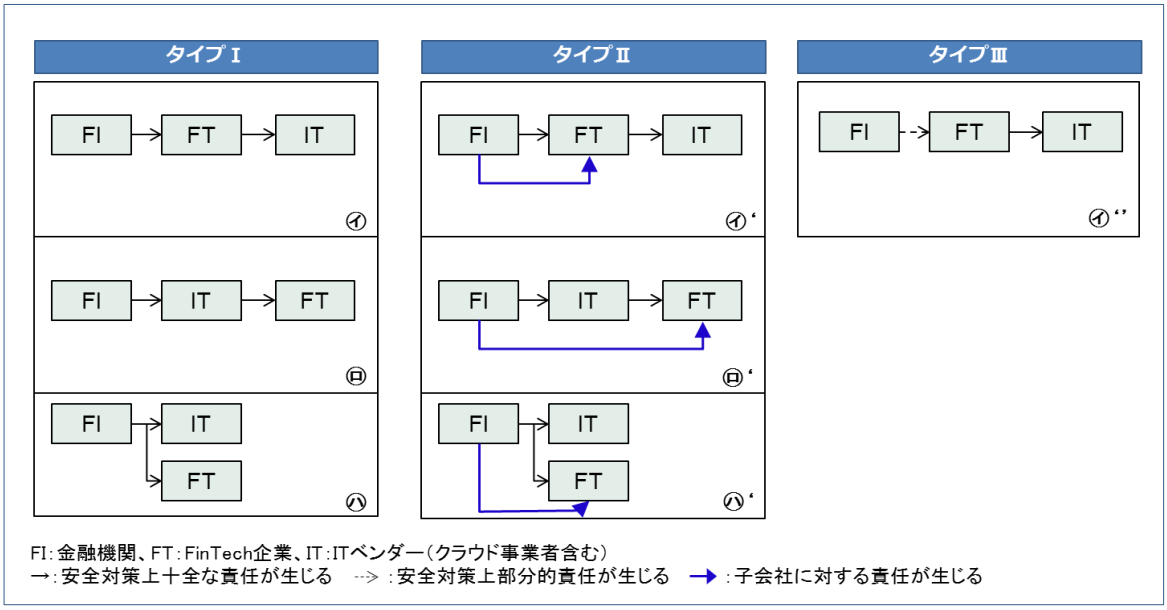
まず、内在する問題を検討するに当たり、「従来の安対基準の概要（外部委託関連）」を、タイプⅠの３者関係に置き直して整理を行った。【資料編資料４参照】

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

【㋒の類型】

【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

【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
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、同等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とど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、外部委託にとど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

---

[27] 仮に、FinTech 企業の負担費用の最小化が選択される場合、金融機関が FinTech 企業に代わって責務を負担することが明らかとなれば、FinTech 企業には、安全対策上の責務を全く果たさなくても、金融機関が負担してくれるのではないかという期待が生まれる可能性がある。一方、金融機関の負担費用の最小化が選択される場合、FinTech 企業に負担が求められることとなり、FinTech 企業は負担を逃れるために安全対策能力を過大に虚偽申告する可能性がある。したがって、関係者が協調し、社会的な観点から、負担費用の総和の最小化が検討されることが望ましい。また、適切な情報開示等による協調を確実に実現するためには、責務を負担した関係者に応分の利益が還元されるスキームを、あらかじめ合意しておくことが考えられる。

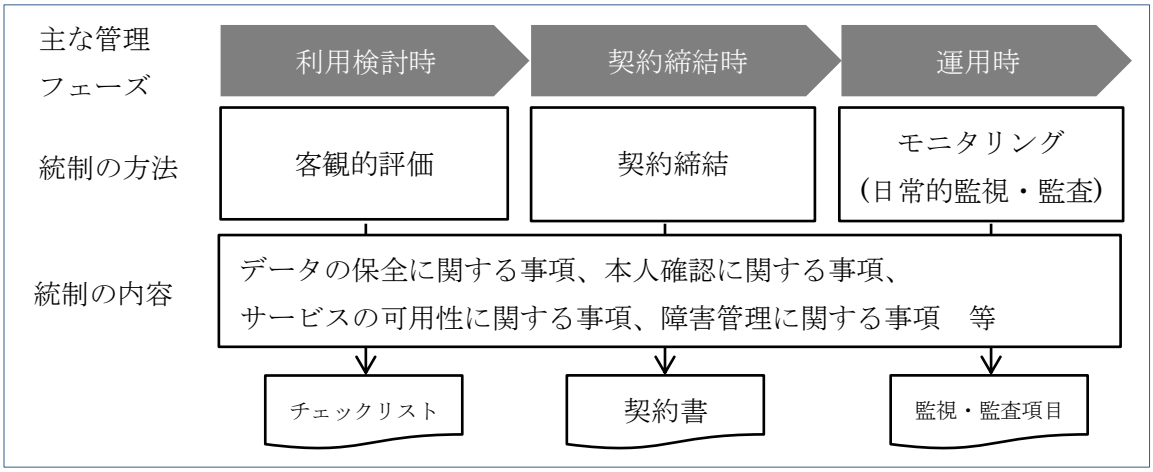
[28] 例えば、３者契約により、金融機関が、FinTech 企業に代わって、IT ベンダーを統制する【責務Ｂ－２】の一部を担うことで、金融機関みずからが IT ベンダーに統制を行うことが考えられる。

[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。

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、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

a.利用検討時	客観的評価の実施
	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
	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
	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
	FinTech 企業は、監査・評価を受忍するか。

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又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、又は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、又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、又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又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、金融機関が関心を持たない項目があることに起因して、FinTech企業において行われるべきシステムに対する統制全体の程度が低下し、その結果、データの保全又は本人確認に係る安全対策の効果まで損なわれることとなる場合には、金融機関は、FinTech企業に対して、関心外の項目に対しても、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、又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、金融機関の責務部分以外に対しても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、顧客に対する一義的な安全対策上の責任はFinTech企業が担うものと解される。そのため、FinTech企業は、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づけ、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づけ等実態に応じて、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[34]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。

[34] 例えば、システム全体では、顧客情報が保有されているが、該当のサブシステム内には顧客情報が保有されていない場合等が考えられる。

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[35]。

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）[36]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[37]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[38]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

