平成 29 年 3 月 23 日
公益財団法人　金融情報システムセンター

第４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 3 月 23 日（木）　15:45～17:45

Ⅱ　場所
FISC 会議室

Ⅲ　議事次第

１．	15:45	開会
２．		事務連絡等
３．	15:50	【議事１】FinTech に関する安対基準適用上の課題（第２回【議事３】再修正案検討）※タイプⅡの特性を踏まえた補足的検討
４．	16:10	【議事２】「同等性の原則」という考え方
５．	16:25	【議事３】クラウドサービス利用時のリスク管理策に関する補足的検討（プレゼンおよび第３回事後意見を踏まえた修正案の提示）
６．	17:25	【議事４】今後の安対基準等改訂の考え方
７．	17:35	【議事５】API接続先チェックリスト（仮称）ワーキンググループ活動状況と今後の予定について
８．	17:40	事務連絡
９．	17:45	閉会

Ⅳ　資料

【資料１】	第４回 FinTech 有識者検討会　座席表
【議事１】	
（参考資料）	第２回【議事３】別紙１「FinTech に関する安対基準適用上の課題」の再修正案（追加部分のみ）
【議事２】	「同等性の原則」という考え方
【議事３】	
（参考資料１）	第３回 FinTech 有識者検討会に対するご意見およびご回答
（参考資料２）	第３回【議事４】別紙１「クラウドサービス利用時のリスク管理策に関する補足的検討」の修正案
【議事４】	今後の安対基準等改訂の考え方
【議事５】	API 接続先チェックリスト（仮称）ワーキンググループ活動実績と今後の予定について

Ⅴ　連絡事項
ご意見等あれば、電子メール＜fintech@fisc.or.jp＞にお送りください。
（送付期限　3 月 30 日(木)　17 時）

Ⅵ　次回の開催予定
第５回　金融機関における FinTech に関する有識者検討会
（予定）平成 29 年５月 15 日（月）15:45～17:45　FISC 会議室

以上

【資料１】

第４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３月23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　○
西村　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※酒井様○
日本マイクロソフト株式会社　平原様○

○慶應義塾大学　安冨様
○日比谷パーク法律事務所　上山様
○株式会社みずほフィナンシャルグループ　田中様

○日本電気株式会社　※　加納様
○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
○アマゾンウェブサービスジャパン　梅谷様
○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
○株式会社南都銀行　山田様

録音業者

窓

通　路

出入口

議事１（参考資料）　第２回【議事３】別紙１「FinTech に関する安対基準適用上の課題」の再修正案（追加部分のみ）

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、金融機関および 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２参照[1]）。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[2]。

---

[1] ここでは、図表２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訳ではない。FinTech 企業に対しては、金融グループ内での位置付け等実態に応じて、金融機関において区々の管理が行われるものである。

[2] 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２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２）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･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。
・メール等システムを親会社と共通化している。
　等

