［ 改めて考える社内ICTシステム ］

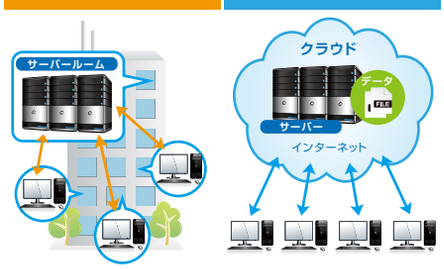
オンプレミスか？クラウドか？

インターネット上にシステムを構築するクラウド。従来は、社内にオンプレミスとして構築していたシステムを、クラウド上に構築する企業も珍しくありません。しかし、ビジネスで重要なデータをクラウド上に保管するとなると、セキュリティー面で懸念があり、導入に二の足を踏んでいる企業も多いのではないでしょうか。
オンプレミス、クラウド両者を比較しながら、導入時に検討すべきことを考えてみましょう。

企業のクラウドサービスの活用が進んでいます。クラウドサービスには、クラウド上でアプリケーションを利用する「SaaS」、インフラを利用する「IaaS」、プラットフォームを利用する「PaaS」など、さまざまな形態があります。情報システムや開発環境を IaaS 上に構築する話はよく耳にしますが、最近では、基幹システムを構築するケースも見受けられます。
しかし、情報漏えいをはじめとするリスクを心配し、クラウド導入をためらう企業もあるでしょう。クラウド導入の前に、どういうリスクがあるのか、そのリスクにはどういう対策が可能なのかを整理して、自社のビジネスやセキュリティーポリシーを踏まえて検討する必要があります。

導入期間、初期投資、BCP対策に利点のあるクラウド

それに対してクラウドはどうでしょうか。SaaS なら、すでに提供が始まっているサービスを利用する、もしくは自社用にカスタマイズして導入するケースが基本です。自由度は下がりますが、導入期間が短縮でき、これまで稼動してきた実績なども評価できます。
IaaS や PaaS は、クラウド上に自社で開発した業務アプリケーションなどを乗せて稼動させます。システムを開発するという点ではオンプレミスに近いのですが、ハードウェアやネットワークなどの初期投資が抑えられるという利点があります。
ビジネスは、スピードで勝負する時代になりました。他社に先駆けてサービスを始めることで、有利にビジネスを進めることができます。料金も月額定額、または利用料に応じた体系のものが多く、初期投資などの予算、経営計画が立てやすいのもメリットです。
さらに BCP の面でも、クラウドに利点があります。社内のサーバールームにオンプレミスのサーバーを設置すると、仮に地震や停電などで会社に影響があった場合、サーバーそのものへのアクセスができなくなります。そのため、地理的に離れた支店やデータセンターに、バックアップを用意しなければなりません。しかしクラウドは、地震対策、停電対策の施された専用の施設（データセンター）で運用されているので、BCP 対策としても期待できます。



	オンプレミス	クラウド
導入期間	△時間がかかる	○スピーディー
初期投資（ハードウェア）	△必要	○不要
BCP 対策（サーバー）	△自社	○クラウド事業者

クラウドにデータを置くリスクは、VPNなどで対応

次に、サーバーに接続するためのネットワークを考えてみます。
オンプレミスの場合、インターネットなどの外部回線を経由せずにサーバーへ接続することができます。そのため、特に機密性が高いデータに関してはオンプレミスを選ぶケースが多くあります。
一方、クラウドの場合、回線を利用してクラウド上のサーバーに接続しますが、インターネットを利用したインターネット VPN（仮想プライベートネットワーク）の場合、通信が遅延するリスクも考えられます。また VPN を利用しているとはいえ、機密性が高い情報を扱うのであれば、脆弱性や設定ミスなど思わぬトラブルにより、盗聴や不正アクセスで情報漏えいが生じるリスクを考慮しなければなりません。

