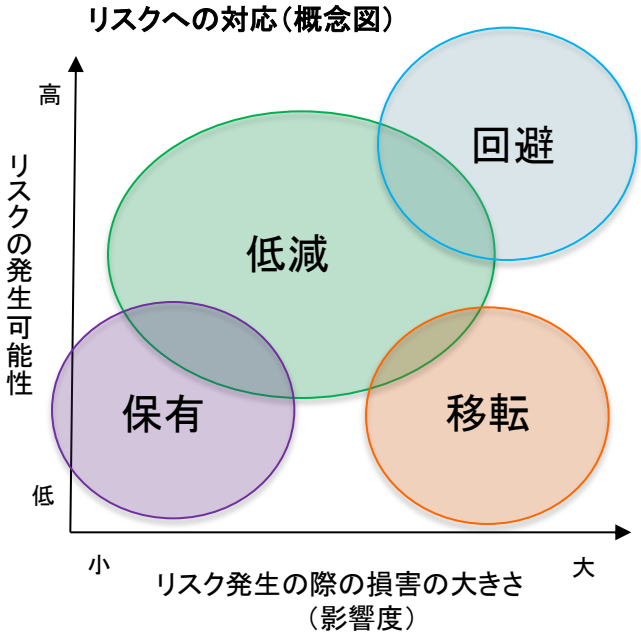
Ksisnetだより
発行:Ksisnet事務局
平成30年9月11日
Vol.53

サイバー保険を知っていますか？

情報セキュリティにおけるリスク対処の方法には、大きく分けて**低減、保有、回避、移転**の4つがあります。

リスクは脆弱性×脅威で表すことができ、脆弱性は「組織の弱点」、脅威は不正アクセスやサイバー攻撃といった「損害を与える可能性のある要因」のことを指します。

脅威は外部要因であるためコントロールできないことから、**リスクを下げるには脆弱性を下げる**ことを考えなくてはいけません。



1　リスクの低減

脆弱性に対して情報セキュリティ対策を講じることにより、脅威発生の可能性を下げること。

(例)　PCの盗難に備えて情報を暗号化しておく。

2　リスクの保有

そのリスクの持つ影響力が小さいため、特にリスクを低減するためのセキュリティ対策を行わず、許容範囲内として受容すること。

(例)　現状では実施すべきセキュリティ対策が見当たらない場合等

3　リスクの回避

脅威発生の要因を停止、又は全く別の方法に変更することにより、リスク発生の可能性を取り除くこと。

(例)　外部との接続を断ち、不正アクセスの脅威から逃れる。

4　リスクの移転

リスクを他社などに移すこと。
ただし多くの場合、金銭的なリスクなど、リスクの一部のみが移転できる。

(例)　リスクが顕在化したときに備えて保険などで損失を充当する。

サイバー保険は「リスクの移転」に分類されます

参考　ＩＰＡ（情報処理推進機構）

サイバー保険ってどんなもの？

外部からの不正アクセスなどにより発生した「個人情報の流出」や「業務妨害」などの被害を、包括的かつ総合的に補償する損害保険のことです。

政府の「サイバーセキュリティ戦略2018」には中小企業の取組の1つとして「サイバーセキュリティ保険の活用促進」が示されています。

サイバー保険のメリットは？

被害が発生した時に金銭的な補償を受けることができます。

マイナンバー制度の導入により、これまでの個人情報に比べて紐ついている情報が広範囲にわたるため、より不正に使用されるリスクが高くなっています。そして一度情報が流出すれば、企業が受けるダメージは大変大きなものとなり、金銭的被害も大きくなります。サイバー保険はこの金銭的被害を補償してくれるのです。

加入の際に気をつけることは？

保険会社によって補償内容が異なるので、保険のメリットを最大限に活用するためには、保険の補償内容についてしっかりと確認する必要があります。

例えば、ランサムウェアの要求に対して支払ってしまった身代金などの補償は受けられないことがあるので、補償内容の確認は重要です。

サイバー保険に加入しても…

セキュリティ対策はしっかりとしましょう！！

たとえ保険に加入したからといって、セキュリティ対策を怠ってはいけません。

サイバー攻撃を100%防ぐことはできません。一度被害が発生すれば、企業のダメージは大きなものです。保険はあくまで被害が発生した際の補償であり、万が一に備えるためのものです。

セキュリティ対策をしっかりとした上で、保険の内容を確認し、自分たちの会社に合った保険を選んで加入することが重要です。