平成28年1月より

マイナンバー制度が始まります③

たかはし労務コンサルタント事務所
社会保険労務士　所長
髙橋真悟

2回にわたりマイナンバーについてとりあげてきましたが、今回は**安全管理措置**についてです。

今回とりあげる安全管理措置とは、特別個人情報保護委員会から「特定個人情報の適正な取扱いに関するガイドライン」が公表されています。

企業規模によってどこまで対応できるのか判断が難しい点もありますが、基本的な考え方は共通です。

今回はその中でも物理的安全管理措置と技術的安全管理措置についてみてみましょう。

まず、「**物理的安全管理措置**」とは通常業務をする場所とマイナンバーの事務を行う場所（管理区域）を明確に隔てることです。もちろん管理区域にはマイナンバーの取扱担当者以外入ることができないようにしましょう。管理区域への入退室状況を記録しておくことも重要です。専用の部屋を用意しICカードや生体認証のシステムの導入を検討してもよいですが、コストの問題もあり難しいのではないかと思います。事務所の一部を壁や間仕切り等で区分け、入退室管理は管理簿などで記録する方法ではコストは抑えられるかもしれません。しかしシステムで強制的に管理されるわけではないのでルールが形骸化しないようより意識しなければなりません。

また、情報端末や関係書類の盗難・紛失を防ぐことも重要な物理的安全管理措置です。

施錠できる書庫に書類を保管し、情報端末等はワイヤーロック等で容易に持ち出されないよう対策を施しましょう。

さらに、盗難等の事故が発生した場合を考えデータの暗号化も重要な対策です。ファイルにパスワードをかけることは当然です。ハードディスク全体を暗号化するツールもあります。端末からハードディスクを取り外し、別の端末に取り付けたとしても読み取ることは難しくなります。USBフラッシュメモリも指紋認証やパスワードに対応しセキュリティーを意識したものがあります。マイナンバーに関するデータを持ち運ぶことがあるようでしたら導入の必要性は非常に高いでしょう。

次に、「**技術的安全管理措置**」を考えてみましょう。多くの企業で社内ネットワークを構築してプリンターやデータを共有しているかと思います。マイナンバーに関する情報は取扱担当者のみがアクセスできるようにしなければなりません。取扱担当者であってもユーザIDやパスワードを複数人で使いまわすようなことは誰がアクセスしたのか判別がつかなくなりますので、適切なアクセス制御とはいえません。つまり、誰がいつどの情報にアクセスしたのかを管理・記録することが重要です。専用システムでこれらの情報を管理している場合はシステムの改修も必要と考えたほうがよいでしょう。

インターネットに接続している場合は、今まで以上に外部からの不正アクセスに注意しなければなりません。ファイアウォールの設置やウイルス対策ソフトの導入、適切な設定等に加えて、疑わしいメールやウェブサイトは閲覧しないよう従業員教育も徹底しなければ防ぐことはできません。

企業の保持している情報を適切に管理することは、マイナンバーだけでなく継続的な事業活動をするうえで切り離すことができません。マイナンバーの導入をきっかけに情報管理のあり方について検討することは、非常に価値のあることといえるでしょう。

マイナンバー取扱者研修

平成27年8月27日　13時30分～16時30分
会員3080円　非会員4110円
講師　社会保険労務士　髙橋真悟