改めて考えるデータの保管・共有法（第2回）

メールでのファイル送信は何が危険なのか

2022.11.21

ビジネスシーンにおいて、社外の人とファイルをやり取りすることは頻繁に起こります。しかし、パスワード付きのzipファイルをメールに添付して送信後にパスワードを送信している場合や、無料のクラウドストレージサービスを使用している場合、セキュリティ面で大きなリスクを抱える可能性もあります。どうすれば安全かつ便利にデータを共有できるのでしょうか？

メールでzipファイルとパスワードを送ることに意味はあるのか？

顧客や同僚、パートナー企業と、メールを使って電子ファイルをやり取りすることは、今やビジネスシーンでは一般的です。例えば、請求書や納品書、契約書、提案書などを紙ではなく文書ファイルとしてメールで共有すれば、郵送するよりも早いため業務効率化につながります。

社外の人とファイルを共有する際に、注意しなければならないのがセキュリティです。ファイルを誤送信した場合、機密情報が意図しない形で第三者に漏れてしまいます。

そのセキュリティ対策としては、ファイルをzipファイルに変換し、そのファイルを添付したメールを相手に送った後、再度、zipファイルを開くためのパスワードを記載したメールを相手に送信する、という手法が存在します。これは「PPAP」と呼ばれる方式で、かつてはメールによるファイル共有の際の有効な手段の1つとして考えられていましたが、現在では政府や大企業など多くの組織でPPAPを取りやめる事態となっています。

見直しの理由は、手間を掛ける割にはセキュリティ強度が高くなく、むしろセキュリティリスクを高める要因となる恐れがあるためです。そもそもzipファイルのパスワードの強度は高くなく、場合によっては数秒で解析される恐れもあります。しかも、zipファイルにパスワードが掛かっていると、メールサーバーに搭載されているウイルスチェックができず、ウイルスがすり抜けて文書とともに相手のパソコンに届く危険性もあります。

とはいえ、USBメモリを使ってファイルを受け渡しするのも考えものです。USBメモリがウイルスの感染経路になる恐れがあるうえ、小型のため紛失や盗難被害に遭いやすくなります。さらにいえば、USBメモリの手渡しや郵送で送ること自体が効率的ではありません。

便利な無料サービスだが、リスクが生じるケースも… 続きを読む