しかし、閉域網を利用した IP-VPN を利用することで、盗聴やデータ改ざん、不正アクセスといったリスクを低減することができます。また一定の帯域を保障しているサービスもあります。
クラウドならではの注意点もあります。例えば、セキュリティー体制の監査を実施する場合を考えてみます。オンプレミスであれば、特に制限なくシステムの監査を実施できます。しかし、自社以外が管理するサーバーや設備となれば、勝手に監査を行うわけにはいきません。
データを保管するデータセンターの中には、監査へ対応してもらえないケースもあります。さらにデータを海外のクラウド上へ保存する場合、その国や地域の法令を遵守しなければなりません。規制によりデータを域外へ越境できない場合もあります。
こうした不安を解消するため、クラウド事業者は、外部監査人から認証を取得したり、セキュリティー基準への適合性について保証を得るなど、さまざまな取り組みをはじめています。

脆弱性が見つかった場合は、クラウド事業者が迅速に対応

昨今、企業のサーバーがサイバー攻撃を受ける事件が話題になることも珍しくありません。例えば、サーバーの処理能力を超えるような大量のアクセスを仕掛けて、クライアントにサービスを提供できない状態にする「DDoS 攻撃」はその一つです。
サーバーで稼動している OS、ミドルウェア、アプリケーションの脆弱性が狙われるケースもあります。脆弱性を突く攻撃によって Web サーバー上にウイルスを仕込まれたことで、アクセスしたユーザーのパソコンがウイルス感染するケースもあります。
このような事件を避けるためには、常に脆弱性情報に目を配り、自社で稼動しているサーバーに問題がないかをチェックし、修正プログラムやパッチを適用する等の対処を行うことが必要になります。
オンプレミスのサーバーの場合、情報システム部が脆弱性の情報を収集し、チェックする必要があります。大企業では何十台、何百台ものサーバーが稼動していることが多いので、それぞれのサーバーの OS、ミドルウェア、アプリケーションの種類、バージョンを把握しておき、脆弱性が該当するか否かを判断する必要があります。脆弱性に該当する場合は、修正プログラムを適用しても問題がないかを確認した上で、適用作業を行います。
このように、自社でサーバーを管理しているからといって脆弱性への対応が容易とは限らず、場合によっては膨大な稼動と時間がかかることもあります。
一方クラウドの場合は、脆弱性が発見されると、クラウド事業者が提供する部分はクラウド事業者が修正を行います。同じ基盤上で多数の利用者がいるからこそノウハウがあり、漏れなく迅速に対応することができます。ただし、契約内容によって脆弱性への対応は異なるため、契約時にしっかり確認しておく必要があります。

クラウドの利点とオンプレミスの利点を生かすならハイブリッドクラウドという選択肢

クラウドの利点は、導入や運用の負荷が軽減され、情報システム部門のリソースを有効に活用できることです。脆弱性が発見された際も、一般的にはクラウドのほうがスピーディーに対応できます。
一方、オンプレミスの利点には、既存の社内システムと連携させやすいことが挙げられます。また、自社のセキュリティーポリシーに合致したシステムを構築できるのも、企業としてはメリットです。
企業は、さまざまなデータを保有しています。事業内容によってデータ量も違いますし、機密性も異なります。また、事業規模や成長速度によって処理能力や投資金額も異なるでしょう。

	オンプレミス	クラウド
脆弱性への対応	△時間がかかる	○スピーディー
運用管理負担	△負担がかかる	○軽減される
社内システム連携	○柔軟に可能	△制限あり
セキュリティーポリシーの設定	○柔軟に可能	△制限あり

クラウド、オンプレミスそれぞれの特長を踏まえて、最適な環境を選択することが重要です。両者のメリットをともに生かすことのできる「ハイブリッドクラウド」という選択肢もあります。
ハイブリッドクラウドとは、クラウドとオンプレミスを組み合わせて使う仕組みです。ハイブリッドクラウドであれば、「どうしても社外に出せないデータはオンプレミスに置く」「利便性、生産性を優先にするシステムは、クラウドに置く」「両者を、連携させて活用する」といった、それぞれの利点を生かした利用が可能になります。
このようにクラウドにもオンプレミスにもそれぞれの特長、メリット、デメリットがあります。これからの会社のビジネスを発展させる ICT システムとして、「最適な ICT システムは何か」「リスクには何があるか」「どのようにして、そのリスクに対処するか」などを吟味して、クラウドかオンプレミスかの選択を検討する必要があります。