# 金融機関におけるクラウド利用に関する
# 有識者検討会報告書

平成 26 年 11 月

公益財団法人 金融情報システムセンター

# 目　次

## はじめに

クラウドコンピューティング（以下「クラウド」という）という言葉は新しいようで古い。平成 18 年に初めてクラウドという言葉が使われて既に８年が経過するが、今やクラウドは多くの IT サービスやソリューションのベースとして存在感を高めている。クラウドには一般的に、資源共同利用のスケールメリットによるコスト削減効果や、短期間でのシステム導入、システム運用負担の軽減といったメリットが認識されている。平成 20 年に米国政府が IT 調達・利用の基本戦略の一環で、データセンターの大幅削減を目的として、パブリッククラウドを最初の選択肢として活用する「クラウドファースト」というコンセプトを打ち出したが、世界中の多くの企業もこうした考え方に追随している。また、日本でもクラウドの利用実績は増えており、特に、東日本大震災の際に安否確認や情報共有のインフラなどで幅広く活用されたこともあって、クラウドの本質的なメリットに関する認識は大いに高まった。その結果、ここ数年、急速に各業界においてクラウドを導入する企業が増えてきている。IT インフラをクラウド等の外部資源を有効に活用して構築することで、システム運用の負担を減らし、戦略的に自社の人的資源を中核業務にシフトさせることは企業にとって自然な流れであるともいえる。

公益財団法人金融情報システムセンター（以下「FISC」という）では、平成 21 年度からクラウドに関する調査を本格化し、金融機関におけるクラウドの利用状況やリスクの整理等を行ってきており、調査レポートを順次発刊してきた[1]。その結果から、金融機関におけるクラウド、特に複数の顧客によってサービスを共有する「パブリッククラウド」の利用については、総じて慎重な姿勢がうかがわれる。主な理由としては、顧客情報のデータ保護など情報セキュリティに対する不安、サービスの信頼性、法律・規制に対する懸念などが挙げられる。FISC が平成 26 年度に行ったアンケート調査『金融機関等のシステムに関する動向及び安全対策実施状況調査』をもとに集計した結果（資料編「【図表Ａ】クラウドの利用状況」）において、パブリッククラウドを実際に利用している、もしくは利用を予定・検討している金融機関は全体の 16%となっている。業態別にみると、大手行や保険会社等での利用が進んでいる一方で、中小金融機関での利用率は低い状況にある[2]。

こうした中、金融機関においてクラウドの利用は全体的に増加傾向にある。資料編【図表Ａ】に、クラウド全体での利用率（利用予定・検討中を含む）の推移を記載しており、

[1] 調査活動の成果として、平成 21 年度に報告書「クラウドコンピューティングの課題と展望」、平成 23 年度に調査レポート「今次震災からの復旧におけるインターネット、クラウドサービス利用に関するノート」及び報告書「金融機関におけるクラウドコンピューティングのセキュリティ確保と外部委託管理」、平成 25 年度に調査レポート「金融機関のクラウド利用者に関する規制監督動向及び課題について」を発刊している。

[2] 資料編「【図表Ｂ】FISC によるヒアリング結果」参照。なお、クラウドの利用が進まない点に関しても、ヒアリングを行ったが、結果として個人情報の取扱い等の一般的な課題と、クラウド事業者に対する統制、監査・検査、利用終了時のデータの取扱い等の金融機関に特徴的な課題が認識されている。

平成 22 年度の利用率は 20%程度にとどまっていたが、平成 25 年度には 37%にまで増加していることがうかがわれる。また、このうちパブリッククラウドの利用事例についても同様に増えてきており、情報系システム（営業支援システムや電子メール、社内情報共有、e ラーニングシステム等）を中心に多くの領域での利用がみられる。FISC で別途ヒアリングした結果では、実際には、顧客管理や取引先管理など、顧客情報を扱う業務での利用事例も多くみられるようになってきた（資料編「【図表Ｃ】パブリッククラウドの利用事例」参照）[3]。

クラウドの技術やサービスは日々進化しており、今後、金融サービスの高度化、競争力強化を図る観点から、クラウドを積極的に活用する金融機関がさらに増えていく可能性はある。わが国金融業界において、クラウドの利用を健全に促進させ、より一層広げていくためには、金融機関やクラウド事業者をはじめとする関係者間で改めてクラウド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・契約管理の在り方等について幅広く議論し、共通の認識と理解を持つことが必要と思われる[4]。

今回、こうした問題意識のもと、FISC 理事長からの諮問により「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「本検討会」という）を開設した。本検討会では、学識経験者や金融機関、クラウド事業者等の委員と官庁等のオブザーバーが参加し、「わが国の金融機関が、クラウド技術の特性とリスクを正しく把握したうえで、リスクを適切に管理し、クラウド技術の持つポテンシャルを最大限に活用していくためにはどうしたらよいか。また、そのような試みをサポートする安全対策の在り方について、どのようなものが相応しいか」について議論を行い、本報告書を取りまとめた。

[3] パブリッククラウドを利用した効果として、資料編【図表Ｃ】のとおり、一般的なクラウドのメリットであるコスト削減やシステムの早期導入、利便性・機能向上のほか、懸案とみられていたセキュリティを強化する事例もみられた。

[4] FISC では平成 25 年３月に『金融機関等コンピュータシステムの安全対策基準・解説書』（以下『FISC 安全対策基準』という）の改訂（第８版追補）を行い、クラウドサービス利用に係る基準として【運 108】を新設した（資料編「【図表Ｄ】『FISC 安全対策基準』（第８版追補）におけるクラウドサービスの取扱い」）。ただし、本改訂に関しては、「クラウドサービスは日々進化しており、コスト削減や短期間での導入等のメリットがある反面、重要業務への利用やクラウド特有のリスクも想定されることから、今回の改訂は、顕在化している課題・問題点に対する当面の暫定的な対応であり、最終形ではない」とし、継続検討の扱いとした。

# Ⅰ　クラウドの特性

## １．クラウドの定義

クラウドについては、さまざまな定義や見方があるが、本検討会においては、以下に示す米国の NIST（National Institute of Standards and Technology ： 国立標準技術研究所）におけるクラウドの定義（〔図表１〕）[5]を採用することとした。

**〔図表１〕NIST におけるクラウドの定義**

| |
|---|
| クラウドとは、最小限の管理負荷やプロバイダー交渉だけで、迅速に提供され稼働する構成変更自在のコンピュータ資源（ネットワーク、サーバー、記憶装置、サービス等）の共有プールに対する、ネットワークを通じた便利で随時のアクセスを可能とするモデル |

（出所）NIST「SP 800-145, The NIST Definition of Cloud Computing」を FISC にて要約

NIST ではクラウドについて、①単一の組織専用に提供される「プライベートクラウド」や、②多数の利用者で共用する「パブリッククラウド」、③特定の複数組織間で共用する「コミュニティクラウド」などの分類を行っているが、本検討会では、このうち、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」を対象として検討を行った[6]。

また、パブリッククラウドは、実質的には業務を営むために必要な情報処理の事務、すなわち「システムの運用・保守」や「開発」、またはその一部をクラウド事業者に委託している関係にあるとみなすことが自然である。このため、本検討会では、諸外国の金融監督当局等での取扱いと同様に、「外部委託」の一形態として扱うことが適当であるとした[7]。金融機関は顧客や決済システムに対する最終的な責任を負っているため、金融機関に対してサービスの提供を行っているクラウド事業者が何らかのトラブルを生じさせ、結果として顧客等に悪影響を及ぼした場合においても、その責任は免れないと考えられる[8]。

---

[5] The NIST Definition of Cloud Computing (Special Publication 800-145)を参照。
（http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf）

[6] パブリッククラウド以外については、資源の利用者の範囲が個別、または金融機関に限定的である、などの特徴から、既存の外部委託管理の枠組みをそのまま適用できる部分も多く、また本検討会の成果を応用できるとし、本検討会では、原則検討の対象外とした。

[7] 金融庁の監督指針における外部委託の定義（資料編「【図表Ｅ】金融庁監督指針における外部委託の定義」）にも、「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。）」とある。

[8] 「パブリッククラウドについては、「外部委託」ではなく「利用」という形態もあり、外部委託とは異なるリスク管理の考え方があり得るのではないか」との意見もあった。金融機関が業務においてクラウドサービスを用いる場合でも、金融機関は業務全体に対する責任を負っており、クラウドサービスの実態把握など、相応のリスク管理が求められる。

## ２．クラウドのメリットとリスク

金融機関はクラウドの利用を検討するにあたって、そのメリット及びリスクを十分に理解することが重要である。

### (1)メリット

クラウドのメリットには〔図表２〕のような例が考えられる。コスト削減やシステム運用負担の軽減に加え、拡張性や柔軟性、業務継続性が高いなどさまざまなメリットが存在している。

**〔図表２〕クラウドのメリット（例）**

| | |
|---|---|
| コスト削減 | 資源共有型スキームで規模の経済が働くスケールメリットによってシステムのコスト削減が見込まれる。 |
| 納期･システム開発期間の短縮 | ユーザーがITインフラを自前で調達・構築するプロセスと比べて、リソースの導入・構築に係る手間が大幅に減少するため、サービスインまでの納期やシステム開発期間を短縮できる。 |
| システム運用負担の軽減 | システムメンテナンス等の運用を事業者に任せることによってユーザーの運用負担を軽減できる。 |
| 拡張性・柔軟性 | スモールスタートや一時的な使用、即時撤退などが可能となり、機会損失の抑制や先行者利得の確保に寄与する可能性がある。 |
| オンデマンドセルフサービス | ユーザー自身でサーバー等の利用や停止をコントロールできるため、無駄な資源利用を排除できる。 |
| 利便性や機能の向上 | 新技術の導入スピードが速いため、ユーザーの利便性や機能向上の効果が大きい。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）等との親和性が高く、社内外環境とのデータ交換や情報共有も容易にできる。 |
| 業務継続性 | 隔地に分散する複数の資源の利用が前提となっているサービスの場合、拠点被災等に対する業務継続性が高い。 |

### (2)リスク

クラウドは、資源共有型スキームであること、サービス内容によっては関与する事業者が複数となり契約・責任関係が複雑となることなどから、リスク管理面で特有の要素を考慮する必要がある。このリスク管理面で考慮する必要がある主なリスクの例を〔図表３〕に示した（詳細は、資料編「【図表Ｆ】金融機関のクラウド利用において考慮すべきリスク」に整理)。

〔図表３〕クラウドのリスク（例）

| リスク | 分類(注) | 内容 |
|---|---|---|
| 法制度の違いによる影響 | 法制度<br>③ | プライバシー保護等の要請が国（法域）によって異なることに伴い、トラブルが生じた場合の対応や個人データの移転に支障が生ずる可能性がある。 |
| 情報漏洩リスク | 技術<br>⑦ | サービス終了時にハードウェアの物理的な破壊・消磁を通じたデータの完全消去が困難なため、残存したデータが漏洩するリスクがある。 |
| | 技術<br>⑧ | オンプレミスの環境と異なり、ネットワークでのデータ伝送をベースとした仕組みであるため、データ伝送中のデータが漏洩するリスクがその分大きい。 |
| リアルタイム性、可用性への懸念 | 運用<br>⑪ | 他ユーザーのトラフィックが高まった場合、自ユーザー分の処理に係るリソースが不足することにより、レスポンスの悪化やシステムの停止につながる可能性があり、求められるサービスレベルが保証されない懸念がある。 |
| インシデント対応の不十分性 | ガバナンス<br>⑱ | クラウド事業者は、コスト節約や機動的なサービス開始を重視するため、標準化されたものより踏み込んだユーザーサポートを行うことに消極的な場合がある。この結果、ユーザーによるリスク管理上必要な情報の開示やインシデント対応が十分に行われない可能性がある。 |

（注）「分類」欄の番号は「資料編【図表Ｆ】金融機関のクラウド利用において考慮すべきリスク」中の項番に対応。

ただし、クラウドのサービス形態によっては、必ずしも資料編【図表Ｆ】に記載したような事項がすべて該当するものではなく、リスクの度合いも異なる。実際にクラウドを利用する際には、サービス内容を精査し、資料編【図表Ｆ】に列挙したリスクの有無や大きさを評価する必要がある。

また、クラウドの技術は日々進化しており、リスクが低減される可能性がある一方で新たなリスクが出現することも考えられる。今後、現時点で認識されていない技術に係る未知の脆弱性や、新たな脅威、規制や法制度といった外部環境の変化なども十分に念頭に置きつつ、クラウドに係るリスク評価を適時適切に見直していくことが望まれる。

## Ⅱ　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による経営判断～

前述のとおり、クラウドにはさまざまなメリットがあり、金融機関はクラウドの利用を通じてコスト節減や環境変化に合わせた迅速なシステム導入が可能になると考えられる。もっとも、システム障害やクラウド事業者の経営破綻などによるサービスの停止、クラウド環境からの顧客情報の漏洩等のリスクが顕在化した場合には、多数の顧客や金融機関自身に多大な影響を及ぼしうる。このため、金融機関としては、クラウドの特性を考慮した適切なリスク管理を行う必要がある。以下では、クラウドに係るリスク管理の基本的な考え方を示す。

### １．クラウドの利用・リスク管理に係るポリシー等の策定

金融機関はクラウドの利用にあたって、経営陣、システム部門、ユーザー部門（事業部門等）、システムリスク管理部門等の関係者がクラウドのメリットやリスクを理解・認識したうえで、経営陣の関与のもと、基本的な利用方針やリスク管理に係る方針を策定することが重要である。

そのために、まず、クラウド利用の目的やクラウドに移行する業務・システムの範囲を定める必要がある。特に、クラウドの利用を検討する金融機関は、例えば、①自社のIT 戦略等に基づきどのような業務・システムをクラウドにより実現していくか、②特定のクラウド事業者やクラウドサービスにどの程度依存・集中させてよいか、③残存するリスクをどの程度まで許容していくかなど社内で十分に検討し、クラウドに係るリスクアペタイト（選好度）等をあらかじめ決めておくことが望まれる。

さらに、クラウド導入に関する全社的な意思決定プロセスを明確に策定し、それを社内に浸透させることが重要である。例えば、システム部門やシステムリスク管理部門が関与・把握していないところで、事業部門などユーザー部門がクラウドを導入し、いつのまにか社外に重要なデータが保存されているといった事態は避けるべきである。

また、クラウドのリスク管理に係る方針等について、クラウドは「外部委託」としての形態を有しているため、既存の外部委託管理に係る方針や基準も勘案して策定することが望まれる。リスク管理態勢については、定期的にリスク管理策の実効性を検証し、必要に応じて見直していくことが重要である。

## ２．リスクベースアプローチの適用

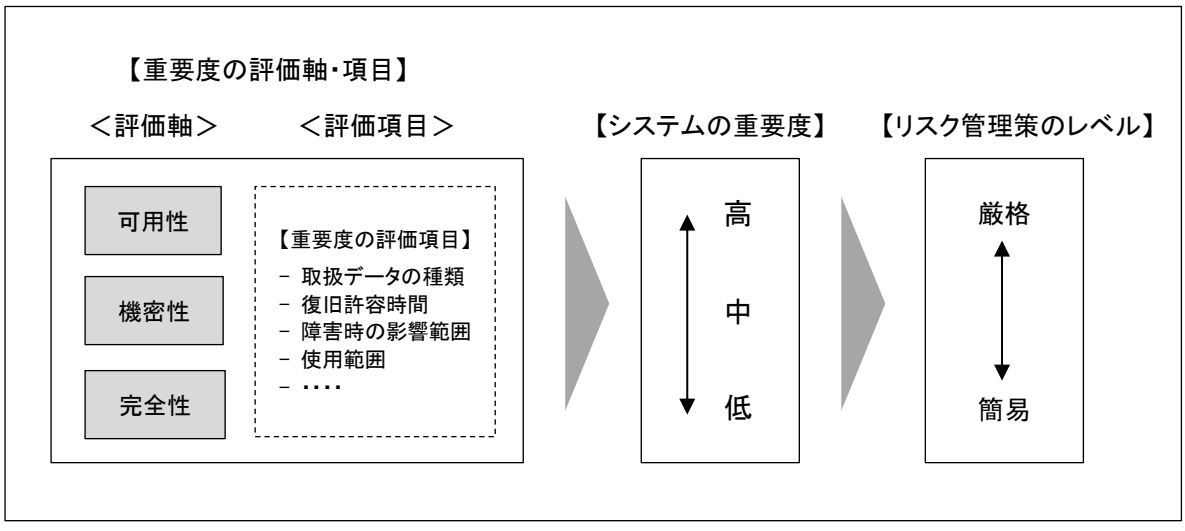
### (1) リスクベースアプローチの考え方

本報告書では、「リスクベースアプローチ」を以下のように捉える。

まず、クラウド利用の対象となる業務（システム処理を含む）について、システムの可用性とデータの機密性などの切り口[9]をもとに、その特性や重要度を分析・把握する。そのうえで、重要度の高い業務についてクラウドを利用してシステム化する場合は、相応に厳格なリスク管理を実施することが求められるが、他方で相対的に重要度が低い業務においてクラウドを利用する場合は、その業務の特性や重要度に応じて簡易なリスク管理でもよいとするといった判断が可能となる。金融機関においてはこうした「リスクベースアプローチ」を適用し、経営判断のもと適切なリスク管理策を策定することが重要である。〔図表４〕にこれらのリスクベースアプローチの考え方を図式化した。

