中小企業の情報セキュリティ対策ー情報漏えいの実態は？

高額な賠償請求や金銭的損失を伴うことも多く、情報漏えいは企業にとって死活問題。中小企業の情報セキュリティ対策について考えてみましょう。（対策編は6月号でご案内予定）

●情報漏えいが与える4つの経営リスク

情報漏えい事故では、①金銭の損失、②顧客の喪失、③業務の停滞といった直接的な問題だけでなく、④従業員への影響というリスクが発生します。

セキュリティ対策不足で内部不正ができるような職場環境にあることで、「従業員のモラルダウンを招いたり、退職者が増えたり」など、思わぬところで影響が出ます。人手不足時代には大きな経営リスクとなりましょう。

★ウィルス感染で業務停止、被害が数千万円

（情報通信業　社員数101～300名）

社内ＰＣやｻｰﾊﾞｰがｳｨﾙｽ感染。数日間業務停止し、復旧のため徹夜対応したその被害額は数千万円！

★顧客情報の入ったＰＣの紛失で取引先の信用を失墜

（情報通信業　社員数101～300名）

社員が顧客情報の入ったﾊﾟｿｺﾝを持ち出し、ﾊﾟｿｺﾝを紛失。顧客に紛失を報告したが信用は失墜。

●情報漏えいしやすい場面とは？

◆情報の持ち出し

ＰＣやＵＳＢ、書類を社外に持ち出すだけで紛失盗難リスクを伴います。一方で、内部関係者や外部委託者などが“意図的に”情報を持ち出すケースも…。

◆メールとＦＡＸの誤送信

メールだけでなくＦＡＸの誤送信も注意が必要！

◆書類やデータの廃棄

機密書類やＰＣ廃棄の際、情報流出するケースがあります。他にもコピー機、複合機内に残っているデータにも注意が必要です。

◆サイバー攻撃

悪意をもった外部攻撃はどんどん進化し、次から次へと新たな手口で狙ってきます。

●まずは現状把握から！

◆社内情報の棚卸と秘密情報の判定

社内の情報をリストアップし、どう管理されているか?、これらのうち漏えいさせてはいけないものがどれなのか、といった現状把握が重要です。

●お客様等取引先の連絡先情報、●従業員のマイナンバーや給与明細、●取引先ごとの仕切り額、●新製品の設計図、●取引先から取扱注意として預かった書類等を、どのように管理しているか、漏えい対策の有無などを確認します。

◆5分でできる情報セキュリティ自社診断

（独法）情報処理推進機構のＨＰで、中小企業向けに無料で情報セキュリティ診断を公開中。

25の質問に答えるだけで、自社のセキュリティ上のリスクが把握できます。項目ごとに費用をかけずに効果がある対策例なども案内されています。

●経験者が語る情報持ち出しのワケ

◆情報持ち出しの理由は“うっかり”が6割

故意または過失で情報流出させたことがある社員（民間企業）へのアンケートでは、情報持ち出しの理由としては“うっかり”と“ルールを知らずに違反”など過失のケースが６割が占めます。

一方故意に持ち出した理由としては、“忙しくて社外で仕事するため”、“処遇や待遇に不満あり”、“持ち出して転職や起業に利用したかった”、“会社や上司に恨みあり”など。

◆持ち出し手段はトップは“ＵＳＢメモリ”

持ち出した情報の種類は、顧客情報、技術情報、営業計画。

方法としては、１位がUSBメモリ（43.6%）。電子メール、パソコンがこれに続きます。持ち出した社員の職種としては、技術者、開発者、システム管理者、派遣社員の順でした。

情報漏えいで問われる企業の責任

法　令	行　　為	処　罰　な　ど
個人情報保護法	不正な利益のために個人情報を提供、盗用した場合	1年以下の懲役又は50万円以下の罰金（社員の違反行為でも法人にも罰金刑あり）
マイナンバー法	不正な利益のために個人情報を提供、盗用した場合	3年以下の懲役又は150万円以下の罰金（社員の違反行為でも法人にも罰金刑あり）
不正競争防止法	企業秘密として法律の保護対象となる情報の漏えい	損害賠償、利益侵害の停止等
金融商品取引法	ｲﾝｻｲﾀﾞｰ取引規制の違反等	5年以下の懲役又は500万円以下の罰金（社員の違反行為でも法人にも罰金刑あり）
民　　法	不法行為による損害賠償	故意または過失による他人の利益侵害に対する損害賠償責任

Copyright© EIWA Consulting, Inc. All Rights Reserved