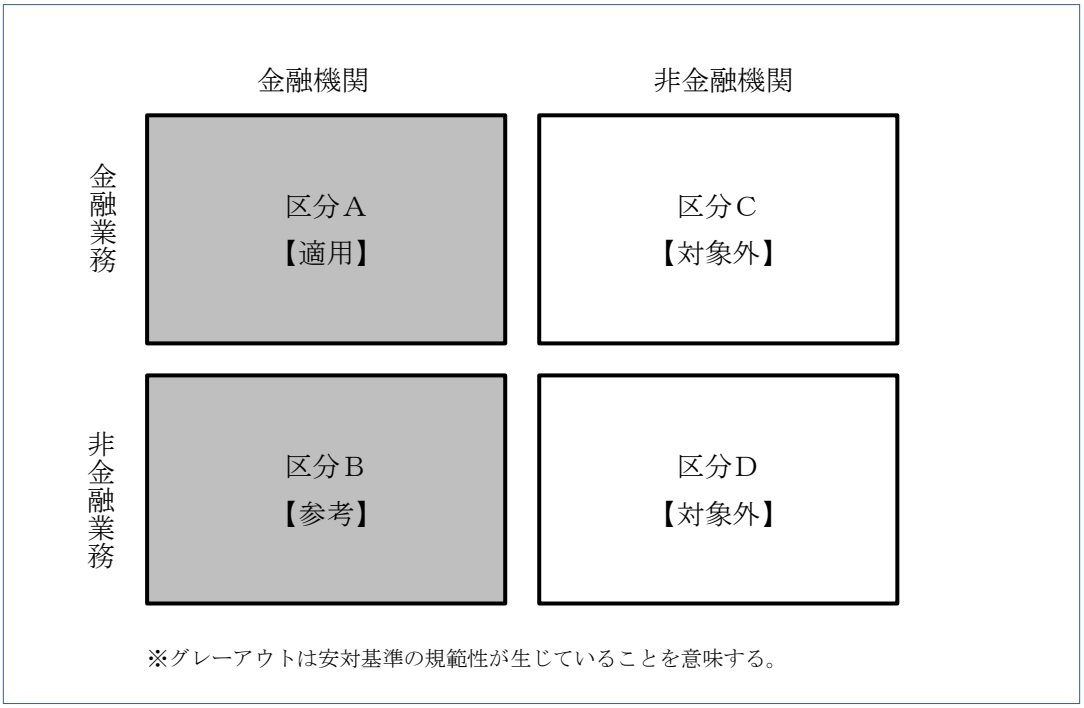
[35] 脚注４を参照。
[36] ソフトローとハードローの説明については、中山信弘編集代表『ソフトローの基礎理論』（2008 年）中の第３部第１章瀬下博之『ソフトローとハードロー』から引用。
[37] 平成 29 年３月末現在、FISC 会員数 644 社のうち金融機関は 542 社と、その 84%を占める。
[38] 安対基準は FISC 会員代表者を中心に構成される安全対策専門委員会とその下部組織である安全対策基準改訂に関する検討部会で検討を行った後、会員への意見募集を経て策定される。

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[39]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

[39] 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[40]。

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

[40] 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[41]」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 ベンダーにとどまらず、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

[41] 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な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[42]。

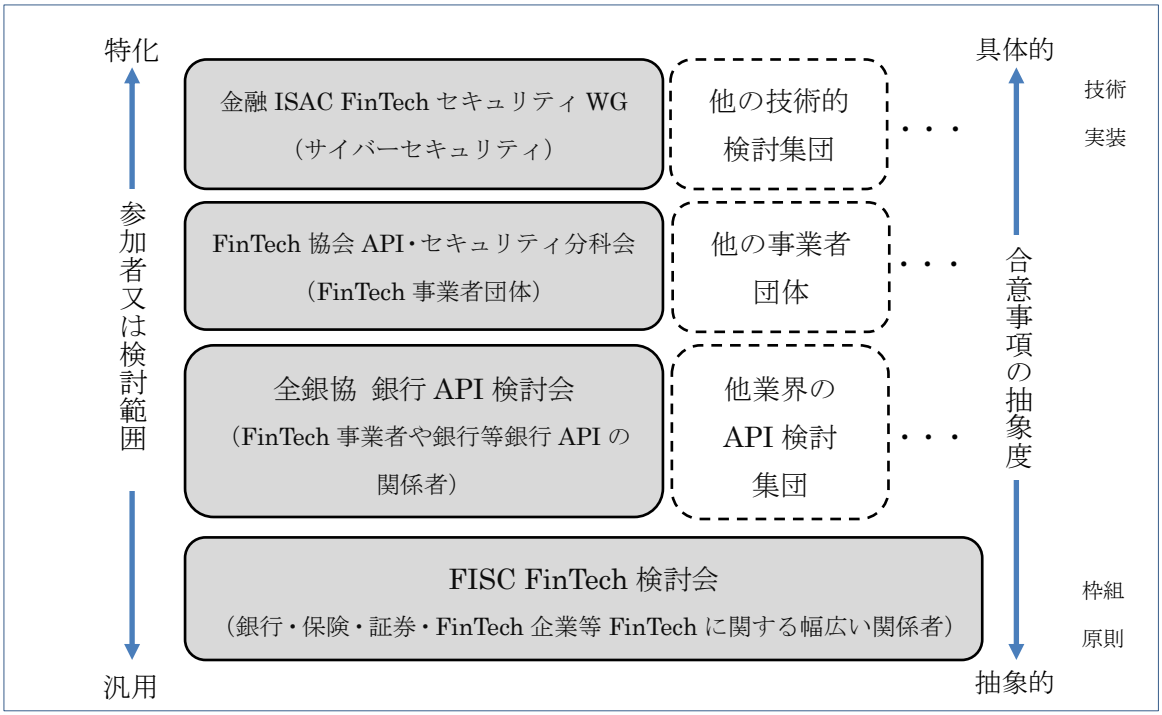
---

[42] 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[43]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[44]。

（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

[43] 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】

[44] 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[45]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

[45] 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[46]。

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[47]。

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[48]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

---

46 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。

47 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。

48 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[49]。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[50]」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[51]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[52]。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[53]。

（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、

---

49 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。

50 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。

51 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。

52 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。

53 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[54]。

（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[55]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、技術変化の影響を受けやすい設備基準や技術基準が、技術変化の状況を踏まえることなく、そのまま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[56]。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。

---

54 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。

55 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。

56 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。

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[57]。

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（要配慮個人情報を含む[58]）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[59]。

---

57 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。

58 ここでいう機微情報は、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』に定める機微情報のことをいい、その内容には、改正個人情報保護法の要配慮個人情報が含まれる。（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。）