以上

【議事２】

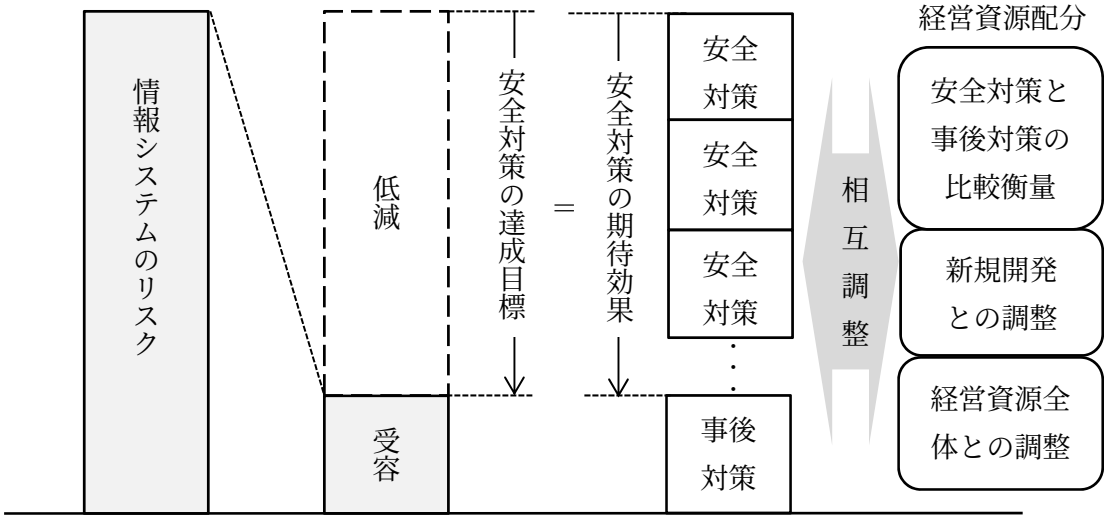
「同等性の原則」という考え方

「同等性の原則」とは、金融業務を担う情報システムの安全対策の効果は、安全対策上の関係者に関わらず、同程度に確保されるべき、とする考え方である。この原則について、リスク評価から安全対策の決定・実施にいた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いたるプロセス

（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。



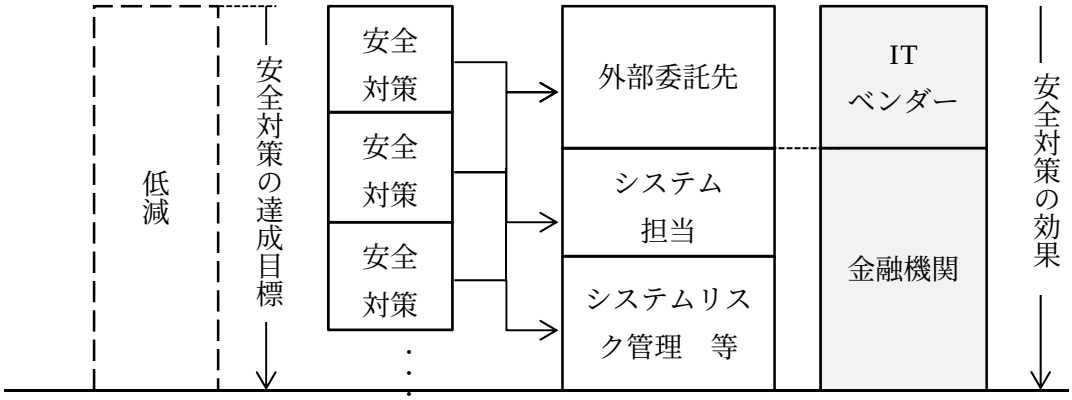
金融機関は、情報システムについて、リスク評価を通じてリスク特性を把握する。経営層は、情報システムのリスクに応じて、リスクをどの程度低減するか、あるいはどの程度受容するか[1]、を決定する。また、リスクを低減するための手段として、安全対策の達成目標を決定する。なお、安全対策の達成目標および個々の安全対策は、リスク特性によって、安対基準を参考としながら、決定されることとなる。

