覚えておきたいクラウド&データのキホン（第18回）

暗号化とは？クラウドストレージに必須の情報セキュリティ対策

2022.03.31

インターネット上でデータを共有できるクラウドストレージで、機密情報や個人情報を管理する場合、暗号化による情報セキュリティ対策が欠かせないものとなりつつあります。

本記事では、クラウドストレージに暗号化が必要な理由、暗号化の方法や種類について紹介します。

クラウドストレージと情報セキュリティの必要性

まずはクラウドストレージについて、おさらいしましょう。またここでは、情報セキュリティの必要性もあわせて解説します。

クラウドストレージとは

クラウドストレージとは、インターネット上でデータの保管・共有ができるサービスです。自社内でデータを保管・共有する方法としては、社内ネットワーク上にサーバーを設置したり、USBメモリーや外付けストレージなどを使ったりして行ってきました。近年は運用コストや使い勝手などの観点から、クラウドストレージを利用するケースが出てきています。

クラウドストレージのメリット

クラウドストレージのメリットは、インターネット環境さえあればどこからでもアクセスできる点です。テレワークを導入する企業の増加に伴い、自宅や外出先から業務関連のデータを扱うニーズが増加傾向にあります。クラウドストレージはテレワークとの親和性も高いといえます。

BCP（Business Continuity Plan）の観点からも、クラウドストレージにはメリットがあります。自然災害などの影響でオフィスの業務用パソコンやサーバーに被害が生じた場合、保管されていたデータが消失する可能性があります。バックアップを取っていたとしても、同じオフィス内に保管していればリスクは同様です。クラウドストレージでデータを保管することで、そういったリスクを軽減できます。

デメリットとしては、クラウドストレージはクラウド事業者が提供しているため、自社に合わせたカスタマイズがしにくい点が挙げられます。例えば、自社で策定した情報セキュリティポリシーがある場合、それに準拠できるクラウド事業者を選択する必要があります。

情報セキュリティ対策の必要性

クラウドストレージは、インターネットを通じてIDとパスワードでどこからでもログインができます。テレワークや他拠点、社外関係者とのデータ共有を効率的に行える一方、情報セキュリティ対策が不十分であると、情報漏えいのリスクが生じます。

例えば、クラウドストレージでは、ファイルごとでアクセス権限や公開設定をすることができます。しかし、従業員が誤って社外秘のデータを外部公開したり、共有リンクを部外者に送信したりしてしまうと、情報漏えいにつながります。万が一、顧客リストなどの機密情報が漏えいすれば、被害は取引先や顧客などへも広がる恐れがあります。インターネットからアクセスできるため、ID・パスワードの管理が不十分であると、それを知った第三者によるアカウント不正使用のリスクも生じます。

そういったことから、クラウドストレージではクラウド事業者がさまざまな情報セキュリティ対策を施しています。

クラウドストレージの暗号化とは… 続きを読む