モノプリ・ニュース！ 第26号

企業（組織）で働くあなたへ　7つのポイント！！

出典：IPA情報漏えい対策のしおり
https://www.ipa.go.jp/security/antivirus/documents/05_rouei.pdf

情報漏えい対策のしおり

本対策のしおりは、企業（組織）で働くあなたに、情報漏えい対策の7つのポイントを示すものです。
本来、企業（組織）として情報漏えい対策を行う場合は、それぞれの企業（組織）において、情報漏えい対策のセキュリティポリシーを策定し、それを守る必要があります。
あなたが、本対策のしおりで示す内容を守ってさえいれば、企業（組織）の大切な情報（データ）を漏えいさせないわけではありません。
本対策のしおりに示す7つのポイントは、あなたが企業（組織）で業務を遂行する上での、あなた自身が情報漏えいを起こさないために、あなたの心構えとしてお読み下さい。

1　企業（組織）の情報資産を、許可なく、持ち出さない

「大切な情報は持ち出さない」「仕事を家に持って帰らない」ということを大原則とすべきでしょう。
持ち出しの許可を得た場合であっても、

- 大切な情報を、管理下にないパソコン（例えばネットカフェのパソコン）で利用する
- 業務で持ち出したパソコンを、不必要に（あるいは無防備な状態で）、企業（組織）外のネットワークに接続する
- 業務で持ち出したパソコンを、業務以外の目的で利用したり、他人に貸したりする

など、安全が確認できない環境での情報資産の利用には注意が必要です。

2　企業（組織）の情報資産を、未対策のまま目の届かない所に放置しない

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、きちんと鍵のかかるキャビネットへ格納！！
また、業務途中で席を離れる場合、起動中のパソコンには、パスワードロックのできるスクリーンセーバーが動作するように設定するなど、習慣として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　企業（組織）の情報資産を、未対策のまま廃棄しない

企業（組織）内で業務に使用していたパソコンを、ハードディスクを消去しないまま廃棄し、そこから情報漏えいすることは、よく聞かれる話です。
重要な書類や電子媒体を、一般ごみと一緒にゴミ箱にポイ捨てするなど言語道断です！！

4　私物（私用）の機器やプログラム等のデータを、許可なく、持ち込まない

持ち込んだ私物（私有）のパソコンやUSBメモリなどの外部記録媒体がウイルスに感染していた場合は、企業（組織）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。そのウイルスがスパイウェアであった場合は、大切な業務情報がインターネットを通じて流出する可能性が考えられます。

5　個人に割り当てられた権限を、許可なく、他の人に貸与または譲渡しない

企業（組織）では、業務で使用する情報や機器に、利用者権限が担当者ごとに与えられています。つまり、利用者IDごとに利用権限が定義されていて、利用者IDはパスワードまたは個人認証で保護されます。これらの利用者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。

6　業務上知り得た情報を、許可なく、公言しない

最近よく聞く話題としては、ブログや掲示板の話があります。SNSを通じて、社会的なネットワークを構築するサービスを利用する人が増加したことにより、誰もが簡単に情報の発信者となり得ます。業務で知り得た情報を、自分ではカモフラージュして発信したつもりでも、インターネット上に散らばった各種の情報と組み合わせると、自分が業務を行っている企業（組織）に多大な迷惑をかける場合もあるようです。

7　情報漏えいを起こしたら、自分で判断せずに、まず報告

何らかの誤りで情報漏えいを起こしたり、あるいは情報漏えいを発見したりした場合は、自分で何とかしようとする前に、まず上司や管理者に報告し、自社の経営方針に基づき全体のバランスを考えながら被害の最小化を図ることが重要です。

京都府警察本部モノづくりプリザーブ事務局　075-451-9111（内線 5821）