59 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

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）統制対象クラウド拠点の把握

「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当たり対象となる事業拠点[60]（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[61]。

「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。

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。

[60] 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。

[61] 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。

（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[62]。（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、データの保全・本人確認・サービスの可用性・障害管理等の「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、入口の利用検討時に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、金融機関と FinTech 企業で、集合的に検討し、合意形成することが考えられる[63]。チェックリストの共通部分を合意しておけば、その後の契約締結時や運用時に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軽

---

62 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。

63 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。

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[64]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[65]。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[66]。

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[67]。

---

64 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。

65 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。

66『銀行法等の一部を改正する法律』（平成29年5月26日成立）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。

67 例えば、FinTech企業集団の事業者団体が会員への指導・勧告に当たり、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 京都産業大学法務研究科客員教授・ 　法教育総合センター長 弁護士（渥美坂井法律事務所・外国法共同事業）
	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 情報通信国際戦略局 参事官（サイバーセキュリティ戦略担当）

（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		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）、岡本　一真（第１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）

Ⅶ　資料編

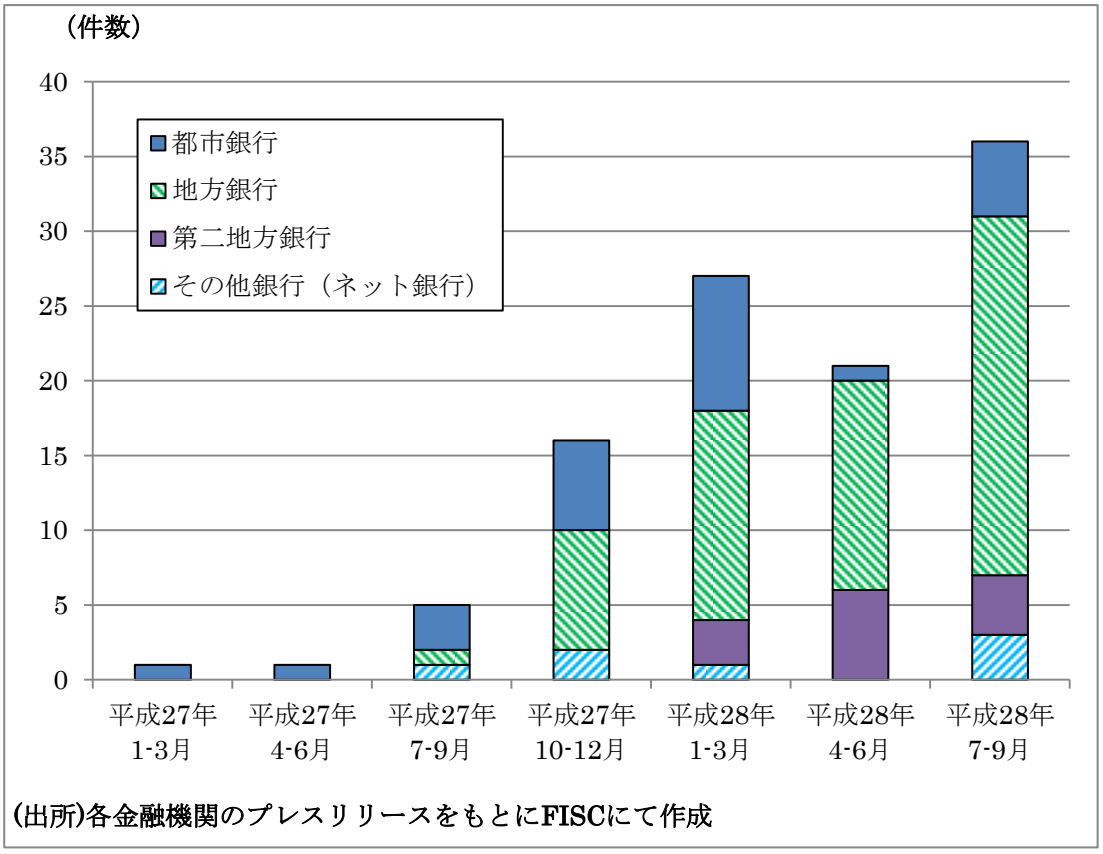
【資料１】金融機関等における FinTech をめぐる動向

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 に取り組むに当たり、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等の改正

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、同年５月 26 日に成立した。

（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・検討会に参加）

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）[68] 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）[69]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

[68] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20150428-1.html
[69] 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[70]。

