BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

クラウドサービス利用における リスク管理上の留意点

日本銀行
金融機構局
2020年11月

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

（金融システムレポート別冊シリーズについて）

日本銀行は、マクロ・プルーデンスの視点からわが国金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年 2 回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を不定期に行い、『金融システムレポート』を補完するものである。本別冊では、クラウドサービスの利用におけるリスク管理上の留意点について解説する。

（本別冊の要旨）

クラウドサービス（以下、クラウド）とは、共用のコンピューター資源（サーバー、ミドルウェア、ストレージなど）をネットワーク経由で利用するサービスであり、多くの金融機関においてシステムを構築する上で不可欠なものになっている。また、デジタル・トランスフォーメーション（DX）の潮流の下で、新たなデジタル技術の活用の有力な選択肢となることも多く、金融機関の経営陣においてもクラウドについて一定の知見を有することが必要となっている。こうした中、金融機関からは、クラウド利用に対し、クラウドの特性に起因するセキュリティや可用性の不安などが懸念事項として挙げられている。

本稿では、そうした懸念を払拭するために対応すべき重要な事項を、「セキュリティ管理」、「可用性管理・レジリエンス」、「委託先管理」の順に整理し、さらにクラウドに期待されるメリットを享受するための「コスト管理」、「開発体制・人材確保」、「利用方針の策定」について解説を加えた。また、（別紙）には、金融機関やベンダー等の協力の下で得られた情報を基に、これらの重要な事項に対応する管理項目と取組事例を取り纏めている。

本稿が、金融機関の経営トップをはじめとする、各関係者のクラウドの利用とリスク管理に関する適切な認識の共有や、クラウドに関するリスク管理体制の整備等を通じた、IT ガバナンス維持・向上の一助になることを期待する。

【目　次】

Ⅰ．はじめに

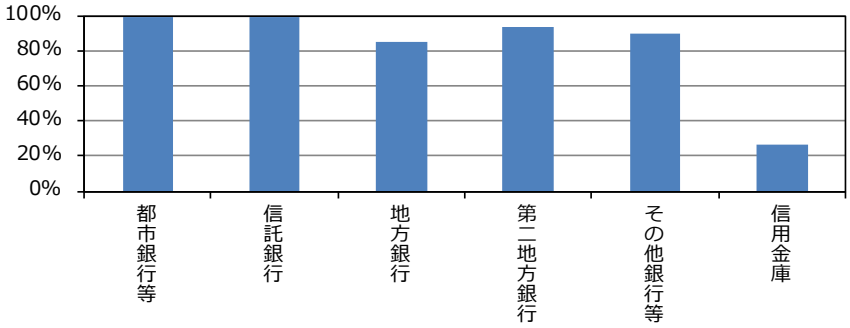
クラウドサービス（以下、クラウド）とは、共用のコンピューター資源（サーバー、ミドルウェア、ストレージなど）をネットワーク経由で利用するサービス[1]である。従来型のコンピューター資源を自ら設置し管理する形態（オンプレミス）と比べ、導入期間の短縮、運用・管理負担の軽減、コスト抑制、先端技術の活用等のメリットが指摘されている（図表 1）。

図表 1 クラウドの利用を通じて期待されるメリット

メリット	概要
導入期間の短縮	コンピューター資源を、簡便な手続きで速やかに利用できる
運用・管理負担の軽減	ハードウェアや OS、アプリケーションに関する運用・管理負担のうち、クラウド事業者が管理する範囲について、その負担を軽減できる
コスト抑制	コンピューター資源の共有によるスケールメリット、柔軟なコンピューター資源の調達、システム廃棄コストの軽減を通じ、システムに要するコストを抑制できる
拡張性、柔軟性の享受	小規模なシステムを開発し、利用者の増加に合わせてリソースを拡張するといった柔軟な使い方ができる
先端技術の活用	先端技術（例：AI や機械学習）の提供をクラウド事業者から受けることができる
セキュリティレベル向上	クラウド事業者が提供する高度なセキュリティ対策を利用できる

