

中小企業が 「サイバー保険」を 検討する際の 勘どころ

高まる サイバーリスク

この数年、IT環境の変化やDXの推進に伴い、情報セキュリティに関する脅威が増大しています。とくに企業が保有する個人情報や技術情報を狙う、サイバー攻撃は増加の一途を辿っています。

企業がサイバー攻撃を受けた際の損失を補償する保険商品が増えています。加入を検討する際に確認したいポイントを解説します。

株式会社セフティー
代表取締役
西方 拓

「中小企業は狙われない」「うちは個人情報や機密情報がないから大丈夫」と他人事のように感じている中小企業も少なくありませんが、情報セキュリティ対策が不十分な中小企業を踏み台にして、大手企業を攻撃する「サプライチェーン攻撃」も増えています。そうしたサイバーリスクに対する備えは、中小企業にとっても避

けて通れない経営課題です。

サイバー保険 とは

サイバー保険とは、「サイバーリスクに起因して発生する様々な損害に対応するための保険」です。サイバーという名前から「サイバー攻撃を受けた際に補償される保険」と思われそうですが、実際には、情報セキュリティに関する事故（以下サイバー事故）について幅広い補償を受けられます。たとえば「カバンの置き忘れにより、取引先の個人情報一覧が記載された書類を紛失してしまい、取引先から損害賠償請求を受けた」など、自社の過失が原因で、電子媒体以外から情報漏えいが発生した場合も、補償の対象になる場合があります。

補償内容は、保険会社が提供するサイバー保険のプランにより異なるので、各保険会社の約款を確認する必要があります。ここでは、サイバー保険の基本的な補償内容について説明します。

サイバー保険の補償内容は、おまに次の3つです。

① 事故対応費用…サイバー事故

に起因して一定期間内に生じた各種費用を補償する

② 損害賠償責任…被保険者（補償の対象者）が法律上負担する損害賠償金や、争訟費用等による損害を補償する

③ 利益損害・営業継続費用…ネットワークを構成するIT機器等が機能停止することによって生じた利益損害（喪失利益・収益減少防止費用）や営業継続費用を補償する

基本補償は、①と②により構成されています。③はオプションとなっている保険もありますので注意が必要です。

事例から見る サイバー保険の補償内容

ここでは、実際に発生し得るサイバー事故と照らし合わせて、補償内容を説明します。

【事例】

外部メールから自社のパソコンがウイルスに感染。意図せず取引先にもウイルスメールを送信し、感染を拡大させてしまった。

また、自社のサーバーから取引先の個人情報流出した可能性があることも判明した。

(1) 事故対応費用

サイバー事故が発生した際に、企業はどういった対応が必要となるでしょうか。基本的な対応の流れと必要になる費用について、3つに分けて考えてみます。

① 影響や被害の調査

自社のパソコンやサーバーがどこまで感染しているのか、取引先に送信されたウイルスメールは何か通くらいあるのか、個人情報などの機密情報の流出はあるのか、それらを調べて影響範囲と被害規模を把握します。

昨今では、取引先や第三者への説明責任を求められ、専門業者を入れて証拠保全や原因究明に向けた調査分析を行なう「デジタルフォレンジック」を実施することが主流になりつつあります。このデジタルフォレンジックは端末1台につき約100万〜200万円が相場なので、ウイルスに感染した端末が複数台に及ぶと高額な費用が必要になります。

② データ復元・システム復旧

感染したウイルスがランサムウェア（身代金要求型ウイルス）の場合、データが強制的に暗号化されてしまい、システムが利用できなくなってしまういます。

通常の対応と異なり、ランサム

ウェアからデータ復元やシステム復旧を行なうのは容易ではありません。こちら結果的に専門業者に依頼することになれば、対応費用が必要です。

③ 再発防止策の策定

同様のサイバー事故が起きないように再発防止策を策定するのは当然ですが、取引先へ再発防止策を報告することも不可欠です。

また、個人情報やセンシティブ情報が漏洩していれば、2022年4月に改正された個人情報保護法に基づいて公的機関への報告が必要になるケースもあります。そうすると、再発防止策の有効性や信頼性を高めるためにも、外部コンサルティングへの相談や指導を受ける費用が掛かります。

ほかにも、B to Cのビジネスをしている企業であれば、記者会見、コールセンター設置、個人情報流出に伴う見舞金の支払いなども行なう必要があります。このような各対応の費用を補償するのが事故対応費用です。

なお、実際にサイバー事故が発生していないくても、「サイバー攻撃や情報漏えいのおそれ」があった際の調査や対応費用も補償対象

になります。

(2) 損害賠償責任

自社が原因で取引先がウイルスに感染した場合、取引先から調査費用・対応費用・業務停止に伴う損害などの賠償請求や、個人情報流出した被害者から訴訟を受ける可能性もあります。

このような損害賠償金や争訟費用など第三者への損害賠償責任を補償します。

なお、サイバー保険が補償する損害賠償責任は、サイバー攻撃だけではなく、次の3つのケースで、他人に損害を与えた場合の賠償責任・争訟費用の補償が受けられます。

① 情報漏洩、またはそのおそれによる損害（個人情報格納された電子媒体の紛失、顧客一覧が印刷された書類等の紛失、FAX誤送信による情報漏洩などに伴う損害賠償請求を受けた場合など）

② 自社ホームページ等に起因した名誉棄損やプライバシー侵害、著作権侵害などによる損害（著作権を確認せずに自社ホームページに載せた写真について著作権者から連絡があり、無断使用の事後承諾料金の請求を受

