マルチクラウド時代の最大の懸念
「セキュリティ」確保に向けたIBMの提案とは

今や国内でもクラウド利用は当たり前、それもハイブリッドクラウドやマルチクラウドで適材適所の使い分けを行う企業が増えている。

そんな中で最大の懸念が「どのようにセキュリティを確保するか」ということだ。

ASAHI INTERACTIVE

「数年前まで、クラウドは使うべきか、いや使わない方がいいのではといった議論があったが、今や国内でも当たり前のようにクラウドを使うようになってきた。それも、単一のクラウドサービスだけを利用するのではなく、複数のクラウドを利用するケースがほとんどだ」――日本 IBM セキュリティー事業本部 第二テクニカル・セールス部長の赤松猛氏は、ここ数年の急激な変化をこのように説明する。

赤松氏が指摘するとおり、デジタル・トランスフォーメーション（DX）の波を受け、それを基盤として下支えするクラウド市場も活況を呈している。市場調査を見れば、パブリッククラウドもプライベートクラウドも、2018 年から 2020 年にかけて十数%の成長が予測されており、その勢いは止まることがなさそうだ。

特に着目したいのは、AWS や Azure といったどれか 1 つのクラウドサービスに絞るのではなく、複数のクラウドサービスを活用する「マルチクラウド」や、既存のオンプレミス環境と適材適所で使い分ける「ハイブリッドクラウド」という選択肢が当たり前になりつつあることだ。赤松氏によれば、企業の 94%がただクラウドを使うのではなく複数のクラウド環境を利用しており、また 67%は複数のパブリッククラウド・プロバイダーを利用しているという。

1 つのサービス、1 つの環境にロックインされるのではなく、ビジネスや顧客のニーズに合わせて最適な選択肢を選び、組み組み合わせていく……それがこれからの DX 時代のクラウドのあり方と言えそうだ。

23%はインシデントを経験 クラウド・セキュリティのヒヤリとする現実

ただ、どんな技術にも利点と課題がある。クラウドも例外ではない。特に多くの企業にとっての大きな懸念となっているのは「クラウド環境上で、どのようにセキュリティを確保すればいいのか」ということだ。

残念ながらこの数年、クラウド上からの大規模情報漏洩事件がたびたびメディアで報じられてきた。中には、米陸軍のように高いセキュリティレベルが求められる組織であっても、クラウドのちょっとした設定ミスが原因となってデータ流出につながったケースもある。

赤松氏はこの状況を次のように見ていると言う。「クラウドだからといって、いきなり設定ミスが増えたわけではない。オンプレミスの環境でも設定ミスはあったが、仮にあっても内部に閉じていたため、『これ、どうなってるんだ』と気付いて修正できたため致命傷にはならなかった。これに対しクラウドでは便利になった反面、設定ミスが直接、セキュリティ事故につながってしまう」（赤松氏）。こうした事態に自ら気付けず、第三者の指摘によってはじめて判明した場合は、企業に与える損失や影響はさらに莫大なものになる恐れがある。

こうした状況は数字によっても裏付けられている。残念ながら、「クラウドを利用していて、12 カ月以内に何らかのセキュリティ・インシデントを経験した」とする企業は全体の 23%に上った。4～5 社に 1 社は、ヒヤリとする経験があった計算だ。

従って、「多くの企業がクラウドの利便性を評価して採用しているが、91%はセキュリティに漠然とした不安を抱いている。特に懸念しているのが、情報漏洩防止やデータ保護だ」（赤松氏）

クラウド上で発生するセキュリティ・インシデントの多くは、前述の設定ミスのほか、ユーザーのパスワードが盗まれるなどして認証を突破されたり、API 経由で情報が盗み見られた結果、発生してきた。こうした事態をどう防ぐのか、そしてその対策を実施するスタッフをどのように育成するか――クラウドなしの世界に戻るのはナンセンスであり、クラウドを利用する以上、こうしたセキュリティ上の課題の解決が不可欠となる。

