情報セキュリティの脅威と対策①
（基礎編・中小企業の情報漏えい対策）

独立行政法人　情報処理推進機構
セキュリティセンター　研究員
中小企業診断士
江島　将和

組合活動においてパソコンやメール等のITツールは必要不可欠な存在になりましたが、同時に、情報セキュリティに関する脅威も増大しています。もし、組合員から預かっている大切な情報を漏えいしてしまうと、組合員から信頼を失うだけでなく訴訟や賠償など大きな問題に発展する可能性もあります。そこで今回は、押さえておきたい情報漏えい対策７つのポイントをご紹介します。

1．持ち出し禁止

自宅や外出先等で業務を実施するために、組合のパソコンや書類を勝手に持ち出すことは、ご法度です。もし、業務情報等を事務所外でうっかり置忘れ・紛失したり、盗難にあったりすると、情報漏えい事故となってしまいます。

事務所外業務で必要な情報を持ち出す際は、持ち出しの許可を得たうえで、書類など紙媒体であれば、外では必要もなく鞄から出さない、鞄は肌身離さず持ち歩くなど盗難・紛失対策が必要です。また、パソコンなど電子媒体であれば、盗難・紛失対策に加えて、推測されにくいパスワードで保護する、データの暗号化をするなど他人に電子媒体の中身が見られないようにする対策が必要です。

しかし、まずは『大切な情報は持ち出さない』ということを原則とすべきでしょう。

2．安易な放置禁止

具体的な、やってはいけない例から考えてみましょう。

× 業務上大切な書類を机の上に放置したまま席を離れる、あるいは帰宅する
× 大切な情報が格納された電子媒体や書類を、鍵のかかるキャビネットなどにしまわない
× 個人宛の伝言メモを誰でも見えるところにおく
× 起動中のパソコンを他の人が利用できる状態で席を離れる（パスワードによるロックをしない）

こんなこと、言われなくても…と思われるでしょうが、大事なことです。

業務上大切な書類や電子媒体、モバイル可能なパソコンを使わない時は、鍵のかかるキャビネットなどに保管するようにしましょう。

また、不特定多数の人たちの目に触れる場所には、情報資産を晒さないように心掛けましょう。

業務途中で席を離れる場合、コンピュータロックを実施するように心掛けましょう。

3．安易な廃棄禁止

業務に使用していたパソコンを安易に廃棄し、そこから情報漏えいしたということは、よく聞く話です。同様に、業務情報を格納したDVDや書類を、安易にゴミ箱に捨てたために情報漏えいしたというのも、よく聞く話です。

最近は、パソコンのハードディスクの内容を完全に消去するサービスや書類を安全に廃棄するサービスもありますので、このようなサービスを利用するか、事務所内で安全に廃棄するための手順等を確立し、それに従うようにしましょう。

重要な書類や電子媒体を、一般ゴミと一緒にポイ捨てするなど言語道断ということです。

4．不要な持ち込みの禁止

これも具体的な、やってはいけない例から考えてみましょう。

× 私物のパソコンやＵＳＢメモリを持ち込んで、事務所のネットワークに接続した（①）
× 業務に関係のないフリーウェアをインターネットからダウンロードして使用した（②）
× 許可してない無料のWebサービスを業務用のパソコンで使用した（③）

①私物の情報機器を持ち込むことの危険性

持ち込んだ私物のパソコンやUSBメモリがウイルス

に感染していた場合、事務所内の他のパソコンやサーバに、ウイルス感染を広げる可能性があります。また、不用意に重要な業務情報が保存されてしまい、意図せずに情報を持ち出してしまう危険性があります。

もし、私物のパソコンやUSBメモリを使用するのであれば、組合としての許可のもとで、組合としてのルールを守って使用してもらうようにしましょう。

②許可されていないソフトウェアの危険性

インターネットからダウンロードしたり、外部から持ち込んだりしたソフトウェアそのものが、ウイルスである可能性もあります。業務に関係のないソフトウェアの利用は慎むべきです。

どうしても、業務に必要なソフトウェアであるならば、事前にインターネットで評判を確認したり、安全な環境で動作確認を行ったりして、組合としての許可・管理のもとで利用をしましょう。

③許可されていないWebサービス利用の危険性

組合の重要な情報を、許可されていないオンラインストレージサービスを利用して保管したり、地図サービスや情報共有サービスを利用して情報管理したりする場合に、安易な設定ミスで情報漏えいが起こる可能性があります。

これらサービスを利用する場合は、サービスの仕組みや利用する上での設定方法をよく理解した上で、組合としての許可・管理のもとで利用をしましょう。

5．権限の貸し借り禁止

組合では、業務や体制に応じて担当者に権限が与えられます。いわゆる職権などがこれにあたりますが、この職権を他の人に貸与または譲渡することは、通常ありえません。

同様に、業務で使用する情報や機器にも、利用者権限が担当者毎に与えられています。担当者を識別するために設定されている利用者 ID やパスワードを共有したり、貸し借りしたりすることは、情報セキュリティ上、非常に大きな問題を引き起こす可能性があります。

また、貸し借りしなくとも、利用者IDやパスワードを忘れないように、パソコンに貼り付けておくことも、セキュリティ上良くない行為です。

権限には必ず責任が付いてきます。責任を果たすために、不注意とも思われる行為は慎みましょう。

6．業務上知り得た情報の公言禁止

そもそも、「業務上知り得た情報を口外しない」ことは守秘義務として、守ることが社会人としてのモラルです。部外者に秘密情報を進んでしゃべる人はいないと思いますが、ちょっとした気の緩みから情報漏えいを起こすことがあります。

例えば、以下のようなケースに心当たりはありませんか？

× 居酒屋で仕事の話を大声でしゃべる
× 不特定多数の人が集まる喫煙所で仕事の電話をする
× 電車の中で社外秘の書類の確認をする
× 業務に関係ないブログや掲示板に、仕事の話をアップする

悪意のある人はどこにいるか分かりません。偶然聞いた情報や盗み見た情報から、大きな情報漏えいへと発展するリスクがあります。自分が情報漏えい源にならないよう、このような行為は慎まなければなりません。

要するに、『壁に耳あり、障子に目あり』ということをお忘れなく、と言うことです。

7．情報漏えいを起こしたら、まず報告

気をつけていても、何らかのミスで情報漏えいを起こすこともあります。その場合、自分で判断せずに、まず上司に報告しましょう。

それから、組合のことだけでなく、情報を漏えいされた最終的な被害者、顧客、取引先、従業員等の関係者のことを考えて、速やかに事後対応を講じましょう。素早い対応によって、問題を最小限に止められる可能性が高まります。

以上、情報漏えい対策7つのポイントをご紹介しましたが如何でしたでしょうか？こんなの当然だよ、自分は気をつけているよという方も多かったのではないでしょうか。しかし、組合においては誰かひとりが情報漏えいを起こすと組合全体の責任になります。もし、あなたの組合にこのようなルールがなければ、あなたから提案してみてはいかがでしょうか。