Grant Thornton

太陽グラントソントン Advisory Insights

ビジネスコンサルティング

今回のテーマ：　デジタルリスク管理とクラウドセキュリティ

デジタルリスクマネジメントの必要性

デジタルトランスフォーメーション（DX）に端を発したさまざまなデジタル化の波は、業務プロセスやビジネスモデルを変革し、新規事業の創出や既存業務の効率化等、様々な恩恵を企業にもたらしています。しかし、この変革には多くのリスクが伴います。セキュリティリスクは最も顕著で、データ漏洩やサイバー攻撃の危険性が増大します。デジタル化を進める中で、IT 人材の不足や外部からの攻撃によるセキュリティ対策の不備が、脆弱性を生み出す原因となり得ます。また、こういった一連のセキュリティ対策の不備は、評判低下のリスクも考慮する必要があり、企業のブランド価値に損害を与えかねません。個人が標的にされるリスクもあり、大量のデータを扱うことで個人情報が特定されやすくなります。データ共有による情報漏洩のリスクも無視できず、適切なデータ管理とセキュリティプロトコルの確立が必要です。

避けては通れないデジタル化を成功させるためには、これらのリスクを理解し、適切なリスクマネジメントとガバナンスを行うことが不可欠です。

デジタルリスクマネジメントは、企業がデジタル化の過程で直面するリスクを特定し、評価し、対応するプロセスです。これには、適切なデータガバナンスの確立や、セキュリティ対策の強化、従業員のデジタルスキルの向上など様々なものが含まれますが、本稿では代表的なデジタルリスクであるクラウドセキュリティについて掘り下げていきます。

クラウドセキュリティ

AWS、Microsoft Azure、Google Cloud Platform といった IaaS,PaaS の活用から、Microsoft365 に代表されるコミュニケーションツール、ローコード開発ツール等の SaaS サービスの活用まで、デジタル化を推進するにあたり、企業にとってクラウドサービスは重要性を増しています。クラウド上では大量のデータがクラウド環境で処理されるため、情報の機密性、完全性、可用性を保護するためのセキュリティ対策が不可欠です。

1.　クラウドサービスの責任共有モデルを理解する。

クラウドセキュリティのベストプラクティスには、多くの要素が含まれますが、まず、重要なのは責任共有モデルの理解です。これは、クラウドサービスプロバイダー（以下、CSP）と利用者がセキュリティの責任を共有するという考え方で、IaaS、PaaS、SaaS 等のサービス形態によって異なります。例えば、アプリケーションを定額利用する SaaS の場合、CSP はサーバやミドルウェア等インフラストラクチャのセキュリティを管理し、利用者はアプリケーション上のデータのセキュリティを管理します。また、データのバックアップについて、CSP 側で保証するサービスもあれば、バックアップは利用者側で管理を求めるサービスもあります。こうした責任共有レベルの理解を怠ると後々重大なインシデントに繋がるリスクを内在させることになります。CSP の利用開始時にはしっかりと利用規約や契約内容を確認し、利用者としての責任を理解しましょう。

2. クラウドサービスプロバイダーのセキュリティ対策状況を評価する。

次に、自社の大切な情報を預けるクラウドサービスプロバイダー自身のセキュリティ対策の状況を評価する必要があります。しかし、そのために自社でセキュリティ専門スキルを持った人材を手配し、直接評価するのは、かなり困難と言わざるを得ません。そこで活用したいのが各種認証や保証レポートです。専門性を持った外部機関が基準に従い、審査（監査）を行い、その結果を認定証や保証レポートという形で提供しています。逆にこうした認定や保証レポートを発行していない CSP は基本的にはセキュリティ対策という意味では大きく、割り引いて評価せざるを得ないでしょう。

代表的な認証や保証の枠組みとして、ISO/IEC 27017 と SOC2 があります。ISO/IEC 27017 は、情報セキュリティ管理策の実践の規範である ISO/IEC 27002 にクラウドサービス固有の事項を追加した国際規格です。これに対し、SOC2 は、米国公認会計士協会（AICPA）が定めた「Trust サービスの原則と規準」に基づき、セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーの 5 つのカテゴリについて評価されるものです。一般的に ISO の認知度が高いですが、認証取得に関するコストや評価方法等から、CSP にとっては、ISO より SOC2 の方が取得のハードルが高くなっております。利用者側からすると、SOC2 を取得しているとより信頼性があがると言って差し支えないでしょう。

3. クラウドサービスの設定の適切性を確保し、監視する。

次に、責任共有モデルの理解をもとに利用者側の責任をもって、適切にクラウドサービスの設定をしていくことが肝要です。クラウドサービスの設定誤りにより、外部からアクセスできてしまうといった脆弱性が生まれたり、不要なユーザに機密情報を公開してしまったりするリスクがあります。こうしたリスクに対応するための技術的な対策の一例として、クラウドセキュリティポスチャ管理ツール（CSPM）が挙げられます。このツールは ISO、NIST、SOC2 等のグローバル標準をもとにチェックルールを設定し、クラウドセキュリティの設定状況を評価し、設定ミスを可視化することができます。複数のマルチクラウドサービスを利用しているケースに対応できるのが特徴で、クラウドサービスのリスクを一元的に管理できます。

また、CASB（Cloud Access Security Broker）と呼ばれるクラウド上のアクセス状況を監視し、データの持ち出し制御等のコンプライアンス違反を検知することができるツールもあります。昨今、正式な手続きを経ず、個人やユーザ部門独自でクラウドサービスを利用するケースも増えています。こうしたシャドーIT を検知するためにも CASB が有効です。

自社のクラウド利用状況に沿ってリスクを正しくとらえ、ツールを組み合わせて対策していくことを検討していきましょう。

4. 組織的対策もあわせて見直しする。

クラウドセキュリティについても、通常のセキュリティ対策と同様の組織的な対策が求められます。これには、情報セキュリティポリシーや規程類の整備、情報セキュリティ体制の構築、情報資産の分類と取り扱いルールの策定、従業員へのセキュリティ教育、脆弱性診断等を含めた定期的な情報セキュリティ監査等が含まれます。既にこれらの情報セキュリティ対策を行っている企業でもクラウドサービスの利用を前提にしていない場合は、すべての取組みを見直す必要があります。合わせて、上記のセキュリティツールを適切に管理・運用していくための人材の育成も重要になってきます。技術的な対策としてツールを入れて安心というわけではなく、ツールを利用して継続してセキュリティを担保する体制の整備もあわせて構築していく必要があります。

最後に・・・

今回はデジタルリスクを管理するための１つとしてクラウドセキュリティに焦点をあて、寄稿させていただきました。冒頭に記載したように、デジタルリスクはクラウド上のみに存在するのではなく、ビジネス基盤上の「データ」が存在するところに様々なリスクが内在する可能性があります。デジタル化によって、新たなイノベーションの創出やビジネス効率化の恩恵を検討する一方で、どのようなリスクが発生しうるのかと懐疑的な目線でもって検証することも重要です。

ただし、セキュリティが心配だからという理由でデジタル化の対応を遅らせてしまうと、今度は市場で競争力を失い、企業成長が阻害されてしまうといったビジネス上のリスクが発生してしまいます。デジタル化の推進とセキュリティを代表としたリスク管理を両輪として、バランスをとりながら適切に経営していくために本稿が少しでもお役に立てば幸いです。