本邦金融機関におけるクラウドの利用状況をみると、「都市銀行等」は全ての先、「地方銀行、第二地方銀行」は 8～9 割の先に達しており（図表 2）、多くの金融機関において、システムを構築する上でクラウドは不可欠なサービスとなっている。わが国の政府でも、情報システムの調達においてクラウド利用を優先する方針「クラウド・バイ・デフォルト原則[2]」が打ち出されており、クラウドの認知度は飛躍的に高まりつつある。

図表 2 クラウドの利用状況



（資料）公益財団法人金融情報システムセンター「令和元年度金融機関アンケート調査結果」

[1] NIST（National Institute of Standards and Technology、米国国立標準技術研究所）ではクラウドを「共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるもの」（独立行政法人情報処理推進機構による翻訳）と定義している。

[2] 「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」（平成 30 年 6 月 7 日 各府省情報化統括責任者（CIO）連絡会議決定）において、政府情報システムを整備する際に、クラウドの利用を第一候補とする原則が採用された。

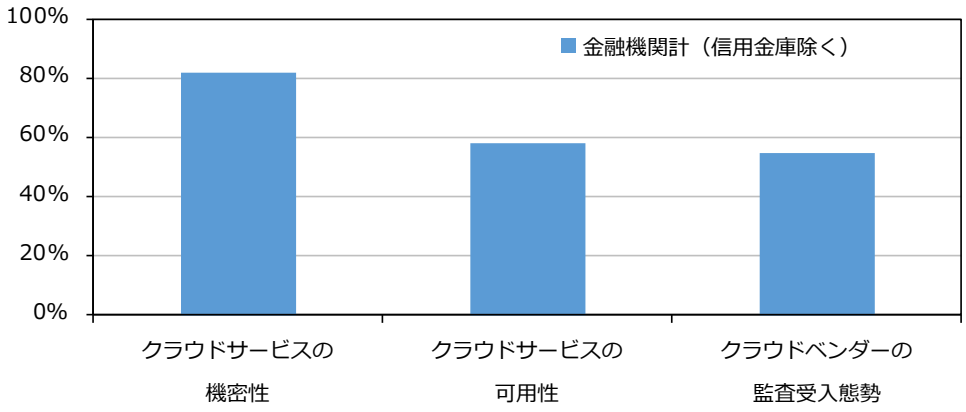
この間、デジタル・トランスフォーメーション（DX）の潮流の下、わが国の金融機関では、国内預貸業務の低収益性に対処すべく業務改革等に取り組む中で、新たなデジタル技術の活用の機運が高まっており、ここでもクラウドの利用が有力な選択肢として検討の俎上に上ることが少なくない。このため、金融機関の経営陣は、たとえシステム担当でなくとも、所掌する業務の改善・改革のためにクラウドについて一定の知見を有することが必要となっている。

本稿では、まずクラウド利用に際して金融機関の経営陣から懸念の声が上がることが多いセキュリティなどの問題の背後にあるクラウドの特性を整理する。次いで、そうした懸念を払拭するために経営陣が対応すべき重要な事項である「セキュリティ管理」、「可用性管理・レジリエンス」、「委託先管理」に関する留意点を整理する。最後に、コスト抑制や先端技術の活用といったクラウドに期待されるメリットを享受するための「コスト管理」、「開発体制・人材確保」、「利用方針の策定」について解説する。

Ⅱ．クラウドの特性と金融機関が抱く懸念

公益財団法人金融情報システムセンターが公表した「令和元年度金融機関アンケート調査結果」をみると、クラウド利用に対する懸念として、８割以上の金融機関[3]が「クラウドサービスの機密性（アクセス管理、暗号化管理等）」、５割以上が「クラウドサービスの可用性（稼働率、稼働時間帯）」および「クラウドベンダーの監査受入態勢」を懸念事項として挙げている（図表 3）。こうした懸念は、以下に掲げるクラウドの特性から生じている。

