

個人情報・機密情報の漏洩対策5つのポイント(管理対策編)

執筆者：ISO9001/14001/ISMS コンサルタント 西村明吉

あなたの会社では、情報漏洩防止のための対策はできていますか？

最近、Winny(ファイル交換ソフト)の脆弱性による個人情報や機密情報等の漏洩事件が数多く報じられています。

漏洩事件の多くは、「人による原因」といわれています。すなわち、会社などでルールを定めていても、それを知らなかったり、また、ルールを知っていながらそれを守らなかったために、漏洩事件につながったという例が多いのです。

ここで、個人情報や機密情報等の漏洩を予防するための方策について考えてみましょう。あなたの会社で、以下の予防策が講じられていますか。今回のレポートでは、今日からでも取り組める「管理的対策」の5つのポイントについて述べてみたいと思います。

『ファイル交換ソフトの使用条件が決まっていますか？』

漏洩事件では、会社の業務に使用するパソコンに、ファイル交換ソフトWinnyがインストールされて、会社の機密情報が漏洩した例があります。また、Winnyソフトがインストールされた私有パソコンに、会社の業務データ(機密情報)が入力されていて、業務データが漏洩した例もあります。従って、会社の業務に使用するパソコンにWinnyソフトをインストールしないこと。また、私有パソコンには会社の業務データを入力しないこと。この2点をルールとして定めておく必要があります。

『私有パソコンの利用条件は決まっていますか？』

上記のように私用パソコンの使用によって、漏洩事件が発生します。

多くの会社では、会社の業務には私用パソコンを使用しないことをルールとして定めて

います。なかには、持ち運びのできるノートパソコンは、会社の業務には使用しないことを定めている会社もあります。

従って、私用パソコンの使用を会社業務に全面的に禁止するか、また一定の条件(使用条件について上司の承認が必要)を設けて、私有パソコンを使用することをルールとして定めておく必要があります。

『個人情報や機密情報等の外部への持ち出しについてルールが定められていますか?』

2005年4月1日に「個人情報保護法」が全面施行されたことによって、多くの会社では、個人情報(個人データ)の取扱いについての社内規則の制定、教育の実施が行われてきました。しかしながら、会社の業務データ(機密情報)についての取扱いについては、十分といえない面があります。

単に、パソコンに入力されているものが機密情報とは限りません。紙に印刷された書類も機密情報が含まれています。例えば、会社の経営情報、新製品・新技術の資料、

顧客先リスト、人事データなどが挙げられます。また、会社の業務を訪問先や自宅で行う場合が考えられます。その場合、書類が入っていたカバンを置き忘れた、また盗難にあったとして個人情報や機密情報が漏洩することがあります。

一般的には、会社の業務データは外部に持ち出さないことが望ましいことですが、業務遂行上、やむを得ず業務データを外部に持ち出す場合があります。そのような場合、外部への持ち出しについて、ルールとして定めておく必要があります。どのような業務データを、どのような媒体(パソコン中の電子データ、CD・FD・USB等の記憶媒体、書類など)で外部に持ち出すかについて上司の承認を得ること、また外部から持ち帰った業務データを確認するなどルールとして定めておきます。

外部に持ち出すことの危険性(リスク)について事前に社内で十分、検討しておかねばなりません。駐車場では、車の中にパソコ

ンや書類の入ったカバンを放置しないこと、
電車の網棚にカバンを置かないことなど、
外部での行動についても、教育等で徹底す
る必要があります。

**『記憶媒体等の廃棄についての手順が決
まっていますか？』**

パソコンを廃棄する場合、内部に記憶し
ているデータを消去するには、専門的な知
識が必要です。産業廃棄物として処理する
前に、データを完全に消去する必要があります。
消去のプログラムの活用、消去作業
を行う専門業者への委託などがあります。
また、取り外し可能な記憶媒体 (CD・FD・
USB 等) を廃棄する場合は、切断などして
記憶媒体そのものを破壊します。

また、個人情報や機密情報等を含む書類
は、シュレッダーなどで切断します。

このように記憶媒体等についての廃棄基
準を明確にルールとして定め、社内教育で
徹底する必要があります。

**『職場におけるクライアントパソコンのウイ
ルス対策状況の把握が十分できています
か？』**

情報漏洩事件は、ウイルスが侵入して発
生することが多いのです。ウイルスは、メー
ルなどを通じて感染します。職場内の全部
のパソコンがウイルス対策 (ソフトの更新・
セキュリティパッチ対策、ウイルスワクチン
のインストール・更新など) を行ってこそ、そ
の職場のウイルス対策が万全ということが
できます。

例えば、1台のパソコンにウイルス対策が
行われていない場合、その1台にウイル
スが感染して、そのパソコンを通じて、会社の
機密情報等が盗まれる場合があります。

従って、職場内にはウイルス対策担当者
において、職場内の全部のパソコンにウイル
ス対策が行われていることを常に把握して
おく必要があります。同時に、それぞれの

パソコンにインストールされているソフトも

監視する必要があります。