マルチクラウド時代、金融機関に求められる継続的なコンプライアンス対応のポイント

金融機関は常にさまざまなサイバー攻撃にさらされてきたが、課題はそれだけではない。グローバルに事業を展開するとなれば、各国の法規制の遵守、コンプライアンスも必須となる。

マルチクラウドが当たり前になりつつある今、どのようにそれを実現すべきだろうか。

ASAHI INTERACTIVE

サイバー攻撃は増加の一途をたどっていることは周知の通りだが、中でも最も狙われているのは「金銭」という価値を扱う金融機関だ。

米 IBM のセキュリティ研究機関である X-Force が、日々監視しているグローバルな脅威情報を基にまとめた調査によれば、サイバー攻撃の 19%は保険・金融業界を標的にしているという。この先 IoT 機器が増加していけば、サイバー犯罪者の侵入の糸口もまた増えることになる。一方で、それらを脅威から守るべきセキュリティ人材の不足は世界的に見ても明らかだ。

金融業界が抱える課題はそれだけではない。セキュリティ対策に加え、米国はもちろん、ヨーロッパや日本、アジア太平洋地域など各国がさだめる法規制に遵守し、コンプライアンスを維持していくことも求められる。

しかもそれを、ダイナミックに変化する環境の中で追求していかなければならない。今や金融機関の多くが、IT システムのモダナイゼーションに取り組み、従来からのオンプレミス環境から、マルチクラウド、ハイブリッドクラウド環境への移行を進めつつある。

このように、複数の課題に同時並行で取り組まなければならない金融機関は、いったい何を指針にすればいいのだろうかーー。IBM はそんな難問への答えを用意しているという。米 IBM IBM セキュリティ担当日本 IBM のシニア・マネージング・コンサルタント、ポール・ヨルゲンセン氏が、そのヒントを紹介した。

マルチクラウドを前提としたセキュリティとコンプライアンスの確保が課題に

とかく保守的と言われがちだった国内の金融機関でも、最近はクラウド採用の動きが広がっている。従量課金制で固定費が不要になる上、新サービスの展開・成長に合わせた柔軟な拡張が可能なクラウドの利点は、あらゆる業種で認められている。

ただ、一口にクラウド移行といっても利用状況もさまざまだ。ヨルゲンセン氏によると、単なるコスト削減を目的とした第 1 世代から始まったクラウド利用は、ハイブリッドクラウド環境で既存アプリケーションのモダナイゼーションに取り組む第 2 世代を経て適材適所で複数のクラウドサービスを使い分けるマルチクラウド環境を前提に、プロセスの革新に取り組む第 3 世代が大勢を占めてきた。

「今や、企業の 94%がマルチクラウドを利用している。複数のクラウドをどう組み合わせ、効率的、効果的に利用するかが問われている」

ただ、そこには課題もある。その最たるものがセキュリティだ。「複数のパブリッククラウドを使うのはいいが、その境界をどう乗り超えるか、それもセキュリティを確保しながら進めるかが課題だ」とヨルゲンセン氏は述べている。それでなくとも、クラウドに関しては、ただでさえ黎明期から「セキュリティ」が課題とされてきた。今もなお、企業の 91%が、クラウド展開に当たってセキュリティを懸念事項として捉えており、ビジネスをフルに加速できないでいるという。

しかも金融機関の場合は、セキュリティ対策に加えコンプライアンスの確保が必須要件だ。IT リスクはもちろん広くビジネスをとりまくリスクを洗い出し、複数のプラットフォームにまたがって統一された形でガバナンスを効かせていかなくてはならない。それも、人材が不足し、コストに制約があり、部署ごとに成熟度に差がある中での対応が求められている。

日本 IBM
シニア・マネージング・コンサルタント
ポール・ヨルゲンセン氏

グローバル金融機関にとっては避けられない、膨大な数の法規制への継続的な対応

金融機関、それもグローバルに事業を展開している金融機関にとって、コンプライアンスは非常に重要かつ重たい課題だ。

ヨルゲンセン氏の知るある金融機関では「24 の国・地域で事業を展開しており、従来型のセキュリティ対策に加えコンプライアンスが求められている。この会社の遵守対象となる法規制に関する文書を積み上げると、のべ 300 万ページに上る」という。その上、法規制は社会や技術の変化にともなって変わっていくため、一度コンプライアンスを満たしたから終わりというものではなく、常に更新し、対応し続けていかなければならない。

かといって金融機関として事業を展開する以上、規制を無視するわけにはいかない。仮に規制に反することがあれば、大きなペナルティが科される。違反した場合、最大で 1,000 万ユーロ、または前年売上高の４%の制裁金が科される EU の一般データ規則（GDPR）が顕著な例だ。また米国の金融業界では、2008 年から 2017 年までの 10 年間だけで、各種法規制違反への罰金額が 3,210 億ドルに達しているという。

このような事態を避けるには、ただセキュリティを強化し、コンプライアンスに対応するだけでは不十分だ。「反復可能な形で対応し、常に規制の状況をモニタリングし、必要に応じて新しいコントロールを取り込む環境を作り上げていかなければならない」

