In the Future 2013

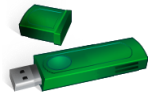
21 世紀型企業への転換を図る

■　情報管理の実効性を向上させるためには ？！ ③

～　組織的対応を強化！ ～

入社時と退職時の意識づけ　　？！

ＵＳＢメモリやＳＤカードなど大容量の記憶媒体が自宅でも日常的に使用されるようになりました。また、記憶媒体が小型・軽量化していることから、持ち運ぶことも簡単で、服のポケットにいつも入れておくことも可能です。



このような状況になると、各種情報を保存することに関する個人の危機意識が希薄となり、「とりあえず保存して…」といった安易な行動に何の問題も感じないようになってしまいます。企業としては、このような社員に対し、情報漏えい防止に向けた教育や情報管理ルールの徹底を図らなければなりません。まずは、入社時に秘密情報の範囲とその帰属、在職中・退職後の守秘義務、情報漏えい時の損害賠償といった事項について教育し、秘密保持誓約書を書かせることが重要です。

また、入社時に退職後の秘密保持を誓約させてはいるものの、これを理解できていない社員が少なくありません。退職時には改めて秘密保持誓約書を書かせ、守秘義務が継続することを認識させるようにしましょう。

情報の持ち出し　！

業務効率化のためには、モバイルＰＣやＵＳＢメモリが欠かせないビジネスツールとなります。

これらの使用について、入社時に“秘密保持誓約書”を提出しているから、あとは個人の判断に任せる、というわけにはいきません。

記憶媒体やデータを外部に持ち出す場合には、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施する必要があります。

◇ モバイルＰＣやＵＳＢメモリ等の使用や外部持ち出しについて、規程を定めておく。
◇ 外部でモバイルＰＣやＵＳＢメモリ等を使用する場合の紛失や盗難対策を講じておく。
◇ モバイルＰＣやＵＳＢメモリ等を外部に持出す際は、利用者の認証（ＩＤ・パスワード設定、ＵＳＢキーやＩＣカード認証等）を行うこと。
◇ 保存されているデータに、重要度に応じてＨＤＤ暗号化、ＢＩＯＳパスワード設定などの技術的対策を実施すること。
◇ ＰＣを持ち出す者、また持出しと返却の管理記録を作成すること。
◇ 盗難、紛失時に情報漏えいの恐れがある情報が何かを正確に把握するため、持ち出し情報の一覧および、内容を管理すること。

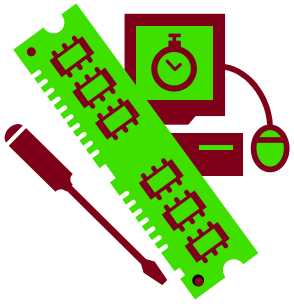
特にＵＳＢメモリについては、持ち出し前・返却の際にウイルスチェックを必ず実施するようにいたしましょう。個人所有の記憶媒体についても、使用を許可するのかしないのかなどの予めのルール作成が必要です。

社員採用時の適性診断実施 ⇒ ﾌﾘｰﾀﾞｲﾔﾙ 0120-81-4864

こんなトラブルが発生したら…　！

Ａ株式会社の営業部Ｂ社員が移動時間やちょっとした空き時間に営業報告を作成するため、私物のノートＰＣを業務に使用していました。
Ａ株式会社では、私物のＰＣを業務で使用することは禁止していましたが、Ｂ社員はその規定を知らなかった（もしかすると、知っていてやった）ようです。
ある日のこと、Ａ株式会社の総務部に、自社の顧客リストのファイルらしきものがＷｉｎｎｙで流れているとの通報が社外からありました。顧客リストの内容を確認すると、Ｂ社員の担当顧客のリストでした。
調査の結果、Ｂ社員の私物のノートＰＣにＷｉｎｎｙがインストールされており、さらにＰＣ内の情報を勝手にＷｉｎｎｙネットワークに放流するウイルスに感染していることがわかりました。

一例ですが、Ｂ社員のようなうっかりタイプは、どこの企業にもいるかもしれません。
Ｂ社員のようにならないようにするためには、次のような対策を確実に実行することがポイントです。以下の対策以外にも、それぞれの企業において必要十分な対策を講じるようにしなければなりません。
情報セキュリティに限らず、実質的に守ることができないような社内規定は、モラルハザードを引き起こす大きな原因となります。規定の形骸化は、規定の不備よりも有害な場合がありますので、全社員が確実に遵守できるような規程内容と運用ルールに見直す必要があります。
ウイルス対策やファイルシステムの暗号化等、必要な対策を強制できるように、業務で必要なＰＣ等の備品は、会社から支給貸与すること。私用ＰＣについては、家族が使用することも想定されるため、業務使用は厳禁とした方がよいかもしれません。



