

## 覚えておきたいクラウド&データのキホン(第30回)

# クラウドストレージの情報セキュリティ対策と想定されるリスク

2023.02.22



クラウドストレージとは、一般的にクラウド上のストレージにデータを保管するサービスのことを指します。インターネット経由で接続するため、社内外を問わずに利用できるなど数多くのメリットはありますが、その一方で情報漏えいなどのリスクも存在します。この記事では、クラウドストレージの特徴やメリット・デメリット、クラウドストレージを利用するにあたって必要な情報セキュリティ対策について解説します。

### 目次

- ・自社サーバーと比較したクラウドストレージの特徴
- ・クラウドストレージのリスクとは
- ・クラウドストレージの情報セキュリティ対策
- ・情報セキュリティ対策が充実したクラウドストレージ選びに迷ったら
- ・まとめ

### 自社サーバーと比較したクラウドストレージの特徴



クラウドストレージとは、業務で使用するデータを、社内のファイルサーバー(以下、自社サーバー)ではなく、クラウド上のストレージ(倉庫)に格納するサービスのことです。まずはクラウドストレージを使うメリットについて、自社サーバーと比較して解説します。

#### どこからでもアクセスできる

クラウドストレージは、インターネットに接続できる環境であれば、自宅や出張先など、さまざまな場所からアクセスできます。パソコンだけでなく、スマートフォン・タブレット端末などからも、インターネット接続ができるデバイスであれば利用可能です。例えばテレワークをする際も、クラウドストレージを利用すれば、社内のデータを持ち出すことなく、社外であっても社内にいる場合と同じように仕事を進められます。

その一方で社内サーバーは、基本的には社内からのアクセスを想定したものです。VPNなどの回線を利用しない限り、社外からはアクセスできません。

#### 社外の人とファイル共有できる

社内サーバーを介して、複数の従業員がデータの共有や編集を行うと、1つのデータが複数の別データとして保存されるおそれがあります。このような事態を防ぐため、社内サーバーでは、1人の従業員がデータを編集している間は、他の従業員が同時に編集できない場合があります。

クラウドストレージであれば、1つのデータを複数の従業員と共有し、編集できるサービスが用意されていることがあるため、効率的な作業が可能になります。データの保管場所のURLやパスワードを伝えれば、社外の人と共同編集・ファイル共有も可能です。

#### 自動的にバックアップできる

クラウドストレージサービスの中には、自動バックアップ機能や履歴管理機能が備わっているものもあります。これらの機能を利用すれば、データを誤って消した場合、データを前のバージョンに戻したい場合にも復元可能です。社内サーバーでもバックアップを取ることは可能ですが、バックアップシステムの構築・運用は自社で行う必要があります。

#### コスト低減が期待できる

社内サーバーは、ハードディスクなど機器の購入やシステム構築が必要となり、サーバー設置後も情報セキュリティ対策やメンテナンスが欠かせません。そのため、初期コスト・運用コストは高くなりがちです。

クラウドストレージの場合、サーバーの購入・設置は不要であり、利用料金以外の初期コストは基本的に不要です。そのため、社内サーバー構築よりもコストを安価に抑えられる傾向があります。トラブル対応やメンテナンスも、基本的にはサービス提供事業者が行うため、運用コストも抑えられるでしょう。

## クラウドストレージのリスクとは

このようにクラウドストレージにはさまざまなメリットがありますが、場合によってはデメリットが生じる場合があります。

#### データを消失する可能性がある

自動バックアップ機能が搭載されたクラウドストレージを利用している場合でも、データ消失のリスクは皆無ではありません。例えば、クラウドストレージのサーバーが停止していたり、システム・ネットワーク障害が生じたりした場合には、保管しているデータにアクセスできなくなります。さらにデータを保管するサーバーが設置されている場所に災害・事故などが生じた場合、データが完全に消失する恐れがあります。

#### 機密情報を外部漏えいする可能性がある

万が一クラウドストレージサービスの提供事業者がサイバー攻撃の標的となり、クラウドストレージにアップロードしていたデータが盗まれた場合、氏名や年齢、住所をはじめとする個人情報や顧客情報、機密情報などが漏えいすることになります。結果的に、企業としての信用が失墜し、賠償問題にも発展しかねません。

#### アカウント情報を漏えいする可能性がある

クラウドストレージの利用には、一般的にID・パスワードなどのアカウント情報が必要です。つまり、アカウント情報を知っている人なら誰でもログインでき、データにアクセスすることが可能です。自社が不正アクセスの被害に遭った場合、アカウント情報が漏えいし、悪意のある人物がクラウドストレージにアクセスする恐れがあります。

クラウドストレージの情報セキュリティ対策… 続きを読む