顧客情報・個人情報、大丈夫ですか？

情報セキュリティ対策は万全に!!

特集2 情報漏えい対策

個人情報保護の大切さは、経営者であれば
どなたでも理解されていることと思います。
けれども、現実には毎週のように「情報漏えい」
の報道が、メディアを賑わせています。
ひとつ間違えば会社の存亡にもかかわる、
個人情報漏えいや情報セキュリティ。
今回はその対策について特集します。

セキュリティ対策は、中小企業が有利

個人情報漏えいについての報道は、残念ながら珍しいものではありません。故意にせよ過失にせよ、漏えいは防ぎようがないのかと思ってしまうほど、しばしば発生しています。

大企業や行政でさえ防げないのであれば、わが社のような中小企業では絶対に無理――そんなふうに考える経営者もおられるのではないでしょうか。

ところが、情報漏えい対策は中小企業の方がやりやすいのです。理由は簡単、組織が小さいからです。

情報セキュリティ対策は、本来それほどコストがかかるものではありません。せいぜいウィルスソフトを導入する程度で済む場合もしばしばです。むしろ、社員全体がセキュリティ意識を共有できるようにする手間の方が、大変なのです。

また、対策を講じるためには問題点の分析をする必要がありますが、その場合でも組織が小さければそれだけ手間も少なくて済みます。

このように、本来は大企業よりも中小企業の方が、セキュリティ対策を実行しやすいのです。

ただ、中小企業の場合、セキュリティ対策専門の部署や社員を置くだけの余裕がないことがほとんどでしょう。セキュリティは総務的な仕事ですから、直接的な利益は生みません。また、ある程度専門知識

が、少なくないのではないでしょうか？

そこで同ホームページには、経営者や社員などが最低限注意すべき項目が、チェックリスト形式で表示されています。それを転載したのが、表1です。ユーザーとあるのは、一般の社員と考えて結構です。

こうしてみると、本当に基本的なことばかりなのですが、仮にあなたがこの半分でもYESと答えられるのであれば、なかなか優秀（？）と言ってもいいでしょう。そのくらい、一般的には何の対策も立てていないことが多いのです。

実は、今年に入って、IPAの職員が個人情報漏えいをしてしまっていたことが発覚しました。情報漏えい対策の総本山でさえ、うっかりするとそんなことが起こるのです。一般企業であれば、なおさら注意が必要です。

〈表1〉情報漏えい対策チェックポイント

経営者のみなさんにチェックしていただきたいポイント

貴方の会社から個人情報が漏えいしたら、企業の信用が失われます。そうなる前に、会社の予防・対策の実施状況をチェックしましょう。

- □ 個人情報漏えいに対する取り組みは経営者層が主導していますか？
- □ 社内に対策の実施内容（セキュリティポリシー等）を明示して、それに沿った対策を実施していますか？
- □ 採用、退職の際に守秘義務に関する書面を取り交わしていますか？
- □ 個人情報保護の必要性を全従業者に意識付けしていますか？
- □ （あなたの会社がWebサイトを運営している場合には、）サイト管理者に、脆弱性対策をしているか、確認していますか？

ユーザのみなさんにチェックしていただきたいポイント

普段PCを使用している中で、思わずこんな事をしていませんか？場合によっては、貴方の大事な個人情報が危険な状態になっているかも知れません、チェックしてみましょう。

- □ 電子メールやFAXを送る前に、送り先をしっかり確認していますか？
- □ 職場から個人情報を許可なく持ち出していませんか？
- □ 職場から個人情報を持ち出した場合は次の点に注意していますか？
  ①大事な情報を置き忘れないように、気をつけていますか？
  ②個人情報の入ったPCやUSBメモリ、書類等を車の中に長時間置いたままにしていませんか？
- □ ファイル交換ソフトを利用していませんか？
- □ ウェブサイトに個人情報を入力するとき、そのサイトが本物であるか確認していますか？
- □ Windows Update等を利用して修正プログラムを適用していますか？ □ ウイルス対策ソフトを導入していますか？
- □ ウイルス対策ソフトのウイルス定義ファイル・パターンファイルは更新していますか？
- □ ウイルス対策ソフトでPC内を定期的にチェックしていますか？
- □ 定期的にパスワードを変更していますか？ □ 個人情報が書かれた書類をシュレッダーなどにかけて廃棄していますか？