けた場合など）

③ 社員のIT業務の遂行に起因して発生した損害（システム運用や利用における誤操作、システム不具合などの事故により第三者に与えた損害の賠償請求を受けた場合など）

損害賠償は被害規模によって金額が大きく異なりますが、数千万円にものぼる損害賠償請求を受けた例もあります。

(3) 利益損害・営業継続費用

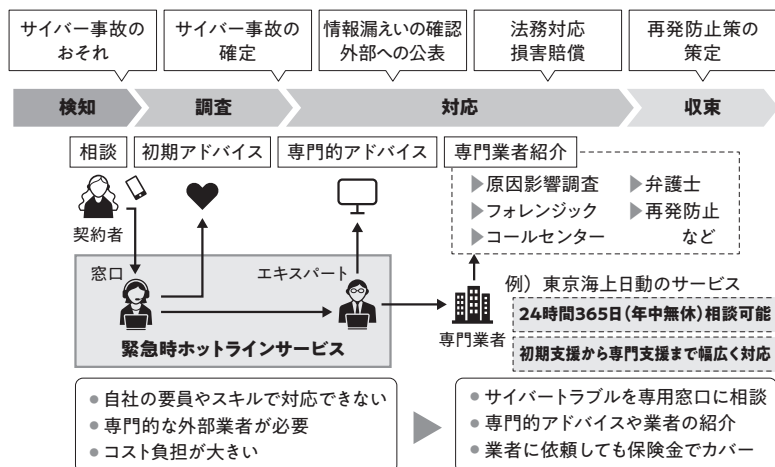
サイバー事故により業務の中断や停止を余儀なくされると、本来得ることができたはずの利益が失われます。その喪失利益（利益損害）や、システムの機能が復旧するまでの期間に支出した費用（営業継続費用）をサイバー保険は補償します。

また、サイバー攻撃だけではなく、不測かつ突発的なシステム操作やデータ処理上の過誤等によりシステムが停止した際に生じた利益損害・営業継続費用も補償範囲に含まれます。

サイバー保険の付帯サービス

ここまで、サイバー保険の基本

●サイバー保険の付帯サービスの例



※保険会社ごとにサイバー保険の補償内容が異なるように、付帯サービスも異なる。また、一部付帯サービスは有料となる場合もあるので注意が必要。

的な補償について説明してきましたが、ほかにもサイバー保険に加入することで得られる大きなメリットがあります。それが付帯サービスです(左図)。

付帯サービスの内容は、サイバー事故が発生していない平時の事前対策に利用できるサービスと、サイバー事故後の有事に利用できるサービスの2つに分かれます。

平時に利用できるサービスで

は、サイバー事故のリスクを事前に把握できる「情報セキュリティ診断サービス」や、社員のセキュリティ教育に関するツールやサイバー関連の最新情報を得られる「教育支援ツールや情報誌の提供」、そして、防災訓練のようにサイバー攻撃の1つである「標的型メールの訓練」等を利用することでサイバー事故の発生リスクを低減させることができます。

サイバー事故後の有事に利用できる「緊急時サポートサービス」は、中小企業が一番恩恵を得られる仕組みです。

たとえば、サイバー事故が発生した際に中小企業では「自社の社員やスキルでは対応できない」「専門業者の手配に時間がかかる」「対応に要するコスト負担が大きい」などの問題が生じます。

そこで、サイバー保険の付帯サービスでは、サイバー事故が発生した際(また

は発生したおそれがある際)に利用できる緊急時のサポート体制を用意しています。

このサービスを利用することにより、迅速に相談できる窓口や、調査や対応を行なう専門業者、再発防止策の相談をするコンサルタント等の手配や支援を保険会社がサポートします。

サイバー保険に加入する際の勘どころ

最後に、サイバー保険に加入する際の勘どころを解説します。

(1) 事前に自社のサイバーリスクの把握と対策を行なう

サイバー保険の保険料は、売上高・業種・補償内容・過去に起こしたサイバー事故、そしてセキュリティ状況によって保険料が決まります。セキュリティ対策の状況によっては、保険料が増加することになります。加入前に自社のサイバーリスクを把握し、セキュリティ対策を行なうことで、保険料を抑えましょう。

(2) 補償内容を把握し、保険金額を検討する

最初から補償範囲を手広くすると保険料が高くなります。実際に

サイバー事故が発生した際に、事故対応費用や損害賠償金額の合計はどのくらいになるのか、リスクとファイナンス状況を照らし合わせて補償範囲を把握し、保険金額を検討しましょう。また、損害の一定部分を自己負担することで、契約時に設定する保険料負担が軽減される「免責金額」を高く設定すれば保険料は安くなります。

しかし、サイバー攻撃などにによりウイルス感染した際に必要なフォレンジック調査は、想定以上に高額となるがあるので注意が必要です。しっかりと自社の状況と補償範囲を確認しましょう。

(3) 複数の保険会社を比較する

サイバー保険は、保険会社によって保険料の算出方法や補償範囲、付帯サービスが大きく異なります。

中小企業では、とくに緊急時のトラブル対応や情報セキュリティ診断サービス、情報提供などの付帯サービスがある保険会社を選択することをおすすめします。

また、サイバー保険は比較的新しい保険なので、補償内容や免責事項が逐次変化しています。加入時は、各保険会社の最新情報を手に入れて比較検討しましょう。

にしかたなく、保険代理店セブティ代表取締役。中小企業の悩みや将来のビジョンに耳を傾け、リスクの洗い出しから対策までを全面的にサポートする。生損保をミックスした個人・法人のリスクコンサルティングに取り組む。