

安全で継続的な クラウド運用を考えるなら、 ISO 認証取得企業に注目だ!

小村 秀生 審査員

インターネットの普及に伴い、今やビジネスの世界でも常識となったクラウド活用。日々利便性を増す一方で、データ量は増大し複雑化が進み、インターネットによる犯罪も高度化している。私たち利用する側が安全かつ継続的にクラウドを活用するにはどうすればいいのか。今回はベターリビングに登録するISMS・ISMSクラウドセキュリティの主任審査員である小村秀生氏にお話を伺った。



ポイントはココ!

- 1 クラウドシステムはコミュニケーションから会計処理まであらゆるシーンで利用されている
- 2 システムを「所有・維持・管理する」から「利用する」に変えることでコストと時間を削減
- 3 クラウドの利用にはある程度の危険性を伴うことを認識しよう
- 4 ISO 認証取得企業を選択することも安全なクラウド利用の指標
- 5 情報の管理方法をしっかり見て選ぶことは企業・組織の社会的信頼を高める

—いま、私たちの身の回りではどのくらいクラウドが使われているんですか？

代表的なものではメールやアドレス帳などコミュニケーションに関わるものを始め、写真、音楽、本や動画などインターネットを通じて閲覧したり共有したりできるものは、何らかのクラウドのシステムを使っているのが一般的ではないかと思います。

ビジネスの世界でも十数年前から利用が増え、今ではほとんどの企業で少なからずクラウドサービスが利用されていると思います。具体的にはメール、スケジュール管理、ファイル保管、会計処理、データベースなど使っていないものはないのではないかと思います。あらゆるシーンで活用されています。

— どうしてビジネスシーンでの利用が進んだのでしょうか。

クラウドの便益について教えてください。

十数年ほど前までは、「オンプレミス」といって社内にサーバーを置いて自社管理していたところが多かったのですが、その対となる「クラウド」を利用すれば導入コストやスペース、システム構築やメンテナンスのための時間やコストを削減できるというメリットがあります。そこにネットワークの高速化といったインフラの強化も後押しして、利用が進んだのだと思います。

かつては「サーバーを建てる」というと、ハードを調達してそれからシステムを作るということを実社内でやらないといけませんでした。クラウドなら手元のパソコンで操作して、簡単に仮想サーバーを建てることができます。少しだけ使ってダメならやめるといったトライアル利用も簡単にできます。さらに容量が足りなければ簡単に増やすことも可能です。またセキュリティへの取り組みも、クラウドサービス提供者側に委ねることにより、サイバー攻撃の高度化に対抗できるような環境が整ってきたので、そういったことも利用が進んだ理由の1つかもしれません。

— クラウドの利用に危険は伴わないのですか？

セキュリティに関してはクラウドシステムの提供側に委ねる形になりますので、どうしても自分側でコントロールできないところが出てきます。

しかし個々の会社がそれぞれで、ID・パスワードの外部漏えい対策を講じたり、外部の第三者からの不正アクセス対策を施したり、隔地にバックアップを取得するなどのセキュリティ対策を行ったりするには限界があるように思います。

システム自体がクラウド化していく流れは今後も進んでいくと思います。情報を委ねる一方で、セキュリティ対策もサービス提供者側にますます委ねることになっていく訳です。サービスを利用する側からすれば、いかに信頼できるサービス提供者を選択するのが鍵となってきます。選択するときには、サービスの利便性だけでなく、セキュリティへの取り組みがどのようになっているかを判断材料に加えることが重要ではないでしょうか。



— 私たちができるだけクラウドを安全に利用するには、どんな方法がありますか？

それには「ISO 認証取得企業」を選択することも、1つの指針になります。ISO/IEC27001（情報セキュリティマネジメントシステム）を認証取得している企業は情報をどう取り扱うべきか、ということについて体系立てた仕組みをつくっています。全社員が情報を漏洩させないということに対して意識が高いだけではなく、いかに正しい情報を維持し、かつ継続的に稼働できるかということにもコストをかけている企業だといえます。また、ISO/IEC27017（ISMSクラウドセキュリティ）を認証取得している企業はクラウドサービスのセキュリティ対策について第三者認証を得ている企業として、さらに信用できるのではないのでしょうか？

情報セキュリティの三要素「機密性」「完全性」「可用性」。 この維持に取り組むのがISO 認証取得企業

「機密性」は情報を安全に管理して、外部に情報を漏らさないようにしたり、外部からの不正アクセスができないようにしたりしているかどうか。

「完全性」は古い情報をそのまま持っているのではなく、きちんと新しい情報に常に更新しているかどうか。例えば社員の情報が変わったら即時に更新するなど、そういったことも行なっています。

「可用性」はシステムがいつでも使える状態を維持しているかどうかです。例えば地震などの災害があっても情報を喪失したり、システムが長時間止まったりといったことがないようにコストをかけている企業です。

——健全なクラウド運用で、利用する側が得られる真のメリットは何ですか？



それは「企業・組織の社会的信頼」です。1つの商品を扱うにも、原材料や部品の調達、製造、販売、配送に至るまで、様々な企業や人の手を介して客先に商品が届けられる仕組みになっている今、このサプライチェーンのどこからいつ情報が漏れるかわからない危険性は常にあります。自身が漏らす立場にならないようにするには、コストや利便性だけではなく、利用するクラウドサービスのセキュリティ対策にも注目するようにしましょう。

そして、ISMSクラウドセキュリティ認証取得企業では行っているセキュリティ対策に関する情報を開示していますので、内容をしっかり見て評価することが大切です。それはあなたの会社が、そういった危険にどれだけ備えているかをきちんと評価しながらクラウド活用を進めているかの証明にもなります。そのような姿勢は、大事な取引先やお客様はもちろん、広くは社会からの信頼を高めていく上で大切な要素になってくるでしょう。

小村 秀生氏 プロフィール

一般財団法人ペターリビングシステム審査登録センター 情報セキュリティマネジメントシステム 主任審査員

一般財団法人 日本要員認証協会 (JRCA) 情報セキュリティマネジメントシステム 主任審査員

情報マネジメントシステム認定センター ISMSクラウドセキュリティ 主任審査員

1969年東京都生まれ。石油業界からIT業界へ転身後、品質マネジメントシステム、個人情報保護マネジメントシステムの構築に携わったのち、主に金融業におけるシステム監査、製造業における内部統制報告制度の構築コンサルティングを行う。現在は企業のISMS構築コンサルティング、教育機関、企業における防災マニュアル作成コンサルティングを行っている。