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。

[70] 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[71]。

（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。

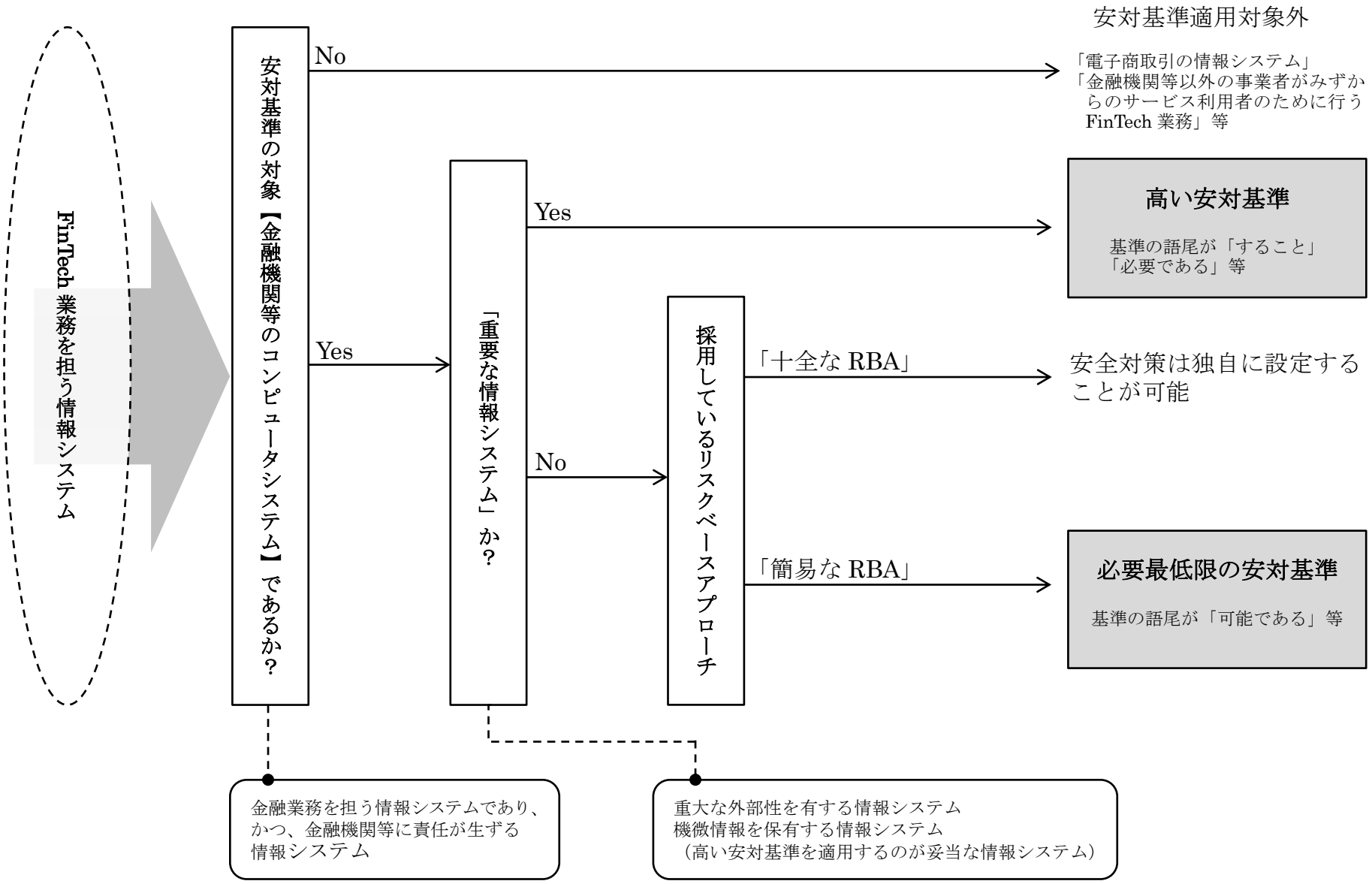
一方で、英国財務省の要請により 2015 年 9 月に「Open Banking Working Group」が設立され、英国銀行業における API のオープン標準推進に向けた検討が開始された。その検討の成果として、2016 年 2 月 8 日に「The Open Banking Standard」[72]が公表された。この報告書には、英国において Open Banking Standard を推進するための詳細なフレームワークが記載されているが、これは、英国がこの分野の国際的なリーダーシップを獲得し、世紀を超えて経済・産業の勝者であり続けることを目指した取組みであるとされている。

・*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。）

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

【資料２】安対基準の適用手順

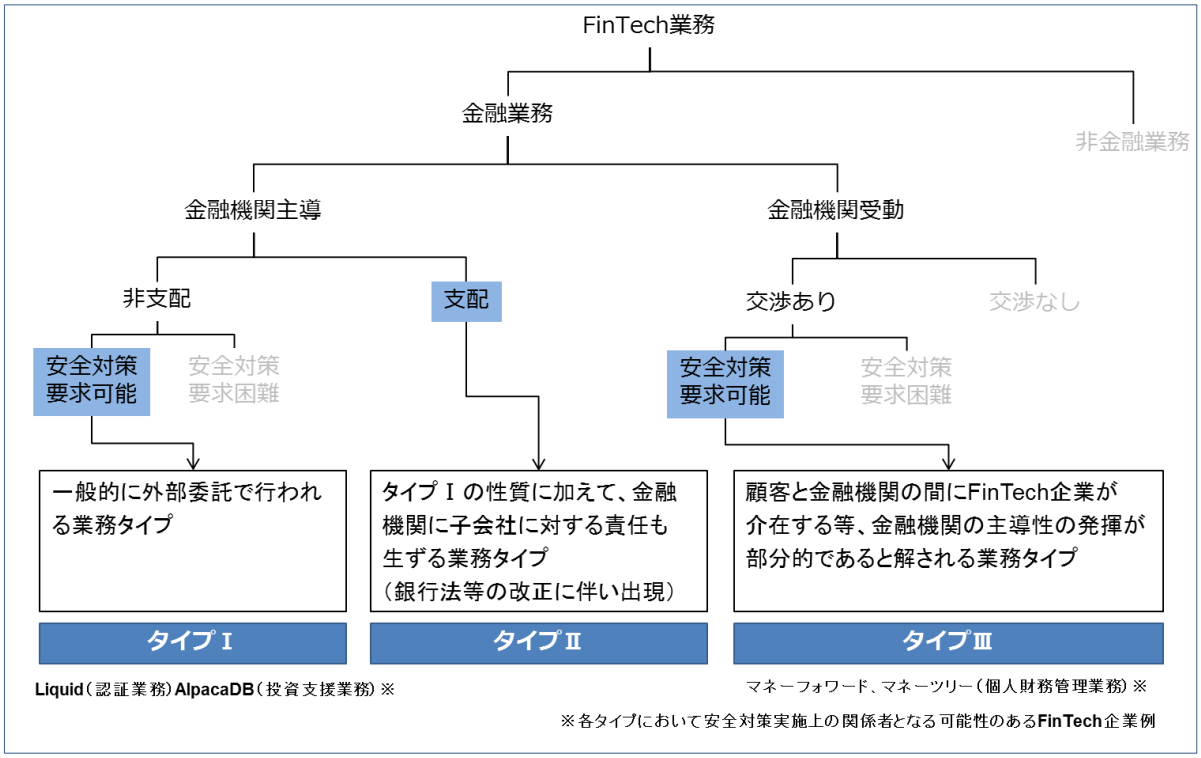


【資料３】FinTech 業務タイプ別類型に関する考察

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[73]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

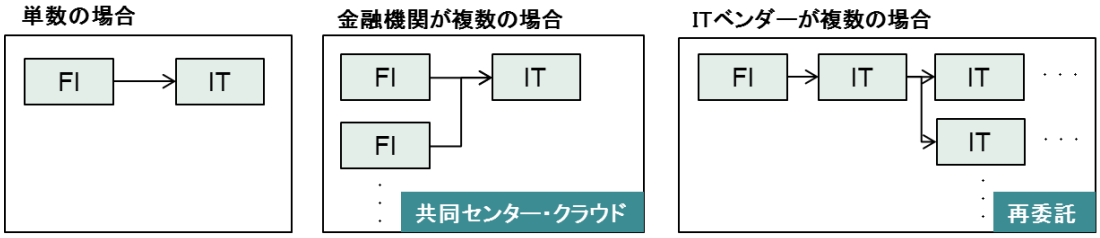
[73] 平成 28 年５月の銀行法等改正においては、あわせて「金融グループにおける経営管理の充実」のために、持株会社等が果たすべき「機能」が明確化された。また、岩原紳作『金融持株会社におけるグループガバナンス－銀行法と会社法の交錯（３）－』において「多くの金融持株会社は、（中略）子会社との間で経営管理契約を結んで経営管理のための助言・指導を行うことを定めている。」としている。

