KPMG Insight

KPMG Newsletter
September 2015

金融機関におけるクラウドサービスの活用と保証報告制度の枠組み

KPMG
cutting through complexity

Volume 14

金融機関におけるクラウドサービスの活用と保証報告制度の枠組み

有限責任 あずさ監査法人 IT 監査部
パートナー 小松 博明
シニアマネジャー 仲 友紀

クラウドサービスを安全に活用してメリットを享受するには、経営判断に基づく適切なリスク管理が必要です。金融機関の自主規制団体である FISC は、2014 年 11 月に公表された「金融機関におけるクラウド利用に関する有識者検討会報告書」に基づき、クラウドサービスの利用への対応を 1 つの目玉として、2015 年 6 月に「安全対策基準」を改訂しました。これらにおいては、金融機関の対応方法の 1 つとして、監査法人等が発行する保証報告書の活用が挙げられています。

日本公認会計士協会は、上記に対応し、金融機関のクラウドサービス利用に際して安全対策基準等、業界の自主規制基準の観点を追加した保証報告書業務の提供が可能となるよう、実務指針を改正し、2015 年 7 月に公開草案を公表しています。本稿では、安全対策基準の改訂内容のほか、監査法人等が行う保証報告書業務の枠組みと保証報告書の利用にあたっての留意事項を解説します。

なお、本文中の意見に関する部分は筆者の私見であることをあらかじめお断りしておきます。

【ポイント】

- クラウドサービスの有するさまざまなメリットやリスク、適切なリスク管理・契約管理のあり方等について幅広く議論され、2014 年 11 月に「金融機関におけるクラウド利用に関する有識者検討会報告書」が公表された。
- 当該有識者検討会報告書では、リスク管理の基本的なアプローチとして、リスクベースによる経営者判断を強調している。
- 金融情報システムセンター（FISC）は、上記報告書の内容を踏まえた具体的な管理策を「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」の改訂に反映し、2015 年 6 月に公表した。
- 日本公認会計士協会は、この動きに対応する形で 2015 年 7 月 23 日に「IT 委員会実務指針第 7 号」の改訂指針を公開草案として公表し、規制当局の要求事項や業界団体の自主規制等の遵守に関連し、追加された主題情報に対して保証業務を提供できるよう必要な修正を行っている。
- クラウドサービスの利用に限らず、金融機関のガバナンスにおいて、今後、委託先管理の重要性が増すものと思われるが、委託元金融機関による立入検査等の代わりとして、監査法人が行う保証報告書業務の活用が有効と考えられる。ただし、活用にあたっては、その枠組みの理解が求められる。

小松 博明（こまつ ひろあき）
有限責任 あずさ監査法人
IT 監査部
パートナー

仲 友紀（なか ゆうき）
有限責任 あずさ監査法人
IT 監査部
シニアマネジャー

Ⅰ はじめに

「クラウドコンピューティング」の概念・技術が登場して以来、我が国の金融機関等においても、それに基づく「クラウドサービス」を経営に生かすための検討が行われてきました。しかし、クラウドサービスに関するセキュリティや信頼性に係る懸念から、特に中小の金融機関においては、利用が進まない状況が続いています。

背景の1つとしては、金融機関におけるコンピュータシステムが一般市民の生活を支える社会インフラとして定着し、極めて高いレベルの安全性と信頼性を求められているという事情があります。

金融機関等は、この高い要請に業界として応えるため、1984年にコンピュータメーカー等と共同して「金融情報システムセンター」(The Center for Financial Industry Information Systems、以下「FISC」という)を設立し、自主基準としての「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」、「金融機関等のシステム監査指針」等を刊行して継続的に改訂を行っています。また、いわゆる金融検査において対象金融機関のシステムリスク管理態勢に問題が見られ、さらに深い業務の具体的検証が必要と認められる場合には、検査官は、この安全対策基準に基づいて検証を行うものとされています。