情報漏えい対策は？

独立行政法人情報処理推進機構（以下IPA）のホームページに、企業の個人情報漏えいを防ぐために設けられたコーナーがあります。

「漏れたら大変！　個人情報」（http://www.ipa.go.jp/security/kojinjoho/index.html）（図1）にアクセスすると、こんな説明が掲示されています。

〈図1〉独立行政法人情報処理推進機構 HP

個人情報が漏れるとこんな事が！

- 顧客の名前や住所、電話番号などの個人情報が漏れると、顧客はもちろん、漏らした本人や企業にとっても大きな損失になります。
- 漏えいした個人情報の中に、銀行口座やクレジットカード番号などの決済情報が含まれていたために、勝手に自分になりすまされて、知らない間に高価な買い物をされてしまう等の金銭的な被害に遭う危険性があります。
- クレジットカード番号や電話番号等の個人情報を闇市場で売買される例もあります。闇市場に流れた個人情報はどこで悪用されるか分かりません。
- 企業から個人情報が漏えいした場合には（社員個人から漏えいした場合も同じです）、企業の信用失墜、損害賠償等、大きな損失に繋がります。

そんなこと、常識でしょう――と思った人も多いと思います。そう、誰でも知っていることなのですが、では漏えい対策をやっているかと言えば…どうでしょうか？　せいぜい「情報管理は徹底するように」など、抽象的な指示を出すだけという会社

ファイル交換ソフトは厳禁！

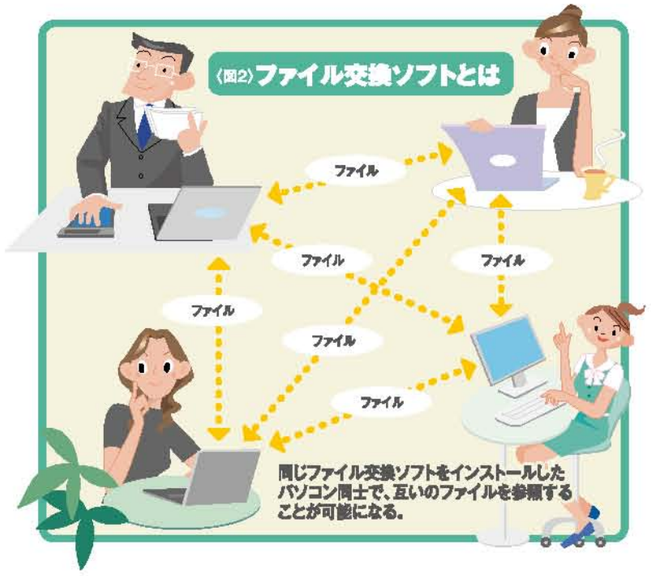
最近の情報漏えいの多くが、「ウィニー」などのファイル交換ソフトが原因で発生しています。

ファイル交換ソフト（ファイル共有ソフトとも呼ばれます）とは、インターネットを通じて動画や音楽、画像などさまざまなファイルを多数のユーザーと共有するソフトウェアのことです。このソフトをインストールすると、自分のパソコン内に他人との共有部分が作られ、そこに置いたファイルは基本的には無制限に、同じソフトをインストールした別のパソコンからアクセスされることになります。（図2）

もともとは、ファイル所有を複数のパソコンに分散させることで利便性を高めることが目的だったのですが、最近では音楽や動画の不正コピーのやりとりに使用されることが多くなりました。つまり、著作権法違反が利用目的になってしまっているのです。