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及ぶ（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[74]。）

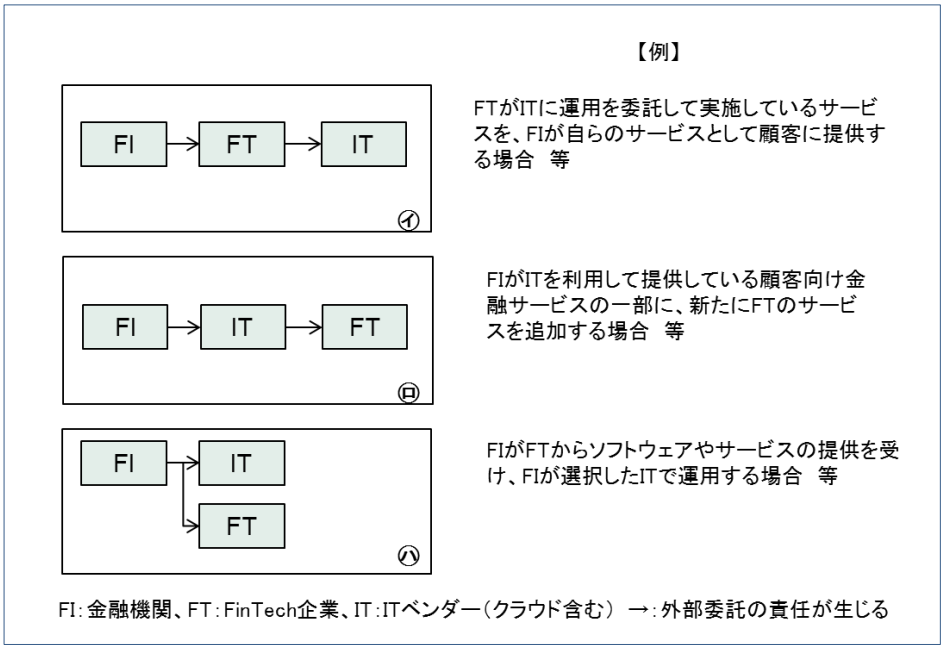
したがって、金融機関と FinTech 企業、IT ベンダーといった３者の単数及び複数の関係性を整理すれば十分[75]と考えられる。まず、３者がいずれも単数である場合については、金融機関は常に委託元となることから、残り２者の組み合わせに応じて、以下の類型が検討すべき類型として考えられる。

---

[74] 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。

[75] 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 ベンダー又は 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。

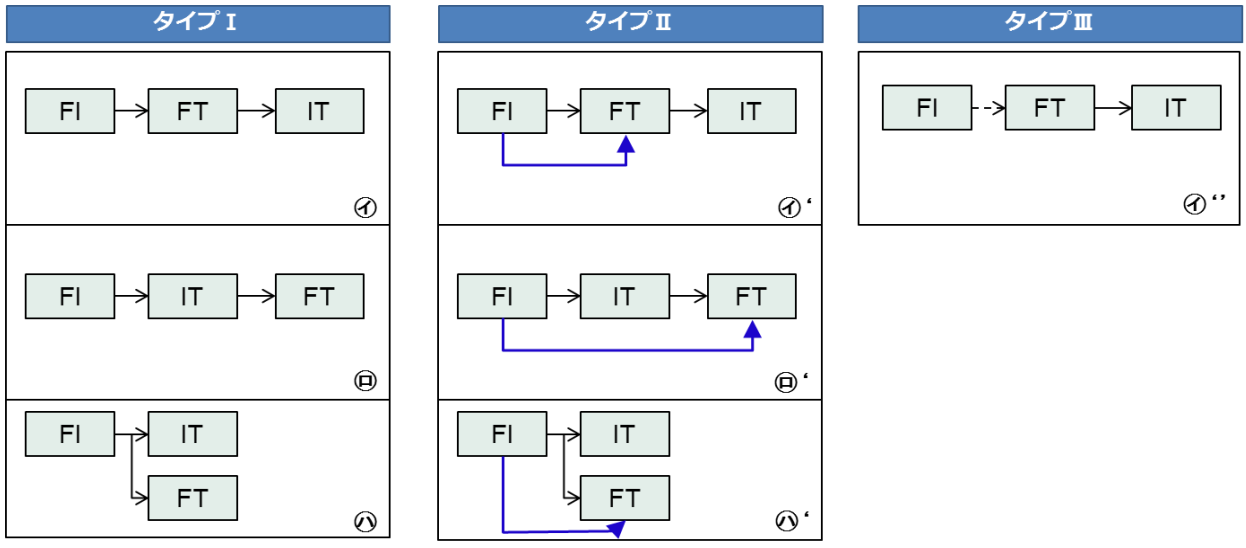
最後に、金融機関が複数となる場合は、既に２者関係の基本的類型の考え方で整理された共同性の性質以外に固有の性質はないと考えられる。

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。

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			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。
	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)	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。