クラウドサービスの利用については、2013年5月に発刊された追補版において暫定的な対応がされましたが、その後、改めてクラウドサービスの有するさまざまなメリットやリスク、適切なリスク管理・契約管理のあり方等について有識者検討会による本格的な検討が行われ、2014年11月に「金融機関におけるクラウド利用に関する有識者検討会報告書」(以下「有識者検討会報告書」という)が公表されました。また、今年6月には、本報告書を踏まえる形で「金融機関等コンピュータシステムの安全対策基準・解説書」(以下「安全対策基準」という)が公表されています。以下、本文Ⅱ章Ⅲ章において、これらの内容を紹介します。

上記の動きに歩調を合わせ、日本公認会計士協会は、規制当局の要求事項や業界団体の自主規制等の遵守に係る追加された主題情報に対して保証業務を提供できるよう、IT委員会実務指針第7号、「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書」(以下「IT7号」という)の改訂作業を行ってきました。

クラウドサービスの利用にあたっては、リスクの度合いに応じて利用金融機関によるクラウド事業者のリスク管理態勢の点検、監査等が想定されますが、米国では監査法人等による内部統制の保証報告書を利用する実務が浸透しており、今回、我が国の金融機関がクラウドサービスを活用する場面においても利用が想定されます。以下、本文Ⅳ章Ⅴ章において、監査法人等[1]が行う保証報告書業務の枠組み、及び保証報告書利用にあたっての留意事項について説明します。

Ⅱ クラウドサービス利用に関するリスク管理の基本的な考え方

まず、クラウドサービスを利用する場合のリスク管理の基本的な考え方について、有識者検討会報告書の内容をご紹介しながら、解説します。

有識者検討会報告書は、次の3つのパートから構成されています。このうち、3番目の具体的なリスク管理策は、Ⅲ章で紹介する安全対策基準の改訂内容に具体化されていますので、ここでは、1番目と2番目について、ポイントを取り上げます。

- クラウドの特性
- リスク管理に関する基本的な考え方(リスクベースアプローチ)
- 具体的なリスク管理策

1. クラウドの特性の理解

まず、有識者検討会報告書は、冒頭部分において、検討の対象を「資源共有型スキームの色合いが最も強い『パブリッククラウド』」に限定していることがポイントとして挙げられます。

我が国における普及の初期には、利用者個別向けに専用の環境を用意する、いわゆる「プライベートクラウド」が市場において盛んに紹介されていましたが、データセンターにおけるホスティングサービスの利用等、従来からある形態と大差がなく、既存の枠組みがそのまま適用できる部分が多いためです。

さらに、パブリッククラウドを「『外部委託』の一形態として扱うことが適当」としています。これも従来のASP(Application Service Provider)において、一部の業者や利用者が「ASPはサービス利用契約であって、業務委託契約(外部委託)ではない(そのため監査の対象にはならない)」旨の主張をすることがあったため、金融機関等がクラウドサービスを利用する場合には、契約形態に限らず外部委託として検査・監査の対象となることを明確にしたものと考えられます。

金融庁の「主要行等向けの総合的な監督指針」には「外部委託には、銀行がその業務を営むために必要な事務を第三者に委託することを含む(形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む)」(下線は筆者による)と記載されています。

1. 監査法人及び公認会計士

2. リスクベースアプローチ

リスク管理に関する基本的な考え方としては、「リスクベースアプローチによる経営判断」を推奨し、リスク管理策設定に至る道筋について、具体例を挙げながら解説しています。

ここでポイントとなるのは、クラウドサービスを利用するにあたって策定すべきリスク管理策の検討において、適用する業務・システムの重要度を一定の評価軸により評価し、相対的に重要度が高くない業務・システムに適用する場合には、Ⅲ章の「具体的なリスク管理策」において「簡易なリスク管理策」を採用できるという議論に繋げている点です。

重要度の評価方法としては、「システムの可用性」と「データの機密性」の2軸により総合的に評価して3段階（高・中・低、又はコアIT領域、セミコアIT領域、ノンコアIT領域）に分ける例と、可用性又は機密性のどちらかを軸として2段階（高・低）に分ける例を挙げています。

