# クラウドコンピューティングと サイバーセキュリティ等に関する 調査報告書

2019年(平成31年)3月31日

pwc

# ■目次

# ■ 1. 調査の概要

## 1.1. 調査の背景と目的

クラウドサービス(以下、「クラウド」)の進化は著しく、システム利用者自身がサーバ等のコンピューティング設備を所有するオンプレミスと比べコスト削減や利便性向上の面の便益が期待されるにとどまらず、多様化・高度化されたテクノロジー利用に欠かせないシステム基盤として、大手金融機関を中心に活用が進み、今後は中小金融機関にも活用が広がることが予想される。

他方、クラウド活用における懸念事項の 1 つとしてセキュリティ面が挙げられる。

これまでクラウドプロバイダー(以下、「クラウド事業者」)は、サイバーセキュリティを含めた様々なセキュリティ対策を進めているが、クラウド利用者に起因するセキュリティインシデントは後を絶たず、報道に取り上げられるケースもある。そのため、クラウドの導入に当たっては、オンプレミスとは異なる、リスクを把握し、適切に管理していく必要がある。

これまで、金融分野では、クラウドの利用は外部委託の一形態と整理されてきているが、契約形態に基づく責任分界やサポート体制など、従来、金融機関がパートナー企業との間で行ってきた IT の外部委託契約とは異なるリスクや考慮点があると考えられる。また、今後はデジタライゼーションの進展によりクラウドの活用が広がり、クラウドに対するサイバー攻撃を含むセキュリティリスクが金融分野の課題となることが懸念されている。

このような背景を踏まえ、本調査では、今後クラウドを導入する中小金融機関向けに、クラウドの活用や適切なリスク管理の在り方の参考とするため、またクラウド導入がどのような変化をもたらし、今後どのようなセキュリティリスクが生じる虞があるか、また当該リスクへの対策やモニタリングの参考とするために、クラウドの活用における現状の取り組みやサイバーセキュリティを含むクラウド活用上の考慮事項を整理する。

## 1.2. 調査期間

2019 年(平成 31 年)2 月 4 日(月)～2019 年(平成 31 年)3 月 15 日(金)

## 1.3. 調査の対象

国内、海外におけるクラウド利用実績のある金融機関、FinTech 事業者およびクラウド事業者

## 1.4. 調査項目

本調査では、以下の項目について調査を行った。

- 国内、海外におけるクラウド利用実績のある金融機関、FinTech 事業者のクラウド活用の概要
- 金融機関がクラウドを活用することで得られる恩恵と活用上の考慮事項
- クラウドの活用におけるサイバーセキュリティ上の考慮事項

## 1.5. 調査手法

本調査では、公表されている文献（インターネットサイトに掲載された情報を含む）の調査のほか、調査対象へのヒアリングやアンケートを実施し、これらの結果を PwC あらた有限責任監査法人が取りまとめ、報告書を作成した。

なお、主なヒアリングおよびアンケートの対象先は以下のとおり。

- 国内の金融機関（FinTech 事業者を含む）
- 海外に本部を置く金融機関（米国、英国、シンガポール）
- 国内外でクラウドを提供している大手クラウド事業者

## 1.6. 調査の前提条件

本調査、および本報告書は、金融庁と PwC あらた有限責任監査法人との間で締結した平成 31 年 2 月 1 日付のアドバイザリー・サービス契約書に基づき実施、作成されたものであり、また、委託元である金融庁担当職員の指示のもとで実施、作成されている。

本報告書は、調査を通じて得られた情報をもとに作成されている。本調査は上記「1.5 調査手法」に記載したとおり、公表されている文献、記事等の閲覧、および本調査テーマに関連のある機関や関係者へのヒアリングおよびアンケートを通じて実施した。そのため、報告書には、調査対象とした文献の作成者や、ヒアリングやアンケートの対象先である個人および組織による私見や経験に基づく内容が含まれている。また、報告書には、本調査を通じて得られた情報をもとに、報告書の作成を担当した当法人執筆者による見解および考察が含まれている。

当法人は、本報告書内に記載されたそれらの内容について如何なる意見表明や証明を行うものではなく、保証を行うものでもない。また、本報告書は上述した調査期間に収集した情報をもとに作成されており、報告書の内容に将来の事象が含まれている場合には、その将来の事象の実現可能性や信頼性を保証するものではない。

# ■ 2. クラウドとは

## 2.1. クラウドの定義と特性

クラウドの定義については、様々な国の標準団体等が公表しているが、我が国では、2018 年 6 月、内閣官房 IT 総合戦略室が公表した「政府情報システムにおけるクラウドサービスの利用に係る基本方針」[1]において以下のように定義されている。

> *「事業者等によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。」*

上記の定義はクラウドの技術的な面が中心となっているが、経営的な観点からクラウドの利点を考えると、アプリケーション、プラットフォーム、インフラストラクチャ等のシステムリソースを短期間で調達できるため、システムの導入までの期間を短縮できるという点が挙げられる。通常、システムを導入する場合は、物理的なシステムリソースを事前に準備する必要がある。クラウドの場合、こうした物理的なリソースはクラウド事業者により既にサービスとして用意されているため、導入までのリードタイムを短縮することができる。

もう一つのクラウド利用の利点はリソースシェアリングである。複数企業がシステムリソースを共同利用することが基本的な考え方となっているため、一般的には、単独でリソースの調達・管理を行うよりコストを抑え安価にシステムを利用することができると言われている。以下に一例を挙げてみる。

通常、システムの設計時は、性能の観点から、CPU、メモリ、ストレージ、ネットワーク等のシステムリソースの見積りが行われる。こうした見積もりは、業務が繁忙となるシステムリソース集中時にも性能要件が確保できるよう検討される。したがって、オンプレミスの場合、リソース集中がない平常時は、所有する IT リソースが性能を十分に発揮することはなく、遊休化するケースがある。クラウドの場合は、基本的に従量課金となるため、繁忙時でも平常時でも金融機関はその時に必要なリソースのみを割り当て、利用することができる。当該金融機関が利用しない遊休リソースは、他のテナント企業（同一のクラウドを利用する他の金融機関や企業等）に開放され利用される。

このように、クラウドはスケールメリットを活かして、複数のテナント企業がリソースを共有することでコスト負担抑えつつ、必要なときに必要なリソースを活用できるサービスモデルである。

[1] https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

## 2.2. クラウドの分類

クラウド事業者は、クラウドを提供するための技術基盤として、仮想化技術を採用している。仮想化技術自体は、システムリソース（CPU、メモリ、ストレージ等）を、物理的な特性・構成にとらわれず、論理的に統合または分割することを可能とするものである。クラウド事業者はこの仮想化技術を最大限活用し、複数のテナント企業が必要とするシステムリソースを最適化して安価に提供している。

クラウドは、こうした仮想化技術を用いて提供されるサービスの内容・種類に応じて、一般的に以下のように分類される。

### 2.2.1. 提供サービスによる分類

図 2-1 クラウドの提供サービスによる分類

| 分類 | 定義 |
|---|---|
| Infrastructure as a Services (IaaS) | 利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。<br>利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能である。 |
| Platform as a Services (PaaS) | IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。<br>利用者は、基本機能等を組み合わせることにより情報システムを構築する。 |
| Software as a Services (SaaS) | 利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能がサービスとして提供されるもの。<br>具体的には、政府外においては、安否確認、ストレスチェック等の業務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等がある。政府内においては、府省共通システムによって提供される諸機能や、政府共通プラットフォーム上で提供されるコミュニケーション系のサービス・業務系のサービスが該当する。 |

※内閣官房 IT 総合戦略室「政府情報システムにおけるクラウドサービスの利用に係る基本方針」[2]を元に PwC あらた作成

[2] https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

### 2.2.2. 共有形態による分類

クラウドは、提供サービスの内容による分類以外に、共有形態方法によっても、以下の通り、3 つのカテゴリーに分類することができる。

図 2-2 共有形態による分類

| 分類 | 定義 |
|---|---|
| パブリッククラウド | 任意の組織で利用可能なクラウドサービスであり、リソースは事業者（クラウドサービス提供者）によって、制御される。 |
| プライベートクラウド | サービス提供元の組織でのみ利用可能なクラウドサービスであり、リソースも自らによって制御する。組織でリソースを確保し、運用を他組織に委託する形態等も含まれる。 |
| オンプレミス | 従来型の構築手法で、アプリケーションごとに個別の動作環境（データセンター、ハードウェア、サーバ等）を準備し、自らコントロールするもの。 |

※内閣官房 IT 総合戦略室「政府情報システムにおけるクラウドサービスの利用に係る基本方針」[3]を元に PwC あらた作成

## 2.3. 利用および導入状況

クラウドの利用は、金融機関においても近年増加傾向にある。総務省が発表した「平成 30 年度版情報通信白書[4]」の金融機関におけるクラウド導入状況のデータによると、下図のとおり、平成 28 年度から平成 29 年度にかけての金融機関全体のクラウド導入率は、37.7%から 44.3%に 6.6 ポイント増加している。

図 2-3 クラウドの金融業態別導入率

| 業態 | 平成 28 年度 | 平成 29 年度 | 増減 |
|---|---|---|---|
| 全体（証券・保険他を含む） | 37.7% | 44.3% | +6.6 ポイント |
| 都銀、信託 | 100.0% | 100.0% | - |
| 地銀 | 76.2% | 81.8% | +5.6 ポイント |
| 第二地銀 | 56.8% | 71.1% | +14.3 ポイント |
| ネット専業他 | 70.0% | 82.0% | +12.0 ポイント |
| 信用金庫 | 15.3% | 20.6% | +5.3 ポイント |
| 信用組合 | 14.6% | 13.1% | -1.5 ポイント |

※総務省「平成 30 年度版情報通信白書」に掲載の日本銀行「IT を活用した金融の高度化に関するワークショップ（第 3 期）」の図表を元に PwC あらた作成

一方、クラウドを活用するにあたっての課題も存在する。例えば、総務省が公表している、「ICT によるイノベーションと新たなエコノミー形成に関する調査研究[5]」では、以下のような点がクラウド活用上の課題だと言われている。

[3] https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

[4] http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/30honpen.pdf

[5] http://www.soumu.go.jp/johotsusintokei/linkdata/h30_02_houkoku.pdf

これらは、クラウドの特性を十分に把握せず、従来のオンプレミスと同じ感覚で安易にクラウドを活用しようとした際の一般的な落とし穴ともいえる。今後クラウドの活用を計画している金融機関では、次章以降で述べるクラウド活用の恩恵、或いは活用上の留意事項等も参考にしつつ、クラウドの特性を把握した上で導入の検討を進めていただきたい。

図 2-4 企業がクラウドを活用するにあたっての課題

| 課題 | 課題が生じる背景 |
|---|---|
| ①セキュリティの担保 | オンプレミスであれば社内ネットワークのみにつながったサーバに重要なデータ を置くことが可能だが、一般的にクラウドはインターネットに直接接続されたサーバ上にデータを置くことになるので、情報漏えいのリスクは高まる。 |
| ②改修コスト・通信コストの増加 | 既存のシステムとクラウドの接続性を担保するために、システム改修にコストがかかる。データやサービスを利用する際に通信が発生することから通信コストが増加する。 |
| ③カスタマイズ性の不足 | クラウド上で提供されているサービスを組み合わせても、必要な社内システムを再現するためのカスタマイズ性が不足している可能性がある。 |

※総務省「ICT によるイノベーションと新たなエコノミー形成に関する調査研究」を元に PwC あらた作成

# ■ 3. クラウドの活用状況

## 3.1. 金融におけるクラウド利用のトレンド

近年のデジタル化の急激な進展により、金融機関を取り巻く環境は大きく変化している。本項では、金融業界におけるクラウド利用のトレンドを捉えるため、金融を取り巻くデジタルマーケットの変化、金融機関におけるクラウド利用および金融機関に対するクラウド事業者の対応の観点に分けて整理した。

### 1) 金融を取り巻くデジタルマーケットの変化

消費者は、スマートフォンなどを通じた即時性の高い、使い易いサービスに慣れてきており、今後、リアルタイム且つ簡便な金融サービスへの期待が更に高まっている。2018 年に公表されたあるデジタルバンキング調査[6]では、銀行顧客の 46%が銀行の支店を全く利用せず、代わりにスマートフォンやタブレット、他のオンラインアプリケーションを使用しているという結果も出ている。人口減少・高齢化の進展、低金利環境の長期化などの要因も加わり、金融機関は従来のビジネスモデルからの変革を迫られている。

また、デジタル化の進展により、顧客データを保有するだけでなく、購買情報等のデジタル化された大規模な情報を分析、活用出来る企業が、市場における優位性を強めており、データによる顧客への理解を武器にマーケットをコントロールできるポジションの獲得を進めている。一方で、国を跨いでやり取りされるこれらのデジタルデータは、個人情報を取り扱う以上、プライバシーの確保がこれまで以上に重視されることとなる。

