金融業界のパブリッククラウド利用
―コンプライアンスの基準とガバナンスのポイント―

金融業界においても、パブリッククラウドへの注目が高まっている。パブリッククラウドは利便性が高い一方で、経営側には、リスクをコントロールし、万が一の有事の場合には適切な対応を行うことが求められている。本稿では、金融業界のシステムでパブリッククラウドを利用する際に必要な、統制面における検討すべきポイントを解説する。

野村総合研究所 クラウドサービス事業本部
クラウドサービス統括部 上級システムエンジニア
内田（うちだ） 英里（えり）
専門はクラウドサービスの統制設計、運営

パブリッククラウド利用への懸念

各業界においてパブリッククラウドの利用が拡大するなか、金融業界においてもパブリッククラウド利用への注目が高まっている。

パブリッククラウドの利用は、システム開発スピードの向上、キャパシティプランニングの柔軟性、災害対策のメリットがある。一方で、金融機関におけるパブリッククラウドの利用は、ガバナンスにおける懸念や不安がある。金融情報システムセンター（FISC）の金融機関アンケートでは、「クラウドサービスの利用に対する懸念・不安について、該当する項目をいくつでも結構ですので選択してください」との質問に対して、「クラウドサービスの機密性」「セキュリティ事故発生時の対応」「クラウドベンダーの監査受入態勢」が回答の上位に並んでいる（FISC金融情報システムセンター『金融機関におけるクラウドサービスの活用動向』平成31年3月15日の調査）。

オンプレミスでは、システムを構成するデータセンターからアプリケーションまでを自社でコントロールできるが、パブリッククラウドの利用に際しては、管理の一部をサービス事業者へ委託することになる。委託した範囲については、直接的なコントロールはオンプレミスのようには効かないが、オンプレミス同様のリスク管理が求められる。

パブリッククラウド利用におけるコンプライアンス対応

パブリッククラウドでは、サービスの利用者がクラウドサービスを安全に利用できるよう、セキュリティや継続性に関わる情報を資料としてまとめて情報開示を行っている。また、サービス事業者自身の運営の有効性を客観的に示すため、業界基準や規格に基づいて、第三者による監査や審査を定期的に受け、各種の認証を取得している。その種類は多岐にわたり、米国公認会計士協会が定めた3つの報告書のなかのSOC1（System and Organization Controls。業務受託会社による内部統制の保証を報告するものとして、うちの1つで、財務報告に関わるもの）、SOC2

（セキュリティ、可用性、処理の誠実さ、機密保持およびプライバシーに関わる内部統制の報告書）、PCI DSS（Payment Card Industry Data Security Standard。クレジットカード業界におけるセキュリティ基準）、ISO27000シリーズ（国際標準化機構が設定するセキュリティマネジメントシステムに関する規格）などが挙げられる。

パブリッククラウド利用時のガバナンスにおける検討ポイント

経営側は、システムの用途（情報系、勘定系、OA系など）によってリスクの発生頻度や影響度を考慮して、そのシステムをどのような技術を使って構築するかを選択する。すなわち、オンプレミスで構築するか、パブリッククラウドを利用するかなど、どういったサービスを利用するかは、システムの用途と安全性やリスクを勘案した上で決められる。パブリッククラウド利用における安全性に関わる基準の整備や、サービス事業者によるコンプライアンス対応が進むなか、統制面で検討すべきポイントは次の3点である。

1点目は、パブリッククラウドで提供される内容とその統制を理解し、対策を行う必要性がある。主要なパブリッククラウドでは、システムの構成要素について、サービス事業者と利用者の双方で役割分担するモデルを採用している。そのため、それぞれが管理する範囲の統制、およびその境界や補完し合う関係に関わる統制を整備する必要がある。サービス事業者の管理範囲に対しては、サービス事業者自身がどのような統制を行っているかを確認する必要がある。サービス事業者が発行するSOC1レポートやSOC2レポートなどでの確認が有効である。一方でユーザーは、セキュリティへの対策が必要である。例えば情報漏えいの対策としてデータを保護するため、データの暗号化、暗号鍵の管理、IDとアクセスの管理、監査ログ管理などがある。各サービス事業者が提供するセキュリティサービスを活用することも可能である。利用の際には、サービス内容の比較検討を行いたい。

2点目は、監査権の確保が挙げられる。特に金融機関における重要なシステムでパブリッククラウドを利用する際には、サービス事業者に対し、情報提供はもちろん、設備の現地視察なども含んだ監査権を契約に含めることが望ましい。また、サービス事業者が提供する金融統制に対応するためのプログラムなども、内容を踏まえて利用を検討したい。

3点目は、適切な運営を行っていてもシステム障害や事故が発生する可能性をゼロにすることは不可能であることを挙げておく。パブリッククラウドでの大規模な障害や、セキュリティ事故が発生した場合を想定し、経営層、システム担当者、クラウドサービス事業者、システムの運用委託先などの関係者と、連絡体制や対応について認識を合わせておくことが大事である。また、有事の際にきちんと機能するよう、連絡フローの確認などを定期的に実施することも推奨する。

パブリッククラウドの利用に必要なガバナンスの仕組みは、一度設計すれば終わりではない。変化する環境のなかで仕組みを改善し続けることで、リスクを低減させることが重要である。■