ちなみに、この金融機関は当初、自力でこうした体制の整備に取り組んだそうだ。だが、24 カ国もの法規制への対応はあまりに複雑過ぎ、手に負えないことが分かった。次に考えた選択肢は「外注」だが、そうすると今度はコントロールを自社ではなく外部に手渡さなければならず、金融機関としては受け入れられないことが分かった。

そこで行き着いたのが、マルチクラウド環境を前提とした「責任共有モデル」だ。マルチクラウドのメリットを享受しつつセキュリティを担保していく術としては、クラウドサービス事業者と自社とでやるべき事柄を分担していくアプローチが最適解だという。

金融業界特有の要件に適合した「HC3 フレームワーク」をベースに継続的な対応を

ただ、マルチクラウド環境でセキュリティやコンプライアンスを確保するには、いくつかの注意点がある。

まず、環境も法規制も動的に変化する以上、人手に頼っていてはさまざまな作業の一貫性が保てない恐れがある。これを避けるには、AI などを組み合わせ、できるところから自動化していく必要があるだろう。また、対応を一回きりで終わらせるのではなく、測定可能な状況を作り出し、反復していくことも重要だ。さらに、異なるクラウドサービスプロバイダーや SaaS の間で、一貫性ある形でデータの移行を管理する術も必要になる。

こうした課題を解決すべく IBM では、「三脚モデル」を提唱し、そのブラッシュアップに努めてきた。

三脚モデルは文字通り、３つの要素から構成されている。１つは、各種法規制が求める要件の「分析とマッピング」だ。２つ目は、クラウドサービスや SaaS を提供する事業者の「認定」で、異なるセキュリティレベルのプロバイダー間でのデータ移行を管理しやすくする。さらに、監視サービスや既存システムとの連携アダプタを提供し、標準化された形でデータを共有できる環境を整える。

これら３本の足の上で、金融業界向けに各種法規制に対応した「フレームワーク」を提供することで、セキュリティやコンプライアンス対応と、ビジネス価値の向上という２つの課題を両立するのが IBM 流のアプローチだ。

IBM では金融業界特有の要件に適合したフレームワークとして「Hybrid Cloud Continuous Compliance（HC3）フレームワーク」を提唱している。ハイブリッドクラウド、マルチクラウド環境を前提に、さまざまな法規制への遵守状況を一元的に可視

化し、リスクの観点からビジネスを把握し、コンプライアンス対応できているかどうかを確認できる環境を実現するものだ。

このHC3フレームワークは、IBMも加盟しているクラウドセキュリティに関する業界団体、「Cloud Security Alliance」（CSA）がまとめたベストプラクティスに準拠しているほか、NISTのサイバーセキュリティフレームワークやISOなどの各種業界標準に対応した上で、金融業界ならではのさまざまな要件を踏まえた内容になっている。PDCAサイクル、すなわち計画を立て、実施し、結果を計測して環境の変化に合わせて改善を加えるという継続的なアプローチを採用していることも特長だ。

HC3フレームワークにはまた、コンプライアンスに関するコンサルティングを手がけ、2016年にIBM傘下となったPromontoryの知見も反映されており、「新しい規定の特定」から「解析」「マッピング」「レポート作成」、さらに「統制更新後の品質確認」に至るまで、10のプロセスからなるライフサイクルを提供する。

例えば3プロセス目の「新しい規制の解析」では、規制に関する共通のデータベースを基に、新しい規制で求められる要件と統制をマッピングし、現状とのギャップを解析して「何から手をつけるべきか」「次に何をすべきか」を把握できるよう手助けしていく。

「最終的には、一連のプロセスを自動化していくことが目標だ。新しい法規制が登場したら、数日程度で評価を終え、自動的に取り入れて必要な変更を加え、金融機関が常に規制に準拠した状態、常に準備が整った状態を保てるようにしていきたい」とヨルゲンセン氏は述べた。

もう始まっている、マルチクラウドの利点とコンプライアンスの両立

既に、HC3フレームワークに沿ってコンプライアンスに取り組み始めた金融機関もあるという。

金融機関にとって法規制遵守は必須の要件だが、大事なのは新たな価値を提供し、ビジネスを成長させていくことだ。この金融機関では、マルチクラウド環境をベースにコンテナ技術を活用し、アジャイル開発やDevOps、継続的インテグレーションといったアプローチを取り入れて、新しい価値をスピーディに提供しようと試みている。同時に、ハイブリッドクラウド、マルチクラウドにまたがってコンプライアンスを遵守し、必要なセキュリティレベルを満たすべく、IBMはもちろん、Pivotalなどオープンなエコシステムを活用し、HC3フレームワークに沿って組み合わせているという。

ハイブリッドクラウド環境、マルチクラウド環境をベースに、金融機関に求められる高いレベルでセキュリティとコンプライアンスを満たしていく――一見、非常に実現困難な課題だが、HC3フレームワークとIBMのソリューション群を活用すれば不可能ではないことは、米国での実績が証明している。これから本格的にマルチクラウド環境での展開を考える金融機関にとって、心強い味方となってくれるだろう。

日本アイ・ビー・エム株式会社

お問い合わせ

日本アイ・ビー・エム株式会社
IBM アクセスセンター　0120-550-210
受付時間 9:00 ～ 17:00（土、日、祝日を除く）

IBM Security
https://ibm.biz/security_jp