クラウド環境のセキュリティ対策では「責任範囲」の確認と「共通基盤」が不可欠に

1 つの指針になりそうなのが、クラウド・セキュリティに関する業界団体、「Cloud Security Alliance」

日本 IBM
セキュリティー事業本部
第二テクニカル・セールス部長
赤松猛氏

（CSA）がまとめている「クラウドの懸念事項」だ。ここでは 12 の項目が挙げられ、それぞれに対策をとるよう推奨している。

一連の項目の中でも特に重要なのは、「情報漏洩対策」「ID･認証管理」「アクセス管理」「脆弱性管理」の 4 項目だ。これらの管理を一歩間違えれば、情報漏洩につながる恐れが高い。

一方で、注意しなければならないポイントがある。そもそも企業がクラウドを利用するのは、迅速にリソースを調達してすぐに利用でき、拡張性に優れるといったさまざまな利点があるからだ。あまりにセキュリティを優先してがんじがらめに管理しようとすると手間や時間がかかり、せっかくのクラウドの利点が損なわれかねない。クラウドならではのメリットとのバランスを取りながら、しかもこれまでオンプレミスで運用してきたシステムとの統合管理という観点も考慮しながらセキュリティ対策を検討しなければならない、という難しい課題に直面しているのだ。

そこで IBM では、2 つの方針に基づいて対策を進めることを推奨している。

1 つ目は、「セキュリティの責任範囲を考える」ことだ。クラウド環境のセキュリティを確保するのは、クラウドサービスを提供する事業者側だけの責任でも、またオンプレミス環境のようにユーザー企業だけの責任でもない。IaaS、PaaS、SaaS と提供形態によって範囲は違うが、それぞれが必要な範囲で対策を講じていくことが重要になる。

「まず、どこまでが自社の責任範囲で、どこから事業者に任せるかを確認しておかなければならない。また、事業者に任せるにしても、果たして事業者がどこまでやっているかを確認することも必要だ」（赤松氏）

2 つ目は、マルチクラウド環境、ハイブリッドクラウド環境の中で、全体を横断的に管理する手法や機能、共通の土台を用意することだ。確かにクラウドサービス事業者はそれぞれに、認証・認可やログ管理のためのさまざまな機能やセキュリティソリューションを用意している。だがそれらはあくまで、サービスごとに個別に提供されるものであるため、それぞれに精通したエンジニアが必要だ。万一異動などでその担当者がいなくなれば、何も分からず途方に暮れることになりかねない。

「できるだけ非属人的にセキュリティを運用していく必要がある。それには、全体を横串でまとめられる、横断的な管理手法を持つべきだ」（赤松氏）

IBM がマルチクラウド環境に向けて用意する 5 種類のセキュリティ･ソリューション

IBM はこうした前提を踏まえた上で、マルチクラウド環境に適用可能な 5 つの分野のセキュリティ・ソリューションを用意している。

クラウド・セキュリティ戦略 / ポリシー立案

IBM セキュリティー部門にはグローバルで約 8,000 名のセキュリティ・プロフェッショナルが在籍し、24 時間 365 日体制でセキュリティ監視を行い、さまざまな知見を蓄積してきた。さらに、オンプレミスからハイブリッドクラウド、マルチクラウド環境への移行を支援してきた経験も豊富だ。それらを基に、業界ごとのガイドラインも参照しつつ、顧客ごとの要望も踏まえながらコンサルティングを行い、ポリシー立案を支援する。

アクセス管理・統合認証

クラウド運用において、アカウントの管理は非常に重要だ。万一パスワードを盗み取られたり、推測されて不正アクセスされれば、あらゆるリソースやデータがリスクにさらされてしまう。そこで、ID に基づいて認証・認可を行うさまざまなソリューションが、クラウドサービス事業者自身が提供するものも含め、用意されている。

IBM の「Cloud Identity Connect」も、そんな認証・認可のためのプラットフォームだ。イントラネットはもちろん、クラウドや SaaS など幅広い環境にまたがってシングルサインオンを実現するほか、「Cloud Identity Verify 」ではいわゆる「多要素認証」を実現し、認証の高度化を可能にする。