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。

[1] 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。

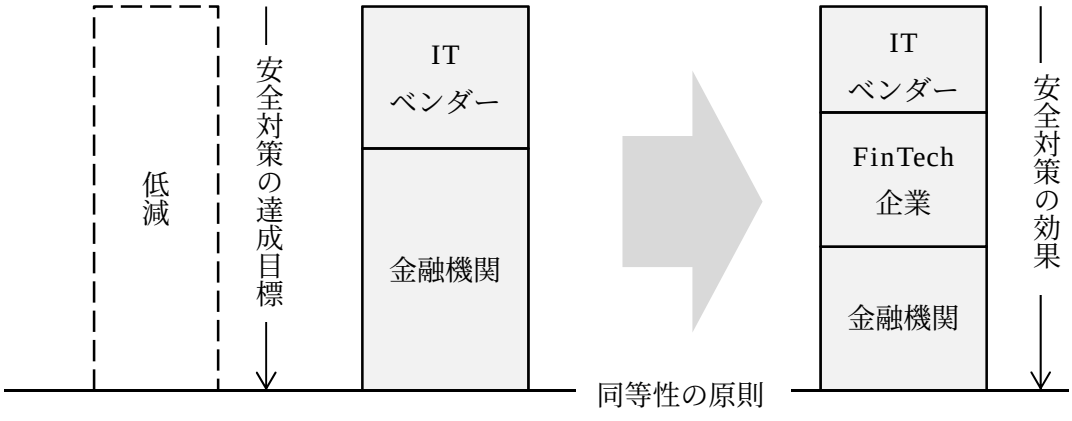


経営層によって、安全対策の達成目標と経営資源配分が決定された後は、管理者のもとで複数の関係者（システムリスク管理部門・システム担当部門・外部委託先等）によって、安全対策が実施される。実施にあたっては、個々の安全対策に応じて関係者間で担われる役割（責務）が特定（配分）される。

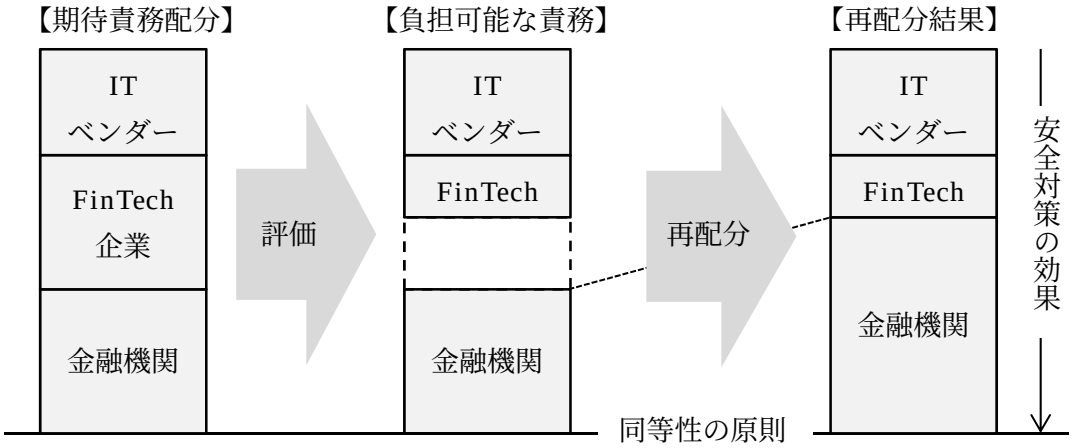
安全対策の責務は、安全対策の技術的側面を担う外部委託先と金融機関の２者に配分されるのが一般的であり、金融機関はあらかじめ安全対策遂行能力を有する外部委託先を選定するとともに、外部委託先において責務を担うために発生する費用は、最終的には、委託料として金融機関が負担することとなる。こうして、安全対策の効果が達成され、経営層が決定した受容可能な程度まで、システムリスクが低減されることを目指す。

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」とされており、責任ある事業者として、FinTech 企業においても、最低限担うべき責務、分配不可能な責務があるものとされている。

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ひとつであるが、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。