またまた、こんなトラブルが…　？！

Ｃ株式会社では、商品リストを顧客に送付するため、商品リストの印刷と併せて宛名ラベルの印刷をＤ印刷に依頼しました。Ｃ株式会社は、日頃からＤ印刷に発注しているため、いつものように顧客情報が入ったリストを電子メールでＣ印刷の担当者に送信しました。
Ｃ印刷では、誰でもログインできるＰＣにその情報を保存しました。
数日後、Ｄ印刷から連絡があり、Ｄ印刷のアルバイトがＣ株式会社の顧客情報を持ち出して、名簿業者に販売していたことが発覚しました。
Ｃ株式会社は、情報漏洩した顧客に連絡すると共に、謝罪文の作成・発表、監督官庁への報告等のため業務遂行に多大な支障を発生し、売り上げが減少するなど、企業業績に大きな打撃を受けてしまいました。

この事件は、Ｃ株式会社の法令遵守に対する意識の低さ、委託先管理の不十分さに尽きるといえます。情報セキュリティ事故の多くは、業務の委託先等において発生しているため、個人情報や営業秘密等を委託先に渡す場合については、何らかの管理が必要になる場合が多いと考えておきましょう。具体的対策については、『中小企業の情報セキュリティ対策ガイドライン』などが参考になります。

労使トラブル業種別診断サービス　⇒ http://www.iwaki-pmo.co.jp

情報セキュリティに対する組織的な取り組み　！！

情報セキュリティに組織的に取り組むうえで一番重要なことは、経営者の考えが社員に明確に示されているかどうかです。そして、その実現に向けて“どのようにすべきか”“責任は何か”が全社員に周知されていることだと思います。
そのためには、次の２つのポイントを起点として押さえておかなければなりません。

※ ***責任者として情報セキュリティと経営を理解する立場の人を任命すること。***
※ ***責任者は、各セキュリティ対策について（社内外を含め）、責任者、担当者それぞれの役割を具体化し、役割を決め、職責を確実に実行させる徹底すること。***

また、多数の社員が情報にかかわることになりますので、重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定めておく必要があります。
そして、全社員が決められたルールを逸脱するようなことがないように教育を行ない、行動を監視し、万が一、ルールから逸脱するような行動があった場合には、懲戒処分を行うという厳しさが必要です。
取引先については、情報の取り扱いに関する注意事項（※１）について、契約書に明記し、委託業務の際に取り交わす書面等に、情報の取り扱いに関する注意事項を含めましょう。

（※1）
システム開発を委託する際の本番データ利用時の際の情報管理、例えば管理体制や受託情報の取り扱い・受け渡し・返却、廃棄等について、注意事項を含めること。また、関係者のみにデータの取り扱いを制限することなど。

情報セキュリティに対するその他の重要項目をチェック　！！

数え上げればキリがありませんが、これまで本誌でご紹介いたしました事項のほか、特に重要なポイントを列記します。あくまでも一例ですので、“万が一”を想定して、現実的な対応をご検討ください。

- ☑ 重要な情報を保管したり、扱ったりする**場所の入退管理と施錠管理**を行っていますか？
- ☑ 重要なＰＣや配線は**地震などの自然災害**や、ケーブルの引っ掛けなどの**人的災害**に配慮し適切に**配置・設置**していますか？
- ☑ 重要な書類、モバイルＰＣ、記憶媒体などについて、整理整頓を行うと共に、**盗難防止対策**や**確実な廃棄**を行っていますか？
- ☑ ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行っていますか？
- ☑ 導入している情報システムに対して、最新のパッチを適用するなどの**脆弱性対策**を行っていますか？
- ☑ 通信ネットワークを流れる重要なデータに対して、**暗号化などの保護策**を実施していますか？インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISP サービス等）を行っていますか？
- ☑ 無線 LAN のセキュリティ対策（WPA2 の導入等）を行っていますか？
- ☑ ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行っていますか？
- ☑ 情報システムに障害が発生した場合、**業務を再開するため何をすべきか**を把握していますか？情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の**緊急時に、何をすべきか**を把握していますか？

労働基準監督署への是正報告対応　⇒　ﾌﾘｰﾀﾞｲﾔﾙ 0120-81-4864