図表 3 金融機関が挙げるクラウド利用に対する懸念事項



（資料）公益財団法人金融情報システムセンター「令和元年度金融機関アンケート調査結果」

（ネットワーク経由の利用と機密性）

コンピューター資源を、インターネットを含むネットワーク経由で利用できるサービスであるクラウドは、保管されているデータ等へのアクセス権限、セキュリティ確保のためのファイアウォールの設定などについて、利用者が直接的に責任を負うことも少なくない。このため、利用者が設定ミスを起こすと、ネットワーク経由で機密情報が流出するリスクがあり、その影響は甚大となるおそれがある。こうした特性が、クラウドの機密性に関する、金融機関の懸念に繋がっている。

（コンピューター資源の共用と可用性）

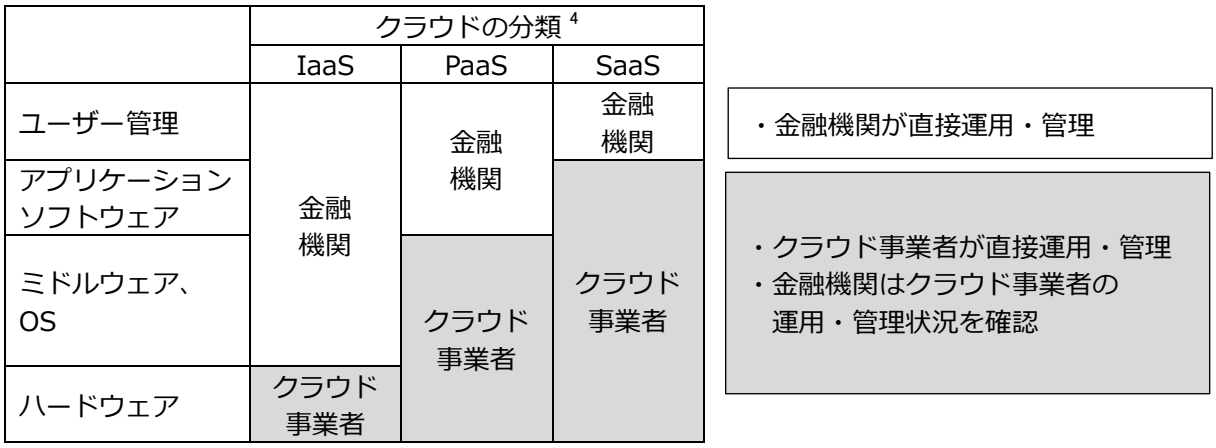
システムが停止する要因の一つに、ハードウェアや OS 等のメンテナンスがあるが、クラウドでは他の利用者とコンピューター資源を共用するため、システムのメンテナンスの実施時期について、事前調整が可能なオンプレミスと異なり金融機関側でコントロールすることが難しいことが多い。こうした特性が、クラウドの可用性に関する、金融機関の懸念に繋がっている。

[3] クラウドを利用している先が少ない信用金庫を除くベース。

（責任の共有と委託先管理）

クラウドでは「責任共有モデル」と呼ばれる枠組みにより、クラウドの運用・管理を利用者（金融機関）とクラウド事業者で分担する。このうちクラウド事業者が運用・管理する範囲についても、金融業務のベースとなる情報およびその情報を取り扱うプロセスの管理に関しては金融機関側に責務が生じることから、委託先管理の枠組みの下で必要な管理水準を確保することが金融機関に求められる（図表 4）。

図表 4 責任共有モデルの下で金融機関とクラウド事業者が運用・管理する範囲



ただ、委託先管理の一環として監査を実施する際、パブリッククラウドのように自身が利用しているコンピューター資源の特定が難しい場合等には、これまでの監査手法では対応できないケースもある。こうした特性が、クラウドベンダーの監査受入態勢に関する、金融機関の懸念に繋がっている。

4 クラウドはサービス内容により大きく以下の 3 つに分類される。
IaaS：ハードウェア等を提供するサービス
PaaS：アプリケーション等の実行環境を提供するサービス
SaaS：アプリケーションの機能を提供するサービス

Ⅲ．クラウドのリスク管理における留意点[5]

１．セキュリティ管理

クラウドにおいてセキュリティ管理のために求められることは、オンプレミスの場合と基本的には変わらない。すなわち、取り扱う情報の機密度に応じて、アプリケーションやデータ等へのアクセス管理、ファイアウォールの設定を含むネットワークセキュリティの確保、セキュリティパッチ[6]の適用、データの暗号化等の情報漏えい対策による保護などの措置を取ることである。

ただし、クラウドでは、「責任共有モデル」の下で、クラウド事業者が運用・管理し、この状況を委託先管理の枠組みで金融機関が確認すべき範囲と、金融機関が自身で運用・管理する範囲とに分かれる点に留意する必要がある。

例えば IaaS では、金融機関は、ハードウェア等を除く広い範囲を自身で運用・管理することになる。このためセキュリティについても、ネットワークの設定やソフトウェアのセキュリティパッチの適用等を含め、システム設計・運用上の自由度は高く、多くを金融機関自身で管理する必要がある。一方、SaaS では、金融機関が自身で運用・管理する範囲は、アプリケーションへのアクセス権限の設定等、ユーザー管理に絞られることが多い。

過去のクラウドへの不正アクセスや情報漏えいの多くは、システムやデータへのアクセス権限やネットワーク等に関する利用者の設定ミスにより発生[7]しており（図表 5）、本番環境に比べ管理が緩やかになりがちな開発環境の構築時や、オンプレミスからのシステム移行時にその傾向は強くなっている。2019 年に発生した、米国の大手金融機関における大量の顧客情報の漏えい事案では、監督当局から当該金融機関に対し、システムのクラウドへの移行にあたり、効果的なリスク評価プロセスの確立を怠った、ネットワークの設定や情報漏えい対策といったクラウド環境における適切なリスク管理の確立を怠った、といった問題が指摘されている。

図表 5 クラウドのセキュリティ管理・対策の不備により発生したインシデント事例

	概要
アクセス管理	・クラウドへシステムを移行した際、機密情報を誤って一般閲覧可能の設定にしたため、URL を入力すれば誰でも閲覧可能となり、機密情報が漏えいした。 ・アクセス時の認証を適切に行っていなかったため、パスワード総当たり攻撃による侵入を許し、クラウド上の情報資産を全て消去されてしまい業務を継続できなくなった。

[5] 本留意点は可能な限りクラウドの分類（IaaS、PaaS、SaaS）によらず汎用的に記述している。

[6] OS やソフトウェアの情報セキュリティの問題(脆弱性)を解決するために提供される修正プログラムのこと。

[7] 米国国家安全保障局「Mitigating Cloud Vulnerabilities」（2020 年 1 月）

ネットワーク セキュリティ	・クラウドに開発環境を構築した際、テストのために一時的に格納した機密情報の消去を失念し、さらにファイアウォールの設定ミスにより外部からアクセスできる状態になっていたため、パスワード総当たり攻撃を受け、機密情報が漏えいした。 ・WAF[8]の初期設定に関する認識不足に起因する設定不備があったため、WEB サーバーに対して WEB アプリケーションの脆弱性を悪用した不正な指示が行われ、大量のデータが流出した。
セキュリティ パッチの適用	・データベース管理システムへのセキュリティパッチの適用漏れから外部の第三者がデータベースにアクセスできる状態になっていたため、ランサムウェア[9]による攻撃を受け、クラウド上のデータが全て利用できなくなった。
情報漏えい対策	・顧客情報の漏えいにおいて、顧客の機微情報やパスワードを暗号化せずに保存していたため、被害が甚大になった。

このため、金融機関の経営陣は、委託先管理の枠組みでクラウド事業者の運用・管理状況を適切に確認した上で、自身でも以下の点に十分な注意を払いセキュリティを管理する必要がある。特に、新型コロナウイルス禍への対応でみられたように、短期間でクラウド上に在宅勤務用のシステム開発環境を新たに構築する場合などには、アクセス権限やネットワークの設定ミスが生じやすいため留意する必要がある。また、金融機関が自身で各種設定の適切性を確認することが難しい場合は、クラウド事業者が提供しているツールや第三者による診断サービスを活用することも一案である。

（1）アクセス管理

不正アクセスを防止する観点から、システムやデータへのアクセス権限者やその権限の範囲を必要最低限に限定することが必要である。また、多要素認証[10]等の活用によりアクセス時の認証を厳格に行うことも有効である。特に、クラウドへのアクセス権限の設定や、クラウド上のサーバー等の起動・停止が可能な「管理コンソール[11]」については、金融機関が運用・管理する範囲となるため厳格な管理が求められる。

（2）ネットワークセキュリティ

インターネット経由での不正な通信を遮断するためのファイアウォール等によるアクセス経路の限定など、利用するクラウドに応じてネットワークの設定を適切に実施する必要がある。また、機密性の高い情報をインターネット経由で取り扱う場合には、VPN[12]等の暗号化技術を用いた保護なども求められる。

---

[8] ウェブアプリケーションの脆弱性を悪用した攻撃等からウェブアプリケーションを保護するソフトウェア、またはハードウェアのこと。Web Application Firewall の略。

[9] コンピューターウイルスの一種。感染するとデータが勝手に暗号化されるとともに、元に戻すための金銭等の要求が行われる。Ransom（身代金）と Software（ソフトウェア）を組み合わせた造語。

[10] 記憶情報（パスワード等）、所持情報（IC カード等）、生体情報（指紋等）などのうち複数要素の認証を組み合わせて、本人であることを確認する方式のこと。

[11] 仮想マシンの追加・削除、ユーザー管理、ネットワーク設定等、クラウドの設定を自由に操作できる管理機能のこと。

[12] 暗号化技術等を用いて構築した仮想的なプライベートネットワークのこと。Virtual Private Network の略。

（3）サイバー攻撃に関する情報収集と対策

金融機関が直接運用・管理する範囲については、自身でクラウドへのサイバー攻撃やクラウド関連製品の脆弱性に関する情報を収集し、OS、ソフトウェア、VPN 製品等へのセキュリティパッチの適用や各種設定の見直し等の対策を適時適切に行うことが求められる。また、セキュリティ上の不備が発生していないか、定期的に診断を行うことも有用である。

2．可用性管理・レジリエンス

可用性の管理にあたっては、業務内容により求められるシステム停止時間の許容水準の違いを踏まえ対応することが重要である。例えば、勘定系システムのように非常に高い可用性を求められるシステムの場合、複数のデータセンター（ゾーン [13]）を利用した冗長構成の確保や、クラウド事業者との特別なサポート契約の締結などの手段により、高い可用性を確保することが考えられる。他方、開発用のシステムや時限性の低い業務に関するシステムの場合、求められる可用性の水準を踏まえた、メリハリをつけた対応をすることも一案である。

また、クラウドの場合、メンテナンスの実施がクラウド事業者の WEB サイトや管理コンソール等で通知されるだけの場合が多いほか、クラウド事業者側の原因でサービスが停止した場合でも、通常は個別に連絡が行われることはなく、WEB サイトや管理コンソール等で障害情報が通知される場合が多い。このため、WEB サイトや管理コンソール等で通知の有無を定期的に確認するなど、金融機関が主体的に情報を収集し、システムへの影響を確認し対応することが求められる。

