

ネットワーク・セキュリティの潮流(第3回)

巨大なデータを安全に使いやすく共有する

2015.07.01

あらゆる企業において、取り扱うデータの量は急増している。そうした中、大企業の多くは巨大なストレージ環境をクラウドまたは自社環境に用意して対応している。いわゆる、ビッグデータの活用だ。

中小企業や個人事業者も、ビジネスに必要な情報量が増加して、パソコンなど単独の機器の容量を超えたデータを扱わなくてはならないケースが増えている。こうした中小企業や個人事業者は、手軽なデータ保管場所としてハードディスクを搭載したファイルストレージを活用している。容量にもよるが、数万円程度である程度のスペックのものが手に入る。

ファイルストレージには据え置きタイプとポータブルタイプがある。据え置きタイプは、セキュリティがある程度確保できる。一方、利便性の点で見劣りする。複数ユーザーによる情報共有が難しくなるからだ。ポータブルタイプは、紛失や盗難、落下による破損などのリスクがやはり避けられない。

セキュアで情報を共有しやすいNAS

こうした問題を解決する手段として、最近ではNAS(Network Attached Storage)を導入するケースが増えている。NASはその名の通り、ネットワークに接続した外部記憶装置(ストレージ)のこと。ネットワーク経由で複数のパソコンからアクセスできる。一定以上のスペックを備えた企業向け製品のほか、個人が動画などの大きなデータを保存するために利用する用途を狙った低価格製品もある。

NASのメリットは情報共有が容易な点だけではない。セキュリティのレベルを上げられること、ネットワークに接続していることでデータのバックアップが容易なのも重要なアドバンテージだ。

NASには様々なタイプがある。法人向けでは、フォルダごとにアクセス権を設定できるものが一般的だ。例えば、個人情報については、担当者しかアクセスできないといった制限をかけられる。マイナンバー制度に対応したIT環境を構築する上で、このようなアクセス管理はセキュリティを向上させる重要なポイントの1つだ。

データのバックアップについては、BCPの観点でニーズが高まっている。東日本大震災のときには、オフィスに置いていたパソコンやサーバーの水没・破損などの被害を受けたり、ネットワークの途絶によりアクセスができなくなったりした企業もあった。こうしたケースを目のあたりにして、データのバックアップを真剣に考える経営者が増えた。

NASを使ったデータのバックアップとしては、2台用意して定期的にバックアップをとって、同じデータを保存しておく方法がある。災害などのリスクを考えると、2台はできるだけ離れた拠点に置いて、ネットワークでつなぐのが望ましい。同じオフィスに2台とも設置したり、近接した拠点に配置したりした場合、地震などへの備えとしては不十分だからだ。

拠点が分散していない企業が効果的にバックアップを行うなら、クラウドの利用が考えられる。[AWS\(Amazon Web Services\)](#)などで提供されているクラウド型のストレージサービスは、堅牢なデータセンターを用意している。平均レベル以上のデータセンターであれば、地震や停電などの事態に対して十分な備えをしているので、データ消失というリスクは最小化できるはずだ。

ただ、クラウドにデータを置くという選択は身軽ではあるが課題も残る。というのは、災害や事故などでネットワークが停止してしまうと、データへのアクセスができなくなるからだ。

こうしたリスクを回避するため、最近ではハードウェアとクラウドによる二重化を検討する企業が増えている。手元にNASを置き、それをクラウドにつないでデータのバックアップを行う方法だ。これならネットワークとハードウェア、データそれぞれの分野で二重化を実現できる。

例えば、社内LANに問題が起きてオフィスのNASが使えなくても、クラウドサービスを利用してカバーできる。もちろん、逆の

ケースにも対応できる。また、NASとNAS内のデータが壊れたとしても、クラウド上には直近までのデータが保存されているのでハードウェアの故障対策にも有効だ。最近では、特に中小企業向けのデータバックアップとして、こうしたハイブリッド型のデータ環境が注目されている。

NAS+クラウドでマイナンバー制度に対応

… 続きを読む