可用性や機密性などの評価軸で直接その業務やシステムの重要度を判断する場合もあるが、金融機関によっては独自の評価項目（取り扱うデータの種類、復旧許容時間、障害時の影響範囲等）でその重要度を評価し、結果的に可用性、機密性などの評価軸における重要度評価と同様の判断をするケースもある。こうした重要度を評価する軸や項目については、各金融機関のリスク管理方針等に基づき策定する必要がある。

〔図表４〕リスクベースアプローチのイメージ




[9] 業務の重要度や特性を評価する切り口として、可用性や機密性のほかにデータの完全性（データの改ざん・喪失が生じないこと）等もある。多数の切り口で重要度を総合的に判断することも考えられるが、スキームは複雑になるため、本章の具体例では議論を単純化する目的で２つの切り口で記述した。

### (2)具体例

#### ①リスク管理策設定の考え方

リスクベースアプローチにより、システムの重要度に応じてリスク管理策のレベルをどのように設定していくか、具体例を〔図表５〕に示した。

この例では、リスク管理策の設定にあたって、システムに求められる可用性と機密性の２つの軸をもとにシステムの重要性を評価し、その重要性をもとにリスク管理策を策定するリスク管理項目と、可用性または機密性のいずれか１つの軸でシステムの重要性を判定し、その重要性をもとにリスク管理策を策定するリスク管理項目の２種類を想定している。

**〔図表５〕リスクベースアプローチによるリスク管理策の設定（例）**

複数の軸（可用性・機密性）の総合的評価に基づくリスク管理策（例①）

| システムの重要度 | | リスク管理策（例：監査等）のレベル |
|---|---|---|
| 可用性・機密性の総合的評価 | 高（コア IT 領域） | 金融機関主導の監査等が必要 |
| | 中（セミコア IT 領域） | 部分的に金融機関主導の監査等が必要 |
| | 低（ノンコア IT 領域） | クラウド事業者主導の監査等で可 |

１つの軸の評価に基づくリスク管理策（例②）

| システムの重要度 | | リスク管理策（例：可用性は SLA、機密性はデータ消去）のレベル |
|---|---|---|
| 可用性 | 高 | 自社の求める稼働率・サービスレベルに応じた SLA が必要 |
| | 低 | クラウド事業者提示の標準的約款に基づき契約 |
| 機密性 | 高 | 契約終了時には、復元不可能な物理的消去・論理的消去[10]が必要 |
| | 低 | データ消去は必須ではない |

a．総合的評価の例

〔図表５〕の「例①」は、可用性と機密性の２つの軸を組み合わせてシステムの重要度を総合的に評価したうえで、その重要度のレベルに応じリスク管理策の範囲・深度を変えていくリスク管理項目の例である。この例では、重要度を３段階（高・中・低）に分類したうえで、その分類に基づいて「監査等」（委託元金融機関による立入監査・モニタリング、第三者監査）に係るレベルを設定している。

[10] 「論理的消去」については、「Ⅲ 1.(4) 〔図表 16〕一定条件を満たしたデータの論理的消去」を参照。

b．個別評価の例

「例②」では、総合的な評価ではなく、可用性または機密性のいずれか１つの軸に基づいてシステムの重要度のレベル（ここでは、高・低の２段階）を評価し、リスク管理策の範囲・深度を変えるリスク管理項目の例を挙げている。リスク管理項目として、可用性の軸では「SLA」を、機密性の軸では「データ消去」を例としている。

前者の「総合的評価」におけるシステムの重要度レベルに関し、その理念系（マトリックス）を資料編「【図表Ｇ】重要度からみたシステム／データ分類例」に示した。一般的に、システムの可用性及びデータの機密性の両方が高い「コア IT 領域」では、重要度が最も高く、厳格なリスク管理を要する。他方、「ノンコア IT 領域」は重要度が低い領域で、簡易なリスク管理でも十分とする考え方をとりうる。「セミコア IT 領域」は両者の中間の領域という位置づけになると考えられる。こうした、「コア IT 領域」、「セミコア IT 領域」及び「ノンコア IT 領域」の区分については、画一的なものではなく、ここでは、金融機関が各々の業務特性やリスク管理のポリシー等に基づき、システムの重要度評価やリスク管理の判断をする際の参考として位置づけられるものである。したがって、金融機関の判断で、さらに細かく領域を設定することも考えられる。また、各領域に対応するリスク管理策のレベルも一律で決まるものではなく、金融機関の判断に基づき決めていくことになる。

リスク管理策の例として、上記では、監査等（例①）や SLA・データ消去（例②）を取り上げたが、その他も含めリスク管理策の設定方法の例を一覧にしたものを、資料編「【図表Ｈ】リスク管理策の一覧（例）」に示した。この表において、「基準」の欄に「総合判断」と示されているリスク管理項目は、上記ａに示した総合的評価をもとにリスク管理策を設定する項目としている。また、「基準」の欄に「機密性」、「可用性」と記載のあるリスク管理項目は、上記ｂに示した、個別評価をもとにリスク管理策を設定する項目としている。

**②可用性・機密性の考え方**

高い可用性が求められるシステム（可用性の高いシステム）については、勘定系システムや資金決済に使うシステムなど、顧客や対外取引に影響のあるシステムが想定される。

また、高い機密性が求められるデータ（機密性の高いデータ）は、社外への漏洩により経営に大きな影響を及ぼす可能性がある情報や営業秘密で法的に厳格な管理が求められる情報などが考えられる（具体的な例は資料編「【図表Ⅰ】機密性の高いデータ（例）」を参照）。この「機密性の高いデータ」を扱うシステムについては、リスクベースアプローチの考え方のもと、求められるリスク管理のレベルに幅を持たせることが可能にな

る。個人情報を含むシステムでは、機密性は高くなるが、データの特性・ボリュームや取り扱われる環境、漏洩した際に想定される影響度などが区々であるため、すべてに画一的なリスク管理を求めないという考え方も可能となる。

例えば、会議室予約システム等の場合、機密情報である顧客の氏名が予定として載る可能性がある。しかし、データが断片的であり、情報漏洩の場合のインパクトに鑑み、そのシステムに対してトータルに厳格なリスク管理を求めないという判断もあり得る。

また、電子メールシステムについては、同様に氏名情報が載ることになるが、これらのデータはアドレス帳としてデータベース化されており、また、メール上にもさまざまな個人情報などの重要情報が含まれる可能性があることからトータルで厳格なリスク管理が必要であるとする判断には妥当性がある。ただし、この場合においても、ユーザーである金融機関において、メール本文や添付ファイルにインサイダー情報やクレジットカード情報などの機密性が極めて高い情報を一切記載しないというルールを導入し適切に管理を実施しているケースにおいては、そのリスク管理の多くを金融機関側で行っているという観点から、クラウド事業者の提供するシステムに求める管理レベルを緩和することも可能になる。当然ながら、こうした電子メールシステムに求められるリスク管理の多くを、クラウド事業者側に委ね、例えば、後述する暗号化等の技術をベースにしたリスク管理策をクラウド事業者側で講じ、その妥当性を金融機関として検証するといったことが考えられる。

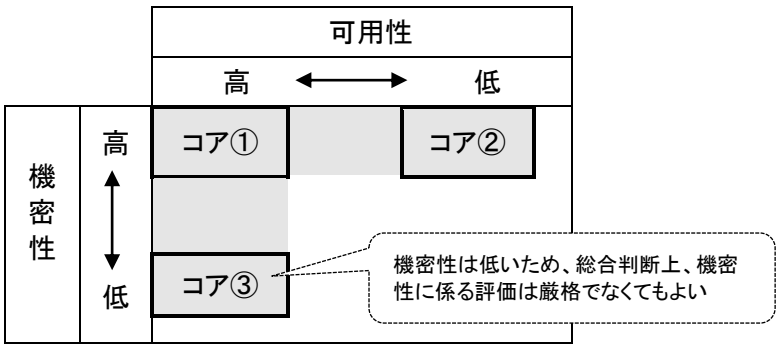
このようにデータそのものに係るリスクやユーザー金融機関側の内部管理、サービスを提供するクラウド事業者側で講じる施策を総合的に勘案したうえでリスク管理のレベルを検討することが重要である。

**③留意点**

前述のとおり、資料編【図表G】においてシステムの重要度レベルの例、すなわち可用性と機密性の２つの軸で重要度を判断した３つの領域（コア IT 領域、セミコア IT 領域、ノンコア IT 領域）を示した。一般的に各領域の間でリスク管理レベルが異なることは既に言及したが、そのほか、同じ領域内においても求められるリスク管理レベルが一律に決まるわけではないことに留意する必要がある。

例えば、〔図表６〕は、資料編【図表G】を単純化したもので、シャドーを掛けた部分はおおむね「コア IT 領域」と位置づけられる。コア IT 領域の中でも、「コア①」の部分は可用性・機密性とも高いリスク管理が求められる領域、「コア②」の部分は機密性のみ高いリスク管理を求められる領域（可用性は比較的低い）、「コア③」の部分は可用性のみ高いリスク管理を求められる領域（機密性は比較的低い）と位置づけて整理することができる。

〔図表６〕「コア IT 領域」内でのリスク管理レベルの差異




リスク管理項目ごとに求められる管理レベルは個別に評価すべきである。例えば、〔図表６〕の「コア③」に定義されるシステムについてはコア IT 領域として定義されるが、資料編【図表H】にあるリスク管理項目のうち、可用性、機密性の総合判断をすべき項目のすべてについて一律に最も厳格な管理（図表では最も左に位置するもの）を求めるものではない。例えば、資料編【図表H】のうち利用検討時における事業者選定においては、機密性に係る評価項目について詳細な情報開示を求める必要性はさほど高くないものと考えられる。

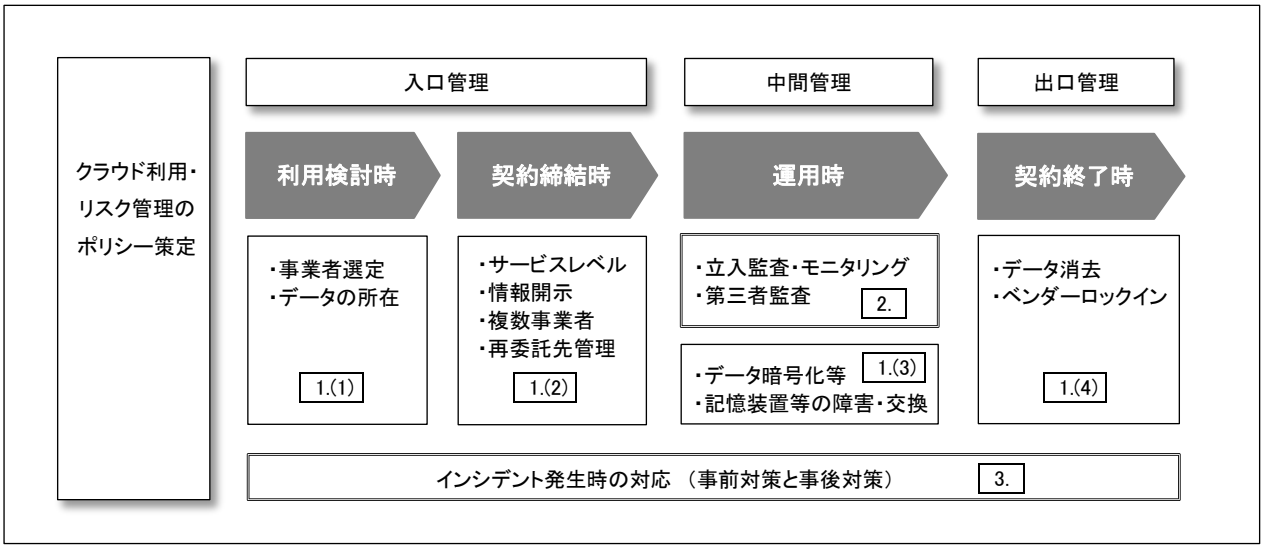
なお、資料編【図表G】と資料編【図表H】はあくまでもリスクベースアプローチによってリスク管理の簡易化をできる範囲をどのような基準で設定していくかの方法を例示したものである。金融機関においては、これらの資料などを参考にリスク管理策を検討していくことが望まれる。

## Ⅲ　具体的なリスク管理策

本章では、①クラウド事業者の選定やそのシステム・データに関する実態把握などのリスク管理策、②契約やSLA等に照らしてクラウド事業者側における管理・運用が実効的に行われているかの検証（クラウド事業者に対する監査等）、及び③インシデントが発生した場合の対応、の３つの観点からリスク管理策についてまとめた。

なお、各リスク管理策において「a. 管理策」の箇所は、重要度が非常に高い業務処理（例：高い可用性や機密性が求められる業務）をパブリッククラウドの利用により実現する場合において必要とされる厳格で高水準のリスク管理の適用例を示している。また、「b. 簡易なリスク管理」の箇所ではシステムや業務の重要度に応じてリスク管理を簡易化していく考え方を記載している[11]。

〔図表７〕リスク管理策の全体像




## １．リスク管理策

クラウドを利用する場合、システムやデータが社外環境に置かれ、利用者側からみると自社構築システムよりも直接把握できる範囲や深度が狭まり、内部統制が及びにくくなる傾向がある。そのため、金融機関としては、特に重要な業務でクラウドを利用する場合、クラウド事業者の業務遂行能力・リスク管理態勢や、提供されるサービスの内容・水準、データの所在など、さまざまな観点からクラウドの実態把握を行い、できるだけブラックボックスの部分が残らないようにすることが重要である。

[11] なお、資料編【図表Ｇ】で例示した「コアIT領域」に対するリスク管理策は、「a. 管理策」におおむね対応し、「セミコアIT領域」や「ノンコアIT領域」に対するリスク管理策は、「b. 簡易なリスク管理」に対応すると考えられる。

以下では、(1)クラウド利用検討時、(2)クラウドサービス契約締結時、(3)クラウドサービス運用時、及び(4)クラウドサービス契約終了時の各フェーズに応じたリスク管理策について詳述する。

### (1)クラウド利用検討時

#### ①事業者選定（クラウド事業者に対するデューデリジェンス）

パブリッククラウドのサービスは、「複数利用者で機能を共通化することでコストメリットを享受する」という資源共有型のサービスであり、導入前に金融機関が期待した機能やサービス水準が実際とは異なっていた場合に、事後的に変更を行うことは相当困難である。そのため、クラウドサービスの導入を検討する場合には細心の注意を払って、事前のデューデリジェンスを実施することが重要である。

a. 管理策

クラウドを利用する業務に求められる可用性・機密性等の観点及び自社の経営の視点から、リスクを分析・認識し、当該業務に求められるリスク管理レベルを検討のうえ、その実現が可能なクラウド事業者を選定する。その際、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デューデリジェンスを行うことが必要である（〔図表８〕）[12]。

クラウド事業者によっては契約前の情報開示に消極的なケースもあるが、必要に応じ機密保持契約を事前に締結したうえで開示を求めることも考慮すべきである。

また、クラウドは比較的新しい技術であるがゆえに、業歴に基づいた信頼ある情報やデータを取得しにくい面があるが、サービスに対する評判や実績等も踏まえ多面的に評価することが重要である。

[12] 資源共有型であるパブリッククラウドの場合、クラウド事業者によっては、標準的な契約・SLA 等の内容に関し個社からの変更要求に応じないことも想定される。金融機関としては、特に重要な項目について、こうした変更要求の交渉が可能であるかを事前に確認しておくことが重要である。

〔図表８〕デューデリジェンス時の重要な評価項目（例）

| |
|---|
| １．クラウド利用を想定する業務に係る実績、技術力[13] |
| ２．事業継続性（経営体力・収益力、人的基盤、経営者の資質・ビジネス戦略、被災時のBCM・データのバックアップ） |
| ３．サービスの可用性・データの安全性（機密性保護）・完全性 |
| ４．クラウド事業者内の内部統制やリスク管理等に関する状況（再委託先管理も含む）、外部監査の受検や各種認証の取得状況 |
| ５．情報開示姿勢 |
| ６．立入監査の受入に関する方針 |
| ７．データの所在（データが保管される場所、または保管の可能性がある場所） |
| ８．既存システムとの連携・新システムへのデータ移行等の容易性 |
| ９．サポート体制（サポートデスク、障害発生時の対応＜トレーサビリティの確保等＞） |
| 10．インシデントが発生した場合の想定損害額（直接損害・間接損害）とクラウド事業者側が提示する損害賠償・補償上限額とのバランス |
| 11．利用廃止時の対応（ベンダーロックインリスク対応、データ消去等） |
| 12．個人データの取扱いの全部又は一部をクラウド事業者に行わせることを内容とする契約を締結する場合は「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」のⅢに定める「個人データ保護に関する委託先選定の基準」（資料編【図表 J】参照）に準拠対応可能か |

（注）上記の評価項目については、「Ⅲ 具体的なリスク管理策」で記載している内容や条件を十分に勘案したうえで検証することが必要である。

b．簡易なリスク管理

クラウドを利用する業務の重要度が必ずしも高くない場合は、クラウド事業者の公開情報や、業界における評判や実績等による客観的な評価にとどめることも考えられる。

### ②データの所在

クラウド事業者によっては世界中に存在する複数のデータセンターに跨って業務・データの管理を行うケースがある。クラウド事業者のポリシーによりデータセンターの所在地の開示に消極的な場合もあるが、金融機関として、紛争が生じた際にどの国の法律が適用されるのか、また、現地の公権力による捜査目的で、データ等が差し押さえられるといった場合に業務の継続性に影響がないかといった点には十分に配慮する必要がある。特に、重要業務を委ねる場合には、データの所在を把握することがより重要になる。

[13] 技術力については、金融機関が委託をする業務に関する専門性や、クラウド事業者が安定して業務に係る開発・運用をしているか等の評価項目がある。

a．管理策

(a)平常時

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、委託元金融機関は、現地の公権力によるデータ閲覧や提出命令等に対応する必要が発生する可能性も鑑み、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。データが分散格納されている場合においても、同様の趣旨から、どの国や地域に格納される可能性があるのかといった情報を把握する必要がある[14]。

(b)インシデント発生時・立入監査時

情報漏洩等のインシデント発生時において、データセンター等への立入が必要となる場面では、必然的に具体的な所在地の把握が必要となる。なお、必要に応じて委託元金融機関による立入監査を実際に行う場合も同様である。

(c)海外でのデータ保管時

海外でデータを保管する場合、〔図表９〕のとおり、立入調査におけるコストやコミュニケーション方法について留意する必要がある。

**〔図表９〕海外でのデータ保管時の留意点**

| | |
|---|---|
| データセンターへの立入監査の時間・コスト | 往査に時間を要したり、人的コストが高くなったりすることもある。このため、現地の監査法人に監査を委託する等の対応が多くなる可能性がある。 |
| 障害対応時のコミュニケーション方法 | 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、クラウド事業者の日本法人等の障害対応窓口設置を契約上で明確にする必要がある。 |

b．簡易なリスク管理

クラウドを利用する業務の特性や重要度に応じて、データ所在の把握の必要性や詳細度に差異が生じることはあり得る。リスクプロファイルの観点から、重要と位置づけられない業務を委ねる場合には、データ所在に関する情報はさほど重要ではないと考えられる。

[14] 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ミッションクリティカルな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ことが必要である。

### (2)クラウドサービス契約締結時

#### ①サービスレベルの合意

クラウド事業者との契約の中には SLA[15]が含まれるのが通例であるが、多くの標準的な SLA では、基準となる月間稼働率などを定めたうえで、実際の稼働率が基準を下回った場合にサービスの利用料を減額するといった内容にとどまっている。そのため、例えば、勘定系システムのオンライン処理など高い稼働率が求められる場合では、こうした標準的な SLA による契約締結では不十分な可能性がある。

クラウド事業者の顧客は金融機関をはじめ、さまざまな業種にわたる。その中で各顧客企業との間で個別の内容の契約を準備するのは効率的ではないとの考えから、クラウド事業者は SLA を個別に締結することに対し消極的な場合もある。一方で、金融機関が特に重要な業務を委託する場合においては、その社会的な重要性に鑑み、相応の高いサービスレベルが求められる。金融機関としては、必要とされるサービスレベルとリスク管理を十分に確保する観点から、クラウド事業者との契約や SLA、SLO[16]の中身を検証し、クラウドを利用する業務のプロファイルに応じて、内容を追加することが必要となることもある。

a. 管理策

契約書[17]、または必要に応じて締結する SLA・SLO には、〔図表 10〕のような事項を盛り込むことが望ましい。当然ながら各金融機関の業務のプロファイルに応じて、〔図表 10〕の例にとどまらず項目や内容を追加、変更していくことも考慮すべきである。

---

[15] Service Level Agreement の略。サービス事業者とサービス委託者である金融機関との間で合意される、提供するサービスの内容と範囲、品質に対する要求（達成）水準（基準値または最低保証値）あるいはそれを明文化した文書、契約書のこと。未達の場合、債務の不完全履行または債務不履行となり賠償責任の対象となり得る。

[16] Service Level Objective の略。サービス事業者がサービスの品質についての目標を定めたもの。提供するサービスやサービスを構成するシステムや機材などに関して、性能や可用性、データ管理、運用体制、サポート体制、セキュリティなどの目標水準や目標値を設定し、利用者に提示する。目標値に対し未達の場合、契約書や SLA のように即時的な賠償責任は発生しないが、目標水準や目標値達成に向けての改善義務、努力義務が生じる。こうした義務を適切に果たさない場合には、不完全履行、債務不履行として賠償請求の対象となり得る。

[17] 主契約に付帯する添付別紙や付帯書類を含む。

〔図表 10〕契約・SLA・SLO に盛り込むべき事項（例）

| | |
|---|---|
| 1 | 契約一般条項（用語の定義、役割分担、責任範囲、債務不履行時の損害賠償範囲、準拠法、裁判管轄等） |
| 2 | 個別契約条件（サービス内容、料金、期間等）、サービス仕様（リソースの割当て等＜仕様上の制限や変更に必要な時間等＞）、データ保護の管理策（データ暗号化等） |
| 3 | サービスレベル項目 |
| | ①システム運用：可用性[18]、信頼性、性能、拡張性 |
| | ②サポート：障害対応、問合せ対応 |
| | ③データ管理：利用者データの保証についての言及 |
| | ④統制環境：再委託先（再々以下の階層の先を含む）管理<br>機密保護・良好な統制環境の維持義務 |
| 4 | サービスレベル未達の場合の対応 |
| 5 | 情報開示範囲、監督当局等による検査等への協力義務、金融機関による監査受入、事業者と利用者間の報告・連絡等の運営ルール、インシデントレスポンスの取扱い |
| 6 | 反社会的勢力・テロ組織と関わりがないことの表明保証 |
| 7 | 利用終了時の原状復帰・新システム移行時の協力義務、データの返却・消去等 |
| 8 | 損害賠償や補償 |
| 9 | クラウド事業者のリソース上のアプリケーションを利用する過程で生成された成果物の知的財産権の帰属（または帰属割合） |
| （注）上記事項については、「Ⅲ 具体的なリスク管理策」で記載している内容や条件を十分に勘案したうえで、契約・SLA・SLO に盛り込む必要がある。 | |

b. 簡易なリスク管理

〔図表 10〕は、重要度の高い業務をクラウド事業者に委託する場合においてカバーすべき項目の一例である。委託する業務の重要度やリスク特性に応じて、各項目の内容や基準値が異なるほか、項目自体の必要性も変わり得る。例えば、重要でない業務を委託する場合は、必ずしも上記項目のすべてを必要とせず、クラウド事業者が金融機関以外に一般的に提示する標準的な SLA のみで締結を行うことも考えられる。あるいは一般的な標準契約の締結のみを行い、SLA 自体の締結を必要としないといった考え方もあり得る。

[18] 可用性の評価にあたって、①障害等に伴うシステムの停止時間のほか、②システムの更新・保守（緊急的なセキュリティパッチ対応を含む）や新サービスの追加などシステムの品質・セキュリティ向上のための計画停止時間も考慮する必要がある。なお、後者の点に関して、グローバルベースでサービスが提供されるパブリッククラウドでは、緊急的なセキュリティ対策等に係る計画停止作業について、ユーザー全体の安定性を優先するため、必ずしも個々のユーザーの要望（作業のタイミングや時間等）に沿わない形で実施される可能性があることにも留意する必要がある。このため、こうしたクラウド事業者の計画停止や緊急的なセキュリティ対策に関する方針・基準について確認することが重要である。

### ②クラウド事業者からの情報開示

金融機関はその業務の特性上、社会的責任が大きく、業務を外部に委託する際には、業務の健全性・適切性の確保を十分に図ることが求められている。そのため、業務の委託にあたっては、クラウド事業者の管理のために、契約締結前、さらには締結後についても事業者の業務遂行の適切性やセキュリティ管理体制の内容や実態についての情報を得たうえで、適切に評価しなければならない。一方でクラウド事業者は、金融機関の業務を受託するうえで、その社会的責任の重大さを踏まえて、こうした情報提供の依頼に応じ、説明責任を果たすことが期待される。

a. 管理策

(a)平常時における標準的な情報開示内容の明記

クラウド事業者が複数の委託元金融機関から多種多様な開示請求を受けた場合、対応負担が増す可能性がある。このため、事前にある程度標準的な情報開示の範囲を契約またはSLA等で定めることによりクラウド事業者の負担軽減を図り、金融機関からの情報開示の請求に対応しやすくする等の配慮をすることが望ましい。クラウド事業者によっては一般に公開している内容以上の情報提供について、その機密性の保全目的もあり消極的なケースがあるものの、金融機関による情報開示請求があった場合には、その必要性の説明が合理的である限り、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が必要である。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が必要となる。

(b)リスク顕在化時の情報開示

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、上記(a)の前提に関わらず、金融機関からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべき旨を契約やSLAに明記する必要がある。

(c)開示拒否があった場合の対応

クラウドサービスのアーキテクチャや仕様等に関する情報はクラウド事業者にとって最重要な機密事項である可能性が高く、クラウド事業者が情報開示に応じない可能性も想定し得る。金融機関としては、リスク管理に直結する事項（〔図表 11〕）については十分に把握しておくことが重要であるため、こうした情報の開示が必ずしも十分でないクラウド事業者と契約してよいか慎重な判断が求められる。

〔図表 11〕リスク管理に直結する事項

| |
|---|
| ①データの入力・保管・処理・バックアップ・出力といった一連のフロー<br>②暗号方式、暗号化されている領域とされていない領域<br>③システムログの取得範囲・取得頻度・保存期間<br>④データコピー（バックアップを含む）の取得内容と保管場所・保管期間<br>等 |

b. 簡易なリスク管理

金融機関の委託する業務の重要度が高くないと判断される場合、クラウド事業者に対し、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る必要はないことも考えられる。この場合には、クラウド事業者が提示する標準的な情報開示の内容で十分であり、さらに付加的な情報を求めることは必須ではない。

**③複数のクラウド事業者への委託**

クラウドサービスには、複数のクラウド事業者がサービスの委託を受けることがある。こうした状況下では、特定のクラウド事業者が所管するリソースにおける性能面のボトルネックや障害がクラウドサービス全体の品質に甚大な影響を与え得ることに留意する必要がある。インシデントが発生した場合に、それぞれのクラウド事業者が自らの責任の所在を認めず、責任の擦り付け合いが生じ、その結果、障害の状況把握や復旧対応が遅延するといった事態を回避しなければならない。

a. 管理策

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・クラウド事業者間での責任関係を明確にし、一元的な窓口機能やクラウド事業者間の相互調整機能を担う事業者（以下「メインコントラクター」という）をあらかじめ決めておくことが必要である。この役割を委託元金融機関が担える場合においては、クラウド事業者側のメインコントラクターは必要ではない。

b. 簡易なリスク管理

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は軽微であるといった判断ができる場合においては、必ずしもメインコントラクターを必要としないケースも考えられる。

### ④再委託先管理

金融機関は、安定したサービスの確保や情報保護等のために、直接の委託先であるクラウド事業者のみならず、再委託先についても同様に実態把握し適切なリスク管理を行うことが重要である。

a．管理策

再委託先の業務健全性を確保するために、〔図表 12〕のとおり、管理策を講じる必要がある。

**〔図表 12〕再委託先の管理策**

| | |
|---|---|
| 再委託先に対する適切な事前審査 | ・再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必要がある[19]。<br>・再委託先に対する事前審査については、例えば、クラウド事業者による再委託先の審査・管理プロセスが金融機関のそれよりも実効的であるとみなされる場合には、クラウド事業者側での事前審査[20]が最善策となり得る点には留意が必要である。<br>（注）特に重要な業務（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）を再委託する場合には、金融機関自らが事前審査することが必要である。 |
| 損害賠償も含めた責任の明確化 | 再委託先が問題を発生させた際、速やかな復旧回復の責任と同時に、委託先が損害賠償上限条項に定められた範囲内で賠償責任を負うことを明確にする。 |
| 再委託先の義務の明確化 | 委託先が金融機関に対して負う報告義務・内部統制確保義務などの各種義務を再委託先も負う扱いとするため、委託先・再委託先間の契約に必要な義務に関する条項を設けることを金融機関と委託先との契約に明記する。 |
| 再委託の中止の扱い | 各種の報告資料等を踏まえ、再委託先の業務遂行能力に対し、問題視し得る状況が生じた場合、金融機関はクラウド事業者に対し、再委託の中止を求めることができることを明確にし、契約上明記することが望ましい。クラウド事業者が中止の求めに応じない場合には、サービス利用の停止も検討する。 |

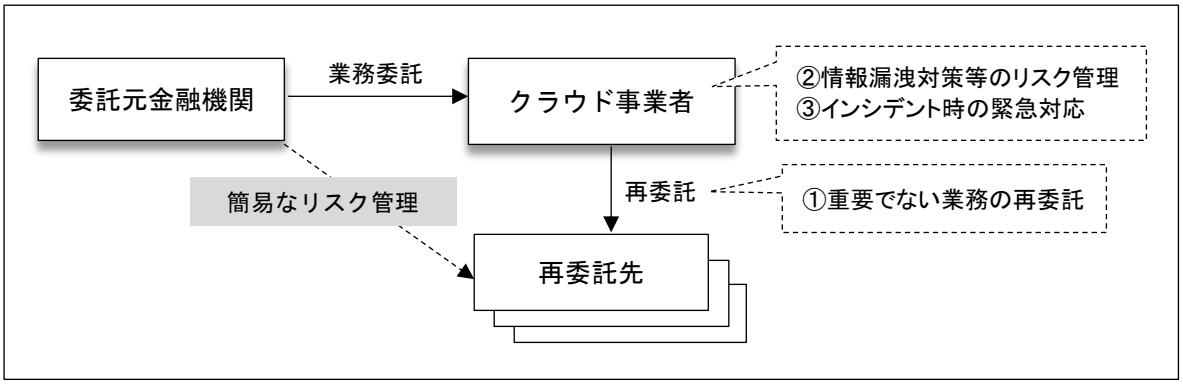
[19] 金融機関が自ら事前審査を行う場合、事前審査作業を効率化するため、クラウド事業者側と金融機関側の合意により、あらかじめ、再委託先の候補先企業群に対し事前審査を行うという工夫を講じることも考えられる。

[20] クラウド事業者側での再委託先の審査については、金融機関のリスク管理ポリシー等と照らし、金融機関自らが行う審査と比較して、その範囲・深度について同等かそれ以上である必要がある。これが満たされる場合は、個別の再委託先（既存分、新規追加・変更分）に係る事前報告や承諾を必ずしも要しない。

b. 簡易なリスク管理

再委託先への業務委託内容によっては、再委託先に対す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が可能と考えられる[21]。例えば、①再委託する対象業務が重要な業務ではなく、②サイバー攻撃対策や内部不正による情報漏洩対策などのリスク管理及び、③ログの取得・分析を含めたインシデント発生時の緊急対応を直接の委託先であるクラウド事業者側で行うといった場合などがこのケースに当たるという判断も可能である（〔図表 13〕）。

**〔図表 13〕再委託先に対するリスク管理の簡易化**




なお、上記の「a. 管理策」及び「b. 簡易なリスク管理」の事項を整理すると〔図表 14〕のとおりとなる。

**〔図表 14〕再委託する業務の重要度と事前審査の主体・レベルの関係**

| | 「a. 管理策」 | | 「b. 簡易なリスク管理」 |
|---|---|---|---|
| | 重要な業務 | 特に重要な業務 | 重要でない業務 |
| 事前審査の主体 | 金融機関 or クラウド事業者 | 金融機関 | 金融機関 or クラウド事業者 |
| 審査レベル | 厳格 | | 簡易 |

[21] リスク管理の簡易化については、例えば、チェック項目や頻度、深度の軽減化が考えられる（ただし、反社会的勢力等については、社会的に厳格な対応が求められていることに留意する）。

### (3)クラウドサービス運用時

ここでは、クラウドサービス運用時のデータ管理の観点として、データ暗号化と記憶装置等の故障時の管理について説明する。なお、運用時にはクラウド事業者が契約やSLAに基づき、適切なサービス提供やリスク管理を実施しているかなどについて、モニタリングや監査を行うことが必要であるが、これに係る論点[22]については「２．クラウド事業者に対する監査等」のパートで記載する。

#### ①データ暗号化等

『FISC 安全対策基準』では、重要なデータについては、暗号化することが望ましいとしたうえで、特に個人データを蓄積・伝送する場合には、暗号化・パスワード設定等、ファイルの不正コピーや盗難の際にもデータの内容が分からないようにするための対策を講じることが必要であるとしている。こうした記述や、諸外国の規制でも暗号化を強く推奨している[23]ことにも鑑み、データ保護の対策を考慮する必要がある。また、暗号化は一つの管理策ではあるが、技術の進化に伴い、よりデータ保護を強固にする管理策が現れた場合には暗号化の代替手段として採用を検討していくことも有効である。

a．管理策

暗号化を含むデータ保護において、〔図表 15〕のとおりの管理策が求められる。

**〔図表 15〕データ保護における管理策**

| | |
|---|---|
| 蓄積・伝送データの暗号化 | 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が必要である。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、金融機関としては、暗号化の仕様（①処理プロセスにおいてどの部分が暗号化されておりどの部分がされていないか、②暗号方式、③暗号鍵の管理態勢等）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をしておく必要がある。 |
| 暗号鍵の管理主体 | 暗号鍵の管理主体は必ずしも金融機関である必要はないが『FISC 安全対策基準』【運 43】に定める管理策[24]は必要である。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 |

[22] ここでは、モニタリングや監査における立入に関する論点が中心であり、モニタリング・監査に係る内容・方法論（稼働状況の監視、定期運用報告の受領・検証等）については言及していない。

[23] 例えば、米国のカリフォルニア州法（Senate Bill 1386：SB1386）等では、消費者の個人情報漏洩の可能性があると判断した場合、企業は各消費者にその旨通知するように義務づけている。ただし、当該「個人データ」が暗号化されている場合は、この通知義務は免除される。「個人データの暗号化」は義務とはしないまでも、暗号化を実施していない場合は、企業に対し厳しい情報開示を求める内容になっている。

[24] 【運 43】「暗号鍵の利用において運用管理方法を明確にすること」

| | |
|---|---|
| | し、同様に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。委託元金融機関が暗号鍵を保管し自ら管理をすることを可能にする技術も提供されてきている。こうした技術をベースとしたソリューションを利用することもリスク管理の向上には有効である。 |
| 暗号化の代替策 | 暗号化はデータ保護の有効な管理策の一つではあるが、①上記の暗号鍵の管理主体の課題や、②そもそも元データをクラウド環境下に出してしまうことに対する不安、③クラウドの業務処理に際し、暗号化と復号の処理を繰り返すことによるパフォーマンス劣化に対する懸念といった課題が考えられる。例えば、トークン化のように、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技術は暗号化の代替策となり得る。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。<br>（注）ファイルの不正コピーや盗難の際にもデータの内容が判読できないようにするための対策は、暗号化やトークン化に限定されない。 |

b. 簡易なリスク管理

暗号化やトークン化等の代替策は顧客データ等の重要データを保全するための管理策であり、情報の機密性や業務におけるリスクプロファイルによって「重要データ」とされないものについては暗号化やトークン化といった管理策を講じる必要性は低いという考え方もある。

**②記憶装置等の障害・交換**

クラウドサービスを利用する際、クラウド事業者において、記憶装置の故障等により機器・部品の交換を行うことがある。その際、交換対象の記憶装置等の機器・部品に金融機関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。金融機関としては、これらの記憶装置等に対しても、データ消去も含めた十分な管理を行う必要がある。

a. 管理策

記憶装置等の障害・交換についての管理策としては以下が考えられる。

①交換された元の記憶装置等において実際にデータが格納されていた可能性のある記憶媒体上のデータの物理的消去（消磁等）または論理的消去を実施する（回転部や論理回路等の機器故障により論理的消去の操作ができない場合は、物理的

消去を実施)。

（注）論理的消去については、後述の「(4) クラウドサービス契約終了時 ①データ消去」の内容を参照。

②クラウド事業者の施設外に搬出される前に物理的消去の作業を実施する。

③復元不可能としたうえで持ち出すといった点をあらかじめ契約書または SLA 等に明記する。

なお、契約中の記憶装置等の障害・交換については、後述のクラウドサービス契約終了時の対応と異なり、契約関係が継続し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も可能であることを踏まえると、消去証明書の発行・取得は、費用対効果を考えると必ずしも効果的とはいえない。

b. 簡易なリスク管理

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・破壊を必要としない。

### (4)クラウドサービス契約終了時

#### ①データ消去

クラウドサービス契約終了時には、金融機関が管理を委ねたデータについて適切な方法とタイミングで消去する必要がある。データ消去の確実な実施を保証するための管理策を講じる必要がある。

a．管理策

機密データの保管を委ねる場合、クラウドサービスの各システムリソースはクラウド事業者の資産であることが一般的であり、金融機関等自らがデータを消去することが困難な場合が想定される。この場合、データ消去はクラウド事業者が実行し、その消去証明書等を受領することが一つの方策として考えられる。ここでのデータ消去については、物理的消去もしくは一定条件を満たした論理的消去（〔図表 16〕）を指す。また、個別の消去証明書の発行・取得負担を軽減するため、クラウドサービス契約終了時には、論理的消去も含めたデータ消去をクラウド事業者が実施することを契約書に記載し、かつ消去プロセスの適切性を外部の第三者が監査等において併せて検証することにより、消去証明書の発行・取得の代わりとすることも考えられる。

ただし、現在のところ、論理的消去によって個人情報の復元を完全に「不可能化」することはできない（情報復元を「著しく困難な状態にできる」にとどまる）ため、情報漏洩リスクをさらに軽減する観点から、将来的なハードウェア更改・撤去時に「物理的消去」をクラウド事業者側が行うことをあらかじめ契約上明記することも望まれる。

契約終了後も、情報漏洩事故等のインシデント対応等のためクラウド事業者に委ねたデータを（バックアップデータとして）利用する可能性があるため、消去のタイミングについてはあらかじめ事業者との間で明確にし、契約上明記しておくことが望ましい。

**〔図表 16〕一定条件を満たしたデータの論理的消去**

| | |
|---|---|
| 切片化されたデータ | データ保存領域には切片化されたデータが保管されており、切片化されたデータのみから個人情報や顧客金融機関に係る情報を復元することが著しく困難な状態である場合、データ管理領域とデータ保存領域とのリンク情報を不可逆的に切断すること。 |
| データ保存領域の完全上書き | データ保存領域の完全上書き（意図的な無意味なデータまたは他ユーザーのデータによる上書き）を行うこと。 |
| 暗号鍵の破棄 | 保管データが暗号化されている場合、暗号鍵を破棄すること。 |

b．簡易なリスク管理

顧客データ等の機密情報を扱わない業務をクラウドに委ねる場合については物理

的・論理的消去の対象となるデータが存在しないため、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、消去証明書も必要としない。

**②ベンダーロックイン**

クラウド事業者が提供するプログラミング言語やサービス等が固定されている場合、ユーザー側が自由にクラウド環境を構築していくことが難しい可能性がある。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サービス契約の続行が困難になるような場合に、速やか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しておくことが望ましい。

a. 管理策

委託元金融機関は、契約の中断・終了に伴うシステム移行を考慮した準備をしておくことが望ましい。その際の管理策は〔図表 17〕のとおりとなる。

**〔図表 17〕ベンダーロックインリスク低減のための管理策**

| | |
|---|---|
| クラウド事業者側の協力義務 | 以下の内容を契約に記載する。<br>・委託元金融機関に対し、新しい委託先、もしくは社内の既存システムに移行すべきデータを抽出する方法をクラウド事業者が提供する。<br>・クラウド事業者は、実際の移行作業に協力する。 |
| 移行作業の事前把握 | 委託元金融機関は、移行データの抽出方法と実際の移行作業内容を、クラウドサービス利用前に把握する。 |
| 費用負担 | 金融機関側の事情によるクラウド契約の解約、クラウド事業者に起因する事情に基づく解約の各々のケースを想定し、あらかじめ移行作業の費用負担について契約上定めておく。 |

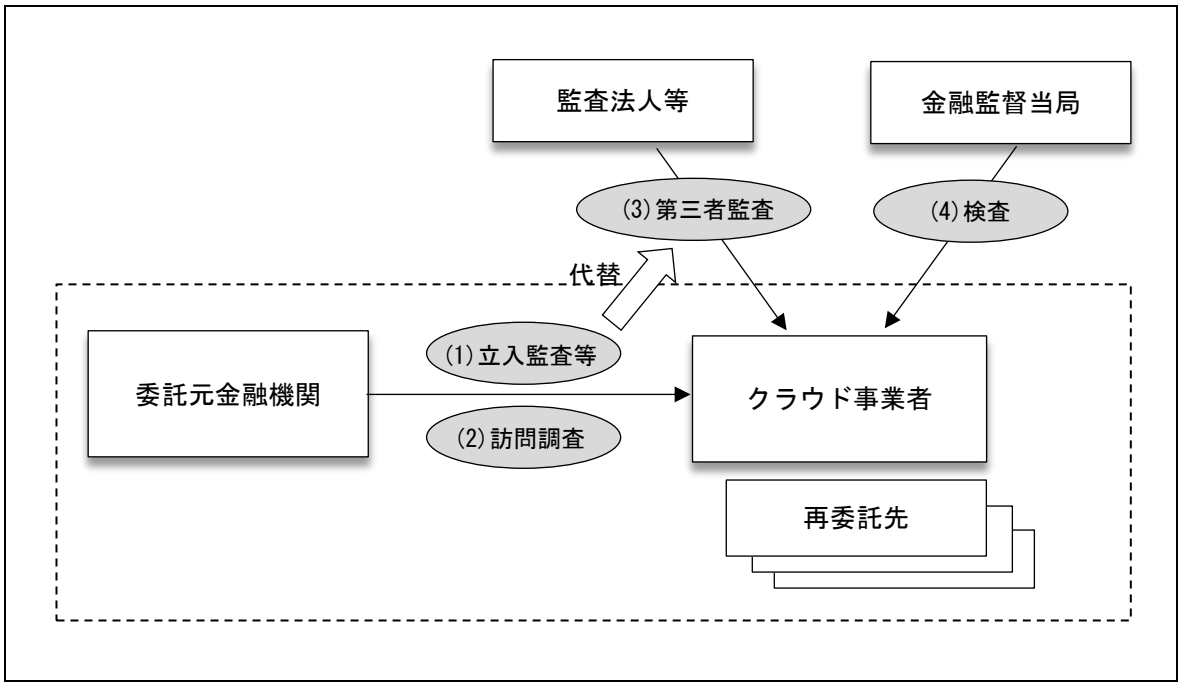
b. 簡易なリスク管理

重要システムをクラウドに移行する場合は、ベンダーロックインリスク低減のための対策を講じることが望ましいが、重要度の低い業務を委託するにとどまる場合にはクラウド事業者の協力を前提とせず、業務を代替する別の事業者に移行するための準備をしておくことをもって十分とする考え方はあり得る。例えば、コンピューティング資源のみを委託する IaaS（Infrastructure as a Service）の場合では、クラウド事業者の協力がなくても比較的容易に別のクラウドサービス基盤に移行することが可能であるため、こうしたケースに該当すると考えられる。

## ２．クラウド事業者に対する監査等

金融業務のベースとなる情報及びその情報を取り扱うプロセスを外部に委ねるクラウドサービスを利用する場合においても、金融機関の経営陣は責任を負う。そのため、直接の内部統制の及びにくいクラウド事業者について、リスク管理態勢等の有効性を検証することが必要である（〔図表 18〕）。

〔図表 18〕クラウド事業者に対する監査等に関する論点のイメージ




### (1)委託元金融機関による立入監査・モニタリング

金融機関は、自らの業務処理を自社の責任で適正に行い、顧客データ等の重要情報を適切に管理する必要があるため、業務委託を行う場合には、当該委託業務が適切に運営されているかを検証することが求められる。この点、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（以下「立入監査等」という）等により実地で確認することが必要である[25]。

[25] クラウド事業者の業務処理施設に委託元金融機関の監査員等の立入を認めることは、同一クラウド事業者と契約している他の多くの委託元企業にとってもセキュリティ上等の問題を惹起し、業務処理の安定性・安全性を損ねるリスクがあるという意見もある。もっとも、そうしたリスクを避けることよりも、ユーザーまたは代行者による検証を受け入れ、業務処理全般の健全性を確認する必要性の方が高いとの意見が多い。

a．管理策（運用方法）

委託元金融機関による立入監査等の運用は、〔図表 19〕のとおりである。

**〔図表 19〕委託元金融機関による立入監査等の運用**

| | |
|---|---|
| 立入監査等の権利の明記 | 業務委託契約に、委託元金融機関の立入監査等を実施する権利を明記する必要がある。 |
| 立入監査等の代替手段 | 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。その場合の要件は後述の「(3)第三者監査」に記載する。 |
| 立入監査等の権利行使 | 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とる場合は、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考えられる。 |
| 立入監査等の受入対応費用 | 立入監査等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何れが負担するか、あらかじめ両者で協議しておく必要がある。 |
| 再委託先への立入監査等 | 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等を実施する権利を明記する必要がある。 |
| 立入監査等の指摘事項の扱い | 立入監査等により判明した指摘事項については、対応の是非も含め、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しておく必要がある。 |

b．簡易なリスク管理

重要度が高くない業務を委託する場合については、委託元金融機関による立入監査等（または後述の「第三者監査」）の代わりに、その業務の必要とする立入監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」[26]のレポートの活用が考えられる。また、重要度によっては、クラウド事業者が準備する「第三者認証」のレポートやセキュリティに係るホワイトペーパー等により代替とするといった管理策も考えられる。

[26] 各国の公認会計士協会や業界団体等が定める事業者等の情報セキュリティ体制やプライバシー保護体制の基準等に係る認証。代表的なものとして、ISMS(ISO27001)や PCI DSS level 1、SOC1、SOC2、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、プライバシーマーク等がある。

### (2)委託元金融機関によるクラウド事業者施設への立入

委託元金融機関によるクラウド事業者施設への立入に関しては、上記「(1)委託元金融機関による立入監査・モニタリング」で述べられた観点以外にもその必要性が認められるので留意が必要である。

a. 管理策（運用方法）

(a)契約締結・業務開始前のクラウド事業者施設訪問

委託元金融機関には、プロセッシングやデータ保管が行われている施設を実地で確認するとともに、管理者と面談を行い、今後のコミュニケーションルートを確保すること等を求めるニーズがある。こうした実地調査は、データセンター等における内部統制環境の不備指摘が主目的ではない。訪問調査の受入可否は、クラウド事業者のポリシーに依存することとなるが、委託元金融機関としては、事業者選定のデューデリジェンスを行う際に訪問受入のスタンスや情報開示姿勢も考慮に入れておくことが考えられる。

(b)インシデント発生時の立入調査

情報漏洩等のインシデント[27]が発生した場合、もしくは発生が疑われる場合に、被害の有無、及び被害があった場合の全貌把握や流出経路の特定のため、クラウド事業者は、委託元金融機関の調査に協力すべきである。重大なインシデント調査で、利用者等が立入監査をする場合、要求に応じた証跡の提示を受容することが望ましい。

クラウド事業者が提供に応じない、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ある場合には、委託元金融機関自ら、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必要となるが、クラウド事業者はこれを認めるべきである。また、これを契約上明記することが望ましい。この調査においては、立入調査人自ら、もしくは、立入調査人の指示によりクラウド事業者側のオペレーターが、機器の操作を行い、証跡（ログ）の収集・解析を行うことになる。

クラウド事業者側が自らのポリシーにより、委託元金融機関の立入調査人や金融機関の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による機器操作のための調査受入を避けたい場合は、トレーサビリティを確保するため、委託元金融機関の施設、クラウド事業者側の施設、または外部施設の何れかにおいて解析に必要な情報を抽出することのできるツールが必要となる。また、これらの抽出ツールが適切に作動すること

[27] ここでいう「インシデント」とは、委託元金融機関が委ねた業務に係るインシデントを指す。また、クラウド事業者が受託している他の顧客に関わる部分でインシデントが発生した場合、当該インシデントの状況によっては、「委託元金融機関の委ねた業務に関わるインシデントの発生が疑われる」事態となり得る。

に関する外部の第三者による検証を受けることが必要である。

こうしたデータ抽出の機能は、アプリケーションの一部機能としてユーザーに提供されるケースもあるが、提供されていない、ないし網羅性に問題がある場合は、別途、抽出ツールの開発・検証が必要になる。この場合、委託金融機関としては、収集の対象となる証跡の範囲（当該クラウド事業者の他の顧客に関わる証跡のため委託元金融機関に一般的には開示できないものも含む）や、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、契約締結時にクラウド事業者とあらかじめ合意を得る必要がある。

(c) クラウド事業者側の経営不安発生時の対応

クラウド事業者側の経営不安が発生した場合、委託元金融機関自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が必要である。

b. 簡易なリスク管理

相対的に重要度が高くないと金融機関が判断し得る業務については、費用対効果を踏まえた管理策を講じることが考えられる。リスク管理に必要なデータ抽出のツールを事業者側で準備・提供してもらう等、実際に立ち入ることなくリスク管理が可能と判断される場合には、必ずしも立入を必要としない。

### (3) 第三者監査

a. 管理策（運用方法）

委託元金融機関の立入監査等が実効的でない場合を想定し、その代替となり得る第三者監査の在り方も検討しておく必要がある。その場合に求められる要件は「検証項目」、「検証の担い手」、及び「検証の機動性」の３つの切り口で、以下のように整理される。

(a) 検証項目

委託元金融機関の立入監査等を第三者監査で代替するとした場合、その検証項目については、一般的なシステムリスクに係る検証項目に加え、クラウドのリスクプロファイルを踏まえた検証、委託元金融機関の検証ニーズに則った検証が必要となる。

なお、委託元金融機関が単独、または他の金融機関と共同で第三者監査人と監査契約を締結し、クラウド事業者に対する監査を行う場合、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と考えられる。

（金融業界におけるクラウド利用に関する監査指針）

リスク管理は、各金融機関が自律的に行うべきものであり、監査の指針・基準についても各自の創意工夫により自己責任で策定すべきものであるが、監査視点の共通化や標準化が図られることによりクラウドに係る監査の実効性を高める効果も相応にあると考えられる。こうした中、今後、FISC では本報告書をもとに、『FISC 安全対策基準』のほか『金融機関等のシステム監査指針』の改訂を行う予定である。第三者監査人も含め業界関係者はこうした監査指針を活用していくことが期待される。

(b) 検証の担い手

監査は、本来、委託元金融機関が自らの責任のもと、自ら主導して行う必要があるという前提を考慮し、クラウド事業者と第三者監査人との独立性の確保や、検証能力が十分でない第三者監査人が関与することによる実効性の低下を防ぐためには、〔図表 20〕に挙げられるような対策が考えられる。

〔図表 20〕検証の担い手の独立性確保、実効性の低下防止のための対策

| | |
|---|---|
| 独立性の確保 | 委託元金融機関が、単独また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し、クラウド事業者に対する監査を行う体制も選択可能とすることが望まれる。 |
| | 委託元金融機関側が、第三者監査に関する費用を負担（または分担）する体制に移行することが望まれる。 |
| | 同一の監査責任者が長期間にわたり監査を行うことによる外観的独立性に対する疑念を払拭するため、適切なサイクルで交代することが適当である。 |
| 実効性の低下防止 | 監査の品質を引き上げるために、SOC2[28]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。 |
| | 第三者監査人の適格性の担保のため、監査人（監査法人）が日本公認会計士協会等の指導や指針等に基づいて、適切な品質管理体制の整備、運用を実施することが必要である。 |
| 効率性の確保 | 第三者監査を効率的に行うため、複数の委託元金融機関が共同で第三者に監査実施を委託することも有効である。 |

(c)検証の機動性

①クラウド技術に関する重要な脆弱性が判明した場合や、②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、③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が求められる。

b．簡易なリスク管理

「Ⅲ ２．(1)委託元金融機関による立入監査・モニタリング」での簡易なリスク管理と同様、重要度が高くない業務を委託する場合については、第三者監査の代わりに、その業務の必要とする立入監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。また、重要度によっては、クラウド事業者が準備する「第三者認証」のレポートやセキュリティに係るホワイトペーパー等により代替とするといった管理策も考えられる。

[28] 業務受託会社のセキュリティ、可用性、処理のインテグリティ、機密保持、またはプライバシーを主題としたコンプライアンスや業務運営の内部統制についての報告書。

### (4)金融監督当局の検査等[29]

金融監督当局は、当該金融機関の業務の健全性について、委託業務も含めて検証する公益上の要請がある。当局の要求があった場合、クラウド事業者としては立入検査等を受け入れることが法律上求められる。当局の立入検査等に関し、委託元金融機関とクラウド事業者に求められる事項は〔図表 21〕のとおりとなる。

**〔図表 21〕委託元金融機関とクラウド事業者に求められる事項**

| | |
|---|---|
| 当局の検査等への協力義務 | 当局の立入検査等の円滑な実施を担保するため、委託元金融機関とクラウド事業者との間の契約に、クラウド事業者の当局検査等への協力義務を明記することが必要である。 |
| 再委託先への立入検査等 | 委託業務の再委託先（再々委託先等を含む）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が必要である。 |
| 検査等後の指摘事項の扱い | 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必要がある。 |

[29] 報告・資料提出を求めることを含む。

## ３．インシデント発生時の対応

### (1)事前対策と事後対策

クラウドで想定されるインシデントについては、オンプレミスシステムにおいて発生するインシデントと異なり、金融機関の完全な管理下にない資産やデータなどがあるため、事態によっては採るべき対策も異なってくる。リスク管理の観点からは、事前に想定されるインシデントに対する準備（バックアップや代替サービスの準備等）のほか、実際のインシデント発生時には、検知と切り分けの作業、インシデント事象解析のためのデータ収集・分析、原因の排除と迅速な復旧作業、再発防止策の策定などが重要である。

### (2)トレーサビリティの確保

クラウドは、仮想化され、かつ動的に変化する環境であるため、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。このため、金融機関としては、トレーサビリティの確保のための方策を準備する必要がある。

金融機関は、インシデント時には必要なデータを抽出し、それを解析し、対策を講じる（もしくは講じさせる）義務を負う。自社で解析が困難な場合にはセキュリティ業者やデジタルフォレンジック業者が代行で行うことになるが、その際には必要に応じて関連施設への立入も必要となる（立入調査の内容については、前述した「Ⅲ　２.(2)委託元金融機関による事業者施設への立入」を参照)。

## おわりに

わが国の金融機関を取り巻く環境は、規制緩和による商品・サービスの多様性、金融機関の統合・再編など今までにない速さで変動している。こうした状況下、金融機関は顧客ニーズをいち早くキャッチし、新しい金融サービス・商品の提供により他の金融機関との差別化を図るなど、より迅速な業務改革と経営判断が必要になる。そのためには、新しい商品・サービス、事業への参入・撤退、拡大・縮小が低コストで迅速に行える必要があり、クラウドはこれを実現する有力なツールになり得ると期待される。

本検討会では、クラウドのうち資源共有型スキームの性格が強いパブリッククラウドを対象にリスク管理の在り方について議論を行った。クラウド利用の対象となる業務やシステムの重要度やプロファイルに応じたリスク管理を行うこととなるが、本報告書ではそのリスク管理策の事例や一定の目線を示した。本検討会を通じて議論を重ねてきた結果を踏まえ、金融機関がリスクを正しく把握し、適切なリスク管理策を講じていくことでクラウドの利用に対する障壁が低くなっていくことを期待する。

また、今後金融業界において、クラウドが益々有効に利用されていくためにも、金融機関やクラウド事業者、金融監督当局等各々のステークホルダーが有機的に連携していくことが大切である。

まず、金融機関においては、前述したとおり、クラウドが迅速な業務改革とスピード経営を実現するための有効なツールの一つであるため、今後改めて利用可否を検討することも重要である。また、利用を拡大するにあたっては、日々進化するクラウド技術がもたらす新しいリスクにも柔軟に対応できる体制を整備するなどリスク管理の向上にも努めることが期待される。

クラウド事業者においては、金融機関の業務の外部委託を受ける立場として、可監査性の確保、リスク管理向上に資する情報開示、インシデント発生時に備えたトレーサビリティに係る情報の提供、金融機関の作業支援など可能な限りの協力が望まれる。

監督当局や自主規制・ガイドライン作成団体等においても、進化するクラウド技術や法制度等の環境変化に伴って、クラウドの実態を十分に反映した規制やガイドラインを順次整備していくことが期待される。

本報告書が、わが国の金融機関のクラウド利用やリスク管理に係るポリシー等の策定・見直しに、そしてクラウド事業者にとっては、金融機関にサービスを提供するために必要となるリスク管理策の立案・実装に少しでも役立てられれば幸いである。

以　上

## 「金融機関におけるクラウド利用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 | 喜連川　優 | 情報・システム研究機構　国立情報学研究所　所長<br>東京大学生産技術研究所　教授 |
| 委員 | 柴山　悦哉 | 東京大学　情報基盤センター<br>情報メディア教育研究部門　教授 |
| | 國領　二郎 | 慶應義塾大学　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　弁護士 |
| | 谷崎　勝教 | 株式会社三井住友銀行　常務執行役員 |
| | 米澤　浩樹 | 株式会社京都銀行　システム部　部長（第３回まで） |
| | 南地　伸昭 | 株式会社池田泉州銀行　常務執行役員　東京支店長<br>兼　東京事務所長（第４回から） |
| | 小出　哲也 | 第一生命保険株式会社<br>IT ビジネスプロセス企画部　部長 |
| | 飯豊　聡 | (旧)株式会社損害保険ジャパン 日本興亜損害保険株式会社<br>執行役員　IT 企画部長（第３回まで） |
| | 西脇　真司 | 損害保険ジャパン日本興亜株式会社　IT 企画部長<br>（第４回から） |
| | 阪上　啓二 | 野村ホールディングス株式会社<br>IT 統括部　マネージング・ディレクター |
| | 岩崎　明 | 株式会社セールスフォース・ドットコム<br>専務執行役員 |
| | 渡辺　弘美 | アマゾン　ジャパン株式会社　渉外本部　本部長 |
| | 小池　裕幸 | 日本アイ・ビー・エム株式会社<br>クラウド事業統括　執行役員 |
| | 古川　公一 | エヌ・ティ・ティ・コミュニケーションズ株式会社<br>常務取締役　ソリューションサービス部長（第３回まで） |
| | 田中　基夫 | エヌ・ティ・ティ・コミュニケーションズ株式会社<br>取締役　クラウドサービス部長（第４回から） |
| | 前田　章 | 株式会社　日立製作所　情報・通信システム社　技師長 |
| | 中村　元彦 | 日本公認会計士協会　常務理事（IT 担当） |
| オブザーバー | 郡山　信 | 金融庁　検査局　総務課<br>システムモニタリング長　統括検査官 |
| | 志村　秀一 | 日本銀行　金融機構局　考査企画課　システム・業務継続<br>グループ長　企画役 |

赤阪　晋介　　総務省　情報流通行政局　情報流通振興課
情報セキュリティ対策室 室長
上村　昌博　　経済産業省　商務情報政策局　情報セキュリティ政策室
室長

（金融情報システムセンター事務局）

| | | |
|---|---|---|
| 理事長 | | 渡辺　達郎 |
| 常務理事 | | 吉田　知生（第４回から） |
| 常務理事 | | 沼波　正　（第３回まで） |
| 企画部 | 部長 | 米山　正夫（第４回から） |
| 調査部 | 部長 | 荒井　隆　（第４回まで） |
| 調査部 | 部長 | 櫻井　康雄 |
| 監査安全部 | 部長 | 西村　敏信 |
| 総務部 | 部長 | 阪　　章伸（第２回から） |
| 総務部 | 部長 | 中田　治彦（第１回） |

◆事務局スタッフ
榎　隆司、小沢　壮（第５回まで）、宮原　武也、岡田　昌一
新林　浩司、本田　愼一（第３回まで）

（参考）検討会の開催日程
第１回（平成 26 年４月 14 日）、第２回（同５月 16 日）、第３回（同６月 16 日）
第４回（同７月７日）、第５回（同９月 30 日）、第６回（同 10 月 20 日）

# 資料編

## 【図表A】クラウドの利用状況

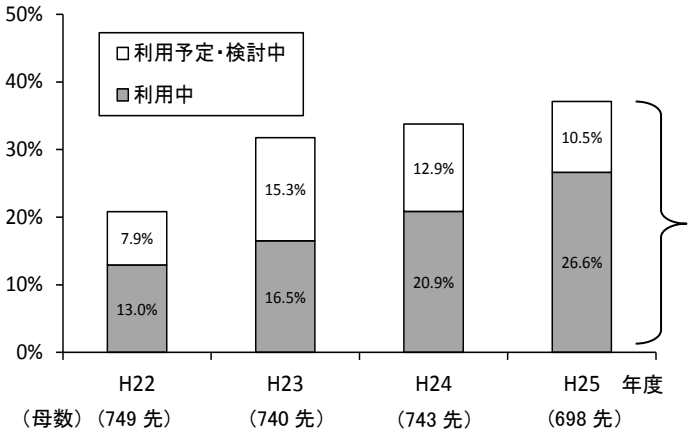
―― FISC『金融機関等のシステムに関する動向及び安全対策実施状況調査』結果をもとに作成

―― 調査基準日：平成 26 年3月 31 日

―― 有効回答先： 698 先

（注）パブリッククラウドは、アンケート調査上、「利用中」と「利用予定・検討中」の区分なし。

### ①クラウド利用率の推移（パブリック／コミュニティ／プライベート等全体）




【H25 年度のクラウド利用先数】

| | クラウド全体 | パブリッククラウド |
|---|---|---|
| 利用予定・検討中 | 73 先 | （注） |
| 利用中 | 186 先 | |
| 合 計 | 259 先 | 112 先 |
| 比 率 | 37.1 % | 16.0 % |
| （H24 年度） | （33.8 %） | （13.5 %） |

### ②クラウドの利用環境（「利用中」及び「利用予定・検討中」の 259 先が回答＜複数回答可＞）

―― 「パブリッククラウド」の利用先数が多い順にソート （先）

| | | パブリッククラウド | コミュニティクラウド | プライベートクラウド | 計 |
|---|---|---|---|---|---|
| 1 | 営業支援システム | 35 | 8 | 38 | 81 |
| 2 | 電子メール | 33 | 11 | 29 | 73 |
| 3 | 社内情報共有 | 29 | 9 | 39 | 77 |
| 4 | eラーニングシステム | 23 | 7 | 16 | 46 |
| 5 | Webサイト構築用 | 22 | 4 | 14 | 40 |
| 6 | スケジュール管理 | 18 | 8 | 23 | 49 |
| 7 | サーバーとして利用 | 17 | 8 | 32 | 57 |
| 8 | 勤怠管理システム | 17 | 4 | 15 | 36 |
| 9 | 人事システム | 10 | 4 | 16 | 30 |
| 10 | 経理システム | 9 | 4 | 13 | 26 |
| 11 | 福利厚生システム | 9 | 5 | 8 | 22 |
| 12 | バックアップシステム | 7 | 7 | 20 | 34 |
| 13 | 総務システム | 7 | 6 | 9 | 22 |
| 14 | 資産運用システム | 6 | 5 | 17 | 28 |
| 15 | システム開発管理 | 6 | 2 | 9 | 17 |
| 16 | 基幹業務系システム | 3 | 10 | 22 | 35 |
| 17 | OA | 3 | 3 | 18 | 24 |

## ③業態別のクラウド利用状況（比率）

### 【パブリック／コミュニティ／プライベート等全体】

（%）

| | 業　態 | 有効回答先 | 利用 | 利用中 | 利用予定・検討中 | 利用・検討の予定なし | 無回答 |
|---|---|---|---|---|---|---|---|
| | 全体 | 698 先 | 37.1 | (26.6) | (10.4) | 60.2 | 2.7 |
| 1 | 都市銀行等 | 5 先 | 100.0 | (100.0) | (−) | − | − |
| 2 | 信託銀行 | 7 先 | 100.0 | (71.4) | (28.6) | − | − |
| 3 | 地方銀行 | 63 先 | 66.7 | (42.9) | (23.8) | 33.3 | − |
| 4 | 第二地方銀行 | 39 先 | 66.7 | (43.6) | (23.1) | 33.3 | − |
| 5 | その他銀行等 | 12 先 | 75.0 | (66.7) | (8.3) | 25.0 | − |
| 6 | 信用金庫等 | 247 先 | 21.5 | (8.5) | (13.0) | 77.7 | 0.8 |
| 7 | 信用組合等 | 68 先 | 7.4 | (7.4) | (−) | 91.2 | 1.5 |
| 8 | 労働金庫 | 13 先 | − | (−) | (−) | 100.0 | − |
| 9 | 県信連 | 31 先 | 3.2 | (3.2) | (−) | 80.6 | 16.1 |
| 10 | 生命保険会社 | 33 先 | 87.9 | (84.8) | (3.0) | 9.1 | 3.0 |
| 11 | 損害保険会社 | 21 先 | 85.7 | (76.2) | (9.5) | 9.5 | 4.8 |
| 12 | 証券会社 | 156 先 | 39.1 | (32.1) | (7.1) | 55.1 | 5.8 |
| 13 | ｸﾚｼﾞｯﾄｶｰﾄﾞ会社等 | 3 先 | 100.0 | (100.0) | (−) | − | − |

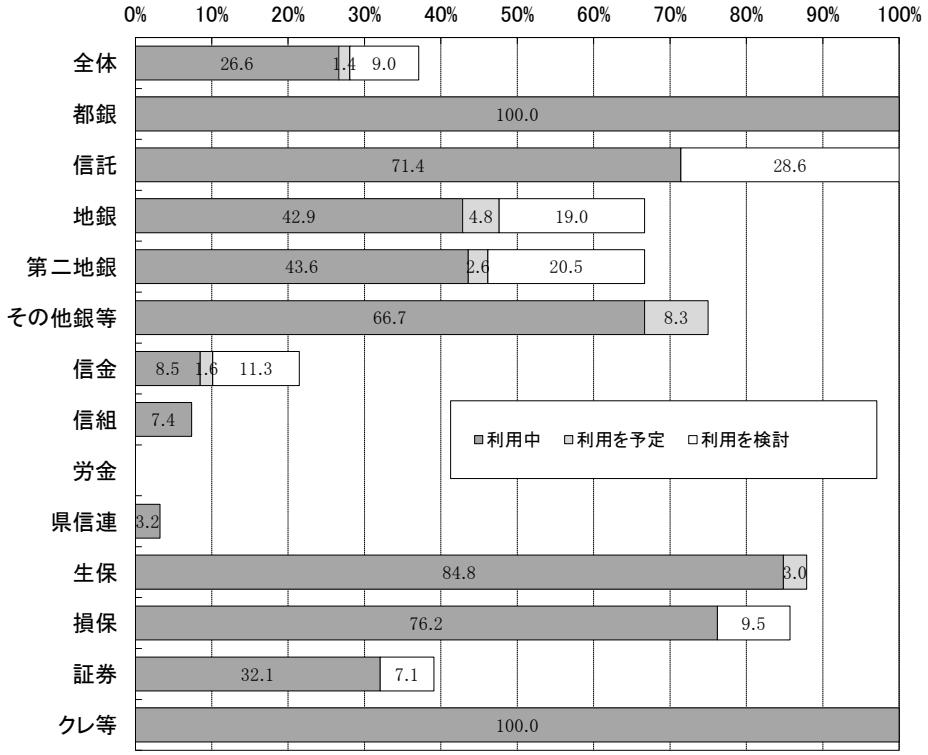
### 【パブリッククラウド】

（%）

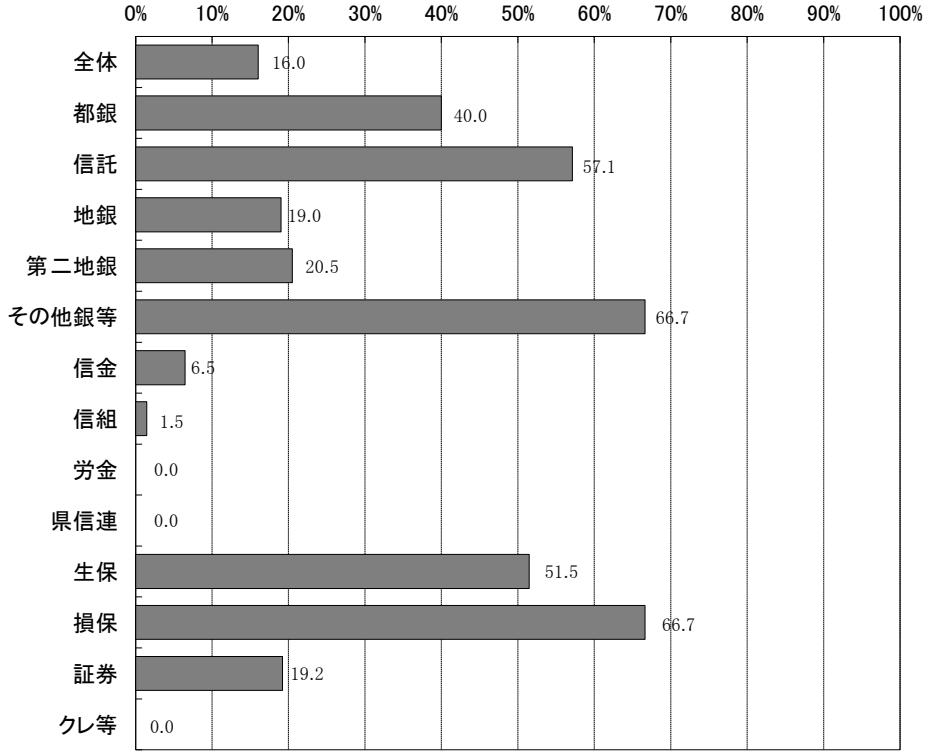
| | 業　態 | 有効回答先 | 利用中　＆<br>利用予定・検討中 | 利用・検討の<br>予定なし | 無回答 |
|---|---|---|---|---|---|
| | 全体 | 698 先 | 16.0 | 81.2 | 2.7 |
| 1 | 都市銀行等 | 5 先 | 40.0 | 60.0 | − |
| 2 | 信託銀行 | 7 先 | 57.1 | 42.9 | − |
| 3 | 地方銀行 | 63 先 | 19.0 | 81.0 | − |
| 4 | 第二地方銀行 | 39 先 | 20.5 | 79.5 | − |
| 5 | その他銀行等 | 12 先 | 66.7 | 33.3 | − |
| 6 | 信用金庫等 | 247 先 | 6.5 | 92.7 | 0.8 |
| 7 | 信用組合等 | 68 先 | 1.5 | 97.1 | 1.5 |
| 8 | 労働金庫 | 13 先 | − | 100.0 | − |
| 9 | 県信連 | 31 先 | − | 83.9 | 16.1 |
| 10 | 生命保険会社 | 33 先 | 51.5 | 45.5 | 3.0 |
| 11 | 損害保険会社 | 21 先 | 66.7 | 28.6 | 4.8 |
| 12 | 証券会社 | 156 先 | 19.2 | 75.0 | 5.8 |
| 13 | ｸﾚｼﾞｯﾄｶｰﾄﾞ会社等 | 3 先 | − | 100.0 | − |

（参考）業態別のクラウド利用状況（比率）のグラフ

【パブリック／コミュニティ／プライベート等全体】

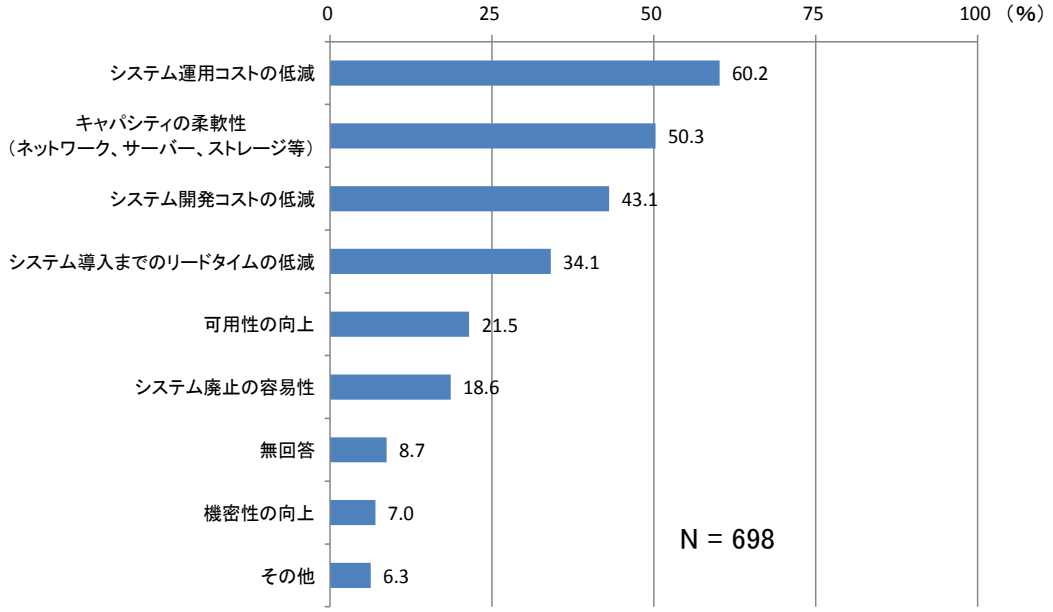



【パブリッククラウド】 ・・・「利用中」+「利用を予定」+「利用を検討」の合算比率



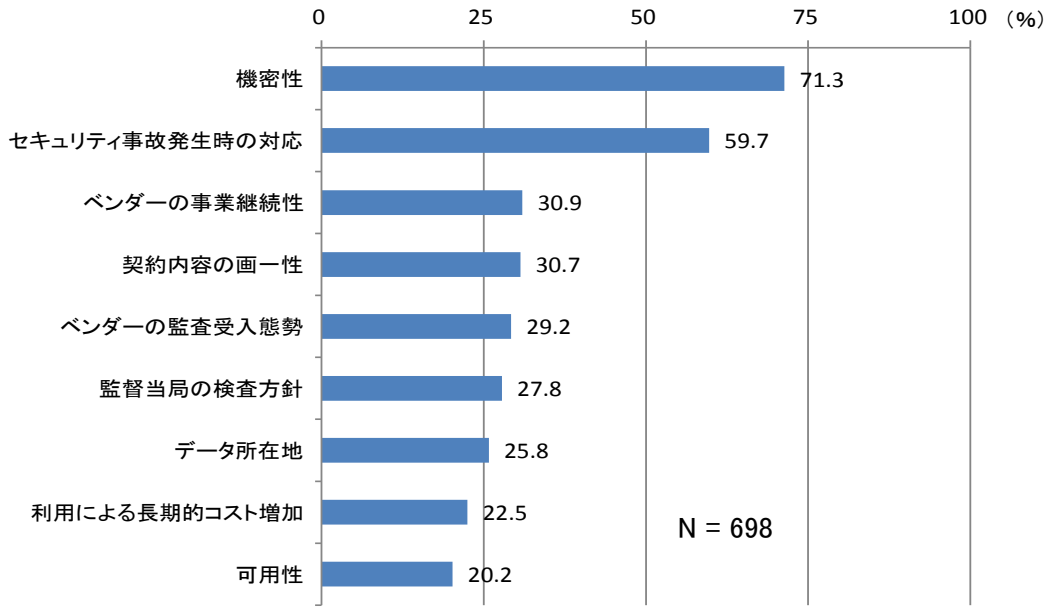
## ④クラウド利用の想定されるメリット

―― すべての金融機関を対象に、クラウド利用について想定されるメリットを調査したところ、「システム運用コストの低減」が 60.2%と最も多く、続いて「キャパシティの柔軟性」が 50.3%となった（回答先数：698 先、複数回答可）。



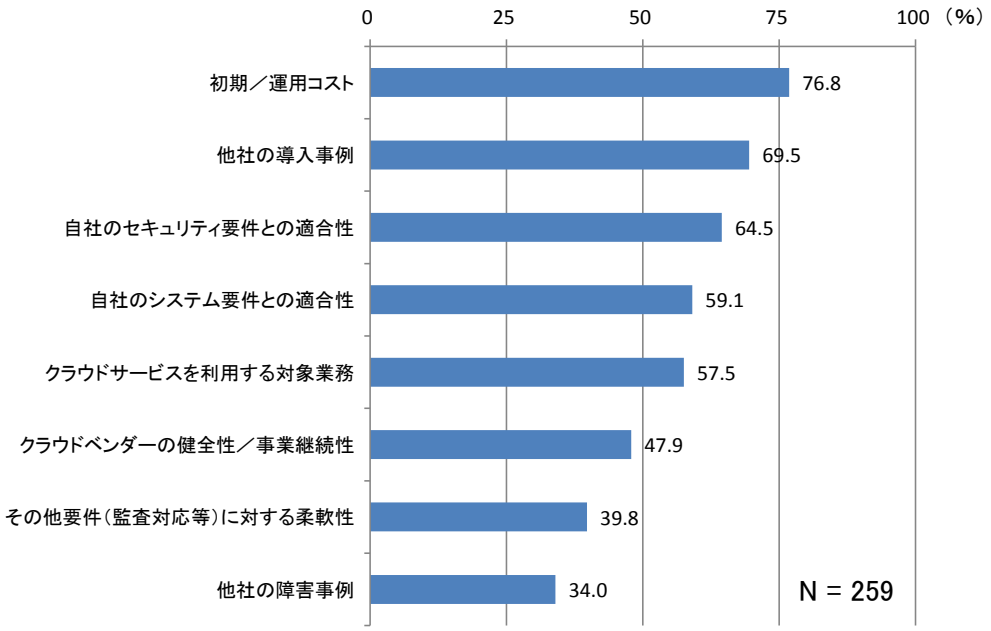

## ⑤クラウド利用に対する懸念・不安

―― すべての金融機関を対象に、クラウド利用に対する懸念や不安について調査したところ、「機密性（アクセス管理、暗号化管理等）」に対する懸念・不安が 71.3%と最も多く、続いて「セキュリティ事故発生時の対応」が 59.7%となった（回答先数：698 先、複数回答可）。



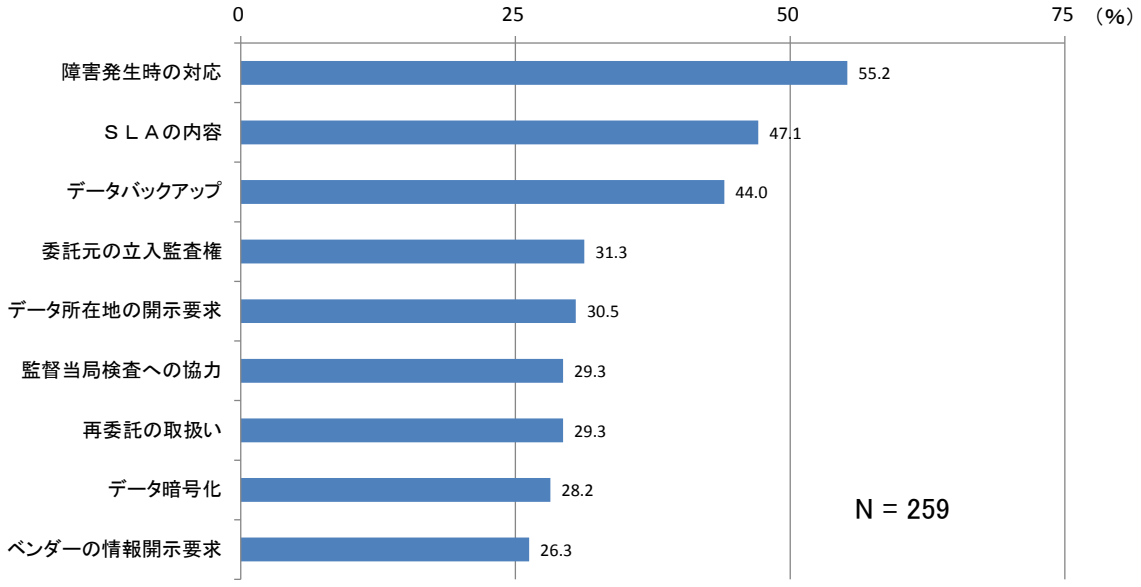
## ⑥クラウドの利用・計画にあたって情報収集している項目

―― クラウドの利用又は計画をしている金融機関を対象に、情報収集している項目を調査した結果は、以下のとおり。「初期／運用コスト」、「他社の導入事例」をはじめ多くの項目で比率が高い（回答先数：259 先、複数回答可）。



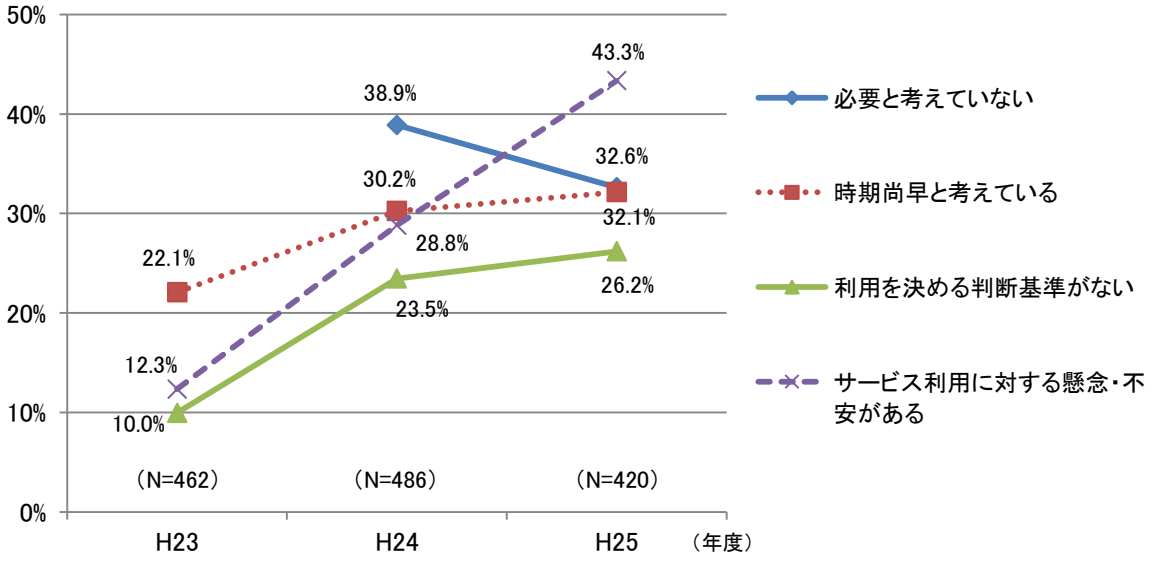

## ⑦クラウドの利用・計画にあたってベンダーと調整した項目

―― クラウドの利用又は計画をしている金融機関を対象に、ベンダーと調整した内容については、「システム障害発生時の対応」が最も多く、続いて「SLA の内容」、「データバックアップ」となっており、サービス品質について調整する傾向が強い。その他、「委託元の立入監査権」や「データ所在地の開示要求」などの回答もあった（回答先数：259 先、複数回答可）。



⑧クラウドの利用／検討なしとする理由（パブリック／コミュニティ／プライベート等全体）

―― クラウドの利用を検討又は予定していない金融機関に対して、その理由を聞いた結果は、以下のとおり。「サービス利用に対する懸念・不安がある」の割合が最も高く、また前年度から増加（回答先数：420 先＜平成 25 年度＞、複数回答可）。



## 【図表B】FISC によるヒアリング結果

▽ 金融機関に特徴的な課題

| | |
|---|---|
| ① | 従来から自社内で十分なセキュリティ対策を行っており、さらに自社構築システムで十分な費用対効果も得られている中で、現時点ではクラウド利用のメリットは少ない。 |
| ② | クラウド利用に関する具体的な安全対策基準やシステム監査指針が存在しないか内容が不十分である。 |
| ③ | クラウド事業者への委託業務ということでも自社でリスク管理を行う責任があるが、クラウド事業者が提示した契約雛形に従わざるを得ず、クラウド事業者に対して十分な統制をかけることができない。 |
| ④ | 利用を取りやめる際に、データを確実に消去してくれるのか判然としない。また、新システムへの引継ぎ作業にクラウド事業者が協力するのか定かではない。 |
| ⑤ | クラウド事業者施設に銀行法に基づき金融庁検査が入ろうとする場合に、クラウド事業者側が検査に協力するか判然としない。 |
| ⑥ | クラウド事業者が立入監査に応じない。また、立入監査の代替として提示される第三者認証の結果についても、監査項目がクラウド事業者と監査法人との間で話し合われた標準的なものとなっており、委託元金融機関側がチェックしてほしい事項をあまり織り込む余地がない。 |
| ⑦ | クラウドの SLA における可用性基準は 24 時間 365 日稼働を保証していないので、基幹勘定系システムに利用することができない。 |

▽ 一般的な課題

| | |
|---|---|
| ⑧ | 個人情報保護法上、クラウド環境に存在するパーソナルデータ（またはこれを暗号化・切片化した情報）の扱いが判然としない。 |
| ⑨ | 個人情報を含む重要データが内外の公権力によって閲覧される可能性がある。 |
| ⑩ | クラウド事業者側の情報開示姿勢が不十分。テロ対策や知的財産権の保護を名目に、所定の事項以外の情報開示に応じない先も少なくない。 |
| ⑪ | 個人情報を含むデータ管理のクラウド化を検討した際、データの機密性が適切に担保されるかをチェックする観点から、暗号化の具体的仕様やアクセスコントロールの具体的な内容を照会したところ、回答を拒否された。 |
| ⑫ | ドキュメントの多くが英語である。また、照会・要望事項に対する回答の権限等がクラウド事業者の日本法人にないケースが多く、何かトラブルが生じた際にきちんと対応してくれるか不安。 |

【図表C】パブリッククラウドの利用事例

―― 本検討会委員から提供された情報をもとに作成。

（国内）

①営業支援システム

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行 | S | 法人 CRM | 取引先情報<br>案件情報<br>活動記録 | | ○ | ○ | ○ | |
| 2 | 銀行 | S | リテール CRM | 顧客情報<br>問合せ情報<br>商品申込情報 | ○ | ○ | | ○ | |
| 3 | 証券 | S | 機関投資家向け<br>グローバル CRM | 顧客情報<br>折衝記録 | ○ | ○ | | | 顧客サービスの向上 |
| 4 | 銀行 | S | 法人営業コンプライアンス管理 | 取引先情報<br>折衝記録 | | ○ | | | コンプライアンス強化 |
| 5 | 証券 | S | 富裕層顧客向け営業管理 | 顧客情報<br>案件情報<br>活動情報 | | | ○ | | 営業力強化<br>カスタマイズ柔軟性 |
| 6 | 損保 | P | 代理店経営管理 | 代理店経営情報<br>募集人情報 | | | | ○ | ペーパーレス |
| 7 | 生保 | P | 職域見込み客統合DB、法人職域向けの対面・Web チャネルを活用した新規顧客開拓 | 顧客情報 | ○ | | | ○ | |
| 8 | 生保 | S<br>P | 顧客管理、法人営業支援等 | 顧客情報等 | | ○ | | | 非システム化領域のシステム化による生産性・セキュリティの向上 |
| 9 | カード | P | 提携カード申込<br>ポータルサイト構築 | 顧客情報 | | ○ | | | |

## ②コンタクトセンター、ヘルプデスク

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行 | S | コンタクトセンター業務 | 顧客情報<br>問合せ情報 | | ○ | | ○ | |
| 2 | 銀行 | S | コールセンター業務 | 顧客応対履歴<br>顧客情報 | ○ | ○ | ○ | | |
| 3 | 生保 | S | アウトバウンド・コールセンター業務 | 顧客情報 | ○ | | | ○ | 見込み顧客DBの統合とアウトバウンド・コールセンターとの情報連携基盤への活用 |
| 4 | 損保 | S<br>P | コールセンター、営業活動管理、販売支援バックオフィス等 | コンタクト履歴、資料請求情報、電話ログ等 | ○ | ○ | | | ITスタッフの本業への集中 |
| 5 | 損保 | S | 代理店システムヘルプデスク | 代理店情報<br>募集人情報 | ○ | ○ | | | |

## ③社内情報共有システム

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行 | S | 行内SNS | SNS 上のコメント | | | ○ | | 行内交流の活性化 |
| 2 | 銀行 | I | 情報共有システム | n.a. | ○ | ○ | | | 災害対策 |
| 3 | 証券 | S | 企業内SNS | （顧客情報は出さない） | | | | ○ | |
| 4 | 証券 | S | 社内案件管理、障害管理 | 社員情報、社内規定、<br>案件情報、障害管理、各種問合せ情報 | ○ | | | | 社内コミュニケーションの活性化 |
| 5 | 損保 | P | 社内情報共有、各種申請ワークフロー、スケジュール等 | 社員情報、各種ドキュメント、顧客情報 | ○ | ○ | | | セキュリティ強化 |
| 6 | 損保 | S | メール、カレンダー | メールデータ、行動予定 | ○ | | | | ITスタッフの本業への集中 |

## ④その他

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行 | I | ワークフローシステム、ドキュメント管理、統合監視、キャンペーンサイト等 | n.a. | ○ | ○ | | ○ | 約 37%のコスト削減 |
| 2 | 銀行 | P | 投資信託の申込管理<br>銀行間での情報共有 | 顧客情報<br>商品情報 | | ○ | | | 提携先金融機関の開拓 |
| 3 | 銀行 | S | 無担保ローン審査申込 | 顧客情報<br>与信情報（他社借入件数・残高） | | ○ | | ○ | 申込管理サイトの早期立上げ |
| 4 | 銀行 | S | ソーシャルリスニング | SNS、ブログ | | | ○ | | 自社商品・サービスの評価確認、プロモーション効果測定、商品企画力向上 |
| 5 | 銀行 | P | IT ベンダーとの間の予算管理 | 案件情報<br>予算情報 | | | ○ | ○ | Excel ベースの管理からの脱却<br>情報共有の効率化 |
| 6 | 銀行 | S | 市場系統合ソリューション | n.a. | ○ | ○ | ○ | | セキュリティ確保<br>BCP 対策 |
| 7 | 銀行 | P | オペレーショナルリスクの損失事象管理<br>カテゴリー別の集計 | 事務リスク、システムリスク、訴訟リスク等のオペリスク情報 | ○ | ○ | | | 既存システム（オンプレミス）からのコスト削減 |
| 8 | 生保 | I | リスク計算システム | n.a. | ○ | ○ | | | 最適なシステム構成の容易な検証 |
| 9 | 銀行 | I | 投信情報提供システム | n.a. | ○ | ○ | | | アプリ開発含め2カ月でリリース |
| 10 | 証券 | I | 株価配信システム | n.a. | ○ | ○ | ○ | | |
| 11 | 証券 | I | Web サイトの負荷分散及び動画配信 | n.a. | | ○ | | | 2日で構築が完了 |
| 12 | 生保 | P | 公開 Web サーバー | 企業情報<br>商品情報等 | ○ | | | | セキュリティ強化<br>災害対策 |
| 13 | 生保 | S | 不動産管理 | n.a. | ○ | | | ○ | |

④その他（続き）

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 14 | 銀行 | P | システム部門のプロジェクト・予算管理 | プロジェクト情報、各種ドキュメント | ○ | ○ | | | |
| 15 | 銀行 | P | 入退室管理、部内業務支援 | 行員情報、投資案件稟議情報 | | | | ○ | 開発生産性、ペーパーレス |
| 16 | 保険 | S<br>P | 新卒採用管理、社用車管理、資産管理 | 顧客情報を含む各種情報 | | ○ | | ○ | セキュリティ向上 |
| 17 | 損保 | S | 開発環境サービス | n.a. | ○ | ○ | | | 必要に応じた開発環境の整備、プロジェクト内の情報共有等 |

（海外）

## ①営業支援システム

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行（欧州） | I | フロントオフィス CRM サービスのバックアップ・リカバリーソリューション | CRM 上情報等 | | ○ | | | 堅牢なセキュリティ確保<br>ビジネス継続性確保 |
| 2 | 銀行（欧州） | I | BtoB 取引支援用基盤ソーシャル機能を擁し新規取引先の開拓やビジネス推進を支援 | 顧客情報<br>取引情報 | ○ | ○ | | | 堅牢なセキュリティ<br>24 時間 365 日の可用性、パフォーマンス確保 |
| 3 | 銀行（北米） | S | ビジネスプロセス管理 | ホールセールバンキング・プロセスに関するデータ類 | | | | ○ | ビジネスプロセスの効率化（目標値：10%増加/1年～2年内） |
| 4 | 銀行（北米） | SP | 顧客管理、情報共有、案件転送追跡等 | 顧客情報<br>社員情報<br>企業情報 | | ○ | | ○ | コンプライアンスやセキュリティをカバーしたうえでの、営業活動のレベルアップ<br>圧倒的なアプリのリリーススピード<br>リード&リファーラル管理による顧客獲得率の向上<br>マネジメントレベルの効率化<br>セキュリティレベルの確保と向上 |
| 5 | 銀行（北米） | SP | ソーシャルコミュニケーションの監視／管理 | 顧客情報 | | | ○ | ○ | ソーシャルバンキングハブの確立<br>リアルタイムの応答 |
| 6 | 銀行（アジア） | SP | マルチチャネルサービス<br>営業とサービスの融合（クロスセル・アップセル） | 顧客情報<br>社員情報 | | | ○ | | 収益成長への貢献<br>先進的 CRM の活用<br>スマホバンキングの推進<br>資産管理の強化 |
| 7 | 銀行（豪州） | I | 自社の持つ３割以上のアプリケーション | n.a. | ○ | | | | |
| 8 | 銀行（北米） | P | 融資オリジネーション | 顧客情報<br>社員情報<br>企業情報 | | | | ○ | 業界平均の4倍のスピードで契約締結<br>中小企業、リテールにも事業拡大 |

## ①営業支援システム（続き）

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 9 | 保険（北米） | S P | 統合ポータル<br>顧客のソーシャル活動追跡 | 顧客情報<br>企業情報 | | | ○ | | 独立系アドバイザー1万人に向けた統合ポータルを実現 |
| 10 | 銀行（北米） | S P | オンライン顧客の動向分析 | 顧客情報<br>企業情報 | | | | ○ | オファー・リード・商品の連携を実現<br>事業部門を跨るエンドツーエンドの総合プロセスの提供 |
| 11 | 銀行（北米） | S P | CRM | 顧客情報<br>企業情報 | | | ○ | ○ | 営業手法の標準化<br>コアシステムとの完全連携 |
| 12 | 銀行（北米） | S P | CRM<br>エンドツーエンド、顧客中心のバンキングプラットフォーム | 顧客情報<br>企業情報 | | ○ | | | フロントオフィス改革を 10 カ月で達成<br>1時間かかっていた口座開設が 10 分で完了 |
| 13 | 銀行（豪州） | S P | 電話と Web 収集による情報のクラウド展開 | 顧客情報<br>企業情報 | ○ | | ○ | | 複数地域からのアクセス<br>コスト削減<br>法令準拠 |
| 14 | 銀行（北米） | S P | 住宅ローン | 顧客情報 | | | | ○ | 業務の効率化<br>顧客満足度の向上<br>見込み客の開拓 |
| 15 | 銀行（北米） | S P | 統合顧客管理（ホールセール）、ソーシャルコミュニケーション、ソーシャルマーケティング | （顧客情報）<br>社員情報<br>企業情報<br>ソーシャル情報 | | | ○ | | マルチチャネル及びソーシャルによる常に顧客とつながることでの顧客サービスの向上<br>スピードと変化への対応 |
| 16 | 保険（欧州） | S P | 顧客管理<br>代理店管理<br>社内コミュニケーション | 顧客情報<br>社員情報<br>企業情報 | | | | ○ | より良い形で顧客とつながる仕組みの構築、iPad の全面活用、顧客サービスの向上、社内コミュニケーションの円滑化 |
| 17 | 証券（北米） | S P | 投資顧問管理<br>顧客管理<br>モバイル | 投資顧問先情報<br>顧客情報<br>企業情報 | | | ○ | ○ | 投資顧問を通じた顧客サービスの一元化<br>モバイル利用による顧客サービス |
| 18 | 生保（北米） | I | 保険購入申請システム | 個人情報 | ○ | | | | GLB 法や PCI DSS などの規制やセキュリティを満たしつつ、クラウド上にシステムを構築 |

## ②コンタクトセンター、ヘルプデスク

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行（米国） | I | サービスデスクの分析ソリューション | サービスデスクのチケット上の情報 | | ○ | | ○ | コール量及びインシデントチケットの削減、エンドユーザーによるセルフヘルプ能力の向上 |
| 2 | 銀行（北米） | SP | 統合カスタマー・ポータルによる照会窓口の一元化<br>住宅ローンのポートフォリオ管理 | 顧客情報<br>法規制情報<br>企業情報 | | ○ | | ○ | 17 種類のシステムを一元化<br>基幹社員2万人の業務の効率化<br>スムーズな法規制コンプライアンスの実現<br>120 日間での導入 |
| 3 | 銀行（北米） | S | CRM<br>コールセンター | 顧客情報<br>社員情報<br>企業情報 | ○ | | ○ | | 顧客情報の一元化と共有化による顧客サービス、リードから契約完了及び次のビジネスまでサイクリックにフォローできる仕組みの構築(営業プロセスの共通化) |

## ③その他

| 業態 | | SaaS PaaS IaaS 区分 | 業務内容 | クラウド上のデータ種類 | 導入効果 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | コスト削減 | 早期導入 | 利便性・機能向上 | 業務効率化 | 備考 |
| 1 | 銀行（豪州） | I | ミッションクリティカルなシステムも含めた 2,000 以上のアプリケーションの移行 | n.a. | | ○ | ○ | | |
| 2 | 銀行（豪州） | I | Web サイトの再構築 | n.a. | ○ | | | | 60%以上のコスト削減 |
| 3 | 銀行（欧州） | I | リスクシミュレーションシステム | n.a. | ○ | | | ○ | 計算時間短縮（23 時間から 20 分）<br>柔軟なリソース利用<br>サーバー購入不要 |

【図表D】『FISC 安全対策基準』(第8版追補)におけるクラウドサービスの取扱い

【運 108】クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。

1. クラウドサービスを利用するにあたっては、外部委託管理の考え方に準じて適切なリスク管理が必要である。

2. 管理すべき事項としては、以下のようなものがある。

(1) クラウドサービスを利用する場合の目的や範囲等の明確化【運 87】

(2) クラウド事業者の選定手続きの明確化 【運 87-1】

(3) 委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結 【運 88】

契約には、クラウド事業者との間の管理境界や責任分界点に関する取決めを盛込むこと。

取り決めるべき事項としては、例えば以下のようなものがある。

①セキュリティ管理方法及び体制【運 1、運 3】

②システム管理体制、データ管理体制、ネットワーク管理体制【運 4～運 6】

③障害時・災害時のマニュアル整備、復旧手順、及び教育・訓練【運 15、運 63、運 83】

④クラウドサービスを利用するためのデータのバックアップ【運 27】

⑤クラウドサービスの利用を中止または終了する場合のデータ消去【運 75】(注)

また、必要に応じて、「サービスを利用するための契約」とは別に「リスク管理に関する契約」を締結することも考えられる。

(注) クラウドサービスの場合、各システムリソースはクラウド事業者の資産であることが一般的であり、金融機関等が自身でデータを消去することが困難な場合も想定される。その場合、データ消去はクラウド事業者が実行し、その証明書等を受領することも考えられる。

(4)クラウド事業者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のリスク評価。

評価すべきリスクとしては、例えば以下のようなものがある。

①現地の各種法制や裁判制度の把握と分析

②現地での活動資格を有する弁護士の確保

③地理不案内な遠隔地での打合せや出廷などに伴う経済的、人的負担

④上記すべてについての外国語での対応

等

3. 利用しているクラウドサービスについて、有効性、効率性、信頼性、遵守性、及び安全性の面から把握、評価するため、システム監査を実施することが必要である。

システム監査については【運 90、運 91】を参照のこと。

4. 本基準項目で参照していない、設備基準や技術基準、及び外部委託管理以外の運用基準についても、必要に応じて参照すること。

5. 参照している各基準に「委託契約」という文言がある場合は、「利用契約」や「利用規約」等の「サービスを利用するための契約」に読み替えて参照のこと。

【図表E】金融庁監督指針における外部委託の定義

銀行が、その業務を第三者に委託すること（以下「外部委託」という。）は、経営の効率化を図ることにとどまらず、より専門性を有する者に業務を委託することで、多様な顧客ニーズへの対応や急速な技術革新を踏まえた迅速な対応等を図ることも期待できる。しかしながら、銀行が外部委託を行う場合には、顧客を保護するとともに、外部委託に伴う様々なリスクを適切に管理するなど業務の健全かつ適切な運営を確保することが求められることから法令により、銀行は委託業務の的確な遂行を確保するための措置を講じなければならないとされている（法第 12 条の2第2項、施行規則第 13 条6の8）。

＜*中略*＞

（注1）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。）。

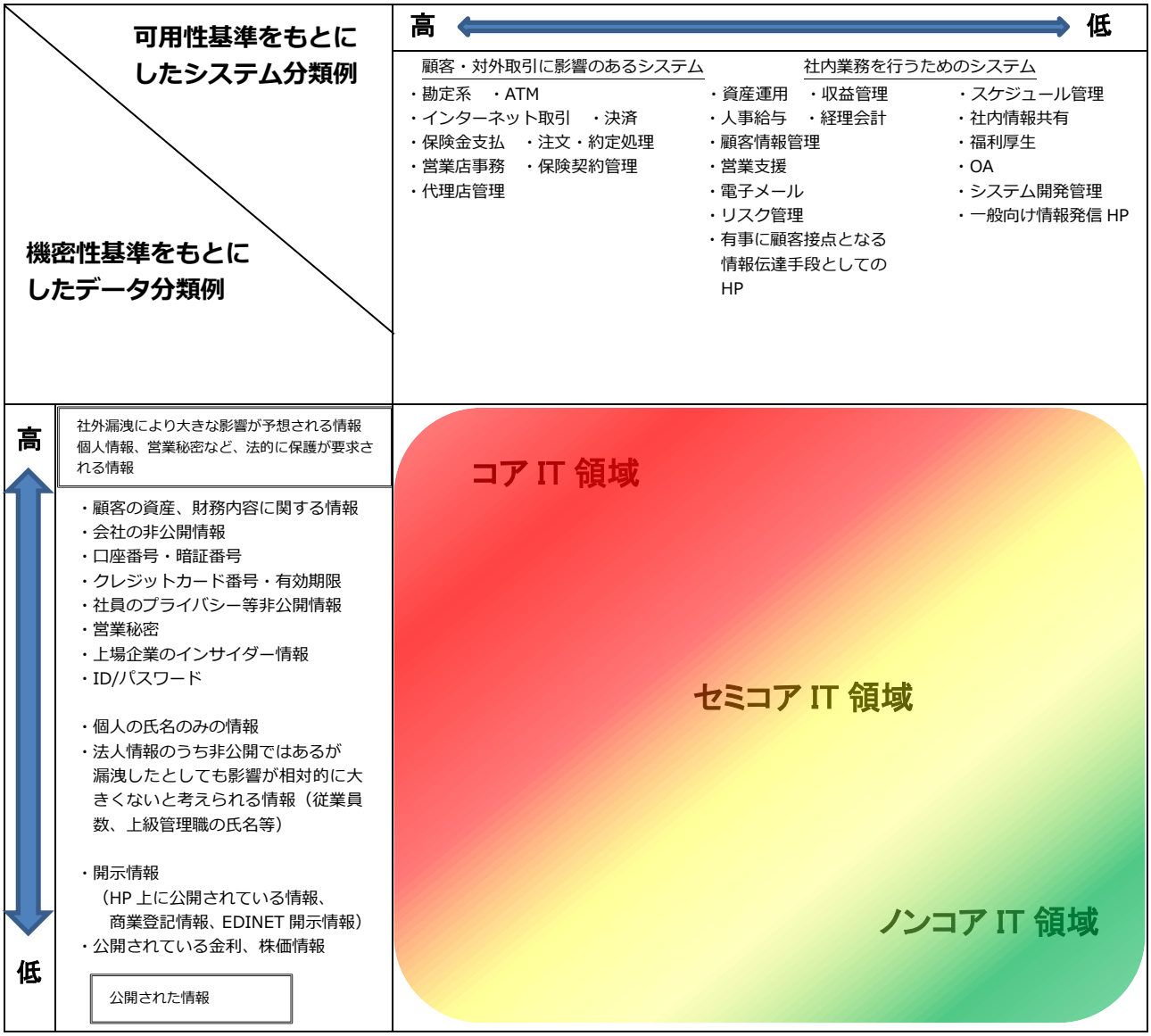
＜*以下略*＞

【図表F】金融機関のクラウド利用において考慮すべきリスク

| No | 分類 | リスク | 内容 |
|---|---|---|---|
| ① | 法制度的な観点でのリスク | 当局の他ユーザーに対する通信傍受、強制執行による影響 | ・万一、他ユーザーに対する強制執行が行われた場合、自社データが格納されたハードウェアの現状変更が禁止されたり、押収されたりすることで、自社のデータ処理続行に支障が生じたり、自社データの内容が当局等に知られたりする可能性がある。<br>・同じく、国内外の公権力が、他ユーザーに対する通信傍受、データ閲覧を行うためのオペレーションを行った際に、自社のデータ処理に係る情報も傍受等の対象になる可能性がある。 |
| ② | | 委託元金融機関による立入監査・本邦当局による検査活動への支障 | ・旅費や手間等の関係から立入監査・検査が行いにくい。<br>・外国人の委託者や外国監督当局の監査・検査実施が困難な場合が生じる可能性がある。 |
| ③ | | 法制度の違いによる影響 | ・プライバシー保護の要請が国（法域）によって異なることに伴い、トラブルが生じた場合の対応や個人データの移転に支障が生ずる可能性がある。<br>・複数の国（法域）で分散処理を行う場合、準拠法が判然としないことがあり得る（プライバシー法制や金融監督法制は強行法規なので、契約で準拠法を縛ることが難しい場合がある）。この場合、法的リスクを回避するため、規制が一番強い国（法域）の法制度を念頭に置いた対応を余儀なくされる。 |
| ④ | | 外国公権力による諜報・データ閲覧 | ・テロ防止や治安維持・脱税防止の観点から、外国政府が自らの法域内に所在する通信回線の傍受を行ったり、データを閲覧したりする可能性がある。 |
| ⑤ | 技術的な観点でのリスク | 外部からの攻撃による影響 | ・データセンター設備、プロセッサー、ストレージ及びネットワークは複数のユーザー間で共有されるため、共有されるインフラを使用する他ユーザーに対する攻撃の影響を受ける可能性がある。 |
| ⑥ | | 他ユーザーの不適切な行動による影響 | ・システムを共有する他ユーザーによる不正・操作ミスにより、自社がその影響を受ける可能性がある。 |
| ⑦ | | データの物理的消去が困難なことによる影響 | ・サービス終了時にハードウェアの物理的な破壊・消磁を通じたデータの完全消去が困難なため、残存したデータが漏洩するリスクがある。 |
| ⑧ | | 伝送路からのデータ漏洩 | ・オンプレミスの環境と異なり、ネットワークでのデータ伝送をベースとした仕組みであるため、データ伝送中のデータ漏洩リスクがその分大きい。 |
| ⑨ | | 外部からの探査の容易性 | ・システム構成の多くの部分がネットワーク上に存在することになるため、専門技術を用いた外部からの探査が比較的容易で、外部者にシステム構成の全貌を把握されやすい。 |
| ⑩ | | ネットワークが途絶した場合の影響 | ・自社ビルでホスティングをしている場合と異なり、ネットワークが途絶した場合にはサービスが受けられなくなる。 |

| No | 分類 | リスク | 内容 |
|---|---|---|---|
| ⑪ | 運用的な観点でのリスク | リアルタイム性、可用性への懸念 | ・他ユーザーのトラフィックが高まった場合、自ユーザー分の処理に係るリソースが不足することにより、レスポンスの悪化やシステムの停止につながる可能性があり、求められるサービスレベルが保証されない懸念がある。 |
| ⑫ | | 外部者によるデータセンター立入による影響 | ・他社の立入監査や、監督当局の検査を行う時期が、自社またはその監督当局が監査・検査を行う時期と重なる場合、当該監査・検査実施に支障をきたす可能性がある。<br>・他社による立入監査により何らかのトラブルが生じた場合、自社の業務に影響が生ずる可能性がある。 |
| ⑬ | | クラウド事業者跨ぎ処理の不調 | ・各クラウド事業者の所掌範囲を跨ぐ業務処理について、要件不一致・結合テスト不足等から処理がうまくいかない障害が発生する可能性がある。 |
| ⑭ | | インシデント対応の不調 | ・インシデントが発生した場合に、各クラウド事業者が責任の擦り付け合い等を行い、状況把握や復旧に支障が生ずる可能性がある。 |
| ⑮ | | リスク管理上必要になる事項の可視化が困難 | ・新技術を使用しているため、クラウド事業者側が情報開示に消極的になる可能性がある。<br>・リソースが冗長化、分散化されることにより、システム構造が複雑化している面がある。 |
| ⑯ | | ベンダーロックイン | ・サービス終了時のデータやシステムの円滑な引継ぎに対する配慮が十分でないケースがある。 |
| ⑰ | ガバナンスの観点でのリスク | 再委託先での不適切な統制環境 | ・クラウド事業者の再委託先は、ユーザーと直接の契約関係にないことから、ユーザーから直接コントロールを行い難い面がある。この結果、再委託先において十分な統制環境が確保されない可能性がある。 |
| ⑱ | | リスク管理に関する個別ニーズへの対応困難 | ・クラウド事業者は、コスト節約や機動的なサービス開始を重視するため、標準化されたものより踏み込んだユーザーサポートを行うことに消極的な場合がある。この結果、ユーザーによるリスク管理上必要な情報の開示やインシデント対応が十分に行われない可能性がある。 |
| ⑲ | | リスク管理面の仕様制約の影響 | ・クラウドサービスによっては、金融界の関心が高い「情報漏洩リスク対策」への配慮が十分でないこともある。 |

【図表G】重要度からみたシステム／データ分類例



## 【図表H】リスク管理策の一覧（例）

<table>
<tr><th colspan="2">リスク管理項目</th><th>基準<br>（注）</th><th colspan="3">厳格な管理 ←――――――――――――――――――――――→ 簡易な管理</th></tr>
<tr><td rowspan="2">利用検討時</td><td>事業者選定</td><td>総合判断</td><td>・公開情報に加え、クラウド事業者に対し、非公開情報の開示を求めリスク管理の状況等を評価</td><td>・公開情報に加え、当該クラウド事業者に対する評判や実績を評価</td><td>・主に公開情報をもとに評価</td></tr>
<tr><td>データの所在</td><td>機密性</td><td>・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）の把握が必要<br>・インシデント発生時に立入が必要となる場面では必然的に所在地の把握が必要</td><td colspan="2">・重要なデータの保管・処理を扱わない場合、データ所在の特定は必要としない</td></tr>
<tr><td rowspan="5">契約締結時</td><td>サービスレベル</td><td>可用性</td><td>・リスク管理に必要な事項を業務委託契約、SLA/SLO に盛り込む<br>・自金融機関のセキュリティポリシーに合わせ、クラウド事業者が提示する標準的約款をカスタマイズ</td><td colspan="2">・クラウド事業者が提示する標準的約款のカスタマイズは必須ではない</td></tr>
<tr><td>情報開示</td><td>総合判断</td><td>・自金融機関のセキュリティポリシーに合わせ、クラウド事業者が提示する標準的な情報開示内容に付加した内容の開示を求める<br>・リスク管理に必要な範囲でアーキテクチャ仕様に関する情報開示も求める</td><td colspan="2">・クラウド事業者が提示する標準的な情報開示内容以上の付加的な内容の情報開示を求めることは必須ではない</td></tr>
<tr><td>複数先への委託</td><td>総合判断</td><td>・メインコントラクターの明確化が必要</td><td>・メインコントラクターの明確化が望ましい</td><td>・メインコントラクターの明確化は必須としない</td></tr>
<tr><td rowspan="2">再委託先管理</td><td rowspan="2">総合判断</td><td>・厳格な事前審査・モニタリングが必要</td><td colspan="2">・重要でない業務の再委託の場合は、厳格な事前審査は必須ではない<br>・必要に応じた再委託先のチェック、モニタリング</td></tr>
<tr><td colspan="3">・クラウド事業者側での事前審査の方が実効的である場合には、クラウド事業者側の審査で代替することも可能<br>（特に重要な業務を再委託する場合は、金融機関自らによる事前審査が必要）</td></tr>
<tr><td rowspan="2">運用時</td><td>データ暗号化等</td><td>機密性</td><td>・機密性の高い個人データ等については、暗号化等による、蓄積・伝送データの保護策は必要<br>・暗号鍵は金融機関にて保管し、管理することが望ましい</td><td>・個人データ以外の比較的機密性の高いデータについては、暗号化等による蓄積・伝送データの保護策の策定が望ましい</td><td>・重要データを扱わない場合には暗号化等による保護を必要としない</td></tr>
<tr><td>記憶装置等の障害・交換</td><td>機密性</td><td>・記憶媒体上のデータの物理的・論理的消去<br>・施設外に出る前に復元不可能な状態にすることを契約書または SLA 上に明文化が必要</td><td colspan="2">・機密性の高い個人データ等の重要データを扱わない場合、物理的・論理的消去は不要</td></tr>
<tr><td rowspan="2">契約終了時</td><td>データ消去</td><td>機密性</td><td>・機密性の高い個人情報等の重要データについて、確実な物理的消去、もしくは復元不可能な論理的消去を実施<br>・消去証明書の発行が望ましいが、契約で消去を明記し、第三者監査によりその有効性が確認できる場合には代替としうる</td><td colspan="2">・機密性の高い個人データ等の重要データを扱わない場合、物理的・論理的消去は不要<br>・データ消去の証明書も不要</td></tr>
<tr><td>ベンダーロックイン</td><td>総合判断</td><td>・新委託先もしくは社内システムに移行すべきデータの抽出と協力義務を求める</td><td>・移行のためのデータ抽出方法が存在することを確認<br>・作業は委託元金融機関が実施</td><td>・あらかじめ代替となり得るクラウド事業者を準備</td></tr>
<tr><td colspan="2">委託元金融機関による立入監査・モニタリング</td><td>総合判断</td><td>・委託業務の管理の適切性を検証するため、委託元金融機関の立入監査権を業務委託契約で明文化<br>・合意のもと、限定的な運用の内容を書面にて明記</td><td>・委託元金融機関の立入監査権を業務委託契約で明文化<br>・第三者認証の結果を活用し、金融機関のリスクプロファイルを加味して、立入監査等の代替とすることも可能</td><td>・立入監査権の明文化は必須ではない<br>・第三者認証の結果やセキュリティホワイトペーパーをもって立入監査等の代替とする</td></tr>
<tr><td colspan="2">委託元金融機関によるクラウド事業者施設への立入</td><td>総合判断</td><td>・インシデント発生時の立入調査は必須<br>・クラウド事業者の経営不安発生時には、施設に立ち入りデータ等の保全を行う必要</td><td>・インシデント発生時に解析に必要な証跡情報を速やかに提出してもらう、もしくは必要な証跡を抽出するツールを準備してもらう<br>・クラウド事業者の経営不安発生時または上記の実現が不可能な場合には、立入等によりデータの保全を行う必要がある</td><td>・立入調査、経営不安時のデータ保全は必須ではない</td></tr>
<tr><td colspan="2">第三者監査</td><td>総合判断</td><td>・金融機関主導の監査が必要<br>・「検証項目」・「検証の担い手」・「検証の機動性」について所定の条件を満たした第三者監査を行う</td><td>・委託元金融機関のリスクプロファイルに照らし、検証内容の十分な、第三者認証を活用することも可能</td><td>・第三者認証やセキュリティホワイトペーパー等で代替することも可能</td></tr>
</table>

（注）各々のリスク管理項目ごとに適切なリスク管理策のレベルを決めていく際に考慮すべき主たる管理軸の例を示している。
可用性：主として可用性の高低によってリスク度を判断するもの
機密性：主として機密性の高低によってリスク度を判断するもの
総合判断：可用性、機密性の両方を総合的に判断するもの

【図表I】機密性の高いデータ（例）

| 区分 | データ例 |
| --- | --- |
| 個人情報 | ・氏名・生年月日・性別・住所<br>・当該個人の信用に関わる情報<br>・当該個人の病歴や宗教・本籍地などの「機微情報」<br>・口座番号･暗証番号、クレジットカード番号・有効期限、取引データ |
| 法人情報 | ・当該法人の信用度に関わる情報<br>・上場企業等に関するインサイダー情報<br>（注）法人の名称・資本金等登記情報を閲覧すれば入手できる情報のみの場合は、「公開情報」として扱う。 |
| 当該金融機関の情報 | ・外部に露見した場合、当該金融機関の信認に影響が及び得る非公開情報 |
| 公的機関等から守秘を前提に渡された情報 | ・外部に露見した場合、公益を損なう可能性がある情報（当局検査結果・反社情報等） |

【図表J】金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針

Ⅲ. 金融分野における個人情報保護に関するガイドライン第 12 条に定める「委託先の監督」について

金融分野における個人情報取扱事業者は、ガイドライン第 12 条第3項に基づき、個人データを適正に取扱っていると認められる者を選定し、個人データの取り扱いを委託するとともに、委託先における当該個人データに対する安全管理措置の実施を確保しなければならない。

（個人データ保護に関する委託先選定の基準）

5－1 金融分野における個人情報取扱事業者は、個人データの取り扱いを委託する場合には、ガイドライン第 12 条第3項①に基づき、次に掲げる事項を委託先選定の基準として定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直さなければならない。

① 委託先における個人データの安全管理に係る基本方針・取扱規程等の整備
② 委託先における個人データの安全管理に係る実施体制の整備
③ 実績等に基づく委託先の個人データ安全管理上の信用度
④ 委託先の経営の健全性

5－1－1 委託先選定の基準においては、「委託先における個人データの安全管理に係る基本方針・取扱規程等の整備」として、次に掲げる事項を定めなければならない。

① 委託先における個人データの安全管理に係る基本方針の整備
② 委託先における個人データの安全管理に係る取扱規程の整備
③ 委託先における個人データの取扱状況の点検及び監査に係る規程の整備
④ 委託先における外部委託に係る規程の整備

5－1－2 委託先選定の基準においては、「委託先における個人データの安全管理に係る実施体制の整備」として、Ⅰ（2）1）の組織的安全管理措置、同2）の人的安全管理措置及び同3）の技術的安全管理措置に記載された事項を定めるとともに、委託先から再委託する場合の再委託先の個人データの安全管理に係る実施体制の整備状況に係る基準を定めなければならない。

5－2 金融分野における個人情報取扱事業者は、5－3に基づき、委託契約後に委託先選定の基準に定める事項の委託先における遵守状況を定期的又は随時に確認するとともに、委託先が当該基準を満たしていない場合には、委託先が当該基準を満たすよう監督しなければならない。

（委託契約において盛り込むべき安全管理に関する内容）

5－3 金融分野における個人情報取扱事業者は、委託契約において、次に掲げる安全管理に関する事項を盛り込まなければならない。

① 委託者の監督・監査・報告徴収に関する権限
② 委託先における個人データの漏えい、盗用、改ざん及び目的外利用の禁止
③ 再委託における条件
④ 漏えい事案等が発生した際の委託先の責任

5－4 金融分野における個人情報取扱事業者は、5－3に基づき、定期的又は随時に委託先における委託契約上の安全管理措置の遵守状況を確認するとともに、当該契約内容が遵守されていない場合には、委託先が当該契約内容を遵守するよう監督しなければならない。また、金融分野における個人情報取扱事業者は、定期的に委託契約に盛り込む安全管理措置を見直さなければならない。