Ⅲ 安全対策基準の改訂について

1. 概要

前述のとおり、安全対策基準は、2015年6月に「第8版追補改訂」として改訂されました。

このうち、クラウドサービス利用に関する改訂内容について、**図表1**にまとめました。

図表1　安全対策基準の改訂

＜第８版追補＞	＜第８版追補改訂＞（今回の改訂）
【運 108】 ・外部委託管理 ・システム監査 ・セキュリティ管理 ・利用終了時のデータ消去	【運 108】 ①事業者選定 ②データ所在の把握 【運 109】 ①契約締結・サービスレベル合意 ②ベンダーロックイン防止 【運 110】 利用中のデータ漏洩防止策 【運 111】 契約終了時のデータ漏洩防止策 【運 112】 立入監査・モニタリング

直近の改訂は2013年の「第8版追補」であり、2011年の全面改訂（第8版）以降に発生した情勢変化（東日本大震災、スマートフォンの利用の進展等）と併せてクラウド関連の基準【運108】を盛り込みました。しかし、内容的には、外部委託管理、システム監査、セキュリティ管理等について、他の基準の参照に留まるという暫定的なものでした。

今回の改訂では、旧【運108】を廃止し、有識者検討報告書の内容に基づき、クラウド特有のリスク管理策とリスクベースアプローチの考え方を採り入れた【運108】～【運112】の5項目を追加しています。次節において、個別にポイントを解説します。

2. 改訂のポイント

（1）事業者選定【運108】

パブリッククラウドサービスは、規模の利益によるコストダウンを前提としたビジネスモデルであるため、事業者は一律の約款による契約を前提とし、利用者からの個別の契約上の要求には応じないことが一般的です。したがって、事業者の選定にあたっては、事業者が対応可能なサービスの事前確認と、それを踏まえた業務・システムの適用範囲の決定を明確な手続きにより行うことが重要です。

また、事業者によっては、海外を含めたデータセンターに利用者のデータを分散格納する可能性や、データの所在を確定できない場合があります。事業者選定にあたっては、このような可能性を事前に把握し、適用しようとする業務・システムの性質に照らして、適用法令やシステムの可用性・信頼性の観点から、適切な事業者・クラウドサービスの選定が行われるような仕組みづくりが求められます。

（2）契約締結・サービスレベル合意（以下「SLA」という）【運109】

上述したように、パブリッククラウドを利用する場合には、事業者が提示する標準的な契約条項の変更を要求することが難しい場合が多いですが、可能な場合に契約やSLAに明記すべき事項の例が挙げられています。

すなわち、事業者からの情報開示（複数のクラウド事業者が関係する場合の他事業者の情報、再委託先に係る情報を含むと考えます）、再委託先の管理、当局検査への対応、委託元金融機関による立入監査を含む事業者の業務に対するモニタリング等です。

また、事業者側・金融機関側の双方事情によって契約の続行が困難になった場合、事業者の協力がなくても、他の事業者にシステム資源を移行できるように対策しておくことが望まれます。

（3）利用中のデータ漏洩防止策【運110】

顧客データ等の重要データを含む業務・システムにパブリッククラウドを適用する場合の対策で、具体的には、暗号化やトークン化によるデータの漏洩防止策と、故障により記憶装置等の交換が必要になった場合、データが記憶された装置等から漏洩が起こるリスクを想定した対応です。

暗号化やトークン化については、それらの仕様上の制約や暗号鍵等の管理策の不備による漏洩が起こらないよう、事前調査や事業者からの情報収集と協議を行うことになります。

また、記憶装置等に物理的にデータが残存している場合（一般的な消去動作のみでは、データは記憶装置に物理的に残存する）、特殊な技術により復元が可能であり、交換した記憶装置等からのデータ漏洩リスクについては、事業者により対応が異なり注意が必要です。

