みなさまの保険情報
INSURANCE INFORMATION

TOPIC

コロナ禍で進むオンラインの活用！

サイバーリスク対策は万全ですか？

新型コロナウイルスの感染拡大の影響でテレワークなどでの活用が進むオンラインですが、それに伴ってサイバー攻撃への懸念が広まっています。2020年12月に損害保険協会が国内企業1,535社に対して行った「サイバーリスク意識・対策実態調査2020」では13.4%、205社の企業が過去にサイバー被害を受けたことがわかりました。

セキュリティ対応に苦慮する中小企業！

被害を受けた205社のうち、116社は中小企業であり、そのうち53社は複数回の被害を経験したと回答しています。

サイバーリスク対策における課題について最も多かった回答は「現在行っている対策が十分なのかわからない」というものでした。また、「対策をする費用が足りない」と回答した企業は、中小企業の比率が高く、中小企業では費用面もネックになっていることがうかがえます。

2020年6月には個人情報保護の改正法が公布されました。これが施行されると、企業において個人情報の漏えい等が発生し個人の権利利益を害するおそれがある場合には、個人情報保護委員会への報告および本人への通知が義務化されます。悪質な場合は社名も公表されるなど、企業に対する規制が強まることから、サイバー事故への対策がますます高まっているといえます。

■サイバー攻撃による被害事例（経済産業省調べ）

古いOSの使用	私物端末の利用	ホテルWi-Fiの利用	サプライチェーン攻撃
▶社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。	▶社員の私物iPhoneが会社のWi-Fiに無断で接続されていたことが判明。 ▶私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバと通信していた。 ▶検知・駆除できていなかった場合の想定被害額は4,925万円。	▶社員が出張先ホテルのWi-Fi環境でなりすましメールを受信し、添付されたマルウェアを実行したことでEmotetに感染。 ▶感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信された。	▶実証参加企業でマルウェア添付メールを集中検知。 ▶取引先のメールサーバがハックされてメールアドレスが漏えいし、それらのアドレスからマルウェア添付メールが送付されていた。 ▶メールは賞与支払い、請求書支払い等を装うなりすましメールであり、サプライチェーンを通じた標的型攻撃であった。

サイバー保険の加入も有効な対策！

企業だけでなく、個人間でもさまざまなオンライン会議システムを使ってのコミュニケーションの機会が増えています。個人や企業ができる対策の一つはセキュリティソフトを導入することです。それにより、ウイルス感染や不正アクセスなどによる情報漏洩が防止できるようになります。また、企業についてはサイバー攻撃や不正アクセスによる損害賠償などを包括的に補償するサイバー保険に加入することも有効です。

■日本代協ＰＲ動画特設サイトを開設！
2021年1月1日から公開しています！（4面に詳細）
https://nihondaikyo-pr.jp

豆事典 **「サイバー保険」とは？** サイバー保険はサイバー事故により企業に生じた第三者に対する損害賠償責任のほか、事故時に必要となる費用や自社の喪失利益を包括的に補償する保険です。