第１６４回　令和８年１月２８日（水）

「リスクマネジメントについて。」

業務改善を行ったり、イノベーションを推進したりするとき、リスクが発生します。情報セキュリティーは大丈夫か、コンプライアンスは十分果たされているか、人権上問題はないかなど、あらゆる角度からの検討が必要です。

リスクは発生する確率と、発生したときの影響度を評価して考えます。損失があまりにも大きい場合にはプロジェクトそのものの見直しが求められる場合もあります。

リスクの大きさや頻度によって対策が変わります。

① 回避　これは活動を停止してリスクを完全に避けることです。高リスクの場合に考えられます。
② 低減　セキュリティーの強化や予防措置などです。発生確率や影響度を和らげます。
③ 移転　リスクを第三者に移してしまうことです。ひどいように思えますが、保険に入ることなどはこれにあたります。何かおきたときは保険会社に支払ってもらいます。
④ 受容　リスクが小さければある程度受け入れることも必要です。リスクは分散することができますがなくなることはないので小さいリスクなら受け止めるほうが被害が少ないことがあります。

近年は情報リスクが増えています。個人情報の流失のニュースは毎日のように新聞をにぎわしています。アサヒビールの被害は記憶に新しいところです。

情報セキュリティーは許可されたものだけがアクセスできる「機密性」と、正確であることが求められる「完全性」、そして必要な時いつでも取り出せる「可用性」が求められます。

悪意のあるソフトウェアによる攻撃や不正アクセスが後を絶ちません。システムの脆弱性はいたちごっこで防御と攻撃がめまぐるしく入れ替わります。ただ情報漏洩で一番多い原因はヒューマンエラーです。電話番号やメールアドレスの漏洩により、営業の電話がかかってくることは珍しくありません。

複雑な携帯番号でも詐欺電話がかかってきます。特に高齢者を狙った特殊詐欺などが個人情報を悪用しています。休日など多いときは２～３件かかってきますが最近は「迷惑電話」の表示が出るので便利です。

警視庁がデジポリスというアプリで詐欺の電話をカットできるようにしました。しかしそのうちデジポリスをかたった詐欺電話がでてくると思います。結局はいたちごっこで被害にあわないように「自分だけは大丈夫」と考えないようにすることが一番の予防です。

便利な世の中になればなるほどリスクは増えていくでしょう。残念ですが何事も疑ってかかることが一番の予防策かもしれません。