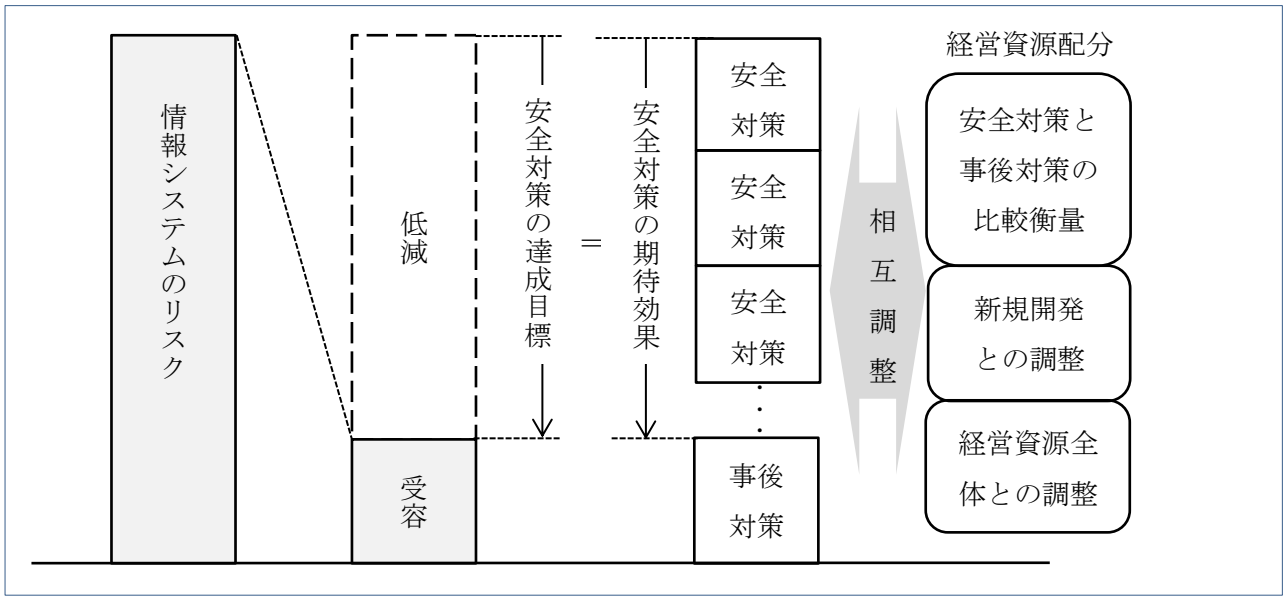
【資料５】「同等性の原則」という考え方

「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、同等に確保されるべき、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。



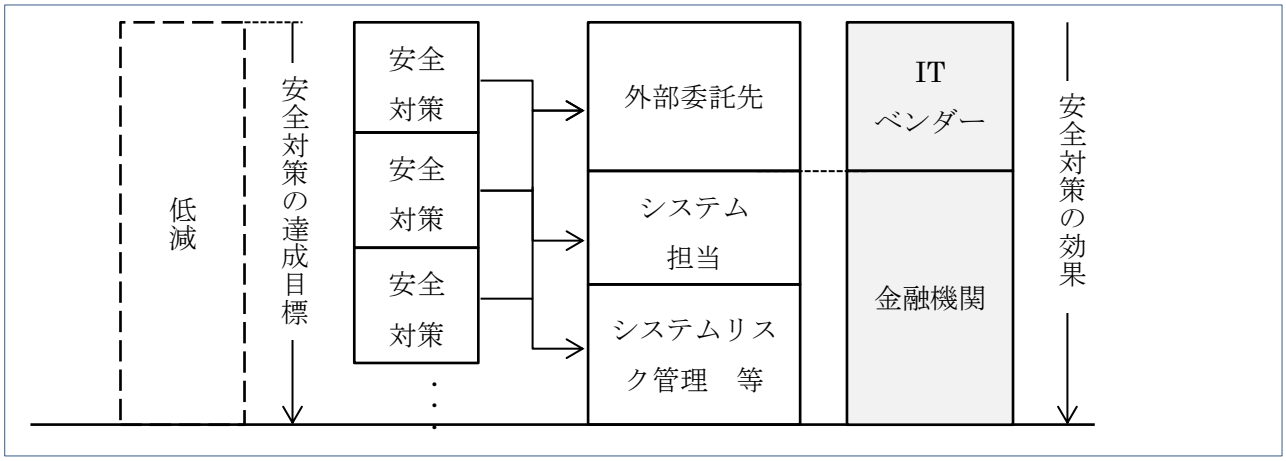
金融機関は、情報システムについて、リスク評価を通じてリスク特性を把握する。経営層は、情報システムのリスクに応じて、リスクをどの程度低減するか、あるいはどの程度受容するか[76]、を決定する。また、リスクを低減するための手段として、安全対策の達成目標を決定する。なお、安全対策の達成目標及び個々の安全対策は、リスク特性によって、安対基準を参考としながら、決定されることとなる。

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。

[76] 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。

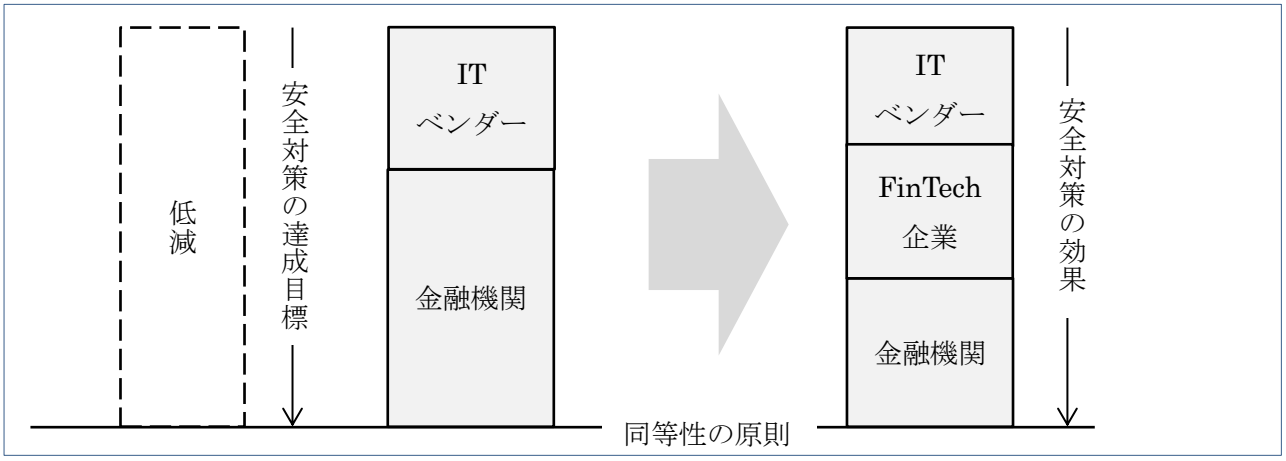


経営層によって、安全対策の達成目標と経営資源配分が決定された後は、管理者のもとで複数の関係者（システムリスク管理部門・システム担当部門・外部委託先等）によって、安全対策が実施される。実施に当たっては、個々の安全対策に応じて関係者間で担われる役割（責務）が特定（配分）される。

