マネジメント講座

クラウド利用の落とし穴

情報漏洩を防ぐ ⑧

総務省が発表した2018年の通信利用動向調査によると、クラウドサービスを利用していると回答した企業の割合は約6割に達した。16年の調査では5割未満だった。今後も利用率は高まり続けるとみられる。

確かにクラウドサービスは便利だが、一定のリスクがあることを認識したうえで従業員に利用させることが重要だ。

クラウドサービスでは、IDとパスワードを組み合わせた情報を使って個人を認証する仕組みが多く用いられている。

しかし従業員が個人や会社で利用するクラウドサービスに認証情報を使い回した場合、1つのサイトの認証情報が漏れてしまえば、悪意のある者によって他のサービスにアクセスされ、情報窃取や不正利用の被害に巻き込まれる恐れがある。

IDとパスワードの使い回しが不可で、二段階認証であるなど、より高度な認証を実装しているクラウドサービスを利用することが重要だ。

クラウドサービスには、自社が貸与するパソコン以外のデバイスからでもアクセスできる機能もある。だが自社管理外のデバイスで同サービスにアクセスした際、認証情報や履歴が残ったり、ダウンロードした情報がデバイス内に残ったりし、社外に重要な情報が漏れる恐れもある。利用するサービスは慎重に選定する必要がある。

クラウドサービスは業務効率の向上など、事業競争力をつけるうえで重要なツールになり得る。半面、デジタル依存度が高まることで情報セキュリティーのリスクも大きくなり、事業に影響をおよぼす可能性がある。

クラウドサービスを採用する際は、デジタル変革と併せて、企業の情報セキュリティーマインドの変革対応を実施すべきである。

（SOMPOリスクマネジメント取締役　宮崎義久）

クラウドサービスのリスクと対応のポイント

主なリスク
- 個人認証情報の使い回しによるリスク
- 自社管理以外のパソコンでも利用可能なリスク

主な対応
- 認証情報の使い回しの禁止
- より高度な個人認証方法を採用したサービス利用
- 自社管理以外のパソコンによるサービス利用の禁止
- 社外のデバイスからアクセスできない仕様の採用
- サービス利用後にデータを残さない方法の採用

（注）SOMPOリスクマネジメント作成

2019年7月30日
日経産業新聞