さて、ファイル交換ソフトの設定を一つ間違えると、実はパソコン全体が他者から丸見えになってしまいます。そうなると、そのパソコンからはすべての情報が他者に漏れてしまうことになります。それに気づかないまま、うっかり個人情報の入ったファイルを持ってきてしまえば、それも「共有」されて、情報漏えいにつながってしまいます。

また、同じソフトをインストールしているどこかのパソコンがウィルスに汚染されたとします。するとそのウィルスは、たちまちソフト経由で広範囲に感染してしまいます。そのウイルスが「パソコンに入っている情報を盗んでくる」能力を持っていれば、これもまた情報漏えいにつながっていきます。



このように、こと業務だけを考えれば、ファイル交換ソフトは百害あって一利なし。会社のパソコンには絶対にインストールさせないようにしましょう。また、個人のパソコンにもインストールしないよう、社員を教育する必要があるでしょう。そうは言っても、経営者が社員の私物まで管理することはできませんから、

- 仕事関係のファイルは、社内から持ち出さない。
- 仕事を家に持ち帰らない。
- USBメモリなどは、社内に持ち込まない。

などの注意をする必要があるでしょう。

情報セキュリティはどこから始める？

個人情報漏えいに限らず、最近では不正アクセスやウィルス汚染など、さまざまな情報セキュリティ問題があります。

情報セキュリティを確立するためには、セキュリティ・ポリシーをしっかり作成し、さまざまな対策を講じる必要があります。けれども、一般の中小企業にとって、なかなか荷が重いことは否めません。

たとえば経済産業省では、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」という文書を出しており、その中で「安全管理措置」として約10ページにわたって何項目もの注意事項を列記しています。確かに重要なことばかりですが、中小企業がいきなりすべて遵守するのは、少々難しいようです。そこで、これらを最終目標としつつ、できるところから始めていくことが重要になってきます。

そこで、まず最初のステップとして、表2の項目から始めてみてはいかがでしょうか。表1のチェックリストと併用すれば、これだけでもかなり高度なセキュリティ対策になります。

また、これはコンピューターに関連した対策ですが、情報漏えいには紙媒体での紛失や盗難なども考えられます。机の上にうっかり置いてしまった機密文書を、打ち合わせに来た他社の人間に見られ、そこから情報漏えいにつながることも、珍しくはありません。こうしたことは、社員教育の問題でしょう。

情報セキュリティと言うと、私たちはついコンピューターにばかり目が行きがちですが、実は大きく言えば組織の在り方自体が、セキュリティに直結しているのです。

「企業は人」とはよく聞く言葉ですが、セキュリティについてもまさにその通り。「セキュリティは人」なのです。制度を作ったりソフトをインストールしただけで安心せずに、ぜひ、社員一人ひとりの啓蒙にも力を注いでください。

〈参考資料〉
- 経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」
- IPAホームページ（http://www.ipa.go.jp/）
- IPA『情報セキュリティ白書2008』

〈表2〉安全対策最初の一歩

◎セキュリティソフトは常に最新版を使用する。

セキュリティソフトは毎年新しいバージョンが出ています。できるだけ最新のものを購入し、インストールしましょう。また、社内のパソコンすべてにインストールしてください。

◎パソコンのID、パスワードの管理はしっかりと行う。

すべてのパソコンはIDとパスワードを設定しましょう。それらは社員1人ひとりが責任を持って管理しましょう。間違っても、メモして見えるところに貼っておいたりしなように。

◎ウェブサイトやメールに注意。

怪しいサイトにアクセスしたり、見知らぬ人からのメールを不用意に開くと、ウィルスに汚染される危険性があります。また最近では個人情報漏えいにつながることもあります。

◎業務に不要なソフトはインストールしない。

社会人として当然ですね。ゲームなどを入れたりしてはいけません。ファイル共有ソフトなどもってのほかです。

◎データのバックアップは定期的に。

できれば、社内でルールを作り、全員が守るようにしましょう。