(4) 契約終了時のデータ漏洩防止策【運111】

上記 (3) において触れたとおり、記憶装置上のデータは、記憶装置を物理的に破壊するか、無意味なデータを論理的に上書きしない限り復元可能です（データの上書きによる完全消去に関しては、欧米を中心に複数の規格があります）。また、データが広範囲にわたり分散格納されるというパブリッククラウドの特性から、ある利用者のデータが格納された可能性がある記憶装置等を特定すること自体が実務上困難であることも想定されます。

このため、顧客データ等の重要データを含む業務・システムにパブリッククラウドを適用する場合には、リスクプロファイルを検討する段階において、暗号化等の対策や事業者側の対応可能性を加味して総合的に判断する必要があります。事業者との契約やSLAに反映する必要がある場合がありますので、契約終了時の対応についてもシステム企画の段階から十分に検討することが望ましいと考えます。

(5) 立入監査・モニタリング【運112】

パブリッククラウドの場合、個別利用者の立入による監査はコスト増に繋がることや、マルチテナントを前提とした場合に他の利用者に影響が出る可能性があることから、金融機関による個別立入監査を受け入れたくないという事情があります。

前章で紹介した有識者検討会報告書においては、委託元金融機関による立入検査等の代わりに、又は、第三者監査の代わりに、その業務の必要とする立入検査等の項目をカバーし、内容が十分に有効と判断できる「第三者認証」のレポートの活用が考えられるとしています（ISMS（ISO27001）、SOC1/2、監査・保証実務委員会実務指針第86号、IT委員会実務指針第7号等）。

特に、検証の実効性を高める方策としては、「SOC2等監査人側の損害賠償責任が契約書上明確化されている監査スキームを活用することが有効と考えられる」とされています。

3. 今後の課題と方向性

今回の安全対策基準の改訂を受け、「金融機関等のシステム監査指針」についても、来年（2016年）の6、7月を目処として改訂が予想されます。

また、昨今の事案を踏まえると、クラウドサービスの利用を含む、より大きなテーマである外部委託管理のあり方に関しても、金融業界全体として、さらに議論を深める方向であると思います。

クラウドサービスの適切な利用を検討するうえでは、今後、これらの動きについても注視していく必要があると考えます。

Ⅳ 監査法人等による保証報告書の枠組み

1. 受託会社に係る内部統制の保証報告書制度の概要

クラウド事業者などの受託会社の内部統制について、監査法人等が行う保証サービスには、財務報告に関連する内部統制を検証するもの（86号、IASE3402、SSAE16の各報告書[2]、以下総称して「SOC1」という）と財務報告に関連しない領域を含む、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関連する内部統制を検証するもの（Trustサービス原則及び規準[3]に基づくIT7号、ISAE3000、AT section 101の各報告書[4]、以下総称して「SOC2」という）など[5]があります（**図表2**を参照）。

従来から86号報告書などの財務報告に係る内部統制の保証報告書は、委託会社及び委託会社の監査人が財務諸表の監査実務のなかで利用されていました。しかし、近年、会計監査の対象となる企業等の業務もASPサービスやクラウドサービスの利用が進み、財務報告に関連しない領域を含む内部統制を対象とする保証報告書のニーズが高まり、日本においてもSOC2と呼ばれる保証サービスが利用されはじめています。

また、金融機関においても、クラウドサービス利用のニーズの高まりもあり、従来Trustサービス原則及び規準に基づく評価に限定していたIT7号の実務指針が見直しされ、規制当局の要求事項や業界団体の自主規制等の遵守に関して、追加された主題情報に対して保証業務を提供できるよう必要な修正が加えられ、2015年7月23日付で改正指針が公開草案として公表されました[6]。

SOC1及びSOC2の報告書は、対象となる内部統制や想定さ

2. 各報告書の略称については、**図表2**を参照。
3. Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy
4. 各報告書の略称については、**図表2**を参照。
5. 受託会社の内部統制に係る保証業務としていわゆるSOC3がありますが、ここでは説明を割愛しています。
6. この他、従前の付録4の「原則及び規準」は、米国SOC2 の2009 年版の規準を参考に作成されていましたが、2014 年版を参考にこの付録4が修正されるとともにプライバシーの原則及び規準が追加されています。

