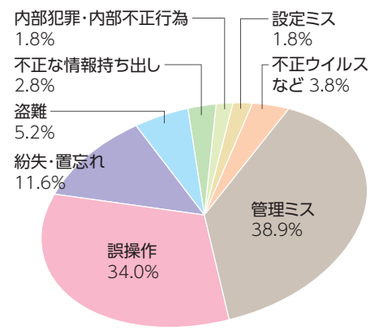
個人情報を守ることは事業者の責任です。

情報システムの進展は多くの企業に浸透し、さまざまな業務でITが活用されています。その反面、管理ミスやウイルス感染等による個人情報の漏えい事故が多く発生しています。そしてその流出した情報は、人権侵害につながったり、犯罪に使われたりする危険性があります。また、事故を起こした企業側も信頼を大きく失墜するとともに、経営的にも多大な損失を受けることになります。そうなる前に、大企業・中小企業にかかわらず、個人情報の保護を自社の問題として取り組むことは、重要な社会的責任なのです。

●情報漏えいの原因



参考:「2012年情報セキュリティインシデントに関する調査報告書【上半期 速報版】」より引用 NPO 日本ネットワークセキュリティ協会調査

もし漏えい事故が起きると、どのような影響があるのでしょうか?

●多額な損害賠償を負うことに▶数百万円、場合によっては数億円

賠償額は概ね被害者1人あたり500円から数万円といわれていますが、流出した件数が多ければ、それだけ賠償額は膨らむことになり、企業にとって致命的な額になることもあります。

●社会的信用が失墜することに▶取引停止や顧客減少に

損害賠償などの損失も大きいですが、その後の社会的信用の低下による取引停止や顧客の減少などの影響は、企業にとってもっと深刻です。

●こんな影響も… ▶**対応措置の見直し費用**……システムやデータの検証にかかるコスト。
▶**業務効率の低下**……殺到する問合せや苦情への対応。

●法律による罰則も… 主務大臣の勧告・命令に従わない場合は「6カ月以下の懲役または30万円以下の罰金」が課せられる場合があります。

できるところから対策を立てることが大切です!

『個人情報の取り扱いに関して適切な管理体制を整え、プライバシーマーク※を取得』というような標準的な対策が、漏えい防止の最も効果的な方法です。
しかし、プライバシーマークの取得には、時間がかかりますし、その間に情報漏えい事故が起こらないとも限りません。そのためにも身近にできる対策から行うことが大切です。

対策1 経営者自らが率先して個人情報の保護に取り組む
経営者の決意が浸透することにより、企業全体の意識改善を促します。

対策2 整理整頓
まず身の回りを整理して、個人情報に関係する書類を机に置いたままにしないなどのルールを作ることが大切です。

対策3 所持している個人情報を洗い出す
個人情報は思わぬところに散在しています。どこにどんな個人情報があるのかを調査し、明らかにすることが重要です。

対策4 不必要なものを廃棄する
必要なものと不必要なものを選択し、不必要な個人情報は適切な方法で廃棄しましょう。また、不必要な個人情報は取得しないようにしましょう。

対策5 管理者を明確にする
管理者を設定して、使用・保管に関して組織で管理する体制を整えます。

※プライバシーマークとは
プライバシーマーク制度は、日本工業規格「JIS Q 15001個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度です。

プライバシーマークの取得を契機に社員の情報保護意識が向上しました

クボタシステム開発株式会社
品質管理部 ISMS審査員補
鳥越 俊郎氏

当社は、製造業向けITソリューションの提供やシステムサービスを主な事業としており、その業務の中で膨大な個人情報を扱っています。当社の「個人情報保護を確実に実施する体制」を評価する指標の一つとして、平成17年に「プライバシーマーク」を取得し、今年４回目の更新をしました。

プライバシーマークの取得は、社会的信用が得られるだけに、取引要件とする企業が増加する昨今では、ビジネス面でのメリットもあると考えます。何より、更新審査における外部機関からの指摘・指導により、社内の管理体制や規程が整備運用され、個人情報保護に関する社員の意識が根付いていくことに意義があると考えます。

当社での個人情報の管理方法は、各社員が「個人データ管理表」と呼ばれる電子データを作成し、事業活動の各場面で入手した個人情報の「保管方法、保管場所、保管期限、件数、予想されるリスク」等を入力し管理しています。

紙台帳では、保管や更新の手間がかかるので、管理不十分となりますが、電子化し個々のPCから閲覧・更新できることで管理レベルも上がります。また、従業員自身は、「自分が所有する個人情報は決められたルールに基づいて自分自身で管理する」意識が育っていると感じています。

このほか、年2回の社内監査での運用状況のチェックや当社独自の「情報セキュリティハンドブック」の配付、eラーニングの実施などにより情報保護の知識と意識の向上を図っています。

企業が保有する情報の漏えい事故が発生すると、企業の社会的信用を失うばかりでなく、多額の損害賠償等を負うこともあり、最悪の場合、企業存続危機を招きます。そのリスクを考えれば、多少コストがかかっても、定期的に外部審査を受け、プライバシーマークなど各種認証を維持する意義は大きいと判断しています。

もちろん、プライバシーマークを取得しなくても管理する仕組み(ルール)と意識があれば個人情報保護は可能です。

当社の情報漏えい対策の一例として紹介すると、①パソコンの社外持ち出しの際、OSだけでなく機器自体にもパスワードをかける、②業務に必要なアプリケーション以外のインストール禁止、③セキュリティアップデートの徹底などがあります。

最後に当社が個人情報保護で最も重要だと考えることは、「個人情報を特定すること、その個人情報を保有・利用などの場面において漏えいに繋がるリスクを洗い出して対策する。」ことです。事業環境は常に変動しており、当社でも「リスクの洗い出しと対策」は継続的な課題です。全社員の意識向上を図る事で、会社全体のセキュリティレベル向上に取組んでいきたいと考えます。

人権侵害や犯罪につながることも

●プライバシーの侵害
他人に知られたくない情報を知られて不快な思いをしたり、結婚や就職の際の身元調査などに悪用されるなどの危険性があります。

●不快な勧誘に利用される
広告メールを筆頭に、パンフレットやカタログなどの送付物、電話勧誘などが増え、精神的な苦痛につながることもあります。

●犯罪に使われる危険性
クレジットカードやキャッシュカードの不正利用をされたり、また、最近では漏えい情報を基に、振り込め詐欺のターゲットにされるなどの危険性があります。

ほんの少しの油断から大きな問題になることをしっかりとご理解ください。

キリトリ

郵便はがき

料金受取人払郵便
大阪西局
承 認
944

差出有効期間
平成26年2月
28日まで

5508790
527

大阪市西区立売堀4-10-18
阿波座センタービル１階
大阪市人権啓発・相談センター 行

プレゼント送付先

ご 住 所	〒
お 名 前	

よろしければ貴社の従業員数をお教えください。 約(　　)人