### 2) 金融機関におけるクラウド利用の変化

金融機関におけるクラウドの利用は急速に広がっており、「大手やネット系金融機関だけでなく中小地域金融機関による活用」、「一部の部門システムでの活用ではなく全社的な IT インフラとしての活用」、「周辺業務領域での活用に加え本業での活用」といったクラウド利用者や活用の範囲・用途も変わりつつある。

### 3) 金融機関に対するクラウド事業者の対応

クラウド事業者も、金融機関の要望を取り込む動きが出ている。ある大手クラウド事業者では、これまで東京圏周辺にのみ設置していたデータセンターに加え、関西圏にもデータセンターを増設し、地理的に十分離れた拠点を国内に設けることで、金融機関の期待する冗長化への対応を行っている。別の大手クラウド事業者では、金融機関向けの契約書を用意し、金融機関が一般に求める内容を標準的に盛り込むことで契約締結しやすいスキームを用意している。加えて、公益財団法人金融情報システムセンター(以下、「FISC」)が定める「金融機関等コンピュータシステムの安全対策基準(第 9 版)(以下、「FISC 安全対策基準」)」への準拠を表明しているクラウド事業者も増えてきている。

[6] https://www.pwc.com/us/en/industries/financial-services/library/digital-banking-consumer-survey.html

## 3.2. 海外金融機関におけるクラウド活用と取り組み状況

本調査では、海外に本部を置く比較的規模の大きな金融機関を対象に、クラウドの活用状況やリスク認識とその対応等についてヒアリングを行った。ここでは、ヒアリングを通じて把握できた内容について述べる。ヒアリングは数社の金融機関を対象とし、IaaS や PaaS のパブリッククラウドを念頭に実施している。

なお、ヒアリングの対象とした金融機関は規模や特性、本店所在地等も異なることから、クラウドへのスタンスは異なる。以下の内容が海外金融機関全体のトレンドを表していない点に留意が必要である。

### 1) 経営陣のクラウド活用に対する期待

海外の大手金融機関では、経営陣がクラウドを以下のように位置付けており、ビジネスを展開していく上で、活用が期待されている。

- 数年前からクラウドのメリットの大きさを認識している。必ずしもコスト削減効果を期待しているわけではなく、スピードや機能性の高さにメリットを感じている。短時間で市場にサービスを投入していくことができる技術であり、活用を推進している。
- システム設備やそのメンテナンスに投資するのではなく、ビジネスへの投資にシフトしていく上でクラウドは戦略的に鍵となる。特にインフラとしての資産を持たなくてよい点、様々な業務を連携させやすい点、機能やサービスが充実している点に優位性があると感じている。

なお、アジアを中心に業務を展開しているリージョナル金融機関では、上記と異なり、経営陣はクラウドの活用に関する明確なスタンスはとっていなかった。

### 2) クラウドの活用状況

上述の通り、海外の大手金融機関ではクラウド活用に対する期待は大きいものの、現時点では IaaS や PaaS が大規模かつ広範に活用されている状況ではなく、クラウドのメリットとデメリットを慎重に検討し、必要な対策を取りながら順次活用範囲の拡大を進めている状況であった。

- 活用は推進しているが、現時点のワークロードは、限定的。レガシーシステムの移行は難易度が高いため、SOE[7]や SOI[8]等の比較的シンプルなシステムから活用または移行を開始している。今後はクラウドネイティブなシステム開発とともに、マイクロサービスアーキテクチャ[9]での開発プロセスの整備や、こうした動きに対応可能な人材の育成に力を入れ、クラウド活用の管理態勢の強化を着実に進める。

---

[7] Systems of Engagement の略称。「繋がりのシステム」で、企業と顧客（ユーザ）をどのように繋いでいくかという点を重視したシステム。

[8] Systems of Insight の略称。SoE 等も含め様々なシステムから得られるデータを用いて顧客（ユーザ）の心理や行動欲求等を分析・考察し、高付加価値な知見を生み出すことを目的とするシステム。

[9] ソフトウェア・アプリケーションを小さく、独立し、疎結合のサービスの組み合わせとして設計する方法。単位が小さくスピーディーに開発が可能になる他、それぞれが 1 つの独立したサービスとして構成されるため、相互に影響なく変更等も可能。

- 本部を中心に活用を拡大しているものの、グローバルで広く活用している状況ではない。本部でも基幹系のような SOR[10]のシステムの移行は現状実施していない。クラウド活用の準備は着実に進めているため、クラウドの機能が充実し、より受入れ可能な範囲が増えてくるのと同時に活用範囲を拡大していくことになる。

またアジアを中心にビジネスを展開しているリージョナル金融機関では、SaaS は活用しているものの、IaaS や PaaS ではクリティカルシステムや顧客データは扱わないとの考えを示した。

### 3) クラウド活用に対する懸念・リスク認識

今回ヒアリング対象とした金融機関では、上記の通りクラウド活用はまだ道半ばの状況であるが、その理由の一部として、以下のようなクラウドに対する懸念やリスク認識が聞かれた。

- 高機密データをクラウド上で扱うにはセキュリティ上の懸念が払拭できていない。一例として、クラウド利用者は仮想マシンを自社のハードウェアのように利用することになるが、実際にはハイパーバイザ[11]による仮想化技術により実現されている。ハイパーバイザは、クラウド事業者がアクセスできる範囲であるほか、多くのテナント企業がハイパーバイザを共有する形になる。こうした構造に技術的な問題はないか懸念を感じている。ただし、こうした懸念に対し大手クラウド事業者が既に研究開発を進めているため、近い将来懸念が払拭される可能性はある。

- クラウド利用者自身の設定ミスにより外部の第三者がクラウド上の情報にアクセスができてしまう事故が多数発生している。こうした設定ミスによるリスクを認識している。

- 可用性についての懸念もある。クラウド事業者が実施するメンテナンス等によるサービス停止は、回避できないため、短時間のダウンタイムも許容できない重要システムをクラウドで運用するのは難易度が高い。

- ベンダーロックインに考慮が必要である。クラウド事業者が規制や要件を満たせなくなった場合に、直ぐにオンプレミスも含む他の環境へ移行できるようイグジットに備えなければならない。

- クラウドを利用する場合の脅威アクターは、いわゆる外部のサイバー攻撃者以外に、「クラウドにアクセスする自社の従業員」、「クラウド事業者の従業員」、「テナントを共有する悪意あるクラウド利用者」の 3 つを考える必要がある。

- クラウド事業者が運営する MarketPlace（オンラインストア）では様々なサードパーティによってクラウド上で活用可能なサービスや仮想マシンの構成イメージが提供されているが、当該 MarketPlace 上には、バックドアが仕掛けられている等、脆弱性を有する構成イメージが存在するリスクがある。

### 4) クラウドを活用する上での取り組み・リスク対応

現状、クラウドの活用を推進している海外の大手金融機関からは、以下のような取り組みが聞かれた。

- クラウドの活用やリスク管理に関するポリシーとスタンダードはグローバルで統一している。策定にあたっては、GDPR やその他各国のプライバシーや金融当局が示している規制、PCIDSS 等多くの公の規制や基準を参考にしている。

---

[10] Systems of Record の略称。「記録のシステム」で内部プロセスのデジタル化によりインプルーブメントを追及する概念。

[11] ハードウェアのシステムリソースを仮想化するためのソフトウェアモジュールの集合体。

- クラウドに関するガバナンスを維持するために、クラウドにフォーカスした定期的な会議体を設け CIO も交えて議論している。またクラウドへ移行するアプリケーションは機密性や可用性の要件を満たせるかを予め評価するとともに、必ず CIO の承認を得た上で移行している。

- クラウドで取り扱う情報の重要度に応じて 3 段階のセキュリティの基準を設定している。最も高機密な情報を扱う場合は、シングルテナントの IaaS を選択したり、ホストベースでのファイアウォールの設置、FISP 140-2 対応の HSM[12]を利用した上でクラウド利用者のオンプレミス環境で暗号鍵を管理する等、様々な強固なセキュリティ対策を実施する。対策を強化することで、クラウドのメリットを一部享受できなくなる部分もあるが、重要度に応じたセキュリティの確保は最優先すべき事項である。

- グローバルレベルで Cloud Center of Excellence（CCoE）のチームを組成している。CCoE は、クラウドに関する技術や最新動向を収集、蓄積し、関連技術の検証を行うほか、クラウドの活用を検討しているビジネス部門に対し、技術的・専門的知見からワンストップでサポートを提供するなど、組織がクラウドを安心安全に使うための中核機能となっている。

- クラウド事業者とは密に連携し、金融機関側の問題意識を伝えている。金融機関が必要と考えているセキュリティ上のコントロールの適用やデータプライバシーに関する各国の規制要件への対応について継続して交渉するようにしている。

- ロックインリスクへの対応としてクラウドに展開するアプリケーションについては、他のクラウドへも移行可能性を高めるため、コンテナ[13]ベースでの設計と開発を取り入れている。

- クラウド環境とオンプレミス環境のセキュリティモニタリングはグローバルで統一したジョイントオペレーションセンター（JOC）でモニタリングしている。なお、JOC では、IT のセキュリティモニタリングのみならず、内部不正や物理的な犯罪、或いは気象や災害、国防関連情報も含めて統合的にモニタリングしている。

- 仮想マシンの管理の自動化を進めている。ソフトウェアに対するセキュリティパッチ適用の自動化や設定値等のコンプライアンスチェックの自動化および一部の修正の自動化を実施している。

[12] 暗号化キーを安全に管理することを目的としたモジュール。通常、強力な認証や物理的な改ざん防止などの保護機能が備わっている。

[13] 仮想化方式の 1 つ。1 つの OS 環境の上に分離した空間を作成し、その分離された空間ごとに異なる OS 環境を実現しアプリケーションを実行できる技術。システム資源の負担は小さく可搬性は高い。

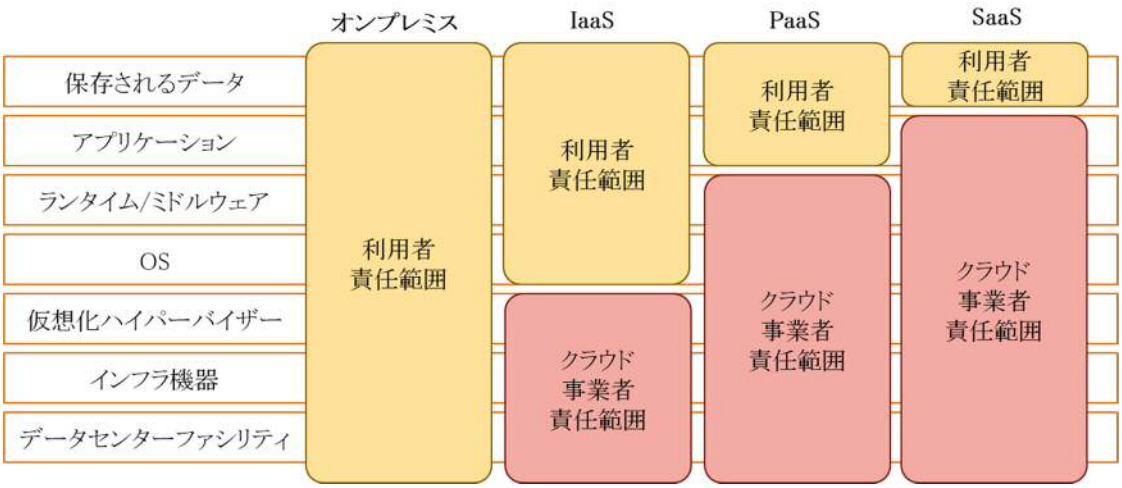
## 3.3. クラウド利用の恩恵

実際にクラウドを活用している国内外の金融機関やクラウド事業者へのヒアリングの結果、クラウド活用の利点として挙げられた主要なものについて以下に述べる。

### 3.3.1. 構成管理や運用保守労力の削減

クラウドの大きな特徴のひとつとして、クラウド利用者とクラウド事業者との責任分界が挙げられる。

図 3-1 クラウドの責任分界




※知見を元に PwC あらた作成

一般に、上図のサービスの中で、より右側のサービスを利用するほど、クラウド事業者の責任範囲と保守運用作業（物理機器のメンテナンス、OS へのパッチ適用、バックアップ作業など）領域は広くなる。言い換えれば、クラウドを利用する金融機関の責任範囲や負担を低減できる。

今回の調査でも、クラウドを積極的に活用している金融機関では、システムをオンプレミスからクラウドに移行することにより、従来の運用・保守偏重の組織体制を改め、人材を IT サービス企画や機能開発等の戦略的な役割にシフトするなどし、IT 人材のポートフォリオの見直しを推進している事例が見られた。