れる利用者が異なり、SOC1の場合は、委託会社とその監査人の利用を想定し、それ以外の第三者には配付されません。これに対して、SOC2の場合は、利用者が幅広く想定されており、委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局が含まれます。よって、SOC2の場合、想定利用者として将来の利用が見込まれるユーザーも含まれるため、これからクラウドサービスの利用を検討しているユーザーも、事前に提供サービスに係る品質管理状況について確認することが容易になることが期待できます。また、規制当局へ何らかの説明が必要となった場合、その報告書を利用することも可能となります。

2. Trustサービスの原則と規準の概要

SOC2報告書では、Trustサービス原則及び規準を利用しますが、その原則及び規準の概要は以下の**図表3、4**に示したとおりになります。Trustサービス原則及び規準は、米国公認会計士協会及びカナダ勅許会計士協会によって共同開発されたもので、2014年に公表したバージョンが最新となっています。なお、7月23日に公表したIT7号の公開草案では、当該バージョンを参照し、付録4として原則及び規準を定めています。

Trustサービス原則には、5つの原則がありますが、モジュラー方式となっているため、クラウド事業者とその委託会社の

図表2　保証報告書別の概要と適用場面

	財務報告に係る内部統制（SOC1）	セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関連する内部統制（SOC2）
概要	ユーザー（委託会社）とその監査人のための詳細な報告書	ユーザー（委託会社）とその監査人及び特定の関係者のための詳細な報告書
適用場面	• 財務報告に関するリスクとクラウド事業者が特定した統制に焦点を当てている。 • クラウド事業者が財務取引業務又は取引処理システムを支援している場合に、最も適している。	以下に焦点を当てており、幅広いシステムに適している。 • セキュリティ • 可用性 • 機密保持 • 処理のインテグリティ • プライバシー
実務上の指針（注）	日本基準：86 号 国際基準：ISAE3402 米国基準：SSAE16	日本基準： IT 7号 国際基準： ISAE3000 米国基準： AT section 101

（注） 日本基準は、日本公認会計士協会の「監査・保証実務委員会実務指針第 86 号」又は「ＩＴ委員会実務指針第７号」となる。
国際基準は、国際会計士連盟（IFAC）の国際保証業務基準（ISAE）を示している。
米国基準は、米国公認会計士協会の米国保証業務基準（SSAE）と専門基準（Professional Standard）を示している。

図表3　Trustサービス原則

領域	Trust サービス原則
セキュリティ	■ システムは（物理、論理双方の）未承認のアクセスに対して保護されている。
可用性	■ システムは、コミット又は合意したとおりに、操作でき、かつ、利用できる。
処理のインテグリティ	■ システム処理は完全、正当、正確、適時かつ権限付与されている。
機密保持	■ 機密として指定された情報が、コミット又は合意したとおりに、保護されている。
プライバシー	■ パーソナル・インフォメーションは、企業のプライバシー通知におけるコミットメント及び一般に公正妥当と認められるプライバシー原則に定められた規準を充足して、収集、利用、保持、開示及び廃棄される。

図表4　Trustサービスの規準構成

可用性に関する追加規準（3）

処理のインテグリティに関する追加規準（6）

機密保持に関する追加規準（6）

プライバシーに関する原則と規準（65）

1.0　管理の規準（14）
2.0　通知の規準（4）
3.0　選択と同意の規準（6）
4.0　収集の規準（6）
5.0　利用、保持及び廃棄の規準（5）
6.0　アクセスの規準（7）
7.0　第三者への開示の規準（6）
8.0　プライバシーのためのセキュリティの規準（8）
9.0　品質の規準（3）
10.0　モニタリングと周知徹底の規準（6）

セキュリティ、可用性、処理のインテグリティ及び機密保持に共通する規準（28）

CC1.0　組織及び管理に関する共通規準（4）
CC2.0　コミュニケーションに関する共通規準（6）
CC3.0　リスク管理及び内部統制の設計と導入に関する共通規準（3）
CC4.0　内部統制のモニタリングに関する共通規準（1）
CC5.0　論理的及び物理的アクセス管理に関する共通規準（8）
CC6.0　システム運用に関する共通規準（2）
CC7.0　変更管理に関する共通規準（4）