この他、クラウドのサービス停止等を想定したレジリエンス [14]の確保も重要である。

3．委託先管理

「責任共有モデル」の下、クラウド事業者が運用・管理する範囲については、金融機関は委託先管理の枠組みを用いて、金融機関の業務を行う上で求められる管理水準を確保する必要がある。

クラウド事業者に対する委託先管理でも、事業者の選定・契約や運用状況の確認など、管理のポイントは通常の委託先管理と大きく変わらないが、約款やサービスレベルの改訂の頻度が高いことや運用状況の確認方法など、クラウド事業者特有の留意点もあることから、これを踏まえた管理を行うことが重要である。

---

[13] クラウドのサービス提供やデータ保管を行うデータセンターの集合体のこと。

[14] 障害、自然災害、テロ、サイバー攻撃等が発生しても重要業務を継続できる能力のこと。

クラウド事業者の運用状況についても、セキュリティや設備等が求められる水準を満たしているか確認することの重要性は変わるものではなく、利用者（金融機関）は統制対象クラウド拠点[15]に対する監査といった確認手段を確保する必要がある。クラウド事業者の運用状況の確認にあたっては、クラウド事業者が公表しているSOC2レポート[16]や監査報告書等を活用するほか、重大なインシデントに備え金融機関自身で統制対象クラウド拠点に対する監査権を確保するのも一案である。

また、クラウドにおけるセキュリティ対策の実施状況を確認する際、「ISO/IEC 27017」や「ISMAP[17]」、「JASA クラウドセキュリティ推進協議会 CS ゴールドマーク」、「（米国の）FedRAMP」といった認証制度を活用することも一案である。

この他、重要業務の委託先については、その委託先がクラウドを利用しているか確認し、利用している場合は、クラウドのリスク管理の状況を確認することも重要である。

４．コスト管理

クラウドに期待されるメリットの一つとしてコストの抑制が挙げられる。しかし、オンプレミスからクラウドに移行すれば必ずコストを抑制できる訳ではなく、適切なコスト管理を行うことで、初めてメリットを享受できる。

まず、コスト抑制効果に関して留意すべきは、移行する業務の性質により効果が大きく異なる点である。例えば、リスク量計算や決算処理など事務量の変動の大きな業務に関するシステムの場合、ピーク時のリソースを平時も含めて用意する必要のあるオンプレミスと比べ、クラウドは事務量の変動に応じサーバー、ネットワーク等のリソースの使用量を柔軟に変更できるため、コスト抑制効果が得られることが期待される。逆に事務量の変動が小さい業務に関するシステムの場合、コスト抑制効果が限定的となる可能性がある。

また、システムに求めるサービスレベルもコスト抑制効果を左右する。例えば、勘定系などの高い可用性が求められるシステムをクラウド上で構築する場合、システムの冗長化やクラウド事業者との間での特別な保守契約の締結といった対応が必要となり、この分のコスト

---

[15] 公益財団法人金融情報システムセンターの安全対策基準で定める「統制対象クラウド拠点」のこと。クラウド事業者への統制上必要となるデータへのアクセスが可能となる情報処理拠点等、実質的な統制を行うにあたり対象となる事業拠点を指し、クラウド事業者の本社、営業所、データセンター、オペレーションセンター等様々な拠点が候補となる。

[16] 業務受託企業のセキュリティや可用性等の内部統制状況を対象に、監査法人が外部監査の国際認証（Service Organization Control）に従って、その有効性を検証した結果の報告書。

[17] 政府でもクラウドの導入円滑化の観点から、2020 年度内に、政府が定めた基準に基づいたセキュリティ対策を実施していることが確認されたクラウドをリストに登録する制度（政府情報システムのためのセキュリティ評価制度＜ISMAP＞）を開始する予定。

が増加する可能性もある。

このため、事前にコストシミュレーション等を行うことで、クラウドに移行した場合に想定されるコスト抑制効果を把握し、クラウドに移行した後も、クラウド利用にかかるコストを継続的に管理する体制を整え、想定外のコストの上振れを早期に発見・把握できるようにすることも重要である。

５．開発体制・人材確保

クラウド事業者が提供するサービスでは、最新技術が積極的に取り入れられることが多く、クラウドが提供するサーバーやデータベース等の仕様の変更も頻繁に行われるため、こうした仕様の変更に対応できる開発体制の整備が重要である。

クラウドの最新技術に速やかに対応できる開発体制を整備するとともに、これに応じたリスク管理体制を機能させるためには、基盤となる人材の確保も重要になる。利用するクラウドのサービス内容や技術に精通し、セキュリティやサービスレベルの管理、クラウドを用いた開発などができる人材を、内部人材の育成や外部人材の採用等により確保することが課題となる。

クラウドは、AI や機械学習等の先端技術を含むサービスが使いやすい環境でもある。例えば、クラウドの特徴であるサーバーやストレージの柔軟な拡張性と組み合わせ、大量データをクラウド上に移し、クラウドで提供されている AI や機械学習等の先端技術で分析することで、新たなビジネスモデルの構築や市場予測を行う、といった使い方も考えられる。

６．利用方針の策定

クラウドは、インターネット等のネットワーク経由でコンピューター資源を共同利用するサービスであるという特性上、「Ⅱ．クラウドの特性と金融機関が抱く懸念」で言及した通り、「機密性」、「可用性」に関してオンプレミスと異なるリスク特性を抱えている。

このため、クラウドの利用を進めるにあたっては、「機密性」、「可用性」の観点からクラウドで構築可能なシステムの範囲を予め定めた上で、そのシステム毎に、オンプレミスで構築する場合と比較した、導入期間の短縮や運用・管理負担の軽減、コスト抑制といったクラウドのメリットの享受度合を見極めながら、移行可否を判断することが適当と考えられる。また、導入に合わせて、「１．セキュリティ管理」や「２．可用性管理・レジリエンス」等で示した通り、クラウドの特性を踏まえたリスク管理体制の整備も求められる。

Ⅳ．おわりに

デジタル・トランスフォーメーション（DX）の進展に伴う環境変化への対応は金融機関経営にとって重要課題であり、こうした環境変化を前向きな収益の向上に結び付けるために、クラウドの利用拡大を志向する金融機関も増加している。

クラウドの利用にあたっては、セキュリティへの不安などが懸念事項として挙げられるが、金融機関の責任範囲については自身で適切にリスク管理を行い、クラウド事業者の責任範囲は委託先管理の枠組みで適切にリスク管理を行えば、必ずしもオンプレミスと比べリスクが高い訳ではない。また、そのリスク管理の内容も、ネットワークを通じたシステムの利用であることや、クラウド事業者との契約関係に基づいて金融機関側とクラウド事業者側に求められる責任範囲を予め明確にしておくことなど、基本的な点を把握すれば決してハードルの高いものではない。

本稿の（別紙）「クラウドサービス利用において必要な管理項目と具体的な取組事例」は、上記のポイントに沿って、クラウド導入の検討段階からの管理項目を時系列に整理したものである。別紙に記載されている取組事例は、金融機関やベンダー等の協力の下で得られた情報を取り纏めたものであり、金融機関の経営トップをはじめとする関係者間のクラウド利用とリスク管理に関する適切な認識の共有や、クラウドに関するリスク管理体制の整備等を通じた IT ガバナンス維持・向上の一助となることを期待する。

もっとも、本稿は、金融機関に一律の取り組みを促すことを目的としたものではなく、業務やシステムの重要度等を踏まえ、リスクベースで対応すべきものである。また、他の方法によるリスク統制を妨げるものでもない。日本銀行としては、今後も、考査・モニタリングやセミナーなどを通じて、金融機関の自発的な取り組みを後押ししていく方針である。

以　上