### 3.3.2. システムリソース調達の柔軟性、および調達コストの抑制

クラウドでは、サーバなどのシステムリソースの調達が簡単な操作により数分で可能となる。オンプレミスと比較した時の圧倒的な調達容易性は、システム開発期間を短縮化すると同時に、システム構築時のキャパシティプランニングに大きな変革をもたらしている。

オンプレミスでは、ピーク時の必要リソースを見積りし、そのピーク時に合わせたリソース調達を実施する必要がある。クラウドでは動的にリソースの調達、解放ができるため、過剰かつ保守的な計算によってリソースを事前に確保する必要がなくなり「必要な時に必要なリソース分だけ増強する」という考え方により、サーバ調達のコス

トを抑えられる。例えば、サービスローンチ時には最小限のリソースで構築し、サービスが成長したらリソースを増加させるといった、余剰なコストを発生させない柔軟なアプローチをとることができる。

またシステム開発では、テスト環境の準備も欠かせない。オンプレミスの場合、本番環境と同等規模のテスト環境を用意することはコストの面などから敬遠されることが多く、結果として本番の構成とは異なる環境下でテストするケースが多い。クラウドは、テスト用環境として本番環境と同等のものを必要な時に、迅速に準備することができる。こうした活用の仕方により、テスト環境に係るコストを抑制しつつ、本番同等の環境でテストができ、テスト品質の向上にも寄与できる。

加えて、金融機関のような装置産業では、オンプレミスの場合システムの廃棄コストも相当程度大きくなるが、クラウドの場合は、簡単な操作で廃棄ができるという点で、廃棄コストがかからない特性がある。

このような柔軟なシステムライフサイクルを取れることは、IT を使った実証実験の実施など、新たな IT の活用にチャレンジする後押しとなる。

### 3.3.3. 最新テクノロジーへのリーチ、および、開発スピードの俊敏性

クラウド活用のメリットとして、従量制課金や初期構築費用が不要などの「経済性」がよく挙げられるが、「俊敏性」も活用のメリットである。

あるクラウド事業者は、およそ 1 年の間に、クラウド上で利用できる新機能やサービス・オプションを多数リリースしている。最新テクノロジーを活用した機能もあり、こうした機能を常に利用者に提供し続けるクラウド事業者の取り組みは、新ビジネスの構築や既存ビジネスの改革を進める金融機関にとっても大きなメリットである。例えば、機械学習やブロックチェーンなどに関するサービスを提供しているクラウド事業者もある。

また金融機関は、最新テクノロジーの基礎部分を自ら開発することなく（結果として設計ミスや実装ミスを低減しつつ）、自社独自の機能や商品開発に注力でき、またシステムリリースまでの期間を大幅に短縮することができる。

### 3.3.4. バックアップの利便性、および業務継続性

オンプレミスでは、バックアップシステムを専用に構築し、バックアップスケジュールをディスクのリソースを鑑みながら設計を行う等、時間とコストがかかっていた。クラウド環境では、クラウド側で用意されたバックアップ機能を用いることで時間とコストを抑えたバックアップシステムを構築できる。またオンプレミスではバックアップに必要なストレージを、業容拡大を予測し予め大きな容量を確保する必要があったが、クラウドでは従量課金制により必要なストレージ容量を動的に拡張させながら利用できる。

広域災害を念頭においた遠隔地バックアップにおいても、オンプレミスではデータセンターの確保や構築、専用線の敷設、リモートバックアップ設定等を行う必要があり、それらの構築のためには多くの時間とコスト、必要な IT スキルを持った人材が必要となる。クラウドではクラウド事業者が国内外に展開しているデータセンター群や障害検知・復旧機能を用いて効率よく構築することが可能となっている。また、クラウド特有の従量課金制やリソースのスケーリング機能を活用することで、平常時には DR（Disaster Recovery）サイトを最小リソースで運用し、障害発生に伴う切り替え時に一気に DR サイト側をスケールアップさせる等の仕組みを構築できる。オンプレミスの DR サイトはその固定資産や維持費等の負担が金融機関の重荷となってきたが、クラウド環境の活用はアドバンテージとなる。

また一部の金融機関は、ログの集約・保管の観点からクラウド特有の低価格ストレージを活用することにメリットを見出している。収集したログデータが一定期間を経過すると自動的により安価なストレージへアーカイブされるクラウドの機能を活用しており、磁気テープの代替手段として利用している。磁気テープは、データの取り出し時に労力がかかることが多いため、アーカイブ後の利用はインシデント対応時など限定的であったが、クラウドではコンソール画面の操作で容易に取り出しが可能なことから、利便性やアーカイブデータの活用用途が高まる。

### 3.3.5. セキュリティ機能の提供

「クラウドのセキュリティには不安がある」との意見が聞かれることは、依然として多い。しかしながら、近年、大手クラウド事業者はセキュリティを最重要事項に掲げ、クラウド事業者の責任範囲のセキュリティ対策だけではなく、クラウド利用者がセキュアにクラウドを活用するための取り組みや機能の充実を進めている。

サイバー攻撃は執拗かつ高度化し、金融機関単体の努力や投資では対応が難しい面も出てきている。クラウド事業者はスケールメリットを活かし、自身が提供するクラウドのセキュリティ対策に多くのコストや人材を投入しており、クラウドに対する悪意のある操作や不正な動作を機械学習やデータ分析機能等を活用し継続的にモニタリングする脅威検出サービスを従量課金制でクラウド利用者に提供している事例等もある。

金融機関が独自に十分なセキュリティ機能を保有するには、相応な労力や専門性が必要となることを考えれば、リソースが限られる中小地域金融機関がセキュリティ機能のメリットの点からクラウドを活用するという選択肢も出てくる。クラウド事業者が提供するセキュリティ機能の恩恵を受けつつ、攻めの投資にリソースを注力するといったことも考えられる。

## 3.4. セキュリティインシデント事例

クラウドには魅力的な利点があり、利用が広がっているが、様々なセキュリティインシデントが発生していることも事実である。以下に、今回の調査で把握したセキュリティインシデントの一例を記載する。

| 事例 1 | 設定ミスによりクラウド上のファイルストレージから情報漏えい |
|---|---|
| 概要 | クラウド上のファイルストレージサービスを使用する際、クラウド利用者の管理者が人的ミスをし、ファイルストレージのアクセスに必要な ID 認証を無効（不要）に設定した。 |
| 影響 | インターネットを通じて全世界の誰もが、当該クラウド利用者のファイルストレージ上のファイルを閲覧できる状態となり、情報が漏えいした。漏えいした情報の中には、クラウド利用者の顧客に関する情報のほか、クラウドを操作・管理するためのアカウント認証情報が含まれていた。 |

| 事例 2 | 組織内へのマルウェアが拡散 |
|---|---|
| 概要 | クラウド利用者がクラウド上のファイアウォール設定を誤り、インターネットからの通信を含む全てのトラフィックを受け入れる設定となっていた。この設定に気づいた攻撃者は、クラウド上の仮想サーバに侵入しただけでなく、WAN 回線で接続されているクラウド利用者が所有するオンプレミスのデータセンターにある内部サーバまで侵入に成功した。 |
| 影響 | アカウント管理システムなどの重要なシステムが攻撃され、ランサムウェアなどの様々なマルウェアが複数のシステムに仕掛けられた。クラウド利用者は感染したシステムの再構築を余儀無くされ、一部業務システムを一定期間停止したほか、マルウェア駆除に多額なコストを必要とした。 |

| 事例 3 | 仮想サーバの脆弱性が悪用され、加害者的立場に |
|---|---|
| 概要 | クラウド利用者がクラウド上の仮想サーバの脆弱性に適切に対処していなかったため、攻撃者に不正アクセスされ、仮想サーバ上が DDoS 攻撃のボットネットとなった。 |
| 影響 | ボットネットを構築されたことで、クラウド利用者はサイバー攻撃の加害者となった。加えて、不正な通信を確認したクラウド事業者がそのクラウド利用者に割り当てたグローバル IP の全通信を強制遮断したため、顧客向けの公開システムを通じた取引が出来なくなり、一部のサービス停止を余儀なくされた。 |

| 事例 4 | リソースの不正利用による仮想通貨の不正マイニング |
|---|---|
| 概要 | クラウド利用者が管理していた、仮想サーバ等のリソースを構築することが可能な権限を持ったアカウント情報が漏えいした。 |
| 影響 | アカウント情報を窃取した攻撃者により、クラウド利用者のリソースとしてクラウド上に不正にサーバが構築され、仮想通貨のマイニングに悪用された。マイニングでは多くのクラウド上のリソースが使われたことから、クラウド利用者はクラウド事業者から多額の利用料を請求された。 |

※上記の事例1～4 は、文献調査やヒアリングを通じて得た情報を参考に PwC あらた作成

上記 4 つの事例の共通点は、原因がいずれもクラウド利用者の責任範囲という点である。クラウド利用者の責任範囲については、オンプレミス同様、技術的なセキュリティ施策も含めた適切な管理を求められるため、金融機関はクラウドに関する正しい知見を持った上で、活用を推進していく必要がある。

なお、今回実施した金融機関やクラウド事業者へのインタビューでは、クラウド事業者に起因する、情報漏えいや不正侵入等のインシデント事例は聞かれなかったものの、クラウド事業者に起因するインシデントがないわけではない。

2018 年 12 月、BIS[14]が公表した「FSI Insight on policy implementation No.13 Regulating and supervising the clouds: emerging prudential approaches for insurance companies」[15](以下「FSI Insight No.13」)では、以下の通り、クラウドに対するサイバーリスクは金融当局の特別な懸念事項だと述べられており、サイバー攻撃やクラウド事業者の機能停止によるクラウドの停止が懸念されている。金融機関は、クラウド事業者に起因するサービス停止等のインシデントも想定し、利用のための準備と対応を行う必要がある。

> ***Information security risks related to cloud computing, in particular cyber-risks, are a particular concern to financial sector authorities.*** *Business continuity of financial firms may be impacted by cyber-attacks and outages of a small number of cloud providers, which are not regulated under the same prudential principles as the financial sector. In the past decade, there have been various outages ・・・(中略)・・・. Their clients were affected in various ways, ranging from being unable to access hosted services for between eight hours to five days or even losing recently written data, affecting the business operations of their clients.・・・(後略)・・・*

***クラウドコンピューティングに関連する情報セキュリティリスク、とりわけサイバーリスクは金融当局にとっての特別な懸念事項である。****金融機関の業務継続は、サイバー攻撃やクラウド事業者の機能停止による影響を受けるだろう。彼ら(クラウド事業者)は、金融機関が求められるプルーデンス原則の規制は受けないのだ。この 10 年間、大手クラウド事業者の提供するサービスは、様々な形で機能が停止した。それにより、クラウド利用者は*

[14] Bank for International Settlements:国際決済銀行

[15] https://www.bis.org/fsi/publ/insights13.pdf

*様々な影響を受けており、例えば、8 時間程度の間、或いは長い時は 5 日もの間サービスへアクセスできなくなり、書き込んだデータが喪失し業務に影響するようなことも発生している。・・・(後略)・・・*

※「FSI Insight No.13」の一部を引用の上、PwC あらた仮訳

# ■ 4. クラウド活用にあたって考慮すべきこと

本章では、文献調査やヒアリングを通じて得られた、金融機関がクラウドを活用する上で考慮すべきことについて述べる。その際、2.2.1 章「提供サービスによる分類」や 2.2.2 章「共有形態による分類」で大別した通り、クラウドにはいくつかの分類があるが、サービス分類のうち SaaS は、事業者側が構築したアプリケーション機能を利用する形態であり、クラウド利用者が考慮できる事項も IaaS や PaaS と比べ限定的である等、特性が大きく異なる。また、共有形態では、複数のテナント企業がリソースを共有する形態が最も考慮すべき事項が多くなると考えられる。したがって、本章では、考慮すべき事項をより広範に整理しておく観点から、パブリッククラウドとして活用する IaaS および PaaS に焦点をあてて述べることとする。

## 4.1. FISC「金融機関におけるクラウド利用に関する有識者検討会報告書」との整理

クラウド活用時の考慮事項については、2014 年 11 月、FISC が既に「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、「FISC クラウド報告書」）」を公表し、その中で多くをとりまとめている。ただし、当該報告書では、クラウドを外部委託の一形態と整理した上で、責任分界のうちクラウド事業者側の責任範囲に対し金融機関がどのように外部委託先管理を行うべきかに重点を置いた整理がなされていることから、金融機関がクラウドを活用する上で、自身の責任範囲となる部分についての考慮事項はあまり触れられていない。

したがって本章では、責任分界上、金融機関の責任範囲となる領域について、金融機関自身がどのような考慮をするべきかに焦点を当てることとし、「FISC クラウド報告書」と重複する内容には、原則触れない。調査の時点や視点の違い等から、「FISC クラウド報告書」を補足する事項や、本調査で新たに得られた事項について、国内外金融機関の取り組み事例を交えて述べる。

なお、「FISC クラウド報告書」では、同報告書の Ⅱ 章以降で、クラウド活用上の考慮事項が述べられている。よって、本章で述べる、「FISC クラウド報告書」を補足する考慮事項、または新たな視点から述べる事項が「FISC クラウド報告書」の内容にどう関連するのかを、執筆者の視点から以下の通り整理した。

「本報告書」或いは「FISC クラウド報告書」を参照する際の参考としていただきたい。

図 4-1「FISC クラウド報告書」と本報告書の関係性

| 「FISC クラウド報告書」に記載の項目 | 本報告書で述べる考慮事項 |
|---|---|
| II リスク管理に関する基本的な考え方 | |
| 1. クラウド利用・リスク管理に係るポリシー等の策定 | 4.2.1 クラウド利用に向けた経営陣の関与と組織体制・教育<br>4.2.2 サイバーセキュリティ管理への対応 |
| 2. リスクベースアプローチの適用 | N/A |
| III 具体的なリスク管理策 | |
| 1. リスク管理策 | |
| (1) クラウド利用検討時 | **(新たな視点として報告書に記載した事項)**<br>「FISC クラウド報告書 III-1-(1) クラウド利用検討時」に関連が深い事項として、以下を本報告書固有の考慮事項として記載<br>✓ 4.3.2 セキュリティ要件定義とクラウド提供機能の活用<br>✓ 4.3.3 事前のコスト検証 |
| 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) | 4.3.1 性能要件のフィット&ギャップ<br>4.3.4 サポート体制・条件<br>4.3.5 公的認証・第三者評価・監査 |
| ②データの所在 | N/A |
| (2) クラウドサービス契約締結時 | N/A |
| ①サービスレベルの合意 | N/A |
| ②クラウド事業者からの情報開示 | N/A |
| ③複数のクラウド事業者への委託 | N/A |
| ④再委託管理 | N/A |
| (3) クラウドサービス運用時 | **(新たな視点として報告書に記載した事項)**<br>「FISC クラウド報告書 III-1-(3) クラウドサービス運用時」に関連が深い事項として、以下を本報告書固有の考慮事項として記載<br>✓ 4.4.1 クラウド環境におけるシステム構築<br>✓ 4.4.2 クラウド環境におけるシステム運用<br>✓ 4.4.3 コスト管理<br>✓ 4.4.4 構成管理とセキュリティパッチ管理<br>✓ 4.4.5 脆弱性スキャンとペネトレーションテスト<br>✓ 4.4.7 ネットワーク対策<br>✓ 4.4.8 リモート管理ツールへのアクセス管理<br>✓ 4.4.9 ログの取得とセキュリティモニタリング |
| ①データ暗号化など | 4.4.6 暗号化対策 |
| ②記憶装置等の障害・交換 | N/A |
| (4)クラウドサービス契約終了時 | 4.3.6 イグジットプラン |
| 2. クラウド事業者に対する監査など | |
| 3. インシデント発生時の対応 | |
| (1) 事前対策と事後対策 | 4.4.10 インシデントレスポンス |
| (2) トレーサビリティの確保 | 4.4.11 フォレンジック |

※「FISC クラウド報告書」と本報告書の内容を元に PwC あらた作成

## 4.2. クラウド活用前の準備

本項では、クラウドの個別具体的な活用を検討する前段階として金融機関が事前準備として実施しておくべき事項について調査の結果を踏まえて述べる。クラウドというオンプレミスとは異なる特徴を有する技術基盤の活用を具体的に検討する前には、組織としての様々な事前準備が必要である。「FISC クラウド報告書」で述べられている、クラウド活用やリスク管理のためのポリシーの策定はもとより、経営陣がどのように役割を担い、関与

し推進するのか、或いは、金融機関として事前に整えておく組織体制や推進していくのに必要な能力をどう整理し準備するのかといった点が重要となる。

## 4.2.1. クラウド利用に向けた経営陣の関与と組織体制・教育

### a) クラウド利用に伴う経営陣の責任

クラウドを利用することは、金融機関の業務の一部や IT に関する設備の保守・運用業務等をアウトソースすることであり、外部委託の一形態として扱うことになる。ただし、業務の一部をクラウド事業者に外部委託した場合でも、金融機関は顧客を含むステークホルダーへの説明責任を、クラウド事業者に移転することはできない。そのため、金融機関の経営陣は、適用される法律および規制を確実に理解した上で、クラウドを安全かつ健全な方法で活用する上での最終的な責任を負う必要がある。クラウドには本報告書或いは「FISC クラウド報告書」で述べられている様々な特性があり、オンプレミスとの違いも多い。金融機関の経営陣は、クラウドを活用する前にその点を十分認識し、経営陣が果たすべき役割や責任を明確にすると同時に、クラウドを推進する責任者やリスク管理を担当する責任者を明らかにした上で、活用に向けて準備をしていくことが重要である。

なお、海外の大手金融機関では、例えば以下のような会議体を通じて、経営陣がクラウド活用に関する役割や責任を果たしているような事例も聞かれた。

図 4-2 海外の大手金融機関におけるクラウドに関する会議体の例

| 会議体名 | 開催 | 概要 |
|---|---|---|
| リスク委員会 | 四半期程度 | 社外取締役も含め取締役が参加するリスク管理上の重要事項が審議・報告される当会議において、クラウドへ移行する全てのシステムが報告される。 |
| テクノロジー検討会議 | 月次程度 | CIO オフィス内のメンバーで構成される会議で、クラウドやサイバーセキュリティ等の最新テクノロジー動向が主たるトピックとして議論される。 |
| クラウド・エグゼクティブ委員会 | 週次程度 | CIO が参加し、現在推進中のクラウド関連プロジェクトについて進捗状況や課題が確認される。 |

※ヒアリング結果を参考に PwC あらた作成

### b) クラウド推進の要となる人材と組織

3 章で述べたように、クラウドには利便性を高めるための様々な最新機能やサービス、セキュリティ機能が次々と提供される。そのためクラウドを金融機関の IT インフラとして広く活用していくためには、実務レベルで専門的な知識や役割をもつ人材または組織が重要となる。金融機関に所属するクラウドの専門人材は限られていると思うが、いくつかの金融機関では、そうした数少ない人材をうまく活用している事例が見られた。金融機関が具体的なクラウドの検討に入る前には、これらの事例のように要となる人材や組織の整備が重要である。

#### 1) 要となる人材

クラウドを積極的に活用できている一部の金融機関では、以下の 2 つの役割を担う人材が登用されクラウド活用を推進している。

1 つ目は、自社の IT 環境に関する知識とクラウドの知識を有する人材の存在である。現状オンプレミスで動いているシステムをクラウドに移行する場合は、両方の知識を持ついわばオンプレミスとクラウドの橋渡し人材が必要となる。クラウドには 3 章や本章で述べる留意事項等も含め、システム開発や運用・保守において技術面

や管理面でオンプレミスとは異なる点が多数存在する。したがって、「オンプレミスで実現していたことをクラウド上で実現するにはどうするべきか」や「オンプレミスでは実現していたものの、クラウドでは考慮が不要になることは何なのか」、或いは「クラウドを利用することにより新たに実現できること、新たに考慮すべきことは何なのか」といった点を検討できる人材が必要となってくる。

2 つ目は、クラウドを組織として利用していくためのリーダーシップを持った人材である。もちろんこの人材にもクラウドの知識は必要だが、とりわけ重要な役割は、クラウドについての知識が必ずしも十分ではない経営陣や社内の各部門に、クラウドのメリットやリスクを正しく理解させることである。例えば、攻めの面では、クラウドを活用することが単なる IT コストの削減目的ではなく、ビジネスの側面から組織にどのような効果をもたらすのか（と同時に、活用しないことでどのような機会損失が想定されうるのか）を関係者に理解させることが重要である。また守りの面では、クラウド活用が IT リスクを含めビジネス上、どのようなリスクを伴うのか正しく理解させる必要がある。クラウドを適切に活用するためには、金融機関の経営陣やビジネス部門がクラウドを正しく理解し、活用可否を判断できるだけの十分かつ分かりやすい情報や知識を提供できる人材が必要となる。

### 2) 要となる組織・チーム

金融機関がクラウドを広く活用していく上では、上述したような人材を中核に据えた、組織或いはチームを組成している事例も聞かれた。こうした組織やチームを組成する理由には次のような点が挙げられている。

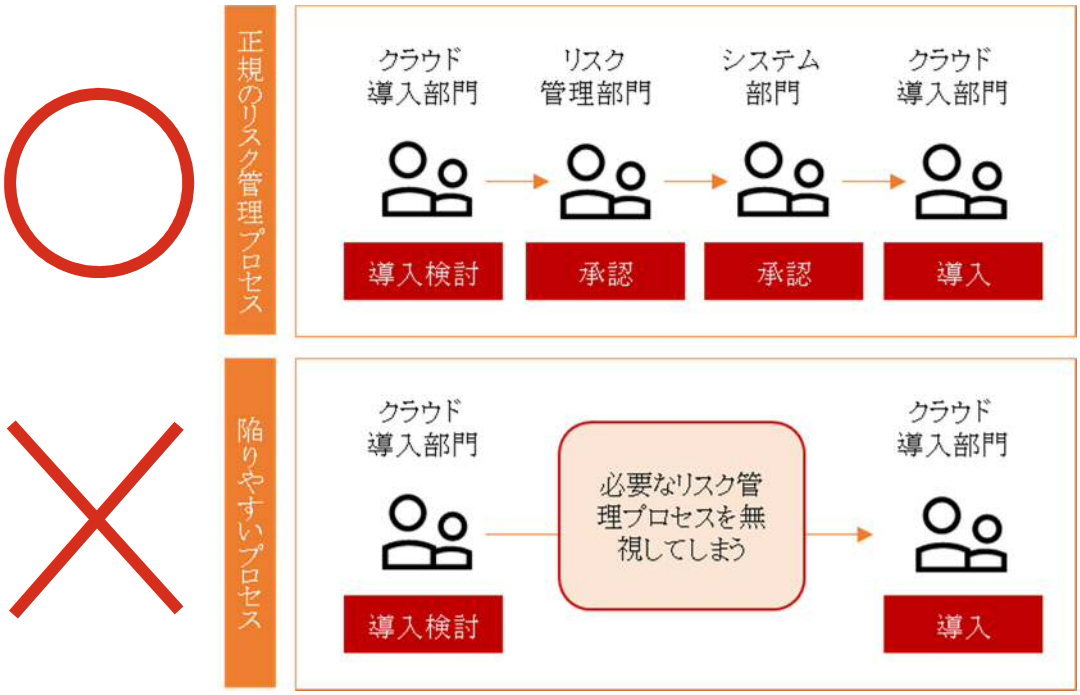
- クラウドの推進を担うチームを構成することで、クラウドの専門知識を持つ数少ない個人の知見やクラウドに関する様々な新しい情報を共有しやすくし、クラウド人材の育成を図る。
- 組織のビジネス戦略に基づいてクラウドに関する技術や最新動向を収集、蓄積し、関連技術の検証やテストを行い、事業部門や IT 部門からの要望に応じてクラウド環境を構築する。
- クラウド活用に関する全社的なルールや管理プロセスを作るには関連する法令やクラウドのリスク、技術的な知見が必要となるため、チームを組成することで効率的に検討と整備を進めることができる。また、クラウド関連プロジェクトのモニタリングを集中的に実施する。
- クラウドの活用を検討している各部門が、活用方法や活用時の留意点についてワンストップで問い合わせすることを可能にする。

## c) 役職員への教育と啓蒙

クラウドの持つメリットを金融機関全体で享受し安心安全に活用を推進するためには、クラウドの恩恵を受ける全ての役職員（派遣社員や外部委託先のサポートスタッフ等も含む）がクラウドに関する十分なリテラシーを持つ必要があり、そのための教育や啓蒙活動が重要となる。クラウドはオンプレミスと比べて導入が容易であり管理コンソールを通じて仮想マシンを短時間に構築できる。また不要になれば速やかに削除も可能である。「試行的にクラウド上にシステムを作ってみよう」、「必要な期間だけシステムを作って終わったら削除しよう」といったことが容易にできるのもクラウドのメリットである。ただし、クラウドリテラシーに関する教育や啓蒙活動が適切に行われず、利便性や活用容易性のみに目がいくと、リテラシーの低い職員や部門により、組織として未承認のシステムがクラウド上に構築される虞がある。これは、企業の SaaS 利用等でもよく聞かれる、「シャドーIT」の問題と同様であり、クラウド活用の結果、情報セキュリティやコンプライアンス上の事故を引き起こしたり、思わぬコスト増を招くことになりかねない。

クラウド事業者からは、このようなクラウド利用者の潜在的なリスクに対応するため、仮想マシンの稼働数や稼働状況等を監視・検知できる機能が提供されているが、金融機関はこれらの機能を活用するだけではなく、クラウドの特性や利用に伴うリスクを含めた教育や啓蒙活動を全社的に実施し、関係者のクラウドリテラシーを向上することが重要である。

図 4-3 クラウド導入におけるプロセスの無効化




※知見を元に PwC あらた作成

## 4.2.2. サイバーセキュリティ管理への対応

クラウドを活用していく前準備としてサイバーセキュリティへの対応も重要となる。クラウドは責任分界モデルであるため、金融機関の責任範囲については、オンプレミス同様にサイバーセキュリティ管理態勢を適切に整えておく必要がある。また、クラウド事業者の責任範囲については、クラウド事業者がサイバーセキュリティを確保する。ただし、通常の外部委託先管理と同様に、クラウドの活用判断や事業者の選定は金融機関の責任で実施される。そのため万一、クラウド事業者に起因するインシデント等によって顧客影響等を及ぼした場合は、金融機関が顧客に対する説明責任は負うことになる点を忘れてはならない。

金融機関の多くは、既に CSIRT 等の組織を中心に、平時と緊急時のサイバーセキュリティ管理態勢を構築しているため、上記の点を踏まえて、既存のサイバーセキュリティ管理態勢にクラウドに関連する事項を統合していくとよい。その際は、従来から広く活用されているサイバーセキュリティのフレームワークが参考となる。例えば、NIST の Cybersecurity Framework や ISMS 等である。今回の調査でヒアリングを行った海外の大手金融機関でも、クラウド固有のサイバーセキュリティフレームワークは採用されておらず、オンプレミスに適用している既存のサイバーセキュリティフレームワークがクラウドの領域に応用・展開されていた。

## 4.3. クラウド活用の検討段階

金融機関がクラウド上で新規システムの構築を検討する場合や、オンプレミスからのシステム移行を検討する場合は、金融機関として実現したいことを整理(要件定義)したり、そのフィージビリティの見極めやコスト予測を行う必要がある。それと同時に、金融機関のニーズをどのクラウド事業者のサービスで実現すべきかを検討し、事業者選定を行う必要がある。本項では、上記のように具体的にクラウドの活用を検討する段階で考慮すべき事項を、調査の結果を踏まえて述べる。

### 4.3.1. 性能要件のフィット&ギャップ

実現したい業務やその機能要件を明確にしておくことはもちろんのこと、性能要件についても事前に十分検討しておく必要がある。クラウドは、責任分界モデルであるためクラウド事業者の責任範囲で実施される保守作業等については、原則金融機関がコントロールすることは不可能である。「FISC クラウド報告書」においても、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することの必要性が述べられている。そのため、金融機関は、実現したい性能要件を予め明らかにした上で、適したクラウド事業者を選定する必要がある。

ただし、性能要件の全てがクラウド事業者によって満たされるわけではない点に留意が必要である。ネットワークに関しては通信事業者との関係があるほか、クラウド事業者が提供する機能やサービスの中には、性能に関する制限が設けられているケースもある。また性能を実現するために、金融機関側で開発や運用の創意工夫を行うことが望ましいケースも出てくる。既存システムの構造によっては、オンプレミスから単純にクラウド上に移行しても、同等のパフォーマンスが出ず、アプリケーションの大幅な改修や、想定以上の処理性能が必要になり、結果として移行の負荷やコストが大きくなってしまうケースもあると言われている。金融機関のシステムの中にはレガシーシステムも多く、内外の接続先が多数あるようなシステムも存在することから、予め業務要件のみならず、性能要件も考慮した上で、クラウド移行の可否或いは、クラウド事業者の検討を行うことが重要となる。

図 4-4 予め検討しておくべき性能要件の例

| 項目 | 概要 |
|---|---|
| サービス提供時間 | クラウド上で稼働する業務やサービスの提供時間を定義する。 |
| サービス稼働率 | 上記のサービス提供時間と合わせてどの程度の稼働率が必要になるのかを定義する。高い稼働率が必要な場合は、可用性を確保できるシステム構成や運用のフィージビリティ等を検討する。 |
| 応答時間 | システムレスポンスの応答時間を定義する。高いレスポンスが必要な場合は、例えばデータベースをインメモリで処理できるサービスを提供しているか、回線のキャパシティ、地理的にデータセンターのロケーションを選べるか等を検討する。 |
| 処理性能 | システムに求める処理性能を定義する。仮想マシンのリソースをどの程度詳細に割り当てることが可能か、優先度の高い業務にリソースを優先的に割り当てるようなシステム上の作りが可能かを検討する。 |
| カスタマイズ性 | システムのカスタマイズの柔軟性を定義する。繁閑の程度や将来の業容拡大等を踏まえ、選定するクラウドがどの程度リソースをスケールアップ、スケールアウト出来るか等を検討する。 |

| | |
|---|---|
| 同時接続利用者数 | システムに必要な同時接続数を定義する。最大想定接続数を考慮し、クラウド事業者が提供するロードバランサ機能やネットワーク関連の機能が要件に耐えうるか、或いは同時接続数を調整するカスタマイズを自身で行う必要があるか等を検討する。 |
| データ容量 | クラウド上で利用するデータ容量を算出する。将来の業容拡大等を踏まえ、データ量の拡大を想定した場合に、選定するクラウドがどの程度まで柔軟かつ容易に拡張可能かを検討する。 |

※文献調査や知見を元に PwC あらた作成

### 4.3.2. セキュリティ要件定義とクラウド提供機能の活用

オンプレミスのシステムでセキュリティ対策を行う場合、金融機関は、様々なセキュリティ製品を検討し、組み合わせ、購入し、設計・導入する必要がある。クラウドでは、様々なセキュリティ機能やサービスがクラウド事業者から提供されているケースも多い。したがって、クラウド事業者から提供されるセキュリティ機能は、金融機関がクラウド事業者を選定する際の一つの考慮事項となる。大手クラウド事業者の場合、例えば、暗号鍵管理、WAF 機能や DDoS 対策機能、およびこうした機能を通じて出力されるログの分析ツール等が提供されている。加えて、クラウド事業者のサードパーティが提供している様々なセキュリティ関連サービスもある。こうしたサービスを使えば、金融機関は、自らセキュリティ製品のライセンスを購入したり、時間をかけて実装したりする必要もなく、一定のセキュリティ対策を実装できるため、国内の金融機関に対するヒアリングでも、クラウド事業者等から提供されているセキュリティ機能は可能な限り利用を検討している、または利用したいとの意見が聞かれた。

したがって、金融機関は、クラウドに移行または構築するシステムに必要なセキュリティ要件を予め整理した上で、まずはクラウド事業者等から提供されるセキュリティ機能でどこまで要件を満たすことが可能かを検討することが有益である。クラウド事業者の提供機能で不足する場合は、自社開発やサードパーティベンダーから提供されるセキュリティ製品の導入を検討する等により、セキュリティ要件の実現方法を検討する必要がある。

### 4.3.3. 事前のコスト検証

クラウドを活用するメリットの1つとしてコスト削減が挙げられるが、2.3 章「利用および導入状況」でも触れた通り、既存システムの改修やクラウドとの通信に係るコストの増加は懸念材料である。クラウド活用の検討時は、以下のような点も考慮しコストシミュレーションを実施し費用対効果を検証することが重要である。

- 現行システムからのデータ移行やカスタマイズ費用、認証システムや既存システムとの連携機能に必要となる費用等も考慮し検討する。
- 既存システムの運用コストは、機器に係る保守費用やバックアップ媒体等の費用、データセンターの電力や設置スペースに係る設備費用、運用担当者の人的コストなども考慮し検討する。クラウド活用時の運用コストは、利用する機能やサービス毎の詳細な課金体系を把握した上で検討する。
- クラウド事業者のデータセンター拠点まで専用線での接続が必要な場合や VPN を利用する等の場合は、回線敷設や VPN の利用に必要な初期費用ならびに月額料金を検討する。
- (IaaS のケースにおいて、)OS 上にインストールするソフトウェアのライセンスは、ソフトウェアベンダーによってはクラウド専用のものが提供されていたり、オンプレミスで使用しているライセンスがクラウドに転用できない等の場合がある。また、オンプレミスとクラウドではライセンス数の計算方式が異なる場合がある。こうしたソフトウェアライセンスに係るコストについて前提条件を考慮してライセンス費用を検討する。

### 4.3.4. サポート体制・条件

「FISC クラウド報告書」の中でも、クラウド事業者の選定時や契約締結時において、サポート条件は、検討或いは契約などに盛り込む事項として整理されている。

クラウドは外部委託の一形態と整理されるものの、契約形態の特性から、オンプレミスの外部委託先と同等のサポートをクラウド事業者から得るのは現実的に難しい。したがって、クラウド事業者を選定するにあたっては、予め平時や緊急時に、金融機関が得られるサポートを確認しておくとともに、クラウド事業者側に窓口担当者（例えば、担当営業、担当技術者）等の設置が可能か等、確認しておくことが重要である。

また、国内金融機関やクラウド事業者へのインタビューからは、金融機関がクラウド活用の検討や導入のサポートを得るために、パートナー企業等の外部専門家を活用している事例が多く聞かれた。IaaS や PaaS の活用をこれから開始しようとする金融機関では、クラウドに精通した人材は不足しており、育成や中途採用にも時間がかかる。クラウドを社内の IT 基盤として広く活用している金融機関では、専門性を有するパートナー企業から継続的なサポートを得てプロジェクトを推進するとともに専門的知見の蓄積を図っている。

### 4.3.5. 公的認証・第三者評価・監査

クラウド事業者の選定にあたり、金融機関は、クラウド事業者の責任範囲となるサービスが安心安全に提供されるか、また金融機関の求める可用性や機密性、完全性等の水準に適合しているかを判断することが重要である。判断には、クラウド事業者が取得している公的認証や第三者評価（外部監査等）レポートが1つの材料となる。公的認証や第三者評価レポートには主に以下のようなものがあるが、その他にも米国や英国では自治体等が安心してクラウドの選択・採用を可能とするための取り組みが存在しており、米国では、クラウド調達の際のセキュリティ基準および認定制度として「FedRAMP[16]」が、英国では、クラウド調達を支援する「Government Cloud (G-Cloud)[17]」がそれぞれ導入されている。

また、我が国においても 2019 年 3 月、「クラウドサービスの安全性評価に関する検討会 中間とりまとめ（案）」[18]が公表されており、その中では、クラウド事業者の提供するサービスが一定の基準を満たしたていると確認された場合、当該サービスは、政府の登録簿に登録された上、政府調達時には当該登録簿からの選定が要件化されるとの報告がなされている。

このように、金融機関は様々な認定制度等の取得状況を参考にしながらクラウド事業者を見極めることができる。また、SOC2 レポートについては、通常クラウド事業者は継続的に取得しているため、選定時のみならず継続的なモニタリングの手段としても活用することも可能である。

[16] https://www.fedramp.gov/

[17] https://www.digitalmarketplace.service.gov.uk/buyers/direct-award/g-cloud/start

[18] https://www.meti.go.jp/press/2018/03/20190315002/20190315002-1.pdf

図 4-5 主な公的認証・第三者評価

| 公的認証・第三者評価 | 概要 |
|---|---|
| SOC2 レポート | 受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に関する内部統制に関する報告書[19]。 |
| ISO/IEC27001 | 情報セキュリティ全般に関するマネジメントシステム規格。情報の機密性・完全性・可用性の 3 つをバランスよくマネジメントし、情報を有効活用するための組織の枠組みを示している[20]。 |
| ISO/IEC27017 | クラウドに関する情報セキュリティ管理策のガイドライン規格。ISO/IEC27001 の取り組みを強化し、クラウドに対応した情報セキュリティ管理態勢の構築が可能[21]。 |
| ISO/IEC27018 | クラウドに特化した規格であり、ISO27002 をベースとした、PII プロセッサとしてのクラウド上の個人が特定できる情報（PII）の保護に関する実践的模範[22]。 |

※公表情報を元に PwC あらた作成

### 4.3.6. イグジットプラン

既存のクラウド事業者から離脱し、別のクラウド事業者へ移行する、またはオンプレミスに回帰する場合の留意事項は、既に「FISC クラウド報告書」で述べられているため、本報告書では多くは触れないものの、本調査の金融機関へのヒアリング等で把握した具体的な取り組み事例について以下で紹介する。

主に海外の大手金融機関へのヒアリングを通じて把握した内容ではあるが、一部の金融機関では、法令・規制の変化、クラウド事業者側のサービスレベル違反等により、金融機関がクラウド事業者から離脱または移行しなければならなくなった場合に備え、契約段階およびサービス利用開始時からフィージビリティスタディーを実施している。クラウド事業者を選定する際は、離脱・移行の容易性等を評価すると共に、システムの構築段階でも常に移行可能性を意識した構築を行い、本番稼働前にはクラウド離脱のための移行テストも必要に応じて実施している。また、別の大手金融機関は、より高度な手法として複数のクラウド事業者を並行して利用するマルチクラウドアプローチを採用している[23]。特定のクラウド事業者のロックインを技術的観点から回避するため、重要なシステムについては、コンテナベースで開発を行い、異なるクラウド事業者への移行性を高めるアプローチが取られている。

## 4.4. クラウドを活用したシステムの開発・運用段階

クラウド上での新規システム構築の検討や移行の検討が完了し、クラウド事業者の選定も完了すると、実際にビジネスをクラウド上に実装するためのシステム開発や移行フェーズを経てシステム運用フェーズとなる。本項では、事前に検討した機能要件や非機能要件をクラウド上で実装・運用するフェーズで考慮すべき事項について、調査結果を踏まえて述べる。

[19] https://www.pwc.com/jp/ja/services/assurance/process-system-organization-data-management/control-advisory-assurance-service/ssae16-arcso86-isae3402.html を参考に PwC あらた作成

[20] https://www.jqa.jp/service_list/management/service/iso27001/の説明を元に PwC あらた作成

[21] https://www.jqa.jp/service_list/management/service/iso27017/ の説明を元に PwC あらた作成

[22] https://www.iso.org/standard/61498.html を参照し PwC あらた作成

[23] 一部のクラウド事業者ではマルチクラウドアプローチは推奨していないとの意見が聞かれている点に留意。

## 4.4.1. クラウド環境におけるシステム構築

### a) 可用性を意識したインフラ設計

クラウド事業者はサービスのダウンタイムを発生させないよう、日々、障害を引き起こすリスクを低減するため、新しいテクノロジーやコントロールを導入し改善を行っている。しかしながら、クラウドでは、数時間程度のダウンタイムが発生することは珍しくない。長い場合は複数日にわたってサービスがダウンし、影響範囲が全世界に及ぶこともある。このようなサービスダウンは、近年も発生しており、結果として金融を含む世界中の重要機能の継続に大小の影響を与えている。したがって、金融機関が可用性を必要とするシステムをクラウド上に構築する場合は、オンプレミス同様に目指すべきサービス水準を明らかにし、可用性を確保する設計と実装が必要である。

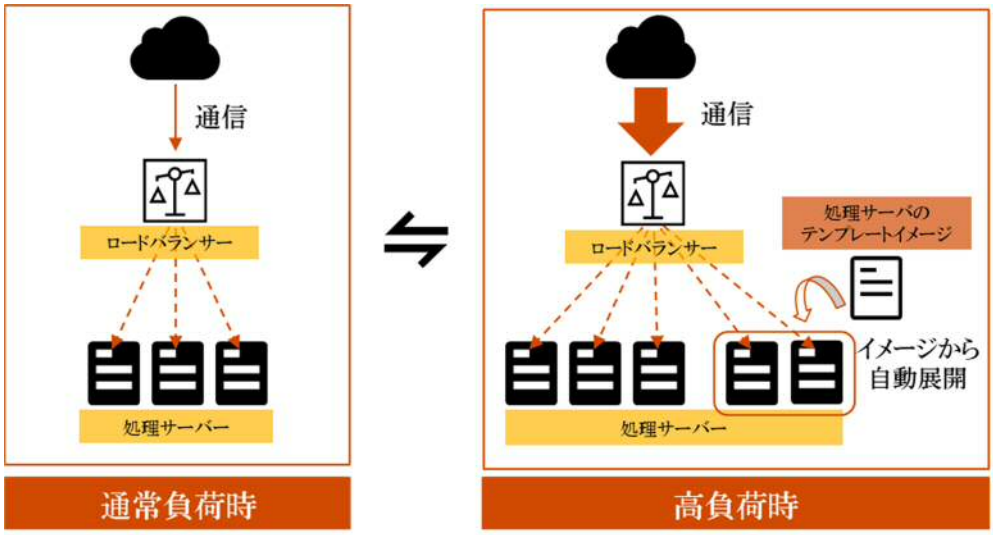
この点はクラウド事業者へのヒアリングでも、「オンプレミス同様、クラウドもダウンする場合はある。またメンテナンスによりサービス停止する場合もある。」「クラウド利用者は、必要に応じて可用性を考慮したインフラ設計をする必要がある。」といった意見が聞かれている。可用性を確保するためのヒントや事例は、クラウド事業者によって Web サイトやホワイトペーパー等の形で提供されているため、こうした公表情報も活用しながら金融機関はクラウド上のシステムを設計、構築する必要がある。

### b) オートスケーリング

オートスケーリングとは、クラウドの特徴の一つであり、クラウド環境において仮想マシンやサーバリソースの割り当てを、時々の負荷の状況に応じて自動的に増減できる仕組みである。こうした機能を使うことにより、クラウド利用者はオンデマンドで効果的かつ効率的にクラウドを活用することができる。例えば、繁閑の大きなシステム（例：バッチ処理、リスクの計算処理）等に有効である。

このような柔軟性はクラウド環境の利点の一つであるが、オートスケーリングの機能を活用してシステムを構築する場合、幾つか考慮しておく点がある。

図 4-6 オートスケーリング機能のイメージ




※知見を元に PwC あらた作成

上図は、オートスケーリング機能を実装し、負荷状況に応じて処理サーバを増減させているイメージである。例えば、「ネットワークから入ってくるトランザクション量を監視し、負荷が一定の閾値を超えたら、事前に用意した処理サーバのひな型イメージの複製が自動的に作成され、増設した処理サーバとして展開・起動される。同時にロードバランサの負荷分散機能と連携し、増えたトランザクションを効果的に分散することを自動的に実現する。また、負荷が落ち着くと、事前に指定した条件にしたがって処理サーバが自動的に停止、削除される。」といったことが実現可能である。

このようにオートスケーリング機能を使うと、自動的に処理サーバの構築または削除が可能だが、増減する処理サーバ上に、本来長期保存が必要なデータやログを保持させたり、セッション情報を保持させると、処理サーバの削除のタイミングで一緒に消失してしまうため留意が必要となる。

また、処理サーバのひな型イメージには、起動と同時に必要となるマルウェア対策ソフト等のエージェントを漏れなくインストールしておくことが必要である。この対応を漏らすと、マルウェア対策ソフトが実装されていない処理サーバが増設され稼働することになってしまう。同様に増減する処理サーバが、SOC（Security Operation Center）等のセキュリティ監視の対象から漏れることのないよう予め構成しておくことも重要である。

このように考慮するべき点は多岐にわたるが、人手を介さず自動化されたシステムを構築することにより運用負荷やランニングコストを軽減することができる。

### 4.4.2. クラウド環境におけるシステム運用

3 章に記載した通り、クラウドでは様々なセキュリティインシデントが発生しているが、その原因の多くは、設定の誤り、脆弱性の放置、認証情報の管理不十分等といったクラウド利用者のミスに起因する。国内外の金融機関へのヒアリングからも以下の意見が聞かれた。

- クラウドで発生している多くのセキュリティインシデントは、クラウド利用組織の管理者による設定ミスが原因だと理解しており、それがリスクである。
- クラウド自体は従来の IT サービスと比べ本質的な面では安全性が低いとは考えていない。
- クラウド利用組織の管理者は、クラウド上に自組織のシステムが正しく構成され、すべてのデータが適切に保護されていることを徹底的に確認する必要がある。

クラウド利用者に起因するミスを防ぐためには、一義的にはクラウド上で提供される各種機能について、十分な技術的知見を有する人材が関与し、システム構築することが重要となるが、それと同時にシステム開発や運用のライフサイクルにおいて確実に正しい設定が反映されていることを継続的に確認するプロセスを設けることも重要となる。

ヒアリングを実施した国内金融機関の中には、本番稼働前の段階のみならず、運用段階に入った後も、外部のクラウド専門家を活用して定期的に設定の検証をつぶさに行っているとの事例が聞かれた。また、クラウド利用者は、通常クラウド事業者が提供するリモート管理ツールの画面（インタフェース）を通じてクラウド上の設定等を行うが、当該管理ツールの画面はクラウド事業者側の裁量により、年に数度変更されることもあるため、画面の見た目の変更に伴い、設定を見落したり誤ったりするケースもあるため十分注意しなければならないという注意点も聞かれた。

加えて、より効果的かつ効率的なアプローチとして、海外の金融機関では自動モニタリング機能を実装している事例も聞かれた。当該金融機関では、クラウドが提供している機能をベースに自社固有の条件設定等をす

ることにより、クラウド上の設定を自動的かつ常時モニタリングする仕組みを実装し、設定誤りが検出された場合は、適時に管理者にアラートを上げ、また特定の設定誤りについては自動的に修復するロジックを組み込んでいる事例も聞かれた。クラウド活用を推進している金融機関では、こうした自動化によりセキュリティリスクと不要な運用コストを減らす取り組みを積極的に採用している。

### 4.4.3. コスト管理

クラウドでは、仮想マシンを稼働させたタイミングをスタート地点として、課金が発生する。クラウド環境の課金体系の多くは従量制であり、リソースを使用した分だけ料金を支払う必要がある。そのため、無駄なコストを発生させないためにも、コストを最適化することにも注意を払う必要がある。従来のオンプレミスであれば、一度サーバ等の機器やライセンスを購入してしまえば、ネットワークの通信料等の一部を除きコストの変動要素は小さかった。しかしながら、クラウドではリソースの利用状況を適切に監視・管理しなければ、予期せぬコスト増に繋がる可能性がある。

クラウド事業者によっては、リソースとコストのモニタリングをサポートするツールを提供している。当月の利用請求料金をオンデマンドで可視化するツールや、一定の閾値を超えた場合は、通知が届くサービスなども用意されており、コスト管理を行う上で有益である。

また、リソースとコストの管理を適正化する手段として、一部のクラウド事業者では、リソース予約プログラムを提供している。長期の使用が想定される仮想マシンやデータベース等については、予めこのプログラムを活用し、利用を確約することでコストを割安に抑えることができる。

なお、昨今のサイバー攻撃では、クラウドに不正侵入し、そのリソースを使って暗号資産の不正マイニングを行わせる事例も複数発生している。コストのモニタリングを適切に実施することで、こうした攻撃を早期に検知することも可能となる。

### 4.4.4. 構成管理とセキュリティパッチ管理

クラウド上での仮想マシンの構築には一定の知識や操作権限が必要となるものの、物理マシンの選定・購入手続きを実施しサーバールームや執務室内に設置するといった一連の作業に比べると、はるかに容易である。容易さがゆえに、適切に仮想マシンの台数や構成情報を管理しなければセキュリティ上の脆弱性を生むこととなる。NIST「SP800-146 クラウドコンピューティングの概要と推奨事項」(訳:IPA)[24]では、以下の通り、クラウドの構成情報の把握とセキュリティアップデートに関する留意事項が述べられている。

> *(前略)・・・IaaS クラウドは、利用者が多くの仮想マシンを作成し、場合によっては様々な状態(例:実行、一時停止、休止)で保持することを可能とする。アクティブでない仮想マシンは、重要なセキュリティアップデートに関して遅れをとる可能性がある。仮に、古くなった仮想マシンがアクティブになった場合、そうした仮想マシンは侵害される可能性がある。原理上は、クラウド提供者が利用者の代わりにアクティブでない仮想マシンをアップデートすることが可能だが、そうしたアップデートのメカニズムは複雑であり、通常、セキュリティアップデートの維持管理は利用者側の責任になる。・・・(後略)*

[24] https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000152.html

金融機関は、仮想マシンの構築に関する正式なプロセスを整備し関係者に適用・周知する必要があるが、これだけでは、不正な仮想マシンの構築を予防したり、早期な発見と対処を行うことは難しいかもしれない。仮想マシンは、物理的にマシンが存在するわけではないため目に見えず、増減するため人手に頼った管理には限界がある。クラウド事業者やサードパーティベンダー等が提供する自動化された資産管理や構成管理のツールを活用したり、セキュリティパッチの適用状況を自動的に可視化し、アラートを挙げたりする仕組みを構築することが有益である。

実際に、海外の大手金融機関では、仮想マシン上のソフトウェアに対するセキュリティパッチ適用の自動化や設定値等のコンプライアンスチェックの自動化および一部の修正の自動化に取り組んでいるという事例が聞かれた。

### 4.4.5. 脆弱性スキャンとペネトレーションテスト

金融機関がクラウド上に構築したシステムの脆弱性に対処する有効的な手法として、脆弱性スキャンやペネトレーションテストが挙げられる。オンプレミス同様、定期的にこれらのテストを実施することで、システムの脆弱性を減少させセキュリティを強化することが可能である。しかしながら、これらのテストを実施する場合、クラウドがリソース共有サービスである点や、クラウド事業者との責任分界モデルである点を考慮する必要がある。具体的には以下のような点がある。

- テストで利用するツールが、金融機関の責任範囲を超えてクラウド事業者の環境や他の共同利用者の環境に悪影響を及ぼす虞がないか。
- テスト行為が本物のサイバー攻撃として検知され、クラウド事業者によって遮断されたり、正規の通信を含む全ての通信が強制遮断される虞はないか。

また一部のクラウド事業者では、利用できる脆弱性スキャンおよびペネトレーションテストの種類や回数等の制約を設けている場合もある。クラウドという性質上、オンプレミスとは異なるこうした考慮が必要になることから、テストを検討する場合は、制約事項や、実施により想定外の悪影響を及ぼすことがないか等、クラウド事業者との間で事前に十分な確認を行っておくことが重要である。

### 4.4.6. 暗号化対策

暗号化対策については「FISC クラウド報告書」でも考慮すべき事項として具体策を交え述べられており、クラウド上にデータを保管する上での重要な考慮事項である。また、ABS[25]が公表している「Cloud Computing Implementation Guide 1.1（以下、「ABS Cloud Implementation Guide」）」[26]では暗号化を実装する管理策の一つとして、暗号鍵のライフサイクル管理について述べられている。具体的には、暗号化キーの生成、保管、使用、失効、期限切れ、更新から、暗号化キーのアーカイブまで、ライフサイクルを管理するためのポリシーと手順の整備を金融機関に求めている。

近年では、大手クラウド事業者が、こうした鍵管理のライフサイクルをサポートするサービスを提供している。また暗号化のポリシー設定機能を用いて暗号化の対象となるデータを自動で識別し暗号化する機能なども提供

[25] The Association of Banks in Singapore：シンガポール銀行協会

[26] https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf

している。金融機関はクラウドにおけるデータの暗号化基準を予め定めておくとともに、こうした暗号化機能を活用することで、クラウド上の重要資産を保護することが可能となる。

なお、今回ヒアリングを実施した海外の大手金融機関では、クラウドで取り扱うデータの重要度に応じて暗号化対策の水準を定めている事例が聞かれた。取り扱うデータの重要度に応じて、暗号化すべき範囲や採用する暗号方式、暗号鍵の管理方法等を定めており、例えば、暗号鍵の管理方法では、重要度が中程度のデータの場合は、暗号鍵をクラウド上で管理することが許容されるが、重要度が高いデータは、暗号鍵を自社のオンプレミス環境で管理するといったルールを適用している事例が聞かれた。

### 4.4.7. ネットワーク対策

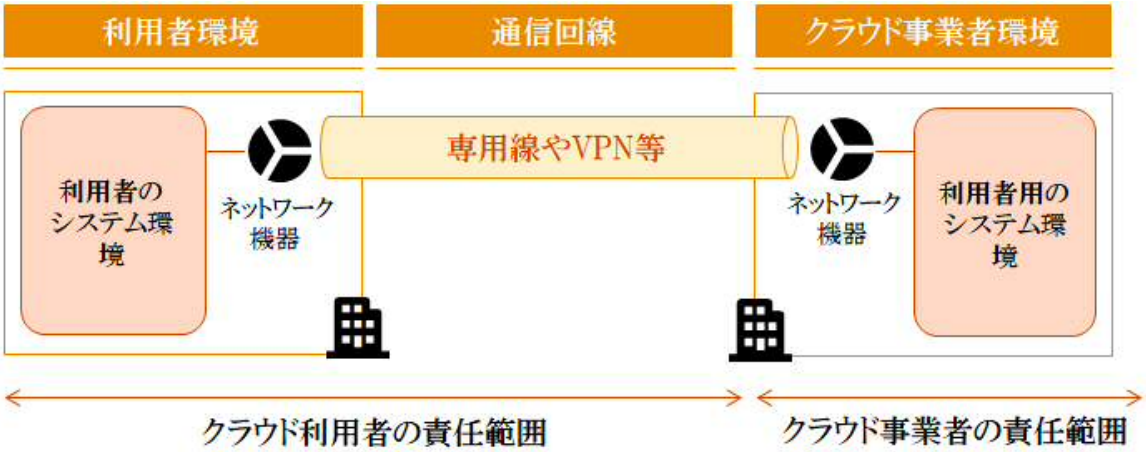
クラウドにシステムを構築または移行した場合でも、オンプレミスにある他のシステムや金融機関の各拠点、或いは他の機関との間でデータ通信を行うことは一般的である。しかも、その多くはデータ伝送経路の保護が必要であることから、金融機関はオンプレミスと同様にセキュアな通信を確保する対策を行う必要がある。ここでは専用線或いは VPN を敷設する場合の一部を例に挙げて、考慮すべき事項を述べたい。

クラウド環境とその他の環境を専用線や VPN 等で接続する場合、どこまでがクラウド利用者の責任範囲となるかを予めクラウド事業者へ確認する必要がある。下に図示したように、一般的には、専用線や VPN の終端となるネットワーク機器の用意や、専用線・VPN の敷設作業については通常、クラウド利用者、即ち金融機関の責任範囲となるケースが多いと言われている。

また、クラウド事業者によっては、回線を引き込むことが許容される通信事業者や、金融機関で使用できる VPN の終端機器、或いは通信ネットワークプロトコルやその設定等が予め定められている場合があるため、そうした点にも留意が必要である。

加えて、ネットワークの冗長化も考慮する必要がある。いくらクラウド環境を冗長化しても、通信経路の可用性が維持されなければ、システム全体の可用性は担保されない。

図 4-7 利用者とクラウド事業者間の専用線や VPN 敷設のイメージ




※知見を元に PwC あらた作成

### 4.4.8. リモート管理ツールへのアクセス管理

金融機関に割り当てられたクラウド環境の管理や、メンテナンス、或いはアプリケーションリリースを行うためには、通常クラウド事業者から提供されているリモート管理ツールへログインし利用する必要がある。これらツールの多くはインターネット経由で提供されており、クラウド環境に関する様々な操作を一元的に行うことができる。言い換えれば当該ツールが悪用されるリスクを十分に認識する必要がある。例えばリモート管理ツールの特権 ID は、クラウド環境のあらゆる操作が可能なため、攻撃者の手に渡ってしまうと、クラウド環境の破壊や情報の窃取、ボットネットの構築などに悪用され、深刻なセキュリティインシデントを招くことに繋がる。クラウド環境からオンプレミス側に不正アクセスされる虞もある。したがって、金融機関はリモート管理ツールに対する厳重なアクセス管理対策を行う必要がある。基本的な考え方は、オンプレミスと同様「FISC 安全対策基準」の「Ⅵ. 1(1)データ保護」や「Ⅵ. 2(2)アクセス権限の管理」が参考となる。

また、リモート管理ツールへのアクセス管理については、「ABS Cloud Implementation Guide」の中でも「10.Administrative Remote Access」として述べられている。内容を要約すると以下の 4 点となる。

- リモート管理ツールには正規の端末からのみ接続を許可するよう、デバイス認証などの技術を実装する。
- リモート管理ツールへのアクセス時は多要素認証、VPN 暗号化などのセキュリティ対策を実装する。
- リモート管理ツールへ接続する際に接続元 IP アドレスを制限する。
- リモート管理ツール用の特権 ID の扱いには特に注意を払い、整備したプロセスにしたがって適切な人員への権限付与や利用管理を行う。

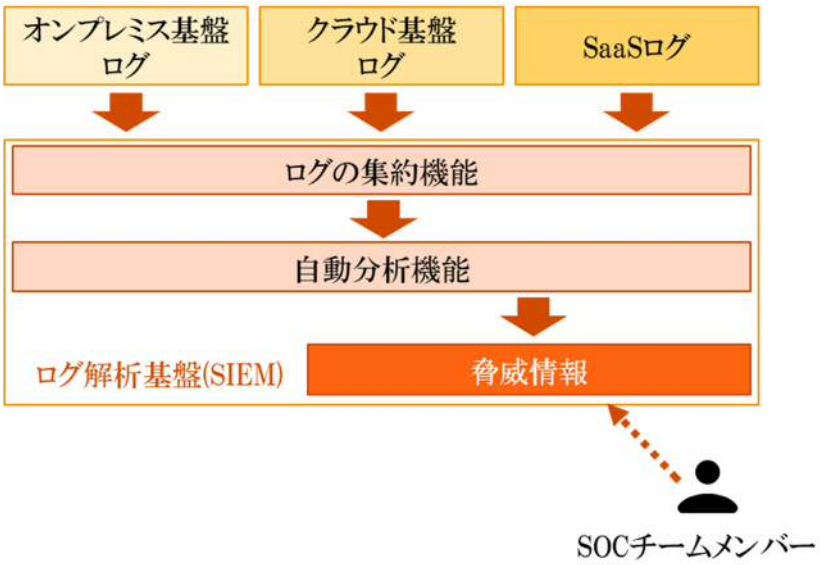
### 4.4.9. ログの取得とセキュリティモニタリング

クラウド上でもオンプレミス同様、目的に応じて必要なログを取得・監視し、必要な期間保管しておく必要があるが、その際クラウドを使用することによって、追加的に管理対象とすべきログを漏れなく識別し、取り扱いを検討しておく必要がある。例えば、リモート管理ツールのログやクラウド事業者の提供する各種機能を使用することで出力されるログ等が該当する。これらのログを用いたセキュリティモニタリングを行う場合、クラウド上のログとオンプレミス上のログは一元管理し、統合的にモニタリングできた方が効率的であり、また相関分析等もしやすい。今回ヒアリングを行った海外の大手金融機関では統合的なモニタリングを実現していた。

また、比較的クラウドを積極的に活用している国内金融機関でも、ログを一元管理し統合的にモニタリングする仕組みを実現している事例が聞かれた。以下に一例を挙げるが、ある国内金融機関では、セキュリティメーカーが SaaS として提供する SIEM[27]機能を用いて、クラウドとオンプレミスのログを集約し分析や脅威の検知を行っていた。

[27] Security Information and Event Management の略。様々な機器のログを一元的に管理・蓄積し、脅威となる事象を分析し、迅速な対応を可能とするための管理手法をいう。

図 4-8 SaaS 型 SIEM を活用しオンプレミスとクラウド上のログを集約・分析するイメージ図




※文献調査やヒアリングで得た情報を参考に PwC あらた作成

## 4.4.10. インシデントレスポンス

クラウド環境を対象としたサイバー攻撃が顕在化した場合に備え、金融機関は、インシデントレスポンス態勢の整備とその実効性の確保が重要となる。

金融機関の責任範囲内で発生したサイバーインシデントは、金融機関が対応しなければならない。基本的な態勢整備の考え方はオンプレミスと同様であり、また攻撃シナリオの類型という点でも、複数のクラウド事業者や金融機関へヒアリングした限り、オンプレミスと大きな違いは聞かれなかった。しかしながら、レスポンスには、クラウドに関する知識も必要になり、また具体的な手順では、オンプレミスとは異なる点が多数でてくる。例えば、リモート管理用ツールにログインする高権限アカウント等が漏えいした場合は、速やかにアカウントを無効化できるようにしておく必要がある。そのため、クラウドを活用する際には、クラウドの特性や自社の活用実態を踏まえた態勢を整備しておくことが重要である。

また、インシデント発生時におけるクラウド事業者との連携の在り方についても検討しておく必要がある。これは、金融機関の責任範囲のみならずクラウド事業者の責任範囲でインシデントが発生した場合も含めて検討しておくことが重要である。この際、金融庁等が 2018 年 10 月に公表している「金融セクターにおけるサードパーティのサイバーリスクマネジメント に関するG7の基礎的要素（仮訳）」[28]等も 1 つの参考となる。基礎的要素の「要素 3」のインシデント対応について以下のように述べられているため、こうした点も踏まえたクラウド事業者との連携態勢を整備しておくことが重要である。

[28] https://www.fsa.go.jp/inter/etc/20181015/20181015.html

*要素3:インシデント対応*

*金融機関は重要なサードパーティを含むインシデント対応計画を策定し、演習 を実施すること。*

*金融機関のインシデント対応計画には、サードパーティに関係するサイバーインシデントの検知・情報収集の方法や、サードパーティ及び適切な当局との 連絡手段が含まれるべきである。また、役割と責任、国のCIRT(サイバーイン シデント対応のためのチーム)を含む関連当局への報告基準も含まれるべきである。定期的な演習は、弱点の特定、サイバー攻撃に対する頑健性のテスト、対応や 復旧の適切性の評価に役立てることができる。可能な場合には、インシデント 対応計画は、金融機関、サードパーティその他の関係者と共同で演習が実施されるべきである。インシデント対応計画は、組織変更や教訓を考慮して見直されるべきである。*

## 4.4.11. フォレンジック

セキュリティインシデントが発生した際の証拠収集、即ちフォレンジックについては、オンプレミスとクラウド環境で幾つかの点で異なる。サイバーインシデントの原因究明にはフォレンジックが欠かせないことから、近年ではクラウド事業者側からの情報提供や協力等も得やすくなってきていると言われているが、ENISA[29]「Exploring Cloud Incidents」(2016)[30]では、クラウド環境の特定の特性により、従来の IT 環境ではデジタルエビデンスを取得する際に通常直面しない技術的、組織的、法的な課題が発生する可能性について述べており、概要は以下の通りである。

### 1) 技術的な課題

クラウドに関する以下の技術的特性がデジタルフォレンジックを複雑化または難化させる要因であると指摘している。

#### マルチテナンシー

システムのマルチテナント化は、クラウドリソースの弾力性が急速に高まり、データ取得の複雑性が増す。あるクラウド利用者がリソースを開放した後に、別のクラウド利用者が同リソースを再利用する場合、物理的に証拠を取得することはクラウド利用者だけでなくクラウド事業者にとっても難題となる可能性がある。

#### 動的なリソースの割り当て

クラウドにおけるリソースが動的に割り当てられる特性は、フォレンジックによる調査においてリソースの正確な分離を妨げる。このことは、インフラストラクチャを共有する他のクラウド利用者の機密性を考慮する必要があるため重大な課題として挙げられている。

#### メモリデータの揮発性

攻撃の痕跡を解析するための仮想マシンのメモリデータ取得は困難であると同時に、インシデント分析を危惧する攻撃者によって意図的にマシンをシャットダウンする攻撃を仕掛ける可能性が考えられる。この場合、揮発したメモリ情報から攻撃の痕跡を辿ることは困難となる。

[29] European Network and Information Security Agency:欧州 ネットワーク情報セキュリティ庁

[30] https://www.enisa.europa.eu/publications/exploring-cloud-incidents

### 2)　組織的な課題

#### 協力の欠如

デジタルフォレンジックは物理的環境などの情報源から証拠を収集することが不可欠である。しかしながら、クラウド環境においては、クラウド事業者の敷地内にある物理的環境から証拠を収集するためにはクラウド事業者からの協力無しでは不可能である。クラウド事業者がこの領域を外部委託している場合は、委託先業者のフォレンジック調査の関与が必要となる可能性がある。

### 3)　法的な課題

#### 国境を超えたインシデント

国境を超えたインシデントの場合、クラウド事業者と法執行機関の連携は更に重要かつ複雑になる。最悪の場合、関与する国の法執行機関またはクラウド事業者が連携しなければ、証拠の収集は不可能となる。国境を超えたインシデントでは、法的手続は法的障害や各国間の法制上のギャップに衝突する可能性があるため、証拠収集に時間を要する。

# ■ 5. クラウド活用の心得

3 章では金融におけるクラウド活用のトレンドやクラウドのもたらす便益或いは、クラウド上で発生しているセキュリティインシデント事例について述べた。また、4 章では今後金融機関での活用が広がる可能性のある IaaS や PaaS を中心に、クラウドの活用段階毎の考慮事項を整理した。

最後となる本章では、執筆者が本報告書をまとめる過程で得た、クラウドを活用していく上での示唆を、「心得」として改めて述べたい。

## 5.1. 十分なリスク管理が必要。しかし恐れ過ぎない

クラウドはオンプレミス環境に比べ、迅速にシステムを構築できる手軽さや設定変更の容易さが特徴の一つである。また、契約形態の多くも従量課金方式であることから、試行的な活用や、必要なときだけ活用するといった柔軟さも兼ね揃えている。しかもクラウド事業者は、市場のニーズに合わせ新しいテクノロジーを取り込み、新機能やサービスを提供していく。こうした最新テクノロジーへのリーチのしやすさもクラウドの大きなメリットの1つである。

しかし、その手軽さや高機能を生み出す変化の多いサービス形態は、使い方を誤ったり、知識が不足しているとセキュリティの欠如を招き、ビジネスに重大な悪影響をもたらすインシデントを発生させる虞がある。海外の大手金融機関においてもクラウドを活用するための準備は慎重に進めていることが今回の調査でうかがえた。

「手軽に便利な機能が使える」或いは「コストが安くなる」といった近視眼的な発想で、安易にクラウドの活用を決断することは避け、クラウドの活用に向けては、しっかりとした事前の態勢整備や検討を行い取り組んでいくことが重要である。

他方で、そのクラウド活用に伴うリスクを過度に意識し、あまりにも「安全性」に偏りすぎた判断をしてしまうと、デジタル化の波から取り残され、機会損失を招く虞もある。もちろん安全性、信頼性の確保は金融システムの大前提であるが、リスクベースアプローチに基づいた合理的な判断と戦略が求められる。

したがって、例えば、クラウド活用の初期段階では、ミッションクリティカルな業務、顧客影響のある業務をクラウドで活用することは避け、比較的リスクが低い「周辺領域」のシステム等からクラウド化を進めるといったアプローチが考えられる。国内外でクラウドの活用を推進している金融機関でも概ねこのアプローチが常道となっている。金融機関は、クラウド活用に関する自らの成熟度を意識しながら、社内人材の経験と知見を積み重ねることが重要である。

クラウドの特徴の1つは従量課金制である。初期費用を少なくサービスを開始できることから、想定より効果が見込めなくても、追加のコストや資産の償却無く撤退できる点も意識しておくとよい。

## 5.2. クラウド人材が成功のカギを握る

クラウド人材の適切な育成と活用が導入成否のカギとなる。ここ数年、我が国の金融分野では金融機能のアンバンドリングとリバンドリングが起きており、テクノロジーを最大限活用した、フットワークが軽い金融ビジネスを展開する企業も増えている。伝統的な金融機関がこうした新興金融サービス企業と連携するのかライバル関係

となるのかはケースバイケースだが、いずれの場合でも、そうした企業のように市場ニーズを適時に予測しスピーディーにサービスを展開または改善していくビジネスモデルと連携、或いは対峙することになる。

伝統的な金融機関が、こうした流れに対応するためには、クラウドの活用を通じてリソース調達の柔軟性や開発スピードの俊敏性を高めることが必要になるだろう。そしてそれを実現するためには、4 章でも述べた通り、要となるクラウド人材やチームが不可欠となる。予めクラウドの知識を豊富に持つ人材は多くはないため、金融機関には、教育・研修のための人材育成投資が欠かせないが、クラウドは責任分界モデルであるため学ぶべき知識領域はオンプレミス程広くない。また、学習の手段も様々存在する。社内での知識共有はもちろん、クラウド事業者の提供するセミナーや勉強会、クラウド利用者で運営されるユーザ会なども存在するケースもあるため、こうした機会を積極的に活用することが有効である。また、オンプレミスとは異なり、大きな時間やコストをかけずに実験的に仮想マシンを構築しハンズオンを実施することもできる。金融機関では、こうしたクラウドの特徴やメリットも活用しながら、要となる人材の育成を進めるべきであろう。

なお、1 点検討すべきはクラウドに精通した外部の専門家の効果的な活用である。金融機関が内部で専門人材を育成するには、一定の時間を要する一方、その間もクラウドは各種サービスや機能が新しいものへ変化していく。したがって、クラウドに関する最新の知識や専門性を内部人材にのみに頼るのは現実的ではない。クラウドの特性と同様に、「必要な時に必要なリソースを」といった考え方をクラウド人材にも適用し、金融機関内部に必要なクラウド人材像と外部の専門家を活用する領域を整理した上で、外部リソースを効果的に活用しながら、自組織の鍵となるクラウド人材の育成を推進していくべきである。

## 5.3. クラウドを学ぶのはシステム部門だけではない

金融機関がクラウドを用いて、市場ニーズに合うサービスをスピーディーに展開または改善していくためには、従来のシステム開発モデルのみでは難しく、システムベンダーや IT 専門の人材だけがクラウドの知識を持っていればよい時代ではなくなるだろう。

むしろ「サービス企画」から「サービス設計」、「サービス実装」、「サービス運用」といった広範な知識を持つ人材によるシステム開発への関与を高める必要がある。すなわち、サービスニーズの創出はビジネス部門が担い、テクノロジーを用いてそれを形にするのが IT 部門といった従来の分担の垣根は、クラウドを活用する中で、相当程度低くなるか、不要になるのかもしれない。事実、あるクラウド事業者のベンダー資格認定では、2017 年から 2018 年で資格取得者数が倍増したが、いわゆる IT 人材ではない、エンドユーザに限定すると 2.5 倍に増加したとも言われている。金融機関では、これまでもビジネス部門自らがシステム開発を担う EUC という形態が存在するが、クラウドを活用し SoE や SoI といったより顧客志向のシステムを構築する上では、ビジネスを推進する部門側がクラウドに関わる知見を有することも重要となる。

また、クラウドの導入にあたっては、社内のリスク管理部門や内部監査部門が適切に牽制機能を果たす必要があるが、そうした部門がクラウドに対する理解不足、知識不足となると、大きなリスクを抱えたままクラウドの活用が推進されたり、またその逆として無用なブレーキとなる虞もある。

アクセルとブレーキのバランスを適正に保つのは他でもない経営陣の役割であるが、ともするとブレーキ機能の整備は、後回しにされがちである。今後クラウドを活用してスピーディーにビジネスを展開していくためにも、経営陣には自らも含めて、全社レベルでクラウドが正しく理解されるための体制と環境整備が求められる。

# ■ 6. 参考文献

クラウドを安全に利用することを目的として、海外の当局等が金融機関に向けて公表している刊行物を一部紹介する。海外金融当局等の視点は、必ずしも我が国の金融当局の視点と一致するとは言えないが、各金融機関が今後クラウドの活用を検討する上で、よい参考材料となると考えられる。

### 1) 国際決済銀行「Insight No.13」(2018)

クラウドを外部委託の一部として捉え、保険業界や金融機関が考慮するべき各国(主にアジア圏)の規制の動向や、クラウド事業者を監督するアプローチについて記述された公表物である。特筆するべき点として、近年ますます多くの保険業や銀行業界がクラウド事業者の限られた資源に依存していることに言及し、サービス障害の場合に感染の脅威が高まるといった集中リスクについて懸念を表明し、集中リスクを監督するためのフレームワークを現在構築途中であることが述べられている。また、クラウド事業者との契約において、クラウド事業者の下請けに対する要件の明確化について述べており、ある規制当局は、クラウド利用者に対し、クラウド事業者およびその下請けを含む重要な全てのサービス提供者を特定し、サプライチェーン全体で当局要件を順守することを期待しているといった言及もなされている。他にも、イグジットプランについて言及し、クラウド利用を終了する際は、アウトソーシングしている業務を過度に中断すること無く、十分かつ包括的に事前検証された文書化された手法にて、クラウド終了計画を立案することをクラウド利用者に期待していることについて述べられている。

### 2) シンガポール銀行協会「Cloud Computing Implementation Guide」(2016)

シンガポールの銀行に向けたクラウド活用時の情報セキュリティコントロールに関するガイドラインである。クラウド環境をセキュアに扱うための考慮事項およびグッドプラクティスがまとめられている。ガイド策定に向けたタスクフォースには、グローバルでビジネスを展開している大手金融機関がメンバーとして名をつらねており、考慮事項やグッドプラクティスは実態に即して詳細に述べられている。例えば、セキュリティイベント監視とインシデント管理については、様々な監視システムからセキュリティログを自動分析、相関づけし、トリアージを提供するために SIEM などの監視インフラストラクチャの導入の必要性や、セキュリティインシデントの定義とさまざまなレベルの重大度を適切に定義し、C-SIRT 組織を金融機関とクラウド事業者で調整および合意する必要性などについて述べられている。他にも、クラウド事業者の災害復旧および事業継続を可能な限り、金融機関とクラウド事業者と共同でテストすることや、暗号鍵の保管として明示的に HSM を指定し、暗号化鍵と HSM の場所、所有権、管理に関する詳細を両社で合意することなどが述べられている。

ご注意

本報告書内に記載されたインターネット上の URL は 2019 年（平成 31 年）3 月現在のものであり、URL およびその内容は、その後、変更、移動、削除される場合がある。

2018 年（平成 30 年）度　金融庁委託調査

クラウドコンピューティングとサイバーセキュリティに関する調査報告書

PwC あらた有限責任監査法人

2019 年（平成 31 年）3 月 31 日　発行