

シリーズ：『挑戦』を支えるもの

～デジタル化の時代を生き抜くためのリスク対策～

■「旅行」のデジタル化

近年のスマートフォンなどの普及とともに、旅行商品や航空券、宿泊のWeb販売といった旅前の手続きはもろろん、旅中コンテンツの普及やSNSなどの旅後の情報拡散も含めて、「旅行流通と旅行行動のデジタル化」が急速に進んでいます。「ツリーズムEXPOジャパン2018」でも、会場のいたる所に「デジタル」の言葉が踊り、旅行会社においてもIT活用や営業のデジタル化対応がさらに進んでいることを実感しました。

世の中のデジタル化に伴い、情報管理に関わる新たなリスクも生まれています。旅行会社は従来から複数の素材提供者と多くの顧客情報をやりとりしており、情報セキュリティ・リスクが高いと言われていますが、デジタル化で生じる新たなリスクとはどのようなものでしょうか。

■すぐそこにあるリスク

まず挙げられるのはサイバー攻撃のリスクです。不正アクセスや「なりすまし」メールの攻撃を受けると、顧客情報の流出や社内ネットワークの停止などにより通常業務もままならない事態に陥ります。

また、社外からの攻撃だけではなく、社内にもリスクが潜んでいます。

す。ヒューマンエラーによる情報流出はメールの誤送信がその代表例ですが、業務情報を保存したPCやスマホ、USBメモリなどの持出しも大きなリスクを孕んでいます。デバイスの進歩は業務効率化や働き方改革につながる反面、情報管理が脆弱になる危険を伴うのです。

■中小企業ほど狙われる？

Web販売サイトを持つ旅行会社やOTAだけではなく、会社のホームページを運営したり日常業務にインターネット・メールを利用していただけでもサイバー攻撃の標的になる可能性があります。また、かつては大量の顧客情報を持つ大企業が攻撃のターゲットとされていましたが、大企業のセキュリティ対策が進んだことで、比較的対策が遅れている中小企業をサイバー攻撃の「踏み台」として、そこから取引先の情報を盗み取る手口が増えています。このような攻撃の被害に遭うと、取引先の信用も失いその後の事業にも大きな影響を生じかねません。

中小企業自身が狙われるケースも増えています。昨今話題の「ランサムウェア（端末をウイルス感染させデータ復旧の見返りに身代金を要求する手口）」もその代表例です。身代金が目的ですから大量の

取引情報を持つているかどうかではなく、セキュリティが甘いとみられた企業が狙われる傾向があります。

■サイバーリスクに備える

サイバーリスクへの備え方は会社規模や業務特性に応じて様々です。まずはサイバーリスクの簡易診断を受け自社のリスクを確認することが有効です。

また、デジタル・リスクに完璧な備えを行うことは困難で、万が一の時に被害を最小限に抑えるには的確な初動がポイントになります。問題発覚をすぐ報告する社内ルールも重要です。

情報被害によって失われる信頼を回復するには一見過剰と思えるような対策・対応が必要となり、大きな金銭的負担が生じる可能性があります。JATAでは会員旅行会社向けに、サイバー事故対応のための様々な費用を補償する「サイバーリスク団体保険」を用意しています。

東京海上日動は、デジタル時代を生き抜く旅行会社のリスク対策のご相談も承っています。

（東京海上日動火災保険株式会社
旅行業営業部）

挑戦の数だけ、 保険がある。

To Be a Good Company



東京海上日動