認証にはいわゆるワンタイムパスワードや SMS、生体認証といったさまざまな手法が利用可能だが、IBM はさらにユニークな認証方法を用意している。それを提供するのが「Trusteer」の持つ振る舞い分析機能だ。ユーザーごとにキーボード入力やマウス操作の速度やクセを解析・記憶することで、本人以外の第三者によるなりすましを検知し、ブロックする。ユーザーに負担をかけず、それでいて高い精度で本人認証を実現することが特徴だ。

Cloud Identity Connectでもう1つ押さえておきたい特長が、オンプレミスや複数のクラウドにまたがる統合認証基盤を実現することだ。「社内システムの中には、合併・吸収時にどうしても統合できず、あぶれてしまっているものも少なくない。Cloud Identity Connectは多様な連携方式でそれらのシステムもシングルサインオンの対象とできる」（赤松氏）。また、認証の仕組みを1つの基盤に統合すれば、アプリやサービスごとに個別に認証の仕組みを実装する必要もなくなる。強固な認証を実現しつつ、将来的な変更や拡張が容易な環境を整えることができるだろう。

データ保護

データ保護の仕組みも個々のクラウド事業者が提供しているが、大事なのは「オンプレミスとクラウド、両方を守ること」（赤松氏）。IBMのデータ保護ソリューション「Guardium」では、どのデータベース内の中にどんな情報がどのくらいあるのか、重要な個人情報が存在するかといった事柄を分析・可視化した上で、監査・監視を通してデータを保護していく。

脆弱性管理

脆弱性管理に銀の弾丸はないが、IBMでは、他社製品も含めてどこにどんな脆弱性があるかを検査するツールを用意し、優先順位を設定しながら、パッチ適用をはじめとする脆弱性対策を支援している。「脆弱性は日々発見されており、1回対策して終わりではない。プロセスを回していくものと捉えることが重要だ」と赤松氏は述べる。

インシデント検知・対応

前述のようなさまざまなセキュリティ対策を実施し、保護しても、残念ながら攻撃がゼロになることはない。従って、不審な兆候や脅威を早期に発見し、致命傷になる前に対応することも、事前の防御と同じくらいに重要だ。そのためにIBMは複数のツールを用意している。

1つは、ログの統合管理を行う「QRadar」だ。さまざまなアラートやログを集約・分析し、全体を俯瞰して見られるようにしてくれる。「ただ、1日に何万件、何十万件と情報があると、訳の分からない状態になってしまう。そこを『Watson』が手伝い、振り分けをしてくれる」（赤松氏）。それでも人手不足でとても回りきらないという場合には、分析と影響範囲の特定、優先順位付けから場合によっては対応支援までを行う、SOCをベースとした「マネージドサービス」という選択肢もある。

ただ、物事に100%はあり得ない。それでも壁が破られてセキュリティ・インシデントが発生したときに備え、どう対応するかという体制やプロセスを整備しておくことも重要だ。

そのための製品が「Resilient」で、有事の際、「今何が起きているか」「次に何をすべきか」をダッシュボードに表示し、迅速な対応を支援していく。インシデント対応においてはスピードが命だが、さまざまな情報が錯綜して混乱しがちなのも事実だ。そこを整理し、あらかじめ定義しておいたプレイブックに沿って必要な対処を示すことで、抜け・漏れや重複なく、効率よくインシデント対応を行えるよう支援していく。また過去のインシデント対応の記録を集約管理することで、ノウハウの蓄積も可能だ。さらにResilientでは各種規制対応のためのテンプレートも用意されている。

IBMではこうしたソリューションを個別にでも、また必要なものを組み合わせ、統合した形で提供することも可能だ。IBM Cloudはもちろん、AWSやAzureといったマルチクラウド環境を見据えたセキュリティ・ポリシーの策定から対策の実装、24時間365日体制での監視と運用に至るまでを、グローバルな体制で支援している。ちょっとした不安や困りごとがあれば、ぜひ声をかけてみてはどうだろうか。

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