以上

【議事３】（参考資料１）　第３回 FinTech 有識者検討会に対するご意見およびご回答

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	議事２、議事３に関連	API接続先チェックリスト（仮称）ワーキンググループにおいて検討されるであろう様々な管理策については、FinTech有識者検討会における内容、FISC安全対策基準や監査指針に関する今後の検討の中でも、整合性をもった検討がなされるかという点について確認させてください。 例えば、議事２（参考資料１）のＰ．11には(API接続先における内部不正対策)として、実質的にITベンダー、あるいはクラウドベンダーへの要求事項が記載されていますが、このようなチェックリストを作成する際には、FinTech有識者検討会における検討内容が反映されるかどうかという点について、お聞かせください。	ご指摘のワーキンググループは、FISCが事務局となって運営するもので、本有識者検討会の内容を踏まえて、検討が行われる予定です。また、その成果物は、本検討会で内容を検証いただいたうえで、報告書の一部として公表し、FISC安全対策基準や監査指針は、その報告書を踏まえて検討が行われることから、それぞれが整合性をもって検討がなされることとなります。	アマゾンウェブサービスジャパン株式会社 梅谷様
2	議事４ ２．（１）匿名の共同性 （別紙Ｐ．５）	地銀共同センターを比較対象としてクラウド環境に足りない統制を語るのではなく、クラウドそのものの特性をもう一度見直し、あるべき統制を考えるほうが実行力のある統制を実現できる可能性があがるのではないかと考えます。 例えば、「安全対策を決定する主な役割は、個々の利用者ではなくサービス全体に責任を負うクラウド事業者に帰属すること」という記述がありますが、クラウドのサービス提供の内容によって責任の分担が実際はことなります。 そのためユーザーとクラウドベンダーにおいて、責任分界点をよく理解した上で統制を決定する必要があるというクラウド固有の特性を考慮し、「安全対策を決定する主な役割は、各々のクラウドサービスにおける責任分界点をよく理解した上で、決定される必要があり、クラウドベンダーとの事前の協議の上で統制の範囲を決定するのが望ましい」という趣旨を論点メモの中に別途記載していただけませんでしょうか。 あるいは匿名の共同性とは別に、記載事項として責任分界点の確認などとしたうえで、性質の重要な要素として記載いた	ご指摘を踏まえて、原案の「２．クラウドサービス固有の性質」に、以下の修正を行うとともに脚注を追加します。 *（修正前）* *統制の検討にあたっては、外部委託検討会報告書で提言された「共同センター」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。* *以上から、重要な情報システムに関する補足的検討にあたっては、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を参考としつつ、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。* *（修正後）* *統制の検討にあたっては、<u>同様に共同性という性質を有する</u>「共同センター」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<u>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</u>*	アマゾンウェブサービスジャパン株式会社 梅谷様

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
		だけませんでしょうか。	*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あたっては、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。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。* *（脚注11 追加）* *FISC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ひとつとして「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り決め」があげられている。*	
3	議事４ ２．（３）技術の先進性 （別紙Ｐ．６）	クラウド環境における監査については、クラウド側で提供している監査機能やサービスを利用することによる、監査の効率化や高度化を実施可能になる場合もあるため、その点については特性を理解した上で積極的な活用も考えられるという点について記述を追加していただけませんでしょうか。	ご指摘を踏まえて、原案の「３．リスク管理策に関する補足」に以下の脚注を追加します。 *（脚注追加）* *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。*	アマゾンウェブサービスジャパン株式会社 梅谷様
4	議事４ ３．（１）客観的評価を実施する際の留意事項 （別紙Ｐ．７）	「安対基準の設備基準や技術基準を含めることをかならずしも意味しないことに留意が必要である」、という点は現在の実務と照らし合わせた上で適切と考えます。	―	アマゾンウェブサービスジャパン株式会社 梅谷様

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
5	議事４ ３.（２）データアクセス拠点の把握 （別紙Ｐ．８）	統制対象クラウド拠点とは具体的にはどのような施設が対象に入るのでしょうか。 また、「統制対象クラウド拠点が原則として国内に所在すること」という記述がありますが、どのような施設が国内に存在すればよいと考えられますでしょうか。 また、統制対象クラウド拠点が国内にあることの実質的な意味を管轄権を踏まえてすこし具体的に示していただけませんでしょうか。	ご指摘を踏まえて、「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」（別紙参照）を追加のうえ、リスク管理策を以下のとおり修正します。 *（修正前）* *また、統制の実効性を担保するため、統制対象クラウド拠点は、原則として、国内に所在すること、としてはどうか。それが不可能な場合は、契約において、金融機関が、必要なデータに実効的にアクセスできる手段を手当てすること* *（修正後）* *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*	アマゾンウェブサービスジャパン株式会社 梅谷様
6	議事４ ３.（３）監査権の明記 （別紙Ｐ．８）	ここで記述されている監査権とは、どのような監査権をさすのでしょうか。 また、統制対象クラウド拠点とは具体的にはどのような施設を対象としてもよいと考えられるのでしょうか。	ご指摘を踏まえて、「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」（別紙参照）を追加のうえ、リスク管理策を以下のとおり修正します。 *（修正前）* *「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、その社会的・公共的な性質に鑑み、金融機関が、統制対象クラウド拠点に対して監査が可能となるよう、業務委託契約に明記すること* *（修正後）* *「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、その社会的・公共的な性質に鑑み、金融機関が、統制対象クラウド拠点に対して、実質的な統制を行うにあたって必要となる権利（監査権等）を、**クラウド事業者と交わす契約書**に明記すること*	アマゾンウェブサービスジャパン株式会社 梅谷様