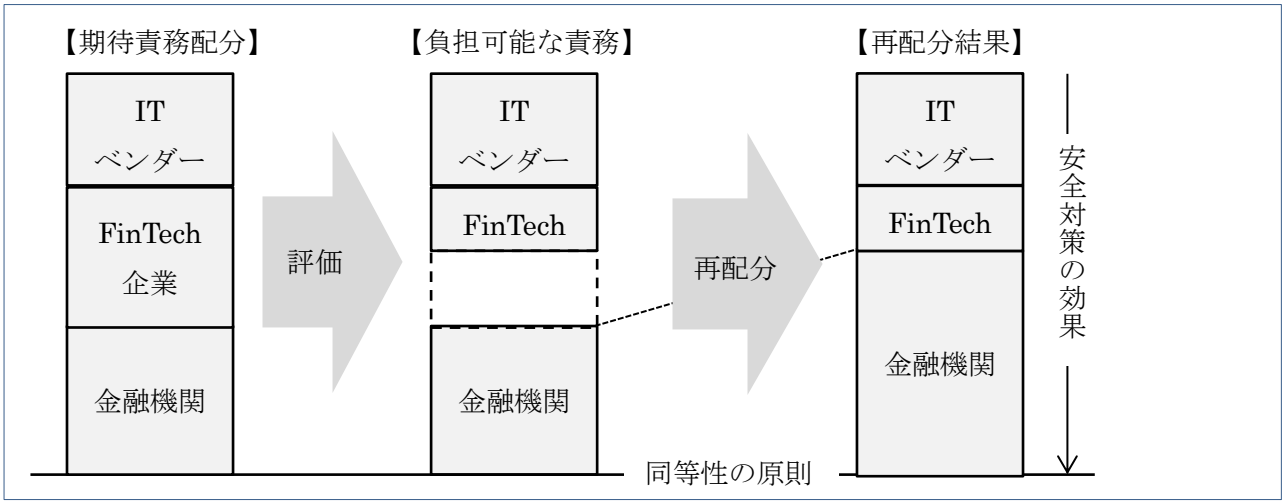
安全対策の責務は、安全対策の技術的側面を担う外部委託先と金融機関の２者に配分されるのが一般的であり、金融機関はあらかじめ安全対策遂行能力を有する外部委託先を選定するとともに、外部委託先において責務を担うために発生する費用は、最終的には、委託料として金融機関が負担することとなる。こうして、安全対策の効果が達成され、経営層が決定した受容可能な程度まで、システムリスクが低減されることを目指す。

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。

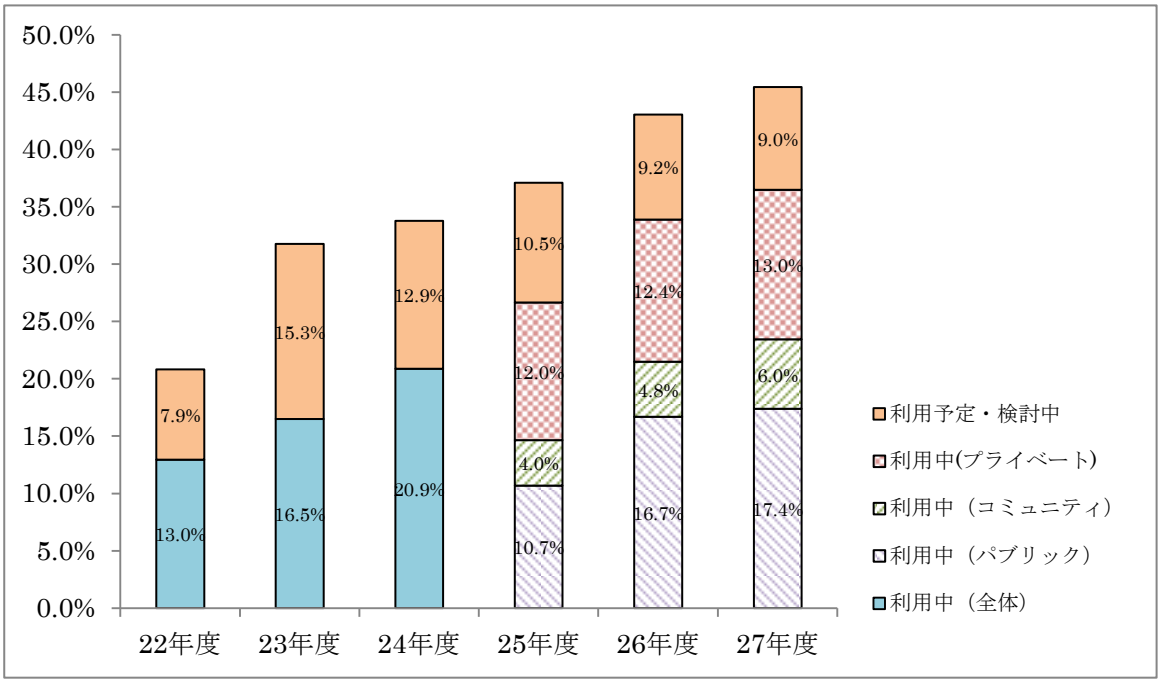
（３） 金融機械化システムに係る共同事業の調査・研究、金融機械化システムに係る斡旋・媒介、システム監査、研修・セミナー・広報等の実施。

（下線は FISC にて付す）

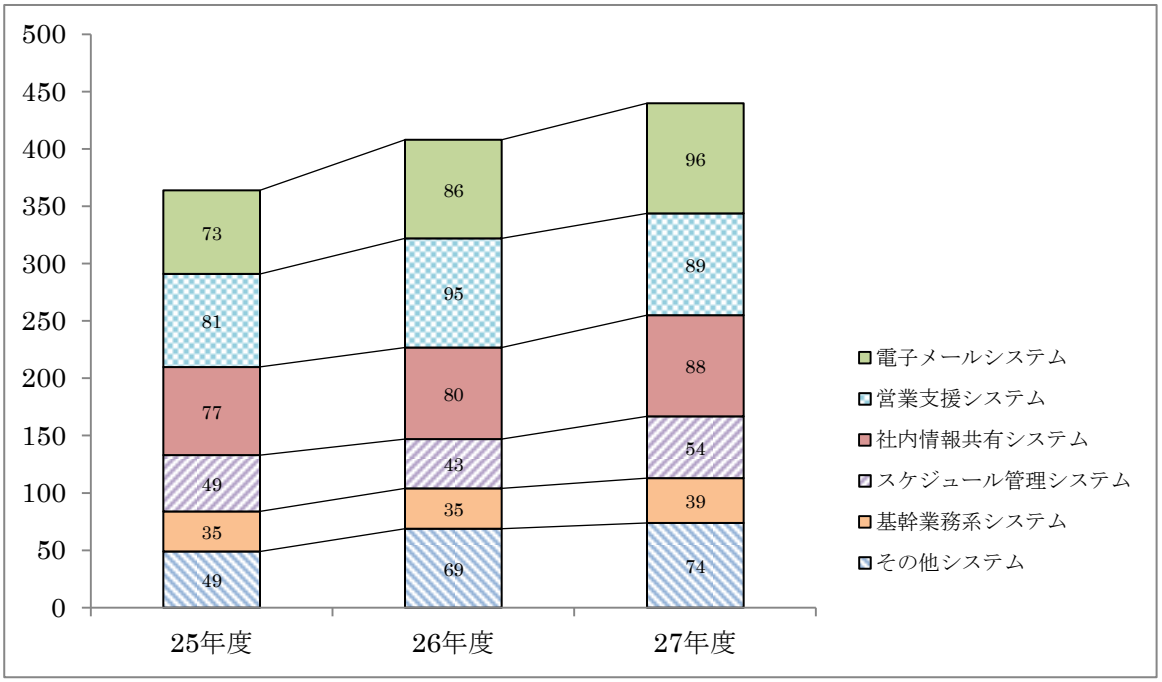
【資料７】クラウドの利用状況

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[77]。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[78]。