（注）表中の（　）は、各規準のカテゴリごとに示される個別の構成要素に定められた規準数（コントロールの例示が示されているもの）を示す。この規準に基づいて、受託会社の内部統制の状況が記述され、その記述が適正に表示されているか、内部統制が重要な点において適切にデザインされ・有効に運用されているかについて、監査法人等が評価を行うことになる。なお、監査法人等の意見表明は、財務諸表監査と同様に、合理的な保証となる。

ニーズにより、当該原則を選択して適用することが可能です。なお、セキュリティの原則は、ユーザーの関心が最も高い領域であり、他のTrustサービスの原則における基礎となります。そして、可用性、処理のインテグリティ及び機密保持に共通する規準として構成されていることから、このセキュリティの原則から開始するのが一番実務的なアプローチです。

プライバシー原則は、プライバシー・プログラムのコントロールの有効性に関する保証として利用することができますが、注意すべき点として、複数のサービスを提供し、地理的に多様なユーザーを持つ組織においてプライバシー規準は複雑な領域と言えます。よって、プライバシーの原則を含むSOC2レポートの作成には、他の規準にもまして、入念な準備が必要です。

V　保証報告書利用に関する委託会社（ユーザー）における留意点

保証報告書は、クラウド事業者が提供するサービスについて、多くのユーザーが存在する場合に、有益なものとなります。つまり、保証報告書の利用者が多ければ多いほど、保証報告書の取得に係るコストに対して、利用者側のメリットが上回るため、クラウドサービスの場合は、保証報告書を利用するケースとして適した状況になると思われます。

利用者側がこれから、クラウドサービスを利用しようと検討する場合には、保証報告書が将来利用できるか否かは、リスク管理の観点からクラウド事業者選定にあたっての1つの判断

図表5　ユーザー側の保証報告書利用にあたっての主要な検討事項

主要なアクティビティ	検討事項
委託先との関係のリスト化	■ 委託している業務の概要（どのようなデータがクラウド事業者に保存されるかの理解も含む）及び委託先が保証報告書を取得している場合、又は、取得を予定している場合はどのような報告書を取得（予定）しているかについてリスト化する。
委託先業務のリスク評価	■ 委託している業務の内容を整理し、当該委託業務に関連するリスクとしてどのようなものが該当するか評価する（財務報告リスク、オペレーショナル・リスクであれば、たとえば、セキュリティ、可用性、機密性など）。
関連するレポートの識別	■ 主要な外部委託先について、リスクの程度に応じて、SOC1又はSOC2報告書のいずれが要求されるか判断する。なお、委託先との契約において監査権があることから、必要に応じて直接監査を行うことで保証報告書を不要とする場合もある。 ■ SOC2報告書の場合は、どの原則（たとえば、セキュリティ、可用性、機密性など）がカバーされるべきか、また、追加の主題（たとえば、FISCが公表する「金融機関等コンピュータシステムの安全対策基準」など）が必要かについて判断する。
契約上の条項等	■ 委託先との契約のなかで、SOC1/2などの保証報告書が要求されているか確認する。 ■ 一定のグループで利用しているサービスの場合、幹事行等と調整し、契約条件について検討を行う。特定行のみのニーズについては、オプションで別途監査等を行うべきか、保証報告書の範囲に含めるべきか検討する。 ■ 選択肢として、単独又は共同で第三者監査人とクラウド事業者に対する監査に関する契約を締結することが適切であるかどうか検討する。
ベンダーのモニタリング	■ 主要な外部委託先を評価する頻度を決定する。 ■ 保証報告書の入手及びレビューのプロセス、懸念される領域をフォローするモニタリングプロセスを構築する。
ベンダーの選定	■ 新規の外部委託先の選定プロセスの一部として、関連する保証報告書の入手を検討する。
ベンダーへの事前確認	■ 保証報告書に関する重要な事項についてクラウド事業者とコミュニケーションを行い確認する。 - 対象としているシステムの範囲 - レポートの種類（SOC1/SOC2など） - 報告書の種別（タイプ1/タイプ2）、基準日及び運用評価期間 - 対象とする内部統制の領域（SOC1の場合は統制目標、SOC2の場合は該当する原則及び規準を含む） - 重要な再受託先の存在（例えばデータセンターなど）及びその再受託先が評価対象に含まれているか。 - 報告書の配布予定日
報告書の利用段階	■ 監査人の評判、能力、独立性に懸念すべき事項はあるか確認する。 ■ 報告書の基準日・運用評価期間等、要求事項と合致していたか確認する。 ■ 報告書の監査人の意見やその他の記載内容（後発事象、対象外としている業務の存在、手続きの内容、相補的内部統制の内容など）を確認し、例外や除外事項等が記載されている場合は、当該事項がリスク評価にどのような影響を与えているか確認し、必要に応じて追加の対応を行う。 ■ 次年度に向けて、委託業務の変更、規制監督官庁の動向も含む環境の変化に応じて、保証報告書の評価対象等の見直しが必要でないか検討する。