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
7	議事４ ３.（４）監査の実施 （別紙Ｐ．８）	「クラウド事業者自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」、という点については賛同します。 また、「定期的に監査を実施する」という記述がありますが、これはどのような監査を想定しているのでしょうか。	ここでいう「監査」とは、「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」（別紙参照）記載の下線のことを指します。 *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*	アマゾンウェブサービスジャパン株式会社 梅谷様
8	議事４ ３.（５）監査人等モニタリング人材の配置 （別紙Ｐ．８）	「必要となる人材を配置すること」の記述に賛同します。	―	アマゾンウェブサービスジャパン株式会社 梅谷様
9	議事４ ３.（１）客観的評価を実施する際の留意事項 （別紙Ｐ．７）	安対基準を用いないとすれば各行が区々の基準で対応することになるため、必要最低限の基準は明確にする必要があるのではないか。	今後、安対基準の改訂において、「必要最低限の安対基準」の策定が予定されており、ご指摘の内容を参考としながら、検討を行います。	南都銀行様
10	議事４ ３.（２）データアクセス拠点の把握 （別紙Ｐ．８）	「統制の実効性を担保するため、統制対象クラウド拠点は、原則として、国内に所在すること、としてはどうか」との記述があるが、重要な情報システムのクラウドサービスの利用に際しては、その事業拠点の把握が出来、実効的な監査が行えるのであれば、クラウド拠点が国内に限るとする必要はないのではないか（海外のクラウド拠点を利用したFinTechサービスの提供も考えられるため）	No.5　回答を参照ください。	南都銀行様

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
11	議事４ ３．（２）データアクセス拠点の把握 （別紙1Ｐ．７）	「重要な情報システム」「必要データ」「統制対象クラウド拠点」の詳細な定義についてご教示願います。	「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」および「機微情報を保有する情報システム」のことをいいます。（詳細は、「外部委託検討会報告書」Ｐ．31を参照ください。） 「必要データ」および「統制対象クラウド拠点」については、No.5回答を参照ください。	日本マイクロソフト株式会社 平原様
12	議事４ ３．（２）データアクセス拠点の把握 （別紙１Ｐ．８）	金融機関が必要データに実効的にアクセスできる手段が契約上手当されていれば、統制の実行性が担保されるので、「統制対象クラウド拠点」を「原則国内とする」必要はないのではないかと思料致しますがいかがでしょうか。	No.5　回答を参照ください。	日本マイクロソフト株式会社 平原様
13	議事４ ３．（４）監査の実施 （別紙１Ｐ．８）	「保証型監査」とは、JASAの整理する「助言型監査」と「保証型監査」の分類のうちの「保証型監査」を意味すると理解してよいでしょうか。監査法人による監査結果の保証は必要ないと理解してよいでしょうか。	保証型監査報告書とは、「金融機関等のシステム監査指針（改訂第３版追補）」（Ｐ．22）の「既にクラウド事業者が受検している監査結果（SOC2,IT7号等）」のことをいいます。 つまり、米国公認会計士協会あるいは日本公認会計士協会が定める内部統制報告の枠組みのもとで作成された報告書を指します。	日本マイクロソフト株式会社 平原様
14	議事４ ３．（４）監査の実施 （別紙１Ｐ．８）	安対基準との整合性が確認できる報告書であれば、必ずしも、検証方法が安対基準と整合的に行われる必要はないのではないかと思料致しますがいかがでしょうか。	整合的であるべきは、検証方法ではなく検証の内容ですので、ご指摘を踏まえて、原案の「３．リスク管理策に関する補足」に以下の修正を行います。 *（修正前）* *安対基準と整合的に検証が行われている報告書を利用することが望ましい* *（修正後）* *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*	日本マイクロソフト株式会社 平原様

第３回議事資料：

議事１：「第２回 FinTech 有識者検討会に対するご意見及びご回答」

議事２：プレゼン（一般社団法人全国銀行協会）「オープンAPIのあり方に関する全銀協の検討状況」

議事３：「API 接続先チェックリスト（仮称）ワーキンググループの設置」

議事４：論点メモ「クラウドサービス利用時のリスク管理策に関する補足的検討」

【議事３】（参考資料２）　第３回【議事４】別紙１「クラウドサービス利用時のリスク管理策に関する補足的検討」の修正案

別紙１

クラウドサービス利用時のリスク管理策に関する補足的検討

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、およ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[1]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益々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更に深められてきた。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更に高める観点から、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[2]。

（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。

削除: [3]

海外先進諸国におけるガイドラインでは、我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。（詳細は【参考２】を参照）

削除: 特に

・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まれる[4]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得るとされている。さらに、管轄権については、データアクセス

[1] 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。詳細は【参考１】を参照。
[2] 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、外部委託報告書脚注31を参照。
[4] 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。

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ェア、そして一部の開発運用要員程度であった[5]。

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

[5] そのため、安全対策における統制にあたっては、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。

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[6]。

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[7]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、利用が一層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、受け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[8]。統制の検討にあたっては、同様に共同性という性質を有する「共同センター[9]」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

削除: サービス全体に責任を負う

削除: サービス

削除: 同様に共同性を有する形態である共同センターと比較して、

削除: 問題

削除: 外部委託検討会報告書で提言された

[6] 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。

[7] 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ベンダーもある）、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。

[8] 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月のシステム監査指針の改訂では、「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。

[9] 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。

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あたっては、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[10]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[11]。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[12]。

（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。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、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を検討することが必要となる。

以上から、重要な情報システムに関する補足的検討にあたっては、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[13]。

（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

---

[10] 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、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。

[11] FISC 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ひとつとして「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り決め」があげられている。

[12] 統制能力の向上策のひと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。

[13] 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。

削除: を

削除: 契約に明記することが

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[14]とともに、ソフトウェア技術自体も、旧来の技術を塗り替える、より実効的な技術が次々と登場する場合がある。したがって、設備基準や技術基準といった技術的な安全対策を、あらかじめ一意に特定しておくことが、必ずしも適切ではないことが生じうる。

そうした中、従来の安対基準では、運用基準・設備基準・技術基準相互の取扱いの考え方が、必ずしも明確に示されていないため、例えば、クラウド事業者選定時の客観的評価において、評価事項に設備基準や技術基準が字義通りに利用される、といった不確実性が残る現状にある。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、検討することが必要となる。

以上から、補足的検討にあたっては、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[15]。

（４）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あたっては、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

[14] 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得る。
[15] 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」とされている。また、「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。

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、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く、金融機関が負うべきものである。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[16]。

３．リスク管理策に関する補足

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

（1）データアクセス拠点の把握

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関は、クラウド事業者の選定時において、統制上必要となるデータ（以下「必要データ」という）へのアクセスが可能となる情報処理拠点等、実質的な統制を行うにあたり対象となる事業拠点[17]（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。

削除: 2

削除: 、としてはどうか

削除: 統制の実効性を担保するため、

削除: 原則として、国内に所在すること

削除: 、としてはどうか

削除: それが不可能な場合は、契約において、金融機関が、必要データに実効的にアクセスできる手段を手当てすること、としてはどうか。

[16] 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、全ての金融機関において、クラウド事業者に一意なリスク管理策を求めることを必ずしも意味しない。例えば、有事には、クラウドサービスの復旧を待つことなく、有事用にスタンバイしているシステムを稼働させるような業務継続計画であれば、クラウドサービスの復旧を前提とした業務継続計画の場合とは、自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、外部委託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。