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ナル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*

77 http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
78 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」、及び「必要最低限の安対基準」[79]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。

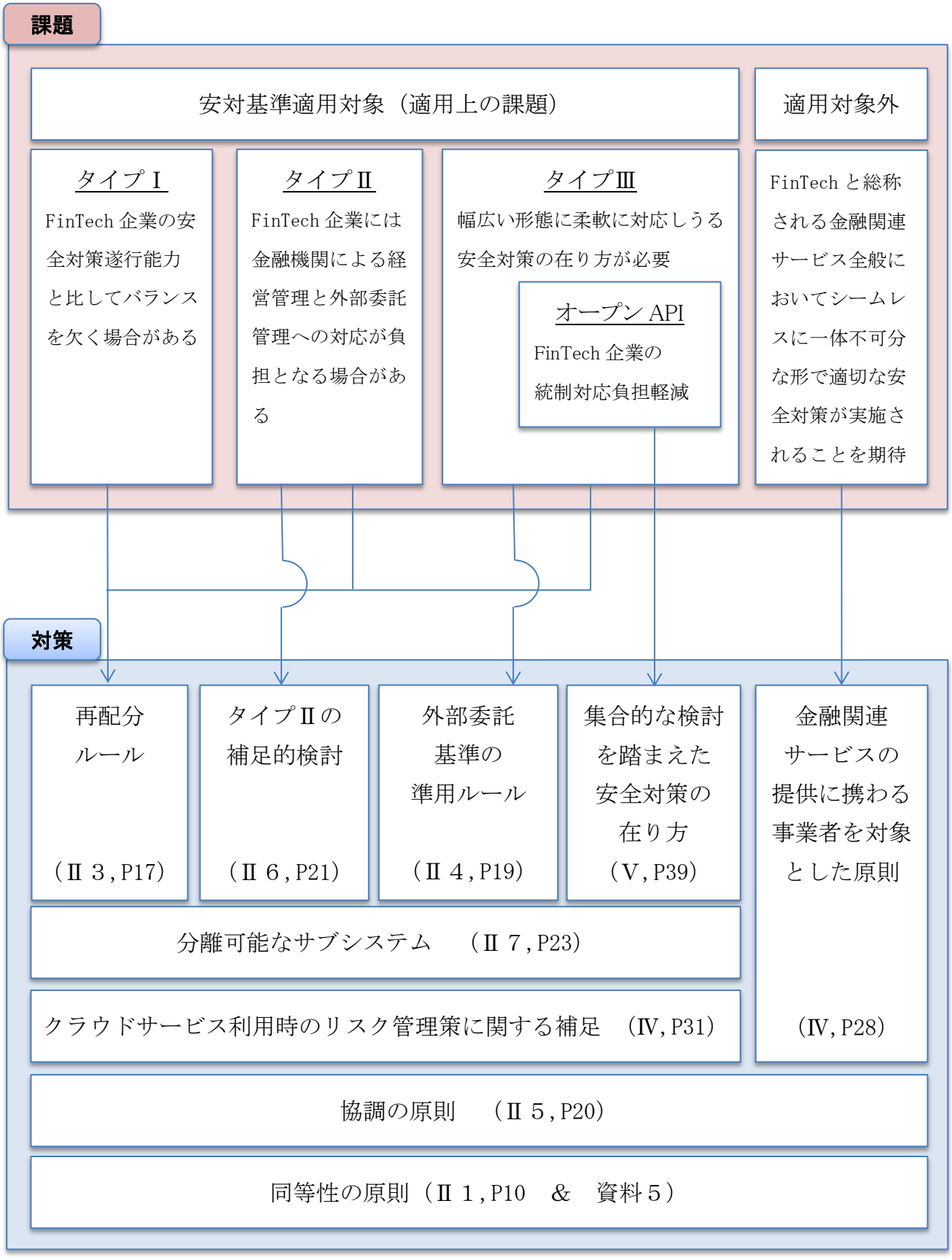
また、FinTech 企業の負担軽減の観点から、社会的規範性をもったチェックリストが制定されることが望ましく、そのためには、金融機関、FinTech 企業、IT ベンダーといった API 接続に携わる関係者が、合意形成を目指して、チェックリストの検討過程に参画することが望ましい。

チェックリストの制定に当たって、以上の集合的な検討が行われ、その結果として、成果物が取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。

[79] 「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。

【資料 10】本検討会で取り上げた課題とその対策



【資料５】

API 接続先チェックリスト ワーキンググループ
活動実績について

本ワーキンググループの活動実績につきまして、以下の通り報告いたします。なお、次回（第 10 回、6 月 20 日（火））が最終回の予定です。

１．開催実績

回数	日時	主な内容
第 1 回	2 月 7 日（火） 10 時～12 時	API 接続先チェックリスト検討の前提（FinTech 有識者検討会における議論）の内容確認
第 2 回	2 月 20 日（月） 15 時～17 時	API チェックリスト検討のたたき台（FinTech 企業の委員による発表）等をもとに議論
第 3 回	3 月 3 日（金） 15 時～17 時	API 接続先チェックリスト作成手順案（事務局案）等をもとに議論
第 4 回	3 月 17 日（金） 15 時～17 時	同上
第 5 回	4 月 11 日（火） 15 時～17 時	API 接続先チェックリスト（案）等をもとに議論
第 6 回	4 月 25 日（火） 15 時～17 時	同上
第 7 回	5 月 11 日（木） 15 時～17 時	同上
第 8 回	5 月 25 日（木） 15 時～17 時	同上
第 9 回	6 月 6 日（火） 15 時～17 時	同上

以　上