覚えておきたいクラウド&データのキホン（第2回）

クラウドへのデータ保存は安全なのか？情報セキュリティ対策はどうすればよい？

2022.03.31

クラウドは、私たちの仕事や暮らしの中で欠かせないツールとなりつつあります。しかし、データをクラウド上のサーバーにアップすることに不安を感じる人がいるかもしれません。

今回はクラウドにおける情報セキュリティ対策と、クラウドを安全に利用する方法を解説します。

クラウドの安全性と情報セキュリティ対策

リモートワークでビジネス利用が拡大

クラウドは、インターネットを通じてITサービスをユーザーに提供する仕組みです。例えば、クラウド上にデータを保管することで、好きなときにデータを取り出したり確認したりできます。クラウドコンピューティングと呼ばれることもありますが、一般的には同義です。

クラウドが登場したことで、ビジネスのスタイルも大きく変わりました。例えばメールはOutlookなどのメールソフトをPCにインストールして送受信を行い、やり取りしたデータはPCに保存していました。しかし、現在はIDやパスワードを持っていれば、ChromeやEdge、Safariなどのブラウザーを通じて、PCやスマートフォン、タブレットなどさまざまな端末からアクセスができます。

ビジネスでのクラウド利用は、働き方改革やリモートワークの拡大に伴って急速に広まっています。メールやファイル共有などですでに活用している人も多いでしょう。

クラウドの安全性と情報セキュリティ

クラウドはインターネットを通じて、自社のデータをやり取りします。データの消失や情報漏えいといったリスクは、かねて指摘されてきました。

昨今、GoogleやAmazon、Microsoftといった法人向けのクラウドを提供している企業は、情報セキュリティ対策機能を備えたクラウドを提供しています。クラウドサービスのメリットのひとつに、「情報セキュリティ対策の水準向上」が挙げられます。前述のGoogleやAmazon、Microsoftのように多くのクラウドサービスは一定水準の情報セキュリティ対策機能を有しているほか、オプションでより高度な情報セキュリティ対策機能が選択できるものもあります。

そのため多くのシステムはオンプレミスで情報セキュリティ対策機能を個別に構築するよりも、新たな情報セキュリティ対策機能を積極的に取り入れるクラウドサービスを利用したほうが、規模の経済からも効率的な情報セキュリティ向上が期待できるのです。そのような背景から、、日本政府のシステム調達でもクラウドを第一候補として検討する「クラウド・バイ・デフォルト」が宣言されるなど、クラウドへの信頼度は高まってきています。

そういった中で、クラウドを利用する企業が懸念すべきは情報流出などをさせてしまうリスクです。例えば、クラウドにアクセス

するためのIDやパスワード、保存されたデータ管理などは、利用企業側の責任となり得ます。仮にIDやパスワードが流出し、不正アクセスや情報漏えいなどを招いた場合、利用企業側が大きな責任を負う可能性があり、事業存続に関わる事態ともなりかねません。

クラウド利用時の5つの情報セキュリティ対策… 続きを読む