[17] 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。

（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、その社会的・公共的な性質に鑑み、金融機関が、統制対象クラウド拠点に対して、実質的な統制を行うにあたって必要となる権利（監査権等）を、クラウド事業者と交わす契約書に明記すること。

（3）監査の実施

監査にあたっては、技術が先進的であることから、クラウド事業者が自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[18]。

「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、実質的な統制が十全かつ実効的に機能するよう、定期的に監査を実施すること。

（4）監査人等モニタリング人材の配置

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

（5）客観的評価を実施する際の留意事項

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

以上

削除: 3
削除: 監査
削除: が可能となるよう
削除: 業務委託契約
削除: 、としてはどうか
削除: 4
削除: 、としてはどうか
削除: に
削除: 、としてはどうか
削除: 、としてはどうか
削除: 5
削除: 、としてはどうか
削除: 、としてはどうか
削除: 1
削除: 、としてはどうか

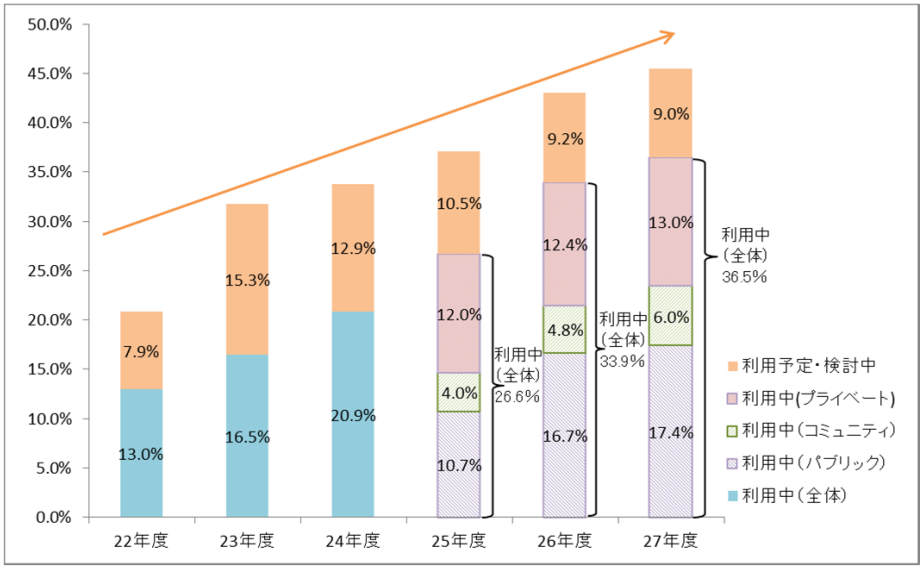
[18] その他に、実効的かつ効率的な監査を実施する手段として、インターネット等を通じて利用者に提供される監査証跡の閲覧等クラウド事業者がサービスとして提供する監査機能を利用することも考えられる。

参考１

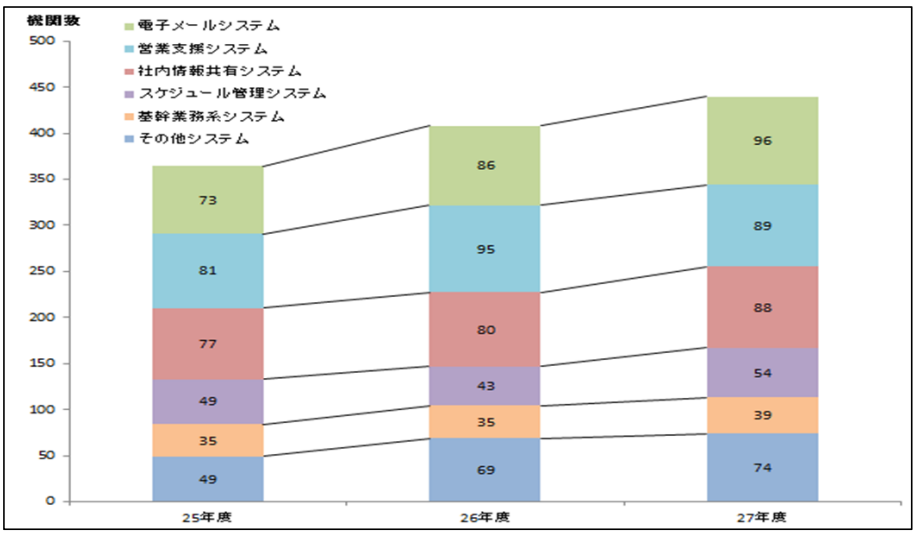
クラウドの利用状況

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。

（図表１）　クラウドの利用推移



（図表２）　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）

参考２

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、我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[19]。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[20]。

ここでは、上記の公表文書および当センターが米国通貨監督庁（Office of the Comptroller of the Currency、以下 OCC）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、統制の強化を求めている。

「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

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

2. 統制に対する考え方

統制にあたっては、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、たと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

19 http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf

20 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、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。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、データおよび事業者に対して、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、クラウド事業者が自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、クラウドには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。また、これまでになかったリスクとして、匿名の利用者同志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 の方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

「委託元毎で、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。

以上

【議事４】

今後の安対基準等改訂の考え方

本検討会の後に、FISC では、外部委託検討会および 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」および「必要最低限の安対基準」の定義および位置づけの明確化

「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、全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）外部に対する統制の形態の整理

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あり方にしたがって、基準等を整理する。

【議事５】

API 接続先チェックリスト（仮称）ワーキンググループ
活動実績と今後の予定について

前回の本検討会（2 月 2 日開催）におきまして承認いただきましたワーキンググループの活動実績等につきまして、以下の通り報告いたします。

１．委員

（別紙１「委員名簿」参照）

２．開催実績

回数	日時・場所	主な内容
第 1 回	2 月 7 日（火）10 時～12 時 FISC 会議室	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 FISC 会議室	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 FISC 会議室	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 FISC 会議室	同上

３．今後の予定

・API 接続先チェックリスト原案等を次回の本検討会（5 月 15 日開催予定）に上程予定。

以　上

別紙１

API 接続先チェックリスト（仮称）ワーキンググループ
委員名簿

（敬称略）

区分	氏名	所属・役職
銀行 （3 名）	奥野　瑞穂	株式会社みずほ銀行 e-ビジネス営業部　調査役
	小原　彰	株式会社三井住友銀行 システム統括部　統括グループ　グループ長
	原田　一雪	株式会社三菱東京 UFJ 銀行 デジタルイノベーション推進部　次長
FinTech 企業 （3 名）	土佐　鉄平	freee 株式会社 開発本部　チーフセキュリティアーキテクト
	大目　晃弘	マネーツリー株式会社 事業開発部　ビジネスデベロプメントマネージャー
	内波　生一	株式会社マネーフォワード アカウントアグリゲーション本部　本部長
IT ベンダー （3 名）	村上　隆	株式会社エヌ・ティ・ティ・データ 第四金融事業本部　企画部　シニア・スペシャリスト
	鎌田　美樹夫	日本アイ・ビー・エム株式会社 グローバル・ビジネス・サービス事業部 金融インダストリー・ソリューション　担当部長
	谷内　圭	富士通株式会社 金融システム事業本部　デジタルビジネス開発室 シニアマネージャー
FISC （1 名）	亀水　宏次	公益財団法人金融情報システムセンター 監査安全部　次長
オブザーバー （4 名）	小林　侑剛	金融庁 総務企画局　企画課　信用制度参事官室　課長補佐
	市村　雅史	金融庁 検査局　総務課　システムモニタリングチーム 専門検査官
	中井　大輔	日本銀行 金融機構局　考査企画課　企画役
	宮　　将史	日本銀行 決済機構局　FinTech センター 決済高度化グループ長　企画役

（事務局：公益財団法人金融情報システムセンター　企画部）