（注）委託会社の監査人が利用を予定している場合は、当該監査人からの意見も踏まえることが適切である。

要素となります。また、既存の利用サービスについても、リスクに見合った保証報告書の取得ができなかった部分について、SOC2報告書を追加取得することを検討することも考えらます。このことは、サービス提供を行うクラウド事業者側においても、保証報告書の新規の取得について検討する要因にもなります。

図表5については、委託先が保証報告書の利用を検討するにあたって、主要な検討事項を示しています。既にSOC1等の保証報告書を入手していることからリスクは十分にカバーされていると考えるのは不適切であり、委託している業務に関するリスクに見合った報告書になっているか確認することが必要です。たとえば、財務報告目的としたSOC1レポートでも、セキュリティリスクについてもアクセス権限管理等の観点から評価の対象とすることが多いですが、あくまでも財務報告目的としての観点にとどまり、利用者側の立場から見てニーズを十分満たさないケースが想定されます。また、SOC1報告書では、財務報告目的に含まれない災害復旧やプライバシーのようなトピックスはカバーすることはできません。

委託している業務に関連するリスクを評価するにあたっては、利用しているサービスの内容も理解する必要があります。つまり、利用しているクラウド事業者にどのようなデータが保存されることになるのかなどによって、求めるリスク対応として該当するTrustサービス原則の範囲が異なってくることになります。また、保証報告書には、特定の基準日現在でのデザインを対象とする報告書“タイプ1”と、特定期間を通じてデザインと運用状況の有効性を対象とする報告書“タイプ2”がありますが、タイプ2の場合は6ヵ月以上の運用状況について評価期間が必要であり[7]、新規取得の場合は、それに加えて事前の準備期間が必要となり、クラウド事業者に要望してから実際に入手するまでに相当の期間を要するため、留意が必要です。

Ⅵ おわりに

クラウドサービスの利用増加に伴って、金融機関等では委託業務のリスク管理の重要性が増していくものと思われます。また、クラウド事業者についても、金融機関等の業務の外部委託を受ける立場として、外部監査への対応、リスク管理向上等に資する情報開示及び提供が求められます。このような状況のなか、SOC報告書は、受託業務に関する内部統制についての状況についての詳細な記述が行われ、それに基づいて監査人が手続きを実施することから、金融機関等の委託業務に係るリスク管理策として、有益なものになると考えられます。

本稿に関するご質問等は、以下の担当者までお願いいたします。

有限責任 あずさ監査法人　IT 監査部
TEL: 03-3548-5315（代表番号）

パートナー　小松　博明
hiroaki.komatsu@jp.kpmg.com

シニアマネジャー　仲　友紀
yuki.naka@jp.kpmg.com

7. 初度の報告書を除き、一般的に運用評価期間は1年間とするケースが多い。

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp